Some problems of applied algebra

M. Hazewinkel

Department of Analysis, Algebra and Geometry

Report AM-R9306 August 1993

CWI is the National Research Institute for Mathematics and Computer Science. CWI is part of the Stichting Mathematisch Centrum (SMC), the Dutch foundation for promotion of mathematics and computer science and their applications.
SMC is sponsored by the Netherlands Organization for Scientific Research (NWO). CWI is a member of ERCIM, the European Research Consortium for Informatics and Mathematics.

Copyright © Stichting Mathematisch Centrum
P.O. Box 94079, 1090 GB Amsterdam (NL)
Kruislaan 413, 1098 SJ Amsterdam (NL)
Telephone +31 20 592 9333
Telefax +31 20 592 4199

Some Problems of Applied Algebra

Michiel Hazewinkel

CWI

P.O. Box 94079, 1090 GB Amsterdam, The Netherlands

Abstract

In contrast to 'classical' applied mathematics a number of applications of algebra and combinatorics are discussed. These are detection arrays, chip wiring diagrams, packing problems, and voting systems. I pay particular attention to the times of symmetry, ability to calculate (symbolically), and notation.

AMS Subject Classification (1991): 05B40, 05B10, 05C35, 90A08, 52A40, 20G99, 20G06, 05B25, 51E15.
Keywords & Phrases: shift register, difference set, radar detection, Costas array, finite projective plane, extremal problem, packing problem, symmetry, voting system.

1. Introduction

When the phrase 'applied mathematics' is mentioned, quite often, the image evoked is something like the following

— there is a physical, chemical, biological, geological, technological, ... phenomenon to be studied
— a mathematical model is constructed by means of differential equations or something similar
— these equations are solved numerically (on a computer).

Frequently, there are additional aspects. For instance there may be control variables and the object of the exercise may be to find optimal controls; or there maybe unknown coefficients which need to be estimated.

There is no doubt that differential equations and numerical mathematics are still the workhorse of applied mathematics as it is currently practised (see, e.g. the proceedings of the five ECMI conferences so far [19, 21, 24, 27, 31]). This type of applied mathematics, together with the somewhat separate (from this) disciplines of programming (optimization) and statistics, accounts for a very large part of the applied field.

It is the purpose of this introductory lecture, which is definitely aimed at a rather general diversified audience, to point out and discuss some examples of a very different kind of applied mathematics, and to describe some (open) research problems that come out of it. These kinds of applications are based on discrete mathematics — in the sense of (finite) algebra, combinatorics, logic, ... — rather than continuous (differentiable) mathematics.

The word algebra in the title must be understood in a very wide sense and not as limited to the consideration of such things as groups, rings, algebras (sic!), lattices, ... The title may not give an optimal first global description of this lecture; it is mainly meant to highlight the contrast with 'applied analysis' ('applied differential equations') in the sense indicated above.

Report AM-R9306
ISSN 0924-2953
CWI
P.O. Box 94079, 1090 GB Amsterdam, The Netherlands

The topics discussed below are:
— Wiring diagrams for shift registers
— Symmetry and extremality
— Radar detection patterns
— Voting systems.

This already indicates that I understand 'applied algebra' as covering quite a large array of tools and results. Other examples include the use of Lie algebras to construct and analyse filters for stochastic dynamical systems with noise disturbed observations [20], aspects of such things as Fourier and wavelet analysis having to do with the encoding of the transformed data and the construction of suitable mathematical microscopes, the devising of suitable notations to help describe and control complicated procedures (such as those describing, the information flow during a large (distributed) numerical a symbolic computation).

A notation which reflects underlying (regular) algebraic structures will be far more useful and enlightening than just any numbering of the objects involved. In some cases this is automatic (almost). Thus Fourier and wavelet coefficients a_k, $s_{a,b}$ actually are labelled by the elements of the underlying group.

In general this matter of good and efficient notations seems to be a virtually unexplored area of 'applied algebra'. Yet, as Leibniz already remarked, good notation is very important. It is a substantial aid in doing mathematics; both for human understanding and for communication with computing machines.

2. Wiring diagrams for shift registers[1]

The general problem is as follows. There are a number of "chips", say, $\{1, \ldots, n\}$; these are connected via "pins" to "busses". It is desired to wire things together so that the contents of the chips can be rearranged (permuted) in one write–read operation. For instance in a case of 4 chips it may be desired to rearrange things according to the following permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}$$

so that after the write–read operation

chip 3	has	the	old	contents	of	chip	1
chip 4	"	"	"	"	"	"	2
chip 2	"	"	"	"	"	"	3
chip 1	"	"	"	"	"	"	4.

It may not be necessary to be able to handle all rearrangements but only a certain collection of them (a subgroup of the group of all permutations). For instance *shift registers* can realize all cyclic permutations

[1] I thank E. Kranakis who first told me about this class of problems.

$$\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix},\quad \begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix},\quad \begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix}.$$

This problem can be solved for instance by having one bus for each pair of chips, i.e. $\frac{1}{2}n(n-1)$ busses, and $n-1$ pins for each chip. This is illustrated for $n=4$ in Figs 1 and 2 below. This solution makes all permutations possible but is (for large n) very wasteful in busses; it is also wasteful in pins and those are expensive. Clearly the minimal number of busses required is n. So let us take that and then try to minimize the number of pins. In that case there is always a solution with $\#G-1$ pins per chip (fairly obviously) but this is very wasteful in pins. It turns out that on the order of $\sqrt{\#G}$ pins is always sufficient. This is also (asymptotically) the best that is possible.

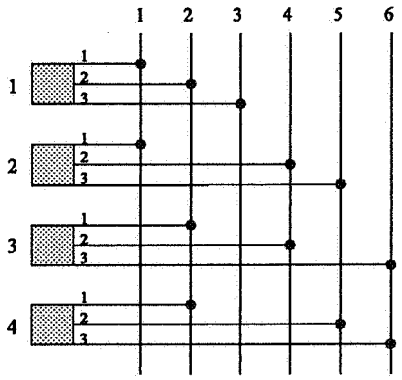

Figure 1

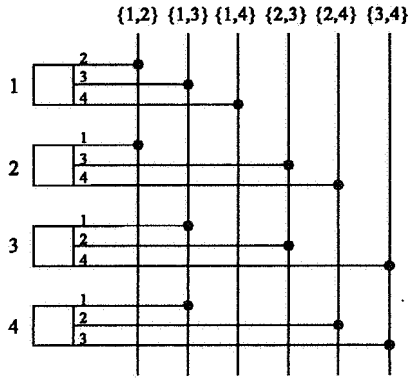

Figure 2

But first let us more carefully examine the wasteful solution below. The recipe (instructions) for realizing the permutation

$$\begin{pmatrix}1&2&3&4\\3&4&2&1\end{pmatrix}$$

are as follows:

chip 1:	write to pin 2:	read from pin 3
chip 2:	write to pin 3:	read from pin 2
chip 3:	write to pin 2:	read from pin 1
chip 4:	write to pin 1:	read from pin 2.

A separate 'instruction table' like this is needed for every separate permutation.

This illustrates in a mild way some of what I meant in the introduction with my remarks on "algebra and notation". There is a much better way to label the busses and pins that systematizes both the wiring requirements and the write-read instructions. This goes as follows: pins of chip i are labelled with the set $\{1,2,3,4\}\backslash\{i\}$, and the bus connecting chip i and chip j is labelled $\{i,j\}$ (the unordered pair i,j).

The wiring is as follows:

chip i connects with pin j ($\neq i$) to bus (i,j)

and the write–read instructions to realize a permutation σ:

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ \sigma(1) & \sigma(2) & \sigma(3) & \sigma(4) \end{pmatrix}$$

are:

chip i:
if $\sigma(i) = i$ do nothing
if $\sigma(i) = j$ write to pin j, read from that pin k for which $\sigma(k) = i$, i.e. $k = \sigma^{-1}(i)$.

Let us show that this works (very elementary):

chip i writes to pin $\sigma(i)$ so that bus $\{i,\sigma(i)\}$ now has those data;
chip j reads from pin $\sigma^{-1}(j)$, i.e. from bus $\{j,\sigma^{-1}(j)\}$.

Thus chip j gets the data from that chip i for which

$$\{i,\sigma(i)\} = \{j,\sigma^{-1}(j)\}$$

so that indeed $\sigma(i) = j$.

