Shapiro Sequences, Reed-Muller Codes, and Functional Equations

Harold S. Shapiro and Jim Byrnes
Prometheus Inc.

$\mathbb{Z}_2^{2^m}$ = set of binary 2^m-tuples, $m \geq 1$.

For each n, $1 \leq n \leq 2^m - 1$, and each j, $1 \leq j \leq m$,
$\delta_{j,n}$ = coefficient of 2^{j-1} in binary expansion of n.
Also $\delta_{0,n} = 1, 0 \leq n \leq 2^m - 1$.

$$n = \sum_{j=1}^{m} 2^{j-1}\delta_{j,n}, \quad \vec{g}_j = \vec{g}_j(m) = \langle\, \delta_{j,0}\, \delta_{j,1}\, \delta_{j,2} \ldots\, \delta_{j,2^m-1} \,\rangle,$$

$$\vec{g}_0 = \vec{g}_0(m) = \langle\, 1\,1\,1 \ldots\, 1 \,\rangle.$$

$$\mathbf{G}_m = \{\vec{g}_0, \vec{g}_1, \ldots, \vec{g}_m\}$$

Example: $m = 3$

n	0	1	2	3	4	5	6	7
$\vec{g}_0$	1	1	1	1	1	1	1	1
$\vec{g}_1$	0	1	0	1	0	1	0	1
$\vec{g}_2$	0	0	1	1	0	0	1	1
$\vec{g}_3$	0	0	0	0	1	1	1	1

$$\mathbf{G}_3 = \{ \quad \langle\, 1\,1\,1\,1\,1\,1\,1\,1 \,\rangle, \quad \langle\, 0\,1\,0\,1\,0\,1\,0\,1 \,\rangle, \quad \langle\, 0\,0\,1\,1\,0\,0\,1\,1 \,\rangle, \quad \langle\, 0\,0\,0\,0\,1\,1\,1\,1 \,\rangle \quad \}$$

The $\vec{g}_m$ are discretized versions of the Rademacher functions.

Claim. The elements of $\mathbf{G}_m$ are linearly independent.

Proof. For any set $\vec{a} = \langle\, a_0\, a_1\, \ldots\, a_m \,\rangle$ of real (or complex) numbers let

$$\vec{V} = \vec{V}(\vec{a}) = \sum_{j=0}^{m} a_j \vec{g}_j = \langle\, v_0\, v_1\, v_2\, \ldots\, v_{2^m-1} \,\rangle.$$

Since $\delta_{0,0} = 1$ and $\delta_{j,0} = 0$ for $1 \le j \le m$, $v_0 = a_0$.
Considering those n, $1 \le n \le 2^m - 1$, which have exactly one 1 in their binary expansion,

$$v_{2^k} = a_0 + a_{k+1} \quad 0 \le k \le m-1.$$

So, if $\vec{V} = \vec{0}$, first $a_0 = 0$ and then $a_j = 0$, $1 \le j \le m$. ■

The *Reed-Muller code* of rank m and order 0 is

$$RM(0,m) = \{\langle 0\,0\,\ldots\,0\rangle, \langle 1\,1\,\ldots\,1\rangle\},$$

where each vector (*codeword*) has 2^m entries. $RM(1,m)$ is the subgroup of $\mathbb{Z}_2^{2^m}$ generated by the codewords in $\mathbf{G}_m$, *i.e.*, the vector space over $\mathbb{Z}_2$ spanned by these codewords. $RM(1,m)$ contains 2^{m+1} codewords.

Define *multiplication* $\cdot$ on $\mathbb{Z}_2^{2^m}$ by

$$\langle x_0\,x_1\,\ldots\,x_{2^m-1}\rangle \cdot \langle y_0\,y_1\,\ldots\,y_{2^m-1}\rangle = \langle x_0y_0\,x_1y_1\,\ldots\,x_{2^m-1}y_{2^m-1}\rangle.$$

Augment $\mathbf{G}_m$ with all products $\vec{g}_i \cdot \vec{g}_j$, $1 \le i < j \le m$, to form $\mathbf{G}_m^{(2)}$.

Example: $m = 3$

n	0	1	2	3	4	5	6	7
$\vec{g}_0$	1	1	1	1	1	1	1	1
$\vec{g}_1$	0	1	0	1	0	1	0	1
$\vec{g}_2$	0	0	1	1	0	0	1	1
$\vec{g}_3$	0	0	0	0	1	1	1	1
$\vec{g}_1 \cdot \vec{g}_2$	0	0	0	1	0	0	0	1
$\vec{g}_1 \cdot \vec{g}_3$	0	0	0	0	0	1	0	1
$\vec{g}_2 \cdot \vec{g}_3$	0	0	0	0	0	0	1	1

$$\mathbf{G}_3^{(2)} = \mathbf{G}_3 \cup \{\langle\, 0\,0\,0\,1\,0\,0\,0\,1\,\rangle, \langle\, 0\,0\,0\,0\,0\,1\,0\,1\,\rangle, \langle\, 0\,0\,0\,0\,0\,0\,1\,1\,\rangle\}.$$

Claim. The $1+m+\binom{m}{2}$ elements of $\mathbf{G}_m^{(2)}$ are linearly independent.

