КРИПТОНИТ

Characteristics of Hadamard square of Reed–Muller subcodes of special type

Victoria Vysotskaya

September 17, 2020

Relevance

- **McEliece and Niederreiter cryptosystems build on Goppa codes are still secure.**
- [Sidelnikov V. M., Shestakov S. O. “On cryptosystems based on generalized Reed–Solomon codes”, Discrete Mathematics 4(3), 1992]
  [Wieschebrink C., “Cryptanalysis of the Niederreiter Public Key Scheme Based on GRS Subcodes”, Lecture Notes in Computer Science (6061), 2010] **attack scheme on Reed–Solomon codes.**
- [Minder L., Shokrollahi A. “Cryptanalysis of the Sidelnikov”, Lecture Notes in Computer Science (4515), 2007],
  [Borodin M. A., Chizhov I. V. “Effective attack on the McEliece cryptosystem based on Reed-Muller codes”, Discrete Mathematics and Applications 24(5), 2014]
  attack scheme on Reed–Muller codes.

Definitions

The Reed–Muller code $RM(r, m)$ is the set of all Boolean functions

$$f(x_1, \dots, x_m),\ \mathbf{deg}(f) \leqslant r.$$

The standard basis of the Reed–Muller code $RM(r, m)$:

$$1,$$

$$x_1, x_2, \cdots, x_m,$$

$$x_1 x_2, \cdots, x_{m-1} x_m,$$

$$\cdots$$

$$x_1 \dots x_r, \cdots, x_{m-r-1} \dots x_m.$$

Hadamard product of two vectors $a \circ b$:

$$(a_1, \dots, a_n) \circ (b_1, \dots, b_n) = (a_1 b_1, \dots, a_n b_n).$$

Hadamard product of two codes A and B is the span of all pairwise products of form $a \circ b$, where $a \in A, b \in B$.

Stable subcode:

$$\left(\mathbf{span}\left(RM(r-1,m)\cup\{f_1,\dots,f_w\}\right)\right)^2 = RM(2r,m),\ \mathbf{deg}(f_i)=r.$$

Unstable subcode:

$$\left(\mathbf{span}\left(RM(r-1,m)\cup\{f_1,\dots,f_w\}\right)\right)^2 \subset RM(2r,m),\ \mathbf{deg}(f_i)=r.$$

[Chizhov I. V., Borodin M. A. “Hadamard products classification of subcodes of Reed–Muller codes codimension 1”, Discrete Mathematics and Applications 32(1), 2020]: attacks schemes on Reed–Muller subcodes of codimention 1.

[Couvreur A., Lequesne M. “On the security of subspace subcodes of Reed–Solomon codes for public key encryption”, https://arxiv.org/abs/2009.05826, 2020] attacks schemes on subcodes of Reed–Solomon codes.

Our goal

We look for minimum number $w(m,r)$ such that there exist monomials $f_1, \dots, f_{w(m,r)}$ for which the code

$$\mathbf{span}\big(RM(r-1,m) \cup \{f_1, \dots, f_{w(m,r)}\}\big)$$

is stable.

Another goal

We look for maximum number $q(m,r)$ such that there exist monomials $g_1, \dots, g_{q(m,r)}$ the code

$$\mathbf{span}\big(RM(r,m) \setminus \{g_1, \dots, g_{q(m,r)}\}\big)$$

is stable.

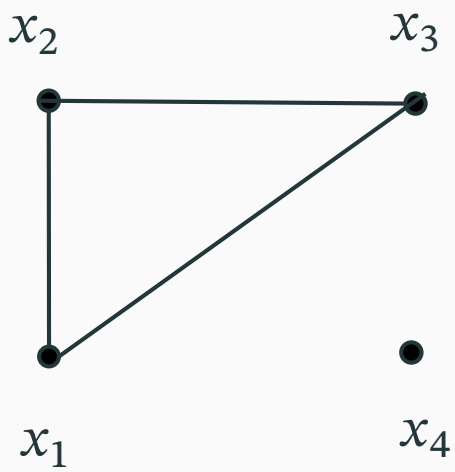
Note $q(m,r) = C_m^r - w(m,r)$.

Corollary
After removing any $q(m,r)+1 = C_m^r - w(m,r)+1$ basis vectors, one gets an unstable subcode.

