Partial permutation decoding of the binary code of the projective plane PG$(2, q)$, q even

Leo Storme

Ghent University
Dept. of Mathematics: Analysis, Logic and Discrete Mathematics
Krijgslaan 281 - Building S8
9000 Ghent
Belgium

Finite Geometries Sixth Irsee Conference
(joint work with D. Crnković, N. Mostarac and B. Rodrigues)

OUTLINE

Outline

1. Permutation decoding of linear codes
2. Linear codes from finite projective planes
3. Basis and 2-PD-set for code of PG$(2, 2^h)$

TRANSMISSION OF INFORMATION

In coding theory,

- **messages** encoded into codewords.
- **Linear** $[n, k, d]$**-code** C **over** $\mathbb{F}_q$ is:
  - k-dimensional subspace of $V(n, q)$,
  - *minimum (Hamming) distance* d = minimal number of positions in which two distinct codewords differ.
- If $d = 2t + 1$ or $d = 2t + 2$, then C is t**-error correcting**.

Transmission of information

- **Generator matrix of** $[n, k, d]$**-code** C**:**

$$G = (g_1 \cdots g_n)$$

  - $G = (k \times n)$ matrix of rank k,
  - rows of G form basis of C,
  - codeword of C = linear combination of rows of G.
- **Message** $(u_1, \ldots, u_k)$ becomes **codeword**

$$(u_1, \ldots, u_k) \cdot G = (c_1, \ldots, c_n).$$

Generator matrix in standard form

- Generator matrix of $[n, k, d]$-code C is in **standard form** when
$$G = (I_k\ A),$$
with A a $k \times (n-k)$ matrix.
- Message $(u_1, \ldots, u_k)$ becomes codeword
$$(u_1, \ldots, u_k) \cdot G = ((u_1, \ldots, u_k), (u_1, \ldots, u_k) \cdot A).$$
- First k positions are the **information positions** and last $n-k$ positions are the **check positions**.

PERMUTATION DECODING OF LINEAR CODES

(F.J. MacWilliams)

Permutation decoding of linear codes

- Let G be the group of the permutations on the positions which leave C invariant.
- An *s*-**PD-set** of permutations is set of elements of G such that for every error vector of weight s, there exists a permutation σ in G which moves the s errors out of the information positions.

Questions:

- Does a linear code have an s-PD set?
- If yes, construct a smallest possible s-PD set.
- How do we know that the s errors are out of the information positions?

Permutation decoding of linear codes

Theorem

Let C be a t-error correcting linear $[n, k, d]$-code, with generator matrix G in standard form $G = (I_k\ A)$ and parity check matrix $H = (-A^t\ I_{n-k})$.
Let c be a transmitted codeword of C and assume that the vector $y = c + e$ is received, where e is an error vector of weight at most t.
Then the errors are outside of the information positions if and only $wt(y \cdot H^t) < t$.

Outline

Codes from projective planes

- PG$(2, q)$, $q = p^h$, p prime, $h \geq 1$.
- Points P_j, $j = 1, \ldots, q^2 + q + 1$, and lines ℓ_i, $i = 1, \ldots, q^2 + q + 1$.
- **Incidence matrix**

$$G = \begin{pmatrix} & & \\ & & \\ & & \end{pmatrix} \leftarrow \text{lines } \ell_i$$

$$\uparrow$$
$$\text{points } P_j$$

with
$G_{ij} = 1$ iff $P_j \in \ell_i$,
$G_{ij} = 0$ iff $P_j \notin \ell_i$.

CODE DEFINED BY THE INCIDENCE MATRIX

- G = generator matrix of $[n, k, d]$-code $C = C(2, q)$ over $\mathbb{F}_p$, with
  - $n = q^2 + q + 1$,
  - $k = \binom{p+1}{2}^h + 1$,
  - $d = q + 1$.
- Similar code arises from AG$(2, q)$, $q = p^h$, p prime, $h \geq 1$.

