CORE
Metadata, citation and similar papers at core.ac.uk
Provided by Elsevier - Publisher Connector

JOURNAL OF COMBINATORIAL THEORY, Series A 55, 49–59 (1990)

A New Restriction on the Lengths of Golay Complementary Sequences*

SHALOM ELIAHOU, MICHEL KERVAIRE, AND BAHMAN SAFFARI

Section de Mathématiques, Université de Genève, Case Postale 240, 1211 Genève 24, Switzerland

Communicated by the Managing Editors

Received September 29, 1988

1. INTRODUCTION

This paper deals with *binary sequences* $a_0, a_1, ..., a_{l-1}$, where each entry a_i equals $+1$ or -1, for $i = 0, 1, ..., l-1$.

Two binary sequences of length l,

$$A = (a_0, a_1, ..., a_{l-1}),$$
$$B = (b_0, b_1, ..., b_{l-1})$$

form a pair of Golay *complementary sequences* if they satisfy the $l-1$ conditions

$$\sum_{i=0}^{l-j-1} (a_i a_{i+j} + b_i b_{i+j}) = 0, \tag{1}$$

for $j = 1, ..., l-1$.

Golay complementary sequences were introduced by Marcel Golay in 1949 [Go1] and 1951 [Go2], in connection with spectrometry.

The simplest example of Golay complementary sequences (of length >1) is

$$A = (1, 1)$$
$$B = (1, -1).$$

It is a classical, and probably very difficult problem to determine the set of lengths for which Golay complementary sequences exist.

* The authors gratefully acknowledge partial support from the Fonds National Suisse de la Recherche Scientifique during the preparation of this paper.

0097-3165/90 $3.00

Copyright © 1990 by Academic Press, Inc.
All rights of reproduction in any form reserved.

Before we recall the status of this unsolved question, let us introduce some notation.

We find it more handy to use the polynomial notation and thus replace a sequence $A = (a_0, ..., a_{l-1})$ by the polynomial $A(z) = \sum_{i=0}^{l-1} a_i z^i$.

Note the identity

$$A(z)\, A(z^{-1}) = \sum_{i=0}^{l-1} a_i^2 + \sum_{j=1}^{l-1} c_j (z^j + z^{-j})$$

in the Laurent polynomial ring $\mathbb{Z}[z, z^{-1}]$, where

$$c_j = c_j(A) = \sum_{i=0}^{l-j-1} a_i a_{i+j} \tag{2}$$

is called the jth *correlation* (or jth *autocorrelation*) of the sequence $A = (a_0, ..., a_{l-1})$, or of the polynomial $A(z) = \sum_{i=0}^{l-1} a_i z^i$.

It is plain that two binary sequences

$$A = (a_0, ..., a_{l-1}),$$
$$B = (b_0, ..., b_{l-1})$$

are complementary if and only if the corresponding polynomials $A(z) = \sum_{i=0}^{l-1} a_i z^i$ and $B(z) = \sum_{i=0}^{l-1} b_i z^i$ satisfy the identity

$$A(z)\, A(z^{-1}) + B(z)\, B(z^{-1}) = 2l \tag{3}$$

in $\mathbb{Z}[z, z^{-1}]$. Both statements mean that the sum of the correlations of A and B is zero:

$$c_j(A) + c_j(B) = 0, \qquad \text{for} \quad j = 1, ..., l-1.$$

It might be of interest to mention that the notion of polynomial pairs (with coefficients ± 1) satisfying (3) arises in Fourier analysis under the name of Rudin–Shapiro polynomial pair. Condition (3) appears there in the equivalent form

$$|A(e^{2\pi i\theta})|^2 + |B(e^{2\pi i\theta})|^2 = 2l \tag{3'}$$

for all $z = e^{2\pi i\theta} \in S^1$ on the unit circle $S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$ in the complex plane.

Historical observation reveals that for many years since 1950, the subjects of Golay complementary sequences (also labelled δ-codes) and Rudin–Shapiro polynomial pairs, although they were really dealing with the same objects, developed along disjoint and independent channels!

We propose to unify the terminology by using the name *dual binary pair* (of polynomials or sequences).

What about the possible lengths of these Golay–Rudin–Shapiro dual binary polynomial pairs?

Let us briefly recall what is known on this problem.

