

# Samoprávné kódy

Alexandr Kazda

Univerzita Karlova

1. dubna 2020

- Lineární kódy nad  $\mathbb{F}_q$  uzavřené na cyklické posuny
- Generující polynom  $\beta \mid x^n - 1$  v  $\mathbb{F}_q[x]$  pro nenulový kód
- „Paritní polynom“  $(x^n - 1)/\beta$  čtený pozpátku nám dá paritní matici
- Poznámka: Všimněte si, že  $\beta$  a  $c\beta$  pro  $c \in \mathbb{F}_q \setminus \{0\}$  generují stejný kód
- $\beta$  poskládáme ze ireducibilních faktorů  $x^n - 1$

- Lineární kódy nad  $\mathbb{F}_q$  uzavřené na cyklické posuny
- Generující polynom  $\beta \mid x^n - 1$  v  $\mathbb{F}_q[x]$  pro nenulový kód
- „Paritní polynom“  $(x^n - 1)/\beta$  čtený pozpátku nám dá paritní matici
- Poznámka: Všimněte si, že  $\beta$  a  $c\beta$  pro  $c \in \mathbb{F}_q \setminus \{0\}$  generují stejný kód
- $\beta$  poskládáme ze ireducibilních faktorů  $x^n - 1$

- Lineární kódy nad  $\mathbb{F}_q$  uzavřené na cyklické posuny
- Generující polynom  $\beta \mid x^n - 1$  v  $\mathbb{F}_q[x]$  pro nenulový kód
- „Paritní polynom“  $(x^n - 1)/\beta$  čtený pozpátku nám dá paritní matici
- Poznámka: Všimněte si, že  $\beta$  a  $c\beta$  pro  $c \in \mathbb{F}_q \setminus \{0\}$  generují stejný kód
- $\beta$  poskládáme ze ireducibilních faktorů  $x^n - 1$

- Lineární kódy nad  $\mathbb{F}_q$  uzavřené na cyklické posuny
- Generující polynom  $\beta \mid x^n - 1$  v  $\mathbb{F}_q[x]$  pro nenulový kód
- „Paritní polynom“  $(x^n - 1)/\beta$  čtený pozpátku nám dá paritní matici
- Poznámka: Všimněte si, že  $\beta$  a  $c\beta$  pro  $c \in \mathbb{F}_q \setminus \{0\}$  generují stejný kód
- $\beta$  poskládáme ze ireducibilních faktorů  $x^n - 1$

- Lineární kódy nad  $\mathbb{F}_q$  uzavřené na cyklické posuny
- Generující polynom  $\beta \mid x^n - 1$  v  $\mathbb{F}_q[x]$  pro nenulový kód
- „Paritní polynom“  $(x^n - 1)/\beta$  čtený pozpátku nám dá paritní matici
- Poznámka: Všimněte si, že  $\beta$  a  $c\beta$  pro  $c \in \mathbb{F}_q \setminus \{0\}$  generují stejný kód
- $\beta$  poskládáme ze ireducibilních faktorů  $x^n - 1$

## Příklad: Kolik je cyklických kódů délky 3 nad $\mathbb{F}_2$ ?

- Str. 52 v učebnici
- Dělitelé  $x^3 - 1$  stupně  $< 3$  v  $\mathbb{F}_2$  nám dají různé kódy (mohou být ekvivalentní)
- $x^3 - 1 = (x + 1)(x^2 + x + 1)$ , tedy dělitelé  $\beta = 1$ ,  $\beta = x + 1$ ,  $\beta = x^2 + x + 1$
- Totální kód, paritní kód, opakovací kód
- Nesmíme zapomenout kód  $\{000\}$

# Příklad: Kolik je cyklických kódů délky 3 nad $\mathbb{F}_2$ ?

- Str. 52 v učebnici
- Dělitelé  $x^3 - 1$  stupně  $< 3$  v  $\mathbb{F}_2$  nám dají různé kódy (mohou být ekvivalentní)
- $x^3 - 1 = (x + 1)(x^2 + x + 1)$ , tedy dělitelé  $\beta = 1$ ,  $\beta = x + 1$ ,  $\beta = x^2 + x + 1$
- Totální kód, paritní kód, opakovací kód
- Nesmíme zapomenout kód  $\{000\}$



## Příklad: Kolik je cyklických kódů délky 3 nad $\mathbb{F}_2$ ?

- Str. 52 v učebnici
- Dělitelé  $x^3 - 1$  stupně  $< 3$  v  $\mathbb{F}_2$  nám dají různé kódy (mohou být ekvivalentní)
- $x^3 - 1 = (x + 1)(x^2 + x + 1)$ , tedy dělitelé  $\beta = 1$ ,  $\beta = x + 1$ ,  $\beta = x^2 + x + 1$
- Totální kód, paritní kód, opakovací kód
- Nesmíme zapomenout kód  $\{000\}$

## Příklad: Kolik je cyklických kódů délky 3 nad $\mathbb{F}_2$ ?

- Str. 52 v učebnici
- Dělitelé  $x^3 - 1$  stupně  $< 3$  v  $\mathbb{F}_2$  nám dají různé kódy (mohou být ekvivalentní)
- $x^3 - 1 = (x + 1)(x^2 + x + 1)$ , tedy dělitelé  $\beta = 1$ ,  $\beta = x + 1$ ,  $\beta = x^2 + x + 1$
- Totální kód, paritní kód, opakovací kód
- Nesmíme zapomenout kód  $\{000\}$

## Příklad: Kolik je cyklických kódů délky 3 nad $\mathbb{F}_2$ ?

- Str. 52 v učebnici
- Dělitelé  $x^3 - 1$  stupně  $< 3$  v  $\mathbb{F}_2$  nám dají různé kódy (mohou být ekvivalentní)
- $x^3 - 1 = (x + 1)(x^2 + x + 1)$ , tedy dělitelé  $\beta = 1$ ,  $\beta = x + 1$ ,  $\beta = x^2 + x + 1$
- Totální kód, paritní kód, opakovací kód
- Nesmíme zapomenout kód  $\{000\}$

## Příklad: Kolik je cyklických kódů délky 3 nad $\mathbb{F}_2$ ?

- Str. 52 v učebnici
- Dělitelé  $x^3 - 1$  stupně  $< 3$  v  $\mathbb{F}_2$  nám dají různé kódy (mohou být ekvivalentní)
- $x^3 - 1 = (x + 1)(x^2 + x + 1)$ , tedy dělitelé  $\beta = 1$ ,  $\beta = x + 1$ ,  
 $\beta = x^2 + x + 1$
- Totální kód, paritní kód, opakovací kód
- Nesmíme zapomenout kód  $\{000\}$

## Příklad: Kolik je cyklických kódů délky 4 nad $\mathbb{F}_2$ ?

- Protože 4 je sudá, tak  $x^4 - 1 = (x + 1)^4$
- Možné volby  $\beta$  jsou 0, 1,  $x + 1$ ,  $x^2 + 1$ ,  $x^3 + x^2 + x + 1$
- Nulový kód, totální kód, paritní kód, divný kód a opakovací kód délky 4
- Nemáme rádi vícenásobné kořeny. . .

## Příklad: Kolik je cyklických kódů délky 4 nad $\mathbb{F}_2$ ?

- Protože 4 je sudá, tak  $x^4 - 1 = (x + 1)^4$
- Možné volby  $\beta$  jsou 0, 1,  $x + 1$ ,  $x^2 + 1$ ,  $x^3 + x^2 + x + 1$
- Nulový kód, totální kód, paritní kód, divný kód a opakovací kód délky 4
- Nemáme rádi vícenásobné kořeny. . .

## Příklad: Kolik je cyklických kódů délky 4 nad $\mathbb{F}_2$ ?

- Protože 4 je sudá, tak  $x^4 - 1 = (x + 1)^4$
- Možné volby  $\beta$  jsou 0, 1,  $x + 1$ ,  $x^2 + 1$ ,  $x^3 + x^2 + x + 1$
- Nulový kód, totální kód, paritní kód, divný kód a opakovací kód délky 4
- Nemáme rádi vícenásobné kořeny. . .

## Příklad: Kolik je cyklických kódů délky 4 nad $\mathbb{F}_2$ ?

- Protože 4 je sudá, tak  $x^4 - 1 = (x + 1)^4$
- Možné volby  $\beta$  jsou 0, 1,  $x + 1$ ,  $x^2 + 1$ ,  $x^3 + x^2 + x + 1$
- Nulový kód, totální kód, paritní kód, divný kód a opakovací kód délky 4
- Nemáme rádi vícenásobné kořeny. . .



## Příklad: Kolik je cyklických kódů délky 4 nad $\mathbb{F}_2$ ?

- Protože 4 je sudá, tak  $x^4 - 1 = (x + 1)^4$
- Možné volby  $\beta$  jsou 0, 1,  $x + 1$ ,  $x^2 + 1$ ,  $x^3 + x^2 + x + 1$
- Nulový kód, totální kód, paritní kód, divný kód a opakovací kód délky 4
- Nemáme rádi vícenásobné kořeny. . .

