Computing Haar Measures

Arno Pauly

Swansea University, UK
http://www.cs.swan.ac.uk/~cspauly/
arno.m.pauly@gmail.com

Dongseong Seon

KAIST, Daejeon, Republic of Korea
instigation@kaist.ac.kr

Martin Ziegler

KAIST, Daejeon, Republic of Korea
http://ziegler.theoryofcomputation.asia/
ziegler@kaist.ac.kr

Abstract

According to Haar's Theorem, every compact topological group G admits a unique (regular, right and) left-invariant Borel probability measure μ_G. Let the *Haar integral* (of G) denote the functional $\int_G : \mathcal{C}(G) \ni f \mapsto \int f \, d\mu_G$ integrating any continuous function $f : G \to \mathbb{R}$ with respect to μ_G. This generalizes, and recovers for the additive group $G = [0;1) \mod 1$, the usual Riemann integral: computable (cmp. Weihrauch 2000, Theorem 6.4.1), and of computational cost characterizing complexity class $\#\mathsf{P}_1$ (cmp. Ko 1991, Theorem 5.32).

We establish that in fact, every computably compact computable metric group renders the Haar measure/integral computable: once using an elegant synthetic argument, exploiting uniqueness in a computably compact space of probability measures; and once presenting and analyzing an explicit, imperative algorithm based on "maximum packings" with rigorous error bounds and guaranteed convergence. Regarding computational complexity, for the groups $\mathcal{SO}(3)$ and $\mathcal{SU}(2)$, we reduce the Haar integral to and from Euclidean/Riemann integration. In particular both also characterize $\#\mathsf{P}_1$.

2012 ACM Subject Classification Theory of computation → Constructive mathematics; Mathematics of computing → Continuous mathematics

Keywords and phrases Computable analysis, topological groups, exact real arithmetic, Haar measure

Digital Object Identifier 10.4230/LIPIcs.CSL.2020.34

Related Version A full version of this work (including additional results and omitted proofs) is available at http://arxiv.org/abs/1906.12220.

Supplement Material The source code of the implementation in Section 6.1 is available at http://github.com/realcomputation/irramplus/tree/master/HAAR

Funding Supported by the National Research Foundation of Korea (grant NRF-2017R1E 1A1A03071032), by the International Research & Development Program of the Korean Ministry of Science and ICT (grant NRF-2016K1A3A7A03950702), and by the European Union's Horizon 2020 MSCA IRSES project 731143.

1 Motivation and Overview

Complementing empirical approaches, heuristics, and recipes [26, 28], Computable Analysis [35] provides a rigorous algorithmic foundation to Numerics, as well as a way of formally measuring the constructive contents of theorems in classical Calculus. Haar's Theorem is such an example, of particular beauty combining three categories: compact metric spaces, algebraic groups, and measure spaces:

28th EACSL Annual Conference on Computer Science Logic (CSL 2020).
Editors: Maribel Fernández and Anca Muscholl; Article No. 34; pp. 34:1–34:17
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

▶ **Fact 1.** Let $(G, e, \circ, \cdot^{-1})$ denote a group and (G, d) a compact metric space such that the group operation $\circ$ and inverse operation $\cdot^{-1}$ are continuous with respect to d (that is, form a topological group). There exists a unique left-invariant Borel probability measure μ_G, called Haar measure, on G. Moreover, μ_G is right-invariant and regular.

We refrain from expanding on generalizations to locally-compact Hausdorff spaces. Recall that a left-invariant measure satisfies $\mu(U) = \mu(g \circ U)$ for every $g \in G$ and every measurable $U \subseteq G$. For the additive group $[0;1) \mod 1$, its Haar measure recovers the standard Lebesgue measure λ, corresponding to the angular measure divided by 2π on the complex unit circle group $\mathcal{U}(1) \cong \mathcal{SO}(2)$.

Each of the categories involved in Fact 1 has a standard computable strengthening, cmp. [34, 30, 5]; and our first main result establishes them to combine nicely:

▶ **Theorem 2.** *Let $\mathbf{X}$ be a computably compact computable metric space with a computable group operation $\circ : \mathbf{X} \times \mathbf{X} \to \mathbf{X}$. Then the corresponding Haar measure μ is computable.*

That the Haar measure is computable means that we can approximate the measure of any given open subset of $\mathbf{X}$ from below, and implies that we can compute the integral of any given continuous function from $\mathbf{X}$ into $\mathbb{R}$.

In contrast, recall that other classical results in Calculus, such as Brouwer's Fixed Point Theorem [19, 2] or Peano's Theorem [27], do not carry over to computability that nicely. And also common classical "constructive" existence proofs of the Haar measure [11, §58] do employ limits without rate of convergence, well-known since Specker [31, 32] to possibly leave the computable realm:

▶ **Fact 3.** For non-empty $A, B \subseteq X$ let $[A : B]$ denote the least number of left translates of B that cover A. Then $\mu(A) = \lim_B \frac{[A:B]}{[X:B]}$ holds for every compact $A \subseteq X$, where the limit exists in the sense of a net of open neighborhoods B of e.

In addition to the possibly uncomputable limit, the *least integer* defining $[A : B]$ depends discontinuously and uncomputably on the underlying data A, B.

We establish Theorem 2 with elegant arguments following the "synthetic" (i.e. implicit, functional) approach to Computable Analysis developed in [21]. It follows the following general strategy [7] (also explained in [21, Section 9]) for proving computability of some object Ω living in an admissibly represented space by three steps:

I) Obtain a definition of Ω as the element of a computably closed set.
II) Obtain a computably compact set containing Ω.
III) Find a classical proof that (I) and (II) uniquely determine Ω.

As warm-up let us illustrate this approach to assert computability of the group unit e from the hypothesis of Theorem 2: For any fixed computable element $a \in G$, (I) e belongs to the computably closed set $\{y : a \circ y = a\}$ and (II) to the compact set $\Omega = X$ and (III) is uniquely determined by (I) and (II). Similarly, for every $x \in G$, its inverse x^{-1} (I) belongs to $\{y : x \circ y = e\}$ and (II) to the compact set $\Omega = X$ and (III) is uniquely defined by $x \circ x^{-1} = e$. Note that this proof does not immediately yield an algorithm computing e or $x \mapsto x^{-1}$.

In this spirit, Section 3 establishes Theorem 2. The challenge consists in (I) obtaining a computable definition of the Haar measure μ: The inequality $\tilde{\mu}(U) \neq \tilde{\mu}(xU)$ expressing a candidate measure $\tilde{u}$ to violate invariance is not even recognizable, since $\tilde{\mu}(U)$ is in general only a lower real. Subsection 3.1 avoids that by allowing to consider pairs of sets in Lemma 12. Section 4 complements Section 3 by devising and analyzing an explicit, imperative algorithm for computing Haar integrals $\mathcal{C}(f) \mapsto \int_X f \, d\mu$. It is based on "maximal packings": finite sets $T_n \subseteq X$ of points with pairwise distance $> 2^{-n}$. Intuitively, the ratio $|T_n \cap A|/|T_n|$ of those points contained in a given set A should approximate its measure $\mu(A)$; however, rigorously, this is wrong – and counting is uncomputable anyway. Subsections 4.1 and 4.2 describe a combination of mathematical and algorithmic approaches that avoid these obstacles. The superficially different hypotheses to Sections 4 and 3 are compared in Section 5. There we also give some examples showing that these requirements are not dispensable; and analyze which information of a compact metric group determines its Haar measure.

