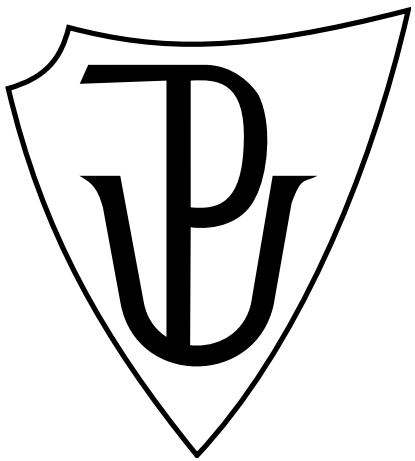
# Teorie informace a kódování (KMI/TIK)

## Reed-Mullerovy kódy



Lukáš Havrlant

Univerzita Palackého

10. ledna 2014

# Primární zdroj

Jiří Adámek: Foundations of Coding. Strany 137–160.

Na webu ke stažení, heslo: burzum.

# Reed-Mullerovy kódy

- Binární lineární blokový kód, značíme $R(r, m)$.
- Délka kódu je $n = 2^m$
- Počet informačních symbolů: $k = \sum_{i=0}^{r} \binom{n}{i}$
- Minimální vzdálenost: $d = 2^{m-r}$
- Opravuje $2^{m-r-1}$ chyb
- Pojmenováno po Irving S. Reed a David E. Muller. Muller objevil kód samotný, Reed vymyslel „jednoduchý“ způsob dekódování.
- $R(1, 5)$ je $(32, 6)$ kód, který využil kosmický koráb Mariner 9 při vysílání fotografií z Marsu v roce 1972.

# Boolovské funkce

# Boolovské funkce

- Boolovská funkce $m$ proměnných je zobrazení $\mathbb{Z}_2^m \longrightarrow \mathbb{Z}_2$.

- Zapisujeme např. pomocí tabulky:

| | | | | |
|---|---|---|---|---|
| $x_1$ | 0 | 1 | 0 | 1 |
| $x_2$ | 0 | 0 | 1 | 1 |
| $f'$ | 1 | 0 | 1 | 1 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| $x_1$ | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 |
| $x_2$ | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 |
| $x_3$ | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 |
| $f''$ | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 1 |

- Hodnoty proměnných $x_i$ zapisujeme tak, aby sloupce tvořily čísla $0, 1, \ldots, 2^m - 1$ v binárním zápise.

# Reprezentace boolovské funkce

Boolovskou funkci o $m$ proměnných můžeme reprezentovat jako slovo délky $2^m$. Např. funkce

| | | | | |
|---|---|---|---|---|
| $x_1$ | 0 | 1 | 0 | 1 |
| $x_2$ | 0 | 0 | 1 | 1 |
| $f'$ | 1 | 0 | 1 | 1 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| $x_1$ | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 |
| $x_2$ | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 |
| $x_3$ | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 |
| $f''$ | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 1 |

můžeme reprezentovat jako slova $f' = 1011$ a $f'' = 11011101$, tj. jen jako poslední řádek.

Jakékoliv slovo o délce $2^m$ reprezentuje nějakou boolovskou funkci.

# Definice boolovské funkce

**Definice:** Slovo $f \in \mathbb{Z}_2^{2^m}$ tvaru $f = f_0 f_1 \dots f_{2^m-1}$, nazveme boolovskou funkcí o $m$ proměnných, definovanou předpisem $f(j_1, j_2, \dots, j_m)$ je rovno $f_j$, pokud má $j$ binární rozvoj $j_m j_{m-1} \dots j_1$.

Příklad: nechť $f = 11110010$ je boolovská funkce o 3 proměnných. Pak $f(0,0,1)$ vyhodnotíme jako číslo $100_2$, což odpovídá číslu $4_{10}$, takže $f(0,0,1) = f_4 = 0$.

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| $x_1$ | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 |
| $x_2$ | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 |
| $x_3$ | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 |
| $f$ | 1 | 1 | 1 | 1 | 0 | 0 | 1 | 0 |

# Zajímavé funkce

- Nulová funkce $\mathbf{0} = 0 \ldots 0$
- Funkce $\mathbf{1} = 1 \ldots 1$
- V proměnné $x_i$ se vždy pravidelně střídají skupiny $2^{i-1}$ nul a $2^{i-1}$ jedniček.

