Kvadratické APN matice

Zuzana Rezková

25. března 2020

Úvod

Existují tzv. APN funkce, které jsou v kryptografii nejlepší volbou pro odolnost vůči diferenciálnímu útoku.
Většina známých APN funkcí je kvadratických (a na ty se také zaměřím).
V této práci představím maticový přístup k hledání nových APN funkcí.

Základní pojmy

Booleovské funkce

- $\mathbb{F}_2$ značí dvouprvkové těleso. Nechť $n, m \in \mathbb{N}$
- $G : \mathbb{F}_2^n \to \mathbb{F}_2$ nazýváme binární booleovská funkce.

Příklad

$$G_1 : \mathbb{F}_2^3 \to \mathbb{F}_2$$
$$(x, y, z) \mapsto (x + y)$$

Příklad

$$G_2 : \mathbb{F}_2^3 \to \mathbb{F}_2$$
$$(x, y, z) \mapsto (x \cdot z)$$

- Vektorová booleovská funkce je tvaru $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$.

Příklad

$$F : \mathbb{F}_2^3 \to \mathbb{F}_2^2$$
$$(x, y, z) \mapsto (G_1(x, y, z), G_2(x, y, z))$$

Základní pojmy

Booleovské funkce

- $\mathbb{F}_2$ značí dvouprvkové těleso. Nechť $n, m \in \mathbb{N}$
- $G : \mathbb{F}_2^n \to \mathbb{F}_2$ nazýváme binární booleovská funkce.

Příklad

$$G_1 : \mathbb{F}_2^3 \to \mathbb{F}_2$$
$$(x, y, z) \mapsto (x + y)$$

Příklad

$$G_2 : \mathbb{F}_2^3 \to \mathbb{F}_2$$
$$(x, y, z) \mapsto (x \cdot z)$$

- Vektorová booleovská funkce je tvaru $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$.

Příklad

$$F : \mathbb{F}_2^3 \to \mathbb{F}_2^2$$
$$(x, y, z) \mapsto (G_1(x, y, z), G_2(x, y, z))$$

- $\mathbb{F}_2$ značí dvouprvkové těleso. Nechť $n, m \in \mathbb{N}$
- $G : \mathbb{F}_2^n \to \mathbb{F}_2$ nazýváme binární booleovská funkce.

Příklad

$$G_1 : \mathbb{F}_2^3 \to \mathbb{F}_2$$
$$(x, y, z) \mapsto (x + y)$$

Příklad

$$G_2 : \mathbb{F}_2^3 \to \mathbb{F}_2$$
$$(x, y, z) \mapsto (x \cdot z)$$

- Vektorová booleovská funkce je tvaru $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$.

Příklad

$$F : \mathbb{F}_2^3 \to \mathbb{F}_2^2$$
$$(x, y, z) \mapsto (G_1(x, y, z), G_2(x, y, z))$$

- Konečné těleso s 2^n prvky budeme značit $\mathbb{F}_{2^n}$.

Tvrzení

Ať $p(x) \in \mathbb{F}_2[x]$ je ireducibilní polynom stupně n. Potom

$$\mathbb{F}_{2^n} \simeq \mathbb{F}_2 / p(x)$$

Příklad

Konečné těleso $\mathbb{F}_{2^2}$ lze chápat jako množinu $\{0, 1, \alpha, \alpha + 1\}$ se sčítáním modulo 2 a násobením modulo $\alpha^2 + \alpha + 1$.

- Konečné těleso s 2^n prvky budeme značit $\mathbb{F}_{2^n}$.

Tvrzení

Ať $p(x) \in \mathbb{F}_2[x]$ je ireducibilní polynom stupně n. Potom

$$\mathbb{F}_{2^n} \simeq \mathbb{F}_2 / p(x)$$

Příklad

Konečné těleso $\mathbb{F}_{2^2}$ lze chápat jako množinu $\{0, 1, \alpha, \alpha + 1\}$ se sčítáním modulo 2 a násobením modulo $\alpha^2 + \alpha + 1$.

- Konečné těleso s 2^n prvky budeme značit $\mathbb{F}_{2^n}$.