Having thus asserted computability, the natural next question is for efficiency. We consider here the non-uniform computational cost of the *Haar integral* functional

$$\int_G \; : \; \mathcal{C}(G) \;\ni\; f \;\mapsto\; \int f \, d\mu_G \;\in\; \mathbb{R} \tag{1}$$

integrating continuous real functions $f : G \to \mathbb{R}$. For the arguably most important additive groups $G = [0;1)^d \bmod 1$ with Lebesgue measure λ^d, this amounts to Euclidean/Riemann integration – whose complexity had been shown to characterize the discrete class $\#\mathsf{P}_1$ [14, Theorem 5.32] cmp. [8, 33]: indicating that standard quadrature methods, although taking runtime exponential in n to achieve guaranteed absolute output error 2^{-n}, are likely optimal. And Section 6 extends this numerical characterization of $\#\mathsf{P}_1$ to the arguably next-most important compact metric groups:

▶ **Theorem 4.** *Let G denote any of the following compact groups, considered as subsets of Euclidean space and equipped with the intrinsic/path metric:*
- **i)** *$\mathcal{SO}(3) \subseteq \mathbb{R}^9$ of orthogonal real 3×3 matrices of determinant 1,*
- **ii)** *$\mathcal{O}(3) \subseteq \mathbb{R}^9$ of orthogonal real 3×3 matrices,*
- **iii)** *$\mathcal{SU}(2) \subseteq \mathbb{R}^8$ of unitary complex 2×2 matrices of determinant 1,*
- **iv)** *$\mathcal{U}(2) \subseteq \mathbb{R}^8$ of unitary complex 2×2 matrices.*

- **a)** *For every polynomial-time computable $f \in \mathcal{C}(G)$, $\int_G f \in \mathbb{R}$ is computable in polynomial space (and exponential time).*
- **b)** *If $\mathsf{FP}_1 = \#\mathsf{P}_1$ and $f \in \mathcal{C}(G)$ is polynomial-time computable, then so is $\int_G f \in \mathbb{R}$.*
- **c)** *There exists a polynomial-time computable $f \in \mathcal{C}(G)$ such that polynomial-time computability of $\int_G f \in \mathbb{R}$ implies $\mathsf{FP}_1 = \#\mathsf{P}_1$.*

The proof of this result proceeds by mutual polynomial-time continuous (i.e. Weihrauch) reduction from and to Euclidean/Riemann integration. Subsection 6.1 describes our implementation and empirical evaluation of rigorous integration on $\mathcal{SU}(2)$ in the `iRRAM` C++ library.

2 Background

In the following, we give a brief introduction to the key notions from computable analysis we need. For a formal treatment, we refer to [21]. Further standard references for Computable Analysis are [35, 1].

Computable analysis is concerned with *represented spaces*, which equip a set with a notion of computability by coding its elements as infinite binary sequences. We have various constructions of new represented spaces available, and use in particular the derived spaces $\mathcal{O}(\mathbf{X})$ of open subsets of $\mathbf{X}$ (characterized by making membership recognizable) and $\mathcal{C}(\mathbf{X}, \mathbf{Y})$ of continuous functions from $\mathbf{X}$ to $\mathbf{Y}$, characterized by making function evaluation computable.

Computable compactness and computable overtness of a space are characterized by making universal and existential quantification preserve computable open predicates. We also use that admissibility of a space means that from a compact singleton we can extract the point [29]. A space is computably Hausdorff, if inequality is semidecidable. It is computably separable, if it has a computable dense sequence. Being computably separable implies being computably overt.

A particular convenient class of represented space are the computable metric spaces (CMS). We can start with a designated dense sequence on which the metric is computable (given indices), and then represent arbitrary points as limits of fast converging sequences. CMSs are in particular computably Hausdorff and computably separable. The prototypic example of a CMS are the reals $\mathbb{R}$. We write *CCCMS* for *computably compact computable metric space.*

There is a further relevant represented space with the reals as underlying set, namely the space of lower reals $\mathbb{R}$. Here a real is represented as the supremum of a sequence of rational numbers (without any limitation on convergence rates). This space is relevant for us as we can introduce the computability structure of the space of (probability) measures on an arbitrary represented space $\mathbf{X}$ by considering them as the subspace of $\mathcal{C}(\mathcal{O}(\mathbf{X}), \mathbb{R}_<)$ of functions satisfying the properties of a (probability) measure. More precisely, these correspond to continuous valuations. Let $\mathcal{PM}(\mathbf{X})$ denotes the space of probability measures on $\mathbf{X}$.

A useful theorem is that for a CCCMS $\mathbf{X}$, also $\mathcal{PM}(\mathbf{X})$ is a CCCMS. Here we can use the *Wasserstein-Kantorovich-Rubinstein* metric

$$W(\mu,\nu) \;=\; \sup\Big\{ \Big| \int f\,d\mu - \int f\,d\nu \Big| \;:\; f : X \to \mathbb{R},\; \forall x, y \in X :\; |f(x) - f(y)| \le d(x,y) \Big\}$$

If $\mathbf{X}$ a complete metric space, $\mathcal{PM}(\mathbf{X})$ is again a complete metric space; and convergence w.r.t. W is equivalent to weak convergence. For an introduction to computable probability theory, see [4]. Some further results are found in [24].

Regarding computational complexity of real numbers and real functions on compact metric spaces, we refer to [14] and [13].

Recall that $\#\mathsf{P}_1$ is the class of all integer functions $\varphi : \{\mathtt{0}\}^* \to \mathbb{N}$ with unary arguments counting the number of witnesses

$$\varphi(\mathtt{0}^n) \;=\; \mathrm{Card}\,\big\{ \vec{w} \in \{\mathtt{0},\mathtt{1}\}^{\mathrm{poly}(n)} : \mathtt{0}^n\,\mathtt{1}\,\vec{w} \in P \big\}$$

to a polynomial-time decidable predicate $P \subseteq \{\mathtt{0},\mathtt{1}\}^*$; a class commonly conjectured to lie strictly between (the integer function versions of) NP_1 and PSPACE [20, §18].

3 The Haar measure is computable

In this section we shall establish Theorem 2 using the approach to computable analysis via synthetic topology [6] outlined in [21]. To this end, we first obtain a more technical result stating that left-invariance of a Radon probability measure for some continuous binary operation constitutes a computably closed predicate:

▶ **Theorem 5.** *Let $\mathbf{X}$ be a computable metric space. For $\mu \in \mathcal{PM}(\mathbf{X})$ and $g \in \mathcal{C}(\mathbf{X} \times \mathbf{X}, \mathbf{X})$ the following predicate is computably closed:*

$$\forall U \in \mathcal{O}(\mathbf{X}),\; \forall x \in \mathbf{X}\;\; \mu(U) = \mu(\{y \in \mathbf{X}\;\, g(x,y) \in U\})$$

In view of the general strategy for computability proofs from Section 1, this establishes (I). Regarding (II) recall [9, §2.5] that, if $\mathbf{X}$ is a computably compact computable metric space, then so is $\mathcal{PM}(\mathbf{X})$. Finally, uniqueness in Haar's theorem takes care of Condition (III).

3.1 Disjoint pairs of open sets

Prima facie, the condition in Theorem 5 appears to be complicated. As measures of open sets are only available as lower reals, we cannot even recognize inequality. The workaround consists in considering pairs of disjoint open sets rather than individual open sets. We shall see that quantification over such pairs is unproblematic for the spaces we are interested in here.

Given a represented space $\mathbf{X}$, we define the space $\mathrm{DPO}(\mathbf{X})$ as the subspace $\{(U, V) \mid U \cap V = \emptyset\} \subseteq \mathcal{O}(\mathbf{X}) \times \mathcal{O}(\mathbf{X})$.

▶ **Observation 6.** $\mathbf{X}$ is computably overt iff $\mathrm{DPO}(\mathbf{X})$ is a computable element of $\mathcal{A}(\mathcal{O}(\mathbf{X}) \times \mathcal{O}(\mathbf{X}))$.

Proof. If $\mathbf{X}$ is computably overt, then $U \cap V \neq \emptyset$ is a recognizable property given $(U, V) \in \mathcal{O}(\mathbf{X}) \times \mathcal{O}(\mathbf{X})$. Conversely, we find that $(U, X) \notin \mathrm{DPO}(\mathbf{X})$ iff $U \neq \emptyset$. ◀

▶ **Corollary 7.** *If $\mathbf{X}$ is computably overt, then $\mathrm{DPO}(\mathbf{X})$ is computably compact.*

Proof. The space $\mathcal{O}(\mathbf{X})$ is computably compact, as it contains $\emptyset$ as a computable bottom element. Then $\mathcal{O}(\mathbf{X}) \times \mathcal{O}(\mathbf{X})$ is computably compact as a product, and finally the claim follows by noting that a computably closed subspace of a computably compact space is computably compact and invoking Observation 6. ◀

▶ **Lemma 8.** *If $\mathbf{X}$ is computably separable, effectively countably based and computably Hausdorff, then $\mathrm{DPO}(\mathbf{X})$ is a computable element of $\mathcal{V}(\mathcal{O}(\mathbf{X}) \times \mathcal{O}(\mathbf{X}))$.*

Proof. It is shown in [25] that under the given conditions, we can obtain an adequate formal disjointness notion on basic open sets. We can then obtain a dense sequence in $\mathrm{DPO}(\mathbf{X})$ by constructing pairs of finite unions of basic open sets with the additional requirements that each basic open set is formally disjoint from all basic open sets listed in the opposite finite union. ◀

▶ **Corollary 9.** *If $\mathbf{X}$ is computably separable, effectively countably based and computably Hausdorff, then $\mathrm{DPO}(\mathbf{X})$ is computably compact and computably overt.*

▶ **Definition 10.** *Given $f \in \mathcal{C}(\mathbf{X}, \mathbf{X})$, $(U, V) \in \mathrm{DPO}(\mathbf{X})$ and $\mu \in \mathcal{PM}(\mathbf{X})$, we say that (U, V) is μ-invariant under f, iff:*

$$\mu(U) + \mu(f^{-1}(V)) \leq 1$$

▶ **Observation 11.** (U, V) being μ-invariant under f is a computably closed property.

