The most popular finite metric space in information theory, its generalizations, and isometry groups

Bogdana Oliynyk

Silesian University of Technology, Gliwice, Poland,
National University of Kyiv-Mohyla Academy, Kyiv, Ukraine

Summer Seminar on Symmetry, Computer Algebra and Algebraic Graph Theory,
Beer-Sheva, September 9, 2025

Fundamental in information theory

Definition

Hamming space H_n is the set of all binary strings (or q-ary strings) of fixed length n, usually denoted $\{0, 1\}^n$ (for the binary case).
The distance between two strings equals the number of positions where they differ.

How is it used in information theory?

- When data is transmitted, errors (bit flips) can occur.
  By encoding data into longer codewords in Hamming space, we can detect and correct errors.
- A good error-correcting code corresponds to a set of points in Hamming space that are far apart.
  The minimum Hamming distance between codewords determines how many errors can be detected or corrected.

Other applications

- Hamming space is used for nearest neighbor search on binary data.
- Codewords in Hamming space are used in source coding (compression) and in designing efficient representations of data.
- DNA/protein sequences can be represented as strings over finite alphabets; Hamming distance is a natural metric for measuring similarity.
- In network coding and error detection in communication protocols.

Connection with hypercube Q_n

On the set of all n-tuples

$$(a_1, \ldots, a_n), \quad a_i \in \{0, 1\}, 1 \le i \le n.$$

define a graph. Two n-tuples $(a_1, \ldots, a_n)$ and $(b_1, \ldots, b_n)$ are adjacent iff

$$d_{H_m}((a_1, \ldots, a_n), (b_1, \ldots, b_n)) = 1.$$

Wreath product of groups

Let (G_1, X_1) and (G_2, X_2) be permutation groups.

Definition

The permutation group

$$(G, X_1 \times X_2) = (G_1, X_1) \wr (G_2, X_2)$$

is called the *wreath product of the groups* (G_1, X_1) and (G_2, X_2) if, for every element $u \in G$, the following conditions hold:

1. if $(x_1, x_2)^u = (y_1, y_2)$, then the value y_1 depends only on x_1;
2. for a fixed x_1, the mapping $g_2(x_1)$ defined by the rule

$$g_2(x_1)(x_2) = y_2$$

Wreath product of groups

From this definition, it follows that elements $u \in G$ can be represented by so-called *tables*:

$$u = [g_1, g_2(x_1)], \qquad g_1 \in G_1, \quad g_2(x_1) \in G_2^{X_1}.$$

In this case, each transformation $u \in G$ acts on elements $(x_1, x_2) \in X_1 \times X_2$ according to the rule:

$$(x_1, x_2)^u = (x_1^{g_1}, x_2^{g_2(x_1)}).$$

Wreath product of groups

The wreath product of permutation groups has the following properties:

1. It is transitive if and only if each factor is a transitive permutation group.
2. The wreath product is always imprimitive.
3. The wreath product is an associative but not commutative operation on the class of permutation groups.

Wreath product of groups

Apart from the realization described above, the group $G_1 \wr G_2$ can also be realized on the set $X_2^{X_1}$. Namely, the *exponentiation* (see) of (G_2, X_2) by (G_1, X_1) is defined as the permutation group

$$(G_1 \wr G_2, X_2^{X_1}),$$

where each element $u = [g_1, g_2(x_1)]$ acts on a function $f(t) \in X_2^{X_1}$ by the rule:

$$f(t)^{[g_1, g_2(x_1)]} = f(t^{g_1})^{g_2(x_1)}.$$

Wreath product of groups

The exponentiation $(G_1 \wr G_2, X_2^{X_1})$ of the permutation group (G_2, X_2) by (G_1, X_1) has the following properties:

1. It is transitive if and only if the group (G_2, X_2) is transitive.
2. It is primitive if and only if (G_1, X_1) is transitive and (G_2, X_2) is primitive and not cyclic.
3. The exponentiation operation is not associative on the class of permutation groups.

