Contemporary Mathematics
Volume **264**, 2000

Combinatorics and algebra: A medley of problems? A medley of techniques?

Man-Keung SIU
Department of Mathematics
University of Hong Kong

1. A fascinating feature of combinatorics is the intimate relationship between its various topics which look disjoint on the surface, like the emerged parts of an archipelago that are nonetheless joined in one submerged mass underneath. This commonality sometimes allows us to bring algebraic techniques to bear on the different topics when once their relationship with algebra is discerned. In this paper we will sample some of these topics to portray how this can be done. We will cover only a rather small part of the vast subject of combinatorics. Actually, this paper should have been more appropriately titled "Some problems in combinatorics I fail to solve " but for its negative tone. Readers will therefore find more problems than answers in this exposition, culminating in the question whether there is some deeper underlying difficulty lurking in these problems. For more on connections with combinatorics see [20]. For more on analogous problems in the 2-dimensional case of binary arrays, see [21]. For a comprehensive reference for various topics in combinatorics consult [3].

2. After obtaining a PhD from Columbia University and teaching for three years at University of Miami, I returned to my alma mater (University of Hong Kong) in 1975. The research environment of Hong Kong at the time was extremely different from what it is today. Funding for research was virtually non-existent (except perhaps in the long established medical school, which was founded as the Hong Kong College of Medicine twenty four years prior to becoming part of the new University of Hong Kong founded in 1911), hence there was no pressure either — but there was real pleasure — for doing research. International academic interaction was scarce. Communication depended heavily on what is today termed the snail-mail. In one word,

Hong Kong back in those days was an isolated spot as far as research was concerned. I immediately realized the difficulty under these circumstances in keeping up with algebraic K-theory, the research field I started as a graduate student under the supervision of Hyman Bass, now that I was so remote from the hub of it. I tried to seek another topic to work on.

By good chance I came across a topic which caught my fancy. Looking back, I can see that it is the algebraic flavour of the topic more than anything else — not even its practical and technological importance — that caught my fancy. I should acknowledge my sincere gratitude to a senior colleague of mine at University of Miami, Alton Butson, for introducing me to the seminal paper of N. Zierler [24] which served as the bait to lure me on to nevigate the ocean of combinatorics. This topic of my first encounter with combinatorics is linear recurrence sequences, or more generally the study of shift register sequences.

In the course of studying the paper by N. Zierler I came up with an observation, which I still cannot explain to this day. To the best of my knowledge, nobody can explain it either, although from time to time one hears that somebody has settled (an equivalent form of) it, only to find out later that the "proof" contains an error. (See [8].) Let me explain what the problem is. Take a periodic binary sequence $S = (s_0, s_1, s_2, \dots)$ of period v. We will usually denote such a sequence by one period $(s_0, s_1, \dots, s_{v-1})$. Shift the sequence (to the right) by t places, $t \in \{0, 1, \dots, v-1\}$ and compare it with the original sequence to see where the entries coincide and where the entries do not coincide. Suppose one period of S contains k 1s and $v-k$ 0s, and suppose (after shifting by t places) there are η coinciding entries and $v-\eta$ noncoinciding entries, then we define:

$$RP(t) = (\text{number of coinciding entries}) - (\text{number of noncoinciding entries}) = 2\eta - v$$

and

$$BP(t) = \text{number of coinciding } 1s\ .$$

The function $RP(t)$ is called the (**real periodic**) **autocorrelation function** of the sequence S. The function $BP(t)$ is called the (**binary periodic**) **autocorrelation function** of the sequence S.

Example 2.1.

$S = (0\ 1\ 0\ 1\ 0\ 1\ 1)$

t	k	η	$RP(t)$	$BP(t)$
0	4	7	7	4
1	4	1	−5	1
2	4	5	3	3
3	4	3	−1	2
4	4	3	−1	2
5	4	5	3	3
6	4	1	−5	1

Note that $RP(t) = RP(v-t)$, $BP(t) = BP(v-t)$, and $RP(t) = v - 4k + 4BP(t)$. Apart from these, the values of $RP(t)$, $BP(t)$ look erratic.

Example 2.2

$S = (0\ 0\ 1\ 1\ 1\ 0\ 1)$

t	k	η	$RP(t)$	$BP(t)$
0	4	7	7	4
1	4	3	−1	2
2	4	3	−1	2
3	4	3	−1	2
4	4	3	−1	2
5	4	3	−1	2
6	4	3	−1	2

The values of $RP(t)$, $BP(t)$ in Example 2.2 display a nice feature in that $RP(t)$ (and hence $BP(t)$ and vice versa) takes on only two values, one for all in-phase shifts (equivalent to no shifting at all) and one common value for all off-phase shifts. We seek sequences with this **two-level autocorrelation property** with $|RP(t)|$ (or $BP(t)$) small for $t \neq 0$, since they play an important role in electrical and electronic engineering and communication science. It is also one measure of the "randomness" of a sequence. I was led to ask the question:

Do we have a periodic binary sequence possessing the two-level autocorrelation property with the off-phase common value zero?

I could easily find one (actually two, simply by interchanging 0 and 1) up to cyclic permutation, viz. (0 0 0 1) (and (1 1 1 0)). But I could not find any other after much search by trial and error. Upon this rather flimsy evidence I boldly conjectured the following.