▶ **Lemma 12.** *Let $\mathbf{X}$ be computably separable, effectively countably based and computably Hausdorff. Then* "all pairs from $\mathrm{DPO}(\mathbf{X})$ are μ-invariant under f" *is a computably closed property in $\mu \in \mathcal{PM}(\mathbf{X})$ and $f \in \mathcal{C}(\mathbf{X}, \mathbf{X})$.*

Proof. Computably closed properties are closed under universal quantification over computably overt sets. So we just combine Observation 11 and Corollary 9. ◀

3.2 Proof of Theorem 5

To be able to invoke the results of the previous subsection we need to relate invariance of disjoint pairs of open sets to invariance of individual open sets.

▶ **Lemma 13.** *For a computable metric space $\mathbf{X}$, $\mu \in \mathcal{PM}(\mathbf{X})$ and $f \in \mathcal{C}(\mathbf{X}, \mathbf{X})$ the following are equivalent:*

1. *All pairs from* $\mathrm{DPO}(\mathbf{X})$ *are μ-invariant under f.*
2. *For all $U \in \mathcal{O}(\mathbf{X})$ it holds that $\mu(U) = \mu(f^{-1}(U))$.*

Proof. 2. implies

$$\mu(U) \;+\; \mu\big(f^{-1}(V)\big) \;=\; \mu\big(f^{-1}(U)\big) \;+\; \mu\big(f^{-1}(V)\big) \stackrel{(*)}{=} \mu\big(f^{-1}(U) \cup f^{-1}(V)\big) \;\leq\; 1$$

with $(*)$ since $f^{-1}(U)$ and $f^{-1}(V)$ are disjoint.

For the converse, assume that U witnesses that f is not invariant, i.e. $\mu(U) \neq \mu(f^{-1}(U))$. We shall argue that this implies the existence of a disjoint pair of open sets which is not μ-invariant under f. Let $\delta = \frac{1}{3}|\mu(U) - \mu(f^{-1}(U))|$. Consider the sets $B_{-\varepsilon}(U) = \{x \in \mathbf{X} \mid d(x, U^C) > \varepsilon\}$. Since $U = \bigcup_{\varepsilon>0} B_{-\varepsilon}(U)$ is a nested union and f is continuous, we find that $\mu(U) = \sup_{\varepsilon>0} \mu(B_{-\varepsilon}(U))$ and $\mu(f^{-1}(U)) = \sup_{\varepsilon>0} \mu(f^{-1}(B_{-\varepsilon}(U)))$. Consequently, there exists some ε_0 such that for all $\varepsilon < \varepsilon_0$ it holds that $|\mu(U) - \mu(B_{-\varepsilon}(U))| < \delta$ and $|\mu(f^{-1}(U)) - \mu(f^{-1}(B_{-\varepsilon}(U)))| < \delta$.

Next, consider the sets $D_{-\varepsilon}(U) := \{x \in \mathbf{X} \mid d(x, U^C) = \varepsilon\}$. Since for different ε these sets are disjoint, we know that for only countably many ε can it hold that $\mu(D_{-\varepsilon}(U)) > 0$. The sets $f^{-1}(D_{-\varepsilon}(U))$ are disjoint, too, and thus the same argument applies. We can thus select some $\varepsilon_1 < \varepsilon_0$ such that $\mu(D_{-\varepsilon_1}(U)) = \mu(f^{-1}(D_{-\varepsilon_1}(U))) = 0$. This ensures that $\mu(B_{-\varepsilon_1}(U)) + \mu((B_{-\varepsilon_1}(U)^C)^\circ) = 1$ and $\mu(f^{-1}(B_{-\varepsilon_1}(U))) + \mu(f^{-1}((B_{-\varepsilon_1}(U))^C)^\circ) = 1$. Moreover, we know that $|\mu(B_{-\varepsilon_1}(U)) - \mu(f^{-1}(B_{-\varepsilon_1}(U)))| > \delta$ from $\varepsilon_1 < \varepsilon_0$, so depending on the sign of the difference, either $(B_{-\varepsilon_1}(U), (B_{-\varepsilon_1}(U)^C)^\circ)$ or $((B_{-\varepsilon_1}(U)^C)^\circ, B_{-\varepsilon_1}(U))$ is not μ-invariant under f. ◀

Proof of Theorem 5. By Lemma 13 we can replace the invariance for open sets by invariance for disjoint pairs of open sets. By Lemma 12, this is a computably closed property for each fixed choice of continuous function $y \mapsto g(x, y)$. The additional universal quantification over the computably overt space $\mathbf{X}$ preserves being a computably closed predicate. ◀

4 Explicit computation of the Haar measure

The synthetic arguments from Section 3 establishing computability (Theorem 2) do not immediately exhibit an actual algorithm. To this end, the present section takes a more explicit approach. Its assumptions superficially differ but will be shown equivalent (in a sense to be formalized) in Section 5. Among others, we suppose computability of the *size of maximum packings*. This is a notion asymptotically related to, yet in detail (maximum packing vs. minimum covering, open vs. closed balls) subtly different from, Kolmogorov's metric entropy [16], to the *separation bound* from [36, Definition 6.2], and to the *capacity* from [13, Definition 12]. All three notions can be regarded as integer Skolemizations (i.e. *moduli*) of total boundedness [15, Def 17.106].

▶ **Definition 14.** *For any compact metric space (X, d) and its subset $U \subseteq X$,*

1. *$T \subseteq U$ is called an n*-packing *of U if $\forall x, y \in T (x \neq y) \to d(x, y) > 2^{-n}$.*
2. *An n-packing T is* maximum *if $|T| \geq |S|$ for every n-packing S of U.*

3. $\{T_n\}_{n=1}^{\infty}$ *is a* sequence *of maximum packings if each T_n is a maximum n-packing.*
4. $\kappa_U : \mathbb{N} \to \mathbb{N}$ *is the* size *of maximum packings of U if $\kappa_U(n) = |T_n|$ where T_n is a maximum n-packing.*

If $U = X$, the term "of U" is omitted.

Our definition features strict inequality of pairwise distances: this asserts that a maximum n-packing T_n can be found algorithmically by exhaustive search, provided that its size is given/computable.

▶ **Theorem 15.** *Let (X, d) be a computable metric space and $(X, e, \circ, \cdot^{-1})$ a compact topological group. Suppose that the metric d is bi-invariant:*

$$\forall a, b, c \in X : \ d(a \circ c, b \circ c) = d(a, b) = d(c \circ a, c \circ b)$$

And suppose that the size of maximum packings $\kappa_X : \mathbb{N} \to \mathbb{N}$ is computable. Then the Haar integral $\mathcal{C}(X) \ni f \mapsto \int_X f \, d\mu$ is computable.

Recall [35, §8.1] that a computable metric space (X, d) comes with a dense sequence $\xi : \mathbb{N} \to X$ such that the real double sequence $d : \mathbb{N} \times \mathbb{N} \ni (a, b) \mapsto d\big(\xi(a), \xi(b)\big)$ is computable. Note that, as opposed to Theorem 2, we do not suppose the group operation $\circ$ (nor neutral element nor inversion) to be computable but instead require the metric to be bi-invariant. See Section 5 for a comparison between the different hypotheses.

4.1 Mathematical Estimates of Haar Measures

Invariance of both metric d and Haar measure μ implies that the content $\mu(B)$ of an open ball $B = B_r(c)$ depends only on its radius r, but not on its center c. Intuitively, for a sufficiently large maximum packing T, said volume should be approximated by the ratio of points in B to the total number of points (Definition 18). If $B_r(c)$ contains significantly smaller a fraction, then by double counting some other $B_r(c')$ would need to "compensate" with a larger fraction, hence invariance suggests that more points can be added to T at $B(r, c)$ as well, contradicting maximality. Lemma 17 below formalizes this idea both in its statement and proof.

