On the structure of non-full-rank perfect codes

Denis Krotov, Sobolev Inst. of Math., Novosibirsk, Russia

joint work with

Olof Heden, KTH, Stockholm, Sweden

ALCOMA'10, Thurnau, Germany

Outline

- If a q-ary 1-perfect code has non-full rank (the dual space is not empty) then the code is the union of "components" which can be studied (constructed, characterized, enumerated, ...) independently.
- To improve the lower bound on the number of 1-perfect codes for odd q, we use switching starting from specially constructed nonlinear code. The linear Hamming code is not the best starting point to obtain a large number of 1-perfect codes by switching. This is illustrated using n-ary quasigroups (latin hypercubes).

1-Perfect codes

- A set of vertices of a discrete metric space is called a 1-perfect code if the radius-1 balls centered in the code vertices partition the space.
- Space: the Hamming space F_q^n (n-dimensional vector space over GF(q) with a Hamming metric)
- 1-Perfect codes in F_q^n exist $\Leftrightarrow n = \dfrac{q^m - 1}{q - 1}$ for some natural m.
- A linear 1-perfect code (Hamming code) is unique up to monomial transformations of the space. A check $m \times n$ matrix consists of complete set of mutually independent columns of height m.

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

1-Perfect codes

- A set of vertices of a discrete metric space is called a 1-perfect code if the radius-1 balls centered in the code vertices partition the space.
- Space: the Hamming space F_q^n (n-dimensional vector space over GF(q) with a Hamming metric)
- 1-Perfect codes in F_q^n exist $\Leftrightarrow n = \dfrac{q^m - 1}{q - 1}$ for some natural m.
- A linear 1-perfect code (Hamming code) is unique up to monomial transformations of the space. A check $m \times n$ matrix consists of complete set of mutually independent columns of height m.

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

1-Perfect codes

- A set of vertices of a discrete metric space is called a 1-perfect code if the radius-1 balls centered in the code vertices partition the space.
- Space: the Hamming space F_q^n (n-dimensional vector space over GF(q) with a Hamming metric)
- 1-Perfect codes in F_q^n exist $\Leftrightarrow n = \dfrac{q^m - 1}{q - 1}$ for some natural m.
- A linear 1-perfect code (Hamming code) is unique up to monomial transformations of the space. A check $m \times n$ matrix consists of complete set of mutually independent columns of height m.

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

1-Perfect codes

- A set of vertices of a discrete metric space is called a 1-perfect code if the radius-1 balls centered in the code vertices partition the space.
- Space: the Hamming space F_q^n (n-dimensional vector space over GF(q) with a Hamming metric)
- 1-Perfect codes in F_q^n exist $\Leftrightarrow$ $n = \dfrac{q^m - 1}{q - 1}$ for some natural m.
- A linear 1-perfect code (Hamming code) is unique up to monomial transformations of the space. A check $m \times n$ matrix consists of complete set of mutually independent columns of height m.

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

Rank

- The rank of a code $C \subset F_q^n$ is the dimension of the linear span of C.
- We say that C has rank $+\Delta$ if $\mathrm{rank}\, C = \log_q |C| + \Delta$.
- A code C is called a full-rank code if $\mathrm{rank}(C) = n$.
- If a code is not full rank then it has a nontrivial orthogonal space.

The weight of a dual vector, $q = 2$

- Known: The weight-3 codewords of a binary 1-perfect code $C \ni \bar{0}$ form a Steiner triple system. Any dual vector of a STS(v) has weight $(v-1)/2$.
- [Doyen, Hubaut, Vandensavel, 1978] Any dual vector of a STS(v) has weight $(v-1)/2$.
- Proof: if $\bar{x} = (111111...10000...0)$ is a dual vector then the set of all blocks containing the first coordinate defines a bijection between the 0-s and 1-s of $\bar{x}$ excluding the first 1.

1	1	1	1	0	0	0
•	•				•	
•		•		•		
•			•			•

- Corollary: Any dual vector of a binary 1-perfect code of length n has weight $(n-1)/2$.

