Next, since $\frac{3n}{7} \le \frac{n-1}{2}$ for $n \ge 7$ and $H_2(\frac{1}{10}) < \frac{3}{7}$, one obtains

$$\sum_{i=0}^{t+1} \binom{n}{i} \le 2^{nH_2(\frac{1}{10})} < 2^{\frac{3n}{7}} \le 2^{\frac{n-1}{2}}. \qquad \square$$

The $(103, 52, 19)$ QR code satisfies the conditions of Lemma 4. Hence, it also is not a quasi-perfect code.

Proof of Theorem 1: From Lemmas 1 and 2 one has

$$d \le 4\left\lfloor \frac{n+1}{24} \right\rfloor + 3 \le \frac{n+1}{6} + 3$$

for the binary QR code $(n, \frac{n+1}{2}, d)$ of length $n = 8m - 1$. It follows that $d < n/5 - 1$ for all $n \ge 125$. Hence, by Lemma 4 the conclusion of Theorem 1 follows. $\square$

Thus, it has been shown that no binary quadratic residue code of length $n = 8m - 1$ is quasi-perfect.

The results in Theorem 1 can be generalized to binary self-dual codes. Conway and Sloane [6] proved the following lemma for binary self-dual codes.

Lemma 5: The minimal distance $d_{\min}$ of a binary self-dual code of length n satisfies

$$d_{\min} \le 2\left\lfloor \frac{n+6}{10} \right\rfloor \tag{4}$$

for $n > 72$.

By using Lemma 5 one can obtain the following corollary.

Corollary 2: No binary self-dual code $(n, \frac{n}{2}, d_{\min})$ is quasi-perfect for $n > 72$.

This corollary of Theorem 1 is proved by the same methods used above in the proofs of Lemma 4 and Theorem 1.

For the class of binary QR code of length $n = 8m+1$, it is known [1] that the $(17, 9, 5)$ QR code is quasi-perfect. However, all other codes of this class which are listed in Fig. 15.02 of [7] are not quasi-perfect, as can be verified by a use of Proposition 1 and Lemma 4. One may thus conjecture that no t-error-correcting binary QR code of length $n = 8m + 1$ with $t > 2$ is quasi-perfect.

Acknowledgment

The authors would like to thank Dr. Z. Zhang for his helpful suggestion about the proof of Lemma 4 in the first version. The author also would like to thank the referee A for several valuable comments, and also referee B for his suggestions that led to a considerable simplification of the proof of Lemma 4.

References

[1] W. W. Peterson and E. J. Weldon, Jr., *Error-Correcting Codes.* Cambridge, MA: The M.I.T. Press, 1972, 2nd ed.

[2] T. Helleseth, "All binary 3-error-correcting BCH codes of length $2^m - 1$ have covering radius 5," *IEEE Trans. Inform. Theory*, vol. IT-24, pp. 257–258, Mar. 1978.

[3] R. L. Graham and N. J. A. Sloane, "On the covering radius of codes," *IEEE Trans. Inform. Theory*, vol. IT-31, pp. 385–401, May 1985.

[4] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes.* Amsterdam, The Netherlands: North-Holland, 1977.

[5] C. L. Mallows and N. J. A. Sloane, "An upper bound for self-dual codes," *Inform. Contr.*, vol. 22, pp. 188–200, 1973.

[6] J. H. Conway and N. J. A. Sloane, "A new upper bound on the minimal distance of self-dual codes," *IEEE Trans. Inform. Theory*, vol. 36, pp. 1319–1333, Nov. 1990.

[7] E. R. Berlekamp, *Algebraic Coding Theory.* New York: McGraw–Hill, 1968.