▶ **Definition 16.** *For a metric space (X, d) and its subset $U \subseteq X$, we introduce the outer generalized closed ball as $\overline{B}_r(U) := \{x \in X \mid d(x, U) \leq r\}$. Similarly, the inner generalized closed ball is introduced as $\overline{B}_{-r}(U) = \{x \in X : d(x, U^c) \geq r\}$.*

For $0 \leq r, s$ it holds

$$\overline{B}_{+r}(\overline{B}_{-r}(U)) \ \subseteq \ \overline{U} \ \subseteq \ \overline{B}_{-r}(\overline{B}_{+r}(U)), \qquad \overline{B}_{+r}(\overline{B}_{+s}(U)) \ \subseteq \ \overline{B}_{+r+s}(U) \tag{2}$$

▶ **Lemma 17.** *Suppose $(X, d, \circ)$ is a compact topological group with bi-invariant metric d and a maximum n-packing T_n of size $\kappa_X(n)$. Then for any $x \in X$ and measurable $U \subseteq X$ it holds:*

$$\kappa_{\overline{B}_{-2^{-n}}(U)}(n) \leq |T_n \cap xU| \leq \kappa_{\overline{B}_{2^{-n}}(U)}(n)$$

▶ **Definition 18.** *Abbreviate $\mu_T := \frac{1}{|T|} \sum_{p \in T} \delta_p$ where δ_p denotes the Dirac measure.*

▶ **Lemma 19.** *Let $(X, d, \circ)$ be a compact topological group with bi-invariant metric d and Haar measure μ, and T_n a maximum n-packing. Then for any $U \subseteq X$:*

$$\mu\big(\overline{B}_{-2^{-n+2}}(U)\big) \ \leq \ \mu_{T_n}\big(\overline{B}_{-2^{-n+1}}(U)\big) \ \leq \ \mu(U) \ \leq \ \mu_{T_n}\big(\overline{B}_{2^{-n+1}}(U)\big) \ \leq \ \mu\big(\overline{B}_{2^{-n+2}}(U)\big)$$

For the illustration of Lemma 19, see Figure 1.

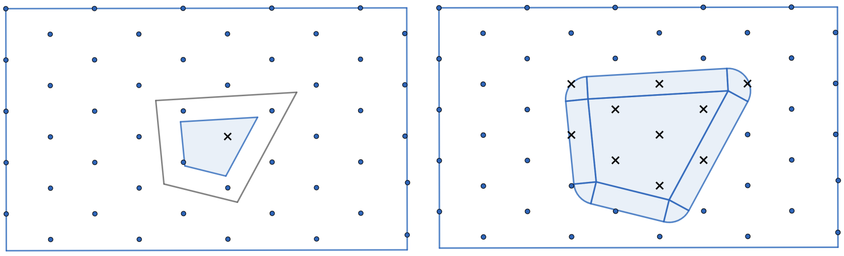

Figure 1 Illustration of Lemma 19. A blue rectangle represents the space. Blue points represent the maximum n-packing. A black shape represents U. Blue colored shapes represent inner and outer generalized balls. Counting cross-marked points and dividing it by the number of (any) points gives $\mu_{T_n}\left(\overline{B}_{-2^{-n+1}}(U)\right)$ and $\mu_{T_n}\left(\overline{B}_{2^{-n+1}}(U)\right)$.

4.2 Algorithmic Approximation of Haar Measures

Our strategy to compute $\mu(U)$ with Lemma 19 is to compute μ_{T_n} and assert that the sequence of intervals $\left\{\ \left[\ \mu_{T_n}\left(\overline{B}_{-2^{-n+1}}(U)\right),\ \mu_{T_n}\left(\overline{B}_{2^{-n+1}}(U)\right)\ \right]\ \right\}_{n=1}^{\infty}$ include $\mu(U)$, and that its length converges to zero. However, there are two obstacles:

1. μ_T is discrete (i.e. the value of $\mu_T(U)$ can jump even by a small perturbation to U), which makes it uncomputable.
2. If $\lim_{r\to 0}\mu(\overline{B}_r(U)) = \mu(U)$, then Lemma 19 guarantees that the length of the interval converges. However, the hypothesis may not hold in general.

This section works around these obstacles and gives an algorithm that can compute the measure of sufficiently rich a class of sets to perform the integration.

The first thing to address is μ_T. It is not computable, but procedure `pseudoCount` below can bound its measure on closed sets whose distances to any given points is computable. The latter condition is known as being (Turing-) located [10]:

▶ **Definition 20.** *A closed subset S of a computable metric space (X, d) is* located *if the continuous function $X \ni p \mapsto d(p, S) \in \mathbb{R}$ is computable.*

Located sets are sometimes called computably closed sets, but being located is different from being a computable element of $\mathcal{A}(X)$.

Our workaround to the second obstacle is, instead of trying to compute the measure of every closed set, to effectively "approximate" the given set by those satisfying the convergence condition and to compute their measure. Let us define such sets first:

▶ **Definition 21.** *On a topological space (X, τ) with a Borel measure μ, call a measurable set U* co-inner regular *iff*

$$\mu(U) \;=\; \sup\left\{\mu(V) \mid V \subseteq U \text{ open and measurable}\right\} \;.$$

On a compact metric group $(X, d, \circ)$ with the Haar measure μ where d is bi-invariant, a real number $r > 0$ is a co-inner regular radius *iff for some/all $p \in X$, the ball $\overline{B}_r(p)$ is co-inner regular.*

Indeed, invariance of d and μ implies that $\overline{B}_r(p)$ is co-inner regular iff $\overline{B}_r(q)$ is. Note that since Haar measures are regular, on a compact metric group with a bi-invariant metric and a Haar measure, if a set U is co-inner regular, then $\mu(\partial U) = 0$, giving $\lim_{r\to 0}\mu(\overline{B}_r(U)) = \mu(U)$.

▶ **Lemma 22.** *Let $(X, d, \circ)$ be a compact topological group with bi-invariant metric d, Haar measure μ, and computable size κ_X of maximum packings. If the closure of U is located and co-inner regular, then the procedure* `computeMeasure` *computes its measure $\mu(U)$.*

Procedure computeMeasure(U, $\{T_m\}_{m=1}^{\infty}$, n).

Data: $\overline{U}$ located co-inner regular set, $\{T_m\}_{m=1}^{\infty}$ computable sequence of maximum packings, n target precision
Result: A rational number q s.t. $|q - \mu(S)| \leq 2^{-n}$.

```
error ← ∞;
m ← 0;
while error > 2^{-n} do
    r ← 2^{-m};
    a ← pseudoCount(B̄_{-r}(Ū), T_m, m+1);
    b ← pseudoCount(B̄_{r/2}(Ū), T_m, m+1);
    error ← b − a ;
    m ← m + 1;
end
return any p ∈ interval
```

Procedure pseudoCount(S, T, n).

Data: S a located set, T a finite set of points, n error parameter, `dist`(p, S, m) approximate distance between $p \in T$ and S up to 2^{-m}.
Result: A rational q where $\mu_T(S) \leq q \leq \mu_T(\overline{B}_{2^{-n}}(S))$

```
count ← 0;
foreach p ∈ T do
    if dist(p,S,n+2) < 2^{-n-1} then
        count ← count + 1;
    end
end
return count/|T|
```

Note that `computeMeasure` in turn calls `pseudoCount`(p, S, n).

Not every closed ball is co-inner regular, but "sufficiently" many are: Co-inner regular radii can be effectively found to compute Haar measures in the form of the Haar integral by `findCoInnerRegularRadius`. Figure 2 illustrates the procedure `findCoInnerRegularRadius`. $\lambda x.$`findCoInnerRegularRadius`$(a, b, \{T_m\}_{m=1}^{\infty}, x)$ is a nested sequence of intervals that converges to a co-inner regular radius. `findCoInnerRegularRadius` achieves this by recursively dividing and outputting the interval. That is, `findCoInnerRegularRadius`$(a, b, \{T_m\}_{m=1}^{\infty}, n)$ first computes the $(n-1)$-th interval (`findCoInnerRegularRadius`$(a, b, \{T_m\}_{m=1}^{\infty}, n-1)$) and outputs the n-th interval by dividing it. The procedure divides the $(n-1)$-th interval into two parts $[r_1, r_5]$ and $[r_5, r_9]$, computes corresponding measures $\mu(\overline{B}_{r_1}), \mu(\overline{B}_{r_5}), \mu(\overline{B}_{r_9})$, and picks the interval which has smaller difference of measures. In this case, since $\mu(\overline{B}_{r_5}) - \mu(\overline{B}_{r_1}) \leq \mu(\overline{B}_{r_9}) - \mu(\overline{B}_{r_5})$, $[r_1, r_5]$ is picked. This strategy makes the difference of measures converges to zero since it is always, at least, halved on each iterations. This gives a co-inner regular radius, because in fact co-inner regular radii are continuity points of the function $r \mapsto \mu(\overline{B}_r)$.