Proof. For any set $\vec{b} = \langle b_0\, b_1\, \ldots b_m\, b_{m+1} \ldots b_{m+\binom{m}{2}} \rangle$ of real (or complex) numbers suppose

$$\sum_{j=0}^{m} b_j \vec{g}_j + \sum_{j=1}^{m-1} \sum_{i=j+1}^{m} b_{jm-\frac{j(j+1)}{2}+i} \vec{g}_i \cdot \vec{g}_j = \vec{0}.$$

By first considering (as above) those n which have exactly one 1 in their binary expansion, $b_0 = b_1 = \ldots = b_m = 0$. Analogously, by then considering those n which have exactly two 1's in their binary expansion,

$$b_{m+1} = b_{m+2} = \ldots = b_{m+\binom{m}{2}} = 0.$$

■

$RM(2,m)$ is the subgroup of $\mathbb{Z}_2^{2^m}$ generated by the codewords in $\mathbf{G}_m^{(2)}$. $RM(2,m)$ contains $2^{1+m+\binom{m}{2}}$ codewords.

Augmenting $\mathbf{G}_m^{(2)}$ with all products of the form $\vec{g}_i \cdot \vec{g}_j \cdot \vec{g}_k$, $1 \leq i < j < k \leq m$, and continuing as above we get $\mathbf{G}_m^{(3)}$, $RM(3,m)$, *etc.*

Theorem. $RM(k,m)$ for $m \geq 1$, $0 \leq k \leq m$ is a subgroup of $\mathbb{Z}_2^{2^m}$ consisting of 2^N codewords, where $N = \sum_{i=0}^{k} \binom{m}{i}$. The minimum *Hamming weight* (*i.e.*, number of ones) of the nonzero codewords in $RM(k,m)$ is 2^{m-k}.

Proof. Exercise, or see Handbook of Coding Theory, V. Pless and W.C. Huffman, Editors, Vol. 1, pp. 122–126.

Let's examine a particular element $\vec{S}_m \in RM(2,m)$ given by

$$\vec{S}_m = \sum_{j=1}^{m-1} \vec{g}_j \cdot \vec{g}_{j+1} = \langle s_0\, s_1\, \ldots\, s_{2^m-1} \rangle.$$

Example. $m = 3$

n	0	1	2	3	4	5	6	7
$\vec{g}_1$	0	1	0	1	0	1	0	1
$\vec{g}_2$	0	0	1	1	0	0	1	1
$\vec{g}_3$	0	0	0	0	1	1	1	1
$\vec{g}_1 \cdot \vec{g}_2$	0	0	0	1	0	0	0	1
$\vec{g}_2 \cdot \vec{g}_3$	0	0	0	0	0	0	1	1
$\vec{S}_3$	0	0	0	1	0	0	1	0

Let $\phi(n)$ be the number of times that the *block* $B = [1\,1]$ occurs in the binary expansion of n, $0 \le n \le 2^m - 1$.

Claim.

$$s_n = \begin{cases} 0 & \text{if } \phi(n) \text{ is even} \\ 1 & \text{if } \phi(n) \text{ is odd.} \end{cases}$$

Proof. Consider the n-th entry in each individual term of the sum $\vec{S}_m$. This entry is 1 iff $\delta(j, n) = \delta(j+1, n) = 1$, otherwise it is 0. ■

Let $\mathcal{G}_m = \{\vec{\gamma}_0, \vec{\gamma}_1, \vec{\gamma}_2, \ldots, \vec{\gamma}_{2^m-1}\}$ be the subgroup of $RM(1,m)$ generated by $\vec{g}_1, \vec{g}_2, \ldots, \vec{g}_m$.