Some New Constructions for Simplex Codes

Hong Y. Song and Solomon W. Golomb

***Abstract*—Three constructions for n-dimensional regular simplex codes α_i, $0 \le i \le n$, are proposed, two of which have the property that α_i for $1 \le i \le n$ is a cyclic shift of α_1. The first method is shown to work for all the positive integers $n = 1, 2, \cdots$ using only three real values. It turns out that these values are rational whenever $n + 1$ is a square of some integer. Whenever a (v, k, λ) cyclic (or Abelian) difference set exists, this method is generalized so that a similar method is shown to work with $v = n$ (the number of dimensions).**

***Index Terms*—Regular simplex codes, cyclic difference sets.**

I. Introduction

In an n-dimensional Euclidean space, for any positive integer n, an *n-dimensional simplex* (or, n-simplex) is the convex body spanned by any $n + 1$ distinct points in general position. An n-simplex is *regular* if all $\binom{n+1}{2}$ edges (the lines connecting pairs of vertices) have the same length. It is known [1] that there is a regular n-simplex for all $n \ge 1$. It is also known [1] that for all $n \ge 5$, there are exactly *three* regular hypersolids in n-dimensional Euclidean space: the regular simplex, the hypercube, and the *cross-polytope.* It is easy to describe a set of vertices for the n-dimensional hypercube [namely, all 2^n point vectors of the form $(\pm1, \pm1, \pm1, \cdots, \pm1)$], and a set of vertices for the n-dimensional cross-polytope [namely, all $2n$ point vectors of the form $(\pm1, 0, 0, \cdots, 0)$, $(0, \pm1, 0, \cdots, 0)$, $(0, 0, \pm1, \cdots, 0), \cdots, (0, 0, 0, \cdots, \pm1)$]. However, it is not easy in general to describe a set of vertices for the n-simplex for all positive integers n.

The codes corresponding to the vertices of the three regular polytopes in n-dimensional space have been studied for their communications applications (see the references in [9]) under various channel assumptions. In communication environments where only white Gaussian noise is present and where the receiver operates synchronously in time and phase, it is most desirable [2], [9], [10] that the signals employed be as far apart as possible. In this sense, it is known [9] that *the code corresponding to the vertices of a regular n-simplex is the only one which maximizes the minimum distance between the pairs of vertices among all sets of n+1 equal energy points in n-dimensional space*. Since the exact bit error probability is also a function of SNR (ratio of signal energy-to-noise spectral density), the above condition does not guarantee the global optimality of the regular n-simplex code for all possible values of SNR. It is known, however, that the n-simplex code gives a local minimum bit error probability at every SNR, and gives the absolute minimum for both "sufficiently small" SNR and "sufficiently large" SNR [9].

To our knowledge, the first systematic representation, for all $n = 1, 2, \cdots$, of the $n + 1$ vertices of a regular n-simplex was given by J. Max in [5]. However, this method uses at least n distinct real values, and does not have any "symmetry" among the $n + 1$ vectors corresponding to the vertices. Whenever a Hadamard matrix of order $n + 1$ exists, there is a *binary* simplex code of *ones* and

Manuscript received November 4, 1992; revised May 6, 1993. This work was supported in part by the United States Office of Naval Research under Grant Number N00014-90-J-1341.

The authors are with the Department of EE–Systems, Communication Sciences Institute, University of Southern California, Los Angeles, CA 90089 USA.

IEEE Log Number 9215440.

minus ones of length n, but for these to exist the order $n+1$ must be 1, 2 or a multiple of 4 [3, 6, 8]. These binary simplex codes are easy to generate (when they exist), but the existence for all multiples of 4 is not yet proved. The order $n+1=428$ is the smallest order for which the existence of a Hadamard matrix of order $n+1$ is not yet known [7].

The purpose of this note is to exhibit two simple ways of assigning coordinates to the $n+1$ vertices of the regular n-simplex (Section II). Each method constructs $n+1$ vectors α_i for $0 \le i \le n$ of length n having the property that α_i for $1 \le i \le n$ is a cyclic shift of α_1. The first method is shown to work for all positive integers n, using only three real values in each case. As an interesting application of (v, k, λ) cyclic difference sets [3, 6, 8], this method is generalized so that a similar method is shown to work whenever a (v, k, λ) cyclic difference set exists with $v = n$. This method is further generalized to work (Section III) whenever an Abelian difference set exists. In this case, the cyclic nature of the vectors is lost but some symmetry remains.