Tvrzení

Ať $p(x) \in \mathbb{F}_2[x]$ je ireducibilní polynom stupně n. Potom

$$\mathbb{F}_{2^n} \simeq \mathbb{F}_2 / p(x)$$

Příklad

Konečné těleso $\mathbb{F}_{2^2}$ lze chápat jako množinu $\{0, 1, \alpha, \alpha + 1\}$ se sčítáním modulo 2 a násobením modulo $\alpha^2 + \alpha + 1$.

Základní pojmy

(n, n)-funkce

Definice

(n, n)-funkcí rozumíme funkci $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$.

Tvrzení

Každá booleovská funkce a každá (n, n)-funkce je jednoznačně určena polynomem

$$f(x) = \sum_{i=0}^{2^n-1} a_i x^i, \ a_i \in \mathbb{F}_{2^n}$$

Důsledek

Zkoumání booleovských funkcí se zjednoduší na zkoumání (n, n)-funkcí, respektive polynomů $f(x) \in \mathbb{F}_{2^n}[x]$.

Základní pojmy

(n, n)-funkce

Definice

(n, n)-funkcí rozumíme funkci $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$.

Tvrzení

Každá booleovská funkce a každá (n, n)-funkce je jednoznačně určena polynomem

$$f(x) = \sum_{i=0}^{2^n-1} a_i x^i, \ a_i \in \mathbb{F}_{2^n}$$

Důsledek

Zkoumání booleovských funkcí se zjednoduší na zkoumání (n, n)-funkcí, respektive polynomů $f(x) \in \mathbb{F}_{2^n}[x]$.

Základní pojmy

(n, n)-funkce

Definice

(n, n)-funkcí rozumíme funkci $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$.

Tvrzení

Každá booleovská funkce a každá (n, n)-funkce je jednoznačně určena polynomem

$$f(x) = \sum_{i=0}^{2^n-1} a_i x^i, \ a_i \in \mathbb{F}_{2^n}$$

Důsledek

Zkoumání booleovských funkcí se zjednoduší na zkoumání (n, n)-funkcí, respektive polynomů $f(x) \in \mathbb{F}_{2^n}[x]$.

Motivace

Kryptografie

Kryptografické útoky na blokové šifry využívají pravděpodobnosti s jakou nastane $F(x) + F(x + a) = b$.
Jde tedy o vztah rozdílu vstupních hodnot a rozdílu výstupních hodnot.
Přirozeně chceme, aby námi použitá funkce byla v tomto ohledu co nejlepší.

Poznámka

Díky charakteristice 2 a komutativitě platí:

$$F(x + a) + F(x) = F((x + a) + a) + F(x + a)$$

Tedy $|\{x \in \mathbb{F}_{2^n} \mid F(x + a) + F(x) = b\}|$ je vždy sudé.
Nejlepší hodnota, které můžeme dosáhnout, je tedy 2.

Motivace

Kryptografie

Kryptografické útoky na blokové šifry využívají pravděpodobnosti s jakou nastane $F(x) + F(x + a) = b$.
Jde tedy o vztah rozdílu vstupních hodnot a rozdílu výstupních hodnot.
Přirozeně chceme, aby námi použitá funkce byla v tomto ohledu co nejlepší.

Poznámka

Díky charakteristice 2 a komutativitě platí:

$$F(x + a) + F(x) = F((x + a) + a) + F(x + a)$$

Tedy $|\{x \in \mathbb{F}_{2^n} \mid F(x + a) + F(x) = b\}|$ je vždy sudé.
Nejlepší hodnota, které můžeme dosáhnout, je tedy 2.

Motivace

APN funkce

Nechť F je (n, n)-funkce určená polynomem $f \in \mathbb{F}_{2^n}[x]$.

