CAMBRIDGE

Cambridge University Press
0521413613 - Designs and their Codes - E. F. Assmus, JR. and J. D. Key
Excerpt
More information

Chapter 1

Designs

1.1 Introduction

We begin by discussing those basic concepts from design theory needed in our development of the use of linear codes as an aid in organizing and classifying designs. The more specific properties of those designs that we use as examples of this development will follow in the chapters devoted to the class of designs in question. Much of the material in this chapter is now quite standard and treatments can be found in related books on designs and geometries, in particular the books of Beth, Jungnickel and Lenz [37], Dembowski [85], Hall [122], and Hughes and Piper [144]. The books of Cameron [63], Cameron and van Lint [64], and Tonchev [281] are also useful for related material, and Batten [31] has an elementary account that highlights the geometry. We restrict our attention to *finite* structures, however, and whenever a set, group, or other mathematical structure is mentioned the reader should assume it to be finite. For background material the books by Wielandt [296] and Passman [232] can be consulted for permutation groups, and that by Lidl and Niederreiter [185] for Galois theory and finite fields.

1.2 Basic definitions

The most basic structure of the theory is a **finite incidence structure** which we denote by $\mathcal{S} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$, and which consists of two disjoint finite sets $\mathcal{P}$ and $\mathcal{B}$, and a subset $\mathcal{I}$ of $\mathcal{P} \times \mathcal{B}$. The members of $\mathcal{P}$ are called **points** and are generally denoted by lower-case Roman letters; the members of $\mathcal{B}$ are called **blocks** and are generally denoted by upper-case Roman letters. If the ordered pair (p, B) is in $\mathcal{I}$ we say that p is **incident** with B, or that

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
0521413613 - Designs and their Codes - E. F. Assmus, JR. and J. D. Key
Excerpt
More information

B contains the point p, or that p is on B, using the general phraseology of geometry, and viewing the incidence structure geometrically. The pair (p, B) is called a **flag** if it is in $\mathcal{I}$, an **anti-flag** if not.

Example 1.2.1 Let $\mathcal{P}$ be any set and take $\mathcal{B}$ to be any subset of the power set $2^{\mathcal{P}}$, the set of all subsets of $\mathcal{P}$. Define incidence by $(p, B) \in \mathcal{I}$ if and only if $p \in B$.

As this example shows, it is sometimes convenient to identify a block of an incidence structure $\mathcal{S}$ with the set of points incident with it, and we may write $p \in B$ or $B \ni p$ instead of $(p, B) \in \mathcal{I}$. In the event that a block of $\mathcal{S}$ becomes a block of a new structure it may then be incident with a different set of points, and hence the abstract definition is needed. Sometimes we will not mention the set $\mathcal{I}$ at all, particularly when we have an instance of the above example with $\mathcal{B}$ a collection of subsets of $\mathcal{P}$ and $\mathcal{I}$ the membership relation.

We will be concerned almost exclusively with those structures that have a particular degree of regularity and that are traditionally called *block designs*, a term that arose in the statistical literature. We will simply call them **designs**, or **t-designs** when the degree of regularity is to be emphasized. Here is the formal definition:

Definition 1.2.1 *An incidence structure $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ is a* **t-(v, k, λ) design**, *or simply a* **t-design**, *where t, v, k and λ are non-negative integers, if*

(1) $|\mathcal{P}| = v$;

(2) every block $B \in \mathcal{B}$ is incident with precisely k points;

(3) every t distinct points are together incident with precisely λ blocks.

Example 1.2.1 above is a t-design provided that $|B|$, the cardinality of the subset B of $\mathcal{P}$, is k for every subset $B \in \mathcal{B}$ and that, for every subset T of $\mathcal{P}$ of cardinality t, $|\{B \in \mathcal{B} | B \supseteq T\}| = \lambda$. Thus the blocks all have the same cardinality and every t-subset (i.e. a subset of cardinality t) is contained in the same number of blocks.

