International Symposium on Information Theory and Its Applications
Honolulu, Hawaii, U.S.A., November 5–8, 2000

Optimal Bipolar Sequences for the Complex Reverse-Jacket Transform

Matthew.G.Parker† and Moon Ho Lee‡

†Code Theory Group,
Institute for Informatikk,
University of Bergen,
N-5020 Bergen, Norway
Email: matthew@ii.uib.no

‡Institute of Information and Communication,
Department of Information & Communication Engineering,
Chonbuk National University,
Chonju 561-756, Korea
Email: moonho@moak.chonbuk.ac.kr

Abstract

A class of bipolar sequences is identified which has optimally flat spectrum using the Complex Reverse Jacket Transform (CRJT). This class is found to correspond exactly to the family of Bent bipolar sequences using the Walsh-Hadamard Transform. In total there are 576 such transforms for which this class has optimal spectrum of which the CRJT is one. The spectral properties of odd-power-of-two length bipolar sequences are also discussed.

1. Introduction

The Complex Reverse-Jacket Transform (CRJT) [2] can be used for image compression and multi-dimensional spectral analysis. It is a close relative of the Walsh-Hadamard Transform (HT) and can also be used, cryptographically, for S-box design [4]. Conventionally, Bent Functions, derived from Bent Sequences, have been used for S-box design, having an optimum distance from the affine functions. Bent Sequences have optimally flat spectra using the HT. In the same way one could use Complex-Reverse-Jacket-Bent (CRJT-Bent) sequences for the construction of CRJT Bent Functions which are optimally distant from linear functions of rows of the CRJT matrix [3]. CRJT-Bent sequences have optimally flat spectra using the CRJT. This paper shows that Bent sequences are also CRJT-Bent, and vice versa. It also identifies a total of 576 such transforms for which Bent sequences have optimal spectra.

The CRJT can be expressed as follows,

$$\mathbf{C_{4.2^t}} = [\mathbf{P}^{\gamma}_{\mathbf{4.2^t}}]^{\mathbf{T}}\overline{\mathbf{C}}_{\mathbf{4.2^t}}[\mathbf{P}^{\varsigma}_{\mathbf{4.2^t}}] \qquad (1)$$

where $\mathbf{P}^{\gamma}_{\mathbf{4.2^t}}$ and $\mathbf{P}^{\varsigma}_{\mathbf{4.2^t}}$ are permutation matrices, $\overline{\mathbf{C}}_{\mathbf{4.2^t}}$ is defined as follows,

$$\overline{\mathbf{C}}_{\mathbf{4.2^t}} = \overline{\mathbf{C}}_{\mathbf{4.2^0}} \otimes \left(\otimes_{\mathbf{i=0}}^{\mathbf{t-1}}\mathbf{H}\right) \qquad (2)$$

M.G.Parker is funded by NFR Project Number 119390/431

$\mathbf{H} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ is the 2-point Discrete Fourier Transform (DFT), and,

$$\overline{\mathbf{C}}_{\mathbf{4.2^0}} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \\ 1 & i & -1 & -i \end{pmatrix}$$

The permutation matrices are,

$$\mathbf{P}^{\gamma}_{\mathbf{4.2^t}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \otimes \mathbf{I_t},$$

$$\mathbf{P}^{\varsigma}_{\mathbf{4.2^t}} = \mathbf{I}_{\mathbf{t+1}} \oplus \left(\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \otimes \mathbf{I_t}\right) = \mathbf{P}^{\varsigma}_{\mathbf{4.2^0}} \otimes \mathbf{I_t}$$

and $\mathbf{I_t}$ is the $2^t \times 2^t$ identity matrix. For notational convenience we abbreviate (1) to,

$$\mathbf{C_t} = [\mathbf{P}^{\gamma}_{\mathbf{t}}]^{\mathbf{T}}\overline{\mathbf{C}}_{\mathbf{t}}[\mathbf{P}^{\varsigma}_{\mathbf{t}}] \qquad (3)$$

and (2) to,

$$\overline{\mathbf{C}}_{\mathbf{t}} = \overline{\mathbf{C}}_{\mathbf{0}} \otimes \mathbf{H_t} \qquad (4)$$

where $\mathbf{H_t}$ is the $2^t \times 2^t$ Walsh-Hadamard transform. For instance, $\overline{\mathbf{C}}_{\mathbf{0}}$ means $\overline{\mathbf{C}}_{\mathbf{4.2^0}}$.

