University of Victoria Notes for Math 322: Intermediate Combinatorics

Peter Dukes and Gary MacGillivray

April 5, 2011

Contents

Chapter 1

Generating Subsets and Permutations

We will discuss methods for listing all subsets, all k-subsets, and all permutations of $\{1, 2, \ldots, n\}$. These can be slightly modified so that they list all subsets, k-subsets, and permutations of an arbitrary n-set $\{x_1, x_2, \ldots, x_n\}$.

Method 1 for listing all subsets of $\{1, 2, \ldots, n\}$: This is based on the following proof by induction that the set $\{1, 2, \ldots, n\}$ has 2^n subsets.

> The number of subsets of $\emptyset$ is $1 = 2^0$, so the statement holds when $n = 0$. Suppose that $\{1, 2, \ldots, n-1\}$ has 2^{n-1} subsets, for some $n \geq 1$. For each subset $X \subseteq \{1, 2, \ldots, n\}$ there are two possibilities: either $n \notin X$ or $n \in X$. If $n \notin X$, then $X \subseteq \{1, 2, \ldots, n-1\}$ and, by the induction hypothesis, there are 2^{n-1} possibilities for X. On the other hand, if $n \in X$, then $X - \{n\} \subseteq \{1, 2, \ldots, n-1\}$. By the induction hypothesis, there are 2^{n-1} possibilities for $X - \{n\}$, and therefore 2^{n-1} possibilities for X. By the rule of sum, the number of subsets of $\{1, 2, \ldots, n\}$ equals $2^{n-1} + 2^{n-1} = 2^n$.

The above argument suggests that one could list the subsets of $\{1, 2, \ldots, n\}$ using the following recursive procedure:

Algorithm 1.1. (listing all subsets of $\{1, \ldots, n\}$)

- If $n = 0$, then the list is $\emptyset$.
- If $n \geq 1$ then,

- List the subsets of $\{1, 2, \ldots, n-1\}$
- List the subsets of $\{1, 2, \ldots, n-1\}$ again, and adjoin n to each of them.

To illustrate the algorithm, we generate the subsets of $\{1, 2, 3\}$.

- List the subsets of $\{1, 2\}$
    - List the subsets of $\{1\}$
        - List the subsets of $\emptyset$: $\quad \emptyset$
        - List the subsets of $\emptyset$ again, and adjoin 1 to each of them: $\quad \{1\}$
    - List the subsets of $\{1\}$ again, adjoining 2 to each: $\quad \{2\}, \{1, 2\}$
- List the subsets of $\{1, 2\}$ again, adjoining 3 to each: $\quad \{3\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}$

We have generated the list

$$\emptyset, \{1\}, \{2\}, \{1, 2\}, \{3\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}.$$

An advantage of recursive procedures is that it is often easy to prove by induction that they work.

Fact 1.2. *Algorithm 1.1 correctly generates the list of all subsets of* $\{1, 2, \ldots, n\}$.

Proof: Since the list of all subsets of $\emptyset$ is $\emptyset$, Algorithm 1.1 correctly generates the list when $n = 0$. Suppose, for some $n \geq 1$, that Algorithm 1.1 correctly generates the list of all subsets of $\{1, 2, \ldots, n-1\}$. Then, since each subset of $\{1, 2, \ldots, n\}$ that does not contain n is a subset of $\{1, 2, \ldots, n-1\}$, it correctly generates the list of all subsets of $\{1, 2, \ldots, n\}$ that do not contain n. Similarly, since deleting n from a subset of $\{1, 2, \ldots, n\}$ containing n yields a subset of $\{1, 2, , \ldots, n-1\}$, it correctly generates the list of all subsets of $\{1, 2, \ldots, n\}$ that contain n. Hence the list of all subsets of $\{1, 2, \ldots, n\}$ is generated correctly. The result now follows by induction. $\square$

Method 2 for listing all subsets of $\{1, 2, \ldots, n\}$: This is based on a 1-1 correspondence suggested by the following argument that shows $\{1, 2, \ldots, n\}$ has 2^n subsets.

> To form a subset $X \subseteq \{1, 2, \ldots, n\}$, there are two choices for each element i: either $i \in X$ or $i \notin X$. Thus, by the rule of product, there are 2^n possibilities for X.

The argument suggests we can associate with each subset $X \subseteq \{1, 2, \ldots, n\}$ a binary sequence $\mathbf{b}_X = b_1 b_2 \ldots b_n$ in which, for $i = 1, 2, \ldots, n$,

$$b_i = \begin{cases} 0 & \text{if } i \notin X \\ 1 & \text{if } i \in X. \end{cases}$$

The vector $\mathbf{b}_X$ is called the *characteristic vector*, or *characteristic function* of X. Every subset gives rise to some binary sequence of length n, and different subsets give rise to different sequences. Since there are the same number of subsets of $\{1, 2, \ldots, n\}$ as there are binary sequences of length n, the association just described is a one-to-one correspondence.

