s-PD-sets for codes from projective planes $\mathrm{PG}(2, 2^h)$, where $5 \leq h \leq 9$

Nina Mostarac (nmavrovic@math.uniri.hr)
Faculty of Mathematics, University of Rijeka, Croatia

Joint work with:

Dean Crnković

Bernardo G. Rodrigues

Leo Storme

RICCOTA 2023
Rijeka Conference on Combinatorial Objects and Their Applications

July 7, 2023

Introduction

- permutation decoding was introduced in 1964 by MacWilliams
- it uses sets of code automorphisms called PD-sets
- the problem of existence of PD-sets and finding them
- we construct 2-PD-sets and 3-PD-sets for partial permutation decoding of codes obtained from certain **Desarguesian projective planes**

Refrences

[1] D. Crnković, N. Mostarac, B. G. Rodrigues, L. Storme, s-PD-sets for codes from projective planes $PG(2, 2^h)$, $5 \leq h \leq 9$, *Adv. Math. Comm.*, **15 (3)** (2021), 423–440.

[2] P. Vandendriessche, Codes of Desarguesian projective planes of even order, projective triads and $(q + t, t)$-arcs of type $(0, 2, t)$, *Finite Fields Appl.*, **17** (2011), 521–531.

- in [1] we construct 2-PD-sets of 16 elements for codes from $\mathrm{PG}(2, q)$, where $q = 2^h$ and $5 \leq h \leq 9$
- we also construct 3-PD-sets of 75 elements for the code from $\mathrm{PG}(2, q)$, where $q = 2^9$
- we use a basis of a code of a projective plane $\mathrm{PG}(2, 2^h)$, that was found by Vandendriessche [2] for $h \leq 9$

Codes

Definition 1

Let p be a prime. A p–ary linear code C of **length** n and **dimension** k is a k-dimensional subspace of the vector space $(\mathbb{F}_p)^n$.

Definition 2

- Let $x = (x_1, \dots, x_n)$ and $y = (y_1, \dots, y_n) \in \mathbb{F}_p^n$. The Hamming distance between words x and y is the number $d(x, y) = |\{i : x_i \neq y_i\}|$.
- The **minimum distance** of the code C is defined by $d = \min\{d(x, y) : x, y \in C,\ x \neq y\}$.

- Notation: $[n, k, d]_p$ code
- it can detect at most $d - 1$ errors in one codeword and correct at most $t = \left\lfloor \frac{d-1}{2} \right\rfloor$ errors

Information sets

- The algorithm of **permutation decoding** (introduced in 1964 by MacWilliams) uses sets of code automorphisms called PD-sets, that are defined **with respect to a given information set** of the code.

Definition 3

Let $C \subseteq \mathbb{F}_p^n$ be a linear $[n, k, d]$ code. For $I \subseteq \{1, \dots, n\}$ let $p_I : \mathbb{F}_p^n \to \mathbb{F}_p^{|I|}$, $x \mapsto x|_I$, be an I-projection of $\mathbb{F}_p^n$. Then I is called an information set for C if $|I| = k$ and $p_I(C) = \mathbb{F}_p^{|I|}$.

- The set of the first k coordinates for a code with a generating matrix in the standard form is an information set.
- The first k coordinates are then called *information symbols* and the last $n - k$ coordinates are the *check symbols* and they form the corresponding check set.

PD-sets

Definition 4

Let $C \subseteq \mathbb{F}_p^n$ be a linear $[n, k, d]$ code that can correct at most t errors, and let I be an information set for C. A subset $S \subseteq \mathrm{Aut}C$ is a PD-set for C if every t-set of coordinate positions can be moved by at least one element of S out of the information set I.

The algorithm of permutation decoding is more efficient the smaller the size of a PD-set is.

A lower bound on the size of a PD-set:

Theorem 2.1 (The Gordon bound)

If S is a PD-set for an $[n, k, d]$ code C that can correct t errors, $r = n - k$, then:

$$|S| \geq \left\lceil \frac{n}{r} \left\lceil \frac{n-1}{r-1} \left\lceil \cdots \left\lceil \frac{n-t+1}{r-t+1} \right\rceil \cdots \right\rceil \right\rceil \right\rceil.$$

s-PD-sets

- for some codes PD-sets do not exist, or they are not easy to find
- then one can use **partial permutation decoding**, which includes finding s-PD-sets, where $s \leq t$

[3] J.D. Key, T.P. McDonough and V.C. Mavron, Partial permutation decoding for codes from finite planes, *European J. Combin.*, **26** (2005), 665–682.