▶ **Lemma 23.** *Procedure* `findCoInnerRegularRadius` *computes a co-inner regular radius in the form of* $\lambda x.$`findCoInnerRegularRadius`$(a, b, \{T_m\}_{m=1}^{\infty}, x)$.

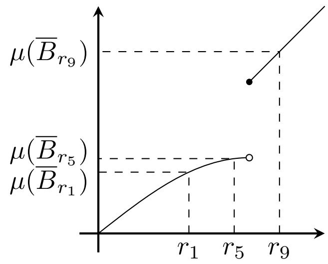

Figure 2 Illustration of procedure `findCoInnerRegularRadius`. Here, an example graph of the discontinuous function $r \mapsto \mu(\overline{B}_r)$ is shown. Note that $\mu(\overline{B}_r(p)) = \mu(\overline{B}_r(q))$ because of the invariance of the metric and the Haar measure.

Procedure findCoInnerRegularRadius$(a, b, \{T_m\}_{m=1}^{\infty}, n)$.

Data: $a < b$ rational bounds between which to look for a co-inner regular radius, $\{T_m\}_{m=1}^{\infty}$ sequence of maximum packings, n target precision.
Result: Rational bounds a_n, b_n s.t. $(a < a_{n-1} < a_n < b_n < b_{n-1} < b) \wedge (b_n - a_n \leq 2^{-n}) \wedge |\mu(\overline{B}_{a_n}(p)) - \mu(\overline{B}_{b_n}(p))| \leq 2^{-n}$ for any/all $p \in X$.
$(a_{n-1}, b_{n-1}) \leftarrow$ `findCoInnerRegularRadius`$(a, b, \{T_m\}_{m=1}^{\infty}, n-1)$;
$r_1, r_5, r_9 \leftarrow \frac{9a_{n-1}+1b_{n-1}}{10}, \frac{5a_{n-1}+5b_{n-1}}{10}, \frac{1a_{n-1}+9b_{n-1}}{10}$;
Pick sufficiently large N s.t. $2^{-N+2} \leq \frac{b_{n-1}-a_{n-1}}{10}$;
Compute an element $p \in X$ using the fact that X is a computable metric space;
$m_1, m_5, m_9 \leftarrow$ `pseudoCount`$(\overline{B}_{r_1}(p), T_N, N)$, `pseudoCount`$(\overline{B}_{r_5}(p), T_N, N)$, `pseudoCount`$(\overline{B}_{r_9}(p), T_N, N)$;
$\epsilon \leftarrow \frac{b_{n-1}-a_{n-1}}{10}$;
if $m_9 - m_5 \leq m_5 - m_1$ **then return** $[r_1 + \epsilon, r_5 - \epsilon]$ **else return** $[r_5 + \epsilon, r_9 - \epsilon]$;

Proof. $\lambda x.$`findCoInnerRegularRadius`$(a, b, \{T_m\}_{m=1}^{\infty}, x)$ represents $r := \lim_{n\to\infty} a_n$, where a_n is the first element of the interval that `findCoInnerRegularRadius` outputs. r is a co-inner regular radius because the fact $r \in (a_n, b_n)$ makes $\partial\overline{B}_r(p) \subseteq \overline{B}_{b_n}(p) \setminus \overline{B}_{a_n}(p)$, which leads to $\mu(\partial\overline{B}_r(p)) \leq |\mu(\overline{B}_{b_n}(p)) - \mu(\overline{B}_{a_n}(p))| \leq 2^{-n}$ for any n. This implies $\mu(\partial\overline{B}_r(p)) = 0$.

Now it is sufficient to prove the postconditions. Let us only prove $\mu(\overline{B}_{a_n}(p)) - \mu(\overline{B}_{b_n}(p)) \leq 2^{-n}$, since others are straightforward. Let $r_i := \frac{ia_{n-1}+(10-i)b_{n-1}}{10}$ and $m_i := \mu(\overline{B}_{r_i}(p))$. Because of Lemma 19 and the fact that N is sufficiently large, $\mu(\overline{B}_{r_i}(p)) \leq \mu_{T_N}(\overline{B}_{r_{i+1}}(p)) \leq m_{i+1} \leq \mu_{T_N}(\overline{B}_{r_{i+1}+2^{-N}}(p)) \leq \mu(\overline{B}_{r_{i+2}}(p))$. Then since $2^{-n+1} \geq |\mu(\overline{B}_{a_{n-1}}(p)) - \mu(\overline{B}_{b_{n-1}}(p))| \geq |m_9 - m_1| \geq |m_9 - m_5| + |m_5 - m_1|$, WLOG $|m_5 - m_1| \leq 2^{-n}$. Then $|\mu(\overline{B}_{r_5-\epsilon}(p)) - \mu(\overline{B}_{r_1+\epsilon}(p))| \leq |m_5 - m_1| \leq 2^{-n}$. ◀

4.3 Main Algorithm for Haar Integration

Explicit algorithm of Theorem 15. The procedure `computeIntegral` computes the Haar integral $\int_X f\, d\mu$. Generalizing classical Riemann sums, it partitions X into subsets U_i, $i \leq N$, of sufficiently small diameter (see Figure 3): given by a modulus of continuity such that f on each U_i varies by at most 2^{-n}. Then it sums those values of $f|_{U_i}$, each weighted by the measure of U_i. In order to invoke `computeMeasure`, we want the U_i to be located and co-inner regular: as provided by `findNicePartition`. Specifically, each U_i will be of the form $U_i = \overline{B}_R(p_i) \setminus \bigcup_{j<i} \overline{B}_R(p_j)$ for $p_1, \ldots, p_N \in T_m$ and real $R > 0$ provided by `findCoInnerRegularRadius`.

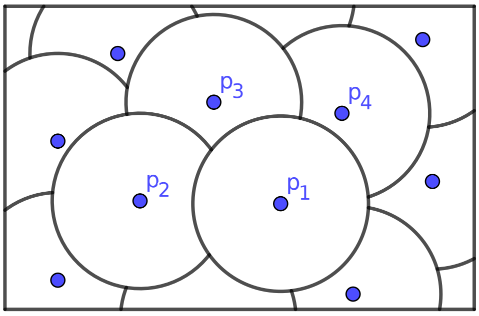

Figure 3 Consider the whole rectangle as the whole space. Then this is how the procedure `computeIntegral` partitions the space. For example, the subset containing p_1 is $\overline{B}_R(p_1)$. Similarly, the subset containing p_2 is $\overline{B}_R(p_2) \setminus \overline{B}_R(p_1)$, the subset containing p_3 is $\overline{B}_R(p_3) \setminus (\overline{B}_R(p_1) \cup \overline{B}_R(p_2))$, and so on. Then the subsets of the partition are of the form $\overline{B}_R(p_i) \setminus \bigcup_{j<i} \overline{B}_R(p_j)$.

Procedure computeIntegral(f, $\{T_m\}_{m=1}^{\infty}$, n).

Data: real function f, sequence of maximum packings $\{T_m\}_{m=1}^{\infty}$, target precision n
Result: a rational number q s.t. $|q - \int_X f d\mu| \le 2^{-n}$
$m_f \leftarrow$ `modulus(`f, $n+1$`)` ; `// modulus is from [14, Definition 2.12]`
$\{U_i\}_{i=1}^{N} \leftarrow$ `findNicePartition(`$\{T_m\}_{m=1}^{\infty}$, m_f`);`
$M \leftarrow$ `bound(`$|f|$`);`
foreach U_i *in* $\{U_i\}_{i=1}^{N}$ **do**
  $p_i \leftarrow$ `center(`U_i`);`
  $m_i \leftarrow$`computeMeasure(`U_i, $\{T_m\}_{m=1}^{\infty}$, $n+1+i+\log M$`);`
end
return $\sum_{i=1}^{N} m_i f(p_i)$

Recall the comment after Definition 14 that we may suppose a sequence T_m of maximum packings is given. ◀

5 Discussion of Hypotheses

While the requirements of Theorem 2 and Theorem 15 appear to be very different, it turns out that actually, both theorems are applicable in the very same cases.