II. Constructions for Simplex Codes

Let $\alpha_0, \alpha_1, \cdots, \alpha_n$ be $n+1$ unit vectors in n-dimensional Euclidean space representing the vertices of a regular simplex. Then, for every pair $\alpha_i = (a_1, a_2, \cdots, a_n)$ and $\alpha_j = (b_1, b_2, \cdots, b_n)$, the dot product $(\alpha_i, \alpha_j) = \sum_{k=1}^{n} a_k b_k$ must satisfy [9], [10]

$$(\alpha_i, \alpha_j) = \frac{-1}{n}, \qquad 0 \le i < j \le n \tag{2.1}$$

$$= 1, \qquad 0 \le i = j \le n. \tag{2.2}$$

Conversely, any set of $n+1$ unit vectors in n-dimensional Euclidean space satisfying the above condition on the dot product for every pair of vertices represents the $n+1$ vertices of a regular n-simplex [9], [10].

Theorem 2.1: Take the following $n+1$ unit vectors:

$$\begin{aligned}\alpha_0 &= \frac{1}{\sqrt{n}}(1, 1, 1, \cdots, 1),\\ \alpha_1 &= \frac{1}{\sqrt{n}}(-a, b, b, \cdots, b),\\ \alpha_2 &= \frac{1}{\sqrt{n}}(b, -a, b, \cdots, b),\\ &\vdots \qquad \ddots \quad \ddots \quad \ddots\\ \alpha_n &= \frac{1}{\sqrt{n}}(b, b, b, \cdots, -a)\end{aligned}$$

where α_i for $2 \le i \le n$ is a cyclic shift of α_1, and where the real numbers a and b are given by

$$(a, b) = \left(\frac{1 \pm (n-1)\sqrt{n+1}}{n}, \frac{-1 \pm \sqrt{n+1}}{n}\right). \tag{2.3}$$

For each positive integer $n = 1, 2, \cdots$, the above scheme locates the $n+1$ vertices of an n-dimensional regular simplex on the unit hypersphere. If, in addition, $n+1 = m^2$ for some integer m, then a and b are rational, with

$$(a, b) = \left(\frac{m^2+m-1}{m+1}, \frac{1}{m+1}\right)$$

or

$$\left(\frac{-m^2+m+1}{m-1}, \frac{-1}{m-1}\right).$$

$$\begin{aligned}
\alpha_0 &= \tfrac{1}{\sqrt{8}}(\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ )\\
\alpha_1 &= \tfrac{1}{\sqrt{8}}(\ -\ +\ +\ +\ +\ +\ +\ +\ )\\
\alpha_2 &= \tfrac{1}{\sqrt{8}}(\ +\ -\ +\ +\ +\ +\ +\ +\ )\\
\alpha_3 &= \tfrac{1}{\sqrt{8}}(\ +\ +\ -\ +\ +\ +\ +\ +\ )\\
\alpha_4 &= \tfrac{1}{\sqrt{8}}(\ +\ +\ +\ -\ +\ +\ +\ +\ )\\
\alpha_5 &= \tfrac{1}{\sqrt{8}}(\ +\ +\ +\ +\ -\ +\ +\ +\ )\\
\alpha_6 &= \tfrac{1}{\sqrt{8}}(\ +\ +\ +\ +\ +\ -\ +\ +\ )\\
\alpha_7 &= \tfrac{1}{\sqrt{8}}(\ +\ +\ +\ +\ +\ +\ -\ +\ )\\
\alpha_8 &= \tfrac{1}{\sqrt{8}}(\ +\ +\ +\ +\ +\ +\ +\ -\ )
\end{aligned}$$

Fig. 1. Vertices of a regular 8-simplex given by the construction in Theorem 2.1. Here, "$-$" represents $-a$ and "$+$" represents $+b$ where $(a, b) = (11/4, 1/4)$ or $(-5/2, -1/2)$.

