ISIT'2013 1569718489

Spherically Punctured Reed-Muller Codes

Olga Kapralova and Ilya Dumer
Department of Electrical Engineering
University of California at Riverside, USA
Email: {okapralova, dumer}@ee.ucr.edu

***Abstract*—Consider a binary Reed-Muller code RM(r,m) defined on the m-dimensional hypercube $\mathbb{F}_2^m$. In this paper, we study punctured Reed-Muller codes $P_r(m,b)$ whose positions form a spherical b-layer and include all m-tuples of a given Hamming weight b. These punctured codes inherit some recursive properties of the original RM codes and can be built from the shorter codes, by decomposing a spherical b-layer into sub-layers of smaller dimensions. However, codes $P_r(m,b)$ cannot be formed by the recursive Plotkin construction. We analyze recursive properties of these codes and find their code distances for arbitrary values of parameters $r, m,$ and b.**

I. Introduction

In this paper, we study code constructions that restrict Reed-Muller (RM) codes to some small subsets of their positions. To specify our design, consider the set $F(m,r)$ of boolean polynomials of degree r or less in m binary variables $x_1,\dots,x_m$, where $r \le m$. Then codes RM(r,m) are defined by the mapping

$$\mathbb{F}_2^m \stackrel{f(x)}{\to} \mathbb{F}_2, \quad f(x) \in F(m,r)$$

that gives the values of polynomials $f(x)$ if the arguments $x = (x_1,...,x_m)$ run through $\mathbb{F}_2^m$. Below arguments x represent code positions.

RM codes have simple recursive structure defined by the Plotkin construction, which represents every codeword c as the combination $(u, u+v)$ of some codewords $u \in RM(r,m-1)$ and $v \in RM(r-1,m-1)$. This structure also yields simple recursive decoding that consecutively outputs different information bits with the overall complexity order of $n\min(r,m-r)$. For long RM codes, these recursive procedures - similar to cancellation decoding of polar codes - separate virtually all information bits into those transmitted over the maximum-noise channels and those used over noise-free channels. Eliminating the most error-prone information bits in RM codes substantially improves their decoding performance [4], while complete channel optimization for codes RM(m,m) gives capacity-achieving polar codes [5]. However, subcodes of RM codes or polar codes, which have been designed to date, achieve good performance only on the very long blocks. Therefore, we wish to substantially reduce the original lengths of RM codes. Our goal is to design shorter codes with an equally good performance while keeping a simple recursive structure of RM codes or their polarized subcodes.

Our first step in this direction is to consider codes RM(r,m) punctured to some spherical layer. Namely, let wt(x) denote the Hamming weight of a binary vector $x = (x_1,\dots,x_m)$. Similarly to RM codes, we consider all m-variate boolean polynomials of degree at most r but restrict their code positions to some binary sphere

$$S_b^m = \{x \in \mathbb{F}_2^m : \text{wt}(x) = b\} \tag{1}$$

of radius $b \in [1,m]$. Let $W_r(m,b)$ be the $(0,1)$-matrix of size $\binom{m}{r} \times \binom{m}{b}$, which is formed by the values of m-variate monomials of degree r at the points $x \in S_b^m$. We also consider the extended matrix $M_r(m,b)$ that stacks the matrices $W_\tau(m,b)$ for all degrees $\tau \in [0,r]$:

$$M_r(m,b) = \begin{bmatrix} W_0(m,b) \\ \vdots \\ W_r(m,b) \end{bmatrix} \tag{2}$$

Matrices $W_r(m,b)$ and $M_r(m,b)$ have been studied in [1], [3]. We will consider codes $P_r(m,b)$ formed as linear spans of matrices $M_r(m,b)$. In other words, we use

Definition 1: A code $P_r(m,b)$ consists of the vectors $(\dots, f(x), \dots)$, where $x \in S_b^m$ and $f \in F(m,r)$.

In the sequel, $P_r(m,b)$ are called the *spherically punctured* Reed-Muller codes. The following important lemma [3] gives the rank of matrix $M_r(m,b)$ over $GF(2)$.

Lemma 2 ([3]): For integers $0 \le r \le m$ and $b \in [r, m-r]$, matrix $M_r(m,b)$ has rank $\binom{m}{r}$.

