A general secondary construction of Boolean functions including the indirect sum and its generalizations

Claude Carlet[1] and Deng Tang[2]

Abstract

We study a secondary construction of Boolean functions, which generalizes the direct sum and the indirect sum. We detail how these two classic secondary constructions are particular cases of this more general one, as well as two known generalizations of the indirect sum. This unifies the known secondary constructions of Boolean functions. We study very precisely the Walsh transform of the constructed functions. This leads us to an interesting observation on the Walsh transforms $W_g, W_{g'}, W_{g''}$, and $W_{g\oplus g'\oplus g''}$ when g, g', g'' are Boolean functions such that $(g \oplus g')(g \oplus g'')$ equals the zero function.

1 Introduction

Constructions of Boolean functions satisfying some desired features (such as being highly nonlinear, and/or plateaued, and/or resilient, and/or algebraic immune see e.g. [5]) are necessary for providing Boolean functions that are applicable to coding theory, combinatorics, or cryptography, in information protection and discrete mathematics. Primary constructions (which build functions from scratch, such as the well-known Maiorana-McFarland construction [8, 1]) are often not sufficient for obtaining enough functions having all the desired features. Secondary constructions (building new functions from so-called initial functions having the desired property) are then also needed. The two main known secondary constructions are the direct sum construction (introduced in [8]) $f(x, y) = g(x) \oplus h(y)$ (where $x \in \mathbb{F}_2^r$ and $y \in \mathbb{F}_2^{n-r}$ and $(x, y) \in \mathbb{F}_2^n$ is the concatenation of x and y) and its generalization, the indirect sum construction (introduced in [4]): $f(x, y) = g(x)\oplus h(y)\oplus(g(x)\oplus g'(x))(h(y)\oplus h'(y))$ (where $x \in \mathbb{F}_2^r$ and $y \in \mathbb{F}_2^{n-r}$ as well). In [13], the indirect sum is used with f_1 and f_2 (resp. g_1 and g_2) being the restrictions of a bent function f (resp. g) to two hyperplanes, complementary of each other.

The indirect sum has been itself generalized in several ways. In [7] are introduced the constructions:

$$f(x, y) = g(x) \oplus h(y) \oplus (g \oplus g')(x)(h \oplus h')(y) \oplus (g' \oplus g'')(x)(h' \oplus h'')(y), \tag{1}$$

$$f(x, y) = g(x) \oplus h(y) \oplus (g \oplus g')(x)(h \oplus h')(y) \oplus (g' \oplus g'')(x)(h' \oplus h'')(y)\oplus (g'' \oplus g''')(x)(h'' \oplus h''')(y). \tag{2}$$

In the present paper, we study a secondary construction, which generalizes all these ones (and gives then a simpler view on them).

[1]Universities of Paris 8, France and Bergen, Norway. Email: claude.carlet@gmail.com

[2]Shanghai Jiao Tong University, China. Email: dtang@foxmail.com

The study of the properties, needed for a Boolean function to be used for instance in a stream cipher, can be made, in almost all cases, through the study of its Walsh transform. The Walsh transform of an n-variable Boolean function $f : \mathbb{F}_2^n \mapsto \mathbb{F}_2$ is the integer-valued function $a \mapsto W_f(a) = \sum_{x\in\mathbb{F}_2^n}(-1)^{f(x)\oplus a\cdot x}$, where "$\cdot$" is some inner product in $\mathbb{F}_2^n$, for instance the usual inner product $a \cdot x = \bigoplus a_i x_i$ (where $a = (a_1, \ldots, a_n)$ and $x = (x_1, \ldots, x_n)$). The Walsh transforms of direct and indirect sums and of the generalization (1) can be nicely expressed by means of the Walsh transforms of the initial functions $g, h, \ldots$ (and this is why they easily provide bent functions from bent functions, plateaued functions from plateaued functions and resilient functions from resilient functions - see the definitions of these notions in Section 2, see also the survey [5]): we have, in the case of direct sum $W_f(a', a'') = W_g(a')W_h(a'')$, and in the case of indirect sum $W_f(a', a'') = \frac{1}{2}W_g(a')\Big(W_h(a'') + W_{h'}(a'')\Big) + \frac{1}{2}W_{g'}(a')\Big(W_h(a'') - W_{h'}(a'')\Big)$. The Walsh transform was not calculated in [7] for Constructions (1) and (2), since the aim of this paper was only to build bent functions and characterizing the bentness of Functions (1) and (2) was possible by using a theorem from [3]. But the Walsh transform of (1) was calculated in [12] (in a rather complex way); the derived formula is:

$$\begin{aligned}
W_f(a', a'') = \frac{1}{4}W_h(a'')\left[W_g(a') + W_{g'}(a') + W_{g''}(a') + W_{g\oplus g'\oplus g''}(a')\right] \\
+\frac{1}{4}W_{h'}(a'')\left[W_g(a') - W_{g'}(a') - W_{g''}(a') + W_{g\oplus g'\oplus g''}(a')\right] \\
+\frac{1}{4}W_{h''}(a'')\left[W_g(a') - W_{g'}(a') + W_{g''}(a') - W_{g\oplus g'\oplus g''}(a')\right] \\
+\frac{1}{4}W_{h\oplus h'\oplus h''}(a'')\left[W_g(a') + W_{g'}(a') - W_{g''}(a') - W_{g\oplus g'\oplus g''}(a')\right]. \qquad (3)
\end{aligned}$$

We study the Walsh transform of the functions generated by the generalized secondary construction. We check that the Walsh transforms of the direct and indirect sums, which correspond to the simplest particular cases of our construction, coincide with what gives our general formula. We study other (more complex) particular cases and we deduce new bent functions.

2 Preliminaries

For any positive integer n, we denote by $\mathbb{F}_2^n$ the vector space of n-tuples over the finite field $\mathbb{F}_2 = \{0, 1\}$, by $\mathbf{0}_n = (0, \ldots, 0)$ the all-zero vector in $\mathbb{F}_2^n$, by $\mathbb{F}_2^{n*}$ the set $\mathbb{F}_2^n \setminus \{\mathbf{0}_n\}$, by $[n]$ the set $\{1, 2, \ldots, n\}$ and by $\mathcal{B}_n$ the $\mathbb{F}_2$-vector space of n-variable Boolean functions $f : \mathbb{F}_2^n \mapsto \mathbb{F}_2$. Given two vectors $x = (x_1, x_2, \ldots, x_n), y = (y_1, y_2, \ldots, y_n)$ in $\mathbb{F}_2^n$, we write $x \preceq y$ and we say that y *covers* x, if $x_i \leq y_i$ for all $i \in [n]$, that is, if $\mathrm{supp}(x) \subseteq \mathrm{supp}(y)$, where $\mathrm{supp}(x)$ is the support of x: $\mathrm{supp}(x) = \{i \in [n] : x_i \neq 0\}$. For a vector $a = (a_1, a_2, \ldots, a_n) \in \mathbb{F}_2^n$, its Hamming weight $w_H(a)$ is defined as the cardinality of its support: $|\mathrm{supp}(a)|$. In the rest of this paper, we use $+$ (resp. $\sum$) to denote an addition (resp. a multiple sum) considered in characteristic 0 (in $\mathbb{Z}$) and $\oplus$ (resp. $\bigoplus$) to denote an addition (resp. a multiple sum)