Codes from projective planes PG$(2, q)$

- Let PG$(2, q)$ denote the *Desarguesian projective plane* of order $q = p^h$, where p is a prime and h is a positive integer, and let M_q be the incidence matrix of PG$(2, q)$.
  - Then M_q has p-rank $\binom{p+1}{2}^h + 1$, and is symmetric, because of the self-duality of PG$(2, q)$.
- The linear code C_{gen} generated by the rows of M_q over $\mathbb{F}_p$ is a p-ary code with parameters $[q^2 + q + 1, \binom{p+1}{2}^h + 1, q + 1]_p$, and the codewords of minimum weight are exactly the incidence vectors of the projective lines.
  - The points of the geometry correspond to the positions of the code.

Codes from projective planes PG(2, q)

- The full automorphism group of PG($\mathbf{2}, q$) is the projective semi-linear group PΓL($\mathbf{3}, q$), acting doubly transitively on points. Moreover, PΓL($\mathbf{3}, q$) is the full automorphism group of the code C_{gen}.
- For a translation $\tau_{u,v} : (\gamma, \beta) \mapsto (\gamma, \beta) + (u, v)$, we denote $\hat{\tau}_{u,v}$ the corresponding element from PΓL($\mathbf{3}, q$). Then for projective lines the following holds:

$$\hat{\tau}_{u,v}([\gamma, \beta, 1]) = [\gamma + u, \beta + v, 1],$$

$$\hat{\tau}_{u,v}([1, 0, 0]) = [1, 0, 0], \ \ \hat{\tau}_{u,v}([\gamma, 1, 0]) = [\gamma, 1, 0].$$

- Let σ_1 be the automorphism that interchanges the first two homogeneous coordinates of the projective lines, and let σ_2 be the automorphism that interchanges the first and the last homogeneous coordinates.

A basis for the code of $\mathrm{PG}(2, q)$, q even

- Let α be a primitive element of $\mathbb{F}_q$ and

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

where all $a_i \in \mathbb{F}_2$ (i.e. $\beta = (a_0, a_1, \ldots, a_{h-1})$).

- The leading position of β is

$$\boxed{lp(\beta) = \max\{i : a_i \neq 0\} + 1}$$

For any projective point $b = (0, 1, \beta)$ on the projective line $X_0 = 0$, we define: $lp(b) = lp(\beta)$

  - the leading position of $(0, 1, 0)$ is defined to be 0
  - the leading position of $(0, 0, 1)$ is defined to be $+\infty$

- Let $|\beta| = |\{i : a_i \neq 0\}|$

A basis for the code of $\mathrm{PG}(2, q)$, q even

- P. Vandendriessche conjectured how a basis for the code of the projective plane can look like for the case $p = 2$ (so $q = 2^h$).
- The conjecture was proven to hold for $h \leq 9$ (i.e. $q \leq 512$) by computer and conjectured to hold for all even q.

Conjecture ([2])

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 C_{gen}.

- The line $X_0 = 0$ has homogeneous coordinates $[1, 0, 0]$.
- The set of lines from the previous Conjecture consists of lines with homogeneous coordinates $[\gamma, \beta, 1]$, where $|\gamma| + lp(\beta) \leq h$.

s-PD-sets for codes from $\mathrm{PG}(2, q)$, $q = 2^h$

- In this section, we describe a construction of 2-PD-sets for the binary codes from projective planes $\mathrm{PG}(2, q)$, where $q = 2^h$ and $5 \leq h \leq 9$, and a construction of 3-PD-sets for the binary code from the projective plane $\mathrm{PG}(2, 2^9)$.
- It was shown in [3] that PD-sets for full error-correction for projective Desarguesian planes do not exist for order q large enough. Specifically, for: $q = p$ prime and $p > 103$, $q = 2^e$ and $e > 12$, $q = 3^e$ and $e > 6$, $q = 5^e$ and $e > 4$, $q = 7^e$ and $e > 3$, $q = 11^e$ and $e > 2$, $q = 13^e$ and $e > 2$, or $q = p^e$ for $p > 13$ and $e > 1$
  - s-PD-sets can be found for some small values of $s \geq 2$

s-PD-sets for codes from $\mathrm{PG}(2, q)$, $q = 2^h$

- Since the full automorphism group of a Desarguesian projective plane is 2-transitive on points, the whole group acts as a 2-PD-set, for any information set.
- Using a Moorhouse basis, 2-PD-sets of 43 elements for Desarguesian projective planes of any **prime order** $q = p$ were constructed in [3].
- The **existence** of 3-PD-sets, for any information set, for the code of any Desarguesian projective plane was also proven in [3]. To ensure that the code will correct three errors, the order $q \geq 7$ must be taken there.