Conjecture 2.3

There is no periodic binary sequence with two-level autocorrelation with off-phase value zero except (0 0 0 1) and (1 1 1 0).

Later I found out there are various ways to look at the same problem (see [20]), which led me to the study of different topics in combinatorics. Conjecture 2.3 will appear in the sequel in a different guise. After more than two decades from the time I made that observation I now have more conviction in the validity of Conjecture 2.3.

3. Readers may have guessed that nice sequences such as (0 0 1 1 1 0 1) (see Example 2.2) are not obtained randomly by luck nor laboriously by trial and error. That brings us to the topic of linear recurrence sequences, which has become a standard topic in some textbooks since the mid 1980s (see e.g. [9;12;13;23]).

Let $S = (s_0, s_1, s_2, \dots)$ be a binary sequence satisfying a recurrence relation

$$c_n s_i + c_{n-1} s_{i+1} + \cdots + c_0 s_{i+n} = 0 \quad \text{for all} \quad i \geq 0 \quad (\text{with } c_0 = 1)$$

with pre-assigned $s_0, s_1, \dots, s_{n-1}$ (initial condition). An alternative standard representation is to write it as $AS_i = S_{i+1}$ for all $i \geq 0$, where

$$A = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ -c_n & -c_{n-1} & -c_{n-2} & & -c_1 \end{bmatrix}, \quad S_i = \begin{bmatrix} s_i \\ s_{i+1} \\ \vdots \\ s_{i+n-1} \end{bmatrix}.$$

Note that the characteristic polynomial of A is $\chi_A(X) = (-1)^n f(X)$ where $f(X) = c_n + c_{n-1}X + \cdots + c_1 X^{n-1} + c_0 X^n$ (with $c_0 = 1$). In engineering, such

a sequence can be implemented easily by a device called a **shift register** (see [7]). Since the recurrence relation is linear, we call such a sequence a **linear recurrence sequence** generated by $f(X)$.

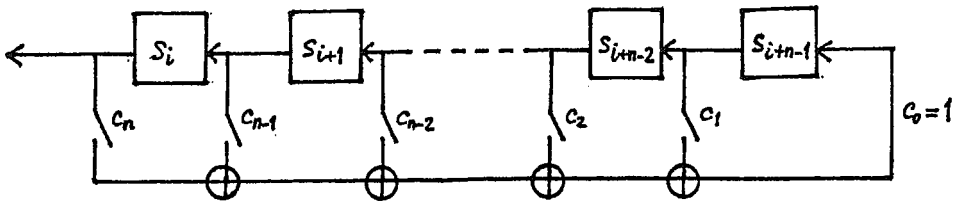


Figure 1

In the following examples we will exhibit $f(X), A$ and the corresponding sequences (with different initial conditions) by the cycle structure of $f(X)$.

Example 3.1

$$f(X) = 1 + X + X^2 + X^3 = (1+X)^3\,, \quad A = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix}$$

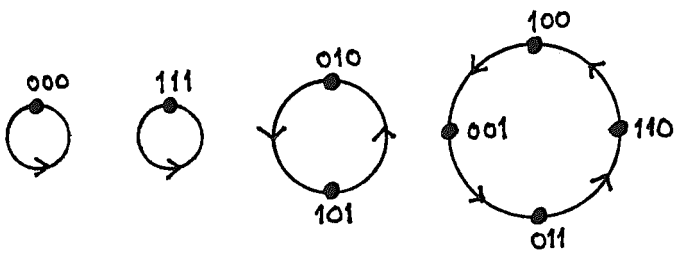


Figure 2

In this case there are 4 possible sequences, viz. (0), (1), (0 1) and (0 0 1 1).

Example 3.2

$$f(X) = 1 + X^2 + X^3\,, \quad A = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{bmatrix}$$

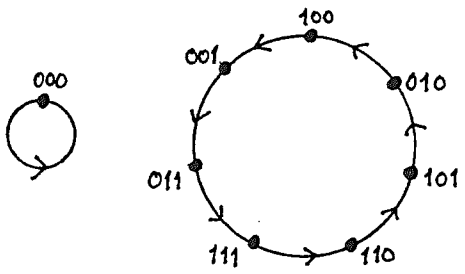


Figure 3

In this case there are only two possible sequences, viz. (0) and (0 0 1 1 1 0 1). Note that the latter sequence is the sequence in Example 2.2.

We are looking for (linear recurrence) sequences of the type depicted in Example 3.2, i.e. sequences generated by $f(X)$ with a very simple cycle structure. By linearity, the addition of two linear recurrence sequences (coordinatewise) generated by $f(X)$ is still a linear recurrence sequence generated by $f(X)$. In particular, the addition of S and S_t (= S shifted by t places to the right) is again a sequence generated by $f(X)$. For instance, take Example 3.1. If $S = (0\,0\,1\,1)$, then $S_1 = (0\,1\,1\,0)$. Note that $S+S_1 = (0\,1)$, which is a sequence generated by the same $f(X) = 1+X+X^2+X^3$ but possibly belonging to another cycle. However, if the cycle structure is of the kind depicted in Example 3.2, then the addition of a nonzero sequence with its own shift is still itself shifted by some places, i.e. $S + S_t = S_{t'}$ for some t'. For instance, take Example 3.2, $S+S_4 = (0\,0\,1\,1\,1\,0\,1)+(1\,0\,1\,0\,0\,1\,1) = (1\,0\,0\,1\,1\,1\,0) = S_6$. An interesting feature about the autocorrelation function follows as a consequence, viz.

$$RP(t) = \begin{cases} \text{period of } S = v = 2^n - 1 & \text{if } t \equiv 0 \pmod{V} \\ (\text{number of } 0s \text{ in } S) - (\text{number of } 1s \text{ in } S) & \\ = (2^{n-1} - 1) - 2^{n-1} = -1 & \text{if } t \not\equiv 0 \pmod{V}\ . \end{cases}$$

Hence S has the two-level autocorrelation property with off-phase value -1.

