Proudové šifry a posuvné registry s lineární zpětnou vazbou

Andrew Kozlík

KA MFF UK

Proudové šifry

- **Bloková šifra**
  Šifruje velké bloky otevřeného textu.
  - Bloky mají pevnou délku.
  - „Velké“ znamená, že je prakticky nemožné enumerovat všechny možné bloky.
  - Používá se ve spojení s operačním režimem.

- **Proudová šifra**
  Šifruje jednotlivé znaky (bity, bajty) otevřeného textu v závislosti na jejich pozici nebo předchozích znacích ŠT.
  - Příklad: Vernamova šifra.
  - Příklad: Bloková šifra v CFB, OFB nebo CTR režimu.

Šifrování proudovou šifrou

- Konečný automat generuje pseudonáhodnou posloupnost znaků $s_0, s_1, \ldots,$ kterou nazýváme *proud hesla* nebo anglicky *keystream*.
- Počáteční stav automatu určuje IV a tajný klíč.
- Inicializační vektor musí být nonce.
- Znak šifrového textu y_i vznikne kombinací znaku otevřeného textu x_i a s_i. Nejčastěji $y_i = x_i \oplus s_i$.

Synchronní a samosynchronizující proudové šifry

- Jestliže každý znak s_i je závislý jen na
  - klíči,
  - inicializačním vektoru a
  - pozici v otevřeném textu,

  říkáme, že proudová šifra je *synchronní*.
- Příklad: Bloková šifra v OFB režimu nebo CTR režimu.

- Jestliže každý znak s_i je závislý jen na
  - klíči,
  - inicializačním vektoru a
  - předchozích N znacích šifrového textu,

  říkáme, že šifra je *samosynchronizující* neboli *asynchronní*.
- Příklad: Bloková šifra v CFB režimu.

Resynchronizace

V některých synchronních proudových šifrách se periodicky provádí tzv. *resynchronizace*.

- Automat se reinicializuje s původním klíčem a novým IV.
- Toto má i bezpečnostní důvody:
  - Z dlouhého šifrového textu by útočník mohl snáze odhalit vnitřní stav automatu.
  - Při odhalení vnitřního stavu automatu je kompromitováno menší množství otevřeného textu.

Výhody proudových šifer oproti blokovým

- Nevyžadují padding.
- Nevyžadují ukládání do vyrovnávací paměti, tj. čekání na naplnění bloku.
- Bývají rychlejší a mívají nižší hardwarovou složitost (levnější implementaci).
- U synchronních proudových šifer navíc:
  - Nedochází k šíření přenosových chyb.
  - Lze předpočítat proud hesla.
- U samosynchronizujících proudových šifer navíc:
  - Šifra se sama vypořádá s výpadkem části šifrového textu.

Výhody blokových šifer oproti proudovým

- Mají komplexnější využití:
  - Zajištění autentizace a integrity (např. CMAC).
  - Efektivní šifrování pevného disku (např. XTS).
- Při použití ve vhodném režimu bývají odolnější proti implementačním chybám jako opakované užití stejného IV.
- Při použití ve vhodném režimu trpí menší mírou tvárnosti.
- Dochází k lepší difuzi znaků OT do ŠT, tj. jeden znak OT ovlivňuje všechny znaky ŠT v rámci bloku.
  Bývají proto považovány za bezpečnější.

Posuvné registry s lineární zpětnou vazbou

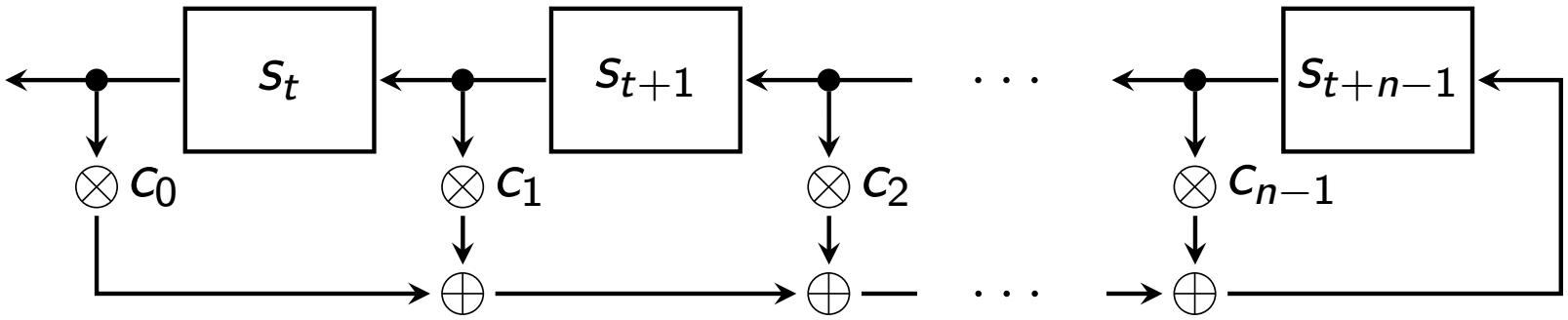
Anglicky: linear feedback shift register (LFSR)

Definice

LFSR délky n nad tělesem $\mathbb{F}_q$ je konečný automat produkující posloupnost $\{s_i\}_{i=0}^{\infty}$ prvků z $\mathbb{F}_q$, která splňuje rekurentní vztah

$$s_{t+n} = \sum_{i=0}^{n-1} c_i s_{t+i}, \qquad \forall t \geq 0.$$

Vektor $(s_0, \ldots, s_{n-1})$ nazýváme *počáteční stav* registru a $(c_0, \ldots, c_{n-1})$ nazýváme *koeficienty* registru.