Isometry group of Hamming space

The isometry group $IsomH_n$ of the metric space H_n is isomorphic to the wreath product $W_n = Z_2 \wr S_n$.
The group W_n consists of all pairs $[\sigma, f]$, where $\sigma \in S_n$, $f \in Z_2^{\underline{n}}$, $\underline{n} = \{1, \ldots, n\}$. Denote $f(i) = a_i$, $(1 \leq i \leq n)$. Each pair $[\sigma, f]$ corresponds to a unique sequence $[\sigma; a_1, \ldots, a_n]$. Then the group operation in $Z_2 \wr S_n$ is determined by the equality

$$[\sigma; a_1, \ldots, a_n][\eta; b_1, \ldots, b_n] = [\sigma\eta; a_1 + b_{1^\sigma}, \ldots, a_n + b_{n^\sigma}],$$

where $+$ denotes the addition in Z_2.

- L.A. Kaloujnine, P.M. Beleckij, V.Z. Fejnberg, *Kranzprodukte*,Leipzig: BSB B.G. Teubner Verlagsgesellschaft, 1987.
- M.Ch. Klin, R. Póschel, K. Rosenbaum. *Angewandte Algebra fúr Mathematiker und Informatiker. Einfúhrung in gruppentheoretisch-kombinatorische Methoden. (Applied algebra for mathematicians and computer scientists. Introduction to group theoretical combinatorial methods)*, 1988.

Countable Hamming Space

Let $\{0,1\}^{\mathbb{N}}$ be the set of all infinite tuples of elements of the set $\{0,1\}$, i.e. the set of all infinite binary sequences.

The countable Hamming space ("Countable cube") $H_{\mathbb{N}}$ consists of all infinite tuples

$$(a_1, a_2, \dots), \quad a_i \in \{0,1\}, i \geq 1,$$

such that almost all their coordinates equal zero (i.e. only finite number of coordinates equal one).

The distance between two such infinite tuples is equal to the number of coordinates where they differ.

Isometries of Countable Hamming Space

Let $g_2 : \mathbb{N} \to S_2$, i.e. $g_2 \in S_2^{\mathbb{N}}$. Denote by $supp(g_2)$ the set of all elements $x_1 \in \mathbb{N}$, such that $g_2(x_1) \neq Id_{S_2}$. Define a restricted wreath product

$$S_2 \bar{\wr} S_{\mathbb{N}} = \{[g_2(x_1), g_1] \mid g_1 \in S_{\mathbb{N}}, \quad g_2(x_1) \in S_2^{\mathbb{N}}, \quad |supp(g_2)| < \infty\},$$

as a subgroup of $S_2 \wr S_{\mathbb{N}}$.

Isometries of Countable Hamming Space

Let $g_2 : \mathbb{N} \to S_2$, i.e. $g_2 \in S_2^{\mathbb{N}}$. Denote by $supp(g_2)$ the set of all elements $x_1 \in \mathbb{N}$, such that $g_2(x_1) \neq Id_{S_2}$. Define a restricted wreath product

$$S_2 \bar{\wr} S_{\mathbb{N}} = \{[g_2(x_1), g_1] \mid g_1 \in S_{\mathbb{N}}, \quad g_2(x_1) \in S_2^{\mathbb{N}}, \quad |supp(g_2)| < \infty\},$$

as a subgroup of $S_2 \wr S_{\mathbb{N}}$.

Theorem (B. O. [1996], P.J. Cameron, S. Tarzi [2008], M. Pankov [2012])

The isometry group $IsomH_{\mathbb{N}}$ of the countable Hamming space $H_{\mathbb{N}}$ is isomorphic to the restricted wreath product

$$S_2 \bar{\wr} S_{\mathbb{N}}.$$

Steinitz numbers

Let $\mathbb{P}$ be the set of all primes. A *Steinitz number* is an infinite formal product of the form

$$\prod_{p\in\mathbb{P}} p^{k_p}$$

where $k_p \in \mathbb{N} \cup \{0, \infty\}$. Denote by $\mathbb{SN}$ the set of all supernatural numbers. The elements of the set $\mathbb{SN} \setminus \mathbb{N}$ are called *infinite Steinitz numbers*.