Hence, one can generate the list of all subsets of $\{1, 2, \ldots, n\}$ by generating the binary sequences $b_1 b_2 \ldots b_n$ of length n and, for each such sequence generated, putting the integer i into X if and only if $b_i = 1$. The list of binary sequences can be produced by counting from 0 to $2^n - 1$ in binary and adding leading zeros as appropriate.

For example, the list of binary sequences of length three in numerical order is

$$000, 001, 010, 011, 100, 101, 110, 111.$$

This corresponds to the list of subsets

$$\emptyset, \{3\}, \{2\}, \{2, 3\}, \{1\}, \{1, 3\}, \{1, 2\}, \{1, 2, 3\}.$$

Method 3 for generating all subsets of $\{1, 2, \ldots, n\}$ (Gray codes): This method uses the same correspondence between subsets of $\{1, 2, \ldots, n\}$ and binary sequences of length n as Method 2, but the sequences are listed in a different order.

A *Gray code* is a list of the 2^n binary sequences of length n such that consecutive sequences in the list differ in exactly one position. If the last and first sequences in the list also differ in exactly one position, then the Gray code is called *cyclic*.

Here is a different way of looking at Gray codes that involves graph theory. The *n-cube* is the graph Q_n whose vertices are the binary sequences of length n, and in which $x_1 x_2 \ldots x_n$ is adjacent to $y_1 y_2 \ldots y_n$ if and only if these two sequences differ in exactly one position. Notice that Q_n has a nice recursive structure. The set of vertices A consisting of the sequences whose first element is 0 induces a subgraph isomorphic to Q_{n-1}, as does the set of vertices B consisting of the sequences whose first element is 1. (Two sequences in A that are adjacent in Q_n must differ in one of the last $n - 1$ positions, and similarly for sequences in B.) Furthermore, every vertex in A is adjacent to exactly one vertex in B, namely the one to which it is identical in the last $n-1$ positions.

Recall that a *Hamilton path* in a graph G with p vertices is a sequence $u_1u_2\ldots u_p$ of vertices of G such that every vertex of G appears in the sequence (exactly once) and, for $i = 1, 2, \ldots, p-1$, vertex u_i is adjacent to vertex u_{i+1}. A *Hamilton cycle* in a graph G with p vertices is a sequence $u_1u_2\ldots u_pu_1$ in which $u_1u_2\ldots u_p$ is a Hamilton path in G, and u_p is adjacent to u_1.

Thus, a Gray code is a Hamilton path in the graph Q_n, and a cyclic Gray code is a Hamilton cycle in Q_n.

The *Binary Reflected Gray Code* (BRGC) is recursively defined as follows.

- $L_1 = 0, 1$.
- For $n \geq 2$, $L_n = 0 \cdot L_{n-1},\ 1 \cdot L_{n-1}^R$, where $x \cdot L$ means concatenate x at the start of every sequence in L, and L^R is the list L in reverse order.

Because the name given to the list just defined includes the term Gray code, one might be led to assume that it satisfies the definition. It does, but a proof is required.

Fact 1.3. *For each $n \geq 1$ the BRGC as defined above is a Gray code.*

Proof: The list L_1 is a Gray code. Suppose, for some $n \geq 2$, that L_{n-1} is a Gray code. The sequences $0 \cdot L_{n-1}$ resulting from concatenating a 0 on the front of each sequence in L_{n-1} still differ in exactly one place. Hence, $0 \cdot L_{n-1}$ is a list of all binary sequences of length n having first element 0, and consecutive sequences in this list differ in exactly one place. Similarly, $1 \cdot L_{n-1}^R$ is a list of all binary sequences of length n having first element 1, and consecutive sequences in this list differ in exactly one place. Finally, since the last element of L_{n-1} is the first element of L_{n-1}^R, the last element of $0 \cdot L_{n-1}$ differs from the first element of $1 \cdot L_{n-1}^R$ in the first position only. It is implicit in the argument that L_n has exactly 2^n elements. Therefore, L_n is a Gray code. The result now follows by induction. □

Corollary 1.4. *For each $n \geq 1$, the graph Q_n has a Hamilton path.*

It is left as an exercise to prove that the BRGC is cyclic (and therefore describes a Hamilton cycle in Q_n) when $n \geq 2$.