Where does the algebra come in? It comes in when we ask the natural question:

> What sort of $f(X)$ yields such sequences? More generally, given $f(X)$, can we predict its corresponding cycle structure?

At first, one may think that it has to do with the fact that $f(X)$ is irreducible or not. But the following example shows that irreducibility of $f(X)$ is not

enough.

Example 3.3

$$f(X) = 1 + X + X^2 + X^3 + X^4\,, \quad A = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix}$$

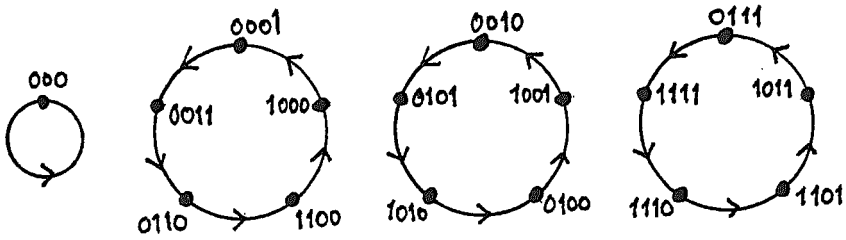


Figure 4

Note that $f(X)$ is irreducible over $\mathbb{F}_2$, but $f(X)$ is not a primitive polynomial.

I will skip the detailed discussion of the complete answer to the question which can be found in [12, Chapter 6; 23, Chapter 3], but give a hint to the key notion of the order of $f(X)$.

Definition 3.4. *Let $f(X) \in \mathbb{F}_q[X]$ with $f(0) \neq 0$. The* **order** *of $f(X)$, denoted by ord (f), is the smallest positive integer e such that $f(X)|X^e - 1$. (Such a positive integer exists. It is actually the order of $X \pmod{f(X)}$ in the multiplicative group of units of $\mathbb{F}_q[X]/\langle f(X)\rangle$. The condition $f(0) \neq 0$ guarantees that X and $f(X)$ are relatively prime so that $X \pmod{f(X)}$ is indeed a unit in $\mathbb{F}_q[X]/\langle f(X)\rangle$).*

When $f(X)$ is irreducible over $\mathbb{F}_q$ of degree n, an alternative way to understand $\mathrm{ord}(f)$ is to describe it as the common order of all zeros of $f(X)$, regarded as elements in the multiplicative group of the finite field $\mathbb{F}_{q^n}$, which is a finite extension of $\mathbb{F}_q$ of degree n. In particular, we see that f is a primitive polynomial of degree n if and only if $\mathrm{ord}(f) = q^n - 1$.

It turns out the cycle structure of an irreducible polynomial $f(X)$ over $\mathbb{F}_2$ consists of the zero sequence plus $\frac{2^n-1}{\mathrm{ord}(f)}$ cycles, each of length ord (f). Hence, a primitive polynomial $f(X)$ will yield a sequence with maximal

period $2^n - 1$, which is called a **maximal length sequence**. It satisfies the two-level autocorrelation property with off-phase value -1.

However, a sequence with the two-level autocorrelation property need not be a maximal length sequence. Let us look at one kind of example. Consider a sequence $S = (s_0, s_1, s_2, \dots)$ with $s_0 = 0$ and for $i \not\equiv 0 \pmod{p}$

$$s_i = \begin{cases} 0 & \text{if } i \text{ is a quadratic residue } \pmod{p} \\ 1 & \text{otherwise .} \end{cases}$$

Example 3.5

$p = 7$,

i	0	1	2	3	4	5	6
s_i	0	0	0	1	0	1	1

It can be shown that $\mathcal{S}$ has the two-level autocorrelation property if and only if $p \equiv 3 \pmod{4}$ (see [1, Chapter 5]). Take $p = 31$. The resulting sequence has the two-level autocorrelation property, but it is not a linear recurrence sequence because it violates the property that the addition of itself with a shifting is a shifting.