- Known: The weight-3 codewords of a binary 1-perfect code $C \ni \bar{0}$ form a Steiner triple system. Any dual vector of a STS(v) has weight $(v-1)/2$.
- [Doyen, Hubaut, Vandensavel, 1978] Any dual vector of a STS(v) has weight $(v-1)/2$.
- Proof: if $\bar{x} = (111111...10000...0)$ is a dual vector then the set of all blocks containing the first coordinate defines a bijection between the 0-s and 1-s of $\bar{x}$ excluding the first 1.

1	1	1	1	0	0	0
•	•				•	
•		•		•		
•			•			•

- Corollary: Any dual vector of a binary 1-perfect code of length n has weight $(n-1)/2$.

The weight of a dual vector, $q = 2$

- Known: The weight-3 codewords of a binary 1-perfect code $C \ni \bar{0}$ form a Steiner triple system. Any dual vector of a STS(v) has weight $(v-1)/2$.
- [Doyen, Hubaut, Vandensavel, 1978] Any dual vector of a STS(v) has weight $(v-1)/2$.
- Proof: if $\bar{x} = (111111...10000...0)$ is a dual vector then the set of all blocks containing the first coordinate defines a bijection between the 0-s and 1-s of $\bar{x}$ excluding the first 1.

$$\begin{array}{c|ccc|ccc}
1 & 1 & 1 & 1 & 0 & 0 & 0 \\
\hline
\bullet & \bullet & & & & \bullet & \\
\bullet & & \bullet & & \bullet & & \\
\bullet & & & \bullet & & & \bullet
\end{array}$$

- Corollary: Any dual vector of a binary 1-perfect code of length n has weight $(n-1)/2$.

The weight of a dual vector, $q = 2$

- Known: The weight-3 codewords of a binary 1-perfect code $C \ni \bar{0}$ form a Steiner triple system. Any dual vector of a STS(v) has weight $(v-1)/2$.
- [Doyen, Hubaut, Vandensavel, 1978] Any dual vector of a STS(v) has weight $(v-1)/2$.
- Proof: if $\bar{x} = (111111...10000...0)$ is a dual vector then the set of all blocks containing the first coordinate defines a bijection between the 0-s and 1-s of $\bar{x}$ excluding the first 1.

$$\begin{array}{c|ccc|ccc}
1 & 1 & 1 & 1 & 0 & 0 & 0 \\
\hline
\bullet & \bullet & & & & \bullet & \\
\bullet & & \bullet & & \bullet & & \\
\bullet & & & \bullet & & & \bullet
\end{array}$$

- Corollary: Any dual vector of a binary 1-perfect code of length n has weight $(n-1)/2$.

The weight of a dual vector, general case

- The binary case can be easily generalized if we consider the generalized STS that formed by the weight-3 words of a q-ary 1-perfect code.
- Given a dual vector $\bar{x} = (\underbrace{111111...1}_{left}\underbrace{0000...0}_{right})$ and considering the weight-3 codewords with 1 in the first position and -1 in another left position we see that $(q-1)$ left positions correspond to one right position.

1	1	1	1	1	1	1	1	1	0	0	0	0
1	2								1			
1		2							2			

- So we get that $wt(\bar{x}) - 1 = (q-1)(n - wt(\bar{x}))$, i.e.,

$$wt(\bar{x}) = \frac{(q-1)n - 1}{q}$$

The weight of a dual vector, general case

- The binary case can be easily generalized if we consider the generalized STS that formed by the weight-3 words of a q-ary 1-perfect code.
- Given a dual vector $\bar{x} = (\underbrace{111111...1}_{left}\underbrace{0000...0}_{right})$ and considering the weight-3 codewords with 1 in the first position and -1 in another left position we see that $(q-1)$ left positions correspond to one right position.

$$
\begin{array}{c|cccccccc|cccc}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
\hline
1 & 2 & & & & & & & & 1 & & & \\
1 & & 2 & & & & & & & 2 & & &
\end{array}
$$

