On the binary codes with parameters of **triply**-shortened 1-perfect codes

Denis Krotov

Sobolev Institute of Mathematics, Novosibirsk, Russia

Workshop on Algebraic and Combinatorial Coding Theory,
Novosibirsk, Russia, 2010

History of the question

- [M.R.Best, A.E.Brouwer, 1977] binary codes with parameters $(n = 2^m - 1 - j, 2^{n-m}, 3)$ are optimal for $j = 1$, 2, and 3.
- [T.Etzion, A.Vardy, 1998] ask: is any $(n = 2^m - 1 - j, 2^{n-m}, 3)$ code a j-times-shortened 1-perfect code for $j = 1$? $j = 2$? ...
- [T.Blackmore, 1999] The answer is "yes" for $j = 1$.
- [P.R.J.Östergård, O.Pottonen, 2009] The answer is "no" for $j = 2$, $n = 13$ (two examples found) and $j = 3$, $n = 12$.
- [D. Krotov, 2009] It is shown that any $(n = 2^m - 1 - \mathbf{2}, 2^{n-m}, 3)$ code $C_{\blacksquare}$ generates an equitable partition $(C_{\blacksquare}, C_{\color{blue}\blacksquare}, C_{\square}, C_{\color{green}\blacksquare})$. Moreover, $C_{\blacksquare}$ is a doubly-shortened 1-perfect iff $C_{\color{green}\blacksquare}$ is splittable into two distance-3 codes, which is equivalent to the biparticity of some graph ($C_{\color{green}\blacksquare}$ is the set of vertices at distance more than 1 from $C_{\blacksquare}$).

Today: $(n = 2^m - 1 - \mathbf{3}, 2^{n-m}, 3)$

Equitable partitions

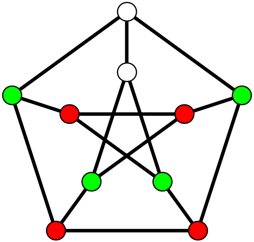
Let $G = (V(G), E(G))$ be a graph.

Definition

A partition $(C_1, \ldots, C_k)$ of $V(G)$ is an equitable partition with quotient matrix $S = (S_{ij})_{i,j=1}^{k}$ iff every element of C_i is adjacent with exactly S_{ij} elements of C_j.

Equitable partitions $\sim$ perfect colorings $\sim$ regular colorings $\sim$ partition designs $\sim$ front divisors of graph $\sim$ graph coverings

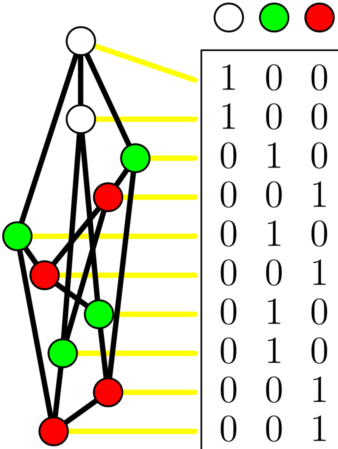
Example: Equitable partition



$$S = \begin{pmatrix} 1 & 2 & 0 \\ 1 & 0 & 2 \\ 0 & 2 & 1 \end{pmatrix}$$

Incidence matrix of an equitable partition

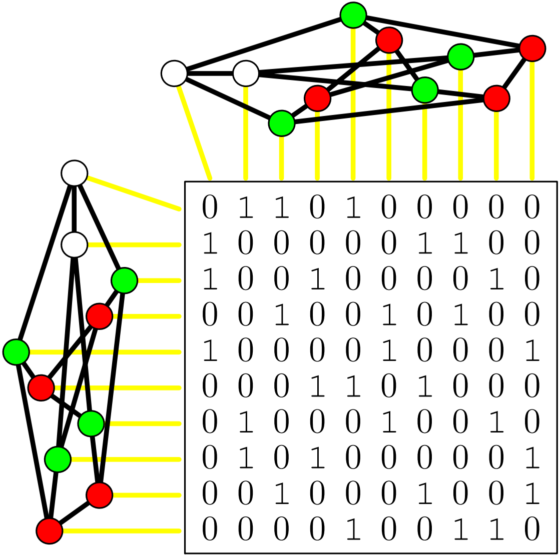
$\bar{C}$:



1	0	0
1	0	0
0	1	0
0	0	1
0	1	0
0	0	1
0	1	0
0	1	0
0	0	1
0	0	1

Adjacency matrix

A:



0	1	1	0	1	0	0	0	0	0
1	0	0	0	0	0	1	1	0	0
1	0	0	1	0	0	0	0	1	0
0	0	1	0	0	1	0	1	0	0
1	0	0	0	0	1	0	0	0	1
0	0	0	1	1	0	1	0	0	0
0	1	0	0	0	1	0	0	1	0
0	1	0	1	0	0	0	0	0	1
0	0	1	0	0	0	1	0	0	1
0	0	0	0	1	0	0	1	1	0

Matrix equation for equitable partition

A – adjacency matrix of the graph;
$\bar{C}$ – incidence matrix of an equitable partition with quotient matrix S.

