Cambridge University Press
978-0-521-21160-4 - Parallelisms of Complete Designs
Peter J. Cameron
Excerpt
More information

Introduction

Through the unknown, remembered gate
When the last of earth left to discover
Is that which was the beginning

(T. S. Eliot: Little Gidding)

The notion of 'parallelism' has always played an important role in mathematics. Euclid's famous 'parallel postulate' (in the form, due to Proclus, known as 'Playfair's axiom') asserted that, given any line and any point in the plane, the given point lies on a unique line parallel to the given line. A long history of controversy surrounded the question of whether this postulate is self-evident, or even necessarily true. The controversy was laid to rest when it was demonstrated that 'non-euclidean geometries', in which Euclid's postulate fails, are valid objects of mathematical study.

The point of view in this book is the opposite of that of non-euclidean geometry, which abandons the parallel postulate while retaining the other geometric axioms. The parallelisms studied here satisfy the parallel postulate, but all other restrictive conditions are cleared away; in place of geometric 'lines', I consider all subsets of the point set X which have cardinality t, for some given integer t. Thus the parallel relation is the only structure these 'geometries' possess.

The book is largely self-contained. Each chapter except the last is followed by one or more appendices treating topics relevant to that chapter. A glance at the titles of the appendices shows that the theory of parallelisms draws on (and often enriches) such diverse areas of finite mathematics as network flows, perfect codes, designs, Latin squares, and multiply-transitive permutation groups.

In addition to the basic definitions and lemmas, Chapter 1 contains a proof that the condition that t divides $n = |X|$ is necessary and sufficient for the existence of a parallelism. This is a recent result of

Baranyai; the proof uses the Integrity Theorem for network flows, which is described and proved in the Appendix to that chapter.

In Chapter 2, all those parallelisms satisfying a certain geometric condition called the 'parallelogram property' are determined. This involves Tietäväinen's determination of all perfect binary linear error-correcting codes, given in an Appendex. (A second Appendex describes association schemes and metrically regular graphs; these provide a setting for a more general theory of perfect codes, and will also be needed in Chapter 5.) The next Chapter is closely related. It describes a construction of parallelisms from Steiner systems, and shows how a parallelism constructed in this way can be recognized, by means of a property which generalizes the parallelogram property. Thus, the main result of Chapter 2 can be used to give geometric characterizations of certain Steiner systems. Among these are the famous Witt systems $S(4, 7, 23)$ and $S(5, 8, 24)$; the uniqueness of these systems is demonstrated in the Appendix.

In the case $t = 2$, the 2-element subsets of X can be identified with the edges of the complete graph K_n with vertex set X; a parallelism is the same thing as a $(n-1)$-edge-colouring of K_n. Several aspects of this case are treated in Chapter 4: rough estimates for the number of different parallelisms (these depend on estimates for the number of $n \times n$ Latin squares, given in the Appendix); structure and automorphisms of some special parallelisms, derived from Abelian groups and Steiner triple systems; structure of 2-coloured subgraphs, including some remarks on colourings in which all 2-coloured subgraphs are isomorphic.

The last topic provides motivation for Chapter 5. Suppose a parallelism has the property that the configurations formed by pairs of parallel classes are all isomorphic: then $t \leq 3$. Such parallelisms with $t = 3$ are closely related to certain incidence structures called biplanes; we define a biplanar parallelism to be one which bears this relation to a biplane. Biplanarity is a generalization of the parallelogram property when $t = 3$. A similar generalization for arbitrary t is the assumption that a graph associated with the parallelism (defined in Chapter 1) is metrically regular. This condition is empty for $t = 2$, equivalent to biplanarity for $t = 3$, and apparently very restrictive for $t \geq 4$, though the complete truth is not yet known. The Appendix discusses biplanes in the context of symmetric designs giving the Bruck-Ryser-Chowla theorem and some results on polarities.

Chapter 6 concerns parallelisms whose automorphism groups have a high degree of transitivity. The highest possible degree for a non-trivial parallelism is $t + 1$; all examples attaining this bound are determined. The general theme is that large groups of automorphisms tend to force the conditions of the previous chapters to occur. The appendix contains the necessary group-theoretic tools.

The final Chapter concerns possible generalizations of the concept of parallelism as studied here. The two main directions are: more general resolutions, of non-trivial structures into non-trivial structures; and objects called 'partition systems', which directly generalize parallelisms. Some examples are given, but no general theory exists.