Example. $m = 3$

	n	0	1	2	3	4	5	6	7
	$\vec{g}_1$	0	1	0	1	0	1	0	1
	$\vec{g}_2$	0	0	1	1	0	0	1	1
	$\vec{g}_3$	0	0	0	0	1	1	1	1
$\mathcal{G}_3$	$\vec{\gamma}_0 = 0 \cdot \vec{g}_1 + 0 \cdot \vec{g}_2 + 0 \cdot \vec{g}_3$	0	0	0	0	0	0	0	0
	$\vec{\gamma}_1 = 1 \cdot \vec{g}_1 + 0 \cdot \vec{g}_2 + 0 \cdot \vec{g}_3$	0	1	0	1	0	1	0	1
	$\vec{\gamma}_2 = 0 \cdot \vec{g}_1 + 1 \cdot \vec{g}_2 + 0 \cdot \vec{g}_3$	0	0	1	1	0	0	1	1
	$\vec{\gamma}_3 = 1 \cdot \vec{g}_1 + 1 \cdot \vec{g}_2 + 0 \cdot \vec{g}_3$	0	1	1	0	0	1	1	0
	$\vec{\gamma}_4 = 0 \cdot \vec{g}_1 + 0 \cdot \vec{g}_2 + 1 \cdot \vec{g}_3$	0	0	0	0	1	1	1	1
	$\vec{\gamma}_5 = 1 \cdot \vec{g}_1 + 0 \cdot \vec{g}_2 + 1 \cdot \vec{g}_3$	0	0	1	1	0	0	1	1
	$\vec{\gamma}_6 = 0 \cdot \vec{g}_1 + 1 \cdot \vec{g}_2 + 1 \cdot \vec{g}_3$	0	0	1	1	1	1	0	0
	$\vec{\gamma}_7 = 1 \cdot \vec{g}_1 + 1 \cdot \vec{g}_2 + 1 \cdot \vec{g}_3$	0	1	1	0	1	0	0	1

Switch gears: rewrite all codewords in $RM(k,m)$ by mapping $0 \to 1$, $1 \to -1$. Since $\vec{g}_1, \vec{g}_2, \ldots, \vec{g}_m$ are discretized versions of the Rademacher functions, $\vec{\gamma}_0, \vec{\gamma}_1, \ldots, \vec{\gamma}_{2^m-1}$, are discretized versions of the Walsh functions. That is, $\mathcal{G}_m$ is the $2^m \times 2^m$ Sylvester Hadamard matrix, which we relabel H_m.

Example.

$$H_3 = \begin{matrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{matrix}$$

Now $s_n = (-1)^{\phi(n)}$.

Claim.

$$s_{2n} = s_n, \quad s_{2n+1} = \begin{cases} s_n & \text{if } n \text{ is even} \\ -s_n & \text{if } n \text{ is odd} \end{cases}.$$

Proof. The binary expansion of $2n$ is the binary expansion of n shifted one slot to the left with a 0 added on the right, so $\phi(2n) = \phi(n)$. Similarly the binary expansion of $2n+1$ is the binary expansion of n shifted one slot to the left with a 1 added on the right. If n is even this does not change $\phi(n)$. If n is odd (*i.e.*, *n ends in* 1) then $\phi(2n+1) = \phi(n) + 1$.

■

Consider the *generating function* of $\{s_n\}$,

$$g(z) = \sum_{n=0}^{\infty} s_n z^n.$$

Claim. $g(z)$ satisfies the functional equation (FE) (Brillhart and Carlitz)

$$g(z) = g(z^2) + zg(-z^2).$$

Proof. Write $g(z)$ as the sum of its even and odd parts, $E(z)$ and $O(z)$, respectively. So

$$E(z) = \sum_{n=0}^{\infty} s_{2n} z^{2n} \quad \text{and} \quad O(z) = \sum_{n=0}^{\infty} s_{2n+1} z^{2n+1}.$$

From the previous claim

$$
\begin{aligned}
E(z) &= \sum_{n=0}^{\infty} s_n z^{2n} \quad = \quad g(z^2) \quad \text{and} \\
O(z) &= \sum_{\substack{n=0 \\ n\,\text{even}}}^{\infty} s_{2n+1} z^{2n+1} + \sum_{\substack{n=0 \\ n\,\text{odd}}}^{\infty} s_{2n+1} z^{2n+1} \\
&= z \sum_{\substack{n=0 \\ n\,\text{even}}}^{\infty} s_n z^{2n} - z \sum_{\substack{n=0 \\ n\,\text{odd}}}^{\infty} s_n z^{2n} \\
&= z \sum_{n=0}^{\infty} (-1)^n s_n z^{2n} \quad = \quad z g(-z^2)
\end{aligned}
$$

■

Iterate the FE for $g(z)$:

$$\begin{aligned} g(z^2) &= g(z^4) + z^2 g(-z^4) \\ g(-z^2) &= g(z^4) - z^2 g(-z^4), \quad \text{so} \\ g(z) &= (1+z)g(z^4) + z^2(1-z)g(-z^4). \end{aligned}$$

Repeat:

$$\begin{aligned} g(z^4) &= g(z^8) + z^4 g(-z^8) \\ g(-z^4) &= g(z^8) - z^4 g(-z^8), \quad \text{so} \\ g(z) &= (1+z+z^2-z^3)g(z^8) + z^4(1+z-z^2+z^3)g(-z^8). \end{aligned}$$

