An injective map from the set of maximum independent sets in a Doob graph to the set of 4-ary distance-2 MDS codes

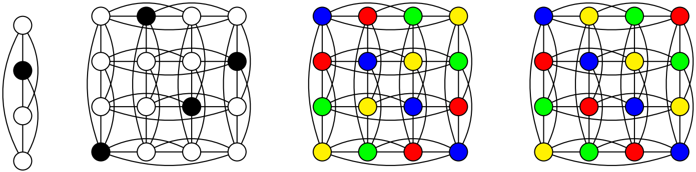
Denis Krotov
Sobolev Institute of Mathematics
Novosibirsk, Russia

G2A2
August 9–15, 2015. Ekaterinburg, Russia

Hamming graph

- The Hamming graph $H(n, q)$ is the Cartesian product K_q^n of n copies of the complete graph K_q of order q.
- The number of vertices in $H(n, q)$ is q^n, and the independence number of $H(n, q)$ is $q^{n-1} = q^n/q$. The maximum (of cardinality q^{n-1}) independent sets in $H(n, q)$ are known as the (distance-2) MDS codes.
- In combinatorics, these objects are also known as the latin hypercubes. In this case, one of the coordinates is usually considered as dependent from the others.
- If a latin hypercube is considered as the value table of an $(n-1)$-ary operation Q, then the corresponding system $(V(K_q), Q)$ is known as a multary, or polyadic, or $(n-1)$-ary quasigroup.

Examples of MDS codes



0	1	2	3	4
1	0	3	4	2
2	4	0	1	3
3	2	4	0	1
4	3	1	2	0

The number of MDS codes

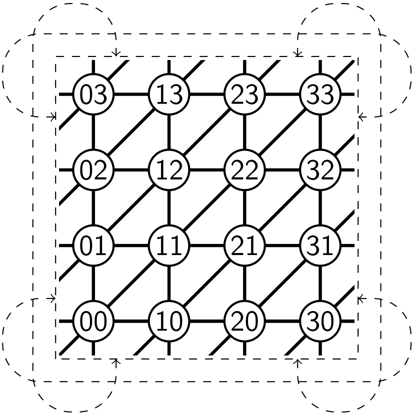
$$
\begin{array}{rcll}
 & |MDS(H(n,2))| & = 2 & \\
 & |MDS(H(n,3))| & = 3\cdot 2^{n-1} & \\
 & |MDS(H(n,4))| & = 2^{2^{n(1+o(1))}} & < 2^{2^{2n}} \text{ (\# of all sets)} \\
2^{2^{n/2}} \leq & |MDS(H(n,5)| & \leq 2^{3^{n(1+o(1))}} & \\
2^{3^n} \leq & |MDS(H(n,6))| & \leq 2^{4^{n(1+o(1))}} & \\
\dots & \dots & \dots & \\
2^{2^{cn}} \leq & |MDS(H(n,q))| & \leq 2^{2^{c'n}} &
\end{array}
$$

To compare, for binary perfect codes, $n = 2^k - 1$,

$$2^{2^{n/2(1+o(1))}} \leq |BPC(H(n,2))| \leq 2^{2^{n(1+o(1))}}$$

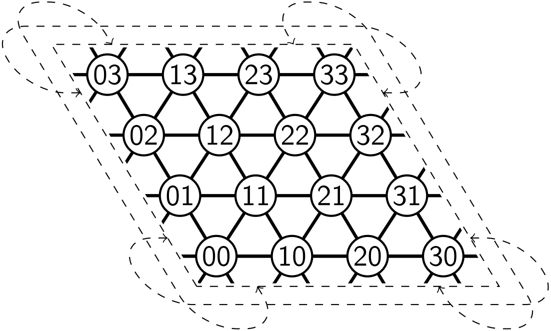
The same situation with Boolean bent functions.

Srikhande graph

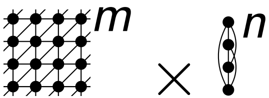


The Shrikhande graph *Sh* can be considered as the Cayley graph of Z_4^2 with the connecting set $\{01, 10, 11, 03, 30, 33\}$.

Srikhande graph



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 as $H(2m+n,4)$.

