On the Algebraic Normal Form and Walsh Spectrum of Symmetric Functions Over Finite Rings

Boris Batteux

July 17, 2012

Cryptographic properties of functions

The Algebraic Normal Form and the Walsh Spectrum gives a lot of information on the cryptographic quality of a function:

- The ANF of a function allows to determine its algebraic degree d. The algebraic degree needs to be high to resist to algebraic attacks.
- The Walsh Spectrum of a function is linked to its non linearity and its order of resiliency t.

However, there exists trade-off between theses important properties, for instance:

Siegenthaler extension (Camion et al.)

For any q-ary function of n variables:

$$d + t < (q - 1)n$$

Symmetric functions

We will focus on symmetric functions over finite rings.

Why using symmetric functions?

- implementation efficiency: the number of gates needed to implement them in hardware is polynomial in number of input.
- multiple inputs give the same output: may be useful in a filtering function of LFSRs.

Summary

This presentation will be divided in 4 parts:

- Link between partitions and symmetric functions.
- Algorithm to compute ANF description.
- Algorithm to compute Walsh Spectrum description.
- Description of a searching strategy.

Partition

A partition $\lambda = (\lambda_1, \ldots, \lambda_n)$ of an integer k in n parts, whose largest part is A, is a sequence of n integers $A \geq \lambda_1 \geq \ldots \geq \lambda_n \geq 0$ such as $k = \sum_{i=1}^{n} \lambda_i$.
For any $x \in (\mathbb{Z}/q\mathbb{Z})^n$, we denote by $P_{n,q}(x)$ the symmetry class of x:

$$\{y \in (\mathbb{Z}/q\mathbb{Z})^n \mid \exists \sigma \in S_n \text{ such that } y = \sigma(x)\}$$

Andrew's lemma

We define $\mathrm{Part}(A, n, nA) = \{$ partition of an integer inferior or equal to nA in n part whose largest part is A $\}$

$$\mathrm{Card}\left(\mathrm{Part}(A, n, nA)\right) = \binom{n+A}{A}$$

Andrew's Lemma $\Rightarrow \binom{n+q-1}{q-1} := N$ distinct symmetry classes in $(\mathbb{Z}/q\mathbb{Z})^n$.
The only partition of a symmetry class is designated as its representative.
We denote by s_j the j^{th} representative according to the lexicographical order.

Definitions

Notations

$\mathcal{M}_n(q, r)$ is the set of functions from $(\mathbb{Z}/q\mathbb{Z})^n$ to $(\mathbb{Z}/r\mathbb{Z})$.
$\mathcal{SM}_n(q, r)$ is the set of symmetric functions from $(\mathbb{Z}/q\mathbb{Z})^n$ to $(\mathbb{Z}/r\mathbb{Z})$.

Symmetric functions

A function of $\mathcal{M}_n(q, r)$ is said to be symmetric if:

$$\begin{aligned} & \forall x \in (\mathbb{Z}/q\mathbb{Z})^n,\ \forall \sigma \in S_n,\ f(x_1, \ldots, x_n) = f(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) \\ \Leftrightarrow\ & \forall x \in (\mathbb{Z}/q\mathbb{Z})^n,\ \forall y \in P_{n,q}(x),\ f(x) = f(y) \end{aligned}$$

$\Longrightarrow$ We only need N values to characterize a function of $\mathcal{SM}_n(q, r)$.

Value vector and simplified value vector

- $f \in \mathcal{M}_n(q,r) \longleftrightarrow f_v \in (\mathbb{Z}/r\mathbb{Z})^{q^n}$

$$f_v = (f(\alpha_1), \ldots, f(\alpha_{q^n}))$$

where α_j is the j^{th} element of E_q^n according to the lexicographical order.

- $f \in \mathcal{SM}_n(q,r) \longleftrightarrow f_{sv} \in (\mathbb{Z}/r\mathbb{Z})^N$

$$f_{sv} = (f(s_1), \ldots, f(s_N))$$

where s_j is the j^{th} partition according to the lexicographical order.

