1 Popis pole F_{2^m} pomocí Optimální normální báze

1.1 Normální báze

Normální báze pro F_{2^m} je množina $B = \{\Theta, \Theta^2, \Theta^{2^2}, ..., \Theta^{2^{m-1}}\}$ s vlastností, že žádná z podmnožin *B* nedá v součtu 0. (V jazyce lineární algebry to znamená, že prvky *B* jsou lineárně nezávislé). Normální báze pro F_{2^m} existuje pro každé kladné celé číslo *m*. Reprezentace F_{2^m} prostřednictvím normální báze *B* je interpretací řetězce bitů ($a_0 a_1 a_2 \ldots a_{m-1}$) jako prvku $a_0\Theta + a_1\Theta^2 + a_2\Theta^{2^2} + ... + a_{m-1}\Theta^{2^{m-1}}$. Všechny prvky normální báze *B* vyhovují stejnému nerozložitelnému polynomu *p*(*t*). Tomuto polynomu se říká *polynom pole* pro bázi. Nerozložitelnému binárnímu polynomu se říká *normální polynom*, pokud je tento polynom polynomem pole pro normální bázi.

1.2 Gaussova normální báze

Výhodnost reprezentace pomocí normální báze je v tom, že výpočet druhé mocniny se dá realizovat velmi efektivně. Na druhé straně ale násobení různých prvků může být velmi nepřehledné. Z tohoto důvodu se běžně využívá třída normálních bází, kterým se říká Gaussova normální báze a pro které je násobení nejen jednodušší, ale i efektivnější.

Gaussovy normální báze pro F_{2^m} existují vždy, když *m* není dělitelné osmi. Gaussova normální báze zahrnují také optimální normální báze, ve kterých je násobení ze všech možných normálních bází nejefektivnější.

Typ Gaussovy normální báze je celé kladné číslo, které je mírou složitosti operace násobení v dané bázi. Čím je typ menší, tím je násobení jednodušší. Pro dané *m* a *T* může mít pole F_{2^m} nejvýše jednu Gaussovu normální bázi typu *T*. Hovoříme o určitém typu *T* Gaussovy normální báze nad F_{2^m}. Gaussovy normální báze Typu 1 a 2 mají nejefektivnější pravidla pro násobení ze všech normálních bází. Proto se jim říká optimální normální báze. Gaussovy normální báze Typu 1 se nazývají optimální normální báze Typ I a Gaussovy normální báze Typu 2 se nazývají optimální normální báze Typ II.

1.3 Testování Gaussových normálních bází

Pokud *m* > 1 a není dělitelné osmi, pak následující algoritmus testuje existenci Gaussovy normální báze pro F_{2^m} daného typu.

Vstup: Číslo *m* > 1a nedělitelné osmi; kladné číslo *T*
Výstup: Pokud existuje Gaussova normální báze typu *T* pro F_{2^m}, tak výstup „True“; jinak“False“

1. Dosadit $p \leftarrow Tm + 1$
2. Pokud p není prvočíslo, tak výstup „False“ a stop.
3. Spočítat řád k čísla 2 mod p.
4. Dosadit $h \leftarrow Tm / k$.
5. Spočítat d:=gcd(h,m) pomocí Euklidova algoritmu
6. Když d = 1, tak výstup „True“; jinak „False.

Příklad: Nechť m = 4 a T = 3. Potom p = 13 a 2 má řád k = modulo 13. Protože h = 1 se chová k m = 4 jako relativní prvočíslo, tak pro F_{2^4} existuje normální Gaussova báze Typ 3.

1.4 Shrnutí

Optimální normální báze poskytuje možnost alternativní definice násobení mezi prvky pole F_{2^m}. Přestože násobení při použití ONB je méně názorné než násobení při popisu pomocí polynomů, jeho použití v praxi podstatně zvyšuje efektivitu výpočtů.

