Characterization and implementation of robust quantum information processing

Swansea University
Prifysgol Abertawe

David Amaro

Department of Physics

Swansea University

Submitted to Swansea University in fulfilment
of the requirements for the degree of

Doctor of Philosophy

2020

Abstract

Quantum information processing has practical applications like exponential speed ups in optimisation problems or the simulation of complex quantum systems. However, well controlled quantum systems realised experimentally to process the information are sensitive to noise. The progress in leading experimental platforms like superconducting qubits or trapped ions has allowed the realisation of high-fidelity quantum processors known as Noisy Intermediate-Scale Quantum (NISQ) devices with roughly 50 qubits. NISQ devices are meant to be large enough to show, despite their imperfections, an advantage over classical processors in some computational tasks and provide a rich playground to prove principles for future quantum algorithms and protocols. However, quantum processors need to be scaled up to implement quantum algorithms that are relevant for practical applications. For this purpose, Quantum Error Correction (QEC) codes, which encode the information in multi-partite quantum states that are generally highly entangled, become crucial to eliminate the errors introduced by noise sources like qubit loss. Here we introduce a protocol to correct qubit loss, i.e., the impossibility to access the information encoded in a qubit, in the color code, a leading candidate for fault-tolerant quantum computation. We show that the achieved tolerance of $46(1)\%$ to qubit loss is related to a novel percolation problem on three coupled lattices. Our work shows the high robustness of the color under our protocol and has practical importance for implementations of fault-tolerant QEC. In our second line of research we propose and analyse local entanglement witnesses as efficient and platform-agnostic detectors of the entanglement between qubit subsystems, providing a description of the entanglement structure in, in principle, arbitrarily large quantum systems. Since entanglement is a genuinely quantum property used as a resource in most quantum algorithms, local witnesses, which can be implemented with current technology, are of interest for current and future quantum processors.

Authorship Declaration

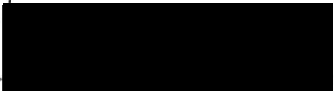The following people and institutions contributed to the publication of work undertaken as part of this thesis:

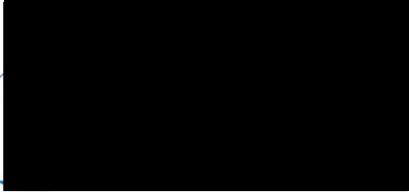|	**Name**	**Institutions**
Candidate	David Amaro	Department of Physics, Swansea University, Singleton Park, Swansea SA2 8PP, United Kingdom
Author 1 (PhD supervisor)	Markus Müller	Department of Physics, Swansea University, Singleton Park, Swansea SA2 8PP, United Kingdom
		Institute for Quantum Information, RWTH Aachen University, D-52056 Aachen, Germany
		Peter Grünberg Institute, Theoretical Nanoelectronics, Forschungszentrum Jülich, D-52425 Jülich, Germany
Author 2	Jemma Bennett	Department of Physics, Swansea University, Singleton Park, Swansea SA2 8PP, United Kingdom
		Department of Physics, Durham University, South Road, Durham DH1 3LE, United Kingdom
Author 3	Davide Vodola	Department of Physics, Swansea University, Singleton Park, Swansea SA2 8PP, United Kingdom
		Dipartimento di Fisica e Astronomia dell'Università di Bologna, I-40127 Bologna, Italy INFN, Sezione di Bologna, I-40127 Bologna, Italy
Author 4	Amit Kumar Pal	Department of Physics, Swansea University, Singleton Park, Swansea SA2 8PP, United Kingdom
		Faculty of Physics, University of Warsaw, ul. Pasteura 5, PL-02-093 Warszawa, Poland
		Department of Physics, Indian Institute of Technology Palakkad, Palakkad, 678557, India
Author 5	M.A. Martin-Delgado	Departamento de Física Teórica I, Universidad Complutense, 28040 Madrid, Spain

"Twins percolation for qubit losses in topological color codes", Davide Vodola, David Amaro, M.A. Martin-Delgado, and Markus Müller, *Physical Review Letters* 121, 060501 (August 2018) [1].

- Located in Chap. 4.

- Candidate contributions (30%): idea and design of the algebraic technique in Sec. 4.2.1 and Python scripts to run it, main contribution to drafting the supplemental material in Ref. [1], contribution to the manuscript.

- Author 1 contributions (20%): contribution to the original idea, supervision, critical revision of the manuscript.

- Author 3 contributions (40%): development of the main analytical and numerical work and Python scripts, main contribution to the manuscript.

- Author 5 contributions (10%): contribution to the original idea.

- We the undersigned agree with the above stated "proportion of work undertaken" for each of the above published peer-reviewed manuscripts contributing to this thesis:

Signed Candidate ... ████████████████ ....

Author 1 ... ██████████████ ....

Author 3 ... ████████████████ ....

Author 5 ... ██████████████████ ....

"Analytical percolation theory for topological color codes under qubit loss", David Amaro, Jemma Bennett, Davide Vodola, and Markus Müller, *arXiv* 1907.12084, (July 2019) [2].

- Located in Chap. [4].

- Candidate contributions (50%): derivation of the necessary and sufficient conditions for the existence of the logical information presented in Sec. [4.2.2], analytical derivation of the fraction of edges erased in Sec. [4.4], computation of the critical qubit loss rate as described in Sec. [4.3.1], contribution to the development of the Python scripts to run the algorithm described in Sec. [4.4.3], main contribution to the manuscript.

- Author 1 contributions (10%): main contribution to the original idea, main supervision, critical revision of the manuscript.

- Author 2 contributions (20%): main contribution to the development of the Python scripts to run the algorithm described in Sec. [4.4.3].

- Author 3 contributions (20%): numerical computation of the fundamental qubit loss rate as described in Sec. [4.3.2], supervision.

- We the undersigned agree with the above stated "proportion of work undertaken" for each of the above published peer-reviewed manuscripts contributing to this thesis:

Signed Candidate ....██████████.................................

Author 1 ██████████.................................

Author 2 ....██████████.................................

Author 3 .██████████.................................

v

"Estimating localizable entanglement from witnesses", David Amaro, Markus Müller, and Amit Kumar Pal, *New Journal of Physics* **20**, 063017 (2018) [3].

- Located in Chap. 5.

- Candidate contributions (50%): idea and derivation of the relation between local witnesses and localizable entanglement (LE) as described in Sec. 5.3.1, idea and derivation of the lower bound of LE using local witnesses as described in Sec. 5.3.2, study of the bound tightness for stabilizer-diagonal states as in Sec. 5.3.3, contribution to the original idea, contribution to the manuscript.

- Author 1 contributions (10%): contribution to the original idea, supervision, critical revision of the manuscript.

- Author 4 contributions (40%): idea and design of alternative techniques to estimate LE (not included in the thesis), contribution to the original idea, main contribution to the manuscript.

- We the undersigned agree with the above stated "proportion of work undertaken" for each of the above published peer-reviewed manuscripts contributing to this thesis:

Signed Candidate ....

Author 1 ....

Author 4 ....

"Scalable characterization of localizable entanglement in noisy topological quantum codes", David Amaro, Markus Müller, and Amit Kumar Pal, *arXiv* 1907.13161 (July 2019) [4].

- Located in Chap. 5.

- Candidate contributions (40%): algebraic algorithm to obtain a graph state from a stabilizer state as presented in Sec. 5.6.2 and Python script [5] to run the algorithm, modification of this algorithm to link any two qubits in the color code, analytical derivation of the dependence of LE with qubit distance as introduced in Sec. 5.7.1, contribution to the manuscript.

- Author 1 contributions (20%): main contribution to the original idea, supervision, critical revision of the manuscript.

- Author 4 contributions (40%): scripts to connect any two qubits with local complementation (LC) operations [6], numerical computation of LE with qubit distance as presented in Sec. 5.7.2, main contribution to the manuscript.
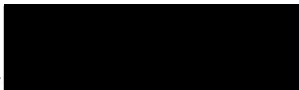
Signed Candidate ... ████████████ ....

Author 1 ..██████████ ....

Author 4 ... ██████████ ....

"Design and experimental performance of local entanglement witness operators", David Amaro, and Markus Müller, *arXiv* 1911.01144 (November 2019) [7].

- Located in Chap. 5.

- Candidate contributions (80%): idea and derivation of the direct method to construct local witnesses as introduced in Ref. 5.4.1, Python scripts to obtain and evaluate all local witnesses for the seven-qubit color code as in Sec. 5.5, study of robustness and comparison of the local witnesses proposed as described in Sec. 5.3.5, contribution to the original idea, main contribution to the manuscript.

- Author 1 contributions (20%): main contribution to the original idea, supervision, critical revision of the manuscript.

Signed Candidate . . ██████████ . . . .

Author 1 . . . ██████████ . . . .

Declaration

This work has not previously been accepted in substance for any degree and is not being concurrently submitted for any degree.

Signed: ... █████████████ .... (candidate)

Date: ...21/01/2020...

Statement 1

This thesis is the result of my own investigations, except where otherwise stated. Where correction services have been used, the extent and nature of the correction is clearly marked in a footnote(s). Other sources are acknowledged by footnotes giving explicit references. A bibliography is appended.

Signed: ... █████████████ .... (candidate)

Date: .....21/01/2020..

Statement 2

I hereby give consent for my thesis, if accepted, to be available for photocopying and for inter-library loan, and for the title and summary to be made available to outside organisations.

Signed: ... █████████████ .... (candidate)

Date: ......21/01/2020..

Contents

Acknowledgements

My thanks go to all those who have helped me through this work.

Firstly to my supervisor Markus Müller, who has dedicated time and effort to guide me in my work, my academic background, and my professional future. He has truly been an inspiration on how to lead and collaborate with a team in the most efficient and satisfying manner. Apart from being a great researcher, Markus is also a good friend.

Secondly, I would like to thank the present and past members of our group: Amit Kumar Pal, Davide Vodola, Mauricio Gutiérrez, Ciaran Ryan-Anderson, Farid Shahandeh, Alejandro Bermúdez, Jemma Bennett, Fernando Martínez and Pedro Parrado. The collaboration with some of them in various projects as well as the fruitful discussions with all of them have made me a better scientist. After all time together they are genuinely good friends. In the same line, I would like to thank PhD students and postdocs in the Physics Department for their friendship.

Third, thanks to the secretaries in the Physics Department and in the College of Science for guiding me through the tedious bureaucracy with efficiency and a kind smile. Similarly, thanks to Swansea University for hosting me as a PhD and providing all the additional elements that are necessary for a proper performance of any academic activity: the office, the cafeteria, the coffee machine...

Finalmente, gracias a Miriam por aguantarme y animarme cada día, en algunos períodos a pesar de la distancia. Gracias a mis padres, mi hermana, mi abuela y al resto de mi familia y amigos por su apoyo incondicional.

List of Figures

List of Tables

LIST OF TABLES

List of Abbreviations and Notation

Abbreviations

NISQ device	Noisy Intermediate-Scale Quantum device.
QEC	Quantum Error Correction.
MPS	Matrix Product State.
LE	Localizable Entanglement.
GHZ state	Greenberger–Horne–Zeilinger state.
CNOT gate	Controlled-NOT gate $U^{\mathrm{CNOT}}_{(q,q')}$.
CZ gate	Controlled-Z gate $U^{\mathrm{CZ}}_{\{q,q'\}}$.
LC	Local Complementation.
LOCC	Local Operations and Classical Communication.
CSS code	Calderbank-Steane-Shor code.
MDI	Measurement-Device-Independent.

Notation

q	label of the q-th qubit.
n	total number of qubits.
f	total number of faces in a lattice.
e	total number of edges in a lattice.
v	total number of vertices in a lattice.
k	number of encoded logical qubits.
$\{\ldots\}$	set with no particular ordering.
$(\ldots)$	ordered list.
$\boldsymbol{q}$	subset of qubits $\{q, q', \ldots\}$ with no particular ordering.
$\vec{\boldsymbol{c}}$	ordered list of qubits $(q_1, q_2, \ldots)$.
$\partial\boldsymbol{q}$	boundary: set of qubits linked to a qubit in $\boldsymbol{q}$.
$\mathbf{supp}(s)$	support of a Pauli operator s.
$\boldsymbol{f}$	set of the qubits in a face of a lattice.
$\boldsymbol{v}$	set of the qubits in a vertex of a lattice.
$\boldsymbol{s}$	set of the qubits in a string in the lattice.
$\boldsymbol{c}$	set of control qubits.
$\boldsymbol{t}$	set of target qubits.
$\boldsymbol{z}$	set of qubits where a phase gate is applied.
$\boldsymbol{\ell}$	loss instance: set of lost qubits.
$\boldsymbol{P}$	patch: the set of qubits at a certain distance from a qubit.
$\boldsymbol{r}$	removed qubits: set of lost and sacrificed qubits.
$\vec{\boldsymbol{\kappa}}$	correction: ordered list of sacrificed qubits.
$p_{\vec{\boldsymbol{\kappa}}}$	probability of the correction $\vec{\boldsymbol{\kappa}}$.
ℓ	number of lost qubits.
$\mathcal{F}$	subset of faces in a lattice.
w^{σ}	weight of a σ-type stabiliser.
w_{PF}	weight the support of a Pauli operator s that anticommutes qubit-wise with Z.
$\varkappa$	string of binary elements $\varkappa_i$.
$|\varkappa\rangle$	multi-qubit pure product state in the computational basis.
$\mathbb{e}$	binary string representing stabiliser excitations.
$\mathbb{m}$	binary string representing a measurement outcome.
$\Pi_{\mathbb{m}}$	projection operator corresponding to the outcome $\mathbb{m}$.
m_q	single-qubit Hermitian operator.
$\mathcal{M}$	local measurement basis: set of single-qubit Hermitian operators.
H	Hadamard gate.
S	phase gate.
T	T-gate.
$U^{\mathrm{CNOT}}_{(q,q')}$	controlled-NOT gate acting on the control qubit q and the target qubit q'.
$U^{\mathrm{CZ}}_{\{q,q'\}}$	controlled-Z gate acting on qubits q and q'.
$|\mathscr{S}\rangle$	stabiliser state.

$\lvert \mathscr{G} \rangle$	graph state.
F	state fidelity.
s	stabiliser operator.
g_q	graph-state generator associated to the qubit q.
S	subset of stabilisers.
$\mathcal{S}$	generator set of a stabiliser state.
$\mathcal{G}$	generator set of a graph state.
$\mathscr{S}$	stabiliser group.
$\mathscr{G}$	stabiliser group of a graph-state.
$\mathbb{S}$	generator set representation in the binary picture.
$\mathbb{G}$	generator set of a graph state represented in the binary picture.
$\mathbb{U}$	unitary operator representation in the binary picture.
$\mathbb{H}$	Hadamard gate representation in the binary picture.
$\mathbb{U}_S$	phase gate representation in the binary picture.
$\mathbb{F}$	binary matrix representing the faces in a lattice.
$\mathbb{s}$	binary column vector representing the qubits in a string $\boldsymbol{s}$.
$\tilde{M}(S)$	pseudo-incidence matrix of a stabiliser subset S.
$\mathcal{L}$	set of links $\{q, q'\}$ between nodes q, q' in a graph.
$G(\boldsymbol{N}, \mathcal{L})$	graph consisting in a set $\boldsymbol{N}$ of nodes and a set $\mathcal{L}$ of links.
d	shortest distance between two qubits in a lattice.
$\boldsymbol{n}_q$	neighbourhood represented by the set of nodes that neighbour the node q in a graph.
Γ	adjacency matrix of a graph.
$\mathbb{M}$	incidence matrix of a graph.
U_{LUE}	local unitary that transforms a stabiliser state into a LUE graph state.
$U_{\mathrm{LC}}^{(q)}$	LC unitary associated to the qubit q.
$U_{\mathrm{LC}}^{\vec{c}}$	sequence of LC unitary operators associated to the ordered list of qubits $\vec{c}$.
$\lvert \mathscr{G}^{\vec{c}} \rangle$	graph state under the action of $U_{\mathrm{LC}}^{\vec{c}}$.
$G(\boldsymbol{N}, \mathcal{L}^{\vec{c}})$	underlying graph of $\lvert \mathscr{G}^{\vec{c}} \rangle$.
$\mathbb{R}$	recombination matrix represented by a square binary matrix that is non-singular modulo 2.
r	Schmidt rank.
β_x	Schmidt coefficients labelled with an index x.
$\gamma_{\lvert \psi \rangle}$	square of the maximal Schmidt coefficient of a state $\lvert \psi \rangle$.
λ_i	i-th eigenvalue.
$\mathcal{E}(\rho)$	entanglement measure of a state ρ.
$\mathcal{E}_{\boldsymbol{q}}(\rho)$	LE of a state ρ on a qubit subsystem $\boldsymbol{q}$.
$\varepsilon(\rho)$	noise channel applied to a state ρ.
ε_{P}	local uncorrelated Pauli noise channel.
$\varepsilon_{\mathrm{BF}}$	bit-flip noise channel.
$\varepsilon_{\mathrm{PF}}$	phase-flip noise channel.
$\varepsilon_{\mathrm{DP}}$	depolarizing noise channel.
ε_{W}	white noise noise channel.

List of Abbreviations and Notation

p_f fundamental qubit loss threshold.

p_c critical qubit loss rate.

r_c bond-percolation threshold of a lattice.

$r(p)$ average fraction of edges erased as a function of the qubit loss rate p.

α_ℓ ℓ-th expansion coefficients of $r(p)$.

$\mathsf{R}_{\vec{\kappa}}$ number of edges erased due to correction $\vec{\kappa}$.

R_1 average number of edges erased from a shrunk lattice to correct a single-qubit loss.

$R_{\boldsymbol{\ell}}$ average number of edges erased to correct a loss instance $\boldsymbol{\ell}$.

$E_{\boldsymbol{\ell}}$ energy associated to the loss instance $\boldsymbol{\ell}$.

$\mathcal{I}$ set of all possible qubit loss instances.

$\mathcal{I}^{\text{(f-i)}}$ set of all fully-interacting qubit loss instances.

$\mathcal{I}^{\text{(f-i)}}_{q_1}$ set of all fully-interacting qubit loss instances that contain the qubit loss q_1.

$\bar{R}_\ell$ average number of edges erased by the loss instances in $\mathcal{I}^{\text{(f-i)}}_{q_1}$ with exactly ℓ losses.

$\bar{E}_\ell$ average energy of the loss instances in $\mathcal{I}^{\text{(f-i)}}_{q_1}$ with exactly ℓ losses.

$\epsilon_{\boldsymbol{\ell}}$ average effect of adding a qubit loss to the loss instance $\boldsymbol{\ell}$.

$\langle \epsilon \rangle_\ell$ average effect of adding a qubit loss to ℓ losses.

ε_ℓ mean-field effect of adding a qubit loss to ℓ losses.

ϱ_ℓ mean-field number of edges erased by ℓ qubit losses.

κ_ℓ mean-field number of corrections performed to correct ℓ qubit losses.

ς_ℓ mean-field number of sacrificed qubits to correct ℓ qubit losses.

Q label of the Q-th encoded qubit.

$W_{|\psi\rangle}$ standard genuine entanglement witness for a state $|\psi\rangle$.

$W^{\text{a}}_{|\mathscr{S}\rangle}$ alternative genuine entanglement witness for a stabiliser state $|\mathscr{S}\rangle$.

$W^{\text{2m}}_{|\mathscr{S}\rangle}$ two-measurement genuine entanglement witness for a stabiliser state $|\mathscr{S}\rangle$.

$W_{\boldsymbol{q}}$ local entanglement witness for a qubit subsystem $\boldsymbol{q}$.

$W^{\text{a}}_{\boldsymbol{q}}$ alternative local entanglement witness for a qubit subsystem $\boldsymbol{q}$.

$W^{\text{2m}}_{\boldsymbol{q}}$ two-measurements local entanglement witness for a qubit subsystem $\boldsymbol{q}$.

$W^{\mathscr{G}}_{\boldsymbol{q}}$ local entanglement witness for a qubit subsystem $\boldsymbol{q}$ prepared for a graph state.

$\mathcal{W}_{\boldsymbol{q}}$ subset of stabilisers to construct $W_{\boldsymbol{q}}$.

$\mathcal{W}^{\mathscr{G}\vec{c}}_{\boldsymbol{q}}$ subset of stabilisers to construct a local witness for the graph state $|\mathscr{G}^{\vec{c}}\rangle$.

$\mathcal{O}_{GHZ}$ operation that generates a GHZ state on a face of the color code.

l^{σ}_Q logical operator of Pauli type σ and corresponding to the encoded qubit Q.

D code distance.

$\lfloor \cdot \rfloor$ floor function.

$\lceil \cdot \rceil$ ceiling function.

$\langle t \rangle$ average time.

$\langle N_{\text{LC}} \rangle$ average number of LC operations performed.

Chapter 1

Introduction

Quantum systems, thanks to genuinely quantum properties like superposition and entanglement, can process information in ways that are not accessible by classical means as Feynman stated in 1981 [8]. He suggested the use of well controlled quantum systems to simulate the physics of entangled quantum matter, a computationally hard task for classical processors in general [9]. Nowadays, an impending milestone in quantum information processing from a fundamental point of view is to prove the "quantum supremacy" [10], i.e., to show that well controlled quantum systems can perform tasks beyond the reach of classical processors. From a practical point of view, multiple quantum algorithms and protocols that use quantum properties like superposition or entanglement as resources have been proposed to show some "quantum advantage" [11], i.e., to solve problems that are intractable for classical processors, or at least, provide a computational speed up.

Quantum metrology, for example, can provide a quantum advantage since the quantum entangled states employed provide quadratically better precisions than non-entangled states in the measurement of physical parameters [12]. Quantum cryptography allows theoretically secure communications because any eavesdropping can be detected given that, due to the no-cloning theorem [13], no information can be copied from a quantum channel without perturbing it [14, 15]. In the quantum algorithm zoo, there are quantum algorithms like Grover's algorithm [16] for database search that provide a quadratic speed up over any classical means. Other quantum algorithms like Shor's algorithm [17] for integer factorisation, solve problems that are (or believed to be) not efficiently solvable by classical processors. Moreover, quantum algorithms

1. INTRODUCTION

like boson sampling [18] or the sampling of random quantum circuits [19] are leading candidates to prove quantum supremacy since the problem size can be selected so classical computers cannot solve the problem in a reasonable time but they can be run in the small and noisy quantum processors with roughly 50 qubits or more that currently exist [20, 21] or will be available in the near future [22].

A quantum computer is an idealised device that can initialise, manipulate and measure quantum states in order to run quantum algorithms, and quantum computation is the branch of quantum information science that studies how information is processed in a quantum computer. The fundamental unit of information in a quantum computer is the *qubit*, a stable quantum system defined by two orthonormal states $|0\rangle$ and $|1\rangle$ that can be controlled individually, and can interact with other qubits in a controlled way. The quantum operations that control the qubit state and the interactions with other qubits are known as *quantum gates*. The gate set available to the quantum computer is a *universal gate set*, which can efficiently approximate any quantum process with an arbitrary precision [13]. Quantum algorithms, in the quantum circuit model of quantum computation, consist of the initialisation of a quantum state that is easy to prepare, the successive application of quantum gates, and the evaluation of observables through qubit measurement.

Experimentally, qubits have been realised in various platforms like trapped ions [23, 24], superconducting qubits [25], photons [26], cold atoms [27], or nuclear spins [28]. Two leading experimental platforms for quantum computation are trapped ions and superconducting qubits due to various features including high fidelity gates: with an error rate below 1 error per 100 two-qubit gates [29, 30]. With trapped ions each ion encodes a qubit into stable energy levels of the ion, quantum gates are realised through the interaction with laser light and the Coulomb interaction between ions, and qubit measurements are made through the fluorescence of short-lived states. Superconducting qubits are encoded into the two lowermost energy levels of an anharmonic oscillator generated by collective excitations in a superconducting resonant circuit with a Josephson junction, single-qubit quantum gates are performed with microwave pulses sent to a transmission line coupled to the qubits while two-qubit gates use a microwave cavity coupling two qubits, and qubit measurement can be done by detecting the change in the resonant frequency of a microwave resonator connected to the qubit.

The main difficulty that quantum computation faces is the unavoidable presence of decoherence in the experimental platforms, which produces errors that destroy the processed information. Errors happen during the state initialisation, measurement, and are introduced by the environment and faulty quantum gates. For example, the proximity of ions in the trap leads to crosstalk errors when a laser cannot address single ions perfectly, which produces an undesired effect on the neighbouring ions in the trap [31]. Besides, errors happen due to qubit imperfections like the presence of more than two accessible states, finite lifetimes, or the unavoidable coupling of an uncontrolled environment. For example, some types of superconducting qubits are sensitive to leakage errors due to their weak anharmonicity [32]. In a leakage error the population of a qubit leaks to states different from $|0\rangle$ and $|1\rangle$ that are usually not accessible, leading to a loss of information [33].

Current and near term quantum processors, also called Noisy Intermediate-Scale Quantum (NISQ) devices [11] consist of roughly 50 to 100 noisy qubits, where the best achieved error rate per two-qubit gate is below 1%. Despite their imperfections, NISQ devices provide a rich experimental playground for quantum algorithms and the study of well controlled quantum systems. Importantly, these processors are believed to be large enough to be impossible to simulate classically, so, in principle, quantum supremacy can be proven on them [34]. Recently, Google sampled a random quantum circuit in 200 seconds with their Sycamore quantum processor consisting of 53 superconducting qubits [20]. They estimated that a state-of-the-art classical supercomputer would need 10.000 years to realise the same task given the exponential time that classical algorithms require compared with quantum algorithms when sampling a random quantum circuit [34]. They claim that this result proves quantum supremacy, but it is still early to convince the quantum information community [35].

The amount of available resources in a NISQ device is limited, while noise sources cannot be completely removed. These limitations have motivated a new generation of quantum algorithms for the NISQ era based on hybrid quantum processors [36], consisting in the combined use of a parametrised quantum circuit and a classical computer. The quantum part consists of single-qubit and two-qubit gates with free parameters that are optimised by the classical part to minimise a cost function associated with the problem at hand. The process is repeated many times until the parameters converge to a minimum of the cost function. The main advantage of hybrid algorithms is that

the learning of the parameters is tailored to the actual noise in the experimental set up and the optimisation is carried by a classical processor, reducing the burden of the quantum part. Examples of hybrid quantum algorithms are the Quantum Approximate Optimisation Algorithm (QAOA) [37] for combinatorial optimisation problems, or the Variational Quantum Eigensolver (VQE) [38], which finds eigenvalues of multipartite quantum systems. There are also hybrid techniques to mitigate errors [39, 40] like the quantum variational error corrector (QVECTOR) algorithm, which optimises a parametrised quantum circuit to learn encoding and error-recovery circuits that extend the lifetime of a quantum state [41].

However, quantum processors need to be scaled up to solve problems that are large enough to have practical application. For example, with perfect qubits and gates, around 6000 perfect qubits would be necessary to factor an integer with 2048 used in current cryptographic techniques [42]. In the more realistic context, large quantum processors suffer noise. Quantum error mitigation techniques, despite being useful for NISQ devices, are not sufficient for larger quantum processors since errors are still present and affect the implementation of quantum algorithms. In contrast, using Quantum Error Correction (QEC) codes one can reduce the number of errors arbitrarily at the cost of making the quantum system even larger [43]. Using the example of integer factorisation, with current estimations of noise and platform limitations like only nearest neighbour interaction in superconducting qubits, around 20 million noisy qubits would be necessary to reduce the number of errors with QEC techniques [42]. Note that Shor's algorithm for integer factorisation is one of the most demanding quantum algorithms. The number of qubits required for implementing other quantum algorithms with the same assumptions is less.

In QEC codes, information is encoded redundantly in the joint, usually entangled, state of a multi-qubit system. The qubits that conform the system are usually called data qubits or physical qubits. Errors can be detected by a syndrome measurement that does not affect the encoded information, and corrected after a classical post-processing of the syndrome using a classical decoder algorithm [44, 45]. Quantum error correction codes are usually benchmarked under simple noise models and assumptions. At the highest level of simplification, the *code capacity channel* assumes local uncorrelated errors and perfect syndrome measurement. The *phenomenological model* takes into

account measurement imperfections, which are handled by repeating the syndrome extraction several times. The *circuit-based model* also takes into account that errors can happen at different intermediate steps of the quantum circuit for syndrome extraction and then proliferate through the circuit. Precisely those QEC codes that do not allow the uncontrolled proliferation of errors are called *fault-tolerant* codes and it has been shown that, as long as the error rate is below a certain threshold, logical quantum operations can be performed arbitrarily precise at the cost of a polylogarithmic overhead in size (number of qubits) and circuit depth (number of non-simultaneous gates) of the fault-tolerant QEC code [43, 46–48]. Then, large fault-tolerant QEC codes allow, in principle, error-free quantum computations. Fault-tolerant QEC codes can be constructed, for example, by concatenating codes in various levels such that the physical qubits forming a high-level code are logical qubits of codes at a lower level [49].

Topological QEC codes can also be made fault-tolerant [50]. These codes arrange physical qubits on lattices that can be embedded in various topologies like a torus or a two-dimensional surface with boundaries such that the code properties depend on the topology. Logical operators, which control the encoded information, have support on non-trivial cycles of the topology so they are highly non-local operators. In contrast, experimental errors are usually assumed to have local nature, so, on average errors tend to spread uniformly in the lattice. Provided this contrast, when the noise rate is low, the support of errors is, most likely, very different to the support of logical operators. Thus, the probability that experimental errors cause a logical error decreases exponentially with increasing code size [51]. The surface code [52] and the color code [53] are topological QEC codes and leading candidates for fault-tolerant quantum computation partially partially due to their high error thresholds. Numerical estimations of error rate thresholds with the circuit-based model are between 0.14% and 1% for the surface code [54–56] and between 0.082% and 0.2% for the color code [57–60]. They also have other desired properties like transversal quantum gates, i.e., logical gates that can be easily applied because they require only the simultaneous application of single-qubit physical gates on each qubit, and the syndrome extraction requires quantum gates only between neighbouring qubits, i.e., no long-range interaction is necessary to implement these gates in a two-dimensional experimental architecture.

Quantum error correction codes must protect the logical information from multiple noise sources. A particularly damaging error source is *qubit loss*. A qubit is lost when

the information in it can no longer be accessed due to a leakage process or the actual loss of the particle out of their trap. A number of protocols to detect and remedy the effect of qubit loss have been proposed and put in practice for trapped ions [61], superconducting qubits [32, 62–64], photons [65, 66], or quantum dots [67–69]. At the level of QEC codes, there are protocols [70, 71] to correct for the erasure channel, an error model where the position of the lost qubits is known. Some protocols [72, 73] correct the erasure channel by reinitialising the lost qubits in their computational space and then measuring the stabilisers, producing computational errors at known locations. Another approach consists of removing the lost qubits from the lattice and redefining the code space without the removed qubits. For the surface code, this protocol, which also extends to computational errors, was proposed in Refs. [74, 75]. As we describe in Sec. 4.1, by mapping the loss events to a percolation problem, it was shown that the surface code presents a tolerance against qubit loss of up to 50% in the absence of other sources of error. The correction of qubit losses in the color code has the additional difficulty, compared to the surface code, that the lattice must stay trivalent and face-three colourable after the code space redefinition. The determination of loss tolerance is of a practical importance for actual and future quantum processors as qubit loss is one of the noise sources of the existing physical platforms. In Chap. 4, we propose a protocol to correct qubit losses in the color code, a leading candidate to correct errors in quantum processors, and study the performance of the protocol.

Small instances of the surface and the color code have been implemented in two leading experimental platforms for quantum computation: trapped ions [76–78] and superconducting qubits [79, 80]. However, a fault-tolerant QEC code has not yet fully realised experimentally. As mentioned previously, in these platforms, gates present high fidelities: on average, less than 1 error per 100 two-qubit gates occurs. This error rate is at the verge of the error threshold for fault-tolerant quantum computation with the surface and color codes. So we are in a moment where the use of fault-tolerant QEC codes might be beneficial in comparison with using a single physical qubit, i.e., the state preparation, logical operations, measurement and lifetime of a logical qubit encoded with a QEC code might be improved over the corresponding operations applied directly to one physical qubit. Theoretical proposals include a fault-tolerant surface code consisting of 17 superconducting qubits (9 data qubits and 8 ancillary qubits for

syndrome extraction) [81], and fault-tolerant implementations of the seven-qubit color code with 2 to 6 extra qubits for syndrome readout [82–84].

In the long term, the scalability of experimental platforms needs to be further developed to take advantage of fault-tolerance. Superconducting qubits can be increased in number thanks to their modular design on two-dimensional chips that allows the necessary interactions for fault-tolerant QEC in the surface code [81]. However, difficulties to implement entangling gates between distant qubits or the reproducibility of the superconducting qubits during fabrication need to be addressed [30, 80]. Trapped ions platforms can be scaled up, by splitting the ions in various linear traps and entangling two ions in different traps by interfering the two photons emitted by the ions, or by including junctions in the trap and shuttling ions to the designated interaction zones where multi-qubit gates are applied [29]. At the theoretical level, efforts focus on the design of fault-tolerant codes that require less resources [85, 86].

At this stage of technology and for the near and long term future, the study and benchmarking of experimental realisations of a quantum processor becomes crucial. Entanglement is a key property to characterise since it is a genuinely "quantum" property that distinguishes classical from quantum processors. It is used as a resource, for instance, in measurement-based quantum computing [87, 88], quantum communication protocols [89, 90], and plays a crucial role in quantum algorithms and QEC. Tremendous technological developments have been made in the laboratory to realise entangled states with trapped ions [24, 91, 92], photonic systems [26, 93, 94], nuclear magnetic resonance molecules [95], superconducting qubits [25, 96], cold atoms [27, 97–99], solid-state systems [100], and set-ups involving hybrids of these systems [101, 102]. However, entanglement characterisation through tomographic techniques like compressed sensing [103–105] is feasible for small systems [106] but becomes impractical as the number of qubits in the system increases, due to the exponential growth of the Hilbert space. Two common approaches to overcome this difficulty are Matrix Product State (MPS) tomography [107–110], which efficiently reconstructs the state of systems close to matrix product states, and entanglement witnesses [111–113] which are observables that detect the presence of entanglement with a reduced number of measurements.

Entanglement witnesses have been developed for diverse scenarios, including multi-qubit states [114–116], continuous variable systems [117–119], thermal states [120–123],

7

high-dimensional states [124–127], or as a way of not only detecting, but also quantifying the amount of entanglement [128–131]. In the context of quantum communications, measurement-device-independent witnesses [132–135] can be used to prevent eavesdropping by certifying entanglement beyond measurement imperfections. With respect to the construction of witness operators, work has mainly focused on the decomposition of witnesses into Pauli operators [136, 137], or on reducing the number of required measurement settings [138, 139]. Most of the efforts are devoted to the detection of genuine entanglement, but there are also witnesses that detect the entanglement depth [140, 141], the entanglement with respect to partitions [142], or witnesses that provide information about the Schmidt number [143–145]. In Chap. 5, we propose, study and develop the necessary tools to construct local entanglement witness operators, which are platform-agnostic observables that detect entanglement (as we show they also estimate the amount of entanglement) in subsystems of qubits using a number of measurements that does not depend on the system size. With this information it is possible to answer e.g. whether qubits in a given subsystem or pairs of qubits are entangled. It also allows one to study the entanglement of the subsystem of interest coupled to an environment represented by the rest of qubits. In the preparation of complex many-qubit quantum states, such information may be useful to detect in which spatial regions and within which subsets of particles errors have occurred.

Moving away from the design, implementation and benchmarking of quantum processors and quantum algorithms, quantum information has shown connections with other fields in physics, like atomic, molecular and optical physics [146], condensed matter [147, 148], but also with computer science [13], and classical statistical mechanics. The connection between quantum information and classical statistical mechanics has proven to be fruitful in both directions [149–151]. On the one hand a connection between measurement-based quantum computation and classical spin models has been used to show that the partition function of the 2D Ising model can generate the partition functions of all classical spin models [152–155]. Furthermore, some quantum algorithms have proven to efficiently approximate the partition function of classical spin models [156–160]. On the other hand, problems in quantum information have found a solution through their connection with solvable classical statistical problems, for instance, to determine which quantum circuits can be efficiently simulated classically [161], or to provide the critical loss threshold of topological QEC codes as the

8

critical point of the order/disorder phase-transition of classical spin models [162, 163]. For instance, the 2D surface code [164] and the color code [53, 165] under computational (single-qubit bit and phase-flip) errors can be mapped to a 2D random-bond Ising model with two-body [166] and three-body interactions [167], respectively. Under computational errors and faulty stabiliser measurements, the surface code maps to a 3D random-plaquette lattice gauge model [168], while the color code maps to a 3D Ising lattice gauge theory [169]. This mapping was recently extended to account for circuit-level noise in the surface code [150]. In Chap. 4 we show the robustness of the color code to qubit loss via a connection with percolation theory: the tolerance of the color code to qubit loss under the protocol that we propose in this chapter is directly related to a novel bond-percolation problem in three coupled lattices.

The content of the thesis is structured as follows. In Chapter 2 we introduce basic concepts of multi-qubit systems and the notation employed. The concepts introduced range from single-qubit states and operations, to multi-qubit states like stabiliser and graph states, entanglement types and entanglement measures, and noise models. Stabiliser states are the playground where the tools and algorithms introduced are applied. Graph states serve in this thesis to create local entanglement witnesses and study their properties. Entanglement can be detected and estimated using these witnesses, so the main entanglement types and measures are introduced in this chapter. Finally, we present the noise models used in this thesis: the erasure channel, which is used to study the tolerance of the color code under qubit loss, and local uncorrelated Pauli noise channels, which are employed to benchmark the performance of local witnesses.

Chapter 3 introduces important concepts in QEC and defines topological codes like the surface and the color code. These codes are among the most promising candidates for fault-tolerant QEC. In this thesis we are interested in the tolerance of the color code against qubit loss, and we use an experimental realisation of this code to test the performance in practice of the local witness operators that we design.

In Chapter 4 we present the results obtained on the study of color codes under qubit loss. We propose a fully local and sequential protocol to correct qubit loss in the color code and study the performance of the code under our protocol. We show that the problem is directly related to a novel bond-percolation problem in three coupled lattices and use this connection to obtain analytical and numerical values of the tolerance. The

results are directly relevant for future implementations of the color code. The content of this chapter was first presented in the following references

- "Twins percolation for qubit losses in topological color codes", Davide Vodola, David Amaro, M.A. Martin-Delgado, and Markus Müller, *Physical Review Letters* **121**, 060501 (August 2018) [1],

- "Analytical percolation theory for topological color codes under qubit loss", David Amaro, Jemma Bennett, Davide Vodola, and Markus Müller, *arXiv* 1907.12684, (July 2019) [2].

Our protocol erases an average fraction $r(p)$ of edges from the color code lattice to correct a qubit loss rate p. This relation is used to obtain analytically the tolerance of the color code to qubit loss through the connection with percolation theory. In Sec. 4.4.4 I introduce a mean-field approximation of $r(p)$ that is not present in the previous papers and was derived individually by me.

Chapter 5 presents the work on local entanglement witnesses. We start by defining these observables and providing an interpretation of the type of entanglement that they detect. We show that local witnesses detect localisable entanglement (LE) and derive a lower bound of this quantity from the expectation value of a local witness. We propose two methods to construct local witnesses for a qubit subsystem of interest in a stabiliser state. All steps required to implement these methods, like the transformation of stabiliser states into graph states and the sequences of local-complementation operations, are described in detail. Then, we benchmark local witnesses in practice by applying them to an experimental realisation of the seven-qubit color code, and by studying the associated lower bound of LE as a function of the distance in noisy models of large color codes. Local witnesses and the tools developed here are of interest to efficiently characterise entanglement in the existing experimental platforms of multi-qubit systems. The work presented in this chapter is included in references

- "Estimating localizable entanglement from witnesses", David Amaro, Markus Müller, and Amit Kumar Pal, *New Journal of Physics* **20**, 063017 (2018) [3],

- "Scalable characterisation of localizable entanglement in noisy topological quantum codes", David Amaro, Markus Müller, and Amit Kumar Pal, *arXiv* 1907.13161 (July 2019) [4],

- "Design and experimental performance of local entanglement witness operators", David Amaro and Markus Müller, *Physical Review A* **101**, 012317 (accepted on December 2019 and published on January 2020) [7].

Finally, in Chapter 6 we summarise the results presented in the thesis, discuss the possible applications in the near and long term given the current status of quantum computation, and suggest possible improvements and extensions.

Chapter 2

Basics of multi-qubit systems

In this chapter we introduce basic concepts of quantum information that are ubiquitously used in this thesis. We start in Sec. 2.1 with fundamental concepts like qubits and quantum gates, continue in Sec. 2.2 with stabiliser and graph states, discuss entanglement measures in Sec. 2.4, and finish with noise models in Sec. 2.5. For the reader interested in the details, the book in Ref. [13] provides an instructive introduction to quantum information and quantum computation.

2.1 Qubits and quantum gates

In this section we define the basic constituents of a quantum computer, as well as the standard formalism behind them. The reader familiar with basic quantum information can jump to Sec. 2.2, where more complex concepts like stabiliser and graph states are described.

2.1.1 Qubit and single-qubit gates

The basic unit of information of a quantum computer is the qubit: an ideal quantum system with only two accessible states named $|0\rangle$ and $|1\rangle$. For example, the spin-up and the spin-down states of an electron can encode the $|0\rangle$ and $|1\rangle$ states, respectively. A qubit is the quantum analogue of a classical bit, but the qubit can be found in a state that is a quantum superposition of both states, consisting of a linear combination of $|0\rangle$ and $|1\rangle$

$$|\psi\rangle = \cos(\theta/2)|0\rangle + \sin(\theta/2)e^{i\phi}|1\rangle, \tag{2.1}$$

given by two angles $\theta \in [0, \pi]$ and $\phi \in [0, 2\pi]$. One can include a global phase $e^{i\gamma}$ as a factor multiplying the right-hand-side of the previous equation, but it is usually disregarded because it is undetectable. Qubit states belong to a Hilbert space $\mathcal{H}$, which is a complex two-dimensional vector space with an inner product. Each quantum state is represented by a vector in the Hilbert space:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \quad |\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}. \tag{2.2}$$

The Dirac notation $|\cdot\rangle$ is commonly used to represent vectors. The dual of a quantum state is denoted by $\langle\psi|$ in the Dirac notation and represents the complex conjugated and transposed vector. The inner product between two quantum states $|\psi\rangle$ and $|\xi\rangle$, represented by $\langle\psi|\xi\rangle$, is the dot product of the vectors corresponding to $|\psi\rangle$ and $\langle\xi|$. Thus, two quantum states are orthogonal if $\langle\psi|\xi\rangle = 0$. The norm of a vector in the Hilbert space is defined with respect to the inner product as $\|\psi\|_2 = \sqrt{\langle\psi|\psi\rangle}$. The set $\{|0\rangle, |1\rangle\}$ is the computational basis of a qubit, which is an orthonormal basis since $\langle 0|0\rangle = \langle 1|1\rangle = 1$ and $\langle 0|1\rangle = \langle 1|0\rangle = 0$.

Four particularly important superposition states of a qubit are:

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \qquad |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle), \tag{2.3}$$

$$|+_Y\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i\,|1\rangle) \quad |-_Y\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i\,|1\rangle). \tag{2.4}$$

When measured, these states return the output 0 or 1 with equal probability. The three sets of states, the computational basis $\{|0\rangle, |1\rangle\}$, the X-basis $\{|+\rangle, |-\rangle\}$, and the Y-basis $\{|+_Y\rangle, |-_Y\rangle\}$ form orthonormal bases of the Hilbert space $\mathcal{H}$. Thus, any state in $\mathcal{H}$ can be represented as a normalised linear combination of the two elements in a basis. It is illustrative to view these bases as three perpendicular axes in a three-dimensional space. The first element of each basis corresponds to a unit vector parallel to the axis, while the second element is antiparallel to the axis. The rest of states in the Hilbert space can be seen as unit vectors in the Bloch sphere: a sphere of radius 1 in the three-dimensional space (see Fig. 2.1 for an illustration of the Bloch sphere).

Three possible bases of the Hilbert space consist of the two eigenstates of a Pauli
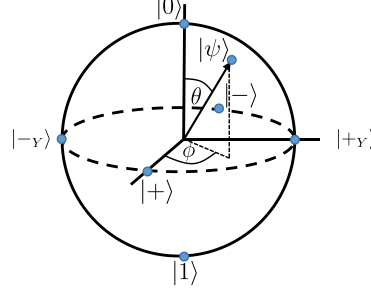
Figure 2.1: Bloch sphere. Representation of the single-qubit state $|\psi\rangle$ as a unit vector on the sphere of radius 1. The two angles θ and ϕ that define the quantum state can be seen as the spherical coordinates defining the unit vector. The computational basis $\{|0\rangle, |1\rangle\}$, the X-basis $\{|+\rangle, |-\rangle\}$, and the Y-basis $\{|+_Y\rangle, |-_Y\rangle\}$ are unit vectors along the three perpendicular axes.

operator from $\{X, Y, Z\}$ with eigenvalues $+1$ and -1:

$$Z|0\rangle = |0\rangle \qquad Z|1\rangle = -|1\rangle, \tag{2.5}$$

$$X|+\rangle = |+\rangle \qquad X|-\rangle = -|-\rangle, \tag{2.6}$$

$$Y|+_Y\rangle = |+_Y\rangle \quad Y|-_Y\rangle = -|-_Y\rangle. \tag{2.7}$$

The action of a Pauli operators on a different basis flips the state:

$$X|0\rangle = |1\rangle \quad X|1\rangle = |0\rangle, \tag{2.8}$$

$$Z|+\rangle = |-\rangle \quad Z|-\rangle = |+\rangle, \tag{2.9}$$

and analogously for Y and $\{|+_Y\rangle, |-_Y\rangle\}$ but with an additional global phase $\pm i$. Their matrix representations are:

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad (2.10)$$

where I is the identity operator. Pauli operators $\sigma \in \{X, Y, Z\}$ are involutory operators $\sigma^2 = I$, have vanishing trace $\text{tr}(\sigma) = 0$, anti-commute $\{\sigma^{(i)}, \sigma^{(j)}\} = 2\delta_{ij}I$ (here δ_{ij} is the Kronecker delta), and satisfy the following commutation relation:

$$[\sigma^{(i)}, \sigma^{(j)}] = 2i\epsilon_{ijk}\sigma^{(k)}, \tag{2.11}$$

where ϵ_{ijk} is the Levi-Civita symbol and we use the notation $\sigma^{(1)} = X$, $\sigma^{(2)} = Y$

2. BASICS OF MULTI-QUBIT SYSTEMS

and $\sigma^{(3)} = Z$. The set containing all operators resulting from the multiplication of single-qubit Pauli operators is the Pauli group of a qubit:

$$\mathcal{P} = \langle X, Y, Z \rangle = \{\pm I, \pm iI, \pm X, \pm iX, \pm Y, \pm iY, \pm Z, \pm iZ\}. \tag{2.12}$$

Here $\langle \cdot \rangle$ indicates the group generated by all possible products of elements.

The set of unitary operators U on a qubit state, i.e., with an inverse that equals the adjoint operator (transposed and conjugated) $U^{-1} = U^\dagger$, forms the $SU(2)$ group. Single-qubit unitary operators are exponentiations of Pauli operators: consider a real unit vector $\vec{r}$ and a vector composed by the Pauli operators $\vec{\sigma} = (X, Y, Z)$, then any element of $SU(2)$ can be written as

$$R_{\vec{r}}(\gamma) = e^{-i\frac{\gamma}{2}\vec{r}\vec{\sigma}} = \cos(\gamma/2)I - \sin(\gamma/2)\,i\,\vec{r}\vec{\sigma}, \tag{2.13}$$

where $\vec{r}\vec{\sigma}$ is the dot product of these two vectors and $\gamma \in [0, 2\pi]$ is an angle. They perform single-qubit rotations because, when applied to a qubit state represented by a unit vector in the Bloch sphere, the resulting state is represented by a another unit vector that has been rotated an angle γ around the direction parallel to $\vec{r}$. Note that Pauli operators also belong to $SU(2)$ and correspond to $\gamma = \pi$ rotations (up to a global phase) around the three orthogonal axes: $\vec{r} = (1, 0, 0)$ for X, $\vec{r} = (0, 1, 0)$ for Y, and $\vec{r} = (0, 0, 1)$ for Z.

Other important unitary operators are the Hadamard gate H, the phase gate S, and the T gate:

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, \quad T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}. \tag{2.14}$$

The Hadamard gate rotates the computational basis $\{|0\rangle, |1\rangle\}$ into the X-basis $\{|+\rangle, |-\rangle\}$ and vice-versa:

$$H|0\rangle = |+\rangle, \quad H|1\rangle = |-\rangle, \quad H|+\rangle = |0\rangle, \quad H|-\rangle = |1\rangle. \tag{2.15}$$

The phase gate is a $\pi/2$ rotation around the Z axis (up to a global phase) $R_Z(\pi/2) = \exp(-i\pi/4\,Z)$ that rotates the X-basis into the Y-basis $\{|+_Y\rangle, |-_Y\rangle\}$. These two gates, as well as Pauli operators, belong to the Clifford group, which is the group of unitary

operators that map Pauli operators into Pauli operators:

$$H\sigma H^\dagger, S\sigma S^\dagger \in \mathcal{P} \quad \forall\, \sigma \in \{X, Y, Z\}. \tag{2.16}$$

In contrast, the T gate, which is a $\pi/4$ rotation around the Z axis (up to a global phase) is a non-Clifford gate because it does not map all Pauli operators to Pauli operators: $T\sigma T^\dagger \notin \mathcal{P}$ for $\sigma \in \{X, Y\}$.

When a qubit in the state in Eq. (2.1) is measured in the computational basis, only two outcomes are possible: $+1$ or -1, corresponding to the states $|0\rangle$ and $|1\rangle$, respectively. The probability to obtain $+1$ is $\cos^2(\theta/2)$ and the probability of obtaining 1 is $\sin^2(\theta/2)$, which add up to 1 as expected. Qubits can be measured in a basis given by a Hermitian operator m, i.e., with $m^\dagger = m$, and get projected into the eigenspace of m corresponding to the resulting outcome ± 1. This projection is represented by a projector, which is an operator

$$\Pi_{\mathbb{m}} = \frac{I + (-1)^{\mathbb{m}} m}{2}, \tag{2.17}$$

where $\mathbb{m} = 0$ if the measurement outcome is $+1$ and $\mathbb{m} = 1$ if the measurement outcome is -1.

2.1.2 Multi-qubit states, Pauli group and two-qubit gates

The pure state of a quantum system with n qubits is a vector in the 2^n-dimensional Hilbert space $\mathcal{H}^{\otimes n}$, which is 2^n-dimensional vector space spanned by 2^n orthonormal vectors $|\mathbb{x}\rangle$ (with $\langle \mathbb{x}|\mathbb{y}\rangle = \delta_{\mathbb{x},\mathbb{y}}$), labelled by n-bit binary strings $\mathbb{x}$. Any pure quantum state of the system can be represented by a normalised linear combination of the elements in the computational basis, with complex coefficients $\alpha_{\mathbb{x}}$:

$$|\psi\rangle = \sum_{\mathbb{x}} |\mathbb{x}\rangle. \tag{2.18}$$

Examples of multi-qubit states are the Bell state for two qubits, and the generalisation for n qubits: the GHZ state (Greenberger–Horne–Zeilinger) [170], which are represented, respectively, by

$$|B\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \quad |\text{GHZ}\rangle = \frac{1}{2^{n/2}}(|00\cdots 0\rangle + |11\cdots 1\rangle), \tag{2.19}$$

where the first string in the GHZ state contains n zeros, and the second contains n ones. These states are genuinely entangled as we describe in Sec. 2.4.

Two states $|\psi\rangle$ and $|\psi'\rangle$ are said to be *local-unitary equivalent* (LUE) states if they differ in a local unitary operation: $U_{\text{LUE}}|\psi\rangle = |\psi'\rangle$. A local unitary is a tensor product of single-qubit unitary operators U_q on qubits $q = 1, \ldots, n$: $U_{\text{LUE}} = \bigotimes_{q=1}^{n} U_q$.

The Pauli group $\mathcal{P}^{\otimes n}$ of the quantum system is the tensor product of n Pauli groups. For two qubits, the Pauli group is:

$$
\begin{aligned}
\mathcal{P}^{\otimes 2} &= \langle X_1, Y_1, Z_1, X_2, Y_2, Z_2 \rangle \\
&= \{ I_1 I_2, X_1 I_2, Y_1 I_2, Z_1 I_2, I_1 X_2, X_1 X_2, Y_1 X_2, Z_1 X_2, \\
&\quad\; I_1 Y_2, X_1 Y_2, Y_1 Y_2, Z_1 Y_2, I_1 Z_2, X_1 Z_2, Y_1 Z_2, Z_1 Z_2, \ldots \},
\end{aligned}
\tag{2.20}
$$

where the elements that are not specified are simply the ones written multiplied by factors -1 and $\pm i$. Note that we have omitted the tensor product symbol and added labels 1 and 2 representing the qubit where the Pauli operator has support. The computational basis is formed by the eigenvectors of the Pauli operator $Z^{\otimes n} \in \mathcal{P}^{\otimes n}$.

Particularly important two-qubit operators are the controlled-not (CNOT) gate and the controlled-Z (CZ) gate, whose respective forms are:

$$
U_{(q,q')}^{\text{CNOT}} = \frac{I_q + Z_q}{2} I_{q'} + \frac{I_q - Z_q}{2} X_{q'},
\tag{2.21}
$$

$$
U_{\{q,q'\}}^{\text{CZ}} = \frac{I_q + Z_q}{2} I_{q'} + \frac{I_q - Z_q}{2} Z_{q'}.
\tag{2.22}
$$

The CZ gate is preserved under the exchange of q and q', so we use the set notation $\{q, q'\}$ to denote that none of the qubits plays a particular role. In contrast, the CNOT gate is not preserved by the exchange of the qubits where it has support, so we use the list notation (q, q') to denote that the role of these qubits is different: the first qubit in the list is the *control qubit*, while the second is the *target qubit*. When acting on the computational basis the CNOT gate flips the target qubit if the control qubit is in a $|1\rangle$ state and preserves the state otherwise:

$$
U_{(q,q')}^{\text{CNOT}} |\varkappa_q \varkappa_{q'}\rangle = |\varkappa_q (\varkappa_{q'} + \varkappa_q)\rangle,
\tag{2.23}
$$

where the sum is performed modulo 2. Thus, when applied to the product state $|+_q 0_{q'}\rangle$ the CNOT gate produces the Bell pair $|B\rangle$ in Eq. (2.19). Analogously, the CZ gate

adds a relative phase ± 1 that depends on the second qubit, if the first qubit is in $|1\rangle$, and preserves the state otherwise:

$$U_{\{q,q'\}}^{\text{CZ}} |\varkappa_q \varkappa_{q'}\rangle = (-1)^{\varkappa_q \varkappa_{q'}} |\varkappa_q \varkappa_{q'}\rangle, \qquad (2.24)$$

where $\varkappa_q \varkappa_{q'}$ is the scalar product. When applied to the product state $|+_q +_{q'}\rangle$ the CZ gate creates an entangled state of two qubits:

$$U_{\{q,q'\}}^{\text{CZ}} |+_q +_{q'}\rangle = \frac{1}{2}(|0_q\, 0_{q'}\rangle + |0_q\, 1_{q'}\rangle + |1_q\, 0_{q'}\rangle - |1_q\, 1_{q'}\rangle). \qquad (2.25)$$

Note that these gates are Hermitian and differ in a Hadamard gate on the target qubit: $U_{\{q,q'\}}^{\text{CZ}} = H_{q'} U_{(q,q')}^{\text{CNOT}} H_{q'}$.

These two-qubit gates, like the Hadamard and the phase gate, transform Pauli operators into Pauli operators: $U_{(q,q')}^{\text{CNOT}} s U_{(q,q')}^{\text{CNOT}} \in \mathcal{P}^{\otimes n}$ and $U_{\{q,q'\}}^{\text{CZ}} s U_{\{q,q'\}}^{\text{CZ}} \in \mathcal{P}^{\otimes n}$ for any Pauli operator $s \in \mathcal{P}^{\otimes n}$, so they belong to the Clifford group. The Clifford group can be generated by the Hadamard gate, the phase gate and the CNOT gate. The Gottesman-Knill theorem states that the Clifford group can be efficiently simulated by classical processors [171], so any quantum advantage requires at least a non-Clifford gate like the T-gate.

Moreover, the Solovay-Kitaev theorem [13] states that using only a discrete set of gates called a *universal gate set*, one can efficiently approximate any unitary gate. A possible universal gate set consists of the Hadamard gate H, the T-gate, and the CNOT gate. For this set, any single-qubit unitary can be approximated to a precision $\epsilon \in [0,1]$ with $\mathcal{O}(\log^c(1/\epsilon))$ gates from the universal set, where $c \approx 2$.

2.1.3 Density matrix and local projective measurements

The state of a quantum system might not be completely known. For example, the state of a qubit can be $|+\rangle$ with a probability p_+ or $|-\rangle$ with a probability p_- (with $p_+ + p_- = 1$). Our ignorance about any quantum state of an n-qubit system can be described by a statistical ensemble of orthonormal states $\{|\psi_x\rangle\}$ labelled by some index x, such that the quantum state of the system is $|\psi_x\rangle$ with a probability p_x (with $\sum_x p_x = 1$). The state is represented by the density matrix

$$\rho = \sum_x p_x |\psi_x\rangle \langle\psi_x|. \qquad (2.26)$$

2. BASICS OF MULTI-QUBIT SYSTEMS

The density matrix is said to be diagonal in the basis $\{|\psi_x\rangle\}$. When expressed in the computational basis, or any other orthonormal basis of the Hilbert space different from $\{|\psi_x\rangle\}$, the density matrix is not diagonal in general:

$$\rho = \sum_{\mathrm{x},\mathrm{y}} c_{\mathrm{x},\mathrm{y}} |\mathrm{x}\rangle \langle \mathrm{y}|, \tag{2.27}$$

where $c_{\mathrm{x},\mathrm{y}}$ are complex coefficients. In any basis, the density matrix has trace equal to one: $\mathrm{tr}(\rho) = 1$, and is a positive operator (non-negative eigenvalues).

The fidelity between two quantum states evaluates how similar they are. The fidelity $F = \langle \psi | \rho | \psi \rangle$ between a pure state $|\psi\rangle$ and a (generally) mixed state ρ is a non-negative value that ranges from 0 for orthogonal states to 1 for identical states. The fidelity between a state $|\psi\rangle$ that is aimed to be produced in an experiment and the experimental state ρ that is actually produced serves as a benchmark figure of merit of the experimental performance.

One can determine the value of observables from quantum states. An observable is a Hermitian operator O (with $O^\dagger = O$ and real eigenvalues) with an expectation value $\langle O \rangle_\rho = \mathrm{tr}(\rho O)$ that can be evaluated on a quantum state ρ. Pauli operators are observables with eigenvalues ± 1. The expectation value of a Pauli operator $s \in \mathcal{P}^{\otimes n}$ with support on the qubit is a weighted average of the eigenvalues:

$$\langle s \rangle_\rho = 1\, p_0 + (-1)\, p_1. \tag{2.28}$$

The weights p_0 and p_1 correspond to the probability of obtaining the outcomes $+1$ and -1, respectively, when s is measured in the state. They can be computed as

$$p_{\mathrm{e}} = \mathrm{tr}(\rho \Pi_{\mathrm{e}}), \tag{2.29}$$

where e is 0 or 1 and

$$\Pi_{\mathrm{e}} = \frac{I + (-1)^{\mathrm{e}} s}{2} \tag{2.30}$$

is the projector into the $(-1)^{\mathrm{e}}$ eigenspace of s. For a subset $S = \{s_1, s_2, \ldots\} \subset \mathcal{P}^{\otimes n}$ of commuting Pauli operators, one can also calculate the joint probability of obtaining a string of outcomes $(-1)^{\mathrm{e}_1}$, $(-1)^{\mathrm{e}_2}$, ... for each Pauli operator s_1, s_2, ..., respectively. The outcome is defined by a binary string e with $|S|$ elements (here $|\cdot|$ indicates the

set cardinality):

$$p_{\mathbb{e}} = \mathrm{tr}(\rho \Pi_{\mathbb{e}}) \,, \quad \Pi_{\mathbb{e}} = \prod_{s \in S} \frac{I + (-1)^{\mathbb{e}_s} s}{2}, \tag{2.31}$$

where $\mathbb{e}_s$ is the binary element of the string $\mathbb{e}$ corresponding to the Pauli operator s.

When the Pauli operators in single-qubit Pauli operators σ_q acting on a subset $\bar{q} = \{q_1, q_2, \ldots\}$ qubits, the measurement $\mathcal{M}_{\bar{q}} = \{\sigma_q : q \in \bar{q}\}$ is called a *local measurement*. The probability of obtaining an outcome $\mathbb{m}$ of the $|\bar{q}|$ Pauli operators and the corresponding projector $\Pi_{\mathbb{m}}$ are described by Eq. (2.31). The quantum state after the projective measurement process is the *reduced state*, which is a generally mixed state with support only on the set of qubits q outside $\bar{q}$ (the $(\bar{\cdot})$ symbol indicates the complementary subset):

$$\rho_{q}^{\mathbb{m}} = \frac{\mathrm{tr}_{\bar{q}}\left(\rho \Pi_{\mathbb{m}}\right)}{\mathrm{tr}\left(\rho \Pi_{\mathbb{m}}\right)}. \tag{2.32}$$

Here $\mathrm{tr}_{\bar{q}}(\cdot)$ indicates the partial trace with respect to the subset of qubits $\bar{q}$. The important property of local measurements for this work is that they do not create entanglement; $\rho_{q}^{\mathbb{m}}$ is entangled only if q is entangled in the state ρ.

2.2 Stabiliser and graph states

Stabiliser states are an important class of multi-qubit quantum states that are broadly employed in quantum computation and QEC. Stabiliser states alone cannot provide any quantum advantage since the Gottesman-Knill theorem shows that stabiliser circuits (quantum circuits consisting of Hadamard, phase, CNOT gates, and single-qubit measurements), which can realise all stabiliser states, can be efficiently simulated by classical processors [171]. However, stabiliser states present a simple structure exploited in the stabiliser formalism to simplify the study of these states by keeping track of the stabiliser operators (Pauli operators defining the states) rather than on their vector representations. Given their simple structure, they have been the object of multiple analyses of entanglement [172] and used as a resource for quantum information processing [173]. For example, they lie at the heart of stabiliser codes [171], a broad class of QEC codes with some leading candidates for fault-tolerant quantum error correction (QEC). A particular class of stabiliser states known as *graph states* has a structure based on an underlying graph. Graph states are introduced in Sec. 2.2.2. Furthermore, graph states generate the entire set of stabiliser states with local unitary operators [174],

so they can be used as a representation of the entire set of stabiliser states. For example, in Chap. 5 we use properties of graph states, preserved by local unitary operators, to demonstrate properties of stabiliser states. Graph states are used as a resource in measurement based quantum computation [175, 176] or in quantum communication protocols that exploit their entanglement properties [177].