Let me now concentrate on cyclic shift registers. More precisely wirings with n chips and n busses for which every cyclic shift

$$i \mapsto i + s \bmod n$$

can be realized in one write-read operation (one clock-tick). For instance for $n = 7$ the shift by 3:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 5 & 6 & 7 & 1 & 2 & 3 \end{pmatrix}.$$

Below, in Fig. 3, there is depicted a solution (for $n = 7$) and the curious and/or mistrustful reader is invited to check that indeed for all seven cyclic shifts there is a "write-read instruction table" which produces the desired result. Three of these tables are written out in Table 1 below Figure 3.

On examining these one notices that the various "read pin" and "write pin" columns are often identical. This suggests that there is a certain 'hidden' symmetry in the arrangement. And indeed there is. By relabelling (and redrawing) busses and pins a very regular arrangement is produced. It is depicted in Fig. 4 below.

The solution depicted in Fig. 4 is extremal in the sense that for (identical) chips with each k pins the number k is minimal. Moreover any minimal solution (with $k = 3$) is like the one depicted. That is up to renumbering the busses and pins the wiring diagram is given by diagonal straight lines.

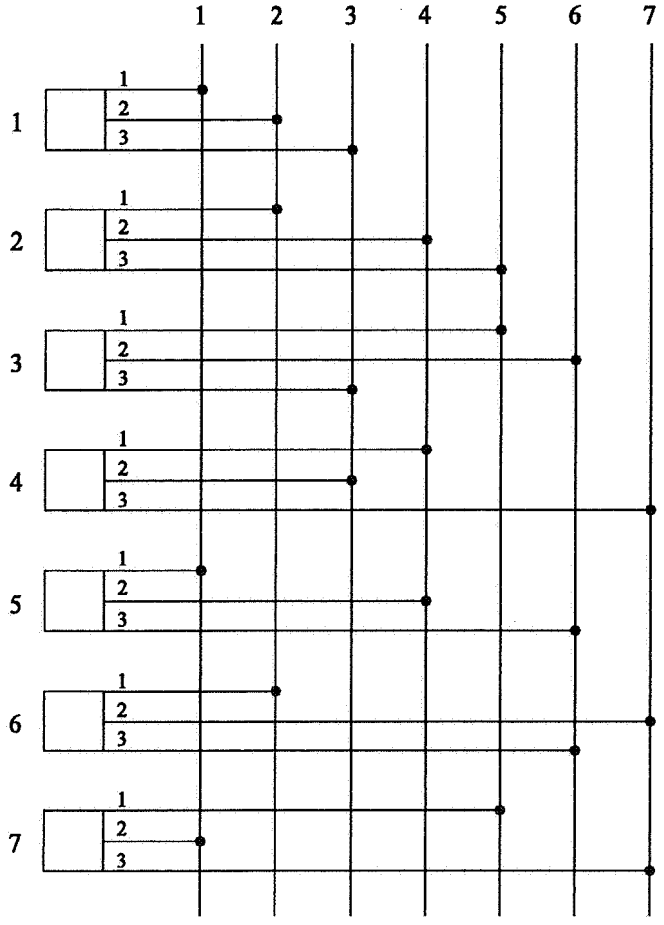

Figure 3

This illustrates a second research direction I want to point-out: a sort of meta-mathematical principle that says that extremal solutions tend to be highly symmetric. There are (besides the one just discussed) all kinds of examples that suggest that some 'principle' like the one just mentioned should be true (under suitable circumstances). The matter is discussed in more detail in Section 3 below.

The construction given above of the 7 bus, 3 pin solution of the wiring problem is based on the notion of a *difference set.*

A difference cover for $\mathbb{Z}/(7)$, the integers modulo 7, is a collection of numbers $D = \{d_1, \ldots, d_r\}$ such that for each $j = 1, 2, \ldots, 7$ there are d_a and d_b in D such that

$$j \equiv d_a - d_b \bmod 7.$$

Table 1

Three write–read instruction tables								
Recipe for a shift of 4			Recipe for a shift of 2			Recipe for a shift of 1		
chip	write pin	read pin	chip	write pin	read pin	chip	write pin	read pin
1	1	3	1	3	2	1	2	1
2	1	2	2	2	3	2	3	1
3	1	2	3	2	3	3	3	1
4	2	3	4	3	1	4	1	2
5	2	1	5	1	3	5	3	2
6	3	1	6	1	2	6	2	3
7	3	1	7	1	2	7	2	3

A minimal difference cover is one of minimal size. A *difference set* is one for which for each $j \not\equiv 0 \bmod 7$ there is precisely one pair (d_a, d_b) such that $j = d_a - d_b \bmod 7$. These are optimally efficient difference covers.

For example $\{0, 1, 3\}$ is a difference set for $\mathbb{Z}/(7)$. Indeed

$$1 \equiv 1 - 0 \bmod 7 \qquad 4 \equiv 0 - 3 \bmod 7$$
$$2 \equiv 3 - 1 \bmod 7 \qquad 5 \equiv 1 - 3 \bmod 7$$
$$3 \equiv 3 - 0 \bmod 7 \qquad 6 \equiv 0 - 1 \bmod 7$$

and as there are precisely 6 pairs (d_a, d_b) with $d_a \neq d_b$ this is indeed a difference set.

A difference set for $\mathbb{Z}/(13)$ is

$$\{0, 1, 3, 9\}.$$

A difference set for $\mathbb{Z}/(91)$ is

$$\{1, 2, 4, 10, 28, 50, 57, 62, 78, 82\}.$$

Difference sets are rather rare. One obvious restriction is that for a difference set for $\mathbb{Z}/(n)$ one must have that $n = k(k-1)$ for some natural number k. This, however, by no means suffices. Indeed for $n \leq 10000$ they only exist for $n = 3$, 7, 13, 21, 31, 57, 73, 91, 133, 183, 273, 307, 381, 553, 651, 757, 871, 993, 1057, 1407, 1723, 1893, 2257, 2451, 2863, 3541, 3783, 4161, 4557, 5113, 5403, 6321, 6643, 6973, 8011, 9507; i.e. for only 36 cases out of 10000.

Given a difference cover $D = (d_1, \ldots, d_k)$ for $\mathbb{Z}/(n)$ the general wiring and write–read instructions are as follows:

Wiring diagram: chip i is connected by pin j to bus $i + d_j \pmod n$.
Write–read instructions: for shift s find d_i, d_j such that $s = d_i - d_j$.
Chip k writes to pin i and reads from pin j.

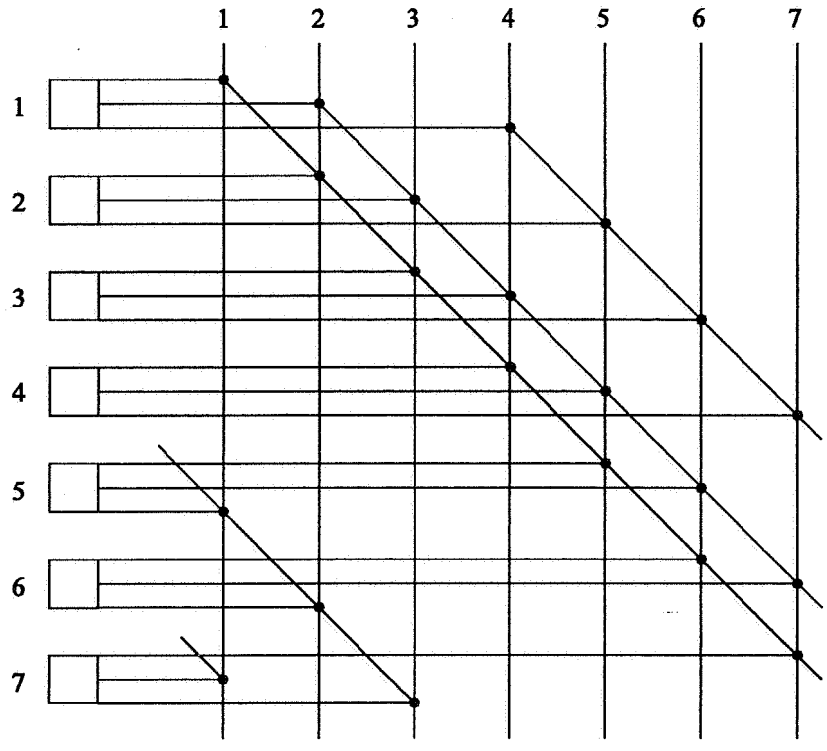

Figure 4

To see that this works note that chip k writes to bus $k+d_i$; chip x reads via pin j, i.e. it reads from bus $x+d_j$. The chip x that reads from bus $k+d_i$ hence satisfies $x+d_j = k+d_i$, i.e. $x = k+d_i-d_j = k+s$ (modulo n).