On the positive side, every integer l of the form $l = 2^r \cdot 10^s \cdot 26^t$ is the length of some dual binary pair.

The lengths $l = 2$, 10, and 26 are realized as follows:

$$1 + z$$
$$1 - z,$$

$$1 + z - z^2 + z^3 - z^4 + z^5 - z^6 - z^7 + z^8 + z^9$$
$$1 + z - z^2 + z^3 + z^4 + z^5 + z^6 + z^7 - z^8 - z^9,$$

$$1 + z + z^2 + z^3 - z^4 + z^5 + z^6 - z^7 - z^8 + z^9 - z^{10} + z^{11} - z^{12} + z^{13}$$
$$- z^{14} - z^{15} + z^{16} - z^{17} + z^{18} + z^{19} + z^{20} - z^{21} - z^{22} + z^{23} + z^{24} + z^{25}$$
$$1 + z + z^2 + z^3 - z^4 + z^5 + z^6 - z^7 - z^8 + z^9 - z^{10} + z^{11} + z^{12} + z^{13}$$
$$+ z^{14} + z^{15} - z^{16} + z^{17} - z^{18} - z^{19} - z^{20} + z^{21} + z^{22} - z^{23} - z^{24} - z^{25}.$$

Note. A convenient way of verifying that polynomials A, B are dual is to observe that the identity

$$A(z)\, A(z^{-1}) + B(z)\, B(z^{-1}) = \text{const.}$$

holds if and only if the same is true for

$$P = \tfrac{1}{2}(A + B) \qquad \text{and} \qquad Q = \tfrac{1}{2}(A - B).$$

This remark can be used to lower the length of the polynomial pair to be checked.

The above examples of binary dual pairs have been rediscovered several times since their first appearance (in some disguise) in [Go1], [Go2], and [Go4].

Furthermore, the set of all integers occuring as the length of some dual binary polynomial pair, is closed under multiplication. (See [T].)

More precisely, if (A_1, A_2) and (B_1, B_2) are two such pairs with lengths a and b, respectively, then a new pair $(C_1, C_2) = (A_1, A_2) \times (B_1, B_2)$ can be defined by the matrix formula

$$\begin{pmatrix} C_1(z) & C_2(z) \\ -C_2^*(z) & C_1^*(z) \end{pmatrix}$$
$$= \frac{1}{2} \cdot \begin{pmatrix} A_1(z) & A_2(z) \\ -A_2^*(z) & A_1^*(z) \end{pmatrix} \cdot \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} B_1(z^a) & B_2(z^a) \\ -B_2^*(z^a) & B_1^*(z^a) \end{pmatrix},$$

where $A^*(z) = z^{\deg(A)} A(z^{-1})$.

It is straightforward to verify that (C_1, C_2) is a dual binary pair of length $c = a \cdot b$.

Hence, by piling up copies of the above examples of lengths 2, 10, and 26, according to this multiplication, one can construct dual binary polynomials of any length of the form $2^r \cdot 10^s \cdot 26^t$.

The multiplication in the set Γ of dual binary pairs is associative, and turns Γ into a cancellation monoid with unit (1, 1), and invertible elements $(\pm 1, \pm 1)$.

Perhaps a particularly blunt way of stressing our ignorance about Γ is to ask:

Question. Is the monoid Γ finitely generated? Or, perhaps more interestingly, is the monoid of lengths $l(\Gamma) \subset \mathbb{N}$ finitely generated?

On the other hand, the known restrictions on the possible lengths l of dual binary polynomials are listed below:

(1) l must be even,

(2) l must be the sum of two integral squares,

(3) l cannot be of the form $2 \cdot 3^t$ for any positive t.

The restrictions (1) and (2) are well known and easy to obtain. (See [Go3].) Since we will use an equivalent form of (2), we reprove it below.

Restriction (3) is due to Malcolm Griffin [Gr].

Finally computer search showed that the integers 34, 36, 50, and 58 cannot be realized as the length of any Golay complementary sequences [AS]. There are no conceptual proofs known yet for the cases 34, 50, and 58.

In this note, we obtain a further restriction on the possible length of Golay complementary sequences, which is quite stronger than condition number (3) above.

THEOREM. *The length l of a pair of Golay complementary sequences has no prime factor congruent to* 3 mod 4.

For example, the exclusion of $l = 36$ as a possible length, which had previously been obtained by computer search, now follows from our result above.