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| $x_1$ | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 |
| $x_2$ | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 |
| $x_3$ | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 |
| $f$ | 1 | 1 | 1 | 1 | 0 | 0 | 1 | 0 |

# Proměnná jako funkce

- Samotné proměnné $x_i$ jsou také funkcemi. Např. pro $m = 2$ máme $x_1 = 0101$ a $x_2 = 0011$:

| | | | | |
|---|---|---|---|---|
| $x_1$ | 0 | 1 | 0 | 1 |
| $x_2$ | 0 | 0 | 1 | 1 |
| $f'$ | 0 | 1 | 0 | 1 |

- Platí, že funkce $f' = x_1$ dvou proměnných je funkce dvou parametrů $f'(x_1, x_2)$, pro kterou platí

$$f'(x_1, x_2) = x_1 = 0101$$

# Logické operace

- Použijeme definice operací $+$ a $\cdot$, které jsme použili u binárních lineárních kódů, tj. sčítání a násobení modulo 2.

- Pak pro boolovské funkce $f = \langle f_0, f_1, \ldots, f_{2^m-1} \rangle$ a $g = \langle g_0, g_1, \ldots, g_{2^m-1} \rangle$ a prvek $x \in \mathbb{Z}_2$ definujeme operace:

$$
\begin{aligned}
f \cdot g &= \langle f_0 \cdot g_0, f_1 \cdot g_1, \ldots, f_{2^m-1} \cdot g_{2^m-1} \rangle \\
f + g &= \langle f_0 + g_0, f_1 + g_1, \ldots, f_{2^m-1} + g_{2^m-1} \rangle \\
x \cdot f &= \langle x \cdot f_0, x \cdot f_1, \ldots, x \cdot f_{2^m-1} \rangle \\
x + f &= \langle x + f_0, x + f_1, \ldots, x + f_{2^m-1} \rangle \\
\neg f &= 1 + f \\
f \cdot f &= f
\end{aligned}
$$

# Pozorování (Currying)

Pokud máme funkci $f$ o třech proměnných, pak slovo $f_0 f_1 f_2 f_3$ je zároveň funkce dvou proměnných tvaru $f(x_1, x_2, 0)$.

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| $x_1$ | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 |
| $x_2$ | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 |
| $x_3$ | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 |
| $f$ | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 0 |

Pokud definujeme $g(x_1, x_2) = f(x_1, x_2, 0)$, pak $g = 0111$, první čtyři symboly funkce $f$. Podobně pro $f(x_1, x_2, 1)$. Obecně:

$$\begin{aligned} f(x_1, x_2, \ldots, x_{m-1}, 0) &= f_0 f_1 \ldots f_{2^{m-1}-1} \\ f(x_1, x_2, \ldots, x_{m-1}, 1) &= f_{2^{m-1}} f_{2^{m-1}+1} \ldots f_{2^m-1} \end{aligned}$$

# Boolovské polynomy

# Boolovské polynomy

Boolovské funkce můžeme také reprezentovat jako součty a součiny funkcí $x_i$ a $\mathbf{1}$. Příklad: $f = 0111$.

| | | | | |
|---|---|---|---|---|
| $x_1$ | 0 | 1 | 0 | 1 |
| $x_2$ | 0 | 0 | 1 | 1 |
| $f$ | 0 | 1 | 1 | 1 |

Funkci můžeme přepsat takto: $f = x_1 + x_2 + x_1 \cdot x_2$, protože:

$$0101 + 0011 + 0101 \cdot 0011 = 0101 + 0011 + 0001 = 0111$$

Tomuto tvaru říkáme boolovský polynom. Lze každou boolovskou funkci zapsat jako polynom?

# Boolovské polynomy 2

- Platí, že $x_i^2 = x_i$, $x_i^1 = x_i$ a $x_i^0 = \mathbf{1}$.

- Boolovský polynom $m$ proměnných je součet funkce $\mathbf{1}$ a členů

$$x_1^{i_1} x_2^{i_2} \dots x_m^{i_m},$$

kde $i_1, \dots, i_m \in \mathbb{Z}_2$. Pro $m = 3$ máme:

$$\begin{aligned} x_1^1 x_2^0 x_3^0 &= x_1 \\ x_1^0 x_2^1 x_3^1 &= x_2 x_3 \\ x_1^0 x_2^0 x_3^0 &= \mathbf{1} \end{aligned}$$

# Boolovské polynomy – definice

**Definice:** Boolovský polynom reprezentující boolovskou funkci $f$ o $m$ proměnných je výraz ve tvaru

$$f = \sum_{i=0}^{2^m-1} q_i \cdot x_1^{i_1} x_2^{i_2} \dots x_m^{i_m},$$

kde $q_i \in \mathbb{Z}_2$ a číslo $i$ má binární rozvoj $i_m i_{m-1} \dots i_2 i_1$.