Definice

Řekneme, že F je APN (almost perfect nonlinear), pokud

$$\forall a, b \in \mathbb{F}_{2^n},\ a \neq 0 :\ |\{x \in \mathbb{F}_{2^n} \mid F(x+a) + F(x) = b\}| \leq 2$$

Příklad

Pro $n = 2,\ F(x) = x^2, a = 1$:

$$\begin{aligned} x = 0 &: & F(0) + F(0+1) &= 1 \\ x = 1 &: & F(1) + F(1+1) &= 1 \\ x = \alpha &: & F(\alpha) + F(\alpha+1) &= 1 \\ x = \alpha + 1 &: & F(\alpha+1) + F(\alpha+1+1) &= 1 \end{aligned}$$

Tedy $|\{x \in \mathbb{F}_{2^2} \mid F(x+1) + F(x) = 1\}| = 4$

Motivace

APN funkce

Nechť F je (n, n)-funkce určená polynomem $f \in \mathbb{F}_{2^n}[x]$.

Definice

Řekneme, že F je APN (almost perfect nonlinear), pokud

$$\forall a, b \in \mathbb{F}_{2^n},\ a \neq 0 :\ |\{x \in \mathbb{F}_{2^n} \mid F(x+a) + F(x) = b\}| \leq 2$$

Příklad

Pro $n = 2,\ F(x) = x^2, a = 1$:

$$x = 0 : \quad F(0) + F(0+1) = 1$$
$$x = 1 : \quad F(1) + F(1+1) = 1$$
$$x = \alpha : \quad F(\alpha) + F(\alpha+1) = 1$$
$$x = \alpha + 1 : \quad F(\alpha+1) + F(\alpha+1+1) = 1$$

Tedy $|\{x \in \mathbb{F}_{2^2} \mid F(x+1) + F(x) = 1\}| = 4$

Motivace

APN funkce

Nechť F je (n, n)-funkce určená polynomem $f \in \mathbb{F}_{2^n}[x]$.

Definice

Řekneme, že F je APN (almost perfect nonlinear), pokud

$$\forall a, b \in \mathbb{F}_{2^n},\ a \neq 0 :\ |\{x \in \mathbb{F}_{2^n} \mid F(x+a) + F(x) = b\}| \leq 2$$

Příklad

Pro $n = 2,\ F(x) = x^2, a = 1$:

$$\begin{aligned} x = 0 &: & F(0) + F(0+1) &= 1 \\ x = 1 &: & F(1) + F(1+1) &= 1 \\ x = \alpha &: & F(\alpha) + F(\alpha+1) &= 1 \\ x = \alpha + 1 &: & F(\alpha+1) + F(\alpha+1+1) &= 1 \end{aligned}$$

Tedy $|\{x \in \mathbb{F}_{2^2} \mid F(x+1) + F(x) = 1\}| = 4$

Motivace

Nové APN funkce

Definice

Řekneme, že (n, n)-funkce F_1, F_2 jsou

- EA-ekvivalentní, pokud $F_1(x) = A_1(F(A_2(x))) + A_3(x)$, kde A_1, A_2 jsou afinní permutace, A_3 je afinní funkce.
- CCZ-ekvivalentní, pokud existuje afinní permutace, která zobrazí graf F_1 na graf F_2.

Tvrzení

Ať F_1, F_2 jsou CCZ-ekvivalentní (n, n)-funkce.
Potom F_1 je APN $\iff$ F_2 je APN.

APN funkci považujeme za novou, pokud není CCZ-ekvivalentní známým APN funkcím.

Motivace

Nové APN funkce

Definice

Řekneme, že (n, n)-funkce F_1, F_2 jsou

- EA-ekvivalentní, pokud $F_1(x) = A_1(F(A_2(x))) + A_3(x)$, kde A_1, A_2 jsou afinní permutace, A_3 je afinní funkce.
- CCZ-ekvivalentní, pokud existuje afinní permutace, která zobrazí graf F_1 na graf F_2.

Tvrzení

Ať F_1, F_2 jsou CCZ-ekvivalentní (n, n)-funkce.
Potom F_1 je APN $\iff$ F_2 je APN.

APN funkci považujeme za novou, pokud není CCZ-ekvivalentní známým APN funkcím.

