Computability of Haar Integrals

Presenter: Dongseong Seon

KAIST, School of Computing

May 16, 2019

Background: Exact Real Computation

- floating point
  $\Rightarrow$ Cannot exactly represent real numbers
- Exact Real
  $\Rightarrow$ Represent $r \in \mathbb{R}$ with $\{q_n\}_{n=1}^{\infty}$ where $|r - q_n| \leq 2^{-n}$
- Compute a real number r
  $\Rightarrow$ Give an algorithm that computes $n \mapsto q_n$
- Compute a function $f : \mathbb{R} \to \mathbb{R}$
  $\Rightarrow$ Give an algorithm that computes $\{q_n\}_{n=1}^{\infty}, m \mapsto p_m$
  where $\{p_m\}_{m=1}^{\infty}$ is a representation of $f(x)$

Problem: motivation

Definition

For any measure space $(X, \mathcal{B}(X), \mu)$ with a Borel probability measure, **integral** means the functional $f \mapsto \int_X f d\mu : C(X) \to \mathbb{R}$.

Problem: motivation

Definition

For any measure space $(X, \mathcal{B}(X), \mu)$ with a Borel probability measure, **integral** means the functional $f \mapsto \int_X f d\mu : C(X) \to \mathbb{R}$.

Examples of computing integrals:

Example

Computing $f \mapsto \int_0^1 f(x)dx$

Problem: motivation

Definition

For any measure space $(X, \mathcal{B}(X), \mu)$ with a Borel probability measure, **integral** means the functional $f \mapsto \int_X f d\mu : C(X) \to \mathbb{R}$.

Examples of computing integrals:

Example

Computing $f \mapsto \int_0^1 f(x)dx$

Example (Matthias Schröder, Alex Simpson)

On some topological spaces, represent probability measures with probabilistic processes

Haar integral is an integral with a unique Haar probability measure

Problem: Haar's theorem

Haar's theorem

On any compact topological group, there exists the unique probability measure on the Borel subsets which is left-translation-invariant and regular.

- $\mu(g \circ S) = \mu(S)$

$\Rightarrow$ We will compute integrals with the Haar probability measures.

Problem: Examples of compact topological group

Recap

Topological group: Group with topology s.t. $(x, y) \mapsto x \circ y$, $x \mapsto x^{-1}$ continuous.

Example

$\mathbb{R}/\mathbb{Z}$ with group operation $\circ$ s.t. $[r_1] \circ [r_2] = [r_1 + r_2]$ and
$d([r_1], [r_2]) = \min_{z \in \mathbb{Z}} |r_1 - r_2 + z|$
$\mu([a, b]) = b - a$ if $0 \leq a \leq b \leq 1$

Example

$\mathbb{Z}/n\mathbb{Z} = \{[0], [1], \dots, [n-1]\}$ with discrete topology and group operation $\circ$ s.t. $[z_1] \circ [z_2] = [z_1 + z_2]$
$\mu(\{0\}) = \frac{1}{n}, \mu(\{0, 1\}) = \frac{2}{n}$ (counting measure)

Problem: Space representation (metric space)

$\Rightarrow$ A measure to calculate an average is determined by the space.
$\Rightarrow$ How can we "know" about the space?

Recap (Weih'00 Chap8.1)

A **computable metric space** is a 4-tuple (M, d, A, α) s.t. (M, d) is a metric space, $\alpha : \Sigma^* \to A$ is a notation of a dense subset $A \subseteq M$, and a function $f : \Sigma^* \times \Sigma^* \to \mathbb{R}$ s.t. $f(s, t) = d(\alpha(s), \alpha(t))$ is computable.

$\Rightarrow$ Will assume that the space is a computable metric space.

Problem: Examples of computable metric space

Recap (Weih'00 Chap8.1)

A **computable metric space** is a 4-tuple (M, d, A, α) s.t. (M, d) is a metric space, $\alpha : \Sigma^* \to A$ is a notation of a dense subset $A \subseteq M$, and a function $f : \Sigma^* \times \Sigma^* \to \mathbb{R}$ s.t. $f(s, t) = d(\alpha(s), \alpha(t))$ is computable.

Example

On $\mathbb{R}$, $\mathbb{D}$ can act as a countable dense subset A and an encoding of $\mathbb{D}$ can act as α. Then the representation of $r \in \mathbb{R}$ can be an encoding of the sequence $\{q_n\}$ where $q_n \in \mathbb{D}$ and $|q_n - r| \leq 2^{-n}$. That is, q_n rapidly converges to r.

