Linear coordinates and symmetry groups of Mollard codes

I.Yu. Mogilnykh, F.I. Solov’eva

Novosibirsk State University
Sobolev Institute of Mathematics

Presented at the 14th International Workshop on Algebraic and Combinatorial Coding Theory
Outline

1. Basic definitions
2. \( \mu \)-linear coordinates of perfect codes
3. Symmetry groups of perfect Mollard codes
Outline

1. Basic definitions
2. $\mu$-linear coordinates of perfect codes
3. Symmetry groups of perfect Mollard codes
Outline

1. Basic definitions
2. $\mu$-linear coordinates of perfect codes
3. Symmetry groups of perfect Mollard codes
A binary code of length $n$ is a collection of vectors from $F_2^n$. 
A binary code with the minimum distance 3 is perfect if $|C| = 2^n/(n + 1)$.

Remark: WLOG all codes contain all-zero vector.
A binary code with the minimum distance 3 is \textit{perfect} if \(|C| = 2^n/(n+1)|.

\textbf{Remark}: WLOG all codes contain all-zero vector.
Hamming code

A linear (over $F_2$) perfect code is called a *binary Hamming code*. 
Steiner triple system

The codewords of weight 3 of a perfect code $C$ form STS, which is denoted by $STS(C)$.

Remark: we use a mixed code-design language for Steiner triple systems.
For $x \in F_2^n$ and $\pi \in \text{Sym}(\{1, \ldots, n\})$ define

$$\pi(x) = (x_{\pi^{-1}(1)}, \ldots, x_{\pi^{-1}(n)})$$

Given a code $C$ of length $n$, define its *symmetry group* $\text{Sym}(C) = \{\pi \in \text{Sym}(\{1, \ldots, n\}) : \pi(C) = C\}$. 
The symmetry group of a code

For $x \in F_2^n$ and $\pi \in Sym\{1, \ldots, n\}$ define

$$\pi(x) = (x_{\pi^{-1}(1)}, \ldots, x_{\pi^{-1}(n)})$$

Given a code $C$ of length $n$, define its symmetry group

$$Sym(C) = \{\pi \in Sym\{1, \ldots, n\} : \pi(C) = C\}.$$
**Invariants of perfect code**

\[ \text{Ker}(C) = \{ k \in C : k + C = C \} \text{ is the kernel of a code } C. \]

**The rank of } C \text{ is } \text{Rank}(C) = \text{dim}(\langle C \rangle). \]
Invariants of perfect code

\[ \text{Ker}(C) = \{ k \in C : k + C = C \} \text{ is the kernel of a code } C. \]

\textbf{The rank of } \textit{C} \text{ is } \text{Rank}(C) = \text{dim}(< C >). \]
$\mu$-linear coordinates of a perfect code

Let $C$ be a perfect code of length $n$, then denote by

$$
\mu_i(C) = |\{x \in \text{STS}(C) \cap \text{Ker}(C) : x_i = 1\}|.
$$

$$
0 \leq \mu_i(C) \leq (n - 1)/2
$$

Define $i$ to be a $\mu$-linear coordinate of $C$ if $\mu_i(C) = (n - 1)/2$. 

I.Yu. Mogilnykh, F.I. Solov'eva

Linear coordinates and symmetry groups of Mollard codes
Let $C$ be a perfect code of length $n$, then denote by

$$\mu_i(C) = |\{ x \in \text{STS}(C) \cap \text{Ker}(C) : x_i = 1 \}|.$$

$$0 \leq \mu_i(C) \leq (n - 1)/2$$

Define $i$ to be a $\mu$-linear coordinate of $C$ if $\mu_i(C) = (n - 1)/2$. 
Let $C$ be a perfect code of length $n$, then denote by

$$\mu_i(C) = |\{ x \in \text{STS}(C) \cap \text{Ker}(C) : x_i = 1 \}|.$$  

$$0 \leq \mu_i(C) \leq (n - 1)/2$$

Define $i$ to be a **$\mu$-linear coordinate** of $C$ if $\mu_i(C) = (n - 1)/2$. 
The set of $\mu$-linear coordinates of $C$ is denoted by $Lin_\mu(C)$. 
Property

A perfect code $C$ of length $n$ is Hamming iff $\text{Lin}_\mu(C) = \{1, \ldots, n\}$
Example

Let $C$ be a $\mathbb{Z}_2\mathbb{Z}_4$-linear perfect code. Then its $\mu$-linear coordinates are $\mathbb{Z}_2$-linear coordinates of $C$. 
The subcode of a perfect code \( C \) on the coordinates \( \text{Lin}_{\mu}(C) \) is a Hamming code of \( C \).
Let $C$ and $D$ be two codes of lengths $t$ and $m$.

