SCIENCE CHINA
Information Sciences Manuscript

• **Supplementary File** •

January 2016, Vol. 59 xxxxxx:1–xxxxxx:4
doi: xxxxxxxxxxxxxx

Further results on constructions of generalized bent Boolean functions

ZHANG Fengrong[1], XIA Shixiong[1*], STĂNICĂ Pantelimon[2] & ZHOU Yu[3]

[1]*School of Computer Science and Technology, China University of Mining and Technology, Xuzhou* 221116*, PR China;*
[2]*Naval Postgraduate School, Applied Mathematics Department, Monterey, CA* 93943*, USA; email: pstanica@nps.edu;*
[3]*Science and Technology on Communication Security Laboratory, Chengdu* 610041*, PR China*

Received September 10, 2014; accepted November 24, 2015; published online January 1, 2016

Abstract

Keywords

Citation Zhang F, Xia S, Stănică P, et al. Further results on constructions of generalized bent Boolean functions. Sci China Inf Sci, 2016, 59(1): xxxxxx, doi: xxxxxxxxxxxxxx

Appendix A Constructions of generalized bent functions in $\mathcal{GB}_n^q$

In this section, we characterize a class of generalized bent Boolean functions (defined on $\mathbb{Z}_2^{n+m}$ with values in $\mathbb{Z}_q$) symmetric with respect to m variables, where m is a positive even integer. We now provide the proof of Theorem 1.

Proof. From Lemma 1, the gbentness of h will be proved if we show that $\mathcal{C}_h(\mathbf{u},\mathbf{v}) = 0$ for any $(\mathbf{u},\mathbf{v}) \neq \mathbf{0}_{n+m}$ and $\mathcal{C}_h(\mathbf{u},\mathbf{v}) = 2^{n+m}$ for $(\mathbf{u},\mathbf{v}) = \mathbf{0}_{n+m}$.

Clearly, as it is known, ϑ is a bent function in m variables. If $\mathbf{c} = \mathbf{0}_m$, then h is gbent since $H_h(\mathbf{u},\mathbf{v}) = H_f(\mathbf{u})H_{\frac{q}{2}\vartheta}(\mathbf{v})$ [1, Theorem 6].

In the following, we suppose that $\mathbf{c} \neq \mathbf{0}_m$. For brevity, we let $D_f(\mathbf{u}) := f(\mathbf{x}) - f(\mathbf{x}\oplus\mathbf{u})$ and $\Delta_{\mathbf{v}}^{\mathbf{u}}(g) := g_{\mathbf{c}\cdot\mathbf{y}}(\mathbf{x}) - g_{\mathbf{c}\cdot(\mathbf{y}\oplus\mathbf{v})}(\mathbf{x}\oplus\mathbf{u})$. Now, for h as defined by Theorem 1, using

$$\begin{aligned} h(\mathbf{x},\mathbf{y}) - h(\mathbf{x}\oplus\mathbf{u},\mathbf{y}\oplus\mathbf{v}) &= f(\mathbf{x}) + \tfrac{q}{2}(\mathbf{c}\cdot\mathbf{y})g_{\mathbf{c}\cdot\mathbf{y}}(\mathbf{x}) + \tfrac{q}{2}\vartheta(\mathbf{y}) \\ &\quad - f(\mathbf{x}\oplus\mathbf{u}) - \tfrac{q}{2}(\mathbf{c}\cdot(\mathbf{y}\oplus\mathbf{v}))g_{\mathbf{c}\cdot(\mathbf{y}\oplus\mathbf{v})}(\mathbf{x}\oplus\mathbf{u}) - \tfrac{q}{2}\vartheta(\mathbf{y}\oplus\mathbf{v}) \\ &= D_f(\mathbf{u}) + \tfrac{q}{2}(\mathbf{c}\cdot\mathbf{y})\Delta_{\mathbf{v}}^{\mathbf{u}}(g) - \tfrac{q}{2}(\mathbf{c}\cdot\mathbf{v})g_{\mathbf{c}\cdot(\mathbf{y}\oplus\mathbf{v})}(\mathbf{x}\oplus\mathbf{u}) - \tfrac{q}{2}(\mathbf{v}\cdot(\mathbf{y}'',\mathbf{y}')\oplus\vartheta(\mathbf{v})), \end{aligned}$$