Motivace

Nové APN funkce

Definice

Řekneme, že (n, n)-funkce F_1, F_2 jsou

- EA-ekvivalentní, pokud $F_1(x) = A_1(F(A_2(x))) + A_3(x)$, kde A_1, A_2 jsou afinní permutace, A_3 je afinní funkce.
- CCZ-ekvivalentní, pokud existuje afinní permutace, která zobrazí graf F_1 na graf F_2.

Tvrzení

Ať F_1, F_2 jsou CCZ-ekvivalentní (n, n)-funkce.
Potom F_1 je APN $\iff$ F_2 je APN.

APN funkci považujeme za novou, pokud není CCZ-ekvivalentní známým APN funkcím.

Kvadratické homogenní funkce

Základní definice

V této práci se zabýváme pouze kvadratickými homogenními funkcemi.

Tvrzení

Díky konečné charakteristice tělesa $\mathbb{F}_{2^n}$ platí

$$\forall a, b \in \mathbb{F}_{2^n} : \ (a+b)^{2^i} = a^{2^i} + b^{2^i}$$

Z tohoto důvodu selhává nad $\mathbb{F}_{2^n}$ intuice pro stupně polynomů.

Definice

Lineární člen polynomu f je člen stupně 2^j pro $1 \leq j \leq 2^n - 1$.

Definice

Kvadratický člen polynomu f je člen stupně $2^j + 2^i$ pro $1 \leq j < i \leq 2^n - 1$.

Kvadratické homogenní funkce

Základní definice

V této práci se zabýváme pouze kvadratickými homogenními funkcemi.

Tvrzení

Díky konečné charakteristice tělesa $\mathbb{F}_{2^n}$ platí

$$\forall a, b \in \mathbb{F}_{2^n} : \ (a+b)^{2^i} = a^{2^i} + b^{2^i}$$

Z tohoto důvodu selhává nad $\mathbb{F}_{2^n}$ intuice pro stupně polynomů.

Definice

Lineární člen polynomu f je člen stupně 2^j pro $1 \leq j \leq 2^n - 1$.

Definice

Kvadratický člen polynomu f je člen stupně $2^j + 2^i$ pro $1 \leq j < i \leq 2^n - 1$.

Kvadratické homogenní funkce

Základní definice

V této práci se zabýváme pouze kvadratickými homogenními funkcemi.

Tvrzení

Díky konečné charakteristice tělesa $\mathbb{F}_{2^n}$ platí

$$\forall a, b \in \mathbb{F}_{2^n} : \ (a+b)^{2^i} = a^{2^i} + b^{2^i}$$

Z tohoto důvodu selhává nad $\mathbb{F}_{2^n}$ intuice pro stupně polynomů.

Definice

Lineární člen polynomu f je člen stupně 2^j pro $1 \leq j \leq 2^n - 1$.

Definice

Kvadratický člen polynomu f je člen stupně $2^j + 2^i$ pro $1 \leq j < i \leq 2^n - 1$.

Kvadratické homogenní funkce

Základní definice

V této práci se zabýváme pouze kvadratickými homogenními funkcemi.

Tvrzení

Díky konečné charakteristice tělesa $\mathbb{F}_{2^n}$ platí

$$\forall a, b \in \mathbb{F}_{2^n} : \ (a+b)^{2^i} = a^{2^i} + b^{2^i}$$

Z tohoto důvodu selhává nad $\mathbb{F}_{2^n}$ intuice pro stupně polynomů.

Definice

Lineární člen polynomu f je člen stupně 2^j pro $1 \leq j \leq 2^n - 1$.

Definice

Kvadratický člen polynomu f je člen stupně $2^j + 2^i$ pro $1 \leq j < i \leq 2^n - 1$.

Kvadratické homogenní funkce

Základní definice

Definice

Kvadratická homogenní funkce je (n, n)-funkce určená polynomem

$$f(x) = \sum_{1 \leq t < i \leq n} c_{i,t} x^{2^{i-1}+2^{t-1}}$$

Jinými slovy jde o kvadratickou funkci bez konstantních a lineárních členů.