Periodic sequences

An infinite sequence a $= (a_1, a_2, \ldots)$ is said to be *periodic* if there exists a natural number k such that the equality

$$a_i = a_{i+k}$$

holds for all $i \in \mathbb{N}$. In this case the number k is called a *period* of the sequence a.

A periodic sequence a is called *u-periodic* for some supernatural number u if its minimal period divides u.

Periodic Hamming spaces

Let u be some infinite Steinitz number. Denote by $\mathcal{H}(u)$ the space of all u-periodic sequences over the set $\{0, 1\}$. We call the metric space $\mathcal{H}(u)$ the *u-periodic Hamming space*.

Proposition

Let u, v be Steinitz numbers. Then $\mathcal{H}(u)$ and $\mathcal{H}(v)$ are isometric if and only if $u = v$.

Besicovitch-Hamming space

Proposition

[P. J. Cameron, S. Tarzi, 2008]
The completion $\mathcal{H}$ of u-periodic Hamming spaces are independent of choice of u.

The completion $\mathcal{H}$ is called the *Besicovitch-Hamming* space.

$2^\infty-$periodic Hamming space

Theorem

[P. J. Cameron, S. Tarzi, 2008]
(a) The points of $H(2^\infty)$ can be identified with the subsets of $[0,1)$ which are unions of finitely many half-open intervals $[x,y)$ with dyadic rational endpoints, the distance between two such sets being the sum of the lengths of their symmetric difference.
(b) The points of $\mathcal{H}$ can be identified with the Lebesgue measurable subsets of $[0,1]$ modulo null sets, the distance between two points being the Lebesgue measure of their symmetric difference.

Problems of P. J. Cameron and S. Tarzi

- *What is the structure of the isometry group of the periodic Hamming space over a finite alphabet?*
- *What is the structure of the isometry group of its completion?*

Peter J. Cameron, Sam Tarzi, *Limits of cubes*, Topology and its Applications, Volume 155, Issue 14 (2008), 1454–1461.

Problems of P. J. Cameron and S. Tarzi

We construct another representation of the periodic Hamming space and provide answers to both of these questions.

Characteristics

A sequence of positive integers $\tau = (m_1, m_2, \ldots)$ is called *divisible* if $m_i | m_{i+1}$ for all $i \in \mathbb{N}$.

Let $\tau = (m_1, m_2, \ldots)$ be an increasing divisible sequence. Denote by $(s_1, s_2, \ldots)$ the sequence of ratios of the sequence τ, i.e.

$$s_1 = m_1, \qquad s_{i+1} = \frac{m_{i+1}}{m_i}, \ i \geq 1.$$

The Steinitz number

$$s_1 \cdot s_2 \cdot s_3 \ldots$$

is called the *characteristic of the sequence* τ and denoted by $char(\tau)$.

Rooted Trees

Assume that T_τ is a spherically homogeneous rooted tree with spherical index $[s_1, s_2, \ldots]$. We consider the boundary ∂T_τ of the tree T_τ, i.e., the set of all infinite simple paths starting at the root. We call these paths rooted paths.

Path Metric

Define a distance ρ on the set ∂T_τ as

$$\rho_\tau(\gamma_1, \gamma_2) = \begin{cases} \frac{1}{k+1}, & \text{if } \gamma_1 \neq \gamma_2 \\ 0, & \text{if } \gamma_1 = \gamma_2 \end{cases},$$

where k is the length of the common beginning of rooted paths γ_1 and γ_2.

Path Metric Topology

Consider the topology on ∂T_τ induced by the metric ρ_τ. Finite unions of cylindrical sets form open (and closed) sets in this topology. The set of all rooted paths in ∂T_τ that pass through a vertex v is denoted by

$$C_v = \{\gamma \in \partial T_\tau \mid v \in \gamma\}$$

and is called the *cylindrical set* C_v corresponding to v.

Bernoulli Measure

Define the Bernoulli measure μ on the Borel σ-algebra of clopen sets of ∂T_τ using the rule:

$$\mu(C_v) = \frac{1}{n_v},$$

where n_v is the number of vertices of T_τ on the level containing the vertex v.