computed in characteristic 2 (in $\mathbb{F}_2$ or $\mathbb{F}_2^n$ or $\mathcal{B}_n$).
Given two positive integers s, k, we call (s,k)-vectorial Boolean function any function $F : \mathbb{F}_2^s \mapsto \mathbb{F}_2^k$. If $k = 1$, we simply call F an s-variable Boolean function and we define its support (resp. its co-support) as the set $\{x \in \mathbb{F}_2^s : F(x) = 1\}$ (resp. $\{x \in \mathbb{F}_2^s : F(x) = 0\}$). An n-variable Boolean function f is called bent (see [5, 6, 10, 11]) if its nonlinearity $2^{n-1} - \frac{1}{2}\max_{a\in\mathbb{F}_2^n} |W_f(a)|$ achieves the optimum $2^{n-1} - 2^{\frac{n}{2}-1}$. It is called plateaued if its Walsh transform $W_f(a) = \sum_{x\in\mathbb{F}_2^n}(-1)^{f(x)\oplus a\cdot x}$ takes all its value in $\{0, \pm\lambda\}$ for some positive integer λ called the amplitude (and necessarily equal to a power of 2 whose exponent is between $\frac{n}{2}$ and n). It is called t-resilient for some $t \in \{0, \ldots, n-1\}$ if its Walsh transform takes value 0 for every $a \in \mathbb{F}_2^n$ of Hamming weight between 0 and t.

3 A generalized indirect sum construction

Construction 1. *Let k, s, t be three positive integers and F be an (s,k)-vectorial Boolean function. Let g be a Boolean function in s variables and for every $u \in \mathbb{F}_2^k$, let h_u be a Boolean functions in t variables. We construct a Boolean function $f(x,y)$ in $n = s + t$ variables as follows*

$$f(x,y) = g(x) \oplus h_{F(x)}(y),$$

where $x \in \mathbb{F}_2^s, y \in \mathbb{F}_2^t$.

Remark 1. *If we restrict ourselves to the case where F is a permutation, we can change the definition of $f(x,y)$ into a simpler one: $f(x,y) = h'_{F(x)}(y)$ (that is, we can without loss of generality avoid the addition of g). Indeed, we can take $h'_z(y) = g(F^{-1}(z)) + h_z(y)$. But in our definition, F is not necessarily a permutation (and its domain and co-domain are not necessarily equal), which gives more freedom and in particular allows to consider cases where the image set of F is small.*

Remark 2. *If we compose F on the left by a function whose restriction to the image set of F is injective (and if we change the h_u's accordingly), we do not change function f. If the image set of F has a size smaller than or equal to some power of 2, say 2^l, then we can without loss of generality assume that F is an (s,l)-function.*

Remark 3. *Let F be a constant function in Construction 1, that is $|Im(F)| = |\{F(x) : x \in \mathbb{F}_2^s\}| = 1$, then Construction 1 becomes the direct sum construction.*
Let F be a two-valued function, that is, $Im(F) = \{u_0, u_1\} \subseteq \mathbb{F}_2^k$. Then, denoting by $1_S(x)$ the indicator (or characteristic) function of a set S, i.e., $1_S(x) = 1$ if $x \in S$ and $1_S(x) = 0$ otherwise, and denoting $g' = g \oplus 1_{F^{-1}(u_1)}$, Construction 1 becomes $f(x,y) = g(x) \oplus h_{u_0}(y) \oplus (g \oplus g')(x)(h_{u_0} \oplus h_{u_1})(y)$, which is the indirect sum construction.
If $Im(F) = \{u_0, u_1, u_2\}$ with u_0, u_1, u_2 distinct, then Construction 1 gives: $f(x,y) = 1_{F^{-1}(u_0)}(x)\big(g(x) \oplus h_{u_0}(y)\big) \oplus 1_{F^{-1}(u_1)}(x)\big(g(x) \oplus h_{u_1}(y)\big) \oplus 1_{F^{-1}(u_2)}(x)\big(g(x) \oplus h_{u_2}(y)\big)$. Still denoting by $g \oplus g' \in \mathcal{B}_s$ the Boolean function $1_{F^{-1}(u_1)}$ whose support equals $F^{-1}(u_1)$ and

by $g \oplus g''$ the Boolean function $1_{F^{-1}(u_2)}$ whose support equals $F^{-1}(u_2)$, we have $1_{F^{-1}(u_0)} = 1 \oplus g' \oplus g''$ and we have then $f(x,y) = (1 \oplus g'(x) \oplus g''(x))\big(g(x) \oplus h_{u_0}(y)\big) \oplus (g(x) \oplus g'(x))\big(g(x) \oplus h_{u_1}(y)\big) \oplus (g(x) \oplus g''(x))\big(g(x) \oplus h_{u_2}(y)\big)$, that is:

$$f(x,y) =$$

$$g(x) \oplus h_{u_0}(y) \oplus (g(x) \oplus g'(x))(h_{u_1}(y) \oplus h_{u_2}(y)) \oplus (g'(x) \oplus g''(x))(h_{u_2}(y) \oplus h_{u_0}(y)). \quad (4)$$

It seems impossible to obtain (1) by calling h, h', h'' the functions $h_{u_0}, h_{u_1}, h_{u_2}$ in some order and the constructions seem then apparently different. Note that (1) is invariant when we exchange g and h, g' and h', g'' and h'', while (4) is not when we exchange g and h_{u_1}, g' and h_{u_2}, g'' and h_{u_0}.

In the next theorem, we extend the study of the Walsh transforms of the direct and indirect sums to the general case of Construction 1.

Remark 4. *For every Boolean function f over $\mathbb{F}_2^s \times \mathbb{F}_2^t$ and every Boolean function g over $\mathbb{F}_2^s$, there exist Boolean functions h_u over $\mathbb{F}_2^t$ and an (s,s)-function F such that f is obtained by Construction 1. Indeed, we can take, for instance, for every $x \in \mathbb{F}_2^s$, $F(x) = x$ and $h_x(y) = g(x) + f(x,y)$. This of course generalizes to any permutation F of $\mathbb{F}_2^s$. We are then here generalizing a construction that has been considered in [3] and reported in [5, Theorem 15], in the particular framework of bent functions. What is interesting with Construction 1 is that we can consider cases where the image set of F is small.*

3.1 The Walsh transform of the constructed functions

In this subsection, we give two expressions of the Walsh transform of f, which will both be useful in the sequel.