For one direction, suppose we have a computably compact computable metric space $(\mathbf{X}, d)$ with a computable group operation $\circ$. Then[1]

$$d'(a,b) \ := \ \sup_{x\in\mathbf{X}} \sup_{y\in\mathbf{X}} d(x \circ a \circ y, x \circ b \circ y)$$

constitutes a topologically equivalent and also computable, but now bi-invariant, metric. The size of maximum packings may be non-computable for a CCCMS. However, for any CCCMS there is a computable sequence of radii converging to zero for which we can compute the maximum packings. It is straightforward to see that this suffices for Theorem 15. As such, we see that the requirements for Theorem 15 are implied by those of Theorem 2.

[1] We appreciate relevant discussion on MathOverflow [22].

Procedure findNicePartition($\{T_m\}_{m=1}^{\infty}$, n).

```
Data: {T_m}_{m=1}^∞ is a sequence of maximum packings, n is the target precision
Result: A partition P = {U_i}_{i=1}^N s.t. each closure(U_i) is a located co-inner regular set of the
        form U_i = B̄_R(p_i) \ ⋃_{j<i} B̄_R(p_j).
P ← {};
R ← λx. findCoInnerRegularRadius((2^{-n-1}, 2^{-n}), {T_m}_{m=1}^∞, x);
foreach p_i in T_{n+1} do
    U_i ← B̄_R(p_i) \ ⋃_{U∈P} U;
    P ← P ∪ {U_i};
end
return P
```

For the converse direction, note that Theorem 15 does not suppose the group operation $\circ$ (nor neutral element nor inversion) to be computable. Indeed, a group operation on a CCCMS can have a computable bi-invariant metric but fail to be computable itself. This is due to the potential for many different group operations to have the same bi-invariant metric:

▶ **Example 24.** Fix some $A \subseteq \mathbb{N}$. Let $G_n := IZ_{p_n^2}$ if $n \in A$, and let $G_n := \mathbb{Z}_{p_n} \times \mathbb{Z}_{p_n}$ if $n \notin A$, where p_n is the n-th prime. Note that both have cardinality p_n^2 but are not isomorphic as additive groups yet both have the same Haar measure under the bi-invariant discrete metric. Now let $G_A := \Pi_{n\in\mathbb{A}} G_n$, equipped with the Baire space metric. For $A \neq B$ we find that G_A and G_B are not homeomorphic. The group operation on G_A is computable iff A is decidable. However, both the bi-invariant metric structure on G_A and the Haar measure are all independent of A, and computable.

Interestingly, the Haar measure on a compact group is determined already by an invariant metric and independent of the potentially many different underlying group operations:

▶ **Corollary 25.** *Consider a compact metric space (X, d) with two group operations $\circ$ and $\circ'$ both rendering d left-invariant. Then $(X, \circ)$ and $(X, \circ')$ induce the same Haar measure.*

Proof. In the metric case, the net of neighborhoods B of e from Fact 3 becomes a sequence of open balls $B_{1/2^n}(e)$. Left-invariance implies that all translates $q \cdot B_r(e) = B_r(q)$ have the same measure; and by the group property, every open ball $B_r(q)$ is a translate of $B_r(e)$: for both $\circ$ and $\circ'$. In particular, $[X : B_{1/2^n}] = \kappa_X(n)$. ◀

On the other hand the collection of different group operations $\circ$ to a given bi-invariant metric d is “tame”:

▶ **Lemma 26.** *Let $(\mathbf{X}, d)$ be a CCCMS. The set $O \subseteq \mathcal{C}(\mathbf{X} \times \mathbf{X}, \mathbf{X})$ of group operations rendering d bi-invariant is a computably compact set.*

Proof. If d is bi-invariant for $\circ \in \mathcal{C}(\mathbf{X} \times \mathbf{X}, \mathbf{X})$, the triangle inequality gives

$$d(a \circ x, b \circ y) \;\leq\; d(a \circ x, b \circ x) \;+\; d(b \circ x, b \circ y) \;=\; d(a, b) + d(x, y) \leq 2d((a, x), (b, y)) \quad ;$$

rendering $\circ$ 2-Lipschitz with respect to the maximum metric on $\mathbf{X} \times \mathbf{X}$. By the effective Arzelà-Ascoli theorem, the subset of 2-Lipschitz $f \in \mathcal{C}(\mathbf{X} \times \mathbf{X}, \mathbf{X})$ is computably compact.

Within this set, we are interested in those satisfying the bi-invariance and group axioms:

$$\forall a,b,c: \quad d\big(f(c,a),f(c,b)\big) \;=\; d(a,b) \;=\; d\big(f(a,c),f(b,c)\big)$$
$$\exists e,a': \quad f(a,e)=a=f(e,a)\wedge f(f(a,b),c)=f(a,f(b,c))\wedge f(a,a')=e=f(a',a)$$

These are computably closed predicates since the quantification is over the computably compact and computably overt space $\mathbf{X}$. This ends the proof, since a computably closed subset of a computably compact set is computably compact. ◀

We can combine Corollary 25 and Lemma 26 to see that Theorem 5 also implies that from a CCCMS (X,d) such that some group operation is bi-invariant for d we can compute the Haar measure for any such group operation.

To conclude this section, we shall consider a family of examples that show that we need more computability requirements than that of the metric and of the group operation. We consider the closed subgroups of $(\mathbf{2}^{\mathbb{N}},\oplus)$, where $\oplus$ denotes the componentwise exclusive or. These subgroups are of the form

$$G_A := \{p\in\mathbf{2}^{\mathbb{N}} \mid \forall n\in A\ p(n)=0\}$$

for some $A\subseteq\mathbb{N}$. Each G_A inherits compactness, computable metrizability and the computability of the group operation from $(\mathbf{2}^{\mathbb{N}},\oplus)$.

G_A is computably compact iff A is c.e., and effectively separable (and thus a computable metric space) iff A is co-c.e. Now if we have the Haar measure μ_A on G_A, we can recover A since $\mu_A(\{p\in G_A \mid p(n)=1\})=\frac{1}{2}$ iff $n\notin A$ and $\mu_A(\{p\in G_A \mid p(n)=1\})=0$ iff $n\in A$. We thus see that G_A is a CCCMS iff μ_A is computable – so neither computable compactness or computable separability are dispensable for the computability of the Haar measure.

If we already have a bi-invariant metric, computable compactness is even necessary:

▶ **Theorem 27.** *Let $(\mathbf{X},d)$ be a computable metric space with computable probability measure μ such that $\mu(B_r(x))$ depends only on r but not on x. Then $\mathbf{X}$ is computably compact.*

6 Computational Complexity of the Haar Integral

We now move beyond mere computability of the Haar measure, and consider the computational complexity of this task for the groups $G=\mathcal{SO}(3)$, $G=\mathcal{O}(3)$, $G=\mathcal{SU}(2)$, and $G=\mathcal{U}(2)$. In each case, the complexity turns out to be closely related to the complexity class $\#\mathsf{P}_1$. We prove Theorem 4, namely

a) For every polynomial-time computable $f\in\mathcal{C}(G)$, $\int_G f\in\mathbb{R}$ is computable in polynomial space (and exponential time).
b) If $\mathsf{FP}_1=\#\mathsf{P}_1$ and $f\in\mathcal{C}(G)$ is polynomial-time computable, then so is $\int_G f\in\mathbb{R}$.
c) There exists a polynomial-time computable $f\in\mathcal{C}(G)$ such that polynomial-time computability of $\int_G f\in\mathbb{R}$ implies $\mathsf{FP}_1=\#\mathsf{P}_1$.

To this end recall [14, Theorem 5.32] that (a), (b), and (c) are known for definite Riemann integration

$$\mathcal{C}[0;1] \;\ni\; \tilde{f} \;\mapsto\; \int_0^1 \tilde{f}(t)\,dt \;\in\; \mathbb{R} \;.$$

Moreover, Item (c) remains true for $\tilde{f}\in\mathcal{C}_0^\infty[0;1]$: the class of smooth (infinitely often differentiable) $\tilde{f}:[0;1]\to\mathbb{R}$ such that $\tilde{f}(0)=0=\tilde{f}(1)$; cmp. [8, 33].

