COMPLEMENTARY PAIRS OF MULTILINEAR POLYNOMIALS

Bahman Saffari
Bâtiment 425
Dept. de Mathématiques
Université de Paris-Sud
91405 Orsay
France
bahman.saffari@math.u-psud.fr

Harold S. Shapiro*
Mathematics Institute
Royal Institute of Technology
S-10044 Stockholm
Sweden
shapiro@math.kth.se

1. Introduction

This paper is an informal account of a talk presented by one of the authors (H.S.S.) at the NATO sponsored conference "Computational noncommutative algebra and applications" held in Tuscany, Italy in July 2003. It is the authors' intention to publish elsewhere a more complete account with detailed proofs.

A *complementary pair* (CP) of polynomials in one or more variables is a pair f, g of polynomials such that $|f|^2 + |g|^2$ is constant when all the variables are restricted to lie on the unit circle of the complex plane. Usually, CP are sought subject to restrictions on the coefficients of the polynomials. Of greatest interest so far have been CP of univariate polynomials with coefficients from $\{-1, 1\}$, a notion originating in work of Golay [3], and motivated by applications to spectrometry. Shortly afterwards, and independently, an important class of CP was rediscovered by one of the present authors [5]. So far as we know, CP of *multilinear* polynomials (*i.e.*, multivariate polynomials which are of degree 1 in

*The second author wishes to thank Prometheus Inc. for partial support.

each variable) are considered here for the first time. We were first led to consider them as a tool for studying CP of univariate polynomials, but they turn out to have interesting and unexpected properties, and seem worthy of study in their own right.

Much of the (by now, very considerable) extant literature dealing with CP is concerned with applications. The present paper shall, however, not deal with these, but with purely mathematical aspects. Also, to keep the presentation focused, we shall study almost exclusively CP where the coefficients are from $\{-1, 1\}$. Some of the results could, however, be generalized to allow coefficients from other sets, such as Γ (the unit circle of the complex plane), the set of fourth roots of unity, *etc.* Also, most of our multilinear results could be generalized to the class of polynomials in $(z_1, \ldots, z_n)$ of degree d_j with respect to the variable z_j, provided each of the numbers $d_j + 1$ is a power of 2. We leave such generalizations for future work, however.

2. Notations and definitions, and overview of main results

We employ the following notations:

$\mathbb{C}$ the field of complex numbers

$\mathbb{R}$ the field of real numbers

$\mathbb{Z}$ the set of integers

$\mathbb{N}$ the set $\{0, 1, 2, \ldots\}$

$E[z_1, z_2, \ldots, z_n]$ the set of polynomials in n indeterminates with coefficients from a given set E

Γ the set of complex numbers of modulus 1

Γ_k (for $k = 2, 3, \ldots$) the multiplicative group of k-th roots of unity

$\mathbb{T}$ the quotient group $\mathbb{R}/\mathbb{Z}$ (also sometimes identified with Γ, but it proves useful to keep the alternate $\mathbb{T}$ notation in the context of harmonic analysis

$\mathcal{P}_m$ the subset of $\mathbb{C}[z]$ having degree at most m

$\mathcal{M}_n$ the subset of $\mathbb{C}[z_1, z_2, \ldots, z_n]$ having degree at most 1 with respect to each variable. We also call $\mathcal{M}_n$ the set of *n-linear polynomials*. We often abbreviate "multilinear" by ML

$\mathcal{P}_m : E$, $\mathcal{M}_n : E$ denote the subsets of $\mathcal{P}_m$ (respectively, $\mathcal{M}_n$) consisting of elements whose coefficients lie in a prescribed set E of complex numbers

$\mathcal{P}'_m$, $\mathcal{M}'_n$ the corresponding sets, in the case $E = \Gamma_2$.

Definition 1.1. *Elements f, g of $\mathbb{C}[z_1, z_2, \ldots, z_n]$ form a* complementary pair *(CP) if $|f|^2 + |g|^2$ is constant when all variables z_j are restricted to lie in Γ (or, in vector notation, when z is in Γ^n, where $z = (z_1, z_2, \ldots, z_n)$.)*

This general notion of CP is not very useful; usually one is interested in CP when the coefficients are subjected to some restrictions. Of especial interest are CP from $\mathcal{P}'_m$, *i.e.*, CP of univariate polynomials with coefficients from $\Gamma_2 = \{-1, 1\}$ (also known as *Golay pairs*) and of CP from $\mathcal{M}'_n$, *i.e.*, CP of n-linear polynomials with coefficients from Γ_2, which will be at the center of our work. If f,g are a CP from one of the above classes, we speak of g as a *complementary mate* (or *Golay mate*) of f, and *vice versa*. If f possesses such a mate, we say f is *complementable* or *complemented*.