2.2.1   Stabiliser states

An n-qubit *stabiliser state* is defined by a *generator set* $\mathcal{S} \subset \mathcal{P}^{\otimes n}$ containing n commuting and independent Pauli operators, called *generators*, with eigenvalues ± 1. Here, the independence means that no generator in $\mathcal{S}$ is equal to the product of other generators in $\mathcal{S}$, or equivalently, that no product of different generators in $\mathcal{S}$ produces the identity operator. The stabiliser state $|\mathscr{S}\rangle$ is the joint $+1$ eigenspace of the generators $s \in \mathcal{S}$:

$$s\,|\mathscr{S}\rangle = |\mathscr{S}\rangle \,, \quad \forall\, s \in \mathcal{S}. \tag{2.33}$$

The set containing all the 2^n products of generators in $\mathcal{S}$, denoted by $\langle\mathcal{S}\rangle$ is the *stabiliser group* $\mathscr{S}$. The elements of the stabiliser group, which includes the generators in $\mathcal{S}$, are called *stabiliser operators* or simply *stabilisers*. The density matrix representation of the stabiliser state is the projector into the $+1$ eigenspace of all generators in a generator set. The projector expands into a sum of all stabilisers:

$$|\mathscr{S}\rangle\langle\mathscr{S}| = \prod_{s\in\mathcal{S}} \frac{I+s}{2} = \frac{1}{2^n} \sum_{s\in\mathscr{S}} s. \tag{2.34}$$

For example, the three-qubit GHZ state $2^{-1/2}(|000\rangle + |111\rangle)$ (and any n-qubit GHZ state) is a stabiliser state. It is defined by the generator set $\mathcal{S} = \{s_1 = X_1 X_2 X_3,\, s_2 = Z_1 Z_2,\, s_3 = Z_2 Z_3\}$, which expands into the stabiliser group

$$\mathscr{S} = \{I,\, X_1 X_2 X_3,\, Z_1 Z_2,\, Z_2 Z_3,\, -Y_1 Y_2 X_3,\, -X_1 Y_2 Y_3,\, Z_1 Z_3,\, -Y_1 X_2 Y_3\}. \tag{2.35}$$

The same stabiliser group can be generated by multiple generator sets. Consider two different generator sets $\mathcal{S}$ and $\mathcal{S}'$ such that the generators s_i' in $\mathcal{S}'$ are products of the generators s_j in $\mathcal{S}$. Consider that the products are given by an invertible $n \times n$

binary matrix $\mathbb{R}$:

$$s'_j = \prod_{i=1}^{n} s_i^{\mathbb{R}_{ij}}, \tag{2.36}$$

where $\mathbb{R}_{ij} \in \{0,1\}$ for all $i,j = 1,2,\ldots,n$ and $s_i^0 = I$ while $s_i^1 = s_j$. Only if $\mathbb{R}$ is invertible the two generator sets define the same stabiliser group: $\langle \mathcal{S} \rangle = \langle \mathcal{S}' \rangle = \mathscr{S}$ and consequently, the same stabiliser state. For example, the generator set $\mathcal{S}$ of the three-qubit GHZ state introduced previously and the generator set $\mathcal{S}' = \{s_1, s_1 s_2, s_1 s_3\}$ differ in the invertible recombination determined by

$$\mathbb{R} = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}. \tag{2.37}$$

Usually stabiliser states have a particular generator set used to define the state because the generators in it present certain structure or symmetries. However, apart from their structure or symmetries, there is no particular reason to define the stabiliser state from a particular generator set instead of invertible recombinations of it.

From the expansion in Eq. (2.34) it becomes clear that computing fidelity of a stabiliser state requires the evaluation of all the 2^n stabilisers in the stabiliser group. This requires, in general, $\sim 2^n$ Pauli measurement settings. A Pauli measurement setting $\mathcal{M} = \{\sigma_q : q = 1, \ldots, n\}$ is a list of single-qubit Pauli operators, one for each qubit in the system, such that Pauli operators consisting of tensor products of only those Pauli operators can be evaluated by the repeated measurement of $\mathcal{M}$. Some stabilisers in the stabiliser group can be evaluated simultaneously with the same measurement setting. For example, the two Z-type stabilisers s_2 and s_3 of the three-qubit GHZ state, as well as the product $s_2 s_3$ can be evaluated simultaneously with the measurement setting $\mathcal{M} = \{Z_1, Z_2, Z_3\}$.

2.2.2   Graph states

A graph state is a stabiliser state that is defined on an underlying graph where each node corresponds to a qubit [177, 178]. Graph states are important for this thesis because graph states are simple to study given their underlying structure, and any stabiliser state can be converted into a graph state by means of a local-unitary operation [174],
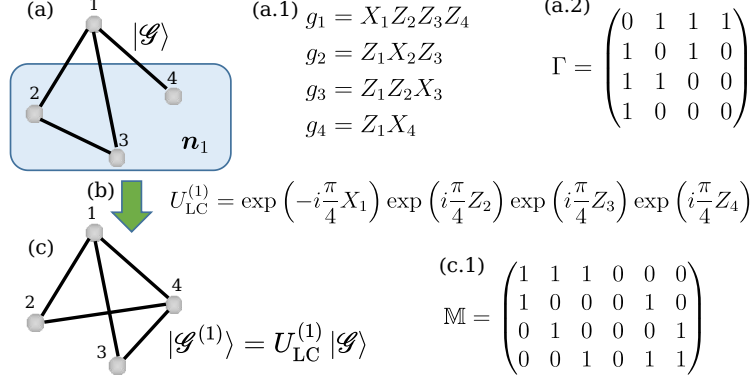
Figure 2.2: Graph state concepts. (a) Underlying graph of a 4-qubit graph state $|\mathcal{G}\rangle$, and neighbourhood $\boldsymbol{n}_1 = \{2, 3, 4\}$ of the node 1. (a.1) Graph state generators. (a.2) Adjacency matrix Γ. (b) Local complementation (LC) unitary $U_{\text{LC}}^{(1)}$ that realises a LC operation with respect to the qubit 1. (c) Graph defining the local-unitary equivalent (LUE) graph state $|\mathcal{G}^{(1)}\rangle$ obtained after applying $U_{\text{LC}}^{(1)}$. (c.1) Incidence matrix $\mathbb{M}$ of the local complemented graph.

which preserves the entanglement properties. Thus, we can study the entanglement of stabiliser states through the study of graph states.

An undirected graph $G(\boldsymbol{N}, \mathcal{L})$ consists of a set $\boldsymbol{N}$ of n nodes and a set $\mathcal{L}$ of links $\{q, q'\}$ between nodes. Provided the one-to-one correspondence between nodes and qubits, $\boldsymbol{N}$ also represents the set of all qubits, and during the rest of the thesis we, in the context of graph states, use the words "nodes" and "qubits" interchangeably. A graph $G(\boldsymbol{N}, \mathcal{L})$ with n nodes can be represented by an adjacency matrix Γ or an incidence matrix $\mathbb{M}$. The adjacency matrix is an $n \times n$ binary matrix with ones on the positions corresponding to linked nodes and zeros elsewhere:

$$\Gamma_{qq'} = \begin{cases} 1 & \text{if } \{q, q'\} \in \mathcal{L} \\ 0 & \text{otherwise} \end{cases}. \tag{2.38}$$

It is a symmetric matrix and has zeros on the diagonal (see example in Fig. 2.2(a.2)). The incidence matrix is an $n \times \binom{n}{2}$ matrix where each row represents a node and each column represents an existing or non-existing link ($\binom{n}{2}$ is the binomial coefficient and is equal to the number of node pairs):

$$\mathbb{M}_{ql} = \begin{cases} 1 & \text{if } q \in l = \{i, j\} \text{ and } l \in \mathcal{L} \\ 0 & \text{otherwise} \end{cases}. \tag{2.39}$$

Here l labels all pairs of nodes from 1 to $\binom{n}{2}$. Each column is either zero or has two ones on the rows corresponding to two linked nodes (see example in Fig. 2.2(c.1)). The order of the columns does not contain any relevant information.

A *disconnected component* in a graph is a subset of connected nodes that are disconnected from the rest of nodes, i.e., there is a path between any two nodes in the subset but there is no path between any node in the subset and the rest of nodes. The rank modulo 2 of the incidence matrix determines the number κ of disconnected components in the graph:

$$\operatorname{rank}(\mathbb{M}) = n - \kappa. \tag{2.40}$$

When $\kappa = 1$, the graph is fully connected. Note that the maximum rank modulo 2 of any incidence matrix is $n-1$ since there is always one constraint: the sum modulo 2 of all rows vanishes since columns have either two ones or none. Importantly, a graph state defined on an underlying graph with $\kappa > 1$ disconnected components is a product state of κ graph states, each one with support on a disconnected component, so there is no entanglement between the subsets of qubits corresponding to the different disconnected components.

This can be checked easily from the creation of a graph states using CZ gates. Graph states can be created from the product state $|+\rangle^{\otimes n}$ of n states $|+\rangle$ by the application of a CZ gate for each linked pair of nodes in the graph:

$$|\mathscr{G}\rangle = \left(\prod_{\{q,q'\}\in\mathcal{L}} U^{\mathrm{CZ}}_{\{q,q'\}} \right) |+\rangle^{\otimes n}. \tag{2.41}$$

The neighbourhood $\boldsymbol{n}_q$ of a node q is the subset of nodes that are linked to q. The n-qubit graph state is defined by a generator set $\mathcal{G}$ containing n generators $g_q \in \mathcal{P}^{\otimes n}$, one for each qubit q:

$$g_q = X_q \bigotimes_{q'\in\boldsymbol{n}_q} Z_{q'}. \tag{2.42}$$

Graph states can be transformed into LUE graph states by the action of a local-complementation unitary [177]. A *local complementation* (LC) unitary $U^{(q)}_{\mathrm{LC}}$ is defined with respect to a qubit q in a graph state $|\mathscr{G}\rangle$ as

$$U^{(q)}_{\mathrm{LC}} = \exp\left(-i\frac{\pi}{4}X_q\right) \prod_{q'\in\boldsymbol{n}_q} \exp\left(i\frac{\pi}{4}Z_{q'}\right). \tag{2.43}$$

When this LC unitary is applied on the graph state one obtains a LUE graph state $|\mathscr{G}^{(q)}\rangle = U_{\text{LC}}^{(q)}|\mathscr{G}\rangle$ with an underlying graph $G(\boldsymbol{N}, \mathcal{L}^{(q)})$. In $G(\boldsymbol{N}, \mathcal{L}^{(q)})$ the links between nodes in the neighbourhood of q are substituted by their complementary links. To be more precise, for every pair of nodes $r, t \in \boldsymbol{n}_q$ that are in the neighbourhood $\boldsymbol{n}_q$ of q, if the link $\{r, t\}$ is (is not) present in the first graph $\{r, t\} \in \mathcal{L}$ ($\{r, t\} \notin \mathcal{L}$), it is not present (it is present) in the new graph $\{r, t\} \notin \mathcal{L}$ ($\{r, t\} \in \mathcal{L}^{(q)}$). See Fig. 2.2 for an example of a unitary performing a LC operation on a graph state.

2.3 Binary picture

Here we provide a few essential details on the binary picture of the stabiliser formalism [177]. The binary picture is an algebraic formalism to represent stabiliser states and operations on them. It was used in Ref. [174] to prove the local-unitary equivalence of stabiliser and graph states, and we use it in this thesis to prove some results on stabiliser states and to provide an algebraic recipe that transforms a stabiliser state into a LUE graph state. In this formalism, stabiliser states are represented by their generator sets instead of a linear combination of state vectors in the computational basis.

In the binary picture, the single-qubit identity I and Pauli operators X, Y, Z are represented, respectively, by the column vectors

$$I \mapsto \begin{pmatrix} 0 \\ 0 \end{pmatrix}, X \mapsto \begin{pmatrix} 0 \\ 1 \end{pmatrix}, Y \mapsto \begin{pmatrix} 1 \\ 1 \end{pmatrix}, Z \mapsto \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \tag{2.44}$$

and the products of these operators are mapped to the sum of columns modulo 2. For example, the product $XY = iZ$ is represented by the sum modulo 2 of the second and third column, which results in the fourth column. Note that in the binary picture, the factors ± 1 and $\pm i$ multiplying a Pauli operator are disregarded.

A Pauli operator $s \in \mathcal{P}^{\otimes n}$ is represented by a $2n \times 1$ column vector where the single-qubit Pauli operator corresponding to a qubit q is represented by a 2×1 column vector like in Eq. (2.44) with the elements q and $q + n$ from the first column vector. For example, the Pauli operator $X_1 Z_2 I_3$ is represented by the column vector $(0\,1\,0\,|\,1\,0\,0)^{\text{T}}$ and X_1 is represented by the first (0) and fourth (1) elements as $(0\,|\,1)^{\text{T}}$. An n-qubit generator set $\mathcal{S}$ is defined by n independent and commuting generator operators $s \in \mathcal{P}^{\otimes n}$, so it is represented by a $2n \times n$ binary matrix $\mathbb{S}$ formed by n columns, each one

representing one generator. For example, the generator set $\mathcal{S} = \{X_1 X_2, Z_1 Z_2\}$ defining the two-qubit Bell pair is represented by

$$\mathbb{S} = \begin{pmatrix} 0 & 1 \\ 0 & 1 \\ 1 & 0 \\ 1 & 0 \end{pmatrix}. \tag{2.45}$$

To simplify the notation $\mathbb{S}$ is written as two $n \times n$ blocks

$$\mathbb{S} = \left(\frac{\mathbb{Z}}{\mathbb{X}} \right). \tag{2.46}$$

The j-th generator is represented by the j-th column, and the qubit q is represented by the rows $\mathbb{Z}_q$ and $\mathbb{X}_q$ in such a way that the column formed by two bits

$$\left(\frac{\mathbb{Z}_{qj}}{\mathbb{X}_{qj}} \right) \tag{2.47}$$

represents, as in Eq. (2.44), the operator from the set $\{I, X, Y, Z\}$ that is applied to the qubit q due to generator j.

Another important example is a graph state defined on an underlying graph represented by the $n \times n$ adjacency matrix Γ. The stabiliser description of the graph state is given in Sec. 2.2.2. Given that the neighbourhood $\boldsymbol{n}_q$ of qubit q includes the nodes corresponding to the non-vanishing elements of the q-th column of Γ, the representation of a graph state is completely defined by the adjacency matrix Γ as

$$\mathbb{G} = \left(\frac{\Gamma}{\mathbb{1}_n} \right), \tag{2.48}$$

where $\mathbb{1}_n$ is the $n \times n$ identity matrix.

In a stabiliser state, all generators are independent, implying that no product of them exists which equals to the identity operator. Since in the binary picture the product of Pauli operators is mapped to a sum modulo 2 of columns, all the columns of $\mathbb{S}$ must be linearly independent, or equivalently, $\mathbb{S}$ must be full rank modulo 2: rank$(\mathbb{S}) = n$. Moreover, an invertible recombination of the generators operators like in Eq. (2.36) is given by an invertible $n \times n$ binary matrix $\mathbb{R}$ that multiplies $\mathbb{S}$ from the right. Finally, the commutation of the generator operators defining a stabiliser state is

guaranteed by the relation $\mathbb{S}^{\mathrm{T}}\mathbb{D}\mathbb{S} = 0$, where $\mathbb{D}$ is the $2n \times 2n$ matrix

$$\mathbb{D} = \left(\begin{array}{c|c} 0 & \mathbb{1}_n \\ \hline \mathbb{1}_n & 0 \end{array} \right). \tag{2.49}$$

The Clifford group, which transforms stabiliser states into stabiliser states has a binary representation as well. Single-qubit Clifford operators U are 2×2 binary matrices $\mathbb{U}$. The action of a Clifford unitary on a single-qubit operator $U\sigma U^{\dagger}$ is represented by the multiplication of $\mathbb{U}$ and the column in Eq. (2.44) representing σ, where $\mathbb{U}$ acts from the left. Given that unitary operators cannot transform Pauli operators into the identity operator, their representative binary matrix must be full-rank. As examples, the Hadamard gate H and the phase gate S are represented by

$$\mathbb{H} = \left(\begin{array}{c|c} 0 & 1 \\ \hline 1 & 0 \end{array} \right), \quad \mathbb{U}_S = \left(\begin{array}{c|c} 1 & 1 \\ \hline 0 & 1 \end{array} \right). \tag{2.50}$$

One can check that, as expected, $\mathbb{H}$ exchanges X and Z while preserving Y, while $\mathbb{U}_S$ exchanges X to Y while preserving Z.

Clifford operations performed on multiple qubits of the stabiliser state are represented by $2n \times 2n$ binary matrices $\mathbb{U}$ that multiply $\mathbb{S}$ from the left. Clifford operations map generator sets into other generator sets, so their binary representation must preserve the rank of $\mathbb{S}$, implying that $\mathbb{U}$ is a full-rank matrix. The matrix $\mathbb{U}$ can be written using four $n \times n$ blocks as

$$\mathbb{U} = \left(\begin{array}{c|c} \mathbb{U}_{XX} & \mathbb{U}_{XZ} \\ \hline \mathbb{U}_{ZX} & \mathbb{U}_{ZZ} \end{array} \right). \tag{2.51}$$

Clifford operations must preserve the commutation of all generators, which implies that $\mathbb{U}^{\mathrm{T}}\mathbb{D}\mathbb{U} = \mathbb{D}$. For local unitary Clifford operators $\mathbb{U}_{\mathrm{LUE}} = \bigotimes_{q=1}^{n} \mathbb{U}_q$ is the tensor product of single-qubit matrices $\mathbb{U}_q$ representing each single-qubit unitary in the local Clifford operator. The matrix $\mathbb{U}_q$ corresponding to the qubit q is a 2×2 binary matrix with the following elements from $\mathbb{U}_{\mathrm{LUE}}$:

$$\mathbb{U}_q = \left(\begin{array}{c|c} [\mathbb{U}_{\mathrm{LUE}}]_{qq} & [\mathbb{U}_{\mathrm{LUE}}]_{q(q+n)} \\ \hline [\mathbb{U}_{\mathrm{LUE}}]_{(q+n)q} & [\mathbb{U}_{\mathrm{LUE}}]_{(q+n)(q+n)} \end{array} \right). \tag{2.52}$$

A local Clifford written in the binary picture by blocks, as in Eq. (2.51), is composed

only of diagonal block matrices [177]. For example,

$$\mathbb{U}_S = \left(\begin{array}{c|c} \mathbb{1}_n & \Lambda \\ \hline 0 & \mathbb{1}_n \end{array} \right) \tag{2.53}$$

represents a phase gate applied on every qubit q for which $\Lambda_{qq} = 1$, where Λ is an $n \times n$ diagonal matrix.

As mentioned previously, given a graph with adjacency matrix Γ, the action on a product state $|+\rangle^{\otimes n}$ of a CZ gate for each link on the graph generates a graph state. The state $|+\rangle^{\otimes n}$ is a stabiliser state with generators $s_1 = X_1,\ s_2 = X_2, \ldots, s_n = X_n$, represented in the binary picture by the $2n \times n$ matrix

$$\left(\begin{array}{c} 0 \\ \mathbb{1}_n \end{array} \right), \tag{2.54}$$

while the graph state is represented in Eq. (2.48). The product of CZ unitary operators that applied to $|+\rangle^{\otimes n}$ generate a graph state is then represented by the $2n \times 2n$ binary matrix

$$\mathbb{U}_\Gamma^{\mathrm{CZ}} = \left(\begin{array}{c|c} \mathbb{1}_n & \Gamma \\ \hline 0 & \mathbb{1}_n \end{array} \right). \tag{2.55}$$

Finally, the local-unitary equivalence between stabiliser and graph states implies that for every stabiliser state represented by $\mathbb{S}$ there is a local Clifford unitary $\mathbb{U}$, a recombination matrix $\mathbb{R}$, and a graph state defined by an underlying graph with adjacency matrix Γ such that

$$\mathbb{U}\mathbb{S}\mathbb{R} = \left(\begin{array}{c} \Gamma \\ \mathbb{1}_n \end{array} \right). \tag{2.56}$$

2.4 Entanglement

Entanglement is one of the fundamental aspects of quantum physics. It is used as a resource for quantum information protocols like quantum communication [89, 90], computation [146], simulation [179], and in QEC codes, where the logical information is spread on multipartite entangled states. Experimentally, a variety of physical systems including trapped ions [24], photons [26], cold atoms [27], or superconducting qubits [25] have been used to produce complex multipartite states. However, the study of entanglement in increasingly larger quantum states becomes challenging with usual tomographic techniques due to the exponential growth of the Hilbert space with

the qubit number [180, 181]. In contrast, local entanglement witnesses presented in Chap. 5 provide a way of not only detecting but also estimating entanglement in large and complex multipartite experimental states.

As we prove in that chapter, local entanglement witnesses can be used to estimate localisable entanglement (LE) [182–184], which is the maximum entanglement that can be localised on average in a subsystem by single-qubit measurements. Apart from being a good quantifier of local entanglement in stabiliser states [50, 174, 177], including topological quantum codes, with or without noise, LE is crucial also in other scenarios. For example, it has been used in conceptualizing the correlation length in certain quantum many-body systems [182, 183, 185, 186], for characterizing local entanglement in cluster-Ising [187, 188] and cluster-XY models [189], and in protocols including measurement-based quantum computation [50, 174, 177] and entanglement percolation in quantum network [190].

In this section, we describe key concepts of entanglement that are used in the rest of the thesis, including the distinction between bipartite and genuine entanglement, entanglement measures like entanglement negativity, and LE is defined in a more thorough manner.

2.4.1 Bipartite and genuine entanglement

An n-qubit state ρ is entangled, or contains some entanglement, if it cannot be written as a statistical mixture of single-qubit states [112]:

$$\rho \neq \sum_x p_x \bigotimes_{q=1}^{n} \rho_q^{(x)}, \tag{2.57}$$

where $\rho_q^{(x)}$ is a state of one qubit q and p_x are probabilities that add up to 1. One can distinguish different types of entanglement. For example, bipartite entanglement refers to the entanglement between the two parts A and B of a bipartition $A|B$ of the qubits in the system. A state has bipartite entanglement with respect to the bipartition $A|B$ if it cannot be written as a statistical mixture of a state in A and a state in B. That is

$$\rho \neq \sum_x p_x \rho_A^{(x)} \otimes \rho_B^{(x)}. \tag{2.58}$$

Note that such state might be entangled with respect to a different bipartition. Similarly, genuine entanglement is defined with respect to all bipartitions, i.e., a state is *genuinely entangled* if it cannot be written as a bipartite state, as in the previous equation, with respect to any bipartition. Thus, all genuinely entangled states have bipartite entanglement with respect to every bipartition, so they are said to be *non-separable*. A separable state is the opposite of a bipartite entangled state: the state can be written as the right-hand-side of Eq. (2.58).

The bipartite entanglement of a pure state can be characterised by the Schmidt decomposition of the state [13]. Given a bipartition $A|B$ of the qubits (assume $|A| \leq |B|$) in a state $|\psi\rangle$, there is an orthonormal set of r states $\{|\psi_1^A\rangle, \ldots, |\psi_r^A\rangle\}$ with support on the subsystem A and an orthonormal set of r states $\{|\psi_1^B\rangle, \ldots, |\psi_r^B\rangle\}$ with support on B such that the *Schmidt decomposition* of $|\psi\rangle$ with respect to the bipartition $A|B$ can be written as

$$|\psi\rangle = \sum_{x=1}^{r} \beta_x |\psi_x^A\rangle |\psi_x^B\rangle, \qquad (2.59)$$

where r is the *Schmidt rank*, x is an index running from 1 to r, and the coefficients β_x are the *Schmidt coefficients* corresponding to the bipartition $A|B$ of $|\psi\rangle$. The state is entangled if and only if the Schmidt rank is strictly larger than 1. For example, the W state $|W\rangle = 3^{-1/2}(|001\rangle + |010\rangle + |100\rangle)$ has the following Schmidt decomposition with respect to the bipartition $1|23$:

$$|W\rangle = \frac{1}{\sqrt{3}} \left(\sqrt{2} |0\rangle |B'\rangle + |1\rangle |00\rangle \right), \qquad (2.60)$$

where $|B'\rangle = 2^{-1/2}(|01\rangle + |10\rangle)$. Then one has $r = 2$, indicating that the W state is entangled with respect to the bipartition $A|B$, and the Schmidt coefficients are $\sqrt{2/3}$ and $\sqrt{1/3}$.

2.4.2 Entanglement measures

The amount of entanglement can be evaluated using entanglement measures. In this section we present only those properties of entanglement measures that are used in the thesis. For the reader interested, more detail can be found in Ref. [112]. An entanglement measure $\mathcal{E}(\rho)$ is a function that takes a state ρ and returns a real non-negative

number, generally between 0 (no entanglement) and 1 (maximum entanglement). Entanglement measures must satisfy some properties:

1. *Monotonocity*: entanglement measures do not increase under local operations and classical communications (LOCC):

$$\mathcal{E}(\Lambda(\rho)) \leq \mathcal{E}(\rho), \tag{2.61}$$

where Λ represent the quantum channel corresponding to some LOCC operations. Importantly for this thesis, LOCC operations include local unitary operators, and local projective measurements.

2. Entanglement measures vanish on separable states: $\mathcal{E}(\rho) = 0$ if ρ is separable with respect to the entanglement type evaluated by the entanglement measure.

3. *Convexity*: the entanglement of a convex sum of states is not greater than the convex sum of entanglement measures:

$$\mathcal{E}\left(\sum_x p_x \rho_x\right) \leq \sum_x p_x \mathcal{E}(\rho_x), \tag{2.62}$$

where p_x are convex weights.

Some entanglement measures are defined on pure states. For example, the *Schmidt measure* [191] with respect to a bipartition $A|B$ is defined as the logarithm of the minimum Schmidt rank r, as defined in Eq. (2.59), over all possible Schmidt decompositions of $|\psi\rangle$ with respect to $A|B$: $\mathcal{E}(|\psi\rangle) = \log_2(\min r)$. An example of a non-bipartite measure of entanglement is geometric entanglement. The *geometric entanglement* evaluates how distant is a quantum state $|\psi\rangle$ from the set of fully separable states $|\phi\rangle$, i.e., that can be written as a product state of single-qubit states $|\phi\rangle = \bigotimes_{q=1}^{n} |\phi_q\rangle$:

$$\mathcal{E}(|\psi\rangle) = 1 - \max_{|\phi\rangle} |\langle\phi|\psi\rangle|^2. \tag{2.63}$$

The notion of distance arises from the metric induced in the Hilbert space of the system by the inner product of two states $\langle\psi'|\psi\rangle$. Note that states with finite geometric entanglement are bipartite entangled with respect to some bipartition but might not be genuinely entangled in general.

The extension to mixed states of entanglement measures defined for pure states like geometric entanglement is done via the *convex-roof construction*

$$\mathcal{E}(\rho) = \min_{p_x, |\psi_x\rangle} \sum_x p_x \mathcal{E}(|\psi_x\rangle), \tag{2.64}$$

where the minimum is taken over all possible decompositions of the state:

$$\rho = \sum_x p_x |\psi_x\rangle \langle\psi_x| . \tag{2.65}$$

However, this minimisation is difficult to compute in practice. There are other entanglement measures like negativity that are defined on mixed states and are easier to compute, like the entanglement negativity. The *entanglement negativity* $\mathcal{E}(\rho)$ with respect to a bi-partition $A|B$ of the state ρ is based on the Peres-Horodecki separability criterion [192, 193], given by

$$\mathcal{E}(\rho) = \|\rho^{\mathrm{T}_A}\|_1 - 1. \tag{2.66}$$

Here, ρ^{T_A} is the partial transposition of the state ρ with respect to A, and $\|\varrho\|_1 = \mathrm{tr}\sqrt{\varrho^\dagger \varrho}$ is the *trace-norm* of the operator ϱ, which is equal to the sum of the absolute values of the eigenvalues of ϱ. Without loss of generality any state can be written with respect to the bipartition $A|B$ as

$$\rho = \sum_{xy} c_{xy} |\psi_A^{(x)}\rangle |\psi_B^{(x)}\rangle \langle\psi_A^{(y)}| \langle\psi_B^{(y)}| , \tag{2.67}$$

where $c_{yx}^* = c_{xy}$. Then, the partially transposed operator is equal to

$$\rho^{\mathrm{T}_A} = \sum_{xy} c_{xy} |\psi_A^{(y)}\rangle |\psi_B^{(x)}\rangle \langle\psi_A^{(x)}| \langle\psi_B^{(y)}| , \tag{2.68}$$

where the indices x and y for the part in A have been exchanged. For example, the density matrix representation of the Bell pair is

$$|B\rangle \langle B| = \frac{1}{2}(|00\rangle \langle 00| + |00\rangle \langle 11| + |11\rangle \langle 00| + |11\rangle \langle 11|), \tag{2.69}$$

so the partially transposed operator is

$$|B\rangle\langle B|^{\mathrm{T}_A} = \frac{1}{2}(|00\rangle\langle00| + |10\rangle\langle01| + |01\rangle\langle10| + |11\rangle\langle11|). \qquad (2.70)$$

The eigenvalues of $|B\rangle\langle B|^{\mathrm{T}_A}$ are $\{1/2,\,1/2,\,1/2,\,-1/2\}$. The trace-norm $\|\varrho\|_1$ admits a *variational characterisation* in terms of an operator D [129]:

$$\|\varrho\|_1 = \max_D \|D\varrho\|_1 \quad \text{subject to } \|D\|_\infty = 1, \qquad (2.71)$$

where $\|D\|_\infty$ is the operator norm of D, which equals the square root of the highest eigenvalue of $D^\dagger D$ (which is non-negative for any D). An alternative but completely equivalent definition of negativity is given by the eigenvalues λ_i of ρ^{T_A}:

$$\mathcal{E}(\rho) = 2 \sum_{\lambda_i < 0} |\lambda_i|. \qquad (2.72)$$

For the Bell pair, for example, the only negative eigenvalue is $-1/2$, so the entanglement negativity of the Bell pair is maximum: $\mathcal{E}(|B\rangle) = 1$.

2.4.3 Localisable entanglement

One can also ask what is the amount of entanglement within a subset of qubits in a multi-qubit state. More precisely, how much entanglement can be localised in a subsystem by means of local projective measurements. Consider an n-qubit state ρ, a subsystem $\boldsymbol{q}$ consisting of a subset of qubits, and a local measurement basis $\mathcal{M}_{\bar{\boldsymbol{q}}} = \{m_q : m_q^\dagger = m_q,\ q \in \bar{\boldsymbol{q}}\}$ on the set of qubits $\bar{\boldsymbol{q}}$ outside $\boldsymbol{q}$, with a projector Π_{m} associated to a measurement outcome m. When $\mathcal{M}_{\bar{\boldsymbol{q}}}$ is measured on ρ and the outcome m is obtained with a probability p_{m} the reduced state on $\boldsymbol{q}$ is denoted as $\rho_{\boldsymbol{q}}^{\mathsf{m}}$. Then, the *localisable entanglement* (LE) $\mathcal{E}_{\boldsymbol{q}}(\rho)$ of ρ in $\boldsymbol{q}$ is the maximum entanglement averaged over all m that can be localised in $\boldsymbol{q}$ by means of all possible local measurement bases $\mathcal{M}_{\bar{\boldsymbol{q}}}$:

$$\mathcal{E}_{\boldsymbol{q}}(\rho) = \max_{\mathcal{M}_{\bar{\boldsymbol{q}}}} \sum_{\mathsf{m}} p_{\mathsf{m}} \mathcal{E}(\rho_{\boldsymbol{q}}^{\mathsf{m}}). \qquad (2.73)$$

Note that the computation of LE becomes unfeasible in general. Every single-qubit measurement $m_q \in \mathcal{M}_{\bar{\boldsymbol{q}}}$ can be characterised with two angles θ and ϕ, so the maximisation requires the optimisation over a set of $2(n - |\boldsymbol{q}|)$ parameters, which might turn

difficult for large n. Besides, there are $2^{n-|\boldsymbol{q}|}$ possible outcomes $\mathfrak{m}$ of a local projective measurement that must be averaged over. Finally, one has to compute an entanglement measure for each outcome. In this thesis we explore lower bounds of LE from local entanglement witnesses that can be evaluated efficiently.

2.5 Noise models

Quantum states cannot be realised perfectly in the lab due to the uncontrolled coupling of quantum system to the environment or the imperfections of gates and measurements. These undesired imperfections appear as noise on quantum information processing tasks. Then, modelling noise is crucial to predict in practice the performance of quantum computation algorithms and protocols [194].

Quantum noise can be described by a quantum channel that performs operations on a quantum state and outputs another quantum state. Often in QEC, noise channels are applied to the perfect realisation of the quantum state, which is usually a pure state. Thus, the quantum state realised experimentally when a pure quantum state $|\psi\rangle$ is aimed to be produced can be described by a quantum channel

$$\rho = \varepsilon(|\psi\rangle). \tag{2.74}$$

The simplest noise models in QEC assume uncorrelated noise sources that induce errors on each qubit independently. Some examples of noise sources are magnetic fluctuations of the environment that induce an extra phase in a qubit, over-rotations of a quantum gate caused by the fluctuation of a laser, or the spontaneous decay of the qubit state during the measurement [23].

When the noise on each qubit takes the form of single-qubit Pauli operators, the noise model is called an uncorrelated Pauli noise model. As we show in Sec. 3.1.2 stabiliser codes transform uncorrelated noise into uncorrelated Pauli noise due to the stabiliser measurement performed to obtain an error syndrome [195]. For these reason, these models are used in stabiliser QEC codes to obtain an error threshold, i.e., a critical value of the noise parameter that determines the critical noise rate that a QEC code can tolerate.

Uncorrelated Pauli noise is the noise model where each qubit may suffer a Pauli error $\sigma \in \{X, Y, Z\}$ with a probability p. Three of these noise channels applied on a

single-qubit state $|\psi\rangle$ are the *bit-flip channel* $\varepsilon_{\mathrm{BF}}$, the *phase-flip channel* $\varepsilon_{\mathrm{PF}}$:

$$\varepsilon_{\mathrm{BF}}(|\psi\rangle) = (1-p)\,|\psi\rangle\,\langle\psi| + p\,X\,|\psi\rangle\,\langle\psi|\,X \tag{2.75}$$

$$\varepsilon_{\mathrm{PF}}(|\psi\rangle) = (1-p)\,|\psi\rangle\,\langle\psi| + p\,Z\,|\psi\rangle\,\langle\psi|\,Z, \tag{2.76}$$

and the depolarizing noise $\varepsilon_{\mathrm{DP}}$:

$$
\begin{aligned}
\varepsilon_{\mathrm{DP}}(|\psi\rangle) &= (1-p)\,|\psi\rangle\,\langle\psi| + \frac{p}{3}\left(X\,|\psi\rangle\,\langle\psi|\,X + Y\,|\psi\rangle\,\langle\psi|\,Y + Z\,|\psi\rangle\,\langle\psi|\,Z\right) \\
&= \left(1 - \frac{4p}{3}\right)|\psi\rangle\,\langle\psi| + \frac{4p}{3}\frac{I}{2},
\end{aligned}
\tag{2.77}
$$

where we have used the relation $\rho + X\rho X + Y\rho Y + Z\rho Z = 2I$ in Ref. [13] for any single-qubit state ρ. The depolarizing channel can be interpreted in two equivalent ways: each Pauli operator from $\{X, Y, Z\}$ is applied with probability $p/3$, or the qubit state is replaced by the completely mixed state $I/2$ with probability $4p/3$.

When the phase- and bit-flip noise channels are applied on all qubits of an n-qubit state $|\psi\rangle$, single-qubit σ errors can happen on each qubit with a probability p. Multiple-qubit errors $\sigma_{\mathbb{e}} = \bigotimes_{q=1}^{n} \sigma_q^{\mathbb{e}_q}$ can be characterised by an n-bit binary string $\mathbb{e}$, and happen with a probability $p^{|\mathbb{e}|}(1-p)^{n-|\mathbb{e}|}$, where $|\mathbb{e}| = \sum_{q=1}^{n} \mathbb{e}_q$. The noise channel is a mixture of all possible errors:

$$\rho_{\mathrm{BF}} = \varepsilon_{\mathrm{BF}}(|\psi\rangle) = \sum_{\mathbb{e}} p^{|\mathbb{e}|}(1-p)^{n-|\mathbb{e}|}\,X_{\mathbb{e}}\,|\psi\rangle\,\langle\psi|\,X_{\mathbb{e}}, \tag{2.78}$$

$$\rho_{\mathrm{PF}} = \varepsilon_{\mathrm{PF}}(|\psi\rangle) = \sum_{\mathbb{e}} p^{|\mathbb{e}|}(1-p)^{n-|\mathbb{e}|}\,Z_{\mathbb{e}}\,|\psi\rangle\,\langle\psi|\,Z_{\mathbb{e}}, \tag{2.79}$$

where the sum is performed over all of the 2^n possible bit strings $\mathbb{e}$. For depolarizing noise, errors can be characterised by a string $\mathbb{e}$ with n elements $\mathbb{e}_q \in \{0, 1, 2, 3\}$ corresponding to no error $\sigma^{(0)} = I$ and $\sigma^{(1)} = X$, $\sigma^{(2)} = Y$, $\sigma^{(3)} = Z$ errors, respectively. Each error is a Pauli operator $\sigma_{\mathbb{e}} = \bigotimes_{q=1}^{n} \sigma_q^{(\mathbb{e}_q)}$, and can happen with probability $(p/3)^{[\mathbb{e}]}(1-p)^{n-[\mathbb{e}]}$, where $[\mathbb{e}]$ is the number of elements $\mathbb{e}_q \in \{1, 2, 3\}$ in $\mathbb{e}$:

$$\rho_{\mathrm{DP}} = \varepsilon_{\mathrm{DP}}(|\psi\rangle) = \sum_{\mathbb{e}} \left(\frac{p}{3}\right)^{[\mathbb{e}]}(1-p)^{n-[\mathbb{e}]}\,\sigma_{\mathbb{e}}\,|\psi\rangle\,\langle\psi|\,\sigma_{\mathbb{e}}. \tag{2.80}$$

The sum in $\mathbb{e}$ is performed over the 4^n possible strings $\mathbb{e}$.

Finally, we present the white noise model, which is used in this thesis to benchmark

the performance of local witnesses in Sec. 5.5. Given an ideal n-qubit state $|\psi\rangle$, the *white noise model* leaves the state unchanged with probability $(1-p)$ and replaces it by the totally mixed state $I/2^n$ with probability p:

$$\rho_{\mathrm{W}} = \varepsilon_{\mathrm{W}}(|\psi\rangle) = (1-p)\,|\psi\rangle\,\langle\psi| + p\,\frac{I}{2^n}. \tag{2.81}$$

2.5.1 Erasure channel

The *erasure channel* applies when errors happen at known locations (qubits). For this thesis, we consider the erasure channel of qubit loss. The loss of qubits is a particularly damaging noise source. A qubit is lost when the information encoded in it can no longer be accessed due to the leakage of the qubit population out of the computational space or due to the actual loss of particles or photons encoding the qubit. From the theoretical point of view, the loss of information carried by the lost qubits is related to the no-cloning theorem [196], and motivated the proposal of holographic QEC codes [197, 198]. Here, the correspondence between the AdS and the CFT spacetimes is identified with the encoding of logical qubits into the multipartite state of the physical qubits. Moreover, in the existing experimental platforms for quantum computation, like trapped ions [24], photons [26], cold atoms [27], or superconducting qubits [25], qubit loss comes in various incarnations like leakage from the computational space or the loss of particles hosting qubits from their traps.

The erasure channel considered in Chap. 4 assumes that every qubit can be lost independently with a probability p. A lost qubit contains no information, so it can be represented by the completely mixed state I/n. The erasure channel for qubit losses on a multi-qubit state multi-qubit state $|\psi\rangle$ is a sum over all possible qubit loss instances $\boldsymbol{\ell}$:

$$\epsilon_{\mathrm{E}}(|\psi\rangle) = \sum_{\boldsymbol{\ell}} p^\ell (1-p)^{n-\ell} \, \mathrm{tr}_{\boldsymbol{\ell}}(|\psi\rangle\,\langle\psi|) \bigotimes_{q\in\boldsymbol{\ell}} \frac{I_q}{2}. \tag{2.82}$$

Here $\ell = |\boldsymbol{\ell}|$ is the number of qubits lost in the lost instance $\boldsymbol{\ell}$. The average number of qubits lost in an n-qubit state is pn, so the loss density coincides with p. This is the model that we employ to benchmark the tolerance of the color code to qubit loss.

Chapter 3

Quantum Error Correction (QEC)

In a nutshell, QEC codes encode the logical information redundantly on a multipartite, usually highly entangled, quantum state in such a way that, under certain noise regimes, is it extremely unlikely that experimental errors destroy the encoded information [199]. Typically, several QEC rounds are applied as intermediate steps of a quantum algorithm to correct errors that appear during the computation.

Errors are identified by extracting an error syndrome from the system without destroying the logical information encoded, and depending on the syndrome, a correction is applied. As long as the error weight is smaller than half the code distance (introduced in Sec. 3.1.2), the logical information stays protected. Syndrome extraction is performed by quantum measurements that pump the entropy generated by the errors into ancillary qubits employed for the measurements without destroying the logical information encoded. Quantum measurement is prone to errors that may lead to the wrong syndrome extraction. Besides, errors can propagate through the quantum circuit that implements a QEC round, usually increasing in number, but also through the quantum circuit that implements logical gates acting on the encoded information. This proliferation might convert a correctable error into a larger error that is no longer correctable. Thus, QEC codes must be combined with fault-tolerant techniques to avoid the error proliferation.

Fault-tolerant QEC codes avoid the error proliferation, so they guarantee that, as long as the error is smaller than half the code distance, it can be corrected. Fault-

tolerant quantum circuits come usually with an overhead in the number of qubits and gates, so part of the current efforts are to propose smaller fault-tolerant circuits. One of the biggest challenges is to apply non-Clifford logical gates fault-tolerantly like the T-gate. This requires "magic state distillation factories" that consume most resources in a fault-tolerant computation [200]. Some alternatives consists in lattice surgery in the surface code [201], or "switching" from a QEC code that can implement some fault-tolerant gates without much overhead to another where a fault-tolerant T-gate is easier to implement [202].

Moreover, QEC codes can be scaled up including more qubits in the system to correct larger errors. The fault-tolerant threshold theorem states that there is a critical error rate called error threshold below which, the probability of uncorrectable errors can be reduced to arbitrary low levels by increasing the code size. This makes the error threshold an important figure of merit for fault-tolerant QEC codes. The threshold value depends heavily on the noise model under consideration but also on the decoder algorithm that takes the error syndrome and proposes a correction. It has been estimated using numerical techniques for a variety of QEC codes but also via a connection between QEC codes and classical statistical models, where the threshold is related to the critical point of a phase transition.

Topological QEC codes like the surface code and the color code are leading candidates for fault-tolerant QEC partially due to their high error threshold. For some circuit-level noise models, which take into account the proliferation of errors, the currently estimated thresholds are between 0.14% and 1% [54–56] for the surface code and between 0.082% and 0.2% [57–60] for the color code. But topological QEC codes have more desirable properties. For instance, these code have transversal gates, which can be implemented by means of a single-qubit operation applied to every physical qubit. These logical gates do not require extra resources to be implemented in a fault-tolerant way. Unfortunately, no code that detects errors can have a universal set of transversal gates as stated by the Eastin-Knill theorem [203]. Another feature of topological QEC codes is that they have local check operators, which allow a syndrome extraction using entangling gates only between neighbouring qubits. This facilitates their realisation in some experimental platforms like superconducting qubits.

Another current line of research is the implementation of QEC codes in experimental platforms. Trapped ions and superconducting qubits present some of the highest gate

fidelities (above 99%) among experimental platforms for fault-tolerant QEC correction. These gate fidelities correspond to error rates that are at the verge of the noise thresholds for topological QEC codes, so the most pressing current challenge experimentally is scaling up these platforms. Superconducting qubits have modular two-dimensional designs that facilitate the addition of more qubits to the system, consequently allowing to scale up QEC codes. Compared to superconducting qubits, where the interactions used for entangling gates are mostly local and between two qubits only, trapped ions allow the implementation of non-local entangling gates between multiple distant ions, which adds more flexibility to the implementation of fault-tolerant quantum circuits. However, adding more qubits to the commonly used linear Paul traps reduces the speed of two-qubit gates, increasing the susceptibility to errors during the gate implementation [204]. Thus, new traps are being designed to scale up the qubit number without decreasing the speed of gates. These new traps accommodate more ions and include electrodes that allow the shuttling of ions to interacting regions where only the desired ions interact.

In this chapter we present stabiliser codes in Sec. 3.1 as one of the most studied classes of QEC codes. We also describe the main noise models studied to determine the error threshold of QEC codes. Prominent instances of stabiliser codes are topological codes. In Sec. 3.2 we introduce the surface code and in Sec. 3.3 we introduce the color code. The color code is present in the rest of the thesis because we propose a protocol to protect it against qubit loss in Chap. 4, and we use it as the playground to analyse the local entanglement witnesses that we propose in Chap. 5.

3.1 Stabiliser codes

Stabiliser codes are some of the simplest codes, yet some of the most promising for fault-tolerant QEC. We use the three-qubit repetition code as an example (see Fig. 3.1 for an illustration of this code).

The fundamental idea is to divide the Hilbert space of the system into orthogonal subspaces and keep the system in one of them, the *code space*. The subspaces in the three-qubit repetition code are two-dimensional subspaces spanned by the following
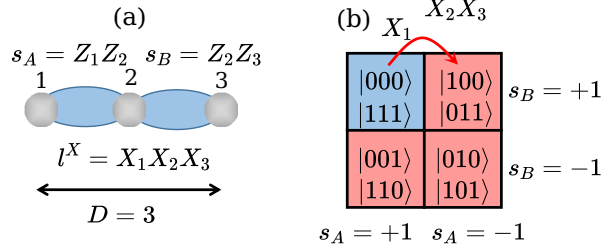
Figure 3.1: Repetition code. (a) The three-qubit repetition code consists of two stabilisers $s_A = Z_1 Z_2$ and $s_B = Z_2 Z_3$ and logical operators $l^X = X_1 X_2 X_3$ and $l^Z = Z_1 Z_2 Z_3$. The code distance against X-type errors is $D = 3$ because the smallest support of l^X multiplied by stabilisers is three. (b) The Hilbert space of three qubits is divided in four subspaces defined by the eigenvalues ± 1 of the two stabilisers. The code space is the subspace (clear blue) spanned by the code words or logical states $|0_L\rangle = |000\rangle$ and $|1_L\rangle = |111\rangle$ corresponding to $+1$ eigenvalues of the stabilisers. An X_1 error (or an $X_2 X_3$ error) moves the code space to a different subspace and excites the stabiliser s_A. This is detected by the stabiliser measurement of s_A, the most likely error X_1 is determined and corrected by applying a correction X_1 that cancels out the error.

orthogonal bases:

$$\{|000\rangle, |111\rangle\}, \quad \{|100\rangle, |011\rangle\}, \quad \{|010\rangle, |101\rangle\}, \quad \{|001\rangle, |110\rangle\}. \qquad (3.1)$$

Note that these bases differ in the parity of the first two bits and/or the parity of the last two bits. The code space contains the code words, or *logical states* $|0_L\rangle$ and $|1_L\rangle$ that determine the state of the encoded information:

$$|\psi_L\rangle = \cos(\theta/2) |0_L\rangle + e^{i\phi} \sin(\theta/2) |1_L\rangle. \qquad (3.2)$$

For the three-qubit code, the code space is spanned by the first basis in Eq. (3.1): $|0_L\rangle = |000\rangle$ and $|1_L\rangle = |111\rangle$. Every quantum state of the system within the code space is a valid logical state of the encoded information. The expectation value of *logical operators* l^X and l^Z (for the three-qubit code $l^X = X_1 X_2 X_2$ and $l^Z = Z_1 Z_2 Z_2$) determine the logical state $|\psi_L\rangle$ of the encoded information.

When detectable errors occur, the system is excited to a subspace different from the code space. For example, a bit-flip X_1 on the first qubit *excites* the three-qubit code to the second subspace in Eq. (3.1) as depicted in Fig. 3.1(b):

$$X_1 |\psi_L\rangle = \cos(\theta/2) |100\rangle + e^{i\phi} \sin(\theta/2) |011\rangle. \qquad (3.3)$$

We need to extract only the relevant information necessary to identify the error without destroying the logical information in the process. Note that in the three-qubit code, if we check the parity of the first two bits, we realise that it does not correspond to the parity of the first two bits in the code space, so we infer the presence of an error. This information can be extracted without destroying the logical information.

3.1.1 Error identification and correction

In stabiliser codes we check the parity of *check operators*, or *stabiliser operators s*, which are Pauli operators that are used to determine in which subspace the code is. A stabiliser code encoding k logical qubits into n physical qubits has $n - k$ stabiliser operators $s \in \mathcal{P}^{\otimes n}$ that commute with each other and with the logical operators, and are independent, i.e., no product of different stabilisers produces the identity operator. The stabiliser operators that detect the parity of the first two bits, and the parity of the last two bits in the three-qubit code are, respectively, $s_A = Z_1 Z_2$ and $s_B = Z_2 Z_3$. The orthogonal subspaces are eigenspaces of the stabilisers with eigenvalues ± 1 and the code space is the subspace for which the eigenvalue of all stabilisers is $+1$, and consequently, stabilisers act trivially on the code space. Thus, when stabilisers are measured with a non-demolition measurement their outcomes ± 1 determine the subspace where the code is. Thanks to the stabiliser commutation, the measurement of one stabiliser does not affect the measurement of the others. Stabilisers are found *excited*, i.e., in their eigenvalue -1, only if the error anti-commutes with them. The measurement outcome of all stabilisers is the *syndrome*, which we represent by an $(n - k)$-bit binary string $\mathbb{e}$ with bits $\mathbb{e}_s = 0 \, (1)$ if the stabiliser s is found with an eigenvalue $+1 \, (-1)$. For the three-qubit code under the error X_1 the syndrome is $\mathbb{e} = (1, 0)$.

The syndrome is all the information that is extracted to correct the code, and from it a correction that returns the system to the code space without affecting the logical information is proposed. In the three-qubit code, two errors are compatible with the syndrome: X_1 and $X_2 X_3$, and we need to decide which one has the highest possibility of producing the syndrome. If the wrong error is selected and we apply a correction that cancels the error, the logical information might get affected. For example, if we select the error $X_2 X_3$ and, in order to cancel the error, we apply the correction $X_2 X_3$ to the state $X_1 \ket{\psi_L}$ of the three-qubit code, the resulting state is not $\ket{\psi_L}$ but rather $l^X \ket{\psi_L}$, which is affected by a logical error. Thus, the correction must maximise the probability

of success. The algorithms employed to correct a QEC code given a syndrome and a noise model are called *decoders*. The most studied noise models for stabiliser codes are local uncorrelated Pauli noise channels like bit-, phase-flip and depolarising noise. In these models the probability of an error with weight w is $\binom{n}{w}p^w(1-p)^{n-w}$, where p is the noise rate. So the probability of an error decreases with the error weight as long as w is above the average number of errors pn. Thus, under these noise models, the correction proposed by a decoder often assumes that the smallest possible error compatible with the syndrome has occurred. In the case of the three-qubit code, the most likely error is X_1, so a correction X_1 is applied to correct the error.

3.1.2 Code distance and Pauli twirling

Note that, despite being less likely, it is still possible that the actual error was X_2X_3, and that, by applying X_1 as a correction, we are actually producing a logical error l^X. This illustrates that QEC codes can correct errors of a maximum weight, in this case one. Since a logical error is produced when the product of the error and the correction equals a logical operator, all errors with a weight smaller than half the size of the shortest logical operator are correctable. If the *code distance D* is the support size of the smallest logical operator, all errors with weight $\lfloor (D-1)/2 \rfloor$ or smaller, where $\lfloor \cdot \rfloor$ indicates the floor function, can be corrected. Note that, since stabilisers act trivially on the code space, the product of a logical operator and a stabiliser operator has the same effect on the logical information that a logical operator: $l^X s \ket{\psi_L} = l^X \ket{\psi_L}$. Therefore, logical operators l^σ and $\tilde{l}^\sigma = l^\sigma s$ that differ on a product of one or more stabilisers are considered *equivalent logical operators*. For the three-qubit code the three logical operators equivalent to l^X have weight three, so the code distance for X-type errors is $D = 3$, and consequently, any error with weight one can be corrected. Nevertheless, stabiliser codes can be scaled up to correct higher-weight errors. For example, the five-qubit repetition code, with logical states $\ket{0_L} = \ket{00000}$ and $\ket{1_L} = \ket{11111}$ has distance $D = 5$ and can correct all X-type errors with weight two or less.

Moreover, the three logical operators in the three-qubit code $l^Z s_A = Z_3$, $l^Z s_B = Z_1$, and $l^Z s_A s_B = Z_2$ equivalent to l^Z have weight one, so the code distance for Z-type errors is $D = 1$, meaning that weight-one Z-type errors cannot be corrected. Note that the stabilisers of the three-qubit code are of Z-type, so they do not anti-commute with Z errors, making these errors undetectable, and consequently, uncorrectable in

this code. The repetition code, independently of its size cannot correct Z-type errors, so we need *complete codes* that can correct all errors.

One might wonder what happens with non-Pauli errors like single-qubit rotations like $R_X(\gamma) = e^{-i\frac{\gamma}{2}X_1}$. The beauty of stabiliser codes is that the stabiliser measurement projects these errors into Pauli errors. For this example in the three-qubit code, when the stabiliser s_A is measured in the state $R_X(\gamma)|\psi_L\rangle$, the stabiliser outcomes are $\mathbb{e}_A = 0$ with probability $\cos^2(\gamma/2)$ and $\mathbb{e}_A = 1$ with probability $\sin^2(\gamma/2)$. This situation is equivalent to the application of a Pauli error X_1 with probability $p = \sin^2(\gamma/2)$. That is why, in stabiliser codes, the *Pauli twirling approximation*, where errors are only of Pauli type, is usually considered [205]. The approximates well incoherent errors but underestimates coherent errors like $R_X(\gamma)$ at the leading order in γ [206].

3.1.3 Noise models for QEC

So far we have assumed local uncorrelated noise with the perfect measurement of stabiliser operators, which is known as the *code capacity channel* and it is one of the simplest error models considered to benchmark QEC codes. But in reality, measurements can fail, returning the wrong outcome. When measurement errors are considered, we are talking about the *phenomenological noise model*. The way to extract information about these errors is to repeat the stabiliser measurement a number of times equals to the code distance. One could simply take the most repeated outcome as the real outcome, but the phenomenological noise model takes into account that errors might occur in between stabiliser measurements. Consider for example that the stabilisers s_A and s_B are measured three times and we obtain the outcome sequences $\vec{\mathbb{e}}_A = (0,0,1)$ and $\vec{\mathbb{e}}_B = (0,0,0)$. This can be caused by a measurement error in the third measurement, or an X_1 error in between the second and the third measurement. In the first case, despite no error has occurred on the system, the third measurement has projected the code space into the wrong subspace, exciting s_A. Thus, independently of which error happened, the correction should be X_1 to return the system to the code space.

The next level of complexity in the noise models used when considering QEC codes is the *circuit noise model*, where every element of the quantum circuit for QEC is assumed to be faulty with some probability [43]. The noise associated to each type of element, e.g., qubits, single-qubit gates, two-qubit gates, and measurements, is typically controlled by a different noise parameter. A faulty quantum gate is represented by the

perfect implementation of the gate, followed by an error with support on the qubits where the gate has support. Thus, errors can occur in between the quantum gates employed for syndrome measurement. This makes errors capable of proliferate through the circuit in such a way that even if the original error was correctable, the weight of the final error is too high to be corrected. Error proliferation occurs due to entangling gates. For example, if a Z_a error occurs in an ancillary qubit a before a CNOT gate $U_{(1,a)}^{\mathrm{CNOT}}$ used for stabiliser measurement, since $U_{(1,a)}^{\mathrm{CNOT}} Z_a = Z_1 Z_a U_{(1,a)}^{\mathrm{CNOT}}$, the error becomes $Z_1 Z_a$. The error has propagated to the data qubit 1 and can possibly be an uncorrectable error due to its increased weight. In order to avoid such uncontrolled proliferation of errors and keep the error weight below the weight of correctable errors, QEC codes must be combined with fault-tolerant techniques. A *fault-tolerant* QEC code employs fault-tolerant circuits for syndrome measurement, but also fault-tolerant logical gates, that guarantee that correctable errors (with weight below half the code distance), independently of when and where they occur in the quantum circuit, can be corrected. An example of a fault-tolerant logical gate U_{L} is a *transversal gate*, i.e., a gate which physical implementation consists in applying a the same physical gate U_q on each physical qubit: $U_{\mathrm{L}} = \bigotimes_{q=1}^{n} U_q$. Since transversal gates employ only local operations, they cannot propagate errors.

Coming back to the noise models, these are used to determine the maximum noise rate per gate that a code can tolerate under a particular noise model. This noise rate is known as the QEC *threshold*. The *fault-tolerant threshold theorem* states that fault-tolerant QEC codes affected by an experimental noise smaller than the threshold can arbitrarily reduce the probability of a logical error by a polylogarithmic increase in size, i.e., by adding more qubits to the code in order to increase the code distance. The actual challenge in QEC correction is to keep experimental error rates below threshold at the same time that we make codes larger. Topological QEC codes, which are explained in the next section, are leading candidates for fault-tolerant QEC in the future quantum computers in part because they present high thresholds.

3.2 Surface code

The surface code [52] has some properties desirable for fault-tolerant QEC like high error thresholds, low weight stabiliser operators and local stabilisers in two-dimensional
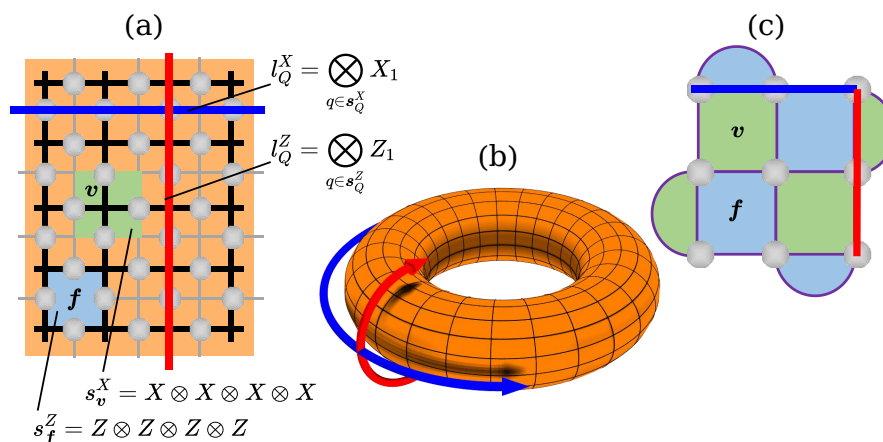
Figure 3.2: Surface code. (a) Surface code lattice in black lines, where qubits (grey circles) sit on the edges, Z-type stabilisers $s_{\boldsymbol{f}}^Z$ are defined on faces like the blue square consisting in a set $\boldsymbol{f}$ of the four qubits in the face, X-type stabilisers $s_{\boldsymbol{v}}^X$ are defined on vertices like the green square consisting in a set $\boldsymbol{v}$ of the four qubits sitting at the edges that are incident to the vertex, a logical operator l_Q^Z corresponding to a logical qubit Q has support on a string $\boldsymbol{s}_Q^Z$ (red line) in the lattice, while a logical operator l_Q^X corresponding to the same logical qubit has support on a string $\boldsymbol{s}_Q^X$ (blue line) in the dual lattice, composed by the grey lines at the background. (b) The number of encoded qubits depends to the topology where the lattice is embedded. For a torus the surface code encodes two qubits, one for each homologically non-trivial cycle. The logical operators have support on strings around the "hole" (blue) and the "tube" (red) of the torus. The code distance D is given by the shortest of these strings. (c) Minimal instance of a surface code containing 9 qubits. In this representation qubits sit at the lattice nodes, but the faces and vertices of the lattice in (a) can be identified by the corresponding colours blue and green. Logical operators are also represented with the corresponding colours in (a). This small instance has four weight-two stabilisers defined on the semicircles. The code distance is $D = 3$.

lattices. These last two properties make superconducting qubits a natural experimental platform to realise the surface code [79, 80] since qubits can be placed in two-dimensional chips containing only the qubits where one stabiliser has support and one ancillary qubit in such a way that the ancillary qubit is close to the other qubits, facilitating the local interactions required for stabiliser measurement and code initialisation preparation [81]. The gate fidelities in superconducting qubits and trapped ions are at the verge of the error threshold of fault-tolerant QEC with the surface code [207].

The surface code is defined on a two-dimensional lattice composed by n edges, f faces, and v vertices as illustrated in Fig. 3.2. Physical qubits sit on the edges, Z-type stabilisers $s_{\boldsymbol{f}}^Z = \bigotimes_{q \in \boldsymbol{f}} Z_q$ are defined on the faces $\boldsymbol{f}$, and X-type stabilisers $s_{\boldsymbol{v}}^X = \bigotimes_{q \in \boldsymbol{v}} X_q$ are defined on the vertices $\boldsymbol{v}$. Here $\boldsymbol{f}$ contains the qubits sitting in

the edges of a face, and $\boldsymbol{v}$ contains the qubits sitting in the edges incident to a vertex. Logical operators l_Q^Z of Z-type corresponding to an encoded qubit Q have support on strings $\boldsymbol{s}_Q^Z$ spanning the lattice, while logical operators l_Q^X of X-type corresponding to an encoded qubit Q (like most QEC codes, surface codes can encode more than one qubit) have support on strings $\boldsymbol{s}_Q^X$ spanning the dual lattice, which is formed by placing a node at the centre of each face and connecting nodes corresponding to adjacent faces. One can see that under this construction, stabiliser operators commute, logical operators can commute or anti-commute, and stabiliser operators commute with the logical operators. Those pairs of logical operators that anti-commute correspond to the same encoded qubit Q. The code distance is the length of the shortest string where a logical operator has support.

The number of encoded qubits depends only on the topology where the lattice is embedded. That is why the surface code is a *topological QEC code*. If the lattice is embedded in a closed manifold, i.e., without boundaries like a torus, not all stabiliser operators are independent: the multiplication of all face stabilisers, and the multiplication of all vertex stabilisers produce the identity operator, so the number of encoded qubits is $k = n - f - v + 2$. The Euler characteristics relates the geometric properties of the lattice $\chi = v - n + f$ with the topological properties $\chi = 2 - 2g$, where g is the number of "holes" in a closed and orientable manifold. Thus, the number of encoded qubits depends on the Euler characteristic as $k = 2 - \chi$ and on the genus as $k = 2g$. For example, a sphere has $g = 0$, so it does not encode any logical qubit, while a torus has $g = 1$, so it encodes two logical qubits. On closed manifolds, logical operators have support on homologically non-trivial cycles of the topology, like the central hole and the "tube" in the torus (see Fig. 3.2(b)). But surface codes can also be defined in two-dimensional lattices where the number of encoded qubits depends on the number of boundaries and logical operators have support on strings extending from one boundary to a non-incident boundary.