Case $RM(2, m)$

Match a subcode $\mathcal{A} \subset RM(2, m)$ with a graph G with m vertices labeled $x_1, \ldots, x_m$. An edge $\{x_i, x_j\}$ is present if and only if monomial $x_i x_j \in \mathcal{A}$.

For $\mathcal{A} = \mathbf{span}(\{x_1x_2, x_1x_3, x_2x_3\}) \subset RM(2, 4)$ graph G has the form



Stable subcodes of $RM(2, m)$

We will say that a graph with m vertices *satisfies the property* P if

1. the degree $\mathbf{deg}(v)$ of any vertex v is not less than $m - 3$;
2. if $\mathbf{deg}(v) = m - 3$ and edges $\{v, u\}$ and $\{v, w\}$ are missing, then the edge $\{u, w\}$ is present.

Theorem
Subcode $\mathbf{span}\big(RM(1, m) \cup \{f_1, \ldots, f_w\}\big)$ is stable iff the property P is satisfied for the corresponding graph.

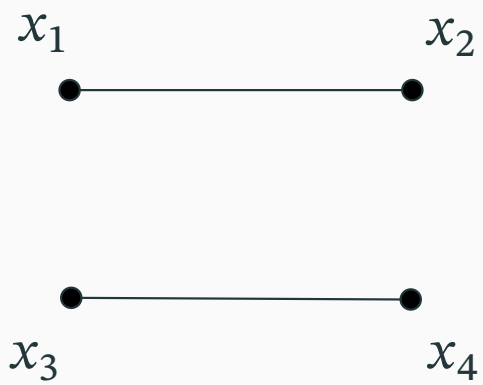
Stable subcodes of $RM(2, m)$

Theorem
$w(m, 2) = m(m-3)/2$ for $m \geqslant 4$.

So removing any $m+1$ or more monomials of degree 2 from the code $RM(2, m)$ we get an unstable subcode.

Stable subcodes of $RM(2, m)$

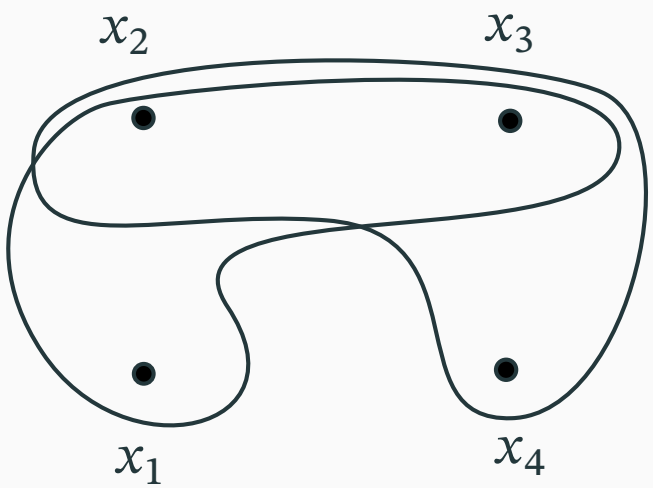
If $\left(\mathbf{span}\left(RM(1, m) \cup \{f_1, \ldots, f_{w(m,r)}\}\right)\right)^2 = RM(4, m)$ iff any induced subgraph of G with 4 vertices has a subgraph isomorphic to the graph



General case

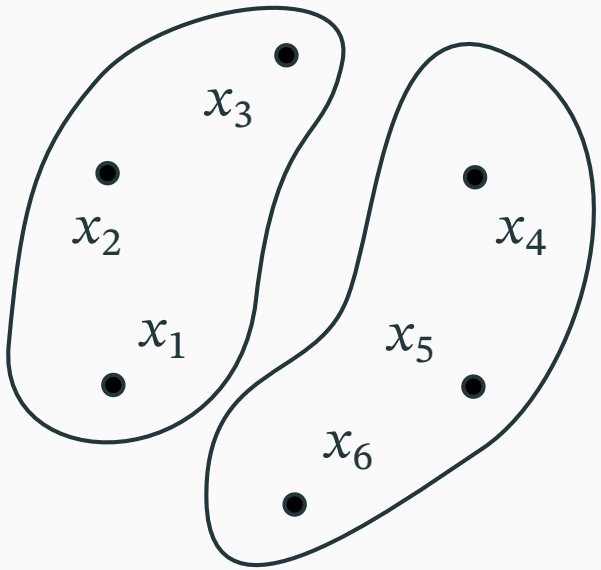
We match a subcode $\mathcal{A} \subset RM(r, m)$ with a hypergraph G with m vertices labeled $x_1, \dots, x_m$. An r-edge $\{x_{i_1}, \dots, x_{i_r}\}$ is present if and only if monomial $x_{i_1} \dots x_{i_r} \in \mathcal{A}$.

