Zväčšovanie ťažkosti

kuko

22.4.2021

Pokročilá teória zložitosti

Plán

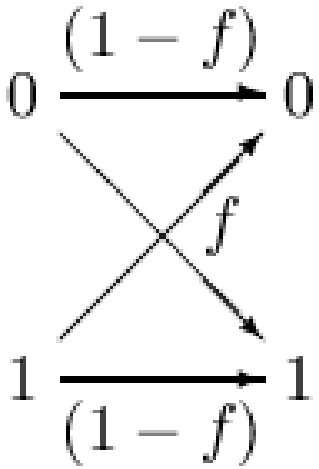
$$\exists \text{ ťažká funkcia} \Longrightarrow \exists \text{ veľmi ťažká funkcia} \Longrightarrow \exists \text{ pekelne ťažká funkcia}$$
$$\Longrightarrow \exists \text{ dobrý PNG} \Longrightarrow \text{vieme odhadnúť Pr[BPP-alg akceptuje]}$$
$$\Longrightarrow \mathsf{P} = \mathsf{BPP}.$$

Veľmi ťažké funkcie z ťažkých v najhoršom prípade

Chceme...

- máme f
- chceme $\hat{f}$ takú, že
  - ak f je ťažká v najhoršom prípade
  - tak $\hat{f}$ je veľmi ťažká
- inými slovami:
  - keby sa $\hat{f}$ dala vypočítať na 99% vstupov
  - tak by sa f dala spočítať všade
  - (nie o moc väčším obvodom)

Chceme...



Chceme...

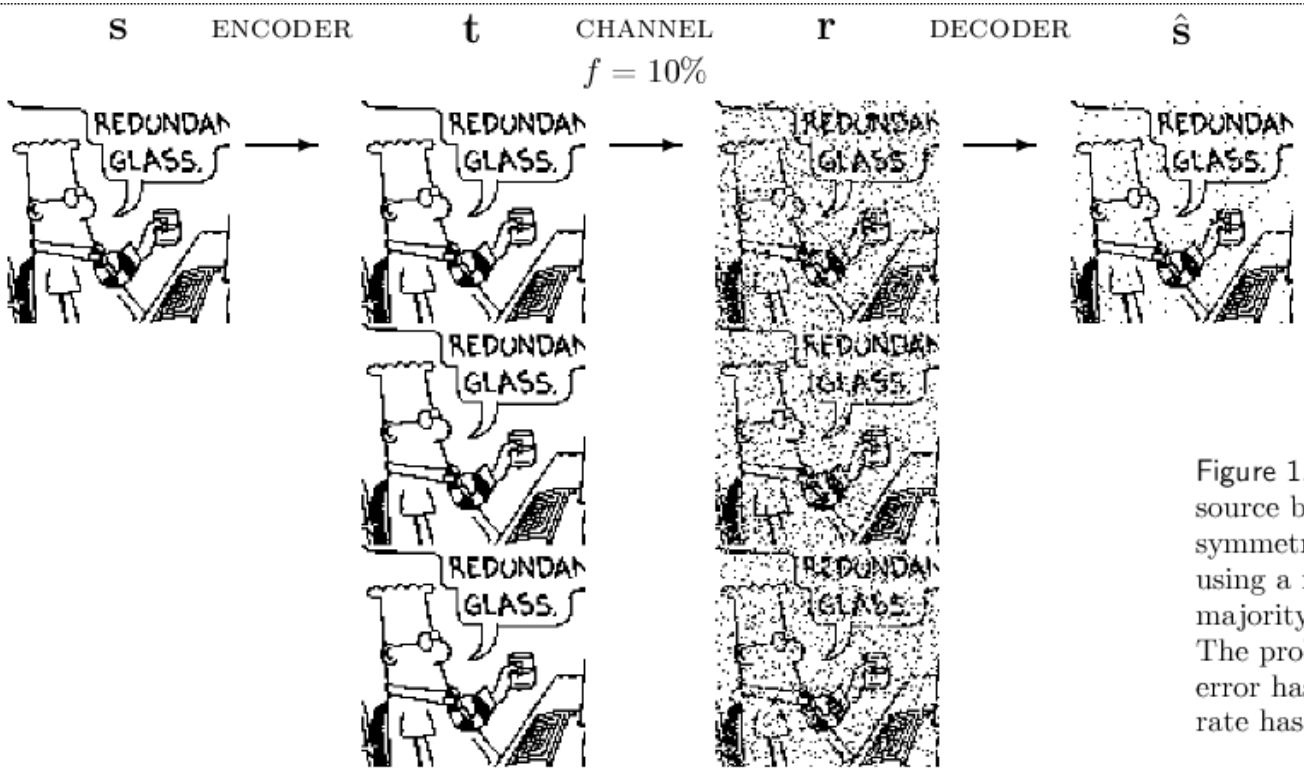


Figure 1.11. Transmitting 10 000 source bits over a binary symmetric channel with $f = 10\%$ using a repetition code and the majority vote decoding algorithm. The probability of decoded bit error has fallen to about 3%; the rate has fallen to 1/3.

Chceme...

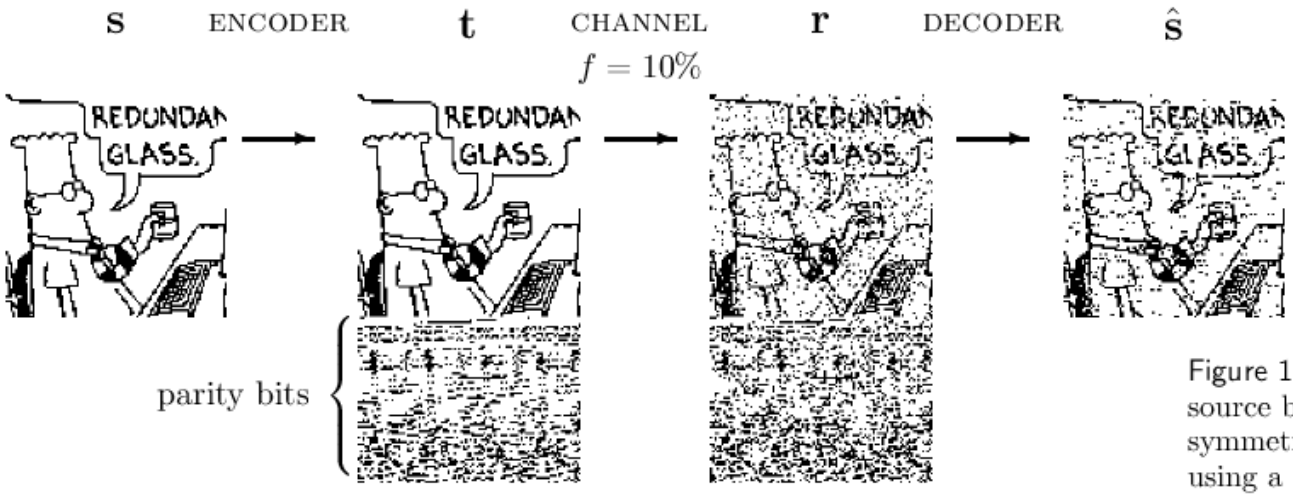
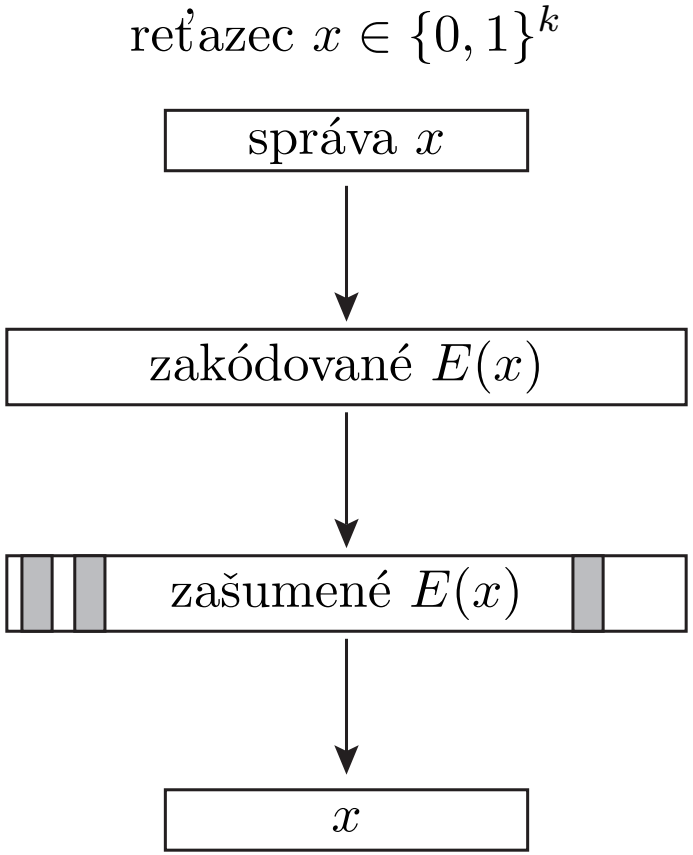
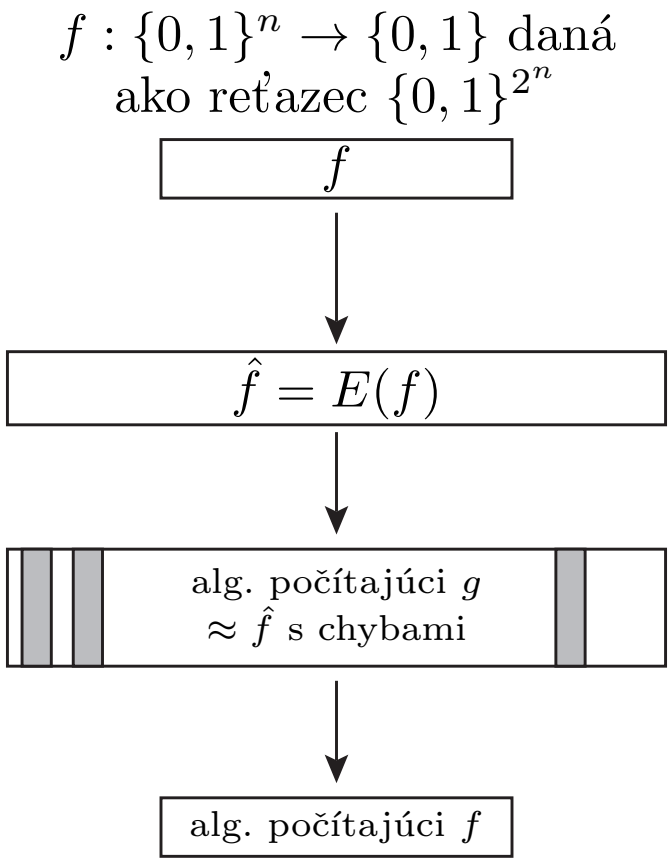


Figure 1.17. Transmitting 10 000 source bits over a binary symmetric channel with $f = 10\%$ using a $(7, 4)$ Hamming code. The probability of decoded bit error is about 7%.

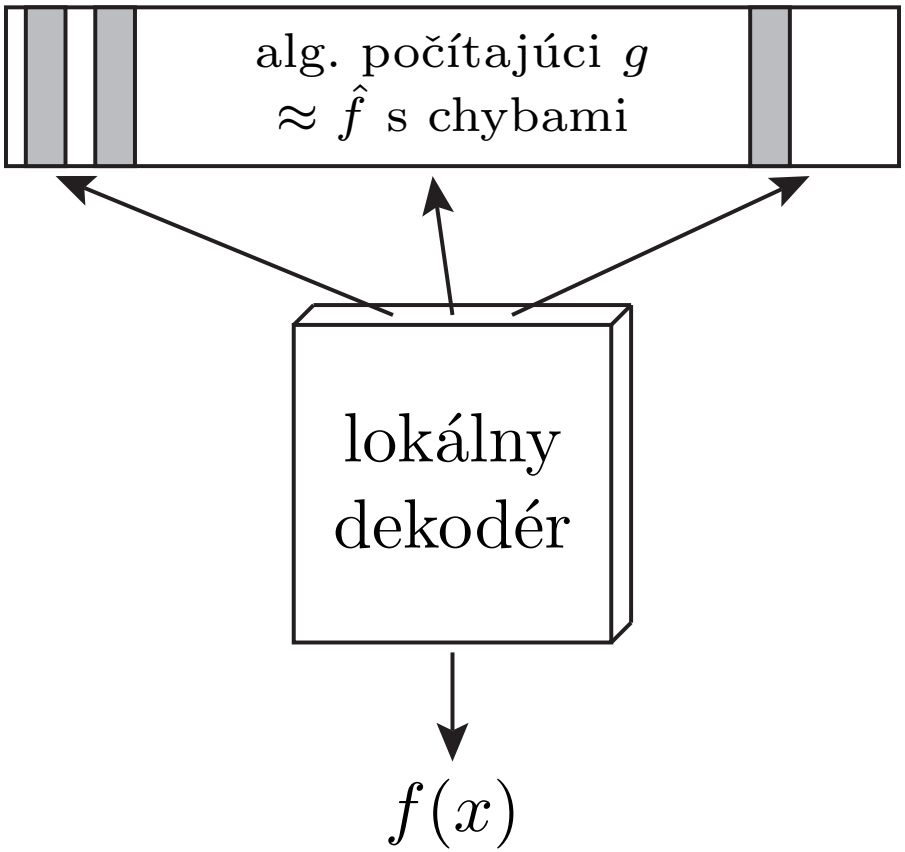
Využitie samoopravných kódov



Využitie samoopravných kódov



Využitie samoopravných kódov



Veľmi ťažké funkcie z ťažkých v najhoršom prípade

Veta

Ak $\exists f \in \mathsf{E},\ \mathsf{H}_{\mathrm{wrs}}(f)(n) \geq S(n) \Longrightarrow \exists g \in \mathsf{E}$ *a* $c > 0$ *také, že*

$$\mathsf{H}^{0.99}_{\mathrm{avg}}(g)(n) \geq S(n/c)/n^c \quad (\forall^{\infty} n).$$