4. Let us digress for a while from autocorrelation function and dabble at a generalization of a linear recurrence sequence $(s_0, s_1, s_2, \dots)$ by formulating its generating polynomial from a slightly different perspective. We consider a polynomial

$$F(X_0, X_1, \dots, X_n) = F_1(X_0, X_1, \dots, X_{n-1}) + X_n$$

in the polynomial ring $\mathbb{F}_2[X_0, X_1, \dots, X_n]$ in $n+1$ indeterminates over the finite field $\mathbb{F}_2$. By writing F in this particular form, we regard F_1 as an element in $\mathbb{F}_2[X_0, X_1, \dots, X_{n-1}]$. With $s_0, s_1, \dots, s_{n-1}$ pre-assigned, the binary sequence $(s_0, s_1, s_2, \dots)$ is generated to satisfy

$$F(s_i, s_{i+1}, \dots, s_{i+n}) = 0 \quad \text{for all} \quad i \geq 0 \ .$$

Note that we recover a linear recurrence sequence when F is a **linear** polynomial, viz.

$$F = c_n X_0 + c_{n-1} X_1 + \cdots + c_1 X_{n-1} + c_0 X_n \quad (\text{with } c_0 = 1) \ .$$

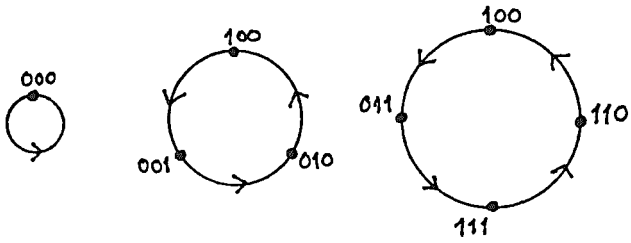
(In the former language, F will be identified as the polynomial

$$f(X) = c_n + c_{n-1}X + \cdots + c_1X^{n-1} + c_0X^n \quad (\text{with } c_0 = 1)$$

in one indeterminate over $\mathbb{F}_2$.)

The following are some examples with the cycle structure depicted along with the generating polynomial.

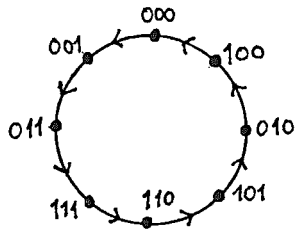
Example 4.1



$F(X_0, X_1, X_2, X_3) = X_0 + X_1X_2 + X_3$

Figure 5

Example 4.2



$F(X_0, X_1, X_2, X_3) = X_0 + X_1 + X_1X_2 + 1 + X_3$

Figure 6

As in the linear case, a sequence of maximal period is again of great interest. Such an example is afforded in Example 4.2, viz. (0 0 0 1 1 1 0 1). The long history of this kind of sequences dated back to a problem solved by C. Flye-Sainte Marie in 1894 and the independent work of N.G. de Bruijn and I.J. Good in 1946. We call such a sequence a **de Bruijn-Good sequence**. (For a good survey, see [5].)

By deleting one zero term from the zero n-tuple of a de Bruijn-Good sequence we obtain a sequence which resembles a maximal length sequence in one respect, viz. all the $2^n - 1$ n-tuples of the resulting sequence are

distinct. However, a sequence obtained in this manner from a de Bruijn-Good sequence may not be a maximal length (linear recurrence) sequence. For instance, (0 0 0 0 1 1 1 1 0 1 1 0 0 1 0 1) is a de Bruijn-Good sequence, but (0 0 0 1 1 1 1 0 1 1 0 0 1 0 1) is not a maximal length (linear recurrence) sequence, since it can be directly checked that its autocorrelation is not two-level. Actually we can count the number of de Bruijn-Good sequences of span n, which far exceeds the number of maximal length (linear recurrence) sequences.

For a period of time in the late 1970s I made an attempt to build up an analogous theory for the **nonlinear** recurrence sequences, i.e. given

$$F(X_0, X_1, \ldots, X_n) = F_1(X_0, X_1, \ldots, X_{n-1}) + X_n \ ,$$

calculate the cycle structure of sequences generated by F. I failed to obtain a theory as complete as that for the linear case, only managed to prove an analogous result about the "containment of cycle structures" as follows.

Theorem 4.3. *(See [15]) Let* $F(X_0, X_1, \ldots, X_n) = F_1(X_0, X_1, \ldots, X_{n-1}) + X_n$ *and* $G(X_0, X_1, \ldots, X_m) = F_1(X_0, X_1, \ldots, X_{m-1}) + X_m$, *then* $F \| G$ *if and only if* $\Omega(F) \subset \Omega(G)$. *Here*

$$\Omega(F) = \{(s_0, s_1, s_2, \ldots) | F(s_i, s_{i+1}, \ldots, s_{i+n}) = 0 \quad \textit{for all } i \geq 0\}$$

and

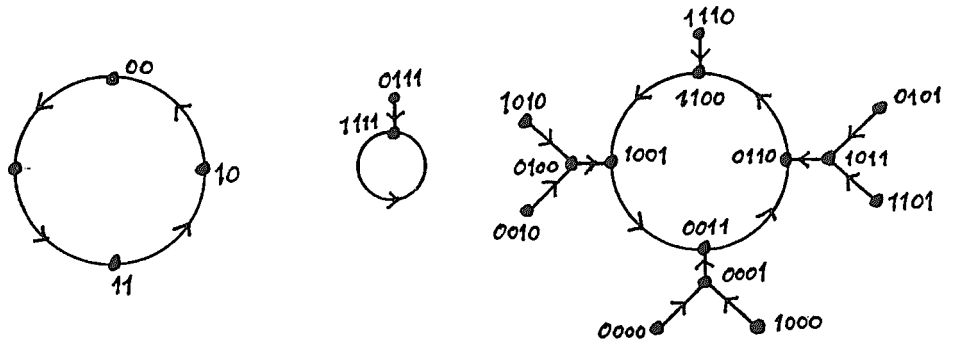
$$\Omega(G) = \{(s_0, s_1, s_2, \ldots) | G(s_i, s_{i+1}, \ldots, s_{i+n}) = 0 \quad \textit{for all } i \geq 0\} \ .$$