we obtain

$$\begin{aligned} \mathcal{C}_h(\mathbf{u},\mathbf{v}) &= \sum_{\mathbf{x}\in\mathbb{Z}_2^n,\mathbf{y}\in\mathbb{Z}_2^m} \zeta^{D_f(\mathbf{u})+\frac{q}{2}(\mathbf{c}\cdot\mathbf{y})\Delta_{\mathbf{v}}^{\mathbf{u}}(g)-\frac{q}{2}(\mathbf{c}\cdot\mathbf{v})g_{\mathbf{c}\cdot(\mathbf{y}\oplus\mathbf{v})}(\mathbf{x}\oplus\mathbf{u})-\frac{q}{2}(\mathbf{v}\cdot(\mathbf{y}'',\mathbf{y}')\oplus\vartheta(\mathbf{v}))} \\ &= \sum_{\mathbf{x}\in\mathbb{Z}_2^n} \zeta^{D_f(\mathbf{u})} \sum_{\mathbf{y}\in\mathbb{Z}_2^m} \zeta^{\frac{q}{2}(\mathbf{c}\cdot\mathbf{y})\Delta_{\mathbf{v}}^{\mathbf{u}}(g)-\frac{q}{2}(\mathbf{c}\cdot\mathbf{v})g_{\mathbf{c}\cdot(\mathbf{y}\oplus\mathbf{v})}(\mathbf{x}\oplus\mathbf{u})-\frac{q}{2}(\mathbf{v}\cdot(\mathbf{y}'',\mathbf{y}')\oplus\vartheta(\mathbf{v}))}. \end{aligned} \tag{A1}$$

Obviously, $\mathcal{C}_h(\mathbf{u},\mathbf{v}) = 2^{n+m}$ for $(\mathbf{u},\mathbf{v}) = \mathbf{0}_{n+m}$. Now we consider the value of $\mathcal{C}_h(\mathbf{u},\mathbf{v})$ for $(\mathbf{u},\mathbf{v}) \neq \mathbf{0}_{n+m}$. We consider the following few cases.

Case 1. For $\mathbf{v} = \mathbf{0}_m \neq \mathbf{c}, \mathbf{u} \neq \mathbf{0}_n$, we have

$$\begin{aligned} \mathcal{C}_h(\mathbf{u},\mathbf{0}_m) &= \sum_{\mathbf{x}\in\mathbb{Z}_2^n} \zeta^{D_f(\mathbf{u})} \sum_{\mathbf{y}\in\mathbb{Z}_2^m} \zeta^{\frac{q}{2}(\mathbf{c}\cdot\mathbf{y})\Delta_{\mathbf{0}_m}^{\mathbf{u}}(g)} \\ &= \sum_{\mathbf{y}\in\mathbb{Z}_2^m,\mathbf{c}\cdot\mathbf{y}=1} \sum_{\mathbf{x}\in\mathbb{Z}_2^n} \zeta^{D_f(\mathbf{u})+\frac{q}{2}\Delta_{\mathbf{0}_m}^{\mathbf{u}}(g)}. \end{aligned}$$

Since $f + \frac{q}{2}g_0$ and $f + \frac{q}{2}g_1$ are gbent, it follows that $\mathcal{C}_h(\mathbf{u},\mathbf{0}_m) = 0$.

Case 2. For $\mathbf{v} \neq \mathbf{0}_m$, we have there are two subcases to be considered.