We show that, for t even, length 2^t bipolar sequences having a flattest CRJT spectrum coincide with bipolar sequences having a flattest HT spectrum, and also coincide with bipolar sequences having a flattest spectrum under the transform defined by the Kronecker product of a 4-point Discrete Fourier Transform (DFT) with repeated copies of the 2-point DFT. Computational results for lengths where t is odd are also presented.

2. The Complex Reverse Jacket Peak Factor

The CRJT obeys Parseval's Theorem, i.e. the transform conserves energy. It is therefore of interest to know which subset of vectors have a CRJT spectrum which spreads out the energy most evenly, i.e. which vectors have a flat or flattish CRJT spectrum. One measure of the flatness is the Peak Factor of a sequence, i.e. the Peak-to-Mean Power Ratio of the sequence, and this is defined below.

Let $\mathbf{D}$ be the length 4.2^t CRJT of the length 4.2^t vector $\mathbf{a}$, specified by,

$$\mathbf{D} = \mathbf{C_t a}$$

Definition 1 *The CRJT Peak Factor (CRJTPF) of* $\mathbf{a}$ *is defined as follows,*

$$CRJTPF(\mathbf{a}) = 2^{-(t+2)} max\{D_i D_i^* | 0 \le i < 2^{t+2}\}$$

where the D_i *are the* 2^{t+2} *elements of the vector* $\mathbf{D}$*. It is easy to show that* $1.0 \le CRJTPF(\mathbf{a}) \le 2^{t+2}$ *if* $\mathbf{a}$ *is unimodular (unimodular means each element of* $\mathbf{a}$ *has a magnitude of 1).*

Definition 2 *A unimodular sequence is described as 'Bent' if it has a Peak Factor of* 1.0 *under the Hadamard Transform (HT), i.e. it has a 'Hadamard Peak Factor' (HPF) of* 1.0*.*

Definition 3 *A unimodular sequence is CRJT-Bent if it has a CRJTPF of* 1.0*.*

2.1. The CRJT Peak Factor of Bipolar Sequences

The output permutation, $\mathbf{P}^\gamma$, does not alter the CRJT spectral values, but just re-orders them. So it is sufficient to study the CRJTPF using the transform,

$$\overline{\mathbf{C}}_\mathbf{t} \mathbf{P}_\mathbf{t}^\varsigma \tag{5}$$

The input permutations, as specified by $\mathbf{P}_\mathbf{t}^\varsigma$, are given below for lengths $N = 4, 8, 16$, respectively,

$(0)(1)(2,3)$
$(0)(1)(2)(3)(4,6)(5,7)$
$(0)(1)(2)(3)(4)(5)(6)(7)(8,12)(9,13)(10,14)(11,15)$

The CRJTPF of a sequence can be computed by first permuting the sequence using $\mathbf{P}_\mathbf{t}^\varsigma$, then multiplying the resultant vector by $\overline{\mathbf{C}}_\mathbf{t}$, then point-multiplying the resultant vector by it's complex conjugate and finding the maximum value of the resultant vector. Bipolar sequences form equivalence classes under the CRJTPF measure, as shown in Appendix A for lengths 4 and 8. For lengths 4,8,16 it is found that the optimum equivalence class has CRJTPFs $1.0, 2.0, 1.0$, respectively.

2.2. Example

Consider the bipolar vector $\mathbf{a} = (1, 1, -1, 1)$. The CRJTPF of this vector is computed as follows.