The list of undecided lengths $l \leqslant 100$ is now reduced to 68, 74, and 82.

As we shall see, adopting the point of view of a pair of polynomials rather than that of a pair of sequences has definite advantages.

For instance, replacing z by 1 in Eq. (3) above, one gets the relation

$$A(1)^2 + B(1)^2 = 2l,$$

which implies that l itself is a sum of two squares of integers. Indeed, $A(1) \equiv B(1) \bmod 2$ since A and B have the same length, and then

$$l = \left(\frac{A(1)+B(1)}{2}\right)^2 + \left(\frac{A(1)-B(1)}{2}\right)^2.$$

Similarly, we will obtain our theorem by substituting for z a suitable root of unity ζ in Eq. (3), and by studying the resulting equation

$$A(\zeta)\, A(\zeta^{-1}) + B(\zeta)\, B(\zeta^{-1}) = 2l \tag{4}$$

in the ring of cyclotomic integers $\mathbb{Z}[\zeta]$.

This will require an elementary lemma on the arithmetic of cyclotomic fields which we state and prove first.

2. Some Cyclotomy, Now

If q is a positive integer, and ζ a primitive qth root of unity, e.g., $\zeta = e^{2\pi i/q}$, we denote by $\mathbb{Z}[\zeta]$ the ring consisting of the integral linear combinations of powers of ζ. Observe that $\mathbb{Z}[\zeta]$ is stable under complex conjugation: $\alpha \in \mathbb{Z}[\zeta]$ implies $\bar{\alpha} \in \mathbb{Z}[\zeta]$.

Lemma. *Let p be a prime number satisfying $p \equiv 3 \bmod 4$. Let N be a positive integer and let ζ be a primitive p^Nth root of unity.*

Suppose $\alpha, \beta \in \mathbb{Z}[\zeta]$ satisfy the condition

$$\alpha \cdot \bar{\alpha} + \beta \cdot \bar{\beta} \in p^2 \mathbb{Z}[\zeta],$$

where the bar denotes complex conjugation.

Then $\alpha, \beta \in p\mathbb{Z}[\zeta]$.

Proof. It is well known that ζ is a root of the cyclotomic polynomial

$$\Phi_q(X) = 1 + X^{p^{N-1}} + \cdots + X^{p^{N-1}(p-1)},$$

where $q = p^N$.

Also, $\mathbb{Z}[\zeta]$ is isomorphic to the quotient ring $\mathbb{Z}[X]/(\Phi_q(X))$. Recall that $\Phi_q(X)$ is irreducible (in $\mathbb{Q}[X]$), hence $\mathbb{Z}[\zeta]$ is an integral domain.

The map $\mathbb{Z}[X] \to \mathbb{F}_p$ which is reduction mod p on the coefficients and sends X to 1 induces a ring map $\rho\colon \mathbb{Z}[\zeta] \to \mathbb{F}_p$ such that $\rho(\zeta) = 1$.

Since $\zeta \cdot \bar{\zeta} = 1$, or $\bar{\zeta} = \zeta^{p^N - 1}$, we also have $\rho(\bar{\zeta}) = 1$, and therefore $\rho(\bar{\xi}) = \rho(\xi)$ for every $\xi \in \mathbb{Z}[\zeta]$.

Of course, $\rho(p\mathbb{Z}[\zeta]) = 0$.

We will need to know that $\ker(\rho)$ is the ideal of $\mathbb{Z}[\zeta]$ generated by $1 - \zeta$. Evidently, $\ker(\rho)$ is generated by $(p, 1 - \zeta)$. However,

$$p = \Phi_q(1) = \Pi_{(s,q)=1}(1 - \zeta^s),$$

where s runs over a complete system of representatives of the classes mod q, prime to $q = p^N$.

Since for every s prime to q, the element

$$\frac{1 - \zeta^s}{1 - \zeta} = 1 + \zeta + \cdots + \zeta^{s-1}$$

is invertible in $\mathbb{Z}[\zeta]$, we have

$$p = (1 - \zeta)^{\phi(q)} \cdot u, \qquad \phi(q) = p^{N-1}(p - 1),$$

with u a unit in $\mathbb{Z}[\zeta]$. (The inverse of $(1 - \zeta^s)/(1 - \zeta)$ is $(1 - \zeta)/(1 - \zeta^s) = (1 - (\zeta^s)^{s'})/(1 - \zeta^s) = 1 + \zeta^s + \zeta^{2s} + \cdots + \zeta^{(s'-1)s} \in \mathbb{Z}[\zeta]$, where $s \cdot s' \equiv 1 \bmod p^N$.)

