DualBent.tex, 04.10.00, M.G.Parker

A Mapping From Length n Binary Linear Block Codes to Length 2^n Bipolar Bent and Almost Bent Sequences

Matthew.G.Parker [1]

Inst. for Informatikk, University of Bergen,

5020 Bergen, Norway,

`matthew@ii.uib.no`

`http://www.ii.uib.no/ matthew/mattweb.html`

Abstract *It is shown how a half-rate length n binary linear block code can always be used to generate a pair of bipolar Bent sequences of length* 2^n*, for n even. The technique uses the length* 2^n *Walsh-Hadamard Transform in conjunction with multidimensional cyclic shifts and multidimensional phase shifts. The technique is also used to generate Almost Bent sequences when n is odd.*

Note: This paper remains unpublished because (as pointed about by a referee), it rediscovers the completed Maiorana-McFarland class of bent functions. So the result is well-known:
Given a binary $[n, n/2]$-linear code $\mathbf{C}$, i.e. an $n/2$-dimensional vector subspace of F_2^n, the set of all cosets of $\mathbf{C}$ and the set of all cosets of $\mathbf{C}^\perp$ both have size $2^{n/2}$. There exist $2^{n/2}!$ bijections between these two sets. By applying a linear isomorphism, we can assume that $\mathbf{C} = F_2^{n/2} \times \{0\}$ and $\mathbf{C}^\perp = \{0\} \times F_2^{n/2}$. The sequences introduced in this paper then correspond to Boolean functions belonging to the Maiorana-McFarland class.

In the case of a binary $[n, (n+1)/2]$-linear code, a similar construction leads to almost bent sequences.

1 Introduction

It is well-known that the dual of a length n binary linear block code can be obtained using the Walsh-Hadamard Transform (HT) of length 2^n [2]. Using a length 2^n vector (indicator) representation for a half-rate length n binary linear block code, $\mathbf{C}$, this paper shows how a length 2^n vector which represents the modified disjoint sum of all cosets of $\mathbf{C}$ has an HT which is a

[1] This work was funded by NFR Project Number 119390/431

vector representing a modified disjoint sum of all cosets of $\mathbf{C}^\perp$. When $\mathbf{C}$ is half-rate (n even) the two vectors are bipolar and therefore form a pair of bipolar Bent sequences [3], (i.e. they are HTs of each other, and therefore both have 'flat' HT spectrums). When $\mathbf{C}$ is rate $\frac{n+1}{2n}$, (n odd), one of the vectors is bipolar and Almost Bent. Central to the argument of this paper is the equivalence between multidimensional 'phase twist' of a vector and the multidimensional cyclic shift of its HT.

2 The Hadamard Transform (HT)

The HT here refers to the length 2^n transform represented by the $2^n \times 2^n$ matrix formed from the nth tensor product of $\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. In the following, unless required, we implicitly normalise all HT output vectors.

2.1 Cyclic Shift and Phase Twist Properties of the HT

Let $i = \sum_{p=0}^{n-1} i_p 2^p$ and $j = \sum_{p=0}^{n-1} j_p 2^p$. Let $\mathbf{V} = (V_0, V_1, \ldots, V_{2^n-1})$. Let $\mathbf{v} = (v_0, v_1, \ldots, v_{2^n-1})$ be the HT of $\mathbf{V}$. Then the multidimensional 'phase twist' of vector $\mathbf{V}$, σ, is defined as follows,

$$\sigma(\mathbf{V}, j) = (\ldots, V_i(-1)^{i \cdot j}, \ldots)$$

where $\cdot$ is the 'dot' (inner) product of i and j when viewed as vectors. The multidimensional cyclic shift of $\mathbf{v}$, $\varsigma = \mathrm{HT}(\sigma)$, is defined as follows,

$$\varsigma(\mathbf{v}, j) = \mathrm{HT}(\sigma(\mathbf{V}, j)) = (v_{0 \oplus j}, v_{1 \oplus j}, \ldots, v_{(2^n-1) \oplus j})$$

where $i \oplus j \equiv (i_0 \oplus j_0, i_1 \oplus j_1, \ldots, i_{2^n-1} \oplus j_{2^n-1}) \bmod 2$. In other words the length 2^n vectors, $\mathbf{v}$ and $\mathbf{V}$, can be viewed as vectors in n dimensions, and multidimensional phase twist in one domain becomes multidimensional cyclic shift in the HT domain.