Note that matrices $M_r(m,b)$ have

$$h_r(m) = \sum_{i=0}^{r} \binom{m}{i} \tag{3}$$

rows. Thus, Lemma 2 shows that for any layer S_b^m, there exist *null* polynomials that have values $f(x) \equiv 0$ for all $x \in S_b^m$. Note also that Lemma 2 immediately leads to the following

Corollary 3: For non-negative integers r, m and $b \in [1,m]$, code $P_r(m,b)$ has length $n_P = \binom{m}{b}$ and dimension

$$k_P = \begin{cases} \binom{m}{r}, & b \in [r, m-r] \\ \binom{m}{b}, & \text{otherwise} \end{cases}$$

Indeed, $W_r(m,b) \equiv 0$ for any $b < r$. Also, for any $x \in S_b^m$, a substitution $x_i = 1 + y_i$ for all $i = 1,...,m$ replaces a polynomial $f(x)$ with a polynomial $f(y)$ and $y \in S_{m-b}^m$. Thus, rank$(M_r(m,b)) = \binom{m}{b}$ for any $b \notin [r, m-r]$.

The main goal of this paper is to define the recursive structure of codes $P_r(m,b)$ and find their minimum distance $d_r(m,b)$. Let

$$\Delta = \Delta(m,b) = \max\{b, m-b\}.$$

The main theorem of this paper is as follows.

Theorem 4: For non-negative integers r, b, m such that $r \in [0, m/2-1]$, $b \in [1, m]$, code $P_r(m, b)$ has minimum distance

$$d_r(m,b) = \begin{cases} 2\binom{m-r-1}{b}, & b = m/2, \\ \max\{\binom{m-r}{\Delta}, 1\}, & b \neq m/2 \end{cases} \quad (4)$$

Note that $d_r(m, b) = 1$ if $b \notin [r, m-r]$. Indeed, polynomials $f(x) = x_1 \dots x_b$ and $f(x) = (x_1 + 1) \dots (x_{m-b} + 1)$ give codewords of weights $\mathrm{wt}_f(m, b) = 1$ for any $b \in [1, r]$ or $b \in [m - r, m]$, respectively.

Below we consider the remaining cases of Theorem 4. This study addresses the following problems. First, codes $P_r(m, b)$ can be obtained by "spherical" recursion that splits the sphere S_b^m into "unequal" sub-spheres

$$S_b^{m-1} \text{ if } x_1 = 0 \quad \text{and} \quad S_{b-1}^{m-1} \text{ if } x_1 = 1$$

By contrast, RM codes yield a simpler recursion, which splits a cube $\mathbb{F}_2^m$ into "equal" sub-cubes $\mathbb{F}_2^{m-1}, x_1 = 0$ and $\mathbb{F}_2^{m-1}, x_1 = 1$. This will make recursive Plotkin $(u, u + v)$ construction invalid for PRM codes.

Second, some polynomials $f(x)$ yield zero codewords on the sub-spheres S_b^{m-1} and S_{b-1}^{m-1}, which is not the case for RM codes.

Third, full recursion into smaller codes will only partially hold for PRM codes. In particular, for $m = 2b \pm 1$, code distance $d_r(m, b)$ exceeds the sum of distances $d_r(m-1, b-1)$ and $d_r(m-1, b)$ on sub-spheres. Therefore, we begin with recursive properties of codes $P_r(m, b)$.

II. Recursive decomposition

Below we use notation $f_{m,r}$ for any polynomial in $F(m, r)$. Any such polynomial can be decomposed into the sum

$$f^{(0)}(x_1, \dots, x_{m-1}) + x_m f^{(1)}(x_1, \dots, x_{m-1}) \quad (5)$$

where $\deg(f^{(0)}) \leq r$ and $\deg(f^{(1)}) \leq r-1$. We also represent matrix $M_r(m, b)$ as

$$\left[\begin{array}{c|c} M_r(m-1,b) & M_r(m-1,b-1) \\ \hline 0 & M_{r-1}(m-1,b-1) \end{array}\right] \quad (6)$$