For example, the BRGC for $n = 3$ is $000, 001, 011, 010, 110, 111, 101, 100$. This corresponds to the list of subsets:

$$\emptyset, \{3\}, \{2, 3\}, \{2\}, \{1, 2\}, \{1, 2, 3\}, \{1, 3\}, \{1\}.$$

Method 4 for listing all subsets of $\{1, 2, \ldots, n\}$: This method is based on the combinatorial proof given below that

$$\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n} = 2^n.$$

> The RHS counts the number of subsets of $\{1, 2, \ldots, n\}$. The LHS counts the same thing by cases organised by the number of elements in the subset, which is between 0 and n, inclusive. For $k = 0, 1, \ldots, n$, the number of k-subsets of $\{1, 2, \ldots, n\}$ is $\binom{n}{k} = n!/k!(n-k)!$. Thus by the rule of sum, the LHS, $\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n}$, is the number of subsets of $\{1, 2, \ldots, n\}$. Since the LHS and RHS count the same thing, they are equal.

The above argument suggests that one can list all subsets of $\{1, 2, \ldots, n\}$ by first listing the $\binom{n}{0}$ subsets of size 0, then the $\binom{n}{1}$ subsets of size 1, and so on until, finally, the $\binom{n}{n}$ subsets of size n are listed. Unfortunately, at this point in time we don't know how to list all k-subsets of $\{1, 2, \ldots, n\}$. This is our next topic.

Listing all k-subsets of $\{1, 2, \ldots, n\}$: There is a 1-1 correspondence between k-subsets of $\{1, 2, \ldots, n\}$ and (*increasing*) sequences $x_1 x_2 \ldots x_k$ with $1 \leq x_1 < x_2 < \cdots < x_k \leq n$ because there are $\binom{n}{k}$ ways to select the k elements and only one way to sort them into increasing order. Thus, it suffices to list the k-element increasing sequences just mentioned. We will do this in the order they would appear in a dictionary. Recall, for different sequences $x_1 x_2 \ldots x_r$ and $y_1 y_2 \ldots y_s$ whose elements are from $\{1, 2, \ldots, n\}$ (but not necessarily distinct or sorted), that $x_1 x_2 \ldots x_r$ *precedes* $y_1 y_2 \ldots y_s$ *in dictionary order* if and only if

- $r < s$ and $x_i = y_i$ for $i = 1, 2, \ldots, r$, or
- there exists a subscript j such that $x_i = y_i$ for $i = 1, 2, \ldots, j-1$ and $x_j < y_j$.

Here, our sequences all have the same length, so the second condition alone determines when one comes before another.

The list of 3-element increasing sequences $x_1x_2x_3$, with $1 \leq x_1 < x_2 < x_3 \leq 5$, in dictionary order is:

$$123, 124, 125, 134, 135, 145, 234, 235, 245, 345.$$

Proposition 1.5. *If $1 \leq x_1 < x_2 < \cdots < x_k \leq n$, then for $i = 1, 2, \ldots, k$, $x_i \leq n-(k-i)$.*

Proof: We use downward induction on i. By hypothesis, $x_k \leq n$. Suppose $x_j \leq n-(k-j)$ for some j, $2 \leq j \leq k$. Then, $x_{j-1} < x_j$, so $x_{j-1} \leq n-(k-j)-1 = n-(k-(j-1))$, as required. The result now follows by induction. □

The first increasing k-element sequence in dictionary order is $123\ldots k$, and the last one is $(n-(k-1))(n-k)\ldots n$. Taken together, the next two propositions say how to find the increasing sequence following $x_1x_2\ldots x_k$, if one exists.

Proposition 1.6. *If $x_1x_2\ldots x_k \neq (n-(k-1))(n-(k-2))\cdots n$, then there exists a subscript i such that $x_i < n-(k-i)$.*

Proof: We prove the contrapositive. Suppose no such subscript i exists. Then, for $i = 1, 2, \ldots, k$, $x_i = n-(k-i)$. That is, $x_1x_2\ldots x_k = (n-(k-1))(n-(k-2))\cdots n$. The result now follows. □

Proposition 1.7. *Suppose $x_1x_2\ldots x_k \neq (n-(k-1))(n-(k-2))\cdots n$, and i is the largest subscript such that $x_i < n-(k-i)$.*

1. *No sequence that starts $x_1x_2\ldots x_i$ comes after $x_1x_2\ldots x_k$ in dictionary order.*

2. *The first sequence in dictionary order that starts $x_1x_2\ldots x_{i-1}(x_i+1)$ is*

$$x_1x_2\ldots x_{i-1}(x_i+1)(x_i+2)\cdots(x_i+(k-i)+1).$$

Proof: We prove (1), and leave the proof of (2) as an exercise. For (1), suppose the statement is false, so that some sequence $x_1x_2\ldots x_iy_{i+1}y_{i+2}\ldots y_k$ comes after $x_1x_2\ldots x_k$ in dictionary order. Then, for some $j > i$ we have $y_j > x_j$. But, since $j > i$, the definition of i implies $x_j = n-(k-j)$. Hence $y_j > n-(k-j)$, contradicting Proposition 1.5. This completes the proof of (1). □

Thus, we arrive at the following procedure.