The non-negative integers t, v, k and λ are referred to as the **parameters** of the design and we will sometimes refer to a t-(v, k, λ) design as a "design with parameters t-(v, k, λ)". It is possible that distinct blocks could be incident with the same set of points, but for the vast majority of designs appearing in this book we shall not have such so-called **repeated blocks**. In the literature, since structures with repeated blocks can be

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
0521413613 - Designs and their Codes - E. F. Assmus, JR. and J. D. Key
Excerpt
More information

important, a t-design without repeated blocks is distinguished by calling it a **simple** t-design, and the further property that if two blocks are incident with the same set of k points, they are equal, is often included in the definition. Here the designs we treat are *always simple* and we will omit this qualifying adjective. When $t = 2$ the restriction that all blocks have the same cardinality is sometimes relaxed and such designs are called **pairwise-balanced** designs; although they are quite important, especially in recursive construction techniques, we shall make no use of the notion.

Although the definition does not demand it, we shall almost always have $0 \leq t \leq k$. As is customary, we set $b = |\mathcal{B}|$. A design is called **trivial** if every set of k points is incident with a block,[1] in which case $b = \binom{v}{k}$. A 1-design is called a **tactical configuration**; a non-trivial 2-design is known as a **balanced incomplete block design** (BIBD) in the statistical literature (and in much of the combinatorial literature as well). For 2-designs another notation that is frequently used, but which we will not employ at all, includes more of the parameters, thus (b, v, r, k, λ), where r is the **replication number** and denotes the number of blocks incident with a point. This number is independent of the point chosen, for, as we will see below, any t-design is an s-design for any $s \leq t$. The parameters shown in this notation are not independent, and the most crucial parameter has not yet appeared. If $t = \lambda = 1$, a design is simply a partition of the point set into subsets of cardinality k. It follows therefore that in this case the parameters are constrained by the condition that k must divide v; we shall soon see the generalization of this simple fact to arbitrary t-designs.

If $k = 2$, a t-(v, k, λ) design is a **graph** (undirected, no loops), and points are called **vertices** and blocks are called **edges**. Two vertices on the same edge are referred to as **adjacent**. A graph is **regular** with **valency** r if $t \geq 1$, and **complete** if $t = 2$ (i.e. all possible edges are present); similarly it is called **null** if it has no edges. A **bipartite** graph is one in which the vertex set is the disjoint union of two sets such that no two vertices in any one of these sets are adjacent, i.e. any edge has exactly one vertex from each of the sets. Of particular relevance to design theory are **strongly regular graphs** : a regular graph which is neither complete nor null is strongly regular if the number of vertices adjacent to both of two distinct vertices p and q depends only on whether p and q are adjacent or not. Its parameters are sometimes specified by the ordered 4-tuple (n, a, λ, μ) where n is the number of vertices, a the valency, λ the number of vertices adjacent to both of two adjacent vertices, and μ the number of vertices adjacent to both of two non-adjacent vertices.

[1] When there are repeated blocks a trivial design is one for which every set of k points is incident with the same number of blocks.

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
0521413613 - Designs and their Codes - E. F. Assmus, JR. and J. D. Key
Excerpt
More information

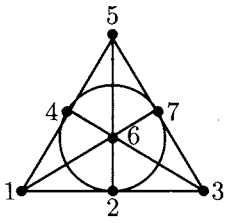

Figure 1.1: The Fano plane

Exercise 1.2.1 If Γ is a strongly regular graph with parameter set (v, k, λ, λ), show that a 2-(v, k, λ) design $\mathcal{D}$ can be defined in the following way: for the points of $\mathcal{D}$ take the vertices of Γ; for each point p define a block B_p to consist of all the points (vertices) adjacent to p. Then this set of points and blocks defines a 2-design with equally many points and blocks, a so-called symmetric design.

A t-(v, k, λ) design is also sometimes described as an $S_\lambda(t, k, v)$ design in the literature: see, for example, Beth *et al.* [37]. If $t \geq 2$ and $\lambda = 1$, then a t-design is called a **Steiner system** or Steiner t-design, and $S_1(t, k, v)$ becomes $S(t, k, v)$. We shall make no further use of the $S(t, k, v)$ notation. For Steiner systems with $t = 2$, blocks are often called **lines**, since any two points determine a unique block. More generally, and for the same reason, an incidence structure is called a **linear space** if every two points are on a unique block, or a **partial linear space** if any two points are on at most one block: see Doyen [98] for a survey article on linear spaces and Steiner systems. For a 2-(v, k, λ) design in general, a **line** is defined to be any set of points that is the intersection of all blocks that contain both of a pair of distinct points of the design, where here we are regarding blocks as sets of points. Thus for Steiner 2-designs the lines are essentially the blocks, and the terminology is consistent.

