PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 85, Number 3, July 1982

HADAMARD MATRICES AND δ-CODES OF LENGTH $3n$

C. H. YANG[1]

ABSTRACT. It is found that four-symbol δ-codes of length $t = 3n$ can be composed for odd $n \leq 59$ or $n = 2^a 10^b 26^c + 1$, where all a, b and $c \geq 0$. Consequently new families of Hadamard matrices of orders $4tw$ and $20tw$ can be constructed, where w is the order of Williamson matrices.

Introduction. An Hadamard matrix $H_n = (h_{ij})$ of order n is an $n \times n$ matrix with entries 1 or -1 such that $H_n H_n^T = nI_n$, where I_n is the $n \times n$ identity matrix and T indicates the transposed matrix. In H_n, row vectors $v_i = (h_{i1}, h_{i2}, \ldots, h_{in})$ are orthogonal, i.e. $v_i \cdot v_j \equiv \sum_{k=1}^{n} h_{ik}h_{jk} = 0$, $i \neq j$. H_n exists only if $n = 1, 2$, or $4k$.

A sequence of vectors $V = (v_k)_n \equiv (v_1, v_2, \ldots, v_n)$, where v_k is one of m orthonormal vectors $i_1, i_2, \ldots, i_m$ or their negatives, is said to be an m-symbol δ-code of length n, if

(I) $v(j) = 0$ for $j \neq 0$, where $v(j) \equiv \sum_{k=1}^{n-j} v_k \cdot v_{k+j}$ is the nonperiodic auto-correlation function of V. Another characterization of $V = (v_k)_n$ being an m-symbol δ-code is that its associated polynomial $V(z) \equiv \sum_{k=1}^{n} v_k z^{k-1} = \sum_{j=1}^{m} P_j(z) i_j$, where $P_j(z) = \sum_{k=1}^{n} p_{jk} z^{k-1}$, $1 \leq j \leq m$, satisfies

(II) $p_{jk} \in \{0, 1, -1\}$ and $\sum_{j=1}^{m} |p_{jk}| = 1$ $(1 \leq k \leq n)$; and

(III) $\sum_{j=1}^{m} |P_j(z)|^2 = n$, for any z on the unit circle $K = \{z \in \mathbf{C}\colon |z| = 1\} = \{z = \exp(ix)\colon 0 \leq x \leq 2\pi\}$, where $\mathbf{C}$ is the complex field and $i = \sqrt{-1}$.

Hadamard matrices of orders $4tw$ and $20tw$ can be composed if there exist a four-symbol δ-code of length t and Williamson matrices of order w (see [**1**]).

For four-symbol δ-codes, we can let $i_1 = (1,0,0,0)$, $i_2 = (0,1,0,0)$, $i_3 = (0,0,1,0)$, $i_4 = (0,0,0,1)$ and $v_k = (q_k, r_k, s_k, t_k)$. Then

$$q_k, r_k, s_k, t_k \in \{0, 1, -1\} \quad \text{and} \quad |q_k| + |r_k| + |s_k| + |t_k| = 1, \tag{1}$$

which corresponds to condition (II). Condition (I) becomes

$$q(j) + r(j) + s(j) + t(j) = 0 \quad \text{for } j \neq 0, \tag{2}$$

where $p(j)$ is the auto-correlation function of a sequence $P = (p_k)$. And (III) becomes

$$|Q|^2 + |R|^2 + |S|^2 + |T|^2 = n \quad \text{for any } z \in K,$$

where P stands for the associated polynomial $P(z)$ of a sequence (p_k). From now on we shall use the same P to represent both a sequence (p_k) and its associated polynomial $\sum p_k z^{k-1}$.

Four sequences Q, R, S and T of length n satisfying conditions (1) and (2) are called *Turyn sequences* (or T-sequences) of length n (abbreviated as $TS(n)$).

Received by the editors September 26, 1980 and, in revised form, February 6, 1981.
1980 *Mathematics Subject Classification*. Primary 05B20, 62K05, 05A19.
[1]Partially supported by SUNY Summer Research Grant.

Four $(1,-1)$ sequences $U = (u_k)_{m+p}$, $W = (w_k)_{m+p}$; $X = (x_k)_m$ and $Y = (y_k)_m$ (where $p \geq 0$) will be called *Turyn base sequences* for length $2m+p$ (abbreviated as $TBS(2m+p)$) if they satisfy

$$u(j) + w(j) + x(j) + y(j) = 0 \quad \text{for } j \neq 0. \tag{3}$$

Condition (3) is also equivalent to

$$|U|^2 + |W|^2 + |X|^2 + |Y|^2 = 2(2m+p) \quad \text{for any } z \in K.$$

If $TBS(2m+p)$: U, W; X and Y exist, then $TS(2m+p)$ can be formed (cf. [1]) as follows: $\frac{1}{2}(U+W,0)$, $\frac{1}{2}(U-W,0)$, $\frac{1}{2}(0',X+Y)$, and $\frac{1}{2}(0',X-Y)$, where $0 = 0_m$ (the sequence of zeros of length m) and $0' = 0_{m+p}$.