Algorithm 1.8. (listing all increasing k-element sequences from $\{1, \ldots, n\}$)

- The first sequence is $123 \ldots k$.
- Suppose the current sequence (the one just generated) is $x_1x_2 \ldots x_k$. Then,
    - If the current sequence is $(n-(k-1))(n-(k-2)) \cdots n$, the list is complete.
    - Otherwise,
        - Let i be the largest subscript such that $x_i < n-(k-i)$.
        - The next sequence is $x_1x_2 \ldots (x_i+1)(x_i+2) \cdots (x_i+(k-i)+1)$.

By Propositions 1.5, 1.6, and 1.7, Algorithm 1.8 correctly generates the list of k-subsets of $\{1, 2, \ldots, n\}$.

Generating permutations of $\{1, 2, \ldots, n\}$ in dictionary order

The list of permutations of $\{1, 2, 3\}$ in dictionary order is: $123, 132, 213, 231, 312, 321$. It is clear that, in general, the first permutation in the list is $123 \ldots n$, and the last one is $n(n-1) \ldots 1$. The next two propositions are the key to our procedure.

Proposition 1.9. *If the permutation $p_1p_2 \ldots p_n \neq n(n-1) \ldots 1$, then there exists i such that $p_i < p_{i+1}$.*

Proof: The contrapositive of this statement states that $p_1p_2 \ldots p_n$ must be nonincreasing. Since each element from $\{1, \ldots, n\}$ is represented exactly once, we have $p_1p_2 \ldots p_n = n(n-1) \ldots 1$. □

Proposition 1.10. *Suppose the permutation $\pi = p_1p_2 \ldots p_n \neq n(n-1) \ldots 1$. Let i be the largest subscript such that $p_i < p_{i+1}$. Let p_j be the smallest element which islarger that p_i among $p_{i+1}, p_{i+2}, \ldots, p_n$, and let*

$$\sigma = p_1p_2 \ldots p_{i-1}p_jp_np_{n-1} \ldots p_{j+1}p_ip_{j-1} \ldots p_{i+1}.$$

Then σ is the element following π in dictionary order.

Proof: Since $p_j > p_i$, the permutation σ comes after π in dictionary order. Also, by definition of i, the elements $p_{i+1}, p_{i+2}, \ldots, p_n$ are in decreasing order in π. Thus, π is the last permutation in dictionary order that begins $p_1p_2 \ldots p_i$. Similar reasoning shows that σ is the first permutation in dictionary order that begins $p_1p_2\ldots p_{i-1}p_j$. Hence, any permutation that comes between σ and π in dictionary order must begin $p_1p_2\ldots p_{i-1}x$, where $p_i < x < p_j$. By definition of p_j, no such x exists. Therefore σ is the element following π in dictionary order. □

This fact is implemented in the following algorithm.

Algorithm 1.11. (listing all permutations of $\{1, 2, \ldots, n\}$ in dictionary order)

- The first permutation in the list is $123\ldots n$.
- Suppose the current permutation (the one just generated) is $\pi = p_1p_2\ldots p_n$.
    - If $\pi = n(n-1)\ldots 1$, the list is complete.
    - Otherwise,
        - Let i be the largest subscript such that $p_i < p_{i+1}$.
        - Let p_j be the next largest element after p_i among $p_{i+1}, p_{i+2}, \ldots, p_n$.
        - The next permutation is $p_1p_2\ldots p_{i-1}p_jq_{i+1}q_{i+2}\ldots q_n$, where $q_{i+1}q_{i+2}\ldots q_n$ are $p_i, p_{i+1}, \ldots, p_{j-1}, p_{j+1}, p_{j+2}, \ldots, p_n$ sorted into increasing order.

Proposition 1.10 implies that Algorithm 1.11 works correctly.

Exercises

1. (a) Give a combinatorial proof – a proof that uses a counting argument – of Pascal's identity: $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$.

   (b) Describe a procedure for listing all k-subsets of $\{1, 2, \ldots, n\}$ that is based on ideas from your proof in (a).

   (c) Prove that the procedure you described in (b) works.

2. Prove that for $n \geq 2$ the Binary Reflected Gray Code is cyclic.

3. (a) Show that if n is even, there is no Hamilton path in Q_n that starts at $00\ldots 0$ and ends at $11\ldots 1$.

   (b) Show that if n is odd then there is a Hamilton path in Q_n that starts at $00\ldots 0$ and ends at $11\ldots 1$. (*Hint*: one way to do this starts by considering the Binary Reflected Gray Code.)

4. Prove statement (2) of Proposition 1.7.

5. List, in dictionary order, all sequences of length 5 which contain exactly two 0s, two 1s, and one 2. (For instance, such a sequence is 01021.) Which algorithm(s) can be used to solve this kind of problem in more generality?