What do we mean by $F \| G$? We define

$$\delta F(X_0, X_1, \ldots, X_n) = F(X_1, X_2, \ldots, X_{n+1}) \ ,$$
$$\delta^2 F(X_0, X_1, \ldots, X_n) = \delta[\delta F(X_0, X_1, \ldots, X_n)] \ , \quad \text{etc.}$$

If $P(\delta) = \Sigma \alpha_i \delta^i$ where α_i is a Boolean function, then we denote $P(\delta)F = \Sigma \alpha_i (\delta^i F)$. Finally, we say that $F \| G$ if and only if $G = P(\delta)F$ for some $P(\delta)$. Note that with this definition, Theorem 4.3 specializes in the linear case to the well-known result that $f | g$ if and only if $\Omega(f) \subset \Omega(g)$. The following example illustrates the theorem.

Example 4.4



$F = X_0 + 1 + X_2$

$G = X_2 + X_1X_2X_3 + 1 + X_4$
$G = (X_1X_2\delta + \delta^2)F$.

Figure 7

Another attempt was explained in [17]. As far as I am aware of, the problem remains unsolved to this day. In the late 1970s I was completely ignorant of the notion, not even the name, of Gröbner basis. I wonder whether that can provide a tool to crack this open problem.

5. Let us go back to the two-level autocorrelation property. Suppose $(s_0, s_1, \ldots, s_{v-1})$ is a binary sequence satisfying the two-level autocorrelation property. Consider $D = \{d_1, \ldots, d_k\} \subset \mathbb{Z}/v\mathbb{Z}$ in which $i \in D$ if and only if $s_i = 1$. It can be shown that D satisfies the following property:

$$\begin{aligned} &\text{For } t \neq 0,\ d_i - d_j = t \text{ has exactly} \\ &\lambda \text{ solution pairs } (d_i, d_j) \in D \times D\ . \end{aligned} \qquad (*)$$

Conversely, if $D \subset \mathbb{Z}/v\mathbb{Z}$ satisfies $(*)$ and $(s_0, s_1, \ldots, s_{v-1})$ is defined by putting $s_i = 1$ if and only if $i \in D$, then $(s_0, s_1, \ldots, s_{v-1})$ will be a sequence (of period v) with two-level autorcorrelation property with $\lambda = BP(t)$.

Example 5.1

$S = (0\ 0\ 1\ 1\ 1\ 0\ 1)$, $D = \{2, 3, 4, 6\} \subset \mathbb{Z}/n\mathbb{Z}$.

Such a subset D of $\mathbb{Z}/v\mathbb{Z}$ is called a **difference set** with parameters (v, k, λ) in the cyclic group $\mathbb{Z}/v\mathbb{Z}$. Clearly we have $k(k-1) = \lambda(v-1)$.

CASE I: $\lambda = 0$.

This is impossible unless $k = 0$ or 1, corresponding to the sequence with all

terms zero or the sequence with exactly one term 1 (in one period).

CASE II: $\lambda = 1$.

Then $v = k^2 - k + 1$. Putting $k = n + 1$, we see that $v = n^2 + n + 1$. The corresponding difference set has parameters $(n^2+n+1, n+1, 1)$ with $n \geq 1$. This kind of difference set is called a **planar** difference set because J. Singer constructed them in 1938 out of hyperplanes in finite projective geometries based on a finite field [19]. For this reason, n is a prime power.

Example 5.2

$n = 2$, $v = 2^2 + 2 + 1 = 7$, $k = n + 1 = 3$, $\lambda = 1$

Set $\mathbb{F}_8 = \mathbb{F}_2[X]/\langle 1+X^2+X^3\rangle$ and $\alpha = X \pmod{1+X^2+X^3}$ is a primitive element.

	α_2	α	1		$T_r(\alpha^i) = \alpha^i + \alpha^{2i} + \alpha^{4i}$
0	0	0	0	0	0
A	0	0	1	1	1
B	0	1	0	α	1
C	1	0	0	α^2	1
D	1	0	1	α^3	0
E	1	1	1	α^4	1
F	0	1	1	α^5	0
G	1	1	0	α^6	0

Note that the last column with the first term deleted gives the sequence (1 1 1 0 1 0 0), which is (0 0 1 1 1 0 1) shifted by two places to the right. Note also that we can represent the situation in the following configuration (called the Fano's seven-point configuration or the finite projective plane of order 2 over $\mathbb{F}_2$), which is the "Coat-of-Arms" of researchers in combinatorial designs.

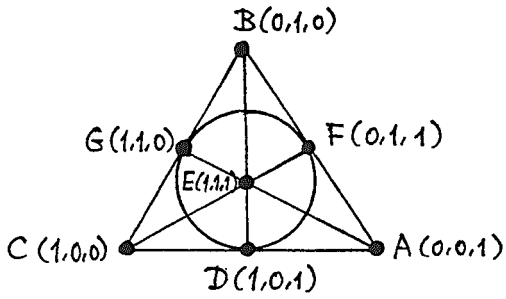


Figure 8

For instance, $\{C, E, F\}$ corresponds to the hyperplane $Y + Z = 0$.

