On MDS and perfect codes in Doob graphs

Denis Krotov, j.w. with Evgeny Bespalov

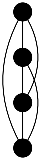
Sobolev Institute of Mathematics, Novosibirsk, Russia

G2S2, Novosibirsk, 15-28 May 2016

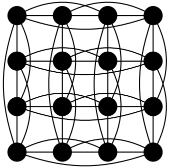
Hamming graph

- $\Sigma = \{0, 1, \ldots, q-1\}$. Σ^n – the set of n-words over Σ.
- The graph with the vertex set Σ^n, where two words are adjacent iff they differ in only one coordinate, is called the Hamming graph $H(n, q)$. The Hamming graph can be considered as the Cartesian product of n copies of the complete graph K_q: $H(n, q) = K_q \times \ldots \times K_q$.

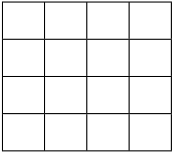
K_4:



$H(2, 4)$:



$H(2, 4)$:



Equitable partitions

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

Definition

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

Equitable partitions $\sim$ regular partitions $\sim$ partition designs $\sim$ perfect colorings $\sim \dots$

1-Perfect codes

- A set C of vertices of a regular graph $G = (V, E)$ is called a 1-perfect code iff every ball of radius 1 contains exactly one element of C.
- In other words, $(C, V \setminus C)$ is an equitable partition with quotient matrix $\begin{pmatrix} 0 & k \\ 1 & k-1 \end{pmatrix}$.

1-Perfect codes

- A set C of vertices of a regular graph $G = (V, E)$ is called a 1-perfect code iff every ball of radius 1 contains exactly one element of C.
- In other words, $(C, V \backslash C)$ is an equitable partition with quotient matrix $\begin{pmatrix} 0 & k \\ 1 & k-1 \end{pmatrix}$.

MDS codes

- A set C of vertices of $H(n,q)$ is called an MDS code with distance d if every subgraph isomorphic to $H(d-1,q)$ contains exactly one element of C.
- In other words, C is a distance-d MDS codes iff it has parameters $(n, q^{n-d+1}, d)_q$.
- C is a distance-2 MDS code iff $(C, V\setminus C)$ is an equitable partition with quotient matrix $\begin{pmatrix} 0 & n(q-1) \\ n & n(q-2) \end{pmatrix}$.

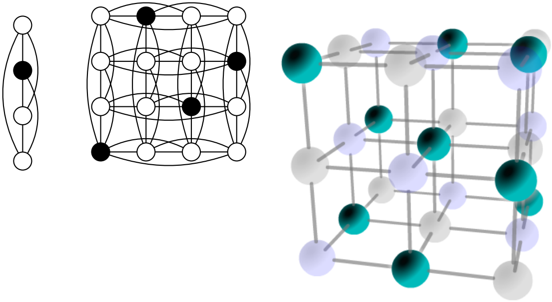
MDS codes

- A set C of vertices of $H(n, q)$ is called an MDS code with distance d if every subgraph isomorphic to $H(d-1, q)$ contains exactly one element of C.
- In other words, C is a distance-d MDS codes iff it has parameters $(n, q^{n-d+1}, d)_q$.
- C is a distance-2 MDS code iff $(C, V \setminus C)$ is an equitable partition with quotient matrix $\begin{pmatrix} 0 & n(q-1) \\ n & n(q-2) \end{pmatrix}$.

MDS codes

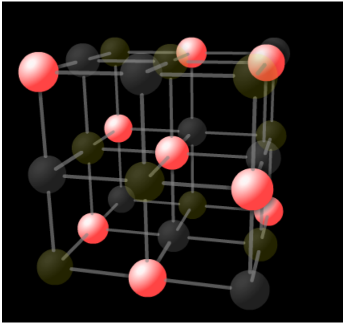
- A set C of vertices of $H(n,q)$ is called an MDS code with distance d if every subgraph isomorphic to $H(d-1,q)$ contains exactly one element of C.
- In other words, C is a distance-d MDS codes iff it has parameters $(n, q^{n-d+1}, d)_q$.
- C is a distance-2 MDS code iff $(C, V \setminus C)$ is an equitable partition with quotient matrix $\begin{pmatrix} 0 & n(q-1) \\ n & n(q-2) \end{pmatrix}$.