- Permute $\mathbf{a}$ using $\mathbf{P}_\mathbf{t}^\varsigma$ to give $(1, 1, 1, -1)$.
- Premultiply the permuted vector by $\overline{\mathbf{C}}_\mathbf{4}$ to give $2(1, 1, -i, i)$.
- Point-multiply this resultant vector by it's complex conjugate and divide by 4 to get $(1, 1, 1, 1)$. The maximum value in this vector is 1 so $\text{CRJTPF}(\mathbf{a}) = 1.0$. Therefore $\mathbf{a}$ is CRJT-Bent.
- To compute the CRJTPF it wasn't necessary to perform the final permutation $[\mathbf{P}_\mathbf{t}^\gamma]^\mathbf{T}$.

Lemma 1 *For* t *odd, the CRJTPF of a length* 2^{t+2} *bipolar sequence is always* > 1.0*.*

Proof of Lemma 1: For t odd, the vector $\mathbf{D}$, which is the CRJT of a bipolar vector, will have an output magnitude of $\sqrt{2^{t+2}}$ only if all the elements of $\mathbf{D}$ are complex. But this is impossible because the CRJT matrix has a subset of rows comprising only ± 1, so $\mathbf{D}$ has real elements. ∎

As a result of Lemma 1 we only need to consider CRJT-Bent bipolar sequences for t even.

3. Two Theorems Regarding CRJT-Bent Bipolar Sequences

We state two Theorems for t even.

Theorem 1 *CRJT-Bent bipolar sequences are invariant (i.e. remain CRJT-Bent) under the permutation* P_t^ς *for all length* 2^{t+2} *bipolar sequences where* t *is even.*

Theorem 2 *CRJT-Bent bipolar sequences are also Bent, and vice versa. These sequences only occur for lengths* 2^{t+2} *when* t *is even.*

The proofs for Theorems 1 and 2 occur as a result of the proofs of Theorem 3 and Corollary 1 in Section 5.

As an example of Theorem 2, the CRJTPF of bipolar sequences of length 2^{t+2} constructed from 'line graphs' which are Reed-Muller 1 cosets with a Reed-Muller 2 coset leader with Algebraic Normal Form $x_0x_1 + x_1x_2 + x_2x_3 + \ldots + x_tx_{t+1}$, or any permutation of the $t+2$ variables, were tested for various t [5] (These are Golay-Davis-Jedwab (GDJ) sequences). It is known that such sequence cosets have optimum Hadamard Peak Factor (HPF) in each case (Bent when

$t+2$ is even). It is found, computationally, that these sequences always have optimal CRJTPF, where CRJTPF = HPF. In other words the CRJTPF for this coset is 1.0 for t even, and 2.0 for t odd. The case where t is even agrees with Theorem 2, and the case where t is odd suggests a similar Theorem when the CRJTPF = 2.0, at least for GDJ sequences, but this is not proved in this paper.

4. A More General Theorem

Our method of proving Theorems 1 and 2 is to prove a more general theorem, Theorem 3, and Corollary 1. The 4-point Discrete Fourier Transform (DFT) is,

$$\mathbf{W_2} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix}$$

Let $\mathbf{W_t} = \mathbf{W_2} \otimes \mathbf{H_t}$. Let $\mathbf{G_2}$ be any row/column permutation of $\mathbf{W_2}$, and let $\mathbf{G_t} = \mathbf{G_2} \otimes \mathbf{H_t}$. There are 576 $\mathbf{G_2}$ matrices, being (number of row permutations $\times$ number of column permutations) = $24 \times 24 = 576$. Each row/column permutation produces a different $\mathbf{G_2}$ matrix.