Periodic Hamming Spaces and Rooted Trees

Define the metric d_μ on the set ΩT_τ of all clopen subsets of ∂T_τ by putting $d_\mu(A, B) = \mu(A \triangle B)$ for all clopen subsets A and B of ∂T_τ.

Theorem (B.O., V. Sushchansky [2013])

The space $H(u)$ of all u-periodic $(0, 1)$-sequences is isometric to the space ΩT_τ of all clopen subsets of ∂T_τ equipped with the metric d_μ.

Besicovitch-Hamming Space and Rooted Trees

Corollary (B.O., V. Sushchansky [2013])

The Besicovitch-Hamming space $\mathcal{H}$ is isometric to the space of all measurable subsets (up to measure zero sets) of ∂T_τ equipped with the metric d_μ.

Theorem (B.O. [2013])

For any tree T_τ, there exist at least continuum many pairwise distinct isometries from the metric space $\overline{\Omega T}_\tau$ to the Hamming space of τ-periodic $(0,1)$-sequences $\mathcal{H}(\tau)$.

Spherically Transitive Automorphisms

An automorphism α of spherically homogeneous rooted tree T_τ is called spherically transitive, if the cyclic group $\langle\alpha\rangle$ acts transitively on each level of the tree T_τ. A typical example of a spherically transitive automorphism is the "adding machine".

Example: Adding Machine

The adding machine is an automorphism of the spherically homogeneous rooted tree T_υ with spherical index $\nu = [n; n; \ldots,]$. This automorphism can be defined via the following figure:

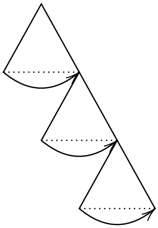

Figure 1

Spherically Transitive Automorphisms

Every automorphism of the rooted tree T_τ acts as an isometry on the boundary $(\partial T_\tau, \rho)$, and conversely, every isometry of the boundary arises from an automorphism of T_τ.

Construction of Isometry

Let t_0 be a fixed point from the boundary ∂T_τ, w be the "adding machine". For any subset $A \subset \partial T_\tau$ let us define an infinite $(0, 1)$-sequence $s_w(A) = (a_0, a_1, a_2, \ldots)$ by the rule

$$a_n = \begin{cases} 1, & \text{if } w^n(t_0) \in A \\ 0, & \text{if } w^n(t_0) \notin A \end{cases}. \tag{1}$$

In this way we obtain the mapping F_w defined on the set of all subsets of the boundary ∂T_τ to the set of all infinite $(0, 1)$-sequences. Let f_w denotes the restriction of F_w on the set ΩT_τ of all clopen subsets of the boundary ∂T_τ.

Periodic Hamming Spaces and Clopen Sets

Theorem (B.O. [2013])

For arbitrary strictly increasing sequence τ of positive integers the mapping f_w is an isometry from the space ΩT_τ of all clopen subsets of the boundary ∂T_τ equpped with the metric d_μ to the Hamming space of τ-periodic $(0,1)$-sequences.

Now we describe, for any Steinitz number u, the isometry group of the u-periodic Hamming space and the isometry group of the Besicovitch-Hamming space. We also introduce constructions similar to the wreath product of groups.

Group of Homeomorphisms

Consider the set $C(\partial T_\tau, S_2)$ of all continuous function from ∂T_τ to S_2. Define a binary operation $*$ on this set. For any $f, g \in C(\partial T_\tau, S_2)$

$$(f * g)(x) = f(x) \cdot g(x)$$

for all $x \in \partial T$. Then $C(\partial T, S_2)$ with operation $*$ is a group. Denote by $(Homeo\partial T_\tau \cap Aut(\partial T_\tau, \mu))$ the group of all homeomorphisms of the boundary ∂T_τ that preserve the measure μ.

Group of Homeomorphisms

The group $(Homeo\partial T_\tau \cap Aut(\partial T_\tau, \mu))$ acts on $C(\partial T_\tau, S_2)$ by generalized translations. Specifically, for $g \in (Homeo\partial T_\tau \cap Aut(\partial T_\tau, \mu))$ and $h \in C(\partial T_\tau, S_2)$ let

$$h^g(x) = h(x^g), x \in \partial T_\tau.$$

This action is an automorphism of $C(\partial T_\tau, S_2)$. Consequently, we can consider the semidirect product $C(\partial T_\tau, Z_2) \rtimes (Homeo\partial T_\tau \cap Aut(\partial T_\tau, \mu))$.