So far nobody has constructed a planar difference set with n not equal to a prime power. A famous conjecture says that the order n $(= k - \lambda)$ of a planar (v, k, λ) difference set is equal to a prime power. An even stronger conjecture says that the only planar difference sets are those constructed by J. Singer. A related conjecture is the long-standing one that says the order of a finite projective plane is a prime power.

CASE III: $RP(t) = 0$ for all $t \not\equiv 0 \pmod{v}$.

By a counting argument on coinciding $0s$ and $1s$ and noncoinciding (0, 1) and (1, 0), we can show that $RP(t) \equiv v \pmod 4$. Moreover

$$v = v + \sum_{t=1}^{v-1} RP(t) = \sum_{t=0}^{v-1} RP(t) = \sum_{t=0}^{v-1}\sum_{i=0}^{v-1}(-1)^{s_i}(-1)^{s_i+t} = \sum_{i=0}^{v-1}(-1)^{s_i} .$$

Hence, $v = 4N^2$ for some positive integer N. The corresponding difference set has parameters $(4N^2, 2N^2 + N, N^2 + N)$ or $(4N^2, 2N^2 - N, N^2 - N)$. (1 1 1 0) corresponds to $\{0, 1, 2\} \subset \mathbb{Z}/4\mathbb{Z}$. We will discuss only the former case as the latter is merely its complement.

Conjecture 2.3 can be rephrased as the following.

Conjecture 5.3

There exists no difference set in $\mathbb{Z}/v\mathbb{Z}$ with parameters $(4N^2, 2N^2 + N, N^2 + N)$ except for $N = 1$.

In this form, the conjecture sounds much more plausible in view of a famous (stronger) conjecture credited to H. Ryser (see [2, Chapter 6]).

Conjecture 5.4

If a (v, k, λ)-difference set exists with n $(= k-\lambda)$ not equal to 0 or 1 in $\mathbb{Z}/v\mathbb{Z}$, then $(v, k) = 1$ (or equivalently $(v, n) = 1$). (In [18, Chapter 9] H. Ryser mentioned a special case of this in the language of circulant **Hadamard matrix**, viz. there does not exist a circulant Hadamard matrix of order greater than 4.)

Along this line of thought, E.S. Lander proposed an even more general conjecture [11, Chapter 6]:

Conjecture 5.5

If D is a (v, k, λ)-difference set with n $(= k - \lambda)$ not equal to 0 or 1 in an abelian group G with a cyclic Sylow p-subgroup, then p does not divide (v, k).

Note that in this form, the cyclic feature is being highlighted. Conjecture 5.4 is false if the group is not required to be cyclic. One counter-example is given by the (16, 6, 2)-difference set $D = \{a, b, c, d, ab, cd\}$ in the group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ where a, b, c, d are the generators of each summand.

For more relationships of this problem with other objects of combinatorial interest, see [20]. This is a convenient point to inject a side-remark on ternary sequence, in which case it is possible to construct a sequence with two-level autocorrelation property with off-phase value zero. Let us look at just one type of construction by V.P. Ipatov in 1979/1980 (see [4, Chapter 7]).

Example 5.6

Find a primitive polynomial over $\mathbb{F}_3$ of degree 3, say $f(X) = 1 + 2X + X^3$. It generates a maximal length sequence (0 0 1 0 1 2 1 1 2 0 1 1 1 0 0 2 0 2 1 2 2 1 0 2 2 2). Construct from this sequence the following ternary sequence:

$$c_i = \begin{cases} (-1)^i \psi(s_i) & \text{if } s_i \neq 0 \\ 0 & \text{if } s_i = 0\ , \end{cases}$$

where $\psi(1) = 1$, $\psi(2) = -1$. The resulting sequence (0 0 + 0 + + + − − 0 + − +) is of period 13 and has the desired property. (Here for ease of typing we replace $1, -1$ by $+$ and $-$ respectively.)

6. Let me conclude this paper with one more frequently used technique, that of **characters** of a finite abelian group or the arithmetic of **cyclotomic fields**. This technique has become an important tool in the field of difference sets ever since its introduction by R. Turyn in his seminal paper [22]. (For an updated account, see [10;16]). I will illustrate through a specific problem about the (binary periodic) autocorrelation function of a binary array, which is defined in an analogous way, viz.

$$BP(u,v) = \text{number of coinciding } 1s$$

when the $r \times s$ array A is compared with itself shifted u places down and v places to the right. We look for an $N \times N$ binary array with $BP(u,v) \leq 1$ for all $(u,v) \not\equiv (0,0) \bmod (N,N)$ and with exactly one 1 in each column. This kind of array, called an **ideal matrix** in communication science, is useful for frequency-hopping technique in satellites and cellular phones. Let the array be (a_{ij}) and consider $D = \{(j,i) \in \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} | a_{s-1-i,j} = 1\}$. If we write $f(j) = i$ where $a_{s-1-i,j} = 1$, then we can also write

$$D = \{(j, f(j)) \in \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} | j \in \{0, 1, \ldots, N-1\}\} .$$

Note that $BP(u,v)$ is equal to the number of j among $0, 1, \ldots, N-1$ such that $f(j+v) + u = f(j)$.