Pro funkce dvou proměnných tak má polynom tvar

$$q_0\mathbf{1} + q_1x_1 + q_2x_2 + q_3x_1x_2$$

a volbou koeficientů $q_i$ určujeme, jestli v polynomu daný člen „bude“ nebo „nebude“.

# Příklad

- Pro $f = x_2 + x_1x_2$ a $m = 2$ máme:

$$q_0 + q_1x_1 + q_2x_2 + q_3x_1x_2,$$

kde $q_0 = q_1 = 0, \quad q_2 = q_3 = 1.$

- Pro $f = 00001111$ a $m = 3$ máme:

$$q_0 + q_1x_1 + q_2x_2 + q_3x_1x_2 + q_4x_3 + q_5x_1x_3 + q_6x_2x_3 + q_7x_1x_2x_3,$$

kde $q_4 = 1$ a zbytek je nula.

# Snížení počtu proměnných

**Věta:** Pro každou boolovskou funkci $m+1$ proměnných $f(x_1, \ldots, x_m, x_{m+1})$ platí

$$f = f(x_1, \ldots, x_m, 0) + [f(x_1, \ldots, x_m, 0) + f(x_1, \ldots, x_m, 1)] \cdot x_{m+1}$$

Důkaz: Dosadíme za $x_{m+1}$ jedna a nula.

Pokud tento postup použijeme rekurzivně dále, můžeme takto získat z boolovské funkce boolovský polynom.

# Příklad

Převedeme funkci dvou proměnných $f = 0111$ na polynom.

$$f = 01 + (01 + 11)x_2 = 01 + 10x_2$$

Dále vidíme, že

$$\begin{aligned} 01 &= 0 + (0 + 1)x_1 = x_1 \\ 10 &= 1 + (1 + 0)x_1 = 1 + x_1 \end{aligned}$$

Takže

$$f = 01 + 10x_2 = x_1 + (1 + x_1)x_2 = x_1 + x_2 + x_1x_2.$$

Funkce 0111 odpovídá polynomu $x_1 + x_2 + x_1x_2$.

# Důsledek

- Každý boolovský polynom jsme schopni převést na boolovskou funkci. (Zkrátka vše sečteme/vynásobíme.)

- Každou boolovskou funkci jsme schopni převést na boolovský polynom.

# Báze lineárního prostoru $\mathbb{Z}_2^{2^m}$

**Věta:** Mějme vektorový prostor $\mathbb{Z}_2^n$, kde $n = 2^m$. Následující polynomy o jednom sčítanci tvoří bázi $B$ tohoto vektorového prostoru:

$$\mathbf{1},$$
$$x_1, x_2, \ldots, x_m,$$
$$x_i x_j \quad \text{pro} \quad i, j \in \{1, \ldots, m\},$$
$$\vdots,$$
$$x_1 x_2 \ldots x_m$$

# Důkaz

Víme, že každá boolovská funkce délky $n = 2^m$ lze vyjádřit jako boolovský polynom o $m$ proměnných. Obalem báze $B$ je zřejmě celý vektorový prostor $\mathbb{Z}_2^n$. Zbývá dokázat, že vektory/polynomy báze jsou nezávislé.

Dokážeme, že počet polynomů v bázi $B$ je shodný s dimenzí prostoru $\mathbb{Z}_2^n$ (dimenze je $n = 2^m$). Máme 1 polynom stupně 0, $m$ polynomů stupně 1, $\binom{m}{2}$ polynomů stupně 2 atd. Celkem máme

$$\binom{m}{0} + \binom{m}{1} + \binom{m}{2} + \cdots + \binom{m}{m-1} + \binom{m}{m} = \sum_{k=0}^{m} \binom{m}{k} = 2^m$$

polynomů. (Rovnost vysvětlena na dalším slajdu.) □

# Binomická věta

Proč platí rovnost na předchozím slajdu? Binomická věta říká:

$$(x+y)^m = \sum_{k=0}^{m} \binom{m}{k} x^{m-k} y^k.$$

Pokud dosadíme $x = y = 1$, máme:

$$2^m = \sum_{k=0}^{m} \binom{m}{k} = \binom{m}{0} + \binom{m}{1} + \binom{m}{2} + \cdots + \binom{m}{m-1} + \binom{m}{m}.$$