Example

$\mathbb{Z}/n\mathbb{Z} = \{[0], [1], \ldots, [n-1]\}$ with $d([i], [j]) = \min_{z \in \mathbb{Z}} |i - j + nz|$
$\mathbb{Z}/n\mathbb{Z}$ itself is A. Any bijective numbering can act as α.

Problem: Space representation (Compactness)

Definition (very similar to Weih'03 Separation bound)

For any compact metric space (X, d) and its subset $T \subseteq X$,

- T is called a **n-packing** if $x, y \in T(x \neq y \Rightarrow d(x, y) > 2^{-n})$
- T is called a **maximal n-packing** if it is a n-packing and $|T|$ is maximal among n-packings.
- $\kappa_X : \mathbb{N} \to \mathbb{N}$ is called the **sizes of maximal packings** if

$$\kappa_X(n) := \max_{T \text{ is a } n\text{-packing}} |T|$$

$\Rightarrow$ Will assume that the sizes of maximal packings is computable.

Problem

What me and my supervisor proved is:

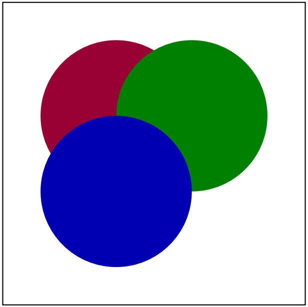
Theorem

Assume that the space $(X, d, \circ)$ is a compact topological group and a computable metric space. Assume that the sizes of maximal packings, $\kappa_X : \mathbb{N} \to \mathbb{N}$ is computable and the metric is bi-invariant. Then the Haar integral functional is computable.

$\Rightarrow$ A metric is called bi-invariant if $d(a \circ c, b \circ c) = d(a, b) = d(c \circ a, c \circ b)$

Proof: Strategy

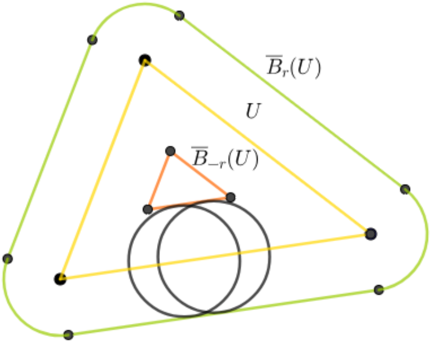
1. Make a partition $P = \{E_1, \ldots, E_n\}$
2. Compute its measures, $\mu(E_i)$
3. Approximate the integral with $\sum_{i=1}^{n} \mu(E_i) f(a_i)$



Proof: Approximating the measure

Definition

- **outer generalized closed ball** $:= \overline{B}_r(U) = \bigcup_{x \in U} \overline{B}_r(x)$
- **inner generalized closed ball** $:= \overline{B}_{-r}(U) = B_r(U^c)^c$
  $= \{x \in U : B_r(x) \subseteq U\}$



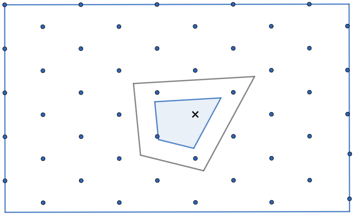
Proof: Approximating the measure

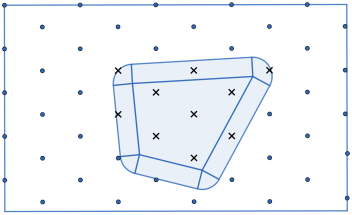
Main lemma

For measurable set $U \subseteq X$, $n \in \mathbb{N}$ and maximal n-packing T_n,

$$\frac{\left|T_n \cap \overline{B}_{-2^{-n+1}}(U)\right|}{|T_n|} \leq \mu(U) \leq \frac{\left|T_n \cap \overline{B}_{2^{-n+1}}(U)\right|}{|T_n|}$$

(In fact, for some nice U, leftmost and rightmost side converges to $\mu(U)$ when $n \to \infty$)





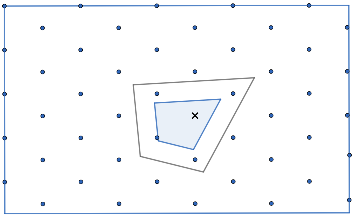
Proof: Approximating the measure

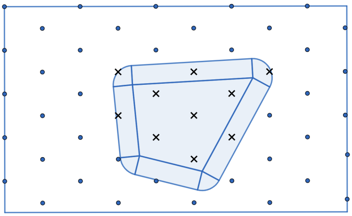
Main lemma

For measurable set $U \subseteq X$, $n \in \mathbb{N}$ and maximal n-packing T_n,

$$\frac{\left|T_n \cap \overline{B}_{-2^{-n+1}}(U)\right|}{|T_n|} \le \mu(U) \le \frac{\left|T_n \cap \overline{B}_{2^{-n+1}}(U)\right|}{|T_n|}$$

(In fact, for some nice U, leftmost and rightmost side converges to $\mu(U)$ when $n \to \infty$)





...But we cannot "count" the number of points! $\Rightarrow$ Need to work around.