Theorem 1. *Let k, s, t be three positive integers and $F = (f_1, f_2, \cdots, f_k)$ be a (s,k)-vectorial Boolean function. Let g be a Boolean function in s variables and for every $u \in \mathbb{F}_2^k$, let h_u be a Boolean functions in t variables, and let f be the $n = s + t$-variable Boolean function defined in Construction 1. Then we have:*

$$f(x,y) = g(x) \oplus \bigoplus_{u \in \mathbb{F}_2^k} \bigoplus_{I \subseteq \{1,\ldots,k\}} \prod_{i \in I} f_i(x) \prod_{i \in \{1,\ldots,k\} \setminus I} (u_i \oplus 1) h_u(y). \quad (5)$$

For any $a = (a', a'') \in \mathbb{F}_2^s \times \mathbb{F}_2^t$ with $a' = (a_1, \cdots, a_s)$ and $a'' = (a_1'', \cdots, a_t'')$ we have

$$\begin{aligned} W_f(a) &= \sum_{u \in \mathbb{F}_2^k} \sum_{(x,y) \in \mathbb{F}_2^s \times \mathbb{F}_2^t} 1_{F^{-1}(u)}(x) (-1)^{g(x) \oplus h_u(y) \oplus a' \cdot x \oplus a'' \cdot y} \quad (6) \\ &= \sum_{u \in \mathbb{F}_2^k} \sum_{x \in \mathbb{F}_2^s} 1_{F^{-1}(u)}(x) (-1)^{g(x) \oplus a' \cdot x} W_{h_u}(a'') \end{aligned}$$

and

$$W_f(a) = \frac{1}{2^k} \sum_{u \in \mathbb{F}_2^k} \sum_{v \in \mathbb{F}_2^k} (-1)^{v \cdot u} W_{g \oplus v \cdot F}(a') W_{h_u}(a''), \quad (7)$$

where $u = (u_1, u_2, \cdots, u_k), v = (v_1, v_2, \cdots, v_k) \in \mathbb{F}_2^k$ *and* $v \cdot F = \bigoplus_{i=1}^k v_i f_i$.
Defining $h(y, u) = h_u(y)$, *we have:*

$$W_f(a) \quad = \quad \frac{1}{2^k} \sum_{v \in \mathbb{F}_2^k} W_{g \oplus v \cdot F}(a') W_h(a'', v). \tag{8}$$

Proof. Relation (5) is directly deduced from the definition of Construction 1, translated into the expression $f(x, y) = g(x) \oplus \bigoplus_{u \in \mathbb{F}_2^k} \prod_{i=1}^k (f_i(x) \oplus u_i \oplus 1) h_u(y)$.
Relation (6) directly comes from the definition of the Walsh transform through a partition by the pre-image sets. Let us prove Relation (7). Using that, for any $c \in \mathbb{F}_2$, and for $1 \leq i \leq k$ and $x \in \mathbb{F}_2^s$, we have

$$\frac{1 + (-1)^{f_i(x) \oplus c}}{2} = \begin{cases} 1, & \text{if } f_i(x) \oplus c = 0 \\ 0, & \text{if } f_i(x) \oplus c = 1 \end{cases},$$

we can easily verify that for any $u = (u_1, u_2, \cdots, u_k) \in \mathbb{F}_2^k$:

$$1_{F^{-1}(u)}(x) = \prod_{i=1}^k \left(\frac{1 + (-1)^{f_i(x) \oplus u_i}}{2} \right).$$

Therefore, we have

$$\begin{aligned}
W_f(a) &= \sum_{(x,y) \in \mathbb{F}_2^s \times \mathbb{F}_2^t} (-1)^{f(x,y) \oplus a' \cdot x \oplus a'' \cdot y} \\
&= \sum_{u \in \{F(z) \,:\, z \in \mathbb{F}_2^s\}} \sum_{(x,y) \in F^{-1}(u) \times \mathbb{F}_2^t} (-1)^{g(x) \oplus h_u(y) \oplus a' \cdot x \oplus a'' \cdot y} \\
&= \sum_{u \in \{F(z) \,:\, z \in \mathbb{F}_2^s\}} \sum_{(x,y) \in \mathbb{F}_2^s \times \mathbb{F}_2^t} 1_{F^{-1}(u)}(x) (-1)^{g(x) \oplus h_u(y) \oplus a' \cdot x \oplus a'' \cdot y} \\
&= \sum_{u \in \mathbb{F}_2^k} \sum_{(x,y) \in \mathbb{F}_2^s \times \mathbb{F}_2^t} 1_{F^{-1}(u)}(x) (-1)^{g(x) \oplus h_u(y) \oplus a' \cdot x \oplus a'' \cdot y} \\
&= \sum_{u \in \mathbb{F}_2^k} \sum_{(x,y) \in \mathbb{F}_2^s \times \mathbb{F}_2^t} \left[(-1)^{g(x) \oplus h_u(y) \oplus a' \cdot x \oplus a'' \cdot y} \prod_{i=1}^k \left(\frac{1 + (-1)^{f_i(x) \oplus u_i}}{2} \right) \right] \\
&= \frac{1}{2^k} \sum_{u \in \mathbb{F}_2^k} \sum_{(x,y) \in \mathbb{F}_2^s \times \mathbb{F}_2^t} \left[(-1)^{g(x) \oplus h_u(y) \oplus a' \cdot x \oplus a'' \cdot y} \sum_{v \in \mathbb{F}_2^k} (-1)^{v \cdot F(x) \oplus v \cdot u} \right] \\
&= \frac{1}{2^k} \sum_{u \in \mathbb{F}_2^k} \sum_{v \in \mathbb{F}_2^k} (-1)^{v \cdot u} W_{g \oplus v \cdot F}(a') W_{h_u}(a'').
\end{aligned}$$

Finally, for any $a = (a', a'') \in \mathbb{F}_2^s \times \mathbb{F}_2^t$ with $a' = (a_1, \cdots, a_s)$ and $a'' = (a_1'', \cdots, a_t'')$, it follows from (7) that

$$W_f(a) = \frac{1}{2^k} \sum_{v \in \mathbb{F}_2^k} W_{g \oplus v \cdot F}(a') \sum_{u \in \mathbb{F}_2^k} (-1)^{v \cdot u} W_{h_u}(a'').$$

This proves (8) since, for any $(a'', v) \in \mathbb{F}_2^t \times \mathbb{F}_2^k$, we have:

$$\begin{aligned} W_h(a'', v) = & \sum_{(y,u)\in\mathbb{F}_2^t\times\mathbb{F}_2^k} (-1)^{h(y,u)\oplus(a'',v)\cdot(y,u)} \\ = & \sum_{u\in\mathbb{F}_2^k} (-1)^{v\cdot u} W_{h_u}(a''). \end{aligned}$$

□

Remark 5. *We have seen in Remark 2 that we can without loss of generality change the co-domain of F (concretely, reduce the value of k). Note that this is true from the viewpoint of the construction of f and of Relation (6), but not really from that of Relation (7). However, for every u outside the image set of F and every a'', the value chosen for $W_{h_u}(a^{''})$ plays in fact no role.*

3.2 The expression of f and Relations (6) and (7) when F has a small image set

3.2.1 $Im(F)$ of sizes 1, 2 and 3

Let us first revisit the cases of direct and indirect sums and study further whether Function (1) recalled above can correspond to Construction 1 with $|Im(F)| = 3$. We shall see how Relation (6) leads in all the first two cases to the values of $W_f(a)$ that we recalled in the introduction, and compare what it gives when $|Im(F)| = 3$ with the formula we have recalled for the Walsh transform of Function (1). We shall also do the same with Relation (7), since it is interesting for the study of future cases, to detail how each of these two relations fits with the known formulas. This will lead us (in Lemma 1) to an observation that we consider interesting for its own sake and that will simplify the formulas that we obtain with Relations (6) and (7) and make them match.