Proof: From (2.1) and (2.2), we have the following system of three equations:

$$(\alpha_0, \alpha_i) = \frac{1}{n}(-a + (n-1)b) = -\frac{1}{n} \qquad \text{for } 1 \le i \le n,$$

$$(\alpha_i, \alpha_j) = \frac{1}{n}(-2ab + (n-2)b^2) = -\frac{1}{n} \qquad \text{for } 1 \le i < j \le n,$$

$$(\alpha_i, \alpha_i) = \frac{1}{n}(a^2 + (n-1)b^2) = 1 \qquad \text{for } 1 \le i \le n.$$

Solving the above system of equations yields the values of a and b given in (2.3). □

As an example, we show 9 unit vectors in Fig. 1 which are the vertices of a regular simplex in 8-dimensional space. In this example, we have $(a, b) = (11/4, 1/4)$ or $(-5/2, -1/2)$.

A (v, k, λ) cyclic difference set $D = \{s_1, s_2, \cdots, s_k\}$ is a set of k residues $\bmod\, v$ such that for each nonzero residue $d \bmod v$ there exist λ solutions (x, y) to the equation $x - y \equiv d \pmod{v}$. A simple counting argument shows that

$$k(k-1) = \lambda(v-1) \tag{2.4}$$

is a necessary condition for the existence of a (v, k, λ) cyclic difference set [3], [6], [8]. The construction in Theorem 2.1 comes from a trivial difference set with parameters $k = 1$, $\lambda = 0$, (thus, $k - \lambda = 1$), and is a special case of the following.

Theorem 2.2: Assume there exists a (v, k, λ) cyclic difference set D and take

$$\begin{aligned}\alpha_0 &= \frac{1}{\sqrt{v}}(1, 1, 1, \cdots, 1),\\ \alpha_1 &= \frac{1}{\sqrt{v}}(\beta_1, \beta_2, \beta_3, \cdots, \beta_v),\\ \alpha_2 &= \frac{1}{\sqrt{v}}(\beta_v, \beta_1, \beta_2, \cdots, \beta_{v-1}),\\ &\vdots \qquad \ddots \quad \ddots \quad \ddots\\ \alpha_v &= \frac{1}{\sqrt{v}}(\beta_2, \beta_3, \beta_4, \cdots, \beta_1)\end{aligned}$$

where $\beta_j = -a$ if $j \in D$, and $\beta_j = b$ if $j \notin D$, and where $\alpha_2, \cdots, \alpha_v$ are all the other cyclic shifts of α_1, and where the real numbers a and b are given by

$$a = \frac{1}{v} \pm \frac{v-k}{v}\sqrt{\frac{v+1}{k-\lambda}} \quad \text{and} \quad b = \frac{-1}{v} \pm \frac{k}{v}\sqrt{\frac{v+1}{k-\lambda}}. \tag{2.5}$$

Then, the $v+1$ vectors $\alpha_0, \alpha_1, \cdots, \alpha_v$ locate the $v+1$ vertices of a v-dimensional regular simplex on the unit hypersphere.

Proof: From (2.1) and (2.2), we have the following system of three equations:

$$(\alpha_i, \alpha_i) = \frac{1}{v}(ka^2 + (v-k)b^2) = 1 \qquad \text{for } 1 \le i \le n,$$

$$(\alpha_0, \alpha_i) = \frac{1}{v}(-ka + (v-k)b) = \frac{-1}{v} \qquad \text{for } 1 \le i \le n,$$

$$(\alpha_i, \alpha_j) = \frac{1}{v}(\lambda a^2 - 2(k-\lambda)ab + (v - 2k + \lambda)b^2) = \frac{-1}{v} \qquad \text{for } 1 \le i < j \le n.$$