Prerequisites for this book are

(a) Linear algebra: linear transformations on real vector spaces; finite fields.

(b) Group theory: up to Sylow's theorems; some familiarity with 'classical' groups.

(c) Number theory: representations of integers as sums of squares; a little quadratic reciprocity.

(d) Topology: we make an inessential appeal to compactness at one point.

The book is written primarily to interest readers in the theory of parallelisms; but, if anyone is stimulated to dig deeper into one of the other topics, using the references given, it will have achieved something. The common application of these topics may serve as additional motivation.

My gratitude is due to my wife, without whom this would never have progressed past the 'good idea' stage; to audiences at Westfield College and elsewhere, who listened to parts of the material; and to the referee, who suggested several improvements in the presentation.

Cambridge University Press
978-0-521-21160-4 - Parallelisms of Complete Designs
Peter J. Cameron
Excerpt
More information

I·The existence theorem

Here the impossible union
Of spheres of existence is actual

(T. S. Eliot: The Dry Salvages)

Throughout this book, X denotes a finite set of n elements called points; we write $n = |X|$. By analogy with the commonest notation for binomial coefficients, we write $\binom{X}{t}$ for the set of all subsets of X containing t points; members of this set are called t-subsets of X. Thus

$$\binom{X}{t} = \{Y \mid Y \subseteq X,\ |Y| = t\},$$

and $|\binom{X}{t}| = \binom{n}{t}$. We ensure that $\binom{X}{t}$ is non-empty by requiring $0 \le t \le n$.

A subset of $\binom{X}{t}$ partitions X if every point of X lies in just one member of the subset. Clearly it is necessary and sufficient for the existence of such a partition that t divides n.

A parallelism of $\binom{X}{t}$ can be defined in two equivalent ways. It is an equivalence relation $\|$ on $\binom{X}{t}$ satisfying Playfair's axiom: for any $x \in X$ and any $Q \in \binom{X}{t}$, there is a unique $Q' \in \binom{X}{t}$ such that $x \in Q'$ and $Q \| Q'$. This condition asserts simply that each equivalence class partitions X. Thus a parallelism may be defined alternatively as a partition of $\binom{X}{t}$ into subsets called parallel classes, each of which partitions X. The number of t-subsets in a partition is n/t; so the number of parallel classes is

$$\binom{n}{t}\Big/\frac{n}{t} = \binom{n-1}{t-1}.$$

This can be seen another way. Given a point $x \in X$, there is a one-to-one correspondence between the set of parallel classes and $\binom{X - \{x\}}{t-1}$. (Each parallel class contains just one set containing x; this set has the form $\{x\} \cup Q$, where Q is a $(t-1)$-subset of $X - \{x\}$. Moreover, any t-subset containing x lies in a unique parallel class.)

There are some trivial examples of parallelisms:

(i) $t = 1$, n arbitrary: a single parallel class, namely $\binom{X}{1}$.

(ii) $t = n$: a single parallel class containing the unique member X. Slightly less trivially,

(iii) $n = 2t$: each t-subset is parallel to its complement. Any partition of X into two t-subsets is a parallel class.

We shall use the neutral word 'subspace' to denote a subset X' of X for which a parallelism is induced on $\binom{X'}{t}$. That is, a subspace is a subset X' of X with the property that, if $Q \in \binom{X'}{t}$, $x \in X'$, $x \in Q' \in \binom{X}{t}$, and $Q \| Q'$, then $Q' \subseteq X'$. The formal definition of a subspace admits the possibility that $|X'| < t$; in this case, we do not strictly have a parallelism induced on $\binom{X'}{t}$, since we have adopted the convention $n \geq t$ for parallelisms. It will be convenient, however, to allow subspaces to have fewer than t points. (Thus any subset with fewer than t points is a subspace.)

We turn now to the proof of the general existence theorem, due to Z. Baranyai [2].

Theorem 1.1. Let n and t be positive integers, and $|X| = n$. There is a parallelism of $\binom{X}{t}$ if and only if t divides n.