Proof: Approximating the measure

Corollary

For a closed ball $\overline{B}_R(p) \subseteq X$, and a maximal n-packing T_n,

$$\mu(\overline{B}_{-2^{-n+2}}(U)) \leq \frac{\left|T_n \cap \overline{B}_{-2^{-n+1}}(U)\right|}{|T_n|} \leq \mu(U) \leq \frac{\left|T_n \cap \overline{B}_{2^{-n+1}}(U)\right|}{|T_n|} \leq \mu(\overline{B}_{2^{-n+2}}(U))$$

Thus we need $\lim_{r\downarrow 0} \mu(\overline{B}_{+r}(U)) = \lim_{r\downarrow 0} \mu(\overline{B}_{-r}(U))$ to approximate the measure of U.

Proof: Approximating the measure

Definition

We say a measurable set U is a **point of continuity** if
$\lim_{r\downarrow 0} \mu(\overline{B}_{+r}(U)) = \lim_{r\downarrow 0} \mu(\overline{B}_{-r}(U))$ holds
(In other words, $\lim_{r\to 0} \mu(\overline{B}_r(U))$ exists).

Recap (Weih'00 Chap5.1)

We say a closed set U is **computable** if $p \mapsto d(p, U)$ is computable.

Corollary

If a set U is a point of continuity and computable, then $\mu(U)$ is computable.

Proof: Approximating the measure

$\exists \lim_{r \to 0} \mu(\overline{B}_r(U))$? Not every balls are points of continuity.

Proof: Approximating the measure

$\exists \lim_{r \to 0} \mu(\overline{B}_r(U))$? Not every balls are points of continuity.

Example

$\mathbb{Z}/n\mathbb{Z} = \{[0], [1], \ldots, [n-1]\}$ with $d([i],[j]) = \min_{z \in \mathbb{Z}} |i - j + nz|$ which gives a discrete topology and it has counting measure
$\mu(\overline{B}_1([1])) = \mu(\{[0],[1],[2]\}) = \frac{3}{n}$ whereas
$\lim_{r \uparrow 1} \mu(\overline{B}_r([1])) = \mu(\{[1]\}) = \frac{1}{n}$

Proof: Approximating the measure

$\exists \lim_{r \to 0} \mu(\overline{B}_r(U))$? Not every balls are points of continuity.

Example

$\mathbb{Z}/n\mathbb{Z} = \{[0], [1], \ldots, [n-1]\}$ with $d([i],[j]) = \min_{z \in \mathbb{Z}} |i - j + nz|$ which gives a discrete topology and it has counting measure
$\mu(\overline{B}_1([1])) = \mu(\{[0],[1],[2]\}) = \frac{3}{n}$ whereas
$\lim_{r \uparrow 1} \mu(\overline{B}_r([1])) = \mu(\{[1]\}) = \frac{1}{n}$

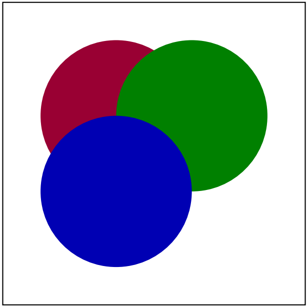
Theorem

For any a, b s.t. $a < b$, we can effectively find r s.t. $a < r < b$ and $\lim_{\epsilon \to 0} \mu(\overline{B}_{r+\epsilon}) = \mu(\overline{B}_r)$.

Corollary

For any a, b s.t. $a < b$, we can effectively find r s.t. $a < r < b$ and $\mu(\overline{B}_r)$ is computable.

Proof: Partitioning(Recap)



$$P = \{E_1, \ldots, E_n\}$$

$$E_i = \overline{B}_r(p_i) \setminus \overline{B}_r(p_{i-1}) \cdots \setminus \overline{B}_r(p_1)$$

Proof: Generalization

Lemma

Sets made with finite union, intersection, closure of complement of **closed balls** are computable.

Lemma

Sets made with finite union, intersection, closure, complement of points of continuity are points of continuity.

Corollary

If U is a set made with finite union, intersection, closure, complement of closed balls that is point of continuity then $\mu(U)$ is computable.