For $\mathcal{A} = \mathbf{span}(\{x_1x_2x_3, x_2x_3x_4\}) \subset RM(3, 4)$ hypergraph G has the form



Stable subcodes of $RM(r, m)$

Graph interpretation: $\left(\mathbf{span}\left(RM(r-1,m) \cup \{f_1, \ldots, f_w\}\right)\right)^2 = RM(2r, m)$ iff each set of $2r$ vertices is covered by two disjoint r-edges.



Trivial lower bound

For any natural r and $m \geqslant 2r$

$$w(m, r) \geqslant C_m^{2r} / C_{m-r}^r.$$

Then $w(6, 2) \geqslant 3$.

Corollary

Any stable graph contains at least $1/C_{2r}^r$ edges of a complete graph.

Improved lower bound

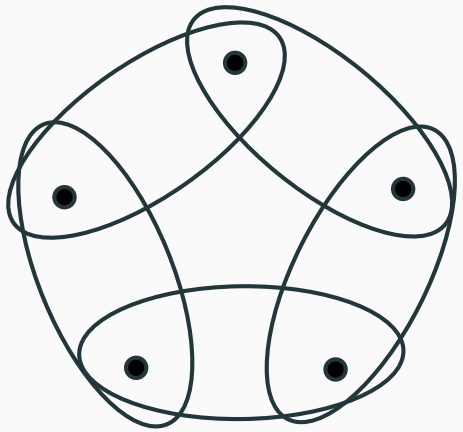
$$w(m, r) \geqslant \sqrt{\gamma + 2C_m^{2r}} + \sqrt{\gamma}, \quad \text{где} \quad \gamma = \frac{1}{4} \sum_{i=\max\{1, 3r-m\}}^{r-1} C_r^i.$$

Then $w(6, 2) \geqslant 6$.

Theoretical upper bound
For any natural $r \geqslant 2$, $m \geqslant 2r$ and $h < r/3$

$$w(m, r) \leqslant C_m^r - T(r, m, h) \cdot (C_{2r}^r - 2)\,.$$

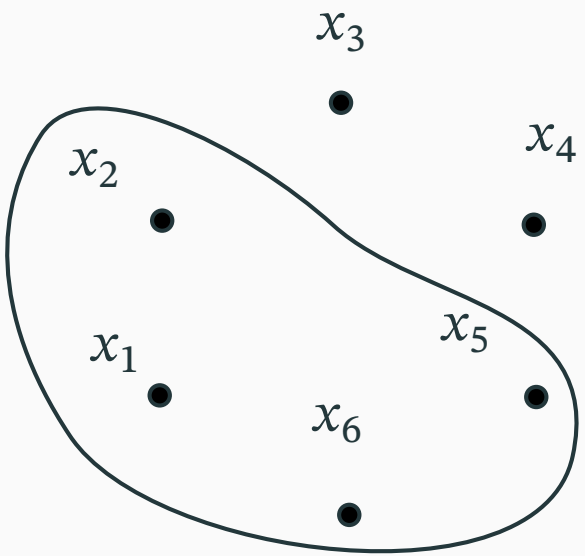
Example: $T(1, 5, 1) = 5$.



Theoretical upper bound
For any natural $r \geqslant 2$, $m \geqslant 2r$ and $h < r/3$

$$w(m, r) \leqslant C_m^r - T(r, m, h) \cdot (C_{2r}^r - 2)\,.$$

Example: $T(2, 6, 0) = 1$; $w(6, 2) \leqslant 15 - 1 \cdot (6 - 2) = 11$.