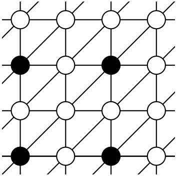
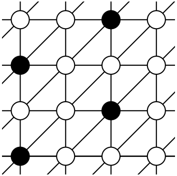
Distance-2 MDS codes

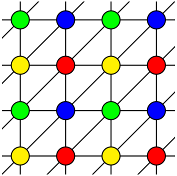
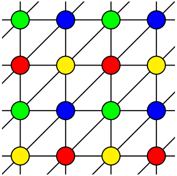
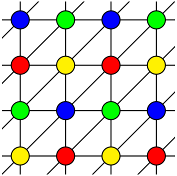
- It is easy to see that the independence number of $D(m, n)$ is $4^{2m+n}/4$.
- The maximum independent sets in the Hamming graphs are known as the (distance-2) MDS codes.
- We call the maximum independent sets in the Doob graphs (distance-2) MDS codes too, as they have the same parameters considered as error-correcting codes and as completely regular codes.

Distance-2 MDS codes

- There are 4 trivial MDS codes in $D(0,1)$;
- 24 equivalent MDS codes in $D(0,2)$;
- 16 MDS codes in $D(1,0)$,
  which form two equivalence classes (with 4 and 12 representatives, respectively).

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

Distance-2 MDS codes

- The number of MDS codes in $D(0, n)$ is

$$2^{2^{n-1}(1+o(1))}$$

(actually, the asymptotics is known [V Potapov, DK, 2006]).

- MAIN THEOREM: The number of MDS codes in $D(m, n)$ is

$$2^{2^{2m+n-1}(1+o(1))}.$$

Lower bound: simple construction

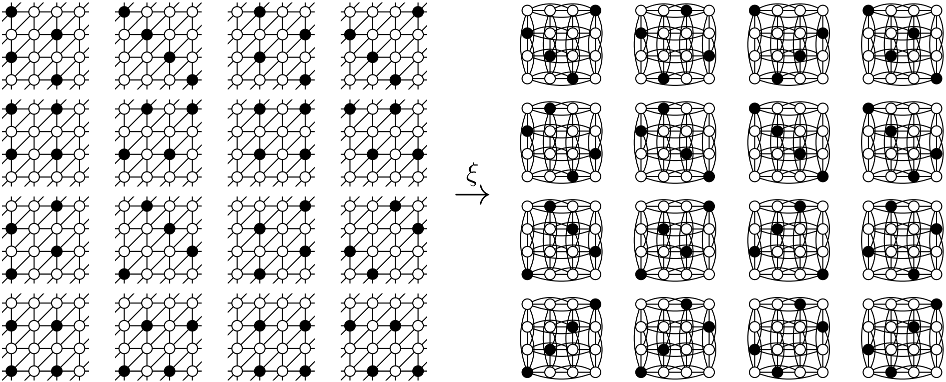
For every function λ from $\left(\{0,1,2,3\}^m \times \{0,1\}^n\right)_{\mathrm{even}}$ to $\{0,1\}$, the set

$$M_\lambda \stackrel{\mathrm{def}}{=} \left\{ (x'_1 x''_1, \ldots, x'_{m+n} x''_{m+n}) \in D(m,n) \quad \middle| \quad \begin{array}{l} \displaystyle\sum_{i=1}^{m+n} x'_i \equiv 0 \bmod 2, \\ \displaystyle\sum_{i=1}^{m+n} x''_i \equiv \lambda(x'_1, \ldots, x'_{m+n}) \bmod 2 \end{array} \right\}$$

is an MDS code. This gives $2^{2^{2m+n-1}}$ different MDS codes in $D(m,n)$.