# Stupeň polynomu

Polynom **0** má stupeň $-1$. Polynom **1** má stupeň 0. Stupeň ostatních boolovských polynomů

$$f = \sum_{i=0}^{2^m-1} q_i \cdot x_1^{i_1} x_2^{i_2} \dots x_m^{i_m}$$

je maximální váha slova $i_1 i_2 \dots i_m$ takového, že $q_i = 1$. Tedy je to největší počet proměnných, které se vyskytují v nějakém sčítanci.

Příklady:

- Polynom $1 + x_1 + x_1 x_2$ má stupeň 2,
- polynom $x_1 x_3 + x_1 x_2 x_3$ má stupeň 3.

# Reed-Mullerovy kódy

# Reed-Mullerovy kódy

**Definice:** Reed-Mullerovým kódem stupně $r$ a délky $2^m$ se nazývá množina $R(r, m)$ všech boolovských polynomů $m$ proměnných stupně nejvýše $r$.

Kódová slova Reed-Mullerových kódů tak jsou polynomy.

Příklad: Kódy $R(0, m)$ jsou kódy, které obsahují polynomy o stupni maximálně 0, tj. obsahují pouze $\mathbf{0}$ a $\mathbf{1}$. Jedná se tak o opakující kód délky $2^m$.

# Příklad Reed-Mullerových kódů

**18.3. Příklad: Všechny Reedovy-Mullerovy kódy délky 4**

| | | |
|---|---|---|
| $0$ | 0 0 0 0 | $R(-1, 2)$ |
| $1$ | 1 1 1 1 | $R(0, 2)$ |
| $x_1$ | 0 1 0 1 | |
| $x_2$ | 0 0 1 1 | |
| $x_1 + x_2$ | 0 1 1 0 | |
| $1 + x_1$ | 1 0 1 0 | |
| $1 + x_2$ | 1 1 0 0 | |
| $1 + x_1 + x_2$ | 1 0 0 1 | $R(1, 2)$ |
| $x_1x_2$ | 0 0 0 1 | |
| $1 + x_1x_2$ | 1 1 1 0 | |
| $x_1 + x_1x_2$ | 0 1 0 0 | |
| $x_2 + x_1x_2$ | 0 0 1 0 | |
| $x_1 + x_2 + x_1x_2$ | 0 1 1 1 | |
| $1 + x_1 + x_1x_2$ | 1 0 1 1 | |
| $1 + x_2 + x_1x_2$ | 1 1 0 1 | |
| $1 + x_1 + x_2 + x_1x_2$ | 1 0 0 0 | $R(2, 2)$ |

# Generující matice

- Reed-Mullerův kód je lineární, protože součet dvou polynomů stupně nejvýše $r$ je také polynom stupně nejvýše $r$.

- Generující matice tvoří všechny polynomy obsahující jediný výraz ve tvaru součinu o stupni $\leq r$. Matice kódu $R(2,3)$:

$$G = \left[\begin{array}{cccccccc|c} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ \hline 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & x_1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & x_2 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & x_3 \\ \hline 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & x_1x_2 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & x_1x_3 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & x_2x_3 \end{array}\right].$$

# $R(1,3)$ – Hammingův kód

Podívejme se na generující matici $R(1,3)$:

$$G = \begin{bmatrix} \mathbf{1} \\ x_1 \\ x_2 \\ x_3 \end{bmatrix} = \left[\begin{array}{c|ccccccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ \hline 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right]$$

Je to generující matice rozšířeného Hammingova $(7,4)$ kódu.

Rozšířený Hammingův kód = ke kódovému slovu Hammingova kódu se přidá jeden symbol tak, aby výsledné kódové slovo mělo sudou paritu.

Odstraněním prvního řádku a sloupce získáme klasický kód.

# Kódování

- Slovo, které chceme zakódovat, má délku $k$, kde

$$k = \sum_{i=0}^{r} \binom{m}{i}$$

- Pokud chceme zakódovat slovo $u$, pak symboly $u_i$ nám říkají, které součiny z generující matice budou ve výsledném polynomu.