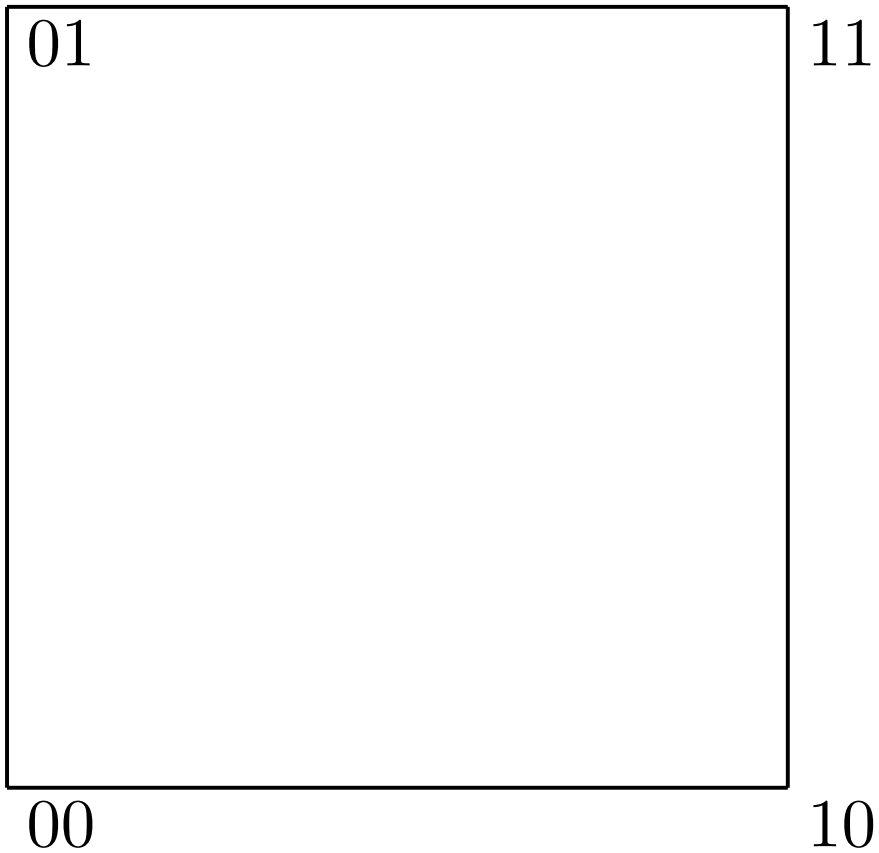
Veľmi ťažké funkcie z ťažkých v najhoršom prípade

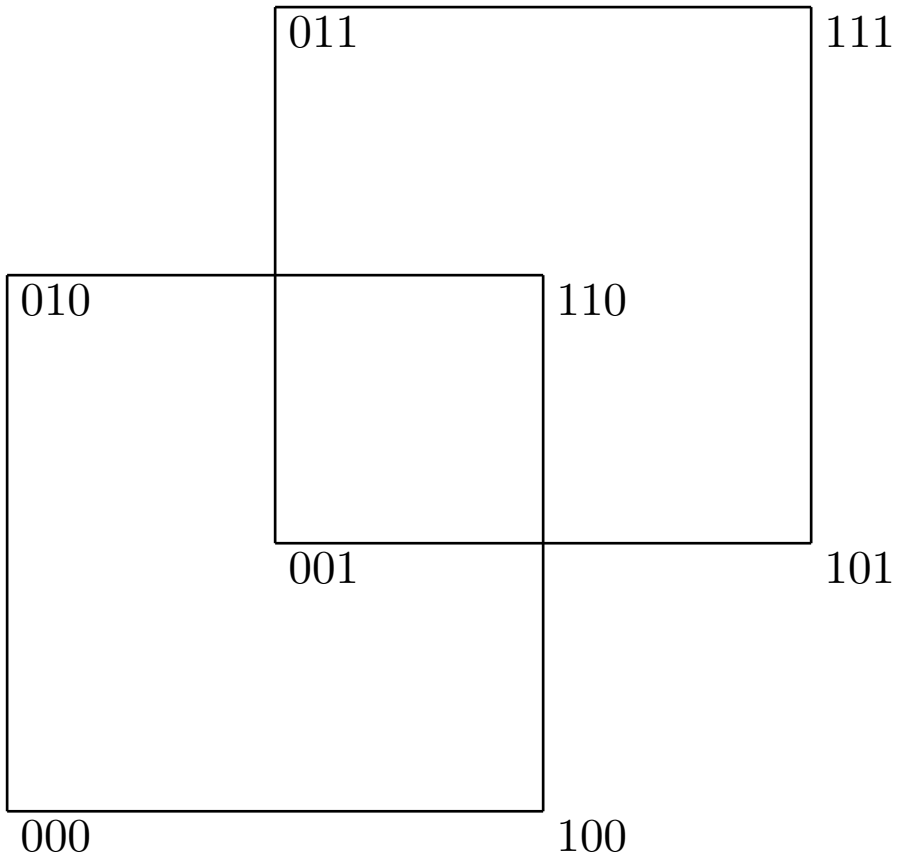
Dôkaz.

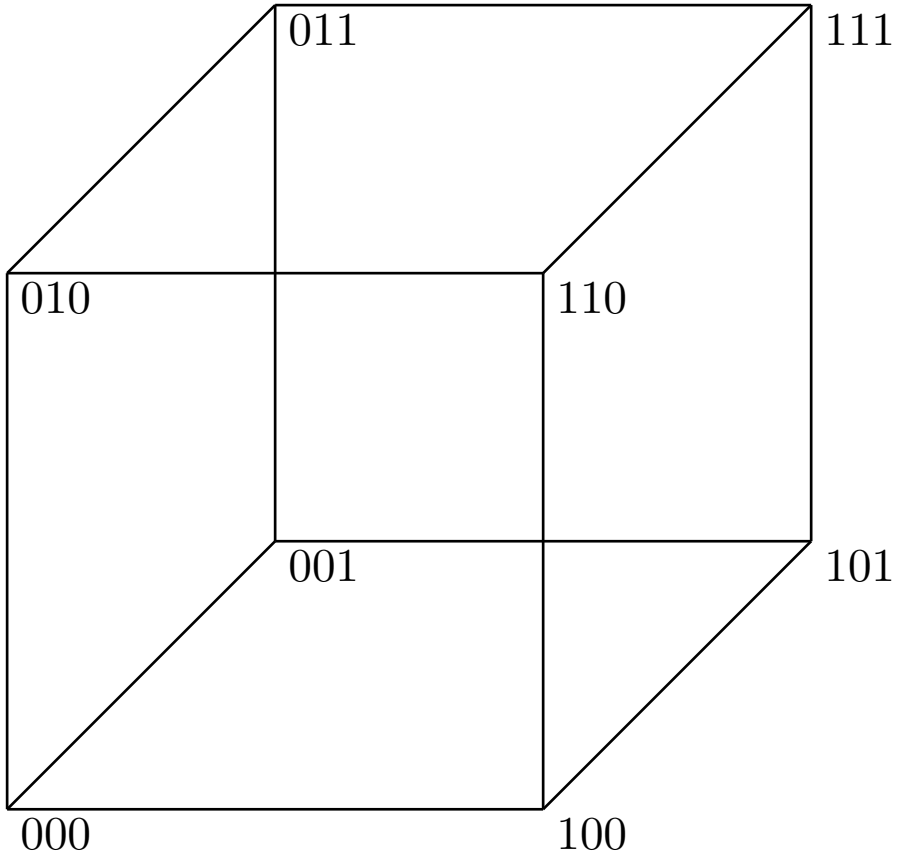
- uvažujme reťazec $F \in \{0,1\}^N$ $(N = 2^n)$ všetkých hodnôt $f(x)$ pre $x \in \{0,1\}^n$
- zakódujme ho SOK $E : \{0,1\}^N \to \{0,1\}^{N^c}$.
- reťazec $\hat{F} = E(F)$ zase interpretujeme ako funkciu $\hat{f} : \{0,1\}^{c \cdot n} \to \{0,1\}$
- použijeme efektívny SOK s lokálnym dekodérom; potrebujeme
  - lokálne dekódovanie
  - vedieť opraviť $1/100$ chýb
  - kódovanie v čase poly$N$
  - dekódovanie v čase poly$n = \text{polylog}N$
- keby $\exists$ obvod g veľkosti $s(n)$ počítajúci $\hat{f}$ na 99% vstupov
  - tak g+dekodér počíta f presne v čase poly$n \cdot s(n)$