• **Size 1:** If $Im(F) = \{u_0\}$, the Boolean function f defined in Construction 1 belongs to the direct sum construction. Note that $1_{F^{-1}(u)} = \mathbb{F}_2^s$ in this case. Relation (6) writes:

$$\begin{aligned} W_f(a) &= \sum_{u\in\mathbb{F}_2^s} \sum_{(x,y)\in\mathbb{F}_2^s\times\mathbb{F}_2^t} 1_{F^{-1}(u)}(x)(-1)^{g(x)\oplus h_u(y)\oplus a'\cdot x\oplus a^{''}\cdot y} \\ &= \sum_{(x,y)\in\mathbb{F}_2^s\times\mathbb{F}_2^t} (-1)^{g(x)\oplus h_{u_0}(y)\oplus a'\cdot x\oplus a^{''}\cdot y} \\ &= W_g(a')W_{h_{u_0}}(a^{''}), \end{aligned}$$

where $a = (a', a^{''}) \in \mathbb{F}_2^s \times \mathbb{F}_2^t$ with $a' = (a_1, \cdots, a_s)$ and $a^{''} = (a_1^{''}, \cdots, a_t^{''})$. This is the relation recalled above for the direct sum.

Relation (7) writes (using that $W_{g\oplus 1} = -W_g$)

$$\begin{aligned} W_f(a) &= \frac{1}{2^k}\sum_{u\in\mathbb{F}_2^k}\sum_{v\in\mathbb{F}_2^k}(-1)^{v\cdot u}W_{g\oplus v\cdot u_0}(a')W_{h_u}(a'') \\ &= \frac{1}{2^k}\sum_{u\in\mathbb{F}_2^k}\sum_{v\in\mathbb{F}_2^k}(-1)^{v\cdot(u+u_0)}W_{g}(a')W_{h_u}(a'') \\ &= W_g(a')W_{h_{u_0}}(a''). \end{aligned}$$

• **Size 2:** If $Im(F) = \{u_0, u_1\}$ with $u_0 \neq u_1$, then as we also saw already, Construction 1 becomes the indirect sum. As we observed in Remark 2, we could[1] take F valued in $\mathbb{F}_2$, and so $k = 1$ (fixing for instance $u_0 = 0$ and $u_1 = 1$). We prefer however not to make such a simplification, for two reasons: this will better prepare us for the study of the case where $Im(F)$ has size 3 below (that we shall also make without restricting the co-domain of F), and this keeps full freedom for the choice of function F. We have: $f(x,y) = 1_{F^{-1}(u_0)}(x)\big(g(x)\oplus h_{u_0}(y)\big)\oplus 1_{F^{-1}(u_1)}(x)\big(g(x)\oplus h_{u_1}(y)\big)$, and for any $a = (a', a'') \in \mathbb{F}_2^s\times\mathbb{F}_2^t$, where $a' = (a_1,\cdots,a_s)$ and $a'' = (a_1'',\cdots,a_t'')$, Relation (6) gives:

$$\begin{aligned} W_f(a) &= \sum_{u\in\mathbb{F}_2^s}\sum_{(x,y)\in\mathbb{F}_2^s\times\mathbb{F}_2^t} 1_{F^{-1}(u)}(x)(-1)^{g(x)\oplus h_u(y)\oplus a'\cdot x\oplus a''\cdot y} \\ &= \sum_{(x,y)\in\mathbb{F}_2^s\times\mathbb{F}_2^t} 1_{F^{-1}(u_0)}(x)(-1)^{g(x)\oplus h_{u_0}(y)\oplus a'\cdot x\oplus a''\cdot y} \\ &\quad + \sum_{(x,y)\in\mathbb{F}_2^s\times\mathbb{F}_2^t} 1_{F^{-1}(u_1)}(x)(-1)^{g(x)\oplus h_{u_1}(y)\oplus a'\cdot x\oplus a''\cdot y}. \end{aligned}$$

Still denoting by $g\oplus g'\in\mathcal{B}_s$ the Boolean function $1_{F^{-1}(u_1)}$ whose support equals $F^{-1}(u_1)$, we have that the co-support of $g\oplus g'\in\mathcal{B}_s$ is $F^{-1}(u_0)$ (and we have seen in Remark 3 that $f(x,y) = g(x)\oplus h_{u_0}(y)\oplus(g\oplus g')(x)(h_{u_0}\oplus h_{u_1})(y))$ and using that $1\oplus(g\oplus g')(x) = \frac{1}{2}\Big(1+(-1)^{(g\oplus g')(x)}\Big)$ and $(g\oplus g')(x) = \frac{1}{2}\Big(1-(-1)^{(g\oplus g')(x)}\Big)$, we have from the latter expression we obtained for $W_f(a)$ above:

$$W_f(a',a'') = \frac{1}{2}W_g(a')\big[W_{h_{u_0}}(a'') + W_{h_{u_1}}(a'')\big] + \frac{1}{2}W_{g'}(a')\big[W_{h_{u_0}}(a'') - W_{h_{u_1}}(a'')\big], \qquad (9)$$

and this is the relation that we recalled in the introduction. Let us now consider Relation (7). For every $u\in\mathbb{F}_2^k$, we have (using again that $W_{g\oplus 1} = -W_g$):

$$\sum_{v\in\mathbb{F}_2^k}(-1)^{v\cdot u}W_{g\oplus v\cdot F}(a') =$$

$$\sum_{v\in\mathbb{F}_2^k}(-1)^{v\cdot u}W_{g\oplus(v\cdot u_0)(g\oplus g'\oplus 1)\oplus(v\cdot u_1)(g\oplus g')}(a') =$$

[1] This is also true for the previous case.

$$\sum_{v\in\mathbb{F}_2^k}(-1)^{v\cdot(u\oplus u_0)}W_{g\oplus(v\cdot(u_0\oplus u_1))(g\oplus g')}(a')=$$

$$\sum_{v\in\langle u_0\oplus u_1\rangle^\perp}(-1)^{v\cdot(u\oplus u_0)}W_g(a')+\sum_{v\in\mathbb{F}_2^k\setminus\langle u_0\oplus u_1\rangle^\perp}(-1)^{v\cdot(u\oplus u_0)}W_{g'}(a')=$$

$$\begin{cases} 2^{k-1}W_g(a') \text{ if } u\in\{u_0,u_1\}\\ 0 \text{ otherwise}\end{cases}+\begin{cases} 2^{k-1}W_g(a') \text{ if } u=u_0\\ -2^{k-1}W_g(a') \text{ if } u=u_1\\ 0 \text{ otherwise}\end{cases}.$$

Relation (7) gives then (9).