Definition

Algebraic Normal Form

Let $f \in \mathcal{M}_n(q, m)$, f can be expressed as a polynomial, called its Algebraic Normal Form:

$$f(x_1, \ldots, x_n) = \sum_{(a_1,\ldots,a_n) \in E_q^n} \underbrace{h_f(a_1, \ldots, a_n)}_{\in \mathbb{Z}/r\mathbb{Z}} x_1^{a_1} \ldots x_n^{a_n} \mod r$$

The ANF of f can be represented by the vector $f_{ANF} \in (\mathbb{Z}/r\mathbb{Z})^{q^n}$:

$$f_{ANF} = (h_f(\alpha_1), \ldots, h_f(\alpha_{q^n}))$$

Symmetric functions ANF

If λ is a partition, we denoted by m_λ the symmetric polynomial defined by:

$$m_\lambda(x) = \sum x_{i_1}^{\lambda_1} \cdots x_{i_n}^{\lambda_n}$$

where the sum is over all distinct monomials whose exponent is λ.

Symmetric functions characterization with ANF

Let $f \in \mathcal{M}_n(q, r)$, f is symmetric if and only if its ANF can be written as follows:

$$f(x) = \sum_{i=1}^{n} h_f(s_j) m_{s_j}(x) \mod r$$

The ANF of $f \in \mathcal{SM}_n(q, r)$ can be represented by the vector $f_{sANF} \in (\mathbb{Z}/r\mathbb{Z})^N$:

$$f_{sANF} = (h_f(s_1), \ldots, h_f(s_N))$$

Algorithm description

Our goal is to define an algorithm to switch from f_{sv} to f_{sANF}.

- 1. First we compute the simplified value vector of each m_{s_j} for $j \in \{1, \ldots, N\}$ to obtain a matrix ANF_to_SV.
- 2. We inverse it to obtain a matrix SV_to_ANF.
- 3. We can switch from f_{sv} to f_{sANF} with one matrix multiplication ($\mathcal{O}(N^2)$).

Computing ANF_to_SV

- All we have to do is computing the value vector of all m_{s_j}. But we can't compute the value vector of each q^n monomial because it is impossible when n is high.
- Our solution consists in computing the value vector of a $m_{s_{j_0}}$ using only value vectors of m_{s_j} for $j < j_0$.

Mathematical Background

Let $x \in (\mathbb{Z}/q\mathbb{Z})^n$ and $\lambda \in (\mathbb{Z}/q\mathbb{Z})^n$.
The matrix ANF_to_SV can be computed using the 4 following rules:

- $m_{(0,\ldots,0)}(x) = 1$

Mathematical Background

Let $x \in (\mathbb{Z}/q\mathbb{Z})^n$ and $\lambda \in (\mathbb{Z}/q\mathbb{Z})^n$.

The matrix ANF_to_SV can be computed using the 4 following rules:

- $m_{(0,\ldots,0)}(x) = 1$
- If $hw(x) < hw(\lambda)$: $m_\lambda(x) = 0$

Mathematical Background

Let $x \in (\mathbb{Z}/q\mathbb{Z})^n$ and $\lambda \in (\mathbb{Z}/q\mathbb{Z})^n$.
The matrix *ANF_to_SV* can be computed using the 4 following rules:

- $m_{(0,\ldots,0)}(x) = 1$
- If $hw(x) < hw(\lambda)$: $m_\lambda(x) = 0$
- If $hw(x) = hw(\lambda)$, and k verifies $\lambda_k \neq 0$ and $\lambda_{k+1} = 0$:

$$\begin{aligned} m_\lambda(x) &= m_{(\lambda_k,\ldots,\lambda_k,0,\ldots,0)}(x) m_{(\lambda_1-\lambda_k,\ldots,\lambda_{k-1}-\lambda_k,0,\ldots,0)}(x) \\ &= (x_1 \cdots x_k)^{\lambda_k} m_{(\lambda_1-\lambda_n,\ldots,\lambda_{k-1}-\lambda_k,0,\ldots,0)}(x) \end{aligned}$$

