On the steps of Shannon's sampling theorem: towards a theory of quantum sampling

Geometria è Fisica: A geometrical vision of physics
Celebrating G. Marmo 70th birthday

Alberto Ibort
ICMAT/UCIIIM

Policeta-San Rufo, July 2016

Index

1. Introduction
2. Shannon's sampling theorem
3. Geometric sampling theory
4. Sampling on groups
5. Sampling on invariant subspaces and representations of compact groups
6. The hidden subgroup problem

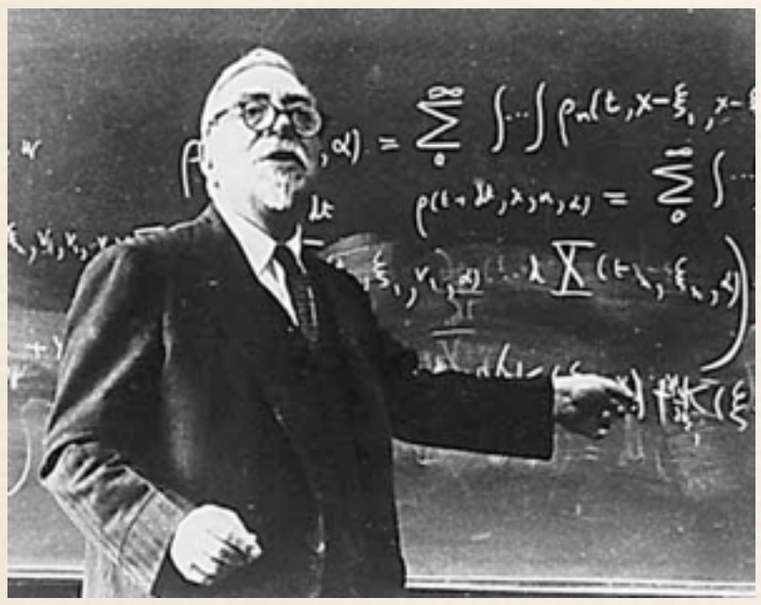
Work in progress with A. García, M.A. Hernández-Medina

1. Shannon's sampling theorem

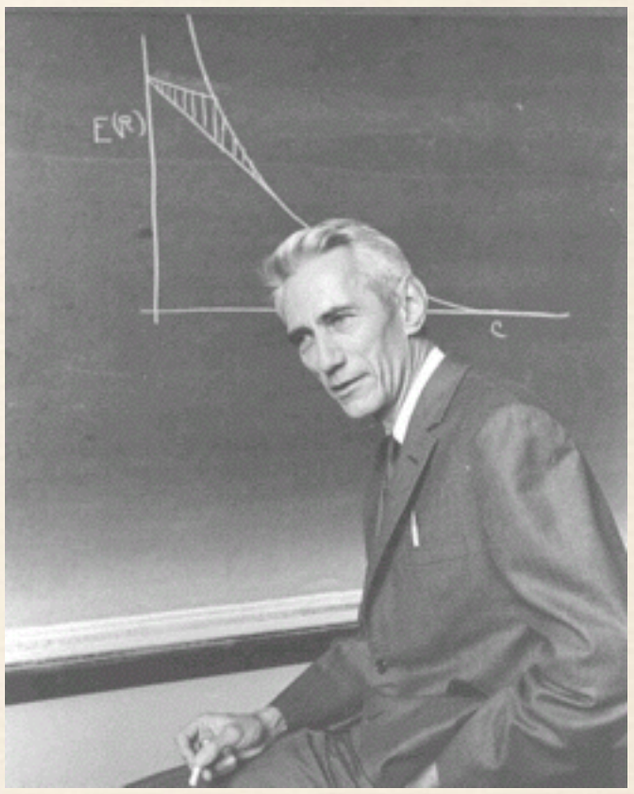
Theorem: If a signal $f(t)$ contains no frequencies higher than w cycles per second, then $f(t)$ is completely determined by its values $f(n/2w)$ at a discrete set of points with spacing $1/2w$, and can be reconstructed from these values by the formula:

$$f(t) = \sum_{n=-\infty}^{\infty} f(\frac{n}{2w}) \frac{\sin \pi(2wt - n)}{\pi(2wt - n)}.$$

Claude E. Shannon. *"Communications in the presence of noise"*. Proc. IRE, **137**, 10-21 (1949).