We apply ρ to the element $\alpha \cdot \bar{\alpha} + \beta \cdot \bar{\beta} \in p^2\mathbb{Z}[\zeta]$ and obtain, since $\rho(\bar{\alpha}) = \rho(\alpha)$ as observed above,

$$\rho(\alpha)\,\rho(\bar{\alpha}) + \rho(\beta)\,\rho(\bar{\beta}) = \rho(\alpha)^2 + \rho(\beta)^2 = 0.$$

Since $p \equiv 3 \bmod 4$, -1 is not a square in $\mathbb{F}_p$ and it follows that the equation

$$x^2 + y^2 = 0$$

in $\mathbb{F}_p$ admits only the trivial solution $x = y = 0 \pmod{p}$.

Therefore, $\rho(\alpha) = \rho(\beta) = 0$.

As we have just seen, the kernel of $\rho\colon \mathbb{Z}[\zeta] \to \mathbb{F}_p$ is the ideal generated by $1 - \zeta$. Hence, for some positive exponent v, one has

$$\alpha = (1 - \zeta)^v \cdot \alpha_1, \qquad \beta = (1 - \zeta)^v \cdot \beta_1,$$

where we can assume that $v \geqslant 1$ is maximal.

We show that if $v < \phi(q) = p^{N-1}(p - 1)$, then α_1, β_1 must still be divisible by $1 - \zeta$. In view of the assumed maximality of v, this will imply $v \geqslant \phi(q)$.

We have

$$\alpha \cdot \bar{\alpha} = (-1)^v \zeta^{-v}(1-\zeta)^{2v} \alpha_1 \cdot \bar{\alpha}_1,$$

and similarly

$$\beta \cdot \bar{\beta} = (-1)^v \zeta^{-v}(1-\zeta)^{2v} \beta_1 \cdot \bar{\beta}_1,$$

because $1-\bar{\zeta} = 1-\zeta^{-1} = -\zeta^{-1}(1-\zeta)$.

Recall that

$$p = (1-\zeta)^{\phi(q)} \cdot u,$$

where $u \in \mathbb{Z}[\zeta]$ is a unit (invertible element) in $\mathbb{Z}[\zeta]$.

Since $\alpha\bar{\alpha} + \beta\bar{\beta} \in (1-\zeta)^{2\phi(q)} \mathbb{Z}[\zeta]$, it follows that

$$\alpha_1 \cdot \bar{\alpha}_1 + \beta_1 \cdot \bar{\beta}_1 \in (1-\zeta)^{2(\phi(q)-v)} \mathbb{Z}[\zeta],$$

and therefore, if $v < \phi(q)$, $\rho(\alpha_1 \cdot \bar{\alpha}_1 + \beta_1 \cdot \bar{\beta}_1) = 0$.

As seen above, this implies

$$\rho(\alpha_1) = \rho(\beta_1) = 0,$$

and thus $\alpha_1, \beta_1 \in (1-\zeta)\mathbb{Z}[\zeta]$, in contradiction to the maximality of v.

We conclude that

$$\alpha = (1-\zeta)^{\phi(q)} \alpha_0, \qquad \beta = (1-\zeta)^{\phi(q)} \beta_0,$$

with $\alpha_0, \beta_0 \in \mathbb{Z}[\zeta]$.

Using again $p = (1-\zeta)^{\phi(q)} \cdot u$, it follows that

$$\alpha = pu^{-1}\alpha_0 \in p\mathbb{Z}[\zeta].$$

Similarly,

$$\beta = pu^{-1}\beta_0 \in p\mathbb{Z}[\zeta].$$

This proves the lemma.

3. The Theorem

We are now ready to prove the theorem:

There are no Golay complementary sequences of length divisible by a prime number of the form $p = 4k + 3$.

Proof. Let A, B be such sequences of length l.

Switching to the polynomial notation, we have the identity

$$A(z)\,A(z^{-1}) + B(z)\,B(z^{-1}) = 2l$$

in the Laurent polynomial ring $\mathbb{Z}[z, z^{-1}]$.