Distance-2 MDS codes: examples



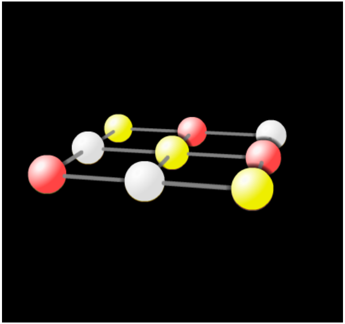
The distance-2 MDS codes are the maximum independent sets in the Hamming graphs.

Latin $(n-1)$-cubes $\leftrightarrow$ distance-2 MDS codes of length n



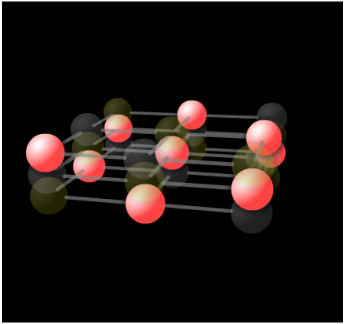
Every coordinate of a distance-2 MDS code is a function of the other coordinates (latin hypercube).

Latin $(n-1)$-cubes $\leftrightarrow$ distance-2 MDS codes of length n



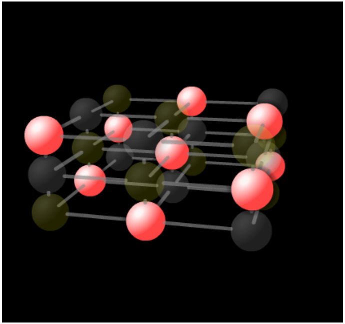
Every coordinate of a distance-2 MDS code is a function of the other coordinates (latin hypercube).

Latin $(n-1)$-cubes $\leftrightarrow$ distance-2 MDS codes of length n



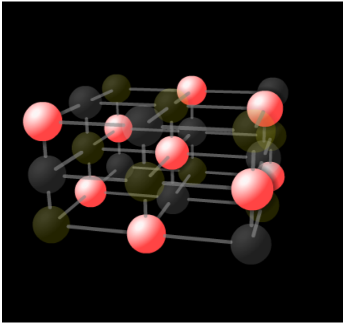
Every coordinate of a distance-2 MDS code is a function of the other coordinates (latin hypercube).

Latin $(n-1)$-cubes $\leftrightarrow$ distance-2 MDS codes of length n



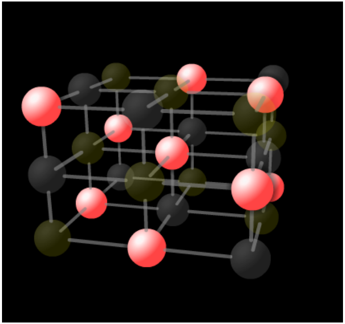
Every coordinate of a distance-2 MDS code is a function of the other coordinates (latin hypercube).

Latin $(n-1)$-cubes $\leftrightarrow$ distance-2 MDS codes of length n



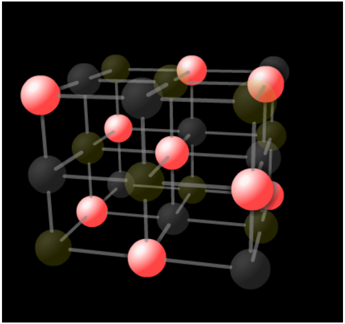
Every coordinate of a distance-2 MDS code is a function of the other coordinates (latin hypercube).

Latin $(n-1)$-cubes $\leftrightarrow$ distance-2 MDS codes of length n



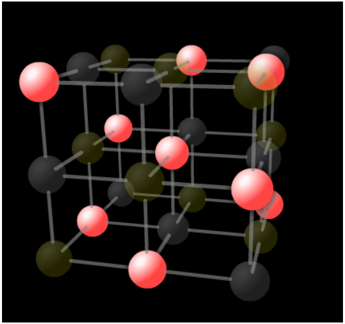
Every coordinate of a distance-2 MDS code is a function of the other coordinates (latin hypercube).

