Weightwise Almost Perfectly Balanced functions, constructions from a group action view.

No Author Given

No Institute Given

Abstract.

1 Introduction

2 Preliminaries

3 Construction with half orbits

Generalization of LM construction based on group action, taking half of each orbit of even cardinal, and the alternatively the floor or ceiling of half of each orbit of odd cardinal. See Construction 1.

Input: $v \in \{-1, 0, 1\}^{n+1}$
Input: $\alpha \in \mathbb{S}_n$. One representative $r_{k,i}$ of each orbit of the action of $< \alpha >$ on $\mathsf{E}_{k,n}$. s_k the number of orbits of $\mathsf{E}_{k,n}$.
Output: $f \in \mathcal{WAPB}_n$.

Initiate $\mathsf{supp}(f) = \emptyset$
for $k \leftarrow 0$ to n **do**
  for $i \leftarrow 1$ to s_k **do**
    $u = r_{k,i}$
    Compute $\ell = |\mathsf{O}_\alpha(r_{k,i})|$
    for $j \leftarrow 1$ to $(\ell + v_k)/2$ **do**
      $\mathsf{supp}(f)$.append(u)
      $u \leftarrow \alpha \circ \alpha \ltimes u$
      $v_k \leftarrow -v_k$
    end for
  end for
end for
return f

Fig. 1. WAPB Construction

We consider Construction 1 with $n = 2^{a_1} + 2^{a_2} + \ldots + 2^{a_w}$ where $0 \leq a_1 < a_2 < \ldots < a_w$ and denote $n_1 = 2^{a_1}, \ldots, n_w = 2^{a_w}$ and:

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

We denote f_n this construction.

Proposition 1. *Let $n \in \mathbb{N}$, $n \geq 2$, f_n satisfies $\mathsf{NL}(f_n) \geq 2^{n-2} - 2^{n-n_w}$.*

Proof. Let denote $x \in \mathbb{F}_2^n$ as (y, z) where $y \in \mathbb{F}_2^{n-n_w}$ and $z \in \mathbb{F}_2^{n_w}$.

We determine the Walsh transform of f in a, $W_f(a)$ for $a \in \mathbb{F}_2^n$, $a = (b, c)$ with $b \in \mathbb{F}_2^{n-n_w}$ and $z \in \mathbb{F}_2^{n_w}$.

$$W_f(a) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+ax} = \sum_{i=1}^{t} \sum_{z \in O_i} \sum_{y \in \mathbb{F}_2^{n-n_w}} (-1)^{f(y,z)+by+cz} + \sum_{i=t+1}^{t+s} \sum_{z \in O_i} \sum_{y \in \mathbb{F}_2^{n-n_w}} (-1)^{f(y,z)+by+cz}, \tag{1}$$

where we denote O_1 to O_t the t even-length orbits of $\mathbb{F}_2^{n_w}$ (relatively to $< (x_1, \ldots, x_{n_w}) >$) and O_{t+1} to O_{t+s} the odd-length ones.

Since n_w is a power of two, $s = 2$, the only orbits of odd lengths are the ones of 0_{n_w} and 1_{n_w}. Thereafter we can derive the following bound on the second sum of Equation 1:

$$|\sum_{i=t+1}^{t+s} \sum_{z \in O_i} \sum_{y \in \mathbb{F}_2^{n-n_w}} (-1)^{f(y,z)+by+cz}| = |\sum_{z \in \{0_{n_w}, 1_{n_w}\}} \sum_{y \in \mathbb{F}_2^{n-n_w}} (-1)^{f(y,z)+by+cz}| \leq 2^{n-n_w+1}$$

Then, we look for a bound for the first sum of Equation 1. We denote $\pi_w = (x_1, \ldots, x_{n_w})$.

$$\begin{aligned}
\sum_{i=1}^{t} \sum_{z \in O_i} \sum_{y \in \mathbb{F}_2^{n-n_w}} (-1)^{f(y,z)+by+cz} &= \frac{1}{2} \sum_{i=1}^{t} \sum_{z \in O_i} \sum_{y \in \mathbb{F}_2^{n-n_w}} \left((-1)^{f(y,z)+by+cz} + (-1)^{f(y,\pi_w(z))+by+c\pi_w(z)} \right) \\
&= \frac{1}{2} \sum_{i=1}^{t} \sum_{z \in O_i} \sum_{y \in \mathbb{F}_2^{n-n_w}} \left((-1)^{f(y,z)+by} \right) \left((-1)^{cz} - (-1)^{c\pi_w(z)} \right)
\end{aligned}$$

Accordingly, for each z such that $cz = c\pi_w(z)$, the term is null in the summation. Thereafter:

$$\begin{aligned}
|\sum_{i=1}^{t} \sum_{z \in O_i} \sum_{y \in \mathbb{F}_2^{n-n_w}} (-1)^{f(y,z)+by+cz}| &= |\frac{1}{2} \sum_{i=1}^{t} \sum_{\substack{z \in O_i \\ c(z+\pi_w(z))=1}} \sum_{y \in \mathbb{F}_2^{n-n_w}} \left((-1)^{f(y,z)+by} \right) 2(-1)^{cz}| \\
&\leq 2^{n-n_w} |\{z \in \mathbb{F}_2^{n_w} \setminus \{0_{n_w}, 1_{n_w}\}, c(z + \pi_w(z)) = 1\}|
\end{aligned}$$

Using Proposition 2 it allows to conclude:

$$|\sum_{i=1}^{t} \sum_{z \in O_i} \sum_{y \in \mathbb{F}_2^{n-n_w}} (-1)^{f(y,z)+by+cz}| \leq 2^{n-1},$$

and finally:

$$\begin{aligned}
\mathsf{NL}(f) &\geq 2^{n-1} - \frac{1}{2} \max_{a \in \mathbb{F}_2^n} |W_f(a)| \\
&\geq 2^{n-1} - \frac{1}{2} \left(2^{n-n_w+1} + 2^{n-1} \right) \\
&\geq 2^{n-2} - 2^{n-n_w}
\end{aligned}$$

□

[**PM:** TODO: redact the proof of the proposition]

Proposition 2. *Let $n \geq 2$ be a power of 2, and $\pi = (x_1, \ldots, x_n)$ the following holds:*

$$|\{z \in \mathbb{F}_2^n \setminus \{0_n, 1_n\}, c(z + \pi(z)) = 1\}| = \begin{cases} 2^{n-1} & \text{if } c \in \mathbb{F}_2^n \setminus \{0_n, 1_n\}, \\ 0 & \text{if } c = 0_n, \\ 0 & \text{if } c = 1_n. \end{cases}$$

Proof. ☐

[**PM:** Add the improvements on the nonlinearity bound, the formula in terms of sets for the NL_k and the generalizations to other subgroups.]

References