Weightwise Almost Perfectly Balanced Functions, Construction From A Permutation Group Action View

Deepak Kumar DALAI, Krishna MALLICK, Pierrick MÉAUX

Luxembourg University, Luxembourg

Dubrovnik — Croatia
Tuesday September 10th

Summary

Balanced and weightwise perfectly balanced functions

$$f: \mathbb{F}_2^4 \to \mathbb{F}_2$$

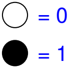
0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1

Balanced and weightwise perfectly balanced functions

$$f\colon \mathbb{F}_2^4 \to \mathbb{F}_2$$

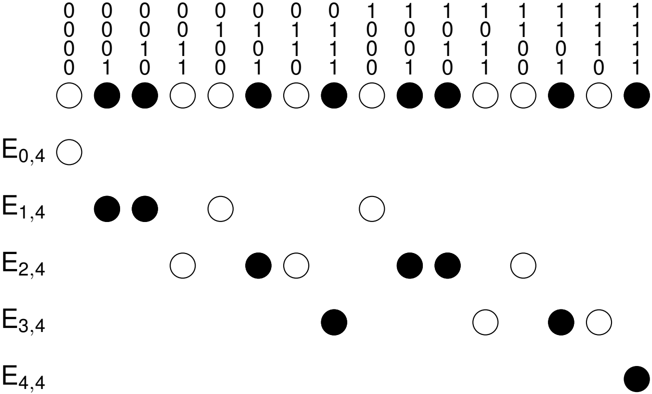
0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1

$\boxed{\text{Balanced}}$



Balanced and weightwise perfectly balanced functions

$$f\colon \mathbb{F}_2^4 \to \mathbb{F}_2$$



$$E_{k,n} = \{x \in \mathbb{F}_2^n \mid w_H(x) = k\}$$

Weightwise almost perfectly balanced functions

Weightwise Perfectly Balanced function (WPB) [CMR17]

Let $n \in \mathbb{N}^*$, f is called WPB if:

- for all $k \in [1, n-1]$:
$$|\mathrm{supp}(f) \cap \mathsf{E}_{k,n}| = |\mathsf{E}_{k,n}|/2,$$
- $f(\mathbf{0}) = 0$, $f(\mathbf{1}) = 1$.

Weightwise almost perfectly balanced functions

Weightwise Perfectly Balanced function (WPB) [CMR17]

Let $n \in \mathbb{N}^*$, f is called WPB if:

- for all $k \in [1, n-1]$:
$$|\mathrm{supp}(f) \cap \mathsf{E}_{k,n}| = |\mathsf{E}_{k,n}|/2,$$
- $f(\mathbf{0}) = 0$, $f(\mathbf{1}) = 1$.

Weightwise Almost Perfectly Balanced:

$$\forall k \in [0, n], \quad \big| |\mathrm{supp}(f) \cap \mathsf{E}_{k,n}| - |\mathrm{supp}(f+1) \cap \mathsf{E}_{k,n}| \big| \leq 1$$

Weightwise almost perfectly balanced functions

Weightwise Perfectly Balanced function (WPB) [CMR17]

Let $n \in \mathbb{N}^*$, f is called WPB if:

- for all $k \in [1, n-1]$:
$$|\mathrm{supp}(f) \cap \mathsf{E}_{k,n}| = |\mathsf{E}_{k,n}|/2,$$
- $f(\mathbf{0}) = 0$, $f(\mathbf{1}) = 1$.

Weightwise Almost Perfectly Balanced:

$$\forall k \in [0, n], \quad \big|\, |\mathrm{supp}(f) \cap \mathsf{E}_{k,n}| - |\mathrm{supp}(f+1) \cap \mathsf{E}_{k,n}| \,\big| \leq 1$$

Motivations:

- cipher FLIP [MJSC16],
- properties on Boolean functions on restricted sets [CMR17],
- link with side channels: leakage of $\mathrm{w_H}(x)$ and $f(x)$.

State of the art

Various constructions:
CMR17, LM19, TL19, LS20, MS21, MSL21, Su21, ZS21, GM22b, GS22, MCL22, MPJDL22, MSLZ22, DM23, YCLXHJZ23, ZS23, ZJZQ23, ZLCQZ23, DM24, Méa24, ...