Příklad

Nad tělesem $\mathbb{F}_{2^3}$ kvadratickou homogenní funkci určuje polynom

$$\begin{aligned} f(x) &= c_{2,3}x^6 + c_{1,3}x^5 + c_{1,2}x^3 \\ &= c_{2,3}x^{2^{2-1}+2^{3-1}} + c_{1,2}x^{2^{1-1}+2^{2-1}} + c_{1,3}x^{2^{1-1}+2^{3-1}} \end{aligned}$$

Kvadratické homogenní funkce

Základní definice

Definice

Kvadratická homogenní funkce je (n, n)-funkce určená polynomem

$$f(x) = \sum_{1 \leq t < i \leq n} c_{i,t} x^{2^{i-1}+2^{t-1}}$$

Jinými slovy jde o kvadratickou funkci bez konstantních a lineárních členů.

Příklad

Nad tělesem $\mathbb{F}_{2^3}$ kvadratickou homogenní funkci určuje polynom

$$\begin{aligned} f(x) &= c_{2,3}x^6 + c_{1,3}x^5 + c_{1,2}x^3 \\ &= c_{2,3}x^{2^{2-1}+2^{3-1}} + c_{1,2}x^{2^{1-1}+2^{2-1}} + c_{1,3}x^{2^{1-1}+2^{3-1}} \end{aligned}$$

Kvadratické homogenní funkce

EA-ekvivalence

Nechť (až do konce prezentace) F je kvadratická homogenní funkce určená polynomem

$$f(x) = \sum_{1 \leq t < i \leq n} c_{i,t} x^{2^{i-1}+2^{t-1}}$$

Tvrzení

Dvě kvadratické APN-funkce jsou EA-ekvivalentní právě tehdy, když jsou CCZ-ekvivalentní.

V obecném případě tato ekvivalence neplatí.
Při hledání nových kvadratických APN funkcí se ale můžeme omezit na ověřování EA-ekvivalence.

Kvadratické homogenní funkce

EA-ekvivalence

Nechť (až do konce prezentace) F je kvadratická homogenní funkce určená polynomem

$$f(x) = \sum_{1 \leq t < i \leq n} c_{i,t} x^{2^{i-1}+2^{t-1}}$$

Tvrzení

Dvě kvadratické APN-funkce jsou EA-ekvivalentní právě tehdy, když jsou CCZ-ekvivalentní.

V obecném případě tato ekvivalence neplatí.
Při hledání nových kvadratických APN funkcí se ale můžeme omezit na ověřování EA-ekvivalence.

Kvadratické homogenní funkce

EA-ekvivalence

Nechť (až do konce prezentace) F je kvadratická homogenní funkce určená polynomem

$$f(x) = \sum_{1 \leq t < i \leq n} c_{i,t} x^{2^{i-1}+2^{t-1}}$$

Tvrzení

Dvě kvadratické APN-funkce jsou EA-ekvivalentní právě tehdy, když jsou CCZ-ekvivalentní.

V obecném případě tato ekvivalence neplatí.
Při hledání nových kvadratických APN funkcí se ale můžeme omezit na ověřování EA-ekvivalence.

Kvadratické homogenní funkce

Vyjádření pomocí matice

Definice

Nechť $\beta = (\beta_1, \ldots, \beta_n)$ je báze $\mathbb{F}_{2^n}$ nad $\mathbb{F}_2$.
Označme $\vec{x} = (\lambda_1, \ldots, \lambda_n)^\top, \lambda_i \in \mathbb{F}_2$ vektor koeficientů $x \in \mathbb{F}_{2^n}$ vzhledem k bázi β.
Definujeme matici $M_\beta[i, u] = \beta_u^{2^{i-1}}$.

Příklad

Nechť $n = 2$. Víme, že na prvky $\mathbb{F}_{2^2}$ lze nahlížet jako na $\{0, 1, \alpha, \alpha + 1\}$. Volme bázi $\beta = (1, \alpha)$.

$$\vec{0} = (0, 0) \qquad \vec{1} = (1, 0)$$

$$\vec{\alpha} = (0, 1) \qquad \alpha \vec{+} 1 = (1, 1)$$

Kvadratické homogenní funkce

Vyjádření pomocí matice

Definice

Nechť $\beta = (\beta_1, \ldots, \beta_n)$ je báze $\mathbb{F}_{2^n}$ nad $\mathbb{F}_2$.
Označme $\vec{x} = (\lambda_1, \ldots, \lambda_n)^\top, \lambda_i \in \mathbb{F}_2$ vektor koeficientů $x \in \mathbb{F}_{2^n}$ vzhledem k bázi β.
Definujeme matici $M_\beta[i, u] = \beta_u^{2^{i-1}}$.