* Corresponding author (email: xiasx@cumt.edu.cn)

(*i*) If $\mathbf{c}\cdot\mathbf{v}=0$, then we have

$$\begin{aligned}\mathcal{C}_h(\mathbf{u},\mathbf{v}) &= \sum_{\mathbf{x}\in\mathbb{Z}_2^n}\zeta^{D_f(\mathbf{u})}\sum_{\mathbf{y}\in\mathbb{Z}_2^m}\zeta^{\frac{q}{2}(\mathbf{c}\cdot\mathbf{y})\Delta_{\mathbf{v}}^{\mathbf{u}}(g)-\frac{q}{2}(\mathbf{c}\cdot\mathbf{v})g_{\mathbf{c}\cdot(\mathbf{y}\oplus\mathbf{v})}(\mathbf{x}\oplus\mathbf{u})-\frac{q}{2}(\mathbf{v}\cdot(\mathbf{y}'',\mathbf{y}')\oplus\vartheta(\mathbf{v}))}\\ &= \sum_{\mathbf{y}\in\mathbb{Z}_2^m}\sum_{\mathbf{x}\in\mathbb{Z}_2^n}\zeta^{D_f(\mathbf{u})-\frac{q}{2}(\mathbf{v}\cdot(\mathbf{y}'',\mathbf{y}')\oplus\vartheta(\mathbf{v}))+\frac{q}{2}(\mathbf{c}\cdot\mathbf{y})\Delta_{\mathbf{0}_m}^{\mathbf{u}}(g)}.\end{aligned} \tag{A2}$$

Further,

(a) For $\mathbf{u}\neq\mathbf{0}_n$,

$$\sum_{\mathbf{x}\in\mathbb{Z}_2^n}\zeta^{D_f(\mathbf{u})-\frac{q}{2}(\mathbf{v}\cdot(\mathbf{y}'',\mathbf{y}')\oplus\vartheta(\mathbf{v}))+\frac{q}{2}(\mathbf{c}\cdot\mathbf{y})\Delta_{\mathbf{0}_m}^{\mathbf{u}}(g)}$$

equals 0 for any $\mathbf{y}\in\mathbb{Z}_2^m$ since f, $f+\frac{q}{2}g_0$ and $f+\frac{q}{2}g_1$ are gbent. According to (A2), we have $\mathcal{C}_h(\mathbf{u},\mathbf{v})=0$.

(b) For $\mathbf{u}=\mathbf{0}_n$, according to (A2), we have

$$\mathcal{C}_h(\mathbf{u},\mathbf{v})=\sum_{\mathbf{x}\in\mathbb{Z}_2^n}\sum_{\mathbf{y}\in\mathbb{Z}_2^m}\zeta^{-\frac{q}{2}(\mathbf{v}\cdot(\mathbf{y}'',\mathbf{y}')\oplus\vartheta(\mathbf{v}))}=0.$$

