Radbound University

Univariate representations of χ_n

Jan Schoone, Joan Daemen

Radboud University

9 February 2024

ESCADA

Introduction

$$\chi_n \colon \mathbb{F}_2^n \to \mathbb{F}_2^n,\ \vec{x} \mapsto \vec{y}$$
$$y_i = x_i + (x_{i+1} + 1)x_{i+2}$$

Investigate univariate form of χ_n:

- Power function;
- Degree;
- Number of monomials;
- Different forms.

Univariate expressions

- Choosing an isomorphism (of vector spaces) from $\mathbb{F}_2^n$ to $\mathbb{F}_{2^n}$: χ_n as a univariate polynomial function: $\chi_n^u(X)$ on $\mathbb{F}_{2^n}$.
- In practice: interpolation on the inputs and outputs for χ_n to obtain $\chi_n^u(X)$.
- Different outcomes for $\chi_n^u(X)$ possible.

Example

Take $\mathbb{F}_{2^3} := \mathbb{F}_2(\alpha) = \mathbb{F}_2[X]/(X^3 + X + 1)$, then the set $\{\alpha^3, \alpha^6, \alpha^5\}$ is a linearly independent set. Let $\varphi \colon \mathbb{F}_2^3 \to \mathbb{F}_{2^3}$ be given by $(a, b, c) \mapsto a\alpha^3 + b\alpha^6 + c\alpha^5$.

$\mathbb{F}_{2^3}^* = \{1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6\}$:

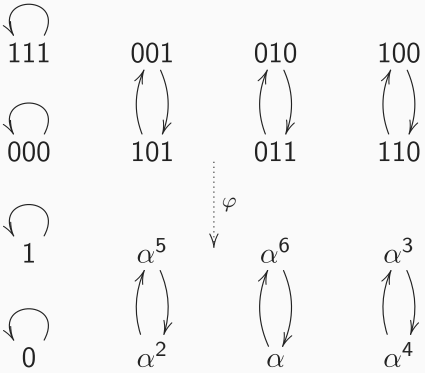
$\alpha^3 = \alpha + 1$

$\alpha^4 = \alpha^2 + \alpha$

$\alpha^5 = \alpha^3 + \alpha^2 = \alpha^2 + \alpha + 1$

$\alpha^6 = (\alpha + 1)^2 = \alpha^2 + 1$

Hence, $\chi_3^u(t) = t^6$.



Power functions

- A *power function* is a function $(-)^e \colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n},\ t \mapsto t^e$.
- Invertible iff $\gcd(e, 2^n - 1) = 1$.
- Easy: χ_n is not a power function when n even.
  $\chi_n((01)^{n/2}) = 0^n \implies \alpha^e = 0$ for some non-zero $\alpha \in \mathbb{F}_{2^n}$.
- Less easy: χ_n is not a power function when $n > 3$.
  Done by investigating the differential probabilities for χ_n and power functions.

Bounds on degrees

- Fact: Since χ_n has degree 2, all exponents in $\chi_n^u(X)$ need to have binary Hamming weight at most 2.
- The degree of χ_n^u is bounded by $2^n - 1$ $(= \#\mathbb{F}_{2^n}^*)$.
- Combining, yields maximum degrees for χ_n^u: $2^{n-1} + 2^{n-2}$.

n	3	5	7	9	11	13	15	17
$\max\deg(\chi_n^u)$	6	24	96	384	1,536	6,144	24,576	98,304
$2^n - 1$	7	31	127	511	2,047	8,191	32,767	131,071

Bounds on sparsity

- Fact: Since χ_n has degree 2, all exponents in $\chi_n^u(X)$ need to have binary hamming weight at most 2.
- $\chi_n(0^n) = 0^n$, so no constant term in $\chi_n^u(X)$.
- Number of monomials bounded by $\binom{n}{1} + \binom{n}{2}$.

n	3	5	7	9	11	13	15	17
max. mon. in χ_n^u	6	15	28	45	66	91	120	153
2^n	8	32	128	512	2,048	8,192	32,768	131,072

Definition (Normal basis)

Consider $\mathbb{F}_2 \subset \mathbb{F}_{2^n}$. Then $\beta \in \mathbb{F}_{2^n}$ is called a *normal element* of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ if the set $\{\beta, \beta^2, \beta^{2^2}, \ldots, \beta^{2^{n-1}}\}$ is a linearly independent set. When considered as an ordered set, it is called a *normal basis* of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$.

