Constructing Bent Functions with Extended Building Sets

An $(a, m, h, \pm)$ covering Extended Building Set (EBS) in a group G is a set of h blocks, $\{B_1, ..., B_h\}$ with $|B_1| = a \pm m$ and $|B_2| = |B_3| = \cdots = |B_h| = a$ so that, for each character χ on G, exactly one block has nonzero character sum, and its character sum has modulus m.

A (v, k, λ, n) Difference Set (DS) in a group G, $|G| = v$, is a subset D of G, $|D| = k$, so that $\{d_i d_j^{-1} | d_i, d_j \in D, d_i \neq d_j\} = \lambda(G - \{e\})$, and $n = k - \lambda$.

A $2n$-variable bent function is a $(2^{2n}, 2^{2n-1} \pm 2^{n-1}, 2^{2n-2} \pm 2^{n-1}, 2^{2n-2})$ DS in the group $\mathbb{Z}_2^{2n}$.

An equivalent definition of a bent function is one whose Walsh-Hadamard transform is constantly 2^n in absolute value. A semi-bent function in $2n-1$ variables is one whose WHT is 0 half the time and 2^n in absolute value the rest of the time.

Let $G = \mathbb{Z}_2^{2n}$. Let $f(x_1, x_2, ..., x_{2n})$ be a boolean function on $2n$ variables. Define $B = \{x \in G | f(x) = 1\}$. We know that $\chi(G) = 0$, so $\chi(G - B) + \chi(B) = 0$ or $\chi(G - B) = -\chi(B)$. We also know that each row of the WHT is equal to $\chi(G-B)-\chi(B)$ for some character χ. Note that this means that $\chi(B) = -W_f(u)/2$.

Let f and G be as above. Pick a variable x_i. Define $f_0 = f|_{x_i=0}$ and $f_1 = f|_{x_i=1}$. These will be referred to as the two subfunctions of f in x_i. It is known how to determine the ANF of these from the ANF of f. Any $x_k, k > i$ will become x_{k-1}. $x_k, k < i$ will be unchanged. This holds true for both subfunctions. An x_i will become a $\bar{0}$ in f_0 and a $\bar{1}$ in f_1. Similarly, for any other function g, $x_i g$ will be $\bar{0}$ in f_0 and g in f_1.

It is known that for any bent function f in $2n$ variables, both of its subfunctions f_0, f_1 for any choice of x_i must be semi-bent. In addition, we know that if we examine the WHT of the subfunctions, in any row, the WHT of exactly one of these subfunctions must be nonzero; specifically, it will be $\pm 2^n$. I will use this fact to show that given any bent function f in $2n$ variables, one may convert this into a $(2^{2n-2}, 2^{n-1}, 2, \pm)$ covering EBS in $\mathbb{Z}_2^{2n-1}$.

Begin with a bent function f in $2n$ variables. Let f_0 and f_1 be the subfunctions in x_1 of f. Then, since each row of the WHT is a character, we know that for any character of $G = \mathbb{Z}_2^{2n-1}$, $|\chi(G-f_j)-\chi(f_j)| = 2^n$ and $|\chi(G - f_{j+1}) - \chi(f_{j+1})| = 0$ for some $j \in \mathbb{Z}_2$. Since $\chi(B) = -W_f(u)/2$, this means that $|\chi(f_j)| = 2^{n-1}$ and $|\chi(f_{j+1})| = 0$. So, making f_0 and f_1 our blocks, we will get a $(2^{2n-2}, 2^{n-1}, 2, \pm)$ covering EBS in $\mathbb{Z}_2^{2n-1}$, with the $\pm$ determined by whether the bent function has high weight or low weight. In this way, we can guarantee that constructing all such covering EBS will guarantee we construct all bent functions.

However, we would like to do better. We would like to be able to show that each bent function in $2n$ variables is actually a $(2^{2n-3}, 2^{n-1}, 4, \pm)$ covering EBS in $\mathbb{Z}_2^{2n-2}$. We would then need 4 blocks that each have modulus 0 or 2^{n-1} for every character, with only one 2^{n-1} for each character. Based on granted-values stuff and weight arguments, we know that for any x_i, the two subfunctions of a semi-bent function are either both bent or both not bent. If they are both not bent, then we know that they must each have 2^{2n-4} $\pm 2^n$ WHT values and the rest 0. In addition, there cannot be any rows where they both have nonzero WHT. Similarly, these subfunctions cannot interfere with the subfunctions of the other semi-bent function. So, we can see that if each semi-bent subfunction of the bent function can be broken into two non-bent subfunctions, then those four subsubfunctions will be the blocks of a $(2^{2n-3}, 2^{n-1}, 4, \pm)$ covering EBS in $\mathbb{Z}_2^{2n-2}$. All that is left to prove is that this is always possible. I suspect it is, but I cannot yet prove it. Unless I am missing something, this seems to be impossible to do with the bent function which contains all quadratic terms...