Note the conciseness and regularity of both the wiring diagram and the write–read instructions as compared to the diagrams and write–read tables of Fig. 3, and Table 1.

The wiring diagram for the cyclic shift register of $\mathbb{Z}/(13)$ based on the difference set $\{0,1,3,9\}$ is depicted below in Fig. 5. In general, for arbitrary n, there is no difference set (as already noted), but one can always find a difference cover with roughly $\sqrt{n}$ elements (which is close to optimal, because the number of elements in the difference cover must satisfy $k(k-1) \geq n$). More precisely there always exists a difference cover of size $\leq 2\lceil\sqrt{n}\rceil - 1$ where $\lceil x\rceil$ denotes the smallest integer equal or larger than x.

More generally one considers an arbitrary finite group $G \subset S_n$ of desired permutations (of the contents) of n chips and the problem of realizing each $g \in G$ in one write–read operation. A difference cover in this setting is a subset $D = \{d_1, \ldots, d_k\} \subset G$ such that for each $g \in G$ there are d_i, d_j in G such that $g = d_j^{-1} d_i$.

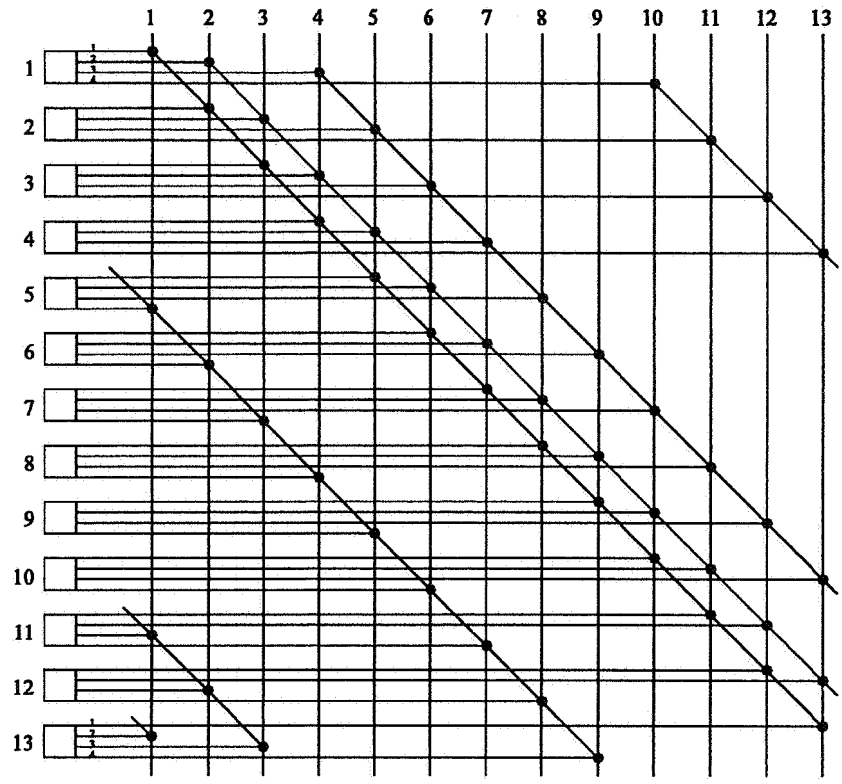

Figure 5

Given such a (noncommutative) difference cover the wiring and write–read instructions are practically the same as in the cyclic case:

Wiring diagram: chip i connects via pin j to bus $d_j(i)$ (recall that $d_j \in D \subset G \subset S_n$, the group of permutations of $\{1, \ldots, n\}$).

Write–read instructions: for a given $g \in G$ find d_i, d_j such that $g = d_j^{-1} d_i$; then, to realize g, chip k writes to pin i and reads from pin j. Let's check that this works.

Chip k writes to pin i, i.e. bus $d_i(k)$; chip x reads from pin j, i.e. bus $d_j(x)$. Thus the chip which receives the contents of chip k satisfies $d_j(x) = d_i(k)$ or $x = d_j^{-1} d_i(k)$ as desired.

In the general case also, for arbitrary finite groups G, it turns out that there exist difference covers of the order of $\sqrt{\#G}$ elements; more precisely there always exists one of $\leq 3\sqrt{\#G}$ elements. This is of the same order of magnitude as the theoretical minimum for the size of a difference cover which is $\lceil \sqrt{\#G} \rceil$ if $\#G$ is of the form $n^2 - n + 1$ and $\lceil 1/2 + \sqrt{\#G} \rceil$ otherwise. The proof uses that every noncyclic group G has a proper subgroup of order $\geq \sqrt{\#G}$. This theorem, in turn,

is proved (at present) by using the classification theorem of the finite simple groups. No other proof is presently known, then this kind of explicit checking of all cases.

Cf. [11, 23] for more details on some of the above.

For the cyclic case a number of systematic constructions of difference sets are known. One of the most useful ones (for moderate size n) is based on the finite projective planes $\mathbb{P}(2, \mathbb{F}_q)$ where $\mathbb{F}_q$ is the finite field of q elements. I will describe the recipe in Section 4. This yields an example for all n of the form $q^2 + q + 1$ with q a power of a prime number. For instance $q = 9$, $n = 91$, the difference set of 10 elements given above. There is nothing like a complete theory even in the cyclic case. In the general case of arbitrary groups almost nothing is known.

3. Symmetry and Extremality

In Section 2 above we saw that an optimal solution of the wiring problem for shift registers was very symmetric. This sort of thing happens quite often, or in any case often enough to merit serious investigation. All the more so because in practice one naturally tends to look for (more or less) symmetric arrangements when trying to construct something optimal. Here are some examples ranging from the trivial and well-known to perhaps some lesser known and more sophisticated instances.

A circle is the closed curve in the plane that for a given length surrounds the largest area.

A number of rather striking examples, in my opinion, come from the theory of systems of intersecting subsets. Consider a set X of size n and systems $\mathfrak{G}$ of subsets of X with various perscribed intersection behaviours, and lets try to find maximally large $\mathfrak{G}$ with such an intersection behaviour.

For instance consider systems $\mathfrak{G}$ of subsets of X such that for all $F_1, F_2 \in \mathfrak{G}$ their intersection is nonempty. The Erdös–Ko–Rado theorem, [10], says that the maximal $\mathfrak{G}$ are those consisting of all subsets of X containing one fixed element. A very regular sort of solution. If one requires that the intersections $F_1 \cap F_2$ may have all cardinalities except 1 the answer is that the maximal $\mathfrak{G}$ consists of all sets containing a fixed two element set, [13], provider $k \geq 4$, n big enough.

At the opposite of the scale for this type of combinatorial problem, let us consider systems of subsets such that the cardinality of the intersections can have only a few values. For instance let us look for systems of subsets $\mathfrak{G}$ such that all intersections $F_1 \cap F_2$ have precisely one element. Then the de Bruijn–Erdös theorem, [7], says that $\#\mathfrak{G} \leq n$ and if $\#\mathfrak{G} = n$ then there are two possibilities:

(i) all members of $\mathfrak{G}$ have the same number of elements k, and each element of X occurs in precisely k members of $\mathfrak{G}$; these are the finite projective planes (including the (degenerate) plane of three elements and three lines ("the projective plane over the field of 1 element")).

(ii) up to relabelling the system $\mathfrak{G}$ is $S_1 = \{1, 2, \ldots, n-1\}$, $S_i = \{i, n\}$, $i =$

$1, \ldots, n-1$.

A finite projective plane is a finite set X (whose elements are called points) with a system of subsets of $\mathfrak{G}$ (whose elements are called lines), such that each two distinct lines intersect in precisely one point and such that there is precisely one line through each two distinct points. It follows that there are precisely $n = \#X$ lines, that all lines have the same number of points $k+1$, that there are precisely $k+1$ lines passing through each point and that $n = k^2 + k + 1$. A very regular (symmetric) structure indeed. The standard illustration for $k = 2$, $n = 7$, is depicted below. The lines are the six straight lines drawn and the circumscribed circle of the triangle.

Given a finite field $\mathbb{F}_q$ of q elements where q is a power of a prime, for example $\mathbb{F}_p = \mathbb{Z}/(p)$ the standard projective plane whose points are ratios $(x : y : z)$ of 3 elements of $\mathbb{F}_q$ (not all zero) provides an example with $q^2 + q + 1$ points. The example of Figure 6 is the standard projective plane over $\mathbb{F}_2 = \mathbb{Z}/(2)$.