In Fig. 3.2(c) we show the minimal instance of a fault-tolerant surface code with nine qubits and code distance $D = 3$. It can correct a weight-one error of X-, Z-, or Y-type. Under this construction, a logical qubit requires $n = D^2$ data qubits. This construction also allows the transversal implementation of the logical operators and the CNOT gate, while the Hadamard, phase-gate and T-gate fault-tolerant implementations require more complex techniques and resources [208]. A fault-tolerant version

of this instance includes eight ancillary qubits at the centre of each face in Fig. 3.2(c), one for each stabiliser [209]. The fault-tolerance is achieved by applying the CNOT gates for stabiliser measurement in a specific order, which keeps error propagation under control. It is a 17-qubit surface code and it has been investigated in order to be implemented using superconducting qubits [81].

Surface code thresholds have been determined via a connection with classical statistical models. For code capacity noise with single-qubit bit and phase-flip errors can be mapped to a 2D random-bond Ising model with two-body [166] interactions where the threshold $10.94\pm0.02\%$ corresponds to the value of critical point of the two-dimensional random-bond Ising model on the Nishimori line. For phenomenological noise the surface code maps to a 3D random-plaquette lattice gauge model [168], which provides a threshold of $\simeq 3.3\%$. The circuit noise model was recently considered in Ref. [150]. Numerical estimations of error rate threshold are between 0.14% and 1% [54–56] for the circuit-level noise model. As we detail in Sec. 4.1, qubit loss can also be corrected in the surface code, showing a tolerance that is related with the bond-percolation threshold of the lattice [74, 75].

3.3   Color code

The color code [53], like the surface code, is a topological QEC code with desired properties like high error thresholds, low weight stabiliser operators and local stabilisers in two-dimensional lattices. With respect to the surface code, the color code requires less physical qubits to achieve the same code distance and presents transversal gates, but stabiliser operators have slightly higher weight. Nevertheless, the entire Clifford group can be applied transversally on triangular color codes whose stabilisers weight is an integer multiple of 4, like color codes [53] defined on the 4.8.8. lattice in Fig. 3.3(a) (the phase gate is not fully transversal in other triangular color codes). These differences suggest that color codes can be better suited for fault-tolerant quantum computation, while surface codes can be employed for quantum memories, i.e., a QEC that protects a saved quantum state of the encoded information without modifying it.

The color code is defined on a trivalent and face three-colourable two-dimensional lattice where qubits sit on the n nodes, and stabilisers are defined on the f faces as shown in Fig. 3.3. The trivalence means that three lattice edges are incident on each
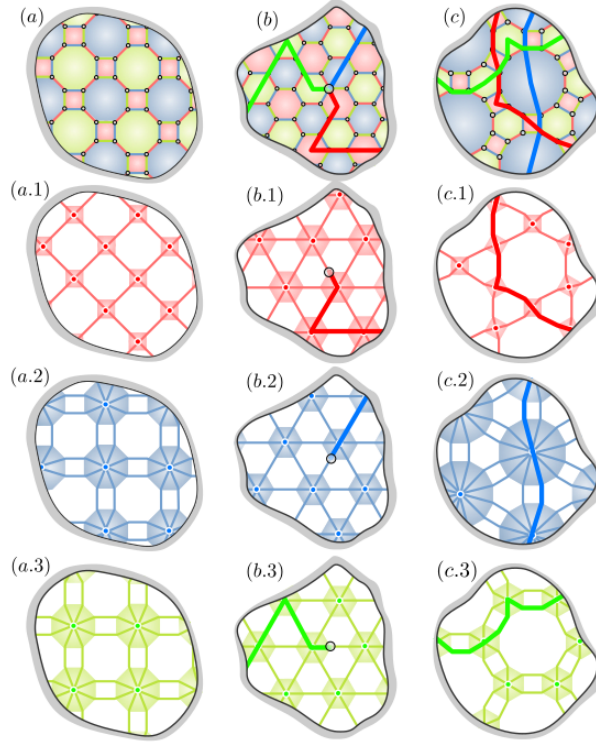
Figure 3.3: Regular color code lattices, shrunk lattices and logical operators.
The lattice where the color code is defined is trivalent and face three-colourable, qubits
sit on the nodes, X-type as well as Z-type stabilisers are defined on the faces, and logical
operators have support on strings and string-nets spanning the lattices. (a) 4.8.8. geometry,
with (a.1) a square red shrunk lattice, (a.2) a double-edge square blue shrunk lattice, and
a (a.3) a double-edge square green shrunk lattice. (b) 6.6.6. or honeycomb geometry. One
logical operator with support on a string-net that branches into the three shrunk lattices.
(b.1) Triangular red shrunk lattice with the red part of the string-net. (b.2) Triangular
blue shrunk lattice with the blue part of the string-net. (b.3) Triangular green shrunk
lattice with the green part of the string-net. (c) 4.6.12. geometry. Three logical operators
with support on strings spanning their corresponding shrunk lattices. (c.1) Kagome red
shrunk lattice with a red string. (c.2) Double-edge triangular blue shrunk lattice with a
blue string. (c.3) Double-edge hexagonal green shrunk lattice with a green string.

node, and face three-colourable lattices can be coloured with three colours R, B, and
G (red, blue, green for example) such that adjacent faces do not share a color. These
properties allow one to colour edges such that the color of each edge is different from
the color of the two faces that share the edge. There are three regular lattices with
these properties as depicted in Fig. 3.3: the 4.8.8. lattice, where each node is in one
square and two octagons, the 6.6.6. or honeycomb lattice, where each node belongs to
three hexagons, and the 4.6.12. lattice, where each node is in one square, one hexagon,

and one dodecagon. Two stabilisers are defined for each face $\boldsymbol{f}$ as shown in Fig. 3.4: one Z-type stabiliser $s_{\boldsymbol{f}}^Z = \bigotimes_{q \in \boldsymbol{f}} Z_q$ and one X-type $s_{\boldsymbol{f}}^X = \bigotimes_{q \in \boldsymbol{f}} X_q$. All stabilisers commute given that the lattice properties guarantee that faces have an even number of qubits and that adjacent faces share two qubits.

Underlying the color code lattice, three shrunk lattices exist, one for each colour as illustrated in Fig. 3.3. The, say, blue shrunk lattice is obtained by placing a node at the centre of each blue face, and connecting these nodes through the blue edges that are incident on the blue faces in the color code lattice. Logical operators l_Q^σ in the color code have support on simple strings $\boldsymbol{s}_Q^\sigma$ spanning a shrunk lattice as shown in Figs. 3.3(c), (c.1), (c.2), and (c.3). They commute with stabilisers, commute with logical operators defined on the same shrunk lattice, and commute or anti-commute with logical operators defined on the other shrunk lattices. A particularity of color codes is that logical operators can also have support on string-nets as shown in Fig. 3.3(b). String-nets operators can be produced, for example, by taking a logical operator l_Q^σ defined on a simple string in the shrunk lattice and multiply if by a stabiliser $s_{\boldsymbol{f}}^\sigma$ defined on a blue face where l_Q^σ has support as it will be shown in Fig. 4.2. The resulting equivalent logical operator $\tilde{l}_Q^\sigma = l_Q^\sigma s_{\boldsymbol{f}}^\sigma$ now has support on a string-net that lives partially on the three shrunk lattices.

Similarly to the surface code, the number of encoded qubits in the color code depends on the topology of the manifold where the color code lattice is embedded. Again, in a closed manifold not all stabilisers are independent. The multiplication of all σ-type stabilisers in the red faces results in σ applied to all qubits, and this happens also for the blue and the green faces, so there are two constraints for each stabiliser type $\sigma \in \{X, Z\}$:

$$\prod_{\boldsymbol{f} \in \mathcal{F}_R} s_{\boldsymbol{f}}^\sigma = \prod_{\boldsymbol{f} \in \mathcal{F}_B} s_{\boldsymbol{f}}^\sigma = \prod_{\boldsymbol{f} \in \mathcal{F}_G} s_{\boldsymbol{f}}^\sigma. \tag{3.4}$$

Here $\mathcal{F}_R$, $\mathcal{F}_B$, and $\mathcal{F}_G$, are the sets of all red, blue, and green faces, respectively. This leads to a number of encoded qubits $k = n - 2f + 4$. For closed trivalent lattices we can assign half of each edge to an incident node, such that there are $3/2$ edges per node, making the number of edges equal to $e = 3/2\,n$. Thus, the number of encoded qubits can be written as $k = 4 - 2n + 2e - 2f$, and, consequently, it can be expressed in terms of the Euler characteristics $\chi = n - e + f$ as $k = 4 - 2\chi$, which in terms of the genus g (where $\chi = 2 - 2g$) results in $k = 4g$. For example, a color code embedded in a torus

$$s_R^Z = Z_1 Z_2 Z_3 Z_4$$
$$s_G^Z = Z_2 Z_3 Z_5 Z_6$$
$$s_B^Z = Z_3 Z_4 Z_6 Z_7$$
$$s_R^X = X_1 X_2 X_3 X_4$$
$$s_G^X = X_2 X_3 X_5 X_6$$
$$s_B^X = X_3 X_4 X_6 X_7$$

$$l^Z = Z_1 Z_2 Z_3 Z_4 Z_5 Z_6 Z_7$$
$$l^X = X_1 X_2 X_3 X_4 X_5 X_6 X_7$$
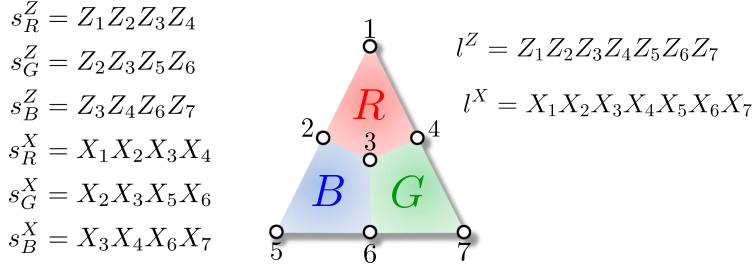
Figure 3.4: Seven-qubit color code. The smallest instance of the color code consists in seven qubits sitting at the nodes of this lattice with three faces, one of each color. Stabilisers (left) are defined on the faces, while logical operators (right) are transversal operators, i.e., act equally on each qubit.

encodes 4 qubits and the logical operators have support on homologically non-trivial cycles in the topology of the shrunk lattice, which adopt the same topology than the color code lattice.

The color code can also be encoded in two-dimensional lattices with boundaries. For instance, triangular color codes are obtained by removing a node, the three incident edges, and the three faces that contain it, from a color code lattice embedded in a sphere. In doing this, the number of physical qubits reduces by one and the number of stabilisers reduces by six, but the four constraints disappear given that the lattice has now a boundary. Thus, the number of encoded qubits increases by one. Since the sphere does not encode logical qubits (recall that for closed manifolds $k = 4g$ and that $g = 0$ for a sphere), when these elements are removed, the resulting lattice with boundaries encodes $k = 1$ logical qubits. These lattices have the form of a triangle (see Fig. 3.4 for the minimal instance of a triangular color code). The number of qubits in triangular codes with the 4.8.8. geometry grows as $(D^2 - 1)/2 + D$ [57], so for the same code distance, color codes require less data qubits than surface codes (recall that for rotated surface codes like the one shown in Fig. 3.2(c) the number of data qubits grows as D^2). Finally, in triangular color codes the two logical operators, the Hadamard gate, and the CNOT gate are transversal. If stabilisers have a weight that is multiple of 4, the phase gate is also transversal, making the entire Clifford group transversal in these codes [53].

The minimal instance of a color code (shown in Fig. 3.4) is the Steane code [210], which coincides with a seven-qubit triangular color code with code distance $D = 3$. A non-fault-tolerant version of this code was realised experimentally with trapped

ions [76]. For this code, various fault-tolerant error correction schemes have been proposed, each aiming to reduce the number of extra qubits required. In Ref. [211] the use of cat states composed for four extra qubits was proposed. This was reduced to two qubits per stabiliser: an ancillary qubit and a flag qubit. These two extra qubits per face could be accommodated in a superconducting chip using only local interactions [82]. Finally, provided that one reuses these two qubits for various stabiliser measurements, the number of extra qubits for a fault-tolerant seven-qubit color code reduces to three if three stabilisers are measured simultaneously, or even to two if only two stabilisers are measured simultaneously [83, 84, 212]. We can now make a simple count of the number of physical qubits required to implement fault-tolerant QEC to show that the color code requires less physical qubits than the surface code for the same code distance D. Following the layout introduced in Ref. [60], a fault-tolerant 6.6.6. triangular color code can be made from $(3D^2 - 1)/2$ physical qubits. On the other hand, the fault-tolerant rotated surface code requires only one ancilla per stabiliser and it possess $D^2 - 1$ stabilisers. Therefore, taking into account the number of ancillas, flags, and data qubits, $2D^2 - 1$ physical qubits are required for a fault-tolerant surface code. Therefore, the number of physical qubits required for the color code is smaller for every code distance $D > 1$.

The error threshold of color codes is studied via a connection with classical statistical models for various noise models. For instance, under computational (single-qubit bit and phase-flip) errors the color code can be mapped to a 2D random-bond Ising model three-body interactions [167], which gives a threshold of 10.9(2)%. Under computational errors and faulty stabiliser measurements the color code maps to a 3D Ising lattice gauge theory [169] and presents a threshold of 4.8(2)%. At the circuit-level noise model, numerical analyses estimate the threshold between 0.08% and 0.2% [57–59]. In Chap. 4 we obtain a new interesting and useful connection between quantum information and statistical mechanics: the tolerance of the color code to qubit loss under the protocol that we propose is directly related to a novel bond-percolation problem in three coupled lattices.

3. QUANTUM ERROR CORRECTION (QEC)

Chapter 4

Qubit losses in the color code

In this chapter we explain the work about qubit losses on color codes that we realised and presented in Refs. [1, 2]. In Ref. [1] we introduced a protocol to cope with qubit losses in the color code. Interestingly, the tolerance of the color code under our protocol is directly related to a novel bond-percolation problem of string-nets spanning three coupled lattices corresponding to the three shrunk lattices of the color code. This shows a new connection between quantum information, in this case, topological QEC, and classical statistical mechanics, which is explored to study analytically the tolerance of the color code. Then, we numerically compute the associated qubit loss thresholds for three families of 2D color code and find that with $p = 0.461 \pm 0.005$ these are close to satisfying the fundamental limit of 50% as imposed by the no-cloning theorem [196]. Moreover, we prove that the logical information is protected if and only if the set of lost qubits does not include the entire support of any logical operator. Our findings reveal a new connection between topological color codes and percolation theory, show high robustness of color codes against qubit loss, and are directly relevant for implementations of topological quantum error correction (QEC) in various physical platforms.

In Sec. 4.2 we introduce the protocol to cope with qubit losses in the color code and study the necessary and sufficient conditions for the preservation of the logical information. In Sec. 4.3 we show the connection between the tolerance of the color code to qubit loss and a novel bond-percolation problem, and use it to obtain the critical values of the qubit loss rate tolerated by the color code under our protocol. This connection is explored in Sec. 4.4 to study analytically the tolerance of the color code. This section includes a mean-field approximation of the fraction of edges erased

(see Sec. 4.4.4) as a function of the qubit loss rate that I derived personally but is not present in Refs. [1, 2].

4.1 Background

Qubit loss is a severe error source that damages the processed information if no correction is applied. The color code, as one leading candidate for fault-tolerant QEC should be able to correct qubit loss in an efficient way that desirably provides a high tolerance against these errors. A qubit is lost when the information encoded in it can no longer be accessed due to the leakage of the qubit population out of the computational space, or due to the actual loss of particles or photons encoding the qubit.

For the surface code a protocol proposed in Refs. [74, 75] consists in removing the lost qubits and redefining the code space without support on the removed qubits. Recall that the surface code arranges the qubits in the edges of a two-dimensional lattice, for each lattice vertex there is an X-type stabiliser with support on the qubits connected to the vertex, for each face in the lattice there is a Z-type stabiliser with support on the qubits in the face, and logical operators have support on strings spanning the lattice as depicted in Fig. 4.2. In the protocol, every lost qubit is removed from the code, then, the edges where qubit losses are sitting are erased from the lattice, and finally, a new set of stabilisers defined in the new lattice is measured. As indicated in Fig. 4.1, vertex stabilisers shrink, while every pair of face stabilisers connected by a lost qubit are merged into a larger face stabiliser. Thus, for each loss, a qubit and a stabiliser are removed, preserving the number of encoded qubits, as expected.

Logical operators with support on the removed qubits are no-longer well defined, but, as long as there are some well defined logical operators in the new lattice, i.e., without support on the removed qubits, the logical information is preserved. Since logical operators have support on strings spanning the lattice, no well defined logical operator exists if the new lattice does not percolate, leading to the destruction of the logical information. Assuming a local-uncorrelated model with qubit loss rate p, the critical probability p_c that causes the destruction of the logical information corresponds to the bond-percolation threshold r_c of the original lattice: $p_c = r_c$. Therefore, the surface code defined on the square lattice, with bond-percolation threshold $r_c = 0.5$ [213], can tolerate the loss of 50% of qubits in the absence of other errors.
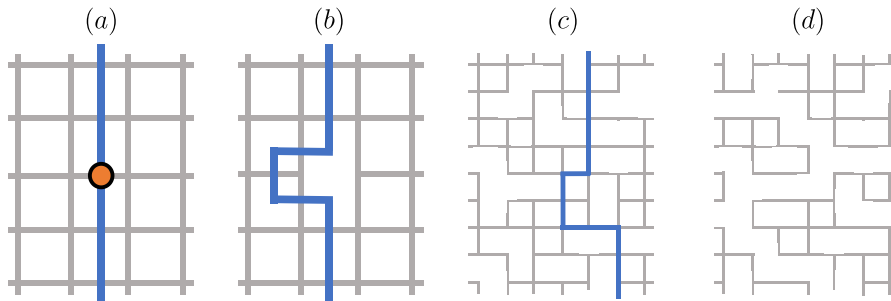
Figure 4.1: Protocol to correct qubit losses in the surface code and relation with percolation theory. (a) A lost qubit (orange) is detected at the centre of the square lattice where the surface code is defined (grey lattice). In this work we assume that the positions of the lost qubits are already known. We also show a logical operator with support on a string (blue line) spanning the lattice. The logical operator is ill-defined because it has support on a lost qubit. (b) New lattice without the edge where the lost qubit was sitting. A well-defined logical operator is shown in blue. (c) Bigger lattice redefined after some losses are corrected. The encoded information is still in the code given that the lattice percolates, as shown by the existence of a well defined logical operator (blue line). (d) New lattice that has been affected by a greater number of qubit losses. The lattice does not percolate so the logical information is destroyed.

The correction of qubit losses in the color code has the additional difficulty, compared to the surface code, that the lattice must stay trivalent and face-three colourable after the lattice redefinition. This is achieved in our protocol by sacrificing a qubit for each lost qubit. Moreover, the analysis of the tolerance becomes more complicated since logical operators in the color code have support on simple strings spanning the shrunk lattices of the color code, but also on string-nets that branch on the three shrunk lattices as represented in Fig. 4.2. Besides, even if we account only for simple strings in the shrunk lattice, the problem becomes more complicated than in the surface code given that, since some qubits need to be sacrificed, the relation between p_c and the bond-percolation threshold r_c of the shrunk lattices is more complex than an equality relation.

4.2 The protocol for the color code

The protocol that we proposed in Ref. [1] to correct the color code from qubit losses consists in "sacrificing", for every lost qubit, a neighbouring qubit which is removed together with the loss. The steps of the protocol are depicted in Fig. 4.3. (i) Detect the lost qubits. In this work we assume that the positions of the lost qubits are known.
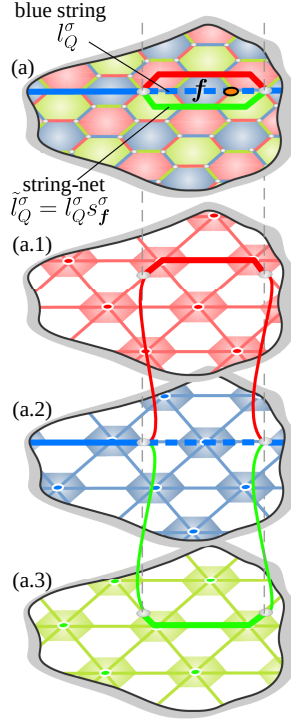
Figure 4.2: Strings and string-nets where logical operators have support. (a) 6.6.6 color code lattice with a blue string operator l_Q^σ on the continuous and discontinuous blue lines, and string-net operator $\tilde{l}_Q^\sigma$. The string-net operator is composed by four paths represented by four continuous lines: (a.1) a red path in the red shrunk lattice, (a.2) two blue paths (the two continuous lines) in the blue shrunk lattice, (a.3) a green path in the green shrunk lattice. Here the blue string operator l_Q^σ, which is not well defined because it has support on a lost qubit (the orange circle), is multiplied by the stabiliser s_f^σ on the blue face $\boldsymbol{f}$ and transformed into the string-net operator $\tilde{l}_Q^\sigma$ that does not have support on the lost qubit.

(ii) Choose randomly the order in which the losses are corrected, and for each loss q, select randomly one of the three neighbouring qubits to the loss as the sacrificed qubit q_s. (iii) For each loss, remove the lost qubit and the sacrificed qubit and modify the faces so they do not have support on the removed qubits: shrink the two faces $\boldsymbol{a}$, $\boldsymbol{b}$ that contain both removed qubits into faces $\boldsymbol{a}'$ and $\boldsymbol{b}'$, respectively, and merge the two faces $\boldsymbol{c}$, $\boldsymbol{d}$ that have support on only one of the qubits into a face $\boldsymbol{c}'$. In this redefinition step the five edges connecting the removed qubits have been erased and two new edges have been added to the lattice. At the same time, a face where two stabilisers are defined is also removed. The new code has two physical qubits and two stabilisers less, so the number of encoded qubits is preserved.
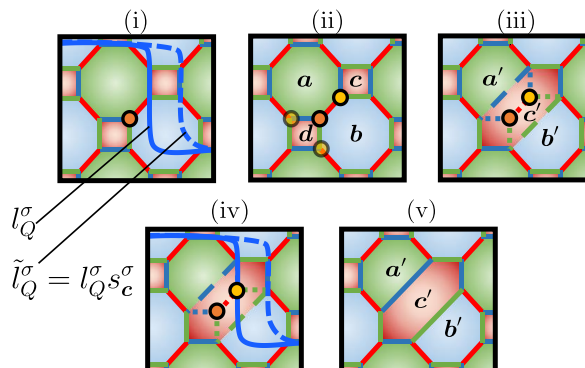
Figure 4.3: Protocol to correct qubit losses in the color code. (i) Detect the lost qubit (orange circle). In this work we assume that the positions of the lost qubits are already known. We also show two string operators l_Q^σ (continuous line), and $\tilde{l}_Q^\sigma = l_Q^\sigma s_{\boldsymbol{c}}^\sigma$ (dashed line) that differ by multiplication with the stabiliser $s_{\boldsymbol{c}}^\sigma$ defined on the face $\boldsymbol{c}$. (ii) Choose one of the three neighbouring qubits (transparent yellow circles) as the sacrificed qubit (yellow circle), (iii) remove both qubits and modify the lattice: the faces $\boldsymbol{a}, \boldsymbol{b}$ that contain both qubits are shrunk into $\boldsymbol{a'}, \boldsymbol{b'}$, and the two faces $\boldsymbol{c}, \boldsymbol{d}$ that contain only one of the removed qubits (lost and sacrificed) are merged into one face $\boldsymbol{c'}$. This correction erases the five edges adjacent to both qubits (dotted lines) and adds two new edges (dashed lines) such that all remaining qubits have an edge of each color. (iv) Check the existence of the logical information by searching for a well-defined logical operator (like $\tilde{l}_Q^\sigma$), which does not have support on the removed qubits. (v) If the logical information exists, measure the redefined stabilisers $\boldsymbol{a'}, \boldsymbol{b'}, \boldsymbol{c'}$. The well defined operators, like $\tilde{l}_Q^\sigma$, remain valid logical operators in the redefined code.

(iv) Check whether the logical information exists or not after the removal of the lost and sacrificed qubits. To this end, a key observation is that logical operators are not uniquely defined. Two logical operators $l_Q^\sigma, \tilde{l}_Q^\sigma$ belong to the same class $\{Q, \sigma\}$, i.e., they encode the same information as explained in Sec. 3.1.2, if and only if they differ in a multiplication with a subset $S \subset \mathcal{S}$ of the generator set $\mathcal{S}$

$$\tilde{l}_Q^\sigma = l_Q^\sigma \prod_{s_{\boldsymbol{f}}^{\sigma'} \in S} s_{\boldsymbol{f}}^{\sigma'}. \tag{4.1}$$

The logical information still exists in the code if for every class $\{Q, \sigma\}$ there is a well defined logical operator $\tilde{l}_Q^\sigma$, meaning that it does not have support on the removed qubits (lost and sacrificed). For example, in Fig. 4.3 we show two logical operators that belong to the same class $\{Q, \sigma\}$ because they differ in the multiplication by the stabiliser $s_{\boldsymbol{c}}^\sigma$: one $\tilde{l}_Q^\sigma$ is well defined, while the other l_Q^σ is not. Another example is shown in Fig. 4.2, where an ill-defined string operator defined on the blue dashed line

is multiplied by a stabiliser defined on the face $\boldsymbol{f}$, producing a string-net composed by four paths: two blue, one red and one green. Given a set of removed qubits (lost and sacrificed) one can determine the existence of well defined logical operators by means of the algebraic technique described in Sec. 4.2.1. Furthermore, using the machinery developed for the algebraic technique we proved, as discussed in Sec. 4.2.2, that the logical information is preserved if and only if the set of removed qubits does not include the entire support of a logical operator. The reader not interested in these details can jump to Sec. 4.3 where we make a connection between the tolerance of the color code under qubit loss and percolation theory.

(v) If the logical information is preserved, the last step of the protocol consists of projecting the state into the common eigenspace of the redefined stabilisers by stabiliser measurement. As the system is not initially defined in the eigenspace of the redefined stabilisers, excitations may appear when measured, i.e., the system might be projected into the -1 eigenspace of these stabilisers. These excitations are correlated: for each qubit loss, the stabilisers of the same type X or Z defined on the three new faces $\boldsymbol{a}'$, $\boldsymbol{b}'$ and $\boldsymbol{c}'$ depicted in Fig. 4.3 are found in the same eigenvalue ± 1 [1]. Instead of cancelling the excitations, one can define the new code space as determined by the measured eigenvalues of the new stabilisers.

4.2.1 Algebraic technique

As discussed during the explanation of the step (iv) of the protocol, the existence of the logical information is equivalent to the existence of a subset S of stabilisers such that the logical operator $\tilde{l}_Q^\sigma$ in Eq. (4.1) has no support on the set of removed qubits (lost and sacrificed). Here we map the problem of finding S to a system of linear binary equations.

Without loss of generality one can choose the logical operator l_Q^σ in Eq. (4.1) as composed of Pauli operators of just one type σ, i.e., $l_Q^\sigma = \bigotimes_{q \in \boldsymbol{s}_Q^\sigma} \sigma_q$ where $\boldsymbol{s}_Q^\sigma$ is the set of qubits where l_Q^σ has support. When a logical operator l_Q^σ composed by Pauli operators of just one type σ is multiplied by stabilisers of another type $\sigma' \neq \sigma$, the support $\tilde{\boldsymbol{s}}_Q^\sigma$ of the new operator $\tilde{l}_Q^\sigma$ contains the support of l_Q^σ: $\tilde{\boldsymbol{s}}_Q^\sigma \supset \boldsymbol{s}_Q^\sigma$, so if a removed qubit is in $\boldsymbol{s}_Q^\sigma$ it is also in $\tilde{\boldsymbol{s}}_Q^\sigma$ and the multiplication with stabilisers of the other type σ' becomes ineffective.

As a consequence, one can restrict the subsets S that multiply l_Q^σ in Eq. (4.1) to those subsets that only contain stabilisers of the same type σ. If the subset of faces where the stabilisers of S are defined is $\mathcal{F}$, the support of $\tilde{l}_Q^\sigma$ is then given by:

$$\tilde{\boldsymbol{s}}_Q^\sigma = \boldsymbol{s}_Q^\sigma \bigoplus_{\boldsymbol{f} \in \mathcal{F}} \boldsymbol{f}, \tag{4.2}$$

where the symbol $\oplus$ indicates the symmetric difference between sets: $\boldsymbol{a} \oplus \boldsymbol{b} = (\boldsymbol{a} \cup \boldsymbol{b}) \setminus (\boldsymbol{a} \cap \boldsymbol{b})$. The symmetric difference comes from the fact that $\sigma^N = \sigma$ for odd N and $\sigma^N = I$ (the identity operator) for even N. For simplicity, from now on we drop the indices q, σ from the qubit subsets.

Given a set of removed qubits $\boldsymbol{r}$, a logical operator $\tilde{l}_Q^\sigma$, defined on the string $\tilde{\boldsymbol{s}}$, has non-empty support on $\boldsymbol{r}$ if $\tilde{\boldsymbol{s}}$ intersects $\boldsymbol{r}$, i.e., if $\boldsymbol{r} \cap \tilde{\boldsymbol{s}} \neq \emptyset$. Therefore, the logical information still exists if there is a subset of faces $\mathcal{F}$ for which:

$$\boldsymbol{r} \cap \left(\boldsymbol{s} \bigoplus_{\boldsymbol{f} \in \mathcal{F}} \boldsymbol{f} \right) = \emptyset. \tag{4.3}$$

In order to map Eq. (4.3) to a system of linear equations let us first define the binary vectors and matrices that represent the sets appearing in the equation. Recall that n is the number of qubits and f the number of faces. Then:

- The set of all faces is represented by an $n \times f$ matrix $\mathbb{F}$ whose elements are $\mathbb{F}_{q\boldsymbol{f}} = 1$ if the qubit q is in the face $\boldsymbol{f}$ and 0 otherwise.

- A string $\boldsymbol{s}$ is represented by an $n \times 1$ column vector $\mathbb{s}$ whose elements are $\mathbb{s}_q = 1$ if the qubit q is in $\boldsymbol{s}$ and 0 otherwise.

- The subset $\mathcal{F}$ of faces is represented by an $f \times 1$ column matrix $\mathbb{x}$ whose elements are $\mathbb{x}_{\boldsymbol{f}} = 1$ if the face $\boldsymbol{f}$ is in $\mathcal{F}$ and 0 otherwise.

The symmetric difference between sets is mapped to the summation modulo 2 of binary vectors and matrices. Then, Eq. (4.2) is mapped to the following binary matrix operations:

$$\tilde{\mathbb{s}} = \mathbb{s} + \mathbb{F}\mathbb{x}, \tag{4.4}$$

where $\mathbb{F}\mathbb{x}$ is the usual matrix product performed modulo 2.

The intersection between sets is mapped to the element-wise product $\mathbb{r} \circ \tilde{\mathbb{s}}$ of binary vectors, i.e., another $n \times 1$ column vector where the q-th element is the product $\mathbb{r}_q \tilde{\mathbb{s}}_q$. Then, Eq. (4.3) is mapped to

$$\mathbb{r} \circ (\mathbb{s} + \mathbb{F}\varkappa) = 0, \tag{4.5}$$

which can be written in the standard form of a system of linear equations as:

$$(\mathbb{r} \circ \mathbb{F})\,\varkappa = \mathbb{r} \circ \mathbb{s}. \tag{4.6}$$

Here $\mathbb{r} \circ \mathbb{F}$ is an $n \times f$ matrix whose elements are the products $[\mathbb{r} \circ \mathbb{F}]_{q\boldsymbol{f}} = \mathbb{r}_q \mathbb{F}_{q\boldsymbol{f}}$.

Finally, the search of a logical operator without support on the removed qubits is equivalent to finding a solution $\varkappa$ of the linear system in Eq. (4.6). This system can be efficiently solved by Gauss elimination modulo 2 in a time that scales as $\sim n^3$ or better.

4.2.2   Condition for the existence of the logical information

Here we prove that *given a set of removed qubits $\boldsymbol{r}$, there exists a logical operator for every class $\{Q, \sigma\}$ without support on the removed qubits if and only if $\boldsymbol{r}$ does not contain the support of a logical operator.* We use the notation defined in Sec. 4.2.1.

Let us start by assuming that $\boldsymbol{r}$ includes the support of a logical operator $l_Q^{\sigma'}$ and prove that all logical operators l_Q^{σ} of another type $\sigma \neq \sigma'$ have non-empty support on $\boldsymbol{r}$. The logical operator $l_Q^{\sigma'}$ anti-commutes with all logical operators l_Q^{σ} of the class $\{Q, \sigma\}$. Consequently the support of $l_Q^{\sigma'}$ and the support of every logical operator l_Q^{σ} have at least one qubit in common. As a consequence, all logical operators l_Q^{σ} have non-empty support on the set of removed qubits.

Now we assume that all operators $\tilde{l}_Q^{\sigma}$ of a class $\{Q, \sigma\}$ have non-empty support on the set of removed qubits $\mathbb{r}$ and prove that the set of removed qubits represented by $\mathbb{r}$ includes a logical operator. Given that assumption, the system of Eq. (4.6) does not have a solution, so the rank of the augmented matrix is bigger than the rank of the matrix $\mathbb{r} \circ \mathbb{F}$:

$$\mathrm{rank}\,(\mathbb{r} \circ [\mathbb{F} \ \ \mathbb{s}]) > \mathrm{rank}\,(\mathbb{r} \circ \mathbb{F}). \tag{4.7}$$

By the rank-nullity theorem, the rank of any matrix A is the number of rows m minus the number of linearly independent column vectors $\mathbb{v}$ that cancel it from the left:

$\mathbb{v}^T A = 0$. From Eq. (4.7) that means that the matrix $\mathbb{r} \circ \mathbb{F}$ has at least one more vector $\mathbb{v}$ that cancels it from the left than the matrix $\mathbb{r} \circ [\mathbb{F} \ \mathbb{s}]$. Note that every vector that cancels $[\mathbb{F} \ \mathbb{s}]$ from the left also cancels $\mathbb{F}$ from the left. Then, that vector satisfies

$$\mathbb{v}^T \left(\mathbb{r} \circ \mathbb{F} \right) = 0, \tag{4.8}$$

$$\mathbb{v}^T \left(\mathbb{r} \circ [\mathbb{F} \ \mathbb{s}] \right) \neq 0, \tag{4.9}$$

or equivalently:

$$\mathbb{v}^T \left(\mathbb{r} \circ \mathbb{F} \right) = 0, \tag{4.10}$$

$$\mathbb{v}^T \left(\mathbb{r} \circ \mathbb{s} \right) \neq 0. \tag{4.11}$$

By using the commutation of the element-wise product $\circ$ with the usual matrix product, one gets that:

$$\left(\mathbb{v} \circ \mathbb{r} \right)^T \mathbb{F} = 0, \tag{4.12}$$

$$\left(\mathbb{v} \circ \mathbb{r} \right)^T \mathbb{s} \neq 0, \tag{4.13}$$

which means that the vector $\mathbb{v} \circ \mathbb{r}$ has an even number of qubits in common with the support of all stabilisers represented by $\mathbb{F}$, but an odd number in common with the support of the logical operator l_Q^σ represented by $\mathbb{s}$. The only possibility is that $\mathbb{v} \circ \mathbb{r}$ is the support of a logical operator $l_Q^{\sigma'}$ of a different type $\sigma \neq \sigma'$.

Since $\mathbb{r}_q = 1$ if $(\mathbb{v} \circ \mathbb{r})_q = 1$, the column vector $\mathbb{r}$ represents a set of qubits $\boldsymbol{r}$ that contains the support of the logical operator $l_Q^{\sigma'}$. Hence, we prove the statement in both logical directions.

4.3 Tolerance to qubit loss and percolation theory

The question of how tolerant is the color code to qubit loss is studied here by making a connection between percolation theory and the edge erasure from the lattice where the code is defined as a consequence of the qubit loss. Well defined logical operators have support on strings and string-nets with empty support on the set of removed qubits, i.e., strings and string-nets that percolate through the removed qubits in the lattice.

Thus, the percolation of the lattice guarantees that a logical operator is well defined, and consequently, it is equivalent to the preservation of the logical information.

We need to clarify the exact type of percolation that relates with the existence of the logical information. On the one hand, string operators span the shrunk lattices of the color code, so the percolation of the shrunk lattices guarantees the existence of well defined logical operators. On the other hand, since some logical operators have support on string-nets living partially in the three shrunk lattices, even when none of the three shrunk lattices percolates, there might be a well defined string-net logical operator. Thus, the existence of a well defined string-net operator is equivalent to a novel percolation problem on the three coupled shrunk lattices of the color code (see Fig. 4.2 for an illustration of a percolating string-net). Thus, we can obtain the tolerance of the color code to qubit loss in two different ways:

(A) From the percolation of strings in single shrunk lattices. This method defines the *critical qubit loss rate p_c* below which the logical information is preserved. Given that the percolation threshold of the shrunk lattices are well known, one can obtain p_c in a fully analytical way (see Table 4.1 for the values obtained) as described in Sec. 4.3.1.

(B) From the percolation of all strings and string-nets. As this method includes the most general form of a logical operator, it provides the *fundamental threshold p_f* of the color code affected by qubit loss (see Table 4.1 for the values of p_f obtained). In Sec. 4.3.2 we numerically compute the value of p_f.

In the following, the error model we consider is the *erasure channel* which assumes local and uncorrelated losses, each of them happening with probability p. In that noise model p is also the loss density, so the average number of qubits lost in an n-qubit system is pn.

4.3.1   Analytical computation of the critical qubit loss rate

In order to compute p_c analytically, in Sec. 4.4 we derive the *average fraction of edges erased $r(p)$* from a shrunk lattice as a function of the qubit loss rate p. As described in Sec. 4.1, that relation is more complicated for the color code than for the surface code, which is simply $p = r$ since in the surface code every loss qubit erases one edge, and no qubits need to be sacrificed.

Geom.	Shrunk	Geometry	r_c		p_c an.	p_c mf.	p_c num.	p_f
	Red	square	$\frac{1}{2}$	$= 0.5$	0.1877	0.1877	0.2028(7)	0.46(1)
4.8.8	Blue	d.b. square	$\sqrt{\frac{1}{2}}$	$\simeq 0.7071$	0.3093	0.3081	0.292(2)	0.48(3)
	Green	d.b. square	$\sqrt{\frac{1}{2}}$	$\simeq 0.7071$	0.3093	0.3081	0.292(2)	0.48(3)
	Red	triangular	$1 - 2\sin\frac{\pi}{18}$	$\simeq 0.6527$	0.2752	0.2719	0.290(2)	0.33(1)
6.6.6	Blue	triangular	$1 - 2\sin\frac{\pi}{18}$	$\simeq 0.6527$	0.2752	0.2719	0.290(2)	0.33(1)
	Green	triangular	$1 - 2\sin\frac{\pi}{18}$	$\simeq 0.6527$	0.2752	0.2719	0.290(2)	0.33(1)
	Red	kagome	0.4756		0.1764	0.1761	0.165(1)	0.198(2)
4.6.12	Blue	d.b. triangular	$\sqrt{1 - 2\sin\frac{\pi}{18}}$	$\simeq 0.8079$	0.3925	0.3904	0.390(5)	0.438(9)
	Green	d.b. hexagonal	$\sqrt{2\sin\frac{\pi}{18}}$	$\simeq 0.5893$	0.2364	0.2343	0.2012(8)	0.202(1)

Table 4.1: Tolerance of the color code o qubit loss. First column: the three regular color code lattices as depicted in Fig. 3.3. Second column: their respective shrunk lattices. Third column: geometry of the shrunk lattices (d.b. stands for double-bonds). Fourth column: analytical and numerical values of the bond-percolation threshold r_c of the shrunk lattices. In the shrunk lattices with double-bonds, two bonds need to be erased to disconnect two nodes. If we call r the probability of erasure of a bond connecting two nodes, the probability of disconnecting two nodes that are linked via a double bond is r^2. Therefore, the bond-percolation threshold r_c (critical probability of disconnecting two nodes) of a shrunk lattice with double-bonds is the square root of the bond-percolation threshold $\tilde{r}_c$ [213] of the lattice with simple bonds $r_c = \sqrt{\tilde{r}_c}$. For shrunk lattices with single bonds $r_c = \tilde{r}_c$. Fifth column: critical loss threshold p_c obtained analytically from the first three expansion coefficients. Sixth column: critical loss threshold p_c obtained analytically from the mean-field approximation. Seventh column: critical qubit loss rate p_c obtained by a numerical scaling analysis. Eighth column: fundamental loss threshold p_f by a numerical scaling analysis. The number between brackets is the error of the last decimal position.

The critical point p_c corresponds to the qubit loss rate p at which the shrunk lattice does no longer percolate. This happens when the average fraction of edges erased $r(p)$ from the original lattice equals the *bond-percolation threshold r_c* [214] of the shrunk lattice

$$r(p_c) = r_c. \tag{4.14}$$

Therefore, p_c can be obtained analytically from the knowledge of $r(p)$ and r_c as shown in Fig. 4.4 where we plot the curve $r(p)$ and the critical loss rates p_c obtained from the intersection of $r(p)$ with the values of r_c for the three shrunk lattices of the 4.6.12 geometry of the color code. In Table 4.1 we summarise the values of r_c and p_c also for the other geometries.
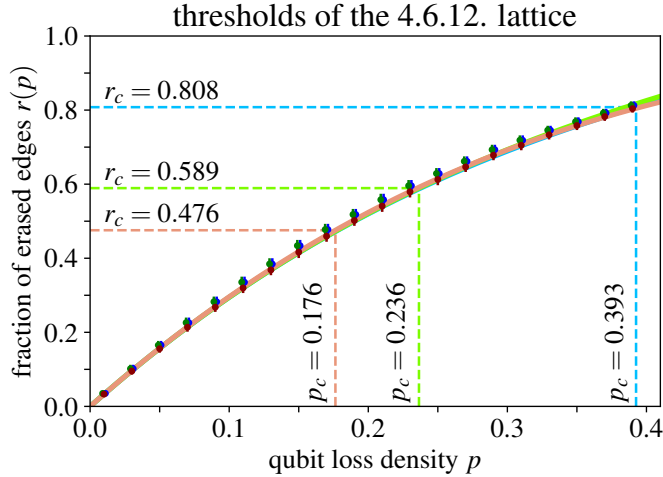
Figure 4.4: Average fraction of edges erased $r(p)$, bond-percolation threshold r_c and critical qubit loss rate p_c for the 4.6.12. lattice. The points correspond to the numerical estimation, while curves are the analytical estimation. The analytical results with the first three coefficients: $r(p) \simeq \alpha_1 p + \alpha_2 p^2 + \alpha_3 p^3$ for the red, blue, and green shrunk lattices are represented by the red, blue, and green points and curves, respectively. By comparing the analytical curves with the bond-percolation thresholds r_c taken from Table 4.1 we obtain the loss thresholds p_c of the shrunk lattices. The numerical data is obtained by a Monte-Carlo sampling of losses at various values of the qubit loss rate p.

The bond-percolation thresholds r_c as well as the functions $r(p)$ depend on the shrunk lattice geometry. A value of p_c is then obtained for each of the three shrunk lattices in each of the three regular geometries of the color code depicted in Fig. 3.3.

We study the bond-percolation problem of the shrunk lattice instead of the site-percolation problem because the erased edges of the lattice of the color code coincide with the erased edges of the shrunk lattices, while the removed qubits do not sit on the nodes of the shrunk lattice (observe in Fig. 3.3 that the nodes of the shrunk lattices are centred on the faces).

We would like to point out that in the bond-percolation problem the edges erased are uniformly distributed in the graph. However, this is not the case in the color code since the edges erased to correct a qubit loss are generally erased in groups, as shown in Fig. 4.3, where the five edges erased are close to each other. However, we assume a uniform distribution of qubit losses without any spatial correlation, so the edges erased are approximately uniformly distributed, and therefore, one can safely identify r_c with $r(p_c)$.

Before moving into the details, we present here the results obtained regarding the fraction of edges erased $r(p)$ and the qubit loss rate p_c below which the logical information is protected. These results include: (A.1) the analytical function $r(p)$ derived in Sec. 4.4, and (A.2) the critical loss rate p_c obtained by solving Eq. (4.14). (A.3) We also compare $r(p)$ with numerical simulations and, (A.4) compute p_c numerically via a scaling analysis.

(A.1) We compute $r(p)$ by calculating the first three expansion coefficients α_1, α_2, α_3:

$$r(p) \simeq \alpha_1 p + \alpha_2 p^2 + \alpha_3 p^3 \tag{4.15}$$

with the tools described in Sec. 4.4 for the three shrunk lattices of the three regular geometries of the color code (values are summarised in Table 4.2), and by the analytical mean-field approximation obtained in Sec. 4.4.4:

$$r(p) \simeq 1 - (1 - p)^{2R_1}. \tag{4.16}$$

(A.2) Then, using the bond-percolation thresholds r_c, we obtain p_c analytically by solving Eq. (4.14) (A.2.i) up to third order with the calculated coefficients:

$$r_c = \alpha_1 p_c + \alpha_2 p_c^2 + \alpha_3 p_c^3, \tag{4.17}$$

and with the expression in Eq (4.16):

$$p_c = 1 - (1 - r_c)^{\frac{1}{2R_1}}. \tag{4.18}$$

The values of r_c and p_c are summarised in Table 4.1. At the critical point, $r(p)$ crosses the value of the bond-percolation threshold r_c as we show in Figs. 4.4 for the 4.6.12 lattice, and in Fig. 4.5 for each of the three shrunk lattices of the three regular geometries of the color code. As one can see in Fig. 4.4, the curves $r(p)$ for the three shrunk lattices of the 4.6.12 color code lattice are almost superposed. Indeed, all curves depicted in Fig. 4.5 corresponding to all shrunk lattices of all lattice geometries are almost superposed (not shown). Besides, the function in Eq. (4.16) obtained with the mean-field approximation, which does not depend on the geometry of the shrunk lattice, also superposes to the other curves in the range $p \in [0.1, 0.4]$ that is relevant to obtain p_c, as

Geom.	Shrunk	I_1	R_1	E_1	α_1	I_2	$\bar{R}_2$	$\bar{E}_2$	α_2	I_3	$\bar{R}_3$	$\bar{E}_3$	α_3
	Red	1	$\frac{5}{3}$	$\frac{5}{3}$	$\frac{10}{3}$	11	$\frac{295}{99}$	$-\frac{35}{99}$	$-\frac{35}{9}$	72	$\frac{3995}{972}$	$\frac{35}{972}$	$\frac{140}{81}$
4.8.8	Blue	1	$\frac{5}{3}$	$\frac{5}{3}$	$\frac{10}{3}$	9	$\frac{233}{81}$	$-\frac{37}{81}$	$-\frac{37}{9}$	102	$\frac{5749}{1377}$	$\frac{95}{2754}$	$\frac{190}{81}$
	Green	1	$\frac{5}{3}$	$\frac{5}{3}$	$\frac{10}{3}$	9	$\frac{233}{81}$	$-\frac{37}{81}$	$-\frac{37}{9}$	102	$\frac{5749}{1377}$	$\frac{95}{2754}$	$\frac{190}{81}$
	Red	1	$\frac{5}{3}$	$\frac{5}{3}$	$\frac{10}{3}$	11	$\frac{295}{99}$	$-\frac{35}{99}$	$-\frac{35}{9}$	122	$\frac{14161}{3294}$	$\frac{29}{1647}$	$\frac{116}{81}$
6.6.6	Blue	1	$\frac{5}{3}$	$\frac{5}{3}$	$\frac{10}{3}$	11	$\frac{295}{99}$	$-\frac{35}{99}$	$-\frac{35}{9}$	122	$\frac{14161}{3294}$	$\frac{29}{1647}$	$\frac{116}{81}$
	Green	1	$\frac{5}{3}$	$\frac{5}{3}$	$\frac{10}{3}$	11	$\frac{295}{99}$	$-\frac{35}{99}$	$-\frac{35}{9}$	122	$\frac{14161}{3294}$	$\frac{29}{1647}$	$\frac{116}{81}$
	Red	1	$\frac{5}{3}$	$\frac{5}{3}$	$\frac{10}{3}$	11	$\frac{295}{99}$	$-\frac{35}{99}$	$-\frac{35}{9}$	64	$\frac{7057}{1728}$	$\frac{1}{27}$	$\frac{128}{81}$
4.6.12	Blue	1	$\frac{5}{3}$	$\frac{5}{3}$	$\frac{10}{3}$	9	$\frac{233}{81}$	$-\frac{37}{81}$	$-\frac{37}{9}$	91	$\frac{10214}{2457}$	$\frac{89}{2457}$	$\frac{178}{81}$
	Green	1	$\frac{5}{3}$	$\frac{5}{3}$	$\frac{10}{3}$	9	$\frac{233}{81}$	$-\frac{37}{81}$	$-\frac{37}{9}$	102	$\frac{5749}{1377}$	$\frac{95}{2754}$	$\frac{190}{81}$

Table 4.2: Analytical results of the expansion of the fraction of edges erased $r(p)$**.** Representative factors for $\ell = 1, 2, 3$ losses for the three shrunk lattices in three regular geometries of the color code. The number of fully-interacting instances is I_ℓ, the average number of edges erased by them is $\bar{R}_\ell$, and the average energy associated is $\bar{E}_\ell$. These quantities are introduced in Sec. 4.4.2. The coefficients of the power expansion in Eq. (4.21) are α_ℓ. All these quantities have been obtained analytically without performing any approximation.

depicted in Fig. 4.6. This seems to indicate that $r(p)$ does not depend strongly on the geometry of the shrunk lattice. Therefore, the differences between the values of p_c in the shrunk lattices depend mostly on their bond-percolation threshold r_c, which is an indication of the strong connection between percolation theory and the tolerance of the color code to qubit loss.

(A.3) We also estimate $r(p)$ numerically by performing a Monte Carlo sampling of qubit loss instances for various values of the qubit loss rate p, and computing the average number of edges erased to correct every instance with a randomly chosen correction. We consider lattices with the three geometries and with a number of qubits close to 4000. The numerical points obtained are compared with the analytical expansion of $r(p)$ expressed in Eq. (4.15) in Figs. 4.4 and 4.5. The error bars are comparable to the point size. In the range $p \in [0.1, 0.4]$ the maximum difference between the analytical (up to third order) and the numerical values of $r(p)$ is below 6%. In Fig. 4.7 we compare the
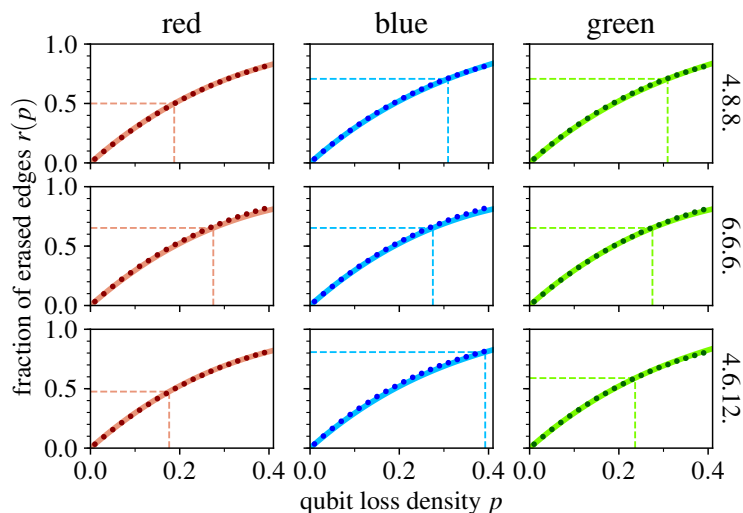
Figure 4.5: Average fraction of edges erased $r(p)$ as a function of the qubit loss rate p for every shrunk lattice of the three regular geometries of the color code. The continuous line correspond to the first three orders in the expansion of $r(p)$ in powers of p (Eq. (4.21)). The coefficients of that curve were obtained analytically without performing any approximation. The numerical data (dots) is obtained by a Monte-Carlo sampling of losses at various values of the qubit loss rate p.

numerical data with the first three orders of $r(p)$ to show how the curves approximate the numerical data as more expansion terms are added. Moreover, we compare the numerical results with the mean-field estimation introduced in Eq. (4.16) as well as the expansion of $r(p)$ expressed in Eq. (4.15) in Fig. 4.6. As one can see, the result of the mean-field approximation superposes the analytical expansion and the numerical results. The maximum difference in the range $p \in [0.1, 0.4]$ between the mean-field approximation and the expansion is 0.5%, and 1% when the mean-field approximation is compared with the numerical results. Limitations of the numerical analysis like the finite-size effects, or the difficulty of sampling instances with a low number of qubits lost are the main sources of discrepancy between the analytical and the numerical analyses.

(A.4) We also obtain p_c numerically by means of the scaling analysis depicted in the first column of Fig. 4.8 in the following way: In a square code of code distance D, we compute the critical fraction of losses $p_c(D)$ at which, for the first time, a percolating string ceases to exist. It is known that percolation theory predicts [214] the scaling of p_c as $D \to \infty$ to be $p_c(D) - p_c(\infty) \propto D^{-1/\nu}$, with the scaling exponent $\nu = 4/3$. As expected, this scaling law is followed by the numerical data. From it, we obtain
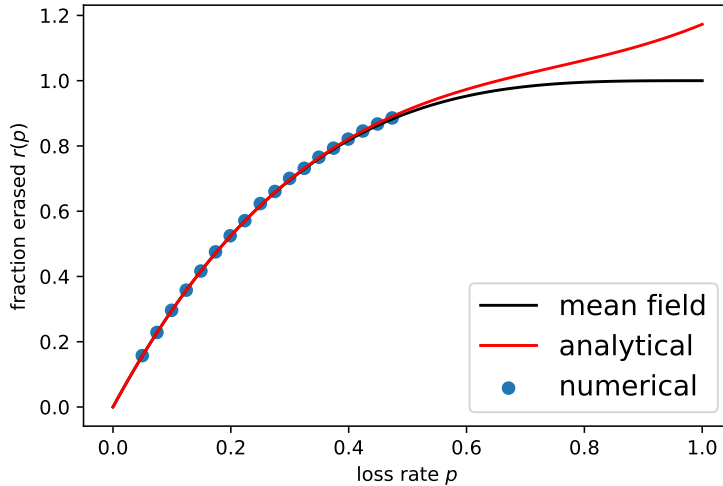
Figure 4.6: Comparison of methods to compute the average fraction of edges erased $r(p)$. Here we plot the three results of the estimation of $r(p)$: (red) the expression in Eq. (4.15) by analytically computing the expansion coefficients α_1, α_2, α_3, (black) the expression $r(p) \simeq 1 - (1 - p)^{2R_1}$ obtained with the mean field approximation, and (blue circles) the numerical results explained in this section.

numerically the value of the critical qubit loss rate p_c in the thermodynamic limit (when $D^{-1/\nu} \to 0$). The values of p_c obtained numerically by this scaling method are in great accordance with the values obtained by the analytical analysis as can be seen in Table 4.1: the maximum difference is below 8%.

4.3.2 Numerical computation of the fundamental qubit loss rate

In relation to (B), i.e., the fundamental qubit loss threshold p_f obtained by taking into account all existing logical operators, including the ones with support on string-nets, was obtained by numerically by generating Monte-Carlo instances of qubit losses in a color code and employing on each one the algebraic technique described in Sec. 4.2.1 that determines if the logical information is preserved. In this section we show how this technique is used in a scaling analysis to obtain numerically the fundamental qubit loss threshold p_f of the color code, and then compare the values of p_c and p_f obtained.

The same scaling analysis performed in (A.4) to obtain p_c is applied to obtain the fundamental loss threshold p_f (second column of Fig. 4.8). The only difference is that the percolation check is replaced by checking the existence of a subset of stabilisers S that are a solution of Eq. (4.1). The resulting values of p_f show the robustness of
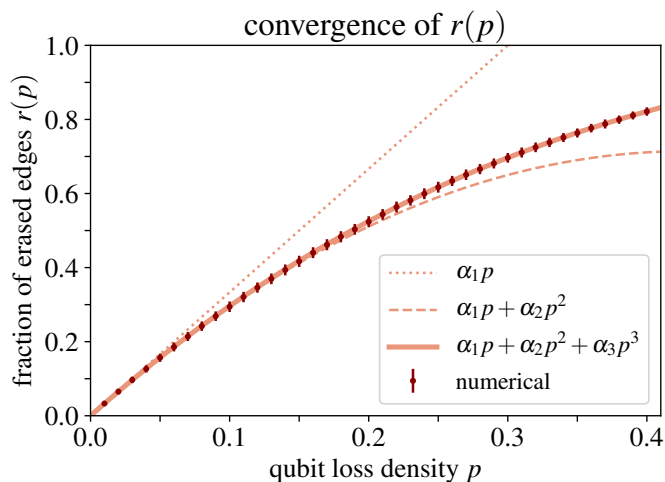
Figure 4.7: Convergence of the first three orders in the power expansion of the average fraction of edges erased $r(p)$ for the red shrunk lattice of the 4.8.8 geometry of the color code. We compute analytically the first three coefficients α_1, α_2, α_3 in Eq. (4.21). The dotted line is the first order of the power expansion, the dashed line contains up to the second order, and the continuous line up to the third order. The lines approach the numerical data (red dots) as more orders are added. The numerical data is obtained by a Monte-Carlo sampling of losses at various values of the qubit loss rate p and a posterior scaling analysis.

color codes under qubit loss: for example, the 4.8.8 geometry can tolerate the loss of the $46(1)\%$ of the qubits before the first class of logical operators becomes ill defined, which is close to the 50% limit imposed by the no-cloning theorem [196].

The differences between the values of p_c and p_f, which are easy to visualise in Fig. 4.8, can be understood by the relation between the two percolation problems that we consider: the percolation of the three decoupled shrunk lattices (provides p_c), and the generalised percolation of the coupled shrunk lattices (provides p_f). Intuitively, p_f is higher than p_c because strings in a shrunk lattices with a low bond-percolation threshold r_c can branch into the other shrunk lattices to increase their tolerance to the erase of edges. For example in the 4.8.8 lattice the red shrunk lattice has a bond-percolation threshold of $1/2$ while the bond-percolation threshold of the blue and the green shrunk lattices is higher: $1/\sqrt{2}$. Then, the possibility of branching increases the critical qubit loss rate of the red shrunk lattice of the 4.8.8 geometry from $p_c \simeq 0.19$ to the fundamental threshold $p_f \simeq 0.46$. On the other hand, since a string in a shrunk lattice needs the two other lattices to branch, the maximum that p_f can reach is given
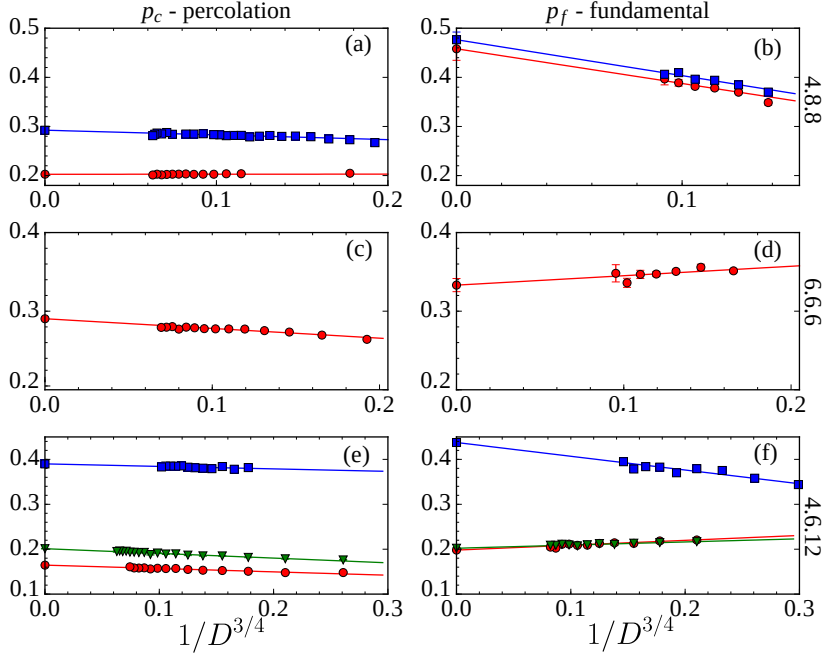
Figure 4.8: Critical qubit loss rate p_c and fundamental qubit loss rate p_f obtained numerically. By sampling loss instances with a Monte Carlo method, we compute the values of p_c (percolation), and p_f (fundamental) for various values of the code distance D for the three regular geometries of the color code. The thresholds are plotted as a function of $1/D^{1/\nu}$ with a critical exponent $\nu = 4/3$ as expected from the percolation theory. Red circles, blue squares and green triangles represent the numerical data for the red, blue and green shrunk lattices, respectively. The continuous lines fit the points and their intercepts (marked with the same symbols as the data) give the critical threshold in the limit $D \to \infty$. In the graphs (a), (b) for the 4.8.8 lattice, the green shrunk lattice is not represented because it has the same geometry as the blue. In (c), (d) the blue and the green shrunk lattices of the 6.6.6 lattice have the same geometry as the red, so only the red is represented. In (e), (f) for the 4.6.12 lattice, the three shrunk lattices are represented.

by the smallest threshold of the other two shrunk lattices. For example, the red shrunk lattice of the 4.6.12 geometry does not improve its tolerance by much (from $p_c \simeq 0.17$ to $p_f \simeq 0.20$) by branching into the blue and the green shrunk lattices (despite that the bond-percolation threshold of the blue shrunk lattice is high: $r_c \simeq 0.81$ and $p_c \simeq 0.39$) because the green shrunk lattice has a low bond-percolation threshold: $r_c \simeq 0.59$ and $p_c \simeq 0.24$.

We would like to stress that the study of tolerance presented in this section assumes the perfect realization of every element of the quantum error correcting code, so the tolerance presented by the three geometries of the color code depends only on their per-

colation properties. In practice, different geometries present different error correction properties: different number of entangling gates and ancillary qubits, different sets of transversal gates, different connectivity constraints between qubits, etc... Therefore, when assessing the performance of the color code geometries in practice, the tolerance to qubit loss has to be balanced with the other quantum error correction properties. However this analysis is beyond the scope of this thesis.

4.4   Average fraction of edges erased

As mentioned previously, $r(p)$ is the average fraction of edges erased, i.e., the number of edges erased divided by the total number of edges $e = n/2$ (n being the total number of qubits) in one shrunk lattice, averaged over all possible loss instances that can happen at a qubit loss density p and averaged over all possible corrections of each loss instance. Here, we obtain $r(p)$ analytically using a systematic way for averaging over corrections as shown in Sec. 4.4.1, and then, averaging over loss instances as described in Sec. 4.4.2.

