AUSTRALASIAN JOURNAL OF COMBINATORICS
Volume **37** (2007), Pages 171–185

Nice lists of differences, and their connections with algebraic properties of unitary polynomials

Andrea Vietri

Dipartimento Me. Mo. Mat.
Università La Sapienza
via A. Scarpa 16
00161 Rome
Italy
vietri@dmmm.uniroma1.it

Abstract

It has been recently shown (Abel and Buratti, *J. Combin. Theory* A 106 (2004), 59–75) that the product of certain unitary trinomials, yielding a further unitary trinomial, is a basic ingredient for constructing a particular class of optical orthogonal codes in $\mathbf{Z}_p$ with p prime. Every code of this class is generated by an initial base block of size 4 whose set of differences is expressible as $\pm\{1, x, x^2, \ldots, x^5\}$ for some $x \in \mathbf{Z}_p$. In this paper we first generalise the construction of such codes by introducing the notion of *nice list of differences*. In order to generate nice lists we exhibit further unitary trinomials arising as a product of unitary trinomials. To the same end we also find common zeros of some prescribed pairs of trinomials, over all fields $\mathbf{Z}_p$ with $p \geq 17$. Suitable combinatorial structures, namely *quasipairings*, are introduced. The further we proceed, the more quasipairings are shown to have notable connections to unitary polynomials obtainable as ratios of unitary trinomials.

1 Introduction

In keeping with the standard terminology (see e.g. [3]), if S is a finite subset of an additive group then by ΔS — the *list of differences from* S — we denote the multiset $\{s-s' \colon s, s' \in S\ ,\ s \neq s'\}$, while $\pm S$ stands for $\{s, -s \colon s \in S\}$. The following property of subsets of a given finite field $\mathbf{Z}_p$ will be the main object of study in the present paper.

Definition 1.1. Let p be a prime number. A k-subset $A \subseteq \mathbf{Z}_p$, with $k \geq 3$, is said to have a *nice list of differences* if $\Delta A = \pm\{1, x, x^2, \ldots, x^{(k^2-k-2)/2}\}$ for some $x \in \mathbf{Z}_p$.

Because the nice list property is not altered by subtracting any fixed $a \in A$ from each element of the set, we can also assume that $0 \in A$. As a consequence, by possibly changing the sign of all elements, we can eventually assume that

$$A = \{0, 1, s_1 x^{i_1}, s_2 x^{i_2}, \ldots, s_{k-2} x^{i_{k-2}}\},$$

where $s_u \in \{-1, 1\}$ for all u and $i_1, \ldots, i_{k-2}$ are distinct positive numbers not greater than $(k^2 - k - 2)/2$.

Using some classical results from number theory, the existence problem for nice lists of differences with $k = 3$ can be settled in a purely number-theoretical way, as explained in the Appendix. In the less known case $k = 4$, nice lists of differences have been recently employed by Abel and Buratti [2] to construct some new classes of *optical orthogonal codes* (OOC for short).[1] The employment of nice lists in [2] led the authors to prove the following result, which provides the very starting point of the present work (we recall that a *primitive square* $z \in \mathbf{Z}_p$ is an element z which has a square root and whose order is the largest admissible, namely $(p-1)/2$. Furthermore, a base block is termed *initial* if all the other base blocks are multiples of this block; see e.g. [5, 8]).

Theorem 1.2. ([2], Theorem 2.2) *Let $p \geq 13$ be a prime such that there exists $x \in \mathbf{Z}_p$ satisfying the identity $x^3 + x^2 - 1 = 0$. Assume, also, that x^2 is a primitive square in $\mathbf{Z}_p$. Then there exists an optimal $(p, 4, 1)$-OOC with initial base block equal to $\{0, 1, x, x^3\}$.*

The main ingredient of the proof of this theorem is that x satisfies also the identity $x^5 + x - 1 = 0$, which is obtained from the identity appearing in the claim. We have in fact that

$$x^5 + x - 1 = (x^3 + x^2 - 1)(x^2 - x + 1). \tag{1}$$

As pointed out in Lemma 2.1 of [2], these two identities imply that

$$\Delta\{0, 1, x, x^3\} = \pm\{1, x, x^2, \ldots, x^5\}. \tag{2}$$

Consequently, using the primitive square hypothesis, the authors establish the mentioned result using the collection $\{x^{6j} \cdot \{0, 1, x, x^3\} \colon 0 \leq j < \lfloor (p-1)/12 \rfloor\}$, which is easily seen to be an OOC.

The first question we address in the present paper is whether there exist identities similar to (1) — involving unitary trinomials[2] again – which may yield a modified version of Lemma 2.1 and, consequently, of the cited Theorem 2.2. Our request amounts therefore to detecting some other nice lists of differences by means of a product of suitable trinomials, similar to that appearing in (1). The above question

[1] A so-termed $(v, k, 1)$-OOC can be defined as a set of k-subsets of $\mathbf{Z}_v$ — the *base blocks* — $\{\mathcal{C}_1, \mathcal{C}_2, \ldots\}$ whose list of differences $\Delta\mathcal{C}_1 \cup \Delta\mathcal{C}_2 \cup \ldots$ does not have repeated elements. An OOC is *optimal* if the set of base blocks has the largest size allowed, namely $\lfloor (v-1)/(k(k-1)) \rfloor$. If $(v-1)/(k(k-1)) \in \mathbf{N}$ an optimal OOC is clearly equivalent to a $(v, k, 1)$-*difference family* (see e.g. [1, 3] for basic notions about difference families; see [4, 6, 7, 9] for basics on OOC's).