The left part of matrix (6) gives the values of all *monomials* at the points $x \in S_b^m$, where $(x_1, \dots, x_{m-1}) \in S_b^{m-1}$ and $x_m = 0$. Here the upper part $M_r(m-1, b)$ gives the values of all $f^{(0)}$-related monomials, which are free of x_m. The lower zero submatrix corresponds to $x_m f^{(1)}$-related monomials. Similarly, monomials in the right part are evaluated at the points x with $x_m = 1$ and $(x_1, \dots, x_{m-1}) \in S_{b-1}^{m-1}$. Here the upper part $M_r(m-1, b-1)$ includes the values of all $f^{(0)}$-related monomials and the lower part gives the values of $x_m f^{(1)}$-related monomials.

Below we write $f(x) \equiv g(x) \mid S$ if the two functions f and g are equal for all points $x \in S$ on some subset $S \subset \mathbb{F}_2^m$ and also use the same notation for the sets of polynomials F and G. Our next goal is to consider the set of null polynomials

$$\mathcal{N}_r(m, b) = \{f_{m,r}(x) : f_{m,r}(x) \equiv 0 \mid S_b^m\} \quad (7)$$

Example. Given some radius b and any $s \in [1, b]$, consider symmetric functions

$$\psi_{m,s}(x) = \sum_{1 \leq i_1 < \dots < i_s \leq m} x_{i_1} \dots x_{i_s} + \binom{b}{s}$$

Note that $\psi_{m,s}(x)$ takes a constant value $\left[\binom{b}{s} + \binom{k}{s}\right] \pmod 2$ on all the points of some sphere S_k^m. For any $s \leq r$ and any $f_{m,r-s}(x)$, we can also consider the set of null polynomials

$$\psi_{m,s}(x) f_{m,r-s}(x) \equiv 0 | S_b^m,$$

or take their linear combinations. Finally, note that any such polynomial has degree $r-1$ or less on any sphere S_k^m, since $\psi_{m,s} = const \mid S_k^m$.

The following theorem generalizes the above example and is central to our study of null polynomials $f_{m,r}(x)$ and codes $P_r(m, b)$. It shows that the set of null polynomials $\mathcal{N}_r(m, b)$ is equivalent to the full set $F(m, r-1)$ of polynomials of degree $r-1$ on the adjacent spheres S_{b-1}^m or S_{b+1}^m.

Theorem 5: For any set of parameters m, r, and b such that $r \leq m$, $b \in [r, m-r]$,

$$\mathcal{N}_r(m, b) \equiv F(m, r-1) \mid S_{b-1}^m \quad (8)$$

$$\mathcal{N}_r(m, b) \equiv F(m, r-1) \mid S_{b+1}^m \quad (9)$$

Proof: Represent matrix $M_r(m+1, b)$ in the recursive form (6)

$$\left[\begin{array}{c|c} M_r(m,b) & M_r(m,b-1) \\ \hline 0 & M_{r-1}(m,b-1) \end{array}\right]$$

It is easy to verify from Lemma 2 that matrices $M_r(m, b)$, $M_{r-1}(m, b-1)$ and $M_r(m+1, b)$ have null spaces of dimensions

$$\begin{aligned} h' &= \dim \mathcal{N}_r(m,b) = h_r(m) - \tbinom{m}{r} = h_{r-1}(m) \\ h'' &= \dim \mathcal{N}_{r-1}(m,b-1) = h_{r-2}(m) \\ h &= \dim \mathcal{N}_r(m+1,b) = h_{r-1}(m+1) \end{aligned}$$

Below we use an important recursive property $h' + h'' = h$ that can be readily verified for binomial coefficients. Now consider any linear combination (LC) $A_r(m, b)$ of $h_r(m)$ rows in $M_r(m, b)$. This LC is a codeword in $P_r(m, b)$ that gives the values of some polynomial $f_{m,r}(x)$ on S_b^m. From now on, we only consider LCs $A_r(m+1, b)$ and $A_r(m, b)$ that give zero codewords in $P_r(m+1, b)$ and $P_r(m, b)$, respectively. Each LC will be counted l times if it can be obtained by l different sets of binary coefficients. Thus, there exist 2^h and $2^{h'}$ such LCs $A_r(m+1, b)$ and $A_r(m, b)$.