Before proceeding to the groups $\mathcal{SO}(3)$, $\mathcal{O}(3)$, $\mathcal{SU}(2)$, $\mathcal{U}(2)$, recall the argument for the case $\mathcal{U}(1) = \big\{ \exp(2\pi i t) : 0 \leq 1 \leq 1 \big\}$ equipped with complex multiplication and the Haar integral

$$\mathcal{C}\big(\mathcal{U}(1)\big) \ \ni \ f \ \mapsto \ \int_0^1 f\big(\exp(2\pi i t)\big)\, dt \quad :$$

So to see (c), consider the polynomial-time computable embedding

$$\mathcal{C}_0[0;1] \ \ni \ \tilde{f} \ \mapsto \ \big(\exp(2\pi i t) \mapsto \tilde{f}(t)\big) \ \in \ \mathcal{C}\big(\mathcal{U}(1)\big) \ .$$

And to see (a) and (b) for $G = \mathcal{U}(1)$, consider the polynomial-time computable embedding

$$\mathcal{C}\big(\mathcal{U}(1)\big) \ \ni \ f \ \mapsto \ \big(t \mapsto f(\exp(2\pi i t))\big) \ \in \ \mathcal{C}[0;1] \ .$$

This also covers $\mathcal{SO}(2) \cong \mathcal{U}(1)$; and integration over $\mathcal{O}(2) \cong \mathcal{SO}(2) \times \{\pm 1\}$ amounts to two integrals over $\mathcal{SO}(2)$.

Let $\mathbb{H} = \{\alpha + i\beta + j\gamma + k\delta : \alpha, \beta, \gamma, \delta \in \mathbb{R}\}$ denote the quaternions, parameterized as real quadruples with respect to units $1, i, j, k$. The group $\mathcal{SU}(2)$ is well-known, and easily verified to be, isomorphic to the multiplicative group $\mathbb{H}_1$ of quaternions of norm 1 (aka *versors*) via isomorphism

$$\mathbb{H}_1 \ \ni \ \alpha + i\beta + j\gamma + k\delta \ \mapsto \ \begin{pmatrix} \alpha + i\beta & -\gamma + i\delta \\ \gamma + i\delta & \alpha - i\beta \end{pmatrix} \ \in \ \mathcal{SU}(2) \tag{3}$$

with $|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1$. Reparameterize $\mathbb{H}_1$ in generalized spherical coordinates

$$\begin{aligned} &[0;\pi) \times [0;\pi) \times [0;2\pi) \ \ni \ (\eta, \vartheta, \varphi) \ \mapsto \ \Psi(\eta, \vartheta, \varphi) \ := \\ &\qquad \cos(\eta) + i\sin(\eta)\cos(\vartheta) + j\sin(\eta)\sin(\vartheta)\cos(\varphi) + k\sin(\eta)\sin(\vartheta)\sin(\varphi) \ \in \ \mathbb{H}_1 \end{aligned}$$

with Jacobian determinant $\big|\det\big(\Psi'(\eta, \vartheta, \varphi)\big)\big| = \sin^2(\eta)\sin(\vartheta)$, and verify that integration by change-of-variables

$$\mathcal{C}(\mathbb{H}_1) \ \ni \ f \ \mapsto \ \int_0^{2\pi} \int_0^{\pi} \int_0^{\pi} f\big(\Psi(\eta, \vartheta, \varphi)\big) \cdot |\det \Psi'(\eta, \vartheta, \varphi)|\, d\eta\, d\vartheta\, d\varphi \tag{4}$$

is left-invariant, hence must coincide with the Haar integral on $\mathcal{SU}(2)$. Items (a) and (b) thus follow by polynomial-time reduction to Euclidean/Riemann integration according to Equation (4). And Item (c) follows by polynomial-time embedding

$$\begin{aligned} &\mathcal{C}\big(\mathcal{U}(1)\big) \ \ni \ f \ \mapsto \ \tilde{f} \ \in \ \mathcal{C}(\mathbb{H}_1) \ \cong \ \mathcal{C}\big(\mathcal{SU}(2)\big), \quad \text{where} \\ &\tilde{f} \ : \ \mathbb{H}_1 \ \ni \ \alpha + i\beta + j\gamma + k\delta \mapsto f\big((\alpha + i\beta)/\sqrt{\alpha^2 + \beta^2}\big) \cdot \sqrt{\alpha^2 + \beta^2} \ \in \ \mathbb{R} \ . \end{aligned}$$

Since continuous f on compact $\mathbb{H}_1$ is bounded, $f\big((\alpha + i\beta)/\sqrt{\alpha^2 + \beta^2}\big) \cdot \sqrt{\alpha^2 + \beta^2} \to 0$ as $\alpha^2 + \beta^2 \searrow 0$. Hence $\tilde{f}$ is indeed well-defined and remains polynomial-time computable by continuous extension also for $\alpha^2 + \beta^2 = 0$.

$\mathcal{SO}(3)$ is doubly-covered by $\mathbb{H}_1$, identifying $q \in \mathbb{H}_1$ with special orthogonal linear map

$$\mathbb{R}^3 \ \ni \ (\beta, \gamma, \delta) \ \mapsto \ (\beta', \gamma', \delta') \ : \ i\beta' + j\gamma' + k\delta' \overset{!}{=} \big(q \cdot (i\beta + j\gamma + k\delta) \cdot q^{-1}\big) \ .$$

Moreover $\mathcal{O}(3) \cong \mathcal{SO}(3) \times \{\pm 1\}$ and $\mathcal{U}(2) \cong \mathcal{SU}(2) \times \mathcal{U}(1)$. ◀

6.1 Implementation and Evaluation

Based on the above reduction to ordinary Riemann integration, we have implemented integration on $\mathcal{SU}(2)$ in the `iRRAM` C++ library [18]. The source code is available at `http://github.com/realcomputation/irramplus/tree/master/HAAR`. Its empirical evaluation produced the following timing results:

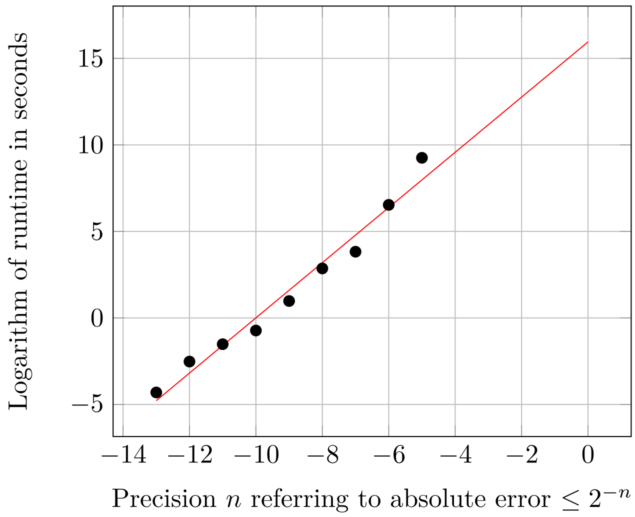

Figure 4 Empirical evaluation of rigorous integration on $\mathcal{SU}(2)$.

Specifically, we chose the Lipschitz-continuous function $\mathbb{H}_1 \ni w + xi + yj + zk \mapsto |w| + |x| + |y| + |z| \in \mathbb{R}$ to integrate with*out* letting the algorithm exploit its particular symbolic form and symmetry. Time measurements were performed on the virtual machine that has Ubuntu 64-bit with 4 cores and 8GB RAM by VMware Workstation 15 Player. The underlying computer has Intel(R) Core(TM) i7-7700K CPU 4.20GHz and 16GB RAM. Execution time for each precision is the average execution time of 5 executions.

Note that the y-axis records the *logarithm* of the execution time in seconds. This time is confirmed to grow exponentially with the output precision parameter n: as expected for a $\#\mathsf{P}_1$-complete problem.

7 Conclusion and Future Work

We have devised a computable version of Haar's Theorem: proven once using the elegant synthetic (implicit) approach and once developing and analyzing an explicit, imperative algorithm. And we have established the computational complexity of the Haar integral to characterize $\#\mathsf{P}_1$ for each of the compact groups $\mathcal{U}(1), \mathcal{U}(2), \mathcal{O}(2), \mathcal{O}(3), \mathcal{SU}(2), \mathcal{SO}(3)$. Moreover, we implemented the algorithm for $\mathcal{SU}(2)$ in *Exact Real Computation* [3] and confirmed that the experiment coincides with the complexity theorem. In fact, our proof shows them mutually second-order polynomial-time Weihrauch reducible [12].

Future work will generalize the above complexity considerations to $\mathcal{SO}(4)$, to $\mathcal{SO}(d)$, and to further classes of compact metric groups; and improve the implementation to achieve practical performance.

On the abstract side of our work, an immediate question is whether we can generalize from compact groups to locally compact groups (as was done for the classical Haar's theorem).

