Complexity and Coding Theory of Hilbert Spaces[1]

Donghyun Lim[a] Svetlana Selivanova[b] Martin Ziegler[c]

[a]KAIST, klimdhn@kaist.ac.kr

[b]KAIST, sseliv@kaist.ac.kr

[c]KAIST, ziegler@kaist.ac.kr

CCA, September 2020

[1]This work was supported by the National Research Foundation of Korea (grant 2017R1E1A1A03071032) and by the International Research & Development Program of the Korean Ministry of Science and ICT (grant 2016K1A3A7A03950702) and by the NRF Brain Pool program (grant 2019H1D3A2A02102240). We particularly thank Akitoshi Kawamura and Florian Steinberg for helpful advice and feedback.

Table of Contents

Complexity and Coding Theory of Hilbert Spaces

Fact

Every infinite-dimensional separable Hilbert spaces are isomorphic.

Example

$\mathcal{L}^2$ is the space of square-integrable functions $f : [0,1] \to \mathbb{C}$ equipped with the inner product

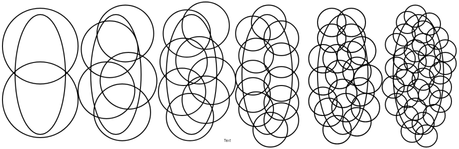
$$\langle f, g \rangle := \int_0^1 f(x)\overline{g(x)}dx.$$

Example

$\{e^{2\pi kix}\}_{k\in\mathbb{Z}}$ is an orthonormal basis of $\mathcal{L}^2$.

Definition

$\eta : \mathbb{N} \to \mathbb{N}$ is the **entropy** of space X if for every $n \in \mathbb{N}$, X can be covered by $2^{\eta(n)}$ closed balls of radius 2^{-n}, but not by $2^{\eta(n)-1}$ closed balls.



Example

The unit interval $[0, 1]$ has the entropy $\eta(n) = n$.

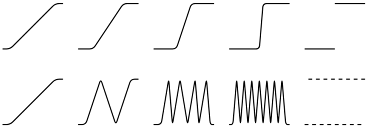
Example (Steinberg, 2017)

$\mathrm{Lip}_1([0, 1], [0, 1])$ has the entropy $\eta(n) = 2^{\mathcal{O}(n)}$.

Definition

$\mu : \mathbb{N} \to \mathbb{N}$ is a **modulus of continuity** of $f : (X, d) \to (Y, e)$ if

$$\forall n \in \mathbb{N} \quad \forall a, b \in X \quad d(a, b) \leq 2^{-\mu(n)} \text{ implies } e(f(a), f(b)) \leq 2^{-n}$$



Dyadic Representation: $\{0, 1\}^{\omega} \twoheadrightarrow [0, 1]$

$$bin(a_0)bin(a_1)bin(a_2)\cdots \mapsto \lim_{n\to\infty} \frac{a_n}{2^n}$$

Signed Binary Representation: $\{0, 1\}^{\omega} \twoheadrightarrow [0, 1]$

$$bin(a_0)bin(a_1)bin(a_2)\cdots \mapsto \sum_{n=0}^{\infty} \frac{a_n}{2^n}$$

$a_i \in \{-1, 0, 1\}$

Dyadic Representation: $\{0,1\}^\omega \twoheadrightarrow [0,1]$; modulus $\Theta(n^2)$

$$bin(a_0)bin(a_1)bin(a_2)\cdots \mapsto \lim_{n\to\infty} \frac{a_n}{2^n}$$

Signed Binary Representation: $\{0,1\}^\omega \twoheadrightarrow [0,1]$; modulus $\Theta(n)$

$$bin(a_0)bin(a_1)bin(a_2)\cdots \mapsto \sum_{n=0}^{\infty} \frac{a_n}{2^n}$$

$a_i \in \{-1,0,1\}$

Steinberg's Lemma (2016)

For a surjection $f : X \to Y$ and its modulus μ,

$$\forall n \quad \eta_X(n) \leq \eta_Y(\mu(n))$$

where η_X and η_Y being the entropy of X and Y, respectively.

- Sometimes we want to find f with (asympotitically) small μ.
- This lemma establishes a lower bound of μ.

Weihrauch-style Representation

A partial surjection $\{0,1\}^\omega \twoheadrightarrow X$

Kawamura-style Representation (2012)

A partial surjection $(\{0,1\}^* \to \{0,1\}^*) \twoheadrightarrow X$

Our-style Representation

A partial surjection $(\{0,1\}^* \to \{0,1\}) \twoheadrightarrow X$ with metric d on domain

$$d(\psi, \varphi) := 2^{-\min\{|w| : \psi(w) \neq \varphi(w)\}}$$

- ψ and φ are close iff they agree on all $w \in \{0,1\}^*$ up to some length.