Table: Codes of PG$(2, q)$: lower bounds on sizes of PD-sets (b) and 2-PD-sets (b_2)

q	Code	t	r	b	b_2
32	[1057,244,33]	16	813	180	3
64	[4161,730,65]	32	3431	1623	3
128	[16513,2188,129]	64	14325	40696	3
256	[65793,6562,257]	128	59231	3965945	3
512	[262657,19684,513]	256	242973	3625171287	3

For $h = 9$, the lower bound on the size of a 3-PD-set equals 4.

In the following constructions, we will use as an information set the basis of Vandendriessche (which is a generalization of the Moorhouse basis for $q = p$ prime to the case $q = 2^h$):

$$I_V = \{[1,0,0]\} \cup \{[\gamma, \beta, 1] : |\gamma| + lp(\beta) \leq h; \gamma, \beta \in \mathbb{F}_q\}.$$

The corresponding check set is then:

$$C_V = \{[\gamma, \beta, 1] : |\gamma| + lp(\beta) > h; \gamma, \beta \in \mathbb{F}_q\} \cup \{[\gamma, 1, 0] : \gamma \in \mathbb{F}_q\}.$$

Construction of 2-PD-sets

The full automorphism group of a Desarguesian plane acts as a 2-PD-set. Our aim is to find smaller 2-PD-sets in the case of $\mathrm{PG}(2, 2^h)$, $5 \leq h \leq 9$.

Theorem 4.1

Let $\Pi = \mathrm{PG}(2, q)$, where $q = 2^h$, and let G be the full automorphism group of Π. Furthermore, let $C_{\mathrm{gen}} = [q^2 + q + 1, 3^h + 1, q + 1]_2$ be the binary code of Π. If $5 \leq h \leq 9$, then G contains a 2-PD-set with 16 elements for C_{gen}, for the information set I_V.

Proof.

Main idea: Let us assume that 2 errors occur.

I. Suppose that 2 errors are in the information set.

a) First, let those errors correspond to the lines $[\gamma_1, \beta_1, 1]$ with $|\gamma_1| + lp(\beta_1) \leq h$ and $[\gamma_2, \beta_2, 1]$ with $|\gamma_2| + lp(\beta_2) \leq h$.

b) Let one of the errors correspond to the line $X_0 = 0$ (i.e. $[1, 0, 0]$), and the other to the line $[\gamma, \beta, 1]$, where $|\gamma| + lp(\beta) \leq h$.

II. Assume that one error is in I_V, and the other is in C_V.

a) Let those errors correspond to the lines $[\gamma_1, \beta_1, 1]$ with $|\gamma_1| + lp(\beta_1) \leq h$ and $[\gamma_2, \beta_2, 1]$ with $|\gamma_2| + lp(\beta_2) > h$.

b) Let the error in I_V correspond to the line $[\gamma_1, \beta_1, 1]$ such that $|\gamma_1| + lp(\beta_1) \leq h$, and the error in C_V to the line $[\gamma_2, 1, 0]$.

c) Let the error in I_V be $X_0 = 0$, and the one in C_V $[\gamma, 1, 0]$.

d) Let the error in I_V be $[1, 0, 0]$, and let the error in C_V be $[\gamma, \beta, 1]$ with $|\gamma| + lp(\beta) > h$.

III. Let us assume that both errors are in the check set. This case is trivial.

□

Remark 1

If Vandendriessche's Conjecture on a basis for the code of $\mathrm{PG}(2, 2^h)$ is proven true also for $h > 9$, then Theorem 4.1 is valid for every $h \geq 5$, since the construction of this 2-PD-set does not require that $h \leq 9$.