- Dále postupujeme standardně, kódování $e : \mathbb{Z}_2^k \to R(r, m)$ bude probíhat takto:

$$e(u) = u \cdot G$$

# Příklad kódování

Použijeme generující matici:

$$G = \left[\begin{array}{cccccccc|c} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ \hline 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & x_1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & x_2 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & x_3 \\ \hline 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & x_1x_2 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & x_1x_3 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & x_2x_3 \end{array}\right] .$$

Zakódujeme slovo 0010110:

$$0010110 \cdot G = x_2 + x_1x_2 + x_1x_3 = 00100111$$

Vidíme, že kódování odpovídá kódu sudé parity.

# Vlastnosti

- $R(m, m) = \mathbb{Z}_2^{2^m}$
- $R(m-1, m)$ je $(2^m, 2^m - 1)$ kód sudé parity (ale není systematický, viz příklad).
- $R(0, m)$ je $(2^m, 1)$ opakovací kód.
- Minimální vzdálenost $R(r, m)$ kódu je $2^{m-r}$.

# Geometrická interpretace

# Analytická geometrie: opakování

Máme Euklidovský prostor $\mathbb{R}^3$, který tvoří vektorový prostor, a body $x_1x_2x_3 \in \mathbb{R}^3$. V $\mathbb{R}^3$ máme přímky popsané parametricky

$$\mathbf{a} + t\mathbf{b},$$

kde $\mathbf{a}, \mathbf{b} \in \mathbb{R}^3$ a $t \in \mathbb{R}, \mathbf{b} \neq \mathbf{0}$. Plochu popíšeme jako

$$\mathbf{a} + t\mathbf{b} + s\mathbf{c},$$

kde $\mathbf{a}, \mathbf{b}, \mathbf{c} \in \mathbb{R}^3$, $\mathbf{b}, \mathbf{c}$ jsou lineárně nezávislé a $t, s \in \mathbb{R}$.

# Binární Euklidovský třídimenzionální prostor

Body tohoto prostoru bude množina $\mathbb{Z}_2^3$. Tzn., že prostor obsahuje **konečně** mnoho bodů! Konkrétně osm. Můžeme je všechny zobrazit do tabulky.

| Bod |
| --- |
| $\mathbf{p}_0 = 000$ |
| $\mathbf{p}_1 = 001$ |
| $\mathbf{p}_2 = 010$ |
| $\mathbf{p}_3 = 011$ |
| $\vdots$ |
| $\mathbf{p}_7 = 111$ |

# Charakteristická funkce bodu

Každému bodu $\mathbf{p}_i \in \mathbb{Z}_2^3$ přiřadíme charakteristickou funkci $f = f_7 f_6 \ldots f_1 f_0$. Platí, že

$$f(\mathbf{p}_i) = f_7 f_6 \ldots f_1 f_0, \quad \text{kde } f_j = \begin{cases} 1 & \text{pokud } j = i \\ 0 & \text{jinak} \end{cases}$$

Tabulka:

| Bod | Charakteristická funkce f |
|---|---|
| $\mathbf{p}_0 = 000$ | 00000001 |
| $\mathbf{p}_1 = 001$ | 00000010 |
| $\mathbf{p}_2 = 010$ | 00000100 |
| $\mathbf{p}_3 = 011$ | 00001000 |
| $\vdots$ | $\vdots$ |
| $\mathbf{p}_7 = 111$ | 10000000 |

# Charakteristická funkce množiny

Pokud $P \subseteq \mathbb{Z}_2^3$, pak můžeme definovat charakteristickou funkci $f$ množiny $P$ takto:

$$f(P) = \sum_{\mathbf{p} \in P} \mathbf{p}$$

Jinými slovy, $f(P) = f_7 f_6 \ldots f_1 f_0$, kde $f_i = 1$ právě tehdy, když $\mathbf{p}_i \in P$, jinak $f_i = 0$. Příklad:

$$\begin{aligned} f(\{\mathbf{p}_1, \mathbf{p}_7\}) &= 00000010 + 10000000 = 10000010 \\ f(\emptyset) &= 00000000 \\ f(\mathbb{Z}_2^3) &= 11111111 \end{aligned}$$

# Přímka v $\mathbb{Z}_2^3$

Přímka je opět popsána parametricky jako

$$\mathbf{a} + t\mathbf{b},$$

ale $\mathbf{a}, \mathbf{b} \in \mathbb{Z}_2^3$ a $t \in \mathbb{Z}_2, \mathbf{b} \neq \mathbf{0}$. Přímka tak má právě dva body $\mathbf{a}, \mathbf{a} + \mathbf{b}$.