(*ii*) If $\mathbf{c}\cdot\mathbf{v}=1$, then we have

$$\begin{aligned}\mathcal{C}_h(\mathbf{u},\mathbf{v}) &= \sum_{\mathbf{x}\in\mathbb{Z}_2^n}\zeta^{D_f(\mathbf{u})}\sum_{\mathbf{y}\in\mathbb{Z}_2^m}\zeta^{\frac{q}{2}(\mathbf{c}\cdot\mathbf{y})\Delta_{\mathbf{v}}^{\mathbf{u}}(g)-\frac{q}{2}g_{\mathbf{c}\cdot(\mathbf{y}\oplus\mathbf{v})}(\mathbf{x}\oplus\mathbf{u})-\frac{q}{2}(\mathbf{v}\cdot(\mathbf{y}'',\mathbf{y}')\oplus\vartheta(\mathbf{v}))}\\ &= \sum_{\mathbf{x}\in\mathbb{Z}_2^n}\sum_{\mathbf{y}\in\mathbb{Z}_2^m,\mathbf{c}\cdot\mathbf{y}=0}\zeta^{D_f(\mathbf{u})-\frac{q}{2}g_1(\mathbf{x}\oplus\mathbf{u})-\frac{q}{2}(\mathbf{v}\cdot(\mathbf{y}'',\mathbf{y}')\oplus\vartheta(\mathbf{v}))}\\ &+ \sum_{\mathbf{x}\in\mathbb{Z}_2^n}\sum_{\mathbf{y}\in\mathbb{Z}_2^m,\mathbf{c}\cdot\mathbf{y}=1}\zeta^{D_f(\mathbf{u})+\frac{q}{2}g_1(\mathbf{x}\oplus\mathbf{u})-qg_0(\mathbf{x}\oplus\mathbf{u})-\frac{q}{2}(\mathbf{v}\cdot(\mathbf{y}'',\mathbf{y}')\oplus\vartheta(\mathbf{v}))}\\ &= \sum_{\mathbf{x}\in\mathbb{Z}_2^n}\sum_{\mathbf{y}\in\mathbb{Z}_2^m,\mathbf{c}\cdot\mathbf{y}=0}\zeta^{D_f(\mathbf{u})-\frac{q}{2}g_1(\mathbf{x}\oplus\mathbf{u})-\frac{q}{2}(\mathbf{v}\cdot(\mathbf{y}'',\mathbf{y}')\oplus\vartheta(\mathbf{v}))}\\ &+ \sum_{\mathbf{x}\in\mathbb{Z}_2^n}\sum_{\mathbf{y}\in\mathbb{Z}_2^m,\mathbf{c}\cdot\mathbf{y}=1}\zeta^{D_f(\mathbf{u})+\frac{q}{2}g_1(\mathbf{x}\oplus\mathbf{u})-\frac{q}{2}(\mathbf{v}\cdot(\mathbf{y}'',\mathbf{y}')\oplus\vartheta(\mathbf{v}))}\\ &= \sum_{\mathbf{x}\in\mathbb{Z}_2^n}\zeta^{D_f(\mathbf{u})}(-1)^{g_1(\mathbf{x}\oplus\mathbf{u})}\sum_{\mathbf{y}\in\mathbb{Z}_2^m}(-1)^{\mathbf{v}\cdot(\mathbf{y}'',\mathbf{y}')\oplus\vartheta(\mathbf{v})}\end{aligned} \tag{A3}$$

Since $\sum_{\mathbf{y}\in\mathbb{Z}_2^m}(-1)^{\mathbf{v}\cdot(\mathbf{y}'',\mathbf{y}')\oplus\vartheta(\mathbf{v})}=0$, then $\mathcal{C}_h(\mathbf{u},\mathbf{v})=0$.

Combining the above two cases, we have $\mathcal{C}_h(\mathbf{u},\mathbf{v})=0$ for any $(\mathbf{u},\mathbf{v})\neq\mathbf{0}_{n+m}$.

Appendix B Further constructions of generalized bent functions in $\mathcal{GB}_n^8$

Let $f\in\mathcal{GB}_n^8$ be as

$$f(\mathbf{x})=v_0(\mathbf{x})+v_1(\mathbf{x})\cdot 2+v_2(\mathbf{x})\cdot 2^2, \tag{B1}$$

where $v_i(\mathbf{x})\in\mathcal{B}_n, i=0,1,2$.

In this section, we concentrate on the design of the initial functions v_0,v_1,v_2 such that f is gbent.

According to the relationship between a bent function and its dual, the equation

$$W_{v_0\oplus v_2}(\mathbf{u})W_{v_1\oplus v_2}(\mathbf{u})=W_{v_2}(\mathbf{u})W_{v_0\oplus v_1\oplus v_2}(\mathbf{u}),\ \text{for all } \mathbf{u}\in\mathbb{Z}_2^n; \tag{B2}$$

in Theorem 2 is equivalent to

$$(-1)^{\widetilde{(v_0\oplus v_2)}(\mathbf{u})}(-1)^{\widetilde{(v_1\oplus v_2)}(\mathbf{u})}(-1)^{\widetilde{v_2}(\mathbf{u})}(-1)^{\widetilde{(v_0\oplus v_1\oplus v_2)}(\mathbf{u})}=1,\ \text{for all } \mathbf{u}\in\mathbb{Z}_2^n. \tag{B3}$$

Based on this, we now provide the proof of Theorem 3.