Observe that $\mathcal{M}_n$ is a vector space over $\mathbb{C}$ of dimension 2^n. A basis for this vector space is the set of monomials

$$\{z_1^{p_1} z_2^{p_2} \ldots z_n^{p_n}, \text{where each } p_j \text{ is 0 or 1}\} .$$

It is important for our purposes to *order* these monomials, which we do according to increasing magnitude of the integers $p_1 + 2p_2 + 4p_3 + \ldots + 2^{n-1}p_n$, *i.e.*, the integers associated to the monomials by considering the p_i (in reversed order) as digits of a binary number. For example, with $n = 3$:

p_1	p_2	p_3	$p_1 + 2p_2 + 4p_3$
0	0	0	0
1	0	0	1
0	1	0	2
1	1	0	3
0	0	1	4
1	0	1	5
0	1	1	6
1	1	1	7

The corresponding ordered monomial basis is then

$$1, z_1, z_2, z_1 z_2, z_3, z_1 z_3, z_2 z_3, z_1 z_2 z_3 .$$

Observe that $\mathcal{M}'_n$ consists of precisely 2^{2^n} elements.

Suppose that, for some n, f and g are a CP from $\mathcal{P}_n$. Writing $f(z) = a_0 + a_1 z + \ldots + a_n z^n$ and $g(z) = b_0 + b_1 z + \ldots + b_n z^n$, the complementarity

relation: $|f(z)|^2 + |g(z)|^2 =$ constant, for z in Γ, can be expressed, by expanding $|f|^2$ and $|g|^2$, in the equivalent form of n coefficient identities:

$$\begin{aligned} a_0\bar{a}_1 + a_1\bar{a}_2 + \ldots a_{n-1}\bar{a}_n + b_0\bar{b}_1 + b_1\bar{b}_2 + \ldots b_{n-1}\bar{b}_n &= 0 \\ &\vdots \\ a_0\bar{a}_n + b_0\bar{b}_n &= 0 \end{aligned}$$

(Moreover, the "constant" in the definition of the complementarity relation is seen to be $|a_0|^2+\ldots+|a_n|^2+|b_0|^2+\ldots+|b_n|^2$.) The sums appearing in the left-hand members of the above equations are called "aperiodic out-of-phase autocorrelations" of the $\{a_j\}$ and $\{b_j\}$ sequences, and the circumstance that they exactly cancel one another pairwise in the case of CP is the main reason why these are of interest in applications.

The earliest known examples of CP from $\mathcal{P}'_n$ are those discovered by Golay, and independently by the second author. Following our presentation in [5], we define recursively two sequences of polynomials $\{P_n\}$, $\{Q_n\}$ by

$$P_0 = Q_0 = 1$$

and, for $n \geq 0$,

$$\begin{aligned} P_{n+1}(z) &= P_n(z) + z^{2^n} Q_n(z) \\ Q_{n+1}(z) &= P_n(z) - z^{2^n} Q_n(z) \ . \end{aligned}$$

Thus, $P_1 = 1+z$, $Q_1 = 1-z$, $P_2 = 1+z+z^2-z^3$, $Q_2 = 1+z-z^2+z^3$, *etc.* It is easy to check that for every $n \geq 0$, P_n and Q_n have degree $2^n - 1$ and all coefficients from $\{-1, 1\}$. Moreover, for $|z| = 1$ we deduce easily

$$|P_{n+1}(z)|^2 + |Q_{n+1}(z)|^2 = 2\left(|P_n(z)|^2 + |Q_n(z)|^2\right)$$

and so, inductively,

$$|P_n(z)|^2 + |Q_n(z)|^2 = 2^{n+1} \quad \text{for all } n,$$

i.e., P_n and Q_n form a CP.

Many authors have observed that the recursive definition of P_n, Q_n can be modified in various ways so as to obtain other CP. Let us here only describe a procedure due to Budisin [2]. However, our presentation will not be that of Budisin, but rather based on the notion of CP of *multilinear polynomials*, via a mapping from $\mathcal{M}_n$ into $\mathcal{P}_{2^m-1}$ which we call *lexicographic unfolding* (LU).

First, let us prove

Theorem 1.1. *For every n in $\mathbb{N}$ there exists a CP from $\mathcal{M}'_n$.*

Proof. We define two sequences f_n, g_n by the recursive scheme

$$\begin{aligned} f_0 &= g_0 = 1 \\ f_{n+1} &= f_n + z_{n+1} g_n \,, \quad g_{n+1} = f_n - z_{n+1} g_n \quad \text{for } n \geq 0. \end{aligned}$$

Thus,

$$\begin{aligned} f_1 &= 1 + z_1 \,, \quad g_1 = 1 - z_1 \\ f_2 &= 1 + z_1 + z_2 - z_1 z_2 \,, \quad g_2 = 1 + z_1 - z_2 + z_1 z_2 \end{aligned}$$

etc.

It is easy to verify by induction that

a) f_n,g_n are in $\mathcal{M}'_n$ for $n = 0, 1, 2, \ldots$

b) $|f_n|^2 + |g_n|^2 = 2^{n+1}$ when all variables have modulus 1.

□

We shall henceforth call f_n, g_n *the standard complementary pair from* $\mathcal{M}'_n$.

If we compare the construction of f_n, g_n with that of the earlier pair P_n, Q_n it is evident that P_n arises from f_n by the substitution $z_1 \to z$, $z_2 \to z^2$, $z_3 \to z^4, \ldots, z_n \to z^{2^{n-1}}$. Likewise, Q_n arises from g_n by this same substitution. This motivates the

Definition 1.2. *The* LU-transform *of an n-variable polynomial $f(z_1, z_2, \ldots z_n)$ to a one-variable polynomial $p(z)$ is the result of substituting.*

$$z_1 \to z,\ z_2 \to z^2,\ z_3 \to z^4, \ldots, z_n \to z^{2^{n-1}} \,.$$

We shall denote it by b_n (or simply by b, if there is no danger of confusion.)