Study of cryptographic parameters:
Nonlinearity [GM23a], Weightwise NL [GM22a], Algebraic immunity [GM23b].

State of the art

Various constructions:
CMR17, LM19, TL19, LS20, MS21, MSL21, Su21, ZS21, GM22b, GS22, MCL22, MPJDL22, MSLZ22, DM23, YCLXHJZ23, ZS23, ZJZQ23, ZLCQZ23, DM24, Méa24, ...

Study of cryptographic parameters:
Nonlinearity [GM23a], Weightwise NL [GM22a], Algebraic immunity [GM23b].

Main issues:

- mostly WPB constructions,
- few constructions with proven/good nonlinearity,
- few constructions with proven/good weightwise nonlinearities.

State of the art

Various constructions:
CMR17, LM19, TL19, LS20, MS21, MSL21, Su21, ZS21, GM22b, GS22, MCL22, MPJDL22, MSLZ22, DM23, YCLXHJZ23, ZS23, ZJZQ23, ZLCQZ23, DM24, Méa24, ...

Study of cryptographic parameters:
Nonlinearity [GM23a], Weightwise NL [GM22a], Algebraic immunity [GM23b].

Main issues:

- mostly WPB constructions,
- few constructions with proven/good nonlinearity,
- few constructions with proven/good weightwise nonlinearities.

Contributions:

- construction based on group actions,
- proven bound of nonlinearity,
- proven bound of weightwise nonlinearities.

Summary

Liu-Mesnager functions

- introduced in 2019, $n = 2^m$
- use the field representation $\mathbb{F}_{2^n}$, monomial basis $\{\alpha, \alpha^2, \ldots, \alpha^{2^{n-1}}\}$
- definition:
  - $f(\mathbf{0}) = 0$, $f(\mathbf{1}) = 1$,
  - $f(x) = 1 + f(x^2)$, for all $x \in \mathbb{F}_{2^n} \setminus \{\mathbf{0}, \mathbf{1}\}$.

Liu-Mesnager functions

- introduced in 2019, $n = 2^m$
- use the field representation $\mathbb{F}_{2^n}$, monomial basis $\{\alpha, \alpha^2, \ldots, \alpha^{2^{n-1}}\}$
- definition:
  - $f(\mathbf{0}) = 0$, $f(\mathbf{1}) = 1$,
  - $f(x) = 1 + f(x^2)$, for all $x \in \mathbb{F}_{2^n} \setminus \{\mathbf{0}, \mathbf{1}\}$.

WPB?

$$x = (x_1, \ldots, x_n), \quad x^2 = (x_2, \ldots, x_n, x_1).$$

square $\rightarrow$ rotation by one position

Liu-Mesnager functions

- introduced in 2019, $n = 2^m$
- use the field representation $\mathbb{F}_{2^n}$, monomial basis $\{\alpha, \alpha^2, \ldots, \alpha^{2^{n-1}}\}$
- definition:
  - $f(\mathbf{0}) = 0$, $f(\mathbf{1}) = 1$,
  - $f(x) = 1 + f(x^2)$, for all $x \in \mathbb{F}_{2^n} \setminus \{\mathbf{0}, \mathbf{1}\}$.

WPB?

$$x = (x_1, \ldots, x_n), \quad x^2 = (x_2, \ldots, x_n, x_1).$$

square $\rightarrow$ rotation by one position

action of ρ_n on the slices

- orbit $O(x) = \{\rho_n^i(x) \mid i \in \mathbb{N}\}$
- ρ_n splits each slice of even cardinal in orbits of even size
- for $k \in [1, n-1]$, f is balanced on each orbit $\Rightarrow$ f balanced on each $\mathsf{E}_{k,n}$

Liu-Mesnager functions

- introduced in 2019, $n = 2^m$
- use the field representation $\mathbb{F}_{2^n}$, monomial basis $\{\alpha, \alpha^2, \ldots, \alpha^{2^{n-1}}\}$
- definition:
  - $f(\mathbf{0}) = 0$, $f(\mathbf{1}) = 1$,
  - $f(x) = 1 + f(x^2)$, for all $x \in \mathbb{F}_{2^n} \setminus \{\mathbf{0}, \mathbf{1}\}$.