Theorem 3 *Bent bipolar sequences are exactly the class of sequences with optimally flat spectrum using $\mathbf{G_t}$, and vice versa. Such sequences are "$\mathbf{G_t}$-Bent".*

A corollary of Theorem 3 is as follows,

Corollary 1 *$\mathbf{G_t}$-Bent bipolar sequences are $\mathbf{G'_t}$-Bent, and vice versa, where $\mathbf{G'_t}$ is a row/column permutation of $\mathbf{G_t}$.*

Corollary 2 *Length $N = 2^s$ Bent and/or $\mathbf{G_t}$-Bent bipolar sequences, s even, form equivalence classes under any combination of permutations of the elements $i, i+\frac{N}{4}, i+2\frac{N}{4}, i+3\frac{N}{4}$, $0 \le i < \frac{N}{4}$.*

5. Proofs of Theorems 1-3

Theorems 1 and 2 follow immediately from the proofs of Theorem 3 and Corollary 1 as follows.

5.1. Proof of Theorem 3

Let $\mathbf{B} = [\mathbf{H_2} \otimes \mathbf{H_t}]\mathbf{a}$, and $\mathbf{E} = [\mathbf{G_2} \otimes \mathbf{H_t}]\mathbf{a}$ for some bipolar vector, $\mathbf{a}$. Then $[\mathbf{H_2} \otimes \mathbf{I_t}]\mathbf{B} = [\mathbf{I_2} \otimes \mathbf{H_t}]\mathbf{a}$, and $[\mathbf{G_2} \otimes \mathbf{I_t}][\mathbf{H_2} \otimes \mathbf{I_t}]\mathbf{B} = [\mathbf{G_2} \otimes \mathbf{H_t}]\mathbf{a}$. Finally,

$$\mathbf{E} = [\mathbf{G_2 H_2} \otimes \mathbf{I_t}]\mathbf{B} = [\mathbf{G_2} \otimes \mathbf{H_t}]\mathbf{a} = \mathbf{G_t a} \qquad (6)$$

Therefore if $\mathbf{B}$ is the HT of $\mathbf{a}$, then $\mathbf{E}$ is computed by the action of $\mathbf{G_2 H_2}$ on length-4 independent subsequences of $\mathbf{B}$. Let $\mathbf{G_2} = \mathbf{W_2}$. Then,

$$\mathbf{G_2 H_2} = \mathbf{W_2 H_2} = \begin{pmatrix} 4 & 0 & 0 & 0 \\ 0 & 0 & 2+2i & 2-2i \\ 0 & 4 & 0 & 0 \\ 0 & 0 & 2-2i & 2+2i \end{pmatrix} \qquad (7)$$

For t even and $\mathbf{a}$ Bent the elements of $\mathbf{B}$ are ± 1 (after normalisation). Therefore the action of $\mathbf{W_2 H_2}$ on length-4 subsequences of $\mathbf{B}$ produces elements of $\mathbf{E}$ which all have magnitude 1 (after normalisation by $\frac{1}{4}$). The 24 matrices, $\mathbf{G_2}$, which are column permutations of $\mathbf{W_2}$, produce 24 matrices, $\mathbf{G_2 H_2}$, which are column permutations of (7) to within a sign-change, and therefore all give $\mathbf{E}$ with a flat spectrum for $\mathbf{B}$ Bent. The 24 row permutations of $\mathbf{W_2}$ only affect the position of the elements in $\mathbf{E}$, not their value. This proves that Bent bipolar sequences are also optimally flat ('$\mathbf{G_t}$-Bent') using any one of the 576 $\mathbf{G_t}$ transforms. Let us now prove that bipolar sequences which are $\mathbf{G_t}$-Bent are also Bent. Initially let $\mathbf{G_2} = \mathbf{W_2}$. Assume $\mathbf{a}$ is not Bent. Can $\mathbf{a}$ be $\mathbf{W_t}$-Bent? Let us try and make $\mathbf{E}$ a flat spectrum. From (7), for each length-4 subsequence of $\mathbf{B}$, acted on by $\mathbf{W_2 H_2}$, $\mathbf{E}$ can only be flat if elements at positions 1 and 2 are ± 1. Call elements at positions 3 and 4, p and q (real). Then $|(2 \pm 2i)p + (2 \mp 2i)q| \neq 4$ unless $|p| = |q| = 1$, in which case $\mathbf{a}$ is Bent. Therefore if $\mathbf{a}$ is not Bent, then it cannot be $\mathbf{W_t}$-Bent. Row-column permutations of $\mathbf{W_2}$ do not change this argument. Hence Theorem 3 is proved. ∎