Proof. We have already noted that the condition $t | n$ is necessary; we must prove that it is sufficient. The proof is by induction on n. Thus, for example, to find a parallelism with $t = 3$, $n = 9$, it is enough to find a collection of partitions of a set of 8 points into sets of size 2, 3, and 3, with the property that any set of size 2 or 3 is contained in exactly one of these partitions; then we simply take an extra point and adjoin it to each set of size 2. We see already that we require a more general object than a simple parallelism; we must allow sets of differing cardinalities. But worse is to come. At the next step, we require partitions of a set of 7 points into sets with sizes 1, 3, 3 or 2, 2, 3; when we add the extra point, in the second case we need a rule about which set of size 2 must receive this point. (This is the root of the difficulty.) Even when we have formulated a suitable inductive hypothesis accounting for these complications, we need an important theorem from the theory of network flows to transfer it from n to $n - 1$. All this was done by Baranyai.

We shall define, for given n, a datum on n to be an r-tuple $(t_1, \ldots, t_r)$, where $r > 0$ and $t_1, \ldots, t_r$ are integers satisfying $0 \le t_i \le n$ for all i, together with an $r \times s$ matrix $A = (a_{ij})$ of non-negative integers satisfying

(i) $\sum_{j=1}^{s} a_{ij} = \binom{n}{t_i}$;

(ii) $\sum_{i=1}^{r} t_i a_{ij} = n$.

(Since $\sum_{i=1}^{r} \sum_{j=1}^{s} t_i a_{ij} = ns = \sum_{i=1}^{r} t_i \binom{n}{t_i}$, we have $s = \sum_{i=1}^{r} \binom{n-1}{t_i - 1}$.)

Theorem 1.2. Given a datum $((t_i), (a_{ij}))$ on n, there exist sets $\mathcal{A}_{ij}$ $(1 \le i \le r,\ 1 \le j \le s)$ of subsets of X, with $|X| = n$, $|\mathcal{A}_{ij}| = a_{ij}$, having the properties

(i) for a fixed i, the sets $\mathcal{A}_{ij}$ form a partition of $\binom{X}{t_i}$;

(ii) for a fixed j, the members of the sets $\mathcal{A}_{ij}$ form a partition of X.

(Thus, if all t_i are distinct, we have a collection of partitions of X into a_{1j} sets of size $t_1, \ldots, a_{rj}$ sets of size t_r, with the property that each t_i-set occurs exactly once. With the datum defined by $r = 1$, $t_1 = t$, $a_{1j} = n/t$ for all j, we obtain Theorem 1.1. However, we do not assume that all t_i must be distinct. Note that conditions (i) and (ii) in the definition of a datum are necessary for conclusions (i) and (ii) of the theorem.)

The proof, as we have indicated, is by induction on n. Clearly the theorem holds if $n = 1$. So assume we are given a datum on n, with $n > 1$, and assume the theorem holds for all data on $n - 1$. Consider the network (see Appendix 1A) whose vertices are a source S, a sink S', r vertices R_i $(1 \le i \le r)$, and s vertices C_j $(1 \le j \le s)$; the edges are (S, R_i) with capacity $\binom{n-1}{t_i-1}$ $(1 \le i \le r)$, (R_i, C_j) with capacity 1 for those pairs (i, j) for which $a_{ij} \ne 0$ (and only those), and (C_j, S') with capacity 1 $(1 \le j \le s)$. Considering edges out of S (or into S'), we see that the capacity of the network is at most

$$\sum_{i=1}^{r} \binom{n-1}{t_i-1} = s.$$

In fact, this is the exact capacity. For consider the flow ϕ defined as follows: $\phi(S, R_i) = \binom{n-1}{t_i-1}$ $(1 \le i \le r)$; $\phi(R_i, C_j) = t_i a_{ij}/n$ $(1 \le i \le r,$ $1 \le j \le s)$ (note that this is at most 1, and is 0 if R_i and C_j are not joined); $\phi(C_j, S') = 1$ $(1 \le j \le s)$. The conditions that the flows into and out of each vertex R_i or C_j are equal are precisely conditions (i) and (ii) in the definition of a datum. (For example, the flow out of R_i is $\sum_{j=1}^{s} t_i a_{ij}/n = \frac{t_i}{n}\binom{n}{t_i} = \binom{n-1}{t_i-1}$.)

Thus, by the Integrity Theorem (Theorem 1A. 3), there is a maximal flow ϕ' whose value on any edge is an integer. Clearly $\phi'(S, R_i) = \binom{n-1}{t_i-1}$ $(1 \le i \le r)$, $\phi'(C_j, S') = 1$ $(1 \le j \le s)$. Let $e_{ij} = \phi'(R_i, C_j)$ for $1 \le i \le r$, $1 \le j \le s$. Then each e_{ij} is 0 or 1; $\sum_{j=1}^{s} e_{ij} = \binom{n-1}{t_i-1}$; $\sum_{i=1}^{r} e_{ij} = 1$; and $e_{ij} > 0$ only if $a_{ij} > 0$.