• **Size 3:** If $Im(F)=\{u_0,u_1,u_2\}$ with u_0,u_1,u_2 distinct, then we have seen in Remark 3 that Construction 1 gives: $f(x,y)=1_{F^{-1}(u_0)}(x)\big(g(x)\oplus h_{u_0}(y)\big)\oplus 1_{F^{-1}(u_1)}(x)\big(g(x)\oplus h_{u_1}(y)\big)\oplus 1_{F^{-1}(u_2)}(x)\big(g(x)\oplus h_{u_2}(y)\big)$, and for any $a=(a',a'')\in\mathbb{F}_2^s\times\mathbb{F}_2^t$, where $a'=(a_1,\cdots,a_s)$ and $a''=(a_1'',\cdots,a_t'')$, Relation (6) gives:

$$\begin{aligned}W_f(a) &= \sum_{u\in\mathbb{F}_2^s}\sum_{(x,y)\in\mathbb{F}_2^s\times\mathbb{F}_2^t}1_{F^{-1}(u)}(x)(-1)^{g(x)\oplus h_u(y)\oplus a'\cdot x\oplus a''\cdot y}\\ &= \sum_{(x,y)\in\mathbb{F}_2^s\times\mathbb{F}_2^t}1_{F^{-1}(u_0)}(x)(-1)^{g(x)\oplus h_{u_0}(y)\oplus a'\cdot x\oplus a''\cdot y}\\ &\quad+\sum_{(x,y)\in\mathbb{F}_2^s\times\mathbb{F}_2^t}1_{F^{-1}(u_1)}(x)(-1)^{g(x)\oplus h_{u_1}(y)\oplus a'\cdot x\oplus a''\cdot y}\\ &\quad+\sum_{(x,y)\in\mathbb{F}_2^s\times\mathbb{F}_2^t}1_{F^{-1}(u_2)}(x)(-1)^{g(x)\oplus h_{u_2}(y)\oplus a'\cdot x\oplus a''\cdot y}. \qquad (10)\end{aligned}$$

Denoting as in Remark 3 by $g\oplus g'\in\mathcal{B}_s$ the Boolean function $1_{F^{-1}(u_1)}$ and by $g\oplus g''$ the Boolean function $1_{F^{-1}(u_2)}$ (which gives $f(x,y)=g(x)\oplus h_{u_0}(y)\oplus(g(x)\oplus g'(x))(h_{u_1}(y)\oplus h_{u_2}(y))\oplus(g'(x)\oplus g''(x))(h_{u_2}(y)\oplus h_{u_0}(y)))$ and using that $1_{F^{-1}(u_0)}=1\oplus(g'\oplus g'')(x)=\frac{1}{2}\Big(1+(-1)^{(g'\oplus g'')(x)}\Big)$ and $1_{F^{-1}(u_1)}=(g\oplus g')(x)=\frac{1}{2}\Big(1-(-1)^{(g\oplus g')(x)}\Big)$ and $1_{F^{-1}(u_2)}=(g\oplus g'')(x)=\frac{1}{2}\Big(1-(-1)^{(g\oplus g'')(x)}\Big)$, we deduce from Relation (10):

$$\begin{aligned}W_f(a) &= \frac{1}{2}\sum_{(x,y)\in\mathbb{F}_2^s\times\mathbb{F}_2^t}\Big((-1)^{g(x)\oplus h_{u_0}(y)\oplus a'\cdot x\oplus a''\cdot y}+(-1)^{g(x)\oplus g'(x)\oplus g''(x)\oplus h_{u_0}(y)\oplus a'\cdot x\oplus a''\cdot y}\Big)\\ &\quad+\frac{1}{2}\sum_{(x,y)\in\mathbb{F}_2^s\times\mathbb{F}_2^t}\Big((-1)^{g(x)\oplus h_{u_1}(y)\oplus a'\cdot x\oplus a''\cdot y}-(-1)^{g'(x)\oplus h_{u_1}(y)\oplus a'\cdot x\oplus a''\cdot y}\Big)\\ &\quad+\frac{1}{2}\sum_{(x,y)\in\mathbb{F}_2^s\times\mathbb{F}_2^t}\Big((-1)^{g(x)\oplus h_{u_2}(y)\oplus a'\cdot x\oplus a''\cdot y}-(-1)^{g''(x)\oplus h_{u_2}(y)\oplus a'\cdot x\oplus a''\cdot y}\Big)\\ &= \frac{1}{2}W_{h_{u_0}}(a'')\big(W_g(a')+W_{g\oplus g'\oplus g''}(a')\big)+\frac{1}{2}W_{h_{u_1}}(a'')\big(W_g(a')-W_{g'}(a')\big)\\ &\quad+\frac{1}{2}W_{h_{u_2}}(a'')\big(W_g(a')-W_{g''}(a')\big). \qquad (11)\end{aligned}$$

This is different from what we recalled in the introduction about Construction 1's Walsh transform and this confirms that we have here a different construction. Note that the

expression of the Walsh transform is simpler here, but we are in a particular case since we have $(g \oplus g')(g \oplus g'') = 0$ while there is no condition on g, g', g'' in (1).
Let us now study what gives Relation (7). For every $u \in \mathbb{F}_2^k$, we have (using again that $W_{g\oplus 1} = -W_g$):

$$\sum_{v\in\mathbb{F}_2^k}(-1)^{v\cdot u}W_{g\oplus v\cdot F}(a') =$$

$$\sum_{v\in\mathbb{F}_2^k}(-1)^{v\cdot u}W_{g\oplus(v\cdot u_0)(1\oplus g'\oplus g'')\oplus(v\cdot u_1)(g\oplus g'))\oplus(v\cdot u_2)(g\oplus g'')}(a') =$$

$$\sum_{v\in\mathbb{F}_2^k}(-1)^{v\cdot(u\oplus u_0)}W_{g\oplus(v\cdot(u_0\oplus u_1))(g\oplus g')\oplus(v\cdot(u_0\oplus u_2))(g\oplus g'')}(a') =$$

$$\sum_{v\in\langle u_0\oplus u_1, u_0\oplus u_2\rangle^\perp}(-1)^{v\cdot(u\oplus u_0)}W_g(a') + \sum_{v\in\langle u_0\oplus u_1\rangle^\perp\setminus\langle u_0\oplus u_2\rangle^\perp}(-1)^{v\cdot(u\oplus u_0)}W_{g''}(a') +$$