6. A *partition* of a set X is an unordered collection of nonempty, pairwise disjoint subsets of X whose union is all of X. For example, the partitions of $\{1, 2, 3\}$ are:

$$\{\{1, 2, 3\}\},\ \{\{1, 2\}, \{3\}\},\ \{\{1, 3\}, \{2\}\},\ \{\{1\}, \{2, 3\}\}, \text{ and } \{\{1\}, \{2\}, \{3\}\}.$$

Give an algorithm to generate all partitions of $\{1, 2, \ldots, n\}$ exactly once each. You may assume a procedure for generating subsets without repeating the details.

7. (a) Suppose $0 \le N < 2^n$ and let $b_{n-1}b_{n-2}\ldots b_0$ be the binary representation of N. Define $b_n = 0$, and for $i = 0, 1, \ldots, n-1$ define $a_{n-1}a_{n-2}\ldots a_0$ according to the rule

$$a_i = \begin{cases} 0 & \text{if } b_i = b_{i+1}, \\ 1 & \text{if } b_i \ne b_{i+1}. \end{cases}$$

Prove that in the Binary Reflected Gray Code, the sequence in the Nth position (when indexing from 0) is $a_{n-1}a_{n-2}\ldots a_0$. (*Hint*: use induction on n and consider the cases $b_{n-1} = 0$ and $b_{n-1} = 1$ separately.)

   (b) Let $a_{n-1}a_{n-2}\ldots a_0$ be some binary sequence of length n. For $i = 0, 1, \ldots, n-1$, let $b_i = a_i + a_{i+1} + \cdots + a_{n-1} \pmod 2$. Let $N \ge 0$ be the integer whose binary representation is $b_{n-1}b_{n-2}\ldots b_0$. Prove that the sequence $a_{n-1}a_{n-2}\ldots a_0$ occurs in the Nth position of the Binary Reflected Gray Code (again, indexing from 0).

8. Let n be a fixed positive integer. The *rank* of a permutation $\pi = p_1p_2\ldots p_n$ is the position in which π appears in the dictionary order, starting from 0. For instance, if $n = 6$, the rank of 123456 is 0 and the rank of 654321 is $6! - 1 = 719$.

   (a) Determine, with proof, the rank of 246135.

   (b) For general n, describe the permutation whose rank is $n!/2$. Justify your answer.

9. Suppose the permutation $\pi = p_1p_2\ldots p_n \ne n(n-1)\ldots 1$. Let i be the largest subscript such that $p_i < p_{i+1}$. Let p_j be the next largest element after p_i among

$p_{i+1}, p_{i+2}, \ldots, p_n$. Let $\sigma = s_1 s_2 \ldots s_n$ be the permutation obtained from π by exchanging p_i and p_j. Prove that the elements $s_{i+1}, s_{i+2}, \ldots, s_n$ appear in decreasing order in σ (so that they may be put into increasing order by simply reversing this part of the permutation).

Chapter 2

Systems of Distinct Representatives

The main idea is that you are given a collection of sets and would like to know if it is possible to select a different element from each of them.

Let $A_1, A_2, \ldots, A_n$ be sets. A *system of distinct representatives* (SDR) for these sets is an n-tuple $(x_1, x_2, \ldots, x_n)$ such that

- (distinct) $x_i \neq x_j$ if $i \neq j$, and
- (representatives) $x_i \in A_i$ for $i = 1, 2, \ldots, n$.

We say that x_i *represents* A_i (or that x_i is the representative of A_i), $1 \leq i \leq n$.

Here are some things to note:

1. The sets $A_1, A_2, \ldots, A_n$ need not be distinct, or non-empty.
2. It is allowed that $x_i \in A_j$ when $i \neq j$ (but x_i is not the representative of A_j).
3. Here, we are interested in the case when $A_1, A_2, \ldots, A_n$ are each finite sets.

Example 2.1. Consider the collection $A_1, A_2, A_3, A_4, A_5, A_6, A_7 = \{1,3,7\}$, $\{1,2,4\}$, $\{2,3,5\}$, $\{3,4,6\}$, $\{4,5,7\}$, $\{1,5,6\}$,$\{2,6,7\}$. Then $(1,2,3,4,5,6,7)$ and $(3,1,5,4,7,6,2)$ are both SDRs of the collection.

Suppose $A_1, A_2, \ldots, A_n$ has a SDR, and let $I \subseteq \{1, 2, \ldots, n\}$. Then, the union of the sets whose indices (subscripts) are in I contains the representatives of these sets, and therefore has at least $|I|$ elements. We define *Hall's condition* to be the statement:

$$\left|\bigcup_{i\in I} A_i\right| \geq |I| \text{ for every } I \subseteq \{1,2,\dots,n\}.$$

If Hall's condition does not hold, then there is a collection of some k of the sets whose union contains fewer than k elements. Since this is fewer than the number of elements needed as representatives for these sets, a SDR can not exist.