Continuing we see that, beginning with

$$g(z) = A(z)g(z^{2^m}) + z^{2^{m-1}} B(z)g(-z^{2^m})$$

and applying

$$\begin{aligned} g(z^{2^m}) &= g(z^{2^{m+1}}) + z^{2^m} g(-z^{2^{m+1}}) \\ g(-z^{2^m}) &= g(z^{2^{m+1}}) - z^{2^m} g(-z^{2^{m+1}}) \end{aligned}$$

we get at the next step

$$\begin{aligned} g(z) = \Big[A(z) + z^{2^{m-1}} B(z)\Big]\, g(z^{2^{m+1}}) \\ + z^{2^m} \Big[A(z) - z^{2^{m-1}} B(z)\Big]\, g(-z^{2^{m+1}}) \quad . \end{aligned}$$

Renaming the initial $A(z)$ and $B(z)$ to $P_0(z)$ and $Q_0(z)$, respectively, and naming the (polynomial) coefficients of $g(z^{2^m})$ and $g(-z^{2^m})$ $P_{m-1}(z)$ and $Q_{m-1}(z)$, respectively, $m \geq 1$, the above yields

$$\begin{aligned} P_0(z) &= Q_0(z) = 1 \\ P_m(z) &= P_{m-1}(z) + z^{2^{m-1}} Q_{m-1}(z) \\ Q_m(z) &= P_{m-1}(z) - z^{2^{m-1}} Q_{m-1}(z) \quad . \end{aligned}$$

Thus, the $\{P_m(z)\}_{m=0}^{\infty}$ and $\{Q_m(z)\}_{m=0}^{\infty}$ are precisely the Shapiro Polynomials! $P_m(z)$ and $Q_m(z)$ are each polynomials of degree $2^m - 1$ with coefficients ± 1. For each m the first 2^m coefficients of $g(z)$ are exactly the coefficients of $P_m(z)$. So, for each m, the 2^m-truncation $\langle\, s_0\, s_1\, \ldots\, s_{2^m-1} \,\rangle$ of the *Shapiro sequence* $\{s_j\}_{j=0}^{\infty}$ is an element of $RM(2, m)$.

Why might that be important?

Recall the fundamental property of the Shapiro polynomials, namely that for each m P_m and Q_m are complementary:

$$|P_m(z)|^2 + |Q_m(z)|^2 = 2^{m+1} \quad \text{for all } |z| = 1.$$

Consequently P_m and Q_m each have *crest factor* (the ratio of the sup norm to the L^2 norm on the unit circle) bounded by $\sqrt{2}$ *independent of* m. *i.e.*, P_m and Q_m are *energy spreading*. So the coefficients of P_m are an energy spreading second order Reed-Muller codeword.

Also, letting $\vec{h}_j$, $0 \leq j \leq 2^m - 1$, denote the rows of $\mathbf{H}_m$, the matrix $\mathbf{P}_m$ whose rows are $\vec{S}_m \cdot \vec{h}_j$, is a *PONS matrix*. Its 2^m rows can be split into 2^{m-1} pairs of complementary rows, with each row having crest factor (bounded by) $\sqrt{2}$.

Since each $\vec{h}_j \in RM(1, m)$ and $\vec{S}_m \in RM(2, m)$, the (rows of the) PONS matrix is a coset of the subgroup $RM(1, m)$ of $RM(2, m)$.

Thus we have constructed 2^m (really 2^{m+1} by considering $-\mathbf{H}_m$) energy spreading second order Reed-Muller codewords.

Let's now briefly examine growth properties of $g(re^{i\theta})$ as $r \uparrow 1$.

For $0 < r < 1$ set

$$M(r) = \max_{\theta} |g(re^{i\theta})| \quad .$$

Using the crest factor bound for $P_m(z)$ and partial summation yields $M(r) = O\left(\frac{1}{1-r}\right)^{\frac{1}{2}}$.

Challenge. Since the FE $g(z) = g(z^2) + zg(-z^2)$ together with the initial condition $g(0) = 1$ uniquely determines $g(z)$, obtain this bound on $M(r)$ directly from the FE, without resorting to the (very beautiful but very specific) complementarity property of P_m and Q_m.

Why bother?

I. Because it *is* a challenge;

II. Blocks other than $B = [1\,1]$ appear in connection with higher-order Reed-Muller codes. For example, the block $[1\,1\,1]$ yields codewords in $RM(3, m)$. The generating functions of these blocks satisfy similar (although more complicated) FE's. The idea (hope?) is that these FE's should yield corresponding crest factor bounds for subsets of $RM(k, m)$, $k \geq 3$, resulting in higher-order energy spreading Reed-Muller codes.