[2] We recall that a polynomial is *unitary* if its coefficients belong to $\{-1, 1\}$.

has an affirmative answer, which will arise as a particular case ($n = 1$) of Corollary 2.3:

Let $f(x)$, $g(x)$ be monic unitary trinomials with $\deg(f) \leq \deg(g)$ *and such that fg is a unitary trinomial of degree at most* 5. *Then the ordered triple (f, g, fg) has precisely one of the three following forms:*

$$(x^2 - \varepsilon x + 1, x^3 + \varepsilon x^2 - \varepsilon, x^5 + x - \varepsilon), \quad (x^2 - \varepsilon x + 1, x^3 - x - \varepsilon, x^5 - \varepsilon x^4 - \varepsilon),$$

$$(x^2 - \varepsilon x + 1, x^2 + \varepsilon x + 1, x^4 + x^2 + 1),$$

with $\varepsilon \in \{-1, 1\}$.

(Notice that, unlike in the other cases, in the last case the two choices of ε produce the same factors.) By the above result, the trinomial $x^3 + x^2 - 1$ appearing in the quoted Lemma 2.1 can be replaced with any of the other three trinomials of degree 3, whence three new identities similar to (1) are obtained (instead, the trinomials of degree 2 cannot be exploited, because the identity $(x^2+\varepsilon x+1)\cdot(x-\varepsilon) = x^3-\varepsilon$ would imply that $x^3 = \varepsilon$, thus clashing with the nice list postulate that forbids repetitions). However, among the three available trinomials we find out that $x^3 - x^2 + 1$ produces the already known list, whereas a unique, new list is produced by $x^3 - x - \varepsilon$ for both choices of ε. The relevant construction of nice lists is subsequently carried out in the same fashion as in [2] (Theorem 2.4).

Corollary 2.3 will be established with the help of the combinatorial structures defined as follows.

Definition 1.3. A *quasipairing* consists of two sets of natural numbers $P = \{0, p_1, p_2\}$, $L = \{0, l_1, \ldots, l_q\}$ (where the indexings preserve $<$) with the following property:

There exists a pair $(p, l) \in P \times L - \{(0, 0), (p_2, l_q)\}$ *such that for any* $(i, j) \in P \times L - \{(0, 0), (p_2, l_q), (p, l)\}$ *there exists a unique* $(i', j') \in P \times L - \{(0, 0), (p_2, l_q), (p, l), (i, j)\}$ *such that* $i + j = i' + j'$.

If $p+l \neq i+j$ for every pair $(i, j) \neq (p, l)$, then (p, l) is termed *singular*. Otherwise, the three elements giving rise to the same sum $p + l$ are said to form a *singular line*. Pairs (of pairs) like $(i, j), (i', j')$ are termed *opposite*.

(Notice that the above definition forces q to be even.) For example, the sets $P = \{0, 1, 2\}$, $L = \{0, 1, 3\}$ form a quasipairing whose singular pair is $(1, 3)$, while $P = \{0, 1, 2\}$, $L = \{0, 1, 2\}$ form a quasipairing whose singular line is $\{(0, 2), (1, 1), (2, 0)\}$. Quasipairings will be represented as in Figure 1.

In Section 2, as a preparatory tool for establishing Proposition 2.2 and hence Corollary 2.3, we associate a given quasipairing (P, L) to a system $S_{(P,L)}$, the solvability of which is equivalent – except in one case – to the existence of a unitary trinomial expressible as a product of a trinomial and a polynomial, both unitary, and whose coefficients are encoded by P and L. Therefore, quasipairing may sometimes provide a combinatorial obstruction to the existence of certain products of polynomials, or be a tool for generating unitary trinomials in a particular fashion.

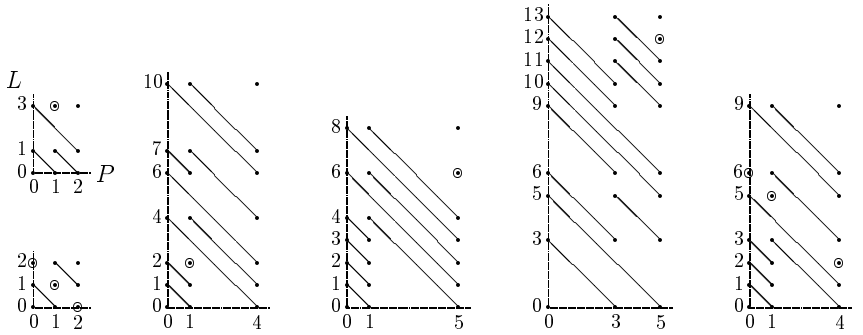

Figure 1: Quasipairings

Leaving aside quasipairings, a natural question is to recognise all those fields $\mathbf{Z}_p$, $p \geq 13$, in which the four trinomial equations of Theorem 2.4 are solvable. A different question is finding *all* solutions to (2) in some fixed field $\mathbf{Z}_p$ without passing through divisibility properties of trinomials. We tackle both these questions in Section 3. The relevant results are condensed in Theorem 3.2. According to its claim, four "sporadic" solutions to (2) in $\mathbf{Z}_{17}$ are exhibited, while all the other solutions—for any $\mathbf{Z}_p$—turn out to depend on whether or not x solves one of the four trinomial equations previously found. Thus, such equations do actually play a major role. Theorem 3.2 is proved in a quite algorithmic fashion.

In Section 4 we come back to quasipairings and study a more general condition than (1), namely by looking for unitary trinomials that arise as a product of two unitary polynomials, only one of which is a trinomial. Although the initial motivation of such study was to obtain existential results on nice lists with $k \geq 5$, a computer search soon showed that $S_{(P,L)}$ is unsatisfiable for any $P = \{0, p_1, p_2\}$ with $p_2 \neq 2p_1$ and $|L| \geq 5$, over all the analysed cases. This noticeable fact led us to conjecture that no satisfiable system exists if $|L| \geq 5$ and $p_2 \neq 2p_1$. As we remark at the end of this work, the truth of such a conjecture might be a basic ingredient for proving the further conjecture that any polynomial ratio of two unitary trinomials is unitary as well.