Naopak každá dvojice různých bodů $\mathbf{a}, \mathbf{b}$ tvoří přímku danou předpisem

$$\mathbf{a} + t(\mathbf{b} - \mathbf{a}).$$

Množina všech přímek pak vypadá takto:
$\{\{\mathbf{p}_0, \mathbf{p}_1\}, \{\mathbf{p}_0, \mathbf{p}_2\}, \ldots, \{\mathbf{p}_6, \mathbf{p}_7\}\}$. Celkem jich je

$$\binom{8}{2} = 27.$$

# Plocha v $\mathbb{Z}_2^3$

Plocha je také popsána parametricky

$$\mathbf{a} + t_1\mathbf{b}_1 + t_2\mathbf{b}_2,$$

kde $\mathbf{a}, \mathbf{b}_1, \mathbf{b}_2 \in \mathbb{Z}_2^3$, $\mathbf{b}_1, \mathbf{b}_2$ jsou nezávislé a $t_1, t_2 \in \mathbb{Z}_2$. Plocha se tak skládá ze čtyř bodů

$$\mathbf{a}, \quad \mathbf{a} + \mathbf{b}_1, \quad \mathbf{a} + \mathbf{b}_2, \quad \mathbf{a} + \mathbf{b}_1 + \mathbf{b}_2.$$

Všechny čtyři body budou po dvou různé, což vyplývá z nezávislosti $\mathbf{b}_1$ a $\mathbf{b}_2$.

# Všechny plochy v $\mathbb{Z}_2^3$

| Plane | Characteristic Function | Boolean Polynomial |
|---|---|---|
| $\{p_1, p_3, p_5, p_7\}$ | 10101010 | $x_0$ |
| $\{p_2, p_3, p_6, p_7\}$ | 11001100 | $x_1$ |
| $\{p_4, p_5, p_6, p_7\}$ | 11110000 | $x_2$ |
| $\{p_0, p_2, p_4, p_6\}$ | 01010101 | $1 + x_0$ |
| $\{p_0, p_1, p_4, p_5\}$ | 00110011 | $1 + x_1$ |
| $\{p_0, p_1, p_2, p_3\}$ | 00001111 | $1 + x_2$ |
| $\{p_1, p_2, p_5, p_6\}$ | 01100110 | $x_0 + x_1$ |
| $\{p_1, p_3, p_4, p_6\}$ | 01011010 | $x_0 + x_2$ |
| $\{p_2, p_3, p_4, p_5\}$ | 00111100 | $x_1 + x_2$ |
| $\{p_1, p_2, p_4, p_7\}$ | 10010110 | $x_0 + x_1 + x_2$ |
| $\{p_0, p_3, p_4, p_7\}$ | 10011001 | $1 + x_0 + x_1$ |
| $\{p_0, p_2, p_5, p_7\}$ | 10100101 | $1 + x_0 + x_2$ |
| $\{p_0, p_1, p_6, p_7\}$ | 11000011 | $1 + x_1 + x_2$ |
| $\{p_0, p_3, p_5, p_6\}$ | 01101001 | $1 + x_0 + x_1 + x_2$ |

# Plocha jako boolovský polynom

Všimněme si – každá plocha $P$ má svou charakteristickou funkci $f(P)$, což je boolovská funkce. Každá boolovská funkce lze převést na boolovský polynom.

Množina všech ploch tvoří kód $R(1,3)$, protože obsahuje všechny polynomy o 3 proměnných a stupni maximálně 1.

# Plocha jako množina řešení rovnice

Všechny plochy procházející počátkem ($\mathbf{a} = \mathbf{0}$) jsou popsány rovnicí

$$h_0 x_0 + h_1 x_1 + h_2 x_2 = 0.$$

Zvolíme koeficienty $h_i$ a dopočítáme souřadnice $x_i$. Např. pro $h_0 = 0, h_1 = 1$ a $h_2 = 1$ máme rovnici

$$0 \cdot x_0 + x_1 + x_2 = 0.$$

Množina řešení rovnice má tvar

$$\{000, 011, 100, 111\} = \{\mathbf{p}_0, \mathbf{p}_3, \mathbf{p}_4, \mathbf{p}_7\}.$$

To odpovídá ploše 10011001, neboli $\mathbf{1} + x_0 + x_1$. Dosazením všech kombinací za $h_i$ získáme všechny plochy procházející počátkem.

