Representation of Boolean and Vectorial Boolean Function

2021-4-28

Theorem

The residue class ring $\mathbb{Z}/p\mathbb{Z}$ is a finite field with p elements under the addition and multiplication modulo p, where p is a prime.

Theorem

The residue class ring $\mathbb{Z}/p\mathbb{Z}$ is a finite field with p elements under the addition and multiplication modulo p, where p is a prime.

Note that if p is not a prime, $\mathbb{Z}/p\mathbb{Z}$ is not a field, but a ring including zero divisor.

Theorem

The residue class ring $\mathbb{Z}/p\mathbb{Z}$ is a finite field with p elements under the addition and multiplication modulo p, where p is a prime.

Note that if p is not a prime, $\mathbb{Z}/p\mathbb{Z}$ is not a field, but a ring including zero divisor.

Question

Does there exist finite field with q elements, where q is not a prime?

Theorem (Existence and Uniqueness of Finite Fields)

Let $f(x) \in \mathbb{F}_p[x]$ *be an irreducible polynomial of degree* n *over* $\mathbb{F}_p$, *then* $\mathbb{F}_p[x]/(f(x))$ *is a finite field with* p^n *elements. Moreover*

$$\mathbb{F}_{p^n} = \mathbb{F}_p[x]/(f(x)) \cong \mathbb{F}_p(\alpha)$$

where α *is a root of* $f(x)$.

The 'uniqueness' is because of the uniqueness (up to isomorphisms) of splitting fields. In fact, $\mathbb{F}_{p^n}$ is the splitting field of $x^{p^n} - x$ over $\mathbb{F}_p$.

Example

Let $f(x) = x^3 + x + 1 \in \mathbb{F}_2[x]$ be irreducible over $\mathbb{F}_2$ and α be a root of it, i.e., $f(\alpha) = \alpha^3 + \alpha + 1 = 0$. Then $\mathbb{F}_2[x]/(f(x)) = \mathbb{F}_2(\alpha)$ is a finite field with 8 elements. In detail,
$\mathbb{F}_8 = \{0, 1, \alpha, \alpha + 1, \alpha^2, \alpha^2 + 1, \alpha^2 + \alpha, \alpha^2 + \alpha + 1\} \cong \mathbb{F}_2^3$.

Example

Let $f(x) = x^3 + x + 1 \in \mathbb{F}_2[x]$ be irreducible over $\mathbb{F}_2$ and α be a root of it, i.e., $f(\alpha) = \alpha^3 + \alpha + 1 = 0$. Then $\mathbb{F}_2[x]/(f(x)) = \mathbb{F}_2(\alpha)$ is a finite field with 8 elements. In detail, $\mathbb{F}_8 = \{0, 1, \alpha, \alpha + 1, \alpha^2, \alpha^2 + 1, \alpha^2 + \alpha, \alpha^2 + \alpha + 1\} \cong \mathbb{F}_2^3$.

Example

Let $f(x) = x^3 + x + 1 \in \mathbb{F}_2[x]$. The companion matrix of f is

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

It is well known in linear algebra that $f(A) = 0$, therefore, A can play the role of a root of f. The field $\mathbb{F}_8$ can be represented in the form $\mathbb{F}_8 = \{0, I, A, A + I, A^2, A^2 + I, A^2 + A, A^2 + A + I\} \cong \mathbb{F}_2^3$.

Let $f : \mathbb{F}_2^n \cong \mathbb{F}_{2^n} \to \mathbb{F}_2$ be an n-ary Boolean function.

- Truth table

x	000	001	010	011	100	101	110	111
$f(x)$	0	0	0	1	1	1	1	1

Let $f : \mathbb{F}_2^n \cong \mathbb{F}_{2^n} \to \mathbb{F}_2$ be an n-ary Boolean function.

- Truth table

x	000	001	010	011	100	101	110	111
$f(x)$	0	0	0	1	1	1	1	1

- Algebraic normal form

$$f(x_1, \ldots, x_n) = \sum_{I \subseteq \{1,\ldots,n\}} a_I \prod_{i \in I} x_i, a_I \in \mathbb{F}_2,$$

where

$$a_I = \sum_{\vec{x} \in \mathbb{F}_2^n, supp(\vec{x}) \subseteq I} f(\vec{x}).$$

e.g., $f(x_1, x_2, x_3) = x_1x_2x_3 + x_1x_2 + x_3$.

Let $F : \mathbb{F}_2^n \cong \mathbb{F}_{2^n} \to \mathbb{F}_2^m \cong \mathbb{F}_{2^m}$ be a vectorial Boolean function.

- Coordinate functions $F(x) = (f_1(x), f_2(x), \ldots, f_m(x))$

Let $F : \mathbb{F}_2^n \cong \mathbb{F}_{2^n} \to \mathbb{F}_2^m \cong \mathbb{F}_{2^m}$ be a vectorial Boolean function.

- Coordinate functions $F(x) = (f_1(x), f_2(x), \dots, f_m(x))$
- Univariate representation (Lagarange interpolation)

$$f(x) = \sum_{a \in \mathbb{F}_{2^n}} F(a)\left(1 + (x+a)^{2^n-1}\right) = \sum_{j=0}^{2^n-1} a_j x^j, a_j \in \mathbb{F}_{2^n}.$$

Let $F : \mathbb{F}_2^n \cong \mathbb{F}_{2^n} \to \mathbb{F}_2^m \cong \mathbb{F}_{2^m}$ be a vectorial Boolean function.