Latin $(n-1)$-cubes $\leftrightarrow$ distance-2 MDS codes of length n



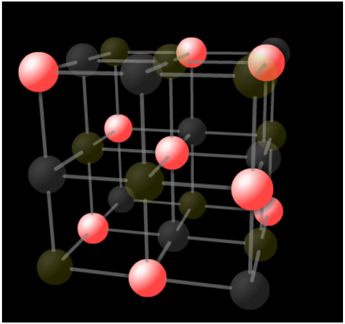
Every coordinate of a distance-2 MDS code is a function of the other coordinates (latin hypercube).

Latin $(n-1)$-cubes $\leftrightarrow$ distance-2 MDS codes of length n



Every coordinate of a distance-2 MDS code is a function of the other coordinates (latin hypercube).

Latin $(n-1)$-cubes $\leftrightarrow$ distance-2 MDS codes of length n



Every coordinate of a distance-2 MDS code is a function of the other coordinates (latin hypercube).

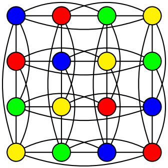
Latin hypercubes

Definition

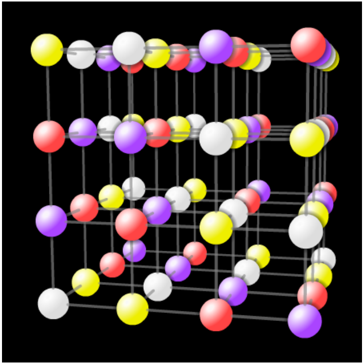
A latin hypercube is an equitable partition of $H(n,q)$ with quotient matrix $nJ_n - nI_n$.

$n = 2$:

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



$n = 3$:



MDS codes

- $d = 1$: the set of all vertices (trivial).
- $d = 2$: latin hypercubes, exist for every n.
    - $q = 2, 3$ — only one, up to equivalence
    - $q = 4$ — completely characterized [K., Potapov, 2009]
- $2 < d < n$: the length is bounded: $n \le 2q - 2$ (MDS conjecture: $n \le q + 2$, moreover, $n \le q + 1$ for most cases)
    - Classification up to equivalence, $q \le 8$: [Kokkala, Östergård, 2015] ($n = 5$, $d = 3$), [K., Kokkala, Östergård, 2015] ($n = 5$, $d > 3$), [Kokkala, Östergård, 2015+] ($d > 3$).
- $d = n$, $|C| = q$; for every n and q there is only one code in this case, up to isomorphism.
- $d = n + 1$: singleton (trivial).

MDS codes

- $d = 1$: the set of all vertices (trivial).
- $d = 2$: latin hypercubes, exist for every n.
  - $q = 2, 3$ — only one, up to equivalence
  - $q = 4$ — completely characterized [K., Potapov, 2009]
- $2 < d < n$: the length is bounded: $n \leq 2q - 2$ (MDS conjecture: $n \leq q + 2$, moreover, $n \leq q + 1$ for most cases)
  - Classification up to equivalence, $q \leq 8$: [Kokkala, Östergård, 2015] ($n = 5$, $d = 3$), [K., Kokkala, Östergård, 2015] ($n = 5$, $d > 3$), [Kokkala, Östergård, 2015+] ($d > 3$).
- $d = n$, $|C| = q$; for every n and q there is only one code in this case, up to isomorphism.
- $d = n + 1$: singleton (trivial).

MDS codes

- $d = 1$: the set of all vertices (trivial).
- $d = 2$: latin hypercubes, exist for every n.
  - $q = 2, 3$ — only one, up to equivalence
  - $q = 4$ — completely characterized [K., Potapov, 2009]
- $2 < d < n$: the length is bounded: $n \leq 2q-2$ (MDS conjecture: $n \leq q+2$, moreover, $n \leq q+1$ for most cases)
  - Classification up to equivalence, $q \leq 8$: [Kokkala, Östergård, 2015] ($n = 5$, $d = 3$), [K., Kokkala, Östergård, 2015] ($n = 5$, $d > 3$), [Kokkala, Östergård, 2015+] ($d > 3$).
- $d = n$, $|C| = q$; for every n and q there is only one code in this case, up to isomorphism.
- $d = n + 1$: singleton (trivial).