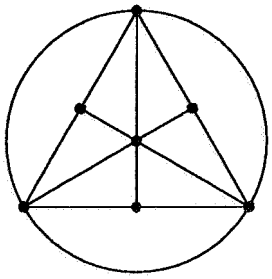

Figure 6

A beautiful generalization of the de Bruijn–Erdös theorem, due to Ryser, [30], deals with the case that the intersections $F_1 \cap F_2$ all have cardinality $\lambda > 1$. There are again two kinds of extremal cases generalizing (i) and (ii), respectively. The generalization of (i) that turns up is the class of symmetric block designs.

The extremal cases of sets where just a few (instead of one) intersection cardinalities are allowed are also very regular. For instance, if the allowed intersection cardinalities are 0 and $r \geq 0$, the extremal families (for $n = \#X$ large enough) look as follows, [14]: write X as a disjoint union $S_1 \cup S_2 \cup \cdots \cup S_{\lfloor n/r \rfloor} \cup S_0$ where each of the S_i, $i = 1, 2, \ldots, \lfloor n/r \rfloor$, has r elements, $\lfloor n/r \rfloor$ is the largest integer $\leq n/r$, and S_0 contains the remaining elements. The extremal family $\mathfrak{G}$ consists of all the unions $S_i \cup S_j$, $i \neq j$, the sets S_i, and all the singleton sets from S_0. This only holds for large enough n compared to r.

To see the symmetry of the situation (apart from the "boundary effects" represented by S_0) one can picture things as follows:

One has a regular k-gonal cyclinder (where $k = \lfloor n/r \rfloor$). The vertical ribs are the sets S_i, $i = 1, \ldots, \lfloor n/r \rfloor$. The sets of $\mathfrak{G}$ are the loose points of S_0, the ribs themselves,

and all vertical diagonal planes through two ribs (including the sides). Besides the sides only one of these diagonal planes is drawn in Fig. 7.

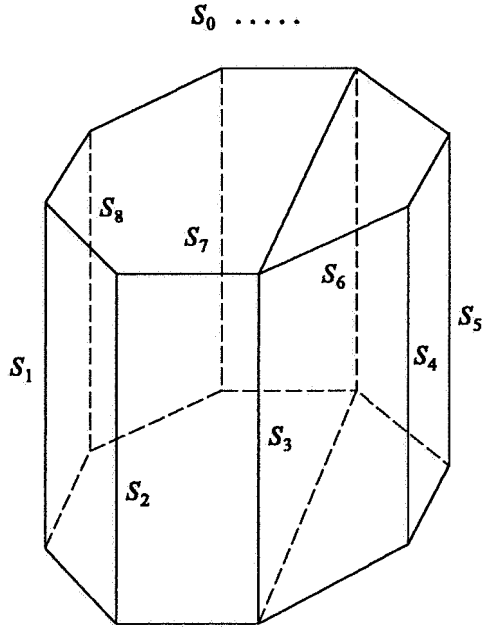

Figure 7

When three intersection cardinalities $0, 1, k$ are allowed (and n is big enough with respect to k) the extremal examples are in fact the finite projective spaces $\mathbb{P}^t$ over $\mathbb{F}_q$, the field of q elements, $k = q+1$, $n = (q-1)^{-1}(q^{t+1}-1)$, and the set $\mathfrak{S}$ consists of the subspaces of dimensions $0, 1$, and 2 of $\mathbb{P}^t$, [15].

A rather different kind of "extremal implies symmetry" group of theorems is exemplified by "turnpike theory". The first turnpike theorem was enunciated in [8]. The setting is economic growth theory, where the state of an economy at a given time is represented by an n-vector x of (capital goods). A von Neumann growth path is one of the form

$$x(t) = \phi(t)(a_1, \ldots, a_n),$$

where $(a_1, \ldots, a_n)$ is a fixed vector and $\phi(t)$ is a scalar valued function. These solutions are highly symmetric in that the relative growth rates of all goods are the same. The initial turnpike theorems said that 'roughly' the fastest way to get from an initial state to a desired final state is to go first to a von Neumann path, the 'turnpike', then follow for most of the time that von Neumann growth path, and then, near the end, leave that path to reach the final state. There are also turnpike theorems for the maximization of the final value of the goods, for portfolio

theory, ... See [2, 6, 22, 25, 28, 29] for a sampling of turnpike theorems. One algebraic (linear programming) version of a turnpike theorem is as follows, [3].

Consider the linear programming problem

$$\max \langle c, x_T \rangle, \quad Ax_t \leq Bx_{t-1}, \qquad t = 1, 2, \ldots, T,$$

where $x_t \in \mathbb{R}^n$, $c \in \mathbb{R}^n$, $x_0 \in \mathbb{R}^n$, is a given vector, and where the maximization is over all feasible paths $(x_0, x_1, \ldots, x_T)$. Suppose that there exists a $\lambda_0 > 0$ such that there is a unique vector $\hat{x}$ satisfying $(A - \lambda_0 B)\hat{x} \leq 0$, $\langle c, \hat{x} \rangle = 1$. Partition A and B in the form

$$A = \begin{pmatrix} A_1 \\ A_2 \end{pmatrix}, \quad B = \begin{pmatrix} B_1 \\ B_2 \end{pmatrix},$$

such that $(A_1 - \lambda_0 B_1)\hat{x} = 0$, $(A_2 - \lambda_0 B_2)\hat{x} < 0$. There is then a vector $\hat{p} \geq 0$ for which $\hat{p}(A - \lambda_0 B) = 0$. Suppose moreover that $A\hat{x} \leq Bx_0$, that there is a $p \geq 0$ such that $pA = c - \hat{p}A$, $pB = 0$, that if $(A_1 - \lambda B_1)z = 0$, $z \neq 0$, $|\lambda| = |\lambda_0|$, than $\lambda = \lambda_0$, and that $A_1\hat{x} > 0$. Under these conditions for any $\varepsilon > 0$ there exists T_1 and T_2 independent of T such that for every optimal trajectory $(x_0, x_1, \ldots, x_T)$ one has

$$\left\| \frac{x_t}{\|x_t\|} - \frac{\hat{x}}{\|\hat{x}\|} \right\| < \varepsilon \quad \text{for} \quad T_1 \leq t \leq T - T_2,$$

where $\|x\| = (x_1^2 + \cdots + x_n^2)^{1/2}$ denotes the norm of a vector x.

In the above, the restrictions $Ax_t \leq Bx_{t-1}$ describe the technological production possibilities of the economy (with x_{t-1} as input, x_t as output), $\hat{x}$ represents a von Neumann growth direction, and the $\hat{p}$ are equilibrium prices. The assumptions are fulfilled in the case of many economic growth models. Thus, indeed, an optimal trajectory is most of the time near the von Neumann ray.

As a final example[2] let us consider packing as many unit squares as possible (without overlap) into one large square of side α. If α is an integer the obvious square packing is optimal and yields a loss of 0. If α is not an integer the square packing yields a linear loss: if $\alpha = n + r$, $n \in \mathbb{N}$, $r \in (0, 1)$, then the loss is $2nr + r^2$. The question is whether one can do better. And indeed, asymptotically one can (i.e. for large $\alpha = n + r$). The basic idea of Erdös and Graham, [9], is to divide the large square of size α into a smaller square of integer size $\lfloor \alpha - \alpha^p \rfloor$ and two rectangles. Here $p \in [0, 1]$. The integer size lower left square is packed in the obvious way and the two rectangles are mainly packed with slightly slanted columns and rows of $m + 1$ unit squares where $m = n - \lfloor \alpha - \alpha^p \rfloor$. Figure 8 below gives the global picture for the case $n + r = \alpha = 100.8$, $p = 2/3$, $m = 21$. Figures 9 and 10 give the details of the triangles I and III (which are the same) and the trapezia II and IV. In this particular case the leftover area on the right of the upper rectangle turned out to be a triangle; this is exceptional; normally a trapezium would be left (w' in Fig. 11 can

[2]Thanks are due to J. K. Lenstra who mentioned the square packing problem to me (as a potential counterexample to the 'extremality implies symmetry' principle).

be (very slightly) negative and that is what happened in this particular case). For the case given, 77 of the square packing loss of 160 is recovered. One needs relatively large α for the procedure to start giving positive results. For instance for $\alpha = 35.6$ a gain of 6 is realized in the upper rectangle and the right rectangle is not yet large enough to be able to improve on the square packing. To see why the idea works