- ONB je speciální podmnožina Gaussovských normálních bází
- Existují různé typy GNB.
- Typ báze je celé kladné číslo vyjadřující míru složitosti násobení s ohledem k dané bázi.
- Čím je číslo menší, tím je násobení za použití dané báze efektivnější.
- Nejefektivnější implementace násobení existuje pro gaussovské normální báze Typu I a II, které se proto nazývají Optimální normální báze (ONB).
- Pro dané m a T má pole F_{2^m} maximálně jednu GNB typu T
- Typ ONB (I nebo II) pro jednotlivé hodnoty m je určen v doporučení IEEE P1363 v dodatku A.8.
- Násobení pomocí ONB má dvě fáze. Nejprve je nutné určit násobící matici, a poté je možné provést vlastní násobení.

2 Příprava k násobení - určení násobící matice

Existují dva druhy ONB - Typ I a Typ II.

1. Pokud F_{2^m} je ONB Typ I pak nerozložitelný polynom f(x) musí mít tvar:

$$f(x) = x^m + x^{m-1} + ... + x^2 + x + 1.$$

Pokud F_{2^m} je ONB Typ II pak nerozložitelný polynom f(x) vypočteme jako $f(x) = f_m(x)$ za použití následující rekurzivního vztahu:

$$f_0(x) = 1$$
$$f_1(x) = x + 1 \text{ f1(x)}$$
$$f_{i+1}(x) = xf_i(x) + f_{i-1}(x), \;\; i = 1,...m$$

V každém kroku jsou koeficienty polynomu $f_i(x)$ podrobeny dělení modulo 2; odtud plyne, že $f(x)$ je polynom stupně m s koeficienty v F_2.

Množina polynomů $\{x, x^{2^1}, x^{2^2}, ..., x^{2^{m-1}}\}$ tvoří základ pole F_{2^m} nad F_2 nazývaný normální báze.

2. Sestavíme matici A o velikosti m $\times$ m.
   Řádky a sloupce matice jsou indexovány od *0* do *m-1*. Její *i*-tý řádek tvoří řetězec odpovídající polynomu $x^{2^i} \bmod f(x)$. Prvky matice A jsou prvky F_2.
3. Určíme matici A-1 , která je inverzní k matici A nad F_2.
   Sestrojíme matici T' o rozměrech m $\times$ m , u které *i*-tý řádek bude odpovídat polynomu $x \cdot x^{2^i} \bmod f(x)$. Poté spočteme matici T = T'A-1 nad F_2.
   Určíme výsledné členy násobící matice L_{ij}, pro i, j = 0 ... m – 1 je $L_{ij} = T_{(j-i,-i)}$.
   Prvek $T_{(g,h)}$ znamená (g,h)-tou část z matice T s indexy vydělenými modulo 2.
   Každý prvek L_{ij} je v F_2.
   Může nastat takový případ, že $L_{0j} = 1$ pro právě jedno j, $0 \le j \le m\text{-}1$, pak pro každé i $0 \le i \le m\text{-}1$ existuje $L_{ij}=1$ pro právě dvě rozdílné j, $0 \le j \le m\text{-}1$. Proto pouze $2m-1$ z celkového množství m^2 prvků matice T mají hodnotu 1, zbytek je nulový. Laicky řečeno v prvním sloupci bude jen jedna jednička, ve všech ostatních budou dvě.
   Tento „nedostatek jedniček“ je hlavní důvod proč se tato normální báze nazývá optimální normální báze.

3 Vlastní násobení v poli F_2^m s pomocí ONB

Máme dánu násobící matici L pro pole F_{2^m}, prvky pole $a = (a_0 a_1 ... a_{m-1})$ a $b = (b_0 b_1 ... b_{m-1})$
.
Pro *k=0,…m-1* uděláme následující kroky:

1. $c_k = a \cdot L \cdot b^{tr}$, b_{tr}- transponovaný vektor b.
2. vektor *a* rotujeme doleva o jednu pozici $(a_0 a_1 a_2 ... a_{m-1}) \rightarrow (a_1 a_2 ... a_{m-1} a_0)$
3. vektor b rotujeme doleva o jednu pozici $(b_0 b_1 b_2 ... b_{m-1}) \rightarrow (b_1 b_2 ... b_{m-1} b_0)$
4. zvýšíme *k* o jedničku
5. skok zpět k bodu 1

Výsledkem násobení je vektor $c = (c_0 c_1 ... c_{m-1}) = (a_0 a_1 ... a_{m-1}) \cdot (b_0 b_1 ... b_{m-1})$

4 Ukázka násobení v F_{2^4} s ONB

Prvky pole F_{2^4} jsou binární řetězce o délce 4.