Any set of binary coefficients that forms a LC $A_r(m, b)$ in the left section of matrix $M_r(m+1, b)$ also forms some LC C in the right section of $M_r(m+1, b)$,

$$C = A_r(m, b-1) \in P_r(m, b-1)$$

Next, we count the number of LCs $A_{r-1}(m, b-1)$ in $M_{r-1}(m, b-1)$ that form a given codeword C. By definition of h'', there exist $2^{h''}$ such LCs if $C \in P_{r-1}(m, b-1)$. Otherwise, no LC $A_{r-1}(m, b-1)$ can give C. Now we see

that there exist $L \le 2^{h'+h''}$ pairs $A_r(m,b)$, $A_{r-1}(m,b-1)$ that form an all-zero codeword in both sections of matrix $M_r(m+1,b)$. Thus, equality $L = 2^h$ holds if and only if

- each LC $A_r(m,b) = 0$ also gives a LC $A_r(m,b-1) \in P_{r-1}(m,b-1)$;
- all LCs $A_r(m,b-1)$ give different codewords in $P_{r-1}(m,b-1)$.

Thus, polynomials $f_{m,r}(x) \equiv 0 \mid S_b^m$ yield a one-to-one mapping to the codewords in $P_{r-1}(m,b-1)$ considered on the set S_{b-1}^m. This completes the proof of (8). To prove the second statement (9), we map any point $x = (x_1, ..., x_m) \in \mathbb{F}_2^m$ onto the *symmetric* point $\overline{x} = (x_1+1, \ldots, x_m+1)$. Then statement (9) for points $x \in S_b^m$ becomes equivalent to the statement (8) for points $\overline{x} \in S_{m-b}^m$:

$$\mathcal{N}_r(m, m-b) \equiv F(m, r-1) \mid S_{m-b-1}^m$$

■

Note. For $b \notin [r, m-r]$, null polynomials can keep their degree on the adjacent spheres. For example, linear polynomial $x_1 + ... + x_{m-1}$ belongs to $\mathcal{N}_1(m,m)$ for odd m but still has degree 1 on the adjacent sphere S_{m-1}^m.

Corollary 6: Code $P_r(m,b)$ is a linear span of the rows of matrix

$$\left[\ M_r(m-1,b) \ \middle|\ M_r(m-1,b-1)\ \right] \tag{10}$$

Proof: We again consider recursive representation (6) of matrix $M_r(m,b)$. By Theorem 5, the set of polynomials $\mathcal{N}_r(m,b)$ gives a fixed, all-zero codeword in the left section of $M_r(m,b)$ and runs through the whole code $P_{r-1}(m,b-1)$ in the right section. Thus, any linear combination of the rows in bottom part $[0, M_{r-1}(m-1,b-1)]$ of matrix (6) can be also obtained from its upper part. ■

Below we use representation (10) and evaluate any m-variate polynomial $f_{m,r}(x)$ on a sphere S_b^m using another $m-1$ variate polynomial $f_{m-1,r}(x)$ that is free of the last variable x_m.

III. Minimum distance of the code $P_r(m,b)$

To find the minimum distance $d_r(m,b)$ of code $P_r(m,b)$, we use decomposition (10). For each information word $f \notin \mathcal{N}_r(m,b)$ we consider two cases:

1) $f \in \mathcal{N}_r(m-1,b)$ or $f \in \mathcal{N}_r(m-1,b-1)$
2) $f \notin \mathcal{N}_r(m-1,b)$ and $f \notin \mathcal{N}_r(m-1,b-1)$

In the first case, polynomials f give zero weights on one of the two submatrices (10). We then use Theorem 5, which shows that any such polynomial f has a relatively high weight f on the second sub-matrix. In the second case, we bound the weight of f using the inductive hypothesis for the submatrices (10). We begin with a simple lower bound for the distance $d_r(m,b)$. Let $\mathrm{wt}_f(m,b)$ be the weight of a codeword generated on a sphere S_b^m by a polynomial $f = f_{m,r}$,

$$\mathrm{wt}_f(m,b) = |\{x \in S_b^m : f_{m,r}(x) = 1\}|\,. \tag{11}$$

We also use notation

$$\delta_r(m,b) = d_r(m-1,b-1) + d_r(m-1,b)$$

Lemma 7:

$$d_r(m,b) \ge \min\{\delta_r(m,b), d_{r-1}(m-1,b), \quad d_{r-1}(m-1,b-1)\} \tag{12}$$