Proof. According to the hypothesis of (*i*) (resp. (*ii*)), Theorem 2 and (B3), it is clear that v_0,v_1,v_2 satisfy the conditions of Theorem 2 for the even case.

From (*iii*), we know that $v_2, v_0\oplus v_2, v_1\oplus v_2, v_0\oplus v_1\oplus v_2$ are all bent since v_0,v_1 are two linear functions. From Lemma 2, we have

$$\begin{aligned}\widetilde{(v_0\oplus v_2)}(\mathbf{x})&=\widetilde{v_2}(\mathbf{x}\oplus\mathbf{a}_0),\\ \widetilde{(v_1\oplus v_2)}(\mathbf{x})&=\widetilde{v_2}(\mathbf{x}\oplus\mathbf{a}_1),\\ \widetilde{(v_0\oplus v_1\oplus v_2)}(\mathbf{u})&=\widetilde{v_2}(\mathbf{x}\oplus\mathbf{a}_0\oplus\mathbf{a}_1).\end{aligned}$$

Thus, if

$$\widetilde{v_2}(\mathbf{x})\oplus\widetilde{v_2}(\mathbf{x}\oplus\mathbf{a}_0)\oplus\widetilde{v_2}(\mathbf{x}\oplus\mathbf{a}_1)\oplus\widetilde{v_2}(\mathbf{x}\oplus\mathbf{a}_0\oplus\mathbf{a}_1)=0,$$

then (B3) holds.

With respect to (*iv*), the proof follows a similar approach as the proof of item (*iii*).

Remark 1. *With respect to (ii), it is easy to find two functions v_0,v_2 such that both v_2 and $v_0\oplus v_2$ are bent. For example, let $v_2(\mathbf{x})$ be a bent-negabent function, then $\sigma_2(\mathbf{x})\oplus v_2(\mathbf{x})$ is bent (i.e., bent-negabent) (see. [2]), where $\sigma_2(\mathbf{x})$ denotes the elementary symmetric Boolean function on n variables with degree 2, i.e.,*

$$\sigma_2(\mathbf{x})=\bigoplus_{i_1,i_2}x_{i_1}x_{i_2},\forall\ \mathbf{x}=(x_1,x_2,\cdots,x_n)\in\mathbb{Z}_2^n, 1\leqslant i_1<i_2\leqslant n.$$

Thus, for any a bent-negabent function v_2, we are able to obtain a gbent function f. In fact, if (v_0, v_2) is a bent $(n,2)-$function (i.e., v_0, v_2 and $v_0 \oplus v_2$ are bent), then we are also able to obtain a gbent function f.

Dillon provided a method to check $\mathcal{M}^{\#}$ [?]. A bent function f in n variables belongs to $\mathcal{M}^{\#}$ if and only if there exists an $\frac{n}{2}$-dimensional vector subspace $\mathbb{V}$ in $\mathbb{Z}_2^n$ such that the second order derivatives

$$D_{\alpha,\beta}f(\mathbf{x}) = f(\mathbf{x}) \oplus f(\mathbf{x}\oplus\alpha) \oplus f(\mathbf{x}\oplus\beta) \oplus f(\mathbf{x}\oplus\alpha\oplus\beta)$$

vanish for any $\alpha, \beta \in \mathbb{V}$. If $v_2 \in \mathcal{M}$, then its dual is easy to be obtained [4]. Hence, for any bent function v_2 belonging to $\mathcal{M}$, we are able to find $\mathbf{a}_0, \mathbf{a}_1$ such that $\widetilde{v_2}(\mathbf{x}) \oplus \widetilde{v_2}(\mathbf{x}\oplus\mathbf{a}_0) \oplus \widetilde{v_2}(\mathbf{x}\oplus\mathbf{a}_1) \oplus \widetilde{v_2}(\mathbf{x}\oplus\mathbf{a}_0\oplus\mathbf{a}_1) = 0$.