As thus defined, b is too general to have many nice properties. However, interesting things appear when we restrict its domain. Thus, it is easy to verify the following

Proposition 1.1. *The LU-transform maps $\mathcal{M}_n$ linearly and bijectively onto the vector space $\mathcal{P}_{2^n-1}$ of (univariate) polynomials of degree at most $2^n - 1$. Moreover, for $f \in \mathcal{M}_n$, every coefficient of bf appears as a coefficient of f, and vice versa. (So, in particular, if f has all its coefficients in some set, the same is true of bf.)*

It is also easy to see that the norm in $L^2(\mathbb{T})$ (w.r.t normalized Haar measure on the unit circle $\mathbb{T}$) of bf equals that of f in $L^2(\mathbb{T}^n)$ (w.r.t.

normalized Haar measure on the n-torus $\mathbb{T}^n$.) For this to hold, it is *essential* that f be restricted to be *multilinear*; for merely polynomial f this is not the case, indeed b is not even a bounded operator on the sphere of all multivariate polynomials when L^2 norms are employed. On the other hand, for any polynomial f in n variables, the range of $bf(z)$ for z in $\mathbb{T}$ is a subset of the range of $f(z_1, z_2, \ldots z_n)$ for $(z_1, \ldots z_n)$ in $\mathbb{T}^n$, so bf *is always contractive from* $L^\infty(\mathbb{T}^n)$ *to* $L^\infty(\mathbb{T})$. Many intriguing questions (mostly not answered, nor perhaps even studied hitherto) arise considering the behavior of LU-transforms relative to various L^p norms, acting in $\mathcal{M}_n$, $\mathcal{M}'_n$ or subsets thereof. However, those matters are beyond the scope of the present paper.

Now, it is an immediate consequence of the above definitions that

Proposition 1.2. *The LU-transform carries each CP f,g from* $\mathcal{M}'_n$ *to a CP of univariate polynomials, of length* 2^n*, with coefficients from* $\{-1, 1\}$*. (The* length *of a polynomial in* $\mathcal{P}'_m$ *is defined to be* $m + 1$*.)*

It is also clear that

Proposition 1.3. *The LU-transform carries the standard ML complementary pair* f_n*,* g_n *onto the pair* P_n*,* Q_n*.*

It is now easy to present (in our context and terminology) Budisin's construction:

First of all, we have the "standard" CP f_n, g_n from $\mathcal{M}'_n$. Applying b to this pair gives us P_n, Q_n. But we can, before applying b, modify f_n and g_n and generate many other CP from $\mathcal{M}'_n$. Although these new pairs (f, g) will be (in a sense) "trivial" modifications of the pair (f_n, g_n), the pairs (bf, bg) of univariate polynomials will by no means be trivial modifications of (P_n, Q_n)! Indeed (and this is a new and quite deep result) *all* univariate CP with coefficients from $\{-1, 1\}$ and lengths 2^n are generated by this procedure.

So, let us now examine these "trivial" operations which transform a CP from $\mathcal{M}'_n$ to another one.

Consider first the vector space $\mathcal{M}_n$. We define two groups of linear operators on $\mathcal{M}_n$:

a) For each permutation π of the index set $\{1, 2, \ldots n\}$ we define by T_π the map of $\mathcal{M}_n$ on itself which performs the corresponding permutation of the variables $\{z_1, z_2, \ldots z_n\}$.

   Clearly T_π is a bijection of $\mathcal{M}_n$ on itself. Moreover, since permuting the variables induces a measure-preserving map of the torus $\mathbb{T}^n$ on itself, T_π is isometric w.r.t. the $L^p(\mathbb{T}^n)$ norm for every value of p. It also maps $\mathcal{M}'_n$ bijectively on itself, and each CP to another

CP. The set of all T_π is a group isomorphic to S_n, the symmetric group on n letters. It has cardinality $n!$ and is non-commutative for $n > 2$.

b) For each subset E of $\{1, 2, \ldots, n\}$, we define S_E as the map of $\mathcal{M}_n$ on itself induced by substituting $z_j \to -z_j$ for each j in E. Each such substitution is a measure-preserving map of $\mathbb{T}^n$ on itself, and induces a linear bijection of $\mathcal{M}_n$, and carries $\mathcal{M}'_n$ onto $\mathcal{M}'_n$.

It is isometric w.r.t. the $L^p(\mathbb{T}^n)$ norm, for every p, and carries CP to CP. The totality of these operators S_E is a commutative group with 2^n elements.

Now, it is easy to check that all products $T_\pi S_E$ where π ranges over all permutations of $\{1, 2, \ldots, n\}$ and E over all subsets of $\{1, 2, \ldots, n\}$ are distinct. In general, T_π and S_E do not commute. However, the *totality* of all the $n!2^n$ products $T_\pi S_E$ is identical with the totality of all products $S_E T_\pi$. Thus, the sets $\{T_\pi\}$ and $\{S_E\}$ of operators generate a (non-commutative) group which we denote by B_n, and call the *basic group* of order n.