2 Unitary trinomials and quasipairings

The basic result of this section is the classification of all products of two unitary trinomials yielding a further unitary trinomial. Such classification will, at the end of the section, allow the construction of a new nice lists of differences in the case $k = 4$, using a product of trinomials similar to (1). We will also show that if $k = 4$ no further nice list can arise by resorting to the present technique on products of unitary trinomials.

For our purposes, quasipairings will play a basic role. Let us then start by

associating a given quasipairing (P, L) to a system $S_{(P,L)}$ in $3|L|$ variables, whose values are assumed to belong to $\{-1, 1\}$. Having denoted such variables by $\{x_{ij} : i \in P, j \in L\}$, we define the system via two schemes of equations, as follows.

$$S_{(P,L)}: \begin{cases} x_{ij}x_{i'j'} = x_{i'j}x_{ij'} & \text{for all } i, i' \in P\ ,\ j, j' \in L, \\ x_{ij} = -x_{i'j'} & \text{for all opposite pairs } (i,j),(i',j'). \end{cases}$$

Note that the first scheme of equations is equivalent to the condition that the triples $(x_{0j}, x_{p_1 j}, x_{p_2 j}), (x_{0j'}, x_{p_1 j'}, x_{p_2 j'})$ are proportional for any choice of $j, j' \in L$, because they form a 2×3 matrix of rank 1. Similarly, another equivalent condition is the proportionality of the two $|L|$-tuples corresponding to any two fixed elements of P. It is then clear that many equations in the first scheme are superfluous. As an example, if $P = \{0, 1, 2\}$ and $L = \{0, 1, 3\}$ we obtain the system (with no redundant equations)

$$S_{(P,L)}: \begin{cases} x_{00}x_{11} = x_{01}x_{10} \\ x_{00}x_{21} = x_{01}x_{20} \\ x_{01}x_{13} = x_{03}x_{11} \\ x_{01}x_{23} = x_{03}x_{21} \end{cases} \quad \text{and} \quad \begin{cases} x_{10} = -x_{01} \\ x_{20} = -x_{11} \\ x_{21} = -x_{03} \end{cases}, \quad x_{ij} \in \{-1, 1\}\ \forall\ i, j.$$

Every solution to $S_{(P,L)}$ will be also called a *correct labelling*. As we point out in the following claim, the existence of a correct labelling is equivalent to the existence of a trinomial—unitary in almost all cases—-arising as a product of a unitary trinomial and a unitary polynomial whose coefficients are strictly related to P and L.

Lemma 2.1. *Let $(P = \{0, p_1, p_2\}, L = \{0 = l_0, l_1, l_2, \ldots, l_q\})$ be a quasipairing. The system $S_{(P,L)}$ admits the solution $\{x_{ij} = a_{ij}\}$, with $a_{p_2,0} = 1$, if and only if*

$$(t^{p_2} + a_{p_1,0}t^{p_1} + a_{0,0}) \cdot \sum_{s=0}^{q} a_{p_2,l_s}t^{l_s} = a_{p_2,l_q}t^{p_2+l_q} + Kt^{p+l} + a_{0,0},$$

where $K = a_{p,l}$ if there exists a singular pair (p, l), otherwise $K = a_{0,l} + a_{p_1,l-p_1} + a_{p_2,l-p_2}$, these summands being the labels of the singular line.

(Notice that the condition on $a_{p_2,0}$ can be postulated without losing generality.)

Proof. From the first scheme of $S_{(P,L)}$ we deduce that

$$(t^{p_2} + a_{p_1,0}t^{p_1} + a_{0,0}) \cdot a_{p_2,l_s}t^{l_s} = a_{p_2,l_s}t^{p_2+l_s} + a_{p_1,l_s}t^{p_1+l_s} + a_{0,l_s}t^{l_s}$$

for every s ranging from 0 to q. By summing all the left-hand terms we obtain the product in the claim. Now the second scheme of equations enables us to eliminate all pairs of monomials related to opposite pairs, in the right-hand summation, so as to obtain the required polynomial. □

As a consequence of this lemma, for some fixed unitary trinomial $f(t) = t^{p_2} + bt^{p_1} + c$ we have that each solvable system $S_{(\{0,p_1,p_2\},\{0,l_1,l_2,\ldots,l_q\})}$, with the quasipairing

containing a singular line, corresponds to a unitary trinomial $g(t) = \alpha t^{p_2+l_q} + \beta t^{p+l} + \gamma$ such that g/f is a unitary polynomial. Conversely, and slightly more generally, if some unitary polynomial h is such that fh is a unitary trinomial, then a solvable system $S_{(\{0,p_1,p_2\},\{0,l_1,l_2,\dots,l_q\})}$ exists which may even contain a singular line (what counts is indeed that $|K| = 1$).

We head to the main results of this section by focusing on the case $|L| = 3$. In this case, all solvable systems arising from quasipairings can be easily described:

Proposition 2.2. *Let $(P = \{0, p_1, p_2\}, L = \{0, l_1, l_2\})$ be a quasipairing. The system $S_{(P,L)}$ is solvable if and only if one of the following five parametric cases arises.*

$$P = \{0, n, 3n\}, L = \{0, n, 2n\};\ P = \{0, 2n, 3n\}, L = \{0, n, 2n\};$$
$$P = \{0, n, 2n\}, L = \{0, n, 3n\};\ P = \{0, n, 2n\}, L = \{0, 2n, 3n\};$$
$$P = L = \{0, n, 2n\},$$

where n is any positive integer.

(Notice that the two families in the second line are obtained from the upper two by interchanging P and L; for, if $|L| = 3$, $S_{(P,L)}$ is solvable if and only if $S_{(L,P)}$ is.)

