ISIT 2002, Lausanne, Switzerland, June 30 – July 5, 2002

# A Construction for Binary Sequence Sets with Low Peak-to-Average Power Ratio

Matthew G. Parker[1]
Dept. of Informatics, University of Bergen
5020 Bergen, Norway
matthew@ii.uib.no,
http://www.ii.uib.no/∼matthew/

Chintha Tellambura
Comp. Sci. and Software Eng.,
Monash University, Clayton, Victoria
3168, Australia
chintha@mail.csse.monash.edu.au

*Abstract* — **Complementary Sequences (CS) have Peak-to-Average Power Ratio (PAR) $\leq 2$ under the one-dimensional continuous Discrete Fourier Transform ($\mathrm{DFT}_1^\infty$). Davis/Jedwab [1] constructed binary CS (DJ Set) for lengths $2^n$ described by $\mathbf{s} = 2^{\frac{-n}{2}}(-1)^{p(\mathbf{x})}$, $p(\mathbf{x}) = \sum_{j=0}^{L-2} x_{\pi(j)}x_{\pi(j+1)} + c_j x_j + k$, $\quad c_j, k \in Z_2$. Hamming Distance, $D$, between sequences in this set satisfies $D \geq 2^{n-2}$. However the rate of the DJ set vanishes for $n \to \infty$, and higher rates are possible for PAR $\leq O(n)$ and $D$ large. We present such a construction which generalises the DJ set. These codesets have PAR $\leq 2^t$ under all Linear Unimodular Unitary Transforms (LUUTs), including all one and multi-dimensional continuous DFTs, and $D \geq 2^{n-d}$ where $d$ is the maximum algebraic degree of the chosen subset of the complete set.**

Let $\mathbf{l} = (l_0, l_1, \ldots, l_{r^n-1})$ be a length $r^n$ complex sequence. $\mathbf{l}$ is unimodular if $|l_i| = |l_j|$, $\forall i,j$, unitary if $\sum_{i=0}^{r^n-1} |l_i|^2 = 1$, and $r$-linear if $\mathbf{l} = r^{\frac{-n}{2}} \bigotimes_{i=0}^{n-1}(a_{i,0}, a_{i,1}, \ldots, a_{i,r-1})$ where $\otimes$, the 'left tensor product', satisfies $\mathbf{A} \otimes (B_0, B_1, \ldots) = (B_0\mathbf{A}, B_1\mathbf{A}, \ldots)$. For $r$ prime, $r$-linear is called linear. $\mathbf{L_{r,n}}$ is the infinite set of length $r^n$ complex $r$-linear, unitary, unimodular sequences. A $r^n \times r^n$ $r$-Linear Unimodular Unitary Transform ($r$-LUUT) matrix $\mathbf{L}$ has rows $\in \mathbf{L_{r,n}}$ such that $\mathbf{L}\mathbf{L}^\dagger = \mathbf{I_{r^n}}$, where $\dagger$ means conjugate transpose, and $\mathbf{I_{r^n}}$ is the $r^n \times r^n$ identity. When $r$ is prime, $r$-LUUT is called LUUT. $q$-LUUTs are a subset of $r$-LUUTs iff $q|r$. Example LUUTs are the $2^n \times 2^n$ Walsh-Hadamard (WHT) and Negahadamard (NHT) Transform matrices, $\bigotimes_{i=0}^{n-1}\mathbf{H}$, and $\bigotimes_{i=0}^{n-1}\mathbf{N}$, respectively, where $\mathbf{H} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, $\mathbf{N} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix}$, and $i^2 = -1$. $\mathrm{DFT}_1^\infty$ is an infinite subset of $2^n \times 2^n$ LUUTs, the union of whose rows form a subset of $\mathbf{L_{2,n}}$ where each row satisfies $a_{i,0} = \frac{1}{\sqrt{2}}$, $a_{i,1} = \frac{\omega^{ik}}{\sqrt{2}}$ for any $k$, and $\omega$ a complex root of unity. We define PAR as, $r$-PAR$(\mathbf{s}) = r^n \max_{\mathbf{l}}(|\mathbf{s}\cdot\mathbf{l}|^2) = r^n \max_{\mathbf{l}}(|\sum_{i=0}^{r^n-1} s_i l_i^*|^2)$ where $\mathbf{l} \in \mathbf{L_{r,n}}$, $\cdot$ means 'inner product', and $^*$ means complex conjugate. When $r$ is prime, $r$-PAR is termed PAR. For $\mathbf{l}$ any row of a **fixed** unitary transform, $\mathbf{U}$, PA$(\mathbf{s}) = r^n \max_{\mathbf{l}}(|\mathbf{s}\cdot\mathbf{l}|^2)$. The rows of an $R \times R'$ matrix, $\mathbf{A}$, form a **complementary set** of $R$ sequences under the $R' \times R'$ unitary transform matrix, $\mathcal{T}$, if $\mathbf{A}\tau_\mathbf{i}^\mathbf{T}$ is unitary, where $\tau_\mathbf{i}$ is the $i$th row of $\mathcal{T}$, and the rows of $\mathbf{A}$ are unitary. Consequently, each row, $\mathbf{a_i}$, of $\mathbf{A}$ satisfies PA$(\mathbf{a_i}) \leq R$ wrt $\mathcal{T}$.