Proof: If $f \in \mathcal{N}_r(m-1,b)$, then by Theorem 5, f acts as a polynomial of degree at most $r-1$ on the matrix $M_r(m-1,b-1)$, so

$$\mathrm{wt}_f(m,b) \ge d_{r-1}(m-1,b-1).$$

If $f \in \mathcal{N}_r(m-1,b-1)$, then again by Theorem 5,

$$\mathrm{wt}_f(m,b) \ge d_{r-1}(m-1,b).$$

Otherwise, the recursive structure of (10) gives

$$\mathrm{wt}_f(m,b) = \mathrm{wt}_f(m-1,b) + \mathrm{wt}_f(m-1,b-1).$$

■

The following proof of Theorem 4 derives tight lower and upper bounds on distance $d_r(m,b)$. Here the lower bounds address the case $m \ne 2b \pm 1$ and use double induction on r and m. The special case $m = 2b \pm 1$ is much more involved and is handled separately in Lemmas 11 and 12.

Proof: Upper bounds. For all m, the estimates (4) are bounded from above using polynomials

$$\begin{cases} \prod_{i=1}^{r} x_i, & b \in [r, m/2) \\ \prod_{i=1}^{r} (x_i+1), & b \in (m/2, m-r] \\ \prod_{i=1}^{r+1} x_i + \prod_{i=1}^{r+1} (x_i+1), & b = m/2 \end{cases}$$

It is easy to see that these polynomials give weights

$$w_1 = \tbinom{m-r}{m-b}, \quad w_2 = \tbinom{m-r}{b}, \quad w_3 = \tbinom{m-r-1}{b} + \tbinom{m-r-1}{m-b}.$$

Here we use estimate w_3 for $b = m/2$, since $w_1 = w_2$ and $w_3 < w_1$. Also, $w_3 = \min\{w_1, w_2\}$ for $m = 2b \pm 1$.

Lower bounds for $m \ne 2b \pm 1$. To prove Theorem 4 for any $b \in [r, m-r]$, we first use the *outer* induction on r and then the *inner* induction on m .

The *base case* $r = 0$ of the outer induction gives $f(x) = const$. Then the distance $d_0(m,b) = \binom{m}{b}$ coincides with (4). Next, we perform the induction step $r-1 \to r$. Here we first assume that the distance $d_{r-1}(m,b)$ satisfies equalities (4) for any $b \in [1,m]$. Given r, we then perform the inner induction step $m \to m+1$.

To find the distance $d_r(m+1,b)$, we assume that equalities (4) hold for $d_\rho(m,b)$ if $\rho \le r$ and $b \in [1,m]$. Any non-null polynomial f, also satisfies boundary conditions $d_r(m+1,1) = 1$ and $d_r(m+1,m+1) = 1$. Now consider two cases.

A. $m > 2b$. Then equalities (4) give identical estimates

$$\delta_r(m+1,b) = d_r(m,b-1) + d_r(m,b) = \binom{m+1-r}{m+1-b}$$

$$\min\{d_{r-1}(m,b), d_{r-1}(m,b-1)\} = \binom{m+1-r}{m+1-b}$$

By induction step $m \to m+1$, Lemma 7 gives

$$d_r(m+1,b) \geq \binom{m+1-r}{m+1-b}$$

B. $m < 2b-2$. Then equalities (4) give

$$\delta_r(m+1,b) = \binom{m+1-r}{b}$$

$$\min\{d_{r-1}(m,b), d_{r-1}(m,b-1)\} = \binom{m+1-r}{b}$$

Thus, $d_r(m+1,b) \geq \binom{m+1-r}{b}$, which completes the inner induction step $m \to m+1$.

C. $m = 2b$. Then estimates (12) give the required bound

$$w_3 = \delta_r(m,b) < d_{r-1}(m-1,b) = d_{r-1}(m-1,b-1)$$

■

Note that inductive estimates (12) become loose for the last remaining case $m = 2b \pm 1$. This case is considered below using a different technique. Namely, we employ multiple code decompositions into Plotkin constructions $(u, u+v)$.