- So we get that $wt(\bar{x}) - 1 = (q-1)(n - wt(\bar{x}))$, i.e.,

$$wt(\bar{x}) = \frac{(q-1)n - 1}{q}$$

The weight of a dual vector, general case

- The binary case can be easily generalized if we consider the generalized STS that formed by the weight-3 words of a q-ary 1-perfect code.
- Given a dual vector $\bar{x} = (\underbrace{111111...1}_{left}\underbrace{0000...0}_{right})$ and considering the weight-3 codewords with 1 in the first position and -1 in another left position we see that $(q-1)$ left positions correspond to one right position.

$$
\begin{array}{c|cccccccc|cccc}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
\hline
1 & 2 & & & & & & & & 1 & & & \\
1 & & 2 & & & & & & & 2 & & &
\end{array}
$$

- So we get that $wt(\bar{x}) - 1 = (q-1)(n - wt(\bar{x}))$, i.e.,

$$wt(\bar{x}) = \frac{(q-1)n - 1}{q}$$

The structure of the orthogonal space

Lemma

Let D be any r-dimensional subspace orthogonal to a perfect code C of length $n = \frac{q^m-1}{q-1}$. Then, for some monomial transformation ψ, the space $\psi(D)$ has a generating matrix of the form

$$H = \left[\begin{array}{ccc|ccc|c|ccc|ccc} | & & | & | & & | & & | & & | & | & & | \\ \bar{\alpha}_1 & \cdots & \bar{\alpha}_1 & \bar{\alpha}_2 & \cdots & \bar{\alpha}_2 & \cdots & \bar{\alpha}_t & \cdots & \bar{\alpha}_t & \bar{0} & \cdots & \bar{0} \\ | & & | & | & & | & & | & & | & | & & | \end{array}\right]$$

$$\underbrace{\qquad\qquad}_{q^{m-r}} \quad \underbrace{\qquad\qquad}_{q^{m-r}} \quad \cdots \quad \underbrace{\qquad\qquad}_{q^{m-r}} \quad \underbrace{\qquad\qquad}_{(q^{m-r}-1)/(q-1)}$$

where

$$H^\star = \left[\begin{array}{cccc} | & | & & | \\ \bar{\alpha}_1 & \bar{\alpha}_2 & \cdots & \bar{\alpha}_t \\ | & | & & | \end{array}\right]$$

is a check matrix of some Hamming code $C^\star$ of length $t = \frac{q^r-1}{q-1}$.

Parity-check law

Assume w.l.o.g. $\psi = \mathrm{Id}$.
Define the generalized parity-check function $\bar{\sigma} : F_q^n \to F_q^t$ as

$$\bar{\sigma}(\bar{x}) = (\sigma_1(\bar{x}), \ldots, \sigma_t(\bar{x}))$$

where

$$\sigma_i = x_{(i-1)q^t+1} + \ldots + x_{iq^t}.$$

Then $\bar{\sigma}(\bar{c}) \in C^\star$ for every $\bar{c} \in C$, i.e.,

$$C = \bigcup_{\bar{\mu} \in C^\star} K_{\bar{\mu}} \tag{1}$$

where $\bar{\sigma}(K_{\bar{\mu}}) = \bar{\mu}$.

Lemma (combining construction)

Let $C^\star$ be a Hamming code. If for every $\bar{\mu} \in C^\star$ we have a distance-3 code $K_{\bar{\mu}}$ of "appropriate" cardinality that satisfies the parity-check law $\bar{\sigma}(K_{\bar{\mu}}) = \bar{\mu}$, then the code C defined by (1) is 1-perfect.

Components

- The sets $K_{\bar{\mu}}$ will be referred to as $\bar{\mu}$-components.
- Clearly, any $\bar{\mu}$-component is a translation of some $\bar{0}$-component.
- $\bar{0}$-components can be considered as 1-perfect codes in the metric subspace

$$\{\bar{x} \in F_q^n \mid \mathrm{wt}(\bar{\sigma}(\bar{x})) \leq 1\}$$

- $\bar{\mu}$-components ($\bar{0}$-components) can be considered for *any* length of $\bar{\mu}$, no need to restrict by only lengths of 1-perfect codes
- This approach is especially convenient for studying 1-perfect codes of rank not more than $+\Delta$ for fixed Δ. For example, for binary 1-perfect codes of rank $+3$ the size of group of coordinates for $\bar{\sigma}$ is 8 and $\bar{\mu}$-components exist in lengths **15**, 23, **31**, 39, 47, 55, **63**, 71, ...