4.1 Určení násobící matice

1. Pole je popsáno **ONB Typ I**; tedy $f(x) = x^4 + x^3 + x^2 + x + 1$.
   Normální báze pole F_{2^4} nad F_2 má tvar množiny polynomů $\{x, x^2, x^4, x^8\}$
2. Řádky matice A jsou sestrojeny následovně:

Řádek 0: $x \cdot \mathrm{mod}\ f(x)$ = x = (0010)
Řádek 1: $x^2 \cdot \mathrm{mod}\ f(x)$ = x^2 = (0100)
Řádek 2: $x^4 \cdot \mathrm{mod}\ f(x)$ = x^3+x^2+x+1 = (1111)
Řádek 3: $x^8 \cdot \mathrm{mod}\ f(x)$ = x^3 = (1000)

$$A = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

čili

3. Sestrojíme matici A^{-1} která je inverzní k matici A

$$= \left(\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{array}\right) =$$

- na pravé straně musíme dostat jednotkovou matici
- nejdříve jsme zaměnili pořadí řádků v matici, 1.→ 3., 3.→4., 4.→1.

$$= \left(\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \end{array}\right) =$$

-protože inverzní prvek k 1 je opět 1,sečetli jsme první tři řádky se čtvrtým, abychom nalevo dostali jednotkovou matici

- matice na pravé straně je nyní inverzní k výchozí matici A

$$= \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix} = A^{-1}$$

4. Řádky matice T' jsou sestrojeny následovně:

Řádek 0: $x \cdot x \cdot \mathrm{mod}\, f(x)$ = x^2 = (0100)
Řádek 1: $x \cdot x^2 \cdot \mathrm{mod}\, f(x)$ = x^3 = (1000)
Řádek 2 $x \cdot x^4 \cdot \mathrm{mod}\, f(x)$ = x^5 mod f(x) = 1 = (0001)
- pozn.: x^5:(x^4+x^3+x^2+x+1)= x+1 a „1“ je zbytek

Řádek 3: $x \cdot x^8 \cdot \mathrm{mod}\, f(x)$ = x^9 mod f(x) = x^3+x^2+x+1= (1111)
- pozn.: x^9:(x^4+x^3+x^2+x+1)= x^5+x^4+1 a „x^3+x^2+x+1“ je zbytek

$$T' = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}$$

$$T = T' \cdot A^{-1} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

a

Násobící matice je tvořena prvky :

$L_{0,0} = T_{(0,0)} = 0$	$L_{1,0} = T_{(3,3)} = 0$	$L_{2,0} = T_{(2,2)} = 1$	$L_{3,0} = T_{(1,1)} = 0$
$L_{0,1} = T_{(1,0)} = 0$	$L_{1,1} = T_{(0,3)} = 0$	$L_{2,1} = T_{(3,2)} = 1$	$L_{3,1} = T_{(2,1)} = 1$
$L_{0,2} = T_{(2,0)} = 1$	$L_{1,2} = T_{(1,3)} = 1$	$L_{2,2} = T_{(0,2)} = 0$	$L_{3,2} = T_{(3,1)} = 0$
$L_{0,3} = T_{(3,0)} = 0$	$L_{1,3} = T_{(2,3)} = 1$	$L_{2,3} = T_{(1,2)} = 0$	$L_{3,3} = T_{(0,1)} = 1$

$$L = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$$

Násobení: (0100)·(1101) = ?