The price to pay for this generalization in the classic setting is that we no longer obtain a unique probability measure, but merely a locally finite measure identified up to a constant scaling factor. A notion of effective local compactness is available (see [23]), but any such generalization seems to require new proof techniques beyond those employed in this article. Recently, Davorin Lešnik has shown that this one can be done in synthetic topology, provided that one is willing to relax the requirement that measures take values in the lower reals to values in the Borel reals [17].

References

1 Vasco Brattka, Peter Hertling, and Klaus Weihrauch. A Tutorial on Computable Analysis. In S. Barry Cooper, Benedikt Löwe, and Andrea Sorbi, editors, *New Computational Paradigms: Changing Conceptions of What is Computable*, pages 425–491. Springer, New York, 2008. doi:10.1007/978-0-387-68546-5_18.

2 Vasco Brattka, Joseph Miller, Stéphane Le Roux, and Arno Pauly. Connected Choice and Brouwer's Fixed Point Theorem. *Journal for Mathematical Logic*, 2019. doi:10.1142/S0219061319500041.

3 Franz Brauße, Pieter Collins, Johannes Kanig, SunYoung Kim, Michal Konecny, Gyesik Lee, Norbert Müller, Eike Neumann, Sewon Park, Norbert Preining, and Martin Ziegler. Semantics, Logic, and Verification of "Exact Real Computation". *CoRR*, abs/1608.05787, 2016. arXiv:1608.05787.

4 Pieter Collins. Computable Stochastic Processes. *CoRR*, abs/1409.4667, 2014. arXiv:1409.4667.

5 Abbas Edalat. A computable approach to measure and integration theory. *Information and Computation*, 207(5):642–659, 2009. doi:10.1016/j.ic.2008.05.003.

6 Martín Escardó. Synthetic Topology of Data Types and Classical Spaces. *Electronic Notes in Theoretical Computer Science*, 87:21–165, 2004. doi:10.1016/j.entcs.2004.09.017.

7 Martín Escardó. Algorithmic solution of higher type equations. *J. Logic Comput.*, 23(4):839–854, 2013. doi:10.1093/logcom/exr048.

8 Hugo Férée and Martin Ziegler. On the Computational Complexity of Positive Linear Functionals on $C[0;1]$. In *Mathematical Aspects of Computer and Information Sciences - 6th International Conference, MACIS 2015, Berlin, Germany, November 11-13, 2015, Revised Selected Papers*, pages 489–504, 2015. doi:10.1007/978-3-319-32859-1_42.

9 Stefano Galatolo, Mathieu Hoyrup, and Cristobal Rojas. Dynamics and abstract computability: computing invariant measures. *Discrete Contin. Dyn. Syst.*, 29(1):193–212, 2011. doi:10.3934/dcds.2011.29.193.

10 Xiaolin Ge and Anil Nerode. On extreme points of convex compact Turing located set. In Anil Nerode and Yu. V. Matiyasevich, editors, *Logical Foundations of Computer Science*, pages 114–128, Berlin, Heidelberg, 1994. Springer Berlin Heidelberg.

11 Paul R. Halmos. *Measure Theory*, volume 018 of *GTM*. Springer, 1950. doi:10.1007/978-1-4684-9440-2.

12 Akitoshi Kawamura and Stephen A. Cook. Complexity Theory for Operators in Analysis. *TOCT*, 4(2):5:1–5:24, 2012. doi:10.1145/2189778.2189780.

13 Akitoshi Kawamura, Florian Steinberg, and Martin Ziegler. Complexity Theory of (Functions on) Compact Metric Spaces. In *Proc. 31st Ann. Symposium on Logic in Computer Science, LICS*, pages 837–846. ACM, 2016. doi:10.1145/2933575.2935311.

14 Ker-I Ko. *Complexity Theory of Real Functions*. Progress in Theoretical Computer Science. Birkhäuser, Boston, 1991. doi:10.1007/978-1-4684-6802-1.

15 Ulrich Kohlenbach. *Applied Proof Theory: Proof Interpretations and their Use in Mathematics*. Springer, Berlin, 2008. doi:10.1007/978-3-540-77533-1.

16 A.N. Kolmogorov and V.M. Tikhomirov. $\mathcal{E}$-Entropy and $\mathcal{E}$-Capacity of Sets in Functional Spaces. *Uspekhi Mat. Nauk*, 14(2):3–86, 1959. doi:10.1007/978-94-017-2973-4_7.

17 Davorin Lešnik. Haar Measure in Synthetic Topology. presentation at CCC 2019, 2019.

18 Norbert Th. Müller. The iRRAM: Exact Arithmetic in C++. In Jens Blanck, Vasco Brattka, and Peter Hertling, editors, *Computability and Complexity in Analysis*, volume 2064 of *Lecture Notes in Computer Science*, pages 222–252, Berlin, 2001. Springer. 4th International Workshop, CCA 2000, Swansea, UK, September 2000. `doi:10.1007/3-540-45335-0_14`.

19 Vladimir P. Orevkov. A constructive mapping of the square onto itself displacing every constructive point (Russian). *Doklady Akademii Nauk*, 152:55–58, 1963. translated in: Soviet Math. - Dokl., 4 (1963) 1253–1256.

20 Christos H. Papadimitriou. *Computational complexity*. Addison-Wesley, 1994.

21 Arno Pauly. On the topological aspects of the theory of represented spaces. *Computability*, 5(2):159–180, 2016. `doi:10.3233/COM-150049`.

22 Arno Pauly. Bi-invariant metrics on compact Polish group. MathOverflow, February 2019. URL: `https://mathoverflow.net/q/322668`.

23 Arno Pauly. Effective local compactness and the hyperspace of located sets. *CoRR*, abs/1903.05490, 2019. `arXiv:1903.05490`.

24 Arno Pauly and Willem Fouché. How constructive is constructing measures? *Journal of Logic & Analysis*, 9, 2017. `doi:10.4115/jla.2017.9.c3`.

25 Arno Pauly and Hideki Tsuiki. T^{ω}-representations of compact sets. *CoRR*, abs/1604.00258, 2016. `arXiv:1604.00258`.

26 Florian Pausinger. Uniformly distributed sequences in the orthogonal group and on the Grassmannian manifold. *Mathematics and Computers in Simulation*, 160:13–22, 2019. `doi:10.1016/j.matcom.2018.11.022`.

27 Marian B. Pour-El and J. Ian Richards. A computable ordinary differential equation which possesses no computable solution. *Annals Math. Logic*, 17:61–90, 1979. `doi:10.1016/0003-4843(79)90021-4`.

28 William H Press. *Numerical recipes: The art of scientific computing*. Cambridge university press, 2007.

29 Matthias Schröder. Admissible Representations in Computable Analysis. In A. Beckmann, U. Berger, B. Löwe, and J.V. Tucker, editors, *Logical Approaches to Computational Barriers*, volume 3988 of *Lecture Notes in Computer Science*, pages 471–480, Berlin, 2006. Springer. Second Conference on Computability in Europe, CiE 2006, Swansea, UK, June 30-July 5, 2006. `doi:10.1007/11780342_48`.

30 Matthias Schröder and Alex Simpson. Representing probability measures using probabilistic processes. *Journal of Complexity*, 22(6):768–782, 2006. `doi:10.1016/j.jco.2006.05.003`.

31 Ernst Specker. Nicht konstruktiv beweisbare Sätze der Analysis. *The Journal of Symbolic Logic*, 14(3):145–158, 1949. `doi:10.2307/2268459`.

32 Ernst Specker. Der Satz vom Maximum in der rekursiven Analysis. In A. Heyting, editor, *Constructivity in mathematics*, Studies in Logic and the Foundations of Mathematics, pages 254–265, Amsterdam, 1959. North-Holland. Proc. Colloq., Amsterdam, Aug. 26–31, 1957. `doi:10.1007/978-3-0348-9259-9_12`.

33 Florian Steinberg. Complexity theory for spaces of integrable functions. *Logical Methods in Computer Science*, Volume 13, Issue 3, September 2017. `doi:10.23638/LMCS-13(3:21)2017`.

34 Klaus Weihrauch. Computability on computable metric spaces. *Theoretical Computer Science*, 113:191–210, 1993. Fundamental Study. `doi:10.1016/0304-3975(93)90001-A`.

35 Klaus Weihrauch. *Computable Analysis*. Springer, Berlin, 2000. `doi:10.1007/978-3-642-56999-9`.

36 Klaus Weihrauch. Computational complexity on computable metric spaces. *Mathematical Logic Quarterly*, 49(1):3–21, 2003. `doi:10.1002/malq.200310001`.