The first two simultaneous equations have two pairs of real roots a and b which can be expressed as shown in (2.5) using the relation $v^2 - 1 = \frac{k(v-k)(v+1)}{k-\lambda}$. Multiplying both sides of the third equation by v^3, one can rewrite it as

$$\lambda(va)^2 - 2(k-\lambda)(va)(vb) + (v-2k+\lambda)(vb)^2 + v^2 = 0. \quad (2.6)$$

If we substitute $(va)^2$, $(vb)^2$, and v^2ab into (2.6) where

$$(va)^2 = 1 + (v-k)^2\frac{v+1}{k-\lambda} \pm 2(v-k)\sqrt{\frac{v+1}{k-\lambda}},$$

$$(vb)^2 = 1 + k^2\frac{v+1}{k-\lambda} \mp 2k\sqrt{\frac{v+1}{k-\lambda}},$$

$$(v^2ab) = -1 + k(v-k)\frac{v+1}{k-\lambda} \pm k\sqrt{\frac{v+1}{k-\lambda}} \mp (v-k)\sqrt{\frac{v+1}{k-\lambda}},$$

then the left-hand side of (2.6) takes the form $R + S\sqrt{\frac{v+1}{k-\lambda}}$ where R and S denote the rational parts. Then,

$$S = \pm 2\lambda(v-k) \mp 2(k-\lambda)k \pm 2(k-\lambda)(v-k) \mp 2k(v-k) \pm 2k(k-\lambda) = 0, \quad \text{and}$$

$$\begin{aligned} R &= \lambda\left[1 + (v-k)^2\frac{v+1}{k-\lambda}\right] - 2(k-\lambda)\left[-1 + k(v-k)\frac{v+1}{k-\lambda}\right] \\ &\quad + (v-2k+\lambda)\left[1 + k^2\frac{v+1}{k-\lambda}\right] + v^2 \\ &= \frac{v+1}{k-\lambda}[\lambda v(v-1) - vk^2 + vk], \end{aligned}$$

which must also be zero by (2.4). □

For the rest of this note, let n denote $k - \lambda$, following the standard notation [3] of cyclic difference sets. Then, it is not hard to show that $4n - 1 \le v \le n^2 + n + 1$ for any (v, k, λ) cyclic difference set D. From these inequalities, one has

$$4 \le \frac{v+1}{n} \le n + 1 + \frac{2}{n} < n + 2. \quad (2.7)$$

When $\frac{v+1}{n} = 4$, D is called a cyclic *Hadamard* difference set and it has parameters $v = 4n - 1$, $k = 2n - 1$, and $\lambda = n - 1$. In this case, the values of a and b are rational, with

$$(a, b) = (-1, -1) \qquad \text{or} \qquad \left(\frac{4n+1}{4n-1}, \frac{4n-3}{4n-1}\right).$$

Note that the first choice corresponds to the $v+1$ binary simplex codes of *ones* and *minus ones* of length v and also to the cyclic *Hadamard matrix* of order $v + 1 = 4n$. When $\frac{v+1}{n} = n + 1 + \frac{2}{n}$, D is called a cyclic *planar* difference set and has parameters $v = n^2 + n + 1$, $k = n + 1$, and $\lambda = 1$. In this case,

$$a = \frac{1 \pm n^2\sqrt{n + 1 + \frac{2}{n}}}{n^2 + n + 1},$$

and

$$b = \frac{-1 \pm (n+1)\sqrt{n + 1 + \frac{2}{n}}}{n^2 + n + 1}$$

which can never be rational unless $n = 1$ [trivial] or $n = 2$ [this is equivalent to the (7, 3, 1) cyclic Hadamard difference set]. As an example, we show 8 unit vectors in Fig. 2 which are the vertices of a regular simplex in 7-dimensional space. This is from the (7, 3, 1) cyclic difference set $D = \{1, 2, 4\}$. In this example, we have $(a, b) = (-1, -1)$ or $(9/7, 5/7)$.