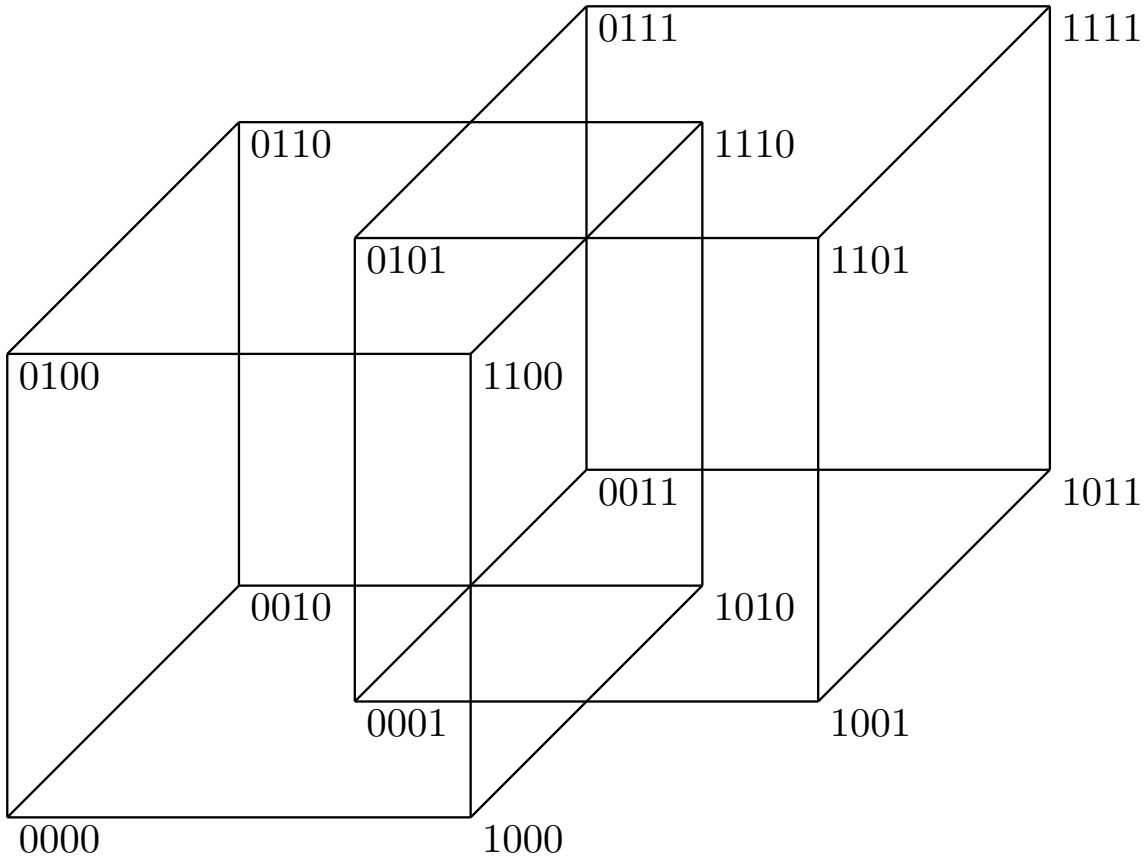
□

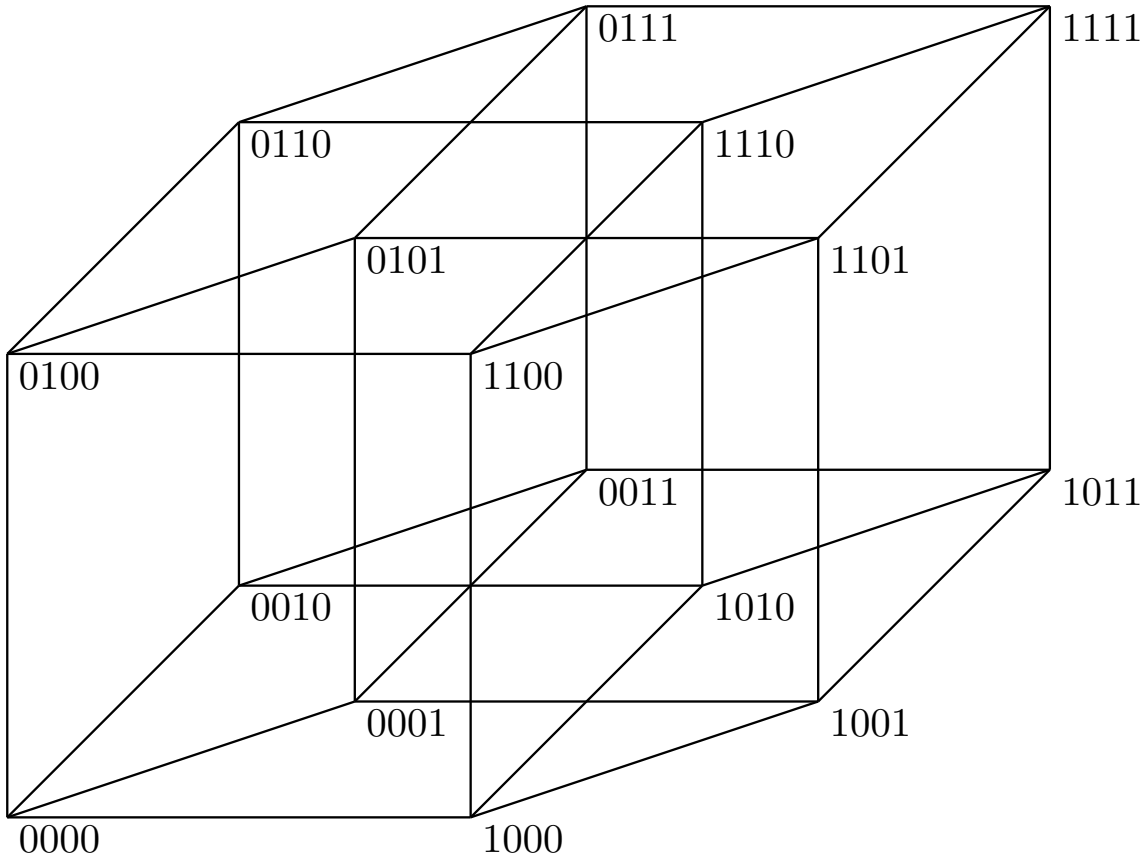
Samoopravné kódy

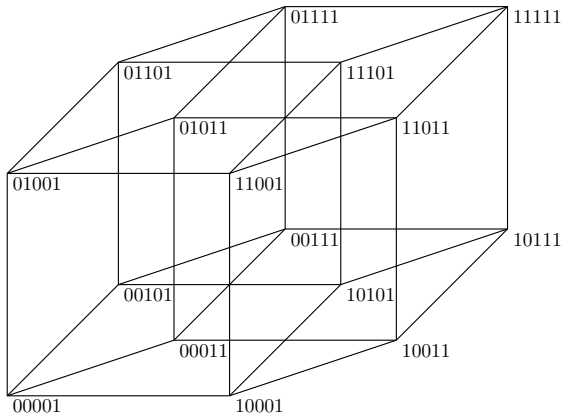

01
11
00
10

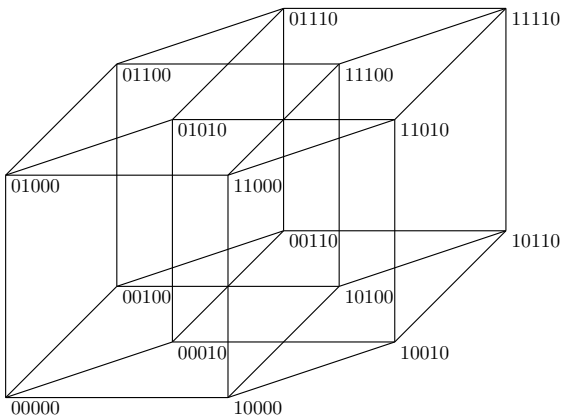

011
111
010
110
001
101
000
100

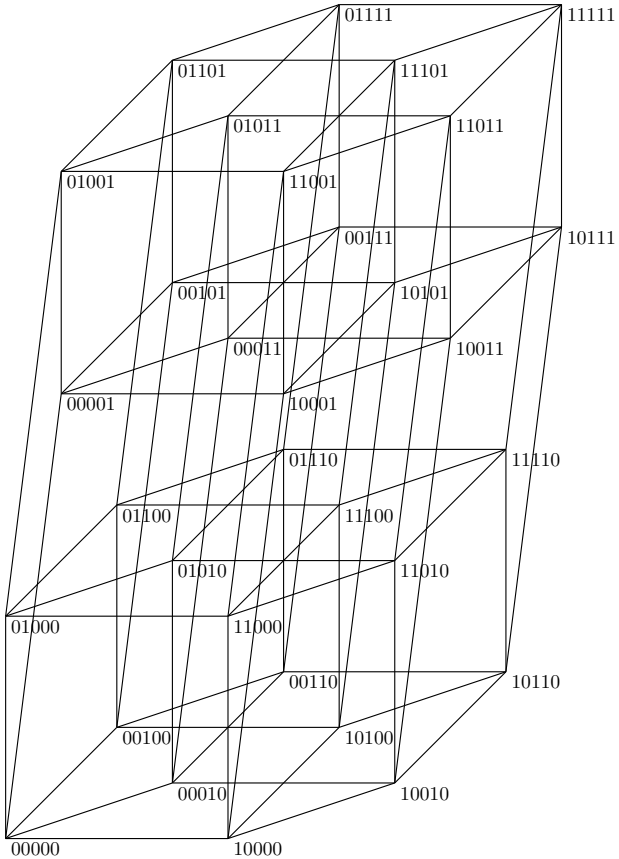

011
111
010
110
001
101
000
100

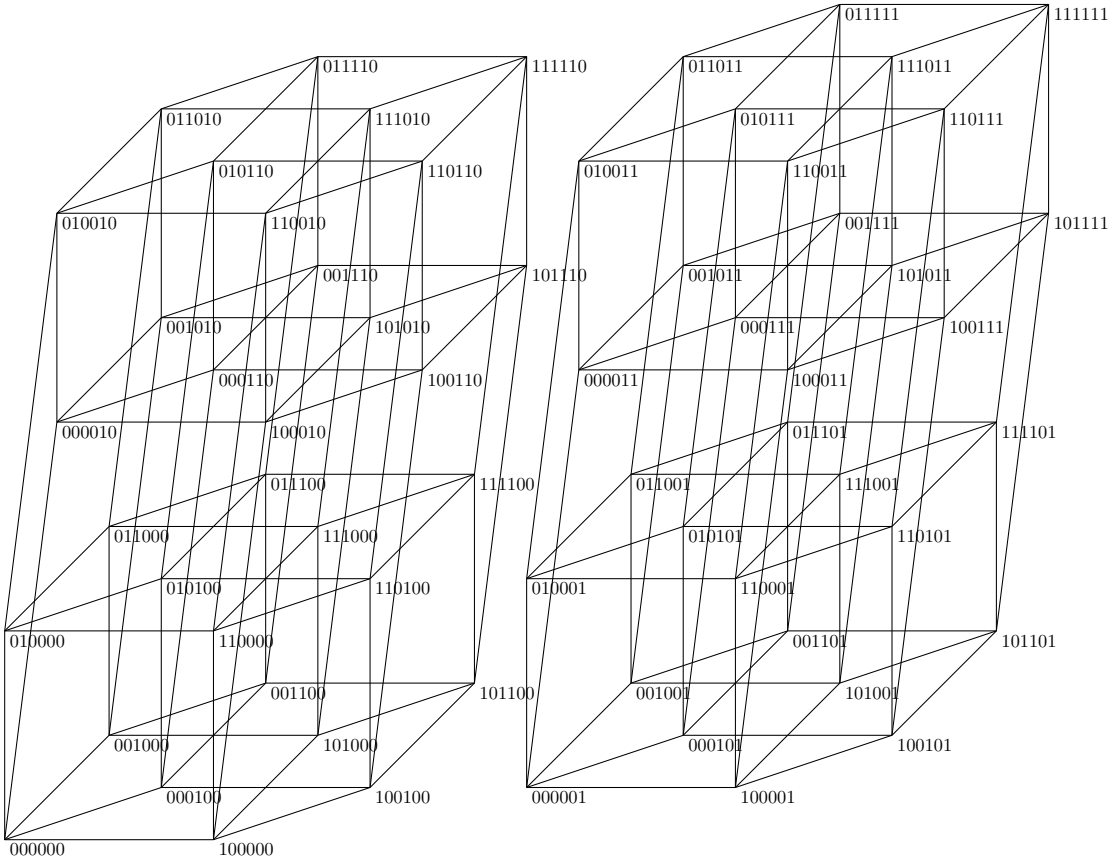

0111
1111
0110
1110
0101
1101
0100
1100
0011
1011
0010
1010
0001
1001
0000
1000

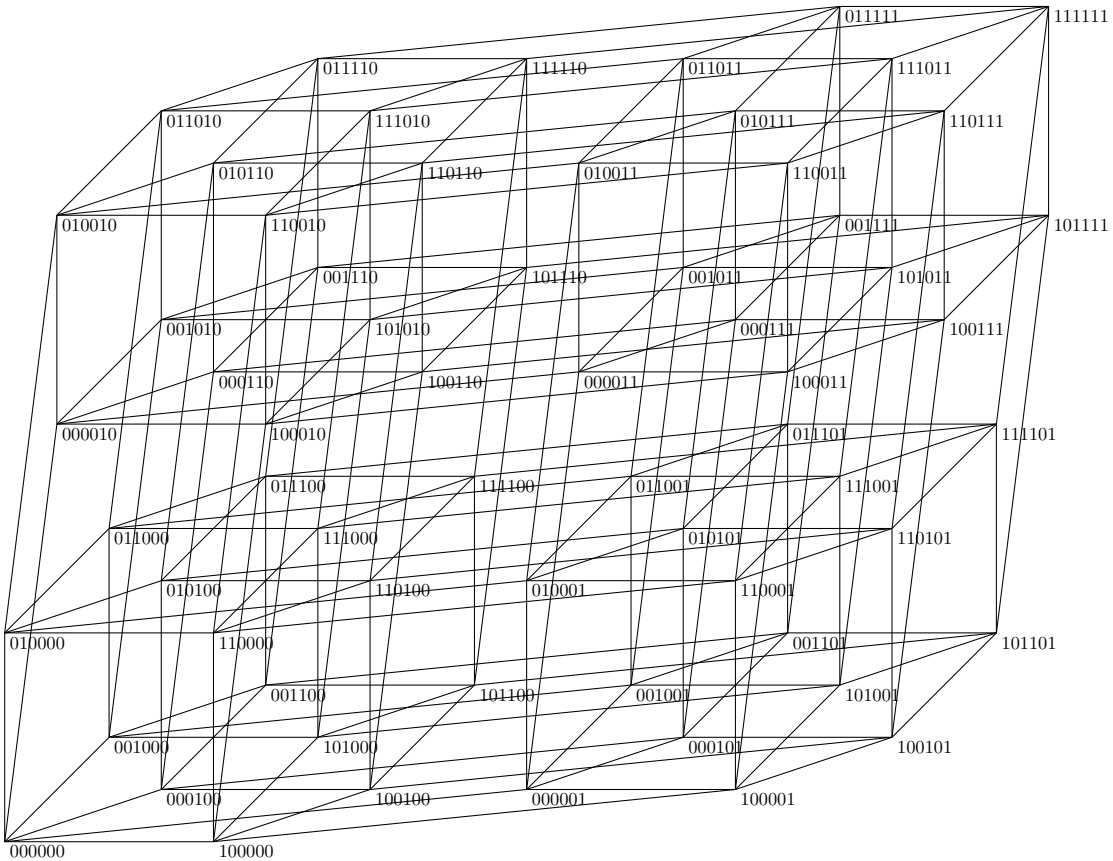

0111
1111
0110
1110
0101
1101
0100
1100
0011
1011
0010
1010
0001
1001
0000
1000

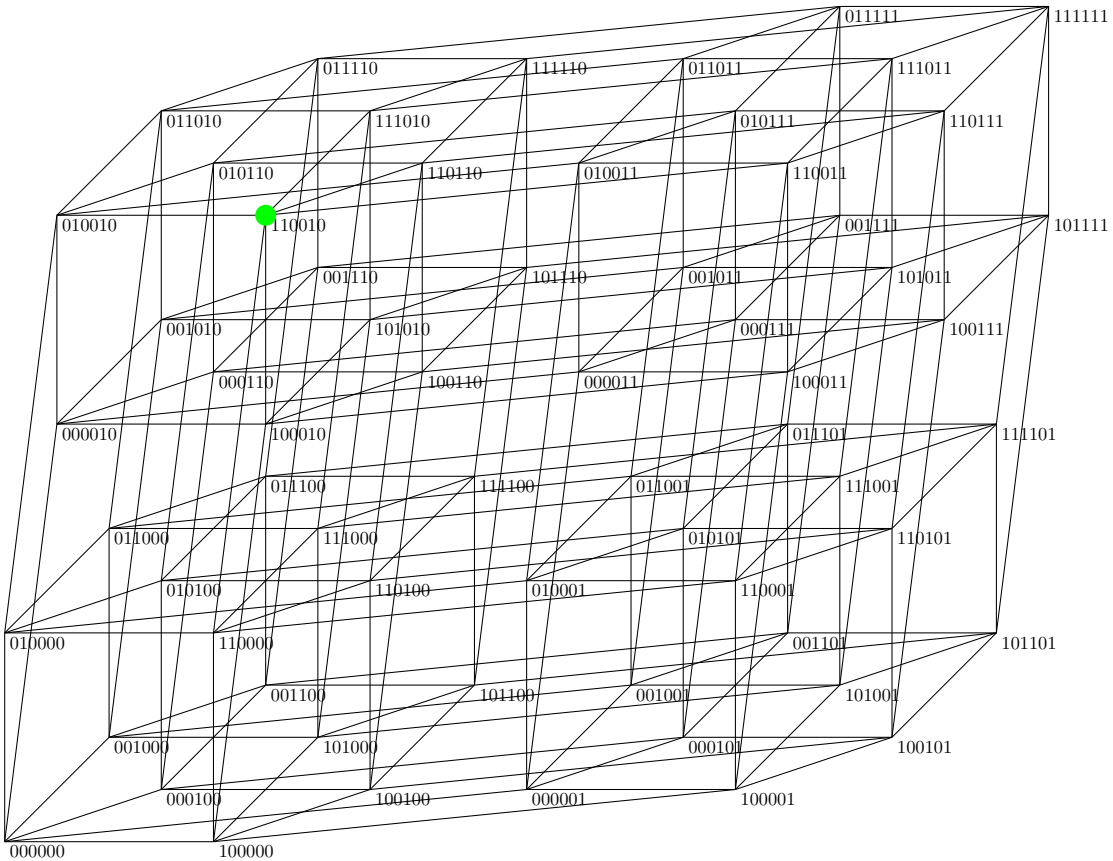

01111
11111
01101
11101
01011
11011
01001
11001
00111
10111
00101
10101
00011
10011
00001
10001