Substituting $z = 1$ in this equation, we see, as in Section 1, that $2l$ is the sum of two integral squares:

$$2l = A(1)^2 + B(1)^2.$$

It follows that if a prime $p \equiv 3 \bmod 4$ divides l, then actually p^2 must divide l. Indeed, $A(1)^2 + B(1)^2 \equiv 0 \bmod p\mathbb{Z}$ is only possible if $A(1) \equiv B(1) \equiv 0 \bmod p\mathbb{Z}$, and then $A(1)^2 + B(1)^2$ is divisible by p^2. All this is of course contained in the well known elementary theorem of arithmetic characterizing the integers which are the sum of two integral squares.

Now, we will show that the assumption $l \equiv 0 \bmod p^2$, where $p \equiv 3 \bmod 4$, leads to a contradiction.

Let $q = p^N$ with N large, and let ζ be a primitive qth root of unity. Then, since $A(\zeta^{-1}) = A(\bar{\zeta}) = \overline{A(\zeta)}$, we have

$$A(\zeta)\,\overline{A(\zeta)} + B(\zeta)\,\overline{B(\zeta)} = 2l \in p^2\mathbb{Z}[\zeta].$$

By the lemma above, this implies

$$A(\zeta),\ B(\zeta) \in p\mathbb{Z}[\zeta].$$

However, $A(\zeta) = a_0 + a_1\zeta + \cdots + a_{l-1}\zeta^{l-1}$, with $a_i = \pm 1$ for all $i = 0, \ldots, l-1$.

The ring $\mathbb{Z}[\zeta]$ is a free $\mathbb{Z}$-module of rank $\phi = \phi(p^N) = p^{N-1}(p-1)$, with $\mathbb{Z}$-basis $1, \zeta, \ldots, \zeta^{\phi-1}$, since $\Phi_q(X)$ is a monic polynomial. Thus, the statement $A(\zeta) \in p\mathbb{Z}[\zeta]$ implies the existence of integers $n_0, n_1, \ldots, n_{\phi-1} \in \mathbb{Z}$ such that

$$A(\zeta) = \sum_{i=0}^{l-1} a_i\zeta^i = \sum_{j=0}^{\phi-1} pn_j\zeta^j. \tag{5}$$

Suppose now that N is taken big enough so that the inequality

$$l < \phi = \phi(p^N) = p^{N-1}(p-1)$$

is satisfied. Since $1, \zeta, \ldots, \zeta^{\phi-1}$ are linearly independent over $\mathbb{Z}$, we deduce from (5) that $a_i = pn_i$ for all $i = 0, \ldots, l-1$.

But this is impossible, because $a_i = \pm 1$ by assumption.

This contradiction proves the non-existence of Golay complementary sequences of length l, if l is divisible by $p \equiv 3 \bmod 4$.

Remark. At the referee's suggestion, we note that the theorem proved is stronger than what has been stated: The argument shows indeed the following

THEOREM. *Let A, B be polynomials with integral coefficients (but not necessarily restricted to ± 1). Suppose that*

$$A(z)\,A(z^{-1}) + B(z)\,B(z^{-1}) = c \in \mathbb{Z}.$$

If c is divisible by some prime number p of the form $p = 4k+3$, then all coefficients of A and B must be divisible by p.[1]

4. BARKER POLYNOMIALS

Another classical problem of a somewhat related nature is to decide existence of the Barker polynomials of a given length.

A polynomial $A(z) = \sum_{i=0}^{l-1} a_i z^i$, still with $a_i = \pm 1$ for all $i = 0, \ldots, l-1$, is said to be a Barker polynomial if all its correlations

$$c_j = \sum_{i=0}^{l-j-1} a_i a_{i+j},$$

for $j = 1, \ldots, l-1$, are "small," i.e., $|c_j| \leqslant 1$. (See [B].)

Barker polynomials of odd lengths have been exhaustively classified by R. Turyn and J. Storer in [TS]. The only occurring lengths are 1, 3, 5, 7, 11, and 13.

It is not known whether there are any Barker polynomials of even length besides

$$1+z \qquad \text{and} \qquad 1+z-z^2+z^3,$$

up to obvious transformations.

