Geometrie związane z kodami binarnymi o stałej odległości

Mariusz Żynel

Uniwersytet w Białymstoku
Wydział Matematyki

Seminarium Wydziału Matematyki UwB, 3 grudnia 2025

Coding theory in most general settings

- *Alphabet* – a finite set, say A, and let $q = |A|$
- *Word* – element of A^n, $n \in \mathbb{N}$
- *Hamming distance* – the number of coordinates at which two words differ, that is, a function

$$\mathrm{d}\colon A^n \times A^n \longmapsto [n] = \{0, 1, \ldots, n\}, \quad \mathrm{d}(a, b) = \left|\{i \colon a_i \neq b_i\}\right|$$

- *Code, q-ary code* – a non-empty subset of A^n, say $C \subseteq A^n$
- *Codeword* – element of a code
- The *length* of C is n, the *dimension* of C is $k = \log_q |C| \in \mathbb{R}$
- Why such a subset C is called an *error-correcting code*?

Linear codes

- *Alphabet* – finite field F_q of q elements
- *Code*, $[n, k]_q$ *code* – k-dimensional subspace of F_q^n, $n \in \mathbb{N}$

Linear equidistant codes

- The *Hamming distance* between any two distinct codewords is constant
- All non-zero codewords have constant *Hamming weight*
- *Simplex codes* are equidistant codes

MacWilliams extension theorem

- Let $V = F_2^n$. The standard basis of V is

$$e_1 = (1, 0, \ldots, 0), \ldots, e_n = (0, \ldots, 0, 1)$$

- A semilinear automorphism of V is called *monomial* if it sends every e_i to a scalar multiple of e_j, that is:

$$e_i \mapsto a_i e_{j(i)}$$

Theorem (F.J. MacWilliams 1962)

Let X, Y be subspaces of V. Every semilinear isomorphism of X onto Y preserving the Hamming weight, in both directions, can be uniquely extended to a monomial semilinear automorphism of V.

Outline of our result

M. Pankov, K. Petelczyc, M. Żynel
Point-line geometries related to binary equidistant codes
J. Combin. Theory Ser. A 210 (2025), 1-30.

- A complete characterization of automorphism of the point-line geometry of linear equidistant codes is given
- In some non-trivial cases, there are automorphism of this geometry induced by non-monomial semilinear automorphism of the ambient vector space

Point-line geometries

- Let $\mathcal{P}$ be a set whose elements will be called *points* and let $\mathcal{L}$ be a family of subsets of $\mathcal{P}$ called *lines*
- A pair $(\mathcal{P}, \mathcal{L})$ is called a *point-line geometry* whenever
  - every line contains at least two points and
  - two distinct lines share at most one point
- Two distinct points are said to be *collinear* if there is a line containing them
- A subset $X \subseteq \mathcal{P}$ is called a *subspace* whenever for any two distinct and collinear points from X, the entire line through them is contained in X
- A subspace is *singular* when every two of its distinct points are collinear

Automorphisms of point-line geometries

- In a point-line geometry, a one-to-one transformation of its pointset preserving the family of its lines in both directions is called an *automorphism* (a *collineation*)
- Collineations preserve binary collinearity as well as binary non-collinearity of points

Settings for our point-line geometry

- Let $V = F_2^n$. The standard basis of V is
$$e_1 = (1, 0, \dots, 0), \dots, e_n = (0, \dots, 0, 1)$$
- For every non-zero vector v of V we have
$$v = e_I = \sum_{i \in I} e_i, \qquad \emptyset \neq I \subseteq [n] = \{1, 2, \dots, n\}$$
- The i-th coordinate of e_I is either 1, if $i \in I$, or 0 otherwise
- $\mathcal{P}(V)$ is the projective space over V
- P_I is the point of $\mathcal{P}(V)$ corresponding to e_I ($e_I \neq 0$, $I \neq \emptyset$)
- If P, Q are distinct points in $\mathcal{P}(V)$, then
$$\overline{P, Q} = \langle P, Q \rangle = \{P, Q, P \odot Q\}$$
- For non-empty subsets $I, J \subset [n]$ we have
$$e_I + e_J = e_{I \triangle J}, \quad \text{consequently} \quad P_I \odot P_J = P_{I \triangle J}$$