- Pokud  $p$  je nekonstantní polynom **nesoudělný se svou derivací [opraveno oproti přednášce]**, tak  $p$  nemá násobné kořeny.
- $x^n - 1$  nemá násobné kořeny, když  $nx^{n-1} \neq 0$ , tedy  $n \neq 0$  v  $\mathbb{F}_q$
- Dále předpokládejme, že  $n, q$  jsou nesoudělné
- Potom  $x^n - 1 = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$  v nějakém rozšíření tělesa  $\mathbb{F}_q$

- Pokud  $p$  je nekonstantní polynom **nesoudělný se svou derivací [opraveno oproti přednášce]**, tak  $p$  nemá násobné kořeny.
- $x^n - 1$  nemá násobné kořeny, když  $nx^{n-1} \neq 0$ , tedy  $n \neq 0$  v  $\mathbb{F}_q$
- Dále předpokládejme, že  $n, q$  jsou nesoudělné
- Potom  $x^n - 1 = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$  v nějakém rozšíření tělesa  $\mathbb{F}_q$

- Pokud  $p$  je nekonstantní polynom **nesoudělný se svou derivací [opraveno oproti přednášce]**, tak  $p$  nemá násobné kořeny.
- $x^n - 1$  nemá násobné kořeny, když  $nx^{n-1} \neq 0$ , tedy  $n \neq 0$  v  $\mathbb{F}_q$
- Dále předpokládejme, že  $n, q$  jsou nesoudělné
- Potom  $x^n - 1 = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$  v nějakém rozšíření tělesa  $\mathbb{F}_q$

- Pokud  $p$  je nekonstantní polynom **nesoudělný se svou derivací [opraveno oproti přednášce]**, tak  $p$  nemá násobné kořeny.
- $x^n - 1$  nemá násobné kořeny, když  $nx^{n-1} \neq 0$ , tedy  $n \neq 0$  v  $\mathbb{F}_q$
- Dále předpokládejme, že  $n, q$  jsou nesoudělné
- Potom  $x^n - 1 = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$  v nějakém rozšíření tělesa  $\mathbb{F}_q$

- Pokud  $p$  je nekonstantní polynom **nesoudělný se svou derivací [opraveno oproti přednášce]**, tak  $p$  nemá násobné kořeny.
- $x^n - 1$  nemá násobné kořeny, když  $nx^{n-1} \neq 0$ , tedy  $n \neq 0$  v  $\mathbb{F}_q$
- Dále předpokládejme, že  $n, q$  jsou nesoudělné
- Potom  $x^n - 1 = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$  v nějakém rozšíření tělesa  $\mathbb{F}_q$

# Rozkladové těleso v příkladu

- Připomínám: Nadtěleso  $\mathbb{F}_q$  je isomorfní  $\mathbb{F}_{q^m}$  pro nějaké  $m$
- $x^2 + x + 1$  je nerozložitelný v  $\mathbb{F}_2$
- Přidejme si k  $\mathbb{F}_2$  prvek  $\alpha$ , že  $\alpha^2 + \alpha + 1 = 0$
- Tím dostaneme  $\mathbb{F}_2[\alpha]/(\alpha^2 + \alpha + 1) = \mathbb{F}_4$
- Pak  $x^2 + x + 1 = (x - \alpha)(x - (\alpha + 1))$

# Rozkladové těleso v příkladu

- Připomínám: Nadtěleso  $\mathbb{F}_q$  je isomorfní  $\mathbb{F}_{q^m}$  pro nějaké  $m$
- $x^2 + x + 1$  je nerozložitelný v  $\mathbb{F}_2$
- Přidejme si k  $\mathbb{F}_2$  prvek  $\alpha$ , že  $\alpha^2 + \alpha + 1 = 0$
- Tím dostaneme  $\mathbb{F}_2[\alpha]/(\alpha^2 + \alpha + 1) = \mathbb{F}_4$
- Pak  $x^2 + x + 1 = (x - \alpha)(x - (\alpha + 1))$



# Rozkladové těleso v příkladu

- Připomínám: Nadtěleso  $\mathbb{F}_q$  je isomorfní  $\mathbb{F}_{q^m}$  pro nějaké  $m$
- $x^2 + x + 1$  je nerozložitelný v  $\mathbb{F}_2$
- Přidejme si k  $\mathbb{F}_2$  prvek  $\alpha$ , že  $\alpha^2 + \alpha + 1 = 0$
- Tím dostaneme  $\mathbb{F}_2[\alpha]/(\alpha^2 + \alpha + 1) = \mathbb{F}_4$
- Pak  $x^2 + x + 1 = (x - \alpha)(x - (\alpha + 1))$

# Rozkladové těleso v příkladu

- Připomínám: Nadtěleso  $\mathbb{F}_q$  je isomorfní  $\mathbb{F}_{q^m}$  pro nějaké  $m$
- $x^2 + x + 1$  je nerozložitelný v  $\mathbb{F}_2$
- Přidejme si k  $\mathbb{F}_2$  prvek  $\alpha$ , že  $\alpha^2 + \alpha + 1 = 0$
- Tím dostaneme  $\mathbb{F}_2[\alpha]/(\alpha^2 + \alpha + 1) = \mathbb{F}_4$
- Pak  $x^2 + x + 1 = (x - \alpha)(x - (\alpha + 1))$

# Rozkladové těleso v příkladu

- Připomínám: Nadtěleso  $\mathbb{F}_q$  je isomorfní  $\mathbb{F}_{q^m}$  pro nějaké  $m$
- $x^2 + x + 1$  je nerozložitelný v  $\mathbb{F}_2$
- Přidejme si k  $\mathbb{F}_2$  prvek  $\alpha$ , že  $\alpha^2 + \alpha + 1 = 0$
- Tím dostaneme  $\mathbb{F}_2[\alpha]/(\alpha^2 + \alpha + 1) = \mathbb{F}_4$
- Pak  $x^2 + x + 1 = (x - \alpha)(x - (\alpha + 1))$

# Rozkladové těleso v příkladu

- Připomínám: Nadtěleso  $\mathbb{F}_q$  je isomorfní  $\mathbb{F}_{q^m}$  pro nějaké  $m$
- $x^2 + x + 1$  je nerozložitelný v  $\mathbb{F}_2$
- Přidejme si k  $\mathbb{F}_2$  prvek  $\alpha$ , že  $\alpha^2 + \alpha + 1 = 0$
- Tím dostaneme  $\mathbb{F}_2[\alpha]/(\alpha^2 + \alpha + 1) = \mathbb{F}_4$
- Pak  $x^2 + x + 1 = (x - \alpha)(x - (\alpha + 1))$

# K čemu je automorfismus

- Jak vím, že  $\alpha + 1$  je také kořen?
- Zobecnění komplexního sdružení: Zobrazení  $a \mapsto a^2$  je automorfismus  $\mathbb{F}_4$ , který nehýbe s prvky  $\mathbb{F}_2$
- Tedy  $0^2 = (\alpha^2 + \alpha + 1)^2 = (\alpha^2)^2 + \alpha^2 + 1$
- Pokud  $\alpha$  je kořen, tak  $\alpha^2 = \alpha + 1$  je také kořen

# K čemu je automorfismus

- Jak vím, že  $\alpha + 1$  je také kořen?
- Zobecnění komplexního sdružení: Zobrazení  $a \mapsto a^2$  je automorfismus  $\mathbb{F}_4$ , který nehýbe s prvky  $\mathbb{F}_2$
- Tedy  $0^2 = (\alpha^2 + \alpha + 1)^2 = (\alpha^2)^2 + \alpha^2 + 1$
- Pokud  $\alpha$  je kořen, tak  $\alpha^2 = \alpha + 1$  je také kořen

# K čemu je automorfismus

- Jak vím, že  $\alpha + 1$  je také kořen?
- Zobecnění komplexního sdružení: Zobrazení  $a \mapsto a^2$  je automorfismus  $\mathbb{F}_4$ , který nehýbe s prvky  $\mathbb{F}_2$
- Tedy  $0^2 = (\alpha^2 + \alpha + 1)^2 = (\alpha^2)^2 + \alpha^2 + 1$
- Pokud  $\alpha$  je kořen, tak  $\alpha^2 = \alpha + 1$  je také kořen

# K čemu je automorfismus

- Jak vím, že  $\alpha + 1$  je také kořen?
- Zobecnění komplexního sdružení: Zobrazení  $a \mapsto a^2$  je automorfismus  $\mathbb{F}_4$ , který nehýbe s prvky  $\mathbb{F}_2$
- Tedy  $0^2 = (\alpha^2 + \alpha + 1)^2 = (\alpha^2)^2 + \alpha^2 + 1$
- Pokud  $\alpha$  je kořen, tak  $\alpha^2 = \alpha + 1$  je také kořen



# K čemu je automorfismus

- Jak vím, že  $\alpha + 1$  je také kořen?
- Zobecnění komplexního sdružení: Zobrazení  $a \mapsto a^2$  je automorfismus  $\mathbb{F}_4$ , který nehýbe s prvky  $\mathbb{F}_2$
- Tedy  $0^2 = (\alpha^2 + \alpha + 1)^2 = (\alpha^2)^2 + \alpha^2 + 1$
- Pokud  $\alpha$  je kořen, tak  $\alpha^2 = \alpha + 1$  je také kořen

# Rozklad $x^n - 1$

- Připomínám  $(n, q) = 1$
- Připomínám, že  $\mathbb{F}_{q^m}^*$  je cyklická
- Co jsou kořeny  $x^n - 1$ ? Přesně  $n$ -té odmocniny z 1; prvky řádu dělitelého  $n$  v multiplikativní grupě tělesa
- Kdy budu mít v  $\mathbb{F}_{q^m}^*$  prvek  $\alpha$  řádu  $n$ ? Když  $n \mid q^m - 1$  (neboli  $q^m \equiv 1 \pmod{n}$ )
- Potom  $x^n - 1 = \prod_{i=0}^{n-1} (x - \alpha^i)$

- Připomínám  $(n, q) = 1$
- Připomínám, že  $\mathbb{F}_{q^m}^*$  je cyklická
- Co jsou kořeny  $x^n - 1$ ? Přesně  $n$ -té odmocniny z 1; prvky řádu dělitelého  $n$  v multiplikativní grupě tělesa
- Kdy budu mít v  $\mathbb{F}_{q^m}^*$  prvek  $\alpha$  řádu  $n$ ? Když  $n \mid q^m - 1$  (neboli  $q^m \equiv 1 \pmod{n}$ )
- Potom  $x^n - 1 = \prod_{i=0}^{n-1} (x - \alpha^i)$