Example 2.2. Consider the collection

$$A_1, A_2, A_3, A_4, A_5 = \{1,2,4,5\}, \{2,3\}, \{3,4\}, \{2,4\}, \{3,4\}.$$

This collection has no SDR since Hall's condition does not hold for $I = \{2,3,4,5\}$:

$$|A_2 \cup A_3 \cup A_4 \cup A_5| = |\{2,3,4\}| = 3 < 4 = |I|.$$

It turns out that Hall's (necessary) condition is also sufficient for the existence of a SDR.

Theorem 2.3. (Hall's Theorem, 1935) *The collection $A_1, A_2, \dots, A_n$ of finite sets has a SDR if and only if*

$$\left|\bigcup_{i\in I} A_i\right| \geq |I| \textit{ for every } I \subseteq \{1,2,\dots,n\}.$$

Proof: ($\Rightarrow$) If $A_1, A_2, \dots, A_n$ has a SDR then, for any $I \subseteq \{1,2,\dots,n\}$, the union of the sets whose indices are in I contains the representatives of these sets, and therefore has at least $|I|$ elements.

($\Leftarrow$) Suppose Hall's condition, $|\cup_{i\in I} A_i| \geq |I|$ for every $I \subseteq \{1,2,\dots,n\}$, holds. The proof is by induction on n. The condition guarantees that any collection of one set contains at least one element, which can be chosen to be its representative. Thus, the statement is true for $n = 1$. Suppose, for some $n \geq 2$ and all k with $1 \leq k < n$, that any collection of k sets satisfying Hall's condition has a SDR. Consider a collection of n sets satisfying Hall's condition. There are two cases:

CASE 1: For every non-empty proper subset $I \subseteq \{1,2,\dots,n\}$, $|\cup_{i\in I} A_i| > |I|$.

By Hall's condition, $A_n \neq \emptyset$. Let $x_n \in A_n$. For $i = 1,2,\dots,n-1$, let $A_i' = A_i - \{x_n\}$. Then, for any $J \subseteq \{1,2,\dots,n-1\}$,

$$|\cup_{j\in J} A_j'| = |\cup_{j\in J} A_j - \{x_n\}| \geq |\cup_{j\in J} A_j| - 1 \geq |J|,$$

where we have used the hypothesis for Case 1. Thus, by the induction hypothesis, the collection $A'_1, A'_2, \ldots, A'_{n-1}$ has a SDR $(x_1, x_2, \ldots, x_{n-1})$. By construction, $x_n \notin A'_i$ for $i = 1, 2, \ldots, n-1$. Therefore $(x_1, x_2, \ldots .x_n)$ is a SDR for $A_1, A_2, \ldots, A_n$.

CASE 2: There exists a non-empty proper subset $I \subseteq \{1, 2, \ldots, n\}$ such that $| \cup_{i \in I} A_i| = |I|$.

Consider any such set I. By the induction hypothesis, the collection of sets $A_i,\ i \in I$ has a SDR. For each $\ell \in \{1, 2, \ldots, n\} - I$, define $A'_\ell = A_\ell - \cup_{i \in I} A_i$. Then, for any subset $M \subseteq \{1, 2, \ldots, n\} - I$,

$$| \cup_{m \in M} A'_m| = | \cup_{m \in I \cup M} A_m| - | \cup_{i \in I} A_i| \geq |I \cup M| - |I| = |M|,$$

by Hall's condition and the hypothesis to Case 2. Thus, by the induction hypothesis, the collection of sets $A_m,\ m \in \{1, 2, \ldots, n\} - I$ has a SDR. By construction, the SDRs we have found for $A_i,\ i \in I$ and $A_m,\ m \in \{1, 2, \ldots, n\} - I$ have no elements in common. Combining them gives a SDR for $A_1, A_2, \ldots, A_n$.

In each case, the given collection has a SDR. The result now follows by induction. □

Hall's Theorem is an example what has been called a *good characterisation*. This means that it is possible to use the theorem to describe an easily checkable proof (or certificate) that the object in question has, or does not have, the property being considered. In this case, one can prove that a collection of sets has a SDR by displaying one, and one can prove that there is no SDR by displaying a sub-collection of k of the sets whose union contains fewer than k elements. It is easy to check whether an n-tuple satisfies the definition of a SDR, and it is easy to check whether the union of some k given sets has fewer than k elements.

Hall's Theorem is sometimes called *Hall's Marriage Theorem* because of its connection to the so-called *marriage problem*:

> In a certain town there are a collection of n boys and n girls. Each of the boys is compatible with exactly $k > 0$ girls, and each of the girls is compatible with exactly k boys. Show that it is possible for each of the n girls to marry one of the boys with whom she is compatible.