Cvičení

- Mějme LFSR nad $\mathbb{F}_2$ s koeficienty $(1, 0, 1, 1)$. Určete výstup, je-li počáteční stav
  1. $(1, 0, 0, 0)$,
  2. $(0, 0, 1, 0)$,
  3. $(1, 1, 1, 1)$.
- Mějme LFSR nad $\mathbb{F}_2$ s koeficienty $(1, 1, 0, 0)$ a počátečním stavem $(1, 0, 0, 0)$. Určete výstup.
- Dá se posloupnost $\overline{11011}$ vytvořit pomocí LFSR délky 2?
- Dá se posloupnost $\overline{1000110}$ vytvořit pomocí LFSR délky 3?
- Dá se posloupnost $\overline{0010111}$ vytvořit pomocí LFSR délky 3?

Periodicita

- LFSR délky n nad $\mathbb{F}_q$ má celkem q^n možných stavů.
- Pokud $c_0 \neq 0$, pak je výstup LFSR periodický.
  Každý stav $(s_{t+1}, \ldots, s_{t+n})$ má totiž jednoznačně určeného předchůdce $(s_t, \ldots, s_{t+n-1})$, kde

$$s_t = \frac{1}{c_0}\left(s_{t+n} - \sum_{i=1}^{n-1} c_i s_{t+i}\right).$$

- Pokud $c_0 = 0$, pak je výstup skoro periodický, tj. až na několik prvních členů posloupnosti, které se vyplaví z počátečního stavu registru.
- LFSR s počátečním stavem $(0, 0, \ldots, 0)$ zůstane konstantní.
- Nejdelší možná perioda LFSR délky n je $q^n - 1$.

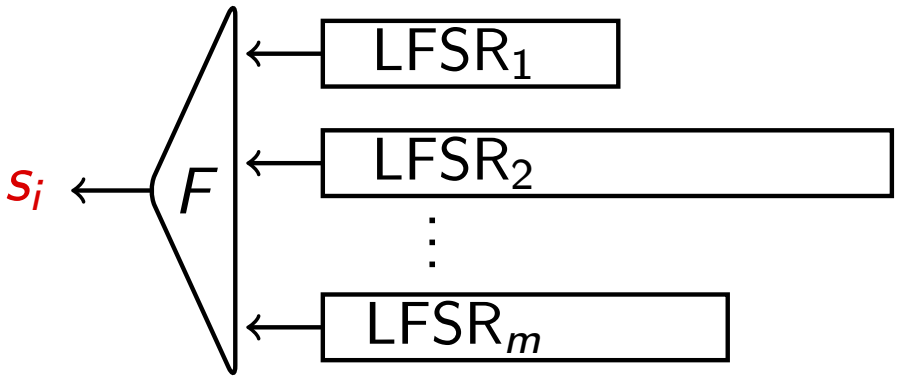
LFSR a proudové šifry

- Samotný LFSR není dobrou proudovou šifrou.
- Kdyby útočník znal zpětnou vazbu LFSR a určil n znaků proudu hesla, pak lze dopočítat celý proud hesla.
- Útočník, který by neznal zpětnou vazbu, ji může určit z proudu hesla $(s_0, \ldots, s_{2n-1})$ délky $2n$ vyřešením soustavy:

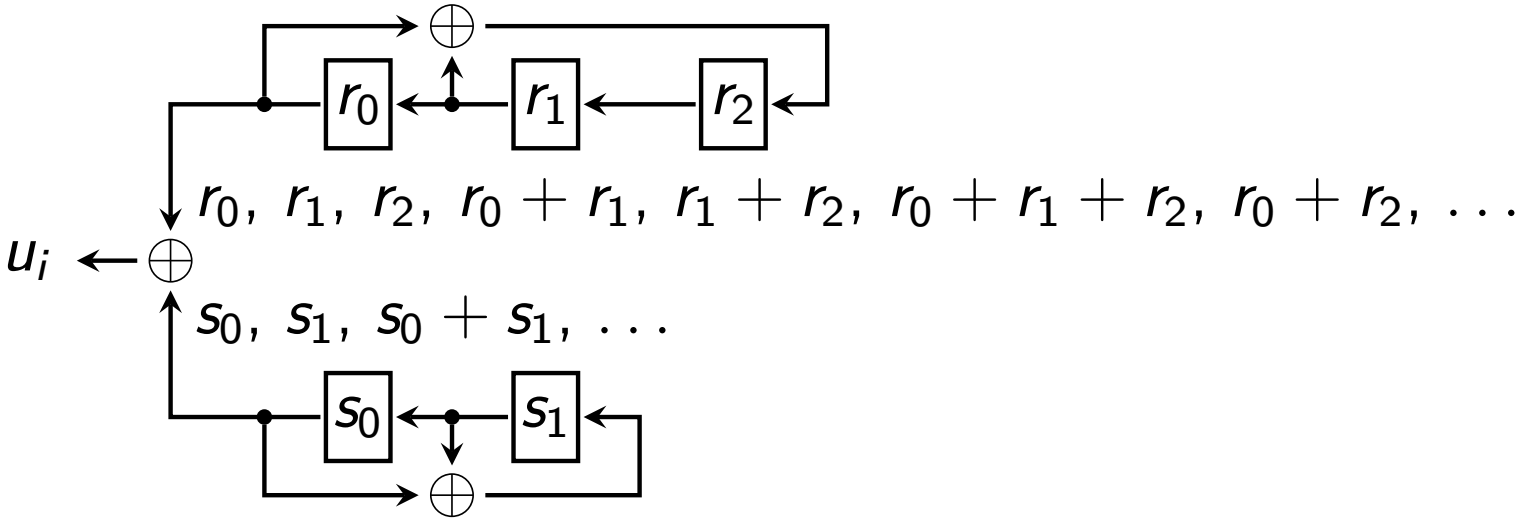
$$\begin{pmatrix} s_0 & s_1 & \ldots & s_{n-1} \\ s_1 & s_2 & \ldots & s_n \\ \vdots & \vdots & \ddots & \vdots \\ s_{n-1} & s_n & \ldots & s_{2n-2} \end{pmatrix} \begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_{n-1} \end{pmatrix} = \begin{pmatrix} s_n \\ s_{n+1} \\ \vdots \\ s_{2n-1} \end{pmatrix}.$$

LFSR a proudové šifry

Řešení: Můžeme kombinovat výstup m LFSR pomocí booleovské funkce $F : \{0,1\}^m \to \{0,1\}$:



Kombinace výstupu několika LFSR – příklad

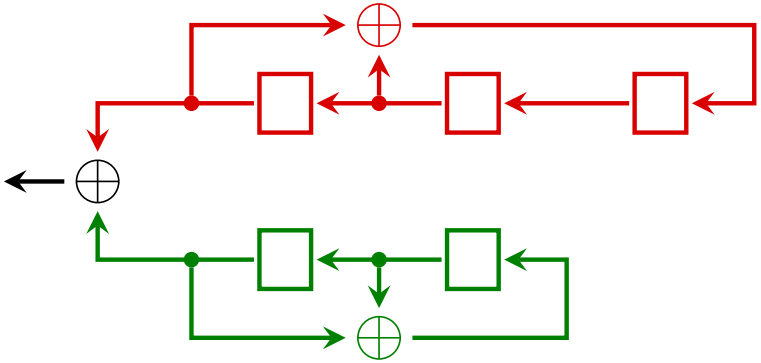


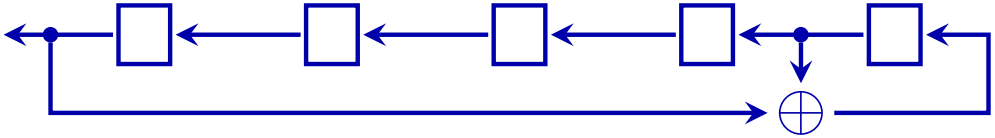
K odhalení vnitřního stavu stačí 5 prvků výstupu:

$$\begin{array}{c} \begin{array}{ccccc} r_0 & r_1 & r_2 & s_0 & s_1 \end{array} \\ \left(\begin{array}{ccc|cc} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \end{array}\right) \end{array} \begin{pmatrix} r_0 \\ r_1 \\ r_2 \\ s_0 \\ s_1 \end{pmatrix} = \begin{pmatrix} u_0 \\ u_1 \\ u_2 \\ u_3 \\ u_4 \end{pmatrix}$$

Kombinace výstupu několika LFSR

- Kombinační generátor lze také převést na jediný LFSR.
- Následující zařízení generují stejné posloupnosti při vhodném nastavení počátečních stavů:





Kombinace výstupu několika LFSR

- *Složitost* lineární rekurentní posloupnosti definujeme jako délku nejkratšího LFSR, kterým ji lze generovat.
- Použijeme-li kombinační funkci, která je lineární, pak složitost výstupní posloupnosti je nejvýše součtem složitostí vstupních posloupností.
- Základní požadavky na kombinační funkci:
  - nelinearita,
  - vysoký stupeň v algebraické normální formě,
  - vyváženost (výstup 0 a 1 v poměru 50:50).

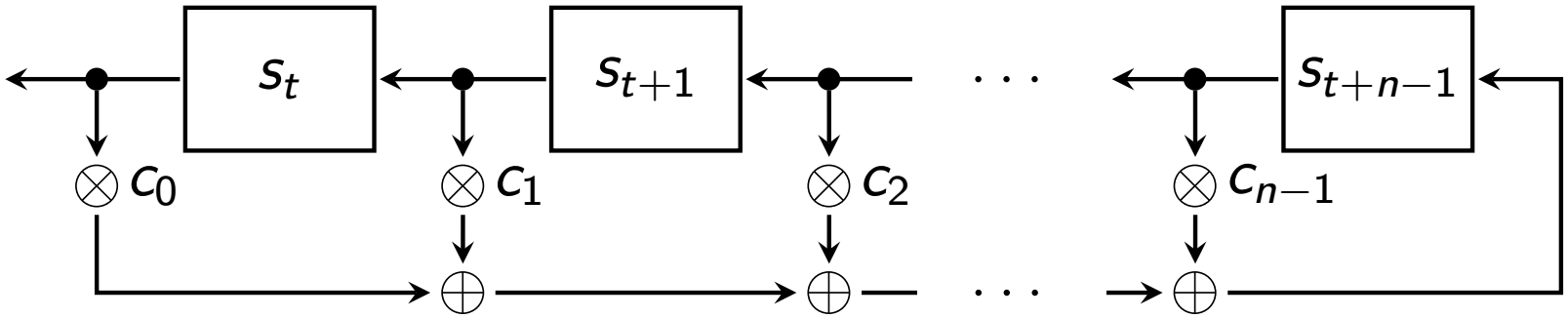
Příklad (Geffeho generátor)

Využívá 3 LFSR a funkci $F(x_1, x_2, x_3) = x_1x_2 \oplus x_2x_3 \oplus x_3$. Je však zranitelný korelačním útokem, viz cvičení.

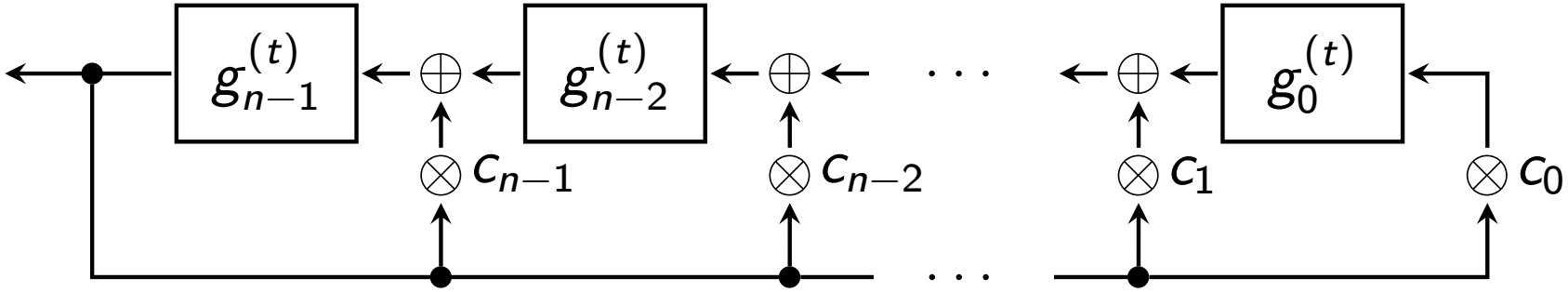
x_1	x_2	x_3	$F(x_1, x_2, x_3)$
0	0	0	0
0	0	1	1
0	1	0	0
0	1	1	0
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	1