- Připomínám  $(n, q) = 1$
- Připomínám, že  $\mathbb{F}_{q^m}^\star$  je cyklická
- Co jsou kořeny  $x^n - 1$ ? Přesně  $n$ -té odmocniny z 1; prvky řádu dělitelého  $n$  v multiplikativní grupě tělesa
- Kdy budu mít v  $\mathbb{F}_{q^m}^\star$  prvek  $\alpha$  řádu  $n$ ? Když  $n \mid q^m - 1$  (neboli  $q^m \equiv 1 \pmod{n}$ )
- Potom  $x^n - 1 = \prod_{i=0}^{n-1} (x - \alpha^i)$

# Rozklad $x^n - 1$

- Připomínám  $(n, q) = 1$
- Připomínám, že  $\mathbb{F}_{q^m}^*$  je cyklická
- Co jsou kořeny  $x^n - 1$ ? Přesně  $n$ -té odmocniny z 1; prvky řádu dělitelého  $n$  v multiplikativní grupě tělesa
- Kdy budu mít v  $\mathbb{F}_{q^m}^*$  prvek  $\alpha$  řádu  $n$ ? Když  $n \mid q^m - 1$  (neboli  $q^m \equiv 1 \pmod{n}$ )
- Potom  $x^n - 1 = \prod_{i=0}^{n-1} (x - \alpha^i)$

# Rozklad $x^n - 1$

- Připomínám  $(n, q) = 1$
- Připomínám, že  $\mathbb{F}_{q^m}^\star$  je cyklická
- Co jsou kořeny  $x^n - 1$ ? Přesně  $n$ -té odmocniny z 1; prvky řádu dělitelého  $n$  v multiplikativní grupě tělesa
- Kdy budu mít v  $\mathbb{F}_{q^m}^\star$  prvek  $\alpha$  řádu  $n$ ? Když  $n \mid q^m - 1$  (neboli  $q^m \equiv 1 \pmod{n}$ )
- Potom  $x^n - 1 = \prod_{i=0}^{n-1} (x - \alpha^i)$

- Připomínám  $(n, q) = 1$
- Připomínám, že  $\mathbb{F}_{q^m}^\star$  je cyklická
- Co jsou kořeny  $x^n - 1$ ? Přesně  $n$ -té odmocniny z 1; prvky řádu dělícího  $n$  v multiplikativní grupě tělesa
- Kdy budu mít v  $\mathbb{F}_{q^m}^\star$  prvek  $\alpha$  řádu  $n$ ? Když  $n \mid q^m - 1$  (neboli  $q^m \equiv 1 \pmod{n}$ )
- Potom  $x^n - 1 = \prod_{i=0}^{n-1} (x - \alpha^i)$

# Cyklotomické polynomy v příkladu

- $q = 2$ ,  $n = 7$ , máme v  $\mathbb{F}_{2^3}$  prvek  $\alpha$ , že

$$x^7 - 1 = (x+1)(x^3+x^2+1)(x^3+x+1) = (x+1)(x+\alpha)(x+\alpha^2) \cdots (x+\alpha^6)$$

- Které mocniny  $\alpha$  se nám sdruží?
- Zobrazení  $a \mapsto a^2$  je automorfismus  $\mathbb{F}_8$ , které fixuje  $\mathbb{F}_2$ , tedy pokud  $\alpha$  je kořen třeba  $x^3 + x^2 + 1$ , tak  $\alpha^2$  a  $\alpha^4$  jsou taky kořeny
- Volím-li  $\alpha$ , že  $\alpha^3 + \alpha^2 + 1 = 0$ , tak mám

$$x + 1 = x + \alpha^0$$

$$x^3 + x^2 + 1 = (x + \alpha)(x + \alpha^2)(x + \alpha^4)$$

$$x^3 + x + 1 = (x + \alpha^3)(x + \alpha^6)(x + \alpha^5)$$



# Cyklotomické polynomy v příkladu

- $q = 2$ ,  $n = 7$ , máme v  $\mathbb{F}_{2^3}$  prvek  $\alpha$ , že

$$x^7 - 1 = (x+1)(x^3+x^2+1)(x^3+x+1) = (x+1)(x+\alpha)(x+\alpha^2) \cdots (x+\alpha^6)$$

- Které mocniny  $\alpha$  se nám sdruží?
- Zobrazení  $a \mapsto a^2$  je automorfismus  $\mathbb{F}_8$ , které fixuje  $\mathbb{F}_2$ , tedy pokud  $\alpha$  je kořen třeba  $x^3 + x^2 + 1$ , tak  $\alpha^2$  a  $\alpha^4$  jsou taky kořeny
- Volím-li  $\alpha$ , že  $\alpha^3 + \alpha^2 + 1 = 0$ , tak mám

$$x + 1 = x + \alpha^0$$

$$x^3 + x^2 + 1 = (x + \alpha)(x + \alpha^2)(x + \alpha^4)$$

$$x^3 + x + 1 = (x + \alpha^3)(x + \alpha^6)(x + \alpha^5)$$

# Cyklotomické polynomy v příkladu

- $q = 2$ ,  $n = 7$ , máme v  $\mathbb{F}_{2^3}$  prvek  $\alpha$ , že

$$x^7 - 1 = (x+1)(x^3+x^2+1)(x^3+x+1) = (x+1)(x+\alpha)(x+\alpha^2) \cdots (x+\alpha^6)$$

- Které mocniny  $\alpha$  se nám sdruží?
- Zobrazení  $a \mapsto a^2$  je automorfismus  $\mathbb{F}_8$ , které fixuje  $\mathbb{F}_2$ , tedy pokud  $\alpha$  je kořen třeba  $x^3 + x^2 + 1$ , tak  $\alpha^2$  a  $\alpha^4$  jsou taky kořeny
- Volím-li  $\alpha$ , že  $\alpha^3 + \alpha^2 + 1 = 0$ , tak mám

$$x + 1 = x + \alpha^0$$

$$x^3 + x^2 + 1 = (x + \alpha)(x + \alpha^2)(x + \alpha^4)$$

$$x^3 + x + 1 = (x + \alpha^3)(x + \alpha^6)(x + \alpha^5)$$

# Cyklotomické polynomy v příkladu

- $q = 2$ ,  $n = 7$ , máme v  $\mathbb{F}_{2^3}$  prvek  $\alpha$ , že

$$x^7 - 1 = (x+1)(x^3+x^2+1)(x^3+x+1) = (x+1)(x+\alpha)(x+\alpha^2) \cdots (x+\alpha^6)$$

- Které mocniny  $\alpha$  se nám sdruží?
- Zobrazení  $a \mapsto a^2$  je automorfismus  $\mathbb{F}_8$ , které fixuje  $\mathbb{F}_2$ , tedy pokud  $\alpha$  je kořen třeba  $x^3 + x^2 + 1$ , tak  $\alpha^2$  a  $\alpha^4$  jsou taky kořeny
- Volím-li  $\alpha$ , že  $\alpha^3 + \alpha^2 + 1 = 0$ , tak mám

$$x + 1 = x + \alpha^0$$

$$x^3 + x^2 + 1 = (x + \alpha)(x + \alpha^2)(x + \alpha^4)$$

$$x^3 + x + 1 = (x + \alpha^3)(x + \alpha^6)(x + \alpha^5)$$

# Cyklotomické polynomy v příkladu

- $q = 2$ ,  $n = 7$ , máme v  $\mathbb{F}_{2^3}$  prvek  $\alpha$ , že

$$x^7 - 1 = (x+1)(x^3+x^2+1)(x^3+x+1) = (x+1)(x+\alpha)(x+\alpha^2) \cdots (x+\alpha^6)$$

- Které mocniny  $\alpha$  se nám sdruží?
- Zobrazení  $a \mapsto a^2$  je automorfismus  $\mathbb{F}_8$ , které fixuje  $\mathbb{F}_2$ , tedy pokud  $\alpha$  je kořen třeba  $x^3 + x^2 + 1$ , tak  $\alpha^2$  a  $\alpha^4$  jsou taky kořeny
- Volím-li  $\alpha$ , že  $\alpha^3 + \alpha^2 + 1 = 0$ , tak mám

$$x + 1 = x + \alpha^0$$

$$x^3 + x^2 + 1 = (x + \alpha)(x + \alpha^2)(x + \alpha^4)$$

$$x^3 + x + 1 = (x + \alpha^3)(x + \alpha^6)(x + \alpha^5)$$

## Theorem

*Bud'  $q$  mocnina prvočísla,  $m \in \mathbb{N}$  a vnořme přirozeně  $\mathbb{F}_q$  do  $\mathbb{F}_{q^m}$ . Potom zobrazení  $a \mapsto a^q$  je automorfismus  $\mathbb{F}_{q^m}$  takový, že  $a = a^q$ , právě když  $a \in \mathbb{F}_q$ .*

## Důkaz.

- $(a + b)^q = a^q + b^q$  je binomická věta
- $a = a^q$  pro  $a \in \mathbb{F}_q$  je Malá Fermatova věta
- Polynom  $a^q - a$  má nejvýše  $q$  kořenů, tedy pro  $a \in \mathbb{F}_{q^m} \setminus \mathbb{F}_q$  neplatí  $a^q - a = 0$



## Theorem

*Bud'  $q$  mocnina prvočísla,  $m \in \mathbb{N}$  a vnořme přirozeně  $\mathbb{F}_q$  do  $\mathbb{F}_{q^m}$ . Potom zobrazení  $a \mapsto a^q$  je automorfismus  $\mathbb{F}_{q^m}$  takový, že  $a = a^q$ , právě když  $a \in \mathbb{F}_q$ .*