4.4.1   Average over corrections

Let us define a qubit *loss instance* $\boldsymbol{\ell}$ as a set $\boldsymbol{\ell} = \{q_1, q_2, \ldots\}$ containing the positions of the $\ell = |\boldsymbol{\ell}|$ qubits lost. In step (ii) of the protocol, we choose randomly the order in which qubit losses are corrected and then, randomly again, we select the qubits that are sacrificed. Each of those random selections constitute a single *correction* of the loss instance $\boldsymbol{\ell}$, and is represented by an ordered list $\vec{\boldsymbol{\kappa}} = (q_{s_1}, q_{s_2}, \ldots)$, where the order corresponds to the order in which sacrificed qubits q_s are selected. The number of sacrificed qubits might be smaller than the number of qubit losses if an already lost qubit is chosen as a sacrificed qubit. In that case, we consider that qubit a lost qubit rather than a sacrificed qubit (see the example (b.1) in Fig. 4.10). If we select with equal probability $(\ell!)^{-1}$ each of the $\ell!$ orderings of lost qubits, and select with equal probability $1/3$ each sacrificed qubit out of the three neighbours of each loss, the probability of a correction $\vec{\boldsymbol{\kappa}}$ is $p_{\vec{\boldsymbol{\kappa}}} = (\ell!)^{-1} 3^{-|\vec{\boldsymbol{\kappa}}|}$, where $|\vec{\boldsymbol{\kappa}}|$ is the size of $\vec{\boldsymbol{\kappa}}$, i.e., the number of sacrificed qubits.

In step (iii) the lattice is modified according to the loss instance $\boldsymbol{\ell}$ that occurred and the correction $\vec{\boldsymbol{\kappa}}$ selected. The number of edges erased from the original shrunk

$$\vec{\kappa} = (q_s) \qquad \vec{\kappa}' = (q_s') \qquad \vec{\kappa}'' = (q_s'')$$
$$p_{\vec{\kappa}} = 1/3 \qquad p_{\vec{\kappa}'} = 1/3 \qquad p_{\vec{\kappa}''} = 1/3$$
$$\mathsf{R}_{\vec{\kappa}} = 1 \qquad \mathsf{R}_{\vec{\kappa}'} = 2 \qquad \mathsf{R}_{\vec{\kappa}''} = 2$$

$$R_1 = \frac{5}{3}$$
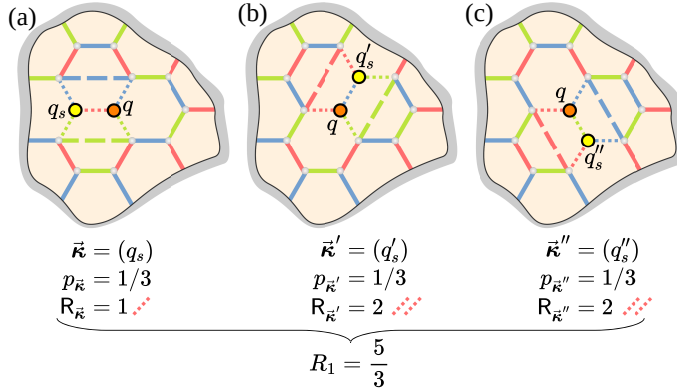
Figure 4.9: Correction of one qubit loss. There are three possible corrections $\vec{\kappa}$ for an instance of one qubit loss $\ell = \{q\}$ (orange dot) depending on the selection of a neighbouring qubit to sacrifice: (a) the qubit q_s on the red edge, (b) the qubit q_s' on the blue edge, (c) the qubit q_s'' on the green edge. Each correction is chosen with a probability $p_{\vec{\kappa}} = 1/3$. The number of red edges erased (red dotted lines) is (a) $\mathsf{R}_{\vec{\kappa}} = 1$, (b) $\mathsf{R}_{\vec{\kappa}'} = 2$, and (c) $\mathsf{R}_{\vec{\kappa}''} = 2$. Therefore, the average number of edges erased from the red shrunk lattice by a one-loss event is $R_1 = 5/3$. This value is the same for every loss instance of one qubit loss and for every shrunk lattice.

lattice is $\mathsf{R}_{\vec{\kappa}}$, and the number of edges erased averaged over the set $\mathcal{K}_\ell$ of all possible corrections of ℓ is:

$$R_\ell = \sum_{\vec{\kappa} \in \mathcal{K}_\ell} p_{\vec{\kappa}} \mathsf{R}_{\vec{\kappa}}. \tag{4.19}$$

Note that, as we are interested in the percolation of the original shrunk lattice before being modified by the corrections, in Eq. (4.19) only the edges belonging to the original shrunk lattice are counted.

As we show in Fig. 4.9, for a loss instance with only one qubit lost $\ell = \{q_1\}$, there are three possible corrections $\vec{\kappa}$ happening with a probability $p_{\vec{\kappa}} = 1/3$, one for each selection of a sacrificed qubit q_{s_1}. The corrections erase $\mathsf{R}_{\vec{\kappa}} = 1$, $\mathsf{R}_{\vec{\kappa}'} = 2$, and $\mathsf{R}_{\vec{\kappa}''} = 2$ red edges, so the average number of edges erased from the original red shrunk lattice to correct $\{q_1\}$ is:

$$R_1 = \frac{5}{3}. \tag{4.20}$$

The value of R_1 is the same for every loss instance containing only one loss and it is also the same for every shrunk lattice. Moreover, since every color code is defined on a trivalent lattice, R_1 is the same for every (also irregular) geometry.

In Fig. 4.10 we show two possible corrections of a two-qubit loss instance $\ell = \{q_1, q_2\}$. In the correction depicted in (b.1), the qubit sacrificed q_{s_1} to correct the loss
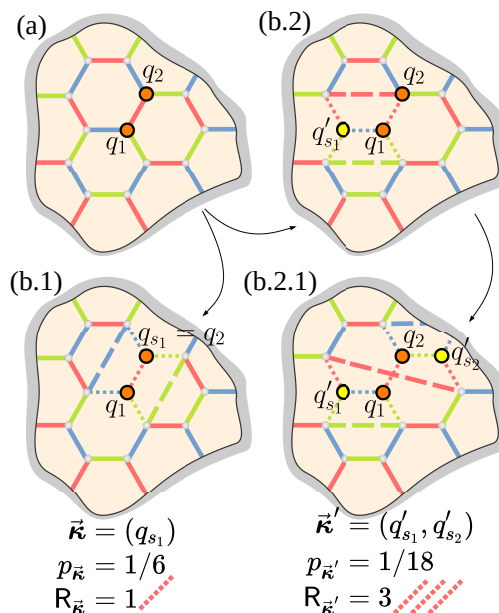
Figure 4.10: Corrections of a loss instance with two qubit losses. To correct a loss instance $\boldsymbol{\ell} = \{q_1, q_2\}$ like the one in (a) composed by two losses indicated with orange dots, the protocol first chooses the order in which the losses are corrected. In that case, the order (q_1, q_2) is chosen with a probability of $1/2$. To correct the first loss q_1, any of the three neighbouring qubits can be chosen with a probability $1/3$ as the sacrificed qubit q_{s_1}. In (b.1) the loss q_2 has been chosen as the sacrificed qubit, so there is no need to correct the loss q_2. The correction is $\vec{\boldsymbol{\kappa}} = (q_{s_1})$. The probability of that correction is $p_{\vec{\boldsymbol{\kappa}}} = (1/2)(1/3) = 1/6$ and $\mathsf{R}_{\vec{\boldsymbol{\kappa}}} = 1$ red edges are erased (red dotted lines). In (b.2) a qubit different from the loss q_2 has been chosen as the sacrificed qubit q'_{s_1} (yellow dot), and the lattice has been modified accordingly. Then, in (b.2.1) a sacrificed qubit q'_{s_2} has been chosen to correct the loss q_2 producing the final erasure of $\mathsf{R}_{\vec{\boldsymbol{\kappa}}'} = 3$ red edges with a probability $p_{\vec{\boldsymbol{\kappa}}'} = (1/2)(1/3)^2 = 1/18$, where the correction is $\vec{\boldsymbol{\kappa}}' = (q'_{s_1}, q'_{s_2})$. Note that the new red edge added in (b.2) has not been counted as an erased edge in (b.2.1), because in $\mathsf{R}_{\vec{\boldsymbol{\kappa}}}$ we count only those edges erased from the original lattice.

q_1 coincides with the second loss q_2, so no second qubit needs to be sacrificed to correct q_2. The probability of that correction is then $p_{\vec{\boldsymbol{\kappa}}} = 1/6$. This correction shows that the set of lost and sacrificed qubits can overlap. In the correction depicted in (b.2.1) two qubits q'_{s_1} and q'_{s_2} have been sacrificed, so the probability is $p_{\vec{\boldsymbol{\kappa}}'} = 1/18$. Note that the $\mathsf{R}_{\vec{\boldsymbol{\kappa}}'} = 3$ edges erased are counted only from the original shrunk lattice.

4.4.2 Average over qubit loss instances

The error model we consider is the *erasure channel*, which assumes local and uncorrelated losses at known positions of qubits, each of these losses happening with probability

p. Here p is also the loss density, so the average number of qubits lost is pn. If the density is low, qubit losses predominantly occur far apart from each other, so they can be treated independently, and therefore, the average number of edges erased per loss is close to $R_1 = 5/3$, giving an average fraction of edges erased of $R_1 pn/e = 2R_1 p$. Then, the average fraction of edges erased grows linearly with p for low densities:

$$r(p) = 2R_1\, p + \sum_{\ell \geq 2} \alpha_\ell\, p^\ell. \tag{4.21}$$

Our goal is to systematically compute the coefficients α_ℓ up to a given desired order ℓ. These coefficients are corrections to the linear behaviour and they are determined by the *interaction* that takes place between losses that are close to each other. We say that ℓ losses *interact* if the number of edges erased from the original lattice to correct those losses is less than ℓR_1, which is the number of edges erased if these losses are far apart from each other. Given that the interaction between losses reduces the number of edges erased, and that the number of interacting instances increases with the density p of losses, the erasure of edges slows down as p increases.

The interaction may come in different fashions as depicted in Fig. 4.10. For example, in correction (b.1) there is interaction because the sacrificed qubit coincides with a lost qubit, and in the correction (b.2.1), there is another type of interaction because one of the edges erased to correct the qubit loss q_2 is not an edge from the original shrunk lattice but rather a new edge added from the correction of the first loss q_1, and therefore, it is not counted in $r(p)$. If one computes the number of edges erased $R_{\{q_1,q_2\}}$ to correct that loss instance as specified by Eq. (4.19) the result is that $R_{\{q_1,q_2\}} < 2R_1$, which indicates an interaction between losses q_1 and q_2.

The interaction between losses can be understood by thinking about the number of edges erased as a sum of *energies*. A single-loss instance $\{q\}$ erases an average of R_1 edges as explained in Fig. 4.9, so let us define $E_{\{q\}} = R_1$ as the *internal energy* of every single loss. As mentioned, an instance $\{q_1, q_2\}$ with two losses erases a number $R_{\{q_1,q_2\}}$ of edges that might be smaller than $2R_1$, so in that case, there is a non-vanishing interaction energy $E_{\{q_1,q_2\}}$ that makes $R_{\{q_1,q_2\}}$ smaller than $2R_1$. We define the two-body interaction energy from the energy sum $R_{\{q_1,q_2\}} = E_{\{q_1\}} + E_{\{q_2\}} + E_{\{q_1,q_2\}}$. Note that $E_{\{q_1,q_2\}} = 0$ if the losses do not interact. Analogously, an instance $\{q_1, q_2, q_3\}$ of

three losses erases a number of edges that can be expressed as:

$$R_{\{q_1,q_2,q_3\}} = E_{\{q_1\}} + E_{\{q_2\}} + E_{\{q_3\}} + E_{\{q_1,q_2\}} + E_{\{q_1,q_3\}} + E_{\{q_2,q_3\}} + E_{\{q_1,q_2,q_3\}}, \quad (4.22)$$

where $\{q_1,q_2\}$, $\{q_1,q_3\}$, $\{q_2,q_3\}$ are the two-body instances contained in $\{q_1,q_2,q_3\}$.

Following this idea, one can write the number of edges erased by any instance as a sum of energies:

$$R_{\boldsymbol{\ell}} = \sum_{\boldsymbol{\ell}' \subset \boldsymbol{\ell}} E_{\boldsymbol{\ell}'}, \quad (4.23)$$

where the sum is performed over all subsets $\boldsymbol{\ell}'$ of the set $\boldsymbol{\ell}$. For the empty set $\emptyset \subset \boldsymbol{\ell}$ we define the interaction energy $E_{\emptyset} = 0$ as zero, while for all single-loss instances $\boldsymbol{\ell} = \{q\}$ the energy is $E_{\{q\}} = R_1$. Equation (4.23) can be represented by a full-rank linear system between $\{R_{\boldsymbol{\ell}}\}$ and $\{E_{\boldsymbol{\ell}}\}$. By inverting it, one obtains the energies defined by the number of edges erased:

$$E_{\boldsymbol{\ell}} = (-1)^{|\boldsymbol{\ell}|} \sum_{\boldsymbol{\ell}' \subset \boldsymbol{\ell}} (-1)^{|\boldsymbol{\ell}'|} R_{\boldsymbol{\ell}'}, \quad (4.24)$$

where $R_{\emptyset} = 0$ and $R_{\boldsymbol{\ell}'} = R_1$ for all $\boldsymbol{\ell}'$ with $|\boldsymbol{\ell}'| = 1$. See Appendix A.1 for the proof of this relation.

Now we can show that the coefficients $\alpha_{\boldsymbol{\ell}}$ are given by the fully-interacting energies. In the model each loss happens with probability p, so the probability of a loss instance $\boldsymbol{\ell}$ is $p^{|\boldsymbol{\ell}|}(1-p)^{n-|\boldsymbol{\ell}|}$. If the average number of edges erased to correct $\boldsymbol{\ell}$ is $R_{\boldsymbol{\ell}}$, the average fraction of edges erased can be written as:

$$r(p) = e^{-1} \sum_{\boldsymbol{\ell} \in \mathcal{I}} p^{|\boldsymbol{\ell}|}(1-p)^{n-|\boldsymbol{\ell}|} R_{\boldsymbol{\ell}}, \quad (4.25)$$

where $\mathcal{I}$ is the set of all possible loss instances. By expanding in powers of p as done in Appendix A.2 and using Eq. (4.24) one can identify the coefficients $\alpha_{\boldsymbol{\ell}}$ of Eq. (4.21) with the energies:

$$\alpha_{\ell} = e^{-1} \sum_{\boldsymbol{\ell} \in \mathcal{I},\, |\boldsymbol{\ell}|=\ell} E_{\boldsymbol{\ell}}. \quad (4.26)$$

This result shows that the ℓ-th coefficient α_{ℓ} is given by the interaction energies of ℓ losses.

However, many energies are zero. For example, as mentioned earlier, the interaction energy of two losses that are far apart from each other vanishes. Analogously, if an instance $\boldsymbol{\ell}$ can be split into two disjoint, non-empty subsets $\boldsymbol{\ell}^{(A)} \cup \boldsymbol{\ell}^{(B)} = \boldsymbol{\ell}$ such that $R_{\boldsymbol{\ell}} = R_{\boldsymbol{\ell}^{(A)}} + R_{\boldsymbol{\ell}^{(B)}}$ the interaction energy $E_{\boldsymbol{\ell}} = 0$ vanishes (proof in Appendix A.3), and we call $\boldsymbol{\ell}$ a *separable instance*. This happens because the parts $\boldsymbol{\ell}^{(A)}, \boldsymbol{\ell}^{(B)}$ are too far from each other to interact. On the contrary, the instances that cannot be divided in this way are called *fully-interacting* instances, and their energy is non-zero. Therefore the sum over $\mathcal{I}$ in Eq. (4.26) can be reduced to the sum over fully-interacting instances $\mathcal{I}^{(\text{f-i})}$ only.

Observe that the values of many energies are repeated in $\mathcal{I}^{(\text{f-i})}$ since there are loss instances that are equal up to the symmetries of the lattice of the color code. In the regular geometries of the color code, every node is indistinguishable under the symmetries of the lattice, so one can represent the set of all fully-interacting instances $\mathcal{I}^{(\text{f-i})}$ by the set of all fully-interacting instances $\mathcal{I}_{q_1}^{(\text{f-i})}$ that have the qubit loss q_1 in common. Then, considering this symmetry, every instance $\boldsymbol{\ell} \in \mathcal{I}_{q_1}^{(\text{f-i})}$ is repeated $n/|\boldsymbol{\ell}|$ times in $\mathcal{I}^{(\text{f-i})}$. Therefore, Eq. (4.26) can be reduced to:

$$\alpha_\ell = 2\ell^{-1} \sum_{\boldsymbol{\ell} \in \mathcal{I}_{q_1}^{(\text{f-i})}, \, |\boldsymbol{\ell}| = \ell} E_{\boldsymbol{\ell}}, \tag{4.27}$$

where we used that $e = n/2$ in the thermodynamic limit.

For a concrete example, in Fig. 4.11, on the horizontal axis we show the values of the energies $E_{\boldsymbol{\ell}}$ of the interacting instances $\boldsymbol{\ell} = \{q_1, q_2\} \in \mathcal{I}_{q_1}^{(\text{f-i})}$ and, on the vertical axis, the number of instances that have the same energy. These energies $E_{\boldsymbol{\ell}}$ are the ones that appear in Eq. (4.27). By recalling that, from Eq. (4.24), the energy $E_{\boldsymbol{\ell}}$ is given by the difference between the number of edges erased by the two-loss instance $\{q_1, q_2\}$ and the number of edges erased separately by each of the single loss $\{q_1\}, \{q_2\}$, it is clear that the instance that has the highest energy (in absolute value) corresponds to the couple of qubits residing at the smallest possible distance, as depicted in panel (a). Likewise, the instance that has the smallest energy (in absolute value) is the one where the qubits are at the largest distance that still allows for some corrections to erase a common edge (panel (b)), producing an interaction.

Note that to be fully-interacting, all losses in an instance $\boldsymbol{\ell} \in \mathcal{I}_{q_1}^{(\text{f-i})}$ must be within a finite distance from q_1. Then, the number of instances in $\mathcal{I}_{q_1}^{(\text{f-i})}$ that have up to a
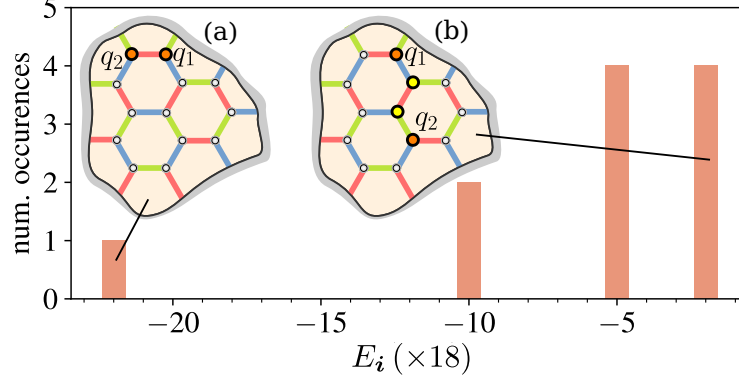
Figure 4.11: Energies E_ℓ of instances $\ell \in \mathcal{I}_{q_1}^{\text{(f-i)}}$ of two losses q_1, q_2 for the red shrunk lattice of the 6.6.6 geometry of the color code. In the horizontal axis we indicate the value of the interacting energies computed from the averaged number of edge erased (Eq. (4.24)). These energies are rescaled by a factor of $2! \cdot 3^2 = 18$ that represents the number of all possible corrections for each instance with two losses. In the vertical axis we indicate the occurrence of each energy, i.e., the number of instances $\ell \in \mathcal{I}_{q_1}^{\text{(f-i)}}$ that have the same energy E_ℓ. The unique instance that has the highest energy (in absolute value) is depicted in (a), while one of the four instances with the smallest energy (in absolute value) is depicted in (b). The other three instances with the same energy as (b) can be found by lattice symmetries. The instance in (b) corresponds to an interacting instance since the red edge between the two sacrificed qubits (yellow circles) is erased to correct both qubit losses.

certain number of losses ℓ does not depend on the lattice size n. From the number I_ℓ of instances in $\mathcal{I}_{q_1}^{\text{(f-i)}}$ with ℓ losses one can compute the following averages, which are independent of the system size n:

$$\bar{R}_\ell = I_\ell^{-1} \sum_{\ell \in \mathcal{I}_{q_1}^{\text{(f-i)}},\, |\ell|=\ell} R_\ell, \tag{4.28}$$

$$\bar{E}_\ell = I_\ell^{-1} \sum_{\ell \in \mathcal{I}_{q_1}^{\text{(f-i)}},\, |\ell|=\ell} E_\ell. \tag{4.29}$$

Note that there is only one instance of one loss, so $\bar{R}_1 = \bar{E}_1 = R_1$. Since the interaction does not increase the number of edges erased, the following hierarchy of inequalities is expected:

$$R_1 \geq \frac{\bar{R}_2}{2} \geq \frac{\bar{R}_3}{3} \geq \cdots \geq \frac{\bar{R}_\ell}{\ell} \geq \cdots \geq \frac{1}{2}. \tag{4.30}$$

By using these definitions one finally obtains that the coefficients in the power expansion of $r(p)$ in Eq. (4.21)

$$\alpha_\ell = 2I_\ell \frac{\bar{E}_\ell}{\ell} \tag{4.31}$$

can be seen as the total energy per loss among the fully-interacting instances. Clearly, given that I_ℓ and $\bar{E}_\ell$ do not depend on the system size n, the coefficients α_ℓ are also independent of the system size. This confirms that the average fraction $r(p)$ of edges erased from a shrunk lattice depends only on the density of losses p, which is a clear signature of the connection with the percolation theory.

The algorithm that we used to obtain I_ℓ, $\bar{R}_\ell$, $\bar{E}_\ell$, α_ℓ is described in Sec. 4.4.3, and the values obtained are summarised in Table 4.2.

4.4.3 Computation of the expansion coefficients

In this section we provide an algorithm to compute the expansion coefficients α_ℓ of $r(p)$ in Eq. (4.21). The computation of the first ℓ coefficients as in Eq. (4.27) requires the energies E_ℓ of all the fully-interacting loss instances $\ell \in \mathcal{I}_{q_1}^{(\text{f-i})}$ that have the loss q_1 in common and contain from 2 to ℓ losses. We explain the algorithm for the case of $\ell = 3$ losses, and provide the pseudo-code 4.4.3 for any ℓ. The steps of the algorithm are the following:

1. Place the central loss q_1 on a qubit in the lattice and extract a set of qubits $\boldsymbol{P}$ (we call it a patch) at a finite distance from q_1. By *distance* between two nodes we mean the number of edges in the shortest path that connects these nodes. In order to consider all fully-interacting instances in $\mathcal{I}_{q_1}^{(\text{f-i})}$ that contain up to ℓ losses it is enough to set a maximum distance of $3(\ell - 1)$ from q_1. For $\ell = 3$, the patch $\boldsymbol{P}$ contains the qubits that are at a distance 6 or less from q_1.

2. Initialise an empty list $\mathcal{I}$ that will contain all loss instances inside the patch, the number of edges that they erase and the associated energies.

3. For every instance $\{q_2, q_3\} \subset \boldsymbol{P}$ with two different losses and $q_1 \notin \boldsymbol{\ell}$ one has to compute $R_{\{q_2,q_3\}}$ from Eq. (4.19) by averaging the number of edges erased over all possible corrections. Then, one has to compute the energy of the instance $\{q_2, q_3\}$ that from Eq. (4.24) takes the form:

$$E_{\{q_2,q_3\}} = R_{\{q_2,q_3\}} - 2R_1. \tag{4.32}$$

Recall that for all instances $\{q\}$ with only one loss, $R_{\{q\}} = R_1$ as explained in Sec. 4.4.1. Append the element $\left[\{q_2, q_3\}, R_{\{q_2,q_3\}}, E_{\{q_2,q_3\}}\right]$ to the list $\mathcal{I}$.

4. For every instance $\{q_1, q_2, q_3\} \subset \boldsymbol{P}$ with three different losses (one of them the central loss q_1) one has to compute $R_{\{q_1, q_2, q_3\}}$ from Eq. (4.19), then compute the energy of the instance from Eq. (4.24), which takes the form:

$$E_{\{q_1, q_2, q_3\}} = R_{\{q_1, q_2, q_3\}} - R_{\{q_1, q_2\}} - R_{\{q_1, q_3\}} - R_{\{q_2, q_3\}} + 3R_1, \qquad (4.33)$$

where we used again that for all instances $\{q\}$ with only one loss, $R_{\{q\}} = R_1$. Note that the values of $R_{\{q_1, q_2\}}$, $R_{\{q_1, q_3\}}$, $R_{\{q_2, q_3\}}$ are stored in $\mathcal{I}$ for every $q_2, q_3 \in \boldsymbol{P} \setminus \{q_1\}$. Append the element $\left[\{q_1, q_2, q_3\}, R_{\{q_2, q_3\}}, E_{\{q_2, q_3\}} \right]$ to the list $\mathcal{I}$.

Finally, from the list $\mathcal{I}$, extract only those instances that contain the central loss q_1 and have non-zero energy. These constitute the set $\mathcal{I}_{q_1}^{\text{(f-i)}}$ that is used to compute the coefficients α_2 and α_3 with Eq. (4.27).

Input: lattice of the color code, a number ℓ.
Outputs: set $\mathcal{I}_{q_1}^{\text{(f-i)}}$ containing all fully-interacting instances $\boldsymbol{\ell}$ that have loss q_1 in common and contain from 2 to ℓ losses, the average number of edges erased $R_{\boldsymbol{\ell}}$, and the energy $E_{\boldsymbol{\ell}}$.

    1. place the central loss q_1 on a qubit of the lattice, extract the patch $\boldsymbol{P}$ of qubits at a distance $3(\ell - 1)$ from q_1.

    2. initialise an empty list $\mathcal{I} = \{\}$.

    3. **for** every instance $\boldsymbol{\ell} = \{q_2, q_3, \ldots\} \subset \boldsymbol{P}$ with $q_1 \notin \boldsymbol{\ell}$, containing from 2 to $\ell - 1$ losses **do**:

        3.1. compute $R_{\boldsymbol{\ell}}$ with Eq. (4.19).

        3.2. compute $E_{\boldsymbol{\ell}}$ with Eq. (4.24), which requires the value of $R_{\boldsymbol{\ell}}$ and the values of $R_{\boldsymbol{\ell}'}$ with $\boldsymbol{\ell}' \subset \boldsymbol{\ell}$ that are stored in $\mathcal{I}$, recall that for all instances $\{q\}$ with only one loss, $R_{\{q\}} = R_1$ as explained in Sec. 4.4.1.

        3.3. Append $[\boldsymbol{\ell}, R_{\boldsymbol{\ell}}, E_{\boldsymbol{\ell}}]$ to $\mathcal{I}$.

    4. **for** every instance $\boldsymbol{\ell} = \{q_1, q_2, q_3, \ldots\} \subset \boldsymbol{P}$ containing ℓ losses (one of them the central loss q_1) **do**:

        4.1. compute $R_{\boldsymbol{\ell}}$ with Eq. (4.19).

        4.2. compute $E_{\boldsymbol{\ell}}$ with Eq. (4.24), which requires the value of $R_{\boldsymbol{\ell}}$ and the values of $R_{\boldsymbol{\ell}'}$ with $\boldsymbol{\ell}' \subset \boldsymbol{\ell}$ that are stored in $\mathcal{I}$, recall that for all instances $\{q\}$ with only one loss, $R_{\{q\}} = R_1$ as explained in Sec. 4.4.1.

        4.3. Append $[\boldsymbol{\ell}, R_{\boldsymbol{\ell}}, E_{\boldsymbol{\ell}}]$ to $\mathcal{I}$.

    5. initialise the output list $\mathcal{I}_{q_1}^{\text{(f-i)}} = \{\}$.

    6. **for** $\boldsymbol{\ell}$ in $\mathcal{I}$, if $E_{\boldsymbol{\ell}} \neq 0$ and $q_1 \in \boldsymbol{\ell}$, append $[\boldsymbol{\ell}, R_{\boldsymbol{\ell}}, E_{\boldsymbol{\ell}}]$ to $\mathcal{I}_{q_1}^{\text{(f-i)}}$.

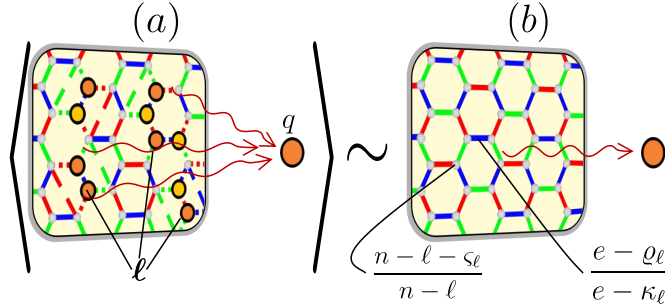   **7.** **return** $\mathcal{I}_{q_1}^{\text{(f-i)}}$.

Figure 4.12: Mean-field approximation of the fraction of edges erased $r(p)$. To obtain $r(p)$ exactly one has to compute the average number of edges erased R_ℓ for every possible loss instance ℓ. Loss instances can be generated by adding a new loss in a qubit q to a qubit loss instance $\boldsymbol{\ell}$ as shown in (a). However computing the number of edges erased $R_{\boldsymbol{\ell} \cup q}$ might turn hard due to the interaction between the new loss and all the qubit losses in $\boldsymbol{\ell}$. When averaged over all loss instances $\boldsymbol{\ell}$ with ℓ losses, the average interaction can be approximated by a mean-field interaction shown in (b). Here I show a lattice where there are ℓ qubits lost, an average of ς_ℓ qubits sacrificed, an average of κ_ℓ corrections have been performed, and an average of $\varrho - \ell$ edges erased. All these elements are uniformly distributed in the lattice, so the interaction can be seen as an interaction between the new loss and the lattice. There are $n - \ell - \varsigma_\ell$ qubits that have not been removed, $n - \ell$ qubits that have not been lost, $e - \varrho_\ell$ edges from the original lattice that have not been erased, and $e - \kappa_\ell$ edges in the lattice. In order to take into account the possibility that the new loss is chosen as a sacrificed qubit (not erasing any additional edge), I allow the new loss to happen on one of the ς_ℓ sacrificed qubits. Then, the probability of the new loss to happen on a non-removed qubit is $(n - \ell - \varsigma)/(n - \ell)$. Moreover, for every correction the lattice one edge (new or old) is erased. Thus, the probability of an edge not to be lost is $(e - \varrho_\ell)/(e - \kappa_\ell)$.

4.4.4 Mean-field approximation

Here I derive the average fraction of edges erased $r(p)$ by approximating the qubit loss interaction by a mean-field interaction. This approximation does not appear in Refs. [1, 2]. Provided that qubit losses happen according to a uniform distribution, when they are corrected, the qubits that are sacrificed, the edges that are erased from the original shrunk lattice, and the new edges that are added, are approximately uniformly distributed as well. In this scenario, if a new qubit loss happens, the interaction with the other losses, can be approximated by the interaction with an external source that places sacrificed qubits, erases and adds edges uniformly in the lattice. An illustration of the mean-field approximation is presented in Fig. 4.12. The mean-field approximation allows one to write an analytical expression for the effect that the interaction has on the new qubit loss.

As mentioned previously, the protocol to correct qubit losses operates sequentially on every lost qubit. Suppose that one corrects a qubit loss instance $\boldsymbol{\ell}$ with ℓ losses, and then adds in a position q a new qubit loss that is subsequently corrected. One can ask what effect has the interaction between the loss instance $\boldsymbol{\ell}$ of corrected losses and the new loss q on the number of edges erased to correct the new loss. This new loss erases R_1 edges from the original shrunk lattice when it is far from the other losses, but in the presence of the loss instance $\boldsymbol{\ell}$, due to the interaction, it erases $\epsilon_{\boldsymbol{\ell}\cup q} R_1$ instead, where $\epsilon_{\boldsymbol{\ell}\cup q}$ is a factor between 0 and 1 that condenses the effect of the interaction (recall that the interaction between qubit losses reduces the number of erased edges). Then, without loss of generality, the number of edges erased by the joint loss instance can be written as:

$$R_{\boldsymbol{\ell}\cup q} = R_{\boldsymbol{\ell}} + \epsilon_{\boldsymbol{\ell}\cup q} R_1. \tag{4.34}$$

By averaging over the $\binom{n}{\ell}$ possible qubit loss instances $\boldsymbol{\ell}$ with ℓ losses, and the $n - \ell$ possible positions q of the new loss one obtains a similar relation for the averaged quantities:

$$\langle R \rangle_{\ell+1} = \langle R \rangle_\ell + \langle \epsilon \rangle_\ell \, R_1. \tag{4.35}$$

Here $\langle \epsilon \rangle_\ell$ condenses the averaged effect that the interaction between all possible qubit loss instances of ℓ losses and a new qubit loss has on the number of edges erased by the new loss, averaged over all of its possible positions. Note that the average fraction of edges erased in Eq. (4.25) can be expressed in terms of $\langle R \rangle_\ell$ as:

$$r(p) = e^{-1} \sum_{\ell=0}^{n} \binom{n}{\ell} p^\ell (1-p)^{n-\ell} \langle R \rangle_\ell. \tag{4.36}$$

Eq. (4.35) presents a recursive sequence that can be solved, i.e., one can obtain $\langle R \rangle_\ell$ as a function of only ℓ if the dependence of $\langle \epsilon \rangle_\ell$ on ℓ and $\langle R \rangle_\ell$ is found. Given that the exact dependence might be hard to find, I use the mean-field approach to approximate $\langle \epsilon \rangle_\ell$ by ε_ℓ, and $\langle R \rangle_\ell$ by ϱ_ℓ. Thanks to the approximation performed, it is possible to obtain the dependence of ε_ℓ with ℓ and ϱ_ℓ, which results in a sequence

$$\varrho_{\ell+1} = \varrho_\ell + \varepsilon_\ell R_1, \tag{4.37}$$

that can be solved. The solution is an expression for ϱ_ℓ in terms of ℓ, which can be used

to substitute $\langle R \rangle_\ell$ in Eq. (4.36), and obtain the approximate average of edges erased:

$$r(p) \simeq e^{-1} \sum_{\ell=0}^{n} \binom{n}{\ell} p^\ell (1-p)^{n-\ell} \varrho_\ell, \qquad (4.38)$$

which can be solved to obtain a function of only p as desired.

Now let us find the dependence of ε_ℓ with ℓ and ϱ_ℓ. Let me introduce two more approximated quantities: the average number of corrections performed κ_ℓ and the average number of qubits sacrificed ς_ℓ. Note that in general κ_ℓ is smaller than ℓ, given that the losses that are chosen as sacrificed qubits do not need to be corrected (see Fig. 4.10 for an example). Also note that for every correction $R_1 = 5/3$ edges are erased and $2/3$ new edges are added to the shrunk lattice (see Fig. 4.9), thus, the number of total edges in the lattice reduces by 1 for each correction. Then, the average number of edges that remains in the lattice after κ_ℓ corrections is $e - \kappa_\ell$, irrespective of whether they are edges belonging to the original shrunk lattice or new edges added from the corrections. Here ς_ℓ accounts only for those sacrificed qubits that are not lost. Note that these two quantities are not fully independent: given that for every correction, either one loss and one sacrificed qubit, or two losses are removed, the following relation applies for the total number of removed qubits:

$$\ell + \varsigma_\ell = 2\kappa_\ell. \qquad (4.39)$$

One can now write the mean-field factor ε_ℓ in terms of these quantities. Assume that ℓ qubits are lost uniformly in the lattice. The correction of these losses causes the average erasure of ϱ_ℓ edges from the original shrunk lattice, reduces the number of present edges in the lattice from e to $e - \kappa_\ell$, and selects ς_ℓ qubits to be sacrificed. One needs to condense in ε_ℓ the two types of interaction between lost qubits as described in Sec. 4.4.1: the possibility that a lost qubit is chosen as a sacrificed qubit, and the possibility that some of the edges erased by the new loss are new edges added from the correction of the rest of losses.

With respect to the first type of interaction, note that the new loss can happen with equal probability on any of the $n - \ell$ qubits that are not lost. It can happen on a sacrificed qubit with probability $\varsigma_\ell/(n-\ell)$, and with probability $(n-\ell-\varsigma_\ell)/(n-\ell)$ on a

qubit that is neither lost nor sacrificed. The first case accounts for the possibility that the new loss is chosen as a sacrificed qubit during the full correction process. In this case, the new qubit does not erase any additional edge given that it does not need to be corrected, but for the second case, some edges are erased to correct it. Consequently, ε_ℓ must be proportional to the probability of the second case: $(n - \ell - \varsigma_\ell)/(n - \ell)$.

The number of edges erased by the new loss depends on the second type of interaction. Taking into account that I am averaging over all possible ways of placing ℓ losses, the edges that are erased to correct them, as well as the new edges added can be assumed to be uniformly distributed as well. Then, only a fraction $(e - \varrho_\ell)/(e - \kappa_\ell)$ of the R_1 edges that the new loss erases, are old edges. Putting both interaction effects together, one obtains that the number of edges erased by the new loss can be approximated by:

$$\varepsilon_\ell R_1 = \frac{n - \ell - \varsigma_\ell}{n - \ell} \frac{e - \varrho_\ell}{e - \kappa_\ell} R_1.$$

(4.40)

Using Eq. (4.39) and the fact that $e = n/2$ one obtains that the mean-field factor is

$$\varepsilon_\ell = \frac{n - 2\varrho_\ell}{n - \ell}.$$

(4.41)

Using the previous result, in Appendix A.4 I solve the recursive sequence in Eq. (4.37), obtaining that

$$\varrho_\ell = \frac{n}{2} \left[1 - \binom{n}{\ell}^{-1} \binom{n - 2R1}{\ell} \right],$$

(4.42)

where $\binom{n - 2R_1}{\ell}$ is the generalised binomial coefficient for non-integer values like $n - 2R_1$, which vanishes for $n - 2R_1 < \ell$. Note that $\varrho_0 = 0$, $\varrho_1 = R1$, and $\varrho_n = e$ as expected. And finally, one can obtain the approximation of the average number of edges erased by summing the series in Eq. (4.38) as performed in Appendix A.5, obtaining

$$r(p) \simeq 1 - (1 - p)^{2R_1}.$$

(4.43)

This result is in agreement with the functions obtained by expanding in power series of p, as can be seen in Fig. 4.6. In fact, it reproduces exactly the value of some of the first expansion coefficients α_ℓ obtained analytically for the three shrunk lattices of the three geometries of color code lattices. Note that, unlike the expressions obtained in Sec. 4.4, the approximated result obtained here does not depend on the geometry of

the shrunk lattice.

Finally, the critical qubit loss rate p_c below which the logical information is preserved as a function of the bond-percolation threshold r_c of a shrunk lattice is:

$$p_c = 1 - (1 - r_c)^{\frac{1}{2R_1}}. \tag{4.44}$$

4.5 Summary

This chapter of the thesis has presented the results that we achieved in Refs. [1, 2], as well as an analytical mean-field approximation of the fraction of edges erased $r(p)$ as a function of the qubit loss rate p that is not included in the previous references.

We have proposed in Sec. 4.2 a protocol to correct qubit losses in the color code consisting in the removal of each lost qubit and the sacrifice of a qubit for each loss. Then, the lattice is redefined without the removed qubits while it stays trivalent and face-three colourable, as required to define a color code on the lattice. Given a set of removed qubits, one can determine efficiently with the algebraic technique introduced in Sec. 4.2.1 if the logical information encoded can be recovered. We have proved in Sec. 4.2.2 that this happens when the set of removed qubits does not contain the entire support of a logical operator.

Our study in Sec. 4.3 has shown a connection between the tolerance of the color code under our protocol to two percolation problems: a simple bond-percolation problem in the shrunk lattices, and a novel bond-percolation problem on the three shrunk lattices coupled to each other. By exploring this connection we have determined analytically and numerically the tolerance of the color code to qubit loss. To be more precise, we have shown that the critical qubit loss rate p_c below which the logical information is protected is related to the bond-percolation threshold r_c of the shrunk lattices of the color code through the equation $r(p_c) = r_c$, where $r(p)$ is the average fraction of edges erased at a qubit loss rate p. In Sec. 4.4 we have developed a technique to systematically obtain the expansion coefficients of $r(p)$, introduced an algorithm to calculate the values of these coefficients, and computed the first three of these coefficients. Besides, using the mean-field approximation introduced in Sec. 4.4.4 we have derived an analytical formula for $r(p)$ that is valid at any range of p. Both analytical expressions have found agreement with numerical estimations.

Moreover, the fundamental loss threshold p_f of the three regular geometries of the color code has been computed numerically as described in Sec. 4.3.2, obtaining a value of 46(1)% for the 4.8.8. lattice, close to limit of 50% imposed by the no-cloning theorem [196]. The results confirm the high robustness to qubit loss of the color code together with the protocol to correct qubit losses, which is of practical relevance for actual and future quantum processors.

Chapter 5

Local entanglement witnesses

In this chapter we describe our work on entanglement witnesses and localisable entanglement (LE), which resulted in three publications [3, 4, 7]. In Ref. [7] we propose local witness operators for stabiliser states, study their relations and resistance to noise, provide two methods to construct these operators, and apply them to the existing experimental realisation of the seven-qubit color code with trapped ions. Then, in Ref. [3], we show that local entanglement witnesses provide a bound on the LE, and test the tightness of this bound. Finally, in Ref. [4], we detail the machinery (partially developed in the previous works) to build local entanglement witnesses for stabiliser states, and test it on the topological color code by studying the behaviour of LE as a function of the distance between two entangled qubits.

5.1 Background

As mentioned in the introduction, entanglement is a genuinely quantum property that should be present in experimental realisations of a quantum processors that can provide a quantum advantage over classical processors. However, multiple sources of decoherence, like experimental imperfections or finite qubit lifetimes, deteriorate the entanglement produced in practice. This makes entanglement characterisation crucial for benchmarking experimental realisations. Tomographic techniques like compressed sensing [103–105] are feasible only for small systems [106] given the exponential growth of the Hilbert space with the qubit number. They become unfeasible for the size of near-term experimental realisations with 50-100 qubits [215], so we need a different way

of estimating entanglement in experiments. A common approach is the use of entanglement witnesses, which are observables that determine the existence of entanglement from only partial information of the state [113]. They are designed to detect the entanglement of states close to a given entangled state of interest. This is particularly useful to detect and estimate the amount of entanglement present in an experimental realisation where the entanglement is reduced with respect to the ideal state of interest due to decoherence. Most of the efforts are devoted to the detection of genuine entanglement, but there are also witnesses that detect the entanglement depth [140, 141], the entanglement with respect to partitions [142], or witnesses that provide information about the Schmidt number [143–145]. In Ref. [216] local entanglement witnesses were proposed to detect the entanglement of qubit subsystems in multi-qubit graph states.

To be more precise, the entanglement detected by local witnesses proposed in Ref. [216] is the genuine entanglement among the qubits in a subsystem $\boldsymbol{q}$ (a subset of qubits) that remains when the rest of qubits are individually measured in the Z-basis. For graph states, this measurement basis guarantees that the reduced state in the subsystem is also a graph state. Rather than performing physically this measurement and then detecting entanglement on $\boldsymbol{q}$ with genuine entanglement witnesses, local witnesses only require the evaluation of a subset of graph state stabilisers. The number of graph state stabilisers that need to be evaluated is $2^{|\boldsymbol{q}|} - 1$, so the number of measurements of a local witness does not depend on the system size, and consequently, local witnesses can be used, in principle, in arbitrarily large experimental states. Besides, in Ref. [216], local witnesses that require only two measurement settings (or as we call them here, two-measurements witnesses) have been proposed. This reduction in the number of measurements comes at the cost of detecting entanglement only in a subset of the states where the standard local witness detects entanglement. However, with only two measurement settings multiple two-measurement witnesses can be evaluated simultaneously, providing an efficient way to obtain the entanglement structure of complex experimental states.

In Ref. [216], the authors apply the local witnesses designed to a simulated graph state of hundreds of qubits realised with two atomic species trapped in a two-dimensional bipartite graph under various noise channels. One noise source is localised on two groups of neighbouring trapped atoms, while the other noise source comes from noisy entangling gates at the lattice boundary. From the information obtained from the local

witnesses, they construct a two-dimensional map of entanglement. This map shows two groups of poorly entangled atoms corresponding to the two groups affected by the localised noise, and a decrease of entanglement at the lattice boundary due to the noisy entangling gates. These results showed the power and efficiency of local entanglement witnesses in detecting the entanglement structure of graph states with a reduced number of measurements.

The local witnesses we propose are constructed for stabiliser states and represent a generalisation of the local witnesses proposed in Ref. [216] for graph states. Stabiliser states play a role in many areas of quantum information, e.g. in quantum error correction (QEC), where fragile quantum information of logical qubits is distributed over many physical qubits and collectively encoded in entangled stabiliser QEC codes [13, 195]. Using the local witnesses proposed here one can, for instance, study the entanglement structure of experimental realisations of the color code [76] or the surface code [79, 80]. As an example, in this chapter we benchmark the proposed entanglement witnesses on an experimental realisation of the seven-qubit color code.

Furthermore, we show that local witnesses can be used to estimate LE [182, 183, 217]. As described in Sec. 2.4.2 LE is the maximum entanglement that can be localised on average in a subsystem by means of single-qubit projective measurements on the rest of the system. Localisable entanglement has been proven to be indispensable in investigating the correlation length in quantum many-body systems [182, 183, 185, 186, 217], in studying quantum phase transitions in cluster-Ising [187, 188] and cluster-XY models [189], in protocols like percolation of entanglement in quantum networks [190], measurement-based quantum computation [50, 174, 177] and entanglement percolation in quantum networks [190], and in quantifying local entanglement in stabiliser states [50, 174, 176, 177]. However, LE is hard to estimate in practice given that it requires an optimisation over a number local measurement settings that grows exponentially with the system size, as well as the averaging over an exponential number of outcomes for each measurement setting, and the evaluation of an entanglement measure for each reduced state. In contrast, the local witnesses that we propose here can be efficiently evaluated and provide a lower bound of LE. Therefore, these witnesses provide an experimentally-friendly technique to estimate LE entanglement in practise.

5.2 Genuine entanglement witnesses

Entanglement witnesses are observables that provide a sufficient (though not necessary) condition for the presence of entanglement from only partial information of the state. They detect entanglement in noisy experimental quantum states as long as the difference with the ideal state is sufficiently small. In this section we revise the concept of genuine entanglement witness operators and show how to construct them for stabiliser states as explained in Refs. [113, 136]. The evaluation of these witnesses requires a number of measurements that grows, in general, exponentially with the number of qubits in the state. Modified versions of the witnesses were proposed in Refs. [137, 138] to reduce the required number of measurement settings.

5.2.1 Witnesses as entanglement detectors

Here we introduce genuine entanglement witnesses and their key properties. An entanglement witness that detects the genuine n-qubit entanglement is an observable which is guaranteed to have a non-negative expectation value if applied to any separable state [111]. Therefore, a negative expectation value unambiguously signals the presence of n-partite genuine entanglement. A witness prepared for the ideal expected state $|\psi\rangle$ is an operator:

$$W_{|\psi\rangle} = \gamma_{|\psi\rangle} I - |\psi\rangle \langle\psi|, \tag{5.1}$$

where $|\psi\rangle$ is a non-separable pure state and $\gamma_{|\psi\rangle}$ is the square of the maximal Schmidt coefficient among all bi-partitions of $|\psi\rangle$ [136].

Note that the witness expectation value is directly related to the quantum state fidelity $\langle\psi| \rho |\psi\rangle$ by $\langle W_{|\psi\rangle}\rangle_\rho = \gamma_{|\psi\rangle} - \langle\psi| \rho |\psi\rangle$, and therefore a sufficiently high quantum state fidelity suffices to signal the presence of entanglement. For many states the state fidelity can be either estimated efficiently [218] or be directly determined [136] via a few measurement settings. In the case of stabiliser states $|\mathscr{S}\rangle$, the projector $|\mathscr{S}\rangle \langle\mathscr{S}|$ can be decomposed into a sum of all stabilisers in the stabiliser group $\mathscr{S}$.

5.2.2 Genuine entanglement witnesses for stabiliser states

In this section genuine witnesses for stabiliser states and modified genuine witnesses that require less measurement settings are introduced. Genuine witnesses for stabiliser

states involve the evaluation of the entire stabiliser group, but the modified ones only include a subset of it. The number of measurement settings required to evaluate the stabilisers in this subset depends on their Pauli type.

For all non-separable multi-qubit stabiliser states $|\mathscr{S}\rangle$ the square of the maximal Schmidt coefficient of all bipartitions is $\gamma_{|\mathscr{S}\rangle} = 1/2$ (as shown in App. A.6), and the fidelity operator is the projector into the $+1$ eigenspace of the n independent stabilisers s in a generator set $\mathcal{S}$, i,e, which generates the entire stabiliser group: $\langle \mathcal{S} \rangle = \mathscr{S}$. Then, the *standard genuine witness* constructed for the stabiliser state is:

$$W_{|\mathscr{S}\rangle} = \frac{1}{2}I - \prod_{s \in \mathcal{S}} \frac{I+s}{2}. \tag{5.2}$$

Given that the product of the projectors expands into a sum of all the elements in the stabiliser group $\mathscr{S}$, the standard genuine witness is the same if one uses any other generator set $\mathcal{S}'$ instead of $\mathcal{S}$ because both expand the same stabiliser group: $\langle \mathcal{S}' \rangle = \langle \mathcal{S} \rangle = \mathscr{S}$. For example, the following generator sets of the seven-qubit color code can be used to construct the same witness:

$$\mathcal{S} = \left\{ s_R^Z, s_B^Z, s_G^Z, s_R^X, s_B^X, s_G^X, s_L^X \right\}, \tag{5.3}$$

$$\mathcal{S}' = \left\{ s_R^Z s_R^X, s_B^Z s_B^X, s_G^Z s_G^X, s_R^X, s_B^X, s_G^X, s_L^X \right\}. \tag{5.4}$$

During the rest of the thesis, the logical operator l^X of the seven-qubit color code is considered as a stabiliser operator, so we represent it as s_L^X.

To compute the expectation value of this witness $2^n - 1$ stabilisers have to be evaluated, which becomes impractical for a large number n of qubits. A way to overcome this problem is to construct modified witness operators that include a smaller number of terms. One option is to consider *alternative witnesses* [137, 138]:

$$W_{|\mathscr{S}\rangle}^{\mathrm{a}} = \frac{n-1}{2}I - \frac{1}{2}\sum_{s \in \mathcal{S}} s, \tag{5.5}$$

which require the measurement of only the n stabilisers in a generator set $\mathcal{S}$, so the number of measurements grows only linearly with n. In this case, by substituting $\mathcal{S}$ for a different generator set $\mathcal{S}'$, like the ones in Eqs. (5.3) and (5.4), one obtains a different alternative witness.

If the stabiliser state $|\mathscr{S}\rangle$ has a generator set $\mathcal{S}$ composed entirely by X-type and Z-type stabilisers s^X and s^Z, respectively, i.e., it is composed of operators involving single-qubit Pauli operators X and Z only, (for instance Calderbank-Steane-Shor (CSS) codes [210, 219]), the *two-measurements witness* can be constructed from those stabilisers:

$$W_{|\mathscr{S}\rangle}^{2\mathrm{m}} = \frac{3}{2}I - \prod_{s^X \in \mathcal{S}} \frac{I + s^X}{2} - \prod_{s^Z \in \mathcal{S}} \frac{I + s^Z}{2}. \tag{5.6}$$

Note that the evaluation of $W_{|\mathscr{S}\rangle}^{2\mathrm{m}}$ requires only two measurement settings, one in the X basis $\{X_1, X_2, \cdots, X_n\}$ and the other in the Z basis $\{Z_1, Z_2, \cdots, Z_n\}$, but rotated versions $\{\sigma_1, \sigma_2, \cdots, \sigma_n\}$ and $\{\sigma'_1, \sigma'_2, \cdots, \sigma'_n\}$ can be used instead as long as $\sigma_q \neq \sigma'_q$ for every qubit q. For instance, in Ref. [216] the authors construct modified witnesses for bi-colourable graph states, where one measurement setting consists of measuring X on every even qubit and Z on every odd qubit, and vice versa for the second measurement setting. The modified operators are witnesses because their expectation value is larger than the expectation value of the standard genuine witness for any state [137, 138],

$$\langle W_{|\mathscr{S}\rangle}\rangle_\rho \leq \langle W_{|\mathscr{S}\rangle}^{\mathrm{a}}\rangle_\rho \quad , \quad \langle W_{|\mathscr{S}\rangle}\rangle_\rho \leq \langle W_{|\mathscr{S}\rangle}^{2\mathrm{m}}\rangle_\rho \quad \forall \rho, \tag{5.7}$$

which guarantees that their expectation value is non-negative for any separable state ρ, as required for being a valid witness.

The price to pay for the reduction in the number of measurement settings required by modified witnesses is that these witnesses are in general less tolerant to noise. They detect entanglement only in a subset of states where the standard genuine witness also detects entanglement.

5.3 Local entanglement witnesses

In this section we introduce local witness operators for stabiliser states. We enunciate a proposition that introduces the necessary and sufficient conditions that a local witness must satisfy to detect entanglement. In Sec. 5.3.1 we prove the proposition and prove that local witnesses detect LE, i.e., if a local witness detects entanglement, the value of LE is non-zero. The connection between local witnesses and LE is further used in Sec. 5.3.2 to bound LE with the expectation value of a local witness. In Sec. 5.3.3 we show the tightness of the bound for stabiliser-diagonal states, which are mixed states

that can be diagonalised in the basis of a stabiliser state and the excited states. In Sec. 5.3.4, we propose modified local witnesses that require less measurement settings, as we did for genuine witnesses in Sec. 5.2.2. Finally, Sec. 5.3.5 discusses the results on the robustness of the witnesses presented and compares the genuine and local witnesses introduced.

A local witness operator $W_{\boldsymbol{q}}$ detects entanglement in a subsystem of qubits $\boldsymbol{q}$ of a state ρ if the expectation value is negative: $\langle W_{\boldsymbol{q}} \rangle_{\rho} < 0$. The local witnesses that we introduce here are designed to detect entanglement in a stabiliser state $|\mathscr{S}\rangle$ and in states ρ sufficiently close. They take the form:

$$W_{\boldsymbol{q}} = \frac{1}{2}I - \prod_{s \in \mathcal{W}_{\boldsymbol{q}}} \frac{I + s}{2},$$ (5.8)

where $\mathcal{W}_{\boldsymbol{q}} \subset \mathscr{S}$ is a subset of the stabiliser group $\mathscr{S}$ that defines the state $|\mathscr{S}\rangle$. The properties of $\mathcal{W}_{\boldsymbol{q}}$ are enunciated in the following proposition.

Proposition. 1 *A subset $\mathcal{W}_{\boldsymbol{q}} \subset \mathscr{S}$ of the stabiliser group $\mathscr{S}$ defines a valid local witness of the form in Eq. (5.8) for the subsystem $\boldsymbol{q}$ if it satisfies the following properties:*

(A) It contains $|\mathcal{W}_{\boldsymbol{q}}| = |\boldsymbol{q}|$ independent and commuting stabilisers.

(B) For every qubit $q \notin \boldsymbol{q}$, the Pauli operators σ_{qi}, σ_{qj} corresponding to any two different stabilisers $s_i, s_j \in \mathcal{W}_{\boldsymbol{q}}$, respectively, commute: $[\sigma_{qi}, \sigma_{qj}] = 0$.

(C) If one considers for each stabiliser $s_i \in \mathcal{W}_{\boldsymbol{q}}$ the part

$$s_i|_{\boldsymbol{q}} = \bigotimes_{q \in \boldsymbol{q}} \sigma_{qi}$$ (5.9)

that has support only on the qubits in $\boldsymbol{q}$, the set formed by these parts $\mathcal{W}_{\boldsymbol{q}}|_{\boldsymbol{q}} = \{s|_{\boldsymbol{q}} : s \in \mathcal{W}_{\boldsymbol{q}}\}$ must be a generator set of the stabiliser group $\mathscr{S}_{\boldsymbol{q}}$ (meaning that $\langle \mathcal{W}_{\boldsymbol{q}}|_{\boldsymbol{q}}\rangle = \mathscr{S}_{\boldsymbol{q}}$) that defines a genuinely multipartite entangled state $|\mathscr{S}_{\boldsymbol{q}}\rangle$ over $\boldsymbol{q}$.

For example, the subset of stabilisers from the seven-qubit color code

$$\mathcal{W}_{\{2,3\}} = \{s_R^Z, s_B^X\}$$ (5.10)

satisfies Prop. 1 for the subsystem $\{2, 3\}$. First, it contains two independent and commuting stabilisers. Second, they commute qubit-wise on every qubit outside $\{2, 3\}$: for

every qubit $q \notin \{2,3\}$ the qubit-wise commutator between the two stabilisers $[\sigma_{qR}, \sigma_{qB}]$ belongs to the set of vanishing commutators $\{[Z, I], [I, X], [I, I]\}$. Third, the reduced set:

$$\mathcal{W}_{\{2,3\}}|_{\{2,3\}} = \{Z_2 Z_3, \ X_2 X_3\} \tag{5.11}$$

is a generator set of the genuinely entangled Bell state $2^{-1/2}(|00\rangle + |11\rangle)$ on qubits $\{2,3\}$.

When expanded in terms of the stabilisers and their products, a local witness can be evaluated with $2^{|q|} - 1$ measurement settings, so the number of measurements does not depend on the system size.

5.3.1 Local witnesses detect localisable entanglement

Here we show that local witnesses defined with Prop. 1 are, indeed, witness operators, and then we show that the operational meaning of a local witness coincides with the operations realised to evaluate LE. In essence, a local witness prepared for a subsystem of qubits is a convex sum of genuine witnesses prepared for the outcome states of a local-projective measurement of the qubits that do not belong to the subsystem. This is such that the negative expectation value of a local witness indicates that at least one of the genuine entanglement witnesses involved in the sum has detected entanglement. This is precisely the type of entanglement evaluated by LE.

Due to property (B), there is a measurement basis $\mathcal{M}_{\partial q} = \{m_q \in \{X, Y, Z\} : q \in \partial q\}$ associated to every local witness, where ∂q is the *boundary* of q, i.e., the set of qubits outside q where at least one stabiliser $s \in \mathcal{W}_q$ has support. The measurement m_q on a qubit $q \in \partial q$ is given by the Pauli operator $\sigma_q \neq I$ of a stabiliser $s \in \mathcal{W}_q$ that has support on q. For the example in Eq. (5.10), the boundary is $\partial\{2,3\} = \{1, 4, 5, 6\}$, and the measurement basis associated is $\mathcal{M}_{\partial\{2,3\}} = \{Z_1, Z_4, X_5, X_6\}$.

Due to properties (B) and (C) one can write the stabilisers $s \in \mathcal{W}_q$ as $s = s|_q \otimes s|_{\partial q} \otimes I_{q_r}$, where $s|_{\partial q}$ is the part of s with support on ∂q and I_{q_r} is the identity operator on the rest of qubits q_r, i.e., the set of qubits outside q and ∂q. One can associate a projector $\Pi_{\mathfrak{m}}$ to the joint measurement of $\mathcal{M}_{\partial q}$ and any local measurement $\mathcal{M}_{q_r} = \{m_q : m_q = m_q^\dagger, q \in q_r\}$ on the rest of qubits:

$$\Pi_{\mathfrak{m}} = \bigotimes_{m_q \in \mathcal{M}_{\partial q}} \frac{I + (-1)^{\mathfrak{m}_q} m_q}{2} \bigotimes_{m_q \in \mathcal{M}_{q_r}} \frac{I + (-1)^{\mathfrak{m}_q} m_q}{2}, \tag{5.12}$$

with measurement outcome represented by a string $\mathbb{m}$ formed by $n - |\boldsymbol{q}|$ binary elements $\mathbb{m}_q \in \{0, 1\}$. The sum of $\Pi_{\mathbb{m}}$ for all possible outcomes gives the identity operator:

$$I = \sum_{\mathbb{m}} \Pi_{\mathbb{m}}. \tag{5.13}$$

The application of such projector to the stabilisers $s \in \mathcal{W}_{\boldsymbol{q}}$ yields:

$$s\left(I_{\boldsymbol{q}} \otimes \Pi_{\mathbb{m}}\right) = (-1)^{\eta(\mathbb{m}, s|_{\partial \boldsymbol{q}})} s|_{\boldsymbol{q}} \otimes \Pi_{\mathbb{m}}, \tag{5.14}$$

where

$$\eta(\mathbb{m}, s|_{\partial \boldsymbol{q}}) = \sum_{q \in \mathbf{supp}(s|_{\partial \boldsymbol{q}})} \mathbb{m}_q. \tag{5.15}$$

Recall that $\mathbf{supp}(s)$ is the support of the stabiliser s. Then, when the sum of all $\Pi_{\mathbb{m}}$, which equals the identity operator, is applied to the local witness, one obtains that:

$$W_{\boldsymbol{q}} = \sum_{\mathbb{m}} W_{|\mathscr{S}_{\boldsymbol{q}}^{\mathbb{m}}\rangle} \otimes \Pi_{\mathbb{m}}, \tag{5.16}$$

where

$$W_{|\mathscr{S}_{\boldsymbol{q}}^{\mathbb{m}}\rangle} = \frac{1}{2}I - \prod_{s \in \mathcal{W}_{\boldsymbol{q}}} \frac{I + (-1)^{\eta(\mathbb{m}, s|_{\partial \boldsymbol{q}})} s|_{\boldsymbol{q}}}{2} \tag{5.17}$$

is a genuine entanglement witness due to property (C). These genuine entanglement witnesses are prepared for the stabiliser states $|\mathscr{S}_{\boldsymbol{q}}^{\mathbb{m}}\rangle$, whose stabilisers $s|_{\boldsymbol{q}}$ have eigenvalues $(-1)^{\eta(\mathbb{m}, s|_{\partial \boldsymbol{q}})}$ that depend on the outcome $\mathbb{m}$ resulting from the measurement $\mathcal{M}_{\partial \boldsymbol{q}}$ only:

$$|\mathscr{S}_{\boldsymbol{q}}^{\mathbb{m}}\rangle \langle \mathscr{S}_{\boldsymbol{q}}^{\mathbb{m}}| = \prod_{s \in \mathcal{W}_{\boldsymbol{q}}} \frac{I + (-1)^{\eta(\mathbb{m}, s|_{\partial \boldsymbol{q}})} s|_{\boldsymbol{q}}}{2}. \tag{5.18}$$

Note that the decomposition of a local witness into genuine witnesses is independent on the measurement $\mathcal{M}_{\boldsymbol{q}_r}$ on the rest of qubits $\boldsymbol{q}_r$.

When a local witness is evaluated on a state ρ, the expectation value obtained can be written as a convex sum of the expectation values of the genuine entanglement witnesses $W_{|\mathscr{S}_{\boldsymbol{q}}^{\mathbb{m}}\rangle}$:

$$\langle W_{\boldsymbol{q}} \rangle_{\rho} = \sum_{\mathbb{m}} p_{\mathbb{m}} \langle W_{|\mathscr{S}_{\boldsymbol{q}}^{\mathbb{m}}\rangle} \rangle_{\rho_{\boldsymbol{q}}^{\mathbb{m}}}, \tag{5.19}$$

where $\rho_{\boldsymbol{q}}^{\mathbb{m}}$ is the reduced state corresponding to the outcome $\mathbb{m}$ when ρ is measured on

the joint measurement basis $\mathcal{M} = \mathcal{M}_{\partial \boldsymbol{q}} \cup \mathcal{M}_{\boldsymbol{q}_r}$, and $p_{\mathbb{m}}$ is the probability of obtaining $\mathbb{m}$. Therefore, $\langle W_{\boldsymbol{q}} \rangle_\rho < 0$ only if at least one of the genuine entanglement witnesses detects entanglement $\langle W_{|\mathscr{S}_{\boldsymbol{q}}^{\mathbb{m}}} \rangle_{\rho_{\boldsymbol{q}}^{\mathbb{m}}} < 0$. In this case, the qubits $\boldsymbol{q}$ in the reduced state $\rho_{\boldsymbol{q}}^{\mathbb{m}}$ are genuinely entangled. This proves that the operator in Eq. (5.8) is indeed an entanglement witness.