MDS codes

- $d = 1$: the set of all vertices (trivial).
- $d = 2$: latin hypercubes, exist for every n.
  - $q = 2, 3$ — only one, up to equivalence
  - $q = 4$ — completely characterized [K., Potapov, 2009]
- $2 < d < n$: the length is bounded: $n \leq 2q-2$ (MDS conjecture: $n \leq q + 2$, moreover, $n \leq q + 1$ for most cases)
  - Classification up to equivalence, $q \leq 8$: [Kokkala, Östergård, 2015] ($n = 5$, $d = 3$), [K., Kokkala, Östergård, 2015] ($n = 5$, $d > 3$), [Kokkala, Östergård, 2015+] ($d > 3$).
- $d = n$, $|C| = q$; for every n and q there is only one code in this case, up to isomorphism.
- $d = n + 1$: singleton (trivial).

MDS codes

- $d = 1$: the set of all vertices (trivial).
- $d = 2$: latin hypercubes, exist for every n.
  - $q = 2, 3$ — only one, up to equivalence
  - $q = 4$ — completely characterized [K., Potapov, 2009]
- $2 < d < n$: the length is bounded: $n \leq 2q-2$ (MDS conjecture: $n \leq q+2$, moreover, $n \leq q+1$ for most cases)
  - Classification up to equivalence, $q \leq 8$: [Kokkala, Östergård, 2015] ($n = 5$, $d = 3$), [K., Kokkala, Östergård, 2015] ($n = 5$, $d > 3$), [Kokkala, Östergård, 2015+] ($d > 3$).
- $d = n$, $|C| = q$; for every n and q there is only one code in this case, up to isomorphism.
- $d = n + 1$: singleton (trivial).

MDS codes

- $d = 1$: the set of all vertices (trivial).
- $d = 2$: latin hypercubes, exist for every n.
  - $q = 2, 3$ — only one, up to equivalence
  - $q = 4$ — completely characterized [K., Potapov, 2009]
- $2 < d < n$: the length is bounded: $n \leq 2q-2$ (MDS conjecture: $n \leq q + 2$, moreover, $n \leq q + 1$ for most cases)
  - Classification up to equivalence, $q \leq 8$: [Kokkala, Östergård, 2015] ($n = 5$, $d = 3$), [K., Kokkala, Östergård, 2015] ($n = 5$, $d > 3$), [Kokkala, Östergård, 2015+] ($d > 3$).
- $d = n$, $|C| = q$; for every n and q there is only one code in this case, up to isomorphism.
- $d = n + 1$: singleton (trivial).

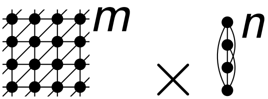
MDS codes

- $d = 1$: the set of all vertices (trivial).
- $d = 2$: latin hypercubes, exist for every n.
  - $q = 2, 3$ — only one, up to equivalence
  - $q = 4$ — completely characterized [K., Potapov, 2009]
- $2 < d < n$: the length is bounded: $n \leq 2q-2$ (MDS conjecture: $n \leq q+2$, moreover, $n \leq q+1$ for most cases)
  - Classification up to equivalence, $q \leq 8$: [Kokkala, Östergård, 2015] ($n = 5$, $d = 3$), [K., Kokkala, Östergård, 2015] ($n = 5$, $d > 3$), [Kokkala, Östergård, 2015+] ($d > 3$).
- $d = n$, $|C| = q$; for every n and q there is only one code in this case, up to isomorphism.
- $d = n + 1$: singleton (trivial).