$$\sum_{v\in\langle u_0\oplus u_2\rangle^\perp\setminus\langle u_0\oplus u_1\rangle^\perp}(-1)^{v\cdot(u\oplus u_0)}W_{g'}(a') + \sum_{v\in\mathbb{F}_2^k\setminus(\langle u_0\oplus u_1\rangle^\perp\cup\langle u_0\oplus u_2\rangle^\perp)}(-1)^{v\cdot(u\oplus u_0)}W_{g\oplus g'\oplus g''}(a') =$$

$$\begin{cases} 2^{k-2}W_g(a') \text{ if } u \in \{u_0, u_1, u_2, u_0\oplus u_1\oplus u_2\} \\ 0 \text{ otherwise}\end{cases} + \begin{cases} 2^{k-2}W_{g''}(a') \text{ if } u \in \{u_0, u_1\} \\ -2^{k-2}W_{g''}(a') \text{ if } u \in \{u_2, u_0\oplus u_1\oplus u_2\} \\ 0 \text{ otherwise}\end{cases}$$

$$+ \begin{cases} 2^{k-2}W_{g'}(a') \text{ if } u \in \{u_0, u_2\} \\ -2^{k-2}W_{g'}(a') \text{ if } u \in \{u_1, u_0\oplus u_1\oplus u_2\} \\ 0 \text{ otherwise}\end{cases} + \begin{cases} 2^{k-2}W_{g\oplus g'\oplus g''}(a') \text{ if } u \in \{u_0, u_0\oplus u_1\oplus u_2\} \\ -2^{k-2}W_{g\oplus g'\oplus g''}(a') \text{ if } u \in \{u_1, u_2\} \\ 0 \text{ otherwise}\end{cases}.$$

Relation (7) gives then

$$W_f(a) = \frac{1}{4}W_g(a')\Big(W_{h_{u_0}}(a'') + W_{h_{u_1}}(a'') + W_{h_{u_2}}(a'') + W_{h_{u_0\oplus u_1\oplus u_2}}(a'')\Big) +$$
$$\frac{1}{4}W_{g''}(a')\Big(W_{h_{u_0}}(a'') + W_{h_{u_1}}(a'') - W_{h_{u_2}}(a'') - W_{h_{u_0\oplus u_1\oplus u_2}}(a'')\Big) +$$
$$\frac{1}{4}W_{g'}(a')\Big(W_{h_{u_0}}(a'') - W_{h_{u_1}}(a'') + W_{h_{u_2}}(a'') - W_{h_{u_0\oplus u_1\oplus u_2}}(a'')\Big) +$$
$$\frac{1}{4}W_{g\oplus g'\oplus g''}(a')\Big(W_{h_{u_0}}(a'') - W_{h_{u_1}}(a'') - W_{h_{u_2}}(a'') + W_{h_{u_0\oplus u_1\oplus u_2}}(a'')\Big), \qquad (12)$$

which is different (as an expression) from (11) but necessarily has the same value. Note in particular that, if we develop the expression, the term $W_{h_{u_0\oplus u_1\oplus u_2}}(a'')$ has for factor $W_g(a') - W_{g''}(a') - W_{g'}(a') + W_{g\oplus g'\oplus g''}(a')$. We can check that this factor equals 0 (as it should, because $u_0 \oplus u_1 \oplus u_2$ being different from u_0, u_1 and u_2, the value of $W_{h_{u_0\oplus u_1\oplus u_2}}(a'')$ is supposed to play no role in the value of W_f) because the two functions $g \oplus g'$ and $g \oplus g''$ have disjoint supports. We check this in the next lemma, which will alow to moreover simplify Relation (12). Note that Expression (12) is similar but different from (3).

Lemma 1. *Let g, g', g'' be any Boolean functions such that $(g \oplus g')(g \oplus g'') = 0$. We have then that the integer-valued functions $g - g' - g'' + (g \oplus g' \oplus g'')$ and $W_g - W_{g'} - W_{g''} + W_{g\oplus g'\oplus g''}$ are identically zero.*

Proof. We have $g\oplus g' = g+g'-2gg'$ and $g\oplus g'' = g+g''-2gg''$. Then $0=(g+g'-2gg')(g+g''-2gg'') = g-gg'-gg''+g'g''$; hence, $g'g'' = gg'+gg''-g$. We have $g\oplus g'\oplus g'' = g+g'+g''-2gg'-2gg''-2g'g''+4gg'g'' = g+g'+g''-2gg'-2gg''-2g'g''+4(gg'+gg''-g)$ and then $g-g'-g''+g\oplus g'\oplus g'' = 2gg'+2gg''-2g'g''-2g=0$. For every s-variable Boolean function h, we have $W_h(a') = 2^s\delta_0(a') - 2\widehat{h}(a')$ where $\widehat{h}(a') = \sum_{x\in\mathbb{F}_2^s} h(x)(-1)^{a'\cdot x}$ and we easily deduce from the relation $g-g'-g''+g\oplus g'\oplus g''=0$ and from the linearity of the Fourier transform with respect to the addition in $\mathbb{Z}$ that $W_g(a') - W_{g''}(a') - W_{g'}(a') + W_{g\oplus g'\oplus g''}(a') = 0$. $\square$

Remark 6. *Lemma 1 can be interpreted in the following way (after denoting $f = g\oplus g'$ and $h = g\oplus g''$) which may present some interest in the framework of algebraic attacks: let f be any Boolean function and h be any annihilator of f (i.e.satisfying $fg=0$). Let g be any Boolean function, then we have $W_g - W_{g\oplus f} - W_{g\oplus h} + W_{g\oplus f\oplus h} = 0$.*

Using now Lemma 1, we obtain from Relation (12): $W_f(a) = \frac{1}{4}W_g(a')\Big(W_{h_{u_0}}(a'') + W_{h_{u_1}}(a'') + W_{h_{u_2}}(a'') + W_{h_{u_0\oplus u_1\oplus u_2}}(a'')\Big) + \frac{1}{4}W_{g''}(a')\Big(W_{h_{u_0}}(a'') + W_{h_{u_1}}(a'') - W_{h_{u_2}}(a'') - W_{h_{u_0\oplus u_1\oplus u_2}}(a'')\Big) + \frac{1}{4}W_{g'}(a')\Big(W_{h_{u_0}}(a'') - W_{h_{u_1}}(a'') + W_{h_{u_2}}(a'') - W_{h_{u_0\oplus u_1\oplus u_2}}(a'')\Big) + \frac{1}{4}\big(W_{g'}(a') + W_{g''}(a') - W_g(a')\big)\Big(W_{h_{u_0}}(a'') - W_{h_{u_1}}(a'') - W_{h_{u_2}}(a'') + W_{h_{u_0\oplus u_1\oplus u_2}}(a'')\Big) = \frac{1}{4}W_g(a')\Big(2W_{h_{u_1}}(a'') + 2W_{h_{u_2}}(a'')\Big) + \frac{1}{4}W_{g''}(a')\Big(2W_{h_{u_0}}(a'') - 2W_{h_{u_2}}(a'')\Big) + \frac{1}{4}W_{g'}(a')\Big(2W_{h_{u_0}}(a'') - 2W_{h_{u_1}}(a'')\Big)$, and we obtain from Relation (11):

$$W_f(a) = \frac{1}{2}W_{h_{u_0}}(a'')\big(W_{g'}(a') + W_{g''}(a')\big) + \frac{1}{2}W_{h_{u_1}}(a'')\big(W_g(a') - W_{g'}(a')\big) + \frac{1}{2}W_{h_{u_2}}(a'')\big(W_g(a') - W_{g''}(a')\big), \quad (13)$$

which is the same.