Example 6.1

$$\begin{array}{c|ccccc} 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 2 & 0 & 0 & 0 & 0 & 0 \\ 3 & 0 & 1 & 0 & 0 & 0 \\ 4 & 0 & 0 & 0 & 0 & 0 \\ \hline & 0 & 1 & 2 & 3 & 4 \end{array}$$

$$D = \{(0,3), (1,1), (2,3), (3,4), (4,4)\}$$

j	0	1	2	3	4
$f(j)$	3	1	3	4	4

We can express our goal in two different versions.

(1) Find $f : \mathbb{Z}/N\mathbb{Z} \to \mathbb{Z}/N\mathbb{Z}$ such that if $f_v : \mathbb{Z}/N\mathbb{Z} \to \mathbb{Z}/N\mathbb{Z}$ is defined by $f_v(j) = f(j+v) - f(j)$, then f_v is bijective for each $v \not\equiv 0 \pmod{N}$. In the literature, such a function f is called a **planar function**.

(2) Each $t \in G \setminus H$ (where $G = \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$, $H = 0 \times \mathbb{Z}/N\mathbb{Z}$) appears exactly once in the set $\{d - d' | d, d' \in D, d \neq d'\}$. D is called a **relative difference set.**

The first version has a deceptively elementary appearance, while the second version is more amenable to algebraic technique in a group algebra $\mathbb{C}[G]$. Represent D as an element $\sum_{g \in D} g$ in $\mathbb{C}[G]$, which for convenience is also denoted as D by abuse of notation. Let D^{-1} denote the set $\{g^{-1} | g \in D\}$, which also means $\sum_{g \in D} g^{-1}$. The condition stated in version (2) is translated into an equation in $\mathbb{C}[G]$, viz.

$$DD^{-1} = G - H + Ne \ , \qquad (**)$$

where e is the identity element in G. The strategy is to analyze $(**)$ through characters. Let me illustrate with a specific case, say $N = 3p$ where p is a prime number. Consider the homomomorphism $\rho = \rho_2 \circ \rho_1$ where $\rho_1 : G \to H$ is the projection onto H and $\rho_2 : H \to H/\langle (0,3) \rangle = K \cong \mathbb{Z}/3\mathbb{Z}$ is the natural epimorphism. From $(**)$ we obtain the equation in $\mathbb{C}[K]$

$$\begin{aligned}(\rho D)(\rho D^{-1}) &= \rho G - \rho H + N\rho(e) \\ &= 3p^2 K - pK + 3pe = (3p^2 - p)K + 3pe \ .\end{aligned}$$

Define $\chi : \mathbb{C}[K] \to \mathbb{C}$ by $\chi(a_0 + a_1 x + a_2 x^2) = a_0 + a_1\omega + a_2\omega^2$ where $\omega = e^{2\pi i/3}$. Then

$$\begin{aligned}\chi(\rho D)\chi(\rho D^{-1}) &= (3p^2 - p)\chi(1 + x + x^2) + 3p\chi(e) \\ &= (3p^2 - p)(1 + \omega + \omega^2) + 3p = 3p \ .\end{aligned}$$

Put $z = \chi(\rho D)$, so $\overline{z} = \chi(\rho D^{-1})$. Hence we have $z\overline{z} = 3p$. The problem is reduced to a problem in factorization in $\mathbb{Z}[\omega]$. In terms of ideals,

$$\langle z \rangle \langle \overline{z} \rangle = \langle 3 \rangle \langle p \rangle \ .$$

Suppose $\langle z \rangle = Q_1 \ldots Q_t$ where Q_i are prime ideas, then $\langle \overline{z} \rangle = \overline{Q_1} \cdots \overline{Q_t}$. From elementary algebraic number theory we know that

$$\langle p \rangle = \begin{cases} \mathcal{P}^2 & \text{if } p = 3 \\ \mathcal{P}_1\mathcal{P}_2 & \text{if } p \equiv 1 \pmod 3 \\ \mathcal{P}_3 & \text{if } p \equiv 2 \pmod 3. \end{cases}$$

where $\mathcal{P} = \langle 1-\omega \rangle$, $\mathcal{P}_1$, $\mathcal{P}_2$, $\mathcal{P}_3$ ($\mathcal{P}_1 \neq \mathcal{P}_2$) are prime ideals. Hence

$$Q_1 \dots Q_t \overline{Q_1} \dots \overline{Q_t} = \begin{cases} \langle 1-\omega \rangle^4 & \text{if } p = 3 \\ \mathcal{P}_1 \mathcal{P}_2 \langle 1-\omega \rangle^2 & \text{if } p \equiv 1 \pmod 3 \\ \mathcal{P}_3 \langle 1-\omega \rangle^2 & \text{if } p \equiv 2 \pmod 3. \end{cases}$$

By unique factorization in $\mathbb{Z}[\omega]$ we conclude right away $p \not\equiv 2 \pmod 3$. Can $p = 3$? If $p = 3$, then $Q_1 \dots Q_t \overline{Q_1} \dots \overline{Q_t} = \langle 1-\omega \rangle^4$, so it follows that $\langle z \rangle = \langle 1-\omega \rangle^2 = \langle 3 \rangle$ so that $\chi(\rho D) \equiv 0 \pmod 3$. Applying a similar argument to χ' where $\chi'(a_0 + a_1 x + a_2 x^2) = a_0 + a_1 \omega^2 + a_2 \omega$, we obtain $\chi'(\rho D) \equiv 0 \pmod 3$. Using a more refined "Fourier analysis" (see [6]) we can show that $p = 3$ is impossible. More generally we can prove the following result, leading to a conjecture.