Dvě reprezentace LFSR

Fibonacciho reprezentace LFSR:



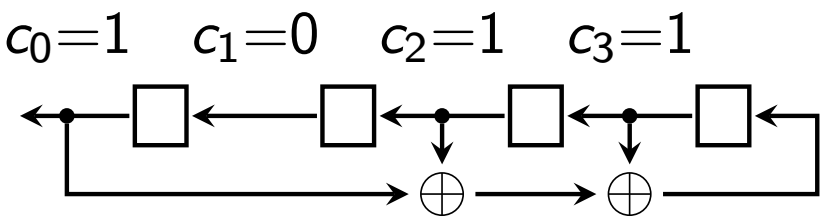
Galoisova reprezentace LFSR:



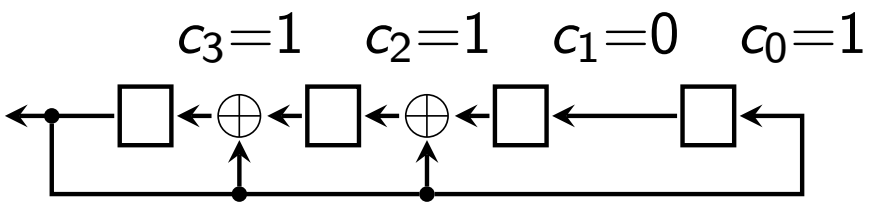
- Obě reprezentace vytvářejí stejnou posloupnost ($g_{n-1}^{(t)} = s_t$).
- Vnitřní stavy jsou však odlišné.

Porovnání vývoje vnitřního stavu

Fibonacciho reprezentace



Galoisova reprezentace



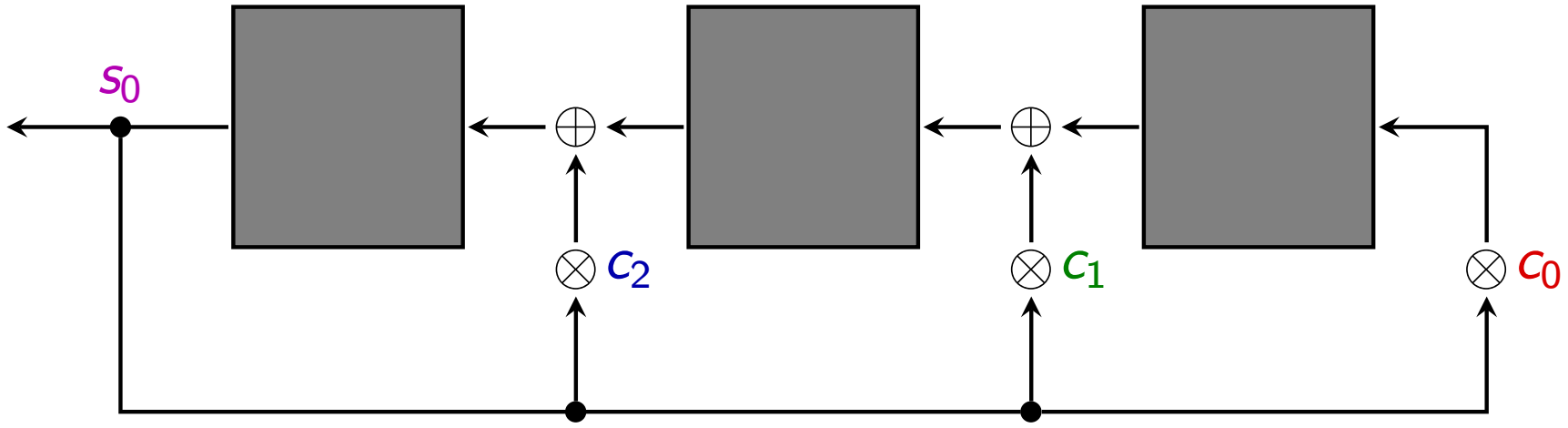
0	0	0	1	t=0	0	0	0	1
0	0	1	1	t=1	0	0	1	0
0	1	1	0	t=2	0	1	0	0
1	1	0	1	t=3	1	0	0	0
1	0	1	0	t=4	1	1	0	1
0	1	0	0	t=5	0	1	1	1
1	0	0	0	t=6	1	1	1	0
0	0	0	1	t=7	0	0	0	1

Galoisova reprezentace LFSR

Výstupní posloupnost LFSR $\{s_t\}_{t=0}^{\infty}$ má splňovat

$$s_{t+n} = \sum_{i=0}^{n-1} c_i s_{t+i}.$$

Vidíme, že vnitřní stav Galoisovy reprezentace sestává z částečných součtů této sumy:

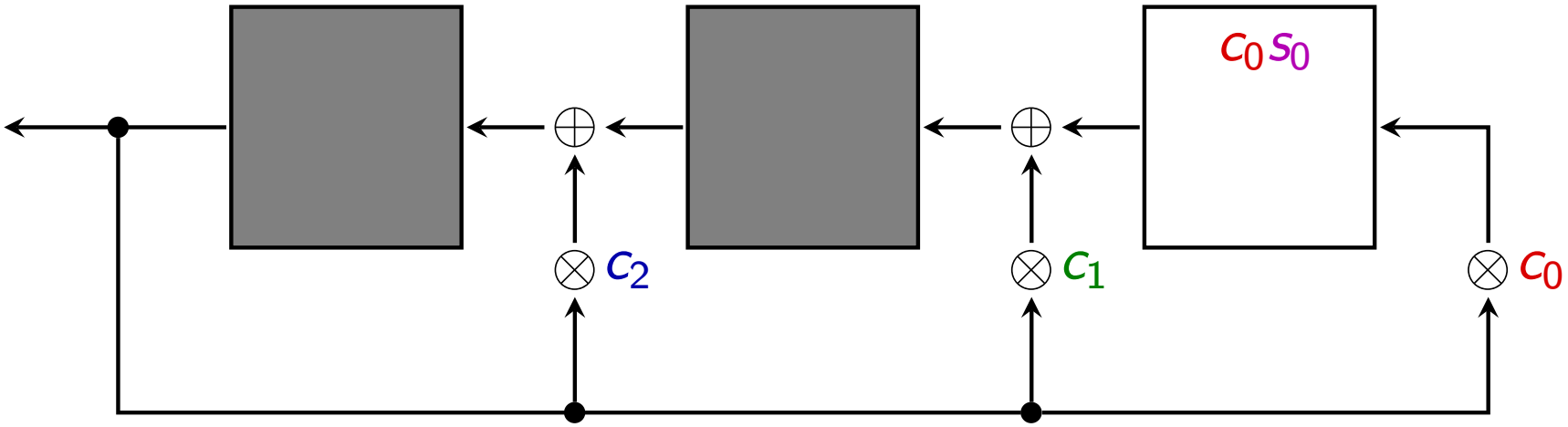


Galoisova reprezentace LFSR

Výstupní posloupnost LFSR $\{s_t\}_{t=0}^{\infty}$ má splňovat

$$s_{t+n} = \sum_{i=0}^{n-1} c_i s_{t+i}.$$

Vidíme, že vnitřní stav Galoisovy reprezentace sestává z částečných součtů této sumy:

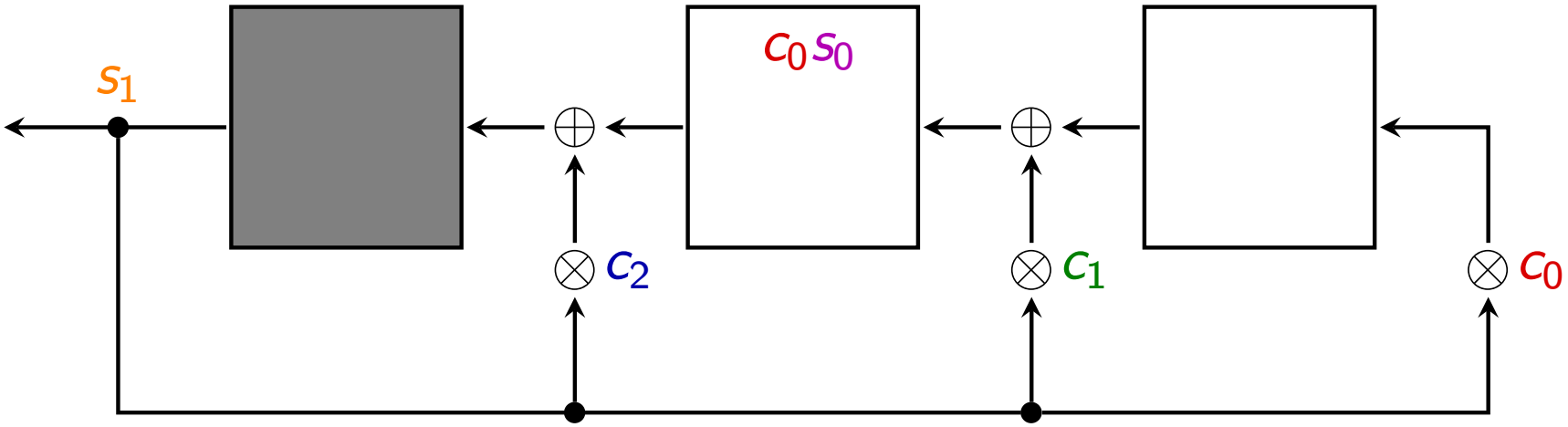


Galoisova reprezentace LFSR

Výstupní posloupnost LFSR $\{s_t\}_{t=0}^{\infty}$ má splňovat

$$s_{t+n} = \sum_{i=0}^{n-1} c_i s_{t+i}.$$

Vidíme, že vnitřní stav Galoisovy reprezentace sestává z částečných součtů této sumy:

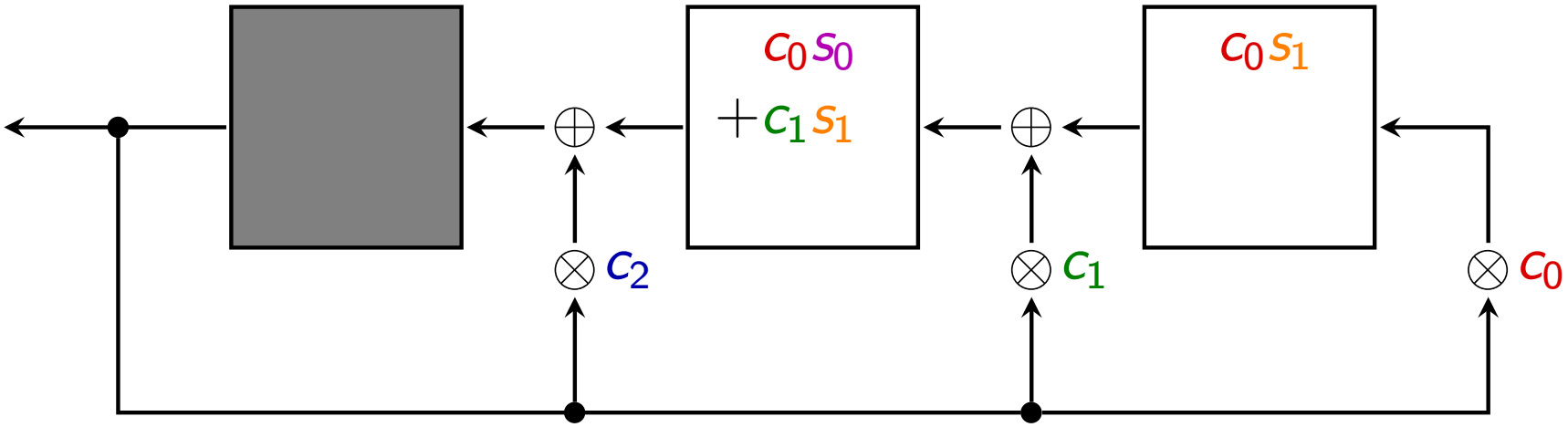


Galoisova reprezentace LFSR

Výstupní posloupnost LFSR $\{s_t\}_{t=0}^{\infty}$ má splňovat

$$s_{t+n} = \sum_{i=0}^{n-1} c_i s_{t+i}.$$

Vidíme, že vnitřní stav Galoisovy reprezentace sestává z částečných součtů této sumy:

