PD-sets for codes related to flag-transitive symmetric designs

Nina Mostarac (nmavrovic@math.uniri.hr)
Dean Crnković (deanc@math.uniri.hr)

Department of Mathematics, University of Rijeka, Croatia

Supported by CSF (Croatian Science Foundation), Grant 6732

Finite Geometry & Friends
A Brussels summer school on finite geometry

June 18, 2019

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 will prove the existence of PD-sets for all codes generated by the incidence matrix of an **incidence graph** of a flag-transitive symmetric design and construct some examples

Refrences

[1] D. Crnković, N. Mostarac, PD-sets for codes related to flag-transitive symmetric designs, *Trans. Comb.*, **7** (2018) 37–50.

[2] P. Dankelmann, J.D. Key and B.G. Rodrigues, Codes from incidence matrices of graphs, *Des. Codes Cryptogr.*, **68** (2013) 373–393.

- for prime p let $C_p(G)$ be the p-ary code spanned by the rows of the incidence matrix G of a graph Γ
- we will show that if Γ is the **incidence graph** of a flag-transitive symmetric design D, then any flag-transitive automorphism group of D can be used as a PD-set for full error correction for the linear code $C_p(G)$ (with any information set)

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 $x = (x_1, ..., x_n)$ and $y = (y_1, ..., y_n) \in \mathbb{F}_p^n$. 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

Graphs

We will discuss undirected graphs, with no loops and multiple edges.

Definition 3

Edge connectivity $\lambda(\Gamma)$ of a connected graph Γ is the minimum number of edges that need to be removed to disconnect the graph.

Remark 1

For every graph Γ: $\lambda(\Gamma) \leq \delta(\Gamma)$.

Codes from incidence matrices of graphs

Let G be the incidence matrix of a graph $\Gamma = (V, E)$ over $\mathbb{F}_p$, p prime and the code $C_p(G)$ the row-span of G over $\mathbb{F}_p$.

Theorem 2.1 (Dankelmann, Key, Rodrigues [2](Result 1))

Let $\Gamma = (V, E)$ be a connected graph and G its incidence matrix. Then:

1. $dim(C_2(G)) = |V| - 1$;
2. *for odd p,* $dim(C_p(G)) = |V|$ *if Γ is not bipartite, and* $dim(C_p(G)) = |V| - 1$ *if Γ is bipartite.*

Codes from incidence matrices of graphs

Theorem 2.2 (Dankelmann, Key, Rodrigues [2](Theorem 1))

Let $\Gamma = (V, E)$ be a connected graph, G a $|V| \times |E|$ incidence matrix for G. Then:

1. *$C_2(G)$ is a $[|E|, |V| - 1, \lambda(\Gamma)]_2$ code;*
2. *if Γ is super-λ, then $C_2(G)$ is a $[|E|, |V| - 1, \delta(\Gamma)]_2$ code, and the minimum words are the rows of G of weight $\delta(\Gamma)$.*

Codes from incidence matrices of graphs

Theorem 2.3 (Dankelmann, Key, Rodrigues [2](Theorem 2))

*Let $\Gamma = (V, E)$ be a connected **bipartite** graph, G a $|V| \times |E|$ incidence matrix for G, and p an **odd** prime. Then:*

1. *$C_p(G)$ is a $[|E|, |V| - 1, \lambda(\Gamma)]_p$ code;*
2. *if Γ is super-λ, then $C_p(G)$ is a $[|E|, |V| - 1, \delta(\Gamma)]_p$ code, and the minimum words are the non-zero scalar multiples of the rows of G of weight $\delta(\Gamma)$.*

Codes from incidence matrices of graphs

Theorem 2.4 (Dankelmann, Key, Rodrigues [2](Result 3))

Let $\Gamma = (V, E)$ be a connected bipartite graph. Then $\lambda(\Gamma) = \delta(\Gamma)$ if one of the following conditions holds:

1. *V consists of at most two orbits under $Aut(\Gamma)$, and in particular if Γ is vertex-transitive;*
2. *every two vertices in one of the two partite sets of Γ have a common neighbour;*
3. *$diam(\Gamma) \leq 3$;*
4. *Γ is k-regular and $k \geq \dfrac{n+1}{4}$;*
5. *Γ has girth g and $diam(\Gamma) \leq g - 1$.*

Information sets

Definition 4

Let $C \subseteq \mathbb{F}_p^n$ be a linear $[n, k, d]$ code. For $I \subseteq \{1, ..., n\}$ 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.