Example 1.2.2 (1) Let $\mathcal{P} = \{1, 2, 3, 4, 5, 6, 7\}$ and set

$$\mathcal{B} = \{\{1, 2, 3\}, \{1, 4, 5\}, \{1, 6, 7\}, \{2, 4, 7\}, \{2, 5, 6\}, \{3, 5, 7\}, \{3, 4, 6\}\}.$$

Then $(\mathcal{P}, \mathcal{B})$ with the natural incidence forms a 2-(7,3,1) design. This is the well-known Fano plane, a Steiner system, and is the smallest design arising from a projective geometry. It is an example of many classes of designs and will appear frequently throughout the book. Its usual representation is by the diagram shown in Figure 1.1, where the labelling coincides with that given above.

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
0521413613 - Designs and their Codes - E. F. Assmus, JR. and J. D. Key
Excerpt
More information

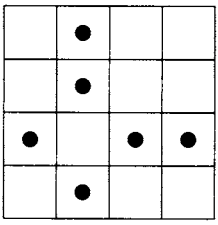

Figure 1.2: The block $B_{3,2}$ of the biplane

(2) Consider a 4×4 array and let the point set $\mathcal{P}$ be the 16 positions (i, j) of this array. For each (i, j) define a block B_{ij} to be incident with the six points (i, k) for $k \neq j$ and (k, j) for $k \neq i$. Figure 1.2 indicates a typical block. Then $|\mathcal{B}| = |\mathcal{P}| = 16$, every two points are incident with two blocks, and $(\mathcal{P}, \mathcal{B})$ is a 2-(16,6,2) design. It is known as a **biplane of order 4**: see page 120 for a general definition. (Notice that an analogous construction with an $n \times n$ array where $n \neq 4$, will only give a 1-design.)

(3) Consider the complete graph on six vertices. Let $\mathcal{P}$ be the set of 15 edges together with another point which we denote by ∞. The blocks containing the point ∞ will consist of ∞ and the five edges of a 5-claw, i.e. the five edges containing a fixed vertex of the graph. The blocks not containing ∞ will consist of the edges of those subgraphs of the complete graph which are two disjoint triangles. It is not difficult to see that once again we have a 2-$(16, 6, 2)$ design; it is not as easy to see that it is essentially the same as the one above.

(4) Let G be a t-transitive permutation group on a set $\mathcal{P}$. With $\mathcal{B}$ the union of any collection of orbits of G on k-subsets, where $k > t$, a t-$(|\mathcal{P}|, k, \lambda)$ design is obtained. If $k = t$, the design is trivial.

(5) A 2-$(n^2 + n + 1, n + 1, 1)$ design, for $n \geq 2$, is called a **projective plane of order *n*.** (The Fano plane is a projective plane of order 2.) Not only do any two points lie on a unique line, but it is also a consequence of the nature of the parameters that any two lines meet in a unique point.

(6) A 1-(v, k, λ) design with the property that any two points are together incident with *at most* one block, and that for x a point and B a block not containing x there is precisely one point on B that is on a block together with x, is called a **generalized quadrangle** provided that

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
0521413613 - Designs and their Codes - E. F. Assmus, JR. and J. D. Key
Excerpt
More information

$k = s + 1$ and $\lambda = t + 1$ are both greater than 1. Then the pair (s, t) is generally referred to as the **type** of the generalized quadrangle. A generalized quadrangle clearly has no triangles, but plenty of quadrangles. (See Exercise 1.2.3.) Some standard classical examples of generalized quadrangles will be given in Chapter 3 (Example 3.7.2, Exercise 3.7.1): see the book of Payne and Thas [233] for more properties of generalized quadrangles, or the survey article of Thas [272] for more examples and a general bibliography.