Mathematical Background

Let $x \in (\mathbb{Z}/q\mathbb{Z})^n$ and $\lambda \in (\mathbb{Z}/q\mathbb{Z})^n$.
The matrix *ANF_to_SV* can be computed using the 4 following rules:

- $m_{(0,\ldots,0)}(x) = 1$
- If $hw(x) < hw(\lambda)$: $m_\lambda(x) = 0$
- If $hw(x) = hw(\lambda)$, and k verifies $\lambda_k \neq 0$ and $\lambda_{k+1} = 0$:

$$\begin{aligned} m_\lambda(x) &= m_{(\lambda_k,\ldots,\lambda_k,0,\ldots,0)}(x) m_{(\lambda_1-\lambda_k,\ldots,\lambda_{k-1}-\lambda_k,0,\ldots,0)}(x) \\ &= (x_1 \cdots x_k)^{\lambda_k} m_{(\lambda_1-\lambda_n,\ldots,\lambda_{k-1}-\lambda_k,0,\ldots,0)}(x) \end{aligned}$$

- If $hw(x) > hw(\lambda)$:

$$m_\lambda(x) = \sum_{\{i \mid hw(s_i)=hw(\lambda)\}} \left(m_\lambda(s_i) \prod_{j \in E_q^*} \binom{x[j]}{s_i[j]} \right)$$

Notation

For any $x \in (\mathbb{Z}/q\mathbb{Z})^n$ and $\ell \in (\mathbb{Z}/q\mathbb{Z})$, $x[\ell] = \mathrm{Card}\left(\{i \mid x_i = \ell\}\right)$

Example

Assume that we have:

$$\begin{cases} m_{(0,0,0)} &= (1,1,1,1,1,1,1,1,1,1) \\ m_{(1,0,0)} &= (0,1,2,2,0,1,0,1,2,0) \\ m_{(2,0,0)} &= (0,1,1,2,2,2,0,0,0,0) \end{cases}$$

Let's compute the simplified value vector of $m_{(2,1,0)}$:
If $x \in \{(0,0,0),(1,0,0),(2,0,0)\}$, $m_{(2,1,0)}(x) = 0$.

$$\Rightarrow m_{(2,1,0)} = (0,0,0,\cdot,\cdot,\cdot,\cdot,\cdot,\cdot,\cdot)$$

If $x \in \{(1,1,0),(2,1,0),(2,2,0)\}$, $m_{(2,1,0)}(x) = (x_1x_2)^1 m_{(1,0,0)}(x)$

$$\Rightarrow m_{(2,1,0)} = (0,0,0,2,0,1,\cdot,\cdot,\cdot,\cdot)$$

If $x \in \{(1,1,1),(2,1,1),(2,2,1),(2,2,2)\}$,

$$\begin{aligned} m_{(2,1,0)}(x) = \quad & m_{(2,1,0)}((1,1,0))\tbinom{x[1]}{2}\tbinom{x[2]}{0} + m_{(2,1,0)}((2,1,0))\tbinom{x[1]}{1}\tbinom{x[2]}{1} \\ & + m_{(2,1,0)}((2,2,0))\tbinom{x[1]}{0}\tbinom{x[2]}{2} \end{aligned}$$

$$\Rightarrow m_{(2,1,0)} = (0,0,0,2,0,1,0,2,1,0)$$

Example $q = 3,\ r = 3,\ n = 3$

$$\begin{pmatrix} 1\\1\\1\\1\\1\\1\\1\\1\\1\\1 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 & 0\\ 1 & 1 & 1\\ 1 & 2 & 1\\ 1 & & \\ 1 & & \\ 1 & & \\ 1 & & \\ 1 & & \\ 1 & & \\ 1 & & \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 & 0\\ 1 & 1 & 1\\ 1 & 2 & 1\\ 1 & 2 & 2\\ 1 & 0 & 2\\ 1 & 1 & 2\\ 1 & 0 & 0\\ 1 & 1 & 0\\ 1 & 2 & 0\\ 1 & 0 & 0 \end{pmatrix}$$