Let $x$ be in $F_{2}^{tm}$. The coordinates of $x$ are indexed by elements of $\{1, \ldots, t\} \times \{1, \ldots, m\}$.

\[
p_1(x) = (\sum_{j=1}^{m} x_{1j}, \ldots, \sum_{j=1}^{m} x_{tj})
\]

\[
p_2(x) = (\sum_{i=1}^{t} x_{i1}, \ldots, \sum_{i=1}^{t} x_{im})
\]
Mollard code

Let $C$ and $D$ be two codes of lengths $t$ and $m$.

Let $x$ be in $F_2^{tm}$. The coordinates of $x$ are indexed by elements of $\{1, \ldots, t\} \times \{1, \ldots, m\}$.

\[
p_1(x) = \left( \sum_{j=1}^{m} x_{1j}, \ldots, \sum_{j=1}^{m} x_{tj} \right)
\]

\[
p_2(x) = \left( \sum_{i=1}^{t} x_{i1}, \ldots, \sum_{i=1}^{t} x_{im} \right)
\]
Mollard code

Let $C$ and $D$ be two codes of lengths $t$ and $m$.

Let $x$ be in $F_2^{tm}$. The coordinates of $x$ are indexed by elements of $\{1, \ldots, t\} \times \{1, \ldots, m\}$.

$$p_1(x) = (\sum_{j=1}^{m} x_{1j}, \ldots, \sum_{j=1}^{m} x_{tj})$$

$$p_2(x) = (\sum_{i=1}^{t} x_{i1}, \ldots, \sum_{i=1}^{t} x_{im})$$
Let $C$ and $D$ be two codes of lengths $t$ and $m$.

Let $x$ be in $F_2^{tm}$. The coordinates of $x$ are indexed by elements of $\{1, \ldots, t\} \times \{1, \ldots, m\}$.

\[ p_1(x) = \left( \sum_{j=1}^{m} x_{1j}, \ldots, \sum_{j=1}^{m} x_{tj} \right) \]

\[ p_2(x) = \left( \sum_{i=1}^{t} x_{i1}, \ldots, \sum_{i=1}^{t} x_{im} \right) \]
Mollard code

Let $C$ and $D$ be two codes of lengths $t$ and $m$.

Let $x$ be in $F_{2}^{tm}$. The coordinates of $x$ are indexed by elements of $\{1, \ldots, t\} \times \{1, \ldots, m\}$.

$$p_1(x) = \left( \sum_{j=1}^{m} x_{1j}, \ldots, \sum_{j=1}^{m} x_{tj} \right)$$

$$p_2(x) = \left( \sum_{i=1}^{t} x_{i1}, \ldots, \sum_{i=1}^{t} x_{im} \right)$$
The Mollard code

Mollard code

\[ M(C, D) = \{(x, p_1(x) + y, p_2(x) + z + f(y)) : x \in F_2^{tm}, y \in C, z \in D\}. \] In the talk \( f \) is the zero function.
Theorem
If $C$ and $D$ are perfect codes, then $M(C, D)$ is perfect.

Theorem
If $S_1$ and $S_2$ are Steiner triple systems (treated as binary codes with all-zero vectors), then $M(S_1, S_2)$ is a STS with all-zero vector.
Mollard code

Theorem

If $C$ and $D$ are perfect codes, then $M(C, D)$ is perfect.

Theorem

If $S_1$ and $S_2$ are Steiner triple systems (treated as binary codes with all-zero vectors), then $M(S_1, S_2)$ is a STS with all-zero vector.
Subcodes of Mollard code

\[ M(C, D) = \{(x, p_1(x) + y, p_2(x) + z) : x \in \mathbb{F}_2^{tm}, y \in C, z \in D\}. \]

Subcodes of \( M(C, D) \)

\[ C^1 = \{(0^t, y, 0^m) : y \in C\}, \quad D^2 = \{(0^t, 0^t, z) : z \in D\}. \]
Subcodes of Mollard code

\[ M(C, D) = \{(x, p_1(x) + y, p_2(x) + z) : x \in F_2^{tm}, y \in C, z \in D\}. \]