Current state of the art

Theorem. For any $\epsilon > 0$, $M(r) = O\left(\frac{1}{1-r}\right)^{\frac{1}{2}+\epsilon}$.

Corollary. Let $s_n(z) = \sum_{j=0}^{n} s_j z^j$ be a partial sum of $g(z)$. Then for each $\alpha > \frac{1}{2}$,

$$\max_{|z|=1} |s_n(z)| = O(n^\alpha) \quad \text{as } n \to \infty.$$

Basic Lemma. Let $F(r)$ be a positive increasing continuous function on $[0, 1)$. If

$$F(r) \leq AF(r^{\alpha})$$

for some $A > 0, \alpha > 1$ then

$$F(r) = O\left(\frac{1}{1-r}\right)^{\frac{\log A}{\log \alpha}}$$

for r near 1.

Proofs. To appear.

Blocks and FE's

Let $B = [\beta_1\, \beta_2\, \ldots\, \beta_r]$, $\beta_j = 0$ or 1, $\beta_1 = 1$ be a *binary block* and $N = N(B) = \beta_r + 2\beta_{r-1} + \ldots + 2^{r-1}\beta_1$ be the integer whose binary expansion is B. Let $\Psi_B(n)$ be the number of occurrences of B in the binary expansion of n and let $f_B(z)$ be the generating function of Ψ_B,

$$f_B(z) = \sum_{n=0}^{\infty} \Psi_B(n) z^n \quad .$$

Theorem. $f_B(z)$ satisfies the FE

$$f_B(z) = (1+z) f_B(z^2) + \frac{z^{N(B)}}{1 - z^{2^r}} \quad .$$

Proof. To appear.

Now consider the *parity sequence* of $\Psi_B(n)$, $\delta_B(n) = (-1)^{\Psi_B(n)}$, and its generating function $g_B(z) = \sum_{n=0}^{\infty} \delta_B(n) z^n$. For the general case it will again be useful to split g_B into its even and odd parts,

$$E_B(z) = \sum_{n=0}^{\infty} \delta_B(2n) z^{2n}$$

$$O_B(z) = \sum_{n=0}^{\infty} \delta_B(2n+1) z^{2n+1}$$

Previous example: $B = [11]$, $\delta_B(n)$ is the Shapiro sequence, $g_B(z)$ satisfies the FE $g_B(z) = g_B(z^2) + z g_B(-z^2)$.

Example: $B = [1]$.
Arguing as before, $\Psi_B(2n) = \Psi_B(n)$ and $\Psi_B(2n+1) = \Psi_B(n)+1$ so that (writing δ_n for $\delta_B(n)$ to ease notation) $\delta_{2n} = \delta_n$, $\delta_{2n+1} = -\delta_n$. Hence $E_B(z) = g_B(z^2)$, $O_B(z) = -zg_B(z^2)$, and we have the FE $g_B(z) = (1-z)g_B(z^2)$. Iterating, $g_B(z) = (1-z)(1-z^2)(1-z^4)\ldots$ and δ_n is the Thue-Morse sequence $[1\ -1\ -1\,1\ -1\,1\,1\ -1\ \ldots]$. Drop the subscript B from now on.

Example: $\beta_r = 0$.
$\Psi(2n+1) = \Psi(n)$, so $\delta_{2n+1} = \delta_n$, so $O(z) = zg(z^2)$. Since $g(z) - g(-z) = 2O(z)$ we have the FE $g(z) = g(-z) + 2zg(z^2)$.

Example: $\beta_r = 1$.
As above, now $g(z) = -g(-z) + 2g(z^2)$.

Example (a typical case?): $B = [1\,1\,0\,0\,1\,0], r = 6.$

$\Psi(2n+1) = \Psi(n)$. $\Psi(2n) = \Psi(n)$ unless the binary expansion of n ends in $[1\,1\,0\,0\,1]$, *i.e.*, unless $n \equiv K (\bmod 2^5)$, where $K = 2^4 + 2^3 + 2^0 = 25$, in which case $\Psi(2n) = \Psi(n) + 1$. So

$$\delta_{2n+1} = \delta_n, \quad \delta_{2n} = \begin{cases} -\delta_n & \text{if } n \equiv 25 (\bmod 32) \\ \delta_n & \text{otherwise} \end{cases} .$$

So $O(z) = zg(z^2)$.

$$E(z) = \sum_{n=0}^{\infty} \delta_{2n} z^{2n} = \sum_{n=0}^{\infty} \delta_n z^{2n} - 2 \sum_{n \equiv 25 \pmod{32}} \delta_n z^{2n}$$

$$= g(z^2) - 2 \sum_{j=0}^{\infty} \delta_{32j+25} z^{64j+50} = g(z^2) - 2z^{50} F(z)$$

where $F(z) = \sum_{j=0}^{\infty} \delta_{32j+25} z^{64j}$.