$$\rightarrow \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0\\ 1 & 1 & 1 & 0 & 0 & 0\\ 1 & 2 & 1 & 0 & 0 & 0\\ 1 & 2 & 2 & 1 & 2 & 1\\ 1 & 0 & 2 & 2 & 0 & 1\\ 1 & 1 & 2 & 1 & 1 & 1\\ 1 & 0 & 0 & & & \\ 1 & 1 & 0 & & & \\ 1 & 2 & 0 & & & \\ 1 & 0 & 0 & & & \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0\\ 1 & 1 & 1 & 0 & 0 & 0\\ 1 & 2 & 1 & 0 & 0 & 0\\ 1 & 2 & 2 & 1 & 2 & 1\\ 1 & 0 & 2 & 2 & 0 & 1\\ 1 & 1 & 2 & 1 & 1 & 1\\ 1 & 0 & 0 & 0 & 0 & 0\\ 1 & 1 & 0 & 2 & 2 & 0\\ 1 & 2 & 0 & 2 & 1 & 0\\ 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

$$\rightarrow \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 1 & 2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 1 & 2 & 2 & 1 & 2 & 1 & 0 & 0 & 0 & 0\\ 1 & 0 & 2 & 2 & 0 & 1 & 0 & 0 & 0 & 0\\ 1 & 1 & 2 & 1 & 1 & 1 & 0 & 0 & 0 & 0\\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1\\ 1 & 1 & 0 & 2 & 2 & 0 & 2 & 2 & 1 & 1\\ 1 & 2 & 0 & 2 & 1 & 0 & 1 & 2 & 2 & 1\\ 1 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 1 \end{pmatrix} = ANF\_to\_SV$$

Link between f_{sANF} and f_{sv}

Knowing ANF_to_SV, we can use following relations to calculate f_{sv} from f_{sANF}:

- $f_{sv} = ANF\_to\_SV \times f_{sANF}$
- If ANF_to_SV is invertible, $f_{sANF} = (ANF\_to\_SV)^{-1} \times f_{sv}$
- If ANF_to_SV is singular, f_{sANF} will be either solutions of $f_{sv} = ANF\_to\_SV \times X$

Example

$$\begin{aligned} m_{(2,0,0,0)}((x_1, x_2, x_3, x_4)) &= x_1^2 + x_2^2 + x_3^2 + x_4^2 \pmod 2 \\ &= x_1 + x_2 + x_3 + x_4 \pmod 2 \\ &= m_{(1,0,0,0)}((x_1, x_2, x_3, x_4)) \end{aligned}$$

Definition

Walsh spectrum

Let $f \in \mathcal{M}_n(q, m)$. The Walsh coefficient of f in point $a \in (\mathbb{Z}/q\mathbb{Z})^n$ corresponds to:

$$\mathcal{F}(f + \phi_a) = \sum_{x \in (\mathbb{Z}/q\mathbb{Z})^n} w^{f(x) - a \cdot x}$$

where $w = e^{\frac{2i\pi}{r}}$.
The Walsh spectrum of f can be represented by the vector $f_{WS} \in \mathbb{C}^{q^n}$:

$$f_{WS} = (\mathcal{F}(f + \phi_{\alpha_1}), \ldots, \mathcal{F}(f + \phi_{\alpha_{q^n}}))$$

Symmetric functions Walsh Spectrum

Simplified Walsh spectrum

Let $f \in \mathcal{SM}_n(q, m)$. The Walsh coefficient of f in point $a \in (\mathbb{Z}/q\mathbb{Z})^n$ verifies:

$$\mathcal{F}(f + \phi_a) = \sum_{i=1}^{N} \left(w^{f(s_i)} \sum_{x \in P_{n,q}(s_i)} w^{-a \cdot x} \right)$$

The simplified Walsh spectrum of f can be represented by the vector $f_{sWS} \in \mathbb{C}^N$:

$$f_{sWS} = (\mathcal{F}(f + \phi_{s_1}), \ldots, \mathcal{F}(f + \phi_{s_N}))$$

Walsh Matrix

We introduce the Walsh matrix defined by:

$$W_{q,r,n}[i][j] = \sum_{x \in P_{n,q}(s_i)} w^{-s_j \cdot x}$$

Algorithm description

- 1. Generate $W_{r,r,n}$.
- 2. Create $W_{q,r,n}$ using $W_{r,r,n}$.
- 3. We can switch from f_{sv} to f_{sWS} with one matrix multiplication ($\mathcal{O}(N^2)$).