Our point-line geometry

- For every point P_I of $\mathcal{P}(V)$ its Hamming weight is

$$\mathrm{w}(P_I) = |I|$$

- Let $m \in \mathbb{N}$ such that $3m \leq n$
- Take all those points of the projective space $\mathcal{P}(V)$ with Hamming weight $2m$

$$\mathcal{P}_m = \{P_I \in \mathcal{P}(V) \colon |I| = 2m\}$$

- $\mathcal{P}_m$ can be considered a point-line geometry where lines are the lines of the projective space $\mathcal{P}(V)$ contained in $\mathcal{P}_m$
- For distinct $P_I, P_J \in \mathcal{P}_m$ we have

$$P_I \odot P_J \in \mathcal{P}_m \quad \text{iff} \quad |I \cap J| = m$$

Point-line geometry of linear equidistant codes

- The Hamming distance between any two distinct collinear points $P, Q \in \mathcal{P}_m$ is

$$\mathrm{d}(P, Q) = \mathrm{w}(P \odot Q) = 2m$$

- There is a natural one-to-one correspondence between singular subspaces of the point-line geometry $\mathcal{P}_m$ and $2m$-equidistant codes of V
- Maximal singular subspaces of the point-line geometry $\mathcal{P}_m$ correspond to maximal $2m$-equidistant codes of V

Geometries in our class

- A line of size 3 ($n = 3m = 3$)
- The Pasch (Veblen) configuration ($n = 3m + 1 = 4$)
- The Cremona-Richmond configuration known also as the generalized quadrangle of type $2, 2$ ($n = 3m = 6$)
- A polar space ($n = 4m - 1 = 7$)
- If $n = 4m - 1 = 2^k - 1$, then the maximal singular subspaces of $\mathcal{P}_m$ correspond to binary simplex codes of dimension k

Remark

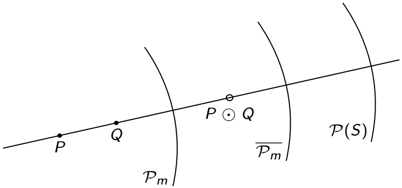
All the geometries in our class can be considered partial Steiner triple systems embedded in Steiner triple systems which are projective spaces over the two-element field

Linear automorphisms

- Every linear automorphism, in particular, a coordinate permutation (a monomial linear automorphism) of V preserving the pointset $\mathcal{P}_m$ induces an automorphism of the point-line geometry of linear equidistant codes $\mathcal{P}_m$

Hyperplane closure

- Let S be the hyperplane of V made up by all vectors
$$(x_1, \dots, x_n) \in V \qquad \text{with} \qquad x_1 + x_2 + \cdots + x_n = 0$$
- A projective point $P_I \in \mathcal{P}(V)$ is contained in S iff $|I|$ is even
- For any distinct $P, Q \in \mathcal{P}_m$ the point $P \odot Q$ belongs to $\mathcal{P}(S)$
- $\overline{\mathcal{P}_m} = \{P \odot Q \in \mathcal{P}(S) \colon P, Q \in \mathcal{P}_m\}$



- $\overline{\mathcal{P}_m} = \mathcal{P}(S)$ only if $n = 4m - 1,\ 4m,\ 4m + 1$
- Every non-zero vector of the hyperplane S is the sum of some vectors of Hamming weight $2m$
- $\mathcal{P}(S)$ is the smallest projective space containing $\mathcal{P}_m$

Horizon

- Let $R \in \overline{\mathcal{P}}_m \setminus \mathcal{P}_m$
- $\mathcal{L}_R = \{\overline{P, Q} \subset \mathcal{P}(S) \colon P, Q \in \mathcal{P}_m, \ R = P \odot Q\}$
- For pairwise distinct points $P, Q, P', Q' \in \mathcal{P}_m$ such that