3 A Vector (Indicator) Representation of a Linear Block Code and its Dual

Consider a binary linear (n, k, d) block code, $\mathbf{C}$. Consider the length 2^n binary vector (indicator) representation of $\mathbf{C}$, $\mathbf{V} = (V_0, V_1, \ldots, V_{2^n-1})$, $V_i \in \{0, 1\}$. Then $V_i = 1$ iff the length n binary representation of i is a codeword of $\mathbf{C}$. Otherwise $V_i = 0$. If $\mathbf{C}$ is a linear code, then the HT of $\mathbf{V}$, $\mathbf{v}$, is the length 2^n binary vector representation of the dual code of $\mathbf{C}$, $\mathbf{C}^{\perp}$ [2]. $\mathbf{C}^{\perp}$ is an $(n, n-k, d')$ binary linear code. If $\mathbf{C} = \mathbf{C}^{\perp}$ then $\mathbf{C}$ is defined to be Self-Dual. In this paper we do not focus on the distance, d, of the code. We simply require that the code is linear. Moreover, for the construction of Bent sequences we use $\mathbf{C}$ with $k = \frac{n}{2}$.

3.1 Example 1

Consider the $(4, 2, 2)$ code, $\mathbf{C} = \{0000, 0111, 1110, 1001\}$. This can be represented using the indicator vector, (reading left to right),

$$\mathbf{V} = (1000000101000010)$$

where $V_i = 1$ if the binary representation of i is in $\mathbf{C}$. The HT of $\mathbf{V}$ is given by,

$$\mathbf{v} = \mathrm{HT}(\mathbf{V}) = (1000001000010100)$$

Therefore $\mathbf{C}^{\perp} = \{0000, 0110, 1011, 1101\}$.

4 Constructing a Bent Bipolar Vector from the Union of all Cosets of the Code, C

Let $\mathbf{v}$ be the vector representation of a length 2^n binary linear $(n, n-k, d')$ code, $\mathbf{C}^{\perp}$, as explained previously. Let $\mathbf{v_j}$ be the vector representation of the coset of this linear code given by $\mathbf{C}^{\perp}_{\mathbf{j}} = \mathbf{C}^{\perp} \oplus j$. In other words $\mathbf{v_j}$ is the multidimensional cyclic shift of $\mathbf{v}$ by j, given by,

$$\mathbf{v_j} = \varsigma(\mathbf{v}, j)$$

Let $\mathbf{D}$ be a (non-unique) maximum size set of length n binary vectors such that $j' \notin \mathbf{C}^{\perp}_{\mathbf{j}}\ \forall\ j, j' \in \mathbf{D}$, $j \neq j'$. Then $|\mathbf{D}| = 2^k$. Moreover,

$$Z_2^n = \bigcup_{j \in \mathbf{D}} \mathbf{C}^{\perp}_{\mathbf{j}}$$

i.e. the union of all cosets of $\mathbf{C}^{\perp}_{\mathbf{j}}$, (which are disjoint), is the set of all binary vectors of length n. This can be rewritten as,

$$\mathbf{1} = \sum_{j \in \mathbf{D}} \mathbf{v_j}$$

[2] A good test of linearity of a code is to take the HT of its indicator vector. If the non-zero output points do not all have the same magnitude then the code is not linear.

where $\mathbf{1} = (1, 1, \ldots, 1)$ is the All One Vector of length 2^n. If the HT of $\mathbf{V_j}$ is $\mathbf{v_j}$ then,

$$\delta = \sum_{j \in \mathbf{D}} \mathbf{V_j}$$

where $\delta = (1, 0, 0, \ldots, 0)$ is the length 2^n 'delta' function.