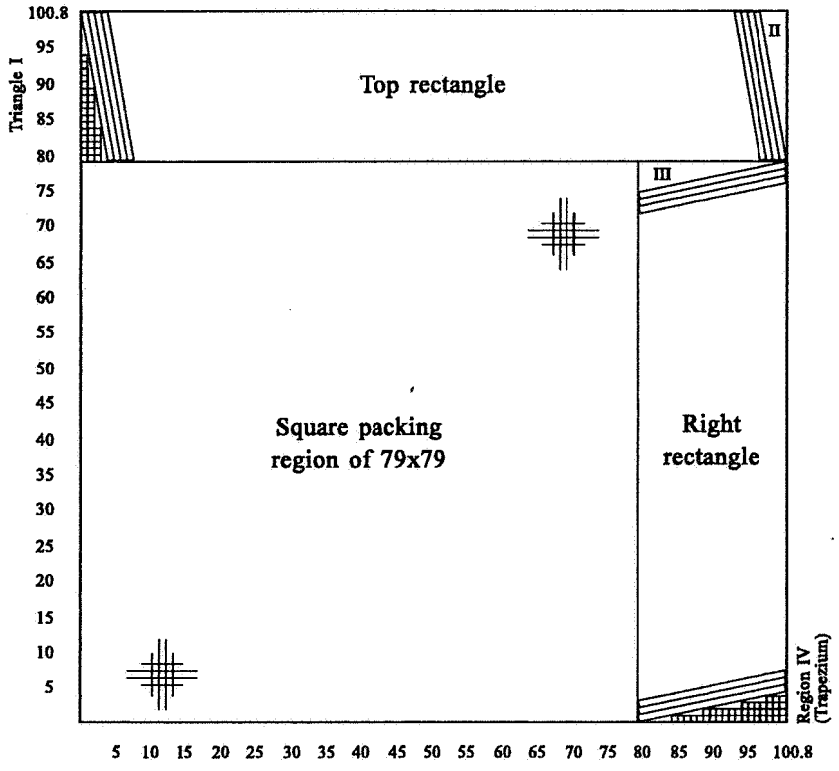

Figure 8

refer to Fig. 11. Obviously $t \leq 1$ (because the slanted column has width 1). But $(x+z)^2 = (m+1)^2-(m+r-t)^2 \leq (m+1)^2-(m-1)^2 = 4m$ so that $x+z \leq 2\sqrt{m}$. Hence $t < 2/\sqrt{m} < r$ for m large, so that $x+z < \sqrt{2m}$ and $t < \sqrt{(2/m)}$. The loss due to the triangles at the top and bottom will be $\leq \alpha\sqrt{(2/m)}$. Here one sees that to do better than linear loss one needs to have m growing with α. The triangles on the left and the trapezium on the right can be packed with linear loss cm. It follows that the optimal p is $2/3 = 0.666\ldots$. One can repeat this idea, and Erdös and Graham do so once more (this needs a good deal of additional cleverness because trapezia are harder to handle than rectangles), and manage to obtain an asymptotic loss of order $\alpha^{7/11}$, $7/11 = 0.636\ldots$. It is fairly easy to see that using the idea only a single time as in Figure 8 the loss can be kept $\leq 11\alpha^{2/3}$ for large α (irrespective of

how small $r \neq 0$ is; but if r is small α needs to be larger for the loss to be $\leq 11\alpha^{2/3}$).

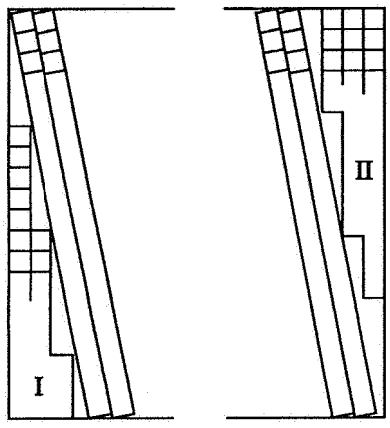

Figure 9
Upper rectangle in Fig.8:
Square packing: $21 \times 100 = 2100$
95 slanted columns of $22 = 2090$
left triangle: 32
right triangle (trapezium): 32
gain: 54

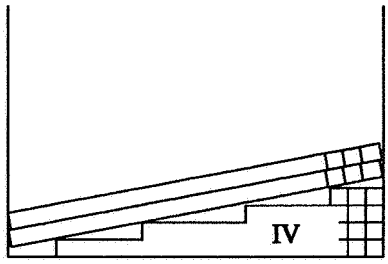

Figure 10
Upper rectangle in Fig.8:
Square packing: $79 \times 21 = 1659$
73 slanted columns of $22 = 1606$
upper triangle: 32
lower trapezium: 44
gain: 23

All of the examples above have the property that the optimal solutions are mostly regular (symmetric) (or almost so in the turnpike case) but that there may well be boundary effects. In the square packing case the boundary grows with α (and this is important: a fixed width boundary would still give asymptotically linear loss) although the size of the boundary compared to the whole square goes to zero. In the case of the intersecting set systems depicted in Fig. 7 there is a boundary effect represented by the singletons of S_0; there is also a second 'boundary effect' for small n. Thus for $n = 8$ and $r = 2$ the picture would be and this is even more symmetrical, and there is (correspondingly) a larger system of sets $\mathfrak{S}$ such that each two members intersect in two points. This is the 14 member set system of 4 element sets consisting of the six sides of the cube $\{1,2,3,4\}$, $\{5,6,7,8\}$, $\{1,2,5,6\}$, $\{3,4,7,8\}$, $\{2,3,6,7\}$, $\{1,4,5,8\}$; the six 'square diagonal' planes $\{1,2,7,8\}$, $\{3,4,5,6\}$, $\{1,3,5,7\}$, $\{2,4,6,8\}$, $\{1,4,6,7\}$, $\{2,3,5,8\}$; and the two 'mod 2 planes' $\{2,4,5,7\}$, $\{1,3,6,8\}$. This is also an extremal configuration[3].

There seems to be but little known concerning the general question of whether "extremal objects incline towards great symmetry". Perhaps the question ought to

[3]This was pointed out to me by J. J. Seidel

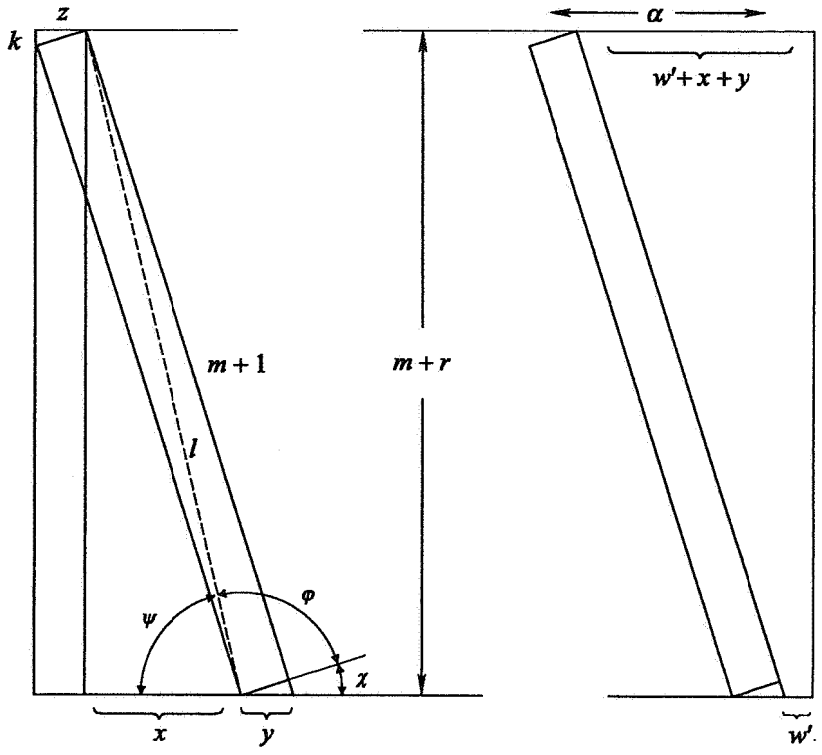

Figure 11

be broken into several parts:

(i) extremals and great regularity in the absence of boundary conditions
(ii) great regularity and symmetry
(iii) continuous dependence of optimal solutions on boundary constraints and parameters.

The first question is related to, but by no means identical with the "principle" that symmetric problems have symmetric solutions, sometimes called the Purkiss principle, [32]. This principle is also not universally valid as is illustrated by the problem of finding the shortest road network connecting four towns located at the vertices of a square. The two solutions are somewhat like those depicted below in Fig. 13. Note that though both solutions are less symmetric than the problem, together they have the full symmetry. On the other hand, there are "Purkiss type theorems", [32].