Proof. Let us first assume that there exists a singular pair of the form $(0, l)$. After a few experiments the reader will realise that the left diagram at the top of Figure 2 displays the only possible configuration. In order to find all correct labellings of these diagram, we can assume that $x_{3n,0} = 1$. Let us then define $x_{2n,0} = x$. Using some suitable equations in $S_{(P,L)}$ it is possible to recursively evaluate all the other variables. In the end we have two solutions, depending on the choice of $x \in \{-1, 1\}$. Similarly, if the singular pair is of the form (p_2, l) one could easily show that the only possible configuration is the middle one at the top of the figure. Also in this case we obtain two solutions, up to changing the sign of $x_{3n,0}$ ($x_{3n,n}$ has been set equal to x). The three lower configurations are instead the only ones to have a singular pair of the form (p_1, l). The two at the extremes can be managed in a fashion similar to the above, while the middle diagram does not admit any correct labelling. In fact, any of the four choices of the variables x, y produces a contradiction (see the arrow). Finally, the right upper configuration refers to the singular line case, and admits four solutions due to the two free variables. (Notice in passing that, as contemplated in Lemma 2.1, setting $y = -1$ results in a product which is not unitary—due to $K = 3$).

□

The above result, reinforced by the analysis in Figure 2 itself and by Lemma 2.1, yields the

Corollary 2.3. *Let $f(x)$, $g(x)$ be monic unitary trinomials with $\deg(f) \leq \deg(g)$. The polynomial fg is a unitary trinomial if and only if the ordered triple (f, g, fg) is equal either to $(x^{2n} - \varepsilon x^n + 1, x^{3n} + \varepsilon x^{2n} - \varepsilon, x^{5n} + x^n - \varepsilon)$ or to $(x^{2n} - \varepsilon x^n + 1, x^{3n} - x^n - \varepsilon, x^{5n} - \varepsilon x^{4n} - \varepsilon)$, or to $(x^{2n} - \varepsilon x^n + 1, x^{2n} + \varepsilon x^n + 1, x^{4n} + x^{2n} + 1)$, for some $\varepsilon \in \{-1, 1\}$ and some $n \in \mathbf{N}^+$ (in the last case, both choices of ε clearly yield the same factorization).*

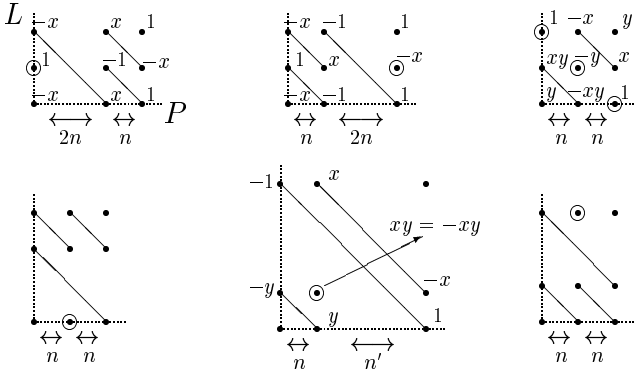

Figure 2: Configurations in the case $|L| = 3$

In the case $n = 1$, the above corollary settles the question of extending (1) to any identity $fg = h$ where f, g, h are monic unitary trinomials and $\deg(f) \leq \deg(g) \leq 5$ (see the Introduction). The relevant claim can be now exploited to generalise the result of Abel and Buratti in [2].

Theorem 2.4. *Let p be a prime greater than 11, and $t \in \mathbf{Z}_p$ be such that $t^3+t^2-1 \equiv 0 \pmod p$. Then each of the sets $\{0, 1, t, t^3\}$, $\{0, 1, -1/t, -1/t^3\}$ has a nice list of differences, obtained using powers of t and of $1/t$ respectively. As a consequence, if in addition t^2 is a primitive square, there exist two distinct optimal $(p, 4, 1)$-OOC's, whose base blocks are equal to*

$$\left\{t^{6j}A\colon 0 \leq j < \lfloor (p-1)/12 \rfloor\right\}$$

and the block A is one of the above two blocks. No further OOC can be obtained by finding a nice list of differences via a product of unitary trinomials of degree not exceeding 5, yielding a further unitary trinomial.

Proof. The reader can check with little difficulty that the root t in the claim has order greater than 10 (use also the associated equation, namely $t^5 + t - 1 = 0$). Furthermore, each of the pairwise distinct numbers $t, -t, 1/t, -1/t$ easily turns out to solve one, and only one, of the four available trinomial equations in Corollary 2.3 (e.g. $1/t$ is a root of $x^3 - x - 1$). Now a similar argument as in [2] yields a nice list for each case, according to the following scheme.

$$\begin{array}{cccc}
\left\{\begin{array}{l} x^3+x^2-1=0 \\ x^5+x-1=0 \end{array}\right. & \left\{\begin{array}{l} x^3-x^2+1=0 \\ x^5+x+1=0 \end{array}\right. & \left\{\begin{array}{l} x^3-x-1=0 \\ x^5-x^4-1=0 \end{array}\right. & \left\{\begin{array}{l} x^3-x+1=0 \\ x^5+x^4+1=0 \end{array}\right. \\
\downarrow & \downarrow & \downarrow & \downarrow \\
(x=t) & (x=-t) & (x=1/t) & (x=-1/t) \\
\{0,1,x,x^3\} & \{0,1,-x,-x^3\} & \{0,1,-x,-x^4\} & \{0,1,x,-x^4\} \\
\| & \| & \| & \| \\
\{0,1,t,t^3\} & \{0,1,t,t^3\} & \{0,1,-1/t,-1/t^4\} & \{0,1,-1/t,-1/t^4\}
\end{array}$$