Example 1.2.2 (3) above illustrates an important theme of finite geometry in its group-theoretical aspect: the transitive extension of a permutation group. The doubly-transitive group which is the automorphism group of the biplane of order 4 that has been constructed is a transitive extension of the symmetric group on six letters viewed as a permutation group on 15 letters, the $\binom{6}{2}$ 2-subsets of the six letters. The following exercise reveals an even simpler example of such a transitive extension, in this case of the symmetric group on four letters viewed as a permutation group on six letters, once again a set of 2-subsets, but now of the four letters. The resulting transitive extension is the automorphism group of the Fano plane, a group of order $168 = 7 \times 24$.

Exercise 1.2.2 Consider the complete graph on four vertices. Let $\mathcal{P}$ be the set of six edges together with another point which we denote by ∞. Construct a biplane of order 2 as follows: the blocks containing ∞ consist of ∞ together with the three edges of a 3-claw of the complete graph, one for each vertex. The blocks not containing ∞ consist of the four edges of the squares of the complete graph, one for each square. Show that the resulting incidence structure is a 2-$(7, 4, 2)$ design, i.e. a biplane of order 2. How is this structure related to the Fano plane?

We next explore the most elementary consequences of Definition 1.2.1 and add to the array of parameters that are naturally associated with a design.

Theorem 1.2.1 *Let $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ be a t-(v, k, λ) design. Then for every integer s such that $0 \leq s < t$, the number λ_s of blocks incident with s distinct points is independent of the s points, and is given by*

$$\lambda_s = \lambda \frac{(v-s)(v-s-1)\cdots(v-t+1)}{(k-s)(k-s-1)\cdots(k-t+1)}.$$

In particular $\mathcal{D}$ is an s-(v, k, λ_s) design for every s with $1 \leq s \leq t$.

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
0521413613 - Designs and their Codes - E. F. Assmus, JR. and J. D. Key
Excerpt
More information

Proof: Let S be a set of s points, where $0 \leq s < t$. Let m be the number of blocks that contain every point of S. Let $\mathcal{T} = \{(T, B) | S \subset T \subseteq B, |T| = t,\ B \in \mathcal{B}\}$. Count $|\mathcal{T}|$ in two ways to get:

$$\lambda \binom{v-s}{t-s} = m \binom{k-s}{t-s},$$

which shows that m is independent of S and given by the formula in the theorem. □

Setting $\lambda_t = \lambda$ the theorem shows that the integers λ_s are most easily calculated from the recursion

$$\lambda_s = \frac{(v-s)}{(k-s)} \lambda_{s+1}.$$

For example, we shall see later (Corollary 7.4.3) that there is a design with parameters 5-$(12, 6, 1)$ and hence, not only for that design but for any design with these parameters, it follows that $\lambda_4 = 4, \lambda_3 = 12, \lambda_2 = 30, \lambda_1 = 66$ and the number of blocks is $b = \lambda_0 = 132$.

Note that for $s = 0$ we get

$$\lambda_0 = b = \lambda \frac{v(v-1)\dots(v-t+1)}{k(k-1)\dots(k-t+1)} \tag{1.1}$$

and, since $\lambda_1 = r$, we have from the recursion the well-known identities

$$bk = vr \tag{1.2}$$

and, for $t = 2$,

$$r(k-1) = \lambda(v-1), \tag{1.3}$$

indicating that the parameters are not independent. Moreover, the fact that λ_s is always an integer means that there are divisibility constraints on the parameters; for our purposes these constraints are much too crude to be helpful and the reader will not encounter in this book a set of parameters that is not at least feasible.

Exercise 1.2.3 (1) Show that a generalized quadrangle $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ with parameters 1-$(v, s+1, t+1)$ (i.e. of type (s, t)) has $v = (st+1)(s+1)$ and $b = (st+1)(t+1)$. Further, if x and y are distinct points that are not together on a block (i.e. non-collinear), then for any two blocks B and C through x there is a unique pair of blocks B' and C' through y such that B meets B' and C meets C'. Show also that the graph $\Gamma = (\mathcal{P}, \mathcal{E})$ defined to have vertex set $\mathcal{P}$, and edge set $\mathcal{E}$ defined by two distinct points x and y being adjacent if they are together on a block, is strongly regular with parameter set $((st+1)(s+1), s(t+1), s-1, t+1)$.