# Plocha jako podprostor

**Věta:** Plocha $P$ procházející počátkem $\mathbf{0}$ je dvoudimenzionální podprostor prostoru $\mathbb{Z}_2^3$.
**Důkaz**: Každá plocha $P$ procházející počátkem lze parametricky vyjádřit jako $\mathbf{0} + t_1\mathbf{b}_1 + t_2\mathbf{b}_2$. Obsahuje tak body

$$\mathbf{0}, \quad \mathbf{b}_1, \quad \mathbf{b}_2, \quad \mathbf{b}_1 + \mathbf{b}_2$$

Plocha tak obsahuje nulový vektor. Ověříme uzavřenost na sčítání:

$$\begin{aligned} \mathbf{b}_1 + \mathbf{b}_2 &\in P \\ (\mathbf{b}_1 + \mathbf{b}_2) + \mathbf{b}_1 = \mathbf{b}_2 &\in P \\ (\mathbf{b}_1 + \mathbf{b}_2) + \mathbf{b}_2 = \mathbf{b}_1 &\in P \end{aligned}$$

□

# Ostatní plochy

Snadno ověříme, že ostatní plochy lze popsat rovnicí

$$h_0x_0 + h_1x_1 + h_2x_2 = 1$$

Každou plochu tak lze popsat rovnicí

$$h_0x_0 + h_1x_1 + h_2x_2 = c,$$

kde $c \in \mathbb{Z}_2$.

# Přímky jako průnik dvou ploch

**Věta:** Každou přímku $\mathbf{a} + t\mathbf{b}$ lze popsat jako průnik dvou ploch.

**Důkaz:** Nechť $\mathbf{b}, \mathbf{d}, \mathbf{d}'$ jsou bází prostoru $\mathbb{Z}_2^3$. Dále mějme plochy

$$P_1 : \mathbf{a} + t\mathbf{b} + s\mathbf{d} = \{\mathbf{a}, \mathbf{a}+\mathbf{b}, \mathbf{a}+\mathbf{d}, \mathbf{a}+\mathbf{b}+\mathbf{d}\}$$
$$P_2 : \mathbf{a} + t\mathbf{b} + s\mathbf{d}' = \{\mathbf{a}, \mathbf{a}+\mathbf{b}, \mathbf{a}+\mathbf{d}', \mathbf{a}+\mathbf{b}+\mathbf{d}'\}$$

Protože jsou body $\mathbf{b}, \mathbf{d}$ a $\mathbf{d}'$ nezávislé, platí, že body $\{\mathbf{a}+\mathbf{d}, \mathbf{a}+\mathbf{d}', \mathbf{a}+\mathbf{b}+\mathbf{d}, \mathbf{a}+\mathbf{b}+\mathbf{d}'\}$ jsou po dvou různé. Průnik je tak roven

$$P_1 \cap P_2 = \{\mathbf{a}, \mathbf{a}+\mathbf{b}\} \quad (= \mathbf{a} + t\mathbf{b}).$$

□

# Plocha jako coset

**Věta:** Pro každou plochu $P : \mathbf{a} + t_1\mathbf{b}_1 + t_2\mathbf{b}_2$ existuje dvoudimenzionální vektorový podprostor $K$ prostoru $\mathbb{Z}_2^3$ takový, že množina $\mathbf{a} + K = \{\mathbf{a} + \mathbf{x} \,|\, \mathbf{x} \in K\}$, je rovna ploše $P$. Množině $\mathbf{a} + K$ říkáme „coset vektorového podprostoru $K$ prostoru $\mathbb{Z}_2^3$“.
**Důkaz:** Dvoudimenzionální podprostor $K$ je roven nějaké ploše, která prochází počátkem. Plocha $K$ tak bude mít tvar

$$K : \mathbf{0} + t_1\mathbf{b}_1 + t_2\mathbf{b}_2 = \{\mathbf{0}, \mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_1 + \mathbf{b}_2\}$$

Množina $\mathbf{a} + K$ pak bude vypadat takto:

$$\mathbf{a} + K = \{\mathbf{a}, \mathbf{a} + \mathbf{b}_1, \mathbf{a} + \mathbf{b}_2, \mathbf{a} + \mathbf{b}_1 + \mathbf{b}_2\},$$

což jsou přesně body plochy $P$. □

# Afinní podprostor

O cosetu v předchozí větě řekneme, že se jedná o afinní podprostor dimenze 2. Jiným slovem také *flat*.