IV. Special case $m = 2b \pm 1$

Note, that for any $x \in S_b^{2b}$ its reflection $\overline{x} \in S_b^{2b}$ also belongs to the same sphere. This leads to the following lemma.

Lemma 8: Polynomials $f \in F(2b,r)$ on the sphere S_b^{2b} generate the Plotkin construction $c = (u,\ u+v)$, where

$$u \in P_r(2b-1,b-1),\ v \in P_{r-1}(2b-1,b-1). \qquad (13)$$

Proof: We use partition $S_b^{2b} = S_0 \cup S_1$ into two subsets of equal size

$$S_i = \{x = (x_1,\ldots,x_{2b}) \in S_b^{2b} :\ x_1 = i\}.$$

Define a polynomial $v(x) = f(x) + f(\overline{x})$. Note that $\deg(v(x)) \leq r-1$. Now for any $x \in S_1$, let

$$u = (\ldots, f(x), \ldots), \quad v = (\ldots, v(x), \ldots).$$

Then vectors u and v satisfy conditions (13). Since $f(\overline{x}) = f(x)+v(x)$ for $x \in S_1$, polynomial f generates vector $u+v$ on the complementary set S_0. Thus, we obtain the Plotkin construction $c = (u,\ u+v)$ for the code $P_r(2b,b)$ on the sphere S_b^{2b}. ■

Below we take $m = 2b+1$; the other case $m = 2b-1$ is similar. First, we define a class of *symmetric* polynomials.

Definition 9: A polynomial $f(x) = f_{m,r}(x)$ is symmetric on the sphere S_b^m, if

$$f(x) + f(\overline{x}) \equiv 0 \mid S_b^m$$

Our analysis for the case $m = 2b+1$ will use partition (10) that splits the code $P_r(2b+1,b)$ into two codes $P_r(2b,b)$ and $P_r(2b,b-1)$, both of which are considered on the sphere S_b^{2b}. Therefore, we will analyze the polynomials in $F(2b,r)$. Our analysis includes two types of polynomials:

(1) non-symmetric on S_b^{2b} polynomials g;

(2) symmetric on S_b^{2b} polynomials f.

We then evaluate the weights wt_g or wt_f that these polynomials generate on both codes $P_r(2b,b)$ and $P_r(2b,b-1)$ and proceed with the combined weight on $P_r(2b+1,b)$. Here we keep the same notation wt_g or wt_f for all three codes. We first enhance our bounds for the weights $\mathrm{wt}_g(2b,b)$ for non-symmetric polynomials with $m = 2b$.

Corollary 10: Let equalities (4) be satisfied for distance $d_{r-1}(2b-1,b-1)$. Then any non-symmetric polynomial g gives on the sphere S_b^{2b} the codeword of weight

$$\mathrm{wt}_g(2b,b) \geq \binom{2b-r}{b}. \qquad (14)$$

Proof: For any polynomial $g(x)$, the polynomial $g(x) + g(\overline{x})$ generates vector $v \neq 0$ in representation (13). Thus,

$$\mathrm{wt}_g(2b,b) \geq \mathrm{wt}(v) \geq d_{r-1}(2b-1,b-1) = \binom{2b-r}{b}.$$

■

We now proceed with $m = 2b+1$.

Lemma 11: Let equalities (4) be satisfied for distances $d_\rho(2b,\beta)$ for $\rho = r-1, r$ and $\beta = b-1, b$. Then for any non-symmetric polynomial $g \in F(2b,r)$,

$$\mathrm{wt}_g(2b+1,b) \geq \binom{2b+1-r}{b+1}.$$

Proof: By Corollary 10, $\mathrm{wt}_g(2b,b) \geq \binom{2b-r}{b}$. We then follow the proof of Lemma 7 using the induction hypothesis. Namely, if g belongs to one of the null-spaces $\mathcal{N}_r(2b,b)$ or $\mathcal{N}_r(2b,b-1)$, we can apply Theorem 5 along with equalities (4). Then

$$\mathrm{wt}_g(2b+1,b) \geq \min\{d_{r-1}(2b,b), d_{r-1}(2b,b-1)\} = \binom{2b+1-r}{b+1}$$