An explicit example of a 2-PD-set:

Corollary 5

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

$$a = (1, 0, \dots, 0), a' = (0, 1, 0, \dots, 0), b = (1, \dots, 1, 0), c = (1, \dots, 1) \in \mathbb{F}_{2^h}.$$

Then the following set is a 2*-PD-set for* C_{gen}*, for the information set* I_V*:*

$$S = \begin{array}{l} \{\hat{\tau}_{0,0}, \hat{\tau}_{a,a}, \hat{\tau}_{a,b}, \hat{\tau}_{a,c}, \hat{\tau}_{a',b}, \hat{\tau}_{b,a}, \hat{\tau}_{b,b}, \hat{\tau}_{b,c}, \hat{\tau}_{c,a}, \hat{\tau}_{c,b}, \hat{\tau}_{c,c}, \\ \sigma_1, \hat{\tau}_{a,b}\sigma_1, \hat{\tau}_{a,c}\sigma_1, \hat{\tau}_{b,c}\sigma_1, \hat{\tau}_{a,c}\sigma_2\}. \end{array}$$

Construction of 3-PD-sets

The following theorem gives a construction of 3-PD-sets for the code of the Desarguesian projective plane $\mathrm{PG}(2, q)$, where $q = 2^9$.

Theorem 4.2

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_V.

Proof.

Main idea:

Assume that 3 errors occur. I. Suppose that 3 errors are in I_V.

(a) First, let those errors correspond to the lines $[\gamma_i, \beta_i, 1]$ with $|\gamma_i| + lp(\beta_i) \leq h$, where $i = 1, 2, 3$.

(b) Let one of the errors correspond to the line $X_0 = 0$, and the other two to be the lines $[\gamma_i, \beta_i, 1]$ with $|\gamma_i| + lp(\beta_i) \leq h$, where $i = 1, 2$.

II. Suppose that 2 errors are in I_V, and one is in C_V.

(a) Let the errors in I_V be $[\gamma_i, \beta_i, 1]$ with $|\gamma_i| + lp(\beta_i) \leq h$, $i = 1, 2$, and the error in C_V the line $[\gamma_3, \beta_3, 1]$ with $|\gamma_3| + lp(\beta_3) > h$.

(b) Let the two errors in I_V correspond to the lines $[\gamma_i, \beta_i, 1]$ with $|\gamma_i| + lp(\beta_i) \leq h$, $i = 1, 2$, and the error in C_V to the line $[\gamma_3, 1, 0]$.

(c) Let one error be the line $X_0 = 0$, second the line $[\gamma_1, \beta_1, 1]$ with $|\gamma_1| + lp(\beta_1) \leq h$, and the last the line $[\gamma_2, \beta_2, 1]$ with $|\gamma_2| + lp(\beta_2) > h$.

(d) Let the errors in I_V be the lines $[1, 0, 0]$ and $[\gamma_1, \beta_1, 1]$ such that $|\gamma_1| + lp(\beta_1) \leq h$, and the error in C_V the line $[\gamma_2, 1, 0]$.

Proof.

III. Suppose that there are 2 errors in the check set, and one in I_V.

(a) Let those errors be $[\gamma_1, \beta_1, 1]$ with $|\gamma_1| + lp(\beta_1) \leq h$, and $[\gamma_i, \beta_i, 1]$ with $|\gamma_i| + lp(\beta_i) > h$, for $i = 2, 3$.

(b) Let the error in I_V be the line $[\gamma_1, \beta_1, 1]$ with $|\gamma_1| + lp(\beta_1) \leq h$, and the errors in C_V the lines $[\gamma_2, \beta_2, 1]$ with $|\gamma_2| + lp(\beta_2) > h$ and $[\gamma_3, 1, 0]$.

(c) Let the error in I_V correspond to the line $[\gamma_1, \beta_1, 1]$ with $|\gamma_1| + lp(\beta_1) \leq h$, and the errors in C_V correspond to the lines $[\gamma_2, 1, 0]$ and $[\gamma_3, 1, 0]$.

(d) Let the error in I_V correspond to the line $[1, 0, 0]$, and the other two correspond to the lines $[\gamma_i, \beta_i, 1]$ with $|\gamma_i| + lp(\beta_i) > h$, $i = 1, 2$.

(e) Let the error in I_V correspond to the line $[1, 0, 0]$ and the errors in C_V correspond to the lines $[\gamma_1, \beta_1, 1]$ with $|\gamma_1| + lp(\beta_1) > h$ and $[\gamma_2, 1, 0]$.