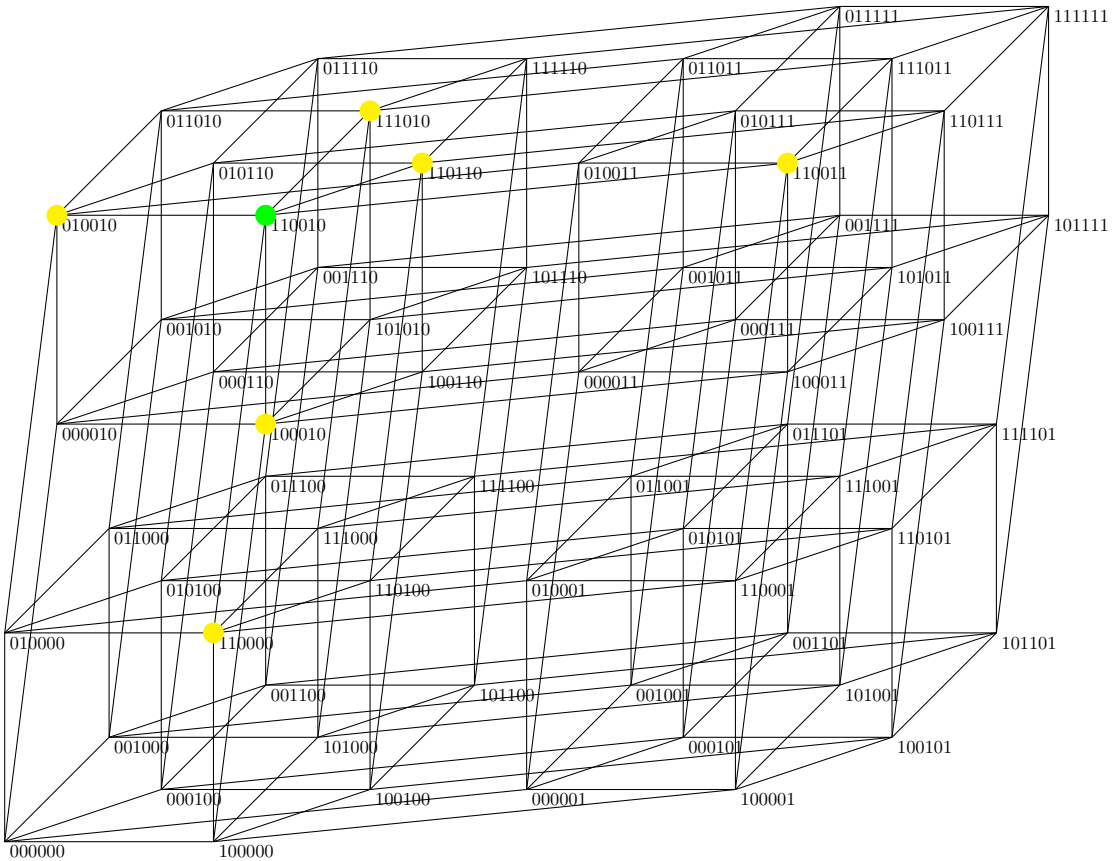

01110
11110
01100
11100
01010
11010
01000
11000
00110
10110
00100
10100
00010
10010
00000
10000

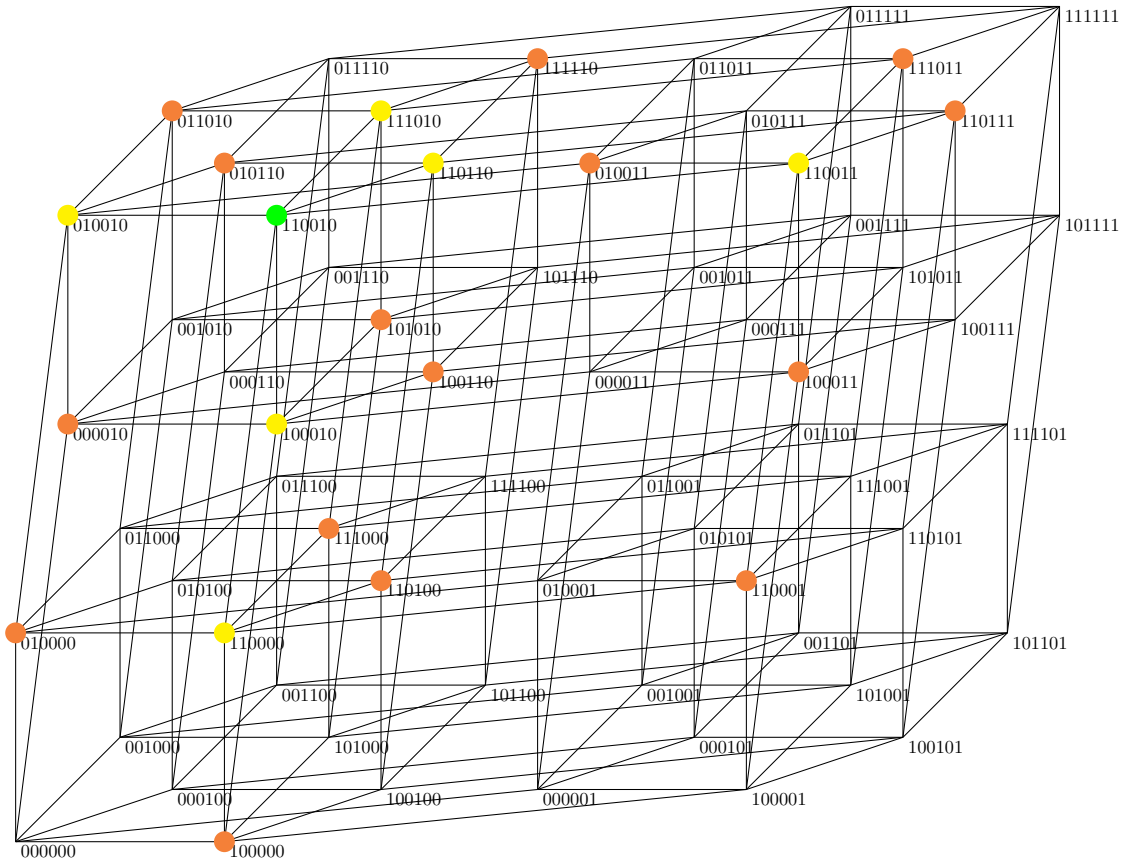

01111
11111
01101
11101
01011
11011
01001
11001
00111
10111
00101
10101
00011
10011
00001
10001
01110
11110
01100
11100
01010
11010
01000
11000
00110
10110
00100
10100
00010
10010
00000
10000

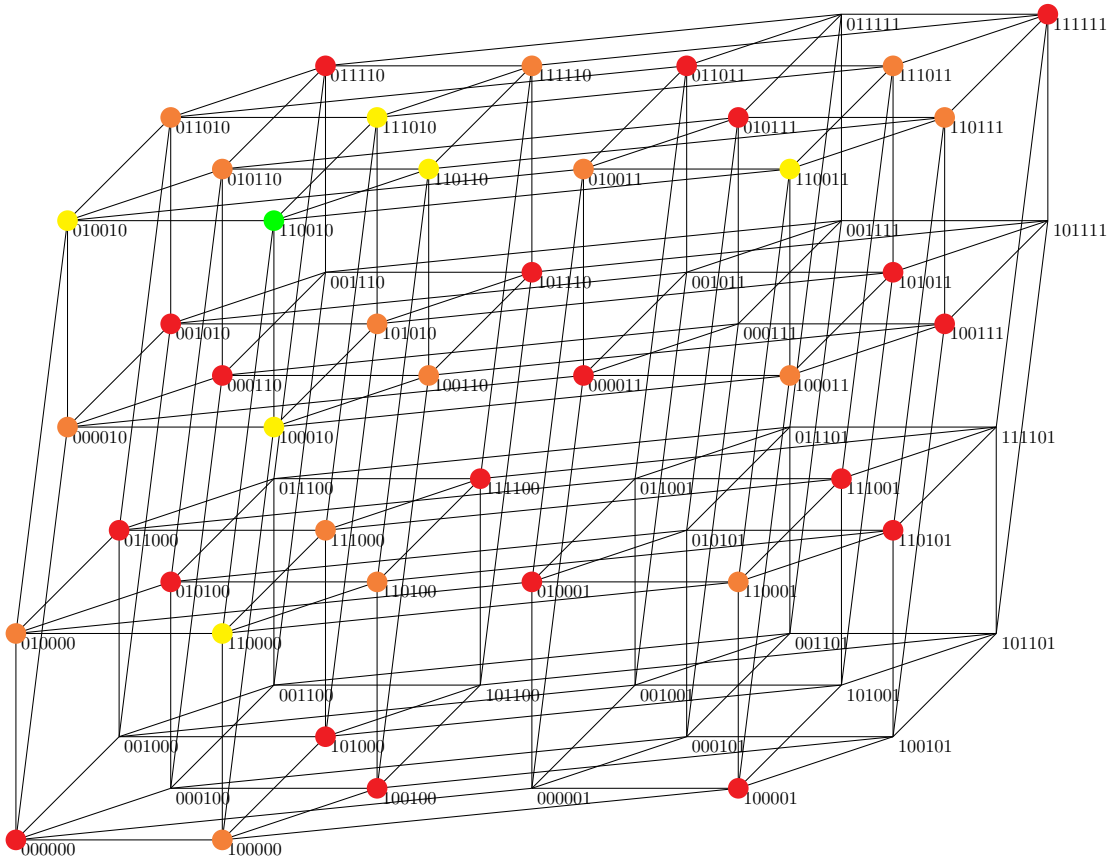

011111
111111
011110
111110
011011
111011
011010
111010
010111
110111
010110
110110
010011
110011
010010
110010
001111
101111
001110
101110
001011
101011
001010
101010
000111
100111
000110
100110
000011
100011
000010
100010
011101
111101
011100
111100
011001
111001
011000
111000
010101
110101
010100
110100
010001
110001
010000
110000
001101
101101
001100
101100
001001
101001
001000
101000
000101
100101
000100
100100
000001
100001
000000
100000

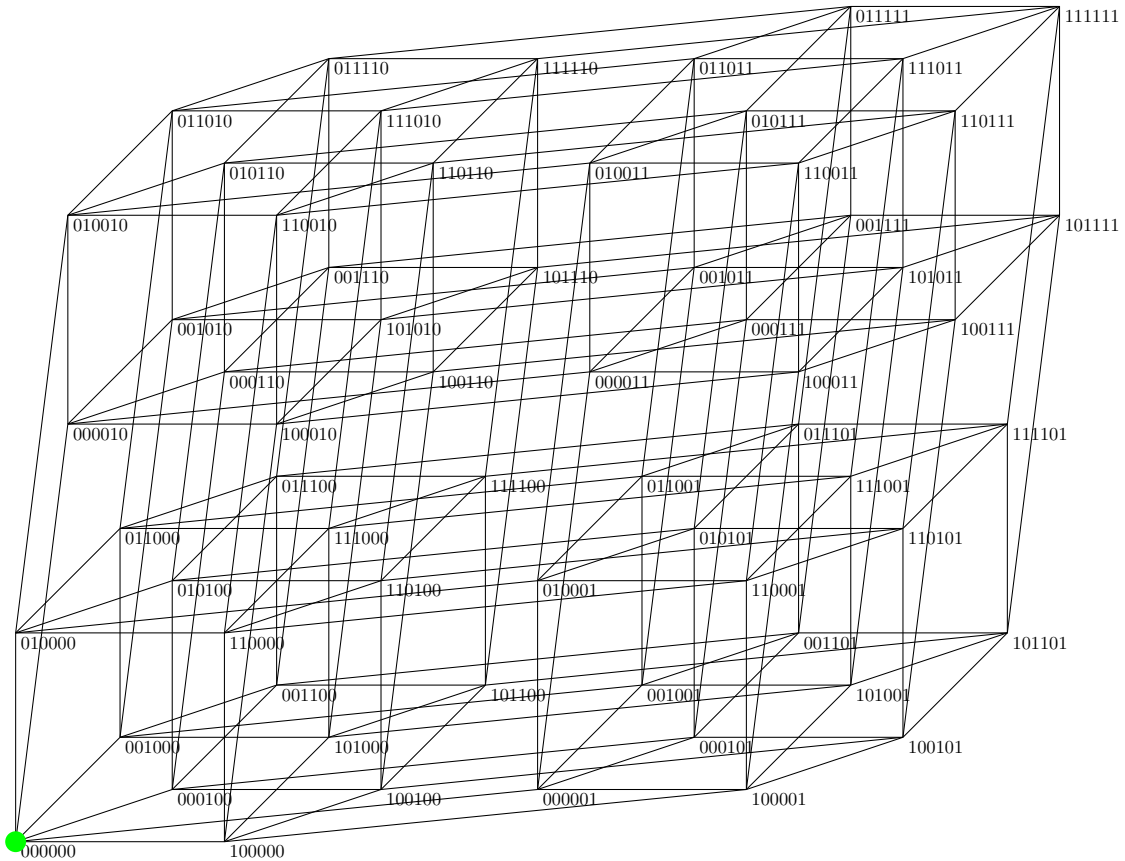

011111
111111
011110
111110
011011
111011
011010
111010
010111
110111
010110
110110
010011
110011
010010
110010
001111
101111
001110
101110
001011
101011
001010
101010
000111
100111
000110
100110
000011
100011
000010
100010
011101
111101
011100
111100
011001
111001
011000
111000
010101
110101
010100
110100
010001
110001
010000
110000
001101
101101
001100
101100
001001
101001
001000
101000
000101
100101
000100
100100
000001
100001
000000
100000