Theoretical upper bound

For any natural $r \geqslant 2$, $m \geqslant 2r$ and $h < r/3$

$$w(m, r) \leqslant C_m^r - T(r, m, h) \cdot (C_{2r}^r - 2)\,.$$

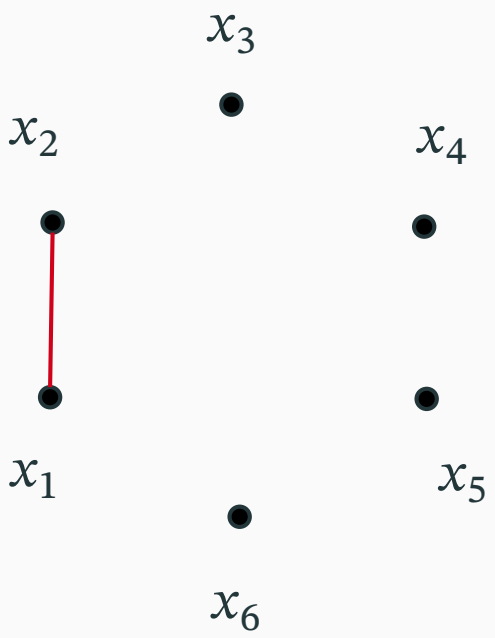
[Rödl V. “On a Packing and Covering Problem”, European Journal of Combinatorics 6(1), 1985]

$$\lim_{m \to \infty} T(r, m, h) \approx \frac{C_m^{\lfloor r/3 \rfloor}}{C_{2r}^{\lfloor r/3 \rfloor}}.$$

Empirical upper bound
Greedy algorithm

`github.com/VysotskayaVictory/StableGraphGreedy`

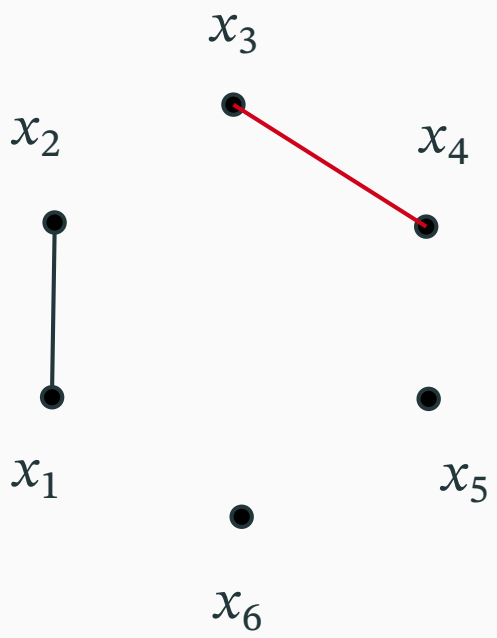
Example: for $r = 2, m = 6$.



Empirical upper bound
Greedy algorithm

`github.com/VysotskayaVictory/StableGraphGreedy`

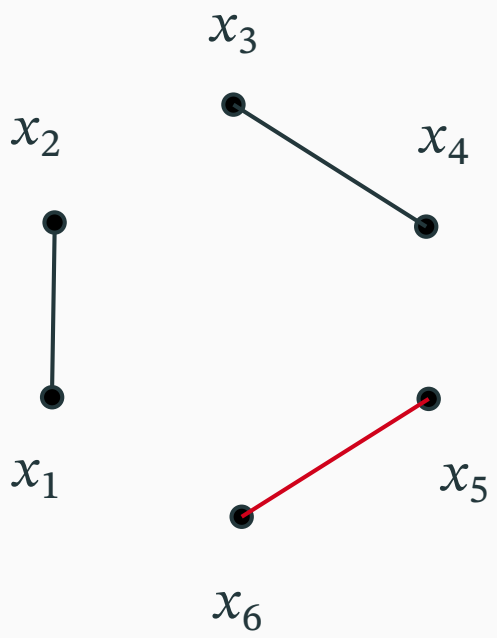
Example: for $r = 2, m = 6$.



Empirical upper bound
Greedy algorithm

`github.com/VysotskayaVictory/StableGraphGreedy`

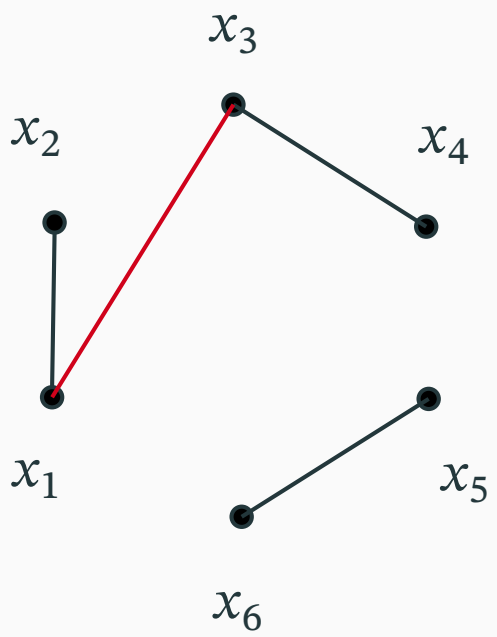
Example: for $r = 2, m = 6$.