## Důkaz.

- $(a + b)^q = a^q + b^q$  je binomická věta
- $a = a^q$  pro  $a \in \mathbb{F}_q$  je Malá Fermatova věta
- Polynom  $a^q - a$  má nejvýše  $q$  kořenů, tedy pro  $a \in \mathbb{F}_{q^m} \setminus \mathbb{F}_q$  neplatí  $a^q - a = 0$



## Theorem

*Bud'  $q$  mocnina prvočísla,  $m \in \mathbb{N}$  a vnořme přirozeně  $\mathbb{F}_q$  do  $\mathbb{F}_{q^m}$ . Potom zobrazení  $a \mapsto a^q$  je automorfismus  $\mathbb{F}_{q^m}$  takový, že  $a = a^q$ , právě když  $a \in \mathbb{F}_q$ .*

## Důkaz.

- $(a + b)^q = a^q + b^q$  je binomická věta
- $a = a^q$  pro  $a \in \mathbb{F}_q$  je Malá Fermatova věta
- Polynom  $a^q - a$  má nejvýše  $q$  kořenů, tedy pro  $a \in \mathbb{F}_{q^m} \setminus \mathbb{F}_q$  neplatí  $a^q - a = 0$



## Theorem

*Bud'  $q$  mocnina prvočísla,  $m \in \mathbb{N}$  a vnořme přirozeně  $\mathbb{F}_q$  do  $\mathbb{F}_{q^m}$ . Potom zobrazení  $a \mapsto a^q$  je automorfismus  $\mathbb{F}_{q^m}$  takový, že  $a = a^q$ , právě když  $a \in \mathbb{F}_q$ .*

## Důkaz.

- $(a + b)^q = a^q + b^q$  je binomická věta
- $a = a^q$  pro  $a \in \mathbb{F}_q$  je Malá Fermatova věta
- Polynom  $a^q - a$  má nejvýše  $q$  kořenů, tedy pro  $a \in \mathbb{F}_{q^m} \setminus \mathbb{F}_q$  neplatí  $a^q - a = 0$





# Kořeny cyklotomických polynomů

## Theorem (Po přednášce: Opravené exponenty u $q$ )

*Bud'  $q$  mocnina prvočísla,  $n \in \mathbb{N}$ ,  $(n, q) = 1$ ,  $m$  takové, že  $q^m \equiv 1 \pmod{n}$ . Bud'  $r$  ireducibilní faktor  $x^n - 1$  v  $\mathbb{F}_q[x]$  (cyklotomický polynom). Bud'  $\gamma$  kořen  $r$  v  $\mathbb{F}_{q^m}$ . Pak ve  $\mathbb{F}_{q^m}$  platí*

$$r = (x - \gamma)(x - \gamma^q)(x - \gamma^{q^2})(x - \gamma^{q^3})(x - \gamma^{q^4}) \cdots (x - \gamma^{q^t}),$$

*kde  $t$  je nejmenší takové, že  $\gamma^{q^{t+1}} = \gamma$  (neboli řád  $\gamma$  dělí  $q^{t+1} - 1$ ).*

## Důkaz.

- Automorfismus  $a \mapsto a^q$  si vynutí kořeny  $\gamma^{q^i}$  pro  $r$
- Značme  $s = (x - \gamma)(x - \gamma^q)(x - \gamma^{q^2}) \cdots (x - \gamma^{q^t})$
- Je to polynom z koeficienty z  $\mathbb{F}_q$ , protože  $s$  je invariantní na  $a \mapsto a^q$
- Tedy  $s \mid r$  v  $\mathbb{F}_q[x]$  a  $r$  je ireducibilní, tj.  $s = r$



# Kořeny cyklotomických polynomů

## Theorem (Po přednášce: Opravené exponenty u $q$ )

*Bud'  $q$  mocnina prvočísla,  $n \in \mathbb{N}$ ,  $(n, q) = 1$ ,  $m$  takové, že  $q^m \equiv 1 \pmod{n}$ . Bud'  $r$  ireducibilní faktor  $x^n - 1$  v  $\mathbb{F}_q[x]$  (cyklotomický polynom). Bud'  $\gamma$  kořen  $r$  v  $\mathbb{F}_{q^m}$ . Pak ve  $\mathbb{F}_{q^m}$  platí*

$$r = (x - \gamma)(x - \gamma^q)(x - \gamma^{q^2})(x - \gamma^{q^3})(x - \gamma^{q^4}) \cdots (x - \gamma^{q^t}),$$

*kde  $t$  je nejmenší takové, že  $\gamma^{q^{t+1}} = \gamma$  (neboli řád  $\gamma$  dělí  $q^{t+1} - 1$ ).*

## Důkaz.

- Automorfismus  $a \mapsto a^q$  si vynutí kořeny  $\gamma^{q^i}$  pro  $r$
- Značme  $s = (x - \gamma)(x - \gamma^q)(x - \gamma^{q^2}) \cdots (x - \gamma^{q^t})$
- Je to polynom z koeficienty z  $\mathbb{F}_q$ , protože  $s$  je invariantní na  $a \mapsto a^q$
- Tedy  $s \mid r$  v  $\mathbb{F}_q[x]$  a  $r$  je ireducibilní, tj.  $s = r$



# Kořeny cyklotomických polynomů

## Theorem (Po přednášce: Opravené exponenty u $q$ )

*Bud'  $q$  mocnina prvočísla,  $n \in \mathbb{N}$ ,  $(n, q) = 1$ ,  $m$  takové, že  $q^m \equiv 1 \pmod{n}$ . Bud'  $r$  ireducibilní faktor  $x^n - 1$  v  $\mathbb{F}_q[x]$  (cyklotomický polynom). Bud'  $\gamma$  kořen  $r$  v  $\mathbb{F}_{q^m}$ . Pak ve  $\mathbb{F}_{q^m}$  platí*

$$r = (x - \gamma)(x - \gamma^q)(x - \gamma^{q^2})(x - \gamma^{q^3})(x - \gamma^{q^4}) \cdots (x - \gamma^{q^t}),$$

*kde  $t$  je nejmenší takové, že  $\gamma^{q^{t+1}} = \gamma$  (neboli řád  $\gamma$  dělí  $q^{t+1} - 1$ ).*

## Důkaz.

- Automorfismus  $a \mapsto a^q$  si vynutí kořeny  $\gamma^{q^i}$  pro  $r$
- Značme  $s = (x - \gamma)(x - \gamma^q)(x - \gamma^{q^2}) \cdots (x - \gamma^{q^t})$
- Je to polynom z koeficienty z  $\mathbb{F}_q$ , protože  $s$  je invariantní na  $a \mapsto a^q$
- Tedy  $s \mid r$  v  $\mathbb{F}_q[x]$  a  $r$  je ireducibilní, tj.  $s = r$



# Kořeny cyklotomických polynomů

## Theorem (Po přednášce: Opravené exponenty u $q$ )

*Bud'  $q$  mocnina prvočísla,  $n \in \mathbb{N}$ ,  $(n, q) = 1$ ,  $m$  takové, že  $q^m \equiv 1 \pmod{n}$ . Bud'  $r$  ireducibilní faktor  $x^n - 1$  v  $\mathbb{F}_q[x]$  (cyklotomický polynom). Bud'  $\gamma$  kořen  $r$  v  $\mathbb{F}_{q^m}$ . Pak ve  $\mathbb{F}_{q^m}$  platí*

$$r = (x - \gamma)(x - \gamma^q)(x - \gamma^{q^2})(x - \gamma^{q^3})(x - \gamma^{q^4}) \cdots (x - \gamma^{q^t}),$$

*kde  $t$  je nejmenší takové, že  $\gamma^{q^{t+1}} = \gamma$  (neboli řád  $\gamma$  dělí  $q^{t+1} - 1$ ).*

## Důkaz.

- Automorfismus  $a \mapsto a^q$  si vynutí kořeny  $\gamma^{q^i}$  pro  $r$
- Značme  $s = (x - \gamma)(x - \gamma^q)(x - \gamma^{q^2}) \cdots (x - \gamma^{q^t})$
- Je to polynom z koeficienty z  $\mathbb{F}_q$ , protože  $s$  je invariantní na  $a \mapsto a^q$
- Tedy  $s \mid r$  v  $\mathbb{F}_q[x]$  a  $r$  je ireducibilní, tj.  $s = r$



# Kořeny cyklotomických polynomů

## Theorem (Po přednášce: Opravené exponenty u $q$ )

*Bud'  $q$  mocnina prvočísla,  $n \in \mathbb{N}$ ,  $(n, q) = 1$ ,  $m$  takové, že  $q^m \equiv 1 \pmod{n}$ . Bud'  $r$  ireducibilní faktor  $x^n - 1$  v  $\mathbb{F}_q[x]$  (cyklotomický polynom). Bud'  $\gamma$  kořen  $r$  v  $\mathbb{F}_{q^m}$ . Pak ve  $\mathbb{F}_{q^m}$  platí*

$$r = (x - \gamma)(x - \gamma^q)(x - \gamma^{q^2})(x - \gamma^{q^3})(x - \gamma^{q^4}) \cdots (x - \gamma^{q^t}),$$

*kde  $t$  je nejmenší takové, že  $\gamma^{q^{t+1}} = \gamma$  (neboli řád  $\gamma$  dělí  $q^{t+1} - 1$ ).*

## Důkaz.

- Automorfismus  $a \mapsto a^q$  si vynutí kořeny  $\gamma^{q^i}$  pro  $r$
- Značme  $s = (x - \gamma)(x - \gamma^q)(x - \gamma^{q^2}) \cdots (x - \gamma^{q^t})$
- Je to polynom z koeficienty z  $\mathbb{F}_q$ , protože  $s$  je invariantní na  $a \mapsto a^q$
- Tedy  $s \mid r$  v  $\mathbb{F}_q[x]$  a  $r$  je ireducibilní, tj.  $s = r$