Pokud má flat dimenzi $s$, mluvíme o $s$-flatu. 3-flat je tak celý prostor $\mathbb{Z}_2^3$, 2-flat jsou plochy, 1-flat jsou přímky a 0-flat jsou body.

Stejně, jako jsme všechny plochy vyjádřili pomocí cosetů podprostoru dimenze 2, můžeme všechny přímky vyjádřit jako cosety podprostoru dimenze 1 atd.

Pokud máme dva flaty $L$ a $L'$, které mají charakteristické funkce $f_L$ a $f_{L'}$ pak jejich průnik $L \cap L'$ je roven součinu $f_L f_{L'}$.

# R(1,3) a R(2,3)

Reed-Mullerův kód $R(1,3)$ je roven množině všech charakteristických funkcí všech ploch v prostoru $\mathbb{Z}_2^3$. Viz výčet všech ploch.

Reed-Mullerův kód $R(2,3)$ je roven obalu množině všech ploch a všech přímek. Proč nestačí jen množina ploch a přímek?

Polynom $x_0 + x_1x_2$ je stupně 2 a tak je v $R(2,3)$. Přitom má charakteristickou funkci 01101010. Funkce má čtyři jedničky, což znamená čtyři body. Přímka je přitom tvořena dvěma body. Tj. neexistuje přímka, která by popsala polynom $x_0 + x_1x_2$.

Stačí ale vzít plochu $x_0$ a přímku danou součinem ploch $x_1x_2$ jako lineární kombinaci.

# Zobecnění prostoru $\mathbb{Z}_2^3$

Nechť $\mathbb{Z}_2^m$ je binární Euklidovský $m$-dimenzionální prostor, který obsahuje $2^m$ bodů $p_0, \ldots, p_{2^m-1}$, kde

$$p_0 = 00\ldots00, p_1 = 00\ldots01, \ldots, p_{2^m-1} = 11\ldots11$$

Dále nechť $K$ je vektorový $r$-dimenzionální podprostor $\mathbb{Z}_2^m$. Každý coset

$$\mathbf{a} + K = \{\mathbf{a} + \mathbf{b} \,|\, \mathbf{b} \in K\}$$

se nazývá $r$-flat.

**Věta:** Charakteristická funkce $r$-flatu je zároveň boolovský polynom stupně $m - r$.

# Reed-Mullerovy kódy jako $r$-flaty

Reed-Mullerův kód $R(r, m)$ můžeme vidět jako obal charakteristických funkcí flatů o dimenzi nejméně $m - r$.

- $R(1, 3)$ jsou $s$-flaty, kde $s \geq 2$, tedy $s \in \{2, 3\}$, tj. obal ploch a celého prostoru.
- $R(2, 3)$ jsou $s$-flaty, kde $s \geq 1$, tedy $s \in \{1, 2, 3\}$, tj. obal přímek, ploch a celého prostoru.
- $R(3, 3)$ jsou $s$-flaty, kde $s \geq 0$, tedy $s \in \{0, 1, 2, 3\}$, tj. obal bodů, přímek, ploch a celého prostoru.

# Dekódování

# Skalární součin

Skalární součin slov $\mathbf{a} = a_1 \cdots a_n$ a $\mathbf{b} = b_1 \cdots b_n$ je roven

$$\mathbf{a} \cdot \mathbf{b} = \sum_{i=1}^{n} a_i \cdot b_i .$$

# Algoritmus pro dekódování

První krok: přijeme slovo $\mathbf{w}$, spočítáme paritu všech $(r+1)$-flatů. Řekneme, že flat $L$ má sudou paritu, pokud $\mathbf{w} \cdot L = 0$, jinak má lichou paritu.

Rekurzivní krok: pro všechny $s = r, r-1, \ldots, 0$ spočítáme paritu $s$-flatu $L$ tak, že řekneme, že $L$ je sudý, pokud je $L$ obsažen ve více sudých $(s+1)$-flatech než v lichých. Jinak je lichý.

Poslední krok: Opravíme $i$-tý bit slova $\mathbf{w}$ právě tehdy, když 0-flat $\{\mathbf{p}_i\}$ má lichou paritu.