MOORHOUSE BASIS FOR $C(AG(2,p))$, p PRIME

- Take one line M in PG$(2, q)$.
- Let $M = \{r_0, r_1, \ldots, r_p\}$.
- Take the p lines through r_0, different from M,
- Take $p-1$ lines through r_1, different from M,
- $\cdots$,
- Take $p-i$ lines through r_i, different from M,
- $\cdots$,
- Take one line through r_{p-1}, different from M.

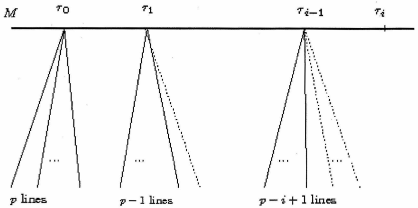


Fig. 1 The basis of Moorhouse

MOORHOUSE BASIS FOR $C(AG(2, p))$, p PRIME

- Line at infinity: $l_1 = [0, 0, 1]$.
- p lines $[1, 0, a]$, $0 \leq a \leq p - 1$, through point (0, 1, 0),
- $p - 1$ lines $[1, 1, a]$, $1 \leq a \leq p - 1$, through point $(1, -1, 0)$,
- $p - 2$ lines $[1, 2, a]$, $2 \leq a \leq p - 1$, through point $(1, -2^{-1}, 0)$,
- $p - i$ lines $[1, i, a]$, $i \leq a \leq p - 1$, through point $(1, -i^{-1}, 0)$
- $\ldots$,
- the line $[1, p - 1, p - 1]$ through the point $(1, 1, 0)$.

Moorhouse basis for $C(AG(2,p))$, p prime

Equivalent formulation: points as information set

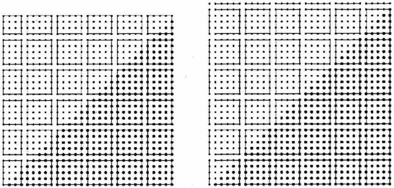
$$\begin{array}{ccccc}
(0,0) & (0,1) & (0,2) & \cdots & (0,p-1) \\
 & (1,1) & (1,2) & \cdots & (1,p-1) \\
 & & (2,2) & \cdots & (2,p-1) \\
 & & & \ddots & \\
 & & & & (p-1,p-1)
\end{array}$$

The information set I and check set H are equal to:

$$I = \{(i,j) : 0 \leq i \leq j \leq p-1\}$$

and

$$H = \{(i,j) : p-1 \geq i > j \geq 0\}.$$



A: $p = 29$.   B: $p = 31$.

Consider the translations $\tau_{a,b} : (x, y) \mapsto (x, y) + (a, b)$.

THEOREM (KEY, MACDONOUGH, MAVRON)

Let C_A be the p-ary code from the affine plane $AG(2, p)$, $p \geq 5$ prime. Let $n = \lfloor \frac{p+1}{6} \rfloor$ and let $Y = \{\tau_{un,-vn} : 0 \leq u, v \leq 5\}$. For the predefined information set I, Y is a 2-PD-set of size 36 for the code of $AG(2, p)$ when $p \equiv -1 \pmod 6$ and $Y \cup \{\tau_{1,1}\}$ is a 2-PD-set of size 37 for the code of $AG(2, p)$ when $p \equiv 1 \pmod 6$.

Outline

NOTATIONS

- Let $q = 2^h$ and let α be a primitive element of $\mathbb{F}_{2^h}$.
- Let

$$\beta = a_{h-1}\alpha^{h-1} + a_{h-2}\alpha^{h-2} + \cdots + a_1\alpha + a_0, \beta \neq 0,$$

  where all $a_i \in \mathbb{F}_2$.
- $|\beta| = |\{i : a_i \neq 0\}|$.
- **Leading position** of β: $lp(\beta) = \max\{i : a_i \neq 0\} + 1$.
- **Leading position** of point $b = (0, 1, \beta)$ is $lp(\beta)$.
- **Leading position** of $(0, 1, 0)$ is 0 and **leading position** of $(0, 0, 1)$ is $+\infty$.