Násobení je v F_{2^4} definováno vztahem $c_k = a \cdot L \cdot b^{tr}$, k=0,…3

$$c_0 = (a_0 a_1 a_2 a_3) \cdot \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix} \cdot (b_0 b_1 b_2 b_3)^{tr} =$$

$$= (a_0 a_1 a_2 a_3) \cdot \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{pmatrix} = (a_0 a_1 a_2 a_3) \cdot \begin{pmatrix} b_2 \\ b_2 + b_3 \\ b_0 + b_1 \\ b_1 + b_3 \end{pmatrix} =$$

$$= (a_0 b_2 + a_1(b_2 + b_3) + a_2(b_0 + b_1) + a_3(b_1 + b_3)) = c_0$$

Nyní pro získání *c_1, c_2, c_3* již stačí jen prohazovat indexy u vektorů *a* a *b.*

To znamená, že u *c_1* zaměníme $a_0 \to a_1$, $a_1 \to a_2$ $a_2 \to a_3$, $a_3 \to a_0$, $b_0 \to b_1$, $b_1 \to b_2$, $b_2 \to b_3$, $b_3 \to b_0$

$c_1 = a_1b_3 + a_2(b_3 + b_0) + a_3(b_1 + b_2) + a_0(b_2 + b_0)$

Pro získání c_2,c_3 bychom opět prohazovali indexy a získali:

$c_2 = a_2b_0 + a_3(b_0 + b_1) + a_0(b_2 + b_3) + a_1(b_3 + b_1)$
$c_3 = a_3b_1 + a_0(b_1 + b_2) + a_1(b_3 + b_0) + a_2(b_0 + b_2)$.

Násobení v F_{2^4} probíhá tedy podle vzorce:

$(a_0 a_1 a_2 a_3) \cdot (b_0 b_1 b_2 b_3) = (c_0 c_1 c_2 c_3)$, kde

$$c_0 = a_0 b_2 + a_1(b_2 + b_3) + a_2(b_0 + b_1) + a_3(b_1 + b_3)$$
$$c_1 = a_1 b_3 + a_2(b_3 + b_0) + a_3(b_1 + b_2) + a_0(b_2 + b_0)$$
$$c_2 = a_2 b_0 + a_3(b_0 + b_1) + a_0(b_2 + b_3) + a_1(b_3 + b_1)$$
$$c_3 = a_3 b_1 + a_0(b_1 + b_2) + a_1(b_3 + b_0) + a_2(b_0 + b_2)$$

$(0100) \cdot (1101) = (c_0 c_1 c_2 c_3)$, kde

$c_0 = 0(0) + 1(0 + 1) + 0(1 + 1) + 0(1 + 1) = 1$

$c_1 = 1(1) + 0(1 + 1) + 0(1 + 0) + 0(0 + 1) = 1$
$c_2 = 0(1) + 0(1 + 1) + 0(0 + 1) + 1(1 + 1) = 0$
$c_3 = 0(1) + 0(1 + 0) + 1(1 + 1) + 0(1 + 0) = 0,$

a tedy $(0100) \cdot (1101) = (1100)$

5 Umocňování v poli F_2^m za použití ONB

Druhá mocnina je definována vztahem:

$(a_0a_1a_2a_3)^2 = (a_0a_1a_2a_3)\cdot(a_0a_1a_2a_3) = (c_0c_1c_2c_3)$, kde

$$c_0 = a_0a_2 + a_1(a_2 + a_3) + a_2(a_0 + a_1) + a_3(a_1 + a_3) = a_3^2 = a_3$$
$$c_1 = a_1a_3 + a_2(a_3 + a_0) + a_3(a_1 + a_2) + a_0(a_2 + a_0) = a_0^2 = a_0$$
$$c_2 = a_2a_0 + a_3(a_0 + a_1) + a_0(a_2 + a_3) + a_1(a_3 + a_1) = a_1^2 = a_1$$
$$c_3 = a_3a_1 + a_0(a_1 + a_2) + a_1(a_3 + a_0) + a_2(a_0 + a_2) = a_2^2 = a_2$$

Tedy $(a_0a_1a_2a_3)^2 = (a_3a_0a_1a_2)$ může být spočteno prostou rotací prvků $(a_0a_1a_2a_3)$.

Výpočet druhé mocniny je tak při použití ONB velmi efektivní. Protože umocňování je často možné rozdělit na opakované výpočty druhých mocnin, je podstatně rychlejší a efektivnější používat vyjádření pole F_2^m pomocí ONB než vyjádření pomocí polynomů.