PD-sets

Definition 5

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 called 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.

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

Theorem 3.1 (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:

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

Symmetric designs

Definition 6

A symmetric (v, k, λ)-design is an incidence structure $D = (P, B, I)$ which consists of the set of points P, the set of blocks B and an incidence relation I such that:

- $|P| = |B| = v$,
- every block is incident with exactly k points
- and every pair of points is incident with exactly λ blocks $(\lambda > 0)$.

A symmetric $(v, k, 1)$-design is called a projective plane of order $k - 1$, and a symmetric $(v, k, 2)$-design is called a biplane.

Incidence graph of a symmetric design

Definition 7

An incidence graph or a Levi graph of a symmetric design is a graph whose vertices are **points and blocks** of the design, and edges are incident **point-block pairs** (flags).

Remark 2

An incidence graph Γ of a symmetric (v, k, λ)-design:

- is bipartite,
- is k-regular,
- has diameter $\mathrm{diam}(\Gamma) = 3$.

Flag transitive symmetric designs

Definition 8

- An automorphism of a symmetric design is a permutation of points which sends blocks to blocks.
- An automorphism group of a symmetric design D is called flag-transitive if it is transitive on flags of D.

Theorem 3.2 (Dankelmann, Key, Rodrigues [2](Result 7))

Let $\Gamma = (V, E)$ be a k-regular graph with the automorphism group A transitive on edges and let G be an incidence matrix of Γ. If $C = C_p(G)$ is a $[|E|, |V| - \varepsilon, k]_p$ code, where p is a prime and $\varepsilon \in \{0, 1, ...|V| - 1\}$, then any transitive subgroup of A is a PD-set for full error correction for C.

Theorem 3.3 (D.C., N.M.)

Let $\Gamma = (V, E)$ be an incidence graph of a symmetric (v, k, λ)-design D with flag-transitive automorphism group A and let G be an incidence matrix for Γ. Then $C = C_p(G)$ is a $[|E|, |V| - 1, k]_p$ code, for any prime p, and any flag transitive subgroup of A can serve as a PD-set (for any information set) for full error correction for the code C.

Examples

- for the following computational results we use programming packages GAP and Magma

1. examples of flag-transitive projective planes
2. examples of flag-transitive biplanes

Parameters of the linear $[n, k, d]_p$ code obtained from a flag-transitive symmetric (v, k', λ)-design in the described way are:

- $n = v \cdot k'$
- $k = 2v - 1$
- $d = k'$

Flag-transitive projective planes

i	Flag-transitive projective plane D_i	Code $C_p(G_i)$	Gordon bound g_i	Orders of all flag-transitive subgroups of autom. group A_i	Smallest PD-set found in A_i
1	$(7,3,1)$	[21,13,3]	3	21,168	4
2	$(13,4,1)$	[52,25,4]	2	5616	4
3	$(21,5,1)$	[105,41,5]	4	20160, 40320, 60480, 120960	64

Flag-transitive biplanes

i	Flag-transitive symmetric design D_i, full automorphism group A_i, point stabilizer	Code $C_p(G_i)$	Gordon bound g_i	Orders of all flag-transitive subgroups of A_i
4	$(4,3,2)$, S_4, S_3	$[12,7,3]$	3	12, 24
5	$(7,4,2)$, $PSL_2(7)$, S_4	$[28,13,4]$	2	168
6	$(11,5,2)$, $PSL_2(11)$, A_5	$[55,21,5]$	4	55, 660
7	$(16,6,2)$, 2^4S_6, S_6	$[96,31,6]$	3	$96, 192, 288, 384, 576, 768, 960, 1152, 1920, 5760, 11520$
8	$(16,6,2)$, $(\mathbb{Z}_2 \times \mathbb{Z}_8)(S_2.4)$, $(S_2.4)$	$[96,31,6]$	3	384, 768

Flag-transitive biplanes

i	Flag-transitive design D_i	Code $C_2(G_i)$	Gordon bound g_i	Smallest PD-set found in A_i
4	$(4, 3, 2)$	[12,7,3]	3	3
5	$(7, 4, 2)$	[28,13,4]	2	3
6	$(11, 5, 2)$	[55,21,5]	4	10
7	$(16, 6, 2)$	[96,31,6]	3	12
8	$(16, 6, 2)$	[96,31,6]	3	9

Thank you!