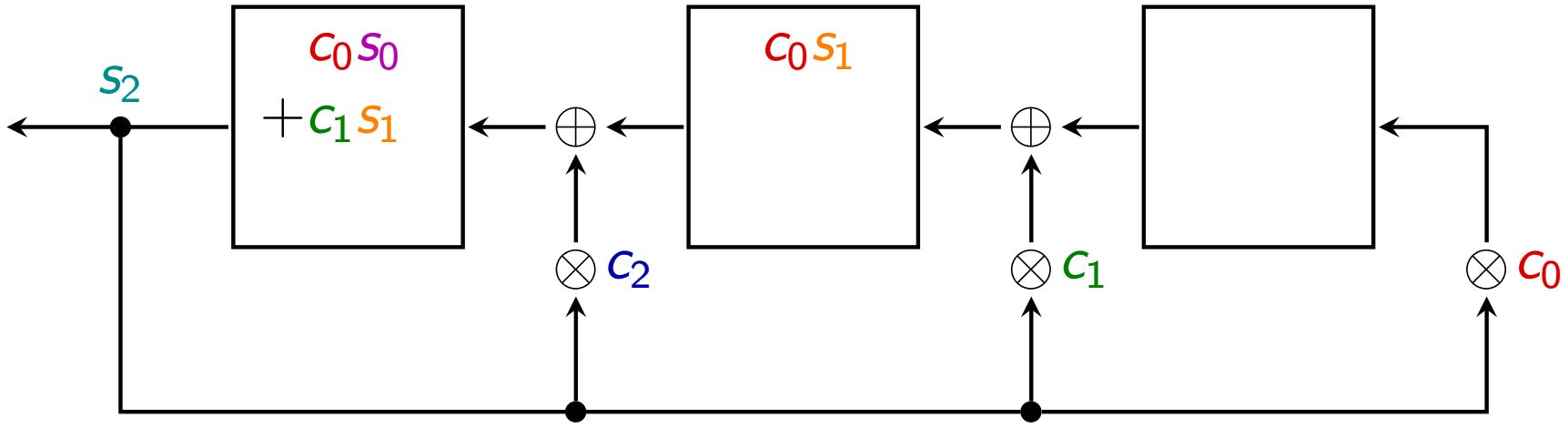


Galoisova reprezentace LFSR

Výstupní posloupnost LFSR $\{s_t\}_{t=0}^{\infty}$ má splňovat

$$s_{t+n} = \sum_{i=0}^{n-1} c_i s_{t+i}.$$

Vidíme, že vnitřní stav Galoisovy reprezentace sestává z částečných součtů této sumy:

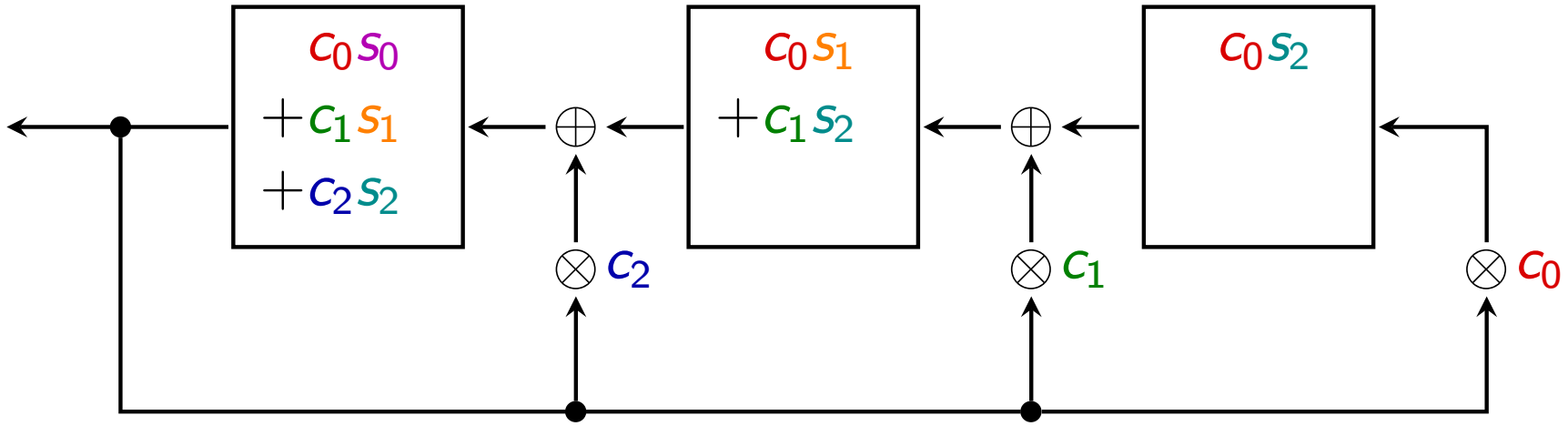


Galoisova reprezentace LFSR

Výstupní posloupnost LFSR $\{s_t\}_{t=0}^{\infty}$ má splňovat

$$s_{t+n} = \sum_{i=0}^{n-1} c_i s_{t+i}.$$

Vidíme, že vnitřní stav Galoisovy reprezentace sestává z částečných součtů této sumy:

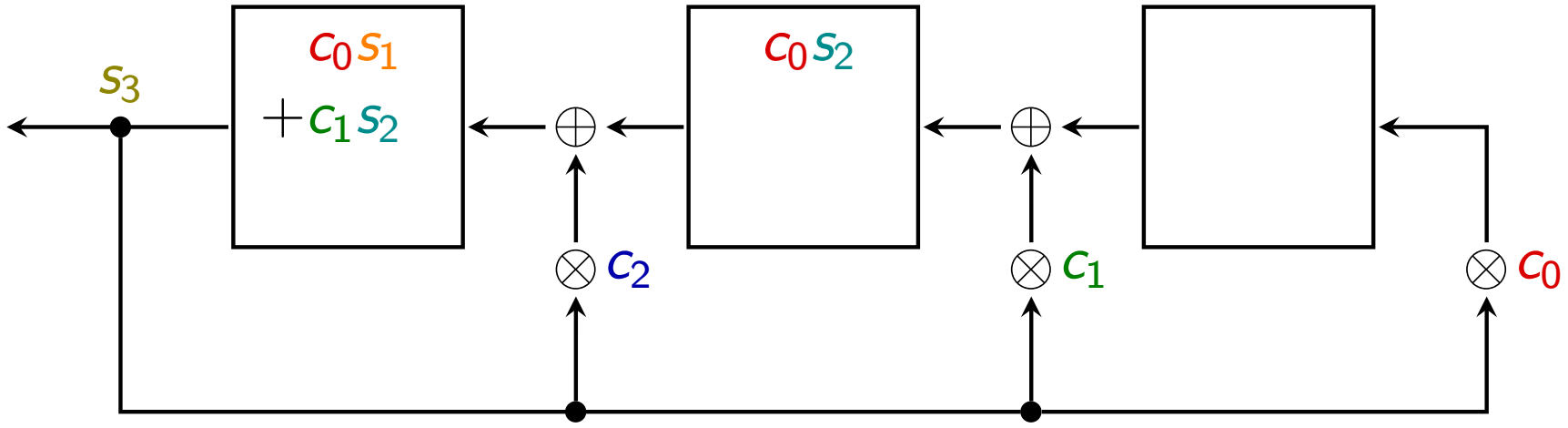


Galoisova reprezentace LFSR

Výstupní posloupnost LFSR $\{s_t\}_{t=0}^{\infty}$ má splňovat

$$s_{t+n} = \sum_{i=0}^{n-1} c_i s_{t+i}.$$

Vidíme, že vnitřní stav Galoisovy reprezentace sestává z částečných součtů této sumy:

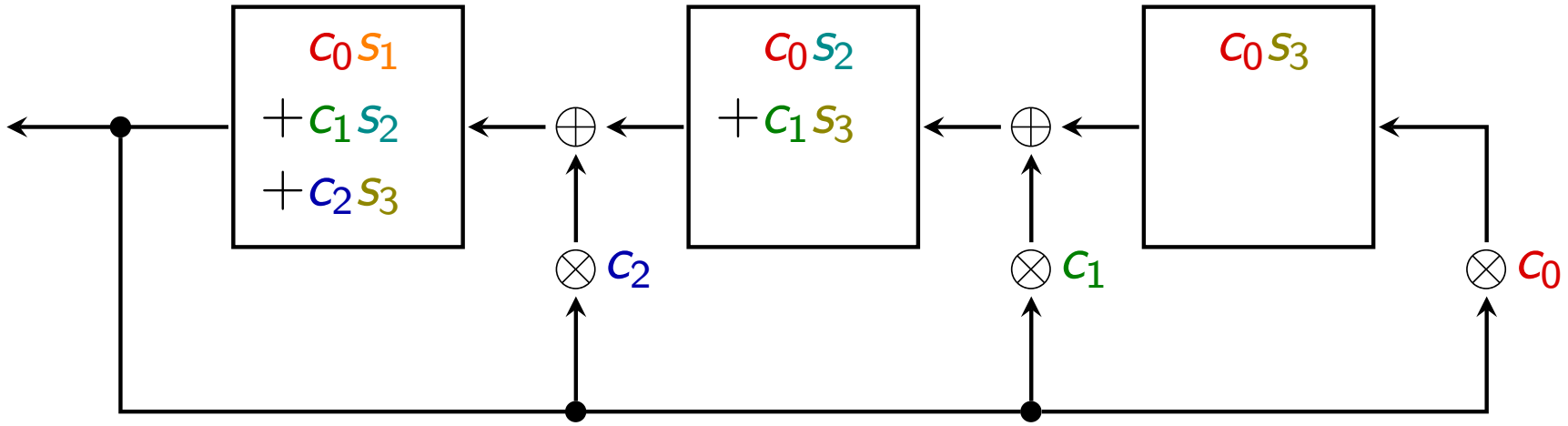


Galoisova reprezentace LFSR

Výstupní posloupnost LFSR $\{s_t\}_{t=0}^{\infty}$ má splňovat

$$s_{t+n} = \sum_{i=0}^{n-1} c_i s_{t+i}.$$

Vidíme, že vnitřní stav Galoisovy reprezentace sestává z částečných součtů této sumy:

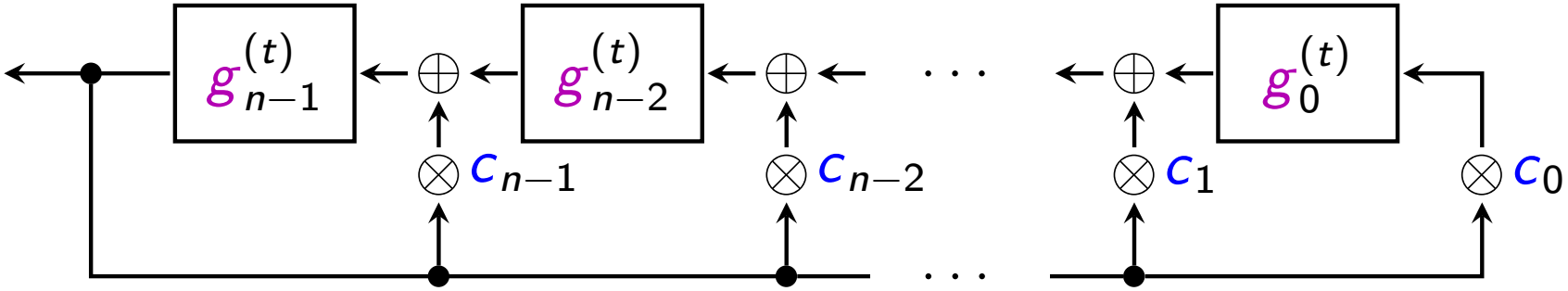


Konverze vnitřního stavu

- Galois $\rightarrow$ Fibonacci
  Galoisovou reprezentací vygenerujeme výstup $s_0, \ldots, s_{n-1}$. Hotovo.

