A COMPOSITION THEOREM FOR δ-CODES

C. H. YANG

Abstract. If Golay complementary sequences (or equivalently a two-symbol δ-code) of length \( n \) and a Turyn δ-code of length \( t \) exist then four-symbol δ-codes of length \( (2n + 1)t \) can be composed. Therefore new families of Hadamard matrices of orders \( 4uw \) and \( 20uw \) can be constructed, where \( u = (2^{a+1}10^b26^c + 1) \) for odd \( t \leq 59 \) or \( t = 2^{d}10^{e}26^{f} + 1 \) (all \( a, b, c, d, e, \) and \( f \geq 0 \)), and \( w \) is the order of Williamson matrices.

The following result has been obtained: If Golay complementary sequences of length \( s \) and Turyn base sequences for length \( t \) (see [1]) exist, then four-symbol δ-codes of length \( (2s + 1)t \) can be composed. Consequently four-symbol δ-codes of length \( u = (2^{a+1}10^b26^c + 1)t \) can be constructed for odd \( t \leq 59 \) or \( t = 2^{d}10^{e}26^{f} + 1 \), where \( a, b, c, d, e \) and \( f \) are nonnegative integers. Therefore new families of Hadamard matrices of orders \( 4uw \) and \( 20uw \) can be constructed, where \( w \) is the order of Williamson matrices.

In this paper, many notations and definitions are the same as in [1]. Turyn base sequences for length \( t = 2m + p \) (abbreviated as TBS(\( t \))) are four \((1, -1)\)-sequences \((A, B; C, D)\), respectively, of lengths \( m + p \) and \( m \) pairwise such that

\[
(1) \quad A = (a_k)_{m+p}, \quad B = (b_k)_{m+p}, \quad C = (c_k)_m \quad \text{and} \quad D = (d_k)_m
\]

having zero auto-correlation sum, i.e. \( a(j) + b(j) + c(j) + d(j) = 0 \) for \( j \neq 0 \), where \( p(j) = \sum_{k=0}^{n-1} p_k p_{k+j} \) for \( P = (p_k)_n \). Another characterization of TBS(\( t \)) is that the associated polynomials satisfy

\[
(2) \quad |A|^2 + |B|^2 + |C|^2 + |D|^2 = 2t, \quad \text{for any} \ z \in K = \{z \in \mathbb{C} : |z| = 1\},
\]

where we use the same notation \( P \) to represent a given sequence \( (p_k)_n \) and its associated polynomial \( P(z) = \sum_{k=0}^{n-1} p_k z^{k-1} \); \( K \) is the unit circle and \( \mathbb{C} \) is the complex field.

Turyn sequences of length \( t \) (abbreviated as TS(\( t \))) or a four-symbol δ-code of length \( t \) are four \((0, \pm 1)\)-sequences \((I, J, K, L)\) of length \( t \), where \( I = (i_h)_t, \quad J = (j_h)_t, \quad K = (k_h)_t \) and \( L = (l_h)_t \), satisfying \( i(h) + j(h) + k(h) + l(h) = 0 \) for \( h \neq 0 \) and \( |i_h| + |j_h| + |k_h| + |l_h| = 1 \) for each \( h \). It is known that the associated polynomials TS(\( t \)) satisfy \( |I|^2 + |J|^2 + |K|^2 + |L|^2 = t \) for any \( z \in K \).

A regular δ-code of length \( u \) (abbreviated as RD(\( u \))) is a quad \((Q, R, S, T)\) of \((0, \pm 1)\)-sequences of length \( u \) such that

\[
(3) \quad Q = I + J, \quad R = I - J, \quad S = K + L \quad \text{and} \quad T = K - L,
\]
which is derived from \( TS(u) \): \((I, J, K, L)\). The existence of \( RD(u) \) and that of \( TS(u) \) are equivalent since, from (3), we also have \( I = (Q + R)/2, J = (Q - R)/2, K = (S + T)/2 \) and \( L = (S - T)/2 \). We note here that the associated polynomials of \( RD(u) \) satisfy

\[
|Q|^2 + |R|^2 + |S|^2 + |T|^2 = 2u \quad \text{for any } z \in \mathbb{K},
\]

and

(5) either \( q_k r_k = \pm 1 \) and \( s_k = t_k = 0 \), or \( q_k = r_k = 0 \) and \( s_k t_k = \pm 1 \), for each \( k \), where \( q_k, r_k, s_k, \) and \( t_k \) are the \( k \)th term of the sequences \( Q, R, S, \) and \( T \), respectively.