# K čemu je to dobré?

- Jak se faktorizuje  $x^{20} - 1$  nad  $\mathbb{F}_3$ ?
- $n = 20$ , chci  $m$ , že  $3^m \equiv 1 \pmod{20}$  (funguje třeba  $m = 4$ )
- Volme  $\alpha$  primitivní 20. odmocninu z 1 v  $\mathbb{F}_{3^m}$
- Jak dopadnou „skupinky“ mocnin  $\alpha$  – cyklotomické třídy?
- $\{0\}$  (odpovídá děliteli  $x - 1$ )
- $\{1, 3, 9, 7\}$
- $\{2, 6, 18, 14\}$
- $\{4, 12, 16, 8\}$
- $\{5, 15\}$
- $\{10\}$  (odpovídá  $x + 1$ )
- $\{11, 13, 19, 17\}$
- Tedy  $x^{20} - 1$  má 2 faktory st. 1, 1 faktor st. 2 a 4 faktory st. 4

# K čemu je to dobré?

- Jak se faktorizuje  $x^{20} - 1$  nad  $\mathbb{F}_3$ ?
- $n = 20$ , chci  $m$ , že  $3^m \equiv 1 \pmod{20}$  (funguje třeba  $m = 4$ )
- Volme  $\alpha$  primitivní 20. odmocninu z 1 v  $\mathbb{F}_{3^m}$
- Jak dopadnou „skupinky“ mocnin  $\alpha$  – cyklotomické třídy?
- $\{0\}$  (odpovídá děliteli  $x - 1$ )
- $\{1, 3, 9, 7\}$
- $\{2, 6, 18, 14\}$
- $\{4, 12, 16, 8\}$
- $\{5, 15\}$
- $\{10\}$  (odpovídá  $x + 1$ )
- $\{11, 13, 19, 17\}$
- Tedy  $x^{20} - 1$  má 2 faktory st. 1, 1 faktor st. 2 a 4 faktory st. 4

# K čemu je to dobré?

- Jak se faktorizuje  $x^{20} - 1$  nad  $\mathbb{F}_3$ ?
- $n = 20$ , chci  $m$ , že  $3^m \equiv 1 \pmod{20}$  (funguje třeba  $m = 4$ )
- Volme  $\alpha$  primitivní 20. odmocninu z 1 v  $\mathbb{F}_{3^m}$
- Jak dopadnou „skupinky“ mocnin  $\alpha$  – cyklotomické třídy?
- $\{0\}$  (odpovídá děliteli  $x - 1$ )
- $\{1, 3, 9, 7\}$
- $\{2, 6, 18, 14\}$
- $\{4, 12, 16, 8\}$
- $\{5, 15\}$
- $\{10\}$  (odpovídá  $x + 1$ )
- $\{11, 13, 19, 17\}$
- Tedy  $x^{20} - 1$  má 2 faktory st. 1, 1 faktor st. 2 a 4 faktory st. 4



# K čemu je to dobré?

- Jak se faktorizuje  $x^{20} - 1$  nad  $\mathbb{F}_3$ ?
- $n = 20$ , chci  $m$ , že  $3^m \equiv 1 \pmod{20}$  (funguje třeba  $m = 4$ )
- Volme  $\alpha$  primitivní 20. odmocninu z 1 v  $\mathbb{F}_{3^m}$
- Jak dopadnou „skupinky“ mocnin  $\alpha$  – cyklotomické třídy?
- $\{0\}$  (odpovídá děliteli  $x - 1$ )
- $\{1, 3, 9, 7\}$
- $\{2, 6, 18, 14\}$
- $\{4, 12, 16, 8\}$
- $\{5, 15\}$
- $\{10\}$  (odpovídá  $x + 1$ )
- $\{11, 13, 19, 17\}$
- Tedy  $x^{20} - 1$  má 2 faktory st. 1, 1 faktor st. 2 a 4 faktory st. 4

# K čemu je to dobré?

- Jak se faktorizuje  $x^{20} - 1$  nad  $\mathbb{F}_3$ ?
- $n = 20$ , chci  $m$ , že  $3^m \equiv 1 \pmod{20}$  (funguje třeba  $m = 4$ )
- Volme  $\alpha$  primitivní 20. odmocninu z 1 v  $\mathbb{F}_{3^m}$
- Jak dopadnou „skupinky“ mocnin  $\alpha$  – cyklotomické třídy?
- $\{0\}$  (odpovídá děliteli  $x - 1$ )
- $\{1, 3, 9, 7\}$
- $\{2, 6, 18, 14\}$
- $\{4, 12, 16, 8\}$
- $\{5, 15\}$
- $\{10\}$  (odpovídá  $x + 1$ )
- $\{11, 13, 19, 17\}$
- Tedy  $x^{20} - 1$  má 2 faktory st. 1, 1 faktor st. 2 a 4 faktory st. 4

# K čemu je to dobré?

- Jak se faktorizuje  $x^{20} - 1$  nad  $\mathbb{F}_3$ ?
- $n = 20$ , chci  $m$ , že  $3^m \equiv 1 \pmod{20}$  (funguje třeba  $m = 4$ )
- Volme  $\alpha$  primitivní 20. odmocninu z 1 v  $\mathbb{F}_{3^m}$
- Jak dopadnou „skupinky“ mocnin  $\alpha$  – cyklotomické třídy?
- $\{0\}$  (odpovídá děliteli  $x - 1$ )
- $\{1, 3, 9, 7\}$
- $\{2, 6, 18, 14\}$
- $\{4, 12, 16, 8\}$
- $\{5, 15\}$
- $\{10\}$  (odpovídá  $x + 1$ )
- $\{11, 13, 19, 17\}$
- Tedy  $x^{20} - 1$  má 2 faktory st. 1, 1 faktor st. 2 a 4 faktory st. 4

# K čemu je to dobré?

- Jak se faktorizuje  $x^{20} - 1$  nad  $\mathbb{F}_3$ ?
- $n = 20$ , chci  $m$ , že  $3^m \equiv 1 \pmod{20}$  (funguje třeba  $m = 4$ )
- Volme  $\alpha$  primitivní 20. odmocninu z 1 v  $\mathbb{F}_{3^m}$
- Jak dopadnou „skupinky“ mocnin  $\alpha$  – cyklotomické třídy?
- $\{0\}$  (odpovídá děliteli  $x - 1$ )
- $\{1, 3, 9, 7\}$
- $\{2, 6, 18, 14\}$
- $\{4, 12, 16, 8\}$
- $\{5, 15\}$
- $\{10\}$  (odpovídá  $x + 1$ )
- $\{11, 13, 19, 17\}$
- Tedy  $x^{20} - 1$  má 2 faktory st. 1, 1 faktor st. 2 a 4 faktory st. 4

# K čemu je to dobré?

- Jak se faktorizuje  $x^{20} - 1$  nad  $\mathbb{F}_3$ ?
- $n = 20$ , chci  $m$ , že  $3^m \equiv 1 \pmod{20}$  (funguje třeba  $m = 4$ )
- Volme  $\alpha$  primitivní 20. odmocninu z 1 v  $\mathbb{F}_{3^m}$
- Jak dopadnou „skupinky“ mocnin  $\alpha$  – cyklotomické třídy?
- $\{0\}$  (odpovídá děliteli  $x - 1$ )
- $\{1, 3, 9, 7\}$
- $\{2, 6, 18, 14\}$
- $\{4, 12, 16, 8\}$
- $\{5, 15\}$
- $\{10\}$  (odpovídá  $x + 1$ )
- $\{11, 13, 19, 17\}$
- Tedy  $x^{20} - 1$  má 2 faktory st. 1, 1 faktor st. 2 a 4 faktory st. 4

# K čemu je to dobré?

- Jak se faktorizuje  $x^{20} - 1$  nad  $\mathbb{F}_3$ ?
- $n = 20$ , chci  $m$ , že  $3^m \equiv 1 \pmod{20}$  (funguje třeba  $m = 4$ )
- Volme  $\alpha$  primitivní 20. odmocninu z 1 v  $\mathbb{F}_{3^m}$
- Jak dopadnou „skupinky“ mocnin  $\alpha$  – cyklotomické třídy?
- $\{0\}$  (odpovídá děliteli  $x - 1$ )
- $\{1, 3, 9, 7\}$
- $\{2, 6, 18, 14\}$
- $\{4, 12, 16, 8\}$
- $\{5, 15\}$
- $\{10\}$  (odpovídá  $x + 1$ )
- $\{11, 13, 19, 17\}$
- Tedy  $x^{20} - 1$  má 2 faktory st. 1, 1 faktor st. 2 a 4 faktory st. 4

# K čemu je to dobré?

- Jak se faktorizuje  $x^{20} - 1$  nad  $\mathbb{F}_3$ ?
- $n = 20$ , chci  $m$ , že  $3^m \equiv 1 \pmod{20}$  (funguje třeba  $m = 4$ )
- Volme  $\alpha$  primitivní 20. odmocninu z 1 v  $\mathbb{F}_{3^m}$
- Jak dopadnou „skupinky“ mocnin  $\alpha$  – cyklotomické třídy?
- $\{0\}$  (odpovídá děliteli  $x - 1$ )
- $\{1, 3, 9, 7\}$
- $\{2, 6, 18, 14\}$
- $\{4, 12, 16, 8\}$
- $\{5, 15\}$
- $\{10\}$  (odpovídá  $x + 1$ )
- $\{11, 13, 19, 17\}$
- Tedy  $x^{20} - 1$  má 2 faktory st. 1, 1 faktor st. 2 a 4 faktory st. 4