**Construction 1:** Let $N = r^n$, $R = r^t$. Let $\mathbf{E_j}$ and $\mathbf{A_j}$, $0 \leq j < L$, be $R \times R$ and $R \times R^{j+1}$ complex matrices, resp., $\mathbf{E_j}$ a unitary, unimodular matrix with rows $\mathbf{e_{i,j}}$, $\mathbf{A_j}$ with unitary, unimodular rows, $\mathbf{a_{i,j}}$, and $\mathbf{A_0} = \mathbf{E_0}$. Let $\gamma_j$ and $\theta_j$ permute $Z_R$, and $\mathbf{E}'_\mathbf{j}$, with rows $\mathbf{e}'_\mathbf{i,j}$, be the row/column permutation of $\mathbf{E_j}$, specified by $\gamma_j$ and $\theta_j$, resp.. Then $\mathbf{A_j}$ is formed as,

$$\mathbf{a_{i,j}} = (\mathbf{a_{0,j-1}}|\mathbf{a_{1,j-1}}|\ldots|\mathbf{a_{R-1,j-1}}) \odot (\mathbf{1} \otimes \mathbf{e}'_\mathbf{i,j})$$

where $\mathbf{x} \odot \mathbf{y} = (x_0y_0, x_1y_1, \ldots, x_{R^j-1}y_{R^j-1})$, $\mathbf{1}$ is the length $R^j$ all-ones vector, and $'|'$ means concatenation.

**Theorem 1** *Let $\mathbf{s}$ be a length $N = R^L$ row of $\mathbf{A_{L-1}}$. Then $\pi_r(\mathbf{s})$ satisfies $r$-PAR$(\pi_r(\mathbf{s})) \leq R$ under all $N \times N$ $r$-LUUTs, where $\pi_r$ is any $r$-symmetric permutation of $\mathbf{s}$.*

**Construction 2:** (special case of Construction 1). Let $r = 2$ and all $\mathbf{E_j}$ be $2^t \times 2^t$ WHTs. Let $\mathbf{x} = \{x_0, x_1, \ldots, x_{n-1}\}$ be $n$ binary variables. Then $\mathbf{s} = 2^{\frac{-n}{2}}(-1)^{\mathbf{p}(\mathbf{x})}$, where,

$$p(\mathbf{x}) = \sum_{j=0}^{L-2} \theta_j(\mathbf{x_j})\gamma_j(\mathbf{x_{j+1}}) + \sum_{j=0}^{L-1} g_j(\mathbf{x_j})$$

where $\theta_j$ and $\gamma_j$ are any permutations: $Z_2^t \to Z_2^t$, $\mathbf{x_j} = \{x_{\pi(tj)}, x_{\pi(tj+1)}, \ldots, x_{\pi(t(j+1)-1)}\}$, $n = Lt$, $\pi$ permutes $Z_n$, and $g_j$ is any $t$-variable function.

**Corollary 1** *The length $N = 2^n$ sequences, $\mathbf{s}$, of Construction 2, satisfy PAR$(\mathbf{s}) \leq 2^t$ under all $N \times N$ LUUTs.*

**Example:** For $t = 3$, $\pi$ the identity, $L = 2$, let $\gamma_0$ and $\theta_0$ be quadratic permutations of $Z_2^3$. Then $\mathbf{s}$ is a length 64 quartic sequence. For instance,

$$p(\mathbf{x}) = \begin{array}{l} 0235, 0245, 023, 025, 1235, 1245, 0234, 0235, 0245, 1234, 1235, 1245, \\ 123, 125, 035, 045, 134, 145, 134, 135, 145, 234, 235, 245, 03, 05, 14, 15 \end{array}$$

where, e.g., 0235, 0245 means $x_0x_2x_3x_5 + x_0x_2x_4x_5$. In this case $\mathbf{s}$ has PAs 6.25, 3.25, and 3.74 under WHT, NHT, and $\mathrm{DFT}_1^\infty$, resp. For all LUUTs, PAR $\leq 8$.

**Theorem 2** *For fixed $t$, let $\mathbf{P}$ be the subset of $p(\mathbf{x})$ of degree 2 or less, generated using Construction 2. Then $D \geq 2^{n-2}$ and,*

$$\frac{|\mathbf{P}|}{2^{n+1}} \leq B = \frac{(\frac{\Gamma}{t!})^{\frac{n}{t}-1} n! (2^{2^t-t-1})^{\frac{n}{t}}}{2t!} \qquad (1)$$

*where $\Gamma = \prod_{i=0}^{t-1}(2^t - 2^i) = |GL(t,2)|$. (GL is the General Linear Group). (For $t = 1$ or $L \leq 2$ the bound is exact).*

The table enumerates quadratic coset leaders for $t = 2$ (PAR $\leq 4.0$) using Constr. 2, comparing with (1) and the DJ set.

| $n$ | 4 | 6 | 8 | 10 |
|---|---|---|---|---|
| $B$ | 72 | 12960 | 4354560 | 2351462400 |
| $\lvert\mathbf{P}\rvert/2^{n+1}$ | 36 | 9240 | 4086096 | 2317593600 |
| $\lvert\mathrm{DJ}\rvert/2^{n+1}$ | 12 | 360 | 20160 | 1814400 |

The full paper describes how to generate the quadratic subset of Construction 2 using 'Bruhat' decomposition, also investigates higher degree subsets, and generalises Constructions 1 and 2 to $\gamma_j$, $\theta_j$, many-to-one and one-to-many mappings.

## References

[1] Davis, J.A.,Jedwab, J.: Peak-to-mean Power Control in OFDM, Golay Complementary Sequences and Reed-Muller Codes. IEEE Trans. Inform. Theory **45.** No 7,2397–2417,Nov (1999)

[1]Funded by NFR Project Number 119390/431