Příklad

Nechť $n = 2$. Víme, že na prvky $\mathbb{F}_{2^2}$ lze nahlížet jako na $\{0, 1, \alpha, \alpha + 1\}$. Volme bázi $\beta = (1, \alpha)$.

$$\vec{0} = (0, 0) \qquad \vec{1} = (1, 0)$$

$$\vec{\alpha} = (0, 1) \qquad \alpha \vec{+} 1 = (1, 1)$$

Kvadratické homogenní funkce

Vyjádření pomocí matice

Definice

Nechť $\beta = (\beta_1, \ldots, \beta_n)$ je báze $\mathbb{F}_{2^n}$ nad $\mathbb{F}_2$.
Označme $\vec{x} = (\lambda_1, \ldots, \lambda_n)^\top, \lambda_i \in \mathbb{F}_2$ vektor koeficientů $x \in \mathbb{F}_{2^n}$ vzhledem k bázi β.
Definujeme matici $M_\beta[i, u] = \beta_u^{2^{i-1}}$.

Příklad

Nechť $n = 2$. Víme, že na prvky $\mathbb{F}_{2^2}$ lze nahlížet jako na $\{0, 1, \alpha, \alpha + 1\}$. Volme bázi $\beta = (1, \alpha)$.

$$M_\beta = \begin{pmatrix} 1^1 & \alpha^1 \\ 1^2 & \alpha^2 \end{pmatrix}$$

Kvadratické homogenní funkce

Vyjádření pomocí matice

Definujme vektor X, matici E následovně.

$$X^\top EX = (x^{2^0}, x^{2^1}, \ldots, x^{2^{n-1}}) \begin{pmatrix} 0 & 0 & \ldots & 0 \\ c_{2,1} & 0 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ c_{n,1} & \ldots & c_{n,n-1} & 0 \end{pmatrix} \begin{pmatrix} x^{2^0} \\ x^{2^1} \\ \vdots \\ x^{2^{n-1}} \end{pmatrix}$$

$$= \sum_{i,t=0}^{n} c_{i,t} x^{2^{i-1}+2^{t-1}}$$

$$= F(x)$$

Kvadratické homogenní funkce

Vyjádření pomocí matice

Definujme vektor X, matici E následovně.

$$X^\top EX = (x^{2^0}, x^{2^1}, \ldots, x^{2^{n-1}}) \begin{pmatrix} 0 & 0 & \ldots & 0 \\ c_{2,1} & 0 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ c_{n,1} & \ldots & c_{n,n-1} & 0 \end{pmatrix} \begin{pmatrix} x^{2^0} \\ x^{2^1} \\ \vdots \\ x^{2^{n-1}} \end{pmatrix}$$

$$= \sum_{i,t=0}^{n} c_{i,t} x^{2^{i-1}+2^{t-1}}$$

$$= F(x)$$

Kvadratické homogenní funkce

Vyjádření pomocí matice

Definujme vektor X, matici E následovně.

$$X^\top EX = (x^{2^0}, x^{2^1}, \ldots, x^{2^{n-1}}) \begin{pmatrix} 0 & 0 & \ldots & 0 \\ c_{2,1} & 0 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ c_{n,1} & \ldots & c_{n,n-1} & 0 \end{pmatrix} \begin{pmatrix} x^{2^0} \\ x^{2^1} \\ \vdots \\ x^{2^{n-1}} \end{pmatrix}$$

$$= \sum_{i,t=0}^{n} c_{i,t} x^{2^{i-1}+2^{t-1}}$$

$$= F(x)$$

Kvadratické homogenní funkce

Vyjádření pomocí matice

Tvrzení

$$M_\beta \vec{x} = \begin{pmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \beta_1^2 & \beta_2^2 & \cdots & \beta_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ \beta_1^{2^{n-1}} & \beta_2^{2^{n-1}} & \cdots & \beta_n^{2^{n-1}} \end{pmatrix} \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} = X$$

$$F(x) = X^\top E X = \vec{x}^\top M_\beta^\top E M_\beta \vec{x}$$

Definice

S využitím matic M_β, E definujme $H = M_\beta^\top (E + E^\top) M_\beta$.