The second part, (ii), has received a great deal of attention. And certainly it has become clear that there can be a great deal of regularity without an (obvious) group of symmetries that accounts for it. Examples are Penrose tilings, 5-fold crystal

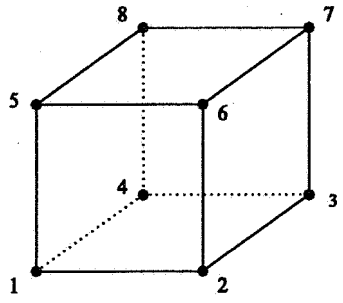

Figure 12

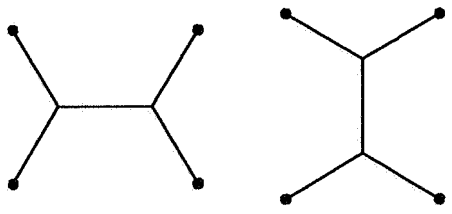

Figure 13

symmetry, various kinds of structures in finite geometry and the kind of symmetry caused by a Hopf algebra that is not a group, [18].

The final part of the problem, (iii), also offers an approach to proving "extremality implies regularity" theorems. Assuming symmetry in the absence of boundary conditions of various kinds, continuous dependence on these conditions will indeed yield such theorems. In this connection note that the Erdös–Graham packing is sort of "continuous" as α rises to the next integer (but not the other way). In the case of turnpike theory the von Neumann paths are the optimal ones in the absence of initial and final conditions, there is continuous dependence, and in fact this can be used to prove turnpike theorems, [2].

4. Radar Detection Patterns

Radar can be used to determine the distance and velocity of distant objects by measuring the time elapsed for the reflected signal to come back and the frequency shift (Doppler effect). As is often the case measurements based on comparison (interference) are more accurate than absolute ones. This leads to the idea of send-

ing out a pattern of signals at different times and frequencies and comparing the reflected signal with the original one. These are called frequency hopping patterns and the question arises of designing them in such a way that optimal detection (determination) results are achieved.

This led, in the engineering world, to the definition of a *Costas array* which is an $n \times n$ matrix with precisely one 1 in each column and in each row, such that for each displacement $(r, s) \neq (0, 0)$ there is at most one cell where both the original and the displaced matrix have a one.

Such a Costas array is for example the following 6×6 matrix of zero's and ones (zero's are empty cells, ones are black (shaded) cells); see Fig. 14. It follows that the "interference cell positions" determine both distance and velocity.

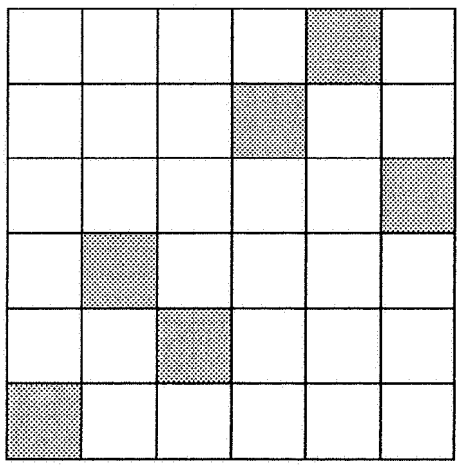

Figure 14

A number of studies have been devoted to Costas arrays and a very large number of them have been constructed. For instance there exist Costas arrays for all $n \leq 31$.

One symmetric construction is as follows (one of the Welch constructions). Let p be a prime number and take $n = p - 1$. Label the columns $1, \ldots, p-1$ and the rows $0, \ldots, p-2$. Put a black square at spot (i, j) iff $j = \alpha^i$ where α is primitive $\bmod p$, i.e. $\alpha^r \not\equiv 1 \bmod p$ for $r < p - 1$. In the example of Fig. 14, $p = 7$, $\alpha = 3$.

Cf., e.g. [17] for a fairly recent and complete survey on Costas arrays.

There are a number of drawbacks to Costas arrays. There will always be shifts $(r, s), |r|, |s| < n$ such that there is no overlap (between the original and the shifted pattern). Extending the original array periodically in the time direction can help. For instance in the case of the Welch construction it then remains true that the overlap is at most one. There remain shifts $(r, s), |r|, |s| < n$, though, with zero overlap. Extending periodically also in the frequency direction seems to be not considered in the engineering world. If one does so one finds that there are still zero

overlap shifts (besides the obvious ones (r, s) with $r \equiv 0 \bmod n$ and $s \not\equiv 0 \bmod n$ or vice versa) and that also, inevitably, there will be shifts with an overlap of ≥ 2. The complete situation in the case of the Welch array of Fig. 14 is detailed in Fig. 15 and Fig. 16 below. (Incidentally, the Welch array does not behave well if it is only extended periodically in frequency; then also one overlap of 2 appears (shift of (4,1))). Mathematically the reason is that the natural periodicity of the exponents (the time direction) is $p-1$ while that in the frequency direction is p. Most of the drawbacks just mentioned arise because Costas arrays are square and have precisely n black cells (and $n(n-1) \neq n^2 - 1$ if $n \neq 1$).

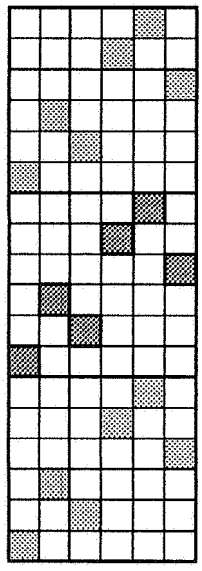

Figure 15

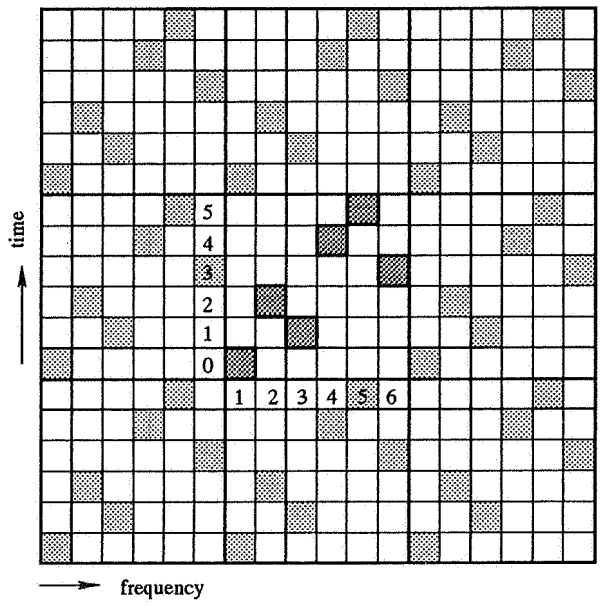

Figure 16

Thus the question arises whether one can perhaps do better by modifying things a bit.

One interesting improvement goes as follows. Take again a prime number p and let $n = p-1$. Label the rows $0, 1, \ldots, n-1$ and the columns $1, \ldots, n, 0$. Put a black cell at those positions (i, j), i a row index, j a column index, for which $j = \alpha^i$ where α is again primitive $\bmod p$. I.e., this is the Welch array extended with one column of empty squares. Extend the array periodically in both directions. The result has the following properties:

a) for a shift of the form $(kp, l(p-1))$ the overlap (with the non-extended shifted array) is (obviously) $n = p-1$ (like in the Costas array case)
b) for a shift of the forms (kp, s) or $(r, l(p-1))$ not of the form a) the overlap is

zero (like in the Costas array case)

c) for all other shifts the overlap is precisely one.

An example is depicted in Fig. 17. The array itself can be described more abstractly as a permutation σ of $\{1, 2, \ldots, n\}$ and the property desired is then

d) the $n(n-1)$ differences $(i, \sigma(i)) - (j, \sigma(j)) \bmod (n, n+1)$ give precisely all the pairs $(r, s) \bmod (n, n+1)$ with $r \not\equiv 0 \bmod n$ and $s \not\equiv 0 \bmod (n+1)$. (Note that there are indeed $n(n+1) - n - (n+1) + 1 = n(n-1)$ such pairs.)