WPB

$$x = (x_1, \ldots, x_n), \quad x^2 = (x_2, \ldots, x_n, x_1).$$

square $\rightarrow$ rotation by one position

action of ρ_n on the slices

- orbit $O(x) = \{\rho_n^i(x) \mid i \in \mathbb{N}\}$
- ρ_n splits each slice of even cardinal in orbits of even size
- for $k \in [1, n-1]$, f is balanced on each orbit $\Rightarrow$ f balanced on each $\mathrm{E}_{k,n}$

[LM19]: good NL and NL_k in practice, and proven bounds

Group action view

$\mathbb{S}_n$ symmetric group on n elements,
$\pi \in \mathbb{S}_n$, cyclic group $< \pi >$.

Group action view

$\mathbb{S}_n$ symmetric group on n elements,
$\pi \in \mathbb{S}_n$, cyclic group $< \pi >$.

$2\pi S$ functions

A Boolean function f is 2-π symmetric ($2\pi S$) if and only if for every orbit $\mathrm{O} \in \mathcal{O}$ with representative element v:

$$f(\pi^{2i+1}(v)) = f(v), \quad f(\pi^{2i}(v)) = f(v) + 1 \qquad \text{for every } 1 \leq i \leq \lfloor \frac{|\mathrm{O}|}{2} \rfloor.$$

Group action view

$\mathbb{S}_n$ symmetric group on n elements,
$\pi \in \mathbb{S}_n$, cyclic group $< \pi >$.

$2\pi S$ functions

A Boolean function f is 2-π symmetric ($2\pi S$) if and only if for every orbit $\mathrm{O} \in \mathcal{O}$ with representative element v:

$$f(\pi^{2i+1}(v)) = f(v), \quad f(\pi^{2i}(v)) = f(v) + 1 \qquad \text{for every } 1 \leq i \leq \lfloor \frac{|\mathrm{O}|}{2} \rfloor.$$

LM WPB functions are 2-rotation symmetric: $\pi = \rho_n$.

WAPB?

- each even orbit is well split,
- odd orbits have an extra 0 or extra 1 to be compensated.

Construction of 2πS WAPB Boolean functions

Input: $\pi \in \mathbb{S}_n$, orbits' representatives $v_{k,n,i}$.
Output: A 2πS WAPB Boolean function $f_\pi \in \mathcal{B}_n$.
Initiate $\mathrm{supp}(f_\pi) = \emptyset$.
Initiate $t = 0$.
for $k = 0$ to n **do**
    for $i \leftarrow 1$ to $g_{k,n}$ **do**
        $u = v_{k,n,i}$; $\ell = |O_\pi(u)|$.
        if ℓ is even **then**
            for $j \leftarrow 1$ to $\frac{\ell}{2}$ **do**
                $\mathrm{supp}(f_\pi)$.append(u)
                $u \leftarrow \pi \circ \pi(u)$
            end for
        else
            for $j \leftarrow 1$ to $\lceil \frac{\ell - t}{2} \rceil$ **do**
                $\mathrm{supp}(f_\pi)$.append(u)
                $u \leftarrow \pi \circ \pi(u)$
            end for
            Update $t \leftarrow 1 - t$
        end if
    end for
end for
return f_π

Summary

ψ_n

Definition:

- $n = n_1 + n_2 + \cdots + n_w$,
- $n_1 = 2^{a_1}, n_2 = 2^{a_2}, \ldots, n_w = 2^{a_w}$,
- $0 \leq a_1 < a_2 < \cdots < a_w$.

$$\psi_n = (x_1, x_2, \ldots, x_{n_1})(x_{n_1+1}, x_{n_1+2}, \ldots, x_{n_1+n_2}) \cdots (x_{n-n_w+1}, x_{n-n_w+2}, \ldots, x_n).$$

$$\psi_n(x) = (\rho_{n_1}(x_1, \ldots, x_{n_1}), \rho_{n_2}(x_{n_1+1}, \ldots, x_{n_1+n_2}), \ldots, \rho_{n_w}(x_{n-n_w+1}, \ldots, x_n)).$$