Standard Representation of $\mathrm{Lip}_1([0,1],[0,1])$

$$(\{0,1\}^* \to \{0,1\}) \twoheadrightarrow \mathrm{Lip}_1([0,1],[0,1])$$

$\varphi \mapsto f$ iff $\varphi(0^n 1^j 0 bin(A)) = j$th bit in the binary encoding of $f(A/2^n)$ approximated to precision 2^{-n}

- $\mathrm{Lip}_1([0,1],[0,1])$ is compact according to Arzela-Ascoli
- The standard representation has a linear modulus.
- n and j are encoded in unary and A is encoded in binary.
- This modulus is (asymptotically) optimal by Steinberg's lemma since both $(\{0,1\}^* \to \{0,1\})$ and $\mathrm{Lip}_1([0,1],[0,1])$ have exponential entropy.

Standard Representation of $\mathrm{Lip}_1([0,1],[0,1])$

$$(\{0,1\}^* \to \{0,1\}) \twoheadrightarrow \mathrm{Lip}_1([0,1],[0,1])$$

$\varphi \mapsto f$ iff $\varphi(0^n 1^j 0 bin(A)) = j$th bit in the binary encoding of $f(A/2^n)$ approximated to precision 2^{-n}

- Use of $(\{0,1\}^* \to \{0,1\})$ instead of $\{0,1\}^* \to \{0,1\}^*$ eliminates the need for second-order complexity.
- Application functional $(f,x) \mapsto f(x)$ is polytime computable with respect to standard representation. (Kawamura, 2012)
- A representation δ of $\mathrm{Lip}_1([0,1],[0,1])$ is polytime reducible to standard representation iff it makes application functional polytime computable. (Kawamura, 2012)

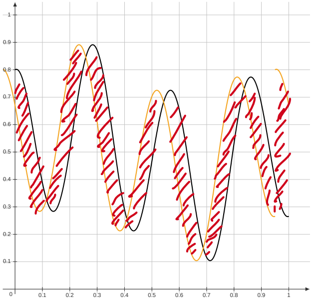
Table of Contents

Definition

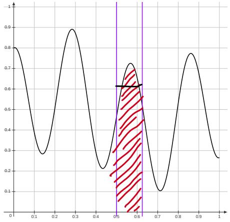
$\mathcal{L}^2_1$ is the space of functions $f : [0,1] \to \mathbb{C}$ such that

$$\|f\| \leq 1 \quad \wedge \quad \forall \epsilon > 0 \; \|\tau_\epsilon f - f\| \leq \epsilon$$

where $\|f\|$ is the norm $\|f\| := \sqrt{\int_0^1 f(x)\overline{f(x)}dx}$
and τ is the cyclic shift $(\tau_\epsilon f)(x) := f(x + \epsilon \bmod 1)$.



- $\mathcal{L}^2_1$ is compact according to Fréchet-Kolmogorov

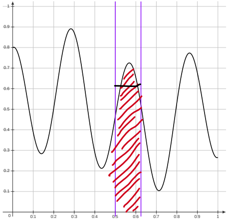


Piecewise Representation of $\mathcal{L}_1^2$

$$(\{0,1\}^* \to \{0,1\}) \twoheadrightarrow \mathcal{L}_1^2$$

$\varphi \mapsto f$ iff $\varphi(0^n 1^j 0 bin(A)) = j$th bit in the binary encoding of $2^n \cdot \int_{A/2^n}^{(A+1)/2^n} f$ approximated up to precision 2^{-n}

- Similar representations have been used for computability investigations.
- $\mathcal{L}_1^2$ has entropy $\eta(n) = 2^{\mathcal{O}(n)}$ (Steinberg, 2016)
- $(\{0,1\}^* \to \{0,1\})$ has entropy $\eta(n) = 2^{\mathcal{O}(n)}$.
- Piecewise representation has linear modulus and this is optimal.



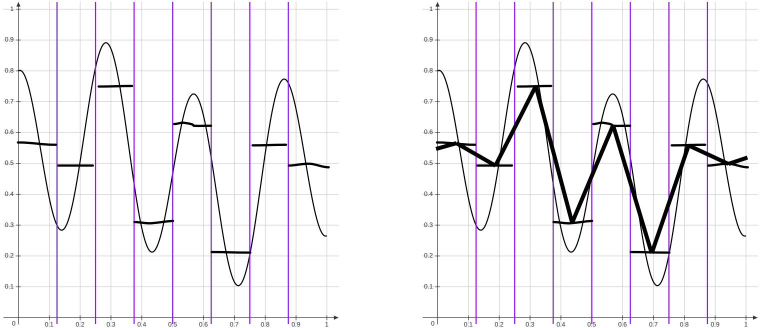
Theorem

Under piecewise representation, the functional $f \mapsto \int_0^1 f$ is not polytime but exptime computable.

Proof. Because exponentially many intervals cannot be accessed in polytime. (Made formal by perturbation argument.)