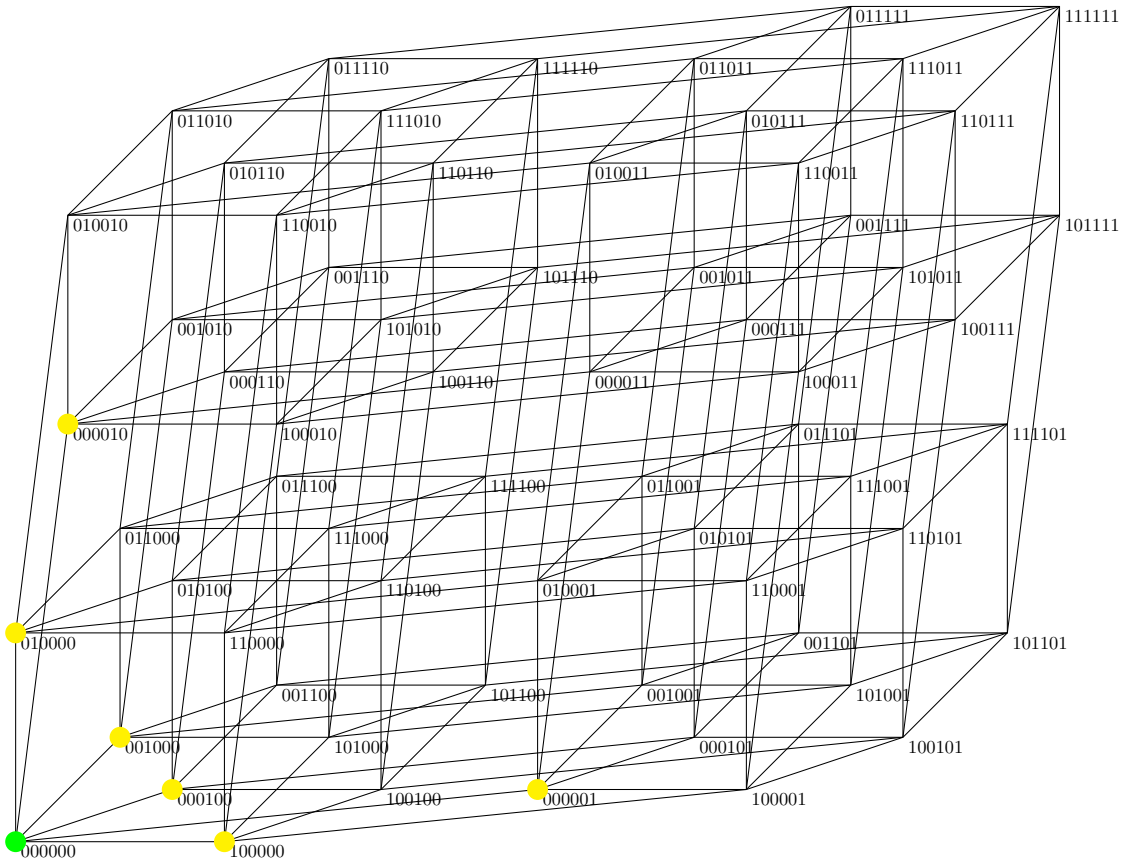

011111
111111
011110
111110
011011
111011
011010
111010
010111
110111
010110
110110
010011
110011
010010
110010
001111
101111
001110
101110
001011
101011
001010
101010
000111
100111
000110
100110
000011
100011
000010
100010
011101
111101
011100
111100
011001
111001
011000
111000
010101
110101
010100
110100
010001
110001
010000
110000
001101
101101
001100
101100
001001
101001
001000
101000
000101
100101
000100
100100
000001
100001
000000
100000

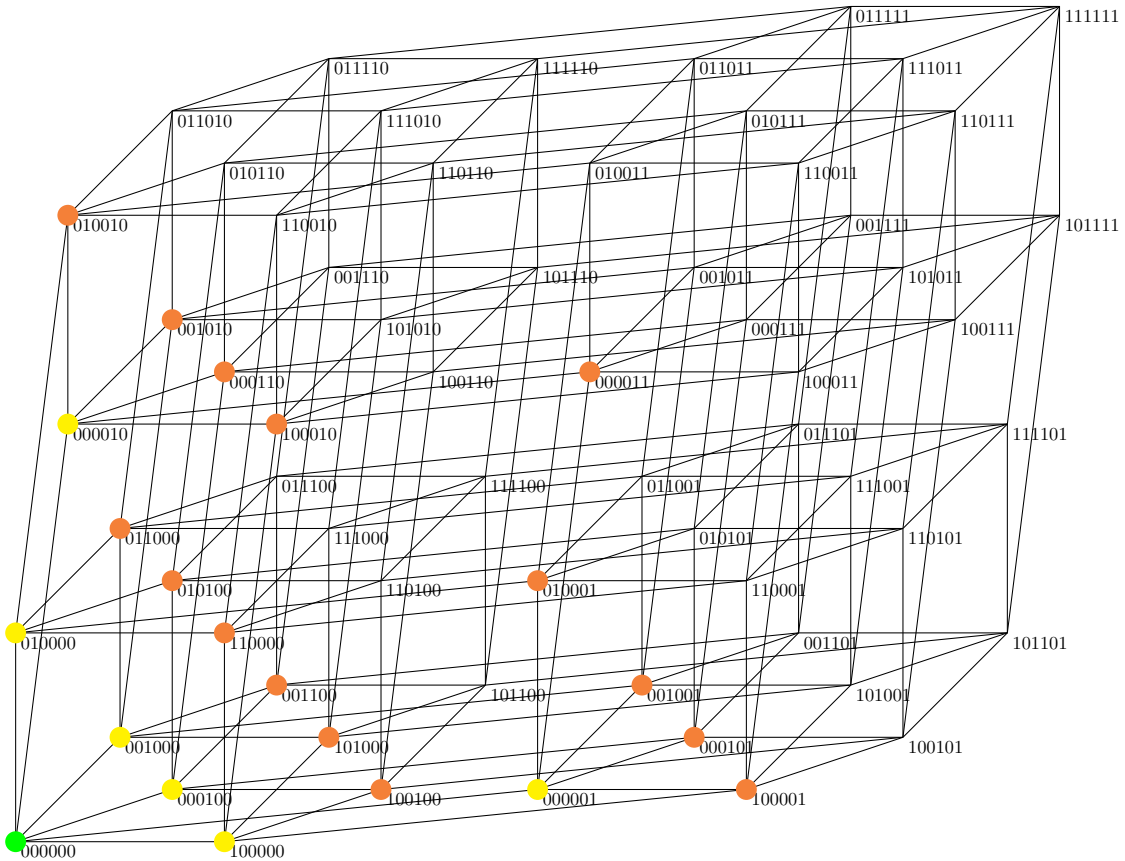

011111
111111
011110
111110
011011
111011
011010
111010
010111
110111
010110
110110
010011
110011
010010
110010
001111
101111
001110
101110
001011
101011
001010
101010
000111
100111
000110
100110
000011
100011
000010
100010
011101
111101
011100
111100
011001
111001
011000
111000
010101
110101
010100
110100
010001
110001
010000
110000
001101
101101
001100
101100
001001
101001
001000
101000
000101
100101
000100
100100
000001
100001
000000
100000

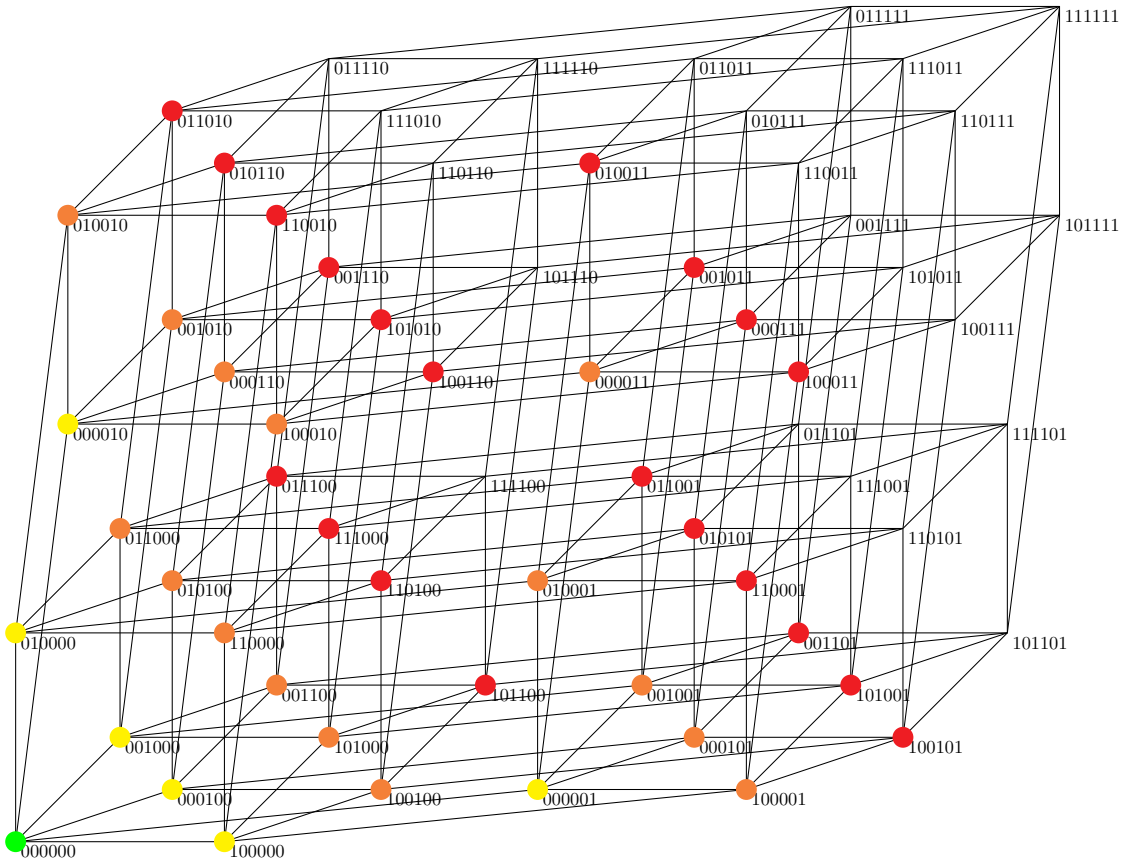

011111
111111
011110
111110
011011
111011
011010
111010
010111
110111
010110
110110
010011
110011
010010
110010
001111
101111
001110
101110
001011
101011
001010
101010
000111
100111
000110
100110
000011
100011
000010
100010
011101
111101
011100
111100
011001
111001
011000
111000
010101
110101
010100
110100
010001
110001
010000
110000
001101
101101
001100
101100
001001
101001
001000
101000
000101
100101
000100
100100
000001
100001
000000
100000

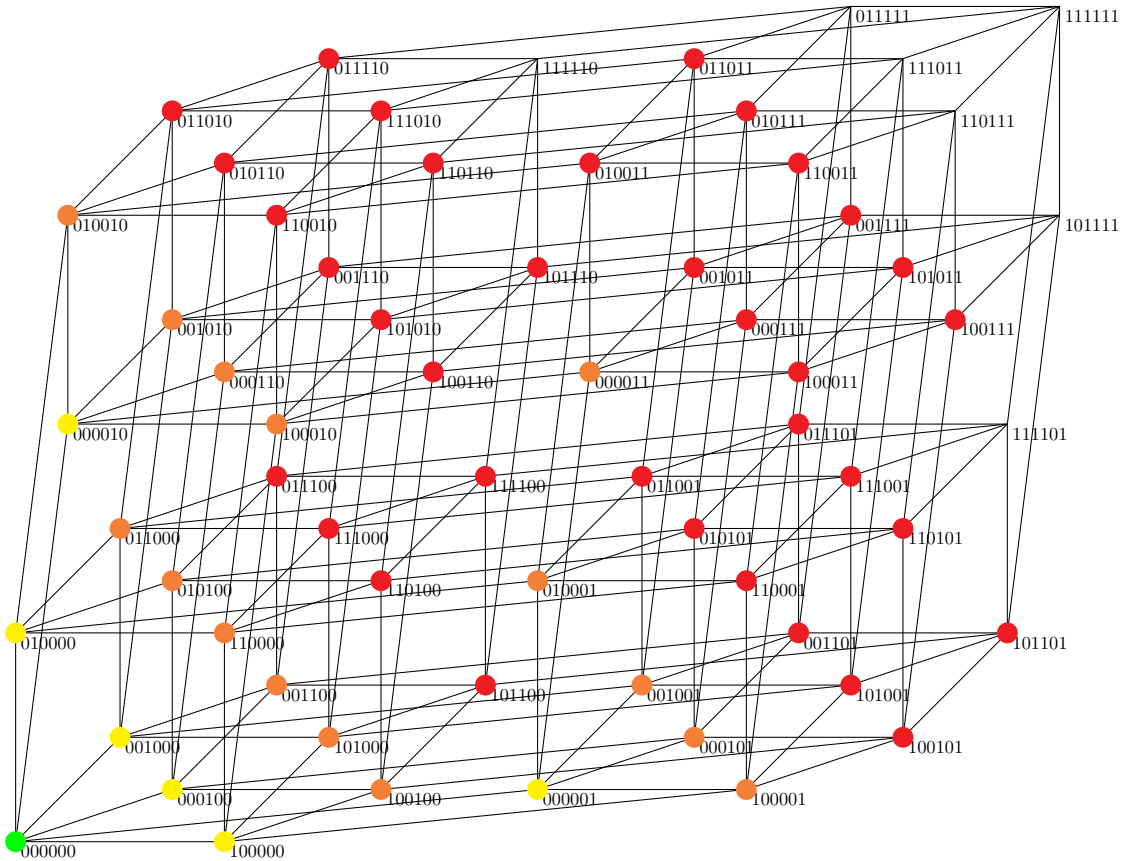

011111
111111
011110
111110
011011
111011
011010
111010
010111
110111
010110
110110
010011
110011
010010
110010
001111
101111
001110
101110
001011
101011
001010
101010
000111
100111
000110
100110
000011
100011
000010
100010
011101
111101
011100
111100
011001
111001
011000
111000
010101
110101
010100
110100
010001
110001
010000
110000
001101
101101
001100
101100
001001
101001
001000
101000
000101
100101
000100
100100
000001
100001
000000
100000


011111
111111
011110
111110
011011
111011
011010
111010
010111
110111
010110
110110
010011
110011
010010
110010
001111
101111
001110
101110
001011
101011
001010
101010
000111
100111
000110
100110
000011
100011
000010
100010
011101
111101
011100
111100
011001
111001
011000
111000
010101
110101
010100
110100
010001
110001
010000
110000
001101
101101
001100
101100
001001
101001
001000
101000
000101
100101
000100
100100
000001
100001
000000
100000


011111
111111
011110
111110
011011
111011
011010
111010
010111
110111
010110
110110
010011
110011
010010
110010
001111
101111
001110
101110
001011
101011
001010
101010
000111
100111
000110
100110
000011
100011
000010
100010
011101
111101
011100
111100
011001
111001
011000
111000
010101
110101
010100
110100
010001
110001
010000
110000
001101
101101
001100
101100
001001
101001
001000
101000
000101
100101
000100
100100
000001
100001
000000
100000


011111
111111
011110
111110
011011
111011
011010
111010
010111
110111
010110
110110
010011
110011
010010
110010
001111
101111
001110
101110
001011
101011
001010
101010
000111
100111
000110
100110
000011
100011
000010
100010
011101
111101
011100
111100
011001
111001
011000
111000
010101
110101
010100
110100
010001
110001
010000
110000
001101
101101
001100
101100
001001
101001
001000
101000
000101
100101
000100
100100
000001
100001
000000
100000


011111
111111
011110
111110
011011
111011
011010
111010
010111
110111
010110
110110
010011
110011
010010
110010
001111
101111
001110
101110
001011
101011
001010
101010
000111
100111
000110
100110
000011
100011
000010
100010
011101
111101
011100
111100
011001
111001
011000
111000
010101
110101
010100
110100
010001
110001
010000
110000
001101
101101
001100
101100
001001
101001
001000
101000
000101
100101
000100
100100
000001
100001
000000
100000


011111
111111
011110
111110
011011
111011
011010
111010
010111
110111
010110
110110
010011
110011
010010
110010
001111
101111
001110
101110
001011
101011
001010
101010
000111
100111
000110
100110
000011
100011
000010
100010
011101
111101
011100
111100
011001
111001
011000
111000
010101
110101
010100
110100
010001
110001
010000
110000
001101
101101
001100
101100
001001
101001
001000
101000
000101
100101
000100
100100
000001
100001
000000
100000

Samoopravné kódy

Definícia

- *zlomková Hammingova vzdialenosť:* $\Delta(x,y) = \frac{1}{m}|\{i \mid x_i \neq y_i\}|$
- $E : \Sigma^n \to \Sigma^m$ *je samoopravný kód (SOK) so vzdialenosťou* $d \in [0,1]$ *nad abecedou* Σ*,*
  - $\forall x \neq y : \Delta(E(x), E(y)) \geq d$

Walsh-Hadamardov kód

Walsh-Hadamard

Definícia (Walsh-Hadamardov kód)

Walsh-Hadamardov kód $\mathrm{WH} : \{0,1\}^n \to \{0,1\}^{2^n}$ *je SOK definovaný* $\mathrm{WH}(x)_i = \langle x, i \rangle$.