- Coordinate functions $F(x) = (f_1(x), f_2(x), \ldots, f_m(x))$
- Univariate representation (Lagarange interpolation)

$$f(x) = \sum_{a \in \mathbb{F}_{2^n}} F(a) \left(1 + (x+a)^{2^n - 1}\right) = \sum_{j=0}^{2^n-1} a_j x^j, a_j \in \mathbb{F}_{2^n}.$$

- Bivariate representation

$$f(x,y) = \sum_{(a,b) \in \mathbb{F}_{2^{\frac{n}{2}}} \times \mathbb{F}_{2^{\frac{n}{2}}}} F(a,b) \left(1 + (x+a)^{2^{\frac{n}{2}}-1}\right) \left(1 + (y+b)^{2^{\frac{n}{2}}-1}\right)$$

$$= \sum_{i,j=0}^{2^{\frac{n}{2}}-1} a_{ij} x^i y^j, a_{ij} \in \mathbb{F}_{2^n}.$$

Definition (Nonlinearity)

1. The Nonlinearity of Boolean function f is defined as

$$NL(f) = \min_{\ell \in A_n} d(f, \ell) = \min_{\ell \in A_n} wt(f - \ell)$$
$$= 2^{n-1} - \frac{1}{2} \max_{\omega \in \mathbb{F}_{2^n}} |W_f(\omega)|$$

2. The Nonlinearity of vect. Boolean function F is defined as

$$NL(F) = \min_{v \neq 0} \{NL(v \cdot F)\}$$

Definition (Nonlinearity)

1. The Nonlinearity of Boolean function f is defined as

$$NL(f) = \min_{\ell \in A_n} d(f, \ell) = \min_{\ell \in A_n} wt(f - \ell)$$
$$= 2^{n-1} - \frac{1}{2} \max_{\omega \in \mathbb{F}_{2^n}} |W_f(\omega)|$$

2. The Nonlinearity of vect. Boolean function F is defined as

$$NL(F) = \min_{v \neq 0} \{NL(v \cdot F)\}$$

- $NL(f) \leq 2^{n-1} - 2^{\frac{n}{2}-1}$. If '=' holds, f is called bent function.
- Bent function with optimal nonlinearity(resist linear attack).
- Are deep holes of the first-order Reed-Muller code.

Definition (Differential uniformity)

The differential uniformity of F is defined as

$$\delta_F = \max_{0 \neq a, b \in \mathbb{F}_{2^n}} |\{x \in \mathbb{F}_{2^n} | F(x+a) - F(x) = b\}|.$$

Definition (Differential uniformity)

The differential uniformity of F is defined as

$$\delta_F = \max_{0\neq a, b\in\mathbb{F}_{2^n}} |\{x \in \mathbb{F}_{2^n} | F(x+a) - F(x) = b\}|.$$

Definition (Boomerang uniformity)

Let $T(a,b)$ be the number of solutions of the following equations

$$\begin{cases} F(x) + F(y) = b \\ F(x+a) + F(y+a) = b \end{cases}$$

the boomerang uniformity of F is defined as

$$\tau_F = \max_{0\neq a, 0\neq b\in\mathbb{F}_{2^n}} T(a,b).$$

- $\delta_F > 0$ is even. If $\delta_F = 2$, F is called Almost Perfect Nonlinear function(resist differential attack).
- $\tau_F \geq \delta_F$. If $\tau_F = \delta_F$, we call F with optimal boomerang uniformity(resist boomerang attack).

- $\delta_F > 0$ is even. If $\delta_F = 2$, F is called Almost Perfect Nonlinear function(resist differential attack).
- $\tau_F \geq \delta_F$. If $\tau_F = \delta_F$, we call F with optimal boomerang uniformity(resist boomerang attack).

Known infinite families of APN power functions over $\mathbb{F}_{2^n}$.

Family	Exponent	Conditions
Gold	$2^i + 1$	$\gcd(i, n) = 1$
Kasami	$2^{2i} - 2^i + 1$	$\gcd(i, n) = 1$
Welch	$2^t + 3$	$n = 2t + 1$
Niho	$2^t + 2^{\frac{t}{2}} - 1$, t even	$n = 2t + 1$
	$2^t + 2^{\frac{(3t+1)}{2}} - 1$, t odd	
Inverse	$2^{2t} - 1$	$n = 2t + 1$
Dobbertin	$2^{4i} + 2^{3^i} + 2^{2^i} + 2^i - 1$	$n = 5i$

- $\delta_F > 0$ is even. If $\delta_F = 2$, F is called Almost Perfect Nonlinear function(resist differential attack).
- $\tau_F \geq \delta_F$. If $\tau_F = \delta_F$, we call F with optimal boomerang uniformity(resist boomerang attack).

Known infinite families of APN power functions over $\mathbb{F}_{2^n}$.

Family	Exponent	Conditions
Gold	$2^i + 1$	$\gcd(i, n) = 1$
Kasami	$2^{2i} - 2^i + 1$	$\gcd(i, n) = 1$
Welch	$2^t + 3$	$n = 2t + 1$
Niho	$2^t + 2^{\frac{t}{2}} - 1$, t even	$n = 2t + 1$
	$2^t + 2^{\frac{(3t+1)}{2}} - 1$, t odd	
Inverse	$2^{2t} - 1$	$n = 2t + 1$
Dobbertin	$2^{4i} + 2^{3^i} + 2^{2^i} + 2^i - 1$	$n = 5i$

Conjecture

There are only 6 infinite classes of APN power functions.

Conjecture

when $n \geq 8$, there does not exist APN permutation on $\mathbb{F}_{2^n}$.

Conjecture

when $n \geq 8$*, there does not exist APN permutation on* $\mathbb{F}_{2^n}$*.*

Conjecture

when $n \equiv 0(mod\ 4)$*, there does not exist permutation with optimal boomerang uniformity on* $\mathbb{F}_{2^n}$*.*