Theorem

Let $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a shift-invariant map. Let β be a normal element of $\mathbb{F}_{2^n}$ and $\varphi_\beta\colon \mathbb{F}_2^n \to \mathbb{F}_{2^n}$, $(x_0, \ldots, x_{n-1}) \mapsto x_0\beta + \ldots + x_{n-1}\beta^{2^{n-1}}$. Consider the map $F^u\colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ defined by $F^u := \varphi_\beta \circ F \circ \varphi_\beta^{-1}$. Then F^u is a polynomial function with $F^u(X) \in \mathbb{F}_2[X]$.

Different univariate expressions

- For $\mathbb{F}_{2^n} := \mathbb{F}_2[X]/(f(X))$ with $\deg f = n$. The choice of the polynomial does not matter!
- Choosing an (ordered) normal basis gives $\chi_n^u \in \mathbb{F}_2[X]$.
- Different normal elements possible.

Theorem (Number of normal elements (Ore, 1934))

Let $n \geq 1$ be an integer. There exist precisely $\Phi_2(X^n - 1)/n$ normal elements in $\mathbb{F}_{2^n}$ (w.r.t. $\mathbb{F}_2$).

- Different orderings of the normal basis possible.
  There are $\varphi(n)$ different orderings given a normal element.

Number of normal elements

Theorem (Number of normal elements (Ore, 1934))

Let $n \geq 1$ be an integer. There exist precisely $\Phi_2(X^n - 1)/n$ normal elements in $\mathbb{F}_{2^n}$ (w.r.t. $\mathbb{F}_2$).

Definition

For the number of coprime polynomials in $\mathbb{F}_2[X]$ that have lower degree than a certain f and are coprime to that f, we write $\Phi_2(f(X))$.

This is, in fact, an extension of the regular $\varphi(n)$ on the ring of integers. It is also equivalent to $\#(\mathbb{F}_2[X]/(f(X))^*$.

Example

If f is irreducible, then $\Phi_2(f(X)) = 2^{\deg f} - 1$.

Let $f(X) = X^4 + X^3 + X + 1$, then $\Phi_2(f) = \Phi_2(X^2 + 1)\Phi_2(X^2 + X + 1) = 2 \cdot 3 = 6$.

Number of orderings of the normal basis

- Let $\gcd(k, n) = 1$. We want to solve the equation $\varphi_\beta^\sigma \circ \tau^k = (\cdot)^2 \circ \varphi_\beta^\sigma$ for $\sigma \in S_n$. We have $\sigma(0) = 0$, since χ_n is shift-invariant.
- $n = 5, \ k = 3$:

$$\begin{array}{ccc}
(x_0, x_1, x_2, x_3, x_4) & \xmapsto{\varphi_\beta^\sigma} & x_0\beta + x_1\beta^{2^{\sigma(1)}} + x_2\beta^{2^{\sigma(2)}} + x_3\beta^{2^{\sigma(3)}} + x_4\beta^{2^{\sigma(4)}} \\
\Big\downarrow \tau^3 & & \Big\downarrow (\cdot)^2 \\
 & & x_0\beta^2 + x_1\beta^{2^{\sigma(1)+1}} + x_2\beta^{2^{\sigma(2)+1}} + x_3\beta^{2^{\sigma(3)+1}} + x_4\beta^{2^{\sigma(4)+1}} \\
 & & \| \\
(x_3, x_4, x_0, x_1, x_2) & \xmapsto[\varphi_\beta^\sigma]{} & x_3\beta + x_4\beta^{2^{\sigma(1)}} + x_0\beta^{2^{\sigma(2)}} + x_1\beta^{2^{\sigma(3)}} + x_2\beta^{2^{\sigma(4)}}
\end{array}$$

Thus: $\sigma = (1\ 3\ 4\ 2)$.

Conclusions

- The map χ_n can be viewed as a univariate map;
- Although it is never a power function for $n \neq 1, 3$;
- $\deg \chi_n^u \leq 2^{n-1} + 2^{n-2}$;
- The number of monomials in χ_n^u is upper bounded by $\binom{n}{1} + \binom{n}{2}$;
- The number of different univariate expressions for χ_n^u is given by

$$\frac{\Phi_2(X^n - 1) \cdot \varphi(n)}{n}$$

Thank you for your attention!