Norbert Wiener (1894-1964)



Claude E. Shannon (1916-2001)

3. Geometric sampling theory

Ω set $\quad\quad$ $\mathbb{H}$ complex separable Hilbert space

$K\colon \Omega \to \mathbb{H}$ kernel map

$\mathcal{F}\colon \mathbb{H} \to \mathcal{F}(\Omega) \quad\quad \mathcal{F}(\psi)(w) = \langle K(w), \psi \rangle_{\mathbb{H}}\,, \quad \psi \in \mathbb{H}$

Example $\quad \Omega = \mathbb{R} \quad\quad \mathbb{H} = L^2([-\pi, \pi])$

$$K\colon \mathbb{R} \to L^2([-\pi,\pi]) \qquad K(w) = \frac{1}{\sqrt{2\pi}} e^{iwx}$$

$$\mathcal{F}\colon L^2([-\pi,\pi]) \to \mathcal{F}(\mathbb{R})$$

$$\mathcal{F}(\psi)(w) = \frac{1}{\sqrt{2\pi}} \int_{-\pi}^{\pi} e^{-iwx} \psi(x) dx$$

$\mathrm{Ran}(\mathcal{F}) = PW_\pi$ $\quad$ Paley-Wiener space

S. Saitoh. *Integral transforms, reproducing kernels and their applications*. Longman, Essex, England, 1997.

R. Paley and N. Wiener. *Fourier transforms in the complex domain*, volume 19, AMS Colloq. Publ., AMS. New York, 1934.

Sampling formulas

$w_n \in \Omega\,, \quad e_n = K(w_n)\,, \quad n = 1, 2, \ldots$ orthonormal basis

$$f = \mathcal{F}(\psi) \in \mathcal{F}(\mathbb{H}) \qquad \psi = \sum_n \langle e_n, \psi \rangle e_n$$

$$f(w_n) = \langle K(w_n), \psi \rangle$$

$$f(w) = \mathcal{F}(\psi)(w) = \sum_n \langle K(w_n), \psi \rangle \mathcal{F}(e_n) = \sum_n f(w_n) S_n(w)$$

Example (contd.) $\qquad w_n = n \in \mathbb{Z}$

$$f(w) = \sum_{n \in \mathbb{Z}} f(n) S_n(w) \qquad S_n(w) = \frac{\sin \pi(w - n)}{\pi(w - n)}$$

If $\ker \mathcal{F} = 0$

$$\langle f, g \rangle_K = \langle \psi, \phi \rangle_{\mathbb{H}}\,, \quad f = \mathcal{F}(\psi), g = \mathcal{F}(\phi)$$

$$k(w, u) = \langle K(w), K(u) \rangle \qquad f(w) = \langle k(w, \cdot), f \rangle_K$$

$\left(\mathcal{F}(\mathbb{H}), \langle \cdot, \cdot \rangle_K\right)$ is a Reproducing Kernel Hilbert Space (RKHS)

4. Sampling theorems on groups

G Lie group

Equivalence classes of continuous irreducible unitary representations

$$\widehat{G} = \{[\mathcal{H}^a, U^a] \mid U^a \colon G \to \mathcal{U}(\mathcal{H}^a)\} = \{a\}$$