Sum up (Dongseong Seon and Martin Ziegler)

Theorem

Assume that the space $(X, d, \circ)$ is a compact topological group and a computable metric space. Assume that the sizes of maximal packings, $\kappa_X : \mathbb{N} \to \mathbb{N}$ is computable and the metric is bi-invariant. Then the Haar integral functional is computable.

1. Make a partition $P = \{E_1, \ldots, E_n\}$
2. Compute its measures, $\mu(E_i)$
3. Approximate the integral with $\sum_{i=1}^{n} \mu(E_i) f(a_i)$

Limitations

Theorem

Assume that the space $(X, d, \circ)$ is a compact topological group and a computable metric space. Assume that the sizes of maximal packings, $\kappa_X : \mathbb{N} \to \mathbb{N}$ is computable and the metric is bi-invariant. Then the Haar integral functional is computable.

- maximal packing: hard to compute
- metric should be bi-invariant: Is it natural?

Represented space approach (Arno Pauly)

Changes in premise

computable maximal packing $\Rightarrow$ computably compact
metric is bi-invariant $\Rightarrow$ computable group operation

Pros:

- Natural and mild premise

Cons:

- Cannot aim for complexity

Complexity

Fact (Ko91, Theorem 5.32)

In fact:

- $\forall f \in \mathcal{C}([0,1])$, *if f is polynomial-time computable, then* $\int_0^1 f dx \in \mathbb{R}$ *is* $\#P_1$ *computable.*
- ($\forall f \in \mathcal{C}([0,1])$, *if f is polynomial-time computable, then* $\int_0^1 f dx \in \mathbb{R}$ *is polynomial-time computable)* $\Leftrightarrow (FP_1 = \#P_1)$.

Complexity

Fact (Ko91, Theorem 5.32)

In fact:

- $\forall f \in \mathcal{C}([0,1])$, *if* f *is polynomial-time computable, then* $\int_0^1 f dx \in \mathbb{R}$ *is* $\#P_1$ *computable.*
- *(*$\forall f \in \mathcal{C}([0,1])$, *if* f *is polynomial-time computable, then* $\int_0^1 f dx \in \mathbb{R}$ *is polynomial-time computable)* $\Leftrightarrow (FP_1 = \#P_1)$.

Theorem (Expanded [Ko91, Theorem 5.32] to $\mathcal{SO}(3)$)

- $\forall f \in \mathcal{C}(\mathcal{SO}(3))$, if f is polynomial-time computable, then $\int_0^1 f\, d\mu \in \mathbb{R}$ is $\#P_1$ computable.
- ($\forall f \in \mathcal{C}(\mathcal{SO}(3))$, if f is polynomial-time computable, then $\int_0^1 f\, d\mu \in \mathbb{R}$ is polynomial-time computable) $\Leftrightarrow (FP_1 = \#P_1)$.

Complexity

Theorem (Expanded [Ko91, Theorem 5.32] to $\mathcal{SO}(3)$)

- $\forall f \in \mathcal{C}(\mathcal{SO}(3))$, if f is polynomial-time computable, then $\int_0^1 f\,d\mu \in \mathbb{R}$ is $\#P_1$ computable.
- $(\forall f \in \mathcal{C}(\mathcal{SO}(3))$, if f is polynomial-time computable, then $\int_0^1 f\,d\mu \in \mathbb{R}$ is polynomial-time computable$) \Leftrightarrow (FP_1 = \#P_1)$.

Recap

decision problems: $P \subseteq NP \subseteq PSPACE$
function problems: $FP \subseteq \#P \subseteq FPSPACE$
$(FP = \#P) \Rightarrow (P = NP)$
$(FP_1 = \#P_1) \Rightarrow (EXP = NEXP)$

Complexity: Method

Theorem (Expanded [Ko91, Theorem 5.32] to $\mathcal{SO}(3)$)

- $\forall f \in \mathcal{C}(\mathcal{SO}(3))$, if f is polynomial-time computable, then $\int_0^1 f\, d\mu \in \mathbb{R}$ is $\#P_1$ computable.
- $(\forall f \in \mathcal{C}(\mathcal{SO}(3))$, if f is polynomial-time computable, then $\int_0^1 f\, d\mu \in \mathbb{R}$ is polynomial-time computable) $\Leftrightarrow (FP_1 = \#P_1)$.

- Restricted setting: Only on $\mathcal{SO}(3)$
- Used standard way to calculate Haar integral in pure mathematics
- Different algorithm from the general algorithm presented earlier

Complexity: Experiment

Integrated a function $(w, x, y, z) \mapsto |w| + |x| + |y| + |z| : S^3 \to \mathbb{R}$