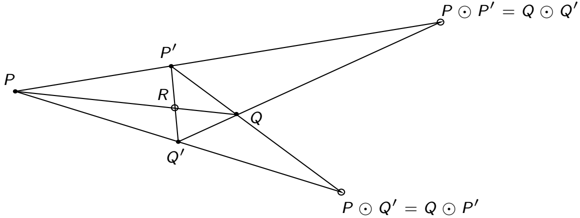
$$R = P \odot Q = P' \odot Q'$$

we write

$$\overline{P, Q} \sim \overline{P', Q'}$$

whenever

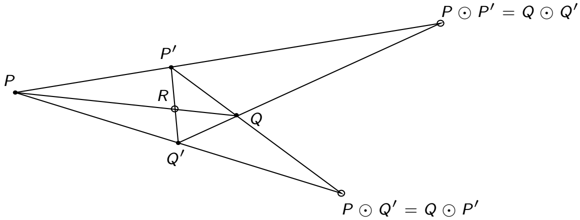
$$P \odot P' = Q \odot Q' \in \mathcal{P}_m \quad \text{or} \quad P \odot P' = Q \odot Q' \in \mathcal{P}_m$$



- Relation $\sim$ on $\mathcal{L}_R$ is transitive

Extension of an automorphism to the horizon

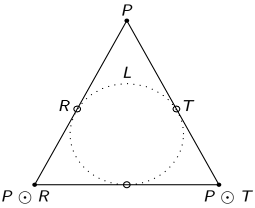
- Let f be an automorphism of $\mathcal{P}_m$
- For points $P, Q, P', Q' \in \mathcal{P}_m$, if $P \odot Q = P' \odot Q'$, then
$$f(P) \odot f(Q) = f(P') \odot f(Q')$$



- For every point $R \in \overline{\mathcal{P}}_m \setminus \mathcal{P}_m$ we take points $P, Q \in \mathcal{P}_m$ such that $R = P \odot Q$ and define
$$f(R) = f(P) \odot f(Q)$$
- This extension of f is bijective and preserves the family of lines containing at least two points from $\mathcal{P}_m$ in both directions

Linear automorphism of the hyperplane

- Triangle is said to be a union of three lines on a Fano plane if their intersections are pairwise distinct
- Line L can be characterized as the set of those points of a triangle which are not its vertices



- If a line L contains two points $R, T \in \overline{\mathcal{P}}_m$ and there is a point $P \in \mathcal{P}_m$ such that $P \odot R, P \odot T \in \mathcal{P}_m$, then the lines

$$\overline{P, R}, \quad \overline{P, T}, \quad \overline{P \odot R, P \odot T}$$

  form a triangle whose vertices are points in $\mathcal{P}_m$
- The extension of f to $\overline{\mathcal{P}}_m$ preserves lines

Theorem (Fundamental Theorem of Projective Geometry)

Every automorphism of a projective space is induced by a semilinear automorphism of the ambient vector space.

Specific linear automorphism for $n = 4m - 1$

- Let $i \in [n]$ and consider a linear automorphism of V

$$f_i(e_j) = \begin{cases} e_j, & j \neq i, \\ e_{[n]}, & j = i, \end{cases}$$

  for all $j \in [n]$

- Note that $f_i(e_I) = e_I$ when $i \notin I$
- For $i \in I \subset [n]$ we have

$$f_i(e_I) = e_{[n]} + e_{I \setminus \{i\}} = e_{[n] \setminus (I \setminus \{i\})}$$

- If $|I| = 2m$, then

$$\big|[n] \setminus (I \setminus \{i\})\big| = 4m - 1 - (2m - 1) = 2m$$

- Therefore f_i preserves the pointset $\mathcal{P}_m$

Specific linear automorphisms for $n = 4m$

- Let $i, j \in [n]$, $i \neq j$, and consider linear automorphisms of V

$$f_{ij}(e_t) = \begin{cases} e_t, & t \neq i, j, \\ e_{[n]\setminus\{i\}}, & t = i, \\ e_{[n]\setminus\{j\}}, & t = j, \end{cases} \qquad g_{ij}(e_t) = \begin{cases} e_t, & t \neq i, j, \\ e_{[n]\setminus\{j\}}, & t = i, \\ e_{[n]\setminus\{i\}}, & t = j, \end{cases}$$

  for all $t \in [n]$
- Note that $f_{ij}(e_I) = g_{ij}(e_I) = e_I$ when $i, j \notin I$
- For $i, j \in I \subset [n]$ we have

$$f_{ij}(e_I) = g_{ij}(e_I) = e_{[n]\setminus\{i\}} + e_{[n]\setminus\{j\}} + e_{I\setminus\{i,j\}} = e_{\{i,j\}} + e_{I\setminus\{i,j\}} = e_I$$