(f) Let the error in I_V correspond to the line $[1, 0, 0]$ and the errors in C_V correspond to the lines $[\gamma_2, 1, 0]$ and $[\gamma_3, 1, 0]$.

IV. If we have 3 errors in the check set, then we can use the identity map.

□

Construction of 3-PD-sets

Remark 2

The preceding explicit example of a 3-PD-set can only be used for the code of the projective plane $\mathrm{PG}(2, 2^9)$ since we explicitly make use of a number of vectors of length 9, which describe field elements of $\mathbb{F}_{2^9}$.

Corollary 6

Let $\Pi = \mathrm{PG}(2, 2^9)$, $C_{\text{gen}} = [2^{18} + 2^9 + 1, 3^9 + 1, 2^9 + 1]_2$ *its* 2*-ary code, and:*

$$
\begin{aligned}
&a = (1, 0, \dots, 0),\ \ a' = (0, 1, 0, \dots, 0),\ \ a'' = (0, 0, 1, 0, \dots, 0),\\
&b = (1, 1, 0, \dots, 0),\ \ b' = (0, 0, 1, 1, 0, \dots, 0),\ \ b'' = (0, 0, 0, 0, 1, 1, 0, 0, 0),\\
&c = (1, 1, 1, 0, \dots, 0),\ \ c' = (0, 0, 0, 1, 1, 1, 0, 0, 0),\ \ c'' = (0, \dots, 0, 1, 1, 1),\\
&d = (1, 1, 1, 1, 0, \dots, 0), d' = (0, 0, 0, 0, 1, 1, 1, 1, 0), d'' = (1, 1, 0, 0, 1, 1, 0, 0, 0),\\
&d''' = (1, 1, 0, 0, 1, 0, 0, 0, 1), d^{IV} = (0, 0, 1, 1, 0, 0, 1, 0, 1), d^{V} = (1, 1, 0, 0, 0, 1, 1, 0, 0),\\
&e = (1, 1, 1, 1, 1, 0, 0, 0, 0), e' = (0, 0, 1, 1, 1, 1, 1, 0, 0), e'' = (0, 0, 0, 0, 1, 1, 1, 1, 1),\\
&f = (1, \dots, 1, 0, 0, 0),\ \ f' = (0, 0, 0, 1, \dots, 1),\ \ g = (1, \dots, 1, 0, 0),\\
&i = (1, \dots, 1, 0),\ \ i' = (1, \dots, 1, 0, 1),\ \ j = (1, \dots, 1)\ \in \mathbb{F}_{2^9}.
\end{aligned}
$$

Then the following set S *is a* 3*-PD-set for* C_{gen}*, for the information set* I_V*:*

$$
\begin{aligned}
S = &\{\hat{\tau}_{x,f} | x \in X_1\} \cup \{\hat{\tau}_{x,g} | x \in X_1 \cup \{c'\}\} \cup \{\hat{\tau}_{x,i} | x \in X_2\} \cup \{\hat{\tau}_{x,j} | x \in \{a, a', i, j\}\}\\
&\cup \{\hat{\tau}_{j,a}, \hat{\tau}_{0,0}, \sigma_1, \hat{\tau}_{a,i}\sigma_1, \hat{\tau}_{a',i}\sigma_1, \hat{\tau}_{i,i}\sigma_1, \hat{\tau}_{j,i}\sigma_1, \hat{\tau}_{a,j}\sigma_1, \hat{\tau}_{a',j}\sigma_1, \hat{\tau}_{a'',j}\sigma_1, \hat{\tau}_{a,g}\sigma_1, \hat{\tau}_{i,g}\sigma_1, \hat{\tau}_{j,g}\sigma_1\}\\
&\cup \{\hat{\tau}_{a,j}\sigma_2\hat{\tau}_{0,a}, \hat{\tau}_{i,i}\sigma_2, \hat{\tau}_{j,i}\sigma_2, \hat{\tau}_{a,j}\sigma_2, \hat{\tau}_{a',j}\sigma_2\},\ \ \textit{where}
\end{aligned}
$$

$$
\begin{aligned}
X_1 &= \{a, a', b, b', b'', c, d, d', d''', d^{IV}, d^{V}, e, e'', f, f', i, i', j\},\\
X_2 &= \{a, a', a'', c, c', c'', d, d', d'', e, e', e'', f, i, i', j\}.
\end{aligned}
$$

Thank you!