Finally, the connection with LE becomes clear: the entanglement detected by a local witness is the genuine entanglement remaining in the state after performing the local projective measurements given by the measurement basis $\mathcal{M}$.

5.3.2 Lower bound of localisable entanglement

In this section we use the existing bound of entanglement measures given by witnesses [129, 220] to provide a lower bound of LE from local witnesses. We obtain the lower bound of entanglement negativity from genuine witnesses, and use the previous decomposition of a local witnesses in Eq. (5.19) into a sum of genuine witnesses to provide a lower bound of LE from the expectation value of the local witness.

Some entanglement measures $\mathcal{E}$ can be bounded by a convex function f of the expectation value of an entanglement witness [129, 220]:

$$\mathcal{E}(\rho) \geq f\left(\langle W \rangle_\rho\right). \tag{5.20}$$

Given that in Eq. (5.19) $p_{\mathbb{m}}$ are convex weights and that f is a convex function, the expectation value of a local witness lower-bounds the amount of LE restricted to the measurement basis $\mathcal{M}$:

$$\mathcal{E}_{\boldsymbol{q}}^{\mathcal{M}}(\rho) = \sum_{\mathbb{m}} p_{\mathbb{m}} \mathcal{E}(\rho_{\boldsymbol{q}}^{\mathbb{m}}) \geq \sum_{\mathbb{m}} p_{\mathbb{m}} f\left(\langle W_{|\mathscr{S}_{\boldsymbol{q}}^{\mathbb{m}}} \rangle_{\rho_{\boldsymbol{q}}^{\mathbb{m}}}\right) \geq f\left(\langle W_{\boldsymbol{q}} \rangle_\rho\right). \tag{5.21}$$

By definition, LE is maximised over all possible measurement settings, so the following hierarchy of inequalities applies:

$$\mathcal{E}_{\boldsymbol{q}}(\rho) \geq \mathcal{E}_{\boldsymbol{q}}^{\mathcal{M}}(\rho) \geq f\left(\langle W_{\boldsymbol{q}} \rangle_\rho\right). \tag{5.22}$$

The entanglement measure that we employ is negativity because it is well defined on mixed states and it is easy to compute. As we show in App. A.7, for any bi-partition, the entanglement negativity can be lower-bounded by the expectation value of a genuine

entanglement witness as $-2 \langle W_{|\psi\rangle} \rangle_\rho$, so the lower bound of LE with negativity is:

$$\mathcal{E}_{\boldsymbol{q}}(\rho) \geq \begin{cases} -2 \langle W_{\boldsymbol{q}} \rangle_\rho & \text{if } \langle W_{\boldsymbol{q}} \rangle_\rho < 0 \\ 0 & \text{otherwise} \end{cases}. \tag{5.23}$$

Obviously, if the expectation value of the local witness is positive (it does not detect entanglement), the lower bound of LE can be set to 0, instead of $-2 \langle W_{\boldsymbol{q}} \rangle_\rho$.

5.3.3 Lower bound on stabiliser-diagonal states

This section presents a particular result for local entanglement witnesses, but it is not necessary to understand the rest of sections in the thesis. For the particular case of *stabiliser-diagonal states* $\rho_{\mathscr{S}\text{D}}$, the lower bound of a local witness that detects entanglement in a subsystem $\boldsymbol{q}$ of two qubits is tight. When a local uncorrelated Pauli noise channel ε_P (like depolarising of phase-flip described in Sec. 2.5) is applied to a stabiliser state $|\mathscr{S}\rangle$, we call the resulting mixed state $\rho_{\mathscr{S}\text{D}} = \varepsilon_\text{P}(|\mathscr{S}\rangle)$ stabiliser-diagonal state because it can be diagonalised in the basis of excitations $|\mathscr{S}^{\mathbb{e}}\rangle$ of the stabiliser state:

$$\rho_{\mathscr{S}\text{D}} = \sum_{\mathbb{e}} p_{\mathbb{e}} |\mathscr{S}^{\mathbb{e}}\rangle \langle \mathscr{S}^{\mathbb{e}}|. \tag{5.24}$$

We say that a stabiliser state is excited if the value of one stabiliser has -1 value. Here $\mathbb{e}$ indicates the excited stabilisers: it is a binary vector with an element $\mathbb{e}_s$ for each of the n stabilisers, which is $1(0)$ if the stabiliser s is (is not) excited, while $p_{\mathbb{e}}$ is the probability that ε_P causes an excitation $\mathbb{e}$.

Let us start by showing that the local measurement $\mathcal{M}_{\partial \boldsymbol{q}}$, with associated projector $\Pi_{\mathbb{m}|\partial \boldsymbol{q}}$, disentangles the subsystem $\boldsymbol{q}$ from the rest of the state $|\mathscr{S}\rangle$. For that, we need to start by showing the effect that $\Pi_{\mathbb{m}|\partial \boldsymbol{q}}$ has on the stabilisers in $\mathcal{S}$. Then, we show the action on $|\mathscr{S}\rangle$.

The generator set $\mathcal{S}$ of $|\mathscr{S}\rangle$ can be split into a subset $S_c \subset \mathcal{S}$ of stabilisers that commute qubit-wise with the measurement basis $\mathcal{M}_{\partial \boldsymbol{q}}$, and a subset $S_a \subset \mathcal{S}$ of stabilisers that anti-commute qubit-wise with $\mathcal{M}_{\partial \boldsymbol{q}}$ on at least one qubit. Without loss of generality $\mathcal{S}$ can be selected such that $\mathcal{W}_{\boldsymbol{q}} \subset S_c$. Then, S_c is composed by $\mathcal{W}_{\boldsymbol{q}}$ and another disjoint subset $S_{\boldsymbol{q}_r}$. For the example in Eq. (5.10) one can consider $\mathcal{S}$ to be formed by $S_a = \{s_B^Z, s_G^Z, s_R^X, s_G^X\}$, $\mathcal{W}_{\{2,3\}} = \{s_R^Z, s_B^X\}$ and $S_{\boldsymbol{q}_r} = \{s_L^X s_R^X s_B^X\}$ for $\boldsymbol{q}_r = \{7\}$.

5. LOCAL ENTANGLEMENT WITNESSES

Let us now take a look at the reduced versions $s|_{\boldsymbol{q}}$ of these stabilisers $s \in \mathcal{S}$. First, the set $\mathcal{W}_{\boldsymbol{q}}|_{\boldsymbol{q}}$ defined in property (C) is a generator set, so it contains all possible reduced stabilisers that are independent and commute. Thus, any other Pauli operator over $\boldsymbol{q}$ either anti-commutes with some reduced stabiliser in $\mathcal{W}_{\boldsymbol{q}}|_{\boldsymbol{q}}$ or it is a product of the reduced stabilisers in $\mathcal{W}_{\boldsymbol{q}}|_{\boldsymbol{q}}$. Second, due to the definition of S_c and property (B), the reduced stabilisers $s|_{\boldsymbol{q}}$ for all $s \in S_{\boldsymbol{q}_r}$ commute with the reduced stabilisers in $\mathcal{W}_{\boldsymbol{q}}|_{\boldsymbol{q}}$. Then, the reduced stabilisers of $S_{\boldsymbol{q}_r}$ are products of the reduced stabilisers in $\mathcal{W}_{\boldsymbol{q}}|_{\boldsymbol{q}}$:

$$s|_{\boldsymbol{q}} = \prod_{s' \in \mathcal{W}_{\boldsymbol{q}}} (s'|_{\boldsymbol{q}})^{\mathbb{T}_{ss'}} \qquad \forall \, s \in S_{\boldsymbol{q}_r} \tag{5.25}$$

for some $|S_{\boldsymbol{q}_r}| \times |\mathcal{W}_{\boldsymbol{q}}|$ binary matrix $\mathbb{T}$ with elements $\mathbb{T}_{ss'}$ for each $s \in S_{\boldsymbol{q}_r}$ and $s' \in \mathcal{W}_{\boldsymbol{q}}$. Note that the row of $\mathbb{T}$ corresponding to a stabiliser $s \in S_{\boldsymbol{q}_r}$ vanishes if s does not have support on $\boldsymbol{q}$. In the example, the reduced version of the stabiliser in $S_{\{7\}}$ is $S_{\{7\}}|_{\{2,3\}} = \{X_2 X_3\}$, which is a trivial recombination of the reduced stabilisers in $\mathcal{W}_{\{2,3\}}|_{\{2,3\}} = \{Z_2 Z_3, X_2 X_3\}$.

Let us consider a subset of stabilisers $S'_{\boldsymbol{q}_r} \subset \mathscr{S}$ consisting of the recombined stabilisers

$$s \prod_{s' \in \mathcal{W}_{\boldsymbol{q}}} (s')^{\mathbb{T}_{ss'}} \qquad \forall \, s \in \mathcal{S}_{\boldsymbol{q}_r}, \tag{5.26}$$

which do not have support on $\boldsymbol{q}$. Thus, $\mathcal{S}' = \mathcal{W}_{\boldsymbol{q}} \cup S'_{\boldsymbol{q}_r} \cup S_a$ is a generator set equivalent to $\mathcal{S}$ where those generators that commute qubit-wise with $\mathcal{M}_{\partial \boldsymbol{q}}$ on all qubits in $\partial \boldsymbol{q}$ either belong to $\mathcal{W}_{\boldsymbol{q}}$ or do not have support on $\boldsymbol{q}$. For the previous example, $S_{\{7\}}$ can be replaced by $S'_{\{7\}} = \{s_L^X s_R^X\}$.

Therefore, when the projector

$$\Pi_{\mathfrak{m}}|_{\partial \boldsymbol{q}} = \bigotimes_{m_q \in \mathcal{M}_{\partial \boldsymbol{q}}} \frac{I + (-1)^{\mathfrak{m}_q} m_q}{2} \tag{5.27}$$

corresponding to the local measurement basis $\mathcal{M}_{\partial \boldsymbol{q}}$ defined by the local witness as in Sec. 5.3.1 is applied on a stabiliser $s \in \mathcal{S}'$ three results are possible:

$$(I_{\boldsymbol{q}} \otimes \Pi_{\mathfrak{m}}|_{\partial \boldsymbol{q}}) \, s \, (I_{\boldsymbol{q}} \otimes \Pi_{\mathfrak{m}}|_{\partial \boldsymbol{q}}) = \begin{cases} (-1)^{\eta(\mathfrak{m}, s|_{\partial \boldsymbol{q}})} s|_{\boldsymbol{q}} \otimes \Pi_{\mathfrak{m}}|_{\partial \boldsymbol{q}} \otimes I_{\boldsymbol{q}_r} & \forall \quad s \in \mathcal{W}_{\boldsymbol{q}} \\ (-1)^{\eta(\mathfrak{m}, s|_{\partial \boldsymbol{q}})} I_{\boldsymbol{q}} \otimes \Pi_{\mathfrak{m}}|_{\partial \boldsymbol{q}} \otimes s|_{\boldsymbol{q}_r} & \forall \quad s \in \mathcal{S}_{\boldsymbol{q}_r} \, , \\ 0 & \forall \quad s \in \mathcal{S}_a \end{cases} \tag{5.28}$$

where $\eta(\mathbb{m}, s|_{\boldsymbol{q}})$ is defined in Eq. (5.15). Consequently, when the projector $\Pi_{\mathbb{m}}|_{\partial \boldsymbol{q}}$ is applied to the stabiliser state $|\mathscr{S}\rangle$ it disentangles the part in $\boldsymbol{q}$ from the part in $\boldsymbol{q}_r$:

$$\left(I_{\boldsymbol{q}} \otimes \Pi_{\mathbb{m}}|_{\partial \boldsymbol{q}} \otimes I_{\boldsymbol{q}_r}\right) |\mathscr{S}\rangle \langle \mathscr{S}| \left(I_{\boldsymbol{q}} \otimes \Pi_{\mathbb{m}}|_{\partial \boldsymbol{q}} \otimes I_{\boldsymbol{q}_r}\right) = |\mathscr{S}_{\boldsymbol{q}}^{\mathbb{m}}\rangle \langle \mathscr{S}_{\boldsymbol{q}}^{\mathbb{m}}| \otimes \Pi_{\mathbb{m}}|_{\partial \boldsymbol{q}} \otimes |\mathscr{S}_{\boldsymbol{q}_r}^{\mathbb{m}}\rangle \langle \mathscr{S}_{\boldsymbol{q}_r}^{\mathbb{m}}|, \tag{5.29}$$

where $|\mathscr{S}_{\boldsymbol{q}}^{\mathbb{m}}\rangle$ is defined in Eq. (5.18) and $|\mathscr{S}_{\boldsymbol{q}_r}^{\mathbb{m}}\rangle$ is similarly defined:

$$|\mathscr{S}_{\boldsymbol{q}_r}^{\mathbb{m}}\rangle \langle \mathscr{S}_{\boldsymbol{q}_r}^{\mathbb{m}}| = \prod_{s \in \mathcal{S}_{\boldsymbol{q}_r}} \frac{I + (-1)^{\eta(\mathbb{m}, s|_{\partial \boldsymbol{q}})} s|_{\boldsymbol{q}_r}}{2}. \tag{5.30}$$

Analogously, for excited states $|\mathscr{S}^{\mathbb{e}}\rangle$, the same result is obtained with $\mathbb{e}_s + \eta(\mathbb{m}, s|_{\partial \boldsymbol{q}})$ instead of just $\eta(\mathbb{m}, s|_{\partial \boldsymbol{q}})$:

$$|\mathscr{S}_{\tilde{\boldsymbol{q}}}^{\mathbb{e},\mathbb{m}}\rangle \langle \mathscr{S}_{\tilde{\boldsymbol{q}}}^{\mathbb{e},\mathbb{m}}| = \prod_{s \in \mathcal{S}_{\tilde{\boldsymbol{q}}}} \frac{I + (-1)^{\mathbb{e}_s + \eta(\mathbb{m}, s|_{\partial \boldsymbol{q}})} s|_{\tilde{\boldsymbol{q}}}}{2} \tag{5.31}$$

for both $\tilde{\boldsymbol{q}} = \boldsymbol{q}$ and $\tilde{\boldsymbol{q}} = \boldsymbol{q}_r$. Then, when the joint measurement $\mathcal{M} = \mathcal{M}_{\partial \boldsymbol{q}} \cup \mathcal{M}_{\boldsymbol{q}_r}$ with projector $\Pi_{\mathbb{m}} = \Pi_{\mathbb{m}}|_{\partial \boldsymbol{q}} \otimes \Pi_{\mathbb{m}}|_{\boldsymbol{q}_r}$ is applied to a stabiliser-diagonal state, the reduced state is obtained:

$$\rho_{\mathscr{S}\mathrm{D},\boldsymbol{q}}^{\mathbb{m}} = \sum_{\mathbb{e}|_{\mathcal{W}_{\boldsymbol{q}}}} p_{\mathbb{e}|_{\mathcal{W}_{\boldsymbol{q}}}} |\mathscr{S}_{\boldsymbol{q}}^{\mathbb{e},\mathbb{m}}\rangle \langle \mathscr{S}_{\boldsymbol{q}}^{\mathbb{e},\mathbb{m}}|, \tag{5.32}$$

where $\mathbb{e}|_{\mathcal{W}_{\boldsymbol{q}}}$ includes only the bits $\mathbb{e}_s$ corresponding to stabilisers $s \in \mathcal{W}_{\boldsymbol{q}}$ and

$$p_{\mathbb{e}|_{\mathcal{W}_{\boldsymbol{q}}}} = \sum_{\mathbb{e}': \, \mathbb{e}'_s = \mathbb{e}_s \, \forall s \in \mathcal{W}_{\boldsymbol{q}}} p_{\mathbb{e}'} \tag{5.33}$$

is the probability to produce the excitation pattern $\mathbb{e}|_{\mathcal{W}_{\boldsymbol{q}}}$ on the stabilisers in $\mathcal{W}|_{\boldsymbol{q}}$. Note that the reduced state $\rho_{\mathscr{S}\mathrm{D},\boldsymbol{q}}^{\mathbb{m}}$ is also a stabiliser-diagonal state. Every excitation induced by the measurement outcome $\mathbb{m}$ can also be produced by a Pauli operator $P_{\mathbb{m}}$ such that $|\mathscr{S}_{\boldsymbol{q}}^{\mathbb{e},\mathbb{m}}\rangle = P_{\mathbb{m}} |\mathscr{S}_{\boldsymbol{q}}^{\mathbb{e},0}\rangle$, where $|\mathscr{S}_{\boldsymbol{q}}^{\mathbb{e},0}\rangle$ is the state defined in Eq. (5.31). Then, the excitations in $\rho_{\mathscr{S}\mathrm{D},\boldsymbol{q}}^{\mathbb{m}}$ due to the measurement can be also induced by some $P_{\mathbb{m}}$:

$$\rho_{\mathscr{S}\mathrm{D},\boldsymbol{q}}^{\mathbb{m}} = P_{\mathbb{m}} \rho_{\mathscr{S}\mathrm{D},\boldsymbol{q}} P_{\mathbb{m}}, \tag{5.34}$$

where

$$\rho_{\mathscr{S}\mathrm{D},\boldsymbol{q}} = \sum_{\mathbb{e}|_{\mathcal{W}_{\boldsymbol{q}}}} p_{\mathbb{e}|_{\mathcal{W}_{\boldsymbol{q}}}} |\mathscr{S}_{\boldsymbol{q}}^{\mathbb{e},0}\rangle \langle \mathscr{S}_{\boldsymbol{q}}^{\mathbb{e},0}|. \tag{5.35}$$

Analogously, the Pauli operator $P_\mathfrak{m}$ can be used to write the genuine entanglement witness in Eq. (5.17) as:

$$W_{|\mathscr{S}_{\boldsymbol{q}}^\mathfrak{m}\rangle} = P_\mathfrak{m} W_{|\mathscr{S}_{\boldsymbol{q}}\rangle} P_\mathfrak{m}. \tag{5.36}$$

Therefore, when the genuine witness $W_{|\mathscr{S}_{\boldsymbol{q}}^\mathfrak{m}\rangle}$ is evaluated on the reduced state $\rho_{\mathscr{S}\mathrm{D},\boldsymbol{q}}^\mathfrak{m}$ the dependence on the outcome $\mathfrak{m}$ cancels out:

$$\langle W_{|\mathscr{S}_{\boldsymbol{q}}^\mathfrak{m}\rangle}\rangle_{\rho_{\mathscr{S}\mathrm{D},\boldsymbol{q}}^\mathfrak{m}} = \langle W_{|\mathscr{S}_{\boldsymbol{q}}\rangle}\rangle_{\rho_{\mathscr{S}\mathrm{D},\boldsymbol{q}}} = \frac{1}{2} - p_0 \quad \forall\, \mathfrak{m}. \tag{5.37}$$

Here p_0 is $p_{\mathbb{e}|\mathcal{W}_{\boldsymbol{q}}}$ for vanishing $\mathbb{e}|\mathcal{W}_{\boldsymbol{q}}$. Finally, from Eq. (5.19), one obtains that a local witness evaluated in a stabiliser-diagonal state is equal to one genuine witness evaluated on a reduced state:

$$\langle W_{\boldsymbol{q}}\rangle_{\rho_{\mathscr{S}\mathrm{D}}} = \langle W_{|\mathscr{S}_{\boldsymbol{q}}^\mathfrak{m}\rangle}\rangle_{\rho_{\mathscr{S}\mathrm{D},\boldsymbol{q}}^\mathfrak{m}} = \langle W_{|\mathscr{S}_{\boldsymbol{q}}\rangle}\rangle_{\rho_{\mathscr{S}\mathrm{D},\boldsymbol{q}}} = \frac{1}{2} - p_0. \tag{5.38}$$

Moreover, for stabiliser-diagonal states like $\rho_{\mathscr{S}\mathrm{D},\boldsymbol{q}}^\mathfrak{m}$ and genuine witnesses like $W_{|\mathscr{S}_{\boldsymbol{q}}^\mathfrak{m}\rangle}$, which are prepared for two-qubit stabiliser states, the inequality in Eq. (5.20) becomes tight as we are about to prove.

As described in Sec. 2.4, the negativity of the state ρ is equal to

$$\mathcal{E}(\rho) = 2 \sum_{\lambda_i < 0} |\lambda_i|, \tag{5.39}$$

where $\{\lambda_i\}$ are the eigenvalues of ρ^{T_A}. Considering now the two qubits in $\boldsymbol{q}$ to be the two parties A and B, $\left(\rho_{\mathscr{S}\mathrm{D},\boldsymbol{q}}^\mathfrak{m}\right)^{T_A}$ is also diagonal in the stabiliser state basis (see App. A.7 for the details) with four eigenvalues

$$\lambda_{\mathbb{e}|\mathcal{W}_{\boldsymbol{q}}} = 1/2 - p_{\mathbb{e}|\mathcal{W}_{\boldsymbol{q}}} \tag{5.40}$$

given by the probabilities defined in Eq. (5.33) for $\mathbb{e}|\mathcal{W}_{\boldsymbol{q}} \in \{00, 01, 10, 11\}$. Note that these are the probabilities that the local-uncorrelated Pauli noise channel ε_P has to produce the excitation pattern $\mathbb{e}|\mathcal{W}_{\boldsymbol{q}}$ in the two stabilisers in $\mathcal{W}_{\boldsymbol{q}}$. For these noise channels, as long as the noise rate is below $1/2$, the probability of not producing any excitation on the stabilisers in $\mathcal{W}_{\boldsymbol{q}}$ is higher than the probability of producing a non-vanishing excitation pattern: $p_{00} \geq p_{01}, p_{10}, p_{11}$. If $p_{\mathbb{e}|\mathcal{W}_{\boldsymbol{q}}} \leq 1/2$ for all $\mathbb{e}|\mathcal{W}_{\boldsymbol{q}}$, then

all eigenvalues $\lambda_{\mathbb{e}|\mathcal{W}_{\boldsymbol{q}}} \geq 0$, implying that the negativity $\mathcal{E}\left(\rho^{\mathfrak{m}}_{\mathscr{S}\mathrm{D},\boldsymbol{q}}\right)$ vanishes. On the other hand, since the probabilities add up to one, if any of the probabilities is strictly bigger than $1/2$, the rest must be strictly smaller than $1/2$. Since $p_{00} \geq p_{01}, p_{10}, p_{11}$, only p_{00} can be bigger than $1/2$. In that case, $\lambda_{00} < 0$ and the rest of eigenvalues are positive, implying that $\mathcal{E}\left(\rho^{\mathfrak{m}}_{\mathscr{S}\mathrm{D},\boldsymbol{q}}\right) = 2p_{00} - 1$. Thus, provided the last equality relation in Eq. (5.38) the bound given by a genuine entanglement witness is tight:

$$\mathcal{E}\left(\rho^{\mathfrak{m}}_{\mathscr{S}\mathrm{D},\boldsymbol{q}}\right) = \begin{cases} -2\left\langle W_{|\mathscr{S}^{\mathfrak{m}}_{\boldsymbol{q}}\rangle}\right\rangle_{\rho^{\mathfrak{m}}_{\mathscr{S}\mathrm{D},\boldsymbol{q}}} & \text{if } \left\langle W_{|\mathscr{S}^{\mathfrak{m}}_{\boldsymbol{q}}\rangle}\right\rangle_{\rho^{\mathfrak{m}}_{\mathscr{S}\mathrm{D},\boldsymbol{q}}} < 0 \\ 0 & \text{otherwise} \end{cases}. \tag{5.41}$$

Finally, from the previous equation and from Eq. (5.38) one concludes that for stabiliser-diagonal states and subsystems of two qubits, the bound on LE restricted to the measurement basis $\mathcal{M}$ associated to a local witness that detects entanglement is tight:

$$\mathcal{E}^{\mathcal{M}}_{\boldsymbol{q}}(\rho_{\mathscr{S}\mathrm{D}}) = \begin{cases} -2\left\langle W_{\boldsymbol{q}}\right\rangle_{\rho_{\mathscr{S}\mathrm{D}}} & \text{if } \left\langle W_{\boldsymbol{q}}\right\rangle_{\rho_{\mathscr{S}\mathrm{D}}} < 0 \\ 0 & \text{otherwise} \end{cases}. \tag{5.42}$$

5.3.4 Modified local witnesses

Here we propose modified local witnesses that require less measurement settings. Like genuine witnesses in Sec. 5.2.2, local witnesses can be constructed with stabiliser operators whose evaluation requires less measurement settings than the standard local witnesses proposed. Again, the price of reducing the number of measurements is that the modified local witnesses are in general less tolerant to noise than standard local witnesses.

Once a valid subset $\mathcal{W}_{\boldsymbol{q}}$ that satisfies Prop. 1 is found, it can be used to construct modified local witnesses that require less measurement settings than the standard local witness in Eq. (5.8). For instance, with $|\boldsymbol{q}|$ measurements the value of the *alternative local witness* can be computed:

$$W^{\mathrm{a}}_{\boldsymbol{q}} = \frac{|\boldsymbol{q}| - 1}{2} I - \frac{1}{2} \sum_{s \in \mathcal{W}_{\boldsymbol{q}}} s. \tag{5.43}$$

If one is interested in the entanglement of multiple subsystems, multiple local witnesses must be evaluated, so the total number of measurement settings that must be measured increases. To avoid this we propose the two-measurements local witness that

can be measured with only two measurement settings. In fact, as we show in Sec. 5.5, these two measurement settings are enough to evaluate simultaneously all these modified witnesses for all the subsystems in the color code. If the stabiliser subset $\mathcal{W}_{\boldsymbol{q}}$ is composed entirely by X-type and Z-type stabilisers s^X and s^Z, respectively, just two measurement settings are enough to measure the *two-measurements local witness*:

$$W_{\boldsymbol{q}}^{2\mathrm{m}} = \frac{3}{2}I - \prod_{s^X \in \mathcal{W}_{\boldsymbol{q}}} \frac{I + s^X}{2} - \prod_{s^Z \in \mathcal{W}_{\boldsymbol{q}}} \frac{I + s^Z}{2}. \tag{5.44}$$

If $\mathcal{W}_{\boldsymbol{q}}$ is not of this form, a different stabiliser subset $\mathcal{W}_{\boldsymbol{q}}'$ can be used instead. For instance, the stabiliser subset $\mathcal{W}_{\{1,2,3,4\}} = \left\{ s_R^X s_R^Z, s_R^X, s_B^Z, s_G^Z \right\}$ is not of this form because three measurement bases are required to evaluate the local witness. In contrast, the stabiliser subset $\mathcal{W}_{\{1,2,3,4\}}' = \left\{ s_R^X, s_R^Z, s_B^Z, s_G^Z \right\}$ obtained by recombining the stabilisers in $\mathcal{W}_{\{1,2,3,4\}}$ has the right form to construct a two-measurement local witness because all the stabilisers in it can be evaluated with only two measurement settings.

Like in Eq. (5.7), the modified local witnesses are valid witnesses because their expectation value is greater than or equal than the expectation value of the standard local witness for every state:

$$\langle W_{\boldsymbol{q}} \rangle_\rho \leq \langle W_{\boldsymbol{q}}^{\mathrm{a}} \rangle_\rho \quad , \quad \langle W_{\boldsymbol{q}} \rangle_\rho \leq \langle W_{\boldsymbol{q}}^{2\mathrm{m}} \rangle_\rho \quad \forall \rho. \tag{5.45}$$

5.3.5 Robustness and comparison of witnesses

In this section we study and compare the witnesses introduced previously in terms of their tolerance to noise using the white noise model [137]. The white noise model provides a critical fidelity between the model and the ideal stabiliser state below which witnesses cannot detect entanglement in this model. Thus, it serves as a benchmark figure of merit of each witness. Moreover, there are witnesses that detect entanglement if another witness detects entanglement. That is, some witnesses are finer entanglement detectors than others.

The white noise model applied to a stabiliser state $|\mathscr{S}\rangle$ is the state

$$\rho_{\mathrm{W}} = F |\mathscr{S}\rangle \langle \mathscr{S}| + (1 - F) \frac{I}{2^n}, \tag{5.46}$$

where $F \in [0, 1]$ is a parameter parameter that interpolates between the ideal stabiliser

		Formula	Meas. set.	Crit. fid. F_c
Genuine witnesses	Standard	$W_{|\mathscr{S}\rangle} = \dfrac{1}{2} I - \prod_{s \in \mathcal{S}} \dfrac{I+s}{2}$	$2^n - 1$	$1/2 + \mathcal{O}(2^{-n})$
	Alternative	$W^a_{|\mathscr{S}\rangle} = \dfrac{n-1}{2} I - \dfrac{1}{2} \sum_{s \in \mathcal{S}} s$	n	$1 - 1/n$
	Two measurements	$W^{2\mathrm{m}}_{|\mathscr{S}\rangle} =$ $\dfrac{3}{2} I - \prod_{s^X \in \mathcal{S}} \dfrac{I+s^X}{2} - \prod_{s^Z \in \mathcal{S}} \dfrac{I+s^Z}{2}$	2	$\in [2/3, 3/4]$
Local witnesses	Standard	$W_{\boldsymbol{q}} = \dfrac{1}{2} I - \prod_{s \in \mathcal{W}_{\boldsymbol{q}}} \dfrac{I+s}{2}$	$2^{|\boldsymbol{q}|} - 1$	$\in [1/3, 1/2]$
	Alternative	$W^{\mathrm{a}}_{\boldsymbol{q}} = \dfrac{|\boldsymbol{q}|-1}{2} I - \dfrac{1}{2} \sum_{s \in \mathcal{W}_{\boldsymbol{q}}} s$	$|\boldsymbol{q}|$	$1 - 1/|\boldsymbol{q}|$
	Two measurements	$W^{2\mathrm{m}}_{\boldsymbol{q}} =$ $\dfrac{3}{2} I - \prod_{s^X \in \mathcal{W}_{\boldsymbol{q}}} \dfrac{I+s^X}{2} - \prod_{s^Z \in \mathcal{W}_{\boldsymbol{q}}} \dfrac{I+s^Z}{2}$	2	$\in [1/2, 3/4]$

Table 5.1: Genuine and local entanglement witnesses. From left to right the table contains: the type of witness, the expressions of witnesses in terms of the stabilisers operators s defining an n-qubit stabiliser state $|\mathscr{S}\rangle$, the maximum number of measurement settings required to compute the expectation value of the witnesses, and the critical fidelity of the white noise state in Eq. (5.46) below which no entanglement is detected. Genuine entanglement witnesses are constructed from a generator set $\mathcal{S}$ of the stabiliser group: $\langle \mathcal{S} \rangle = \mathscr{S}$, while for local witnesses, $\mathcal{W}_{\boldsymbol{q}}$ is simply a subset of stabilisers $\mathcal{W}_{\boldsymbol{q}} \subset \mathscr{S}$.

state $|\mathscr{S}\rangle$ for $F = 1$ and the completely mixed state $I/2^n$ of n qubits for $F = 0$. It is also, up to a small factor, the fidelity

$$F = \langle \mathscr{S} | \rho_{\mathrm{W}} | \mathscr{S} \rangle - \frac{2^{-n}}{1 - 2^{-n}} (1 - \langle \mathscr{S} | \rho_{\mathrm{W}} | \mathscr{S} \rangle) \tag{5.47}$$

between $|\mathscr{S}\rangle$ and ρ_{W}.

The *robustness* of a witness is then given by the critical fidelity F_c that guarantees that the expectation value of the witness operator evaluated in the state ρ_{W} is negative, and thus entanglement is detected. The critical fidelities of all witnesses discussed are summarised in Table 5.1.

Moreover, one witness W is said to be *finer* than another W' if the expectation value of W is negative on every state where the expectation value of W' is negative. Thus, there is a positive coefficient $\beta > 0$ such that $\langle W \rangle_\rho \le \beta \langle W' \rangle_\rho$ for any state ρ. In that case, one can be sure that W detects entanglement if W' detects it. If one witness is finer than another, it is also more robust.

There is a hierarchy between the proposed witnesses considering this criterion. First, the standard genuine witness is finer than the modified genuine witnesses [137, 138]:

$$\langle W_{|\mathscr{S}\rangle}\rangle_\rho \leq \langle W^{\mathrm{a}}_{|\mathscr{S}\rangle}\rangle_\rho \quad , \quad \langle W_{|\mathscr{S}\rangle}\rangle_\rho \leq \langle W^{2\mathrm{m}}_{|\mathscr{S}\rangle}\rangle_\rho \quad \forall \rho, \tag{5.48}$$

which again shows that reducing the number of measurements by means of modifying the witnesses leads to a decrease of the tolerance to noise. Similarly, and using the same ideas used in Refs. [137, 138], the standard local witness constructed with the stabiliser subset $\mathcal{W}_{\boldsymbol{q}}$ is finer than the modified witnesses constructed from the same stabiliser subset:

$$\langle W_{\boldsymbol{q}}\rangle_\rho \leq \langle W^{\mathrm{a}}_{\boldsymbol{q}}\rangle_\rho \quad , \quad \langle W_{\boldsymbol{q}}\rangle_\rho \leq \langle W^{2\mathrm{m}}_{\boldsymbol{q}}\rangle_\rho \quad \forall \rho. \tag{5.49}$$

Second, standard local witnesses, for every subsystem $\boldsymbol{q}$, are finer than the standard genuine witness:

$$\langle W_{\boldsymbol{q}}\rangle_\rho \leq \langle W_{|\mathscr{S}\rangle}\rangle_\rho \quad \forall \rho. \tag{5.50}$$

This means that all local witnesses prepared for the stabiliser state $|\mathscr{S}\rangle$ detect entanglement for all subsystems $\boldsymbol{q}$ if the genuine entanglement witness prepared for $|\mathscr{S}\rangle$ detects genuine entanglement.

Third, a local witness $W_{\boldsymbol{q}}$ is finer than a local witness $W_{\boldsymbol{q}'}$ prepared for a different subsystem $\boldsymbol{q}'$:

$$\langle W_{\boldsymbol{q}}\rangle_\rho \leq \langle W_{\boldsymbol{q}'}\rangle_\rho \tag{5.51}$$

if the subgroup $\langle \mathcal{W}_{\boldsymbol{q}}\rangle$ generated by the stabiliser subset $\mathcal{W}_{\boldsymbol{q}}$ corresponding to $W_{\boldsymbol{q}}$ is contained in the subgroup $\langle \mathcal{W}_{\boldsymbol{q}'}\rangle$ generated by the stabiliser subset $\mathcal{W}_{\boldsymbol{q}'}$ corresponding to $W_{\boldsymbol{q}'}$ as $\langle \mathcal{W}_{\boldsymbol{q}}\rangle \subset \langle \mathcal{W}'_{\boldsymbol{q}}\rangle$. For instance, the standard local witness constructed from $\mathcal{W}_{\{2,3\}} = \left\{ s^X_R, s^Z_B \right\}$ is finer than the standard local witness constructed from $\mathcal{W}_{\{2,3,4\}} = \left\{ s^X_R, s^Z_B s^Z_G, s^Z_G \right\}$. Note that $\mathcal{W}_{\boldsymbol{q}} \subset \mathcal{W}_{\boldsymbol{q}'}$ is not necessary for the previous condition.

5.4 Construction of local witnesses

The construction of local witnesses for stabiliser states is not straightforward because Prop. 1 is hard to use in practice. We propose two methods to find a stabiliser subset $\mathcal{W}_{\boldsymbol{q}}$ that satisfies the proposition: the *stabiliser-based method* proposed in Sec. 5.4.1 uses a theorem that is equivalent to Prop. 1 but the properties are more intuitive and

easier to check in practice. For simple stabiliser states Prop. 1 can be applied by simple inspection. The *graph-based method* in Sec. 5.4.2 employs the local-unitary equivalence of stabiliser and graph states to construct local witnesses. Since the stabiliser-based method provides the necessary and sufficient criteria for the construction of valid local witnesses for a stabiliser state of interest, using this method exhaustively one can construct all existing local witnesses of this type for a stabiliser state of interest. In contrast, we prove in App. A.9 that there are some local witnesses that cannot be constructed with the graph-based method. Moreover, we show that generally there are multiple local witness for every subsystem, and one just needs the positive detection of one of them to guarantee that the subsystem is entangled.

5.4.1 Stabiliser-based method

Here we propose a theorem which properties are operationally simpler to check than Prop. 1 but is equivalent to it. Local witnesses can be constructed by checking whether a given stabiliser subset satisfies the properties of this theorem. We show with an example how to use this theorem to construct local witnesses for the color code. In essence, the last property of Prop. 1 can be hard to check in practice, so we replace it by a property related to the structure of qubit-wise commutation and anti-commutation of the stabilisers involved in the local witness. This structure can be checked by simple inspection.

Properties (A) and (B) in Prop. 1 are operationally simple to implement. In contrast, property (C) does not provide intuition on how the stabilisers must be selected, so we enunciate and prove a theorem equivalent to Prop. 1 that substitutes (C) by two properties.

Let us start by defining the *pseudo-incidence matrix* $\tilde{\mathbb{M}}(S)$ of a subset S of stabilisers of an N-qubit stabiliser state. It is the $N \times \binom{|S|}{2}$ binary matrix created from the commutation/anti-commutation of each pair of different stabilisers $s_i, s_j \in S$ on each qubit (see Fig. 5.1 for an example):

$$\tilde{\mathbb{M}}(S)_{ql} = \begin{cases} 1 & \text{if} \quad \{\sigma_{qi}, \sigma_{qj}\} = 0 \\ 0 & \text{if} \quad [\sigma_{qi}, \sigma_{qj}] = 0 \end{cases}, \tag{5.52}$$

where the Pauli operators σ_{qi} are given by the form of the stabilisers $s_i = \bigotimes_{q=1}^{n} \sigma_{qi}$. The index $l = \{i, j\}$ labels all pairs of different stabilisers $s_i, s_j \in S$ from 1 to the

Figure 5.1: Stabiliser-based method to decide if a given (a) stabiliser subset $\mathcal{W}_{\boldsymbol{q}} \subset \mathscr{S}$ composed by the stabilisers in (b) (belonging to the seven-qubit color code stabilisers in Fig. 3.4) constructs a local witness for the subsystem $\boldsymbol{q} = \{2, 3, 4\}$. It contains $|\boldsymbol{q}| = 3$ independent and commuting stabilisers so it satisfies property (A) in Theorem 1. The stabilisers in it commute qubit-wise outside $\boldsymbol{q}$, so $\mathcal{W}_{\boldsymbol{q}}$ also satisfies property (B). (c) The set $\mathcal{W}_{\boldsymbol{q}}|_{\boldsymbol{q}}$ of reduced stabilisers in the subsystem $\boldsymbol{q}$ are also independent and commute, so it satisfies property (C.i) as well. (d) In order to check property (C.ii) obtain the pseudo-incidence matrix $\tilde{\mathbb{M}}(\mathcal{W}_{\boldsymbol{q}}|_{\boldsymbol{q}})$: for each pair of reduced stabilisers $s_i|_{\boldsymbol{q}}, s_j|_{\boldsymbol{q}} \in \mathcal{W}_{\boldsymbol{q}}|_{\boldsymbol{q}}$ and for each qubit $q \in \boldsymbol{q}$ write a 0 if the Pauli operators $\sigma_{qi}, \sigma_{qj} \in \{I, X, Y, Z\}$ corresponding to $s_i|_{\boldsymbol{q}}, s_j|_{\boldsymbol{q}}$, respectively, commute $[\sigma_{qi}, \sigma_{qj}] = 0$, and 1 if they anti-commute $\{\sigma_{qi}, \sigma_{qj}\} = 0$. (e) The rank modulo 2 of the pseudo-incidence matrix is $|\boldsymbol{q}| - 1 = 2$, so it satisfies property (C.ii). Hence, $\mathcal{W}_{\boldsymbol{q}}$ satisfies Theorem 1, so it constructs a valid local witness for the subsystem $\boldsymbol{q} = \{2, 3, 4\}$.

number of pairs $\binom{|S|}{2}$, and the index q labels the qubits from 1 to n. The order of the columns does not provide any information. Given that local unitary operators V_{LUE} preserve the qubit-wise commutation/anti-commutation of stabilisers, they also preserve the pseudo-incidence matrix:

$$\tilde{\mathbb{M}}\left(V_{\text{LUE}} S V_{\text{LUE}}^{\dagger}\right) = \tilde{\mathbb{M}}(S), \tag{5.53}$$

where, for a subset S of stabilisers, $KSK^{\dagger} = \{KsK^{\dagger} : s \in S\}$ for any operator K.

The pseudo-incidence matrix can be used to enunciate the following theorem:

Theorem. 1 *A subset $\mathcal{W}_{\boldsymbol{q}} \subset \mathscr{S}$ of the stabiliser group $\mathscr{S}$ defines a valid local witness of the form in Eq. (5.8) for the subsystem $\boldsymbol{q}$ if it satisfies the following properties:*

(A) It contains $|\mathcal{W}_{\boldsymbol{q}}| = |\boldsymbol{q}|$ independent and commuting stabilisers.

(B) For every qubit $q \notin \boldsymbol{q}$, the Pauli operators σ_{qi}, σ_{qj} corresponding to any two stabilisers s_i, $s_j \in \mathcal{W}_{\boldsymbol{q}}$ commute: $[\sigma_{qi}, \sigma_{qj}] = 0$.

(C.i) The set of reduced stabilisers $\mathcal{W}_{\boldsymbol{q}}|_{\boldsymbol{q}}$ defined in Prop. 1 contains $|\boldsymbol{q}|$ independent and commuting stabilisers.

(C.ii) The rank modulo 2 of the pseudo-incidence matrix is:

$$\text{rank}\left(\tilde{\mathbb{M}}\left(\mathcal{W}_{\boldsymbol{q}}|_{\boldsymbol{q}}\right)\right) = |\boldsymbol{q}| - 1. \tag{5.54}$$

In order to prove this theorem, we need to prove that a stabiliser state of N qubits with generator set $\mathcal{S}$ is genuinely entangled if and only if the pseudo-incidence matrix satisfies that $\text{rank}(\tilde{\mathbb{M}})(\mathcal{S}) = N - 1$. We prove it first for graph states, and then use the local-unitary equivalence between stabiliser and graph states to prove it for stabiliser states.

It is not difficult to check that the pseudo-incidence matrix of a graph state defined by the generator set $\mathcal{G}$ is equal to the incidence matrix of the underlying graph $G(\boldsymbol{N}, \mathcal{L})$:

$$\tilde{\mathbb{M}}(\mathcal{G}) = \mathbb{M}. \tag{5.55}$$

The matrix element $\tilde{\mathbb{M}}(\mathcal{G})_{q\{i,j\}}$ corresponding to the row q and the column $\{i,j\}$ is zero if $q \notin \{i,j\}$ (in that case $\sigma_{qi}, \sigma_{qj} \in \{I, Z\}$, so σ_{qi}, σ_{qj} commute) or if the link is not present in the graph $\{i,j\} \notin \mathcal{L}$ (in that case $\sigma_{qi}, \sigma_{qj} \in \{X, I\}$, so they also commute). Therefore the only non-zero columns of $\tilde{\mathbb{M}}(\mathcal{G})$ correspond to the existing links $\{i,j\} \in \mathcal{L}$, and in these columns, the only two non-zero elements correspond to $q = i$ and $q' = j$. This is exactly the definition of the incidence matrix $\mathbb{M}$ of the underlying graph $G(\boldsymbol{N}, \mathcal{L})$.

The rank of the incidence matrix of a graph with N nodes determines the number κ of connected components in the graph, i.e., the number of connected groups of nodes that are disconnected from the rest of groups:

$$\text{rank}(\mathbb{M}) = N - \kappa. \tag{5.56}$$

Thus, a graph is connected, i.e., the nodes cannot be separated in disconnected groups without breaking a link, if $\kappa = 1$. Consequently, given that genuinely entangled graph states are defined on connected graphs, a generator set $\mathcal{G}$ defines a genuinely entangled

graph state if

$$\text{rank}(\tilde{\mathbb{M}}(\mathcal{G})) = N - 1. \tag{5.57}$$

Moreover, every stabiliser state of N qubits with generator set $\mathcal{S}$ can be transformed into a graph state with generator set $\mathcal{G}$ by means of a local unitary U_{LUE}. Furthermore, $\mathcal{S}$ can be directly transformed into $\mathcal{G}$ by means of the local unitary V_{LUE} and a recombination of stabilisers $\mathbb{R}$ [174]. Here $\mathbb{R}$ is an $N \times N$ binary and invertible matrix that defines how the stabilisers are multiplied among themselves:

$$s'_j = \prod_{s_i \in \mathcal{S}} s_i^{\mathbb{R}_{ij}}. \tag{5.58}$$

These recombined stabilisers s'_j form a different generator set $\mathcal{S}'$ that defines the same stabiliser state than $\mathcal{S}$ given that $\langle \mathcal{S} \rangle = \langle \mathcal{S}' \rangle = \mathscr{S}$. Then, all graph state generators $g_q \in \mathcal{G}$ can be obtained from $\mathcal{S}$ by means of V_{LUE} and $\mathbb{R}$ as:

$$\mathcal{G} = \left\{ g_q = V_{\text{LUE}} \left(\prod_{s_i \in \mathcal{S}} s_i^{\mathbb{R}_{iq}} \right) V_{\text{LUE}}^\dagger : \forall q \right\}. \tag{5.59}$$

Invertible recombinations $\mathbb{R}$ preserve the rank of the pseudo-incidence matrix as we prove in App. A.8. Given that local unitary operators V_{LUE} also preserve the rank of the pseudo-incidence matrix, one obtains that the rank of the pseudo-incidence matrices of $\mathcal{S}$ and $\mathcal{G}$ coincide:

$$\text{rank}\left(\tilde{\mathbb{M}}(\mathcal{S}) \right) = \text{rank}\left(\tilde{\mathbb{M}}(\mathcal{G}) \right). \tag{5.60}$$

Furthermore, V_{LUE} preserves the separability of the stabiliser state, so the stabiliser state defined by $\mathcal{S}$ is genuinely entangled if the graph state defined by $\mathcal{G}$ is genuinely entangled. Consequently, with Eqs. (5.57) and 5.60 one arrives to the following conclusion for generator sets $\mathcal{S}$:

Lemma. 1 *A set $\mathcal{S}$ of stabilisers defines a genuinely entangled state of N qubits, i.e., it is a generator set, if and only if:*

$$\tilde{\mathbb{M}}(\mathcal{S}) = N - 1. \tag{5.61}$$

In order to prove Theorem 1 we start by assuming that a given stabiliser subset $\mathcal{W}_q$ satisfies Prop. 1. Then, property (C) says that $\mathcal{W}_q|_q$ is a generator set, so it satis-

fies property (C.i) trivially. In this scenario, from Lemma 1 one obtains that $\mathcal{W}_{\boldsymbol{q}}$ also satisfies property (C.ii). Therefore, Theorem 1 is satisfied if Prop. 1 is satisfied. To complete the proof now assume that $\mathcal{W}_{\boldsymbol{q}}$ satisfies Theorem 1. Then, due to properties(A) and (C.i) $\mathcal{W}_{\boldsymbol{q}}|_{\boldsymbol{q}}$ is a generator set. Thus, Lemma 1 can be applied to $\mathcal{W}_{\boldsymbol{q}}|_{\boldsymbol{q}}$. Given that it satisfies property (C.ii), provided the Lemma, $\mathcal{W}_{\boldsymbol{q}}$ also satisfies property (C). Therefore, Prop. 1 is satisfied if Theorem 1 is satisfied. Hence, this shows that Theorem 1 is equivalent to Prop. 1.

Given that Theorem 1 is equivalent to Prop. 1, one can use this theorem to find all possible local witnesses that can be constructed for a given stabiliser state. In Sec. 5.5 we obtain all possible local witnesses for the seven-qubit color code and apply them to an experimental realisation of this state. For some stabiliser states like the CSS states, including the color code and the surface code, this method can be used by simple inspection. We also employ this method in Sec. 5.7 to obtain local witnesses for the color code with the aim of studying the decay of LE as a function of the qubit distance.

5.4.2 Graph-based method

In this section we describe the graph-based method to construct local witnesses. On graph states the construction of local witnesses is generally simple [216]. The method consists in obtaining a graph state that is local-unitary equivalent (LUE) to a stabiliser state of interest and constructing a local witness for the graph state. By applying to this local witness the inverse local unitary that transforms the stabiliser state into the graph state one obtains a local witness for the stabiliser state. The construction of a LUE graph state is described in detail in Sec. 5.6 and can be implemented in practice with the Python code **StabGraph** [5] that we developed. However, local witnesses can only be constructed for a graph state if the subsystem of interest is connected in the underlying graph. Thus, we show how to obtain LUE graph states where the subsystem might be connected by means of local complementation (LC) unitary operators.

First, one has to find the local unitary U_{LUE} that transforms the stabiliser state into a graph state: $U_{\mathrm{LUE}}|\mathscr{S}\rangle = |\mathscr{G}\rangle$. Consequently, U_{LUE} transforms a stabiliser generator set $\mathcal{S}$ of $|\mathscr{S}\rangle$ into a graph state generator set $\mathcal{G}$ of $|\mathscr{G}\rangle$ up to a recombination $\mathbb{R}$ as stated in Eq. (5.59). In Sec. 5.6 we provide an explicit recipe to obtain U_{LUE}, $\mathbb{R}$, and the adjacency matrix Γ that defines the underlying graph of $|\mathscr{G}\rangle$. Second, check that

the subsystem of interest $\boldsymbol{q}$ is connected in the underlying graph, i.e., that the reduced graph in $\boldsymbol{q}$ obtained by removing all nodes outside $\boldsymbol{q}$ and their links is a connected graph. Third, construct a local witness prepared for the graph state $|\mathscr{G}\rangle$, with the subset $\mathcal{W}_{\boldsymbol{q}}^{\mathscr{G}} = \{g_q \in \mathcal{G} : q \in \boldsymbol{q}\}$ as described in Ref. [216]:

$$W_{\boldsymbol{q}}^{\mathscr{G}} = \frac{1}{2} I - \prod_{g_q \in \mathcal{W}_{\boldsymbol{q}}^{\mathscr{G}}} \frac{I + g_q}{2}. \tag{5.62}$$

Fourth, given that local unitary operators preserve the properties in Prop. 1, the subset $\mathcal{W}_{\boldsymbol{q}} = U_{\mathrm{LUE}}^{-1} \mathcal{W}_{\boldsymbol{q}}^{\mathscr{G}} U_{\mathrm{LUE}}$ is composed of stabilisers in the stabiliser group $\mathscr{S}$ and serves to construct a valid local witness of the form in Eq. (5.8) for the stabiliser state $|\mathscr{S}\rangle$.

This process is illustrated for the example of the first graph state in Fig. 5.2(b). The local unitary $U_{\mathrm{LUE}} = H_1 H_5 H_7$ transforms the seven-qubit stabiliser color code into a graph state $|\mathscr{G}\rangle$ with the following correspondence between stabilisers and graph state generators:

$$
\begin{aligned}
U_{\mathrm{LUE}}^{-1} g_1 U_{\mathrm{LUE}} &= s_R^Z & , & \quad U_{\mathrm{LUE}}^{-1} g_2 U_{\mathrm{LUE}} = s_G^X s_L^X, \\
U_{\mathrm{LUE}}^{-1} g_3 U_{\mathrm{LUE}} &= s_R^X s_B^X s_G^X & , & \quad U_{\mathrm{LUE}}^{-1} g_4 U_{\mathrm{LUE}} = s_B^X s_L^X, \\
U_{\mathrm{LUE}}^{-1} g_5 U_{\mathrm{LUE}} &= s_B^Z & , & \quad U_{\mathrm{LUE}}^{-1} g_6 U_{\mathrm{LUE}} = s_R^X s_L^X, \\
U_{\mathrm{LUE}}^{-1} g_7 U_{\mathrm{LUE}} &= s_G^Z.
\end{aligned}
\tag{5.63}
$$

As illustrated in Fig. 5.2(b), the subsystem $\{5, 6\}$ is connected in the resulting underlying graph, so one can construct a local witness prepared for $|\mathscr{G}\rangle$ from the generator subset $\mathcal{W}_{\{5,6\}}^{\mathscr{G}} = \{g_5, g_6\}$. The corresponding local witness prepared for the stabiliser state $|\mathscr{S}\rangle$ of interest is constructed from the stabiliser subset $\mathcal{W}_{\{5,6\}} = U_{\mathrm{LUE}}^{-1} \mathcal{W}_{\{5,6\}}^{\mathscr{G}} U_{\mathrm{LUE}} = \{s_B^Z, s_R^X s_L^X\}$:

$$W_{\{5,6\}} = \frac{1}{2} I - \frac{I + s_B^Z}{2} \frac{I + s_R^X s_L^X}{2}. \tag{5.64}$$

In contrast, the subsystem $\{2, 3, 4\}$ in red is not connected within this graph, thus the stabiliser subset $\mathcal{W}_{\{2,3,4\}} = \{s_G^X s_L^X, s_R^X s_B^X s_G^X, s_B^X s_L^X\}$ does not provide a local witness. This illustrates that construction of a witness using the graph-based method requires finding a LUE graph state for which the qubits corresponding to the subsystem of interest are connected.

If the subsystem $\boldsymbol{q}$ of interest is not connected within the graph underlying the graph state $|\mathscr{G}\rangle$, one might obtain a LUE graph state where the subsystem is connected
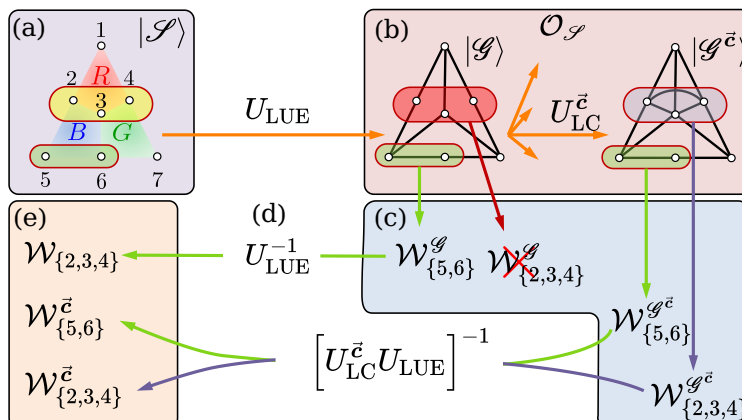
Figure 5.2: Graph-based method. Here, local witnesses for (a) subsystems $\{5,6\}$ (green) and $\{2,3,4\}$ (yellow) of the seven-qubit color code $|\mathscr{S}\rangle$ are constructed. The method consists of the following steps: Find a local unitary U_{LUE} that generates a local-unitary equivalent (LUE) graph state $|\mathscr{G}\rangle = U_{\text{LUE}} |\mathscr{S}\rangle$. (b) With a sequence $\vec{c}$ of local complementation (LC) unitary operations $U_{\text{LC}}^{\vec{c}}$ explore the orbit $\mathcal{O}_{\mathscr{S}}$ of graph states LUE to $|\mathscr{S}\rangle$, i.e., $|\mathscr{G}^{\vec{c}}\rangle = U_{\text{LC}}^{\vec{c}} |\mathscr{G}\rangle$. For each graph consider the subsystems that are connected (e.g., $\{5,6\}$ is connected in both depicted graphs, but $\{2,3,4\}$ is connected only in the second) and take the (c) generator subsets $\mathcal{W}_{\boldsymbol{q}}^{\mathscr{G}^{\vec{c}}}$. (d) Apply the local unitary $\left[U_{\text{LC}}^{\vec{c}} U_{\text{LUE}} \right]^{-1}$ to obtain (e) the stabiliser subsets $\mathcal{W}_{\boldsymbol{q}}^{\vec{c}}$ that construct local witnesses for the stabiliser state $|\mathscr{S}\rangle$.

by means of a LC unitary [177] (see Sec. 2.2.2). One can use a sequence of LC unitary operations $U_{\text{LC}}^{\vec{c}} = U_{\text{LC}}^{(q_{|\vec{c}|})} \cdots U_{\text{LC}}^{(q_1)}$ corresponding to an ordered list of $|\vec{c}|$ qubits $\vec{c} = (q_1, q_2, \ldots, q_{|\vec{c}|})$ (qubits might appear more than once) to generate other LUE graph states: the entirety of the LUE graph states $|\mathscr{G}\rangle$, $|\mathscr{G}^{(q)}\rangle$, ..., $|\mathscr{G}^{\vec{c}}\rangle$, ... reached by applying all possible sequences is a finite set and corresponds to the orbit of the graph $G(\boldsymbol{N}, \mathcal{L})$ associated to the initial graph state $|\mathscr{G}\rangle$ [177].

The determination of a sequence of LC operations that yields a graph state where the subsystem is connected is not a simple problem in general. However, as we show in Sec. 5.6.3, for subsystems of two qubits we can find such sequence. We use two-qubit subsystems in Sec. 5.7.2 to study how LE decays with distance in noisy color codes.

Then, for each connected subsystem in the graph underlying each of the graph states $|\mathscr{G}^{\vec{c}}\rangle$ obtained in this manner one can take the following subset of the corresponding generator set $\mathcal{G}^{\vec{c}}$:

$$\mathcal{W}_{\boldsymbol{q}}^{\mathscr{G}^{\vec{c}}} = \left\{ g_q^{\vec{c}} \in \mathcal{G}^{\vec{c}} : \ q \in \boldsymbol{q} \right\}, \tag{5.65}$$

and transform these graph state generators back into a subset $\mathcal{W}_{\boldsymbol{q}}^{\vec{c}} \subset \mathscr{S}$ of the stabiliser

group $\mathscr{S}$:

$$\mathcal{W}_{\boldsymbol{q}}^{\vec{c}} = U_{\text{LUE}}^{-1} \left[U_{\text{LC}}^{\vec{c}} \right]^{-1} \mathcal{W}_{\boldsymbol{q}}^{\mathscr{G}\vec{c}} U_{\text{LC}}^{\vec{c}} U_{\text{LUE}}, \qquad (5.66)$$

by the inverse chain of local unitary operations corresponding to the sequence of LC operations. This subset of stabilisers satisfies Prop. 1, so it can be used to construct a valid local witness for a stabiliser state of interest.

5.5 Local witnesses on an experimental state: the seven-qubit color code

Here we test the performance of local witnesses to detect entanglement in an experimental realisation of the seven-qubit color code implemented in trapped ions by means of a complex quantum circuit [76]. This circuit is described in Sec. 5.6.1 in more detail. In Sec. 5.5.1 we use both methods described previously to construct multiple local witnesses, and then, in Sec. 5.5.2, we evaluate them using the experimental data. In fact, we construct all local witnesses that can be constructed with each method for all 119 subsystems of the seven-qubit color code and evaluate the witnesses using the experimental data extracted from the experimental state: the expectation value of the 127 stabilisers. These 119 subsystems are simply the $2^7 = 128$ possible subsets of seven qubits excluding the empty set, the subset containing the seven qubits, and the seven subsets containing only one qubit. A local witness having a negative expectation value indicates the detection of entanglement. From the collection of detections it is possible to obtain relevant information about the entanglement structure of the experimental seven-qubit color code.

As we show, the detection of entanglement in many subsystems does not require the construction of all local witnesses and the measurement of all the stabilisers. For instance, with only two measurements one can compute all the two-measurements local witnesses simultaneously, which for the seven-qubit color code, detect the entanglement in most of the two-qubit subsystems and on six of the three-qubit subsystems.

5.5.1 Local witnesses obtained

Here we show the results of applying the graph-based method and the stabiliser-based method to construct local witnesses. Given the small size of the seven-qubit color code,

$|q|$	Subsystem q	G.-b.	S.-b.	Two-m.
2	all	54	72	4
3	string like	32	40	4
	non-string like	34	44	5
4	face like	17	30	9
	non-face like	18	18	3
5	all	8	8	3
6	all	3	3	2
Total	119	3122	3927	476

Table 5.2: Number of constructed local witnesses for the seven-qubit color code. Columns from left to right: number of qubits in the subsystem, classification of subsystems, number of standard local witnesses constructed with the graph-based method, number of standard local witnesses constructed with the stabiliser-based method, and number of two-measurements local witnesses.

we can use the methods exhaustively to provide all existing local witnesses as defined in Prop. 1 for the state. With the graph-based method we obtain 3122 standard local witnesses for the seven-qubit color code. These are obtained by exhaustively exploring the orbit of LUE graph states, constructing all valid local witnesses for each graph state, and finally filtering out the ones that are repeated. The witnesses found with the graph-based method are a subset of the 3927 local witnesses found with the stabiliser-based method. The set found with the stabiliser-based method was obtained by exhaustively checking for each possible stabiliser subset $\mathcal{W}_q \subset \mathscr{S}$ that can be formed with the 127 stabilisers in the stabiliser group $\mathscr{S}$ if the subset satisfies Theorem 1. Given that this theorem defines the necessary and sufficient criteria to construct a witness, the set of 3927 local witnesses found with the stabiliser-based method is the set of all possible local witnesses for the seven-qubit color code. In contrast, the graph-based method provides only a subset of these witnesses because the method does not employ necessary, but only sufficient conditions. We prove it in App. A.9 by showing an example of a local witness that can be constructed with the stabiliser-based method but not with the graph-based method. The results, which are summarised in Table 5.2, were obtained by means of a Python code that I developed.

The distribution of local witnesses on the 119 possible subsystems depends only on the stabiliser structure of the seven-qubit color code. One can distinguish between two types of three-qubit subsystems and two types of four-qubit subsystems. The "string like subsystems" are the three-qubit subsystems that are the support of a logical op-

erator: $\{1,2,5\}$, $\{1,4,7\}$, $\{5,6,7\}$, $\{1,3,6\}$, $\{3,4,5\}$, $\{2,3,7\}$, and $\{2,4,6\}$, while the "non-string like subsystems" are the rest of three-qubit subsystems. The "face like subsystems" are the four-qubit subsystems that are the support of a face operator or a product of them: $\{1,2,3,4\}$, $\{2,3,5,6\}$, $\{3,4,6,7\}$, $\{1,2,6,7\}$, $\{1,4,5,6\}$, $\{2,4,5,7\}$, and $\{1,3,5,7\}$, while the "non-face like subsystems" are the rest of four-qubit subsystems.

5.5.2 Evaluation of experimental data

The seven-qubit color code was realised experimentally using a trapped-ion quantum processor [76]. Seven $^{40}\text{Ca}^+$ ions were used to encode one logical qubit into seven physical qubits. The experimental state was implemented by the successive creation of four-qubit entanglement on each face using non-local unitary operations combined with multiple single-qubit operations in a sequence involving more than one hundred operations.