A quick glance is enough to see that precisely two distinct lists are obtained. Accordingly, two OOC's can be constructed using the method described in [2], provided t^2 (or, equivalently, $(1/t)^2$) is a primitive square. It is also clear that finding a solution to some trinomial equation different from the one in the claim is equivalent to finding a solution to that equation itself (by performing the sign change, or the inversion, or both). Finally, as noticed in the Introduction, the trinomial equations of degree 2 cannot be used in place of the equations of degree 3 for generating nice lists (in a nice list, repeated elements are not allowed). □

3 Describing all nice lists with $k = 4$

Though one might conceivably object that the above technique is too selective when seeking nice lists with $k = 4$, the lists previously obtained turn out to cover almost all possible cases. To show this, in the present section we analyse all nice lists of blocks $\{0, 1, u, v\}$ in an arbitrary field $\mathbf{Z}_p$. Quasipairings will be, for the moment, dismissed. We can also assume that $p \geq 17$, because every 4-subset $A \subseteq \mathbf{Z}_{13}$ having a nice list of differences is simply a difference set with no further property (by choosing a primitive element, say $t = 2$, we have indeed that $\mathbf{Z}_{13} - \{0\} = \pm\{1, 2, 4, 8, 3 \equiv 2^4, 6 \equiv 2^5\}$).

The following theorem (see e.g. [12] for a proof) will contribute to establish the subsequent result.

Theorem 3.1. (König-Rados Theorem) *Let $f(t) = a_0 + a_1 t + \cdots + a_{q-2} t^{q-2}$ be a polynomial in $\mathbf{F}_q[t]$. The number of nonzero roots of f in $\mathbf{F}_q$ is equal to $q - 1 - r$, where r is the rank of the* circulant matrix

$$\begin{pmatrix} a_0 & a_1 & \dots & a_{q-3} & a_{q-2} \\ a_1 & a_2 & \dots & a_{q-2} & a_0 \\ \vdots & \vdots & & \vdots & \vdots \\ \vdots & \vdots & & \vdots & \vdots \\ a_{q-2} & a_0 & \dots & a_{q-4} & a_{q-3} \end{pmatrix}.$$

In the sequel we will denote such a matrix by $\mathcal{C}_{q-1}(a_0, a_1, \ldots, a_{q-2})$. We now proceed with the main result of the section.

Theorem 3.2. *Let p be a prime greater than 13. A 4-subset $\{0, 1, u, v\} \subseteq \mathbf{Z}_p$ has a nice list of differences $\pm\{1, t, t^2, \ldots, t^5\}$, for some t, if and only if one of the following two cases arises.*

(I) *$p = 17$ and $\{u, v\} \in \{\{5, 7\}, \{5, 8\}, \{10, 13\}, \{11, 13\}\}$. In each of these cases, t^2 is a primitive square.*

(II) *The equation $t^3 + t^2 - 1 = 0$ is solvable in $\mathbf{Z}_p$. Equivalently, p divides* $\det(\mathcal{C}_{p-1}(1, 1, 0, -1, 0, 0, \ldots, 0))$.

None of the former four cases is comprised in the latter class.

Proof. Let us assume that, for some $t \in \mathbf{Z}_p$,

$$\Delta\{0, 1, u, v\} = \pm\{1, t, t^2, \ldots, t^5\} \ . \tag{3}$$

Then, necessarily, u, v are of the form $s_1 t^{i_1}$, $s_2 t^{i_2}$ for some suitable numbers s_1, s_2, i_1, i_2. It follows that for certain $s_1, s_2, s_3, s_4 \in \{-1, 1\}$ and distinct $i_1, i_2, i_3, i_4 \in \{1, 2, 3, 4, 5\}$, the number t satisfies the system

$$\mathcal{S} \ : \quad s_1 t^{i_1} + s_3 t^{i_3} + 1 = 0 \quad \wedge \quad s_2 t^{i_2} + s_4 t^{i_4} + 1 = 0, \tag{4}$$

where we can assume, without loss of generality, that $i_1 > i_3$, $i_2 > i_4$ and $i_1 > i_2$. Let us now consider the *resultant*[3] of the trinomials on the left sides. By examining all the possible systems it could be seen that the resultants equal to zero are precisely those related to all pairs (f, fg) and (g, fg) of the trinomials described in Corollary 2.3 with $n = 1$ (not counting the last parametric case, for which the monomial of degree 2 occurs in both trinomials). All other possible solutions to (4) must therefore be related to a nonzero resultant that vanishes only (mod p) for some prime p. The following elementary algorithm can be used to detect any of these latter common roots (mod p), with $p \geq 17$:

Among all non-vanishing resultants, select those divisible for $p = 17$. For each selected resultant try to solve the corresponding system, in $\mathbf{Z}_{17}$. If some solution to the system is also a solution to (3)*, keep track of that solution together with the prime* 17*. Proceed similarly, until all selected resultants are checked. Then choose the prime just larger than p and repeat the whole procedure, until p is large enough (say, more than the largest absolute value of a resultant).*

The above algorithm has been implemented using MATLAB, thus obtaining the only four solutions in the part **(I)** of the theorem. The corresponding values of t are 6, 3, 3, 6 (mod 17) respectively; since 3 and 6 are primitive elements in $\mathbf{Z}_{17}$, the list of differences has no repetitions, while the primitive square property is also satisfied.

Now applying the König-Rados Theorem to the equation in **(II)** yields the equivalent assertion in brackets. Finally, again using MATLAB, we have obtained $\det(\mathcal{C}_{16}(1, 1, 0, -1, 0, 0, \ldots, 0)) = 85 = 5 \cdot 17$. However, the unique root of $t^3 + t^2 - 1$ in $\mathbf{Z}_{17}$ is 7, and $7^3 \equiv 3 \pmod{17}$, whence the resulting pair $\{3, 7\}$ is different from any of the above 4 pairs. □

As a result of the above result we obtain some OOC's (this discovery is admittedly not so crucial, because the existence of such OOC's could be proved directly, without invoking nice lists).