In terms of matrices, *i.e.*, linear transformations performed on $(z_1, z_2, \ldots, z_n)$, the T_π correspond to $n \times n$ *permutation matrices*, whereas the S_E correspond to $n \times n$ *diagonal matrices* with entries from $\{-1, 1\}$ on the diagonal.

Summarizing the above discussion: the basic group B_n consists of $2^n \cdot n!$ linear mappings of $\mathcal{M}_n$ onto itself. Each of these is isometric w.r.t. all $L^p(\mathbb{T}^n)$ norms, and carries $\mathcal{M}'_n$ onto itself. It also carries every CP to another CP.

Finally, then, here is our recipe for constructing CP from $\mathcal{P}'_{2^n-1}$:

a) Start from the standard CP f_n, g_n from $\mathcal{M}'_n$.

b) Now generate new CP from $\mathcal{M}'_n$ by applying to f_n, g_n in turn each transformation from the basic group B_n.

c) To each of the CP obtained in step b), apply the LU-transform to obtain a CP of univariate polynomials of lengths 2^n.

There are some subtle points concealed within these formal procedures:

(i) In step a) we operate on the pair (f_n, g_n) by each of the $2^n \cdot n!$ operations of the basic group. But, does this procedure yield $2^n \cdot n!$ distinct CP? The answer is "No". For, it turns out that the polynomials f_n admit an unexpected symmetry. The exact description of this symmetry and its consequences for the enumeration of CP in $\mathcal{M}'_n$ and $\mathcal{P}'_{2^n-1}$ will be given in Section 3.

There are now two further questions which pose themselves:

(ii) Does the orbit of f_n under the action of the basic group comprise *all* complementable elements of $\mathcal{M}'_n$ (or, more precisely, all those with constant term $+1$, since f_n has this normalization, which is preserved by all operations in B_n)?

(iii) Is the LU-map from complementable elements of $\mathcal{M}'_n$ to complementable elements of $\mathcal{P}'_{2^n-1}$ *surjective*?

We shall see (and these are our main results) that both questions (ii) and (iii) are answered in the affirmative. We thus obtain *a simple and explicit algorithm for describing all univariate CP with coefficients from* $\{-1, 1\}$ *whose lengths are a power of 2.* Further details are in Section 3

In the concluding Section 4 we demonstrate a surprising connection between CP from $\mathcal{M}'_n$ and the well-studied notion of *bent Boolean functions.* We also indicate (what is, however, not new in principle) a link between polynomials in $\mathcal{M}'_n$ and Hadamard matrices.

3. Complementary pairs in $\mathcal{M}'_n$

We begin with some preliminary results. In this section, if we speak of CP or complementable polynomials, we always tacitly assume all coefficients are from Γ_2.

For any f in $\mathbb{C}[z_1, \ldots, z_n]$, $f^\natural$ denotes the polynomial obtained from f upon replacing each coefficient of f by its complex conjugate. Suppose now f is in $\mathcal{M}_n$. Then, for z_1, z_2, ..., z_n in Γ (or, vectorially: z in Γ^n, for $z = (z_1, z_2, \ldots z_n)$):

$$\overline{f(z)} = f^\natural(1/z_1, 1/z_2, \ldots 1/z_n) \; .$$

Hence, for z in Γ^n, we have

$$z_1 z_2 \ldots z_n \overline{f(z)} = z_1 z_2 \ldots z_n f^\natural(1/z_1, \ldots 1/z_n) =: f^\#(z_1, \ldots, z_n)$$

where $f^\#$ is in $\mathcal{M}_n$. Thus, to each f in $\mathcal{M}_n$ we have associated in $f^\#$ in $\mathcal{M}_n$ *which has the same modulus as* f *at all points of* Γ^n. Moreover, if f is in $\mathcal{M}'_n$ so is $f^\#$. it is easy to check that the map $f \to f^\#$ from $\mathcal{M}_n$ on itself is skew-linear (that is, real-linear and satisfies $(af)^\# = \bar{a} f^\#$ for complex scalars a) and *involutive*, *i.e.*, $(f^\#)^\# = f$.

The converse is not true without further hypotheses.

Proposition 1.4. *If* f *and* g *are in* $\mathcal{M}_n$ *and have equal modulus at all points of* Γ^n*, and moreover* f *is irreducible (i.e., has no nontrivial factorization in* $\mathbb{C}[z_1, z_2, \ldots, z_n]$*) then* g *must be of the form* λf *or* $\lambda f^\#$ *where* λ *is a complex number of modulus* 1*.*

Sketch of proof. In light of the preceding discussion, we have for $z \in \Gamma^n$

$$|f(z)|^2 = f(z)\overline{f(z)} = f(z)f^{\#}(z)/\left(z_1 z_2 \dots z_n\right)$$

and a similar formula for $|g(z)|^2$. Hence, the hypotheses imply $ff^{\#} = gg^{\#}$. Since f is irreducible, it divides g or $g^{\#}$, and this readily yields the desired conclusion. Observe that if f, g are in $\mathcal{M}'_n$, λ must be 1 or -1. Basic for all that follows is

Theorem 1.2. *Every complementable element of $\mathcal{M}'_n$ is irreducible.*

Remark. This theorem holds also in the wider class of n-linear complementable polynomials with *complex coefficients of modulus* 1.