$W_{r,r,n}$ generation

If $r = 2$, we have:

$$W_{2,2,n}[i][j] = K_i(j, n) = \sum_{j=0}^{i} \binom{x}{j} \binom{n-x}{i-j}$$

So, $W_{2,2,n}$ can be built using Krawtchouk polynomials.
However, we didn't find an extension for $r > 2$.

Mathematical background

Our algorithm is based on the 2 following rules:

- If $(s_{j_1} \mod r) \in P_{q,n}(s_{j_2})$, then for all $i \in \{1, \ldots, N\}$:

$$\sum_{x \in P_{n,q}(s_i)} w^{-s_{j_1} \cdot x} = \sum_{x \in P_{n,q}(s_i)} w^{-s_{j_2} \cdot x}$$

$$\Longrightarrow W_{q,r,n}[\cdot][j_1] = W_{q,r,n}[\cdot][j_2]$$

- If $(s_{i_1} \mod r) \in P_{q,n}(s_{i_2})$, then for all $j \in \{1, \ldots, N\}$:

$$\sum_{x \in P_{q,n}(s_i)} w^{-s_{j_1} \cdot x} = \frac{\mathrm{Card}(P_{q,n}(s_{i_1}))}{\mathrm{Card}(P_{q,n}(s_{i_2}))} \sum_{x \in P_{q,n}(s_i)} w^{-s_{j_2} \cdot x}$$

$$\Longrightarrow W_{q,r,n}[i_1][\cdot] = \frac{\mathrm{Card}(P_{q,n}(s_{i_1}))}{\mathrm{Card}(P_{q,n}(s_{i_2}))} W_{q,r,n}[i_2][\cdot]$$

Algorithm description

Partition of $(\mathbb{Z}/2\mathbb{Z})^4$: $(0,0,0,0)$
Partition of $(\mathbb{Z}/3\mathbb{Z})^4$: $(0,0,0,0)(2,0,0,0)(2,2,0,0)(2,2,2,0)(2,2,2,2)$

$$W_{2,2,4} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 4 & 2 & 0 & -2 & -4 \\ 6 & 0 & -2 & 0 & 6 \\ 4 & -2 & 0 & 2 & -4 \\ 1 & -1 & 1 & -1 & 1 \end{pmatrix}$$

$$\downarrow$$

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 4 & 4 & 4 & 4 & 4 \\ 6 & 6 & 6 & 6 & 6 \\ 4 & 4 & 4 & 4 & 4 \\ 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Algorithm description

Partition of $(\mathbb{Z}/2\mathbb{Z})^4$: $(1,0,0,0)$
Partition of $(\mathbb{Z}/3\mathbb{Z})^4$: $(1,0,0,0),(2,1,0,0),(2,2,1,0),(2,2,2,1)$

$$W_{2,2,4} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 4 & 2 & 0 & -2 & -4 \\ 6 & 0 & -2 & 0 & 6 \\ 4 & -2 & 0 & 2 & -4 \\ 1 & -1 & 1 & -1 & 1 \end{pmatrix}$$

$$\downarrow$$

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 4 & 2 & 4 & 2 & 4 & 2 & 4 & 2 & 4 \\ 6 & 0 & 6 & 0 & 6 & 0 & 6 & 0 & 6 \\ 4 & -2 & 4 & -2 & 4 & -2 & 4 & -2 & 4 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 \end{pmatrix}$$