Otherwise, we again use bound (14) and obtain the same estimate

$$\mathrm{wt}_g(2b+1,b) \geq \mathrm{wt}_g(2b,b) + d_r(2b,b-1) \geq \binom{2b-r}{b} + \binom{2b-r}{b+1} = \binom{2b+1-r}{b+1} \qquad (15)$$

■

Finally, we complete the proof of Theorem 4 in the following Lemma. Here we study symmetric polynomials for $m = 2b$ and consider several cases. The main idea is to apply multiple two-level decompositions using all m variables $x_1, ..., x_m$. In essence, some decompositions will always involve Plotkin construction for all nontrivial cases.

Lemma 12: Let equalities (4) hold for distances $d_\rho(\mu,\beta)$ where $\rho \leq r$, $\beta \leq b$, and $\mu \leq 2b$. Then for any symmetric polynomial f,

$$\mathrm{wt}_f(2b+1,b) \geq \binom{2b+1-r}{b+1}.$$

Proof: Fig. 1 shows a two-level partition of the sphere S_b^{2b+1}. The first partition splits S_b^{2b+1} into two spheres S_b^{2b} and S_{b-1}^{2b}, depending on the value of $x_{2b+1} = 0, 1$. The second

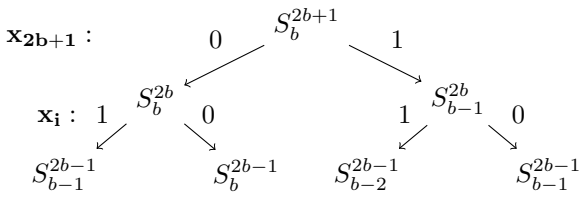

Fig. 1. Decomposition of S_b^{2b+1}

partition uses any other coordinate x_i for $i \in [1, 2b]$. The overall result is 4 hemispheres S_j^i, $j \in [1, 4]$:

$$\underbrace{x \in S_b^{2b} : x_i = 1}_{S_1^i} \quad | \quad \underbrace{x \in S_b^{2b} : x_i = 0}_{S_2^i} \quad |$$
$$\underbrace{x \in S_{b-1}^{2b} : x_i = 1}_{S_3^i} \quad | \quad \underbrace{x \in S_{b-1}^{2b} : x_i = 0}_{S_4^i}$$

Given a symmetric polynomial f, consider 4 vectors $u_j^i = (\dots, f(x), \dots)$ as $x \in S_j^i$. We first show that any codeword of $P_r(2b+1, b)$ can be represented as

$$[\quad u_1^i \quad | \quad u_1^i \quad | \quad u_3^i \quad | \quad u_1^i + v^i \quad], \tag{16}$$

where $u_1^i \in P_r(2b-1, b-1)$, $u_3^i \in P_r(2b-1, b-2)$, $v^i \in P_{r-1}(2b-1, b-1)$.

First, note that $\overline{x} \in S_2^i$ if $x \in S_1^i$. Thus, $u_1^i = u_2^i$ (up to permutation) for any $i \in [1, 2b]$ and any symmetric polynomial $f(x) = f(\overline{x})$. Next, let $e_i \in \mathbb{F}_2^{2b}$ be the vector that has 1 in position i only. For any $x \in S_1^i$, $x + e_i \in S_4^i$. Also, note that any polynomial

$$v_i(x) = f(x) + f(x + e_i)$$

is the derivative $\partial f / \partial x_i$ of $f(x)$ in the direction e_i and has $\deg(g_i(x)) \le r - 1$. Then vector $u_4^i = u_1^i + v^i$ includes $v^i \in P_{r-1}(2b-1, b-1)$. Thus, we have representation (16).

In the next part of the proof, we consider codewords (16) and study two different cases.