ψ_n

Definition:

- $n = n_1 + n_2 + \cdots + n_w$,
- $n_1 = 2^{a_1}, n_2 = 2^{a_2}, \ldots, n_w = 2^{a_w}$,
- $0 \leq a_1 < a_2 < \cdots < a_w$.

$$\psi_n = (x_1, x_2, \ldots, x_{n_1})(x_{n_1+1}, x_{n_1+2}, \ldots, x_{n_1+n_2}) \cdots (x_{n-n_w+1}, x_{n-n_w+2}, \ldots, x_n).$$

$$\psi_n(x) = (\rho_{n_1}(x_1, \ldots, x_{n_1}), \rho_{n_2}(x_{n_1+1}, \ldots, x_{n_1+n_2}), \ldots, \rho_{n_w}(x_{n-n_w+1}, \ldots, x_n)).$$

First properties:

- $ord(\psi) = 2^{a_w} = n_w$, $\Rightarrow$ orbits with cardinal a power of 2,
- there are 2^ω orbits of cardinal 1 where $\omega = \mathrm{w_H}(n)$.
- the number of orbits of weight k and cardinal 1 is 1 if $k \preceq n$, otherwise 0.

Example: $n = 6$, $\omega = \mathrm{w_H}(110) = 2$, orbits of lengths 1:

$$\{000000, 110000, 001111, 111111\}.$$

ψ_n

Definition:

- $n = n_1 + n_2 + \cdots + n_w$,
- $n_1 = 2^{a_1}, n_2 = 2^{a_2}, \ldots, n_w = 2^{a_w}$,
- $0 \leq a_1 < a_2 < \cdots < a_w$.

$$\psi_n = (x_1, x_2, \ldots, x_{n_1})(x_{n_1+1}, x_{n_1+2}, \ldots, x_{n_1+n_2}) \cdots (x_{n-n_w+1}, x_{n-n_w+2}, \ldots, x_n).$$

$$\psi_n(x) = (\rho_{n_1}(x_1, \ldots, x_{n_1}), \rho_{n_2}(x_{n_1+1}, \ldots, x_{n_1+n_2}), \ldots, \rho_{n_w}(x_{n-n_w+1}, \ldots, x_n)).$$

First properties:

- $ord(\psi) = 2^{a_w} = n_w$, $\Rightarrow$ orbits with cardinal a power of 2,
- there are 2^ω orbits of cardinal 1 where $\omega = \mathrm{w_H}(n)$.
- the number of orbits of weight k and cardinal 1 is 1 if $k \preceq n$, otherwise 0.

Proposition: if $f(\psi(x)) = 1 + f(x)$ holds for all $x \in \mathbb{F}_2^n \setminus \mathcal{O}_o$, then f is WAPB.

Nonlinearity bound

Nonlinearity

$$\mathrm{NL}(f) = \min_{g,\, \deg(g) \le 1} \{\mathrm{d_H}(f, g)\} = 2^{n-1} - \frac{1}{2} \max_{a \in \mathbb{F}_2^n} \Big| \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) + a \cdot x} \Big|.$$

Nonlinearity bound

Nonlinearity

$$\mathrm{NL}(f) = \min_{g,\, \deg(g) \leq 1} \{ \mathrm{d_H}(f, g) \} = 2^{n-1} - \frac{1}{2} \max_{a \in \mathbb{F}_2^n} \Big| \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) + a \cdot x} \Big|.$$

Theorem:

Let f be any function from Construction 1 with $\pi = \psi_n$:

$$\mathrm{NL}(f) \geq 2^{n-2} - 2^{\omega - 1}.$$

Nonlinearity bound

Nonlinearity

$$\mathrm{NL}(f) = \min_{g,\,\deg(g)\leq 1}\{\mathrm{d_H}(f,g)\} = 2^{n-1} - \frac{1}{2}\max_{a\in\mathbb{F}_2^n}\Big|\sum_{x\in\mathbb{F}_2^n}(-1)^{f(x)+a\cdot x}\Big|.$$