# K čemu je to dobré?

- Jak se faktorizuje  $x^{20} - 1$  nad  $\mathbb{F}_3$ ?
- $n = 20$ , chci  $m$ , že  $3^m \equiv 1 \pmod{20}$  (funguje třeba  $m = 4$ )
- Volme  $\alpha$  primitivní 20. odmocninu z 1 v  $\mathbb{F}_{3^m}$
- Jak dopadnou „skupinky“ mocnin  $\alpha$  – cyklotomické třídy?
- $\{0\}$  (odpovídá děliteli  $x - 1$ )
- $\{1, 3, 9, 7\}$
- $\{2, 6, 18, 14\}$
- $\{4, 12, 16, 8\}$
- $\{5, 15\}$
- $\{10\}$  (odpovídá  $x + 1$ )
- $\{11, 13, 19, 17\}$
- Tedy  $x^{20} - 1$  má 2 faktory st. 1, 1 faktor st. 2 a 4 faktory st. 4



# K čemu je to dobré?

- Jak se faktorizuje  $x^{20} - 1$  nad  $\mathbb{F}_3$ ?
- $n = 20$ , chci  $m$ , že  $3^m \equiv 1 \pmod{20}$  (funguje třeba  $m = 4$ )
- Volme  $\alpha$  primitivní 20. odmocninu z 1 v  $\mathbb{F}_{3^m}$
- Jak dopadnou „skupinky“ mocnin  $\alpha$  – cyklotomické třídy?
- $\{0\}$  (odpovídá děliteli  $x - 1$ )
- $\{1, 3, 9, 7\}$
- $\{2, 6, 18, 14\}$
- $\{4, 12, 16, 8\}$
- $\{5, 15\}$
- $\{10\}$  (odpovídá  $x + 1$ )
- $\{11, 13, 19, 17\}$
- Tedy  $x^{20} - 1$  má 2 faktory st. 1, 1 faktor st. 2 a 4 faktory st. 4

# K čemu je to dobré?

- Jak se faktorizuje  $x^{20} - 1$  nad  $\mathbb{F}_3$ ?
- $n = 20$ , chci  $m$ , že  $3^m \equiv 1 \pmod{20}$  (funguje třeba  $m = 4$ )
- Volme  $\alpha$  primitivní 20. odmocninu z 1 v  $\mathbb{F}_{3^m}$
- Jak dopadnou „skupinky“ mocnin  $\alpha$  – cyklotomické třídy?
- $\{0\}$  (odpovídá děliteli  $x - 1$ )
- $\{1, 3, 9, 7\}$
- $\{2, 6, 18, 14\}$
- $\{4, 12, 16, 8\}$
- $\{5, 15\}$
- $\{10\}$  (odpovídá  $x + 1$ )
- $\{11, 13, 19, 17\}$
- Tedy  $x^{20} - 1$  má 2 faktory st. 1, 1 faktor st. 2 a 4 faktory st. 4

# BCH kódy (primitivní v užším smyslu)

- Raj Bose, Dijen K. Ray-Chaudhuri, Alexis Hocquenghem
- $\text{BCH}_{q,m,\delta}$  je cyklický nad tělesem  $\mathbb{F}_q$ , délky  $q^m - 1$ , dimenze aspoň  $q^m - m(\delta - 1) - 1$  a min. vzdálenosti aspoň  $\delta$
- Zvolme  $\alpha$  generátor  $\mathbb{F}_{q^m}$
- Kódová slova jsou  $(a_0, a_1, \dots, a_{q^m-2}) \in \mathbb{F}_q$ , že polynom  $\sum_{j=0}^{q^m-2} a_j x^j$  má nuly v bodech  $\alpha^i$  pro  $i \in \{1, 2, \dots, \delta - 1\}$
- Je to vůbec cyklické?!
- Platí  $\alpha^{q^m-1} = 1$ , takže

$$\alpha(a_0 + a_1\alpha + a_2\alpha^2 + \dots + a_{q^m-1}\alpha^{q^m-2}) = a_0\alpha + a_1\alpha^2 + a_2\alpha^3 + \dots + a_{q^m-1}$$

# BCH kódy (primitivní v užším smyslu)

- Raj Bose, Dijen K. Ray-Chaudhuri, Alexis Hocquenghem
- $\text{BCH}_{q,m,\delta}$  je cyklický nad tělesem  $\mathbb{F}_q$ , délky  $q^m - 1$ , dimenze aspoň  $q^m - m(\delta - 1) - 1$  a min. vzdálenosti aspoň  $\delta$
- Zvolme  $\alpha$  generátor  $\mathbb{F}_{q^m}$
- Kódová slova jsou  $(a_0, a_1, \dots, a_{q^m-2}) \in \mathbb{F}_q$ , že polynom  $\sum_{j=0}^{q^m-2} a_j x^j$  má nuly v bodech  $\alpha^i$  pro  $i \in \{1, 2, \dots, \delta - 1\}$
- Je to vůbec cyklické?!
- Platí  $\alpha^{q^m-1} = 1$ , takže

$$\alpha(a_0 + a_1\alpha + a_2\alpha^2 + \dots + a_{q^m-1}\alpha^{q^m-2}) = a_0\alpha + a_1\alpha^2 + a_2\alpha^3 + \dots + a_{q^m-1}$$

# BCH kódy (primitivní v užším smyslu)

- Raj Bose, Dijen K. Ray-Chaudhuri, Alexis Hocquenghem
- $\text{BCH}_{q,m,\delta}$  je cyklický nad tělesem  $\mathbb{F}_q$ , délky  $q^m - 1$ , dimenze aspoň  $q^m - m(\delta - 1) - 1$  a min. vzdálenosti aspoň  $\delta$
- Zvolme  $\alpha$  generátor  $\mathbb{F}_{q^m}$
- Kódová slova jsou  $(a_0, a_1, \dots, a_{q^m-2}) \in \mathbb{F}_q$ , že polynom  $\sum_{j=0}^{q^m-2} a_j x^j$  má nuly v bodech  $\alpha^i$  pro  $i \in \{1, 2, \dots, \delta - 1\}$
- Je to vůbec cyklické?!
- Platí  $\alpha^{q^m-1} = 1$ , takže

$$\alpha(a_0 + a_1\alpha + a_2\alpha^2 + \dots + a_{q^m-1}\alpha^{q^m-2}) = a_0\alpha + a_1\alpha^2 + a_2\alpha^3 + \dots + a_{q^m-1}$$

# BCH kódy (primitivní v užším smyslu)

- Raj Bose, Dijen K. Ray-Chaudhuri, Alexis Hocquenghem
- $\text{BCH}_{q,m,\delta}$  je cyklický nad tělesem  $\mathbb{F}_q$ , délky  $q^m - 1$ , dimenze aspoň  $q^m - m(\delta - 1) - 1$  a min. vzdálenosti aspoň  $\delta$
- Zvolme  $\alpha$  generátor  $\mathbb{F}_{q^m}$
- Kódová slova jsou  $(a_0, a_1, \dots, a_{q^m-2}) \in \mathbb{F}_q$ , že polynom  $\sum_{j=0}^{q^m-2} a_j x^j$  má nuly v bodech  $\alpha^i$  pro  $i \in \{1, 2, \dots, \delta - 1\}$
- Je to vůbec cyklické?!
- Platí  $\alpha^{q^m-1} = 1$ , takže

$$\alpha(a_0 + a_1\alpha + a_2\alpha^2 + \dots + a_{q^m-1}\alpha^{q^m-2}) = a_0\alpha + a_1\alpha^2 + a_2\alpha^3 + \dots + a_{q^m-1}$$

# BCH kódy (primitivní v užším smyslu)

- Raj Bose, Dijen K. Ray-Chaudhuri, Alexis Hocquenghem
- $\text{BCH}_{q,m,\delta}$  je cyklický nad tělesem  $\mathbb{F}_q$ , délky  $q^m - 1$ , dimenze aspoň  $q^m - m(\delta - 1) - 1$  a min. vzdálenosti aspoň  $\delta$
- Zvolme  $\alpha$  generátor  $\mathbb{F}_{q^m}$
- Kódová slova jsou  $(a_0, a_1, \dots, a_{q^m-2}) \in \mathbb{F}_q$ , že polynom  $\sum_{j=0}^{q^m-2} a_j x^j$  má nuly v bodech  $\alpha^i$  pro  $i \in \{1, 2, \dots, \delta - 1\}$
- Je to vůbec cyklické?!
- Platí  $\alpha^{q^m-1} = 1$ , takže

$$\alpha(a_0 + a_1\alpha + a_2\alpha^2 + \dots + a_{q^m-1}\alpha^{q^m-2}) = a_0\alpha + a_1\alpha^2 + a_2\alpha^3 + \dots + a_{q^m-1}$$

# BCH kódy (primitivní v užším smyslu)

- Raj Bose, Dijen K. Ray-Chaudhuri, Alexis Hocquenghem
- $\text{BCH}_{q,m,\delta}$  je cyklický nad tělesem  $\mathbb{F}_q$ , délky  $q^m - 1$ , dimenze aspoň  $q^m - m(\delta - 1) - 1$  a min. vzdálenosti aspoň  $\delta$
- Zvolme  $\alpha$  generátor  $\mathbb{F}_{q^m}$
- Kódová slova jsou  $(a_0, a_1, \dots, a_{q^m-2}) \in \mathbb{F}_q$ , že polynom  $\sum_{j=0}^{q^m-2} a_j x^j$  má nuly v bodech  $\alpha^i$  pro  $i \in \{1, 2, \dots, \delta - 1\}$
- Je to vůbec cyklické?!
- Platí  $\alpha^{q^m-1} = 1$ , takže

$$\alpha(a_0 + a_1\alpha + a_2\alpha^2 + \dots + a_{q^m-1}\alpha^{q^m-2}) = a_0\alpha + a_1\alpha^2 + a_2\alpha^3 + \dots + a_{q^m-1}$$