A. $v^i \equiv 0 \mid S_{b-1}^{2b-1}$ for all $i \in [1, 2b]$. Note that in this case $f(x) = const$ on S_b^{2b}. Indeed, consider any two points $x, y \in S_b^{2b}$ that disagree in two positions i and j and have symbols $x_i = y_j = 1$. Then

$$f(y) - f(x) = v^i + v^j = 0$$

More generally, consider step-by-step replacement of b ones in x with b ones in y. Each of b (or fewer) replacements moves the current point x from S_b^{2b} to S_{b-1}^{2b-1} and back onto S_b^{2b}. Now we see that $f(y) \equiv f(x) \mid S_b^{2b}$ since all changes $g_i(x)$ generate vectors $v^i \equiv 0 | S_b^{2b}$. Since $f(x) + const \equiv 0 \mid S_b^{2b}$, we proceed with Theorem 5 and obtain codewords $f \in P_{r-1}(2b, b-1)$ on the other sphere S_{b-1}^{2b}. Thus,

$$\mathrm{wt}_f(2b+1, b) \ge \binom{2b+1-r}{b+1}. \tag{17}$$

B. Let $v^i \neq 0$ for some $i \in [1, 2b]$. This gives 3 sub-cases.

$\mathbf{B}_1$. If $u_1^i = 0$, then $f \in \mathcal{N}_r(2b, b)$ and Theorem 5 gives

$$\mathrm{wt}_f(2b+1, b) \ge \mathrm{wt}_f(2b, b-1)$$
$$\ge d_{r-1}(2b, b-1) = \binom{2b+1-r}{b+1}$$

$\mathbf{B}_2$. For $u_1^i \neq 0$ and $u_3^i \neq 0$, induction hypothesis gives

$$\mathrm{wt}_f(2b+1, b) \ge \mathrm{wt}(v^i) + \mathrm{wt}(u_1^i) + \mathrm{wt}(u_3^i)$$
$$\ge \binom{2b-r}{b} + \binom{2b-1-r}{b} + \binom{2b-1-r}{b+1}$$

$\mathbf{B}_3$. If $u_1^i \neq 0$ and $u_3^i = 0$, then $f \in \mathcal{N}_r(2b-1, b-2)$. According to Theorem 5, f acts as a polynomial of degree at most $r-1$ on S_1^i. Then the two blocks u_1^i, u_1^i give weight

$$2\mathrm{wt}_f(2b-1, b-1) \ge 2\binom{2b-r}{b-r} \tag{18}$$

Now Lemma 12 follows from the estimates (17)- (18). ■

V. Concluding remarks

This paper presents a new class of spherically-punctured RM codes $P_r(m, b)$. We also study recursive properties of these codes and define their parameters. As an open problem, note [6] that any codeword in a spherically-punctured biorthogonal code $P_1(m, b)$ has weight that only depends on the weight of its information block. As a result, we can use precoding of information blocks in codes $P_1(m, b)$ and produce some high-distance codes that even meet the Griesmer bound. One interesting problem is to use a similar precoding and increase code distance in general codes $P_r(m, b)$. Note also that spherical constructions include many equal-weight parity checks. It would be interesting to design good decoding algorithms that combine message-passing properties of these parity checks with recursive structure of spherical RM constructions.

Acknowledgment

Research was supported by NSF grant ECCS 1102074 and ARO grant W911NF-11-1-0027.

References

[1] D. H. Gottlieb, "A certain class of incidence matrices," *Proc. Amer. Math. Soc.*, vol. 17, pp. 1233-1237, 1966.
[2] F.J. MacWilliams and N.J.A. Sloane, *"The Theory of Error-Correcting Codes,"* North-Holland, Amsterdam, 1981.
[3] R. M. Wilson, "A diagonal form for the incidence matrices of t-subsets vs k-subsets," *European J. of Combinatorics,* vol. 11, pp. 609-615, 1990.
[4] I. Dumer, "Recursive decoding and its performance for low-rate Reed-Muller codes", *IEEE Trans. Inform. Theory*, vol. 50:5, pp. 811-823, 2004.
[5] E. Arıkan, "Channel polarization: A method for constructing capacity achieving codes for symmetric binary-input memoryless channels," *IEEE Trans. Inform. Theory*, vol. 55:9, pp. 3051–3073, 2009.
[6] I. Dumer and O. Kapralova, "Spherically punctured biorthogonal codes", *Proc. ISIT 2012*, Cambridge, MA, USA, pp. 264-268.