Násobení v konečném tělese charakteristiky 2 a XOR-metriky

Nikita Carulkov

18. března 2020

Značení, opakování

- značení $\mathbb{F}_2 = \mathbb{Z}_2$ jsou ekvivalentní a rozumíme jimi dvouprvkové konečné těleso
- z kurzu algebry víme, že těleso $\mathbb{F}_{2^m}$ a má 2^m prvků
- jeho prvky se dají reprezentovat jako polynomy nad $\mathbb{F}_2$ stupně nejvýše $m - 1$
- sčítání prvků odpovídá obvyklému sčítání polynomů, kde modulíme jednotlivé koeficienty (v naše případě dvojkou)
- násobení prvků odpovídá násobení polynomů modulo nějaký ireducibilní polynom stupně právě m

Motivace

- s postupným rozšiřováním IoT a potřebou implementace kryptografických šifer na přístojích s omezenou výpočetní kapacitou, vzniká poptávka po algoritmech s nízkou výpočetní náročností
- bezpečnost šifer zpravidla nezávisí na konkrétní reprezentaci prvků konečných těles, a proto je zajímavé zkoumat, jaké reprezentace jsou nejméně náročné
- každé lineární zobrazení $\mathbb{F}_{2^m}^n \to \mathbb{F}_{2^m}^n$ se dá reprezentovat maticí řádu n s prvky z $\mathbb{F}_{2^m}$
- takové matice můžeme reprezentovat maticí řádu $m \cdot n$ s prvky z $\mathbb{F}_2$

XOR-count a cíl práce

- měření náročnosti implementace operace násobení se pak „jen“ redukuje na počet operací XOR (sčítání nad $\mathbb{F}_2$)
- zavádíme proto dvě metriky: *sequential XOR-count* (s-XOR-count) a *direct XOR-count* (d-XOR-count)
- cílem práce je:
  - zjistit, pro jaké matice nastane případ d-XOR-count $<$ s-XOR-count
  - najít nejmenší řád matice, pro které toto nastane
  - popsat sestrojení matice libovolného řádu s takovou vlastností
  - potažmo i navrhnout nějaký odhad na počet matic s touto vlastností
  - lépe dokázat a lépe formulovat tvrzení z článku od L. Kölshe, ze kterého vycházím (odkaz je na konci prezentace na slidu s literaturou)
- pokud vás (díky za čtení) při čtení napadnou nějaké paralely s jinými oblastmi matematiky tak, mi určitě dejte vědět!
- trošku to připomíná problém optimální pivotace z numerické matematiky, či možná myšlenku dynamického programování

Definice d-XOR-countu

Definice

Direct XOR-count *(d-XOR-count)* **invertibilní** matice M řádu n nad $\mathbb{F}_2$, který značíme $wt_d(M)$ definujeme jako

$$wt_d(M) = \omega(M) - n$$

kde $\omega(M)$ označuje počet jedniček v matici M.

Definice s-XOR-countu

Definice

Sequential XOR-count (*s-XOR-count*) **invertibilní** matice M nad $\mathbb{F}_2$ definujeme jako minimální počet t elementárních řádkových operací takový, že M může být převedena do permutační matice.

$$M = P_\sigma \prod_{k=1}^{t} A_{i_k,j_k}$$

kde P_σ je permutační matice a A_{i_k,j_k} jsou jednotkové matice s jedničkou navíc na pozici i_k, j_k. Tento rozklad matice M nazýváme *s-XOR-reprezentace* a s-XOR-reprezentace s právě $wt_s(M)$ součiniteli se nazývá *optimální s-XOR-reprezentace*.