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
0521413613 - Designs and their Codes - E. F. Assmus, JR. and J. D. Key
Excerpt
More information

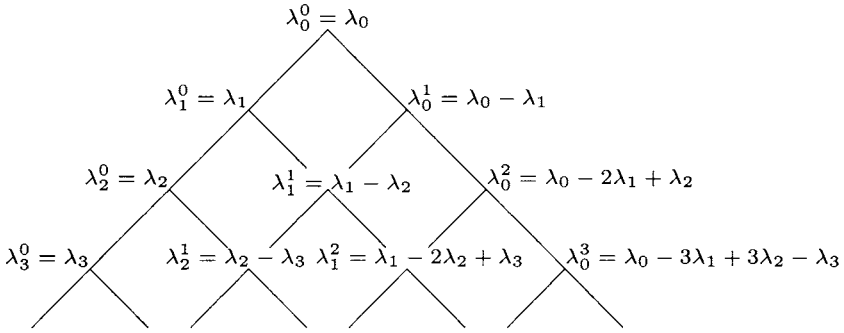

Figure 1.3: Pascal triangle for designs

(2) Let $\mathcal{D}$ be a 2-(v, k, λ) design. Show that there is a unique line through any two distinct points, that the number of points on any line is at most $(b - \lambda)/(r - \lambda)$ (where b and r are as above), and that equality holds for some line L if and only if every block meets L. (See the definition of a line in a 2-design on page 4.)

A kind of **Pascal triangle** can be used to compute certain more refined lambdas first explicitly discussed by R. M. Wilson. Let $\mathcal{D}$ be a design with parameters t-(v, k, λ), and suppose that i and j are non-negative integers. Then for disjoint point sets I and J with $|I| = i$ and $|J| = j$ the number of blocks containing I and disjoint from J is independent of these point sets provided $i + j \leq t$. We denote this number by λ_i^j; the fact that it is independent of the point sets follows easily from Theorem 1.2.1 and inclusion-exclusion, but, as we shall soon see, the independence follows from a simple recursion and the fact that $\lambda_i^0 = \lambda_i$.

In fact these refined lambdas fit into the "Pascal triangle[2]" shown in Figure 1.3. With λ_i^j in the $(i, j)^{\text{th}}$ position, and $\lambda_i^0 = \lambda_i$ for $0 \leq i \leq t$, the Pascal property, *viz.*

$$\lambda_i^j = \lambda_{i+1}^j + \lambda_i^{j+1}, \tag{1.4}$$

follows immediately from the definition of the λ_i^j's in precisely the same way that the similar recursion for the binomial coefficients does: take an additional point not in $I \cup J$. Thus (1.4) yields the independence of the λ_i^j for $i + j \leq t$.

Moreover, if $\mathcal{D}$ is a Steiner system, then these integers remain independent of the point sets for $i + j \leq k$ *provided* $I \cup J \subseteq B$ for some block B and we set $\lambda_i^0 = 1$ for $t \leq i$. We have, of course, $\lambda_t = \lambda = 1$. This is easily

[2]Our Pascal triangle is a mirror image of the triangle most usually depicted.

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
0521413613 - Designs and their Codes - E. F. Assmus, JR. and J. D. Key
Excerpt
More information

established by induction. Then the triangle can be extended to the $(k+1)^{st}$ row, corresponding to $i = k$.[3] The reader may wish to look at Gross [111] where these integers are called "block intersection numbers".