Empirical upper bound
Greedy algorithm

`github.com/VysotskayaVictory/StableGraphGreedy`

Example: for $r = 2, m = 6$.

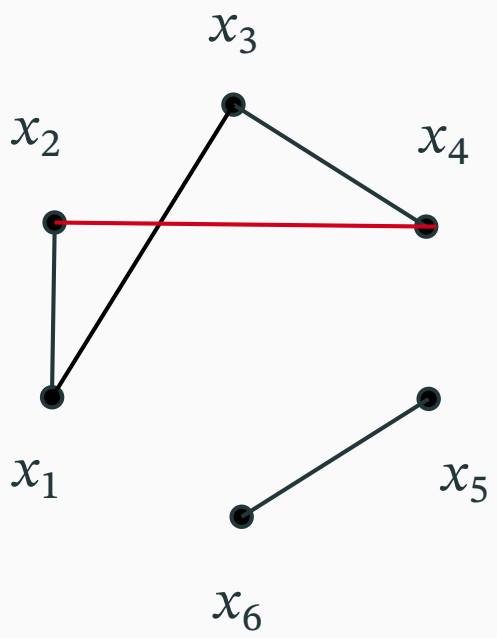


Empirical upper bound

Greedy algorithm

`github.com/VysotskayaVictory/StableGraphGreedy`

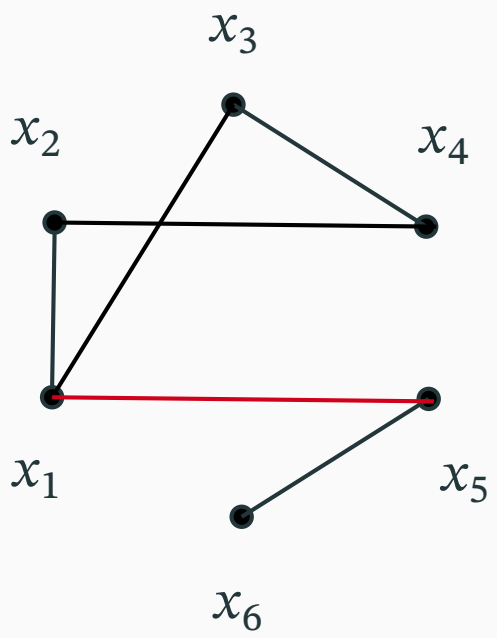
Example: for $r = 2, m = 6$.



Empirical upper bound
Greedy algorithm

`github.com/VysotskayaVictory/StableGraphGreedy`

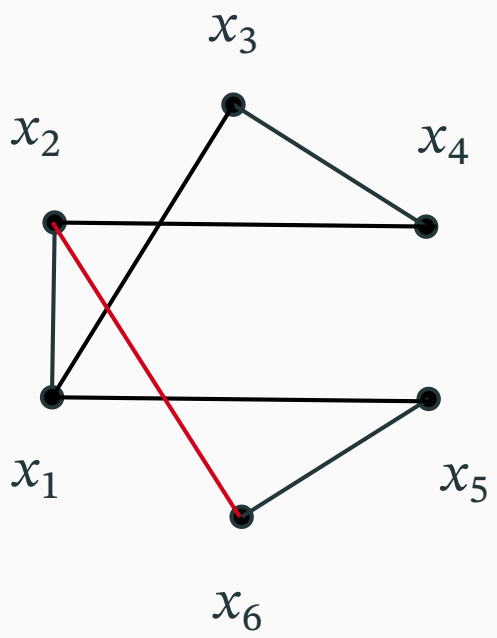
Example: for $r = 2, m = 6$.



Empirical upper bound
Greedy algorithm

`github.com/VysotskayaVictory/StableGraphGreedy`

Example: for $r = 2, m = 6$.