So we have formed the All One Vector (AOV) in the Hadamard domain from the union of all cosets of the dual code, $\mathbf{C}^{\perp}$ and, of course, the inverse HT of the AOV is the delta function. In this paper, we aim to have the vector $\mathbf{V}$ and its HT, $\mathbf{v}$, to be both bipolar vectors (i.e. a pair of Bent sequences), i.e. we do not want the delta function. Instead we want an All Magnitude One Vector whose inverse HT is also an All One Magnitude Vector. To achieve this we must simultaneously cyclically shift in both transform domains, and this is the subject of the following argument.

Define the vector $\mathbf{v_{j,m}}$ as follows,

$$\mathbf{v_{j,m}} = \sigma(\mathbf{v_j}, m)$$

In other words, $\mathbf{v_{j,m}}$ is the multidimensional cyclic shift of $\mathbf{v}$ by j (which performs a multidimensional phase twist of $\mathbf{V}$), followed by the multidimensional phase twist of $\mathbf{v_j}$ (which performs a multidimensional cyclic shift of $\mathbf{V_j}$ by m).

Let $\mathbf{D_v}$ be the set of coset leaders for $\mathbf{v}$, and $\mathbf{D_V}$ be the set of coset leaders for $\mathbf{V}$. Define the index pair $(j, m) \in \mathbf{D_v} \otimes \mathbf{D_V}$.

Definition 1 $\mathbf{S}$ *is a (non-unique) maximum size set of index pairs* (j, m), $j \in \mathbf{D_v}$, $m \in \mathbf{D_V}$, *such that, if* $(j, m), (j', m') \in \mathbf{S}$, *then* $j \neq j'$, $m \neq m'$. *Then* $|\mathbf{S}| = 2^k$ *and there are* $(2^k)!$ *distinct choices for* $\mathbf{S}$.

Each of the index pairs in $\mathbf{S}$ specifies a distinct length 2^n Bent bipolar sequence, $\mathbf{V_{j,m}}$. Let the HT of $\mathbf{V_{j,m}}$ be $\mathbf{v_{j,m}}$. We are now in a position to state the main theorem,

Theorem 1 *Let,*

$$\mathbf{w_S} = \sum_{(j,m) \in \mathbf{S}} \mathbf{v_{j,m}} = HT(\mathbf{W_S})$$

where $\mathbf{W_S} = \sum_{(j,m) \in \mathbf{S}} \mathbf{V_{j,m}}$. *Then both* $\mathbf{w_S}$ *and* $\mathbf{W_S}$ *are flat bipolar sequences. Consequently,* $\mathbf{w_S}$ *and* $\mathbf{W_S}$ *are a pair of length* 2^n *Bent bipolar sequences.*

The reasoning for Theorem 1 follows from the fact that the constituent vector, $\mathbf{v}$, undergoes 2^k cyclic shifts in both transform domains. Therefore, as the union of the 2^k cosets of $\mathbf{C}$ covers the complete length 2^n binary vector space, the union of these 2^k cyclic shifts 'fills in' all the zeroes in the vectors in both transform domains with 1's or -1's according to the phase twists.

Corollary 1 *Theorem 1 allows the construction of* $(2^k)!$ *Bent sequence 'pairs' comprising* $(2^k)!$ *distinct length* 2^n *Bent sequences,* $\mathbf{w_S}$.

The binary form of each of these $(2^k)!$ Bent sequences can be shown to be a coset leader for a Reed-Muller $\mathrm{RM}(1,n)$ coset code, such that each member of the bipolar form of the $\mathrm{RM}(1,n)$ coset is Bent. However these cosets are not completely disjoint as we see from the following argument. Let $\mathbf{r}$ be a length 2^n vector from $\mathrm{RM}(1,n)$ which is also in the subspace $\mathrm{RM}(1,\frac{n}{2})$ which covers the same space as that generated by linear combinations of members of $\mathbf{D_v}$. In this subspace $\mathbf{r}$ is referred to as $\mathbf{r'}$. Then $\mathbf{v_{j,m}}$ is in the same $\mathrm{RM}(1,n)$ coset as $\mathbf{v_{j\oplus r,m}}$. Moreover there exists $\mathbf{w_S} = \mathbf{v_{j_0,m_0}} \oplus \mathbf{v_{j_1,m_1}} \oplus \ldots \oplus \mathbf{v_{j_{2^k-1},m_{2^k-1}}}$ and $\mathbf{w_S} \oplus \mathbf{r} = \mathbf{v_{j_0\oplus r',m_0}} \oplus \mathbf{v_{j_1\oplus r',m_1}} \oplus \ldots \oplus \mathbf{v_{j_{2^k-1}\oplus r',m_{2^k-1}}}$ which are distinct and exist in the same coset of $\mathrm{RM}(1,n)$ with coset leader $\mathbf{w_S}$. To ensure the union of $\mathrm{RM}(1,n)$ cosets is disjoint we modify the generation of $\mathbf{w_S}$ of Theorem 1 by replacing $\mathbf{S}$ with $\mathbf{T}$,