Corollary 3.3. *There exist four optimal* $(17, 4, 1)$*-OOC's with base block equal to* $\{0, 1, 5, 7\}, \{0, 1, 5, 8\}, \{0, 1, 10, 13\}, \{0, 1, 11, 13\}$ *respectively.*

[3] The resultant of two polynomials of degree m and n is, loosely speaking, the determinant of an $(m + n) \times (m + n)$ matrix obtained by positioning, in a prescribed way, the coefficients of the two polynomials. For details about resultants, see e.g. [11]. We recall that two polynomials $f, g \in K[t]$, K being a field, have some nontrivial common factor if and only if their resultant vanishes. Thus, in particular, having a common root forces the resultant to vanish.

When proving Theorem 3.2 it has been shown that the resultant vanishes in the only cases described in Corollary 2.3, not counting the last. Therefore, if we regard each trinomial as belonging to $\mathbf{C}[t]$, we can well say that the trinomials appearing in those cases are the only ones to have some common root among all pairs, as $\mathcal{S}$ varies. Although the complex case is not strictly related to nice lists of differences, we deem it worth being highlighted.

Theorem 3.4. *If P and P' are monic unitary trinomials in $\mathbf{C}[t]$ such that $\deg(P) \leq \deg(P') \leq 5$ and no term t^i with $i > 0$ occurs in both trinomials, then $MCD(P, P') = 1$ unless the pair (P, P') is equal to either (f, fg) or (g, fg), where the triple (f, g, fg) has one of the first two forms appearing in Corollary 2.3 with $n = 1$. It follows that there exist $t \in \mathbf{C}$, $s_1, s_2 \in \{-1, 1\}$ and distinct $i_1, i_2 \in \{1, 2, 3, 4, 5\}$ such that $\Delta\{0, 1, s_1 t^{i_1}, s_2 t^{i_2}\} = \pm\{1, t, t^2, \ldots, t^5\}$, with no repeated elements, if and only if t is a root of one of the trinomials $x^3 + x^2 - 1$, $x^3 - x^2 + 1$, $x^3 - x - 1$, $x^3 - x + 1$.*

4 Quasipairings of larger size

At this stage it is clear that quasipairings having $|L|$ arbitrarily large are related to all those trinomials obtainable as a product of a trinomial and a polynomial, both unitary. The solvability question for $S_{(P,L)}$ with no restriction on L might turn out to be related to nice lists with $k \geq 5$, by considering more general systems than (4). To say it better, one should succeed in extract some valuable information from the polynomial under examination, so as to obtain identities of the form $s_1 t^{i_1} + s_2 t^{i_2} + 1 = 0$, as already done in the case $|L| = 3$. Also, one might wonder if more than 2 unitary equations are satisfiable, provided the bound on the degree is increased. Leaving aside these good reasons for studying general quasipairings, we admit that such combinatorial structures seem to us interesting enough in their own right. Let us therefore devote the present section to analysing general quasipairings which yield solvable systems $S_{(P,L)}$, also casting a glance at connections with divisibility properties of unitary polynomials. In accordance with the above formalism, some particular cases of unsolvability can be swiftly detected, as for example the one depicted in Figure 3 (we assume, without loosing generality, that $a_{1,4} = 1$).

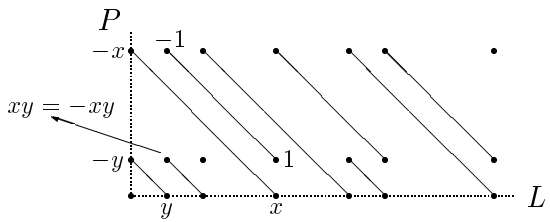

Figure 3: A contradiction in $S_{(\{0,1,4\},\{0,1,2,4,6,7,10\})}$

The reader will observe that this quasipairing—as well as the middle one at the

bottom of Figure 2—enjoys the following property.

$$\textit{For some index } i\ ,\ \{l_i + p_1, l_i + p_2\} \subseteq L\ . \qquad (\mathcal{P})$$

In our example such property is satisfied if either $i = 0$ or $i = 4$. Diagrams of quasipairings for which $(\mathcal{P})$ holds can be easily recognised, as they are characterised by containing two pairs of opposite points whose connecting edges are the bases of an isosceles trapeze. The following claim will now relate $(\mathcal{P})$ to the solvability question.

Proposition 4.1. *If (P, L) satisfies $(\mathcal{P})$, then $S_{(P,L)}$ is not solvable.*

Proof. We generalise the proof illustrated in the above figure. If some index i makes $(\mathcal{P})$ hold, then the assignments

$$x_{0,l_i+p_1} = y\ ,\ x_{0,l_i+p_2} = x\ ,\ x_{p_1,l_i+p_2} = 1$$

force the further assignments

$$x_{p_1,l_i} = -y\ ,\ x_{p_2,l_i} = -x\ ,\ x_{p_2,l_i+p_1} = -1\ .$$

Hence, x_{p_1,l_i+p_1} should be equal to both xy and $-xy$, which is a contradiction. □

Remarkably, a computer search performed over all quasipairings with $q \leq 8$, $p_2 \leq 20$, $l_q \leq 35$ has shown that quasipairings not satisfying $(\mathcal{P})$, and with $|L| > 3$, are all of the form $(\{0, p, 2p\}, L)$. We were consequently led to the

Conjecture 4.2. *Let (P, L) be a quasipairing which does not satisfy $(\mathcal{P})$, and assume that $P = \{0, p_1, p_2\}$ with $p_2 \neq 2p_1$. Then $|L| = 3$.*