With respect to (iv), we are able to find examples of application of item (iv) (there are two examples in [5, Example 1, 2]).

For (i), it is not easy to find three different *bent functions v_0, v_1, v_2 such that $\widetilde{(v_0 \oplus v_2)}(\mathbf{x}) = \widetilde{v_0}(\mathbf{x}) \oplus \widetilde{v_2}(\mathbf{x})$, $\widetilde{(v_1 \oplus v_2)}(\mathbf{x}) = \widetilde{v_1}(\mathbf{x}) \oplus \widetilde{v_2}(\mathbf{x})$, $\widetilde{(v_0 \oplus v_1 \oplus v_2)}(\mathbf{x}) = \widetilde{v_0}(\mathbf{x}) \oplus \widetilde{v_1}(\mathbf{x}) \oplus \widetilde{v_2}(\mathbf{x})$.*

We now provide the proof of Theorem 4.

Proof. From Theorem 2 (ii), there are two conditions to be satisfied by a gbent f. We know that $\phi(\mathbf{y}) \cdot \mathbf{x} \oplus g(\mathbf{y})$ is a bent function in $2k$ variables, where ϕ is a Boolean permutation on $\mathbb{Z}_2^k$. From Lemma 3, $\phi(\mathbf{y}_0^{(j)}) \cdot \mathbf{x} \oplus g(\mathbf{y}_0^{(j)})$ and $\phi(\mathbf{y}_1^{(j)}) \cdot \mathbf{x} \oplus g(\mathbf{y}_1^{(j)})$ are complementary semibent functions on $\mathbb{Z}_2^{2k-1}$, where $j = 1, 2, \cdots, k$. Further, we know v_2 and $v_2 \oplus v_1$ are complementary semibent functions on $\mathbb{Z}_2^{2k-1}$. Since $\mathbf{a}_0 \cdot \mathbf{x}$ is a linear function in k variables, and $\phi \oplus \varphi$ is a Boolean permutation on $\mathbb{Z}_2^k$, we have $v_0 \oplus v_2$ and $v_0 \oplus v_1 \oplus v_2$ are complementary semibent functions on $\mathbb{Z}_2^{2k-1}$. Thus, it is sufficient to show

$$supp(W_{v_2}) = supp(W_{v_0 \oplus v_2})$$

for the secondary condition of Theorem 2 (ii).

Let $\alpha, \beta \in \mathbb{Z}_2^k, \beta_\epsilon^{(j)} = (\beta_1, \ldots, \beta_{j-1}, \epsilon, \beta_{j+1} \ldots, \beta_k)$. We have

$$\begin{aligned} W_{v_2}(\alpha, \beta_0^{(j)}) = & \sum_{\mathbf{y}_0^{(j)} \in \mathbb{Z}_2^k, \phi(\mathbf{y}_0^{(j)}) = \alpha \oplus \mathbf{a}_0} (-1)^{g(\mathbf{y}_0^{(j)}) \oplus \mathbf{y}_0^{(j)} \cdot \beta_0^{(j)}} \sum_{\mathbf{x} \in \mathbb{Z}_2^k} (-1)^{\phi(\mathbf{y}_0^{(j)}) \cdot \mathbf{x} \oplus (\alpha \oplus \mathbf{a}_0) \cdot \mathbf{x}} \\ & + \sum_{\mathbf{y}_0^{(j)} \in \mathbb{Z}_2^k, \phi(\mathbf{y}_0^{(j)}) \neq \alpha \oplus \mathbf{a}_0} (-1)^{g(\mathbf{y}_0^{(j)}) \oplus \mathbf{y}_0^{(j)} \cdot \beta_0^{(j)}} \sum_{\mathbf{x} \in \mathbb{Z}_2^k} (-1)^{\phi(\mathbf{y}_0^{(j)}) \cdot \mathbf{x} \oplus (\alpha \oplus \mathbf{a}_0) \cdot \mathbf{x}}. \end{aligned}$$