Basis of P. Vandendriessche

Theorem

The line $X_0 = 0$ and the set of lines

$$\{\langle (0, 1, \beta), (1, 0, \gamma)\rangle : |\gamma| + lp(\beta) \leq h\}$$

together form a basis for code of PG$(2, 2^h)$, with $5 \leq h \leq 9$.

The line $X_0 = 0$ has homogeneous coordinates $[1, 0, 0]$. The set of lines from the previous theorem consists of lines with homogeneous coordinates $[\gamma, \beta, 1]$, where $|\gamma| + lp(\beta) \leq h$.
Question: Is this also basis for $h > 9$?

2-PD-set for code of PG$(2, 2^h)$, $5 \leq h \leq 9$.

- $$\hat{\tau}_{u,v}([\gamma, \beta, 1]) = [\gamma + u, \beta + v, 1],$$
  $$\hat{\tau}_{u,v}([1, 0, 0]) = [1, 0, 0],\ \hat{\tau}_{u,v}([\gamma, 1, 0]) = [\gamma, 1, 0].$$
- $\sigma_1 : [u, v, w] \mapsto [v, u, w]$,
- $\sigma_2 : [u, v, w] \mapsto [w, v, u]$.

2-PD-SET FOR CODE OF PG$(2, 2^h)$, $5 \leq h \leq 9$.

THEOREM (CRNKOVIĆ, MOSTARAC, RODRIGUES, STORME)

Let $\Pi = \mathrm{PG}(2, 2^h)$*,* $5 \leq h \leq 9$*, and let*
$C : [2^{2h} + 2^h + 1, 3^h + 1, 2^h + 1]_2$ *be its binary code.*
Let

$$a = (1, 0, ..., 0), a' = (0, 1, 0, ..., 0),$$

$$b = (1, ..., 1, 0), c = (1, ..., 1).$$

Then following set S *is 2-PD-set of size 16 for* C*, for the information set* I*:*

$$S = \{\hat{\tau}_{0,0}, \hat{\tau}_{a,a}, \hat{\tau}_{a,b}, \hat{\tau}_{a,c}, \hat{\tau}_{a',b}, \hat{\tau}_{b,a}, \hat{\tau}_{b,b}, \hat{\tau}_{b,c}, \hat{\tau}_{c,a}, \hat{\tau}_{c,b}, \hat{\tau}_{c,c}, \sigma_1,$$

$$\hat{\tau}_{a,b}\sigma_1, \hat{\tau}_{a,c}\sigma_1, \hat{\tau}_{b,c}\sigma_1, \hat{\tau}_{a,c}\sigma_2\}.$$

Search for these permutations

Example:

- Assume two errors in the positions $[\gamma_1, \beta_1, 1]$, with $|\gamma_1| + lp(\beta_1) \leq h$, and $[\gamma_2, \beta_2, 1]$, with $|\gamma_2| + lp(\beta_2) \leq h$.
- Find translations $\tau_{u,v}$ such that

$$(\gamma_i, \beta_i) + (u, v) = (\gamma_i + u, \beta_i + v),$$

with

$$|\gamma_i + u| + lp(\beta_i + v) > h, i = 1, 2.$$

3-PD-SET FOR CODE OF PG$(2, 2^9)$

THEOREM (CRNKOVIĆ, MOSTARAC, RODRIGUES, STORME)

Let $\Pi = \mathrm{PG}(2, q)$, $q = 2^h$, and let G be its automorphism group. Furthermore, let $C_{\mathrm{gen}} = [q^2 + q + 1, 3^h + 1, q + 1]_2$ be the binary code of Π. If $h = 9$, a 3-PD-set for C_{gen} consisting of 75 elements can be found in G, for the information set I.

Thank you very much for your attention!