Proposition 4.1 along with Proposition 2.2 and the above conjecture, if true, would provide an affirmative answer to the

Conjecture 4.3. *If $P = \{0, p_1, p_2\}$ with $p_2 \neq 2p_1$, the system $S_{(P,L)}$ is unsolvable unless $|L| = 3$ and one of the following two cases arises:*

$$p_2 = 3p_1,\ l_1 = p_1,\ l_2 = 2p_1; \quad p_1 = 2l_1,\ p_2 = 3l_1,\ l_2 = 2l_1.$$

Equivalently, let $\alpha(x)$, $\beta(x)$ be monic unitary trinomials such that $\deg(\alpha) \leq \deg(\beta)$, with α not of the form $x^{2n} + ax^n + b$. Then β/α is a unitary polynomial in $\mathbf{C}[x]$ if and only if the triple $(\beta/\alpha, \alpha, \beta)$ has one of the forms appearing in Corollary 2.3 (except the last form).

Let us finally concentrate on the remaining cases, namely those where $p_2 = 2p_1$.

Theorem 4.4. *The pair $(\{0, p, 2p\}, L)$ is a quasipairing if and only if there exist two multiples of $3p$, say M and Ω, such that $0 \leq \Omega \leq M$, $M \geq 3p$, and*

$$L = \{0, p, 2p, ..., M\} \\ -(\{x \leq \Omega - p\colon x \equiv 2p \pmod{3p}\} \cup \{x \geq \Omega + p\colon x \equiv E \pmod{3p}\})\ ,$$

where $E \in \{0, p\}$. The singular line case occurs precisely when $\Omega < M$ and $E = 0$.

(For example, if $|L| = 3$ we find again the three admissible configurations in Figure 2, with (M, Ω, E) equal to $(3n, 0, 0), (3n, 0, n), (3n, 3n, E)$; notice that, in general, E has no effect if $\Omega = M$.)

Proof. Let us first assume that the quasipairing contains a singular point of the form (p, l). Then, by direct construction it could be easily seen that l is a multiple of $3p$ and that the elements of L smaller than l (if any of these exists) are precisely all multiples of p not congruent to $2p \pmod{3p}$. Similarly, the elements of L that are greater than l (if any exists) are characterised by being multiples of p not congruent to $p \pmod{3p}$, and the largest of them is a multiple of $3p$. It could be also seen with few difficulties that no configuration can have the first component of the singular pair different from p. Finally, a singular line occurs if and only if 9 points are arranged in a square. Again by direct construction, one sees that the corresponding elements of L must be consecutive and of the form $3hp, 3hp + p, 3hp + 2p$ with $h \geq 0$, while all preceding [all following] numbers are precisely the multiples of p not congruent to $2p$ [to 0] $\pmod{p}$, the largest number being congruent to $2p \pmod{p}$. By defining Ω as either l or $3hp$, and M as either the largest element of L or the largest plus p, respectively in the singular pair and singular line case, we obtain the claimed assertion. □

The above characterisation is useful to get some insight about a special class of unitary trinomials:

Proposition 4.5. *Let ε be chosen in $\{-1, 1\}$, n be a positive natural number, and define $S(\alpha)$ as the remainder of the Euclidean division of the natural number α by 2. The unitary trinomials in $\mathbf{C}[x]$, arising as a product of $x^{2n} + \varepsilon x^n + 1$ times a unitary polynomial $f(x) \neq 1$ such that $f(0) = 1$, are precisely those of the form*

$$\varepsilon^{S(M)} x^{(M+2)n} + \varepsilon^{1-S(\Omega)} x^{(\Omega+1)n} + 1,$$

where M, Ω are multiples of 3 such that $0 \leq \Omega \leq M$, and those of the form

$$\varepsilon^{1-S(M)} x^{(M+1)n} + \varepsilon^{S(\Omega)} x^{(\Omega+2)n} + 1,$$

where M, Ω are multiples of 3 such that $0 \leq \Omega < M$. Instead, no unitary trinomial can be likewise obtained as a multiple of $-x^{2n} + \varepsilon x^n + 1$.

We omit the relevant proof, which is essentially based on the same heuristic argument as in the proof of Proposition 2.2. One in fact realises that in the present case the 3 points in the first row must be labelled respectively by $1, \varepsilon, 1$, while all other rows turn out to be univocally labelled, without ever reaching a contradiction. An equivalent result can be likewise established in terms of monic polynomials.

5 Concluding remarks

Quasipairings can be generalised by allowing the singular pairs to be as many as any fixed natural number (possibly zero):

Definition 5.1. Let d be a non-negative integer. A *d-quasipairing* consists of two sets of natural numbers $P = \{0, p_1, p_2\}$, $L = \{0, l_1, \ldots, l_q\}$ (where the indexings preserve $<$) with the property that there exist d pairs $(\bar{p}_1, \bar{l}_1), \ldots, (\bar{p}_d, \bar{l}_d) \in P \times L - \{(0,0), (p_2, l_q)\}$ such that

$$\forall (i,j) \in P \times L - \{(0,0), (p_2, l_q), (\bar{p}_1, \bar{l}_1), \ldots, (\bar{p}_d, \bar{l}_d)\}$$

$$\exists! (i', j') \in P \times L - \{(0,0), (p_2, l_q), (\bar{p}_1, \bar{l}_1), \ldots, (\bar{p}_d, \bar{l}_d), (i,j)\} : i + j = i' + j'.$$

For example, $(\{0,1,2\}, \{0,1,3,4,6,7\})$ is a 0-quasiparing, whereas $(\{0,1,3\}, \{0,3,4,5\})$ is a 2-quasiparing. Without going into details, we limit ourselves to say that an adequate understanding of d-quasipairings with $0 \leq d \leq 2$ (including both the affirmative answer to Conjecture 4.2 and some results on solvability in the same vein as in Proposition 2.2) might be in our opinion crucial for giving an affirmative answer to the

Conjecture 5.2. *If $g(t)$, $h(t)$ are unitary trinomials such that h/g is a polynomial in $\mathbf{C}[t]$, then h/g is unitary.*

Notice that the above conjecture does not hold in the case of ratios of unitary quadrinomials. For example, we have that $(t^3+t^2+t+1)(t^2-2t+1) = t^5-t^4-t+1$.