Algorithm description

Partition of $(\mathbb{Z}/2\mathbb{Z})^4$: $(1,1,0,0)$
Partition of $(\mathbb{Z}/3\mathbb{Z})^4$: $(1,1,0,0),(2,1,1,0),(2,2,1,1)$

$$W_{2,2,4} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 4 & 2 & 0 & -2 & -4 \\ 6 & 0 & -2 & 0 & 6 \\ 4 & -2 & 0 & 2 & -4 \\ 1 & -1 & 1 & -1 & 1 \end{pmatrix}$$

$$\downarrow$$

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 4 & 2 & 4 & 0 & 2 & 4 & 0 & 2 & 4 & 0 & 2 & 4 \\ 6 & 0 & 6 & -2 & 0 & 6 & -2 & 0 & 6 & -2 & 0 & 6 \\ 4 & -2 & 4 & 0 & -2 & 4 & 0 & -2 & 4 & 0 & -2 & 4 \\ 1 & -1 & 1 & 1 & -1 & 1 & 1 & -1 & 1 & 1 & -1 & 1 \end{pmatrix}$$

Algorithm description

Partition of $(\mathbb{Z}/2\mathbb{Z})^4$: $(1,1,1,0)$
Partition of $(\mathbb{Z}/3\mathbb{Z})^4$: $(1,1,1,0), (2,1,1,1)$

$$W_{2,2,4} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 4 & 2 & 0 & -2 & -4 \\ 6 & 0 & -2 & 0 & 6 \\ 4 & -2 & 0 & 2 & -4 \\ 1 & -1 & 1 & -1 & 1 \end{pmatrix}$$

$$\downarrow$$

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 4 & 2 & 4 & 0 & 2 & 4 & -2 & 0 & 2 & 4 & -2 & 0 & 2 & 4 \\ 6 & 0 & 6 & -2 & 0 & 6 & 0 & -2 & 0 & 6 & 0 & -2 & 0 & 6 \\ 4 & -2 & 4 & 0 & -2 & 4 & 2 & 0 & -2 & 4 & 2 & 0 & -2 & 4 \\ 1 & -1 & 1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 \end{pmatrix}$$

Algorithm description

Partition of $(\mathbb{Z}/2\mathbb{Z})^4$: $(1,1,1,1)$
Partition of $(\mathbb{Z}/3\mathbb{Z})^4$: $(1,1,1,1)$

$$W_{2,2,4} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 4 & 2 & 0 & -2 & -4 \\ 6 & 0 & -2 & 0 & 6 \\ 4 & -2 & 0 & 2 & -4 \\ 1 & -1 & 1 & -1 & 1 \end{pmatrix}$$

$$\downarrow$$

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 4 & 2 & 4 & 0 & 2 & 4 & -2 & 0 & 2 & 4 & -4 & -2 & 0 & 2 & 4 \\ 6 & 0 & 6 & -2 & 0 & 6 & 0 & -2 & 0 & 6 & 6 & 0 & -2 & 0 & 6 \\ 4 & -2 & 4 & 0 & -2 & 4 & 2 & 0 & -2 & 4 & -4 & 2 & 0 & -2 & 4 \\ 1 & -1 & 1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 & 1 \end{pmatrix}$$

Algorithm description

$$
\begin{array}{l}
(0,0,0,0)\\
(1,0,0,0)\\
(1,1,0,0)\\
(1,1,1,0)\\
(1,1,1,1)
\end{array}
\begin{pmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1\\
4 & 2 & 4 & 0 & 2 & 4 & -2 & 0 & 2 & 4 & -4 & -2 & 0 & 2 & 4\\
6 & 0 & 6 & -2 & 0 & 6 & 0 & -2 & 0 & 6 & 6 & 0 & -2 & 0 & 6\\
4 & -2 & 4 & 0 & -2 & 4 & 2 & 0 & -2 & 4 & -4 & 2 & 0 & -2 & 4\\
1 & -1 & 1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 & 1
\end{pmatrix}
$$