$$\begin{array}{lcl} \alpha_0 &=& \frac{1}{\sqrt{7}}(\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ ) \\ \alpha_1 &=& \frac{1}{\sqrt{7}}(\ -\ -\ +\ -\ +\ +\ +\ ) \\ \alpha_2 &=& \frac{1}{\sqrt{7}}(\ +\ -\ -\ +\ -\ +\ +\ ) \\ \alpha_3 &=& \frac{1}{\sqrt{7}}(\ +\ +\ -\ -\ +\ -\ +\ ) \\ \alpha_4 &=& \frac{1}{\sqrt{7}}(\ +\ +\ +\ -\ -\ +\ -\ ) \\ \alpha_5 &=& \frac{1}{\sqrt{7}}(\ -\ +\ +\ +\ -\ -\ +\ ) \\ \alpha_6 &=& \frac{1}{\sqrt{7}}(\ +\ -\ +\ +\ +\ -\ -\ ) \\ \alpha_7 &=& \frac{1}{\sqrt{7}}(\ -\ +\ -\ +\ +\ +\ -\ ) \end{array}$$

Fig. 2. Vertices of a regular 7-simplex given by the construction in Theorem 2.2. Here, "$-$" represents $-a$ and "$+$" represents $+b$ where $(a, b) = (-1, -1)$ or $(9/7, 5/7)$.

If $\frac{v+1}{n}$ is the square of an integer, then the values of a and b in Theorem 2.2 are rational. Equation (2.7) implies that $\frac{v+1}{n}$ can have values m^2 for $4 \le m^2 \le n + 1$. Except for the cyclic Hadamard difference sets in which $\frac{v+1}{n} = 2^2$ for all positive integers $n > 2$, it turned out that, for $2 \le n \le 343$, there are only two possible sets of parameters (v, k, λ), which are (377, 48, 6) and (2911, 195, 13), and their complements, for which (1) $\frac{v+1}{n}$ is the square of an integer and (2) both k and λ come out as integers. However, one can easily rule out the existence of both the (377, 48, 6) and (2911, 195, 13) cyclic difference sets (and hence, of their complements as well) by the *multiplier theorem* and its consequences [3, 6, 8]. Nonexistence of (v, k, λ) cyclic difference sets for which $\frac{v+1}{k-\lambda}$ is the square of an integer, except for the cyclic Hadamard difference sets, is still unsettled for $n \ge 344$.

III. Generalization to Abelian Difference Sets

A further generalization of the previous methods to "Abelian difference sets" is quite straightforward and can be done easily. All the terminologies and basic results on abelian difference sets in the following are from standard texts, e.g., [3, 6, 8]. Let G be an abelian group of order v. A (v, k, λ) difference set in G is a k-subset D of G such that for each nonzero element $g \in G$ there exist λ solutions