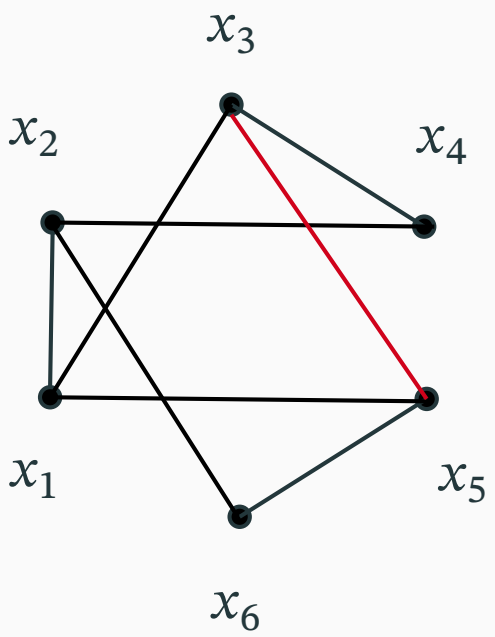


Empirical upper bound

Greedy algorithm

`github.com/VysotskayaVictory/StableGraphGreedy`

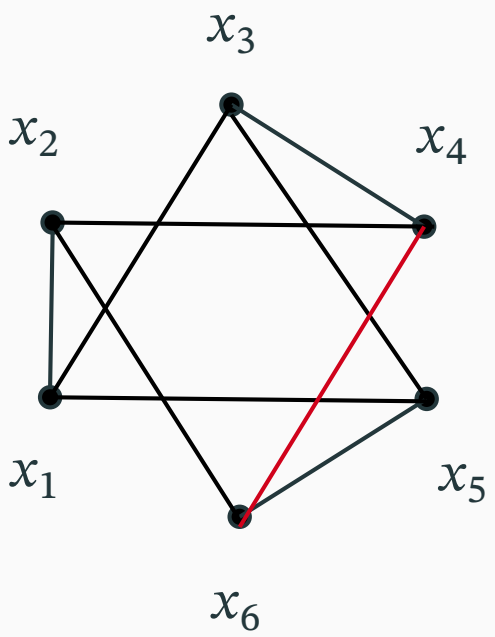
Example: for $r = 2, m = 6$.



Empirical upper bound
Greedy algorithm

`github.com/VysotskayaVictory/StableGraphGreedy`

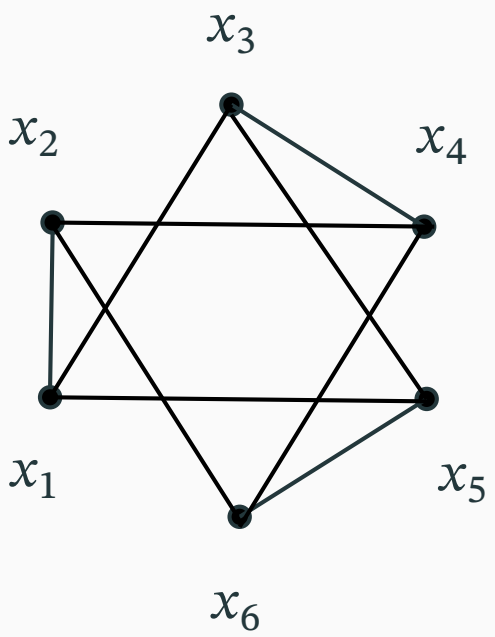
Example: for $r = 2, m = 6$.