MDS codes

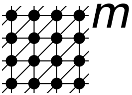
- $d = 1$: the set of all vertices (trivial).
- $d = 2$: latin hypercubes, exist for every n.
  - $q = 2, 3$ — only one, up to equivalence
  - $q = 4$ — completely characterized [K., Potapov, 2009]
- $2 < d < n$: the length is bounded: $n \leq 2q-2$ (MDS conjecture: $n \leq q + 2$, moreover, $n \leq q + 1$ for most cases)
  - Classification up to equivalence, $q \leq 8$: [Kokkala, Östergård, 2015] ($n = 5$, $d = 3$), [K., Kokkala, Östergård, 2015] ($n = 5$, $d > 3$), [Kokkala, Östergård, 2015+] ($d > 3$).
- $d = n$, $|C| = q$; for every n and q there is only one code in this case, up to isomorphism.
- $d = n + 1$: singleton (trivial).

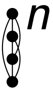
The Doob graphs

- $D(m,n) = Sh^m \times K_4^n =$ 

- If $m > 0$ then $D(m,n)$ is a Doob graph.
- $D(0,n)$ is the Hamming graph $H(n,4)$
(in general, $H(n,q) = K_q^n$)
- $D(m,n)$ is a distance-regular graph with the same parameters (intersection numbers) as $H(2m+n,4)$.

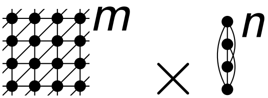
The Doob graphs

- $D(m, n) = Sh^m \times K_4^n =$ 

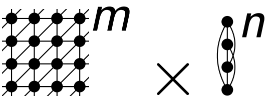
$\times$ 

- If $m > 0$ then $D(m, n)$ is a Doob graph.
- $D(0, n)$ is the Hamming graph $H(n, 4)$
(in general, $H(n, q) = K_q^n$)
- $D(m, n)$ is a distance-regular graph with the same parameters (intersection numbers) as $H(2m + n, 4)$.

The Doob graphs

- $D(m,n) = Sh^m \times K_4^n =$ 
- If $m > 0$ then $D(m,n)$ is a Doob graph.
- $D(0,n)$ is the Hamming graph $H(n,4)$
  (in general, $H(n,q) = K_q^n$)
- $D(m,n)$ is a distance-regular graph with the same parameters (intersection numbers) as $H(2m+n,4)$.

The Doob graphs

- $D(m, n) = Sh^m \times K_4^n =$ 

- If $m > 0$ then $D(m, n)$ is a Doob graph.
- $D(0, n)$ is the Hamming graph $H(n, 4)$
  (in general, $H(n, q) = K_q^n$)
- $D(m, n)$ is a distance-regular graph with the same parameters (intersection numbers) as $H(2m + n, 4)$.

Codes in Doob graphs

- In Doob graphs MDS codes can be defined by parameters $(2m+n, |C|, d)$.
- A distance-2 MDS code can be defined as the first cell of an equitable partition with the quotient matrix $\begin{pmatrix} 0 & 3N \\ N & 2N \end{pmatrix}$, $N = 2m+n$.
- A distance-2 MDS code can be defined as a maximum independent set of vertices (a maximum coclique) of the Doob graph.

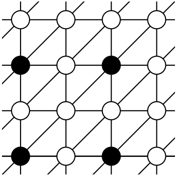
Codes in Doob graphs

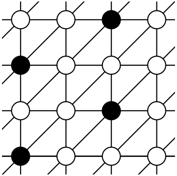
- In Doob graphs MDS codes can be defined by parameters $(2m+n, |C|, d)$.
- A distance-2 MDS code can be defined as the first cell of an equitable partition with the quotient matrix $\begin{pmatrix} 0 & 3N \\ N & 2N \end{pmatrix}$, $N = 2m+n$.
- A distance-2 MDS code can be defined as a maximum independent set of vertices (a maximum coclique) of the Doob graph.

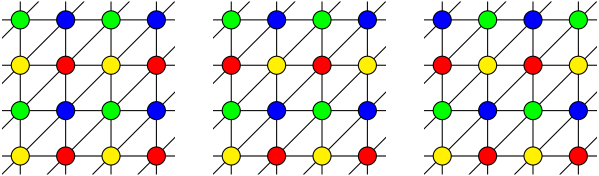
Codes in Doob graphs

- In Doob graphs MDS codes can be defined by parameters $(2m+n, |C|, d)$.
- A distance-2 MDS code can be defined as the first cell of an equitable partition with the quotient matrix $\begin{pmatrix} 0 & 3N \\ N & 2N \end{pmatrix}$, $N = 2m+n$.
- A distance-2 MDS code can be defined as a maximum independent set of vertices (a maximum coclique) of the Doob graph.