We first prove the following **Lagrange identity theorem for polynomials**, which is the key to our constructions for \( RD(u) \).

**Theorem 1.** Let \( A, B, C, D, E, F, G \) and \( H \) be polynomials in \( z \in \mathbb{K} \) with real coefficients. Also let

\[
\begin{align*}
W &= -B'E + AF' + CG + DH, \\
X &= A'E + BF' + DG' - CH', \\
Y &= -D'E - CF + AG' - BH, \\
Z &= C'E - DF + BG + AH',
\end{align*}
\]

where \( P' = P(z^{-1}) \) for \( P = P(z) \). Then

\[
\]

**Proof.** Since

\[
|W|^2 + |X|^2 + |Y|^2 + |Z|^2 = WW' + XX' + YY' + ZZ' \quad \text{and}
\]

\[
\begin{align*}
W' &= -BE' + A'F + C'G' + D'H', \\
X' &= AE' + B'F + D'G - C'H, \\
Y' &= -DE' - C'F' + A'G - B'H', \\
Z' &= CE' - D'F' + B'G' + A'H',
\end{align*}
\]

by substituting the right-hand sides of (6) and (9) into that of (8), and by expansions, simplifications and regrouping, (7) can be derived.

**Golay complementary sequences of length \( s \)** (abbreviated as \( GCL(s) \)) are two \((L-1)\)-sequences: \( F = (f_k)_s \) and \( G = (g_k)_s \) having zero auto-correlation sum, \( f(j) + S(j) = 0 \) for \( j \neq 0 \). Another characterization of \( GCL(s) \) (see [2]) is that the associated polynomials satisfy \(|F|^2 + |G|^2 = 2s \) for any \( z \) in \( \mathbb{K} \). \( GCL(s) \) are known to exist for \( s = 2^a10^b26^c \), where \( a, b, \) and \( c \) are nonnegative integers (see [3]).

**Theorem 2.** Let \((A, B; C, D)\) be \( TBS(t) \) of (1) and \( F = (f_k)_s \) and \( G = (g_k)_s \) be \( GCL(s) \), where \( s = 2r \). Then the following \((Q, R, S, T)\) are the associated polynomials of \( RD((2s+1)t) \).

\[
\begin{align*}
Q &= (-B'E + AF' + CG)U, \\
S &= (-D'E - CF + AG')V, \\
R &= (A'E + BF' + DG')U, \\
T &= (C'E - DF + BG)V,
\end{align*}
\]
where $P = P(z)$, for $P = A, B, C, D,$ and $E = z^{(s+1)\tau-1}$,

$$F = \sum_{k=-r}^{r-1} f_{r+k+1} z^{(2k+1)\tau+M}, \quad G = \sum_{k=-r}^{r-1} g_{r+k+1} z^{(2k+1)\tau};$$

$M = m + p = t - m; \quad U = z^{(s-1)\tau+M}$, and $V = z^{st}.$

**Proof.** By applying Theorem 1 to $(Q, R, S, T)$ and observing that $UU' = 1 = VV'$, $|F|^2 + |G|^2 = 2s$, $|E|^2 = 1$ and $H = 0$, we obtain, from (2),

$$|Q|^2 + |R|^2 + |S|^2 + |T|^2 = (|A|^2 + |B|^2 + |C|^2 + |D|^2)(|E|^2 + |F|^2 + |G|^2) = 2t(2s + 1),$$

for any $z$ in $K$. Therefore, (4) is satisfied. And since

$$I' = \sum_{h=-r}^{r-1} f_{r-h} z^{-(2k+1)\tau-M} = \sum_{h=-r}^{r-1} f_{r-h} z^{(2k+1)\tau-M}$$

and

$$G' = \sum_{h=-r}^{r-1} g_{r-h} z^{-(2k+1)\tau} = \sum_{h=-r}^{r-1} g_{r-h} z^{(2k+1)\tau},$$

we have from ($*$)