Construct a datum on $n - 1$ as follows. Put $t_i^* = t_i$ and $t_{i+r}^* = t_i - 1$ $(1 \le i \le r)$; $a_{ij}^* = a_{ij} - e_{ij}$, $a_{i+rj}^* = e_{ij}$ $(1 \le i \le r,$ $1 \le j \le s)$. The condition $0 \le t_i^* \le n - 1$ will be violated only if $t_i = n$ or $t_{i-r} = 0$, but then the corresponding row consists entirely of zeros and can be deleted or ignored. To verify that this is a datum: $a_{ij}^* \ge 0$: for $1 \le i \le r$, a_{ij} and e_{ij} are integers, $e_{ij} \le 1$, and $e_{ij} > 0$ only if $a_{ij} > 0$. For $r + 1 \le i \le 2r$ it is clear.

$$\sum_{j=1}^{s} a_{ij}^* = \begin{cases} \sum_{j=1}^{s} a_{ij} - \sum_{j=1}^{s} e_{ij} = \binom{n}{t_i} - \binom{n-1}{t_i-1} = \binom{n-1}{t_i} = \binom{n-1}{t_i^*} \; (1 \le i \le r) \\ \sum_{j=1}^{s} e_{i-rj} = \binom{n-1}{t_{i-r}-1} = \binom{n-1}{t_i^*} \; (r + 1 \le i \le 2r). \end{cases}$$

$$\begin{aligned} \sum_{i=1}^{2r} a_{ij}^* t_i^* &= \sum_{i=1}^{r} (a_{ij} - e_{ij}) t_i + \sum_{i=1}^{r} e_{ij}(t_i - 1) \\ &= \sum_{i=1}^{r} a_{ij} t_i - \sum_{i=1}^{r} e_{ij} \\ &= n - 1. \end{aligned}$$

So, by the induction hypothesis, there are sets $\mathcal{A}^*_{ij}$ of subsets of $X - \{x_0\}$ satisfying the appropriate conditions. Note that, for given j and $1 \le i \le r$, there is exactly one non-empty $\mathcal{A}^*_{i+rj}$, which consists of a single $(t_i - 1)$-set A_{ij} (say). Now put

$$\mathcal{A}_{ij} = \begin{cases} \mathcal{A}^*_{ij} & \text{if } e_{ij} = 0, \\ \mathcal{A}^*_{ij} \cup \{A_{ij} \cup \{x_0\}\} & \text{if } e_{ij} = 1. \end{cases}$$

We claim that these sets satisfy the conclusion of the theorem.

First,

$$|\mathcal{A}_{ij}| = \begin{cases} |\mathcal{A}^*_{ij}| = a_{ij} & \text{if } e_{ij} = 0, \\ |\mathcal{A}^*_{ij}| + 1 = (a_{ij} - e_{ij}) + 1 = a_{ij} & \text{if } e_{ij} = 1. \end{cases}$$

(i) Let Y be a t_i-subset of X. If $x_0 \notin Y$, then Y occurs exactly once in $\mathcal{A}^*_{ij}$; if $x_0 \in Y$, then $Y - \{x_0\}$ occurs exactly once in $\mathcal{A}^*_{i+rj}$. In either case, Y occurs exactly once in $\mathcal{A}_{ij}$.

(ii) For fixed j, the members of $\mathcal{A}^*_{ij}$ partition $X - \{x_0\}$, and x_0 has been added to just one of them.

This completes the proof of the theorem. //

In his paper [2], Baranyai proves a more general result than Theorem 1.2, which implies (for example) the existence of a partition of $\binom{X}{t}$ into classes with the property that each point lies in $t/(n, t)$ members of each class, for any n and t. His data are the same as ours except that condition (ii) is not required; his main theorem is the same as ours except that (ii) is replaced by the statement

(ii)' For any j, and for all $x, x' \in X$, the number of members of $\bigcup_{i=1}^{r} \mathcal{A}_{ij}$ containing x differs from the number containing x' by at most one.

The proof proceeds along similar lines to that given here, but a more general version of the Integrity Theorem is needed, dealing with networks in which the flow in any edge is bounded above and below by integers.

The direction of subsequent research in similar subjects (such as Steiner triple systems and Latin squares), for which general existence theorems have been proved, suggests several questions.