We assume that the relation "is compatible with" is symmetric, so that if Bob is compatible with Grace, then Grace is compatible with Bob. Thus each boy would also marry a person with whom he is compatible.

A more general version of this problem involves m boys and n girls, each of whom is compatible with a non-empty subset of members of the opposite gender. Hall's Theorem gives necessary and sufficient conditions for each girl to marry a boy with whom she is compatible: for $r = 1, 2, \ldots, n$, every subset of r of the girls must be compatible with at least r of the boys.

We now use Hall's Theorem to solve the marriage problem.

Theorem 2.4. *Let $k > 0$ and let $A_1, A_2, \ldots, A_n$ be a collection of k-subsets of a finite set X such that every element of X appears in exactly k sets in the collection. Then $A_1, A_2, \ldots, A_n$ has a SDR.*

Proof: It is sufficient to show that Hall's condition holds. Let $I \subseteq \{1, 2, \ldots, n\}$. The total number of pairs (a, B), where $a \in B \in \{A_i : i \in I\}$, including repetitions, is clearly $k|I|$. Now we consider a first, followed by B. Since each element of X belongs to at most k of the sets A_i, $i \in I$, the number of such pairs (a, B) is no more than $k| \cup_{i \in I} A_i|$. Thus, $k| \cup_{i \in I} A_i| \geq k|I|$ and we get Hall's condition upon cancelling k. □

To solve the marriage problem, number the girls $1, 2, \ldots, n$ and let A_i be the set of boys with which girl i is compatible. Since each girl is compatible with $k > 0$ boys, each of these sets has size k, and since each boy is compatible with k girls, each element of the set of boys appears in exactly k of the sets. A SDR of this collection of sets corresponds to a situation in which each girl marries a boy with whom she is compatible and, by Theorem 2.4, a SDR exists.

Once we know a collection of sets has a SDR (which can be determined using Hall's Theorem), we might want an estimate of how many SDRs it has. This is the topic we consider next. Before proceeding, we should be sure to understand what it means for two SDRs of $A_1, A_2, \ldots, A_n$ to be different. A SDR is an n-tuple, and $(x_1, x_2, \ldots, x_n) \neq (y_1, y_2, \ldots, y_n)$ if an only if there exists i such that $x_i \neq y_i$, so two SDRs are the different if and only if some set has a different representative in one of them than it does in the other. For example, $(1, 2)$ and $(2, 1)$ are different SDRs of $A_1 = \{1, 2\}, A_2 = \{1, 2, 3\}$. These contain the same elements, but in $(1, 2)$ the element 1 is the representative of A_1 while in $(2, 1)$ the element 2 is the representative of A_1.

Theorem 2.5. *Suppose the collection of finite sets $A_1, A_2, \ldots, A_n$ has a SDR. If $|A_i| \geq k$ for $i = 1, 2, \ldots, n$, then the number of SDRs of the collection is at least*

$$s(k, n) = \begin{cases} k! & \text{if } k \leq n, \\ k!/(k-n)! & \text{if } k > n. \end{cases}$$

Proof: We use induction on n. The idea is to follow the argument used to prove Hall's Theorem and get an estimate of how many choices there are. Note that since the collection has a SDR, $k \geq 1$.

If $n = 1$, then any collection of one set with at least k elements has $k = s(k, 1)$ SDRs. Suppose, for some $n \geq 2$ and all t such that $1 \leq t < n$, that any collection of t sets satisfying the hypotheses has at least $s(k, t)$ SDRs. Consider a collection of finite sets $A_1, A_2, \ldots, A_n$, with $|A_i| \geq k$ for $i = 1, 2, \ldots, n$, that has a SDR.

In Case 1 of the proof of Hall's Theorem, there are $|A_n| \geq k$ choices for the element x_n, and the reduced collection of sets $A'_1, A'_2, \ldots, A'_{n-1}$ has an SDR and $|A_i| \geq k - 1$ for $i = 1, 2, \ldots, n - 1$. Thus, by the induction hypothesis, $A'_1, A'_2, \ldots, A'_{n-1}$ has at least $s(k - 1, n - 1)$ SDRs. By the rule of product, the number of SDRs of $A_1, A_2, \ldots, A_n$ is at least $k \cdot s(k - 1, n - 1) = s(k, n)$.

In Case 2 of the proof of Hall's Theorem, since each set in the collection contains at least k elements, we must have $k \leq |I| < n$. By the induction hypothesis, the collection $A_i, i \in I$ has at least $s(k, |I|) = s(k, n)$ SDRs, each of which can be extended to a SDR of $A_1, A_2, \ldots, A_n$.