- vzdialenosť: $1/2$
- lokálny dekodér opravujúci $< 1/4$ chýb v čase $O(n)$
- vzdialenosť je SUPER, ale vstup sa až príliš nafúkne

Walsh-Hadamard

$101 \mapsto 01011010$

pozícia	hodnota
000	0
001	1
010	0
011	1
100	1
101	0
110	1
111	0

Walsh-Hadamard

$$\min_{x,y} \Delta(\mathrm{WH}(x),\mathrm{WH}(y)) = \min_{x,y} \Delta(\mathrm{WH}(x-y),\mathrm{WH}(0)) = \min_{z} \Delta(\mathrm{WH}(z),0)$$

$$f(y) \oplus f(y \oplus e^j) = (\langle x,y\rangle) \oplus (\langle x,(y+e^j)\rangle) = \langle x,e^j\rangle = x_j$$

- $\Pr_y[f(y) \neq \langle x,y\rangle] \leq \rho$
- $f(y)$ je zle s pp. ρ,
- $f(y+e^j)$ je zle s pp. ρ,
- obe sú správne s pp. $1-2\rho \geq 1/2$

Walsh-Hadamard

$$\min_{x,y} \Delta(\mathrm{WH}(x),\mathrm{WH}(y)) = \min_{x,y} \Delta(\mathrm{WH}(x-y),\mathrm{WH}(0)) = \min_{z} \Delta(\mathrm{WH}(z),0)$$

$$f(y) \oplus f(y \oplus e^j) = (\langle x,y\rangle) \oplus (\langle x,(y+e^j)\rangle) = \langle x,e^j\rangle = x_j$$

- $\Pr_y[f(y) \neq \langle x,y\rangle] \leq \rho$
- $f(y)$ je zle s pp. ρ,
- $f(y+e^j)$ je zle s pp. ρ,
- obe sú správne s pp. $1-2\rho \geq 1/2$

Walsh-Hadamard

$$\min_{x,y} \Delta(\mathrm{WH}(x),\mathrm{WH}(y)) = \min_{x,y} \Delta(\mathrm{WH}(x-y),\mathrm{WH}(0)) = \min_{z} \Delta(\mathrm{WH}(z),0)$$

$$f(y) \oplus f(y \oplus e^j) = (\langle x,y\rangle) \oplus (\langle x,(y+e^j)\rangle) = \langle x,e^j\rangle = x_j$$

- $\Pr_y[f(y) \neq \langle x,y\rangle] \leq \rho$
- $f(y)$ je zle s pp. ρ,
- $f(y+e^j)$ je zle s pp. ρ,
- obe sú správne s pp. $1-2\rho \geq 1/2$

Walsh-Hadamard

$$\min_{x,y} \Delta(\mathrm{WH}(x),\mathrm{WH}(y)) = \min_{x,y} \Delta(\mathrm{WH}(x-y),\mathrm{WH}(0)) = \min_{z} \Delta(\mathrm{WH}(z),0)$$

$$f(y) \oplus f(y \oplus e^j) = (\langle x,y\rangle) \oplus (\langle x,(y+e^j)\rangle) = \langle x,e^j\rangle = x_j$$

- $\Pr_y[f(y) \neq \langle x,y\rangle] \leq \rho$
- $f(y)$ je zle s pp. ρ,
- $f(y+e^j)$ je zle s pp. ρ,
- obe sú správne s pp. $1-2\rho \geq 1/2$

Walsh-Hadamard

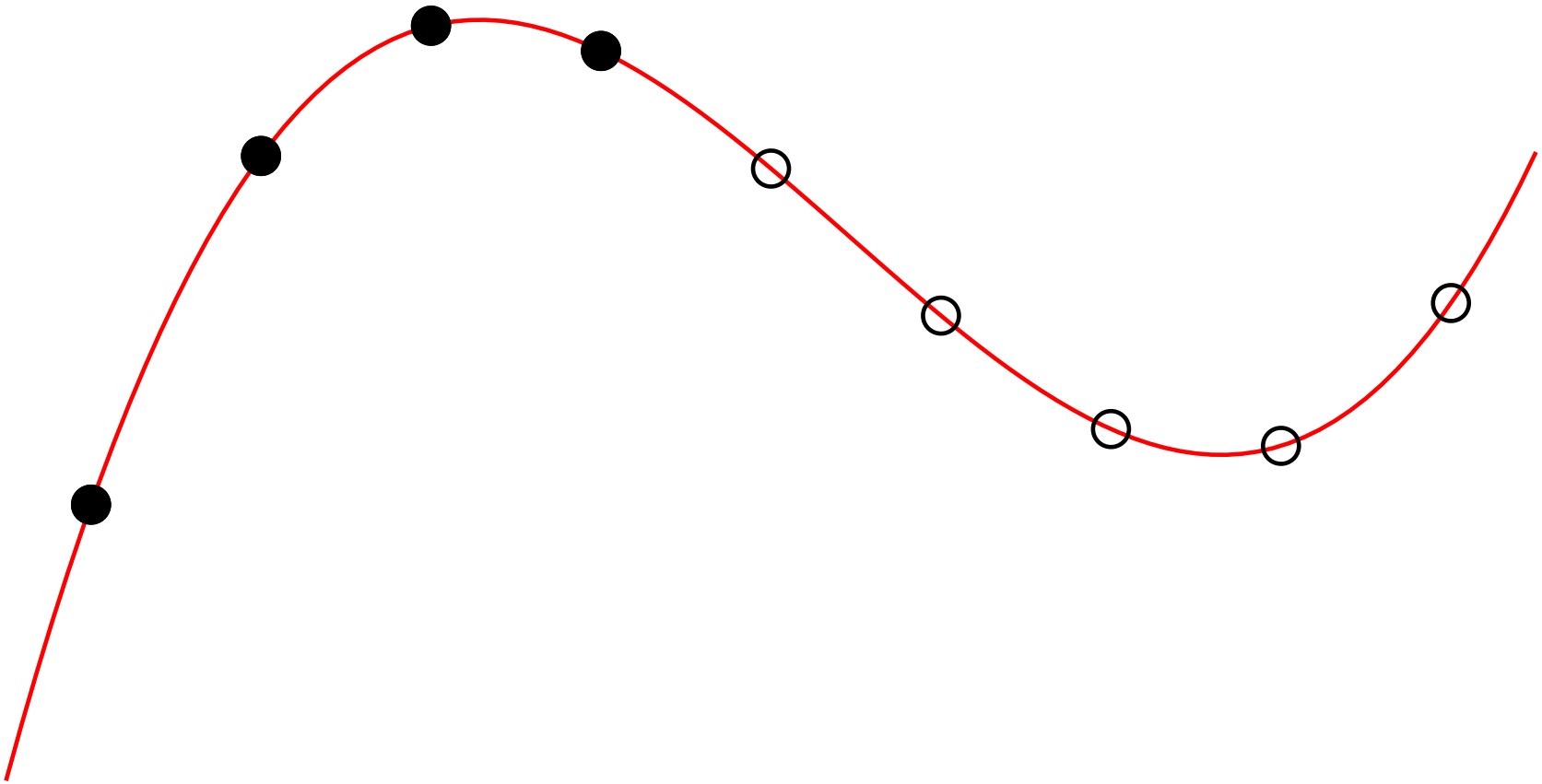
$$\min_{x,y} \Delta(\mathrm{WH}(x),\mathrm{WH}(y)) = \min_{x,y} \Delta(\mathrm{WH}(x-y),\mathrm{WH}(0)) = \min_{z} \Delta(\mathrm{WH}(z),0)$$

$$f(y) \oplus f(y \oplus e^j) = (\langle x,y\rangle) \oplus (\langle x,(y+e^j)\rangle) = \langle x,e^j\rangle = x_j$$

- $\Pr_y[f(y) \neq \langle x,y\rangle] \leq \rho$
- $f(y)$ je zle s pp. ρ,
- $f(y+e^j)$ je zle s pp. ρ,
- obe sú správne s pp. $1-2\rho \geq 1/2$

Reed-Solomonov kód

Reed-Solomon



Definícia (Reed-Solomonov kód)

Nech $\mathbb{F} = \mathbb{F}_q$ *je pole,* $d \leq n \leq q$ *a nech* $a_0, \ldots, a_{n-1} \in \mathbb{F}$.
Správu $c_0 \ldots c_{d-1}$ *interpretujme ako koeficienty polynómomu*

$$p(x) = \sum_i c_i x^i.$$

Reed-Solomonov kód $\mathrm{RS} : \mathbb{F}^d \to \mathbb{F}^n$ *je zobrazenie*

$$c_0 \ldots c_{d-1} \mapsto p(a_0) \ldots p(a_{n-1}).$$

- vzdialenosť: $1 - d/n$
  - $p(x)$ je polynóm stupňa $d-1$, čiže má $\leq d$ koreňov

Veta

Daný je zoznam dvojíc $(a_1, b_1), \ldots, (a_n, b_n)$ *z* $\mathbb{F}^2$, *pričom existuje polynóm* $p : \mathbb{F} \to \mathbb{F}$ *stupňa* d, *pre ktorý* $p(a_i) = b_i$ *pre* $t > n/2 + d/2$ *dvojíc. Existuje algoritmus, ktorý dokáže* p *zrekonštruovať v polynomiálnom čase.*

■ **Dôkaz.**

- $p(a_i) = b_i$ pre $k = n - t = \lfloor n/2 - d/2 \rfloor$ bodov nie je splnená
- majme polynóm e: $p(a_i) \neq b_i \implies e(a_i) = 0$

$$e(a_i)p(a_i) = e(a_i)b_i \qquad (\forall i)!$$

- hľadáme poly p stupňa d + nenulový poly e stupňa $\leq k$
- súčin $e \cdot p = q$ je poly stupňa $k + d = \lfloor n/2 + d/2 \rfloor$

$$q(a_i) = e(a_i)b_i.$$

- potom $p = q/e$

■ **Dôkaz.**

- $p(a_i) = b_i$ pre $k = n - t = \lfloor n/2 - d/2 \rfloor$ bodov nie je splnená
- majme polynóm e: $p(a_i) \neq b_i \implies e(a_i) = 0$

$$e(a_i)p(a_i) = e(a_i)b_i \qquad (\forall i)!$$

- hľadáme poly p stupňa d + nenulový poly e stupňa $\leq k$
- súčin $e \cdot p = q$ je poly stupňa $k + d = \lfloor n/2 + d/2 \rfloor$

$$q(a_i) = e(a_i)b_i.$$

- potom $p = q/e$

Dôkaz.

- $p(a_i) = b_i$ pre $k = n - t = \lfloor n/2 - d/2 \rfloor$ bodov nie je splnená
- majme polynóm e: $p(a_i) \neq b_i \implies e(a_i) = 0$

$$e(a_i)p(a_i) = e(a_i)b_i \qquad (\forall i)!$$

- hľadáme poly p stupňa d + nenulový poly e stupňa $\leq k$
- súčin $e \cdot p = q$ je poly stupňa $k + d = \lfloor n/2 + d/2 \rfloor$

$$q(a_i) = e(a_i)b_i.$$

- potom $p = q/e$

Dôkaz.

- $p(a_i) = b_i$ pre $k = n - t = \lfloor n/2 - d/2 \rfloor$ bodov nie je splnená
- majme polynóm e: $p(a_i) \neq b_i \implies e(a_i) = 0$

$$e(a_i)p(a_i) = e(a_i)b_i \qquad (\forall i)!$$

- hľadáme poly p stupňa d + nenulový poly e stupňa $\leq k$
- súčin $e \cdot p = q$ je poly stupňa $k + d = \lfloor n/2 + d/2 \rfloor$

$$q(a_i) = e(a_i)b_i.$$

- potom $p = q/e$

■ **Dôkaz.**

- $p(a_i) = b_i$ pre $k = n - t = \lfloor n/2 - d/2 \rfloor$ bodov nie je splnená
- majme polynóm e: $p(a_i) \neq b_i \implies e(a_i) = 0$

$$e(a_i)p(a_i) = e(a_i)b_i \qquad (\forall i)!$$

- hľadáme poly p stupňa d + nenulový poly e stupňa $\leq k$
- súčin $e \cdot p = q$ je poly stupňa $k + d = \lfloor n/2 + d/2 \rfloor$

$$q(a_i) = e(a_i)b_i.$$

- potom $p = q/e$

Dôkaz.