- Fibonacci $\rightarrow$ Galois
  Vezmeme $s_0, \ldots, s_{n-1}$ a pustíme Galoisovu reprezentaci ve zpětném chodu. Viz cvičení.

Galoisova reprezentace a polynomy



- Definujeme
  - charakteristický polynom LFSR s koeficienty $c_0, \ldots, c_{n-1}$
  - polynom vnitřního stavu Galoisovy reprezentace v čase t

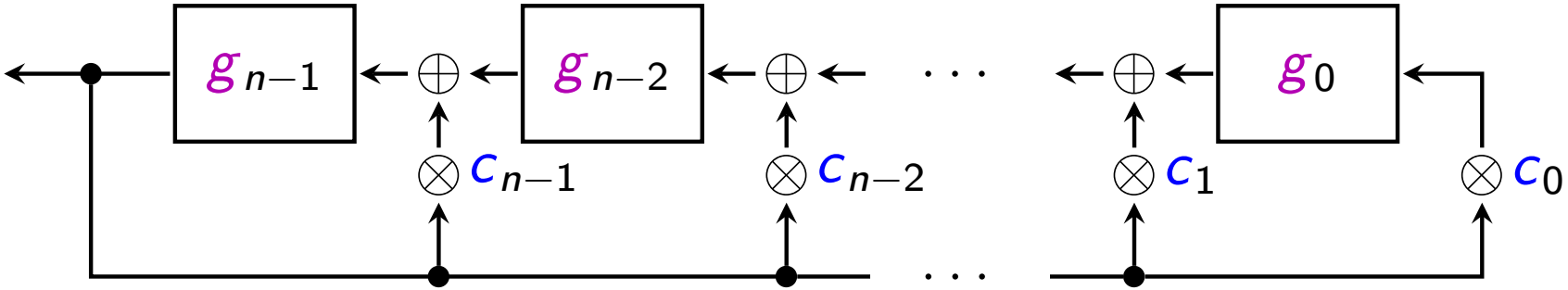
$$f(x) = x^n - \sum_{i=0}^{n-1} c_i x^i, \qquad g^{(t)}(x) = \sum_{i=0}^{n-1} g_i^{(t)} x^i.$$

- Potom

$$g^{(t+1)}(x) = x \cdot g^{(t)}(x) \bmod f(x).$$

  - Operace $x \cdot g^{(t)}(x)$ posune koeficienty stavu nahoru.
  - Operace mod pak odečte $g_{n-1}^{(t)} \cdot f(x)$ od posunutého stavu.

Galoisova reprezentace a polynomy



$$x \cdot g(x) \bmod f(x) = x \cdot g(x) - g_{n-1} \cdot f(x)$$

$$= x \left(\sum_{i=0}^{n-1} g_i x^i \right) - g_{n-1} \left(x^n - \sum_{i=0}^{n-1} c_i x^i \right)$$

$$= g_{n-1} c_0 + \sum_{i=1}^{n-1} (g_{i-1} + g_{n-1} c_i) x^i$$

Primitivní charakteristický polynom

Definice

Říkáme, že polynom $f \in \mathbb{F}_q[x]$ stupně n je *primitivní*, jestliže

- monický, tj. vedoucí koeficient je 1,
- je ireducibilní a
- nějaký jeho kořen je primitivní prvek $\mathbb{F}_{q^n}$, tj. generuje $\mathbb{F}_{q^n}^*$.

Tvrzení

Nechť f je charakteristický polynom LFSR délky n nad $\mathbb{F}_q$. Jestliže je f primitivní, pak každý nenulový počáteční stav generuje posloupnost s periodou $q^n - 1$.

Důkaz.

- Ukážeme, že perioda posloupnosti stavů $g^{(t)}(x)$ je $q^n - 1$.
  - Perioda výstupu pak musí být stejná, protože pro libovolné t lze z $s_t, \ldots, s_{t+n-1}$ jednoznačně určit $g^{(t)}(x)$.
- Víme, že $g^{(t)}(x) = (g^{(0)}(x) \cdot x^t) \bmod f(x)$.
- Nechť $P \in \mathbb{N}$ je nejmenší kladné číslo takové, že

$$g^{(0)}(x) \cdot x^P \equiv g^{(0)}(x) \pmod{f(x)}.$$

- Čili $f(x) \mid g^{(0)}(x) \cdot x^P - g^{(0)}(x) = g^{(0)}(x) \cdot (x^P - 1)$.
- Jelikož $\mathbb{F}_q[x]$ je Gaussův obor a f je ireducibilní, je f prvočinitel. Tedy $f(x)$ dělí buď $g^{(0)}(x)$ nebo $(x^P - 1)$.
- Zároveň víme, že $0 < \deg g^{(0)} < \deg f$, takže varianta, že $f(x) \mid g^{(0)}(x)$, je vyloučena a platí $f(x) \mid (x^P - 1)$.

Důkaz (pokračování).

- Nyní víme, že $x^P - 1 = f(x) \cdot h(x)$ pro nějaké $h \in \mathbb{F}_q[x]$.
- Nechť α generuje $\mathbb{F}_{q^n}^*$ a je kořenem polynomu f.
- Pak α je také kořenem $x^P - 1$, čili $\alpha^P = 1$.
- P je tedy násobek řádu prvku α, který je roven $q^n - 1$.
- Ale perioda P je nejvýše $q^n - 1$. Jedinou možností je proto $P = q^n - 1$. $\square$