Components

- The sets $K_{\bar{\mu}}$ will be referred to as $\bar{\mu}$-components.
- Clearly, any $\bar{\mu}$-component is a translation of some $\bar{0}$-component.
- $\bar{0}$-components can be considered as 1-perfect codes in the metric subspace

$$\{\bar{x} \in F_q^n \mid \mathrm{wt}(\bar{\sigma}(\bar{x})) \leq 1\}$$

- $\bar{\mu}$-components ($\bar{0}$-components) can be considered for *any* length of $\bar{\mu}$, no need to restrict by only lengths of 1-perfect codes
- This approach is especially convenient for studying 1-perfect codes of rank not more than $+\Delta$ for fixed Δ. For example, for binary 1-perfect codes of rank $+3$ the size of group of coordinates for $\bar{\sigma}$ is 8 and $\bar{\mu}$-components exist in lengths **15**, 23, **31**, 39, 47, 55, **63**, 71, ...

Components

- The sets $K_{\bar{\mu}}$ will be referred to as $\bar{\mu}$-components.
- Clearly, any $\bar{\mu}$-component is a translation of some $\bar{0}$-component.
- $\bar{0}$-components can be considered as 1-perfect codes in the metric subspace

$$\{\bar{x} \in F_q^n \mid \mathrm{wt}(\bar{\sigma}(\bar{x})) \leq 1\}$$

- $\bar{\mu}$-components ($\bar{0}$-components) can be considered for *any* length of $\bar{\mu}$, no need to restrict by only lengths of 1-perfect codes
- This approach is especially convenient for studying 1-perfect codes of rank not more than $+\Delta$ for fixed Δ. For example, for binary 1-perfect codes of rank $+3$ the size of group of coordinates for $\bar{\sigma}$ is 8 and $\bar{\mu}$-components exist in lengths **15**, 23, **31**, 39, 47, 55, **63**, 71, ...

Components

- The sets $K_{\bar{\mu}}$ will be referred to as $\bar{\mu}$-components.
- Clearly, any $\bar{\mu}$-component is a translation of some $\bar{0}$-component.
- $\bar{0}$-components can be considered as 1-perfect codes in the metric subspace

$$\{\bar{x} \in F_q^n \mid \mathrm{wt}(\bar{\sigma}(\bar{x})) \leq 1\}$$

- $\bar{\mu}$-components ($\bar{0}$-components) can be considered for *any* length of $\bar{\mu}$, no need to restrict by only lengths of 1-perfect codes
- This approach is especially convenient for studying 1-perfect codes of rank not more than $+\Delta$ for fixed Δ. For example, for binary 1-perfect codes of rank $+3$ the size of group of coordinates for $\bar{\sigma}$ is 8 and $\bar{\mu}$-components exist in lengths **15**, 23, **31**, 39, 47, 55, **63**, 71, ...

Components

- The sets $K_{\bar{\mu}}$ will be referred to as $\bar{\mu}$-components.
- Clearly, any $\bar{\mu}$-component is a translation of some $\bar{0}$-component.
- $\bar{0}$-components can be considered as 1-perfect codes in the metric subspace

$$\{\bar{x} \in F_q^n \mid \mathrm{wt}(\bar{\sigma}(\bar{x})) \leq 1\}$$

- $\bar{\mu}$-components ($\bar{0}$-components) can be considered for *any* length of $\bar{\mu}$, no need to restrict by only lengths of 1-perfect codes
- This approach is especially convenient for studying 1-perfect codes of rank not more than $+\Delta$ for fixed Δ. For example, for binary 1-perfect codes of rank $+3$ the size of group of coordinates for $\bar{\sigma}$ is 8 and $\bar{\mu}$-components exist in lengths **15**, 23, **31**, 39, 47, 55, **63**, 71, . . .