Using the above identity, we derive

$$W_{v_2}(\alpha, \beta_0^{(j)}) = \begin{cases} 0, & \text{if } \phi^{-1}(\alpha \oplus \mathbf{a}_0) \notin \mathbb{Z}_2^{j-1} \times \{0\} \times \mathbb{Z}_2^{k-j} \\ 2^k (-1)^{g(\phi^{-1}(\alpha \oplus \mathbf{a}_0)) \oplus \phi^{-1}(\alpha \oplus \mathbf{a}_0) \cdot \beta_0^{(j)}} & \text{if } \phi^{-1}(\alpha \oplus \mathbf{a}_0) \in \mathbb{Z}_2^{j-1} \times \{0\} \times \mathbb{Z}_2^{k-j}. \end{cases}$$

Further, we have

$$supp(W_{v_2}) = (\mathbf{a}_0 \oplus \Delta_j) \times \left(\mathbb{Z}_2^{j-1} \times \{0\} \times \mathbb{Z}_2^{k-j} \right),$$

and similarly,

$$supp(W_{v_0 \oplus v_2}) = \{\mathbf{a}_0 \oplus (\phi \oplus \varphi)(\mathbf{y}) | \mathbf{y} \in \mathbb{Z}_2^{j-1} \times \{0\} \times \mathbb{Z}_2^{k-j}\} \times \left(\mathbb{Z}_2^{j-1} \times \{0\} \times \mathbb{Z}_2^{k-j} \right).$$

From the hypothesis, there exists one positive integer $\varrho (\leqslant k)$ such that

$$\{(\phi \oplus \varphi)(\mathbf{y}) | \mathbf{y} \in \mathbb{Z}_2^{\varrho-1} \times \{0\} \times \mathbb{Z}_2^{k-\varrho}\} = \Delta_\varrho,$$

Δ_ϱ is a linear subspace of $\mathbb{Z}_2^k$ and $\mathbf{a}_0 \in \Delta_\varrho$ (we assumed $\mathbf{a}_0 \neq \mathbf{0}$, as the other case is similar), then we set $j = \varrho$, and have

$$supp(W_{v_2}) = (\mathbf{a}_0 \oplus \Delta_\varrho) \times \left(\mathbb{Z}_2^{\varrho-1} \times \{0\} \times \mathbb{Z}_2^{k-\varrho} \right) = supp(W_{v_0 \oplus v_2}).$$

Moreover, we have $W_{v_0 \oplus v_2}(\alpha, \beta_0^{(\varrho)}) = W_{v_2}(\alpha, \beta_0^{(\varrho)}) = 0$, $|W_{v_1 \oplus v_2}(\alpha, \beta_0^{(\varrho)})| = |W_{v_0 \oplus v_1 \oplus v_2}(\alpha, \beta_0^{(\varrho)})| = 2^k$; or, $|W_{v_0 \oplus v_2}(\alpha, \beta_0^{(\varrho)})| = |W_{v_2}(\alpha, \beta_0^{(\varrho)})| = 2^k$, $W_{v_1 \oplus v_2}(\alpha, \beta_0^{(\varrho)}) = W_{v_0 \oplus v_1 \oplus v_2}(\alpha, \beta_0^{(\varrho)}) = 0$, for all $(\alpha, \beta_0^{(\varrho)}) \in \mathbb{Z}_2^n$.