This experimental state reached an overall quantum state fidelity of $0.33(1)$ with respect to the ideal expected seven-qubit color code. The perfect realisation would lead to the pure genuinely entangled state where the expectation value of all witnesses is $-1/2$, but the imperfections on the experiment degrade the entanglement structure, so the expectation value of local witnesses increases with respect to the ideal state. Here, the experimental data corresponding to the measurement of the 127 stabilisers is used to compute the expectation values of the genuine and local witnesses and represent them in Fig. 5.3. Error bars correspond to the variance based on independent binomial distributions of expectation values for each stabiliser operator (see App. A.10 for the derivation of the variance).

The first observation is that the entanglement of multiple subsystems has been detected, as summarised in Table 5.3. The detections by the standard local witnesses are: all the 21 two-qubit subsystems, all the 35 three-qubit subsystems except $\{1,2,5\}$ and $\{1,3,5\}$, and 6 four-qubit subsystems out of the possible 35. The detections of the two-measurements local witnesses are: all the 21 two-qubit subsystems except $\{1,3\}$, $\{1,4\}$, and $\{4,7\}$, and 6 three-qubit subsystems out of the possible 35. Only two measurement settings have been required to evaluate the entire set of two-measurement local witnesses. Regarding the distribution of points one can confirm what Eq. (5.51) suggests: local witnesses for small subsystems tend to have more negative expectation values,
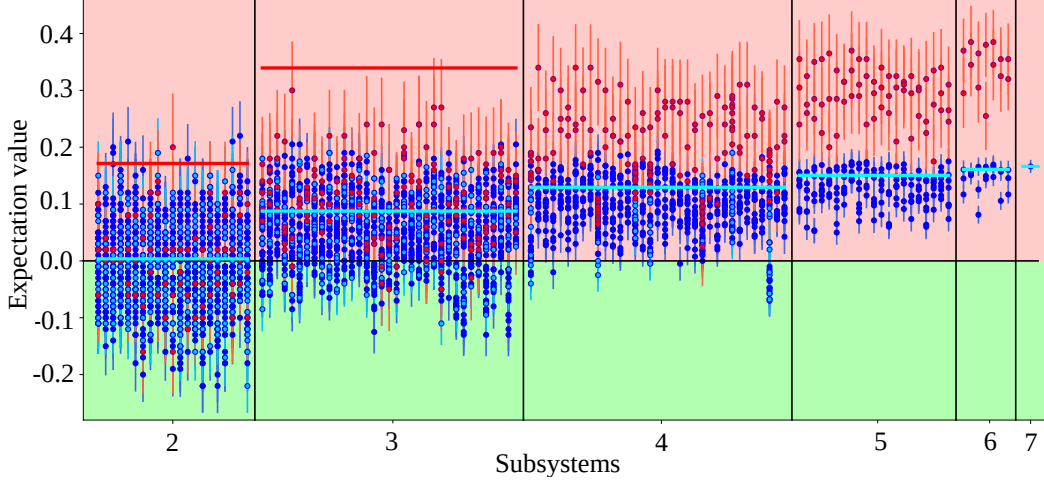
Figure 5.3: Entanglement structure of the seven-qubit color code. Each point corresponds to the expectation value of a witness evaluated on the experimental implementation of the seven-qubit color code [76], so each point in the green area represents an entanglement detection. The subsystems q are ordered in 119 columns from left to right in the following way: two-qubit subsystems $\{1, 2\}$, $\{1, 3\}$, ..., $\{1, 7\}$, $\{2, 3\}$, ..., $\{2, 7\}$, ..., $\{6, 7\}$, then three-qubit subsystems $\{1, 2, 3\}$, ..., $\{1, 2, 7\}$, $\{1, 3, 4\}$, ..., $\{1, 3, 7\}$, ..., $\{2, 3, 4\}$, ..., $\{5, 6, 7\}$, and so on until the last six-qubit subsystem $\{2, 3, 4, 5, 6, 7\}$. The point in the very last column is the standard genuine entanglement witness. The value of the two-measurements genuine entanglement witness is 0.52(5), which lies out of the plot. Clear blue points represent the local witnesses obtained only with the stabiliser-based method, and the dark blue one are found with both the stabiliser-based method and the graph-based method. Red points represent two-measurements local witnesses. The horizontal blue and red lines are the positions where the standard local witnesses and the two-measurements local witnesses, respectively, would be if the state was the ideal state affected by a white noise adjusted to reproduce the experimental fidelity of 0.33(1) (missing red lines lie above the figure).

while the entanglement of larger subsystems is harder to detect. In fact, for every subsystem q where entanglement is detected, all subsystems $q' \subset q$ present entanglement as well. For instance, all the two-qubit and three-qubit subsystems with qubits only in the red face have been detected because the entanglement of the subsystem $\{1, 2, 3, 4\}$ was detected.

One can also check that the two-measurements witnesses tend to be more positive than the standard ones as it was predicted by Eq. (5.45), and the difference increases as the number of qubits in the subsystem increases. Therefore, with two-measurements local witnesses one can detect the entanglement of small subsystems with just two measurement settings, but for larger subsystems the standard local witnesses perform

Standard local witnesses detections

Confi. %	>97	73	84	55	87	84	77	81	60	87	73	69	>55	92	75	80	57	57	99
Subsystem q	⊂	1 3 6	1 4 7	1 5 7	2 3 6	2 4 6	2 5 7	2 5 6	2 5 7	3 5 6	3 5 7	4 5 7	⊂	1 2 3 4	1 2 3 7	1 2 6 7	1 4 5 6	2 3 4 5	3 4 6 7
Size of q	2					3										4			

Two-meas. local witnesses detections

Confi. %	>97	77	59	69	77	69	69	>59	55	71	75	56	75	66
Subsystem q	⊂	1 6	2 4	3 4	4 5	4 6	5 7	⊂	1 2 7	2 3 5	2 3 6	2 3 7	2 6 7	3 5 6
Size of q	2			2							3			

Table 5.3: Entanglement detections on the seven-qubit color code with standard local witnesses (top table) and with two-measurements local witnesses (bottom table). Rows contain from top to bottom: the type of witness, the confidence (in %) in the fact that the most negative expectation value of all witnesses for a subsystem q (in the same column of Fig. 5.3) is below 0, the subsystem q, and number $|q|$ of qubits in each q. The columns with the subset symbol (⊂) represent all subsystems q' contained in at least one of the subsystems at the right of the symbol. For instance, the first column of $n = 2$ represents the 21 two-qubit subsystems inside the three and four-qubit subsystems presented in the following columns. To obtain confidence of this column we compare the most negative witnesses for each subsystem q' and then take the confidence on the most positive one among them.

better.

A further interesting observation is that the white noise model in Eq. (5.46) can at best be a rough approximation of the experimental state at hand. In this model, all stabilisers have the same expectation value F, and this value coincides with the fidelity between the ideal state with white noise and the stabiliser state. Thus, to compare the white noise model with the experimental state we set the value of F as the experimental state fidelity of 0.33(1). The resulting expectation value of all local witnesses is positive when evaluated on the white noise model, so no entanglement is detected. However, when evaluated on the experimental state, different stabilisers have varying expectation values. Then, local witnesses constructed predominantly from stabilisers with an expectation value above the fidelity have an expectation value below the prediction of the white noise model. Some of these witnesses have negative expectation values significantly below zero when evaluated on the experimental state (see Fig. 5.3), resulting in the detection of entanglement in the respective qubit subsystems.

The discrepancy of the entanglement detection in qubit subsystems as predicted

from the simple white noise model and as obtained by evaluating the witnesses for experimental data of the seven-qubit color code indicates that the local entanglement properties of the experimental state are not captured by the one-parameter Werner state description. A quantitative prediction of the structure of the experimental state, to predict the observed entanglement structure, would require a modelling of the experimental state preparation process, which takes into account the microscopic details of the experimental gates and other operations [76, 221].

5.6 Graphs from stabiliser states

The surface code, which is a stabiliser code, can be transformed into a LUE graph state using the quantum circuit that realises the code [222]. We propose in Sec. 5.6.1 an analogous geometric approach for the color code using the structure of the quantum circuit that realises the state to obtain a LUE graph state. We also detail a specific way of guaranteeing that any two qubits are connected in the resulting graph state. More generally, in Ref. [174] the authors proved that every stabiliser state is LUE to a graph state. In Sec. 5.6.2 we use the previous work to propose an algebraic technique to realise this transformation. This transformation of a stabiliser state into a graph state is fundamental for the graph-based method described in Sec. 5.4.2. Moreover, in Sec. 5.6.3 we describe a sequence of LC operations that connects any subsystem of two qubits in the graph. Having two qubits connected in the graph guarantees that a local witness can be constructed for such subsystem.

5.6.1 Geometric approach

Here we describe a geometric approach to obtain a graph state that is LUE to a color code using the quantum circuit that realises the code [76]. This approach was performed in Ref. [222] for the surface code. As the authors show, the quantum circuit that creates the surface code qubits differs in the circuit that creates a LUE graph state only in Hadamard gates on certain qubits. In essence, the quantum circuit consists in creating GHZ-type entanglement among the qubits in each face. This is done by dividing the qubits into control and target qubits, initialising control qubits in $|+\rangle$ and target qubits in $|0\rangle$, and finally, applying CNOT gates between each control qubit and the target qubits that belong to the same face (or "product of faces") as the control qubit. The

difficulty consists in selecting the sets of control and target qubits such that only one control qubit belongs to each face (or "product of faces"). Here we show that for the color code, as well as for the surface code, the quantum circuit is equal to the quantum circuit that constructs a graph state, up to a Hadamard gate on each target qubit. Thus, the links in the graph underlying the resulting graph state are in one-to-one correspondence with the CNOT gates. The only difference between our approach here and the one in Ref. [222] is the lattice where color codes and surface codes are defined.

The creation of the color code involves creating GHZ-type entanglement within the qubits in each face of the lattice where the code is defined as illustrated in Fig. 5.4. For a four-qubit face $\boldsymbol{f} = \{c, t_1, t_2, t_3\}$ this type of entanglement is created by initialising the four qubits in the product state $|+_c 0_{t_1} 0_{t_2} 0_{t_3}\rangle$, and then applying CNOT gates $U^{\text{CNOT}}_{(c,t_i)}$ successively between a qubit c that we call *control qubit* and the rest of qubits t_i in the face, which we call *target qubits*. This leads to the four-qubit GHZ state

$$|GHZ_{\boldsymbol{f}}\rangle = U^{\text{CNOT}}_{(c,t_3)} U^{\text{CNOT}}_{(c,t_2)} U^{\text{CNOT}}_{(c,t_1)} |+_c 0_{t_1} 0_{t_2} 0_{t_3}\rangle = \frac{1}{\sqrt{2}}(|0000\rangle + |1111\rangle).$$

The creation of the $|0_L\rangle$ logical state of the seven-qubit color code, which is a stabiliser state, consists in repeating this process for the three faces: (1) choose qubit 1, 5, and 7, as the control qubits of the red, blue and green faces, respectively, and the rest of qubits as target qubits, (2) initialise the seven qubits in the state $|+_1 0_2 0_3 0_4 +_5 0_6 +_7\rangle$, and (3) for each face, apply CNOT gates $U^{\text{CNOT}}_{(c,t)}$ between the control qubit and the target qubits in that face.

The creation of $|0_L\rangle$ is very similar to the creation of a graph state $|\mathscr{G}\rangle$ defined on a bi-colourable underlying graph $G(\boldsymbol{N}, \mathcal{L})$. That is, a graph where nodes can be separated in two disjoint sets: *control nodes* $\boldsymbol{c}$ and *target nodes* $\boldsymbol{t}$ such that all links in $\mathcal{L}$ involve a node in $\boldsymbol{c}$ and a node in $\boldsymbol{t}$. The creation of such graph state involves (1) the selection of the sets $\boldsymbol{c}$ and $\boldsymbol{t}$, (2) the initialisation of all qubits in $|+\rangle$, and (3) the application of controlled-Z (CZ) gates between all pairs of linked qubits $\{c, t\} \in \mathcal{L}$. Note that $U^{\text{CZ}}_{\{c,t\}}$ is the result of applying H_t to the CNOT operator $U^{\text{CZ}}_{\{c,t\}} = H_t U^{\text{CNOT}}_{(c,t)} H_t$.

The similarity between the creation of the $|0_L\rangle$ logical state and the graph state becomes clear when one applies the Hadamard gates

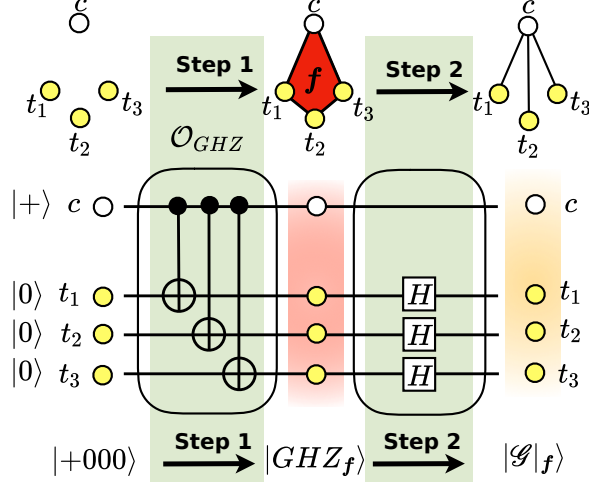$$U_{\text{LUE}} = \bigotimes_{t \in \boldsymbol{t}} H_t \qquad (5.67)$$

Figure 5.4: Quantum circuit creating a local-unitary equivalent (LUE) graph state to a four-qubit GHZ state in a face of the color code. The quantum circuit (denoted by $\mathcal{O}_{GHZ}$) that takes the state $|+000\rangle$ to the four-qubit GHZ state $|GHZ_{\boldsymbol{f}}\rangle = 2^{-1/2}(|0000\rangle + |1111\rangle)$ consists of three CNOT gates between the control qubit c and the three target qubits t_1, t_2 and t_3. The circuit that transform the GHZ state into a four-qubit graph state $|\mathcal{G}|_{\boldsymbol{f}}\rangle = 2^{-1/2}(|0++\rangle + |1---\rangle)$ consists of three Hadamard gates on the target qubits. The repeated creation of GHZ states on each face of the color code creates the logical state $|0_L\rangle$, (a stabiliser state) as illustrated in Fig. 5.5. The subsequent application of a local unitary U_{LUE} consisting of a Hadamard gate on every target qubit produces a graph state $|\mathcal{G}\rangle$ that is LUE to the stabiliser state $|0_L\rangle$.

on all target qubits at the end of the quantum circuit that creates the logical state $|0_L\rangle$. One can pull these Hadamard operators from the end of the circuit to the initial state to check that the quantum circuit obtained performs the creation of the LUE graph state $|\mathcal{G}\rangle = U_{\text{LUE}} |0_L\rangle$. The underlying graph has links between all pairs of qubits $\{c, t\}$ for which a CNOT operator $U_{(c,t)}^{\text{CNOT}}$ has been applied in the construction of the logical state $|0_L\rangle$ of the color code. In terms of the stabiliser operators, the face stabiliser $s_{\boldsymbol{f}}^X = X_c X_{t_1} X_{t_2} X_{t_3}$ is transformed to the graph-state generator $g_c = X_c Z_{t_1} Z_{t_2} Z_{t_3}$ via application of U_{LUE}. The Z-type stabilisers $s^Z \in \mathcal{S}$ in the generator set $\mathcal{S}$ transform into a product of graph state generators.

Note that the color code is determined by the generator set $\mathcal{S}$ defined on the faces of the color code lattice, but also by other generator sets $\mathcal{S}'$ composed by products of stabilisers. In particular, $\mathcal{S}'$ might be formed by products of stabilisers of the same type σ:

$$s_{\tilde{\boldsymbol{f}}}^{\sigma} = \prod_{\boldsymbol{f} \in \mathcal{F}} s_{\boldsymbol{f}}^{\sigma}, \tag{5.68}$$
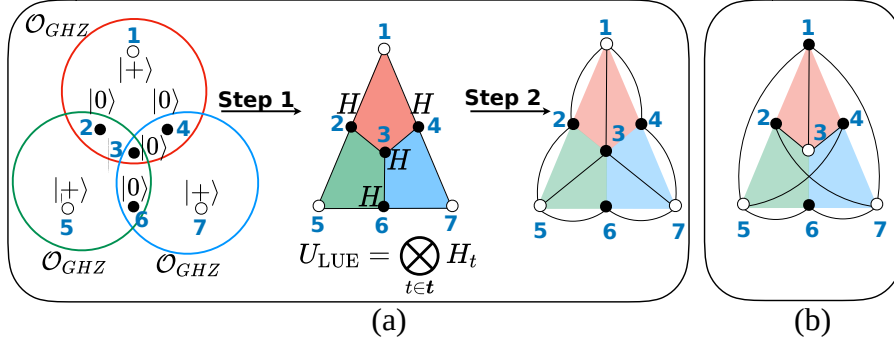
Figure 5.5: Graph states from the seven-qubit color code. (a) Application of the quantum circuit that creates the $|0_L\rangle$ logical state (which is stabiliser state) of the seven-qubit color code, and the local unitary U_{LUE} that transforms $|0_L\rangle$ into a local-unitary equivalent (LUE) graph state $|\mathscr{G}\rangle$. The realisation of $|0_L\rangle$ consist in selecting qubits 1, 5, and 7 as control qubits and the rest as target qubits, initialising qubits in the state $|+_1 0_2 0_3 0_4 +_5 0_6 +_7\rangle$, and generating GHZ-type entanglement with the operation $\mathcal{O}_{GHZ}$ described in Fig. 5.4 on groups of four qubits, given by $\{1, 2, 3, 4\}$, $\{5, 2, 3, 6\}$, and $\{7, 3, 4, 6\}$ corresponding to the three faces of the seven-qubit color code. The application of Hadamard operations on the target qubits $2, 3, 4, 6$ leads to a graph state corresponding to a graph obtained by creating three star graphs on the three groups of qubits, $\{1, 2, 3, 4\}$, $\{5, 2, 3, 6\}$, and $\{7, 3, 4, 6\}$, where qubits 1, 5, and 7 are used as control qubits, respectively. (b) If one assumes the qubits 3, 5, and 7 to be the control qubits, controlling the target qubits in the faces $\boldsymbol{f}_R$, $\boldsymbol{f}_R \oplus \boldsymbol{f}_B$, and $\boldsymbol{f}_R \oplus \boldsymbol{f}_G$, respectively, leads to the graph formed by the star graphs on the groups of qubits $\{1, 2, 3, 4\}$, $\{1, 4, 5, 6\}$, and $\{1, 2, 6, 7\}$.

where $\mathcal{F}$ is some set of faces. The support of these stabilisers is what we call a *product of faces*:

$$\tilde{\boldsymbol{f}} = \bigoplus_{\boldsymbol{f} \in \mathcal{F}} \boldsymbol{f}, \tag{5.69}$$

where $\oplus$ indicates the symmetric difference between sets. For example, the X-type stabilisers in $\mathcal{S}$ might be s_R^X, $s_R^X s_B^X$, and $s_R^X s_G^X$. These stabilisers are defined on the products of faces $\{1, 2, 3, 4\}$, $\{1, 4, 5, 6\}$, and $\{1, 2, 6, 7\}$, respectively. These products of faces can, for instance, be controlled by the qubits 3, 5, and 7, respectively. The quantum circuit arising from this selection also produces the logical state $|0_L\rangle$. However, the local-unitary graph state associated with this quantum circuit, as illustrated in Fig. 5.5(b) is different.

For a general color code, the above recipe to construct the logical state of all logical qubits in $|0_L\rangle$ is analogous. A set of control qubits is chosen such that each product of faces is controlled by a control qubit that belongs to it. The creation of GHZ-type entanglement in each face is guaranteed as long as the sets of control and target qubits
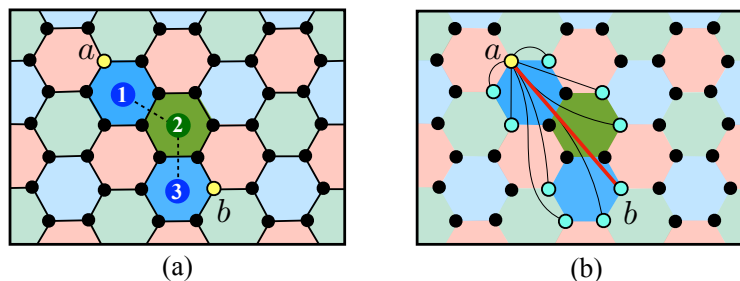
Figure 5.6: Graph-based method: Creation of a link without local complementation (LC). (a) In order to create a link between two given qubits *a* and *b*, a path of adjacent faces, constituted of faces 1, 2, and 3 is chosen, so that the given qubits are contained by the composite larger face constituted of the faces from the path. (b) The next step of constructing the graph corresponding to the local unitary connected graph state would require creating the star graph with the qubits on the larger face, using qubit *a* (yellow circle) as control, and qubit *b* as one of the targets (turquoise circles). This method creates a link (red link) between *a* and *b*.

do not overlap.

One can use products of faces to obtain a local-unitary graph state where a pair of qubits $\{a, b\}$ of interest are linked in the underlying graph. This is important in the graph-based method discussed in Sec. 5.4.2, where one has to ensure the creation of a link between two given qubits to construct a valid local witness. The presence of the link $\{a, b\}$ in the graph can be ensured by choosing a set $\mathcal{F}$ of adjacent faces forming a path between the two qubits such that both qubits are contained in the product of faces $\tilde{\boldsymbol{f}}$ defined from $\mathcal{F}$ as in Eq. (5.69). Then, by choosing one of the qubits as the control qubit that controls $\tilde{\boldsymbol{f}}$ and the other as a target qubit, one ensures that the link $\{a, b\}$ is present in the graph underlying the LUE graph state. See Fig. 5.6 for an illustration.

The success of the geometric method depends explicitly on the correct choice of a set of control qubits, and the determination of the sets of target qubits that are controlled by the control qubits. While this is possible irrespective of the size of the code, the choice of a correct set of control qubits may prove difficult in the case of larger codes. This leads to an algebraic approach for creating the graph, exploiting the binary picture of the code. We introduce the algebraic method for a general stabiliser state. The geometric recipe for the color code proposed above is inherent in the algebraic

approach for determining the adjacency matrix of the graph from the stabiliser structure of the color code, which becomes clear in the subsequent discussion.

5.6.2 Algebraic approach

In this section we describe an algebraic approach to obtain a LUE graph state. It is based on the proof that stabiliser and graph states are LUE given in Ref. [174]. The algebraic approach consists in using the binary representation [177] of the stabiliser state (as described in Sec. 2.3) as an input and then perform algebraic operations on it that lead to the binary representation of a graph state. This approach solves the difficulty of selecting the sets of control and target qubits arising in the geometric approach described in Sec. 5.6.1 by studying the linear dependence of the rows in the binary matrix representing the stabiliser state. The algorithm described here can be found in the Python package **StabGraph** [5] that we developed. The algorithm takes as an input a generator set $\mathcal{S}$ that defines a stabiliser state of interest, and provides the adjacency matrix representing the graph state, the local unitary that transforms the stabiliser state into the graph state, and the required recombination of the stabilisers in the input generator set. We use the notation and definitions presented in Sec. 2.3.

A generator set $\mathcal{S}'$ obtained by an invertible recombination $\mathbb{R}$ of the stabilisers in $\mathcal{S}$ is represented by $\mathbb{S}' = \mathbb{S}\mathbb{R}$. Then, assuming that the rank of $\mathbb{X}$ in Eq. (2.46) is x, one can perform Gaussian elimination on the columns of $\mathbb{S}$ by means of the invertible recombination $\mathbb{R}^{(1)}$ to obtain the representation

$$\mathbb{S}' = \mathbb{S}\mathbb{R}^{(1)} = \left(\begin{array}{c|c} \mathbb{Z}_l & \mathbb{Z}_r \\ \hline \mathbb{X}_l & 0 \end{array} \right). \tag{5.70}$$

Here the "left" blocks $\mathbb{Z}_l$ and $\mathbb{X}_l$ contain x columns, while the "right" block $\mathbb{Z}_r$ contains $n - x$. Note that $\mathbb{X}_l$ is an $n \times x$ matrix of full rank. In the case of a CSS code [13], $\mathbb{Z}_l$ can be considered to be 0, ensuring that the left block of columns in $\mathbb{S}'$ represents only X-type stabilisers, while the right block of columns represents only Z-type stabilisers.

Since the matrix $\mathbb{X}_l$ has rank x, the same number of linearly independent rows can be chosen from it, which forms an $x \times x$ invertible matrix $\mathbb{X}_{l,\boldsymbol{c}}$. These rows correspond to the $|\boldsymbol{c}| = x$ control qubits in the set $\boldsymbol{c}$. The rest of the rows in $\mathbb{X}_l$ stand for the set $\boldsymbol{t}$ of target qubits. Rows are labelled as $q = 1, 2, \cdots, x, x+1, \cdots, n$ from the top, the first

x rows correspond to the control qubits, while the remaining $n - x$ rows correspond to target qubits. Therefore the matrix $\mathbb{S}'$ takes the form

$$\mathbb{S}' = \mathbb{S}\mathbb{R}^{(1)} = \left(\begin{array}{cc} \mathbb{Z}_{l,\boldsymbol{c}} & \mathbb{Z}_{r,\boldsymbol{c}} \\ \mathbb{Z}_{l,\boldsymbol{t}} & \mathbb{Z}_{r,\boldsymbol{t}} \\ \hline \mathbb{X}_{l,\boldsymbol{c}} & 0 \\ \mathbb{X}_{l,\boldsymbol{t}} & 0 \end{array} \right). \tag{5.71}$$

The approach towards extracting the adjacency matrix Γ underlying a local unitary connected graph state from a generator set represented by $\mathbb{S}$ can be summarised via the following equation:

$$\mathbb{U}_{\text{LUE}}\mathbb{S}'\mathbb{R}^{(2)} = \left(\begin{array}{c} \Gamma \\ \hline \mathbb{1}_n \end{array} \right), \tag{5.72}$$

where $\mathbb{R}^{(2)}$ is an invertible binary matrix, and $\mathbb{U}_{\text{LUE}} = \mathbb{U}_S \mathbb{H}_{\boldsymbol{t}}$ is constituted of local unitary operations $\mathbb{U}_S$ representing a phase gate on a subset of the control qubits that is specified later, and $\mathbb{H}_{\boldsymbol{t}}$ representing Hadamard operations on the set of target qubits $\boldsymbol{t}$. In the subsequent discussion, we explicitly calculate the l.h.s. of Eq. (5.72), and demonstrate the extraction of Γ.

The first step is to apply Hadamard operations on all target qubits, which, in the binary picture, implies the exchange of the elements above and below the horizontal line in Eq. (5.70), i.e.,

$$\mathbb{H}_{\boldsymbol{t}}\mathbb{S}' = \left(\begin{array}{cc} \mathbb{Z}_{l,\boldsymbol{c}} & \mathbb{Z}_{r,\boldsymbol{c}} \\ \mathbb{X}_{l,\boldsymbol{t}} & 0 \\ \hline \mathbb{X}_{l,\boldsymbol{c}} & 0 \\ \mathbb{Z}_{l,\boldsymbol{t}} & \mathbb{Z}_{r,\boldsymbol{t}} \end{array} \right). \tag{5.73}$$

The next step is to multiply $\mathbb{H}_{\boldsymbol{t}}\mathbb{S}'$ by $\mathbb{R}^{(2)}$ from the right. In order to produce the $n \times n$ identity matrix $\mathbb{1}_n$ in Eq. (5.72) we choose $\mathbb{R}^{(2)}$ to be the inverse of the lower block of $\mathbb{H}_{\boldsymbol{t}}\mathbb{S}'$. Since the lower block of $\mathbb{H}_{\boldsymbol{t}}\mathbb{S}'$ is in a lower-triangular form $\mathbb{R}^{(2)}$ can be written as

$$\mathbb{R}^{(2)} = \left(\begin{array}{cc} \mathbb{X}_{l,\boldsymbol{c}}^{-1} & 0 \\ \mathbb{Z}_{r,\boldsymbol{t}}^{-1}\mathbb{Z}_{l,\boldsymbol{t}}\mathbb{X}_{l,\boldsymbol{c}}^{-1} & \mathbb{Z}_{r,\boldsymbol{t}}^{-1} \end{array} \right). \tag{5.74}$$

The binary matrix $\mathbb{R}^{(2)}$ is invertible if $\mathbb{Z}_{r,\boldsymbol{t}}$ is invertible (see App. A.11 for a proof of the invertibility of $\mathbb{Z}_{r,\boldsymbol{t}}$). Therefore, the lower block of $\mathbb{H}_{\boldsymbol{t}}\mathbb{S}'$, when multiplied by $\mathbb{R}^{(2)}$

from the right, becomes the identity, while the upper block becomes

$$
\begin{pmatrix}
\mathbb{Z}_{l,c}\mathbb{X}_{l,c}^{-1} + \mathbb{Z}_{r,c}\mathbb{Z}_{r,t}^{-1}\mathbb{Z}_{l,t}\mathbb{X}_{l,c}^{-1} & \mathbb{Z}_{r,c}\mathbb{Z}_{r,t}^{-1} \\
\mathbb{X}_{l,t}\mathbb{X}_{l,c}^{-1} & 0
\end{pmatrix}. \tag{5.75}
$$

We now show that the upper block of $\mathbb{H}_t \mathbb{S}' \mathbb{R}$ is symmetric, for which we exploit the fact that every stabiliser state, say, $\mathbb{S}'$, due to the commutativity between all pairs of stabilisers, has to satisfy $\mathbb{S}'^{T}\mathbb{D}\mathbb{S}' = 0$, where $\mathbb{D}$ is a $2n \times 2n$ binary matrix with zeros in the two $n \times n$ diagonal blocks, and $n \times n$ identity matrices in the off-diagonal blocks [177] as described in Sec. 2.3. This leads to

$$
\mathbb{X}_{l,c}^{T}\mathbb{Z}_{l,c} + \mathbb{X}_{l,t}^{T}\mathbb{Z}_{l,t} = \mathbb{Z}_{l,c}^{T}\mathbb{X}_{l,c} + \mathbb{Z}_{l,t}^{T}\mathbb{X}_{l,t}, \tag{5.76}
$$

$$
\mathbb{X}_{l,c}^{T}\mathbb{Z}_{r,c} = \mathbb{X}_{l,t}^{T}\mathbb{Z}_{r,t}. \tag{5.77}
$$

By multiplying Eq. (5.77) from the left hand side by $\left(\mathbb{X}_{l,c}^{T}\right)^{-1}$, and from the right hand side by $\mathbb{Z}_{r,t}^{-1}$, one obtains

$$
\mathbb{Z}_{r,c}\mathbb{Z}_{r,t}^{-1} = \left[\mathbb{X}_{l,t}\mathbb{X}_{l,c}^{-1}\right]^{T}. \tag{5.78}
$$

Next, by multiplying Eq. (5.76) from the left by $\left(\mathbb{X}_{l,c}^{T}\right)^{-1}$ and from the right by $\mathbb{X}_{l,c}^{-1}$ one obtains that

$$
\left[\mathbb{Z}_{l,c} + \left(\mathbb{X}_{l,c}^{T}\right)^{-1}\mathbb{X}_{l,t}^{T}\mathbb{Z}_{l,t}\right]\mathbb{X}_{l,c}^{-1} = \left(\mathbb{X}_{l,c}^{T}\right)^{-1}\left[\mathbb{Z}_{l,c}^{T} + \mathbb{Z}_{l,t}^{T}\mathbb{X}_{l,t}\mathbb{X}_{l,c}^{-1}\right]. \tag{5.79}
$$

The use of Eq. (5.78) leads to the modified form of the upper block of $\mathbb{H}_t \mathbb{S}' \mathbb{R}^{(2)}$ as

$$
\tilde{\Gamma} = \begin{pmatrix}
\mathbb{C} & \mathbb{B}^{T} \\
\mathbb{B} & 0
\end{pmatrix}, \tag{5.80}
$$

where

$$
\mathbb{B} = \mathbb{X}_{l,t}\mathbb{X}_{l,c}^{-1}, \tag{5.81}
$$

$$
\mathbb{C} = \left[\mathbb{Z}_{l,c} + \left(\mathbb{X}_{l,c}^{T}\right)^{-1}\mathbb{X}_{l,t}^{T}\mathbb{Z}_{l,t}\right]\mathbb{X}_{l,c}^{-1}, \tag{5.82}
$$

with $\mathbb{C}$ being symmetric given Eq. (5.79). For the above matrix $\tilde{\Gamma}$ to be the adjacency matrix Γ of a graph, the diagonal elements of $\mathbb{C}$ must vanish, which is achieved by

multiplying $\mathbb{H}_{\boldsymbol{t}}\mathbb{S}'\mathbb{R}^{(2)}$ by $\mathbb{U}_S$ from the left, given by

$$\mathbb{U}_S = \left(\begin{array}{c|cc} \mathbb{1}_n & \begin{matrix} \mathrm{diag}(\mathbb{C}) & 0 \\ 0 & 0 \end{matrix} \\ \hline 0 & \mathbb{1}_n \end{array} \right), \tag{5.83}$$

where $\mathbb{U}_S$ represents phase gates applied on the qubit subset $\boldsymbol{z}$ formed by those control qubits $q \in \boldsymbol{c}$ for which $\mathbb{C}_{qq} = 1$. This leads to the adjacency matrix Γ of the form

$$\Gamma = \left(\begin{array}{c|c} \mathbb{C} + \mathrm{diag}(\mathbb{C}) & \mathbb{B}^{\mathrm{T}} \\ \hline \mathbb{B} & 0 \end{array} \right). \tag{5.84}$$

Based on the above discussion, one can develop an algorithm for obtaining the adjacency matrix Γ representing the graph underlying a graph state that is LUE to the stabiliser state by utilising the stabiliser structure of the state only. The pseudocode of this algorithm is:

Graph local-unitary equivalent (LUE) to a stabiliser state.
input: generator set $\mathcal{S}$ of a stabiliser state.

1. *obtain the binary representation $\mathbb{S}$ of the generator set $\mathcal{S}$ as in Eq. (2.46).*

2. *obtain $\mathbb{S}'$ via Gauss elimination on the columns of $\mathbb{S}$ and obtain the invertible matrix $\mathbb{R}^{(1)}$ that performs the Gauss elimination.*

3. *reorder the rows to determine $\mathbb{X}_{l,\boldsymbol{c}}$ in the bottom block, the set of control qubits $\boldsymbol{c}$, as well as the set of target qubits $\boldsymbol{t}$.*

4. *apply same reordering in top block to get $\mathbb{S}'$ in Eq. (5.71).*

5. *identify $\mathbb{X}_{l,\boldsymbol{c}}$, $\mathbb{X}_{l,\boldsymbol{t}}$, $\mathbb{Z}_{l,\boldsymbol{c}}$, $\mathbb{Z}_{l,\boldsymbol{t}}$ from $\mathbb{S}'$.*

6. *determine $\mathbb{B}$ and $\mathbb{C}$ as in Eqs. (5.81) and (5.82), and determine $\mathbb{R}^{(2)}$ as in Eq. (5.74).*

7. *calculate Γ as in Eq. (5.84), compute $\mathbb{R} = \mathbb{R}^{(1)}\mathbb{R}^{(2)}$, and obtain the set $\boldsymbol{z}$ of qubits q for which $\mathbb{C}_{qq} = 1$.*

output Γ, $\mathbb{R}$, $\boldsymbol{c}$, $\boldsymbol{t}$, and $\boldsymbol{z}$.

We developed this algorithm in the form of a Python open-source package called **StabGraph** [5], which yields a graph state that is LUE to a stabiliser state of interest. The package provides the adjacency matrix Γ corresponding to the graph underlying the graph state, the recombination $\mathbb{R}$ performed on the stabilisers in the generator set $\mathcal{S}$, the set of control qubits $\boldsymbol{c}$, the set of target qubits $\boldsymbol{t}$ where a Hadamard gate has to be

applied, and the set of qubits $\boldsymbol{z}$ where a phase gate has to be applied. The most time-consuming routine in the package is the Gaussian elimination, which runtime scales as $\mathcal{O}(n^3)$ with the system size n. I developed the Python script that performs the Gauss elimination modulo 2.

Note here that in the case of CSS codes [13], $\mathbb{Z}_{l,\boldsymbol{c}}$ and $\mathbb{Z}_{l,\boldsymbol{t}}$ in $\mathbb{S}'$ can be set to zero by stabiliser recombination, implying $\mathbb{C} = 0$:

$$\Gamma = \left(\begin{array}{c|c} 0 & \mathbb{B}^{\mathrm{T}} \\ \hline \mathbb{B} & 0 \end{array} \right). \tag{5.85}$$

This also implies that links between a pair of control qubits and a pair of target qubits are prohibited, thereby ensuring that the resulting graph is bicolourable. Besides, given that $\mathbb{C} = 0$, the transformation of the stabiliser state to the graph state does not require the application of the local unitary operation $\mathbb{U}_S$.

5.6.3 Local complementation (LC) to put a link between any two qubits

Here we describe the sequence of LC unitary operators that transforms a graph state where two qubits of interest are not linked into a LUE graph state where the two qubits are linked. This is fundamental to construct local witnesses for two qubits using the graph-based method described in Sec. 5.4.2. In essence, this graph state transformation consists in sequentially applying LC operators with respect to the qubits that belong to a path that connects the two qubits of interest. The sufficient condition (though maybe not necessary) on this path is that it does not contain any shorter path. Under this condition we show how the sequence of LC operators creates a link between the two qubits. The algorithm introduced here can be implemented via the Python Package **ALCPack** [6] that we developed.

Let us denote a path with length ℓ between two nodes $\boldsymbol{q} = \{a, b\}$ of interest that conform the subsystem $\boldsymbol{q}$ by an ordered list of nodes $\vec{\boldsymbol{c}} = (q_1, q_2, \ldots, q_{\ell-1})$. We have deliberately excluded qubits a and b from the ordered list $\vec{\boldsymbol{c}}$. Then, $\vec{\boldsymbol{c}}$ is a valid path to put a link between a and b if the sequence of LC operations

$$U_{\mathrm{LC}}^{\vec{\boldsymbol{c}}} = U_{\mathrm{LC}}^{(q_{\ell-1})} \cdots U_{\mathrm{LC}}^{(q_2)} U_{\mathrm{LC}}^{(q_1)}, \tag{5.86}$$
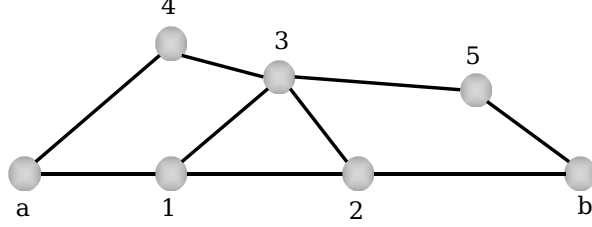
Figure 5.7: Examples of valid and non-valid paths. A simple, connected, and undirected graph of seven nodes. For illustration, we consider the path $\vec{c} = (1, 3, 2)$ between a and b, which is a non-valid path due to the existence of a shorter path $\vec{c'} = (1, 2)$ between a and b that belongs to it: $\vec{c'} \subset \vec{c}$. On the other hand, the shortest path $\vec{c'} = (1, 2)$ and the path $\vec{c''} = (4, 3, 5)$ between a and b are valid paths. That is, if a sequence of local complementation (LC) unitary operations is applied with respect to the qubits in $\vec{c'}$ or in $\vec{c''}$, the resulting local-unitary equivalent (LUE) graph state has a and b connected in the underlying graph. One can check that the path $\vec{c}$ does not produce a graph where a and b are connected.

when applied on the graph state $|\mathscr{G}\rangle$ with underlying graph $G(\boldsymbol{N}, \mathcal{L})$, results in a graph state $|\mathscr{G}^{\vec{c}}\rangle = U_{\text{LC}}^{\vec{c}} |\mathscr{G}\rangle$ defined on an underlying graph $G(\boldsymbol{N}, \mathcal{L}^{\vec{c}})$ where the nodes a, b are connected.

The paths that are valid for this task are those paths $\vec{c}$ (of length ℓ) that do not contain a shorter path, i.e., there is no path $\vec{c'}$ between a and b of length $\ell' < \ell$ such that $\vec{c'} \subsetneq \vec{c}$ (see Fig. 5.7 for examples and counterexamples of valid paths). For ordered lists $\vec{q}, \vec{q'}$ the relation $\vec{q'} \subsetneq \vec{q}$ means that $q \in \vec{q}$ for all $q \in \vec{q'}$ irrespective of the order of the elements, and that $\vec{q'} \neq \vec{q}$. Note that shortest paths do not contain shorter paths, so all shortest paths are valid paths.

In order to prove that this sequence of LC unitary operators connects qubits a and b let us consider a valid path $\vec{c}$, between the nodes a and b in a simple, connected, and undirected graph $G(\boldsymbol{N}, \mathcal{L})$. Given that $\vec{c}$ does not contain shorter paths, no node in $\vec{c}$ except a and q_2 belongs to the neighbourhood $\boldsymbol{n}_{q_1}$. The LC operation w.r.t. the node q_1 creates the link $\{a, q_2\}$ thereby introducing a in the neighbourhood $\boldsymbol{n}_{q_2}$ of q_2, while keeping the neighbourhoods of the rest of nodes $q_3, q_4, \ldots, q_{\ell-1} \in \vec{c}$ and b unchanged. Besides, the LC operation does not affect the links $\{q_i, q_{i+1}\} \in \mathcal{L}$ for $i = 2, 3, \ldots, \ell - 1$. Therefore, in the LC graph $G(\boldsymbol{N}, \mathcal{L}^{(q_1)})$, there exists a simple path between a and b of length $\ell^{(q_1)} = \ell - 1$, given by $\vec{c}^{(q_1)} = (q_2, q_3, \cdots, q_{\ell-1})$. Note that the new path satisfies that $\vec{c}^{(q_1)} \subset \vec{c}$. This, together with the preservation of the neighbourhoods and links mentioned, implies that $\vec{c}^{(q_1)}$ does not contain shorter paths in $G(\boldsymbol{N}, \mathcal{L}^{(q_1)})$. Thus, it

is a valid path to apply the next LC operation. One can continue performing a total of $\ell - 1$ LC operations successively on the nodes $q_2, q_3, \cdots, q_{\ell-1} \in \vec{c}$ in the same order as they are in the sequence $\vec{c}$, where, during each individual LC operation on the node $q_i \in \vec{c}$, the above arguments apply and a link is created between the node a and the node q_{i+1}. The last LC operation on the node $q_{\ell-1}$ creates a link between the nodes a and b. Hence the proof.

As mentioned previously, all shortest paths are valid paths to apply the sequence of LC operations. However, there is no intuitive reason behind using a shortest path to create the link, since the value of the local witness computed via the graph-based method depends explicitly on the structure of links among the nodes in $\boldsymbol{q} \cup \partial \boldsymbol{q}$, and these links change during the LC sequence in an unoptimised way. In a graph with high connectivity, there may exist other paths having length larger than the shortest length which may provide a better local witness compared to the local witness obtained from the shortest path (we elaborate more on this in Sec. 5.7).

A word on the run-time required to apply a sequence of LC operations on a graph with n nodes is in order here. Since the LC operations in the sequence take into account the transformed graphs at each step, it is difficult to determine an exact dependence of the run-time with n. However, one can determine an estimate based on a worst-case scenario. It is easy to see that the maximum size of the neighbourhood $\boldsymbol{n}_q$ of a node q can be $n - 1$, and it can host at most $\binom{n-1}{2}$ links. Therefore, the maximum number of links that can be created or deleted during a LC operation on a single node is $\binom{n-1}{2}$. Since there can be at most $n - 1$ nodes on a path between a and b, the total number of link operations during the LC sequence can be $(n - 1)\binom{n-1}{2} \sim \mathcal{O}(n^3)$, which indicates a polynomial scaling with system size. Our numerical study presented in Sec. 5.7.2 confirms the polynomial scaling.

5.7 Entanglement vs distance

Localisable entanglement has been used in conceptualizing the correlation length in certain quantum many-body systems [182–186], and in protocols including measurement-based quantum computation [50, 174, 177] or entanglement percolation in quantum networks [190]. However, as we explained previously, computing LE is resource-demanding in general. In contrast, local witnesses, which can be evaluated efficiently and provide a

lower bound of LE, are a very handy tool for this task. Here we test the performance of local witnesses and the tools that we developed in Refs. [3, 4, 7] to obtain the behaviour of LE as a function of the qubit distance. The state chosen to perform this test is a large color code (with hundreds of qubits) defined on a hexagonal lattice, and affected by depolarising and phase-flip noise. We consider the qubit distance as the length of the shortest path composed of lattice edges between two qubits.

In Sec. 5.7.1, we use the stabiliser-based method to construct local witnesses for two qubits in the hexagonal color code and study the dependence of their expectation value as a function of the distance between the qubits. This provides an analytical expression of a lower bound of LE with respect to distance. Then, in Sec. 5.7.2 we show how the construction of multiple local witnesses using the graph-based method can also serve to study the behaviour of entanglement with distance. Unlike the stabiliser-based method, the graph-based method does not employ any particular intuition to construct local witnesses. Instead, we construct many local witnesses and then select the ones that provide a tighter lower bound of LE.

5.7.1 Analytical bounds with the stabiliser-based method

Here we use the stabiliser-based method described in Sec. 5.4.1 to construct local witnesses for a color code defined on a hexagonal lattice and obtain their expectation value as a function of the distance between two qubits of interest, which serves us to provide an analytical expression for the lower bound of LE. Due to Prop. 1 and, equivalently, to Theorem 1, the construction of local witnesses for two qubits involves two stabilisers defined on a path of faces that connects the two qubits. If the distance increases the expectation value of a local witness also increases (thus, the lower bound of LE decreases as can be seen from Eq. 5.23) due to the increase in weight of the stabilisers involved in the local witness. We provide the relation between the weights and the distance for two qubits sitting on a particular path of lattice edges in the lattice of the color code. From this relation one finally obtains the analytical expression for the lower bound of LE.

The state where local witness are evaluated is the color code $|\mathscr{S}\rangle$ affected by a noise channel ε as $\rho = \varepsilon(|\mathscr{S}\rangle)$ with noise rate p. We consider the noisy state ρ_{DP} produced by depolarising channel, and the state ρ_{PF} produced by phase flip noise. These noise models are described in Sec. 2.5.

We explicitly compute the expectation value of a local witness operator $W_{\boldsymbol{q}}$ of the form given in Eq. (5.8) constructed for a subsystem $\boldsymbol{q} = \{a, b\}$ composed of two qubits a and b. Due to Theorem 1, such a local witness can be constructed from a subset $\mathcal{W}_{\boldsymbol{q}} = \{s^X, s^Z\}$ of two stabilisers, one X- and one Z-type that anti-commute qubit-wise on the qubits a, b and commute qubit-wise on the rest of qubits. From the form of a local witness for a two-qubit subsystem one can check that the expectation value of such local witness evaluated on the color code depends on the weights $w^X = |\mathbf{supp}(s^X)|$ and $w^Z = |\mathbf{supp}(s^Z)|$ of the stabilisers as:

$$\langle W_{\{a,b\}} \rangle_{\rho_{\mathrm{DP}}} = \frac{1}{4} \left(1 - (1-2p)^{w^X} - (1-2p)^{w^Z} - (1-2p)^{w^X + w^Z - 2} \right) \qquad (5.87)$$

for depolarising noise. For phase-flip noise only the weight of the stabiliser s^X matters:

$$\langle W_{\{a,b\}} \rangle_{\rho_{\mathrm{PF}}} = -\frac{1}{2} (1-2p)^{w^X}. \qquad (5.88)$$

These stabilisers are constituted of a product of stabilisers $s^\sigma_{\boldsymbol{f}}$ defined on a set $\mathcal{F}^\sigma = \{\boldsymbol{f}, \boldsymbol{f}', \dots\}$ of faces that forms a path between the two qubits. In order to minimise the expectation value of the local witnesses, the weights w^X and w^Z of the two stabilisers must be minimised. This motivates the selection of the shortest path $\mathcal{F}^X$ of adjacent faces such that the stabiliser $s^X = \prod_{\boldsymbol{f} \in \mathcal{F}^X} s^X_{\boldsymbol{f}}$ has support on a and b. The stabiliser s^Z must have support on a and b as well, but not on any other qubit where s^X has support. Under these conditions we choose s^Z to be defined on a set of faces $\mathcal{F}^Z$ that are adjacent to the faces in $\mathcal{F}^X$, and that, again, form a path of adjacent faces between the qubits a and b. See Fig. 5.8 for an example of this construction.

This construction can be applied to any pair of qubits $\{a, b\}$ at a distance d. In the color code there is no particular definition of distance between qubits. Thus, we define the distance between two qubits as the length of the shortest path constituted of lattice edges. For the examples in Fig. 5.8, the distance is (a) $d = 4$ and (b) $d = 12$. The aim now is to find an analytical relation between the distance and the weights of the stabilisers. For the hexagonal lattice, the weights w^σ depend on the number of faces $|\mathcal{F}^\sigma|$ in the selected path of faces as

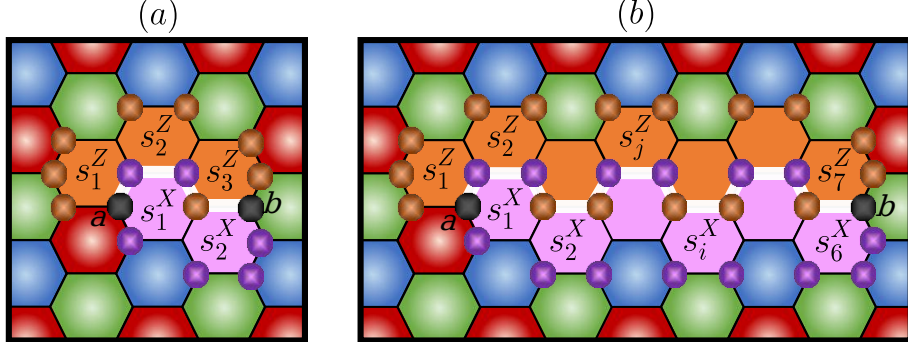$$w^\sigma = 2|\mathcal{F}^\sigma| + 4. \qquad (5.89)$$

Figure 5.8: Construction of local witness operators for a subsystem of two qubits. Local witness operators for two-qubit subsystems $\{a, b\}$ (in black circles) according to Theorem 1 can be constructed from two stabiliser operators $\mathcal{W}_{\{a,b\}} = \{s^X, s^Z\}$. Here, stabilisers s^X and s^Z are obtained by multiplying, respectively, the Z- and X-type stabilisers s_i^X and s_j^Z corresponding to the faces on two adjacent paths $\mathcal{F}^X$ and $\mathcal{F}^Z$ of faces (pink and orange, respectively) connecting the two qubits a and b. The support of s^X is given by the purple and black circles, while the support of s^Z is given by the brown and black dots. The distance, given by the length of the shortest path constituted of lattice edges marked in white, between qubits a and b is (a) $d = 4$, and (b) $d = 12$. Along paths of this form, the weight of stabilisers s^X and s^Z is $w^X = 4 + 2\lfloor d/2 \rfloor$ and $w^Z = 6 + 2\lceil d/2 \rceil$, respectively. The purple and brown qubits stand for the boundary set $\partial \boldsymbol{q}$ (see Sec. 5.3.1). The two different colours, turquoise and yellow on a qubit $q \in \partial \boldsymbol{q}$ represent the single-qubit measurements $m_q = X$ and $m_q = Z$, respectively, in $\mathcal{M}_{\partial \boldsymbol{q}}$. The significance of this particular construction and the path between the two qubits is further discussed in Sec. 5.7.

In general, $|\mathcal{F}^\sigma|$ grows linearly with the distance d, but the exact relation depends on the relative position of the nodes a, b along the path marked in white in Fig. 5.8. For this path, $|\mathcal{F}^X|$ and $|\mathcal{F}^Z|$ depend on whether the distance is even or odd:

$$|\mathcal{F}^X| = \left\lfloor \frac{d}{2} \right\rfloor, \tag{5.90}$$

$$|\mathcal{F}^Z| = 1 + \left\lceil \frac{d}{2} \right\rceil. \tag{5.91}$$

Thus, the weights of the stabilisers depend on the distance as:

$$w^X = 4 + 2 \left\lfloor d/2 \right\rfloor, \tag{5.92}$$

$$w^Z = 6 + 2 \left\lceil d/2 \right\rceil, \tag{5.93}$$

From these results one can obtain the expectation value of the local witness, which from Eq. (5.23) provides an analytical lower bound of LE. For the pure state affected

by depolarising noise:

$$\mathcal{E}_{\boldsymbol{q}}(\rho_{\text{DP}}) \geq \max\left\{\frac{1}{2}\left((1-2p)^{4+2\lfloor d/2 \rfloor} + (1-2p)^{6+2\lceil d/2 \rceil} + (1-2p)^{8+2d} - 1\right), \, 0\right\}$$

$$(5.94)$$

while for the phase flip noise:

$$\mathcal{E}_{\boldsymbol{q}}(\rho_{\text{PF}}) \geq \max\left\{(1-2p)^{6+2\lfloor \frac{d-1}{2} \rfloor}, \, 0\right\}. \tag{5.95}$$

Both results show a slow exponential decay of the bound of LE as the distance increases as illustrated in Fig. 5.9.

5.7.2 Bounds from the graph-based method

Here we employ the graph-based method in Sec. 5.4.2 to obtain multiple local witnesses for multiple qubit pairs $\{a, b\}$ in the color code and plot the lower bound of LE provided by these witnesses against the distance between the two qubit in each pair. We also numerically study the run-time of the **ALCPack** [6] algorithm used to connect qubit pairs in a graph state by means of LC sequences as explained in Sec. 5.6.3. We consider hexagonal color codes with code distance D and a qubit number n (scaling as $n \sim D^2$). The lattice is embedded in a two-dimensional surface delimited by four boundaries as in Fig. 5.10(a), where the code distance D coincides with the length of the boundaries. Qubits are selected from the lattice bulk, which we define as the set of qubits at a distance $D/4$ or greater from a boundary qubit. This selection reduces possible boundary effects due to the different connectivity of qubits in the boundary and close to it. Again, we consider depolarising and phase-flip noise. Recall that here the distance d between two qubits is the number of edges in the shortest path formed by edges in the color code lattice that connects qubits a and b.

Before moving to the analysis of the numerical results, a word on the notion of the existence of local and non-local links in the graph, and the relation with the topological properties of the system is in order here. In the color code lattice, the edges are all local because they only connect qubits belonging to same face. In contrast, the graph underlying a graph state that is LUE to the color code may contain a number of *non-local* links connecting qubits belonging to two different and distant faces (see Fig. 5.10(d) for an example). For this reason we call the LUE graph state of the color
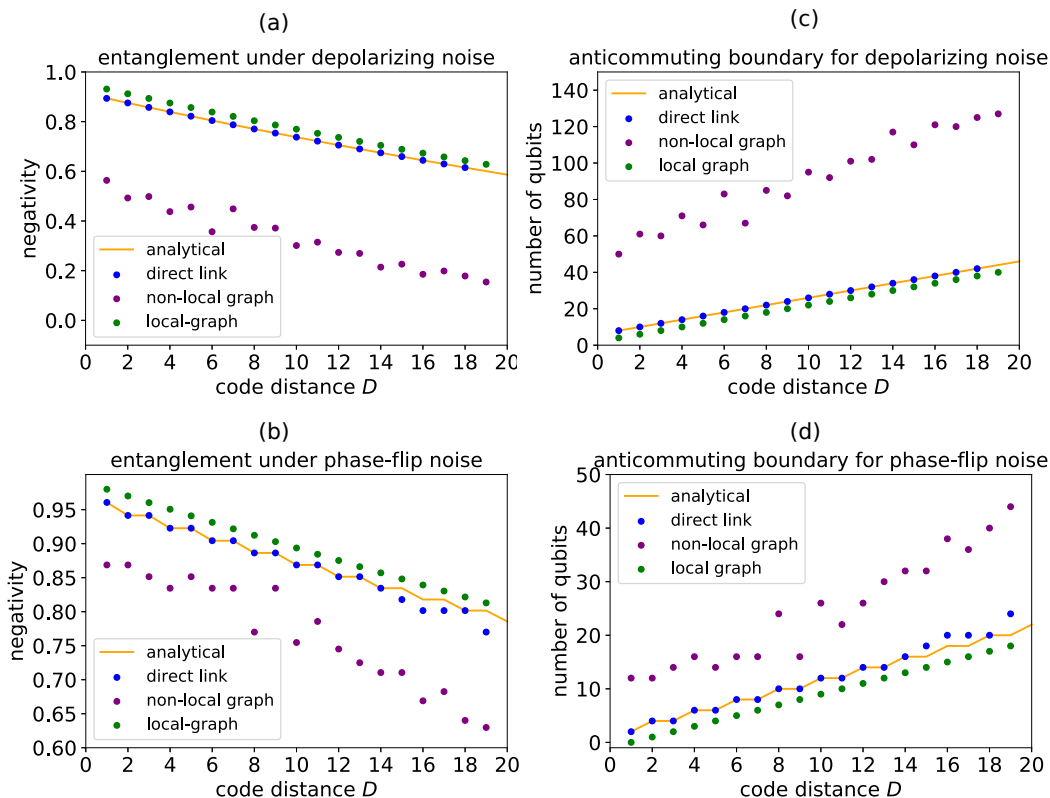
Figure 5.9: Entanglement and boundary size dependence with qubit distance
d**.** From the local witnesses constructed for multiple subsystems of two qubits $\boldsymbol{q} = \{a, b\}$ at various distances d in a color code with code distance $D = 20$, we obtain a lower bound of LE and plot it against d in (a) and (b). Moreover, (c) and (d) show the size of the boundary $\partial \boldsymbol{q}$ as defined in Sec. 5.3.1 that anti-commutes with the noise. We consider two noise channels: the depolarising noise ρ_{DP} in (a) and (c), and the phase-flip noise ρ_{PF} in (b) and (d). The orange lines correspond to the analytical expectation obtained with the stabiliser-based method: (a) corresponds to Eqs. (5.94), (b) corresponds to Eq. (5.95), (c) plots $w^Z + w^X - 4$, and (d) plots $w^X - 2$, where w^X and w^Z are presented in Eqs. (5.92) and (5.93), respectively. Circles correspond to local witnesses constructed with the graph-based method: Purple circles correspond to witnesses constructed using approach (1), consisting in applying LC sequences to connect qubits a and b, while blue circles are obtained with approach (2), consisting in the direct generation of a LUE graph state where qubits a and b are linked. Finally, the green points correspond to the witnesses constructed for multiple qubit pairs in the local graph. As we explain in the main text, the local graph is defined from the edges of the color code lattice, so it only has links between qubits that belong to the same face. Each circle corresponds to the tightest lower bound LE for each value of the distance.

code a *non-local graph*. It has been shown that small and simple codes diminish the

effect of these non-local links, and a critical size is to be achieved to observe the effect
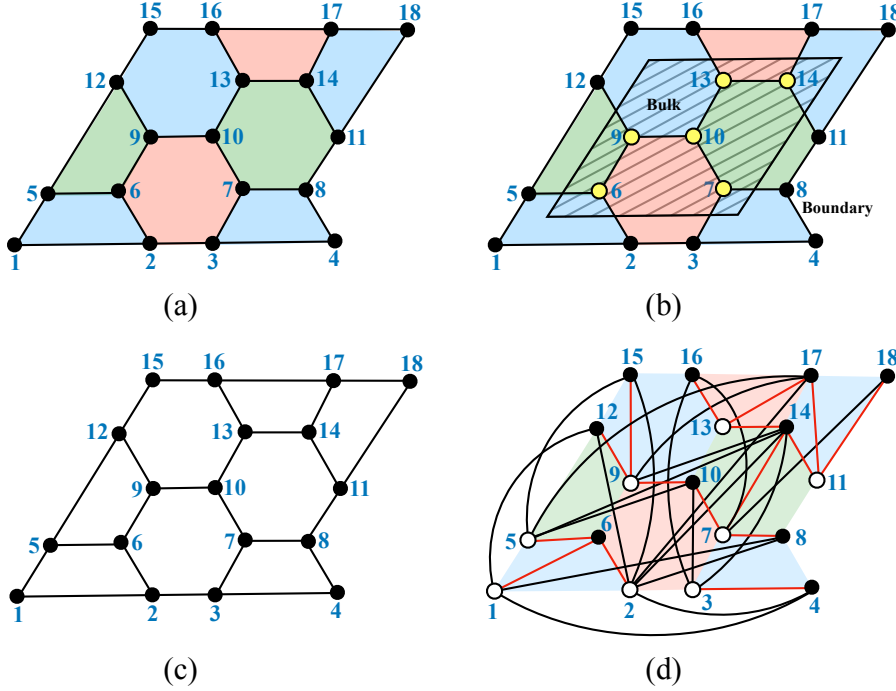
Figure 5.10: Local and non-local graphs. (a) A color code of code distance $D = 4$ defined on a square hexagonal lattice with $n = 18$ qubits, and $f = 8$ faces, containing $k = n - 2f = 2$ logical qubits. (b) The bulk qubits (yellow circles) are obtained by removing $D/4$ qubits in the direction from the boundary to the centre on all sides of the square hexagonal lattice. (c) A local graph, which is composed of local links only, which are those links connecting qubits belonging to the same faces. (d) A non-local graph underlying a graph state that is local-unitary equivalent (LUE) to the square hexagonal color code of distance $D = 4$, where many links (those in black) are non-local links. The chosen control and target qubits in the construction of the LUE graph state (see Sec. 5.6) are represented by white and black circles, respectively.

of the topological properties in terms of the existence of the non-local links in the graph [222]. However, one can also take a different perspective, and ask whether a differentiation can be made in terms of entanglement. The graph-based algorithms are appropriate for such investigations.

We aim to study the effect of non-local links on the entanglement decay. For that purpose, we compare the non-local graph with a fully *local graph* where the links are in one-to-one correspondence with the local edges in the color code lattice (see Fig. 5.10(c) for an example). We compare the entanglement decay in both graphs to see if the presence of non-local links may be related to the existence of long-range entanglement. We choose to construct the local graph from the lattice edges to have a graph state
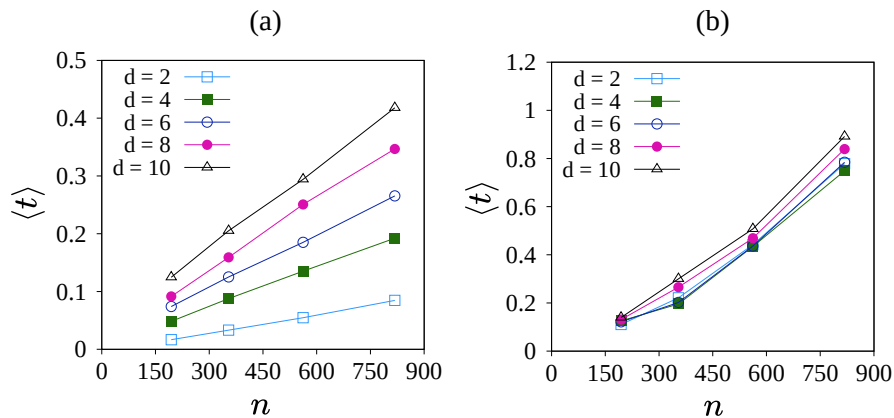
Figure 5.11: Average runtime $\langle t \rangle$ of the ALCPack scripts [6] to link two qubits in a graph state. The average time taken by the algorithm to create a link between two chosen qubits sitting at a specific distance d from each other in the bulk of (a) a local graph mimicking the square hexagonal lattice hosting a color code of code distance D as in Fig. 5.10(c), and (b) a non-local graph as in Fig. 5.10(d) obtained by the method discussed in Sec. 5.6, as a function of the system size n. The value of $\langle t \rangle$ increases with increasing d for a fixed system size. The unit of the $\langle t \rangle$ axis is in seconds, and the n axis is dimensionless. The codes are run on a standard desktop computer.

that is comparable in number and and distribution of qubits with the non-local graph. Nevertheless, note that the local graph is not LUE to the color code, but rather just a tool used for comparison that has no other relevant relation with the color code.