Solved cases

- Case $q = 2$ rank $\leq +2$:
  [Avgustinovich, Heden, Solov'eva, 2004] One-to-one correspondence between $\bar{0}$-components and $(n-3)/4$-ary quasigroups of order 4.
  [K, Potapov, 2009] Characterization of multary quasigroups of order 4.
- Case $q = 4$ rank $\leq +1$: generalized concatenated construction [V.Zinoviev] results in binary 1-perfect codes of rank $\leq +2$, so this case probably can be solved.
- Case $q = 3$ rank $\leq +1$: probably not more complicate than for $q = 4$.

Solved cases

- Case $q = 2$ rank $\leq +2$:
  [Avgustinovich, Heden, Solov'eva, 2004] One-to-one correspondence between $\bar{0}$-components and $(n-3)/4$-ary quasigroups of order 4.
  [K, Potapov, 2009] Characterization of multary quasigroups of order 4.
- Case $q = 4$ rank $\leq +1$: generalized concatenated construction [V.Zinoviev] results in binary 1-perfect codes of rank $\leq +2$, so this case probably can be solved.
- Case $q = 3$ rank $\leq +1$: probably not more complicate than for $q = 4$.

Solved cases

- Case $q = 2$ rank $\leq +2$:
  [Avgustinovich, Heden, Solov'eva, 2004] One-to-one correspondence between $\bar{0}$-components and $(n-3)/4$-ary quasigroups of order 4.
  [K, Potapov, 2009] Characterization of multary quasigroups of order 4.
- Case $q = 4$ rank $\leq +1$: generalized concatenated construction [V.Zinoviev] results in binary 1-perfect codes of rank $\leq +2$, so this case probably can be solved.
- Case $q = 3$ rank $\leq +1$: probably not more complicate than for $q = 4$.

Unsolved cases

- Case $q = 5$ rank $\leq +1$: open problem (even characterization in terms of multary quasigroups of order 5).
- Case $q = 2$ rank $\leq +3$: open problem. But the case $n = 15$ is solved using computer [Zinoviev, Zinoviev, 2006], [Östergård, Pottonen, 2009] (there are 1990 non-isomorphic extended 1-perfect codes). This gives some basic knowledge on the structure of "rank +3" components of larger lengths, similarly as knowledge of all latin squares when studying latin hypercubes.

Unsolved cases

- Case $q = 5$ rank $\leq +1$: open problem (even characterization in terms of multary quasigroups of order 5).
- Case $q = 2$ rank $\leq +3$: open problem. But the case $n = 15$ is solved using computer [Zinoviev, Zinoviev, 2006], [Östergård, Pottonen, 2009] (there are 1990 non-isomorphic extended 1-perfect codes). This gives some basic knowledge on the structure of "rank $+3$" components of larger lengths, similarly as knowledge of all latin squares when studying latin hypercubes.

Number of 1-perfect codes

- The number of 1-perfect codes is known to be doubly-exponential in n:
$$2^{2^{\alpha n + o(n)}}$$
- All lower bounds are obtained by switching approach.
- For binary case, $\alpha \geq \frac{1}{2}$ [Vasil'ev 1962], and $\alpha \leq 1$ (trivial).
- A generalization to nonbinary case: [Schönheim 1968] — possibility to switch linear switching components.
- [Los' 2006]: in the case of nonprime q a linear component of the Hamming code is partitioned into exponential number of nonlinear switching components. This improves the lower bound on α.

Number of 1-perfect codes

- The number of 1-perfect codes is known to be doubly-exponential in n:

$$2^{2^{\alpha n + o(n)}}$$

- All lower bounds are obtained by switching approach.
- For binary case, $\alpha \geq \frac{1}{2}$ [Vasil'ev 1962], and $\alpha \leq 1$ (trivial).
- A generalization to nonbinary case: [Schönheim 1968] — possibility to switch linear switching components.
- [Los' 2006]: in the case of nonprime q a linear component of the Hamming code is partitioned into exponential number of nonlinear switching components. This improves the lower bound on α.

Number of 1-perfect codes

- The number of 1-perfect codes is known to be doubly-exponential in n:
$$2^{2^{\alpha n+o(n)}}$$
- All lower bounds are obtained by switching approach.
- For binary case, $\alpha \geq \frac{1}{2}$ [Vasil'ev 1962], and $\alpha \leq 1$ (trivial).
- A generalization to nonbinary case: [Schönheim 1968] — possibility to switch linear switching components.
- [Los' 2006]: in the case of nonprime q a linear component of the Hamming code is partitioned into exponential number of nonlinear switching components. This improves the lower bound on α.