Example 1. *Let $\phi^{(1)}(y_1, \ldots, y_{k-1}) = (\phi_1(y_1, \ldots, y_{k-1}), \ldots, \phi_{k-1}(y_1, \ldots, y_{k-1}))$ be a Boolean permutation on $\mathbb{Z}_2^{k-1}$. Let $\pi(y_1, \ldots, y_{k-1})$ be a orthomorphic permutations on $\mathbb{Z}_2^{k-1}$. Set $\varphi^{(1)}(y_1, \ldots, y_{k-1}) = \pi\left(\phi^{(1)}(y_1, \ldots, y_{k-1})\right)$. Thus, according to the properties of orthomorphic permutation, we know $\phi^{(1)}$ and $\phi^{(1)} \oplus \varphi^{(1)}$ are two Boolean permutations on $\mathbb{Z}_2^{k-1}$ [5]. We set $\varphi(y_1, \ldots, y_k) = (\varphi^{(1)}(y_1, \ldots, y_{k-1}), 0)$, $\phi(y_1, \ldots, y_k) = (\phi^{(1)}(y_1, \ldots, y_{k-1}), y_k)$ and $\varrho = k$. Moreover, we have $\{(\phi \oplus \varphi)(\mathbf{y}) | \mathbf{y} \in \mathbb{Z}_2^{\varrho-1} \times \{0\}\} = \Delta_\varrho = \{\phi(\mathbf{y}) | \mathbf{y} \in \mathbb{Z}_2^{\varrho-1} \times \{0\}\}$. From [5], we know that at least $2^{2^{n-2}}$ orthomorphic permutations in $n-1$ variables can be constructed. We also know there are $2^{n-1}!$ Boolean permutations in $in-1$ variables. Hence, we are able to construct at least $2^{2^{n-2}} \times 2^{n-1}!$ gbent functions f in n variables when n is odd.*

If we set $\varphi = \mathbf{0}_k$, then we immediately have the following corollary.

Corollary 1. Let k, n be two integers and $n = 2k-1$. Let $\mathbf{x}, \mathbf{y} \in \mathbb{Z}_2^k$. Let $\phi = (\phi_1, \phi_2, \ldots, \phi_k)$ be one Boolean permutation on $\mathbb{Z}_2^k$. Set $\Delta_j = \{\phi(\mathbf{y}) | \mathbf{y} \in \mathbb{Z}_2^{j-1} \times \{0\} \times \mathbb{Z}_2^{k-j}\}$, $\mathbf{y}_\epsilon^{(j)} = (y_1, \ldots, y_{j-1}, \epsilon, y_{j+1} \ldots, y_k)$, where $1 \leqslant j \leqslant k, \epsilon \in \mathbb{Z}_2$. Let $f \in \mathcal{GB}_n^8$ be as in (B1), and let $v_0(\mathbf{x}, \mathbf{y}_0^{(j)}) = \mathbf{a}_0 \cdot \mathbf{x}$, $v_1(\mathbf{x}) = \left(\phi(\mathbf{y}_0^{(j)}) \oplus \phi(\mathbf{y}_1^{(j)})\right) \cdot \mathbf{x} \oplus g(\mathbf{y}_0^{(j)}) \oplus g(\mathbf{y}_1^{(j)})$ and $v_2(\mathbf{x}) = \phi(\mathbf{y}_0^{(j)}) \cdot \mathbf{x} \oplus g(\mathbf{y}_0^{(j)})$, where $\mathbf{a}_0 \in \mathbb{Z}_2^k$. If there exists one positive integer $\varrho (\leqslant k)$ such that Δ_ϱ is a linear subspace of $\mathbb{Z}_2^k$ and $\mathbf{a}_0 \in \Delta_\varrho$, then v_0, v_1, v_2 satisfy the conditions of Theorem 2 for the odd case, that is, f is gbent.

References

1 Singh B K. On cross-correlation spectrum of generalized bent functions in generalized Maiorana-McFarland class. Inform. Sci. Lett., 2013, 2-3: 139–145.

2 Zhang F, Wei Y, Pasalic E. Constructions of Bent-Negabent Functions and Their Relation to the Completed Maiorana-McFarland Class. IEEE Trans. Inf. Theory, 2015, 61: 1496–1506.

3 Dillon J. Elementary Hadamard difference sets, Ph.D. Dissertation, Univ. Maryland, College Park, 1974.

4 Mesnager S. Several new infinite families of bent functions and their duals, IEEE Trans. Inf. Theory, 2014, 60: 4397–4407.

5 Carlet C, Zhang F, Hu Y. Secondary constructions of bent functions and their enforcement. Adv. Math. Comm., 2012, 6: 305–314.