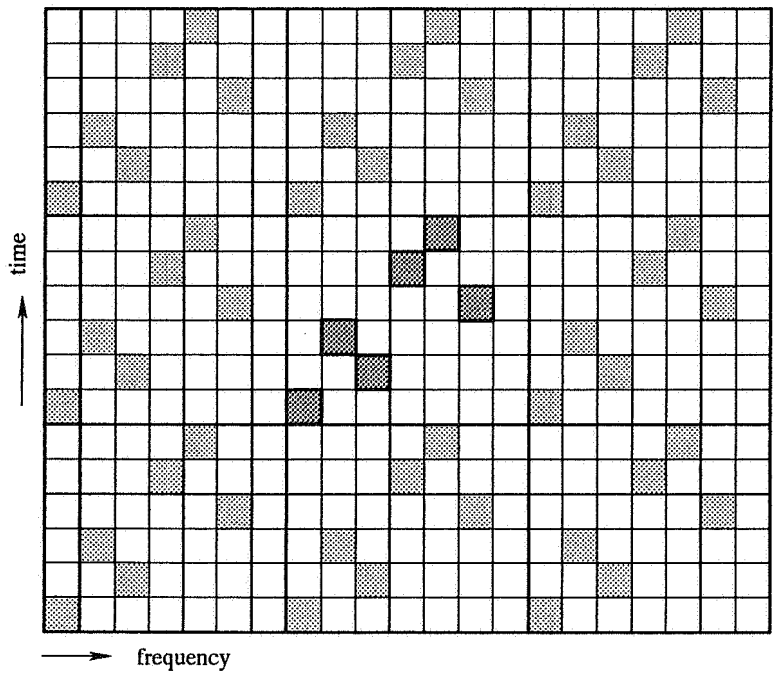

Figure 17

I experimented a bit with such permutations and the evidence seems to indicate the conjecture: "up to trivial equivalences the only examples of such permutations are those given by the rule above, i.e. $\sigma(i) = \alpha^i$ with $n+1$ a prime, p, and α primitive mod p. This holds for $n \leq 10$. There is some additional interest in the conjecture. For by a rather ad hoc construction, which I do not really understand completely, every permutation σ of $\{1, \ldots, n\}$ satisfying d) gives rise to a finite projective plane of order $n+1$ (i.e. with $(n+1)^2+(n+1)+1$ points and $n+2$ points on each line). Thus it would be really nice if the conjecture were false for some interesting numbers n. The construction is described in the intermezzo at the end of this section.

A second possible improvement asks for numbers n and m and a corresponding

pattern such that the overlap between a shifted pattern and the both ways periodically extended pattern is exactly one for all shifts not of the form $(r, s) = (kn, lm)$, $kl \in \mathbb{Z}$ (for which cases the overlap is automatically q if there are q black squares).

A few seconds thought gives that what we are asking for is a difference set for the group $\mathbb{Z}/(n) \times \mathbb{Z}/(m)$. Now if n and m are relatively prime $\mathbb{Z}/(n) \times \mathbb{Z}/(m) \simeq \mathbb{Z}/(nm)$ and the various known cyclic difference sets can be used. For instance the one for $\mathbb{Z}/(91)$ which is $D = \{1, 2, 4, 10, 28, 50, 57, 62, 78, 82\}$ yields the pattern depicted in Fig. 18 below. The construction is as follows: to $d \in D$ associate the black square at coordinates (d mod 13, d mod 7). For example $50 \in D$ gives rise to the black square at (11,1), and $62 \in D$ to that at (10,6).

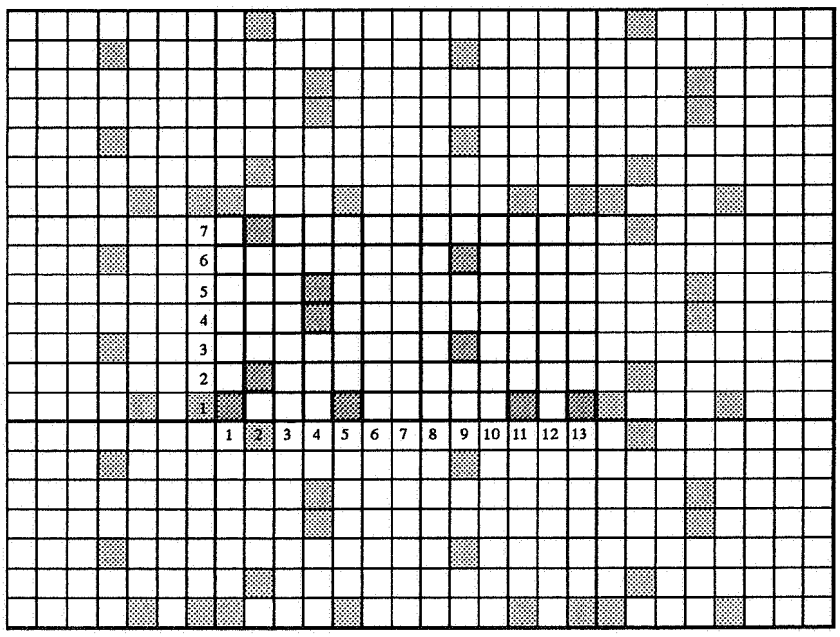

Figure 18

This particular difference set is of projective plane type. The recipe is as follows. Let n be of the form $q^2 + q + 1$ where q is a power of a prime number. (Here $q = 9$ and $n = 91$.) Consider the field $\mathbb{F}_q$ of q-elements and construct a field extension $\mathbb{F}_{q^3}$ of degree 3 of $\mathbb{F})_q$. Find an element $\alpha \in \mathbb{F}_{q^3}$ that is primitive, i.e. such that $\alpha^m \neq 1$ for $m < q^3 - 1$. As a vector space over $\mathbb{F}_q$ the field $\mathbb{F}_{q^3}$ is a vector space of dimension 3. Let L be any nonzero linear mapping $\mathbb{F}_{q^3} \to F_q$. Consider the exponents (mod $q^2 + q + 1$) of those α^m that are in L. These form a difference set for $\mathbb{Z}/(n)$, $n = q^2 + q + 1$. For a proof cf. [4, Chapter V].

This is the mathematical theory, which, moreover, guarantees that all the objects asked for do indeed exist. It is, however, quite another matter to write them down

explicitly. In order to illustrate this point let me give the details I used to write down the particular difference set above.

First one needs an $\mathbb{F}_{729}$, i.e. a concrete representation of the field of 729 elements. For this one uses an irreducible polynomial of degree 6 over $\mathbb{F}_3 = \mathbb{Z}/(3) = \{0,1,2\}$ (with addition and multiplication modulo 3). There are many such, but, again, to write down an explicit one is another matter. In this case I realized $\mathbb{F}_{729}$ as a composite of an $\mathbb{F}_9$ (a degree 2 extension) and an $\mathbb{F}_{27}$ (a degree 3 extension), viz.

$$\mathbb{F}_{729} = \mathbb{F}_3[x,y]/(x^2+1, y^3+2y+1).$$

Next a primitive element of $\mathbb{F}_{729}$ is needed, i.e. an element $\alpha \neq 0$ such that $\alpha^m \neq 1$ for all $m < 728$. Again, there are many, but finding one explicitly is another matter. The element $\alpha = (xy+1)$ works. Finally the elements of $\mathbb{F}_{729}$ were coded as expressions $\alpha y^2 + \beta y + \gamma$ with $\alpha = a_1x + b_1$, $\beta = a_2x + b_2$, $\gamma = a_3x + b_3$ with $a_i, b_j \in \{0,1,2\}$ and for the linear functional I took $L(\alpha y^2 + \beta y + \gamma) = \gamma$.

All this serves to illustrate that there is a certain difference between an abstract mathematical theorem like the one above describing the 'projective plane construction of difference sets' and actually writing down explicit results, in this case an explicit difference set for a smallish number like 91.

This is part of the domain of computer algebra: the devising of efficient explicit algorithms and the implementation of them in terms of software packages on readily available machines. Moreover these software packages should be user friendly enough to be used by nonspecialists (in the area of mathematics with which the package deals).

The third main point I want to stress here in this paper is that in this domain there is great activity, and that very, very much remains to be done.

Intermezzo

Let σ: $\{1,2,\ldots,n\} \to \{1,2,\ldots,n\}$ be a permutation with the property that for all (r,s), $r \not\equiv 0 \bmod n$, $s \not\equiv 0 \bmod (n+1)$ there is precisely one pair $i,j \in \{1,\ldots,n\}$ such that $(r,s) \not\equiv (i,\sigma(i)) - (j,\sigma(j)) \bmod (n,n+1)$ (i.e. $i - j \not\equiv r \bmod n$ and $\sigma(i) - \sigma(j) \not\equiv s \bmod n+1$).

From such a σ one obtain a finite projective plane of order $n+1$ as follows.