Number of 1-perfect codes

- The number of 1-perfect codes is known to be doubly-exponential in n:

$$2^{2^{\alpha n + o(n)}}$$

- All lower bounds are obtained by switching approach.
- For binary case, $\alpha \geq \frac{1}{2}$ [Vasil'ev 1962], and $\alpha \leq 1$ (trivial).
- A generalization to nonbinary case: [Schönheim 1968] — possibility to switch linear switching components.
- [Los' 2006]: in the case of nonprime q a linear component of the Hamming code is partitioned into exponential number of nonlinear switching components. This improves the lower bound on α.

Number of 1-perfect codes

- The number of 1-perfect codes is known to be doubly-exponential in n:

$$2^{2^{\alpha n + o(n)}}$$

- All lower bounds are obtained by switching approach.
- For binary case, $\alpha \geq \frac{1}{2}$ [Vasil'ev 1962], and $\alpha \leq 1$ (trivial).
- A generalization to nonbinary case: [Schönheim 1968] — possibility to switch linear switching components.
- [Los' 2006]: in the case of nonprime q a linear component of the Hamming code is partitioned into exponential number of nonlinear switching components. This improves the lower bound on α.

Further improvement

For odd q, the Hamming code is not the best choice to start switching!

To show this, we use the [Phelps 1984] construction, which can be treated as a way to construct a $\bar{\mu}$-component from a multary quasigroup.

Def: multary quasigroup

$\Sigma = \{0, 1, \ldots, q-1\}$. Σ^n – the set of n-words over Σ. The set of q words in Σ^n that coincide in $n-1$ positions is called a line.

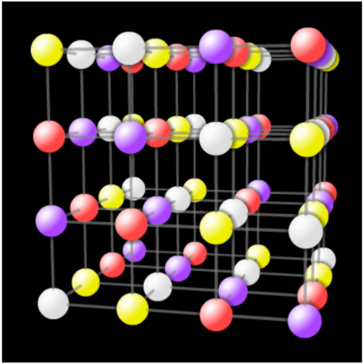
Definition

A function $f : \Sigma^n \to \Sigma$ is called an n-ary (multary) quasigroup, or a latin n-cube of order q if $f(L) = \Sigma$ for every line L.

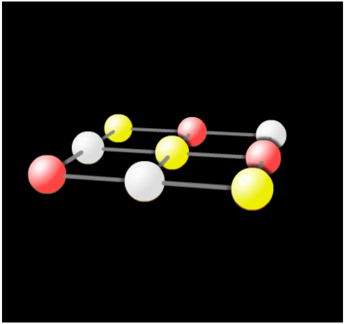
$n = 2:$

0	1	2	3
1	0	3	2
2	3	1	0
3	2	0	1

$n = 3:$



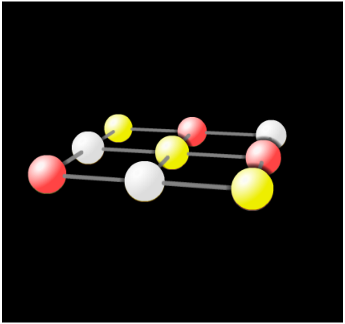
n-Ary quasigroups $\leftrightarrow$ $(n+1, 2)$ MDS codes



Well known

$f : \Sigma^n \to \Sigma$ is an n-ary quasigroup if and only if $M = \{(x_0, x_1, ..., x_n) \mid x_0 = f(x_1, ..., x_n)\}$ is a distance-2 MDS code.

n-Ary quasigroups $\leftrightarrow$ $(n+1,2)$ MDS codes



Well known

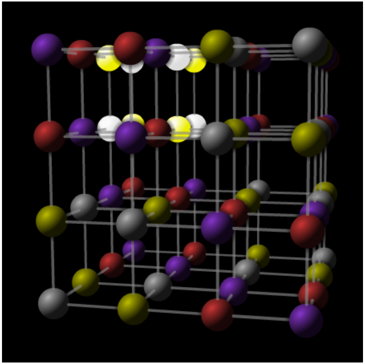
$f : \Sigma^n \to \Sigma$ is an n-ary quasigroup if and only if $M = \{(x_0, x_1, ..., x_n) \mid x_0 = f(x_1, ..., x_n)\}$ is a distance-2 MDS code.

n-Ary quasigroups of order 4

Theorem ([K, Potapov, 2009])

Every n-ary quasigroup is a repetition-free composition of (one or more) multary quasigroups equivalent (isotopic) to multary quasigroups (latin hypercubes) of anti-sudoku type.