5.2. Proof of Corollary 1

From Theorem 3: If $\mathbf{a}$ is $\mathbf{G_t}$-Bent, then $\mathbf{a}$ is Bent. If $\mathbf{a}$ is Bent then $\mathbf{a}$ is $\mathbf{G'_t}$-Bent. ∎

5.3. Proofs of Theorems 1 and 2

Theorems 1 and 2 follow by observing that $\mathbf{C_t}$ and $\overline{\mathbf{C_t}}$ are row/column permutations of $\mathbf{W_t}$. ∎

6. What About When t is Odd?

Computational results for low t suggest that, for t odd, the optimum equivalence class is exactly the same for both CRJT and HT. This is computationally proved for $t = 1$ (length 8), and stated in Lemma 2 below. It is already known that bipolar sequences with HPF < 2.0 exist for t odd, $t \ge 15$. The optimum HPF is 2.0 for $t = 3, 5, 7$, and it is not known for $t = 9, 11, 13$. The study of optimum HPF for t odd is equivalent to finding the minimum 'Covering Radius' of the First-Order Reed-Muller Code [1].

However a subsequent alternative proof of Lemma 2 suggests that the optimum equivalence class may not be identical for both CRJT and HT when odd t becomes large. Further work will seek to clarify this situation.

Lemma 2 *Let* $t = 1$ *and* $\mathbf{a}$ *be a bipolar vector. The set of length 8 bipolar sequences with CRJTPF* $= 2.0$ *are exactly the set of bipolar sequences with HPF* $= 2.0$.

Proof of Lemma 2: This has already been proved computationally. This proof is given to show why the property probably cannot be extended to all odd t. When $t = 1$ the sequences with CRJTPF $= 2.0$ have a $\mathbf{D}$ vector whose elements, $a + bi$ (before normalisation), must be taken from the set $\{\pm 4, \pm 4i, \pm 2 \pm 2i, \pm 2, \pm 2i, 0\}$. This value set is restricted enough to ensure that the HPF is also 2.0. ■

However, when $t = 3$ for length 32 sequences, a CRJTPF $= 2.0$ will probably not guarantee HPF $= 2.0$ as there could be pathological elements such as $6 + 4i$ which satisfy $\frac{6^2+4^2}{32} \leq 2.0$, but do not satisfy $\frac{(6+4)^2}{32} \leq 2.0$. We have not yet checked the length 32 case computationally. In general we do not expect the equivalence of Lemma 2 to hold for $t > 2$.

7. Conclusion

This paper shows that the class of Bent bipolar sequences of length 2^t, t even, also have optimally-flat spectra using the Complex Reverse-Jacket Transform (i.e. they are CRJT-Bent), and vice versa. More generally, there are 576 transform matrices which are row-column permutations of the CRJT, and for each transform, Bent bipolar sequences coincide with the class of sequences with optimally flat magnitude spectra using the transform. Computational results suggest the optimal class coincides for t odd aswell, but the situation is less clear here. CRJT-Bent sequences define functions for S-boxes which are resistant to correlation attack using sequences constructed from linear combinations of rows of the CRJT.