Periodic Hamming Spaces and Homeomorphisms

Theorem (B.O., V. Sushchansky [2013])

The isometry group $Isom\mathcal{H}(u)$ of the u-periodic Hamming space $\mathcal{H}(u)$ is isomorphic as a transformation group to the semidirect product

$$C(\partial T_\tau, Z_2) \rtimes (Homeo\partial T_\tau \cap Aut(\partial T_\tau, \mu)),$$

where T_τ is the spherically homogeneous rooted tree and μ is the Bernoulli measure on the σ-algebra of clopen sets of ∂T_τ.

Isometries of the Besicovitch-Hamming Space

Denote by $Fun_\mu(\partial T_\tau, S_2)$ the group of measurable functions from ∂T_τ to S_2.

Theorem (B.O., V. Sushchansky [2013])

The isometry group $Isom\mathcal{H}$ of the Besicovitch-Hamming space $\mathcal{H}$ is isomorphic as a transformation group to the semidirect product

$$Fun_\mu(\partial T_\tau, S_2) \rtimes Aut(\partial T_\tau, \mu),$$

where T_τ is the spherically homogeneous rooted tree and μ is the Bernoulli measure on the σ-algebra of clopen sets of ∂T_τ.

Hyperoctahedral Groups

The group W_n consists of all pairs $[\sigma, f]$, where $\sigma \in S_n$, $f \in Z_2^{\underline{n}}$, $\underline{n} = \{1, \ldots, n\}$. Denote $f(i) = a_i$, $(1 \leq i \leq n)$. Each pair $[\sigma, f]$ corresponds to a unique sequence $[\sigma; a_1, \ldots, a_n]$. Then the group operation in $Z_2 \wr S_n$ is determined by the equality

$$[\sigma; a_1, \ldots, a_n][\eta; b_1, \ldots, b_n] = [\sigma\eta; a_1 + b_{1^\sigma}, \ldots, a_n + b_{n^\sigma}],$$

where $+$ denotes the addition in Z_2.

Hyperoctahedral Groups

The inverse of the element $[\sigma; a_1, \ldots, a_n]$ is the element

$$[\sigma^{-1}; a_{1^{\sigma^{-1}}}, \ldots, a_{n^{\sigma^{-1}}}].$$

A transformation $u = [\sigma; a_1, \ldots, a_n]$ acts on the vector $\bar{t} = (t_1, \ldots, t_n) \in Z_2^n$ according to the rule

$$t^u = (t_{1^\sigma} + a_1, \ldots, t_{n^\sigma} + a_n).$$

Direct Limits of Hyperoctahedral Groups

We define embeddings between permutation groups:

$$(W_{m_i}, Z_2^{m_i}) \hookrightarrow (W_{m_{i+1}}, Z_2^{m_{i+1}})$$

via two maps:

$$h_i : W_{m_i} \to W_{m_{i+1}}, \qquad \delta_i : Z_2^{m_i} \to Z_2^{m_{i+1}}.$$

- $h_i([\sigma; a_1, \ldots, a_{m_i}]) = [\theta^{s_{i+1}}\sigma;\ \text{repetition of } (a_1, \ldots, a_{m_i})]$
- $\delta_i(t_1, \ldots, t_{m_i}) = \text{repetition of } (t_1, \ldots, t_{m_i})$

Action of $\theta^{s_{i+1}}\sigma$

The permutation $\theta^{s_{i+1}}\sigma$ acts blockwise:

$$\theta^{s_{i+1}}\sigma =$$
$$\left(\begin{array}{ccc|c|ccc} 1 & \dots & m_i & \dots & (s_{i+1}-1)m_i+1 & \dots & s_{i+1}m_i \\ 1^\sigma & \dots & m_i^\sigma & \dots & (s_{i+1}-1)m_i+1^\sigma & \dots & (s_{i+1}-1)m_i+m_i^\sigma \end{array}\right).$$