Corollary 1.1. *The standard complementable elements f_n, g_n of $\mathcal{M}'_n$ are irreducible.*

Corollary 1.2. *If f is complementable in $\mathcal{M}'_n$ it has at most four Golay mates (and only* two *if we impose the normalization that only polynomials with constant term $+1$ are considered.)*

Proof. If g, h are Golay mates of f their moduli are equal at all points of Γ^n. Moreover, they are irreducible, by Theorem 1.2, hence h is identical with one of the following: g, $-g$, $g^{\#}$, $-g^{\#}$. □

We defer until the end of this Section the proof of Theorem 1.2. Corollary 1.1, which is much easier, was discovered and proved earlier by W. Moran.

Symmetry properties of f_n. We state without proof:

Theorem 1.3. *f_n is a fixed point of the operator T_ρ where ρ is the permutation of $\{1, 2, \dots, n\}$ defined by:*

$$\rho(j) = n + 1 - j \quad (j = 1, 2, \dots, n)\ .$$

Moreover, no other permutation σ (excluding the identity) has the property that $T_\sigma f_n = f_n$.

It is convenient for the sequel to define the following subclasses of $\mathcal{M}'_n$:

Definition 1.3. *An element of $\mathcal{M}'_n$ is* normalized *if its constant term equals* 1. *The set of normalized elements is denoted by $\mathcal{M}''_n$.*

Definition 1.4. *An element of $\mathcal{M}''_n$ is* strongly normalized *if moreover the coefficients of z_1, z_2, …, z_n in it are all $+1$.*

Observe that f_n is strongly normalized, and the same is true for each element of its orbit under group of operators $\{T_\pi\}$ where π runs over all permutations of $\{1, 2, \ldots, n\}$.

Corollary 1.3. *For $n \geq 2$, the orbit of f_n under the basic group consists of precisely $2^{n-1}n!$ elements.*

Indeed, it follows from Theorem 1.3 that its orbit under the subgroup consisting of all the T_π, π in S_n comprises $n!/2$ elements (each occurring twice.) Now, suppose two elements of the basic group, say $S_E T_\pi$ and $S_F T_\sigma$ satisfy

$$S_E T_\pi f_n = S_F T_\sigma f_n \tag{1}$$

where E, F are subsets of $\{1, 2, \ldots, n\}$ and π, σ are in S_n (notations as in Section 2.) Then

$$S_F S_E T_\pi f_n = T_\sigma f_n \ .$$

The right-hand member is strongly normalized. The left-hand member is not, unless $S_F S_E$ is the identity, *i.e.*, $E = F$. So, (1) implies $T_\pi f_n = T_\sigma f_n$ which, in view of Theorem 1.3, implies $\sigma^{-1}\pi = \rho$. Thus, the only way two operators in the basic group can have the same action on f_n is if they are of the form $S_E T_\sigma$ and $S_E T_{\rho\sigma}$, where E is an arbitrary subset of $\{1, 2, \ldots n\}$, σ is some element of S_n, and ρ is the permutation defined in Theorem 1.3. Hence:

Proposition 1.5. *For $n \geq 2$, the orbit of f_n under the basic group consists of precisely $2^{n-1}n!$ elements. All of these are complementable.*

We can now state a main result.

Theorem 1.4. *every normalized, complementable element of $\mathcal{M}'_n$ is in the orbit of f_n under the action of the basic group.*

Corollary 1.4. *For $n \geq 2$, there are precisely $2^{n-1}n!$ normalized, complementable elements in $\mathcal{M}'_n$.*

Under the action of the LU-transform, these give rise to $2^{n-1}n!$ distinct complementable univariate polynomials which are normalized (*i.e.*, have constant term 1). Now comes another of our main results: *this map yields all of them*! More precisely:

Theorem 1.5. *The normalized complementable univariate polynomials of length 2^n are precisely those which arise as images, under the LU-transform, of normalized complementable elements of $\mathcal{M}'_n$. For $n \geq 2$, their number is precisely $2^{n-1}n!$.*

Remark. An equivalent statement is: the LF (or *lexicographic folding*) operator (*i.e.*, the inverse to the LU-transform) carries each CP

of univariate polynomials of length 2^n with coefficients from Γ_2 to a CP from $\mathcal{M}'_n$. It is not known whether the corresponding assertion for polynomials with coefficients in Γ is true.

The proofs of Theorems 1.4 and 1.5 shall be presented elsewhere. In the remainder of this section, we shall, however, show the flavor of the development by presenting some of the key ideas on which the proof of Theorem 1.4 is based, namely, remarkable structural properties (or, functional equations) satisfied by f_n and g_n. We begin with some elementary observations. It is convenient to introduce some more notation:

Definition 1.5. *For $1 \leq j \leq n$, S'_j denotes the operator S_E where E is the singleton $\{j\}$.*

It is easy to verify the identity

$$S'_j T_\rho = T_\rho S'_{n-j+1} \quad (j = 1, 2, \ldots n)\,. \tag{2}$$

Observe also that, immediately from the definitions

$$g_n = S'_n f_n\,. \tag{3}$$

Proposition 1.6. *f_n has precisely two normalized Golay mates, namely g_n and $(-1)^n g^{\#}{}_n$.*