Examples: $G = U(1)\,, \quad \widehat{U(1)} = \mathbb{Z}$

$G = \mathbb{Z}\,, \quad \widehat{\mathbb{Z}} = U(1)$

$G = \mathbb{Z}_n\,, \quad \widehat{\mathbb{Z}}_n = \mathbb{Z}_n$

G compact Lie group

$\widehat{G}$ countable, $\{a\} = [n_a]$, $a = 1, 2, \ldots,$ $n_a = \dim \mathcal{H}^a$

In what follows $\qquad n_a = \dim \mathcal{H}^a < \infty\,, \quad \forall a \in \widehat{G}$

$$\chi_a(g) = \mathrm{Tr}(U^a(g)) \quad \text{character}$$

$$K \colon \widehat{G} \to L^2(G) \quad K(a) = n_a \chi_a \quad \text{Kernel group map}$$

4. Sampling theorems on groups (Cont.)

$$K\colon \widehat{G} \to L^2(G) \qquad K(a) = \chi_a \quad \text{Kernel group map}$$

$$\mathcal{F}\colon L^2(G) \to \mathcal{F}(\widehat{G})\,, \quad \mathcal{F}(\psi)(a) = \langle K(a), \Psi \rangle = \int_G \overline{\chi}_a(g)\psi(g)d\mu_G(g)$$

Example: G is a locally compact Abelian group (LCA)
$\widehat{G}$ is LCA too. Plancherel's theorem

$$\mathcal{F}\colon L^2(G) \to L^2(\widehat{G})\,, \quad \mathcal{F}(\psi)(a) = \int_G \overline{\chi}_a(g)\psi(g)d\mu_G(g)$$

G Abelian finite

$|G| = |\widehat{G}|\,, \quad G \cong \widehat{G}$

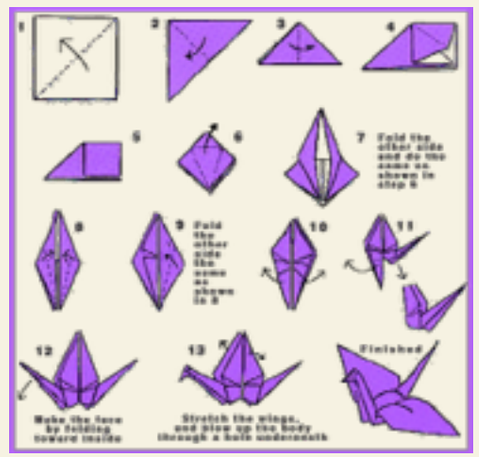
$$\mathcal{F}(|g\rangle) = \frac{1}{\sqrt{|G|}} \sum_{g'} \overline{\chi}_{g'}(g)|g'\rangle$$

Sampling with subgroups

G group $\qquad$ K normal subgroup

$H = G/K$ quotient group of right cosets

$$e \to K \to G \xrightarrow{\pi} H \to e$$



Sampling and subgroups

G group $\qquad$ K normal subgroup

$H = G/K$ quotient group of right cosets

$$e \to K \to G \xrightarrow{\pi} H \to e$$

$$\pi^* \colon \widehat{H} \to \widehat{G}\,, \quad \pi^*(U)(g) = U(\pi(g))$$

$$\begin{array}{ccc} K_H \colon \widehat{H} & \to & L^2(H) \\ \pi^* \downarrow & & \downarrow \sigma \\ K_G \colon \widehat{G} & \to & L^2(G) \end{array}$$

Suppose from now on that K is a discrete subgroup

$$\sigma \colon H \to G, \quad \pi \circ \sigma = id_H$$

cross-section

If H is Abelian, functions on $\mathcal{F}_G \circ \sigma$ can be sampled with respect to the system $S_a = \mathcal{F}_G(\chi_a)$, $a \in \widehat{H}$ and for them

$$f(\alpha) = \sum_{a \in \widehat{H}} f(a) S_a(\alpha)$$

Example: $\quad G = \mathbb{R}\,, \quad K = \mathbb{Z}\,, \quad H = G/K = U(1)$

Samplig formula = Shannon's sampling theorem

5. Sampling theorems and representations of compact groups

Sampling theorems on invariant subspaces

$U : G \to \mathcal{U}(\mathcal{H})$ Square integrable unitary representation

G compact group

$$|f(\Omega)\rangle = \int_G f(g) U(g) |\Omega\rangle d\mu(g)\,, \quad f \in L^2(G)$$