Then

$$A\bar{C} = \bar{C}S$$

Generalization: Equitable collection

Let $G = (V(G), E(G))$ be a graph.

Definition

A collection $(C_1, \ldots, C_k)$ of subsets of $V(G)$ is equitable with quotient matrix $S = (S_{ij})_{i,j=1}^k$ iff every element $\bar{x}$ is adjacent with exactly $\sum_{i:\bar{x}\in C_i} S_{ij}$ elements of C_j.

Again we have

$$A\bar{C} = \bar{C}S$$

Distance infariancy of equitable partitions

Equitable partitions of distance-regular graph are distance invariant:

Distance invariancy (equitable partition)

The weight distributions of the cells $C_1, \ldots, C_k$ with respect to a vertex $\bar{x} \in C_i$ depend only on i (do not depend on the choice of $\bar{x}$ in C_i).

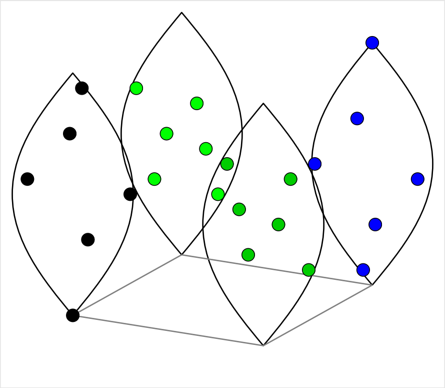
Distance infariancy of equitable collections

An equitable collection of has a similar property

Distance invariancy (equitable collection)

The weight distributions of the cells $C_1, \ldots, C_k$ with respect to a vertex $\bar{x}$ depend only on $\{i : \bar{x} \in C_i\}$.

But any partial subset from the collection is not nesessarily distance invariant!



Consider an arbitrary 1-perfect code $C \subset V(H^{n+2})$.

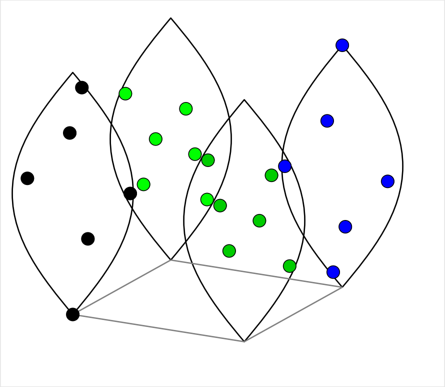
$$C = C_{\blacksquare}00 \cup C'_{\color{green}\blacksquare}01 \cup C''_{\color{green}\blacksquare}10 \cup C_{\color{blue}\blacksquare}11$$

where $C_{\blacksquare}$, $C'_{\color{green}\blacksquare}$, $C''_{\color{green}\blacksquare}$, $C_{\color{blue}\blacksquare} \subset V(H^n)$ are doubly-shortened 1-perfect codes (by definition).

$$\text{Define } C_{\color{green}\blacksquare} := C'_{\color{green}\blacksquare} \cup C''_{\color{green}\blacksquare}$$

$$C_{\square} := V(H^n) \setminus (C_{\blacksquare} \cup C_{\color{green}\blacksquare} \cup C_{\color{blue}\blacksquare})$$

Then $C_{\blacksquare{\color{blue}\blacksquare}\square{\color{green}\blacksquare}} = (C_{\blacksquare}, C_{\color{blue}\blacksquare}, C_{\square}, C_{\color{green}\blacksquare})$ is a partition of $V(H^n)$.



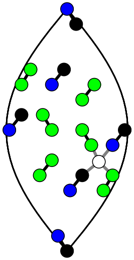
Consider an arbitrary 1-perfect code $C \subset V(H^{n+2})$.