But $\delta_{32j+25} = \delta_{2(16j+12)+1} = \delta_{16j+12} = \delta_{2(8j+6)} = \delta_{8j+6} = \delta_{2(4j+3)} = \delta_{4j+3} = \delta_{2(2j+1)+1} = \delta_{2j+1} = \delta_j$, where we have used the fact that neither $8j + 6$ nor $4j + 3$ can be congruent to $25 \pmod{32}$. So $F(z) = \sum_{j=0}^{\infty} \delta_j z^{64j} = g(z^{64})$, and we have the FE

$$g(z) = (1 + z)g(z^2) - 2z^{50} g(z^{64}).$$

How *typical* is this example? Do we always get *Full Reduction* (FR) of the index of δ?

Consider the general case:

$$\begin{aligned} B &= [\beta_1\,\beta_2\,\ldots\,\beta_r] \\ N &= \beta_r + 2\beta_{r-1} + \ldots + 2^{r-1}\beta_1 \\ K &= \beta_{r-1} + 2\beta_{r-2} + \ldots + 2^{r-2}\beta_1 \quad . \end{aligned}$$

Case I: $\beta_r = 0$. As above,

$$\delta_{2n+1} = \delta_n, \quad \delta_{2n} = \begin{cases} -\delta_n & \text{if } n \equiv K (\operatorname{mod} 2^{r-1}) \\ \delta_n & \text{otherwise} \end{cases} \quad .$$

$$O(z) = zg(z^2), \quad E(z) = g(z^2) - 2z^{2K} \sum_{j=0}^{\infty} \delta_{2^{r-1}j+K} z^{2^r j} \quad .$$

To get FR the index $I(1) = I_{j,K}(1) = 2^{r-1}j + K$ must reduce to j by repeated applications of the mapping $\mu(n)$:

$$\mu(2n+1) = n, \quad \mu(2n) = n \quad \text{unless } n \equiv K (\operatorname{mod} 2^{r-1}).$$

Let $\{I(1), I(2), \ldots\}$ be the succession of indices that we get by repeating μ (assuming it works), and let I denote one of these indices. Whether $I = 2n+1$ or $I = 2n$, reduction to n occurs by dropping the last binary digit on the right of I and shifting what's left 1 slot to the right. For reduction to fail at the first step, $I(1)$ must be of the form $2n$ where $n \equiv K (\operatorname{mod} 2^{r-1})$, or $n = 2^{r-1}m + K$ for some integer m, or $2n = 2^r m + 2K$.

The binary expansion (BE) of K is $(\beta_1\, \beta_2\, \ldots\, \beta_{r-1})$ so that of $2K$ is $(\beta_1\, \beta_2\, \ldots\, \beta_{r-1}\, 0)$.

So for the first reduction $I(1) \to I(2)$ to fail the BE of $I(1)$ must end in $(\beta_1\,\beta_2\,\ldots\,\beta_{r-1}\,0)$. This is possible (*i.e.*, there are integers j which make it possible) iff the BE of $I(1)$ ends in $(\beta_2\,\beta_3\,\ldots\,\beta_{r-1}0)$, or (since the BE of $I(1)$ ends in that of K)

$$(\beta_1\,\beta_2\,\ldots\,\beta_{r-1}) = (\beta_2\,\beta_3\,\ldots\,\beta_{r-1}0) \quad .$$

Assuming this equation does not hold we get $I(2)$ whose BE ends in $(\beta_1\,\beta_2\,\ldots\,\beta_{r-2})$. As above, $I(2) \to I(3)$ fails iff the BE of $I(2)$ ends in $(\beta_1\,\beta_2\,\ldots\,\beta_{r-1}\,0)$ which is possible (again, there are integers j which make it possible) iff $I(2)$ ends in $(\beta_3\,\beta_4\,\ldots\,\beta_{r-1}\,0)$, or

$$(\beta_1\,\beta_2\,\ldots\,\beta_{r-2}) = (\beta_3\,\beta_4\,\ldots\,\beta_{r-1}\,0) \quad .$$

Call the block $B = [\beta_1\, \beta_2\, \ldots\, \beta_r]$ *nonrepeatable* if

$$[\beta_1\, \beta_2\, \ldots\, \beta_\nu] \neq [\beta_{r-(\nu-1)}\, \beta_{r-(\nu-2)}\, \ldots\, \beta_r]$$

for each ν, $1 \leq \nu \leq r-1$.

Theorem. FR works iff B is nonrepeatable. When FR works we get the FE $g(z) = (1+z)g(z^2) - 2z^{2K}g(z^{2^r})$.