- $p(a_i) = b_i$ pre $k = n - t = \lfloor n/2 - d/2 \rfloor$ bodov nie je splnená
- majme polynóm e: $p(a_i) \neq b_i \implies e(a_i) = 0$

$$e(a_i)p(a_i) = e(a_i)b_i \qquad (\forall i)!$$

- hľadáme poly p stupňa d + nenulový poly e stupňa $\leq k$
- súčin $e \cdot p = q$ je poly stupňa $k + d = \lfloor n/2 + d/2 \rfloor$

$$q(a_i) = e(a_i)b_i.$$

- potom $p = q/e$

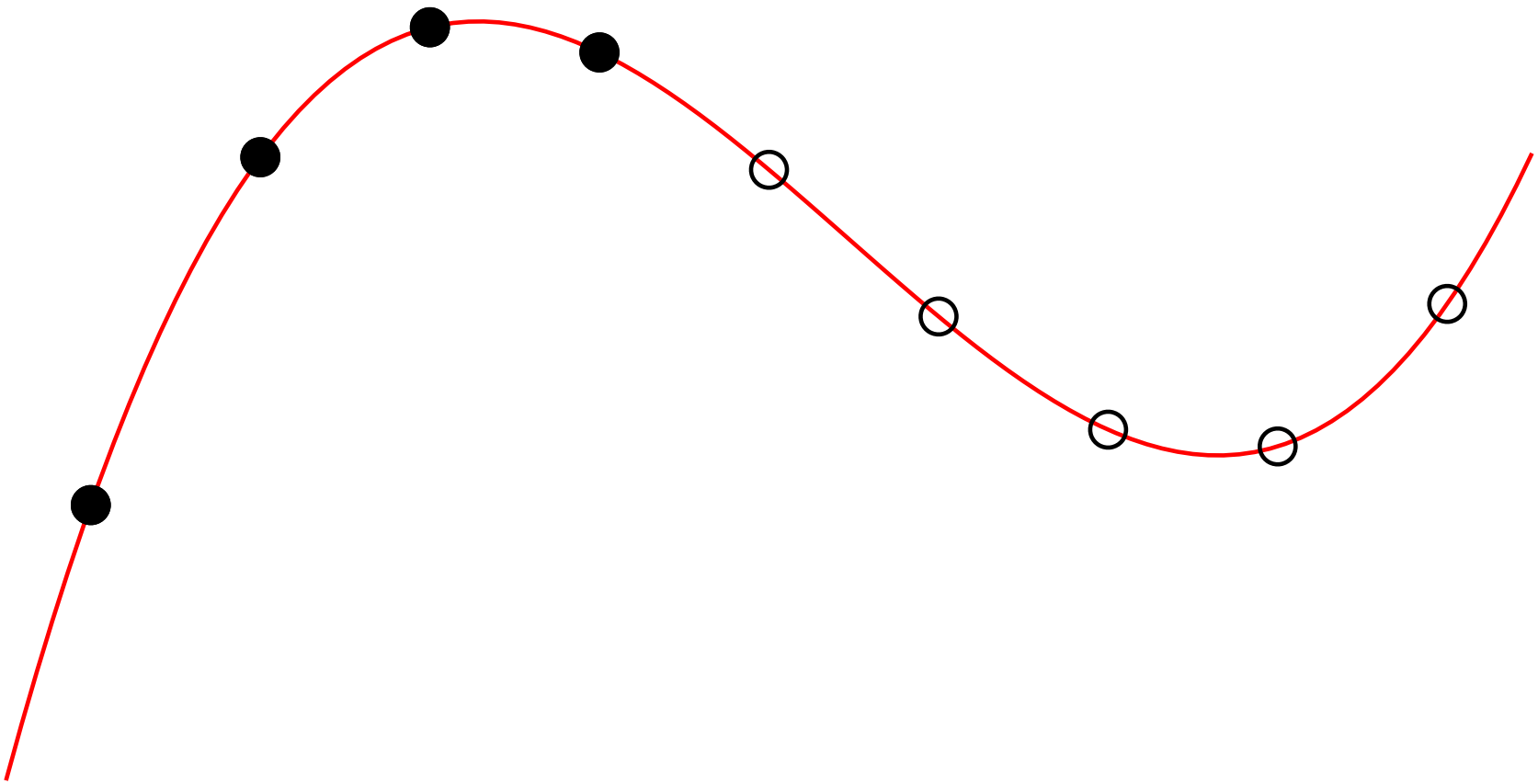
- nech $e_k = 1$, neznáme koef. $e_0, \ldots, e_{k-1}$ a $q_0, \ldots, q_{k+d}$

$$q_0 + q_1 a_i + q_2 a_i^2 + \cdots + q_{k+d} a_i^{k+d} = e_0 b_i + e_1 a_i b_i + \cdots + e_{k-1} a_i^{k-1} b_i + a_i^k b_i,$$

- n lineárnych rovníc o $\leq n$ neznámych

□

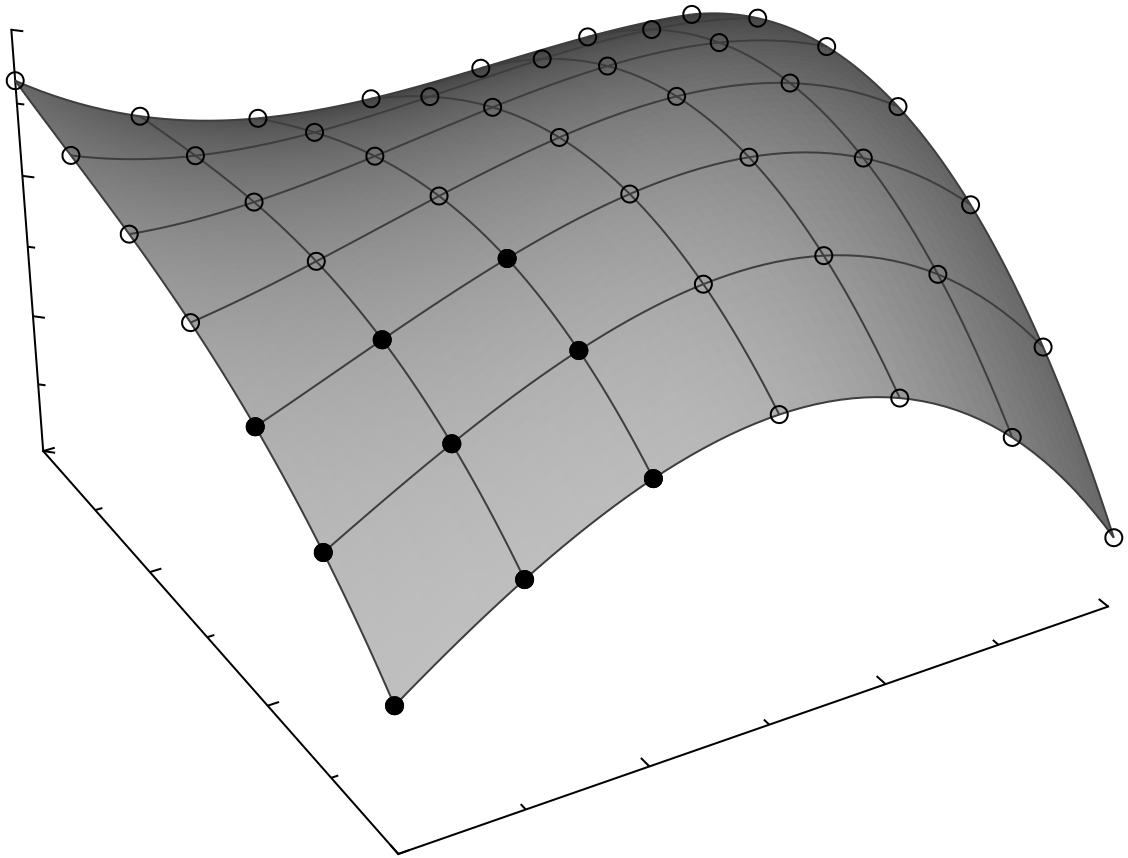
Reed-Solomon



- $d \leq n \leq q$, vzdialenosť $1 - d/n$
- veľká abeceda, veľký stupeň poly, nemá lokálny dekodér

Reed-Mullerov kód

Reed-Muller



Reed-Muller

- Reed-Mullerov kód s parametrami $\mathbb{F}, \ell, d$, $d < |\mathbb{F}|$, je zovšeobecnením RS kódu
- namiesto polynómu $A(x)$ jednej premennej uvažuje polynómy ℓ premenných

Definícia (Reed-Mullerov kód)

RM : $\mathbb{F}^{\binom{m+d}{d}} \to \mathbb{F}^{q^m}$, *ktorá správu c interpretuje ako koeficienty polynómu celkového stupňa d s m premennými nad* $\mathbb{F}_q$

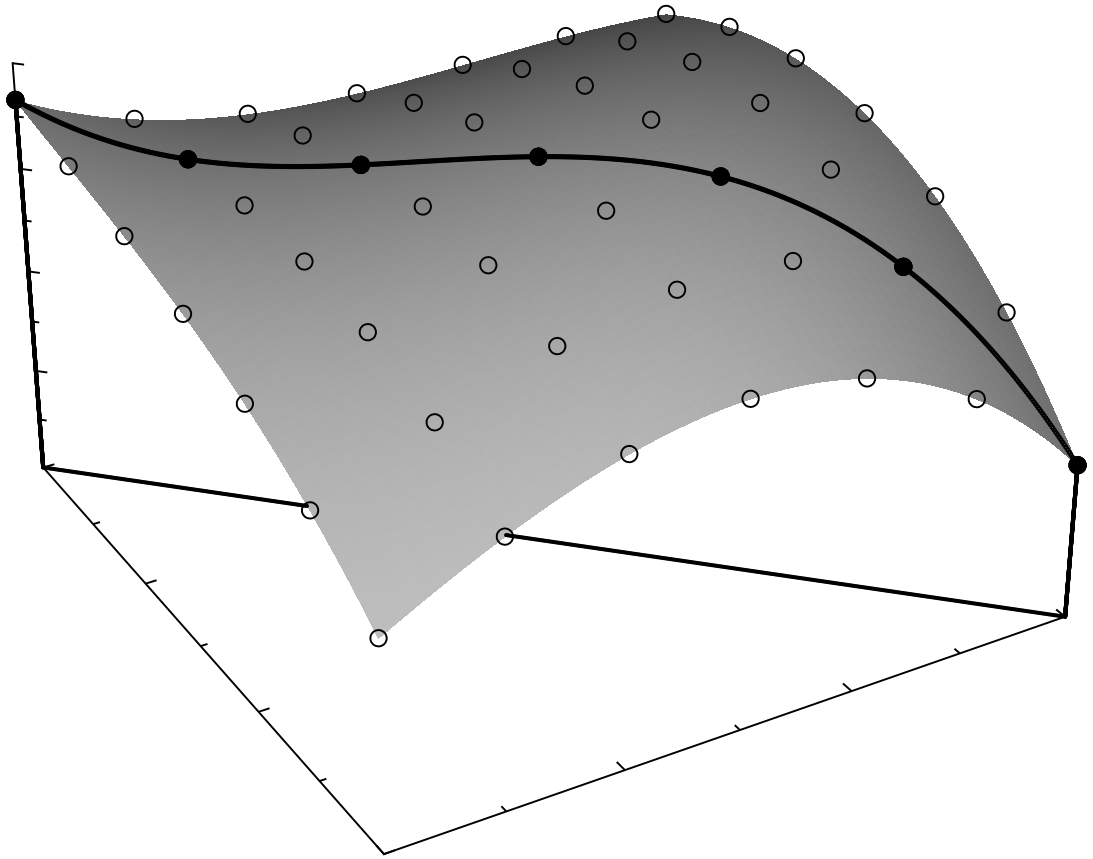
$$p(x_1, \ldots, x_m) = \sum_{i_1 + \cdots + i_m \leq d} c_{i_1, \ldots, i_m} x_1^{i_1} x_2^{i_2} \cdots x_m^{i_m}$$

a na výstup dáme postupnosť $\{p(x_1, \ldots, x_m)\}$ *pre všetky* $x_1, \ldots, x_m \in \mathbb{F}$.