Remark 7. *In Relation (3), to make the coefficient of $W_{h\oplus h'\oplus h''}(a'')$ equal to 0, we are led to take g, g', g'' such that $W_{g\oplus g'\oplus g''}(a') + W_{g''}(a') = W_g(a') + W_{g'}(a')$. For being able to apply Lemma 1, we exchange the roles of g and g'' and we get then $W_f(a', a'') = \frac{1}{2}W_h(a'')\left[W_{g''}(a') + W_{g'}(a')\right] + \frac{1}{2}W_{h'}(a'')\left[W_{g''}(a') - W_g(a')\right] + \frac{1}{2}W_{h''}(a'')\left[W_g(a') - W_{g'}(a')\right]$, similar to (13) but not the same.*

3.2.2 $Im(F)$ of size 4

In this case, we apply what we observed in Remark 2 and take then $k=2$, since continuing in the most general setting as we did with the previous cases would lead to complex relations. Let us recall Theorem 1 in the particular case of $k=2$. Given $F = (f_1, f_2)$ a $(s,2)$-vectorial Boolean function with image set $\{(0,0),(0,1),(1,0),(1,1)\}$ and g an s-variable Boolean function, and $h_{(0,0)}, h_{(0,1)}, h_{(1,0)}, h_{(1,1)}$ four Boolean functions in t variables, we define the $n=s+t$-variable Boolean function $f(x,y) = g(x)\oplus h_{F(x)}(y)$, where $x\in\mathbb{F}_2^s, y\in\mathbb{F}_2^t$. Then we have

$$\begin{aligned} f(x,y) &= g(x)\oplus f_1(x)f_2(x)[h_{(0,0)}(y)\oplus h_{(0,1)}(y)\oplus h_{(1,0)}(y)\oplus h_{(1,1)}(y)] \\ &\quad \oplus f_1(x)[h_{(0,0)}(y)\oplus h_{(1,0)}(y)] \oplus f_2(x)[h_{(0,0)}(y)\oplus h_{(0,1)}(y)] \oplus h_{(0,0)}(y). \quad (14) \end{aligned}$$

Defining $h(y,u) = h_u(y)$, that is, $h = h_{(0,0)}||h_{(0,1)}||h_{(1,0)}||h_{(1,1)}$, we have:

$$\begin{aligned} W_f(a) &= \frac{1}{4}\Big[W_h(a^{''},0,0)W_g(a^{'}) + W_h(a^{''},0,1)W_{g\oplus f_2}(a^{'}) \\ &\quad + W_h(a^{''},1,0)W_{g\oplus f_1}(a^{'}) + W_h(a^{''},1,1)W_{g\oplus f_1\oplus f_2}(a^{'})\Big]. \end{aligned} \tag{15}$$

Function (1) as a particular case: Let $g, g', g^{''}$ be three Boolean functions in s variables such that $f_1(x) = (g \oplus g')(x)$ and $f_2(x) = (g \oplus g^{''})(x)$. Assuming that:

$$h_{(0,1)} = h_{(0,0)} \oplus h_{(1,0)} \oplus h_{(1,1)},$$

there exist three Boolean functions $h, h', h^{''}$ in t variables such that $h_{(0,0)}(y) = h(y)$, $h_{(0,1)}(y) = (h \oplus h' \oplus h^{''})(y)$, $h_{(1,0)}(y) = h^{''}(y)$, $h_{(1,1)}(y) = h'(y)$. Then by (14) we have

$$\begin{aligned} f(x,y) &= g(x) \oplus h(y) \oplus (g \oplus g')(x)(h \oplus h^{''})(y) \oplus (g \oplus g^{''})(x)(h' \oplus h^{''})(y) \\ &= g(x) \oplus h(y) \oplus (g \oplus g^{'})(x)(h \oplus h^{'})(y) \oplus (g^{'} \oplus g'')(x)(h^{'} \oplus h'')(y) \end{aligned}$$

which is equal to Function (1) and the Walsh spectrum given by (15) is the same as (3). Indeed, (3) can be rewrote as

$$\begin{aligned} W_f(a', a^{''}) &= \frac{1}{4}W_g(a')\Big[W_h(a^{''}) + W_{h\oplus h'\oplus h''}(a^{''}) + W_{h''}(a^{''}) + W_{h'}(a^{''})\Big] \\ &\quad + \frac{1}{4}W_{g''}(a')\Big[W_h(a^{''}) - W_{h\oplus h'\oplus h''}(a^{''}) + W_{h''}(a^{''}) - W_{h'}(a^{''})\Big] \\ &\quad + \frac{1}{4}W_{g'}(a')\Big[W_h(a^{''}) + W_{h\oplus h'\oplus h''}(a^{''}) - W_{h''}(a^{''}) - W_{h'}(a^{''})\Big] \\ &\quad + \frac{1}{4}W_{g\oplus g'\oplus g''}(a')\Big[W_h(a^{''}) - W_{h\oplus h'\oplus h''}(a^{''}) - W_{h''}(a^{''}) + W_{h'}(a^{''})\Big] \\ &= \frac{1}{4}\Big[W_{\tilde{h}}(a^{''},0,0)W_g(a') + W_{\tilde{h}}(a^{''},0,1)W_{g''}(a') + W_{\tilde{h}}(a^{''},1,0)W_{g'}(a') \\ &\quad + W_{\tilde{h}}(a^{''},1,1)W_{g\oplus g'\oplus g''}(a')\Big], \end{aligned} \tag{16}$$

where $\tilde{h} = h||h \oplus h' \oplus h^{''}||h^{''}||h'$. Recall that $f_1(x) = (g \oplus g')(x)$, $f_2(x) = (g \oplus g^{''})(x)$, $h_{(0,0)}(y) = h(y)$, $h_{(0,1)}(y) = (h \oplus h' \oplus h^{''})(y)$, $h_{(1,0)}(y) = h^{''}(y)$, $h_{(1,1)}(y) = h'(y)$. (16) is the same as (15) by replacing $\tilde{h}$ with h.