Ray-Chaudhuri and Wilson [245] have given a formula that is more compact than the one obtained from inclusion-exclusion and we record it in the following:

Proposition 1.2.1 *For i and j non-negative integers with $i + j \leq t$ the number of blocks of a t-(v, k, λ) design containing an i-set and disjoint from a j-set is*

$$\lambda_i^j = \lambda \frac{\binom{v-i-j}{k-i}}{\binom{v-t}{k-t}}.$$

Proof: It is only necessary to check that the numbers given in the proposition satisfy the initial conditions, namely that $\lambda_i^0 = \lambda_i$, and the recursion $\lambda_i^j = \lambda_{i+1}^j + \lambda_i^{j+1}$. The initial conditions are almost obvious and the recursion is satisfied because of the recursion for the binomial coefficients of the numerator. □

It is a simple matter, for a particular design, to start at the lower left vertex of the triangle working up to the top vertex via the recursion $\lambda_s = \lambda_{s+1}(v - s)/(k - s)$ and then to fill in the triangle using the recursion $\lambda_i^j = \lambda_{i+1}^j + \lambda_i^{j+1}$. For example, for the Fano plane of Figure 1.1, the triangle is as follows:

$$\begin{array}{cccccc} & & & 7 & & \\ & & 3 & & 4 & \\ & 1 & & 2 & & 2 \\ 1 & & 0 & & 2 & & 0 \end{array}$$

with the last line existing because the design is a Steiner system.

The difference of a particular pair of lambdas has an especially important role to play in the theory, so we introduce a special notation and name for it.

Definition 1.2.2 *If $\mathcal{D}$ is a t-design, where $t \geq 2$, then the* **order** *of $\mathcal{D}$ is $n = \lambda_1 - \lambda_2 = \lambda_1^1$, i.e. $r - \lambda$ if $t = 2$.*

The order of a design is crucial in determining those primes ℓ for which the linear codes — taken over the prime field $\mathbf{F}_\ell$ — associated with the

[3] It does not seem to have been observed that the triangle can also be extended to the $(k+1)^{st}$ row when the design is a biplane; this fact does not, however, appear to be useful.

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
0521413613 - Designs and their Codes - E. F. Assmus, JR. and J. D. Key
Excerpt
More information

$$\begin{array}{ccc} & b & \\ r & & b-r \\ \lambda & n & b-r-n \end{array}$$

Figure 1.4: Triangle for a 2-design

design may be of significance. The Fano plane has order 2 and the biplanes of Example 1.2.2, as we have already indicated, have order 4. Observe that for a 2-(v, k, λ) design the Pascal triangle is as shown in Figure 1.4, and that the order n is centrally located; for symmetric designs especially, it is the most important parameter.

Even for Steiner systems the order can be brought into a prominent position by observing that the divisibility constraints amount to demanding that k divide $n(n+1)$ when $t = 2$. Fisher's inequality (see Corollary 1.4.1) is expressed in this case by $k \leq n + 1$, and the parameters of a 2-$(v, k, 1)$ design are given in terms of n and k by 2-$(k + n(k-1), k, 1)$. For any particular n there are only finitely many feasible parameter sets that might yield such a Steiner system. The more usual approach has been to fix k and let n vary so as to get, possibly, an infinite class. Historically, the starting point was $k = 3$, and these designs are known as **Steiner triple systems.** Here the divisibility constraint is that the order be congruent to 0 or 2 modulo 3, and the parameters are 2-$(3+2n, 3, 1)$; the first possible order is 2, and this is a design we have already seen, the Fano plane. For order 3 we have the affine plane of that order, the residual (in a sense that will be made clear in Section 1.3) of the projective plane of order 3. It has been shown that for all admissible orders Steiner triple systems exist; for order 5 there are two distinct systems, in a sense that we are about to make clear, and, as the order increases, the number of distinct systems of that order tends rapidly to infinity. There is an enormous literature devoted to this topic and it is much too extensive to be dealt with here, but we include a short section on Steiner triple systems in Chapter 8.

The question of the "essential" identity of designs, and of incidence structures in general, through **isomorphism**, must arise: it is defined in the natural way. Since conceptually we should not distinguish between the role of points and blocks, mappings that interchange points and blocks will also have an important part to play.

Definition 1.2.3 *Let $\mathcal{S} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ and $\mathcal{T} = (\mathcal{Q}, \mathcal{C}, \mathcal{J})$ be incidence structures, and let φ be a bijection from $\mathcal{P} \cup \mathcal{B}$ to $\mathcal{Q} \cup \mathcal{C}$. Then:*

© Cambridge University Press www.cambridge.org