Case II: $\beta_r = 1$. The above argument works when B is nonrepeatable up to the last step, yielding:

Theorem. If $[\beta_1\, \beta_2\, \ldots\, \beta_\nu] \neq [\beta_{r-(\nu-1)}\, \beta_{r-(\nu-2)}\, \ldots\, \beta_r]$ for each ν, $2 \leq \nu \leq r-1$, and $\beta_1 = \beta_r = 1$, then reduction works up until the final step and we get the FE

$$g(z) = (1+z)g(z^2) - 2z^{2K+1-2^{r-1}}\left[g(z^{2^{r-1}}) - g(z^{2^r})\right] \quad .$$

Other cases are not so neat.

Example. $B = [1\,1\,0\,1\,1\,1]$.

The FE is

$$g(z) = (1+z)g(z^2) - 2z^7 g(z^{16}) + 2z^7 g(z^{32}) + 2z^{23} g(z^{64}) \quad .$$

Example. $B = [1\,0\,1\,1\,0\,1]$.

The FE is

$$g(z) = (1+z)g(z^2) - 2z^5[g(z^8) - (1+z^8)g(z^{16})] - 2z^{13}[g(z^{32}) - g(z^{64})].$$

The general "1-1" case, $\beta_1 = \beta_r = 1$.

$$\delta_{2n} = \delta_n, \quad \delta_{2n+1} = \begin{cases} -\delta_n & \text{if } n \equiv K \pmod{2^{r-1}} \\ \delta_n & \text{otherwise} \end{cases},$$

$$K = \beta_{r-1} + 2\beta_{r-2} + \ldots + 2^{r-2}\beta_1\,,$$

$$E(z) = g(z^2)\,,$$

$$O(z) = zg(z^2) - 2 \sum_{\substack{n \equiv K \\ \pmod{2^{r-1}}}} \delta_n z^{2n+1} = zg(z^2) - 2G_B(z)$$

$$\text{where} \quad G_B(z) = \sum_{j=0}^{\infty} \delta_{2^{r-1}j+K} z^{2^r j + 2K + 1}.$$

Basic idea: Reduce subscript of δ as much as possible, express $G_B(z)$ in terms of $G_B(z^{2^p})$ for some $p > 0$, replace $G_B(z^{2^p})$ by using $-2G_B(z^{2^p}) = O(z^{2^p}) - z^{2^p} g(z^{2^{p+1}}) = g(z^{2^p}) - g(z^{2^{p+1}}) - z^{2^p} g(z^{2^{p+1}})$ and then repeat to get the desired expression for $O(z) = g(z) - g(z^2)$.

Details for the "fully repeatable" case, $\beta_j = 1$, $1 \le j \le r$.

Now $K = 2^{r-1} - 1$. For $1 \le m \le r-1$ let

$$G_m(z) = \sum_{j=0}^{\infty} \delta_{2^{r-m}j+2^{r-m}-1} z^{2^r j+2^r-1} \quad ,$$

so that $G_B(z) = G_1(z)$.

For $2 \le q \le r-1$,

$$\delta_{2^q j + 2^q - 1} = \delta_{2(2^{q-1} j + 2^{q-1} - 1) + 1} =$$
$$= \begin{cases} -\delta_{2^{q-1} j + 2^{q-1} - 1} & \text{if } j \equiv 2^{r-q} - 1 (\operatorname{mod} 2^{r-q}) \\ \delta_{2^{q-1} j + 2^{q-1} - 1} & \text{otherwise} \end{cases},$$

since

$$2^{q-1} j + 2^{q-1} - 1 \equiv (2^{r-1} - 1)(\operatorname{mod} 2^{r-1})$$
$$\Leftrightarrow j \equiv (2^{r-q} - 1)(\operatorname{mod} 2^{r-q}).$$

Let $q = r - m$, so $m = r - q$, so $1 \le m \le r - 2$. Then

$$\delta_{2^{r-m}j+2^{r-m}-1} = \begin{cases} -\delta_{2^{r-m-1}j+2^{r-m-1}-1} & \text{if } j \equiv (2^m - 1) (\operatorname{mod} 2^m) \\ \delta_{2^{r-m-1}j+2^{r-m-1}-1} & \text{otherwise} \end{cases}$$

So, for $1 \le m \le r - 2$,

$$G_m(z) = \sum_{j=0}^{\infty} \delta_{2^{r-m-1}j+2^{r-m-1}-1} z^{2^r j + 2^r - 1} - 2 \sum_{\substack{j \equiv (2^m - 1) \\ (\operatorname{mod} 2^m)}} \delta_{2^{r-m-1}j+2^{r-m-1}-1} z^{2^r j + 2^r - 1}.$$