$\mathcal{H}_\Omega = \{|f(\Omega)\rangle\}$ Invariant subspace

$$|f(\Omega)\rangle = \sum_{a \in \widehat{H}} f(a) |S_n(\Omega)\rangle$$

A. García-García, M.A. Hernández-Media, A. Ibort,. Towards a quantum sampling theory: the case of finite groups (2016).

6. The Hidden subgroup problem.

G group $\qquad$ K subgroup

$H = G/K$ homogenous space of right cosets

$e \to K \to G \xrightarrow{\pi} H$

$F\colon G \to S\,, \quad F(gk) = F(g)\,, \quad \forall k \in K, g \in G$

Hidden subgroup problem: Given a function F as above, determine the subgroup K (i.e., find a set of generators)

Hidden Abelian subgroup problem: Given G an Abelian group, and a function F as above, determine the Abelian subgroup K (i.e., find a set of generators).

Example $\quad G = \mathbb{Z}_n\,, \quad n = pq \qquad K = \mathbb{Z}_p$ Schor's algorithm

A. Kitaev. *Quantum measurements and the abelian stabilizer problem,* ECCC, Report TR96-003, 1996.

Solution Hidden Abelian subgroup problem: G Finite

$|g\rangle \in L^2(G)$ standard orthonormal basis $\quad |\psi\rangle = \sum_{g\in G} \psi(g)|g\rangle$

Kitaev's algorithm:

1. Superposition: $\quad \frac{1}{\sqrt{|G|}} \sum_g |g\rangle$

2. Computing F: $\quad \frac{1}{\sqrt{|G|}} \sum_g |g\rangle \otimes |0\rangle$

$$U_F \left(\frac{1}{\sqrt{|G|}} \sum_g |g\rangle \otimes |0\rangle \right) = \frac{1}{\sqrt{|G|}} \sum_g |g\rangle \otimes |F(g)\rangle$$

3. Measure the second register

$$|\psi\rangle = \frac{1}{\sqrt{|K|}} \sum_{k\in K} |\tilde{g}k\rangle \otimes |F(\tilde{g})\rangle$$

Kitaev's algorithm (Cont.):

4. Quantum Fourier transform on the first factor

$$\mathcal{F}(|\psi\rangle) = \frac{1}{\sqrt{|G||K|}} \sum_{g\in G} \sum_{k\in K} \chi_g(k)\chi_g(\tilde{g})|g\rangle \otimes |F(\tilde{g})\rangle$$

$$\frac{1}{\sqrt{|H|}} \sum_{k\in K} \chi_g(k) = \delta(g, K^\perp) \qquad K^\perp = \{\chi_g \in \widehat{G} \mid \chi_g(k) = 1\,, \forall k \in K\}$$

$$\mathcal{F}(|\psi\rangle) = \frac{1}{\sqrt{|G|}} \sum_{g\in G} \delta(g, K^\perp)\chi_g(\tilde{g})|g\rangle \otimes |F(\tilde{g})\rangle$$

5. Measure the first register. If non zero, you get a generator of $K^\perp$

An application: new public keys

Given G and and two Abelian (non commuting) subgroups K and H, define a function f by means of the corresponding sampling formula. Alice transmit the values $f(a)$ (S_a are public). Hence Bob (that nows K) reconstruct $F(g)$ for all g.

Scolium

"La meccanica quantistica è scritta in lingua geometrica senza la quale è impossibile capire nulla"

G. Marmo's dictum

Thanks again Beppe!

That's almost all...!