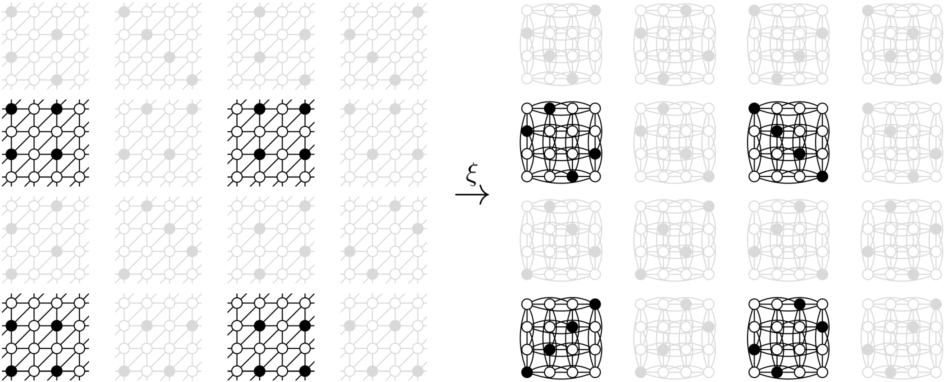
Upper bound: the map ξ

The map ξ from $\mathrm{MDS}_{D(1,0)}$ to $\mathrm{MDS}_{D(0,2)}$



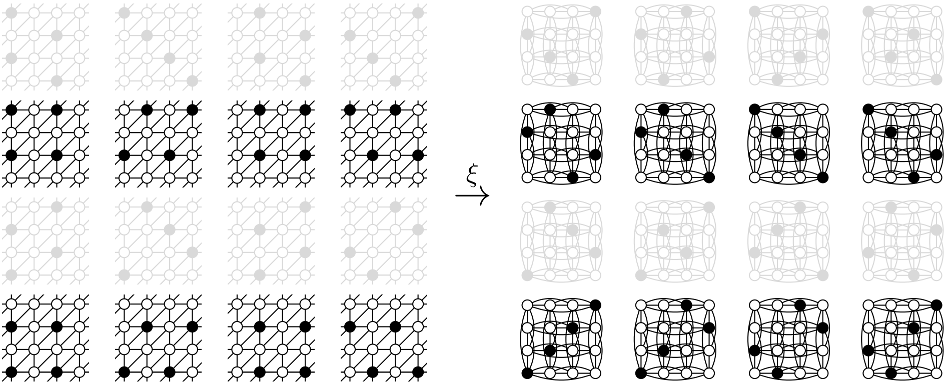
Upper bound: the map ξ

The map ξ from $\mathrm{MDS}_{D(1,0)}$ to $\mathrm{MDS}_{D(0,2)}$



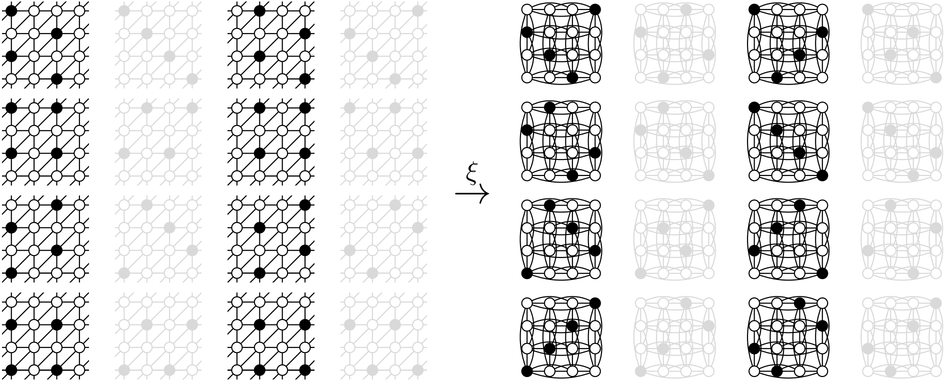
Upper bound: the map ξ

The map ξ from $\mathrm{MDS}_{D(1,0)}$ to $\mathrm{MDS}_{D(0,2)}$



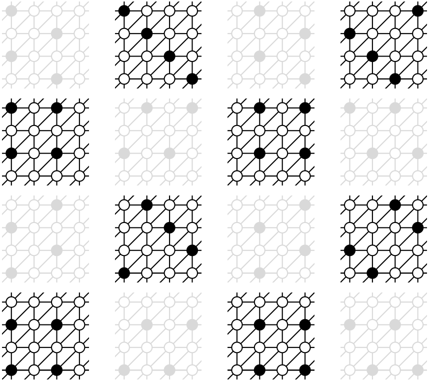
Upper bound: the map ξ

The map ξ from $\mathrm{MDS}_{D(1,0)}$ to $\mathrm{MDS}_{D(0,2)}$

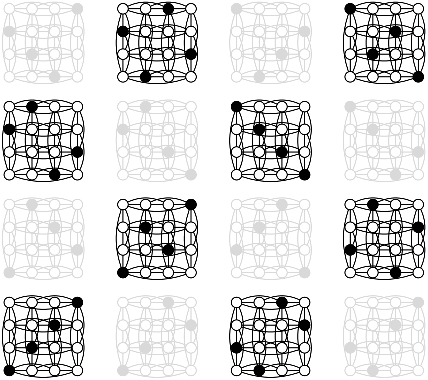


Upper bound: the map ξ

The map ξ from $\mathrm{MDS}_{D(1,0)}$ to $\mathrm{MDS}_{D(0,2)}$

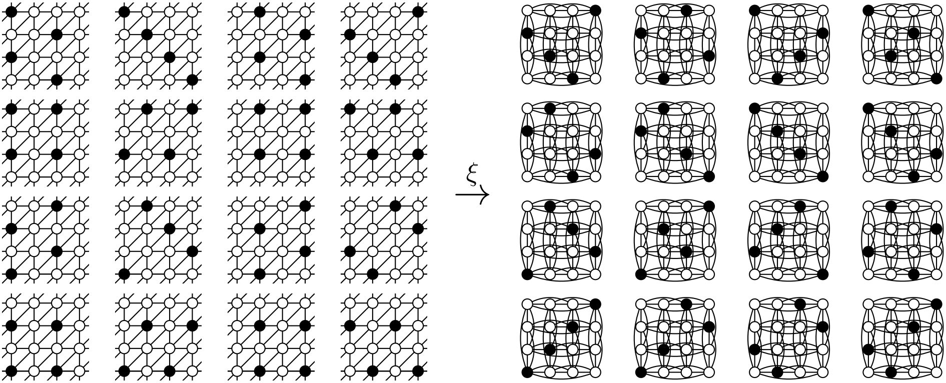


$\xrightarrow{\xi}$



Upper bound: the map ξ

The map ξ from $\mathrm{MDS}_{D(1,0)}$ to $\mathrm{MDS}_{D(0,2)}$



Upper bound: the map κ

- For arbitrary m, $n \geq 0$, the action of $\kappa : \mathrm{MDS}_{D(m+1,n)} \to \mathrm{MDS}_{D(m+1,n)}$ is defined as follows:

$$\kappa M \stackrel{\text{def}}{=} \Big\{(x_1, \ldots, x_m, z_1, z_2, y_1, \ldots, y_n) \in D(m, n+2) \\ \Big| \, (z_1, z_2) \in \xi M_{x_1,\ldots,x_m,y_1,\ldots,y_n}\Big\},$$

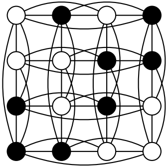
where

$$M_{x_1,\ldots,x_m,y_1,\ldots,y_n} \stackrel{\text{def}}{=} \{v \in Sh \mid (x_1, \ldots, x_m, v, y_1, \ldots, y_n) \in M\}$$

- Then, κ^m injectively maps $\mathrm{MDS}_{D(m,n)}$ into $\mathrm{MDS}_{D(0,2m+n)}$.
- COROLLARY:
$|\mathrm{MDS}_{D(m,n)}| \leq |\mathrm{MDS}_{D(0,2m+n)}| = 2^{2^{2m+n-1}(1+o(1))}$.

Two-fold MDS codes

The problem of asymptotic of log log of the number of objects is unsolved for so-called two-fold MDS codes in $H(n,4)$.