- If $|I| = 2m$ and I contains only one of i, j, say i, then

$$f_{ij}(e_I) = e_{[n]\setminus\{i\}} + e_{I\setminus\{i\}} = e_{[n]\setminus I}$$

$$g_{ij}(e_I) = e_{[n]\setminus\{j\}} + e_{I\setminus\{i\}} = e_{([n]\setminus\{j\})\setminus(I\setminus\{i\})}$$

$$\big|[n] \setminus I\big| = 2m \qquad \text{and} \qquad \big|([n] \setminus \{j\}) \setminus (I \setminus \{i\})\big| = 2m$$

- Therefore, both f_{ij} and g_{ij} preserve the pointset $\mathcal{P}_m$

Our result

Theorem (M. Pankov, K. Petelczyc, M.Ż. 2025)

Every automorphism of the geometry $\mathcal{P}_m$ is induced by a coordinate permutation (monomial linear automorphism) of V or it is the composition of the automorphism induced by a coordinate permutation and, in case

- $n = 4m - 1$

$$f_i(e_j) = \begin{cases} e_j, & j \neq i, \\ e_{[n]}, & j = i, \end{cases}$$

  for some $i \in [n]$,

- $n = 4m$

$$f_{ij}(e_t) = \begin{cases} e_t, & t \neq i, j, \\ e_{[n]\setminus\{i\}}, & t = i, \\ e_{[n]\setminus\{j\}}, & t = j, \end{cases} \quad \text{or} \quad g_{ij}(e_t) = \begin{cases} e_t, & t \neq i, j, \\ e_{[n]\setminus\{j\}}, & t = i, \\ e_{[n]\setminus\{i\}}, & t = j, \end{cases}$$

  for some distinct $i, j \in [n]$.

Non-binary case

- Let $V = F_q^n$ where $q > 2$
- Take all those vectors of V which Hamming weight is t

$$V_t = \{v \in V \colon |v| = t\}$$

- Take all those points of the projective space $\mathcal{P}(V)$ which are spanned by vectors from V_t

$$\mathcal{H}_t = \{\langle v \rangle \in \mathcal{P}(V) \colon v \in V_t\}$$

- $\mathcal{H}_t$ can be considered a point-line geometry whose lines are the lines of the projective space $\mathcal{P}(V)$ contained in $\mathcal{H}_t$
- For $n = \frac{q^k - 1}{q - 1}$ and $t = q^{k-1}$ maximal singular subspaces of $\mathcal{H}_t$ correspond to q-ary simplex codes of dimension k
- There are lines of $\mathcal{P}(V)$ connecting non-collinear points of $\mathcal{H}_t$ that contain more than one point not in $\mathcal{H}_t$

Dziękuję za uwagę

The Pasch (Veblen) configuration

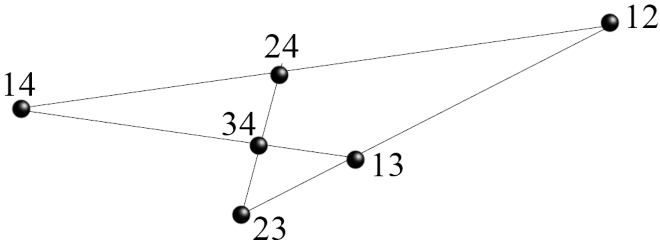


Figure: Points and lines of $\mathcal{P}_1$ for $n = 3m + 1 = 4$

The Cremona-Richmond configuration

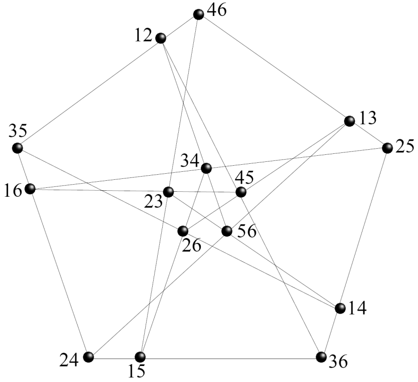


Figure: Points and lines of $\mathcal{P}_2$ for $n = 3m = 6$

Every $P_I \in \mathcal{P}_2$ is identified with its complement, the 2-element subset $[6] \setminus I$, and three points of $\mathcal{P}_2$ form a line if and only if the corresponding 2-element subsets are mutually disjoint.