Toto vyjádření je relativní vůči zvolené bázi.

Kvadratické homogenní funkce

Vyjádření pomocí matice

Tvrzení

$$M_\beta \vec{x} = \begin{pmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \beta_1^2 & \beta_2^2 & \cdots & \beta_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ \beta_1^{2^{n-1}} & \beta_2^{2^{n-1}} & \cdots & \beta_n^{2^{n-1}} \end{pmatrix} \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} = X$$

$$F(x) = X^\top E X = \vec{x}^\top M_\beta^\top E M_\beta \vec{x}$$

Definice

S využitím matic M_β, E definujme $H = M_\beta^\top (E + E^\top) M_\beta$.

Toto vyjádření je relativní vůči zvolené bázi.

Kvadratické homogenní funkce

Vyjádření pomocí matice

Tvrzení

$$M_\beta \vec{x} = \begin{pmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \beta_1^2 & \beta_2^2 & \cdots & \beta_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ \beta_1^{2^{n-1}} & \beta_2^{2^{n-1}} & \cdots & \beta_n^{2^{n-1}} \end{pmatrix} \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} = X$$

$$F(x) = X^\top E X = \vec{x}^\top M_\beta^\top E M_\beta \vec{x}$$

Definice

S využitím matic M_β, E definujme $H = M_\beta^\top (E + E^\top) M_\beta$.

Toto vyjádření je relativní vůči zvolené bázi.

Kvadratické homogenní funkce

Vyjádření pomocí matice

Tvrzení

$$M_\beta \vec{x} = \begin{pmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \beta_1^2 & \beta_2^2 & \cdots & \beta_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ \beta_1^{2^{n-1}} & \beta_2^{2^{n-1}} & \cdots & \beta_n^{2^{n-1}} \end{pmatrix} \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} = X$$

$$F(x) = X^\top E X = \vec{x}^\top M_\beta^\top E M_\beta \vec{x}$$

Definice

S využitím matic M_β, E definujme $H = M_\beta^\top (E + E^\top) M_\beta$.

Toto vyjádření je relativní vůči zvolené bázi.

Kvadratické APN matice

Základní definice

Definice

Matice $A \in \mathbb{F}_{2^n}^{n \times n}$ je QAM (kvadratická APN matice), pokud

- je symetrická
- má nulovou diagonálu
- libovolná nenulová lineární kombinace n řádků matice A má rank (nad $\mathbb{F}_2$) $n - 1$

Kvadratické APN matice

Vlastnosti

Tvrzení

F je APN $\iff$ H je QAM

Toto tvrzení nám dává jednoznačnou korespondenci mezi QAM a APN funkcemi.
Pokud nalezneme QAM matici, nalezli jsme APN funkci. Ještě je ale nutné ověřit, že se jedná o novou APN funkci.

Kvadratické APN matice

Vlastnosti

Tvrzení

Nechť F_1, F_2 jsou (n, n)-funkce, H_1, H_2 jejich matice.
F_1, F_2 jsou EA-ekvivalentní, pokud $H_1 = L(P^T H_2 P)$, kde $P \in \mathbb{F}_2^{n \times n}$ invertibilní, L lineární permutace na $\mathbb{F}_{2^n}$.

Víme, že u kvadratických funkcí je EA-ekvivalence to stejné jako CCZ-ekvivalence.
Hledání nových kvadratických homogenních APN funkcí můžeme (částečně) převést na konstrukci nových QAM.

Do prezentace bych chtěla doplnit

- algoritmus pro hledání nových QAM z již známých a jeho vysvětlení

Děkuji za pozornost.