$G = Z_2 \times Z_2 \times Z_2 \times Z_2 = \{g_i | i = 1, 2, \ldots, 16\}$

$D = \{0000, 1000, 0100, 0010, 0001, 1111\}$

$= \{1, 2, 3, 4, 5, 16\}$ as a set of indices

i	g_i	position =	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
		$4\alpha_0$ =	(1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1)
1	0000	$4\alpha_1$ =	(−	−	−	−	−	+	+	+	+	+	+	+	+	+	+	−)
2	1000	$4\alpha_2$ =	(−	−	+	+	+	−	+	+	−	−	+	−	+	+	+	+)
3	0100	$4\alpha_3$ =	(−	+	−	+	+	−	−	+	+	+	−	+	−	+	+	+)
4	0010	$4\alpha_4$ =	(−	+	+	−	+	+	−	−	+	−	+	+	+	−	+	+)
5	0001	$4\alpha_5$ =	(−	+	+	+	−	+	+	−	−	+	−	+	+	+	−	+)
6	1100	$4\alpha_6$ =	(+	−	−	+	+	−	+	−	+	+	+	+	+	−	−	+)
7	0110	$4\alpha_7$ =	(+	+	−	−	+	+	−	+	−	+	+	−	+	+	−	+)
8	0011	$4\alpha_8$ =	(+	+	+	−	−	−	+	−	+	+	+	−	−	+	+	+)
9	1001	$4\alpha_9$ =	(+	−	+	+	−	+	−	+	−	+	+	+	−	−	+	+)
10	1010	$4\alpha_{10}$ =	(+	−	+	−	+	+	+	+	+	−	−	+	−	+	−	+)
11	0101	$4\alpha_{11}$ =	(+	+	−	+	−	+	+	+	+	−	−	−	+	−	+	+)
12	0111	$4\alpha_{12}$ =	(+	−	+	+	+	+	−	−	+	+	−	−	+	+	+	−)
13	1011	$4\alpha_{13}$ =	(+	+	−	+	+	+	+	−	−	−	+	+	−	+	+	−)
14	1101	$4\alpha_{14}$ =	(+	+	+	−	+	−	+	+	−	+	−	+	+	−	+	−)
15	1110	$4\alpha_{15}$ =	(+	+	+	+	−	−	−	+	+	−	+	+	+	+	−	−)
16	1111	$4\alpha_{16}$ =	(−	+	+	+	+	+	+	+	+	+	+	−	−	−	−	−)

Fig. 3. Vertices α_j of a regular 16-simplex by the rule $\beta_{i,j} = -a$ if $g_j \in D + g_i$ and $\beta_{i,j} = b$ if $g_j \notin D + g_i$ where $\alpha_i = \frac{1}{\sqrt{v}}(\beta_{i,1}, \beta_{i,2}, \beta_{i,3}, \cdots, \beta_{i,v})$ for $i = 1, \cdots, v$, and where D is a (16, 6, 2) difference set in an abelian group G. Here, "−" represents $-a$ and "+" represents $+b$ where $(a, b) = \left(\frac{1 \pm 4\sqrt{17}}{16}, \frac{-1 \pm 3\sqrt{17}}{16}\right)$.

(x, y) where $x, y \in D$ to the equation $x - y = g$. Abelian difference sets are known to exist for $(v, k, \lambda) = (4u^2, 2u^2 \pm u, u^2 \pm u)$ whenever $u = 2^r 3^s$ where r and s are arbitrary nonnegative integers [4].

Assuming there exists a (v, k, λ) difference set D in an abelian group $G = \{g_1 = \text{identity}, g_2, g_3, \cdots, g_v\}$ of order v, take the following $v + 1$ unit vectors of dimension v:

$$\alpha_0 = \frac{1}{\sqrt{v}}(1, 1, 1, \cdots, 1),$$

$$\alpha_i = \frac{1}{\sqrt{v}}(\beta_{i,1}, \beta_{i,2}, \beta_{i,3}, \cdots, \beta_{i,v}), \quad \text{for } i = 1, 2, \cdots, v$$

where $\beta_{i,j} = -a$ if $g_j - g_i \in D$, and $\beta_{i,j} = b$ if $g_j - g_i \notin D$, and where a and b are also given by (2.5). Then, the $v + 1$ unit vectors $\alpha_0, \alpha_1, \cdots, \alpha_v$ locate the $v + 1$ vertices of a v-dimensional regular simplex on the unit hypersphere.