Definition 2 $\mathbf{T}$ *is a (non-unique) maximum size set of index pairs* (j,m), $j \in \mathbf{D_v}$, $m \in \mathbf{D_V}$, *such that, if* $(j,m),(j',m') \in \mathbf{T}$, *then* $j \neq j'$, $m \neq m'$. *Moreover, if* $j = h_v$ *then* $m = h_V$ *and vice versa, where* h_v *is a pre-chosen element from* $\mathbf{D_v}$, *and* h_V *is a pre-chosen element from* $\mathbf{D_v}$. *Then* $|\mathbf{T}| = 2^k - 1$ *and there are* $(2^k-1)!$ *distinct choices for* $\mathbf{T}$.

We now replace Theorem 1 with the following,

Theorem 2 *Let,*

$$\mathbf{w_T} = \sum_{(j,m)\in\mathbf{T}} \mathbf{v_{j,m}} = HT(\mathbf{W_T})$$

where $\mathbf{W_T} = \sum_{(j,m)\in\mathbf{T}} \mathbf{V_{j,m}}$. *Then both* $\mathbf{w_T}$ *and* $\mathbf{W_T}$ *are flat bipolar sequences. Consequently,* $\mathbf{w_T}$ *and* $\mathbf{W_T}$ *are a pair of length* 2^n *Bent bipolar sequences. Moreover, the set of* $\mathbf{w_T}$ *belong to distinct cosets of* $RM(1,n)$.

Noting that $\mathrm{RM}(1,n)$ is of size 2^{n+1}, we state the following,

Corollary 2 *The union of all $RM(1,n)$ cosets of sequences whose bipolar form is constructed using Theorem 2 has size $(2^k-1)!2^{n+1}$.*

It appears that we cannot construct all possible Bent sequences of a given length by using Theorem 1, and this goal is the subject of ongoing research.

4.1 Example 1 (continued)

For $\mathbf{C}^\perp$ as defined in Example 1, we choose $\mathbf{D_v} = \mathbf{D_V} = \{0000, 0001, 0010, 0011\}$, therefore $j, m \in \{0,1,2,3\}$. Let us choose, say, to restrict such that, $\forall$ $\mathbf{T}$, $(j=0) \Leftrightarrow (m=0)$. Then we have $3! = 6$ choices for $\mathbf{T}$. For instance, we will generate $\mathbf{w_T}$ for $\mathbf{T} = \{(0,0),(1,2),(2,1),(3,3)\}$. In the following, '+' means 1 and '$-$' means -1. We have,
$\mathbf{v_0} = +00000+0000+0+00$, $\mathbf{v_{0,0}} = +00000+0000+0+00$,
$\mathbf{v_1} = 0+00000+00+0+000$, $\mathbf{v_{1,2}} = 0+00000-00-0+000$,
$\mathbf{v_2} = 00+0+0000+00000+$, $\mathbf{v_{2,1}} = 00+0+0000-00000-$,
$\mathbf{v_3} = 000+0+00+00000+0$, $\mathbf{v_{3,3}} = 000+0-00+00000-0$,
Therefore $\mathbf{w_T} = \mathbf{v_{0,0}} \oplus \mathbf{v_{1,2}} \oplus \mathbf{v_{2,1}} \oplus \mathbf{v_{3,3}} = {+}{+}{+}{+}{+}{-}{+}{-}{+}{-}{-}{+}{+}{+}{-}{-}$. $\mathbf{w_T}$ is Bent and has a HT given by $\mathbf{W_T} = {+}{+}{+}{+}{+}{-}{-}{+}{+}{+}{-}{-}{+}{-}{+}{-}$. The binary form of $\mathbf{w_T}$ has Algebraic Normal Form $w_T(x) = x_0x_2 + x_0x_3 + x_1x_3$. Moreover the RM$(1,4)$ coset having $w_T(x)$ as a coset leader will be Bent.