Conjecture

Under piecewise representation, the pointwise operator $(f, g) \mapsto \sqrt{f \cdot g}$ is polytime computable.



- Let $f \in \mathcal{L}^2_1$.
- For each interval, we can calculate the average by integration.
- Not closed under piecewise constant approximation $f \in \mathcal{L}^2_1 \not\Rightarrow \tilde{f} \in \mathcal{L}^2_1$.
- Closed under piecewise *linear* approximation $f \in \mathcal{L}^2_1 \Rightarrow \hat{f} \in \mathcal{L}^2_1$.

Table of Contents

Definition

ℓ^2_1 is the space of sequences $(z_K)_{K\in\mathbb{Z}} \subseteq \mathbb{C}$ such that

$$\sqrt{\sum_K |z_K|^2} \leq 1 \quad \wedge \quad \sqrt{\sum_K |2\pi i K z_K|^2} \leq 1.$$

Lemma

ℓ^2_1 is isometric to $\mathcal{L}^2_1$.
Proof. By Parseval's identity and some additional arguments.

Fourier Coefficient Representation

$$(\{0,1\}^* \to \{0,1\}) \twoheadrightarrow \ell^2_1$$

$\varphi \mapsto (z_K)_{K\in\mathbb{Z}}$ iff $\varphi(0^n 1^j 0 bin(K)) = j$th bit in the binary encoding of z_K approximated up to precision 2^{-n}

- Since ℓ^2_1 can be isometrically identified with $\mathcal{L}^2_1$, a representation of ℓ^2_1 is also a representation of $\mathcal{L}^2_1$ and vice versa.

Fourier Coefficient Representation

$$(\{0,1\}^* \to \{0,1\}) \twoheadrightarrow \ell_1^2$$

$\varphi \mapsto (z_K)_{K\in\mathbb{Z}}$ iff $\varphi(0^n 1^j 0 bin(K)) =$ jth bit in the binary encoding of z_K approximated up to precision 2^{-n}

- n and j encoded in unaryy; K encoded in binary
- Fourier coefficient representation has linear modulus and this is optimal by Steinberg's lemma.

Observation

In Fourier representation, the functional $f \mapsto \int_0^1 f$ is polytime computable by directly reading it off from the encoding.

A Characterization of Fourier Coefficient Representation

A representation δ is polytime reducible to Fourier coefficient representation iff δ makes polytime computable the functional $(f, \mathrm{bin}(K)) \mapsto K$-th Fourier coefficient.

Fourier Coefficient Representation

$$(\{0,1\}^* \to \{0,1\}) \twoheadrightarrow \ell_1^2$$

$\varphi \mapsto (z_K)_{K\in\mathbb{Z}}$ iff $\varphi(0^n 1^j 0 bin(K)) = j$th bit in the binary encoding of z_K approximated up to precision 2^{-n}

Conjecture

The functional $f \mapsto \int_0^{1/3} f$ is not polytime but exptime computable under Fourier coefficient representation.

Conjecture

The functional $(f, g) \mapsto \int_0^1 f(x)\overline{g(x)}dx$, the 0th Fourier coefficient of $f \cdot g$, is not polytime computable but exptime computable under Fourier coefficient representation. (Can be computed by convolution)

Table of Contents

Piecewise Representation of $\mathcal{L}^2_1$

$$(\{0,1\}^* \to \{0,1\}) \twoheadrightarrow \mathcal{L}^2_1$$

$\varphi \mapsto f$ iff $\varphi(0^n 1^j 0 bin(A)) = j$th bit in the binary encoding of $2^n \cdot \int_{A/2^n}^{(A+1)/2^n} f$ approximated up to precision 2^{-n}

Fourier Coefficient Representation

$$(\{0,1\}^* \to \{0,1\}) \twoheadrightarrow \ell^2_1$$

$\varphi \mapsto (z_K)_{K\in\mathbb{Z}}$ iff $\varphi(0^n 1^j 0 bin(K)) = j$th bit in the binary encoding of z_K approximated up to precision 2^{-n}

Conjecture

	Piecewise Repr	Fourier Coef Repr
$f \mapsto \int_0^1 f$	Not polytime	Polytime
$(f, unary(n)) \mapsto 2^n \cdot \int_0^{2^{-n}} f$	Polytime	Not polytime

- Therefore the two representations are not polytime convertible.

Summary

- $\mathcal{L}_1^2$ and piecewise representation.
- ℓ_1^2 and Fourier Coefficient representation.
- The two are not polytime equivalent.
- One needs to pick one depending on the purpose.

Future Work

- With respect to the basis $\{e^{2\pi kix}\}_{k\in\mathbb{Z}}$ of $\mathcal{L}_1^2$, we get Fourier coefficients.
- What if we use another orthonormal basis?
- Is there a functional that characterizes the piecewise representation?
- Combining representations makes more functionals polytime computable, but may destroy closure under operations.