Before showing the results for LE, we test how the **ALCPack** algorithm scales with the system size by looking at the average time $\langle t \rangle$ required to create a link between two qubits a and b of interest. Four code distances $D = 12, 16, 20, 24$ corresponding to system sizes $n = 194, 354, 562, 818$, respectively, are considered. In Fig. 5.11, we present the variation of $\langle t \rangle$ as a function of n for qubit pairs situated at different distances $d = 2, 4, 6, 8, 10$, where the average value $\langle t \rangle$ is determined over a sample of 10^4 paths between a and b for each value of d. From that figure, it is evident that $\langle t \rangle$ increases with n for a fixed d, and increases with d for a fixed n when the graph is local, which is in contrast with the variation of $\langle t \rangle$ with n in the case of a non-local graph obtained from the square hexagonal code. In the latter case, $\langle t \rangle$ increases only negligibly with d for a fixed value of n. This can be understood from the fact that there exists a number of non-local links in the non-local graph, which results in comparable lengths of the paths connecting the chosen qubits in the graph, irrespective of the actual distance d between the qubits. This leads to a similar number of required LC operations, which
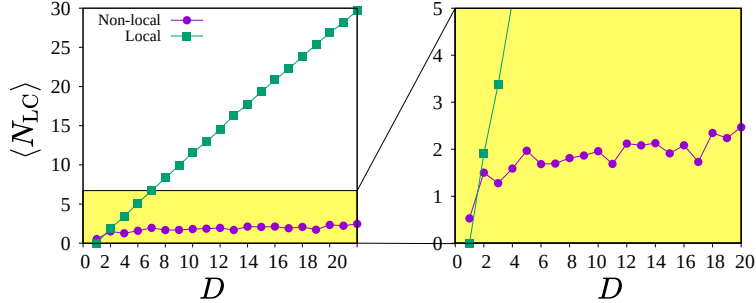
Figure 5.12: Average number of local complementation (LC) operations required to create a link between two given qubits a and b in the bulk, as a function of the distance d between the two qubits in the case of a local (green) and a non-local (purple) graph corresponding to the square hexagonal code with $D = 20$. The average value of N_{LC} is calculated over a sample of 10^4 graphs. The range $0 \leq \langle N_{LC} \rangle \leq 5$ is enlarged.

results in slowly increasing values of $\langle t \rangle$ with d for a fixed n. On the other hand, in the local graph, the typical length of a path connecting a and b increases with increasing distance d between qubits a and b, subsequently increasing the required number of LC operations, and consequently, the average value of $\langle t \rangle$ also increases. Also, the variation of $\langle t \rangle$ with increasing n for a fixed d validates the polynomial scaling of the **ALCPack** algorithm predicted in Sec. 5.6.3.

Given the above discussion, it is interesting to investigate whether the average number of LC operations, $\langle N_{LC} \rangle$, required to create a link between two chosen qubits in the bulk varies with the distance between the qubits when the system-size is fixed. Figure 5.12 depicts the variation of $\langle N_{LC} \rangle$ with d in the case of the local and non-local graphs corresponding to a code distance $D = 20$, where the average value has been taken from a sample size of 10^4 paths for each value of d. In the case of the local graph, $\langle N_{LC} \rangle$ rapidly increases with increasing d, while for the non-local graph, the increasing trend slows down considerably when d increases. These results are in agreement with the variations of $\langle t \rangle$ against d for a fixed value of n.

The lower bound of LE given in Eq. 5.23 is plotted in Figs. 5.9(a) (for depolarising noise) and (c) (for the phase-flip noise) against qubit distance. For this plot multiple local witnesses $W_{\{a,b\}}$ have been constructed with the graph-based method in two different ways: (1) From the color code we obtain one LUE graph state and select multiple qubit pairs, for each pair $\{a,b\}$ we select multiple valid paths between a and b as described in Sec. 5.6.3, apply a LC sequence on each path to link a and b, and finally, for

each LC sequence we construct a local witness. (2) We select multiple qubit pairs in the color code, for each pair we obtain a LUE graph states using the geometric construction provided in Sec. 5.6.1 integrated in the algebraic recipe described in Sec. 5.6.2 ensuring that the pair is connected, and then construct a local witness for that pair in that LUE graph state without performing any LC sequence. We also consider the local graph and apply LC sequences as in (1) to link multiple qubit pairs and construct local witnesses for each LC sequence. Finally, for each qubit distance we consider only the qubit pair and the local witness that provides the tightest lower bound of LE. The noise rate is chosen to be $p = 10^{-2}$.

As mentioned previously, the expectation value of local witnesses depends on the size of the boundary $\partial \boldsymbol{q}$ that anti-commutes qubit-wise with the noise. This size, which we plot in Fig. 5.9, depends on the support of the stabilisers that conform it. For depolarising noise the size is given by $|\mathbf{supp}(s_i) \cup \mathbf{supp}(s_j)| - 2$. Note that these stabilisers, in general, are not entirely composed of the Pauli X, or entirely composed of the Pauli Z. Thus, under phase-flip noise, the size of the anti-commuting boundary is given by $|\mathbf{supp}_{XY}(s_i) \cup \mathbf{supp}_{XY}(s_j)| - 2$. Here $\mathbf{supp}_{XY}(s_i)$ and $\mathbf{supp}_{XY}(s_i)$ are the parts of the supports that anti-commute qubit-wise with the Pauli Z. That is: $\mathbf{supp}_{XY}(s_i) = \{q \in \mathbf{supp}(s_i) : \sigma_{qi} \in \{X, Y\}\}$ for s_i and for s_j. In Figs. 5.9(c) and (d), the minimum values of the anti-commuting boundary size is plotted as a function of the distance d, where the minimisation is achieved over a sample size of 10^4 paths for each value of d. In both cases of the local and the non-local graphs, the size increases monotonically with d.

Figures 5.9(a) and (b) show a slow exponential decay of LE with distance as predicted by the analytical analysis in the previous section. Both local and non-local graphs present this decay but the non-local graph (blue and purple circles, and orange line) presents lower LE than the local graph (green circles) which is in correspondence with the increase of the anti-commuting boundary shown in Figs. 5.9(c) and (d). This might be due to the presence of non-local links in the non-local graphs that increase qubit connectivity with respect to the local graph, increasing the neighbourhood size that determines the witness expectation value. A further observation is that the approach (2) performs better than the approach (1), which is natural given that the approach (2) is partially optimised as described in Sec. 5.6.1. Note also that approach (2) almost coincides with the analytical expressions derived in Sec. 5.7.1, which provide

the tightest bound of LE achieved in this work. The superposition of the analytical analysis and approach (2) is expected since both consider the shortest path of faces between qubits a and b. The partial optimisation performed in (2) might not be easy for general stabiliser states; in contrast with the color code, where stabilisers have a regular and symmetric construction.

The numerical results presented in this section are demonstrations of the applicability of the algorithms developed and discussed in previous sections for determining non-trivial lower bounds of the LE over bulk qubit-pairs in the case of color codes. The lower bounds decrease exponentially with increasing d. However, in order to infer the exact dependence of the bound on d, one has to consider the optimality of the algorithms for obtaining the maximum value of the lower bound. This issue needs to be thoroughly investigated, which is beyond the scope of the present work.

5.8 Summary

In this chapter we have presented our work on entanglement witnesses [3, 4, 7]. In Sec. 5.2 we have presented the concept of entanglement witness as observables that can detect entanglement using incomplete information of the state. The witnesses presented in Sec. 5.2.2 detect genuine entanglement on stabiliser states. In Sec. 5.3 we have introduced the main concept of this chapter: local entanglement witnesses. These observables serve to detect and estimate LE. Localisable entanglement quantifies the maximum amount of entanglement that can be accumulated in a subsystem of qubits. In general, the resources required to evaluate it scale exponentially with the size of the state, but local witnesses for stabiliser states can be evaluated with a number of measurement settings that does not depend on the system size. Genuine and local entanglement witnesses for stabiliser states can be modified to require less measurement settings as we have shown in Sec. 5.2.2 for genuine entanglement witnesses and in Sec. 5.3.4 for local witnesses. However, when modified, witnesses become less tolerant to the noise in the state as we have shown in Sec. 5.3.5.

In Sec. 5.4 we have proposed two methods to construct local witnesses for stabiliser states: the stabiliser-based method in Sec. 5.4.1 provides necessary and sufficient criteria for the construction, while the graph-based method in Sec. 5.4.2 is based in the local-unitary equivalence of stabiliser and graph states, for which the construction of

local witnesses is simple. In Sec. 5.5, we have tested local witnesses and their construction on an experimental realisation of the seven-qubit color code. The evaluation of multiple local witnesses provides meaningful insight into the entanglement structure of this stabiliser state.

The graph-based method to construct local witnesses requires two tools: the transformation of a stabiliser state into a local-unitary graph state, and algorithm to link any two qubits in a graph state by means of LC operations. In Sec. 5.6.1 we have shown a geometric approach to the transformation, while in Sec. 5.6.2 we have introduced an algebraic approach. For the second tool, we have proven in Sec. 5.6.3 that there is a sequence of LC unitary operators that transforms a graph state where two qubits are not linked into a local-unitary graph state where they are linked.

Finally, in Sec. 5.7 we have put in practice all the tools developed to study the decay of entanglement with the distance of two qubits in a large noisy stabiliser state. In Sec. 5.7.1 we have provided analytical expressions for this decay by constructing local witnesses with the stabiliser-based method, while Sec. 5.7.2 has presented the results obtained from the construction of multiple local witnesses using the graph-based method.

The tools developed in this work can be efficiently applied in the existing experimentally realised multi-partite states. The results show that local witnesses perform well in large noisy states as well as in complex states like the seven-qubit color code.

Chapter 6

Conclusions and Outlook

Quantum information science is living a moment where the surprising achievements at the theoretical and experimental level are starting to condensate on small quantum processors and quantum algorithms that can be tested with current technology, showing opportunities for the near and long term. Proofs of that are the number of start-ups devoted to quantum information engineering that are emerging or the vast investments that governments, companies and investors are devoting to quantum technologies [223].

With respect to the near term, well controlled small quantum processors with gate fidelities above 99% and 50-100 qubits known as Noisy Intermediate-Scale Quantum (NISQ) devices [11] are being developed. These devices are encouraging the quantum information community to run small quantum algorithms like the sampling of random quantum circuits [19] in order to test the power of these devices, and possibly show any quantum advantage over classical processing, a desired computation paradigm in the road towards a functional quantum computer. In line of this, recently Google claimed the achievement of quantum supremacy with their superconductor Sycamore processor[20]. Furthermore, some of these NISQ devices are accessible online for the public [224–226], which has generated the appearance of multiple quantum algorithms adapted to the reduced size and imperfections in NISQ devices. In particular, hybrid algorithms, which combine the use of a quantum circuit with variational parameters with a classical computer that optimises the parameters, are becoming ubiquitous [36]. One reason is that the quantum circuits for these algorithms can be designed beforehand attending to the specifications of the NISQ device where they are meant to be run. The other is that the optimisation performed classically is fast thanks to the ex-

tensive development of optimisation algorithms like gradient descent [227], and allows the learning of the experimental imperfections in the device, which helps to minimise the effect of noise.

In regard to the medium term, high gate fidelities are putting fault-tolerant quantum computation at the reach of current technology. Superconducting qubits and trapped ions, as two of the leading experimental platforms, show gates with error rates of the order of 0.1% [29, 30]. This error rate is comparable with the fault-tolerant thresholds of, for instance, surface codes [54–56] and color codes [57–59]. These two topological quantum error correction (QEC) codes have fault-tolerant designs that allow, in principle, to reduce the presence of errors arbitrarily if the experimental error rate is below threshold. However, fault-tolerance requires scaling up the size of the codes by adding more qubits and performing longer computations [43]. Currently, the closest milestone on the route towards fault-tolerant quantum computing is the implementation of small fault-tolerant codes encoding a logical qubit that presents longer lifetimes than a physical qubit. Experimentally, various QEC proofs of principles have been shown, for example, the initialisation of the seven-qubit color code with trapped ions [76], QEC with the repetition code in trapped ions [228] and with superconducting qubits [79], the fault-tolerant error detection in a weight-four stabiliser code checks with trapped ions [77], or the fault-tolerant preparation of a five-qubit code with superconducting qubits [229]. The next step is the implementation of a fault-tolerant QEC code that provides logical qubits with a longer lifetime than single-physical qubits. Theoretical proposals towards the design of small fault-tolerant instance of these codes include the 17 superconducting qubit surface code [81], or flagged-syndrome readout in the seven-qubit color code [82–84, 221].

In the longer term, experimental architectures should allow to increase the size of quantum codes to exploit the fault-tolerant threshold theorem. Superconducting qubits are naturally designed to be scaled up thanks to their modular architecture and two-dimensional arrays, but difficulties like the implementation of non-local gates between distant qubits or the reproducibility of Josephson junctions need to be addressed [30, 80]. Trapped ions in linear Paul traps with fast entangling gates are limited to a a few dozens of qubits [230] due to the increase of the time required to implement entangling gates as the ion number increases. Besides, the distance between ions decreases when more ions are in the trap, making the individual addressing of

ions harder and, consequently, producing cross-talk errors [23]. New traps that can split ions into smaller chains to reduce these undesired effects are being designed and tested [29]. They are also able to shuttle ions towards interaction areas where only the ions of interest interact. On the theoretical side, efforts focus on the reduction of resources required for fault-tolerant quantum computation by designing QEC codes with a universal set of transversal gates [85, 86], or magic state distillation [200] protocols like lattice surgery [201] or code switching [202].

The research presented in this thesis contributes towards the existing challenges in quantum information science. The color code, as a leading candidate for fault-tolerant quantum computation must be able to correct not only for the traditionally considered computational errors, but also for qubit loss, an error source usually overlooked in the literature. A qubit is lost when the information encoded in it can no longer be accessed due to noise processes like leakage out the qubit computational space, or the actual loss of a particle like a photon. This process damages the encoded information when it is not corrected. Thus, in Chap. 4 we have proposed a fully local and sequential protocol to correct the presence of qubit loss in the color code that does not require a decoder. We have shown that under our protocol the color code can tolerate the average loss of $46(1)\%$ of qubits. This is directly relevant for the performance of color codes in practice since the protocol does not require any decoder algorithm that is computationally hard to run and shows the high tolerance to qubit loss. Interestingly, in this chapter we have shown that the tolerance is related to a novel bond-percolation threshold in coupled lattices. This new connection between quantum information and classical statistical physics, more concretely between QEC and percolation theory, can motivate the study of further fruitful cross-connections between these fields.

Moreover, the rapid development of well-controlled quantum processors requires new tools to study their quantum properties. Entanglement, for example, is believed to be essential for these processors to show any quantum advantage over classical processors. An argument supporting this is that unentangled quantum systems can be efficiently simulated by classical means. Furthermore, entanglement is used as a resource in most quantum algorithms for quantum computation, in protocols for quantum communications and quantum sensing, as well as in measurement-based quantum computation

or in QEC codes, where the logical information is encoded in large multi-partite entangled states. Therefore, quantum processors must show entanglement. The use of tomographic techniques becomes impossible for current NISQ devices with 50-100 qubits, so more efficient methods need to be used. In Chap. 5 we ave proposed and studied local entanglement witnesses for stabiliser states as platform-agnostic entanglement detectors in experiments. The number of measurements required to evaluate them does not depend on the system size, so they can be efficiently evaluated in arbitrarily large quantum states. As we have shown, local witnesses provide a lower bound of localisable entanglement (LE) that contrast with the computationally hard to calculate LE in practice. Localisable entanglement, which is the entanglement present among qubit subsystems of the entire state, provides useful information about the entanglement structure of quantum states: which and how intensely qubits are entangled, how does the interaction of a qubit subsystem with other qubits affect the entanglement inside the subsystem, which entanglement length do topological QEC codes or other quantum many-body systems [182, 183, 185, 186]. Therefore, local witnesses, which can be implemented with current technology, can be used to determine the entanglement structure of NISQ devices to reveal local experimental imperfections or benchmark their "quantum resources".

Regarding future improvements of the results presented in this thesis, some of our techniques can be extended to account for more general situations or studied under more realistic circumstances. With respect to our protocol to correct for qubit losses, more realistic noise models combine the presence of qubit loss and computational errors. Our protocol removes qubits from the lattice, so the code distance reduces in general, making the code more vulnerable against computational errors as qubits are lost. One question in this direction is how does the code distance decrease with the number of lost qubits and numerically study the performance of the code under both noise sources at different noise rates. Besides, a decoder that accounts for both error sources should be able to distinguish stabiliser excitations coming from computational errors form the correlated excitations arising in our protocol to correct qubit losses. Moreover, in this thesis we considered the code-capacity model where losses can be perfectly detected and happen only on the data qubits. A more phenomenological noise model would include the possibility that the detection of lost qubits is not perfect, and even more realistically, we could consider a circuit-based model where losses can happen also on

the ancillary qubits employed for the stabiliser measurement. Furthermore, we can consider the use quantum circuits for qubit loss detection and for the implementation of our protocol that are fault-tolerant against computational errors.

For local witnesses, one could think about extending the design to non-stabiliser states in order to increase their accuracy to estimate LE in these states. This is important given that non-stabiliser states are necessarily realised in quantum processors that cannot be efficiently simulated by classical means due to the Gottesman-Knill theorem [171]. Besides, the local witnesses constructed detect genuine entanglement in qubit subsets, local witnesses that detect other types of entanglement different from genuine entanglement [113], like bipartite entanglement, on qubit subsystems, could, potentially, reveal additional aspects of the entanglement properties of experimental states. In the context of quantum communication, but also in condensed matter systems, local witnesses could be used to investigate the entanglement length, a key property of quantum networks [231] and spin systems [232]. In quantum cryptography protocols [89, 90], where entanglement is used a resource, estimating the entanglement structure in a measurement-device-independent (MDI) way is critical to guarantee the security of the quantum channel [132–135], so MDI versions of local witness might also be useful in quantum networks.

Appendix A

Appendices

A.1 Proof of Eq. (4.24)

In this appendix we prove that the energy E_i of a loss instance i can be expressed in terms of the average number of edges R_j as expressed in Eq. (4.24).

Let us rewrite Eqs. (4.23) and (4.24) by using a delta function that equals 1 if $j \subset \ell$ and zero otherwise:

$$R_j \qquad = \sum_{k \in \mathcal{I}} E_k \delta_{k \subset j}, \tag{A.1}$$

$$E_i \quad = (-1)^{|i|} \sum_{j \in \mathcal{I}} (-1)^{|j|} R_j \delta_{j \subset i}. \tag{A.2}$$

Here $\mathcal{I}$ is the set of all loss instances. Substituting the first equation into the second one yields:

$$E_i = (-1)^{|i|} \sum_{k \in \mathcal{I}} E_k \sum_{j \in \mathcal{I}} (-1)^{|j|} \delta_{k \subset j} \delta_{j \subset i}. \tag{A.3}$$

Instead of summing over j we sum over the set difference $t = j \setminus k$, which contains all the subsets of $i \setminus k$. Then, one has that:

$$\sum_{j \in \mathcal{I}} (-1)^{|j|} \delta_{k \subset j} \delta_{j \subset i} = \delta_{k \subset i} \sum_{t \subset i \setminus k} (-1)^{|t| + |k|}, \tag{A.4}$$

where $\delta_{k \subset i}$ indicates that all the terms vanish if $k \not\subset i$. The sum over t equals zero unless $|t| = 0$, thus the number of elements of the sets k and i needs to be equal, i.e.

149

$|\boldsymbol{k}| = |\boldsymbol{i}|$:

$$\sum_{\boldsymbol{t} \subset \boldsymbol{i} \backslash \boldsymbol{k}} (-1)^{|\boldsymbol{t}|+|\boldsymbol{k}|} = (-1)^{|\boldsymbol{k}|} \delta_{|\boldsymbol{k}|=|\boldsymbol{i}|}. \tag{A.5}$$

Then, the sum over $\boldsymbol{j}$ is reduced to a sign and two deltas:

$$E_{\boldsymbol{i}} = (-1)^{|\boldsymbol{i}|} \sum_{\boldsymbol{k} \in \mathcal{I}} E_{\boldsymbol{k}} (-1)^{|\boldsymbol{k}|} \delta_{\boldsymbol{k} \subset \boldsymbol{i}} \delta_{|\boldsymbol{k}|=|\boldsymbol{i}|}. \tag{A.6}$$

The condition imposed by the two deltas is satisfied if the sets $\boldsymbol{k}$ and $\boldsymbol{i}$ are equal so the only term surviving in the sum over $\boldsymbol{k}$ is $\boldsymbol{k} = \boldsymbol{i}$. Hence the proof of Eq. (4.24).

A.2 Proof of Eq. (4.26)

In this appendix we prove that the ℓ-th coefficient α_ℓ in the expansion of the average fraction of edges erased $r(p)$ in powers of p is given by the sum of energies $E_{\boldsymbol{i}}$ of loss instances $\boldsymbol{i}$ that contain ℓ losses.

By substituting the number of edges erased $R_{\boldsymbol{i}}$ in Eq. (4.25) by its expression in terms of energies in Eq. (4.23) one gets that the average fraction of edges erased is:

$$r(p) = e^{-1} \sum_{\boldsymbol{i} \in \mathcal{I}} p^{|\boldsymbol{i}|} (1-p)^{n-|\boldsymbol{i}|} \sum_{\boldsymbol{j} \subset \boldsymbol{i}} E_{\boldsymbol{j}}. \tag{A.7}$$

The condition in the second sum can be dropped by introducing a delta function $\delta_{\boldsymbol{j} \subset \boldsymbol{i}}$ that equals 1 if $\boldsymbol{j} \subset \boldsymbol{i}$ and 0 otherwise:

$$r(p) = e^{-1} \sum_{\boldsymbol{j} \in \mathcal{I}} E_{\boldsymbol{j}} \sum_{\boldsymbol{i} \in \mathcal{I}} p^{|\boldsymbol{i}|} (1-p)^{n-|\boldsymbol{i}|} \delta_{\boldsymbol{j} \subset \boldsymbol{i}}. \tag{A.8}$$

For a fixed $\boldsymbol{j}$ the instances $\boldsymbol{i}$ for which the delta does not vanish are of the form $\boldsymbol{i} = \boldsymbol{j} \cup \boldsymbol{k}$ where $\boldsymbol{k}$ is a subset of the rest of qubits $\boldsymbol{k} \subset \boldsymbol{N} \backslash \boldsymbol{j}$. Here $\boldsymbol{N}$ is the set of all qubits. Then $|\boldsymbol{i}| = |\boldsymbol{j}| + |\boldsymbol{k}|$ and the sum on $\boldsymbol{i}$ can be substituted by a sum over $\boldsymbol{k}$:

$$r(p) = e^{-1} \sum_{\boldsymbol{j} \in \mathcal{I}} E_{\boldsymbol{j}} p^{|\boldsymbol{j}|} \sum_{\boldsymbol{k} \in \boldsymbol{N} \backslash \boldsymbol{j}} p^{|\boldsymbol{k}|} (1-p)^{(n-|\boldsymbol{j}|)-|\boldsymbol{k}|}. \tag{A.9}$$

The second sum equals one because it is a sum of the probabilities of every loss instance constrained to the qubits in $\boldsymbol{N} \backslash \boldsymbol{j}$. This finalises the proof of Eq. (4.26).

A.3 Separable instances have zero energy

In this appendix we prove that the energy for a separable instance $\boldsymbol{i}$ the energy $E_{\boldsymbol{i}}$ vanishes. If two disjoint parts $\boldsymbol{i}^{(A)}$, $\boldsymbol{i}^{(B)}$ of an instance $\boldsymbol{i} = \boldsymbol{i}^{(A)} \cup \boldsymbol{i}^{(B)}$ are far enough apart from each other, the number of edges erased is the sum of the edges erased by the two parts: $R_{\boldsymbol{i}} = R_{\boldsymbol{i}^{(A)}} + R_{\boldsymbol{i}^{(B)}}$. This is defined as a separable instance.

In this situation, every loss in $\boldsymbol{i}^{(A)}$ is far apart from every loss in $\boldsymbol{i}^{(B)}$, so every subset $\boldsymbol{j} \subset \boldsymbol{i}$ that contains some losses from $\boldsymbol{i}^{(A)}$ and some losses from $\boldsymbol{i}^{(B)}$:

$$\boldsymbol{j} \cap \boldsymbol{i}^{(A)} \neq \emptyset \quad , \quad \boldsymbol{j} \cap \boldsymbol{i}^{(B)} \neq \emptyset \tag{A.10}$$

is also a separable instance:

$$R_{\boldsymbol{j}} = R_{\boldsymbol{j} \cap \boldsymbol{i}^{(A)}} + R_{\boldsymbol{j} \cap \boldsymbol{i}^{(B)}}. \tag{A.11}$$

In particular, for the subsets $\{j_1, j_2\}$ with just two losses, $R_{\{j_1,j_2\}} = R_{\{j_1\}} + R_{\{j_2\}}$. So from Eq. (4.24) one gets that the energy of these subsets vanishes $E_{\{j_1,j_2\}} = 0$.

For separable subsets $\{j_1, j_2, j_3\}$ containing three losses $R_{\{j_1,j_2,j_3\}} = R_{\{j_1\}} + R_{\{j_2,j_3\}}$. These subsets contain two subsets, $\{j_1, j_2\}$, $\{j_1, j_3\}$ whose energy vanishes. Then, using Eq. (4.24) and cancelling the vanishing energies at both two sides one has that the left and the right side of the previous equation are

$$R_{\{j_1,j_2,j_3\}} = E_{\{j_1,j_2,j_3\}} + E_{\{j_2,j_3\}} + E_{\{j_1\}} + E_{\{j_2\}} + E_{\{j_3\}}, \tag{A.12}$$

$$R_{\{j_1\}} + R_{\{j_2,j_3\}} = E_{\{j_1\}} + E_{\{j_2,j_3\}} + E_{\{j_2\}} + E_{\{j_3\}}, \tag{A.13}$$

respectively. This results in a vanishing energy $E_{\{j_1,j_2,j_3\}} = 0$.

Applying this derivation iteratively from subsets $\boldsymbol{j} \subset \boldsymbol{i}$ of a separable instance $\boldsymbol{i}$ one obtains that all energies $E_{\boldsymbol{j}} = 0$ vanish. In particular, for the last iteration, when $\boldsymbol{j} = \boldsymbol{i}$, the energy of $\boldsymbol{i}$ vanishes $E_{\boldsymbol{i}} = 0$, proving the initial statement.

A.4 Solution of the recursive sequence in Eq. (4.37)

In this appendix we solve by induction the recursive sequence of Eq. (4.37) with the mean-field factor of Eq. (4.41):

$$\varrho_{\ell+1} = \varrho_\ell + \frac{n - 2\varrho_\ell}{n - \ell} R_1, \tag{A.14}$$

which can be rewritten as:

$$\eta_{\ell+1} = \eta_\ell \frac{n - \ell - 2R_1}{n - \ell}, \tag{A.15}$$

where $\eta_\ell = n - 2\varrho_\ell$.

For $\ell = 0$, $\varrho_0 = \varepsilon_0 = 0$, and $\eta_0 = n$ trivially. Then, the first elements of the sequence are:

$$\eta_0 \quad = n, \tag{A.16}$$

$$\eta_1 \quad = n \frac{n - 2R_1}{n}, \tag{A.17}$$

$$\eta_2 \quad = n \frac{(n - 2R_1)(n - 2R_1 - 1)}{n(n - 1)}, \tag{A.18}$$

$$\eta_3 \quad = n \frac{(n - 2R_1)(n - 2R_1 - 1)(n - 2R_1 - 2)}{n(n - 1)(n - 2)}. \tag{A.19}$$

By induction, one obtains that for the ℓ-th element:

$$\eta_\ell = n \frac{\Gamma(1 + n - 2R_1)}{\Gamma(1 + n - 2R_1 - \ell)} \frac{\Gamma(1 + n - \ell)}{\Gamma(1 + n)}, \tag{A.20}$$

where $\Gamma(1 + x) = x(x - 1)(x - 2) \cdots (x - \lfloor x \rfloor)$ is the Gamma function generalised to non-integer values x ($\lfloor x \rfloor$ being the closest integer to x that is smaller than x). Using the relation with the binomial coefficient $\Gamma(1 + x)/\Gamma(1 + y) = \binom{x}{y}\Gamma(1 + x - y)$ one can express η_ℓ as:

$$\eta_\ell = \binom{n}{\ell}^{-1} \binom{n - 2R_1}{\ell}. \tag{A.21}$$

Finally, one obtains the result presented in Eq. (4.42):

$$\varrho_\ell = \frac{n}{2} \left[1 - \binom{n}{\ell}^{-1} \binom{n - 2R1}{\ell} \right]. \tag{A.22}$$

A.5 Solution of the sum in Eq. (4.38)

In this appendix we obtain the mean-field approximation of the average number of edges erased $r(p)$ by inserting the expression for ϱ_ℓ of Eq. (4.42) in Eq. (4.38):

$$r(p) \simeq \frac{2}{n} \sum_{\ell=0}^{n} \binom{n}{\ell} p^\ell (1-p)^{n-\ell} \frac{n}{2} \left[1 - \binom{n}{\ell}^{-1} \binom{n-2R1}{\ell} \right]. \tag{A.23}$$

Using that the sum of probabilities $\sum_{\ell=0}^{n} \binom{n}{\ell} p^\ell (1-p)^{n-\ell}$ equals one, one can simplify the above expression to:

$$r(p) \simeq 1 - \sum_{\ell=0}^{n} p^\ell (1-p)^{n-\ell} \binom{n-2R1}{\ell}. \tag{A.24}$$

By extracting $(1-p)^{2R_1}$ from $(1-p)^{n-\ell}$ one obtains that:

$$r(p) \simeq 1 - (1-p)^{2R_1} \sum_{\ell=0}^{n} p^\ell (1-p)^{n-2R_1-\ell} \binom{n-2R1}{\ell}. \tag{A.25}$$

From the generalised binomial theorem, one obtains that the sum reduces to $[p + (1-p)]^{n-2R_1} = 1$, obtaining the final result presented in Eq. (4.16)

$$r(p) \simeq 1 - (1-p)^{2R_1}. \tag{A.26}$$

A.6 Maximal Schmidt coefficient for stabiliser states

In this appendix we prove that the maximal Schmidt coefficient of non-separable stabiliser states is $\beta = 1/\sqrt{2}$. We prove it for graph states, given that every stabiliser state is local-unitary equivalent (LUE) to a graph state and local unitary operators preserve the Schmidt coefficients.

Given a bipartition $A|B$ of the qubits (assume $|A| \leq |B|$) in a state $|\psi\rangle$, there is an orthonormal set of states $\{|\psi_1^A\rangle, \ldots, |\psi_r^A\rangle\}$ with support on the subsystem A and an orthonormal set of states $\{|\psi_1^B\rangle, \ldots, |\psi_r^B\rangle\}$ with support on B such that the Schmidt decomposition of $|\psi\rangle$ can be written as:

$$|\psi\rangle = \sum_{x=1}^{r} \beta_x |\psi_x^A\rangle |\psi_x^B\rangle, \tag{A.27}$$

A. APPENDICES

where r is the Schmidt rank, x is an index running from 1 to r, and the coefficients β_x are the Schmidt coefficients corresponding to the bipartition $A|B$ of $|\psi\rangle$.

Here, we obtain the Schmidt coefficients of a graph state $|\mathscr{G}\rangle$ defined on an underlying graph with adjacency matrix Γ. For that, we need to write a graph state $|\mathscr{G}\rangle$ of n qubits in the computational basis $|\varkappa\rangle$, where $\varkappa$ is a binary string of length n. Graph states can be constructed by applying a control-phase (CZ) gate $U_{\{i,j\}}^{\mathrm{CZ}}$ for every pair of linked qubits i, j (for which $\Gamma_{ij} = 1$) on the product state $|+\rangle^{\otimes n}$. On the computational basis the CZ gates acts as:

$$U_{\{i,j\}}^{\mathrm{CZ}} |\varkappa\rangle = (-1)^{\varkappa_i \varkappa_j} |\varkappa\rangle, \tag{A.28}$$

where $\varkappa_q$ is the q-th element of $\varkappa$, corresponding to the qubit q. Then, when all CZ gates for which $\Gamma_{ij} = 1$ are applied to $|+\rangle^{\otimes n}$ one obtains the expression of the graph state in the computational basis:

$$|\mathscr{G}\rangle = \frac{1}{2^{n/2}} \sum_{\varkappa} (-1)^{\varkappa^{\mathrm{T}} \Gamma \varkappa} |\varkappa\rangle. \tag{A.29}$$

Here we used the upper triangular part Γ of Γ, i.e., $\Gamma_{ij} = \Gamma_{ij}$ for all elements for which $i \leq j$ and 0 for the rest. All operations between binary matrices and vectors in this appendix are performed modulo 2.

For the bipartition $A|B$ we assume without loss of generality that $i \leq j$ for every $i \in A$ and $j \in B$. Then, Γ can be written in blocks:

$$\Gamma = \begin{pmatrix} \Gamma_A & \Gamma_{AB} \\ 0 & \Gamma_B \end{pmatrix}, \tag{A.30}$$

where Γ_A and Γ_B have also an upper triangular form, Γ_A represents the links between qubits in A, Γ_B represents the links between qubits in B, and Γ_{AB} represents the links between qubits in A and qubits in B. Analogously, the binary string $\varkappa$ can be split in two parts $\varkappa_A$ and $\varkappa_B$ for the qubits in the parts A and B, respectively. Then, the graph state can be represented with respect to the bipartition $A|B$ as:

$$|\mathscr{G}\rangle = \frac{1}{2^{|A|/2}} \sum_{\varkappa_A} (-1)^{\varkappa_A^{\mathrm{T}} \Gamma_A \varkappa_A} |\varkappa_A\rangle |\psi_{\varkappa_A}^B\rangle, \tag{A.31}$$

where the states $|\varkappa_A\rangle$ with support on A are orthonormal, and the states $|\psi_{\varkappa_A}^B\rangle$ with

support on B are normalised:

$$|\psi_{\varkappa_A}^B\rangle = \frac{1}{2^{|B|/2}} \sum_{\varkappa_B} (-1)^{\varkappa_A^{\mathrm{T}} \Gamma_{AB} \varkappa_B} (-1)^{\varkappa_B^{\mathrm{T}} \Gamma_B \varkappa_B} |\varkappa_B\rangle. \tag{A.32}$$

However, not all the $2^{|A|}$ states $|\psi_{\varkappa_A}^B\rangle$ are orthogonal to the rest.

Here we show that one can select $\mathrm{rank}(\Gamma_{AB}^{\mathrm{T}})$ many of these states such that they are orthogonal to each other. Thus, the Schmidt rank is the rank modulo 2 of Γ_{AB}: $r = 2^{\mathrm{rank}(\Gamma_{AB}^{\mathrm{T}})}$. For that we compute the dot product

$$\langle \psi_{\varkappa_A}^B | \psi_{\mathsf{y}_A}^B \rangle = \frac{1}{2^{|B|}} \sum_{\varkappa_B} (-1)^{(\varkappa_A + \mathsf{y}_A)^{\mathrm{T}} \Gamma_{AB} \varkappa_B} = \begin{cases} 1 & \text{if } \varkappa_A + \mathsf{y}_A \in \mathrm{kernel}(\Gamma_{AB}^{\mathrm{T}}) \\ 0 & \text{otherwise} \end{cases}, \tag{A.33}$$

where $\mathrm{kernel}(\Gamma_{AB}^{\mathrm{T}})$ contains all binary vectors z_A of length $|A|$ such that $\Gamma_{AB}^{\mathrm{T}} \mathsf{z}_A = 0$. The number of elements in the kernel is $2^{|A| - \mathrm{rank}(\Gamma_{AB}^{\mathrm{T}})}$.

Thus, the set of all binary vectors of length $|A|$ can be split into $2^{\mathrm{rank}(\Gamma_{AB}^{\mathrm{T}})}$ disjoint subsets $\mathcal{V}_x$ (with $x = 1, \ldots, 2^{\mathrm{rank}(\Gamma_{AB}^{\mathrm{T}})}$) for which the product $\varkappa_A^{\mathrm{T}} \Gamma_{AB}$ is equal:

$$\mathcal{V}_x = \left\{ \varkappa_A : \quad \varkappa_A^{\mathrm{T}} \Gamma_{AB} = \mathsf{v}_x \right\}, \tag{A.34}$$

where v_x is a binary vector of length $|B|$, and all v_x are different. Each subset contains $2^{|A| - \mathrm{rank}(\Gamma_{AB}^{\mathrm{T}})}$. Then, any two states are orthogonal only if their corresponding binary vector corresponds to different subsets;

$$\langle \psi_{\varkappa_A}^B | \psi_{\mathsf{y}_A}^B \rangle = \begin{cases} 1 & \text{if } \varkappa_A^B, \mathsf{y}_A^B \in \mathcal{V}_x & \text{for any } x \\ 0 & \text{if } \varkappa_A^B \in \mathcal{V}_x, \ \mathsf{y}_A^B \in \mathcal{V}_{x'} & \text{for any } x \neq x' \end{cases}. \tag{A.35}$$

Let us take a representative state $|\psi_x^B\rangle = |\psi_{\varkappa_A}^B\rangle$ with $\varkappa_A \in \mathcal{V}_x$ for every subset $\mathcal{V}_x$.

In view of this, we can group all $\varkappa_A \in \mathcal{V}_x$ in Eq. (A.31):

$$|\mathscr{G}\rangle = \frac{1}{2^{|A|/2}} \sum_{x=1}^{2^{\mathrm{rank}(\Gamma_{AB})}} \left(\sum_{\varkappa_A \in \mathcal{V}_x} (-1)^{\varkappa_A^{\mathrm{T}} \Gamma_A \varkappa_A} |\varkappa_A\rangle \right) |\psi_x^B\rangle, \tag{A.36}$$

which can be written in the form of a Schmidt decomposition

$$|\mathscr{G}\rangle = \sum_{x=1}^{2^{\mathrm{rank}(\Gamma_{AB})}} \frac{1}{2^{\mathrm{rank}(\Gamma_{AB})}} |\psi_x^A\rangle |\psi_x^B\rangle, \tag{A.37}$$

where the orthonormal states with support on A are:

$$|\psi_x^A\rangle = \frac{1}{2^{|A|/2}} \sum_{\varkappa_A \in \mathcal{V}_x} (-1)^{\varkappa_A^\mathrm{T} \Gamma_A \varkappa_A} |\varkappa_A\rangle. \tag{A.38}$$

From the Schmidt decomposition one can safely identify the Schmidt rank as $r = 2^{\mathrm{rank}(\Gamma_{AB})}$ and the Schmidt coefficients as $\beta_x = 2^{-\mathrm{rank}(\Gamma_{AB})}$, which do not depend on the index x.

We are interested in the maximum Schmidt coefficient among all bipartitions $A|B$. The highest Schmidt coefficient is then given by the bipartition with the minimum $\mathrm{rank}(\Gamma_{AB})$. Recall that Γ_{AB} represents the links between the qubits in A and the qubits in B. Thus, if A and B are two sets of qubits that are not connected, $\mathrm{rank}(\Gamma_{AB}) = 0$. However, we are interested in non-separable graph states, so this situation is not possible. The next smallest rank is given when one of the bipartitions includes only one qubit. In that case $\mathrm{rank}(\Gamma_{AB}) = 1$ because this qubit must be connected to another qubit to have a non-separable graph state. Finally, the maximum Schmidt coefficient of a graph state, and consequently of any non-separable stabiliser state is $\beta_{\max} = 1/\sqrt{2}$. Hence the proof.

A.7 Optimising the lower bound of localisable entanglement (LE) provided by local witnesses

As discussed in Section 5.3.2, one needs to determine the minimum value of negativity that is consistent with an experimentally determined expectation value ω of a genuine witness operator. We only focus on the witness operator $W_{|\mathcal{G}\rangle}$ defined for a graph state $|\mathcal{G}\rangle$, and the optimisation problem aims to find the solution of

$$\begin{aligned} \mathcal{E}(\rho_{AB}) = \quad & \inf \|\rho_{AB}^{T_A}\|_1 - 1, \\ \text{subject to} \quad & \mathrm{Tr}\left(\rho_{AB} W_{|\mathcal{G}\rangle}\right) = \omega, \\ & \rho_{AB} \geq 0, \\ & \mathrm{Tr}\left(\rho_{AB}\right) = 1, \end{aligned} \tag{A.39}$$

where the optimisation is done over all possible states ρ_{AB}. Due to the preservation of the entanglement measures under local-unitary operators and the local-unitary equiv-

A.7 Optimising the lower bound of localisable entanglement (LE) provided by local witnesses

alence between graph and stabiliser states, the result of the problem above is the same for a witness prepared for any stabiliser state. Here, we have considered a specific bipartition of the state into the subparts A and B, and $\mathcal{E}(\rho_{AB})$ is the quantity to be computed. Using the variational characterisation of trace-norm, and following the procedure described in Ref. [129], one arrives at

$$\mathcal{E}(\rho_{AB}) \geq \quad \mathcal{E}^{\text{lb}}(\omega) = \inf \text{Tr}\left[D\rho_{AB}^{T_A}\right] - 1,$$

$$\text{subject to} \quad \text{Tr}[\rho_{AB}W_{|\mathscr{G}\rangle}] = \omega,$$

$$\rho_{AB} \geq 0,$$

$$\text{Tr}[\rho_{AB}] = 1, \tag{A.40}$$

where D is any operator such that $\|D\|_\infty = 1$, and the right-hand-side of the inequality in Eq. (A.40) provides a lower bound $\mathcal{E}^{\text{lb}}(\omega)$ of negativity. Considering D to be of the form $D = -f\left(W_{|\mathscr{G}\rangle}\right)^{T_A} + hI$ involving the partial transpose of the local witness operator that has been measured, where the coefficients f and h are such that $\|D\|_\infty = 1$, one arrives at a simple form of the lower bound, given by

$$\mathcal{E}^{\text{lb}}(\omega) = \max_{f,h}(-fw + h - 1) \text{ subject to } \|D\|_\infty = 1. \tag{A.41}$$

Note that the form chosen for D allows one to avoid the minimisation involved in (A.40). Note also that any set of values of f, h subject to $\|D\|_\infty = 1$ provides a value of the lower bound.

However, we would like to find the best possible value by performing the optimisation in Eq. (A.41). In order to do so, note that $\left(W_{|\mathscr{G}\rangle}\right)^{T_A} = 1/2\,I - |\mathscr{G}\rangle\langle\mathscr{G}|^{T_A}$, and since $|\mathscr{G}\rangle\langle\mathscr{G}|^{T_A}$ is diagonal in the graph state basis, so is D. In the case of an entangled graph state of size two $|\mathscr{G}\rangle = 2^{-1/2}(|0+\rangle + |1-\rangle)$, A and B denote single qubits, and

$$|\mathscr{G}\rangle\langle\mathscr{G}|^{T_A} = \frac{1}{2}\big[|\mathscr{G}\rangle\langle\mathscr{G}| + Z_1|\mathscr{G}\rangle\langle\mathscr{G}|Z_1 + Z_2|\mathscr{G}\rangle\langle\mathscr{G}|Z_2 - Z_1Z_2|\mathscr{G}\rangle\langle\mathscr{G}|Z_1Z_2\big]. \tag{A.42}$$

In the case of $\boldsymbol{q}$ constituted of three qubits, say, 1, 2, and 3, one can consider three possible bipartitions of $\boldsymbol{q}$, which are equivalent under qubit permutations. For the

bipartition 1|23 of the fully-connected three qubit graph state, one obtains

$$
|\mathscr{G}\rangle \langle \mathscr{G}|^{T_A} \;=\; \frac{1}{2}\big[\, |\mathscr{G}\rangle \langle \mathscr{G}| + Z_1 |\mathscr{G}\rangle \langle \mathscr{G}| Z_1 + Z_2 Z_3 |\mathscr{G}\rangle \langle \mathscr{G}| Z_2 Z_3 - Z_1 Z_2 Z_3 |\mathscr{G}\rangle \langle \mathscr{G}| Z_1 Z_2 Z_3 \,\big].
$$

$$(A.43)$$

The singular values of D are $\{|h|, |h-f|\}$ and $\{|h|, |h-f|, |h-f/2|\}$ for regions of size two and three, respectively. Since $\|D\|_\infty = 1$, the maximum singular value among them must be 1, which implies $\max\{|h|, |h-f|\} = 1$, because the third singular value is smaller than or equal than the first or the second for any pair h, f. This can be satisfied with four sets of solutions of f and h, given by (i) ($h = 1$, $0 \le f \le 2$), (ii) ($h = -1, -2 \le f \le 0$), (iii) ($h = 1 + f$, $-2 \le f \le 0$), and (iv) ($h = -1 - f$, $0 \le f \le 2$). As mentioned earlier, although any of the four pairs of values of f and h provides a valid lower bound for $\mathcal{E}(\rho_{AB})$, we choose the best of them. In the case when $\omega < 0$, the optimal pair is ($h = 1$, $f = 2$) from (i), and for $\omega \ge 0$, the optimal values are ($h = 1$ and $f = 0$) from (i) and (iii), which leads to

$$
\mathcal{E}^{\mathrm{lb}}(\omega) \;=\; \begin{cases} -2\omega & \text{for } \omega < 0, \\ 0 & \text{for } \omega \ge 0, \end{cases}.
$$

$$(A.44)$$

A.8 Invertible recombinations of stabilisers preserve the rank of the pseudo-incidence matrix

Here we prove that the rank of the pseudo-incidence matrix of a generator set of stabilisers does not change when the stabilisers are recombined. The idea of the proof consists in writing the generator set $\mathcal{S}$ in the binary representation and prove that an invertible recombination of $\mathcal{S}$ results in an invertible recombination of the rows of $\tilde{\mathbb{M}}(\mathcal{S})$. We are interested in the case where $\mathcal{S}$ is a generator set that completely defines a stabiliser state, but the proof applies to any subset of stabilisers.

Given the binary representation $\mathbb{S}$ shown in Eq. (2.46) of the generator set $\mathcal{S}$, the elements of the pseudo-incidence matrix of $\mathcal{S}$ can be written as:

$$
\tilde{\mathbb{M}}(\mathcal{S})_{q\{i,j\}} = \mathbb{Z}_{qi}\mathbb{X}_{qj} + \mathbb{Z}_{qj}\mathbb{X}_{qi} = \big(\mathbb{u}_q^{\mathrm{T}} \mid 0\big)\, \mathbb{S}\, \big(\mathbb{v}_i \mathbb{v}_j^{\mathrm{T}} + \mathbb{v}_j \mathbb{v}_i^{\mathrm{T}}\big)\, \mathbb{S}^{\mathrm{T}} \begin{pmatrix} 0 \\ \mathbb{u}_q \end{pmatrix},
$$

$$(A.45)$$

where the column index $l = \{i, j\}$ runs over all pairs of stabilisers in s_i, $s_j \in \mathcal{S}$. Here the

auxiliary binary column vectors $\mathbb{u}_q$, $\mathbb{v}_i$ of size n have one 1 in the position $q = 1, \ldots, n$ and $i = 1, \ldots, n$, respectively, and zeros elsewhere.

For simplicity, let us expand $\tilde{\mathbb{M}}(\mathcal{S})$ to have one column for each of the N^2 possible pairs (i, j), including those with equal indices (i, i), and both orderings (i, j) and with (j, i). Note that this expanded pseudo-incidence matrix has the same rank because the new columns (i, i) are defined as zero columns and the new columns (j, i) coincide with the existing columns (i, j). Thus, in the following, the pair of indices (i, j) run over all N^2 possibilities and hence, the pseudo-incidence matrix is an $N \times N^2$ matrix.

Moreover, a generator set $\mathcal{S}'$ obtained by an invertible recombination $\mathbb{R}$ of $\mathcal{S}$ is represented by $\mathbb{S}\mathbb{R}$, where $\mathbb{R}$ is a non-singular $N \times N$ binary matrix. Then:

$$\tilde{\mathbb{M}}(\mathcal{S}')_{q(i,j)} = \left(\mathbb{u}_q^{\mathrm{T}} \mid 0\right) \mathbb{S}\mathbb{R} \left(\mathbb{v}_i\mathbb{v}_j^{\mathrm{T}} + \mathbb{v}_j\mathbb{v}_i^{\mathrm{T}}\right) \mathbb{R}^{\mathrm{T}}\mathbb{S}^{\mathrm{T}} \left(\frac{0}{\mathbb{u}_q}\right). \tag{A.46}$$

One can check that the intermediate terms can be rewritten:

$$\mathbb{R} \left(\mathbb{v}_i\mathbb{v}_j^{\mathrm{T}} + \mathbb{v}_j\mathbb{v}_i^{\mathrm{T}}\right) \mathbb{R}^{\mathrm{T}} = \sum_{a,b=1}^{N} \left(\mathbb{v}_a\mathbb{v}_b^{\mathrm{T}} + \mathbb{v}_b\mathbb{v}_a^{\mathrm{T}}\right) \mathbb{R}_{ai}\mathbb{R}_{bj}, \tag{A.47}$$

where we have used that $\mathbb{R} = \sum_{a,b=1}^{N} \mathbb{R}_{ab}\mathbb{v}_a\mathbb{v}_b^{\mathrm{T}}$ and that $\mathbb{v}_b^{\mathrm{T}}\mathbb{v}_i = \delta_{bi}$.

The products $\mathbb{R}_{ai}\mathbb{R}_{bj}$ are the matrix elements $\tilde{\mathbb{R}}_{(a,b)(i,j)}$ of an $N^2 \times N^2$ matrix $\tilde{\mathbb{R}} = \mathbb{R} \times \mathbb{R}$, which is non-singular because $\mathbb{R}$ is non-singular. This matrix performs a recombination of columns on the modified pseudo-incidence matrix:

$$\begin{aligned}\tilde{\mathbb{M}}(\mathcal{S}')_{q(i,j)} &= \sum_{a,b} \left(\mathbb{u}_q^{\mathrm{T}} \mid 0\right) \mathbb{S} \left(\mathbb{v}_a\mathbb{v}_b^{\mathrm{T}} + \mathbb{v}_b\mathbb{v}_a^{\mathrm{T}}\right) \mathbb{S}^{\mathrm{T}} \left(\frac{0}{\mathbb{u}_q}\right) \tilde{\mathbb{R}}_{(a,b)(i,j)} \\ &= \sum_{a,b} \tilde{\mathbb{M}}(\mathcal{S})_{q(a,b)} \tilde{\mathbb{R}}_{(a,b)(i,j)}.\end{aligned} \tag{A.48}$$

Given that $\tilde{\mathbb{R}}$ is non-singular, the rank of the pseudo-incidence matrix is preserved. Hence the proof.

A.9 Example of a valid local witness that cannot be found with the graph-based method

Here we show an example of a local witness that can be found with the stabiliser-based method, but not with the graph-based method. This proves that the graph-based method cannot find all local witnesses found with the stabiliser-based method.

Both methods find stabiliser subsets $\mathcal{W}_{\boldsymbol{q}}$ that satisfy property (A) in Proposition 1. The graph-based method uses the local unitary operations U_{LUE} that transform the stabiliser state into a graph state $U_{\mathrm{LUE}}\,|\mathscr{S}\rangle = |\mathscr{G}\rangle$. These U_{LUE} guarantee the existence of $\mathcal{W}_{\boldsymbol{q}}$ because $\mathcal{W}_{\boldsymbol{q}}^{\mathscr{G}}$ exists:

$$U_{\mathrm{LUE}}\,|\mathscr{S}\rangle = |\mathscr{G}\rangle \;\; \Rightarrow \;\; U_{\mathrm{LUE}}\mathcal{W}_{\boldsymbol{q}}U_{\mathrm{LUE}}^{\dagger} = \mathcal{W}_{\boldsymbol{q}}^{\mathscr{G}}. \tag{A.49}$$

On the other hand every stabiliser subset $\mathcal{W}_{\boldsymbol{q}}$ found with the stabiliser-based method is directly built to satisfy property (A) in Proposition 1, i.e., there exists a local unitary V_{LUE} that transforms $\mathcal{W}_{\boldsymbol{q}}$ into some $\mathcal{W}_{\boldsymbol{q}}^{\mathscr{G}}$ (up to some recombination). But this does not imply that V_{LUE} transforms the stabiliser state $|\mathscr{S}\rangle$ into a graph state $|\mathscr{G}\rangle$:

$$V_{\mathrm{LUE}}\,|\mathscr{S}\rangle = |\mathscr{G}\rangle \;\; \nLeftarrow \;\; V_{\mathrm{LUE}}\mathcal{W}_{\boldsymbol{q}}V_{\mathrm{LUE}}^{\dagger} = \mathcal{W}_{\boldsymbol{q}}^{\mathscr{G}}. \tag{A.50}$$

For instance, the subset $\mathcal{W}_{\{2,3,4\}}$ in Fig. 5.1(a) is transformed into a generator subset $\mathcal{W}_{\boldsymbol{q}}^{\mathscr{G}}$ with the local unitary $V_{\mathrm{LUE}} = H_3 H_5 H_6 H_7$:

$$\begin{aligned}
s_R^Z &= Z_1 Z_2 Z_3 Z_4 \mapsto g_3 = Z_1 Z_2 X_3 Z_4, \\
s_B^X &= X_2 X_3 X_5 X_6 \mapsto g_2 = X_2 Z_3 Z_5 Z_6, \\
s_G^X &= X_3 X_4 X_6 X_7 \mapsto g_4 = Z_3 X_4 Z_6 Z_7,
\end{aligned} \tag{A.51}$$

but $V_{\mathrm{LUE}}\,|\mathscr{S}\rangle$ is not a graph state because the rest of generators in the basis S in Eq. (5.3) do not convert to graph state generators under any recombination:

$$\begin{aligned}
s_R^X &= X_1 X_2 X_3 X_4 \mapsto X_1 X_2 Z_3 X_4, \\
s_B^Z &= Z_2 Z_3 Z_5 Z_6 \mapsto Z_2 X_3 X_5 X_6, \\
s_G^Z &= Z_3 Z_4 Z_6 Z_7 \mapsto X_3 Z_4 X_6 X_7, \\
s_L^X &= X_1 X_2 X_3 X_4 X_5 X_6 X_7 \mapsto X_1 X_2 Z_3 X_4 Z_5 Z_6 Z_7.
\end{aligned} \tag{A.52}$$

What we prove in this appendix is that $\mathcal{W}_{\{2,3,4\}}$ is an example of a stabiliser subset for which there is no local unitary V_{LUE} that transforms it into a subset of graph state generators $\mathcal{W}^{\mathcal{G}}_{\{2,3,4\}}$ and also transforms the stabiliser state $|\mathscr{S}\rangle$ into a graph state $|\mathscr{G}\rangle$. In the binary picture it becomes clear that V_{LUE} is partially fixed because it transforms $\mathcal{W}_{\{2,3,4\}}$ into some $\mathcal{W}^{\mathcal{G}}_{\boldsymbol{q}}$. The condition that V_{LUE} transforms $\mathcal{W}_{\{2,3,4\}}$ into some $\mathcal{W}^{\mathcal{G}}_{\{2,3,4\}}$ is enough to forbid the existence of any non-singular matrix $\mathbb{R}$ that recombines the generator set $\mathcal{S}$ of $|\mathscr{S}\rangle$ to obtain a generator set $\mathcal{G}$ under the action of V_{LUE}.

First, let us show that the binary form of a stabiliser subset $\mathcal{W}_{\boldsymbol{q}}$ that satisfies Proposition 1, or equivalently, which satisfies Theorem 1, is the $2n \times |\boldsymbol{q}|$ binary matrix $\mathbb{W}_{\boldsymbol{q}}$:

$$
\mathbb{W}_{\boldsymbol{q}} = \begin{pmatrix} \mathbb{Z}_{\boldsymbol{q}} \\ \hline \varLambda^Z \varSigma_{\bar{\boldsymbol{q}}} \\ \hline \mathbb{X}_{\boldsymbol{q}} \\ \hline \varLambda^X \varSigma_{\bar{\boldsymbol{q}}} \end{pmatrix}.
\tag{A.53}
$$

The rows have been reordered to represent the qubits in $\boldsymbol{q}$ with the $|\boldsymbol{q}| \times |\boldsymbol{q}|$ binary block matrices $\mathbb{Z}_{\boldsymbol{q}}, \mathbb{X}_{\boldsymbol{q}}$, and the qubits in $\bar{\boldsymbol{q}}$ with the product of the $(n-|\boldsymbol{q}|) \times |\boldsymbol{q}|$ matrix $\varSigma_{\bar{\boldsymbol{q}}}$ and the $(n-|\boldsymbol{q}|) \times (n-|\boldsymbol{q}|)$ diagonal matrices $\varLambda^Z, \varLambda^X$.

To satisfy property (A), the rank modulo 2 of this matrix must be $|\boldsymbol{q}|$. To satisfy property (C), the rank modulo 2 of the following matrix, which represents the set of reduced Pauli operators $\mathcal{W}_{\boldsymbol{q}}|_{\boldsymbol{q}}$, must be $|\boldsymbol{q}|$ as well:

$$
\begin{pmatrix} \mathbb{Z}_{\boldsymbol{q}} \\ \hline \mathbb{X}_{\boldsymbol{q}} \end{pmatrix}.
\tag{A.54}
$$

The form of the blocks $\varLambda^Z \varSigma_{\bar{\boldsymbol{q}}}$ and $\varLambda^X \varSigma_{\bar{\boldsymbol{q}}}$ that represent the single-qubit Pauli operators in the qubits of $\bar{\boldsymbol{q}}$ guarantees that the stabilisers commute qubit-wise on each qubit in $\bar{\boldsymbol{q}}$, which constitutes property (B). To see this note that the matrices $\varLambda^Z, \varLambda^X$ are diagonal, so they just make zero certain rows of $\varSigma_{\bar{\boldsymbol{q}}}$. For a qubit $q \in \bar{\boldsymbol{q}}$ the rows q and $n+q$ of $\mathbb{W}_{\boldsymbol{q}}$ can be of any of these four types:

$$
\begin{pmatrix} \varSigma_{\bar{\boldsymbol{q}},\nu} \\ \hline \varSigma_{\bar{\boldsymbol{q}},\nu} \end{pmatrix} \ , \ \begin{pmatrix} \varSigma_{\bar{\boldsymbol{q}},\nu} \\ \hline 0 \end{pmatrix} \ , \ \begin{pmatrix} 0 \\ \hline \varSigma_{\bar{\boldsymbol{q}},\nu} \end{pmatrix} \ , \ \begin{pmatrix} 0 \\ \hline 0 \end{pmatrix}
\tag{A.55}
$$

depending on the four combinations of 1 and 0 that Λ^Z, Λ^X have in the diagonal position corresponding to the qubit q. Here $\Sigma_{\bar{\boldsymbol{q}},\nu}$ is the ν-th row of $\Sigma_{\bar{\boldsymbol{q}}}$, with $\nu = q - |\boldsymbol{q}|$.

With respect to the first possibility, for every stabiliser $s_i \in \mathcal{W}_{\boldsymbol{q}}$, the single-qubit Pauli operator σ_{qi} is I or Y, in the second possibility it is either I or Z, in the third I or X depending if $\Sigma_{\bar{\boldsymbol{q}},\nu i} = 0$ or 1, respectively, and in the fourth possibility $\sigma_{qi} = I$. Consequently, every stabiliser $s_i \in \mathcal{W}_{\boldsymbol{q}}$ commutes on every qubit $q \in \bar{\boldsymbol{q}}$ by construction, as demanded by property (B).