3.2.3 $Im(F)$ of size at most 8

We now consider the vectorial Boolean function $F(x) = (f_1(x), f_2(x), f_3(x)) \in \mathbb{F}_2^3$ in Construction 1. According to Theorem 1, we have:

$$\begin{aligned} f(x,y) &= g(x) \oplus h_{(0,0,0)}(y) \oplus f_1(x)f_2(x)f_3(x) \\ &\quad [(h_{(0,0,0)} \oplus h_{(0,0,1)} \oplus h_{(0,1,0)} \oplus h_{(0,1,1)} \oplus h_{(1,0,0)} \oplus h_{(1,0,1)} \oplus h_{(1,1,0)} \oplus h_{(1,1,1)})(y)] \\ &\quad \oplus f_1(x)f_2(x)[(h_{(0,0,0)} \oplus h_{(0,1,0)} \oplus h_{(1,0,0)} \oplus h_{(1,1,0)})(y)] \\ &\quad \oplus f_1(x)f_3(x)[(h_{(0,0,0)} \oplus h_{(1,0,0)} \oplus h_{(0,0,1)} \oplus h_{(1,0,1)})(y)] \\ &\quad \oplus f_2(x)f_3(x)[(h_{(0,0,0)} \oplus h_{(0,0,1)} \oplus h_{(0,1,0)} \oplus h_{(0,1,1)})(y)] \\ &\quad \oplus f_1(x)[(h_{(0,0,0)} \oplus h_{(1,0,0)})(y)] \oplus f_2(x)[(h_{(0,0,0)} \\ &\quad \oplus h_{(0,1,0)})(y)] \oplus f_3(x)[(h_{(0,0,0)} \oplus h_{(0,0,1)})(y)]. \end{aligned} \tag{17}$$

Function (2) **as a particular case:** Let g, g', g'', g''' be four s-variable Boolean functions such that $f_1(x) = (g \oplus g')(x)$, $f_2(x) = (g \oplus g'')(x)$, $f_3(x) = (g \oplus g''')(x))$, and assuming:

$$\begin{aligned} h_{(0,0,1)} &= h_{(0,0,0)} \oplus h_{(1,0,0)} \oplus h_{(1,0,1)}, \\ h_{(0,1,0)} &= h_{(0,0,0)} \oplus h_{(1,1,1)} \oplus h_{(1,0,1)}, \\ h_{(0,1,1)} &= h_{(0,0,0)} \oplus h_{(1,1,1)} \oplus h_{(1,0,0)}, \\ h_{(1,1,0)} &= h_{(1,1,1)} \oplus h_{(1,0,0)} \oplus h_{(1,0,1)}, \end{aligned}$$

let h, h', h'', h''' be four t-variable Boolean functions such that: $h_{(0,0,0)}(y) = h(y)$, $h_{(0,0,1)}(y) = (h \oplus h'' \oplus h''')(y)$, $h_{(0,1,0)}(y) = (h \oplus h' \oplus h''')(y)$, $h_{(0,1,1)}(y) = (h \oplus h' \oplus h'')(y)$, $h_{(1,0,0)}(y) = h''(y)$, $h_{(1,0,1)}(y) = h'''(y)$, $h_{(1,1,0)}(y) = (h' \oplus h'' \oplus h''')(y)$, and $h_{(1,1,1)}(y) = h'(y)$. Then the coefficients of $f_1(x)f_2(x)f_3(x)$, $f_1(x)f_2(x)$, $f_1(x)f_3(x)$, and $f_2(x)f_3(x)$ are all equal to 0 in (17), which becomes

$$\begin{aligned} & f(x,y) \\ = \; & g(x) \oplus h(y) \oplus f_1(x)[(h_{(0,0,0)} \oplus h_{(1,0,0)})(y)] \oplus f_2(x)[(h_{(0,0,0)} \oplus h_{(0,1,0)})(y)] \oplus \\ & f_3(x)[(h_{(0,0,0)} \oplus h_{(0,0,1)})(y)] \\ = \; & g(x) \oplus h(y) \oplus (g \oplus g')(x)(h \oplus h'')(y) \oplus \\ & (g \oplus g'')(x)(h' \oplus h''')(y) \oplus (g \oplus g''')(x)(h'' \oplus h''')(y) \\ = \; & g(x) \oplus h(y) \oplus g(x)h(y) \oplus g'(x)h(y) \oplus g'(x)h''(y) \oplus g(x)h'(y) \\ & \oplus g''(x)h'(y) \oplus g''(x)h'''(y) \oplus g'''(x)h''(y) \oplus g'''(x)h'''(y) \end{aligned}$$

which is equal to Function (2). We can then consider Construction 1 as a proper general construction covering as particular cases most of the main known secondary constructions.

References

[1] P. Camion, C. Carlet, P. Charpin and N. Sendrier. On correlation-immune functions, *Proceedings of CRYPTO 1991, Lecture Notes in Computer Science* 576, pp. 86-100, 1991.

[2] C. Carlet. A construction of bent functions. *Finite Fields and Applications, London Mathematical Society*, Lecture Series 233, Cambridge University Press, pp. 47-58, 1996.

[3] C. Carlet. A construction of bent functions. *Finite Fields and Applications, London Mathematical Society*, Lecture Series 233, Cambridge University Press, pp. 47-58, 1996.

[4] C. Carlet. On the secondary constructions of resilient and bent functions. *Coding, Cryptography and Combinatorics*, pages 3–28, 2004.

[5] C. Carlet. Boolean Functions for Cryptography and Coding Theory. Monograph in *Cambridge University Press*, 2021.

[6] C. Carlet and S. Mesnager. Four decades of research on bent functions. *Designs, Codes and Cryptography* 78(1), pp. 5-50, 2016.

[7] C. Carlet, F. Zhang and Y. Hu. Secondary constructions of bent functions and their enforcement. *Advances in Mathematics of Communications* 6 (3), pp. 305-314, 2012.

[8] John F Dillon. *Elementary Hadamard difference sets.* PhD thesis, Univ. of Maryland, 1974.

[9] Robert L McFarland. A family of difference sets in non-cyclic groups. *Journal of Combinatorial Theory, Series A*, 15(1):1–10, 1973.

[10] S. Mesnager. *Bent functions: fundamentals and results.* Springer, pp. 1-544, 2016.

[11] O. S. Rothaus. On "bent" functions. *Journal of Combinatorial Theory, Series A* 20, pp. 300-305, 1976.

[12] F. Zhang, C. Carlet, Y. Hu and T.-J. Cao. Secondary constructions of highly nonlinear Boolean functions and disjoint spectra plateaued functions. *Information Sciences* 283, pp. 94-106, 2014.

[13] F. Zhang, C. Carlet, Y. Hu and W. Zhang. New secondary constructions of bent functions. *Applicable Algebra in Engineering, Communication and Computing (AAECC)* 27 (5), pp. 413-434, 2016.