As a consequence of our theorem, we obtain

COROLLARY. *If l is even and divisible by a prime $p \equiv 3 \bmod 4$, then there is no Barker polynomial of length l.*

Proof. We will associate with a Barker polynomial of length l some dual binary pair of the same length.

Let l be even and suppose that $A(z) = \sum_{i=0}^{l-1} a_i z^i$ is a Barker polynomial of length l.

[1] *Note added in proof.* We have recently found another proof of this theorem which does not involve cyclotomic integers, and is thus simpler. See our forthcoming paper "On Golay Polynomial Pairs," to appear in *Advances in Applied Mathematics.*

Since

$$c_{2k} = \sum_{i=0}^{l-2k-1} a_i a_{i+2k} \equiv l - 2k \equiv 0 \mod 2,$$

the condition $|c_{2k}| \leqslant 1$ implies $c_{2k} = 0$ for $k = 1, \ldots, m$, where $m = l/2$.

Therefore, we have

$$A(z)\, A(z^{-1}) = l + \sum_{k=1}^{m} c_{2k-1}(z^{2k-1} + z^{-(2k-1)}). \tag{6}$$

Now, set

$$B(z) = A(-z) = \sum_{i=0}^{l-1} (-1)^i a_i z^i.$$

Then we have

$$B(z)\, B(z^{-1}) = l - \sum_{k=1}^{m} c_{2k-1}(z^{2k-1} + z^{-(2k-1)})$$

and therefore

$$A(z)\, A(z^{-1}) + B(z)\, B(z^{-1}) = 2l.$$

Thus, (A, B) constitutes a pair of Golay complementary sequences of length l.

By our theorem, $l = \text{length}(A)$ cannot be divisible by any prime number $p \equiv 3 \mod 4$.

Remark 1. An alternate construction which also implies the corollary would be the following.

If

$$A(z)\, A(z^{-1}) = l + \sum_{k=1}^{m} c_{2k-1}(z^{2k-1} + z^{-(2k-1)})$$

with $m = l/2$ as in (6), let $P(z)$ be the polynomial such that

$$P(z^2) = \tfrac{1}{2}(A(z) + A(-z)).$$

Clearly, the length of P is $m = \frac{1}{2}(\text{length}(A))$, and P is a binary polynomial. Explicitly,

$$P(z) = \sum_{i=0}^{m-1} a_{2i} z^i, \qquad a_{2i} = \pm 1.$$

Similarly, let $Q(z)$ be the polynomial defined by

$$zQ(z^2) = \tfrac{1}{2}(A(z) - A(z^{-1})).$$

Then, it is easy to see that

$$P(z^2)\,P(z^{-2}) + Q(z^2)\,Q(z^{-2}) = l.$$

Substituting z for z^2 in this identity, we see that (P, Q) is a pair of dual binary polynomials, and hence m has no prime factor $p \equiv 3 \bmod 4$.

Remark 2. Note that neither of the two arguments above used the condition on odd correlations.

REFERENCES

[AS] T. H. ANDRES AND R. G. STANTON, Golay sequences, pp. 44–54 *in* "Lecture Notes in Mathematics, Vol. 622," Springer-Verlag, Berlin/New York, 1977.

[B] R. H. BARKER, Group synchronizing of binary digital systems, *in* "Communication Theory," pp. 273–287, Butterworth, London, 1953.

[Go1] M. J. E. GOLAY, Multislit spectrometry, *J. Opt. Soc. Amer.* **39** (1949), 437–444.

[Go2] M. J. E. GOLAY, Static multislit spectrometry and its application to the panoramic display of infrared spectra, *J. Opt. Soc. Amer.* **41** (1951), 468–472.

[Go3] M. J. E. GOLAY, Complementary series, *IRE Trans. Inform. Theory* **IT-7** (1961), 82–87.

[Go4] M. J. E. GOLAY, Note on complementary series, *Proc. IRE* **50** (1962), 84.

[Gr] M. GRIFFIN, There are no Golay complementary sequences of length 2.9^t, *Aequationes Math.* **15** (1977), 73–77.

[T] R. TURYN, Hadamard matrices, Baumert–Hall units, four-symbol sequences, pulse compression and surface wave encodings, *J. Combin. Theory Ser. A* **16** (1974), 313–333.

[TS] R. TURYN AND J. STORER, On binary sequences, *Proc. Amer. Math. Soc.* **12** (1961), 394–399.