$C = C_{\color{gray}\blacksquare} 00 \cup C'_{\color{lightgreen}\blacksquare} 01 \cup C''_{\color{lightgreen}\blacksquare} 10 \cup C_{\color{lightblue}\blacksquare} 11$

where $C_{\color{gray}\blacksquare}$, $C'_{\color{lightgreen}\blacksquare}$, $C''_{\color{lightgreen}\blacksquare}$, $C_{\color{lightblue}\blacksquare} \subset V(H^n)$ are doubly-shortened 1-perfect codes (by definition).

$$\begin{aligned} \text{Define } C_{\color{green}\blacksquare} &:= C'_{\color{green}\blacksquare} \cup C''_{\color{green}\blacksquare} \\ C_{\square} &:= V(H^n) \setminus (C_{\blacksquare} \cup C_{\color{green}\blacksquare} \cup C_{\color{blue}\blacksquare}) \end{aligned}$$

Then $C_{\blacksquare{\color{blue}\blacksquare}\square{\color{green}\blacksquare}} = (C_{\blacksquare}, C_{\color{blue}\blacksquare}, C_{\square}, C_{\color{green}\blacksquare})$ is a partition of $V(H^n)$.



Lemma

The partition $C_{\blacksquare\textcolor{blue}{\blacksquare}\square\textcolor{green}{\blacksquare}}$ *is equitable with quotient matrix*

$$\begin{pmatrix} & \blacksquare & \textcolor{blue}{\blacksquare} & \square & \textcolor{green}{\blacksquare} \\ \blacksquare & 0 & 1 & n-1 & 0 \\ \textcolor{blue}{\blacksquare} & 1 & 0 & n-1 & 0 \\ \square & 1 & 1 & n-4 & 2 \\ \textcolor{green}{\blacksquare} & 0 & 0 & n-1 & 1 \end{pmatrix}$$

Lemma (alternative definition of $C_{\blacksquare\textcolor{blue}{\blacksquare}\square\textcolor{green}{\blacksquare}}$)

$C_{\textcolor{blue}{\blacksquare}}$ *consists of vectors complementary to the vectors of* $C_{\blacksquare}$;

$C_{\textcolor{green}{\blacksquare}}$ *consists of vectors at distance* >1 *from* $C_{\blacksquare}$;

$C_{\square} = V(H^n) \setminus (C_{\blacksquare} \cup C_{\textcolor{green}{\blacksquare}} \cup C_{\textcolor{blue}{\blacksquare}})$.

Main theorem (doubly-shortened case)

Now consider an arbitrary $(n = 2^m - 1 - \mathbf{2}, 2^{n-m}, 3)$ code $C_{\blacksquare}$ and define $C_{\blacksquare{\color{blue}\blacksquare}\square{\color{green}\blacksquare}} = (C_{\blacksquare}, C_{\color{blue}\blacksquare}, C_{\square}, C_{\color{green}\blacksquare})$ by the same rules:

$C_{\color{blue}\blacksquare}$ consists of vectors complementary to the vectors of $C_{\blacksquare}$;

$C_{\color{green}\blacksquare}$ consists of vectors at distance > 1 from $C_{\blacksquare}$;

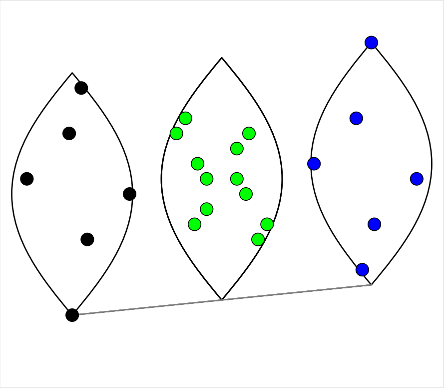
$C_{\square} = V(H^n) \setminus (C_{\blacksquare} \cup C_{\color{green}\blacksquare} \cup C_{\color{blue}\blacksquare})$.

Theorem

For every $(n = 2^m - 1 - \mathbf{2}, 2^{n-m}, 3)$ code $C_{\blacksquare}$ the collection $C_{\blacksquare{\color{blue}\blacksquare}\square{\color{green}\blacksquare}}$ is an equitable partition with quotient matrix

$$\begin{pmatrix} & \blacksquare & {\color{blue}\blacksquare} & \square & {\color{green}\blacksquare} \\ \blacksquare & 0 & 1 & n-1 & 0 \\ {\color{blue}\blacksquare} & 1 & 0 & n-1 & 0 \\ \square & 1 & 1 & n-4 & 2 \\ {\color{green}\blacksquare} & 0 & 0 & n-1 & 1 \end{pmatrix}$$

Embedding in a 1-perfect code of length $n+2$



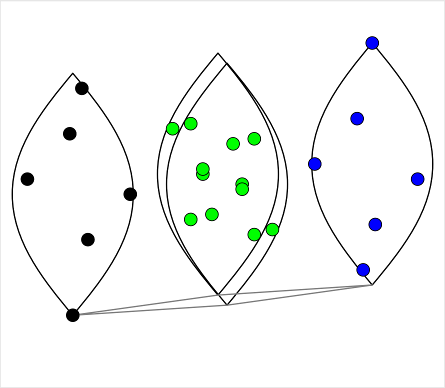
Recall: $C_{\textcolor{green}{\blacksquare}} = \{v \mid d(v, C_{\blacksquare}) = 2\}$