For the proof of this method, one needs to note that the family of v subsets $D + g_i \subset G$ of size k for $i = 1, 2, \cdots, v$ forms a *symmetric* $2 - (v, k, \lambda)$ *balanced incomplete block design* [6], [3], [8]. Here, the underlying group G is the point set of size v and the incidence structure is the set-membership. Furthermore, note that the positions of α_i (except for α_0) into which we put $-a$ are the indexes j of $g_j \in G$ such that $g_j \in D + g_i$. Since each block $D + g_i$ contains k elements, we have

$$(\alpha_i, \alpha_i) = \frac{1}{v}(ka^2 + (v - k)b^2) \quad \text{for } 1 \le i \le n,$$

$$(\alpha_0, \alpha_i) = \frac{1}{v}(-ka + (v - k)b) \quad \text{for } 1 \le i \le n.$$

The value of (α_i, α_j) for $1 \le i < j \le n$ can easily be computed by the property of the symmetric BIBD [3], [6], [8] that any two elements of G are members of exactly λ blocks [or equivalently, any two blocks have exactly λ elements in common]. Therefore, in the summation $\beta_{i,1}\beta_{j,1} + \beta_{i,2}\beta_{j,2} + \cdots + \beta_{i,v}\beta_{j,v}$, the term $(-a)^2$ occurs λ times, the term $-ab$ occurs $2(k - \lambda)$ times, and finally, the term b^2 occurs $(v - 2k + \lambda)$ times. This proves

$$(\alpha_i, \alpha_j) = \frac{1}{v}(\lambda a^2 - 2(k - \lambda)ab + (v - 2k + \lambda)b^2) \quad \text{for } 1 \le i < j \le n.$$

Now, the rest follows easily as in the Proof of Theorem 2.2.

As an example, we show 17 unit vectors in Fig. 3 which are the vertices of a regular simplex in 16-dimensional space. This is from a (16, 6, 2) difference set

$$D = \{(0000), (1000), (0100), (0010), (0001), (1111)\}$$

in an Abelian group $Z_2 \times Z_2 \times Z_2 \times Z_2$ of order 16. In this example, we have $(a, b) = \left(\frac{1 \pm 5\sqrt{17}}{16}, \frac{-1 \pm 3\sqrt{17}}{16}\right)$. Note that the 16×16 matrix of +'s and −'s corresponding to the components of $\alpha_1, \alpha_2, \cdots, \alpha_{16}$ is indeed the incidence matrix of a symmetric (16, 6, 2) BIBD, and that it is symmetric along the diagonal.

ACKNOWLEDGMENT

The authors are grateful to the anonymous referees for bringing [4] to their attention and for helpful comments on generalizing the methods to Abelian difference sets.

REFERENCES

[1] H. S. M. Coxeter, *Regular Polytopes.* New York: Dover, 1973, 3rd ed.

[2] S. W. Golomb, Ed., *Digital Communications with Space Applications.* Englewood Cliffs, NJ: Prentice-Hall, 1964; also, Peninsula Publishing Company, Los Altos, CA, 1981.

[3] M. Hall, Jr., *Combinatorial Theory.* New York: Wiley, 1986, 2nd ed.

[4] D. Jungnickel, "Difference sets," in *Contemporary Design Theory—A Collection of Surveys*, J. H. Dinitz and D. R. Stinson, Eds. New York: 1992, pp. 241–324.

[5] J. Max, "Signal sets with uniform correlation properties," *J. Soc. Indust. Appl. Math.*, vol. 10, no. 1, pp. 113–118, Mar. 1962.

[6] H. J. Ryser, "Combinatorial mathematics," in *The Carus Mathematical Monographs No. 14.* New York: Wiley, 1963.

[7] J. Seberry and M. Yamada, "Hadamard matrices, sequences, and block designs,"in *Contemporary Design Theory—A Collection of Surveys*, J. H. Dinitz and D. R. Stinson, Eds. New York: Wiley, 1992, pp. 431–560.

[8] J. H. van Lint and R. M. Wilson, *A Course in Combinatorics.* Cambridge, UK: Cambridge Univ. Press, 1992.

[9] C. L. Weber, *Elements of Detection and Signal Design.* New York: Springer-Verlag, 1987.

[10] J. M. Wozencraft and I. M. Jacobs, *Principles of Communication Engineering.* New York: Wiley, 1967.