8. Appendix A

All bipolar sequences are represented in binary form, 0 for 1, and 1 for -1.

```
Length 4 Bipolar Sequences
CRJTPF is 4.000000:
0000,0110,1001,1111,
CRJTPF is 2.000000:
0011,0101,1010,1100,
CRJTPF is 1.000000:
0001,0010,0100,0111,1000,1011,1101,1110,
There are 3 equivalence classes, 16 messages displayed
------------------------------------------

Length 8 Bipolar Sequences
CRJTPF is 8.000000:
00000000,00111100,01010101,01101001,10010110,10101010,11000011,11111111,
CRJTPF is 4.500000:
00000001,00000010,00000100,00001000,00010000,00010101,00010110,00011100,
00100000,00101001,00101010,00101100,00110100,00111000,00111101,00111110,
01000000,01000011,01000101,01001001,01010001,01010100,01010111,01011101,
01100001,01101000,01101011,01101101,01110101,01111001,01111100,01111111,
10000000,10000011,10000110,10001010,10010010,10010100,10010111,10011110,
10100010,10101000,10101011,10101110,10110110,10111010,10111100,10111111,
11000001,11000010,11000111,11001011,11010011,11010101,11010110,11011111,
11100011,11101001,11101010,11101111,11110111,11111011,11111101,11111110,
CRJTPF is 4.000000:
00001111,00110011,01011010,01100110,10011001,10100101,11001100,11110000,
CRJTPF is 2.500000:
00000111,00001011,00001101,00001110,00010011,00011001,00011010,00011111,
00100011,00100101,00100110,00101111,00110001,00110010,00110111,00111011,
01000110,01001010,01001100,01001111,01010010,01011000,01011011,01011110,
01100010,01100100,01100111,01101110,01110000,01110011,01110110,01111010,
10000101,10001001,10001100,10001111,10010001,10011000,10011011,10011101,
10100001,10100100,10100111,10101101,10110000,10110011,10110101,10111001,
11000100,11001000,11001101,11001110,11010000,11011001,11011010,11011100,
11100000,11100101,11100110,11101100,11110001,11110010,11110100,11111000,
CRJTPF is 2.000000: (112 sequences)
00000011,00000101,00000110,00001001,00001010,00001100,00010001,00010010,
00010100,00010111,00011000,00011011,00011101,00011110,00100001,00100010,
00100100,00100111,00101000,00101011,00101101,00101110,00110000,00110101,
00110110,00111001,00111010,00111111,01000001,01000010,01000100,01000111,
01001000,01001011,01001101,01001110,01010000,01010011,01010110,01011001,
01011100,01011111,01100000,01100011,01100101,01101010,01101100,01101111,
01110001,01110010,01110100,01110111,01111000,01111011,01111101,01111110,
10000001,10000010,10000100,10000111,10001000,10001011,10001101,10001110,
10010000,10010011,10010101,10011010,10011100,10011111,10100000,10100011,
10100110,10101001,10101100,10101111,10110001,10110010,10110100,10110111,
10111000,10111011,10111101,10111110,11000000,11000101,11000110,11001001,
11001010,11001111,11010001,11010010,11010100,11010111,11011000,11011011,
11011101,11011110,11100001,11100010,11100100,11100111,11101000,11101011,
11101101,11101110,11110011,11110101,11110110,11111001,11111010,11111100,
There are 5 equivalence classes, 256 messages displayed
---------------------------------------
```

References

[1] T.Helleseth,T.Kløve,J.Mykkeltveit, "On the Covering Radius of Binary Codes", *IEEE Trans. Inform. Theory*, Vol IT-24, No 5, pp. 627-628, 1978

[2] M.H.Lee, "The Complex Reverse Jacket Transform," *22nd Int. Symp. on Inf. Theory and its Applications (SITA 99), Yuzawa, Niigata, Japan*, Nov 30-Dec 1st, '99

[3] M.H.Lee,J.Park,S.Hong, "A Simple Binary Generation for Reverse Jacket Sequence," *Accepted for Int. Symp. on Inf. Theory and its Applications (SITA 2000), Sheraton Waikiki Hotel, Honolulu, Hawaii, USA*, Nov 5-8, 2000

[4] S.Mister,C.Adams, "Practical S-Box Design," *Workshop Record of the Workshop on Selected Areas in Cryptography (SAC '96)*, Aug. 15-16, '96, pp. 61-76

[5] M.G.Parker, "The Constabent Properties of Golay-Davis-Jedwab Sequences," *IEEE Int. Symp. Information Theory, Sorrento, 2000*