Now we focus on the particular stabiliser subset $\mathcal{W}_{\{2,3,4\}}$. It contains $|\boldsymbol{q}| = 3$ independent stabilisers so it can be part of a generator set $\mathcal{S}$ represented by $\mathbb{S}$ of the stabiliser state. Without loss of generality, one can write the binary representation $\mathbb{W}_{\{2,3,4\}}$ in the first three columns of $\mathbb{S}$ and write the rest of generators in the other four columns:

$$
\mathbb{S} = \left(\begin{array}{c|c} \mathbb{Z}_{\boldsymbol{q}} & \tilde{\mathbb{Z}}_{\boldsymbol{q}} \\ \Lambda^Z \Sigma_{\bar{\boldsymbol{q}}} & \tilde{\mathbb{Z}}_{\bar{\boldsymbol{q}}} \\ \hline \mathbb{X}_{\boldsymbol{q}} & \tilde{\mathbb{X}}_{\boldsymbol{q}} \\ \Lambda^X \Sigma_{\bar{\boldsymbol{q}}} & \tilde{\mathbb{X}}_{\bar{\boldsymbol{q}}} \end{array} \right) = \left(\begin{array}{ccc|cccc} 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ \hline 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{array} \right). \tag{A.56}
$$

Note that we have reordered the rows to identify easily the blocks. From the first to the last row, the order of the qubits that they represent is: $2, 3, 4, 1, 5, 6, 7$, so the first three rows represent the qubits in $\boldsymbol{q} = \{2, 3, 4\}$ and the last four rows the rest of qubits. From the left column to the right column, the order of the stabilisers that they represent is: s_R^Z, s_B^X, s_G^X, s_B^Z, s_G^Z, s_R^X, s_L^X, so the first three columns represent

the stabilisers in $\mathcal{W}_{\{2,3,4\}}$. Thus, the following blocks can be identified:

$$
\Lambda^Z \Sigma_{\bar{\boldsymbol{q}}} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad \Lambda^X \Sigma_{\bar{\boldsymbol{q}}} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix},
$$

$$
\tilde{\mathbb{Z}}_{\bar{\boldsymbol{q}}} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \quad \tilde{\mathbb{X}}_{\bar{\boldsymbol{q}}} = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \tag{A.57}
$$

From the blocks $\Lambda^Z \Sigma_{\bar{\boldsymbol{q}}}, \Lambda^X \Sigma_{\bar{\boldsymbol{q}}}$ one can read $\Lambda^Z, \Lambda^X, \Sigma_{\bar{\boldsymbol{q}}}$:

$$
\Sigma_{\bar{\boldsymbol{q}}} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \quad \Lambda^Z = \mathrm{diag}(1000), \quad \Lambda^X = \mathrm{diag}(0111). \tag{A.58}
$$

The diagonal matrices Λ^Z and Λ^X fix partially the part $V_{\mathrm{LUE}}|_{\bar{\boldsymbol{q}}}$ of the local Clifford unitary $V_{\mathrm{LUE}} = V_{\mathrm{LUE}}|_{\boldsymbol{q}} \otimes V_{\mathrm{LUE}}|_{\bar{\boldsymbol{q}}}$ acting on the qubits in $\bar{\boldsymbol{q}}$. This part must transform all the single-qubit Pauli operators in $\bar{\boldsymbol{q}}$ into I or Z because the generator subsets $\mathcal{W}_{\boldsymbol{q}}^{\mathscr{G}}$ have only I or Z on each qubit of $\bar{\boldsymbol{q}}$. To do so, the part $V_{\mathrm{LUE}}|_{\bar{\boldsymbol{q}}}$ must be represented by:

$$
\mathbb{V}_{\mathrm{LUE}}|_{\bar{\boldsymbol{q}}} = \left(\begin{array}{c|c} A & B \\ \hline \Lambda^X & \Lambda^Z \end{array} \right), \tag{A.59}
$$

where A, B are some $(n - |\boldsymbol{q}|) \times (n - |\boldsymbol{q}|)$ binary diagonal matrices that satisfy $A\Lambda^Z + B\Lambda^X = \mathbb{1}_{\bar{\boldsymbol{q}}}$. It transforms all the single-qubit Pauli operators in $\bar{\boldsymbol{q}}$ into I or Z of the stabilisers in $\mathcal{W}_{\boldsymbol{q}}$:

$$
\mathbb{V}_{\mathrm{LUE}}|_{\bar{\boldsymbol{q}}} \left(\frac{\Lambda^Z \Sigma_{\bar{\boldsymbol{q}}}}{\Lambda^X \Sigma_{\bar{\boldsymbol{q}}}} \right) = \left(\frac{\Sigma_{\bar{\boldsymbol{q}}}}{0} \right). \tag{A.60}
$$

But how does it affect the rest of stabilisers? One can see that the effect on the corresponding blocks is:

$$
\mathbb{V}_{\mathrm{LUE}}|_{\bar{\boldsymbol{q}}} \left(\frac{\tilde{\mathbb{Z}}_{\bar{\boldsymbol{q}}}}{\tilde{\mathbb{X}}_{\bar{\boldsymbol{q}}}} \right) = \left(\frac{A\tilde{\mathbb{Z}}_{\bar{\boldsymbol{q}}} + B\tilde{\mathbb{X}}_{\bar{\boldsymbol{q}}}}{\Lambda^X \tilde{\mathbb{Z}}_{\bar{\boldsymbol{q}}} + \Lambda^Z \tilde{\mathbb{X}}_{\bar{\boldsymbol{q}}}} \right). \tag{A.61}
$$

Therefore, the modified block is fixed by Λ^X, Λ^Z as:

$$\tilde{\mathbb{X}}'_{\bar{q}} \equiv \Lambda^X \tilde{\mathbb{Z}}_{\bar{q}} + \Lambda^Z \tilde{\mathbb{X}}_{\bar{q}} = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \tag{A.62}$$

which importantly, is not an invertible matrix.

We are trying to show that there is no local unitary V_{LUE} represented by some $\mathbb{V}_{\mathrm{LUE}}$ that transforms the generator set $\mathcal{S}$ into graph state generators and also transforms $\mathbb{W}_{\boldsymbol{q}}$ into graph state generators. That means that $\mathbb{V}_{\mathrm{LUE}}\mathbb{S}\mathbb{R}$ does not represent the generator set $\mathcal{G}$ of a graph state for any $\mathbb{R}$. The binary representation of a graph state can be written respecting the block structure

$$\left(\begin{array}{c} \begin{array}{cc} \Gamma_{\boldsymbol{q}} & \Gamma_{\boldsymbol{q}\bar{\boldsymbol{q}}} \\ \Gamma^{\mathrm{T}}_{\boldsymbol{q}\bar{\boldsymbol{q}}} & \Gamma_{\bar{\boldsymbol{q}}} \\ \hline \mathbb{1}_{\boldsymbol{q}} & 0 \\ 0 & \mathbb{1}_{\bar{\boldsymbol{q}}} \end{array} \end{array} \right). \tag{A.63}$$

One can write by blocks a completely general non-singular matrix $\mathbb{R}$

$$\mathbb{R} = \begin{pmatrix} \mathbb{R}_{\boldsymbol{q}} & \mathbb{R}_{\boldsymbol{q}\bar{\boldsymbol{q}}} \\ \mathbb{R}_{\bar{\boldsymbol{q}}\boldsymbol{q}} & \mathbb{R}_{\bar{\boldsymbol{q}}} \end{pmatrix}, \tag{A.64}$$

where $\mathbb{R}_{\boldsymbol{q}}$, $\mathbb{R}_{\bar{\boldsymbol{q}}}$ are any $|\boldsymbol{q}| \times |\boldsymbol{q}|$ and $(n - |\boldsymbol{q}|) \times (n - |\boldsymbol{q}|)$ binary matrices, respectively, and $\mathbb{R}_{\boldsymbol{q}\bar{\boldsymbol{q}}}$, $\mathbb{R}_{\bar{\boldsymbol{q}}\boldsymbol{q}}$ are any $|\boldsymbol{q}| \times (n - |\boldsymbol{q}|)$ and $(n - |\boldsymbol{q}|) \times n$ binary matrices, respectively, such that $\mathbb{R}$ is non-singular.

Then, the lower blocks in Eq. (A.56) change in this way:

$$\mathbb{V}_{\mathrm{LUE}}|_{\bar{q}} \left(\Lambda^X \Sigma_{\bar{q}} \quad \mathbb{X}_{\bar{q}} \right) \mathbb{R} = \left(0 \quad \tilde{\mathbb{X}}'_{\bar{q}} \right) \mathbb{R} = \left(\tilde{\mathbb{X}}'_{\bar{q}} \mathbb{R}_{\bar{q}q} \quad \tilde{\mathbb{X}}'_{\bar{q}} \mathbb{R}_{\bar{q}} \right). \tag{A.65}$$

The key is that the new block $\tilde{\mathbb{X}}'_{\bar{q}} \mathbb{R}_{\bar{q}}$ in the right should be $\mathbb{1}_{\bar{q}}$ to represent the generator set of a graph state.

However, given that $\tilde{\mathbb{X}}'_{\bar{q}}$ is not invertible, there is no matrix $\mathbb{R}_{\bar{q}q}$ such that:

$$\tilde{\mathbb{X}}'_{\bar{q}} \mathbb{R}_{\bar{q}q} = \mathbb{1}_{\bar{q}}. \tag{A.66}$$

This proves that there is no local unitary V_{LUE} that satisfies Proposition 1 for the stabiliser subset $\mathcal{W}_{\{2,3,4\}}$ of Fig. 5.1 and transforms the stabiliser state $|\mathcal{S}\rangle$ into a graph

state. Therefore, $\mathcal{W}_{\{2,3,4\}}$ is an example of a local witness that can be found with the stabiliser-based method but not with the graph-based method.

A.10   Variance of the witnesses

Here we obtain the variance of the witnesses expectation values from the the expectation values of the stabilisers computed experimentally.

The expectation value of a stabiliser operator is the mean value of the outcomes $+1$ and -1 when the operator is measured M times. We treat the experimental value of a stabiliser operator as a binomially distributed random variable with two possible values: $+1$ and -1 with probabilities p_i and $1 - p_i$, so the expectation value is:

$$\langle s_i \rangle = 2p_i - 1. \tag{A.67}$$

The binomial distribution gives the probability of obtaining M_i times in a sample of M repetitions the result $+1$, which is the one obtained with probability p_i. The variance of binomial distributions is given by:

$$\sigma^2(M_i) = Mp_i(1 - p_i). \tag{A.68}$$

The binomial variable $\langle s_i \rangle$ is related to M_i by:

$$\langle s_i \rangle = \frac{2M_i}{M} - 1. \tag{A.69}$$

The variance of a function f depending of M_i is related to $\sigma^2(M_i)$:

$$\sigma^2(f(M_i)) = \left[\frac{\mathrm{d}f(M_i)}{\mathrm{d}M_i}\right]^2 \bigg|_{Mp_i} \sigma^2(M_i). \tag{A.70}$$

Using simple algebra one obtains the variance of the stabiliser operator:

$$\sigma^2\left(\langle s_i \rangle\right) = \frac{1}{M}\left(1 - \langle s_i \rangle^2\right). \tag{A.71}$$

Since the variance of a sum of independent random variables is given by the sum of the variances of each variable, one can finally compute the variance of witness operators with just the experimental value $\langle s_i \rangle$ of the stabilisers involved in the witness and the

number of times M that the measurement was repeated:

$$\sigma^2\left(W_{|\mathscr{S}\rangle}\right) = \frac{1}{M}\sum_{i=1}^{2^N-1}\frac{1-\langle s_i\rangle^2}{2^{2N}}, \tag{A.72}$$

$$\sigma^2\left(W_{|\mathscr{S}\rangle}^{\mathrm{a}}\right) = \frac{1}{2M}\sum_{i=1}^{N}\left(1-\langle s_i\rangle^2\right), \tag{A.73}$$

$$\sigma^2\left(W_{|\mathscr{S}\rangle}^{\mathrm{2m}}\right) = \frac{1}{M}\sum_{s_i^X\in\mathcal{S}}\frac{1-\langle s_i^X\rangle^2}{\left(|\mathscr{S}^X|+1\right)^2},$$
$$+ \frac{1}{M}\sum_{s_i^Z\in\mathscr{S}}\frac{1-\langle s_i^Z\rangle^2}{\left(|\mathscr{S}^Z|+1\right)^2}, \tag{A.74}$$

where $\mathscr{S}^X$ are the X-type stabilisers $s_i^X\in\mathscr{S}$ in the stabiliser group $\mathscr{S}$, and $\mathscr{S}^Z$ are the Z-type stabilisers $s_i^Z\in\mathscr{S}$.

The variances of local witnesses constructed from the stabiliser subset $\mathcal{W}_{\boldsymbol{q}}$:

$$\sigma^2\left(W_{\boldsymbol{q}}\right) = \frac{1}{M}\sum_{s_i\in\langle\mathcal{W}_{\boldsymbol{q}}\rangle}\frac{1-\langle s_i\rangle^2}{2^{2n}}, \tag{A.75}$$

$$\sigma^2\left(W_{\boldsymbol{q},a}\right) = \frac{1}{2M}\sum_{s_i\in\mathcal{W}_{\boldsymbol{q}}}\left(1-\langle s_i\rangle^2\right), \tag{A.76}$$

$$\sigma^2\left(W_{\boldsymbol{q},2m}\right) = \frac{1}{M}\sum_{s_i^X\in\langle\mathcal{W}_{\boldsymbol{q}}\rangle}\frac{1-\langle s_i^X\rangle^2}{\left(\left|\langle\mathcal{W}_{\boldsymbol{q}}\rangle^X\right|+1\right)^2},$$
$$+ \frac{1}{M}\sum_{s_i^Z\in\langle\mathcal{W}_{\boldsymbol{q}}\rangle}\frac{1-\langle s_i^Z\rangle^2}{\left(\left|\langle\mathcal{W}_{\boldsymbol{q}}\rangle^Z\right|+1\right)^2}, \tag{A.77}$$

where $\langle\mathcal{W}_{\boldsymbol{q}}\rangle^X$, $\langle\mathcal{W}_{\boldsymbol{q}}\rangle^Z$ are the X-type and Z-type stabilisers s_i^X, s_i^Z in the spanned subgroup $\langle\mathcal{W}_{\boldsymbol{q}}\rangle$, respectively, and the cardinality of these sets is $\left|\langle\mathcal{W}_{\boldsymbol{q}}\rangle^X\right|$, $\left|\langle\mathcal{W}_{\boldsymbol{q}}\rangle^Z\right|$, respectively.

A.11   Obtaining the inverse matrix $\mathbb{R}^{(2)}$

Here we prove that the lower block of $\mathbb{H}_{\boldsymbol{t}}\mathbb{S}'$ is invertible, and determine its inverse, which is designated by $\mathbb{R}^{(2)}$. We take a different approach than the one used in Ref. [174]. We apply a Clifford operation represented by $\mathbb{U}$ that makes the upper block vanish

and leaves the lower block unchanged to $\mathbb{H}_t S'$. The unitary that we construct for the purpose of the proof is represented by

$$
\mathbb{U} = \left(\begin{array}{c|cc} \mathbb{1} & \mathbb{C} & \mathbb{B}^{\mathrm{T}} \\ & \mathbb{B} & 0 \\ \hline 0 & & \mathbb{1} \end{array} \right), \tag{A.78}
$$

where $\mathbb{B}$, $\mathbb{C}$ are defined in Eqs. (5.81) and (5.82), respectively. The matrix $\mathbb{U}\mathbb{H}_t S'$ is given by

$$
\left(\begin{array}{c|cc} \mathbb{Z}_{l,\boldsymbol{c}} + \mathbb{C}\mathbb{X}_{l,\boldsymbol{c}} + \mathbb{B}^{\mathrm{T}}\mathbb{Z}_{l,\boldsymbol{t}} & \mathbb{Z}_{r,c} + \mathbb{B}^{\mathrm{T}}\mathbb{Z}_{r,\boldsymbol{t}} \\ \mathbb{X}_{l,\boldsymbol{t}} + \mathbb{B}\mathbb{X}_{l,\boldsymbol{c}} & 0 \\ \hline \mathbb{X}_{l,\boldsymbol{c}} & 0 \\ \mathbb{Z}_{l,\boldsymbol{t}} & \mathbb{Z}_{r,\boldsymbol{t}} \end{array} \right). \tag{A.79}
$$

From the form of the matrix $\mathbb{C}$ in Eq. (5.81), the non-zero diagonal terms of the upper block vanish, while the off-diagonal terms vanish due to Eq. (5.77). Hence the proof of the invertibility of the lower block of $\mathbb{H}_t S'$. Note that Clifford operations are represented by full-rank matrices, and therefore $\mathbb{U}$ preserves the rank n of $\mathbb{H}_t S'$. Consequently, the matrix $\mathbb{U}\mathbb{H}_t S'$, which contains only the lower block, is of full rank, and therefore, the lower block is invertible.

In order to determine $\mathbb{R}^{(2)}$, note that the lower block of $\mathbb{H}_t S'$ has the form of a lower triangular matrix, and the diagonal terms $\mathbb{X}_{l,\boldsymbol{c}}$ and $\mathbb{Z}_{r,\boldsymbol{t}}$ of the lower block of $\mathbb{H}_t S'$ are also invertible due to the invertibility of the lower block of $\mathbb{H}_t S'$. Therefore, $\mathbb{R}^{(2)}$ is another lower triangular matrix by blocks having the form

$$
\mathbb{R}^{(2)} = \left(\begin{array}{cc} \mathbb{X}_{l,\boldsymbol{c}}^{-1} & 0 \\ \mathbb{E} & \mathbb{Z}_{r,\boldsymbol{t}}^{-1} \end{array} \right), \tag{A.80}
$$

where $\mathbb{E}$ must satisfy that $\mathbb{Z}_{l,\boldsymbol{t}}\mathbb{X}_{l,\boldsymbol{c}}^{-1} + \mathbb{Z}_{r,\boldsymbol{t}}\mathbb{E} = 0$, leading to $\mathbb{E} = \mathbb{Z}_{r,\boldsymbol{t}}^{-1}\mathbb{Z}_{l,\boldsymbol{t}}\mathbb{X}_{l,\boldsymbol{c}}^{-1}$. Hence, one arrives at the form of $\mathbb{R}^{(2)}$ in Eq. (5.74).

A.12 StabGraph code

We developed the **StabGraph** [5] code as a Python code consisting of a function that inputs a generator set $\mathcal{S}$ of a stabiliser state $|\mathscr{S}\rangle$ and outputs the local unitary U_{LUE} that transforms the stabiliser state into a graph state $|\mathscr{G}\rangle = U_{\mathrm{LUE}} |\mathscr{S}\rangle$, and the adjacency matrix Γ defining the graph underlying $|\mathscr{G}\rangle$. The function outputs all the

elements described in Section 5.6: a set $\boldsymbol{c}$ of control qubits, a set $\boldsymbol{t}$ of target qubits, a subset $\boldsymbol{z} \subset \boldsymbol{c}$ of qubits where Z-rotations are applied, and a recombination matrix $\mathbb{R}$.

The function gives the possibility to preselect some control and target qubits. This is useful, for instance, to make sure that the resulting graph has two qubits of interest connected as described in Section 5.6.1. Given an input stabiliser state, not all the sets of control and target qubits are valid, so the function raises a warning and stops the program when these sets are not properly selected at the input. It also allows one to select randomly the sets of control and target qubits, allowing the production of multiple random graphs that are LUE to the stabiliser state.

The function calls a subroutine called `gaus_binary.py` that performs Gauss elimination on linear systems with binary variables.

References

[1] D. Vodola, D. Amaro, M. A. Martín-Delgado, and M. Müller, "Twins percolation for qubit losses in topological color codes," *Phys. Rev. Lett.* **121**, 060501 (2018). iv, 10, 55, 56, 57, 60, 82, 86

[2] D. Amaro, J. Bennett, D. Vodola, and M. Müller, "Analytical percolation theory for topological color codes under qubit loss," *ArXiv e-prints* `1907.12684` (2019). v, 10, 55, 56, 82, 86

[3] D. Amaro, M. Müller, and A. K. Pal, "Estimating localizable entanglement from witnesses," *New J. Phys.* **20**, 063017 (2018). vi, 10, 89, 131, 140

[4] D. Amaro, M. Müller, and A. K. Pal, "Scalable characterization of localizable entanglement in noisy topological quantum codes," *ArXiv e-prints* `1907.13161` (2019). vii, 10, 89, 131, 140

[5] D. Amaro, "stabgraph." Availale at `https://github.com/davamaro/stabgraph`, (2019). vii, 111, 124, 127, 167

[6] D. Amaro, M. Müller, and A. K. Pal, "alcpack." Available at `https://github.com/amitkpal/alcpack`, (2019). vii, xvi, 128, 134, 137

[7] D. Amaro and M. Müller, "Design and experimental performance of local entanglement witness operators," *Phys. Rev. A* **101**, 012317 (Jan, 2020). viii, 11, 89, 131, 140

[8] R. P. Feynman, "Simulating physics with computers," *Int. J. Theor. Phys.* **21**, 467-488 (1982). 1

REFERENCES

[9] J. I. Cirac and P. Zoller, "Goals and opportunities in quantum simulation," *Nat. Phys.* **8**, 264-266 (2012). 1

[10] J. Preskill, "Quantum computing and the entanglement frontier," *ArXiv e-prints* `1203.5813` (2012). 1

[11] J. Preskill, "Quantum Computing in the NISQ era and beyond," *Quantum* **2**, 79 (2018). 1, 3, 143

[12] C. L. Degen, F. Reinhard, and P. Cappellaro, "Quantum sensing," *Rev. Mod. Phys.* **89**, 035002 (2017). 1

[13] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information.* Cambridge University Press, (2000). 1, 2, 8, 13, 19, 31, 36, 91, 124, 128

[14] C. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," vol. 560, 175-179, (1984). 1

[15] A. K. Ekert, "Quantum cryptography based on Bell's theorem," *Phys. Rev. Lett.* **67**, 661-663 (1991). 1

[16] L. K. Grover, "A fast quantum mechanical algorithm for database search," *ArXiv e-prints* `quant-ph/9605043` (1996). 1

[17] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM J. Comput.* **26**, 1484-1509 (1997). 1

[18] S. Aaronson and A. Arkhipov, "The computational complexity of linear optics," in *Proceedings of the Forty-third Annual ACM Symposium on Theory of Computing*, STOC '11, 333-342, (2011). ACM, New York, NY, USA. 2

[19] S. Aaronson and L. Chen, "Complexity-Theoretic Foundations of Quantum Supremacy Experiments," *ArXiv e-prints* `1612.05903` (2016). 2, 143

[20] F. Arute *et al.*, "Quantum supremacy using a programmable superconducting processor," *Nature* **574**, 505-510 (2019). 2, 3, 143

[21] B. Villalonga, S. Boixo, B. Nelson, C. Henze, E. Rieffel, R. Biswas, and S. Mandrà, "A flexible high-performance simulator for verifying and benchmarking quantum circuits implemented on real hardware," *npj Quantum Inf.* **5**, 86 (2019). 2

[22] IBM, "IBM announces advances to IBM quantum systems & ecosystem," *press release by IBM, posted online Nov 10, 2017* . `https://www-03.ibm.com/press/us/en/pressrelease/53374.wss`. Accessed: 2020-01-10. 2

[23] P. Schindler, D. Nigg, T. Monz, J. T. Barreiro, E. Martinez, S. X. Wang, S. Quint, M. F. Brandl, V. Nebendahl, C. F. Roos, M. Chwalla, M. Hennrich, and R. Blatt, "A quantum information processor with trapped ions," *New J. Phys.* **15**, 123012 (2013). 2, 35, 145

[24] K. R. Brown, J. Kim, and C. Monroe, "Co-designing a scalable quantum computer with trapped atomic ions," *npj Quantum Inf.* **2**, 16034 (2016). 2, 7, 29, 37

[25] J. Clarke and F. K. Wilhelm, "Superconducting quantum bits," *Nature* **453**, 1031-1042 (2008). 2, 7, 29, 37

[26] S. Barz, "Quantum computing with photons: introduction to the circuit model, the one-way quantum computer, and the fundamental principles of photonic experiments," *J. Phys B-At. Mol. Opt.* **48**, 083001 (2015). 2, 7, 29, 37

[27] I. Bloch, J. Dalibard, and W. Zwerger, "Many-body physics with ultracold gases," *Rev. Mod. Phys.* **80**, 885-964 (2008). 2, 7, 29, 37

[28] R. M. Serra and I. S. Oliveira, "Nuclear magnetic resonance quantum information processing," *Philos. T. R. Soc. A* **370**, 4615-4619 (2012). 2

[29] C. D. Bruzewicz, J. Chiaverini, R. McConnell, and J. M. Sage, "Trapped-ion quantum computing: Progress and challenges," *Appl. Phys. Rev.* **6**, 021314 (2019). 2, 7, 144, 145

REFERENCES

[30] M. Kjaergaard, M. E. Schwartz, J. Braumüller, P. Krantz, J. I-Jan Wang, S. Gustavsson, and W. D. Oliver, "Superconducting Qubits: Current State of Play," *ArXiv e-prints* `1905.13641` (2019). 2, 7, 144

[31] C. Piltz, T. Sriarunothai, A. F. Varón, and C. Wunderlich, "A trapped-ion-based quantum byte with 10-5 next-neighbour cross-talk," *Nat. Commun.* **5**, 4679 (2014). 3

[32] M. A. Rol, F. Battistel, F. K. Malinowski, C. C. Bultink, B. M. Tarasinski, R. Vollmer, N. Haider, N. Muthusubramanian, A. Bruno, B. M. Terhal, and L. DiCarlo, "Fast, high-fidelity conditional-phase gate exploiting leakage interference in weakly anharmonic superconducting qubits," *Phys. Rev. Lett.* **123**, 120502 (2019). 3, 6

[33] C. J. Wood and J. M. Gambetta, "Quantification and characterization of leakage errors," *Phys. Rev. A* **97**, 032306 (2018). 3

[34] S. Boixo, S. V. Isakov, V. N. Smelyanskiy, R. Babbush, N. Ding, Z. Jiang, M. J. Bremner, J. M. Martinis, and H. Neven, "Characterizing quantum supremacy in near-term devices," *Nat. Phys.* **14**, 595-600 (2018). 3

[35] IBM, "On "quantum supremacy"," *IBM public online blog about research made at IBM* (2019). `https://www.ibm.com/blogs/research/2019/10/on-quantum-supremacy/`. Accessed: 2020-01-10. 3

[36] M. Benedetti, E. Lloyd, S. Sack, and M. Fiorentini, "Parameterized quantum circuits as machine learning models," *Quantum Sci. Technol.* **4**, 043001 (2019). 3, 143

[37] E. Farhi, J. Goldstone, and S. Gutmann, "A Quantum Approximate Optimization Algorithm," *ArXiv e-prints* `1411.4028` (2014). 4

[38] A. Peruzzo, J. McClean, P. Shadbolt, M.-H. Yung, X.-Q. Zhou, P. J. Love, A. Aspuru-Guzik, and J. L. O'Brien, "A variational eigenvalue solver on a photonic quantum processor," *Nat. Commun.* **5**, 4213 (2014). 4

[39] M. Otten and S. K. Gray, "Accounting for errors in quantum algorithms via individual error reduction," *npj Quantum Inf.* **5**, 11 (2019). 4

[40] A. Kandala, K. Temme, A. D. Córcoles, A. Mezzacapo, J. M. Chow, and J. M. Gambetta, "Error mitigation extends the computational reach of a noisy quantum processor," *Nature* **567**, 491-495 (2019). 4

[41] P. D. Johnson, J. Romero, J. Olson, Y. Cao, and A. Aspuru-Guzik, "QVECTOR: an algorithm for device-tailored quantum error correction," *ArXiv e-prints* `1711.02249` (2017). 4

[42] C. Gidney and M. Ekerå, "How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits," *ArXiv e-prints* `1905.09749` (2019). 4

[43] D. Gottesman, "An Introduction to Quantum Error Correction and Fault-Tolerant Quantum Computation," *ArXiv e-prints* `0904.2557` (2009). 4, 5, 45, 144

[44] S. Bravyi, M. Suchara, and A. Vargo, "Efficient algorithms for maximum likelihood decoding in the surface code," *Phys. Rev. A* **90**, 032326 (2014). 4

[45] A. Kubica and N. Delfosse, "Efficient color code decoders in $d \geq 2$ dimensions from toric code decoders," *ArXiv e-prints* `1905.07393` (2019). 4

[46] D. Aharonov and M. Ben-Or, "Fault Tolerant Quantum Computation with Constant Error," *ArXiv e-prints* `quant-ph/9611025 [quant-ph]` (1996). 5

[47] E. Knill, R. Laflamme, and W. Zurek, "Threshold accuracy for quantum computation," *ArXiv e-prints* `quant-ph/9610011` (1996).

[48] A. Y. Kitaev, "Quantum error correction with imperfect gates," in *Quantum Communication, Computing, and Measurement (Proc. 3rd Int. Conf. of Quantum Communication and Measurement) (Plenum Press, New York)*, 181–188, (1997). 5

[49] E. Knill and R. Laflamme, "Concatenated Quantum Codes," *ArXiv e-prints* `quant-ph/9608012` (1996). 5

REFERENCES

[50] K. Fujii, "Quantum computation with topological codes: from qubit to topological fault-tolerance," *ArXiv e-prints* `1504.01444` (2015). 5, 30, 91, 130

[51] F. H. E. Watson and S. D. Barrett, "Logical error rate scaling of the toric code," *New J. of Phys.* **16**, 093045 (2014). 5

[52] E. Dennis, A. Kitaev, A. Landahl, and J. Preskill, "Topological quantum memory," *J. Math. Phys.* **43**, 4452-4505 (2002). 5, 46

[53] H. Bombín and M. A. Martín-Delgado, "Topological quantum distillation," *Phys. Rev. Lett.* **97**, 180501 (2006). 5, 9, 49, 52

[54] R. Raussendorf and J. Harrington, "Fault-tolerant quantum computation with high threshold in two dimensions," *Phys. Rev. Lett.* **98**, 190504 (May, 2007). 5, 40, 49, 144

[55] E. T. Campbell, B. M. Terhal, and C. Vuillot, "Roads towards fault-tolerant universal quantum computation," *Nature* **549**, 172-179 (2017).

[56] A. M. Stephens, "Fault-tolerant thresholds for quantum error correction with the surface code," *Phys. Rev. A* **89**, 022321 (2014). 5, 40, 49, 144

[57] A. J. Landahl, J. T. Anderson, and P. R. Rice, "Fault-tolerant quantum computing with color codes," *ArXiv e-prints* `1108.5738` (2011). 5, 40, 52, 53, 144

[58] A. M. Stephens, "Efficient fault-tolerant decoding of topological color codes," *ArXiv e-prints* `1402.3037` (2014).

[59] C. Chamberland, A. Kubica, T. J. Yoder, and G. Zhu, "Triangular color codes on trivalent graphs with flag qubits," *ArXiv e-prints* `1911.00355` (2019). 53, 144

[60] P. Baireuther, M. D. Caio, B. Criger, C. W. J. Beenakker, and T. E. O'Brien, "Neural network decoder for topological color codes with circuit level noise," *New J. Phys.* **21**, 013003 (2019). 5, 40, 53

[61] J. A. Sherman, M. J. Curtis, D. J. Szwer, D. T. C. Allcock, G. Imreh, D. M. Lucas, and A. M. Steane, "Experimental recovery of a qubit from partial collapse," *Phys. Rev. Lett.* **111**, 1-5 (2013). 6

[62] J. Ghosh, A. G. Fowler, J. M. Martinis, and M. R. Geller, "Understanding the effects of leakage in superconducting quantum-error-detection circuits," *Phys. Rev. A* **88**, 062329 (2013). 6

[63] A. Galiautdinov, "Quantum Zeno effect: A possible resolution to the leakage problem in superconducting quantum computing architectures," *ArViv e-prints* 1805.06877 (2018).

[64] A. Strikis, A. Datta, and G. C. Knee, "Quantum leakage detection using a model-independent dimension witness," *Phys. Rev. A* **99**, 032328 (2019). 6

[65] T. C. Ralph, A. J. Hayes, and A. Gilchrist, "Loss-tolerant optical qubits," *Phys. Rev. Lett.* **95**, 1-4 (2005). 6

[66] T. Yang, J.-W. Pan, W.-B. Gao, C.-Y. Lu, X.-Q. Zhou, and J. Zhang, "Experimental quantum coding against qubit loss error," *Proc. Natl. Acad. Sci.* **105**, 11050-11054 (2008). 6

[67] S. Mehl, H. Bluhm, and D. P. DiVincenzo, "Fault-tolerant quantum computation for singlet-triplet qubits with leakage errors," *Phys. Rev. B* **91**, 085419 (2015). 6

[68] R. W. Andrews *et al.*, "Quantifying error and leakage in an encoded si/sige triple-dot qubit," *Nat. Nanotechnol.* (2019).

[69] G. X. Chan and X. Wang, "Suppression of leakage for a charge qubit in triangular triple quantum dots," *Adv. Quantum Technol.* **2**, 1900072 (2019). 6

[70] M. Grassl, T. Beth, and T. Pellizzari, "Codes for the quantum erasure channel," *Phys. Rev. A* **56**, 33-38 (1997). 6

[71] M. Suchara, A. W. Cross, and J. M. Gambetta, "Leakage suppression in the toric code," in *2015 IEEE International Symposium on Information Theory (ISIT)*, 1119-1123, (2015). 6

[72] N. Delfosse and G. Zémor, "Linear-Time Maximum Likelihood Decoding of Surface Codes over the Quantum Erasure Channel," *ArXiv e-prints* 1703.01517 (2017). 6

[73] N. Delfosse and N. H. Nickerson, "Almost-linear time decoding algorithm for topological codes," *ArXiv e-prints* `1709.06218v1` (2017). 6

[74] T. M. Stace, S. D. Barrett, and A. C. Doherty, "Thresholds for Topological Codes in the Presence of Loss," *Phys. Rev. Lett.* **102**, 200501 (2009). 6, 49, 56

[75] T. M. Stace and S. D. Barrett, "Error correction and degeneracy in surface codes suffering loss," *Phys. Rev. A* **81**, 022317 (2010). 6, 49, 56

[76] D. Nigg, M. Müller, E. A. Martínez, P. Schindler, M. Hennrich, T. Monz, M. A. Martín-Delgado, and R. Blatt, "Quantum computations on a topologically encoded qubit," *Science* **345**, 302-305 (2014). 6, 53, 91, 114, 116, 117, 119, 144

[77] N. M. Linke, M. Gutierrez, K. A. Landsman, C. Figgatt, S. Debnath, K. R. Brown, and C. Monroe, "Fault-tolerant quantum error detection," *Science Advances* **3**, (2017). 144

[78] K. Wright *et al.*, "Benchmarking an 11-qubit quantum computer," *Nat. Commun.* **10**, 5464 (2019). 6

[79] J. Kelly *et al.*, "State preservation by repetitive error detection in a superconducting quantum circuit," *Nature* **519**, 66-69 (2015). 6, 47, 91, 144

[80] J. M. Gambetta, J. M. Chow, and M. Steffen, "Building logical qubits in a superconducting quantum computing system," *Nature Phys. J. Quant. Inf.* **3**, 2 (2017). 6, 7, 47, 91, 144

[81] R. Versluis, S. Poletto, N. Khammassi, B. Tarasinski, N. Haider, D. J. Michalak, A. Bruno, K. Bertels, and L. DiCarlo, "Scalable quantum circuit and control for a superconducting surface code," *Phys. Rev. Applied* **8**, 034021 (2017). 7, 47, 49, 144

[82] T. J. Yoder and I. H. Kim, "The surface code with a twist," *Quantum* **1**, 2 (2017). 7, 53, 144

[83] B. W. Reichardt, "Fault-tolerant quantum error correction for Steane's seven-qubit color code with few or no extra qubits," *ArXiv e-prints* `1804.06995` (2018). 53

[84] R. Chao and B. W. Reichardt, "Quantum error correction with only two extra qubits," *Phys. Rev. Lett.* **121**, 050502 (2018). 7, 53, 144

[85] S. Bravyi and A. Cross, "Doubled color codes," *ArXiv e-prints* 1509.03239 (2015). 7, 145

[86] T. Jochym-O'Connor and S. D. Bartlett, "Stacked codes: Universal fault-tolerant quantum computation in a two-dimensional layout," *Phys. Rev. A* **93**, 022323 (2016). 7, 145

[87] M. A. Nielsen, "Cluster-state quantum computation," *Rep. Math. Phys.* **57**, 147-161 (2006). 7

[88] H. J. Briegel, D. E. Browne, W. Dür, R. Raussendorf, and M. Van den Nest, "Measurement-based quantum computation," *Nature* **5**, 19-26 (2009). 7

[89] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Mod. Phys.* **74**, 145-195 (2002). 7, 29, 147

[90] G. Cariolaro, *Quantum Communications.* Springer, Heidelberg, (2015). 7, 29, 147

[91] D. Leibfried, R. Blatt, C. Monroe, and D. Wineland, "Quantum dynamics of single trapped ions," *Rev. Mod. Phys.* **75**, 281-324 (2003). 7

[92] D. Leibfried, E. Knill, S. Seidelin, J. Britton, R. B. Blakestad, J. Chiaverini, D. B. Hume, W. M. Itano, J. D. Jost, C. Langer, R. Ozeri, R. Reichle, and D. J. Wineland, "Creation of a six-atom 'schrödinger cat' state," *Nature* **438**, 639-642 (2005). 7

[93] J. M. Raimond, M. Brune, and S. Haroche, "Manipulating quantum entanglement with atoms and photons in a cavity," *Rev. Mod. Phys.* **73**, 565-582 (2001). 7

[94] R. Prevedel, G. Cronenberg, M. S. Tame, M. Paternostro, P. Walther, M. S. Kim, and A. Zeilinger, "Experimental realization of dicke states of up to six qubits for multiparty quantum networking," *Phys. Rev. Lett.* **103**, 020503 (2009). 7

REFERENCES

[95] C. Negrevergne, T. S. Mahesh, C. A. Ryan, M. Ditty, F. Cyr-Racine, W. Power, N. Boulant, T. Havel, D. G. Cory, and R. Laflamme, "Benchmarking quantum control methods on a 12-qubit system," *Phys. Rev. Lett.* **96**, 170501 (2006). 7

[96] A. J. Berkley, H. Xu, R. C. Ramos, M. A. Gubrud, F. W. Strauch, P. R. Johnson, J. R. Anderson, A. J. Dragt, C. J. Lobb, and F. C. Wellstood, "Entangled macroscopic quantum states in two superconducting qubits," *Science* **300**, 1548-1550 (2003). 7

[97] J. Hald, J. L. Sørensen, C. Schori, and E. S. Polzik, "Spin squeezed atoms: A macroscopic entangled ensemble created by light," *Phys. Rev. Lett.* **83**, 1319-1322 (1999). 7

[98] O. Mandel, M. Greiner, A. Widera, T. Rom, T. W. Hänsch, and I. Bloch, "Controlled collisions for multi-particle entanglement of optically trapped atoms," *Nature* **425**, 937-940 (2003).

[99] I. Bloch, "Exploring quantum matter with ultracold atoms in optical lattices," *J. Phys. B: At. Mol. Opt. Phys.* **38**, S629-S643 (2005). 7

[100] H. Bernien, B. Hensen, W. Pfaff, G. Koolstra, M. S. Blok, L. Robledo, T. H. Taminiau, M. Markham, D. J. Twitchen, L. Childress, and R. Hanson, "Heralded entanglement between solid-state qubits separated by three metres," *Nature* **497**, 86-90 (2013). 7

[101] E. Togan, Y. Chu, A. S. Trifonov, L. Jiang, J. Maze, L. Childress, M. V. G. Dutt, A. S. Sørensen, P. R. Hemmer, A. S. Zibrov, and M. D. Lukin, "Quantum entanglement between an optical photon and a solid-state spin qubit," *Nature* **466**, 730-734 (2010). 7

[102] I. Marinković, A. Wallucks, R. Riedinger, S. Hong, M. Aspelmeyer, and S. Gröblacher, "Optomechanical bell test," *Phys. Rev. Lett.* **121**, 220404 (2018). 7

[103] D. Gross, Y.-K. Liu, S. T. Flammia, S. Becker, and J. Eisert, "Quantum state tomography via compressed sensing," *Phys. Rev. Lett.* **105**, 150401 (2010). 7, 89

[104] S. T. Flammia, D. Gross, Y.-K. Liu, and J. Eisert, "Quantum tomography via compressed sensing: error bounds, sample complexity and efficient estimators," *New J. Phys.* **14**, 095022 (2012).

[105] A. Steffens, C. A. Riofrío, W. McCutcheon, I. Roth, B. A. Bell, A. McMillan, M. S. Tame, J. G. Rarity, and J. Eisert, "Experimentally exploring compressed sensing quantum tomography," *Quantum Sci. and Technol.* **2**, 025005 (2017). 7, 89

[106] C. A. Riofrío, D. Gross, S. T. Flammia, T. Monz, D. Nigg, R. Blatt, and J. Eisert, "Experimental quantum compressed sensing for a seven-qubit system," *Nat. Commun.* **8**, 15305 (2017). 7, 89

[107] M. Cramer, M. B. Plenio, S. T. Flammia, R. Somma, D. Gross, S. D. Bartlett, O. Landon-Cardinal, D. Poulin, and Y.-K. Liu, "Efficient quantum state tomography," *Nat. Commun.* **1**, 149 (2010). 7

[108] M. Ohliger, V. Nesme, and J. Eisert, "Efficient and feasible state tomography of quantum many-body systems," *New J. Phys.* **15**, 015024 (2013).

[109] Y.-Y. Zhao, Z. Hou, G.-Y. Xiang, Y.-J. Han, C.-F. Li, and G.-C. Guo, "Experimental demonstration of efficient quantum state tomography of matrix product states," *Opt. Express* **25**, 9010-9018 (2017).

[110] B. P. Lanyon, C. Maier, M. Holzäpfel, T. Baumgratz, C. Hempel, P. Jurcevic, I. Dhand, A. S. Buyskikh, A. J. Daley, M. Cramer, M. B. Plenio, R. Blatt, and C. F. Roos, "Efficient tomography of a quantum many-body system," *Nat. Phys.* **13**, 1158-1162 (2017). 7

[111] B. M. Terhal, "Detecting quantum entanglement," *Theor. Comput. Sci.* **287**, 313-335 (2002). 7, 92

[112] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, "Quantum entanglement," *Rev. Mod. Phys.* **81**, 865-942 (2009). 30, 31

[113] O. Gühne and G. Tóth, "Entanglement detection," *Phys. Rep.* **474**, 1-75 (2009). 7, 90, 92, 147

REFERENCES

[114] W. Wieczorek, R. Krischek, N. Kiesel, P. Michelberger, G. Tóth, and H. Weinfurter, "Experimental entanglement of a six-photon symmetric dicke state," *Phys. Rev. Lett.* **103**, 020504 (2009). 7

[115] C.-F. Li, J.-S. Xu, X.-Y. Xu, K. Li, and G.-C. Guo, "Experimental investigation of the entanglement-assisted entropic uncertainty principle," *Nat. Phys.* **7**, 752-756 (2011).

[116] Y. Pu, Y. Wu, N. Jiang, W. Chang, C. Li, S. Zhang, and L. Duan, "Experimental entanglement of 25 individually accessible atomic quantum interfaces," *Sci. Adv.* **4**, eaar3931 (2018). 7

[117] P. Horodecki and M. Lewenstein, "Bound entanglement and continuous variables," *Phys. Rev. Lett.* **85**, 2657-2660 (2000). 7

[118] P. Hyllus and J. Eisert, "Optimal entanglement witnesses for continuous-variable systems," *New J. Phys.* **8**, 51-51 (2006).

[119] C. Zhang, S. Yu, Q. Chen, and C. H. Oh, "Detecting and estimating continuous-variable entanglement by local orthogonal observables," *Phys. Rev. Lett.* **111**, 190501 (2013). 7

[120] G. Tóth, "Entanglement witnesses in spin models," *Phys. Rev. A* **71**, 010301 (2005). 7

[121] A. M. C. Souza and F. A. G. Almeida, "Thermal entanglement witness for materials with variable local spin lengths," *Phys. Rev. A* **79**, 052337 (2009).

[122] A. N. Ribeiro and C. A. Macedo, "Thermal entanglement witness for interacting itinerant fermion systems," *Phys. Rev. A* **86**, 022320 (2012).

[123] T. Chakraborty, T. K. Sen, H. Singh, D. Das, S. K. Mandal, and C. Mitra, "Experimental detection of thermal entanglement in a molecular chain," *J. Appl. Phys.* **114**, 144904 (2013). 7

[124] M. Krenn, M. Huber, R. Fickler, R. Lapkiewicz, S. Ramelow, and A. Zeilinger, "Generation and confirmation of a (100 x 100)-dimensional entangled quantum system," *Proc. Natl. Acad. Sci.* **111**, 6243-6247 (2014). 8

[125] Z. Huang, L. Maccone, A. Karim, C. Macchiavello, R. J. Chapman, and A. Peruzzo, "High-dimensional entanglement certification," *Sci. Rep.* **6**, 27637 (2016).

[126] D.-S. Ding, W. Zhang, S. Shi, Z.-Y. Zhou, Y. Li, B.-S. Shi, and G.-C. Guo, "High-dimensional entanglement between distant atomic-ensemble memories," *Light-Sci. Appl.* **5**, e16157-e16157 (2016).

[127] G. A. Howland, S. H. Knarr, J. Schneeloch, D. J. Lum, and J. C. Howell, "Compressively characterizing high-dimensional entangled states with complementary, random filtering," *Phys. Rev. X* **6**, 021018 (2016). 8

[128] F. G. S. L. Brandão, "Quantifying entanglement with witness operators," *Phys. Rev. A* **72**, 022310 (2005). 8

[129] J. Eisert, F. G. S. L. Brandão, and K. M. R. Audenaert, "Quantitative entanglement witnesses," *New J. Phys.* **9**, 46-46 (2007). 34, 98, 157

[130] O. Gühne, M. Reimpell, and R. F. Werner, "Lower bounds on entanglement measures from incomplete information," *Phys. Rev. A* **77**, 052317 (2008).

[131] M. Cianciaruso, T. R. Bromley, and G. Adesso, "Accessible quantification of multiparticle entanglement," *npj Quantum Inf.* **2**, 16030 (2016). 8

[132] C. Branciard, D. Rosset, Y.-C. Liang, and N. Gisin, "Measurement-device-independent entanglement witnesses for all entangled quantum states," *Phys. Rev. Lett.* **110**, 060405 (2013). 8, 147

[133] P. Xu, X. Yuan, L.-K. Chen, H. Lu, X.-C. Yao, X. Ma, Y.-A. Chen, and J.-W. Pan, "Implementation of a measurement-device-independent entanglement witness," *Phys. Rev. Lett.* **112**, 140506 (2014).

[134] M. Nawareg, S. Muhammad, E. Amselem, and M. Bourennane, "Experimental measurement-device-independent entanglement detection," *Sci. Rep.* **5**, 8048 (2015).

[135] E. Verbanis, A. Martin, D. Rosset, C. C. W. Lim, R. T. Thew, and H. Zbinden, "Resource-efficient measurement-device-independent entanglement witness," *Phys. Rev. Lett.* **116**, 190501 (2016). 8, 147

REFERENCES

[136] M. Bourennane, M. Eibl, C. Kurtsiefer, S. Gaertner, H. Weinfurter, O. Gühne, P. Hyllus, D. Bruß, M. Lewenstein, and A. Sanpera, "Experimental detection of multipartite entanglement using witness operators," *Phys. Rev. Lett.* **92**, 087902 (2004). 8, 92

[137] G. Tóth and O. Gühne, "Entanglement detection in the stabilizer formalism," *Phys. Rev. A* **72**, 022340 (2005). 8, 92, 93, 94, 104, 106

[138] G. Tóth and O. Gühne, "Detecting genuine multipartite entanglement with two local measurements," *Phys. Rev. Lett.* **94**, 060501 (2005). 8, 92, 93, 94, 106

[139] F. Shahandeh, M. Ringbauer, J. C. Loredo, and T. C. Ralph, "Ultrafine entanglement witnessing," *Phys. Rev. Lett.* **118**, 110502 (2017). 8

[140] Y.-C. Liang, D. Rosset, J.-D. Bancal, G. Pütz, T. J. Barnea, and N. Gisin, "Family of bell-like inequalities as device-independent witnesses for entanglement depth," *Phys. Rev. Lett.* **114**, 190401 (2015). 8, 90

[141] Q. Zhao, X. Yuan, and X. Ma, "Efficient measurement-device-independent detection of multipartite entanglement structure," *Phys. Rev. A* **94**, 012343 (2016). 8, 90

[142] J. Sperling and W. Vogel, "Multipartite entanglement witnesses," *Phys. Rev. Lett.* **111**, 110503 (2013). 8, 90

[143] J. Sperling and W. Vogel, "Determination of the schmidt number," *Phys. Rev. A* **83**, 042315 (2011). 8, 90

[144] M. Huber and J. I. de Vicente, "Structure of multidimensional entanglement in multipartite systems," *Phys. Rev. Lett.* **110**, 030501 (2013).

[145] F. Shahandeh, J. Sperling, and W. Vogel, "Structural quantification of entanglement," *Phys. Rev. Lett.* **113**, 260502 (2014). 8, 90

[146] T. D. Ladd, F. Jelezko, R. Laflamme, Y. Nakamura, C. Monroe, and J. L. O'Brien, "Quantum computers," *Nature* **464**, 45-53 (2010). 8, 29

[147] M. Lewenstein, A. Sanpera, V. Ahufinger, B. Damski, A. Sen(De), and U. Sen, "Ultracold atomic gases in optical lattices: mimicking condens. matter phys. and beyond," *Adv. Phys.* **56**, 243-379 (2007). 8

[148] L. Amico, R. Fazio, A. Osterloh, and V. Vedral, "Entanglement in many-body systems," *Rev. Mod. Phys.* **80**, 517-576 (2008). 8

[149] G. De las Cuevas, "A quantum information approach to statistical mechanics," *J. Phys. B* **46**, 243001 (2013). 8

[150] C. T. Chubb and S. T. Flammia, "Statistical mechanical models for quantum codes with correlated noise,". 9, 49

[151] M. H. Zarei and A. Montakhab, "Phase transition in a noisy kitaev toric code model," *Phys. Rev. A* **99**, 052312 (2019). 8

[152] M. Van den Nest, W. Dür, and H. J. Briegel, "Completeness of the classical 2d ising model and universal quantum computation," *Phys. Rev. Lett.* **100**, 110501 (2008). 8

[153] G. De las Cuevas, W. Dür, H. J. Briegel, and M. A. Martín-Delgado, "Unifying all classical spin models in a lattice gauge theory," *Phys. Rev. Lett.* **102**, 230502 (2009).

[154] Y. Xu, G. De las Cuevas, W. Dür, H. J. Briegel, and M. A. Martín-Delgado, "TheU(1) lattice gauge theory universally connects all classical models with continuous variables, including background gravity," *J. Stat. Mech-Theory E* **2011**, P02013 (2011).

[155] G. De las Cuevas and T. S. Cubitt, "Simple universal models capture all classical spin physics," *Science* **351**, 1180-1183 (2016). 8

[156] M. V. den Nest, W. Dür, and H. J. Briegel, "Classical spin models and the quantum-stabilizer formalism," *Phys. Rev. Lett.* **98**, 117207 (2007). 8

[157] "Quantum algorithms for classical lattice models," *New J. Phys.* **13**, 093021 (2011).

REFERENCES

[158] J. Geraci and D. A. Lidar, "On the exact evaluation of certain instances of the potts partition function by quantum computers," *Commun. Math. Phys.* **279**, 735-768 (2008).

[159] D. A. Lidar and O. Biham, "Simulating ising spin glasses on a quantum computer," *Phys. Rev. E* **56**, 3661-3681 (1997).

[160] R. D. Somma, C. D. Batista, and G. Ortiz, "Quantum approach to classical statistical mechanics," *Phys. Rev. Lett.* **99**, 030603 (2007). 8

[161] J. Geraci and D. A. Lidar, "Classical ising model test for quantum circuits," *New J. Phys.* **12**, 075026 (2010). 8

[162] S. S. Jahromi, S. F. Masoudi, M. Kargarian, and K. P. Schmidt, "Quantum phase transitions out of a $z_2 \times z_2$ topological phase," *Phys. Rev. B* **88**, 214411 (2013). 9

[163] M. H. Zarei and A. Montakhab, "Dual correspondence between classical spin models and quantum Calderbank-Shor-Steane states," *Phys. Rev. A* **98**, 1-9 (2018). 9

[164] A. Kitaev, "Fault-tolerant quantum computation by anyons," *Ann. Phys.* **303**, 2-30 (2003). 9

[165] H. Bombín and M. A. Martín-Delgado, "Topological computation without braiding," *Phys. Rev. Lett.* **98**, 160502 (2007). 9

[166] E. Dennis, A. Kitaev, A. Landahl, and J. Preskill, "Topological quantum memory," *J. Math. Phys.* **43**, 4452-4505 (2002). 9, 49

[167] H. G. Katzgraber, H. Bombín, and M. A. Martín-Delgado, "Error threshold for color codes and random three-body Ising models," *Phys. Rev. Lett.* **103**, 090501 (2009). 9, 53

[168] T. Ohno, G. Arakawa, I. Ichinose, and T. Matsui, "Phase structure of the random-plaquette Z_2 gauge model: accuracy threshold for a toric quantum memory," *Nucl. Phys. B* **697**, 462-480 (2004). 9, 49

[169] R. S. Andrist, H. G. Katzgraber, H. Bombín, and M. A. Martín-Delgado, "Tricolored lattice gauge theory with randomness: fault tolerance in topological color codes," *New J. of Phys.* **13**, 083006 (2011). 9, 53

[170] M. Kafatos, *Bell's Theorem, Quantum Theory and Conceptions of the Universe.* Kluwer Academic Publishers, (1989). 17

[171] D. Gottesman, "Stabilizer codes and quantum error correction," *ArXiv e-prints* `quant-ph/9705052` (1997). 19, 21, 147

[172] D. Fattal, T. S. Cubitt, Y. Yamamoto, S. Bravyi, and I. L. Chuang, "Entanglement in the stabilizer formalism," *ArXiv e-prints* `quant-ph/0406168` (2004). 21

[173] D. Gottesman and I. L. Chuang, "Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations," *Nature* **402**, 390-393 (1999). 21

[174] M. Van den Nest, J. Dehaene, and B. De Moor, "Graphical description of the action of local clifford transformations on graph states," *Phys. Rev. A* **69**, 022316 (2004). 21, 23, 26, 30, 91, 110, 119, 124, 130, 166

[175] R. Raussendorf and H. J. Briegel, "A one-way quantum computer," *Phys. Rev. Lett.* **86**, 5188-5191 (2001). 22

[176] R. Raussendorf, D. E. Browne, and H. J. Briegel, "Measurement-based quantum computation on cluster states," *Phys. Rev. A* **68**, 022312 (2003). 22, 91

[177] M. Hein, W. Dür, J. Eisert, R. Raussendorf, M. V. den Nest, and H. J. Briegel, "Entanglement in graph states and its applications," *ArXiv e-prints* `quant-ph/0602096` (2006). 22, 23, 25, 26, 29, 30, 91, 113, 124, 126, 130

[178] M. Hein, J. Eisert, and H. J. Briegel, "Multiparty entanglement in graph states," *Phys. Rev. A* **69**, 062311 (2004). 23

[179] I. M. Georgescu, S. Ashhab, and F. Nori, "Quantum simulation," *Rev. Mod. Phys.* **86**, 153-185 (2014). 29

REFERENCES

[180] A. Ibort, V. I. Man'ko, G. Marmo, A. Simoni, and F. Ventriglia, "An introduction to the tomographic picture of quantum mechanics," *Phys. Scripta* **79**, 065013 (2009). 30

[181] A. I. Lvovsky and M. G. Raymer, "Continuous-variable optical quantum-state tomography," *Rev. Mod. Phys.* **81**, 299-332 (2009). 30

[182] F. Verstraete, M. Popp, and J. I. Cirac, "Entanglement versus correlations in spin systems," *Phys. Rev. Lett.* **92**, 027901 (2004). 30, 91, 130, 146

[183] M. Popp, F. Verstraete, M. A. Martín-Delgado, and J. I. Cirac, "Localizable entanglement," *Phys. Rev. A* **71**, 042306 (2005). 30, 91, 146

[184] D. Sadhukhan, S. S. Roy, A. K. Pal, D. Rakshit, A. Sen(De), and U. Sen, "Multipartite entanglement accumulation in quantum states: Localizable generalized geometric measure," *Phys. Rev. A* **95**, 022301 (2017). 30

[185] F. Verstraete, M. A. Martín-Delgado, and J. I. Cirac, "Diverging entanglement length in gapped quantum spin systems," *Phys. Rev. Lett.* **92**, 087201 (2004). 30, 91, 146

[186] B.-Q. Jin and V. E. Korepin, "Localizable entanglement in antiferromagnetic spin chains," *Phys. Rev. A* **69**, 062314 (2004). 30, 91, 130, 146

[187] S. O. Skrøvseth and S. D. Bartlett, "Phase transitions and localizable entanglement in cluster-state spin chains with ising couplings and local fields," *Phys. Rev. A* **80**, 022316 (2009). 30, 91

[188] P. Smacchia, L. Amico, P. Facchi, R. Fazio, G. Florio, S. Pascazio, and V. Vedral, "Statistical mechanics of the cluster ising model," *Phys. Rev. A* **84**, 022304 (2011). 30, 91

[189] S. Montes and A. Hamma, "Phase diagram and quench dynamics of the cluster-xy spin chain," *Phys. Rev. E* **86**, 021101 (2012). 30, 91

[190] A. Acín, J. I. Cirac, and M. Lewenstein, "Entanglement percolation in quantum networks," *Nat. Phys.* **3**, 256-259 (2007). 30, 91, 130

[191] J. Eisert and H. J. Briegel, "Schmidt measure as a tool for quantifying multiparticle entanglement," *Phys. Rev. A* **64**, 022306 (2001). 32

[192] A. Peres, "Separability Criterion for Density Matrices," *Phys. Rev. Lett.* **77**, 1413-1415 (1996). 33

[193] M. Horodecki, P. Horodecki, and R. Horodecki, "Separability of mixed states: necessary and sufficient conditions," *Phys. Lett. A* **223**, 1-8 (1996). 33

[194] C. Gardiner and P. Zoller, *Quantum Noise: A Handbook of Markovian and Non-Markovian Quantum Stochastic Methods with Applications to Quantum Optics.* Springer Series in Synergetics. Springer, (2004). 35

[195] S. J. Devitt, W. J. Munro, and K. Nemoto, "Quantum error correction for beginners," *Rep. Progr. Phys.* **76**, 076001 (2013). 35, 91

[196] C. H. Bennett, D. P. DiVincenzo, and J. A. Smolin, "Capacities of quantum erasure channels," *Phys. Rev. Lett.* **78**, 3217-3220 (1997). 37, 55, 71, 87

[197] A. Almheiri, X. Dong, and D. Harlow, "Bulk locality and quantum error correction in ads/cft," *J. High Energy Phys.* **2015**, 163 (2015). 37

[198] F. Pastawski, B. Yoshida, D. Harlow, and J. Preskill, "Holographic quantum error-correcting codes: toy models for the bulk/boundary correspondence," *J. High Energy Phys.* **2015**, 149 (2015). 37

[199] B. M. Terhal, "Quantum error correction for quantum memories," *Rev. Mod. Phys.* **87**, 307-346 (2015). 39

[200] J. O'Gorman and E. T. Campbell, "Quantum computation with realistic magic-state factories," *Phys. Rev. A* **95**, 032338 (2017). 40, 145

[201] C. Gidney and A. G. Fowler, "Efficient magic state factories with a catalyzed $|CCZ\rangle$ to $2|T\rangle$ transformation," *Quantum* **3**, 135 (2019). 40, 145

[202] H. Poulsen Nautrup, N. Friis, and H. J. Briegel, "Fault-tolerant interface between quantum memories and quantum processors," *Nat. Commun.* **8**, 1321 (2017). 40, 145

REFERENCES

[203] B. Eastin and E. Knill, "Restrictions on transversal encoded quantum gate sets," *Phys. Rev. Lett.* **102**, 110502 (Mar, 2009). 40

[204] C. Monroe, R. Raussendorf, A. Ruthven, K. R. Brown, P. Maunz, L.-M. Duan, and J. Kim, "Large-scale modular quantum-computer architecture with atomic memory and photonic interconnects," *Phys. Rev. A* **89**, 022317 (Feb, 2014). 41

[205] M. R. Geller and Z. Zhou, "Efficient error models for fault-tolerant architectures and the pauli twirling approximation," *Phys. Rev. A* **88**, 012314 (2013). 45

[206] M. Gutiérrez, C. Smith, L. Lulushi, S. Janardan, and K. R. Brown, "Errors and pseudothresholds for incoherent and coherent noise," *Phys. Rev. A* **94**, 042338 (Oct, 2016). 45

[207] R. Barends *et al.*, "Superconducting quantum circuits at the surface code threshold for fault tolerance," *Nature* **508**, 500-503 (2014). 47

[208] D. Browne, "Topological Codes and Computation," *Lecture notes* (2014). https://sites.google.com/site/danbrowneucl/teaching/lectures-on-topological-codes-and-quantum-computation. 48

[209] C. Horsman, A. G. Fowler, S. Devitt, and R. V. Meter, "Surface code quantum computing by lattice surgery," *New J. Phys.* **14**, 123011 (Dec, 2012). 49

[210] A. M. Steane, "Error correcting codes in quantum theory," *Phys. Rev. Lett.* **77**, 793-797 (1996). 52, 94

[211] D. P. DiVincenzo and P. Aliferis, "Effective fault-tolerant quantum computation with slow measurements," *Phys. Rev. Lett.* **98**, 020501 (2007). 53

[212] C. Chamberland and M. E. Beverland, "Flag fault-tolerant error correction with arbitrary distance codes," *Quantum* **2**, 53 (Feb., 2018). 53

[213] X. Feng, Y. Deng, and H. W. J. Blöte, "Percolation transitions in two dimensions," *Phys. Rev. E* **78**, 031136 (2008). 56, 65

[214] D. Stauffer, *Introduction to percolation theory.* Taylor & Francis, Lodon, (1985). 65, 69

[215] E. Pednault, J. A. Gunnels, G. Nannicini, L. Horesh, T. Magerlein, E. Solomonik, E. W. Draeger, E. T. Holland, and R. Wisnieff, "Breaking the 49-Qubit Barrier in the Simulation of Quantum Circuits," *ArXiv e-prints* `1710.05867` (2017). 89

[216] E. Alba, G. Tóth, and J. J. García-Ripoll, "Mapping the spatial distribution of entanglement in optical lattices," *Phys. Rev. A* **82**, 062321 (2010). 90, 91, 94, 111, 112

[217] D. Sadhukhan, S. S. Roy, A. K. Pal, D. Rakshit, A. Sen(De), and U. Sen, "Multipartite entanglement accumulation in quantum states: Localizable generalized geometric measure," *Phys. Rev. A* **95**, 022301 (2017). 91

[218] S. T. Flammia and Y.-K. Liu, "Direct fidelity estimation from few pauli measurements," *Phys. Rev. Lett.* **106**, 230501 (2011). 92

[219] A. R. Calderbank and P. W. Shor, "Good quantum error-correcting codes exist," *Phys. Rev. A* **54**, 1098-1105 (1996). 94

[220] O. Gühne, M. Reimpell, and R. F. Werner, "Estimating entanglement measures in experiments," *Phys. Rev. Lett.* **98**, 110502 (2007). 98

[221] A. Bermudez, X. Xu, R. Nigmatullin, J. O'Gorman, V. Negnevitsky, P. Schindler, T. Monz, U. G. Poschinger, C. Hempel, J. Home, F. Schmidt-Kaler, M. Biercuk, R. Blatt, S. Benjamin, and M. Müller, "Assessing the progress of trapped-ion processors towards fault-tolerant quantum computation," *Phys. Rev. X* **7**, 041061 (2017). 119, 144

[222] N. Lang and H. P. Büchler, "Minimal instances for toric code ground states," *Phys. Rev. A* **86**, 022336 (2012). 119, 120, 136

[223] "Quantum computing report." `https://quantumcomputingreport.com/players/`. Accessed: 2020-01-10. 143

[224] "Ibm quantum experience." `https://quantum-computing.ibm.com/`. Accessed: 2020-01-10. 143

REFERENCES

[225] "Rigetti quantum computing systems." `https://www.rigetti.com/systems`. Accessed: 2020-01-10.

[226] ""quantum in the cloud", university of bristol." `http://www.bristol.ac.uk/physics/research/quantum/engagement/qcloud/`. Accessed: 2020-01-10. 143

[227] S. Ruder, "An overview of gradient descent optimization algorithms," *ArXiv e-prints* `1609.04747` (2016). 144

[228] P. Schindler, J. T. Barreiro, T. Monz, V. Nebendahl, D. Nigg, M. Chwalla, M. Hennrich, and R. Blatt, "Experimental repetitive quantum error correction," *Science* **332**, 1059-1061 (2011). 144

[229] M. Takita, A. W. Cross, A. D. Córcoles, J. M. Chow, and J. M. Gambetta, "Experimental demonstration of fault-tolerant state preparation with superconducting qubits," *Phys. Rev. Lett.* **119**, 180501 (2017). 144

[230] P. H. Leung and K. R. Brown, "Entangling an arbitrary pair of qubits in a long ion crystal," *Phys. Rev. A* **98**, (2018). 144

[231] S. Perseguers, G. J. Lapeyre, D. Cavalcanti, M. Lewenstein, and A. Acín, "Distribution of entanglement in large-scale quantum networks," *Rep. Prog. Phys.* **76**, 096001 (Sep, 2013). 147

[232] A. Osterloh, "Entanglement and its facets in condensed matter systems,". 147