To conclude the present study, we want to stress the fact that quasipairings theory does not take into account most algebraic properties of finite fields. Quite conceivably, the detection of polynomial ratios of unitary trinomials with coefficients in a finite field can be carried out with far more tools. For example, the claim of Exercise 3.95 of [12] provides an interesting suggestion for producing new unitary trinomials as multiples of a fixed unitary trinomial, in some prescribed finite field:

Property 5.3. (Exercise 3.95, [12]) *Let $f(x) = x^n + ax^k + b \in \mathbf{F}_q[x]$, with $n > k \geq 1$, and let $m \in \mathbf{N}$ be a multiple of* $\mathrm{ord}(f)$ *(namely, the least positive integer e such that f divides $x^e - 1$). Then f divides the trinomial $x^{m-k} + b^{-1}x^{n-k} + ab^{-1}$.*

Examples like this, however, do not prevent us from feeling that quasipairings still conceal some fascinating and exploitable arithmetical properties.

Appendix

As mentioned in the Introduction, nice lists with $k = 3$ can be completely characterised, using some tools from classical number theory.

Proposition 5.4. *Let p be a prime number greater than 5. There exists a 3-subset of $\mathbf{Z}_p$ with a nice list of differences if and only if either $p \equiv 1 \pmod 6$ or $p \equiv \pm 1 \pmod{10}$.*

Proof. Under the requirement that $\Delta\{0, 1, sx^i\} = \pm\{1, x, x^2\}$ for some $x \in \mathbf{Z}_p$, with $s \in \{-1, 1\}$ and $i \in \{1, 2\}$, 4 cases arise.

(**1**) $s = i = 1$. In this case, either $x^2 + x - 1 \equiv 0$ or $x^2 - x + 1 \equiv 0 \pmod{p}$. In the first subcase, using the well-known formula for quadratic equations we find that the existence of a solution is equivalent to the existence of a square root of 5 in that field. Now the *quadratic reciprocity law*[4] implies that the last condition is equivalent to $p \equiv \pm 1 \pmod{10}$. Instead, in the second subcase any solution x is such that $x^3 + 1 = 0$, whence x has order 6. Now according to Fermat's Little Theorem, $x^{p-1} \equiv 1 \pmod{p}$. Therefore, we have that $p \equiv 1 \pmod{6}$. On the other hand, if we consider a primitive element $\theta \in \mathbf{Z}_p$ (thus, the order of θ is $p-1$) with $p \equiv 1 \pmod{6}$, then $\theta^{(p-1)/6}$ solves the equation $x^2 - x + 1 = 0$.

(**2**) $s = -1, i = 1$. In this case either $x^2 + x + 1 = 0$ or $x^2 - x - 1 = 0$ holds. In the first subcase we obtain, similarly as above, $p \equiv 1 \pmod{3}$, which is equivalent to $p \equiv 1 \pmod{6}$. In the other case we require again that $\sqrt{5} \in \mathbf{Z}_p$, and we proceed as above.

The remaining cases (**3**) and (**4**), which we do not mention, can be managed in a similar fashion. □

Acknowledgement

The author is grateful to Professor M. Buratti, for his valuable remarks, as well as for his strong and steady encouragement.

References

[1] R.J.R. Abel, *Difference families*, in: CRC Handbook of Combinatorial Designs (C.J. Colbourn and J.H. Dinitz eds.), CRC Press, Boca Raton, FL, 1996.

[2] R.J.R. Abel and M. Buratti, Some progress on $(v, 4, 1)$ difference families and optical orthogonal codes, *J. Combin. Theory* **A 106** (2004), 59–75.

[3] T. Beth, D. Jungnickel and H. Lenz, *Design theory*, Cambridge University Press, Cambridge, 1999.

[4] C.M. Bird and A.D. Keedwell, Design and applications of optical orthogonal codes — A survey, *Bull ICA* **11** (1994), 21–44.

[5] R.C. Bose, On the construction of balanced incomplete block designs, *Ann. Eugenics* **9** (1939), 353–399.

[6] E.F. Brickell and V. Wei, Optical orthogonal codes and cyclic block designs, *Congressus Numerantium* **58** (1987), 175–182.

[4] See e.g. [10] for details about the quadratic reciprocity law. This celebrated result guarantees, for example, that the equations $x^2 \equiv 5 \pmod{p}$ and $x^2 \equiv p \pmod{5}$ are equivalent, from which we easily obtain the required characterisation of p.

[7] M. Buratti, A packing problem and its application to Bose's families, *J. Combin. Designs* **4** (1996), 457–472.

[8] K. Chen and L. Zhu, Existence of $(q, k, 1)$ difference families with q a prime power and $k = 4, 5$, *J. Combin. Designs* **7** (1999), 21–30.

[9] F.R.K. Chung, J.A. Salehi and V.K. Wei, Optical orthogonal codes: Design, analysis and applications, *IEEE Trans. Inform. Theory* **35** (1989), 13–25.

[10] G.H. Hardy and E.M. Wright, *An Introduction to the Theory of Numbers*, Clarendon Press, Oxford, Fifth edition, 1978.

[11] S. Lang, *Algebra*, Addison-Wesley, Reading, Mass., 1974.

[12] R. Lidl and H. Niederreiter, *Finite Fields*, Addison-Wesley, Reading, Mass., 1983.

(Received 8 Jan 2006)