Proof. In view of the preceding, we have only to verify that $(-1)^n g^{\#}{}_n$ is normalized, *i.e.*, that the coefficient of $z_1 z_2 \ldots z_n$ in g_n is $(-1)^n$ or, in view of (3), that the coefficient of $z_1 z_2 \ldots z_n$ in f_n is $(-1)^{n+1}$. Now, the coefficient sequence of f_n (w.r.t. the order we have introduced) is precisely the so-called "Rudin-Shapiro sequence", and (denoting this sequence by $(a_0, a_1, a_2, \ldots)$) what we have to verify is $a_{2^n-1} = (-1)^{n+1}$. But (see Brillhart and Carlitz [1]) a_m is 1 or -1 according as the number of occurrences of a pair of consecutive ones in the binary representation of m is even or odd. For $m = 2^n - 1$, the binary expansion consists of n consecutive ones, so $a_{2^n-1} = (-1)^{n-1}$, which establishes the Proposition. □

Now, the Proposition implies that the Golay mates of $T_\rho f_n$ are $T_\rho g_n$ and $(-1)^n T_\rho g^{\#}{}_n$. Since $T_\rho f_n = f_n$, we must have $(-1)^n g^{\#}{}_n = T_\rho g_n$. Hence:

$$g^{\#}{}_n = (-1)^n T_\rho g_n\,. \tag{4}$$

After this compendium of trivial identities, we are now ready to state something more interesting. Observe that for every f in $\mathcal{M}_n$ and every j, $1 \leq j \leq n$ there is a "canonical splitting" of f as

$$f = A + z_j B$$

where A and B are $(n-1)$-linear functions of those $n-1$ variables which have index distinct from j. These properties uniquely determine A and B. For $f = f_n$ it turns out that the "A" and "B" are explicitly representable in terms of the f_i and g_i with $i < n$. This is the key to the proofs of several of our main theorems, and we just state the result (whose proof, once the formula has been discovered, is by a not-too-difficult induction:

Theorem 1.6. *For $1 \le j \le n$ we have*

$$f_n = f_{j-1}(z_1, z_2, \dots z_{j-1}) f_{n-j}(z_{j+1}, z_{j+2}, \dots z_n) + (-1)^{n-j} g_{j-1}(z_1, z_2, \dots z_{j-1}) g^{\#}{}_{n-j}(z_{j+1}, \dots, z_n) \cdot z_j \ . \qquad (5)$$

Remark. A similar identity holds, with g_n in the left-hand member, which we omit (it is derivable from the above by applying S'_n to both sides and simplifying, using identities established earlier.)

Observe that for $j = n$, (5) reduces to the recursion relation defining f_n.

Theorem 1.7. *If f is a complementable element of $\mathcal{M}'_n$, then* $\max |f(z)|$ *over z in Γ^n equals $2^{(n+1)/2}$.*

Proof. Let g be a Golay mate of f. From the complementarity it follows at once that the maximum of $|f(z)|$ on Γ^n cannot exceed $2^{(n+1)/2}$. To complete the proof, we need only show g vanishes at some point of Γ^n. This follows from the following, more general

Theorem 1.8. *If h in $\mathcal{M}_n$, for some $n \ge 1$, has all its coefficients of modulus 1, then it vanishes at some point of Γ^n.*

Proof. We may write $h = A + z_n B$ where A, B are $(n-1)$-linear functions of z_1, z_2, …, z_{n-1} with all coefficients of modulus 1. Hence $|A|^2 - |B|^2$ has mean value 0 over Γ^{n-1}, and therefore vanishes at some point $\omega = (\omega_1, \omega_2, \dots, \omega_{n-1})$ of Γ^{n-1}, hence $|A(\omega)| = |B(\omega)| =: c \ge 0$. If $c = 0$, then $h(\omega; z_n)$ vanishes for any choice of z_n in Γ. If $c > 0$, then $h(\omega; z_n)$ vanishes for $z_n = -\frac{A(\omega)}{B(\omega)}$, which lies on Γ. The proof is concluded. □

This also completes the proof of Theorem 1.7. □

Remark. For univariate complementable polynomials of length 2^n, the maximum modulus on Γ cannot exceed $2^{(n+1)/2}$. But it may be strictly less than this bound, in other words, its Golay mate may have no zeros on Γ.

Theorem 1.8 is also a key element in the proof of Theorem 1.2 whose proof we now sketch. Thus, we are given a CP f, g from $\mathcal{M}_n$. We assume f, g *have all coefficients in* Γ, and shall deduce that f is irreducible. The proof is by contradiction. We have

$$|f|^2 + |g|^2 = 2^{n+1} \quad \text{on } \Gamma^n\,. \tag{6}$$

Suppose f has a nontrivial factorization $f = GH$. It is easy to check that for some r, $1 \leq r < n$, G is r-linear and H is $(n-r)$-linear, the variables in G and H being mutually disjoint. Moreover, G and H have all coefficients in Γ. We may assume without loss of generality that G is a function of $z_1, \ldots, z_r$ and H a function of $(z_{r+1}, \ldots z_n)$. We may also assume $r \leq n/2$ (otherwise reverse the roles of G and H.) By Theorem 1.8 there is a point ω in Γ^r where G vanishes. Hence from (6)