Reed-Muller

- pre $m = 1$ dostávame RS kód
- pre $d = 1$ a $\mathbb{F} = \{0, 1\}$ dostávame variant WH kódu, ktorý zobrazí $x \mapsto z$, kde $z_{y,a} = \langle x, y \rangle \oplus a$
- vzdialenosť: $1 - d/|\mathbb{F}|$ (Schwartz-Zippelova lema)
- lokálny dekodér opravujúci $(1 - d/q)/6$ chýb v čase $\text{poly}(q, m, d)$ s pp. $\geq 2/3$

Reed-Muller



Reed-Muller

- predp. f je blízko poly p stupňa d ($\Pr_x[f(x) \neq p(x)] < \rho$)
- $\ell_{a,b}(t) = a + tb$
- nech $f|_\ell : \mathbb{F} \to \mathbb{F}$ zúženie na f na ℓ:

$$f|_\ell(t) = f(\ell(t))$$

- $f|_\ell$ – poly 1 premennej stupňa $\leq d$ (RS)

Reed-Muller

- predp. f je blízko poly p stupňa d ($\Pr_x[f(x) \neq p(x)] < \rho$)
- $\ell_{a,b}(t) = a + tb$
- nech $f|_\ell : \mathbb{F} \to \mathbb{F}$ zúženie na f na ℓ:

$$f|_\ell(t) = f(\ell(t))$$

- $f|_\ell$ – poly 1 premennej stupňa $\leq d$ (RS)

Reed-Muller

- predp. f je blízko poly p stupňa d ($\Pr_x[f(x) \neq p(x)] < \rho$)
- $\ell_{a,b}(t) = a + tb$
- nech $f|_\ell : \mathbb{F} \to \mathbb{F}$ zúženie na f na ℓ:

$$f|_\ell(t) = f(\ell(t))$$

- $f|_\ell$ – poly 1 premennej stupňa $\leq d$ (RS)

Reed-Muller

- predp. f je blízko poly p stupňa d ($\Pr_x[f(x) \neq p(x)] < \rho$)
- $\ell_{a,b}(t) = a + tb$
- nech $f|_\ell : \mathbb{F} \to \mathbb{F}$ zúženie na f na ℓ:

$$f|_\ell(t) = f(\ell(t))$$

- $f|_\ell$ – poly 1 premennej stupňa $\leq d$ (RS)

Reed-Muller

- nech $L = \ell_{x,z}$ je náhodná priamka idúca cez x
- pozrieme všetky body $f|_L$ a dekódujeme RS $r : \mathbb{F} \to \mathbb{F}$
- odpovieme $r(0)$.
- body $\ell_{x,z}$ pre náhodné z sú distribuované rovnomerne po $\mathbb{F}^m$
- očak. #chýb na L, je $\leq \rho \cdot q$
- $\Pr[\#\text{chýb na } L \geq 3 \times \rho q] \leq 1/3$ (Markov)
- $3 \times \rho q < (1 - d/q)q/2 = q/2 - d/2 \implies$ RS vie r správne dekódovať: $r = p|_L$ a $r(0) = p(x)$

Reed-Muller

- nech $L = \ell_{x,z}$ je náhodná priamka idúca cez x
- pozrieme všetky body $f|_L$ a dekódujeme RS $r : \mathbb{F} \to \mathbb{F}$
- odpovieme $r(0)$.
- body $\ell_{x,z}$ pre náhodné z sú distribuované rovnomerne po $\mathbb{F}^m$
- očak. #chýb na L, je $\leq \rho \cdot q$
- $\Pr[\#\text{chýb na } L \geq 3 \times \rho q] \leq 1/3$ (Markov)
- $3 \times \rho q < (1 - d/q)q/2 = q/2 - d/2 \implies$ RS vie r správne dekódovať: $r = p|_L$ a $r(0) = p(x)$

Reed-Muller

- nech $L = \ell_{x,z}$ je náhodná priamka idúca cez x
- pozrieme všetky body $f|_L$ a dekódujeme RS $r : \mathbb{F} \to \mathbb{F}$
- odpovieme $r(0)$.
- body $\ell_{x,z}$ pre náhodné z sú distribuované rovnomerne po $\mathbb{F}^m$
- očak. #chýb na L, je $\leq \rho \cdot q$
- $\Pr[\#\text{chýb na } L \geq 3 \times \rho q] \leq 1/3$ (Markov)
- $3 \times \rho q < (1 - d/q)q/2 = q/2 - d/2 \implies$ RS vie r správne dekódovať: $r = p|_L$ a $r(0) = p(x)$

Reed-Muller

- nech $L = \ell_{x,z}$ je náhodná priamka idúca cez x
- pozrieme všetky body $f|_L$ a dekódujeme RS $r : \mathbb{F} \to \mathbb{F}$
- odpovieme $r(0)$.
- body $\ell_{x,z}$ pre náhodné z sú distribuované rovnomerne po $\mathbb{F}^m$
- očak. #chýb na L, je $\leq \rho \cdot q$
- $\Pr[\#\text{chýb na } L \geq 3 \times \rho q] \leq 1/3$ (Markov)
- $3 \times \rho q < (1 - d/q)q/2 = q/2 - d/2 \implies$ RS vie r správne dekódovať: $r = p|_L$ a $r(0) = p(x)$

Reed-Muller

- nech $L = \ell_{x,z}$ je náhodná priamka idúca cez x
- pozrieme všetky body $f|_L$ a dekódujeme RS $r : \mathbb{F} \to \mathbb{F}$
- odpovieme $r(0)$.
- body $\ell_{x,z}$ pre náhodné z sú distribuované rovnomerne po $\mathbb{F}^m$
- očak. #chýb na L, je $\leq \rho \cdot q$
- $\Pr[\#\text{chýb na } L \geq 3 \times \rho q] \leq 1/3$ (Markov)
- $3 \times \rho q < (1 - d/q)q/2 = q/2 - d/2 \Longrightarrow$ RS vie r správne dekódovať: $r = p|_L$ a $r(0) = p(x)$

Reed-Muller

- nech $L = \ell_{x,z}$ je náhodná priamka idúca cez x
- pozrieme všetky body $f|_L$ a dekódujeme RS $r : \mathbb{F} \to \mathbb{F}$
- odpovieme $r(0)$.
- body $\ell_{x,z}$ pre náhodné z sú distribuované rovnomerne po $\mathbb{F}^m$
- očak. #chýb na L, je $\leq \rho \cdot q$
- $\Pr[\#\text{chýb na } L \geq 3 \times \rho q] \leq 1/3$ (Markov)
- $3 \times \rho q < (1 - d/q)q/2 = q/2 - d/2 \implies$ RS vie r správne dekódovať: $r = p|_L$ a $r(0) = p(x)$

Reed-Muller

- nech $L = \ell_{x,z}$ je náhodná priamka idúca cez x
- pozrieme všetky body $f|_L$ a dekódujeme RS $r : \mathbb{F} \to \mathbb{F}$
- odpovieme $r(0)$.
- body $\ell_{x,z}$ pre náhodné z sú distribuované rovnomerne po $\mathbb{F}^m$
- očak. #chýb na L, je $\leq \rho \cdot q$
- $\Pr[\#\text{chýb na } L \geq 3 \times \rho q] \leq 1/3$ (Markov)
- $3 \times \rho q < (1 - d/q)q/2 = q/2 - d/2 \implies$ RS vie r správne dekódovať: $r = p|_L$ a $r(0) = p(x)$

Samoopravné kódy

	WH	RS	RM
dĺžka správy	n	d	$\binom{d+m}{m} \geq (d/m)^m \geq N$
dĺžka kódu	2^n	n	$q^m = N^5$
veľkosť abecedy	2	$q \geq n$	$q = \text{polylog}(N)$
vzdialenosť	$1/2$	$1 - d/n$	$1 - d/q \approx 1 - \varepsilon$
lok. opravuje	$1/4$	—	$1/6 - d/6q \approx 1/6 - \varepsilon$

Abeceda

- problém: abeceda je $\mathbb{F}$ – nie binárna
- v praxi: vezmime $\mathbb{F} = \mathbb{F}_{256}$, t.j. 1 byte
  - pre $n = 230$, $m = 256$ dostávame RS kód opravujúci 13 chýb (5% bytov / 0.6% bitov)
- všeobecne: 1 prvok $\mathbb{F} \longrightarrow \log|\mathbb{F}|$ bitov
  - RS : $\{0,1\}^{n \log|\mathbb{F}|} \to \{0,1\}^{m \log|\mathbb{F}|}$
  - problém: malá vzdialenosť: $< 1/\log|\mathbb{F}|$

Abeceda

- problém: abeceda je $\mathbb{F}$ – nie binárna
- v praxi: vezmime $\mathbb{F} = \mathbb{F}_{256}$, t.j. 1 byte
  - pre $n = 230$, $m = 256$ dostávame RS kód opravujúci 13 chýb (5% bytov / 0.6% bitov)
- všeobecne: 1 prvok $\mathbb{F} \longrightarrow \log|\mathbb{F}|$ bitov
  - RS : $\{0,1\}^{n \log|\mathbb{F}|} \to \{0,1\}^{m \log|\mathbb{F}|}$
  - problém: malá vzdialenosť: $< 1/\log|\mathbb{F}|$

Abeceda

- problém: abeceda je $\mathbb{F}$ – nie binárna
- v praxi: vezmime $\mathbb{F} = \mathbb{F}_{256}$, t.j. 1 byte
  - pre $n = 230$, $m = 256$ dostávame RS kód opravujúci 13 chýb (5% bytov / 0.6% bitov)
- všeobecne: 1 prvok $\mathbb{F} \longrightarrow \log|\mathbb{F}|$ bitov
  - RS : $\{0,1\}^{n \log|\mathbb{F}|} \to \{0,1\}^{m \log|\mathbb{F}|}$
  - problém: malá vzdialenosť: $< 1/\log|\mathbb{F}|$

Zložené kódy

- použime WH kód s $n = \log \mathbb{F}$, t.j. $\mathrm{WH} : \{0,1\}^{\log \mathbb{F}} \to \{0,1\}^{\mathbb{F}}$:

$$\mathbb{F}^n \mathbb{F}^m \sim \{0,1\}^{m \log \mathbb{F}} \xrightarrow{\mathrm{WH}} \{0,1\}^{m\mathbb{F}}$$

Zložené kódy

$$
\begin{aligned}
E_1: &\quad \{0,1\}^n \xrightarrow{E_1} \Sigma^m \\
E_2: &\quad \Sigma \xrightarrow{E_2} \{0,1\}^k \\
E_2 \circ E_1: &\quad \{0,1\}^n \xrightarrow{E_1} \Sigma^m \xrightarrow{E_2} \{0,1\}^{mk}
\end{aligned}
$$

$$
E_2 \circ E_1 : x \mapsto E_2(y_1) \cdots E_2(y_m), \qquad \text{kde } y = E_1(x)
$$

- vzdialenosť: $\geq \delta_1 \cdot \delta_2$

Zložené kódy

$$\begin{aligned}
\mathrm{RM}: &\quad \{0,1\}^k \xrightarrow{\mathrm{RM}} \quad \mathbb{F}_q^{q^m} \sim \{0,1\}^{\log q \cdot q^m} \\
\mathrm{WH}: &\quad\quad\quad\quad\quad \{0,1\}^{\log q} \xrightarrow{\mathrm{WH}} \{0,1\}^q \\
\mathrm{WH} \circ \mathrm{RM}: &\quad \{0,1\}^k \xrightarrow{\mathrm{RM}} \quad \{0,1\}^{\log q \cdot q^m} \xrightarrow{\mathrm{WH}} \{0,1\}^{q^{m+1}}
\end{aligned}$$

Zložené kódy

Použijeme RM-kód s parametrami

- $q = \log^5 N$
- $m = \log N / \log\log N$
- $d = \log^2 N$

Samoopravné kódy

- potrebujeme:
  - $E : \{0,1\}^N \to \{0,1\}^{N^c}$ v čase poly(N)
  - lokálne dekódovanie v čase polylog$(N) =$ poly(n)
  - opravovať $1/100$ chýb

Samoopravné kódy

- WH má vzdialenosť $1/2$, lokálne vieme opraviť $1/4$ chýb
- RM má vdialenosť $1 - \log^2 N / \log^5 N = 1 - 1/n^3$, lokálne vieme dekódovať $\approx 1/6$ chýb
- WH $\circ$ RM vie lokálne opravovať $\approx (1/4) \cdot (1/6) = 1/24 > 4\%$ chýb
- kódovanie v $\text{poly}(N)$
- dekódovanie WH je v $O(n) = O(\log q) = O(\log \log N)$
- dekódovanie RM je v $\text{poly}(q, m, d) = \text{polylog}(N)$.

Samoopravné kódy

- WH má vzdialenosť $1/2$, lokálne vieme opraviť $1/4$ chýb
- RM má vdialenosť $1 - \log^2 N / \log^5 N = 1 - 1/n^3$, lokálne vieme dekódovať $\approx 1/6$ chýb
- WH $\circ$ RM vie lokálne opravovať $\approx (1/4) \cdot (1/6) = 1/24 > 4\%$ chýb
- kódovanie v $\text{poly}(N)$
- dekódovanie WH je v $O(n) = O(\log q) = O(\log \log N)$
- dekódovanie RM je v $\text{poly}(q, m, d) = \text{polylog}(N)$.

Samoopravné kódy

- WH má vzdialenosť $1/2$, lokálne vieme opraviť $1/4$ chýb
- RM má vdialenosť $1 - \log^2 N / \log^5 N = 1 - 1/n^3$, lokálne vieme dekódovať $\approx 1/6$ chýb
- WH $\circ$ RM vie lokálne opravovať $\approx (1/4) \cdot (1/6) = 1/24 > 4\%$ chýb
- kódovanie v $\text{poly}(N)$
- dekódovanie WH je v $O(n) = O(\log q) = O(\log \log N)$
- dekódovanie RM je v $\text{poly}(q, m, d) = \text{polylog}(N)$.

Samoopravné kódy

- WH má vzdialenosť $1/2$, lokálne vieme opraviť $1/4$ chýb
- RM má vdialenosť $1 - \log^2 N / \log^5 N = 1 - 1/n^3$, lokálne vieme dekódovať $\approx 1/6$ chýb
- WH $\circ$ RM vie lokálne opravovať $\approx (1/4) \cdot (1/6) = 1/24 > 4\%$ chýb
- kódovanie v $\text{poly}(N)$
- dekódovanie WH je v $O(n) = O(\log q) = O(\log \log N)$
- dekódovanie RM je v $\text{poly}(q, m, d) = \text{polylog}(N)$.

Samoopravné kódy

- WH má vzdialenosť $1/2$, lokálne vieme opraviť $1/4$ chýb
- RM má vdialenosť $1 - \log^2 N / \log^5 N = 1 - 1/n^3$, lokálne vieme dekódovať $\approx 1/6$ chýb
- WH $\circ$ RM vie lokálne opravovať $\approx (1/4) \cdot (1/6) = 1/24 > 4\%$ chýb
- kódovanie v $\text{poly}(N)$
- dekódovanie WH je v $O(n) = O(\log q) = O(\log \log N)$
- dekódovanie RM je v $\text{poly}(q, m, d) = \text{polylog}(N)$.

Samoopravné kódy

- WH má vzdialenosť $1/2$, lokálne vieme opraviť $1/4$ chýb
- RM má vdialenosť $1 - \log^2 N / \log^5 N = 1 - 1/n^3$, lokálne vieme dekódovať $\approx 1/6$ chýb
- WH $\circ$ RM vie lokálne opravovať $\approx (1/4) \cdot (1/6) = 1/24 > 4\%$ chýb
- kódovanie v $\text{poly}(N)$
- dekódovanie WH je v $O(n) = O(\log q) = O(\log \log N)$
- dekódovanie RM je v $\text{poly}(q, m, d) = \text{polylog}(N)$.