Direct Limits of Hyperoctahedral Groups

The increasing divisible sequence $\tau = (m_1, m_2, \ldots)$ determines the direct spectrum

$$\langle (W_{m_i}, Z_2^{m_i}), F_i \rangle_{i \in \mathbb{N}}. \tag{2}$$

of hyperoctahedral groups $(W_{m_i}, Z_2^{m_i})$.
We call the direct limit of directed system (2) the *D-hyperoctahedral group* corresponding to the sequence τ and denote it by $W(\tau)$.

Isomorphic D-Hyperoctahedral Groups

Theorem (B.O., V. Sushchansky [2014])

Let τ_1, τ_2 be increasing divisible sequences. The groups $W(\tau_1)$ and $W(\tau_2)$ are isomorphic if and only if $char \tau_1 = char \tau_2$.

Metric Groups of Homeomorphisms

Equip the group of homeomorphisms $Homeo\partial T_\tau$ and the group $C(\partial T_\tau, Z_2)$ with the metrics

$$\sigma_\tau(f,g) = \max_{x\in\partial T_\tau} \rho_\tau(x^g, x^f), \qquad \text{for all } f,g \in Homeo\partial T_\tau,$$

$$\hat{\sigma}_\tau(h,t) = \begin{cases} 1, & \text{if } h \neq t \\ 0, & \text{if } h = t \end{cases}, \qquad \text{for all } h,t \in C(\partial T_\tau, Z_2).$$

Isometry Groups of Periodic Hamming Spaces

Theorem (B.O., V. Sushchansky [2013])

The isometry group $\mathcal{H}(u)$ of the u-periodic Hamming space $\mathcal{H}(u)$ is the closure of D-hyperoctahedral group $W(\tau)$, $char\tau = u$, regarded as a subgroup of $C(\partial T_\tau, Z_2) \rtimes Homeo\partial T_\tau$ in the Tychonoff product of topologies induced by the metrics σ_τ and $\hat{\sigma}_\tau$.

Open question

- *What is the structure of the isometry group of the periodic Hamming space over an alphabet $|B|$, $|B| > 2$?*
- *What is the structure of the isometry group of its completion?*

Peter J. Cameron, Sam Tarzi, *Limits of cubes*, Topology and its Applications, Volume 155, Issue 14 (2008), 1454–1461.

References

M. Baake, *Structure and representation of the hyperoctahedral group*, J. Math. Phys., 25 (1984), 3171–3182.

M. Ch. Klin, R. Poeschel, K. Rosenbaum, *Angewandte Algebra f?r Mathematiker und Informatiker*, VEB Deutscher Verlag der Wissenschaften, Berlin, 1988.

F. Blanchard, E. Formenti, P. Kurka, *Cellular Automata in Cantor, Besicovitch and Weil Topological Spaces*, Complex Systems, 11 (1997), 107–123.

A. M. Vershik, *The Pascal automorphism has a continuous spectrum*, Funct. Anal. Appl., 45 (2011), 173–186.

A. M. Vershik, *Theory of decreasing sequences of measurable*

References

- B. Oliynyk, *Isometry groups of an extended Hamming space and an infinite-dimensional hypercube*, Dopov. Nats. Akad. Nauk Ukr., Mat. Pryr. Tekh. Nauky, no. 12 (2013), 25–29.
- B. Oliynyk, *An isometric representation of the Hamming space of periodic sequences on the boundary of a rooted tree*, Dopov. Nats. Akad. Nauk Ukr., Mat. Pryr. Tekh. Nauky, no. 11 (2013), 31–36.
- B. Oliynyk, V. Sushchanskii, *Isometry groups of Hamming spaces of periodic sequences*, Sib. Math. J., 54 (2013), no. 1, 124–136.
- B. Oliynyk, V. Sushchanskii, *Imprimitivity systems and lattices of normal subgroups in D-hyperoctahedral groups*, Sib. Math. J., 55 (2014), no. 1, 132–141.

Thank you for your attention!