$n = 3: \ g:$



$n = 2: \ h:$

0	1	2	3
1	0	3	2
2	3	1	0
3	2	0	1

Example:

$$f(x_1, x_2, x_3, x_4) = h(x_2, g(x_1, x_3, x_4))$$

The number of n-ary quasigroups. LOWER bound

- How to obtain large number of multary quasigroups of fixed order q?
- !!! Switching
- Starting to switch from the linear multary quasigroups is not a good idea sometimes. For example, $f(x_1, x_2, ..., x_n) = x_1 + x_2 + ... + x_n \mod 7$

0	**1**	2	3	4	5	6
1	2	3	4	5	6	**0**
2	3	4	5	6	**0**	**1**
3	4	5	6	**0**	**1**	2
4	5	6	**0**	**1**	2	3
5	6	**0**	**1**	2	3	4
6	**0**	**1**	2	3	4	5

The number of n-ary quasigroups. LOWER bound

- How to obtain large number of multary quasigroups of fixed order q?
- !!! Switching
- Starting to switch from the linear multary quasigroups is not a good idea sometimes. For example, $f(x_1, x_2, ..., x_n) = x_1 + x_2 + ... + x_n \bmod 7$

0	**1**	2	3	4	5	6
1	2	3	4	5	6	**0**
2	3	4	5	6	**0**	**1**
3	4	5	6	**0**	**1**	2
4	5	6	**0**	**1**	2	3
5	6	**0**	**1**	2	3	4
6	**0**	**1**	2	3	4	5

The number of n-ary quasigroups. LOWER bound

- How to obtain large number of multary quasigroups of fixed order q?
- !!! Switching
- Starting to switch from the linear multary quasigroups is not a good idea sometimes. For example, $f(x_1, x_2, ..., x_n) = x_1 + x_2 + ... + x_n \bmod 7$

0	**1**	2	3	4	5	6
1	2	3	4	5	6	**0**
2	3	4	5	6	**0**	**1**
3	4	5	6	**0**	**1**	2
4	5	6	**0**	**1**	2	3
5	6	**0**	**1**	2	3	4
6	**0**	**1**	2	3	4	5

The number of n-ary quasigroups. LOWER bound

Lower bound on the number of n-ary quasigroups of order q:
2^T where T is the maximal number of independent switching components (trades) in an n-ary quasigroup. Since the minimal trade size is 2^n, $T \le (q/2)^n$ which is tight for even q, but for odd q we have only $T \ge \left(\frac{q-3}{2}\right)^n$ in the iterated n-ary quasigroup $\psi(x_1, \psi(x_2, \psi(x_3, \ldots \psi(x_{n-1}, x_n)\ldots)))$ [Potapov, K, subm.].

ψ :

1	8	4	5	6	7	2	3	0
8	0	5	4	7	6	3	2	1
6	7	3	8	0	1	4	5	2
7	6	8	2	1	0	5	4	3
2	3	6	7	5	8	0	1	4
3	2	7	6	8	4	1	0	5
4	5	0	1	2	3	7	8	6
5	4	1	0	3	2	8	6	7
0	1	2	3	4	5	6	7	8

Back to 1-perfect codes

Returning to the codes, the q-ary Hamming code can be treated as obtained by the Phelps construction from the linear multary quasigroup of order q. Switching components in this code correspond to switching components in the multary quasigroup, which are not minimal possible. Replacing the linear multary quasigroup by a specially constructed nonlinear one, we can improve the constant α in the second floor of the lower bound for odd $q \geq 5$.

Thank you for your attention!

Thank organizers for the wonderful conference!