# BCH kódy (primitivní v užším smyslu)

- Raj Bose, Dijen K. Ray-Chaudhuri, Alexis Hocquenghem
- $\text{BCH}_{q,m,\delta}$  je cyklický nad tělesem  $\mathbb{F}_q$ , délky  $q^m - 1$ , dimenze aspoň  $q^m - m(\delta - 1) - 1$  a min. vzdálenosti aspoň  $\delta$
- Zvolme  $\alpha$  generátor  $\mathbb{F}_{q^m}$
- Kódová slova jsou  $(a_0, a_1, \dots, a_{q^m-2}) \in \mathbb{F}_q$ , že polynom  $\sum_{j=0}^{q^m-2} a_j x^j$  má nuly v bodech  $\alpha^i$  pro  $i \in \{1, 2, \dots, \delta - 1\}$
- Je to vůbec cyklické?!
- Platí  $\alpha^{q^m-1} = 1$ , takže

$$\alpha(a_0 + a_1\alpha + a_2\alpha^2 + \dots + a_{q^m-1}\alpha^{q^m-2}) = a_0\alpha + a_1\alpha^2 + a_2\alpha^3 + \dots + a_{q^m-1}$$

- Délka  $q^m - 1$
- Dimenze: Máme  $q^m - 1$  dimenzi prostoru nad  $\mathbb{F}_q$  a  $\delta - 1$  lineárních podmínek. . .
- **Bacha!** Každá lineární podmínka je nad  $\mathbb{F}_{q^m}$ ; je to  $m$  lineárních podmínek na  $\mathbb{F}_q$
- Dimenze je tedy aspoň  $q^m - 1 - m(\delta - 1)$

- Délka  $q^m - 1$
- Dimenze: Máme  $q^m - 1$  dimenzi prostoru nad  $\mathbb{F}_q$  a  $\delta - 1$  lineárních podmínek. . .
- **Bacha!** Každá lineární podmínka je nad  $\mathbb{F}_{q^m}$ ; je to  $m$  lineárních podmínek na  $\mathbb{F}_q$
- Dimenze je tedy aspoň  $q^m - 1 - m(\delta - 1)$

- Délka  $q^m - 1$
- Dimenze: Máme  $q^m - 1$  dimenzi prostoru nad  $\mathbb{F}_q$  a  $\delta - 1$  lineárních podmínek. . .
- **Bacha!** Každá lineární podmínka je nad  $\mathbb{F}_{q^m}$ ; je to  $m$  lineárních podmínek na  $\mathbb{F}_q$
- Dimenze je tedy aspoň  $q^m - 1 - m(\delta - 1)$

- Délka  $q^m - 1$
- Dimenze: Máme  $q^m - 1$  dimenzi prostoru nad  $\mathbb{F}_q$  a  $\delta - 1$  lineárních podmínek. . .
- **Bacha!** Každá lineární podmínka je nad  $\mathbb{F}_{q^m}$ ; je to  $m$  lineárních podmínek na  $\mathbb{F}_q$
- Dimenze je tedy aspoň  $q^m - 1 - m(\delta - 1)$

- Délka  $q^m - 1$
- Dimenze: Máme  $q^m - 1$  dimenzi prostoru nad  $\mathbb{F}_q$  a  $\delta - 1$  lineárních podmínek. . .
- **Bacha!** Každá lineární podmínka je nad  $\mathbb{F}_{q^m}$ ; je to  $m$  lineárních podmínek na  $\mathbb{F}_q$
- Dimenze je tedy aspoň  $q^m - 1 - m(\delta - 1)$

# Minimální vzdálenost BCH kódu

- Aby měl polynom  $\delta - 1$  kořenů, musí mít stupeň aspoň  $\delta - 1 \dots$
- **Bacha!** Některé koeficienty polynomu mohou být nuly
- Je důležité, že ty kořeny nejsou náhodné
- Zvolme indexy  $\{i_1, \dots, i_{\delta-1}\}$
- Pak matice

$$\begin{pmatrix} \alpha^{i_1} & \alpha^{i_2} & \dots & \alpha^{i_{\delta-1}} \\ \alpha^{2i_1} & \alpha^{2i_2} & \dots & \alpha^{2i_{\delta-1}} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha^{(\delta-1)i_1} & \alpha^{(\delta-1)i_2} & \dots & \alpha^{(\delta-1)i_{\delta-1}} \end{pmatrix}$$

je regulární (transponuj!)

# Minimální vzdálenost BCH kódu

- Aby měl polynom  $\delta - 1$  kořenů, musí mít stupeň aspoň  $\delta - 1 \dots$
- **Bacha!** Některé koeficienty polynomu mohou být nuly
- Je důležité, že ty kořeny nejsou náhodné
- Zvolme indexy  $\{i_1, \dots, i_{\delta-1}\}$
- Pak matice

$$\begin{pmatrix} \alpha^{i_1} & \alpha^{i_2} & \dots & \alpha^{i_{\delta-1}} \\ \alpha^{2i_1} & \alpha^{2i_2} & \dots & \alpha^{2i_{\delta-1}} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha^{(\delta-1)i_1} & \alpha^{(\delta-1)i_2} & \dots & \alpha^{(\delta-1)i_{\delta-1}} \end{pmatrix}$$

je regulární (transponuj!)



# Minimální vzdálenost BCH kódu

- Aby měl polynom  $\delta - 1$  kořenů, musí mít stupeň aspoň  $\delta - 1 \dots$
- **Bacha!** Některé koeficienty polynomu mohou být nuly
- Je důležité, že ty kořeny nejsou náhodné
- Zvolme indexy  $\{i_1, \dots, i_{\delta-1}\}$
- Pak matice

$$\begin{pmatrix} \alpha^{i_1} & \alpha^{i_2} & \dots & \alpha^{i_{\delta-1}} \\ \alpha^{2i_1} & \alpha^{2i_2} & \dots & \alpha^{2i_{\delta-1}} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha^{(\delta-1)i_1} & \alpha^{(\delta-1)i_2} & \dots & \alpha^{(\delta-1)i_{\delta-1}} \end{pmatrix}$$

je regulární (transponuj!)

# Minimální vzdálenost BCH kódu

- Aby měl polynom  $\delta - 1$  kořenů, musí mít stupeň aspoň  $\delta - 1 \dots$
- **Bacha!** Některé koeficienty polynomu mohou být nuly
- Je důležité, že ty kořeny nejsou náhodné
- Zvolme indexy  $\{i_1, \dots, i_{\delta-1}\}$
- Pak matice

$$\begin{pmatrix} \alpha^{i_1} & \alpha^{i_2} & \dots & \alpha^{i_{\delta-1}} \\ \alpha^{2i_1} & \alpha^{2i_2} & \dots & \alpha^{2i_{\delta-1}} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha^{(\delta-1)i_1} & \alpha^{(\delta-1)i_2} & \dots & \alpha^{(\delta-1)i_{\delta-1}} \end{pmatrix}$$

je regulární (transponuj!)

# Minimální vzdálenost BCH kódu

- Aby měl polynom  $\delta - 1$  kořenů, musí mít stupeň aspoň  $\delta - 1 \dots$
- **Bacha!** Některé koeficienty polynomu mohou být nuly
- Je důležité, že ty kořeny nejsou náhodné
- Zvolme indexy  $\{i_1, \dots, i_{\delta-1}\}$
- Pak matice

$$\begin{pmatrix} \alpha^{i_1} & \alpha^{i_2} & \dots & \alpha^{i_{\delta-1}} \\ \alpha^{2i_1} & \alpha^{2i_2} & \dots & \alpha^{2i_{\delta-1}} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha^{(\delta-1)i_1} & \alpha^{(\delta-1)i_2} & \dots & \alpha^{(\delta-1)i_{\delta-1}} \end{pmatrix}$$

je regulární (transponuj!)

# Minimální vzdálenost BCH kódu

- Aby měl polynom  $\delta - 1$  kořenů, musí mít stupeň aspoň  $\delta - 1 \dots$
- **Bacha!** Některé koeficienty polynomu mohou být nuly
- Je důležité, že ty kořeny nejsou náhodné
- Zvolme indexy  $\{i_1, \dots, i_{\delta-1}\}$
- Pak matice

$$\begin{pmatrix} \alpha^{i_1} & \alpha^{i_2} & \dots & \alpha^{i_{\delta-1}} \\ \alpha^{2i_1} & \alpha^{2i_2} & \dots & \alpha^{2i_{\delta-1}} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha^{(\delta-1)i_1} & \alpha^{(\delta-1)i_2} & \dots & \alpha^{(\delta-1)i_{\delta-1}} \end{pmatrix}$$

je regulární (transponuj!)