Theorem:

Let f be any function from Construction 1 with $\pi = \psi_n$:

$$\mathrm{NL}(f) \geq 2^{n-2} - 2^{\omega-1}.$$

Proof intuition:

- split the Walsh transform following the orbits,

Nonlinearity bound

Nonlinearity

$$\mathrm{NL}(f) = \min_{g,\,\deg(g)\leq 1}\{\mathrm{d_H}(f,g)\} = 2^{n-1} - \frac{1}{2}\max_{a\in\mathbb{F}_2^n}\Big|\sum_{x\in\mathbb{F}_2^n}(-1)^{f(x)+a\cdot x}\Big|.$$

Theorem:

Let f be any function from Construction 1 with $\pi = \psi_n$:

$$\mathrm{NL}(f) \geq 2^{n-2} - 2^{\omega-1}.$$

Proof intuition:

- split the Walsh transform following the orbits,
- split even and odd orbits,
- bound the contribution from odd orbits,

Nonlinearity bound

Nonlinearity

$$\mathrm{NL}(f) = \min_{g,\,\deg(g)\leq 1}\{\mathrm{d_H}(f,g)\} = 2^{n-1} - \frac{1}{2}\max_{a\in\mathbb{F}_2^n}\Big|\sum_{x\in\mathbb{F}_2^n}(-1)^{f(x)+a\cdot x}\Big|.$$

Theorem:

Let f be any function from Construction 1 with $\pi = \psi_n$:

$$\mathrm{NL}(f) \geq 2^{n-2} - 2^{\omega-1}.$$

Proof intuition:

- split the Walsh transform following the orbits,
- split even and odd orbits,
- bound the contribution from odd orbits,
- on even orbits, rewrite: $2\sum_{x\in O}(-1)^{f(x)+a\cdot x}$ as:

$$\sum_{x\in O}\left((-1)^{f(x)+a\cdot x} + (-1)^{f(\psi(x))+a\cdot\psi(x)}\right) = \sum_{x\in O}(-1)^{f(x)}\left((-1)^{a\cdot x} - (-1)^{a\cdot\psi(x)}\right)$$

Nonlinearity bound

Nonlinearity

$$\mathrm{NL}(f) = \min_{g,\, \deg(g)\leq 1} \{\mathrm{d_H}(f,g)\} = 2^{n-1} - \frac{1}{2} \max_{a\in\mathbb{F}_2^n} \Big| \sum_{x\in\mathbb{F}_2^n} (-1)^{f(x)+a\cdot x} \Big|.$$

Theorem:
Let f be any function from Construction 1 with $\pi = \psi_n$:

$$\mathrm{NL}(f) \geq 2^{n-2} - 2^{\omega-1}.$$

Proof intuition:

- split the Walsh transform following the orbits,
- split even and odd orbits,
- bound the contribution from odd orbits,
- on even orbits, rewrite: $2\sum_{x\in O}(-1)^{f(x)+a\cdot x}$ as:

$$\sum_{x\in O}\left((-1)^{f(x)+a\cdot x} + (-1)^{f(\psi(x))+a\cdot\psi(x)}\right) = \sum_{x\in O}(-1)^{f(x)}\left((-1)^{a\cdot x} - (-1)^{a\cdot\psi(x)}\right)$$

- terms cancel when $a\cdot(x+\psi(x)) = 0$,
- determine $|\{x\in\mathbb{F}_2^n \setminus \mathcal{O}_o : a\cdot(x+\psi(x)) = 1\}|$.

Nonlinearity in practice

$n \in [4, 6]$, exhaustive search.

n	4	5	6
# functions	$2^4 \times \binom{2}{1} = 2^5$	$2^8 \times \binom{4}{2} = 3 \times 2^9$	$2^{18} \times \binom{4}{2} = 3 \times 2^{19}$
NL achieved	$[4]$	$[6, 12]$	$[14, 26]$
% functions	100	4.17, 22.92	0.26, 0.65
Th. bounds	$[3, 4]$	$[6, 12]$	$[14, 26]$

$n \in [7, 10]$, random search.