5 Constructing an Almost Bent Bipolar Vector Using the Same Technique

Consider the (n,k,d) code $\mathbf{C}^\perp$ where n is odd and $k = \frac{n+1}{2}$. Then its indicator vector, $\mathbf{v}$, will have weight 2^k, and the indicator vector for $\mathbf{C}$ will have weight 2^{k-1}. Therefore the set of index pairs, $\mathbf{S}$, now satisfies $|\mathbf{S}| = 2^{k-1}$. We once more apply Theorem 2, but now the disjoint sum of the vectors, $\mathbf{v_{j,m}}$, is only sufficient to make $\mathbf{w_S}$ a bipolar vector. In contrast, the vector, $\mathbf{W_S}$ will be two-valued in magnitude, with half it's elements 0. As $\mathbf{w_s}$ is a bipolar sequence, it therefore fits the description of an Almost Bent sequence [1]. Using similar arguments as above, there are now $\frac{(2^k-1)!}{2^{k-1}!}$ distinct choices for $\mathbf{T}$, each choice identifying a distinct Almost Bent sequence, $\mathbf{w_T}$, from a distinct coset of RM$(1,n)$. These Almost Bent sequences allow us to identify $\frac{(2^k-1)!}{2^{k-1}!}2^{n+1}$ distinct Almost Bent sequences.

5.1 Example 2

Let $\mathbf{C} = \{000, 111\}$. Therefore $\mathbf{V} = (10000001)$. Therefore $\mathbf{v} = \mathrm{HT}(\mathbf{V}) = (10010110)$. Therefore $\mathbf{C}^{\perp} = \{000, 011, 101, 110\}$. We choose $\mathbf{D_v} = \{000, 001\}$ and $\mathbf{D_V} = \{000, 001, 010, 100\}$. Let us choose, say, to restrict such that, $\forall$ $\mathbf{T}$, $(j = 0) \Leftrightarrow (m = 0)$. We therefore have $\frac{3!}{2!} = 3$ choices for $\mathbf{T}$. For instance, we will generate $\mathbf{w_T}$ for $\mathbf{T} = \{(0, 0), (1, 4)\}$. We have,
$\mathbf{v_0} = +00 + 0 + +0$, $\mathbf{v_{0,0}} = +00 + 0 + +0$,
$\mathbf{v_1} = 0 + +0 + 00+$, $\mathbf{v_{1,4}} = 0 + +0 - 00-$,
Therefore $\mathbf{w_T} = \mathbf{v_{0,0}} \oplus \mathbf{v_{1,4}} = + + + + - + +-$. $\mathbf{w_S}$ is Almost Bent and has a HT given by $\mathbf{W_T} = +00 + -00+$. The binary form of $\mathbf{w_T}$ has Algebraic Normal Form $w_T(x) = x_0x_2 + x_1x_2 + x_2$. Moreover the $\mathrm{RM}(1, 3)$ coset having $w_T(x)$ as a coset leader will be Almost Bent.

6 Conclusion

We have presented a technique for constructing Bent and Almost Bent bipolar sequences from Linear Block Codes, by using properties of the Hadamard Transform. Ongoing research will seek to identify those Bent and Almost Bent sequences which <u>cannot</u> be constructed by the technique of this paper (if any).

References

[1] C.Carlet,P.Charpin,V.Zinoviev, "Codes, Bent Functions and Permutations Suitable for DES-like Cryptosystems", *Des., Codes Cryptogr.*, Vol 15, No 2, pp 125-156, Nov. 1998

[2] F.J.MacWilliams,N.J.A.Sloane, **The Theory of Error-Correcting Codes**, Amsterdam: North-Holland, '77

[3] O.Rothaus, "On 'Bent' Functions", *J. Comb. Theory*, Ser A., Vol 20, pp 300-305, 1976