MDS codes in $D(1,0)$ and $D(1,1)$

"Linear": 

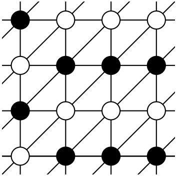
"Nonlinear": 

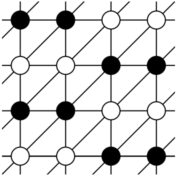


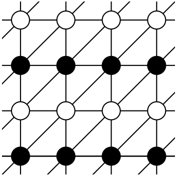
As in the case of $H(n,4)$, for a distance-2 MDS code in $D(m, n > 0)$, the value one Hamming coordinate can be considered as the color of the vertex of $D(m, n-1)$, we call such colorings latin-like colorings.

2-fold MDS codes

A 2-fold MDS code in $D(m,n)$ is defined as a cell of an equitable partition with quotient matrix $\begin{pmatrix} N & 2N \\ 2N & N \end{pmatrix}$, $N = 2m + n$.





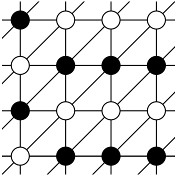
"Linear": 

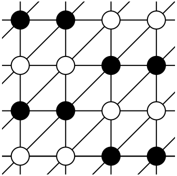
Lemma

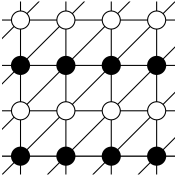
The 2-fold MDS codes in $D(m,n)$ are the solutions of the maximum-cut problem (the number of black-white edges is maximized).

2-fold MDS codes

A 2-fold MDS code in $D(m,n)$ is defined as a cell of an equitable partition with quotient matrix $\begin{pmatrix} N & 2N \\ 2N & N \end{pmatrix}$, $N = 2m + n$.





"Linear": 

Lemma

The 2-fold MDS codes in $D(m,n)$ are the solutions of the maximum-cut problem (the number of black-white edges is maximized).

Decomposable 2-fold MDS codes

- A 2-fold MDS code is called decomposable (indecomposable) if its characteristic function can (cannot) be represented as a modulo-2 sum of two or more $\{0,1\}$- functions in disjoint nonempty collections of variables.
- A 2-fold MDS code is called linear if its characteristic function is a modulo-2 sum of the characteristic functions of linear 2-fold MDS codes in Sh and 2-fold MDS codes in K_4.

Theorem

A 2-fold MDS code in $D(m,n)$ is decomposable if an only if it induces a disconnected subgraph of $D(m,n)$.

Decomposable 2-fold MDS codes

- A 2-fold MDS code is called decomposable (indecomposable) if its characteristic function can (cannot) be represented as a modulo-2 sum of two or more $\{0,1\}$- functions in disjoint nonempty collections of variables.
- A 2-fold MDS code is called linear if its characteristic function is a modulo-2 sum of the characteristic functions of linear 2-fold MDS codes in Sh and 2-fold MDS codes in K_4.

Theorem

A 2-fold MDS code in $D(m,n)$ is decomposable if an only if it induces a disconnected subgraph of $D(m,n)$.

Decomposable 2-fold MDS codes

- A 2-fold MDS code is called decomposable (indecomposable) if its characteristic function can (cannot) be represented as a modulo-2 sum of two or more $\{0,1\}$- functions in disjoint nonempty collections of variables.
- A 2-fold MDS code is called linear if its characteristic function is a modulo-2 sum of the characteristic functions of linear 2-fold MDS codes in Sh and 2-fold MDS codes in K_4.

Theorem

A 2-fold MDS code in $D(m, n)$ is decomposable if an only if it induces a disconnected subgraph of $D(m, n)$.

Semilinear and reducible MDS codes

- A distance-2 MDS code is called semilinear if it is a subset of a linear 2-fold MDS code.
- A distance-2 MDS code is called reducible if the corresponding latin-like coloring is a repetition-free composition of latin-like colorings of Doob (Hamming) graphs of smaller diameter.