Theorem 6.2. *(See [6]) If N is odd and not square-free, then there does not exist an $N \times N$ ideal matrix.*

Conjecture 6.3

An $N \times N$ ideal matrix exists if and only if N is an odd prime number. (When N is an odd prime number, it has been proved that the corresponding planar function must be a quadratic function.)

It can be shown that from an $N \times N$ ideal matrix we can construct a finite projective plane of order N. Hence if the long-standing conjecture that the order of a finite projective plane is a prime power, then Theorem 6.2 is enough to clinch Conjecture 6.3. It has been proved that Conjecture 6.3 is true for $N = pq$ where p, q are prime numbers (see [14]). In particular, the first undecided case is $N = 15655$.

We can ask another analogous question on a binary periodic $r \times s$ array with two-level autocorrelation property with common off-phase value zero, i.e.

$$RP(u,v) = \begin{cases} rs & \text{if } (u,v) \equiv (0,0) \bmod (r,s)\ , \\ 0 & \text{otherwise}\ . \end{cases}$$

Unlike the one-dimensional case of sequences, there are lots of these, corresponding to what are known as **Menon difference sets** (or **Hadamard difference sets** by some authors). For more on this topic, see [2, Chapter 6;10;21].

References

[1] L.D. Baumert, *Cyclic Difference Sets*, Springer-Verlag, Berlin-Heidelberg-New York, 1971.

[2] T. Beth, D. Jungnickel, H. Lenz, *Design Theory, Volume I and II, Second Edition*, Cambridge University Press, Cambridge, 1999; originally published by BI-Wissenschaftsverlag, Mannheim, 1986.

[3] C.J. Colbourn, J.H. Dinitz (eds.), *The CRC Handbook of Combinatorial Designs*, CRC Press, Boca Raton, 1996.

[4] P.Z. Fan, M. Darnell, *Sequence Design For Communications Applications*, Wiley, New York, 1996.

[5] H.M. Fredricksen, A survey of full length nonlinear shift register cycle algorithms, *SIAM Rev.*, 24(1982), 195-221.

[6] C.I. Fung, M.K. Siu, S.L. Ma, On arrays with small off-phase binary autocorrelation, *Ars Combinatoria*, 29A(1990), 189-192.

[7] S.W. Golomb, *Shift Register Sequences*, Holden Day, San Francisco, 1967; revised edition, Aegean Park, Laguna Hill, 1980.

[8] J. Jedwab, S. Lloyd, A note on the nonexistence of Barker sequences, *Designs, Codes & Cryptography*, 2(1992), 93-97.

[9] D. Jungnickel, *Finite Fields: Structure and Arithmetics*, BI-Wissenschaftsverlag, Mannheim, 1993.

[10] D. Jungnickel, A. Pott, Difference sets: An introduction, in *Difference Sets, Sequences and Their Correlation Properties*, edited by A. Pott et al, Kluwer Academic Publishers, Dordrecht, 1999, 259-295.

[11] E.S. Lander, *Symmetric Design: An Algebraic Approach*, Cambridge Univ. Press, Cambridge, 1983.

[12] R. Lidl, H. Niederreiter, *Introduction to Finite Fields and Their Applications*, Cambridge Univ. Press, Cambridge, 1986; revised edition, 1994.

[13] R. Lidl, G. Pilz, *Applied Abstract Algebra*, Springer-Verlag, Berlin-Heidelberg-New York, 1984.

[14] S.L. Ma, Planar functions, relative difference sets and character theory, *J. Algebra*, 185(1996), 342-356.

[15] J. Mykkeltveit, M.K. Siu, P. Tong, On the cycle structure of some nonlinear shift register sequences, *Inform. Control*, 43(1979), 202-215.

[16] A. Pott, *Finite Geometry and Character Theory*, Springer-Verlag, Berlin-Heidelberg-New York, 1995.

[17] C. Ronse, *Feedback Shift Registers*, Springer-Verlag, Berlin-Heidelberg-New York, 1984.

[18] H. Ryser, *Combinatorial Mathematics*, Math. Asso. Amer., Washington, D.C., 1963.

[19] J. Singer, A theorem in finite projective geometry and some applications to number theory, *Trans. Amer. Math. Soc.*, 43(1938), 377-385.

[20] M.K. Siu, From binary sequences to combinatorial designs, *J. Math. Res. Exposition*, 9(1989), 605-621.

[21] M.K. Siu, The combinatorics of binary arrays, *J. Stat. Planning & Inference*, 62(1997), 103-113.

[22] R. Turyn, Character sums and difference sets, *Pacific J. Math.*, 15(1965), 319-346.

[23] Z.X. Wan, *Algebra and Coding* (in Chinese), Science Press, Beijing, 1976; revised edition 1980 (partly translated as *Introduction to Abstract and Linear Algebra*, Studentlitteratur, Lund, 1992).

[24] N. Zierler, Linear recurring sequences, *J. Soc. Ind. Appl. Math.*, 7(1959), 31-48.