When you replace j in the second sum by $2^m j + 2^m - 1$ it becomes

$$\begin{aligned}
&\sum_{j=0}^{\infty} \delta_{2^{r-1}j+2^{r-1}-2^{r-m-1}+2^{r-m-1}-1} z^{2^{r+m}j+2^{r+m}-2^r+2^r-1} \\
=&\sum_{j=0}^{\infty} \delta_{2^{r-1}j+2^{r-1}-1} z^{2^{r+m}j+2^{r+m}-1} \\
=&z^{2^m-1} \sum_{j=0}^{\infty} \delta_{2^{r-1}j+2^{r-1}-1} z^{2^{r+m}j+2^m(2^r-1)} \\
=&z^{2^m-1} \sum_{j=0}^{\infty} \delta_{2^{r-1}j+2^{r-1}-1} \left(z^{2^m}\right)^{2^r j+2^r-1} \\
=&z^{2^m-1} G_1\left(z^{2^m}\right) .
\end{aligned}$$

The first sum is obviously $G_{m+1}(z)$, so

$$G_m(z) = G_{m+1}(z) - 2z^{2^m-1}G_1(z^{2^m})$$

for $1 \le m \le r-2$. For $m = r-1$,

$$\begin{aligned} G_{r-1}(z) &= \sum_{j=0}^{\infty} \delta_{2j+1} z^{2^r j + 2^r - 1} \\ &= z^{2^{r-1}-1} \sum_{j=0}^{\infty} \delta_{2j+1} (z^{2^{r-1}})^{2j+1} \\ &= z^{2^{r-1}-1} O(z^{2^{r-1}})\,. \end{aligned}$$

Combining these G_m's in turn yields: $G_B(z) = G_1(z) =$

$$
\begin{aligned}
&= G_2(z) - 2zG_1(z^2) = G_3(z) - 2zG_1(z^2) - 2z^3G_1(z^4) \\
&= G_4(z) - 2zG_1(z^2) - 2z^3G_1(z^4) - 2z^7G_1(z^8) = \ldots \\
&= G_{r-1} - 2zG_1(z^2) - 2z^3G_1(z^4) - \ldots - 2z^{2^{r-2}-1}G_1(z^{2^{r-2}}) \\
&= z^{2^{r-1}-1}O(z^{2^{r-1}}) + z[-2G_1(z^2) - 2z^2G_1(z^4) - 2z^6G_1(z^8) \\
&\quad - \ldots - 2z^{2^{r-2}-2}G_1(z^{2^{r-2}})] \\
&= z^{2^{r-1}-1}[g(z^{2^{r-1}}) - g(z^{2^r})] + z[g(z^2) - g(z^4) - z^2g(z^4) \\
&\quad + z^2\{g(z^4) - g(z^8) - z^4g(z^8)\} + z^6\{g(z^8) - g(z^{16}) - z^8g(z^{16})\} \\
&\quad + \ldots + z^{2^{r-2}-2}\{g(z^{2^{r-2}}) - g(z^{2^{r-1}}) - z^{2^{r-2}}g(z^{2^{r-1}})\}] \\
&= zg(z^2) - zg(z^4) - z^3g(z^8) - z^7g(z^{16}) \\
&\quad - \ldots - z^{2^{r-2}-1}g(z^{2^{r-1}}) - z^{2^{r-1}-1}g(z^{2^r})
\end{aligned}
$$

With

$$g(z) = E(z) + O(z) = g(z^2) + zg(z^2) - 2G_B(z)$$

we finally have the FE

$$g(z) = (1-z)g(z^2) + 2z[g(z^4) + z^2 g(z^8) + z^6 g(z^{16}) + \ldots + z^{2^{r-2}-2} g(z^{2^{r-1}}) + z^{2^{r-1}-2} g(z^{2^r})].$$

References

1 Papers, patent, *etc.*, at www.prometheus-inc.com/public/pons

2 Brillhart & Carlitz, "Note on the Shapiro Polynomials". Proc. AMS 25, 1970 (pp. 114-118)

3 H.S. Shapiro, "Extremal Problems for Polynomials and Power Series", Sc.M. thesis, MIT, 1951

4 J.A. Davis and J. Jedwab, "Peak-to-mean power control in OFDM, Golay complementary sequences, and Reed-Muller codes", IEEE Trans. Inf. Th., **45**(7), pp. 2397–2417, 1999

5 S. R. Weller, W. Moran and J. S. Byrnes, "On the Use of the PONS Sequences for Peak-to-Mean Power Control in OFDM", Proc. of the Workshop on Defense Applications in Signal Processing, LaSalle, Illinois, pp. 203–209, 1999

6 P.-G. Becker, "k-Regular Power Series and Mahler-Typer Functional Equations", Journal of Number Theory, Vol. 49, pp. 269–286, 1994

7 Handbook of Coding Theory, V. Pless and W.C. Huffman, Eds., Vol. 1