$$|g(\omega_1, \ldots, \omega_r, z_{r+1}, \ldots, z_n)|^2 = 2^{n+1} \tag{7}$$

for all $(z_{r+1}, \ldots, z_n)$ in Γ^{n-r}. Now, it is an easily proved elementary fact that a polynomial in any number m of variables which has constant modulus on Γ^m must be a *monomial*. Hence, from (7), $g(\omega_1, \ldots \omega_r, z_{r+1}, \ldots z_n)$ is a monomial in the variables $z_{r+1}, \ldots, z_n$ times a constant c. This constant is easily seen to be some r-linear polynomial with unimodular coefficients, evaluated at $(\omega_1, \ldots, \omega_r)$ and hence $|c| \leq 2^r$. Hence from (7)

$$2^{n+1} \leq (2^r)^2$$

which is a contradiction, since $r \leq n/2$, QED.

4. Relation of CP to "bent functions", biunimodular sequences, Hadamard matrices

A *Boolean function* of order n is a map from $\{0,1\}^n$ to $\{0,1\}$. There are 2^{2^n} distinct Boolean functions of order n. An important subclass of these is the so-called *bent functions* which occur in various connections in coding theory. A good reference is [4]. There is an obvious correspondence between Boolean functions and functions from $\{-1,1\}^n$ to $\{-1,1\}$ and for our purposes here it is more convenient to work with the latter class of functions. considering $\{-1,1\}$ as a group G_2 w.r.t. multiplication, $\{-1,1\}^n = G_2^n$ is an Abelian group whose elements are ordered n-tuples from $\{-1,1\}$ with coordinatewise multiplication as the group operation.

Concretely, let us establish a correspondence between n-tuples $(a_1, a_2, \ldots a_n)$ from $\{-1,1\}^n$ and $(b_1, b_2, \ldots b_n)$ from $\{0,1\}^n$ by $a_k = (-1)^{b_k}$, $k = 1, 2, \ldots, n$. We shall consider the elements of $\{-1,1\}^n$ *ordered* in accord with their corresponding elements from $\{0,1\}^n$, the order in the

latter set (which may be identified via binary representations with the integers $\{0, 1, 2, \ldots 2^n - 1\}$) taken as the natural one on $\mathbb{N}$, just as we ordered the monomials in Section 2.

In this context, an element of $\{-1, 1\}^n$ is defined to be *bent* if (and only if) *its Fourier transform w.r.t. the group* G_2^n (which is a vector having 2^n components) *has all its components of equal magnitude*. It is convenient for our purposes to normalize Haar measures so that each element of the dual (character) group of G_2^n has measure 1. Then, the Fourier transform of a vector turns out to be the same thing as applying to it the standard "Sylvester-Hadamard matrix" (also called "Walsh-Hadamard matrix") of size $2^n \times 2^n$. (For all this terminology, and background, see [4], where the Fourier transform (in the context of the group G_2^n is also called the *Hadamard transform*. Explicitly, it maps a vector ω of 2^n complex numbers

$$\omega := \{\omega(0), \omega(1), \ldots, \omega(2^n - 1)\}$$

to another such vector

$$\hat{\omega} := \{\hat{\omega}(0), \hat{\omega}(1), \ldots, \hat{\omega}(2^n - 1)\}$$

by the formula

$$\hat{\omega}(k) = \sum_{j=0}^{2^n-1} (-1)^{j \cdot k} \omega(j)\,,\ k = 0, 1, \ldots 2^n - 1\,. \tag{8}$$

Here $j \cdot k$ denotes the sum $\sum_{m=0}^{n-1} \beta_m(j)\beta_m(k)$ where $\beta_0(\cdot), \ldots, \beta_{n-1}(\cdot)$ denote the binary digits of an integer in the range $[0, 2^n - 1]$.

For example, in case $n = 2$ the matrix $\left[(-1)^{j \cdot k}\right]$ appearing in (8) is computed as follows: First, compute the 4×4 matrix $[j \cdot k]$ as j, k run through the values $0 \approx 00$, $1 \approx 01$, $2 \approx 10$, $3 \approx 11$:

$\cdot$	00	01	10	11
00	0	0	0	0
01	0	1	0	1
10	0	0	1	1
11	0	1	1	2

Thus, $\left[(-1)^{j \cdot k}\right]$ is the matrix

$$\begin{array}{rrrr} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{array}$$

which is the 4×4 Sylvester-Hadamard matrix. That this matrix corresponds exactly to the Fourier transform relative to the group G_2^n is a

consequence of the way we have ordered the elements of the group (and likewise, of its character group which is isomorphic to G_2^n. For more particulars see [4]. We shall henceforth use the terminology *Hadamard transform* for (8).

So, to summarize: A Boolean function of order n,

$$b = (b_0, b_1, \ldots, b_{2^n-1})\,,\ b_j \in \{0,1\}$$

is *bent* if and only if the Hadamard transform $\hat{\omega}$ of ω, where $\omega(k) := (-1)^{b_k}$ $(k = 0, 1, \ldots, 2^n - 1)$ satisfies the condition $|\hat{\omega}(j)| = c$, $j = 0, 1, \ldots, 2^n - 1$, where c is independent of j.