- Skoro paritní matice BCH kódu

$$P = \begin{pmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^{n-1} \\ 1 & \alpha^2 & \alpha^4 & \dots & \alpha^{2(n-1)} \\ & & \ddots & & \\ 1 & \alpha^{\delta-1} & \alpha^{2(\delta-1)} & \dots & \alpha^{(n-1)(\delta-1)} \end{pmatrix}$$

- Vyberu si  $\delta - 1$  sloupců libovolně
- Vznikne regulární  $(\delta - 1) \times (\delta - 1)$  matice
- Tedy minimální vzdálenost je aspoň  $\delta$  (BCH nerovnost)

- Skoro paritní matice BCH kódu

$$P = \begin{pmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^{n-1} \\ 1 & \alpha^2 & \alpha^4 & \dots & \alpha^{2(n-1)} \\ & & \ddots & & \\ 1 & \alpha^{\delta-1} & \alpha^{2(\delta-1)} & \dots & \alpha^{(n-1)(\delta-1)} \end{pmatrix}$$

- Vyberu si  $\delta - 1$  sloupců libovolně
- Vznikne regulární  $(\delta - 1) \times (\delta - 1)$  matice
- Tedy minimální vzdálenost je aspoň  $\delta$  (BCH nerovnost)

- Skoro paritní matice BCH kódu

$$P = \begin{pmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^{n-1} \\ 1 & \alpha^2 & \alpha^4 & \dots & \alpha^{2(n-1)} \\ & & \ddots & & \\ 1 & \alpha^{\delta-1} & \alpha^{2(\delta-1)} & \dots & \alpha^{(n-1)(\delta-1)} \end{pmatrix}$$

- Vyberu si  $\delta - 1$  sloupců libovolně
- Vznikne regulární  $(\delta - 1) \times (\delta - 1)$  matice
- Tedy minimální vzdálenost je aspoň  $\delta$  (BCH nerovnost)

- Skoro paritní matice BCH kódu

$$P = \begin{pmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^{n-1} \\ 1 & \alpha^2 & \alpha^4 & \dots & \alpha^{2(n-1)} \\ & & \ddots & & \\ 1 & \alpha^{\delta-1} & \alpha^{2(\delta-1)} & \dots & \alpha^{(n-1)(\delta-1)} \end{pmatrix}$$

- Vyberu si  $\delta - 1$  sloupců libovolně
- Vznikne regulární  $(\delta - 1) \times (\delta - 1)$  matice
- Tedy minimální vzdálenost je aspoň  $\delta$  (BCH nerovnost)



- Skoro paritní matice BCH kódu

$$P = \begin{pmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^{n-1} \\ 1 & \alpha^2 & \alpha^4 & \dots & \alpha^{2(n-1)} \\ & & \ddots & & \\ 1 & \alpha^{\delta-1} & \alpha^{2(\delta-1)} & \dots & \alpha^{(n-1)(\delta-1)} \end{pmatrix}$$

- Vyberu si  $\delta - 1$  sloupců libovolně
- Vznikne regulární  $(\delta - 1) \times (\delta - 1)$  matice
- Tedy minimální vzdálenost je aspoň  $\delta$  (BCH nerovnost)

# BCH kódy algebraicky

- Co je generující polynom? Nejmenší polynom z  $\mathbb{F}_q[x]$  s kořeny  $\alpha, \alpha^2, \dots, \alpha^{\delta-1}$ .
- $\beta = \prod_{e \in E} (x - \alpha^e)$
- Zde  $E$  je nejmenší podmnožina  $\mathbb{Z}_{q^m-1}$  uzavřená na násobení  $q$  a obsahující  $\{1, 2, \dots, \delta - 1\}$
- Příklad:  $H_3$  je ekvivalentní  $\text{BCH}_{2,3,3}$
- $\beta = (x - \alpha)(x - \alpha^2)(x - \alpha^4)$
- Příklad: ~~Paritní kód~~ Oprava: opakovací kód délky 3 je  $\text{BCH}_{2,2,3} = \text{BCH}_{2,2,2}$
- $\beta = (x - \alpha)(x - \alpha^2) = x^2 + x + 1$

- Co je generující polynom? Nejmenší polynom z  $\mathbb{F}_q[x]$  s kořeny  $\alpha, \alpha^2, \dots, \alpha^{\delta-1}$ .
- $\beta = \prod_{e \in E} (x - \alpha^e)$
- Zde  $E$  je nejmenší podmnožina  $\mathbb{Z}_{q^m-1}$  uzavřená na násobení  $q$  a obsahující  $\{1, 2, \dots, \delta - 1\}$
- Příklad:  $H_3$  je ekvivalentní  $\text{BCH}_{2,3,3}$
- $\beta = (x - \alpha)(x - \alpha^2)(x - \alpha^4)$
- Příklad: ~~Paritní kód~~ Oprava: opakovací kód délky 3 je  $\text{BCH}_{2,2,3} = \text{BCH}_{2,2,2}$
- $\beta = (x - \alpha)(x - \alpha^2) = x^2 + x + 1$

- Co je generující polynom? Nejmenší polynom z  $\mathbb{F}_q[x]$  s kořeny  $\alpha, \alpha^2, \dots, \alpha^{\delta-1}$ .
- $\beta = \prod_{e \in E} (x - \alpha^e)$
- Zde  $E$  je nejmenší podmnožina  $\mathbb{Z}_{q^m-1}$  uzavřená na násobení  $q$  a obsahující  $\{1, 2, \dots, \delta - 1\}$
- Příklad:  $H_3$  je ekvivalentní  $\text{BCH}_{2,3,3}$
- $\beta = (x - \alpha)(x - \alpha^2)(x - \alpha^4)$
- Příklad: ~~Paritní kód~~ Oprava: opakovací kód délky 3 je  $\text{BCH}_{2,2,3} = \text{BCH}_{2,2,2}$
- $\beta = (x - \alpha)(x - \alpha^2) = x^2 + x + 1$

# BCH kódy algebraicky

- Co je generující polynom? Nejmenší polynom z  $\mathbb{F}_q[x]$  s kořeny  $\alpha, \alpha^2, \dots, \alpha^{\delta-1}$ .
- $\beta = \prod_{e \in E} (x - \alpha^e)$
- Zde  $E$  je nejmenší podmnožina  $\mathbb{Z}_{q^m-1}$  uzavřená na násobení  $q$  a obsahující  $\{1, 2, \dots, \delta - 1\}$
- Příklad:  $H_3$  je ekvivalentní  $\text{BCH}_{2,3,3}$
- $\beta = (x - \alpha)(x - \alpha^2)(x - \alpha^4)$
- Příklad: ~~Paritní kód~~ Oprava: opakovací kód délky 3 je  $\text{BCH}_{2,2,3} = \text{BCH}_{2,2,2}$
- $\beta = (x - \alpha)(x - \alpha^2) = x^2 + x + 1$

- Co je generující polynom? Nejmenší polynom z  $\mathbb{F}_q[x]$  s kořeny  $\alpha, \alpha^2, \dots, \alpha^{\delta-1}$ .
- $\beta = \prod_{e \in E} (x - \alpha^e)$
- Zde  $E$  je nejmenší podmnožina  $\mathbb{Z}_{q^m-1}$  uzavřená na násobení  $q$  a obsahující  $\{1, 2, \dots, \delta - 1\}$
- Příklad:  $H_3$  je ekvivalentní  $\text{BCH}_{2,3,3}$ 
  - $\beta = (x - \alpha)(x - \alpha^2)(x - \alpha^4)$
  - Příklad: ~~Paritní kód~~ Oprava: opakovací kód délky 3 je  $\text{BCH}_{2,2,3} = \text{BCH}_{2,2,2}$
  - $\beta = (x - \alpha)(x - \alpha^2) = x^2 + x + 1$

- Co je generující polynom? Nejmenší polynom z  $\mathbb{F}_q[x]$  s kořeny  $\alpha, \alpha^2, \dots, \alpha^{\delta-1}$ .
- $\beta = \prod_{e \in E} (x - \alpha^e)$
- Zde  $E$  je nejmenší podmnožina  $\mathbb{Z}_{q^m-1}$  uzavřená na násobení  $q$  a obsahující  $\{1, 2, \dots, \delta - 1\}$
- Příklad:  $H_3$  je ekvivalentní  $\text{BCH}_{2,3,3}$
- $\beta = (x - \alpha)(x - \alpha^2)(x - \alpha^4)$
- Příklad: ~~Paritní kód~~ Oprava: opakovací kód délky 3 je  $\text{BCH}_{2,2,3} = \text{BCH}_{2,2,2}$
- $\beta = (x - \alpha)(x - \alpha^2) = x^2 + x + 1$

- Co je generující polynom? Nejmenší polynom z  $\mathbb{F}_q[x]$  s kořeny  $\alpha, \alpha^2, \dots, \alpha^{\delta-1}$ .
- $\beta = \prod_{e \in E} (x - \alpha^e)$
- Zde  $E$  je nejmenší podmnožina  $\mathbb{Z}_{q^m-1}$  uzavřená na násobení  $q$  a obsahující  $\{1, 2, \dots, \delta - 1\}$
- Příklad:  $H_3$  je ekvivalentní  $\text{BCH}_{2,3,3}$
- $\beta = (x - \alpha)(x - \alpha^2)(x - \alpha^4)$
- Příklad: ~~Paritní kód~~ Oprava: opakovací kód délky 3 je  $\text{BCH}_{2,2,3} = \text{BCH}_{2,2,2}$
- $\beta = (x - \alpha)(x - \alpha^2) = x^2 + x + 1$



- Co je generující polynom? Nejmenší polynom z  $\mathbb{F}_q[x]$  s kořeny  $\alpha, \alpha^2, \dots, \alpha^{\delta-1}$ .
- $\beta = \prod_{e \in E} (x - \alpha^e)$
- Zde  $E$  je nejmenší podmnožina  $\mathbb{Z}_{q^m-1}$  uzavřená na násobení  $q$  a obsahující  $\{1, 2, \dots, \delta - 1\}$
- Příklad:  $H_3$  je ekvivalentní  $\text{BCH}_{2,3,3}$
- $\beta = (x - \alpha)(x - \alpha^2)(x - \alpha^4)$
- Příklad: ~~Paritní kód~~ Oprava: opakovací kód délky 3 je  $\text{BCH}_{2,2,3} = \text{BCH}_{2,2,2}$
- $\beta = (x - \alpha)(x - \alpha^2) = x^2 + x + 1$