Příklad

D-XOR-count matice M je roven 6 ($wt_d = \omega(M) - n = 10 - 4 = 6$), ve stejnou chvíli však násobení maticí může být implementováno s pomocí pouze 3 XOR operací, neboť předchozí výsledky mohou být použity při nových výpočtech.

$$M = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \end{pmatrix} = \begin{pmatrix} a_1 \\ a_1 + a_2 \\ (a_1 + a_2) + a_3 \\ ((a_1 + a_2) + a_3) + a_4 \end{pmatrix}$$

Domněnky a zjištění

- zjištění: matice řádu n s d-XOR-countem menším než s-XOR-countem existuje právě tehdy, když $n \geq 6$
- to jsem ověřil prohledáním prostoru matic řádu menšího než 5 a sestrojením konstrukce pro matice řádu většího než 6
- domněnka: matic s d-XOR-countem menším než s-XOR-countem je málo (intuice tak radí, není to však zatím dokázáno)

Konstrukce matice řádu 6 s d-XOR-coutem menším než s-XOR-countem

$$M = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix} \in GL(6, \mathbb{F}_2).$$

značení z algebry: GL je grupa regulárních matic, 6 je řád matice, $\mathbb{F}_2 = \mathbb{Z}_2$ je konečné dvouprvkové těleso, které uvažujeme

Věta

Matice M je invertibilní a platí $wt_d(M) < wt_s(M)$ (d-XOR-count je nižší než s-XOR-count).

Odůvodnění správnosti předchozí konstrukce

- větu dokážeme tím, že spočítáme, kolik nejméně je potřeba úprav typu „přičtení jednoho řádku matice k jinému“ k převedení M do permutační matice
- přesněji, budeme zkoumat jak řádky sečíst nejefektivněji, abychom dostali permutační matici
- nejdříve však potřebujeme pomocné lemma

Definice

Hammingovou váhou vektoru v rozumíme počet nenulových prvků v, značíme $wt(v)$.

Lemma

Pro libovolné vektory u, v platí

$$wt(u+v) = wt(u) + wt(v) - 2wt(u \cdot v).$$

Odůvodnění správnosti předchozí konstrukce

$$M = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix} \in GL(6, \mathbb{F}_2).$$

- uvažujme různé kombinace řádků tak, aby se nám sečetly na nějaký jednotkový vektor
- z předchozího lemmatu plyne, že abychom dostali vektor s právě jednou jedničkou, tak nestačí sčítat prvních 5 řádků (sečtení dvou řádků s hammingovou váhou 2 nám dá vektor se sudou váhou)
- nestačí sečíst jeden z prvních pěti řádků (označme v) a poslední (označme u), abychom dostali vektor s právě jednou jedničkou (v by musel mít jedničky ve sloupcích, kde je má u)
- takový v však neexistuje a proto budeme muset sčítat více řádků

Odůvodnění správnosti předchozí konstrukce

$$M = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix} \in GL(6, \mathbb{F}_2).$$

- hledejme dvojici vektorů z prvních pěti řádků (označme v, k) takovou, že $u + k + v =$ „vektor s právě jednou jedničkou“ (u značíme poslední řádek)
- v musí mít jednu jedničku ve stejném sloupci jako má u jedničku
- k musí mít jednu jedničku ve stejném sloupci jako má u jedničku
- v musí mít jednu jedničku ve stejném sloupci jako má k jedničku
- taková dvojice vektorů neexistuje

Odůvodnění správnosti předchozí konstrukce

$$M = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix} \in GL(6, \mathbb{F}_2).$$

- ukázali jsme, že abychom dostali vektor s právě jednou jedničkou, tak musíme sečíst alespoň 4 řádky
- můžeme přičíst například 3., 4., 5. řádek k 6. řádku
- tím dostaneme v posledním řádku právě jednu jedničku
- každý zbylý řádek dokážeme převést do tvaru s jednou jedničkou právě jednou úpravou
- $wt_s(M) = 3 + 5 = 8, wt_d(M) = 13 - 6 = 7$

Stejná konstrukce pro řád matice ≥ 6

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

- konstrukce pro matice řádu 6 lze rozšířit pro libovolný řád $n > 6$
- pro matici A platí $wt_s(A) = wt_d(A) + 1$

literatura

- Kölsch, L.: XOR-Counts and Lightweight Multiplication with Fixed Elements in Binary Finite Fields. In: Advances in Cryptology – EUROCRYPT 2019, LNCS, vol. 11476, Springer, Heidelberg (2019), 285-312

Děkuji za přečtení a za zpětnou vazbu!