Because the matrix in (8) is, after multiplication by the scalar factor $2^{-(n/2)}$, unitary one sees easily that $c = 2^{n/2}$. Thus, *b is bent if and only if the Hadamard transform of the vector $\left((-1)^{b_0}, (1)^{b_1}, \ldots, (-1)^{b_{2^n-1}}\right)$ is a vector each of whose components equals $2^{n/2}$ or $2^{-n/2}$.*

For our purposes, this can serve as the definition of "bent". Observe that (since the Hadamard transform of a vector with integer components has integer components) *bent Boolean functions of order n cannot exist for odd n.* It is well known that they exist for even n, and are very abundant for large even n. Their tie-in with the present paper is via

Theorem 1.9. *Let n be even, f a complementable element of $\mathcal{M}'_n$, and $(\omega(0), \omega(1), \ldots, \omega(2^n - 1))$ its coefficient sequence (in accord with the ordering of the monomials introduced in Section 2). Then, the Hadamard transform $\hat{\omega}$ of the vector ω satisfies*

$$\hat{\omega}(j) = \pm 2^{n/2}\ ,\ j = 0, 1, \ldots, 2^n - 1\ .$$

Corollary 1.5. *$\omega(k) = (-1)^{b_k}$ where $(b_0, b_1, \ldots, b_{2^n-1})$ is a bent Boolean function.*

Corollary 1.6. *There exist at least $n!/2$ bent Boolean functions of order n satisfying the* strong normalization *$b_0 = b_1 = b_2 = \ldots = b_n = 0$.*

Remark. For n larger than 2 and even, there are bent functions not derivable from complementable elements of $\mathcal{M}'_n$ in the above way. For example, there are 12 strongly normalized complementable elements of $\mathcal{M}'_4$, but 28 strongly normalized bent Boolean functions.

Theorem 1.9 is equivalent to

Theorem 1.10. *Let n be even, and f a complementable element of $\mathcal{M}'_n$. Then $|f(z)| = 2^{n/2}$ at all points z in $\{-1, 1\}^n \subset \Gamma^n$.*

Definition 1.6. *The subset $\{-1, 1\}^n$ of Γ^n will be called the* discrete torus *(in $\mathbb{C}^n$.) Thus, we can state the conclusion of Theorem 1.1 as "f has constant modulus on the discrete torus."*

The equivalence of Theorems 1.9 and 1.10 lies in verifying that, imposing the "canonical" order on the 2^n points of the discrete torus, the sequence of values taken on it by any element of $\mathcal{M}_n$ coincides with the Hadamard transform of its coefficient sequence. This is a "remarkable coincidence"!

Proof of Theorem 1.10. Let g be a Golay mate of f from $\mathcal{M}'_n$. Then

$$|f(z)|^2 + |g(z)|^2 = 2^{n+1}\,,\ z \text{ in } \Gamma^n. \tag{9}$$

For z in the discrete torus, $f(z)$ and $g(z)$ are integers. Now, it is elementary to show that for n even, the only way to partition 2^{n+1} as a sum of two non-negative squares is $2^n + 2^n$. Hence, $f(z) = \pm 2^{n/2}$ at each point of the discrete torus. □

Remark. There is a general problem in harmonic analysis, of great depth and importance: to find all complex-valued functions on a given (say, for simplicity) discrete Abelian group which has constant modulus, and whose Fourier transform has constant modulus on the dual group. For the special group G_2^n this is equivalent to the problem of bent functions, and is closely related with other combinatorial notions such as "Hadamard difference sets."

ML functions and Hadamard matrices. The following is well known, at least as "folklore" but worth recording.

Theorem 1.11. *Let f be any element of $\mathcal{M}'_n$ and write, as consecutive rows of a $2^n \times 2^n$ matrix, the coefficient sequences of $S_E f$ where E runs through all subsets of $\{1, 2, \ldots, n\}$ (including the empty one.) The matrix so obtained is Hadamard.*

Proof. Clearly all entries of the matrix are from $\{-1, 1\}$, so we have only to check mutual orthogonality of all the rows. In view of the Parseval theorem, this is equivalent to the assertion: $S_E f$ is orthogonal to $S_{E'} f$ in $L^2(\mathbb{T}^n)$ if E, E' are distinct subsets of $\{1, 2, \ldots n\}$. This verification is straightforward, and left to the reader. □

Remark. For the choice $f = (1 + z_1)(1 + z_2)\ldots(1 + z_n)$ the matrix obtained in this way (assuming the subsets of $\{1, 2, \ldots, n\}$ are appropriately ordered, *i.e.*, again in our canonical way) is the Sylvester-Hadamard matrix. For $f = f_n$ one obtains a so-called PONS matrix.

References

[1] J. Brillhart and L. Carlitz. Note on the Shapiro polynomials. *Proc. AMS*, 25:114–118, 1970.

[2] S.Z. Budisin. Efficient pulse compressor for Golay complementary sequences. *Electronics Letters*, 27(3):219–220, 31 January 1991.

[3] M.J.E. Golay. Multislit spectrometry. *J. Optical Society Am.*, 39:437, 1949.

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

[5] H.S. Shapiro. Extremal problems for polynomials and power series. Sc.M. thesis, Massachusetts Institute of Technology, 1951.