Subcodes of \( M(C, D) \)

\[ C^1 = \{(0^{tm}, y, 0^m) : y \in C\}, \quad D^2 = \{(0^{tm}, 0^t, z) : z \in D\}. \]
Subcodes of Mollard code

\[ M(C, D) = \{ (x, p_1(x) + y, p_2(x) + z) : x \in F_{2^m}^t, y \in C, z \in D \}. \]

Subcodes of \( M(C, D) \)

\[ C^1 = \{ (0^{tm}, y, 0^m) : y \in C \}, \quad D^2 = \{ (0^{tm}, 0^t, z) : z \in D \}. \]
Problem statement

Describe $\text{Sym}(M(C, D))$. $\text{Stab}_{D^2}\text{Sym}(M(C, D)) = ?$

Avgustinovich, Heden, Solov’eva, 2005

The description in case when $D$ is of length 1.
Problem statement

Describe $\text{Sym}(M(C, D))$. $\text{Stab}_{D^2}\text{Sym}(M(C, D)) = ?$

Avgustinovich, Heden, Solov’eva, 2005

The description in case when $D$ is of length 1.
Problem statement

Describe $\text{Sym}(M(C, D))$. $\text{Stab}_{D^2}\text{Sym}(M(C, D)) =$?

Avgustinovich, Heden, Solov’eva, 2005

The description in case when $D$ is of length 1.
Main results

Theorem

Let $C$ and $D$ be two perfect codes. Then

$$Stab_{D^2}(Sym(M(C, D))) \cong (Sym(C) \ltimes Z_2^{(\log_2(1+|Lin_\mu(C)|)^{t-rank(C)})}) \times Sym(D).$$
Given STS $S$ of order $n$ define a point $i$ to be \textit{$\nu$-linear} if $i$ is in $(n - 1)(n - 3)/4$ Pasch configurations of $S$.

**Theorem**

Let $S_1$ and $S_2$ be two STS (Steiner triple system treated as STS with all-zero vector). Then

$$
\text{Stab}_{S_2}(\text{Sym}(M(S_1, S_2))) \cong (\text{Sym}(S^2) \rtimes Z_2^{(\log_2(1 + |\text{Lin}_\nu(S_1)|))^{t - \text{rank}(S_1)}}) \times \text{Sym}(S_2).
$$
Given STS $S$ of order $n$ define a point $i$ to be $\nu$-linear if $i$ is in $(n - 1)(n - 3)/4$ Pasch configurations of $S$.

**Theorem**

Let $S_1$ and $S_2$ be two STS (Steiner triple system treated as STS with all-zero vector). Then

$$\text{Stab}_{S_2}(\text{Sym}(M(S_1, S_2))) \cong$$

$$(\text{Sym}(S^2) \ltimes \mathbb{Z}_2^{(\log_2(1 + |\text{Lin}_\nu(S_1)|))t - \text{rank}(S_1)}) \times \text{Sym}(S_2).$$
Conclusion

- The characteristic $\mu_i(C)$ and the notion of $\mu$-linear coordinate for a perfect code are suggested

- The description for $\text{Stab}_{D^2}(M(C, D))$ is obtained

- The same approach works for STS

- Next talk: utilization of $\mu_i(C)$ for constructing codes with extremal algebraic properties
The characteristic $\mu_i(C)$ and the notion of $\mu$-linear coordinate for a perfect code are suggested.

The description for $\text{Stab}_{D^2}(M(C, D))$ is obtained.

The same approach works for STS.

Next talk: utilization of $\mu_i(C)$ for constructing codes with extremal algebraic properties.
Conclusion

- The characteristic $\mu_i(C)$ and the notion of $\mu$-linear coordinate for a perfect code are suggested
- The description for $\text{Stab}_{D^2}(M(C, D))$ is obtained
- The same approach works for STS
- Next talk: utilization of $\mu_i(C)$ for constructing codes with extremal algebraic properties
Conclusion

- The characteristic $\mu_i(C)$ and the notion of $\mu$-linear coordinate for a perfect code are suggested

- The description for $\text{Stab}_{D^2}(M(C, D))$ is obtained

- The same approach works for STS

- Next talk: utilization of $\mu_i(C)$ for constructing codes with extremal algebraic properties
THANK YOU FOR YOUR ATTENTION