THEOREM. *Let $U = (u_k)_{m+p}$, $W = (w_k)_{m+p}$; $X = (x_k)_m$ and $Y = (y_k)_m$ be $TBS(n)$ for $n = 2m+p$. Then the following are $TS(3n)$:* [2]

$$\begin{aligned}
Q &= \frac{1}{2}(U+W, X+Y; 0', 0; (U-W)^*, 0),\\
R &= \frac{1}{2}(U-W, X-Y; 0', 0; -(U+W)^*, 0),\\
S &= \frac{1}{2}(0', 0; U+W, -(X+Y); 0', (X-Y)^*),\\
T &= \frac{1}{2}(0', 0; U-W, -(X-Y); 0', -(X+Y)^*),
\end{aligned} \tag{4}$$

or

$$\begin{aligned}
Q &= \frac{1}{2}((U-W)^*, 0; U+W, X+Y; 0', 0),\\
R &= \frac{1}{2}(-(U+W)^*, 0; U-W, X-Y; 0', 0),\\
S &= \frac{1}{2}(0', (X-Y)^*; 0', 0; U+W, -(X+Y)),\\
T &= \frac{1}{2}(0', -(X+Y)^*; 0', 0; U-W, -(X-Y)),
\end{aligned} \tag{5}$$

where $A^* = (a_N, a_{N-1}, \ldots, a_1)$ is the reverse of $A = (a_1, a_2, \ldots, a_N)$.

LEMMA. *Let a, b, c and d be polynomials with real coefficients in $z \in K$. And let $e = a+b+c$, $f = a-b+d$, $g = a-c-d$, and $h = b-c+d$. Then*

$$|e|^2 + |f|^2 + |g|^2 + |h|^2 = 3(|a|^2 + |b|^2 + |c|^2 + |d|^2) \quad \textit{for any } z \in K.$$

The Lemma can be proved easily by straightforward computations and by observing that $|p|^2 = pp'$, where $p' = p(z^{-1})$ for any $z \in K$.

PROOF OF THEOREM. Let $a = U$, $b = -z^{n-m}X$, $c = -z^{2n-m}Y^*$, and $d = -z^{2n}W^*$ in the Lemma. Then as sequences, $e = (U, -X; 0', -Y^*)$, $f = (U, X; 0', 0; -W^*)$, $g = (U, 0; 0', Y^*; W^*)$ and $h = (0, -X; 0', Y^*; -W^*)$. Consequently $g^* = (W, Y; 0', 0; U^*)$ and $h^* = (-W, Y; 0', -X^*; 0')$. In case (4), we have $Q = (f+g^*)/2$, $R = (f-g^*)/2$, $S = z^n(e-h^*)/2$, and $T = z^n(e+h^*)/2$. By noting that $|z| = 1$ and $|p^*|^2 = |p|^2$ since $|p^*(z)| = |p(z^{-1})|$, we obtain $|Q|^2 +$

[2] This neat form of case (4), which contains less $*$'s than my original one, was suggested by R. J. Turyn.

$|R|^2+|S|^2+|T|^2 = (|e|^2+|f|^2+|g|^2+|h|^2)/2 = 3(|a|^2+|b|^2+|c|^2+|d|^2)/2 = 3(|U|^2+|W|^2+|X|^2+|Y|^2)/2 = 3n$, for any $z \in K$. Similarly we can establish case (5) by letting $a = X^*$, $b = z^m U^*$, $c = -z^{n+m}W$ and $d = z^{2n}Y$ in the Lemma.

Since $TBS(n)$ are known to exist for odd $n \leq 59$ or $n = 2^a 10^b 26^c + 1$ (cf. [**1**, **2**, **3**]), $TS(3n)$ can be composed for these n. Consequently four-symbol δ-codes of length $3n$ can be found for these n.

References

1. R. J. Turyn, *Hadamard matrices, Baumert-Hall units, four symbol sequences, pulse compression, and surface wave encodings*, J. Combin. Theory **16A** (1974), 313–333.
2. ——, *Computation of certain Hadamard matrices*, Notices Amer. Math. Soc. **20** (1973), A-1.
3. ——, Personal communication (1980).
4. J. S. Wallis, *On Hadamard matrices*, J. Combin. Theory **18A** (1975), 149–164.
5. A. V. Geramita and J. Seberry, *Orthogonal designs*, Dekker, New York, 1979.
6. A. C. Mukhopadyay, *Some infinite classes of Hadamard matrices* J. Combin. Theory **25A** (1978), 128–141.
7. C. H. Yang, *Hadamard matrices, finite sequences, and polynomials defined on the unit circle*, Math. Comp. **33** (1979), 688–693.

Department of Mathematical Sciences, SUNY-College at Oneonta, Oneonta, New York 13820