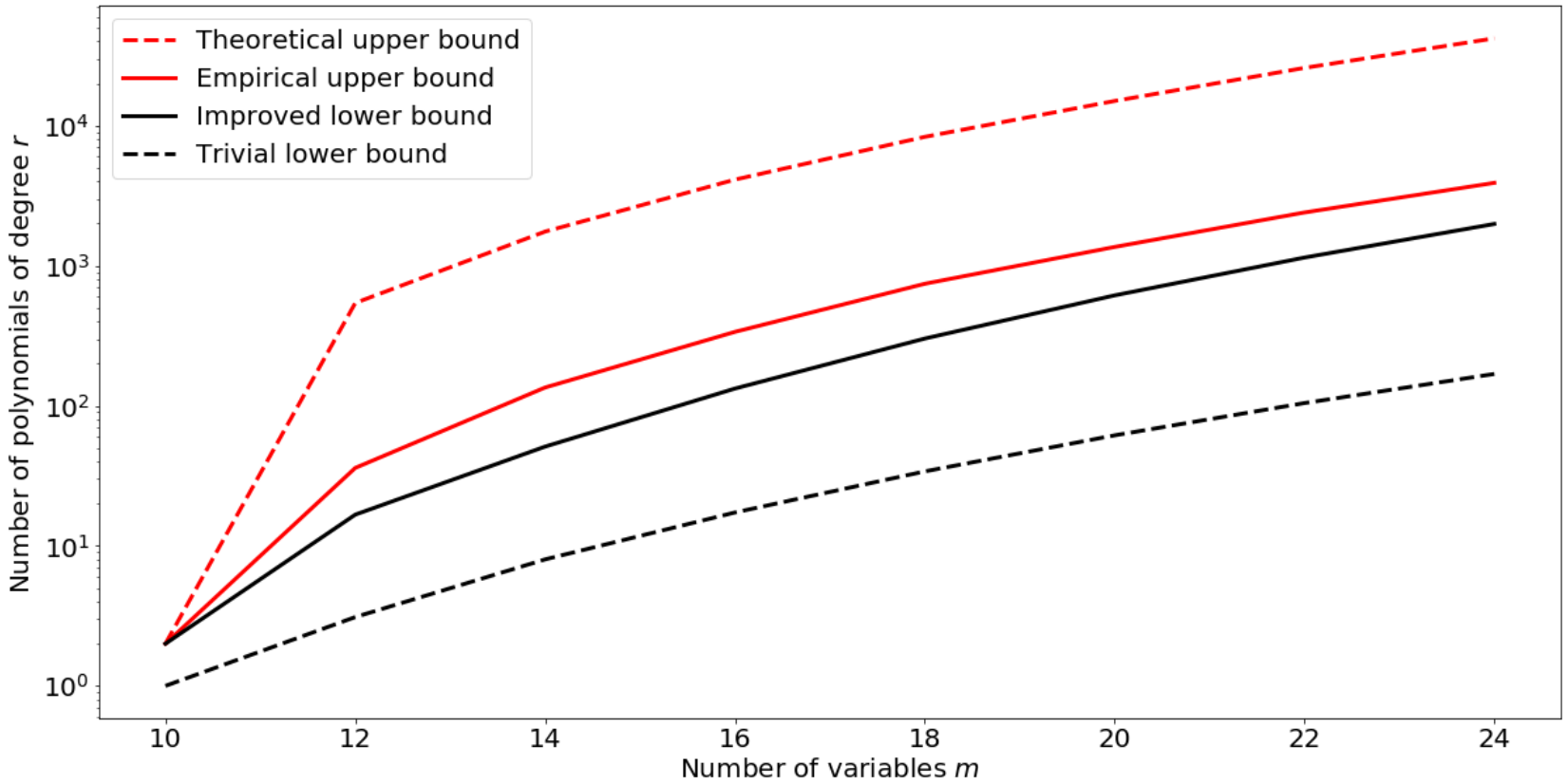
Empirical upper bound
Greedy algorithm

`github.com/VysotskayaVictory/StableGraphGreedy`

Example: for $r = 2, m = 6$. **Result:** 9 edges.



Comparison of upper bounds



The ratio of unstable $RM(r,m)$ subcodes

Theorem
The number of unstable $RM(r,m)$ subcodes is

$$\theta \leqslant \sum_{s=2}^{2r} C_m^s \cdot \sum_{\alpha \in \{1,2,3\}^{\upsilon(s)}} C_{k-1-2\upsilon(s)}^{\ell-\upsilon(s)-\#_3(\alpha)} + C_{k-1}^{\ell-1},$$

where

$$\upsilon(s) = \sum_{p=\max\{s-r,1\}}^{\min\{r,s-1\}} \frac{1}{2} C_s^p, \quad |I| = s.$$

Theorem
If $\ell = const$ and $r \geqslant 2\ell + 1$, then the ratio of unstable $RM(r,m)$ subcodes tends to zero as $m \to \infty$.

Here ℓ is a number of missing vectors,
k is the dimension of the original code.

1. For $RM(2, m)$ the exact structure of all stable subcodes was found.
2. For an arbitrary code $RM(r, m)$ the number $q(m, r)$ was estimated from both sides ($q(m, r) + 1$ is the minimum number such that any $q(m, r)$ monomials discarded from basis of $RM(m, r)$ result in unstable code).
3. The ratio of unstable subcodes tends to zero as $m \to \infty$ (with some not very restrictive assumptions).

Questions?