The set of points is the union

$$\begin{aligned} X \;=\; & \{(i,j)\colon i = 1,\ldots,n;\ j = 0,1,\ldots,n\} \\ & \cup \{P_1,\ldots,P_n\} \cup \{Q_0,\ldots,Q_n\} \cup \{*_1,*_2\}. \end{aligned}$$

Let Δ be the set $\{(i,\sigma(i))\colon i = 1,\ldots,n\}$. The lines in X are defined to be the sets

$$
\begin{aligned}
&(i,j)+\Delta \cup \{P_i, Q_j\} = l_{ij}, && i = 1,\dots,n;\ j = 0,\dots,n\\
&\{(i,j):\ j = 0,1,\dots,n\} \cup \{*_2\} = p_i, && i = 1,\dots,n\\
&\{(i,j):\ i = 1,\dots,n\} \cup \{*_1\} \cup \{Q_j\} = q_j, && j = 0,\dots,n\\
&\{P_1,\dots,P_n,*_1,*_2\} = p\\
&\{Q_0,\dots,Q_n,*_2\} = q.
\end{aligned}
$$

Here, in the definition of l_{ij}, in the sum $(i,j)+\Delta$, one calculates modulo $(n, n+1)$.

The verification that this works is a straightforward (if slightly tedious) matter.

5. Voting Systems

The last illustration which I would like to discuss as an example of applied noncontinuous mathematics concerns voting systems. It is well known and has often been discussed. I include it here very briefly, to illustrate quite another aspect of applied mathematics.

It frequently happens that in engineering, or society, or ... , would like to have a device, a system, a procedure, ... possessing certain desirable qualities. For instance a computable filter to take out transmission noice, or a voting system: a procedure for aggregating individual lists of preferences to one for the societal group involved as a whole. It is then up to the mathematical community to analyze the situation and determine whether the requirements desired are compatible or whether no such thing as desired can possibly exist. This last outcome happens rather frequently; in fact in both the two cases mentioned just above. For voting systems this is the content of the various Arrow impossibility theorems, cf. below; in the case of the filtering of nonlinear stochastic dynamical systems one has for instance the result that there is no exact, recursive, finite dimensional filter for the socalled cubic sensor and many other systems, [20].

That there are difficulties with voting systems has been known since around 1750 (the Condorcet paradox). Indeed consider the voting system which aggregates individual preference lists as follows. Alternative A is ranked above alternative B in the societal ranking of more individuals prefer A to B then vice versa. Now consider three individuals 1,2,3 whose individual rankings are, respectively,

$$
\begin{aligned}
1 &: A \succ B \succ C\\
2 &: B \succ C \succ A\\
3 &: C \succ B \succ A.
\end{aligned}
$$

The 'simple majority' aggregation procedure described then gives $A \succ B$, $B \succ C$, and $C \succ A$ for the society as a whole; a circular nontransitive 'ordering'.

It turns out that this 'paradox' is basic and not easily circumvented. Indeed, K. J. Arrow proved in a certain sense that all 'desirable' voting systems have flaws, [1]. More precisely, one version of the Arrow impossibility says that there is no voting system which has the following desirable (democratic) properties.

(1) (Consistency.) The social ordenings that result from the voting system are transitive.
(2) (Unanimity.) If all individuals agree on preferring alternative A to B then the society does so also.
(3) (Independence of irrelevant alternatives.) The societal ranking of two alternatives A and B depends only on the rankings of A versus B of all the individuals.
(4) (No dictator.) There is no individual i such that the societal ranking is simply that of individual i.

There are a great many of these 'impossibility theorems'. Cf. [5, 12, 26] for more material, more precision, and more detail, the discussion in [16], Chapter 9 is especially recommended for the laymathematician curious.

Not all the results of the analysis of voting systems have been negative. One result has been the discovery (more precisely, rediscovery) of 'approval voting'. This means that each individual simply indicates on the list of alternatives of which alternatives he approves. An individual can approve of as many alternatives as he wishes. Alternatives are ranked according to the number of approval votes they receive.

This scheme still has flaws but it has a lot in its favour, and would seem to be ready for widespread implementation, [5]. As far as I know the American Mathematical Society is the only official body which has adopted approval voting for its elections. Perhaps this illustrates yet another problem in applied mathematics: knowing the solution is by no means enough.

Bibliography

[1] K. J. Arrow, *Social choice and individual values*, 2nd edition, Yale Univ. Press, 1963.

[2] A. Araujo and J. A. Scheinkman, *Smoothness, comparative dynamics and the turnpike property*, Econometrica **45**:3 (1979), 601–620.

[3] S. A. Asmanov, *An algebra approach to the proof of turnpike theorems*, Sov. Math. Doklady **25**:2 (1982), 413–414.

[4] L. D. Baumert, *Cyclic difference sets*, Springer, 1971.

[5] S. J. Brams and P. C. Fishburn, *Approval voting*, Birkhäuser, 1982.

[6] D. Cass, *Optimum growth in an aggregation model of capital accumulation; a turnpike theorem*, Econometrica **34** (1966), 833–850.

[7] N. G. de Bruijn and P. Erdös, *On a combinatiorial problem*, Indagationes Math., **10** (1948), 421–423.

[8] R. Dorfman, P. Samuelson and R. Solow, *Linear programming and economic analysis*, McGraw-Hill, 1958.

[9] P. Erdös and R. L. Graham, *On packing squares with equal squares*, J. Comb. Theory **A19** (1975), 119–123.

[10] P. Erdös, C. Ko and R. Rado, *Intersection theorems for systems of finite sets*, Quart. J. Math. (2), **12** (1961), 313–320.

[11] L. Finkelstein, D. Kleitman and T. Leighton, *Applying the classification theorems for finite simples groups to minimize pin count in uniform permutation architectures*, In: J. H. Reif (ed.), VLSI algorithms and architectures, Springer, 1989, 247–256.

[12] P. C. Fishburn, *The theory of social choice*, Princenton Univ. Press, 1973.

[13] P. Franki, *Families of finite sets containing no two intersecting in a singleton*, Bull. Austral. Math. Soc. **17** (1977), 125–134.

[14] Z. Füredi, *Set systems with perscribed cardinalities for pairwise intersections*, Discrete Math. **40** (1982), 53–67.

[15] Z. Füredi, *An intersection problem whose extremum is the finite projective space*, J. Comb. Theory **A32** (1982), 66–72.

[16] S. Garfunkel, *For all practical purposes*, 2nd edition, Freeman, 1982.

[17] S. W. Golomb and H. Taylor, *Constructions and properties of Costas arrays*, Proc. IEEE.

[18] M. Hazewinkel, *Introductory recommendations for the study of Hopf algebras in mathematics and physics*, CWI Quarterly 4 (1992), 3–31.

[19] M. Hazewinkel, R. M. M. Mattheij and E. W. van Groesen (eds), *Proc. of the First European Symposium on Mathematics in Industry*, Teubner/KAP, 1988.

[20] M. Hazewinkel, *Lectures on linear and nonlinear filtering*, In: W. Schiehlen and W. Wedig (eds), *Analysis and estimation of stochastic mechanical systems*, CISM course June 1987, Springer, 1988, 316–340.

[21] M. Heilio (ed.), *Proc. of the Fifth European Conference on Mathematics in Industry*, Teubner/KAP, 1991.

[22] G. Huberman and S. Ross, *Portfolio turnpike theorems, risk aversion and regularly varying utility functions*, Econometrica **51**:5 (1983), 1345–1361.

[23] J. Kilian, S. Kipnis and Ch. E. Leierson, *The organization of permutation architectures with bussed interconnections*, In: Proc. 1987 IEEE Conf. on the Foundations of Comp. Sci., IEEE, 1987, 305–315.

[24] J. Manley, S. McKee and D. Owens (eds), *Proc. of the Third European Conference on Mathematics in Industry*, Teubner/KAP, 1990.

[25] L. W. McKenzie, *Turnpike theory*, Econometrica **44** (1976), 841–865.

[26] Y. Murakami, *Logic and social choice*, Routledge and Kegan Paul, 1968.

[27] H. Neunzert (ed.), *Proc. of the Second European Conference on Mathematics in Industry*, Teubner/KAP, 1988.

[28] H. Nikaido, *Persistance of continual growth near the von Neumann ray: a strong version of the Radner turnpike theorem*, Econometrica **32** (1964), 151–163.

[29] V. M. Polterovich, *Equilibrium trajectories of economic growth*, Econometrica **51**:3 (1983), 693–729.

[30] H. J. Rijser, *An extension of a theorem of de Bruijn and Erdös on combinatorial designs*, J. of Algebra **10** (1968), 246–261.

[31] H.-J. Wacker and W. Zulehner (eds), *Proc. of the Fourth European Conference on Mathematics in Industry*, Teubner/KAP, 1990.

[32] W. C. Waterhouse, *Do symmetric problems have symmetric solutions*, Amer. Math. Monthly **90** (1983), 378–387.