n	7	8	9	10
# functions	$2^{36} \times \binom{8}{4} = 35 \times 2^{37}$	$2^{34} \times \binom{2}{1} = 2^{35}$	$2^{68} \times \binom{4}{2} = 3 \times 2^{69}$	$2^{138} \times \binom{4}{2} = 3 \times 2^{139}$
NL achieved	$[28, 56]$	$[64, 116]$	$[192, 236]$	$[328, 480]$
% functions	0.01, 0.30	0.01, 0.01	0.00, 0.07	0.00, 0.01
Th. bounds	$[28, 56]$	$[63, 116]$	$[144, 240]$	$[254, 492]$

Weightwise nonlinearity

Definition:

$$\mathrm{NL}_k(f) = \min_{g,\, \deg(g) \leq 1} \{\mathrm{d}_{\mathrm{H},\mathrm{E}_{\mathrm{k},\mathrm{n}}}(f, g)\} = \frac{|\mathrm{E}_{k,n}|}{2} - \frac{1}{2} \max_{a \in \mathbb{F}_2^n} \Big| \sum_{x \in \mathrm{E}_{k,n}} (-1)^{f(x)+a \cdot x} \Big|.$$

Weightwise nonlinearity

Definition:

$$\mathrm{NL}_k(f) = \min_{g,\,\deg(g)\leq 1}\{\mathrm{d}_{\mathrm{H},\mathrm{E}_{\mathrm{k,n}}}(f,g)\} = \frac{|\mathrm{E}_{k,n}|}{2} - \frac{1}{2}\max_{a\in\mathbb{F}_2^n}\Big|\sum_{x\in\mathrm{E}_{k,n}}(-1)^{f(x)+a\cdot x}\Big|.$$

Bound intuition:

- Walsh transform restricted to the slices, use of Krawtchouk polynomials,
- Bound $|\{x \in \mathrm{E}_{k,n} \setminus \mathcal{O}_o : a \cdot (x + \psi(x)) = 1\}|$.

Weightwise nonlinearity

Definition:

$$\mathrm{NL}_k(f) = \min_{g,\, \deg(g)\leq 1}\{\mathrm{d}_{\mathrm{H},\mathrm{E}_{k,n}}(f,g)\} = \frac{|\mathrm{E}_{k,n}|}{2} - \frac{1}{2}\max_{a\in\mathbb{F}_2^n}\Big|\sum_{x\in\mathrm{E}_{k,n}}(-1)^{f(x)+a\cdot x}\Big|.$$

Bound intuition:

- Walsh transform restricted to the slices, use of Krawtchouk polynomials,
- Bound $|\{x\in\mathrm{E}_{k,n}\setminus\mathcal{O}_o : a\cdot(x+\psi(x))=1\}|$.

Theorem:
Let f be any function from Construction 1 with $\pi=\psi_n$, for all $k\in[2,n-2]$:

$$\mathrm{NL}_k(f) \geq \begin{cases} \frac{1}{4}\left(\binom{n}{k} + \min\limits_{\substack{2\leq\ell\leq n\\ \ell \text{ even}}} \mathrm{K}_k(\ell,n)\right) & \text{if } k \not\preceq n,\\ \frac{1}{4}\left(\binom{n}{k} + \min\limits_{\substack{2\leq\ell\leq n\\ \ell \text{ even}}} \mathrm{K}_k(\ell,n) - 2\right) & \text{if } k \preceq n.\end{cases}$$

Summary

Conclusion and open questions

Conclusion:

- Construction of WAPB functions based on group actions,
- proven lower bounds of nonlinearity and NLk,
- functions with good nonlinearity in practice.

Conclusion and open questions

Conclusion:

- Construction of WAPB functions based on group actions,
- proven lower bounds of nonlinearity and NLk,
- functions with good nonlinearity in practice.

Open questions:

- improve the NLk bounds,
- generalize the NL and NLk results for all π.

Conclusion and open questions

Conclusion:

- Construction of WAPB functions based on group actions,
- proven lower bounds of nonlinearity and NLk,
- functions with good nonlinearity in practice.

Open questions:

- improve the NLk bounds,
- generalize the NL and NLk results for all π.

Thank you!