Question 1.1. How many different parallelisms of $\binom{X}{t}$ are there when t divides n?

In Chapter 4 we will give a partial answer to this question, in the form of upper and lower limits as $n \to \infty$, in the case $t = 2$. For larger t, the problem is open. (The reader will be able to supply crude upper bounds.)

Question 1.2. Under what conditions can partial parallelisms be extended to parallelisms?

This question is not precisely formulated, because it is not clear what the definition of a 'partial parallelism' should be. We could define it to be a collection ot partitions of X into parts of size at most t such that each set of size t is a part of at most one partition; or (more restrictedly) the same thing with one 'at most' replaced by 'exactly'. (The structure induced on a subset of X by a parallelism satisfies the condition with the second 'at most' replaced by 'exactly'.)

We conclude this chapter with some more general theory of parallelisms. Any permutation $g : x \mapsto xg$ of a set X induces in a natural way a permutation of $\binom{X}{t} : Q \mapsto Qg = \{xg \mid x \in Q\}$. We define an <u>automorphism</u> of a parallelism to be a permutation which 'maps parallel pairs of t-subsets to parallel pairs'; that is, g is an automorphism if, whenever $Q_1, Q_2 \in \binom{X}{t}$ and $Q_1 \| Q_2$, we have $Q_1 g \| Q_2 g$. A related concept is that of a <u>strict automorphism,</u> a permutation which 'maps t-subsets to parallel t-subsets'; that is, g is a strict automorphism if, for all $Q \in \binom{X}{t}$, we have $Qg \| Q$. Thus, any strict automorphism is an automorphism. (If g is a strict automorphism and $Q_1 \| Q_2$, then $Q_1 g \| Q_1 \| Q_2 \| Q_2 g$.) So the set of automorphisms is a group, in which the set of strict automorphisms is a subgroup. Since an automorphism preserves the relation of parallelism, it maps any parallel class to another parallel class, and so induces a permutation on the set of parallel classes. The strict automorphism group is just the kernel of this representation (the set of automorphisms fixing all parallel classes), and so is a normal subgroup.

Consider the following example, which will be important later. X is the set of vectors in a vector space of dimension d over the field $GF(2)$ with two elements; $n = 2^d$. Define a parallelism of $\binom{X}{2}$ by the rule that $\{x_1, x_2\} \| \{x_3, x_4\}$ if and only if $x_1 + x_2 = x_3 + x_4$. The reader should verify that this is a parallelism; we call it the affine line-parallelism in $AG_1(d, 2)$. (This notation will be elaborated later.) For all $x \in X$, the transformation s_x which adds x to everything is a strict automorphism. (For $(x_1 + x) + (x_2 + x) = x_1 + x_2$, so $\{x_1 + x, x_2 + x\} \| \{x_1, x_2\}$.) Thus the strict automorphism group contains the additive group of X, which is an elementary abelian 2-group, transitive and regular on X. (For terminology of permutation groups, see Appendix 6A.)

Theorem 1.3. Let A be the group of strict automorphisms of a parallelism of $\binom{X}{t}$, with $n > t > 1$.

(i) If $t = 2$, then A is an elementary abelian 2-group acting semiregularly on X; A is transitive only in the case of the affine line-parallelisms.

(ii) If $t > 2$, then $A = 1$.

Proof. If a strict automorphism fixes x_1 and maps x_2 to x_3, then it maps every t-subset containing x_1 and x_2 into a parallel (and hence equal) t-subset containing x_1 and x_3, and it fixes the intersection of all these subsets, which is just $\{x_1, x_2\}$. So $x_2 = x_3$. This means that A is semiregular: only the identity fixes any point. Furthermore, if g is a strict automorphism mapping x_1 to x_2 $(x_1 \neq x_2)$, then g maps every t-subset containing x_1 and x_2 to a parallel (and hence equal) t-subset containing x_2, and it fixes the intersection of all these subsets, which is just $\{x_1, x_2\}$. Thus $x_2 g = x_1$. Then $x_1 g^2 = x_1$, so $g^2 = 1$. So every non-identity element $g \in A$ has order 2, whence A is elementary abelian.

If A is transitive and $t = 2$, then for any point x, a parallel class consists of the images under A of a pair containing x, and thus the parallelism is uniquely determined. So it must be the same as the affine line-parallelism. Alternatively, take a point $x_0 \in X$; every element $g \in A$ can be identified with the point $x_0 g \in X$ (Appendix 6A).