Theorem

Let $C_{\blacksquare}$ be an arbitrary $(n = 2^m - 3, 2^{n-m}, 3)$ code. The following statements are equivalent

- *$C_{\blacksquare}$ is a doubly-shortened 1-perfect code;*
- *$C_{\textcolor{green}{\blacksquare}}$ is the union of two distance-3 codes;*
- *the graph $(C_{\textcolor{green}{\blacksquare}}, d(\cdot,\cdot) \in \{1,2\})$ is bipartite.*

Embedding in a 1-perfect code of length $n+2$



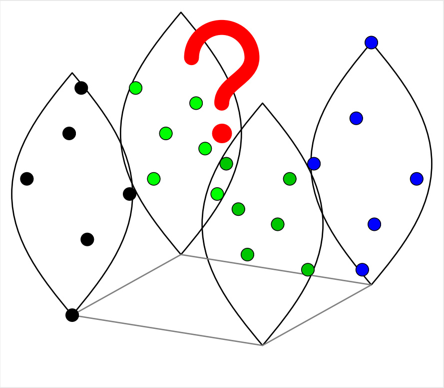
Recall: $C_{\blacksquare} = \{v \mid d(v, C_{\blacksquare}) = 2\}$

Theorem

Let $C_{\blacksquare}$ be an arbitrary $(n = 2^m - 3, 2^{n-m}, 3)$ code. The following statements are equivalent

- *$C_{\blacksquare}$ is a doubly-shortened 1-perfect code;*
- *$C_{\blacksquare}$ is the union of two distance-3 codes;*
- *the graph $(C_{\blacksquare}, d(\cdot,\cdot) \in \{1,2\})$ is bipartite.*

Embedding in a 1-perfect code of length $n + 2$



Recall: $C_{\textcolor{green}{\blacksquare}} = \{v \mid d(v, C_{\blacksquare}) = 2\}$

Theorem

Let $C_{\blacksquare}$ be an arbitrary $(n = 2^m - 3, 2^{n-m}, 3)$ code. The following statements are equivalent

- *$C_{\blacksquare}$ is a doubly-shortened 1-perfect code;*
- *$C_{\textcolor{green}{\blacksquare}}$ is the union of two distance-3 codes;*
- *the graph $(C_{\textcolor{green}{\blacksquare}}, d(\cdot,\cdot) \in \{1, 2\})$ is bipartite.*

Now consider an arbitrary $(n = 2^m - 1 - \mathbf{3}, 2^{n-m}, 3)$ code C_0 and define $(C_0, C_1, C_2, C'_0, C'_1, C'_2,)$ by the rules:

C'_0 consists of vectors complementary to the vectors of C_0;

(C_0, C_1, C_2) is the distance partition of C_0;

(C'_0, C'_1, C'_2) is the distance partition of C'_0.

Main theorem (triply-shortened case)

Theorem

For every $(n = 2^m - 1 - \mathbf{3}, 2^{n-m}, 3)$ *code* C_0 *the collection* $(C_0, C_1, C_2, C_0', C_1', C_2',)$ *is equitable with quotient matrix*

$$\begin{pmatrix} 0 & n & 0 & 0 & 0 & 0 \\ 1 & n-4 & 3 & 0 & 0 & 0 \\ 0 & n-2 & 2 & 0 & 2 & -2 \\ 0 & 0 & 0 & 0 & n & 0 \\ 0 & 0 & 0 & 1 & n-4 & 3 \\ 0 & 2 & -2 & 0 & n-2 & 2 \end{pmatrix}$$

A code is called completely regular if its weight distribution with respect to some initial vertex depends only on the distance between the initial vertex and the code. We call a code completely semiregular if its weight distribution with respect to some initial vertex $\bar{x}$ depends only on the distance between $\bar{x}$ and the code and the distance between $\bar{x} + \overline{1}$ and the code.

completely regularity

Corollary

(a) *Any* $(n = 2^k - 1 - \mathbf{3}, 2^{n-k}, 3)$ *or* $(n = 2^k - 1 - \mathbf{2}, 2^{n-k}, 3)$ *code is completely semiregular.*
(b) *Any self-complementary (i.e.,* $C_0 = C_0 + \overline{1}$*) code with parameters* $(n = 2^k - 1 - \mathbf{3}, 2^{n-k}, 3)$ *is completely regular.*

Orthogonal arrays (OA)

Corollary

Any $(n = 2^k - 1 - \mathbf{3}, 2^{n-k}, 3)$ *code forms an orthogonal array of strength* $n/2 - 2$.