Theorem

Every distance-2 MDS code in $D(m, n)$ is semilinear or reducible.

Semilinear and reducible MDS codes

- A distance-2 MDS code is called semilinear if it is a subset of a linear 2-fold MDS code.
- A distance-2 MDS code is called reducible if the corresponding latin-like coloring is a repetition-free composition of latin-like colorings of Doob (Hamming) graphs of smaller diameter.

Theorem

Every distance-2 MDS code in $D(m, n)$ is semilinear or reducible.

Semilinear and reducible MDS codes

- A distance-2 MDS code is called semilinear if it is a subset of a linear 2-fold MDS code.
- A distance-2 MDS code is called reducible if the corresponding latin-like coloring is a repetition-free composition of latin-like colorings of Doob (Hamming) graphs of smaller diameter.

Theorem

Every distance-2 MDS code in $D(m, n)$ is semilinear or reducible.

MDS codes, $2 < d < 2m + n$

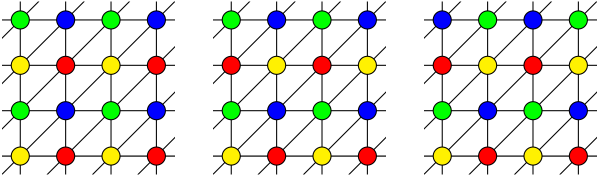
diam	graph	$d = 3$	$d = 4$	graph	diam
4	$D(1, 2)$	1 code	1 code	$D(1, 3)$	5
4	$D(2, 0)$	2 codes	2 codes	$D(2, 1)$	5
5	$D(1, 3)$	1 code	0	$D(1, 4)$	6
5	$D(2, 1)$	2 codes	1 code	$D(2, 2)$	6
			0	$D(3, 0)$	6

The distance-3 codes in Doob graphs of diameter 5 are 1-perfect. Two of these three codes were constructed in [Koolen, Munemasa, 2000]. Only one of these three codes can be extended to a distance-4 code in a Doob graph of diameter 6.

Partition lemma

Lemma

If $\{G_1, G_2, G_3\}$ is an edge partition of the complete graph K_{16} and G_1 and G_2 are strongly regular graphs with $\lambda = \mu = 2$ (i.e., $K_4 \times K_4$ or Sh), then K_3 is $K_4 + K_4 + K_4 + K_4$.



A distance-3 MDS code in $D(2,0)$ or $D(1,2)$ can be sonsidered as a set $\{(x, f(x) \,|\, x \in V(Sh)\}$. If $(x, f(x))$ and $(x', f(x'))$ are elements of a distance-3 MDS code in $D(2,0)$ or $D(1,2)$, then $\{x, x'\}$ and $\{f(x), f(x')\}$ cannot be edjes simultaneously. Applying Lemma, we see three non-isomorphic situations, two corresponding to $D(2,0)$ and one corresponding to $D(1,2)$.

MDS codes, $d = 2m + n$

A distance-$2m + n$ MDS code in $D(m, n)$ consists of 4 vertices $(x_1^i, ..., x_m^i, y_1^i, ..., y_n^i)$, $i = 1, 2, 3, 4$. for every Shrikhande coordinate j, the set $\{x_j^1, x_j^2, x_j^3, x_j^4\}$ is a coclique in Sh. There are two nonisomorphic 4-cocliques in Sh. For the nonlinear coclique, there are three nonisomorphic ordering..... The total number of non-isomorphic MDS codes is $m^3/36 + O(m^2)$.

Smallest eigenvalue

It can be seen that the eigenvalues of the quotient matrices $\begin{pmatrix} 0 & 3N \\ N & 2N \end{pmatrix}$, and $\begin{pmatrix} N & 2N \\ 2N & N \end{pmatrix}$, $N = 2m + n$, are the largest $(3N)$ and the smallest $(-N)$ eigenvalue of $D(m, n)$.

The only other admissible quotient matrix with this property is $\begin{pmatrix} 0.5N & 2.5N \\ 1.5N & 1.5N \end{pmatrix} = \begin{pmatrix} m & 5m \\ 3m & 3m \end{pmatrix}$.