References

[1] D. S. Krotov, V. N. Potapov. On the Reconstruction of n-Quasigroups of Order 4 and the Upper Bounds on Their Number. *Proc. the Conference Devoted to the 90th Anniversary of Alexei A. Lyapunov, Novosibirsk, Russia*, 323–327, 2001. http://www.sbras.ru/ws/Lyap2001/2363

[2] Toru Ito. Creation Method of Table, Creation Apparatus, Creation Program and Program Storage Medium. Patent 2004/0243621A1, 2004. http://ip.com/patapp/US20040243621

[3] V. N. Potapov, D. S. Krotov. Asymptotics for the Number of n-Quasigroups of Order 4. *Sib. Math. J.* 47(4):720–731, 2006. http://dx.doi.org/10.1007/s11202-006-0083-9, translated from *Sib. Mat. Zh.* 47(4):873–887, 2006.

[4] D. S. Krotov, V. N. Potapov, P. V. Sokolova. On Reconstructing Reducible n-Ary Quasigroups and Switching Subquasigroups. *Quasigroups Relat. Syst.* 16(1):55–67, 2008. http://dx.doi.org/10.17686/sced_rusnauka_2008-1040

[5] B. D. McKay, I. M. Wanless. A Census of Small Latin Hypercubes. *SIAM J. Discrete Math.* 22(2):719–736, 2008. http://dx.doi.org/10.1137/070693874

References

[6] D. S. Krotov, V. N. Potapov. n-Ary Quasigroups of Order 4. *SIAM J. Discrete Math.* 23(2):561–570, 2009. `http://dx.doi.org/10.1137/070697331`

[7] V. N. Potapov, D. S. Krotov. On the Number of n-ary Quasigroups of Finite Order. *Discrete Math. Appl.* 21(5–6):575–585, 2011. `http://dx.doi.org/10.1515/dma.2011.035`, translated from *Diskretn. Mat.* 24(1):60–69, 2012.

[8] D. S. Krotov. On the Number of Maximum Independent Sets in Doob Graphs. *Siberian Electronic Mathematical Reports* 12, 2015. To appear.