($**$) $Q = \sum_{h=-r}^{r-1} (A_f_{r-h} z^{(2k+1)\tau} + C g_{r+h+1} z^{(2k+1)\tau+M}) z^{(s-1)\tau} - B'z^{2st+M-1},$

$$R = \sum_{h=-r}^{r-1} (B_f_{r-h} z^{(2k+1)\tau} + D g_{r-h} z^{(2k+1)\tau+M}) z^{(s-1)\tau} + A'z^{2st+M-1},$$

$$S = \sum_{h=-r}^{r-1} (A g_{r-h} z^{(2k+1)\tau} - C f_{r+h+1} z^{(2k+1)\tau+M}) z^{st} - D'z^{(2s+1)\tau-1},$$

$$T = \sum_{h=-r}^{r-1} (B g_{r+h+1} z^{(2k+1)\tau} - D f_{r+h+1} z^{(2k+1)\tau+M}) z^{st} + C'z^{(2s+1)\tau-1}.$$

Consequently, (5) is also satisfied. When $s = 1$, Theorem 2 takes the following form: i.e. $r = \frac{1}{2}$, thus $F = z^M$ and $G = 1$, if $f_1 = g_1 = 1$.

**Corollary.** When $s = 1$, we let $F = z^M$, $G = 1$, and $E, U$ and $V$ be as in Theorem 2. Then $(Q, R, S, T)$ is $RD(3t)$.

For example, from the corollary, we obtain $RD(3t)$ as follows:

$$Q = (A, C; 0, 0; -B', 0), \quad S = (0, 0; A, -C; 0, -D'),$$

$$R = (B, D; 0, 0; A', 0), \quad T = (0, 0; B, -D; 0, C').$$

We note here that the above $(Q, R, S, T)$ corresponds to $(f, g^*, e, -h^*)$ in the proof of the theorem of [1]. By setting $F = (-1, 1)$ and $G = (1, 1)$ as $GCL(2)$, we obtain the following $RD(5t)$ from ($**$).

$$Q = (A, C; 0, 0; -A, 0; -B', 0), \quad S = (0, 0; A, C; 0, 0; A, -C; 0, -D'),$$

$$R = (B, D; 0, 0; -B, D; 0, 0; A', 0), \quad T = (0, 0; B, D; 0, 0; B, -D; 0, C').$$
In general, we obtain the following $RD((2s + 1)t)$ from Theorem 2, (**).

\[(A_{f_1}, C_{g_1}; 0, 0; A_{f_2}, C_{g_2}; 0, 0; \ldots; A_{f_s}, C_{g_s}; 0, 0; -B', 0),\]
\[(B_{f_1}, D_{g_1}; 0, 0; B_{f_2}, D_{g_2}; 0, 0; \ldots; B_{f_s}, D_{g_s}; 0, 0; A', 0),\]
\[(0, 0; A_{g_1}, -C_{f_1}; 0, 0; A_{g_2}, -C_{f_2}; 0, 0; \ldots; 0, 0; A_{g_s}, -C_{f_s}; 0, -D'),\]
\[(0, 0; B_{g_1}, -D_{f_1}; 0, 0; B_{g_2}, -D_{f_2}; 0, 0; \ldots; 0, 0; B_{g_s}, -D_{f_s}; 0, C').\]

**References**

2. *_, Hadamard matrices, finite sequences, and polynomials defined on the unit circle*, Math. Comp. **33** (1979), 688–693.

**Department of Mathematical Sciences, State University of New York, Oneonta, New York 13820**