$$\downarrow$$

$$
\begin{array}{lr}
(0,0,0,0) & 1\\
(1,0,0,0) & 4\\
(2,0,0,0) & 4\\
(1,1,0,0) & 6\\
(2,1,0,0) & 12\\
(2,2,0,0) & 6\\
(1,1,1,0) & 4\\
(2,1,1,0) & 12\\
(2,2,1,0) & 12\\
(2,2,2,0) & 4\\
(1,1,1,1) & 1\\
(2,1,1,1) & 4\\
(2,2,1,1) & 6\\
(2,2,2,1) & 4\\
(2,2,2,2) & 1
\end{array}
\begin{pmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1\\
4 & 2 & 4 & 0 & 2 & 4 & -2 & 0 & 2 & 4 & -4 & -2 & 0 & 2 & 4\\
4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4\\
6 & 0 & 6 & -2 & 0 & 6 & 0 & -2 & 0 & 6 & 6 & 0 & -2 & 0 & 6\\
12 & 6 & 12 & 0 & 6 & 12 & -6 & 0 & 6 & 12 & -12 & -6 & 0 & 6 & 12\\
6 & 6 & 6 & 6 & 6 & 6 & 6 & 6 & 6 & 6 & 6 & 6 & 6 & 6 & 6\\
4 & -2 & 4 & 0 & -2 & 4 & 2 & 0 & -2 & 4 & -4 & 2 & 0 & -2 & 4\\
12 & 0 & 12 & -4 & 0 & 12 & 0 & -4 & 0 & 12 & 12 & 0 & -4 & 0 & 12\\
12 & 6 & 12 & 0 & 6 & 12 & -6 & 0 & 6 & 12 & -12 & -6 & 0 & 6 & 12\\
4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4\\
1 & -1 & 1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 & 1\\
4 & -2 & 4 & 0 & -2 & 4 & 2 & 0 & -2 & 4 & -4 & 2 & 0 & -2 & 4\\
6 & 0 & 6 & -2 & 0 & 6 & 0 & -2 & 0 & 6 & 6 & 0 & -2 & 0 & 6\\
4 & 2 & 4 & 0 & 2 & 4 & -2 & 0 & 2 & 4 & -4 & -2 & 0 & 2 & 4\\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1
\end{pmatrix}
$$

Link between f_{sv} and f_{sWS}

Knowing $W_{q,r,n}$, we can calculate f_{sWS} from f_{sv} using the following relations:

- $\phi(f_{sv}) = (w^{f(s_1)}, \ldots, w^{f(s_n)})$
- $f_{sWS} = W_{q,r,n}^T \times \phi(f_{sv})$

Gray codes

Gray Code

- A Gray Code is a code where each word differs from the next in only one digit.
- We denote by (q, n)-Gray Code, the q-ary Gray Code with n digits.

For instance, $(3, 2)$-Gray Code is:

$$\{(00), (01), (02), (12), (10), (11), (21), (22), (20)\}$$

Method

Using the (r, N)-Gray code, we are able to create a list (f^j) of r^N vectors of $\mathbb{Z}_r^N$ such as:

$$\exists! i_j \in \{1, \ldots, N\} \text{ such that } f^j(s_{i_j}) \neq f^{j+1}(s_{i_j})$$

Knowing the associated ANF and Walsh Spectrum of f^j, we can compute the ANF and Walsh Spectrum of f^{j+1} in $\mathcal{O}(N)$ additions:

- $f^{j+1}_{sANF} = f^j_{sANF} + (f^{j+1}(s_{i_j}) - f^j(s_{i_j}))SV\_to\_ANF[\cdot][i_j]$
- $f^{j+1}_{sWS} = f^j_{sWS} + (w^{f^{j+1}(s_{i_j})} - w^{f^j(s_{i_j})})W_{q,r,n}[\cdot][i_j]$

Complexities results

q	2					3		4
n	10	20	30	40	100	5	10	5
Our complexity	2^{14}	2^{25}	2^{36}	2^{46}	2^{108}	2^{19}	2^{61}	2^{62}
Other complexity	2^{24}	2^{45}	2^{66}	2^{86}	2^{208}	2^{25}	2^{74}	2^{68}

Conclusion

Our contribution consists in:

- An algorithm to compute ANF of symmetric functions over finite rings.
- An algorithm to compute Walsh spectrum of symmetric functions over finite rings.
- A searching method using Gray codes.

Questions

Thanks for your attention.
Questions ?