The result now follows by induction. □

Corollary 2.6. *Let $k > 0$ and let $A_1, A_2, \ldots, A_n$ be a collection of k-subsets of $\{1, \ldots, n\}$ such that for $i = 1, 2, \ldots, n$ the element i belongs to exactly k sets in the collection. Then $A_1, A_2, \ldots, A_n$ has at least $k!$ SDRs.*

There are a large number of theorems in combinatorics that are equivalent in the sense that any one of them can be used to prove all of the others. Hall's Theorem is one of these. A second one is König's theorem, below. We will meet others later on.

A *0-1 matrix* is a matrix whose entries a_{ij} each equal 0 or 1. A *line of a matrix A* is a row or a column of A.

Corollary 2.7. (König's Theorem) *Let A be a 0-1 matrix. The minimum number of lines containing all the ones of A equals the maximum number of ones in A, no two on a line.*

Proof: Let m be the minimum number of lines containing all 1s of A, and let M be the maximum number of 1s in A, no two on a line. Since there are M 1s, no two on a line, at least M lines are needed to contain all 1s in A. Hence, $m \geq M$.

Suppose the minimum number of lines that contains all ones of A consists of the rows in the set R and the columns in the set C, so that $m = |R| + |C|$. For each $i \in R$, define A_i to be the set of all $j \notin C$ such that $a_{ij} = 1$.

We claim that these sets satisfy Hall's Condition (and thus have a SDR). Consider any collection of k of the sets $A_i, i \in R$. If these together contained $k - 1$ or fewer elements, then the corresponding k rows could be replaced by $k - 1$ or fewer columns (any other 1s in these rows are contained in columns belonging to C) and the resulting set of lines would still contain all 1s in A. This contradiction proves the claim.

By Hall's Theorem, the collection $A_i, i \in R$ had a SDR. This gives a set of $|R|$ 1s, no two on a line, among the rows in R and the columns not in C.

By a similar argument there is a set of $|C|$ 1s, no two on a line, among the columns in C and the rows not in R. Thus $M \geq |R| + |C| = m$, and therefore $m = M$. This completes the proof. □

To illustrate the main part of the proof, consider the matrix

$$A = \begin{bmatrix} 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{bmatrix}.$$

A minimum set of (four) lines that contains all ones of A consists of the rows in $R = \{2, 5\}$ and the columns in $C = \{2, 3\}$. We follow the proof of König's theorem to find a collection of four ones, no two on a line. For the rows in R, we define the sets $A_2 = \{1, 4, 5\}$ and $A_5 = \{4, 5\}$. These have the SDR $(1, 4)$. Similarly, for the columns in C, we define the sets $B_2 = \{1, 3, 4\}$ and $B_3 = \{1, 3, 4\}$. These have the SDR $(1, 3)$. Thus four ones, no two on a line, are located in positions $(2, 1), (5, 4)$, $(1, 2)$, and $(3, 3)$. The first two of these arise from the SDR for A_2, A_5, and the last two arise from the SDR for B_2, B_3 (remember that 2 and 3 are the column indices).

We proved König's Theorem by showing that it followed from the truth of Hall's Theorem. The converse implication, that the truth of König's Theorem implies the truth of Hall's Theorem, is left as an exercise.

Exercises

1. Determine if each collection of sets has a SDR. In each case, certify your answer in the sense of the discussion following the proof of Hall's Theorem.

   (a) $A_1 = \{1,4\}, A_2 = \{1,3\}, A_3 = \{2,3,6\}, A_4 = \{2,5,6\}, A_5 = \{3,6\}$.

   (b) $A_1 = \{1,2,6\}, A_2 = \{1,7\}, A_3 = \{1,2,3,4,6\}, A_4 = \{1,2,7\}, A_5 = \{2,6\}, A_6 = \{3,4,5,6\}$, $A_7 = \{1,6,7\}$.

   (c) $A_1 = \{1,3,5\}, A_2 = \{1,2,3\}, A_3 = \{3,5,7\}, A_4 = \{1,3,7\}, A_5 = \{1,2,5,6,7\}$, $A_6 = \{1,5,7\}, A_7 = \{2,3,4,7,8\}, A_8 = \{2,4,6,7,8\}$.

2. For $i = 1,2,\ldots,n$, let $A_i = \{1,2,\ldots,n\} - \{i\}$. Show that there is a 1-1 correspondence between SDRs of $A_1, A_2, \ldots, A_n$ and derangements of $\{1,2,\ldots,n\}$. (Recall that a *derangement* of $\{1,2,\ldots,n\}$ is a permutation $p_1p_2\ldots p_n$ such that $p_i \neq i,\ 1 \leq i \leq n$.)

3. For each $n \geq 1$, find a collection of finite sets $A_1, A_2, \ldots, A_n$ that has exactly two SDRs.

4. Suppose $A_1, A_2, \ldots, A_n$ contain $2, 3, \ldots, n+1$ elements, respectively. Show that this collection has at least 2^n SDRs. Find such a collection with exactly 2^n SDRs.

5. Let $A_1, A_2, \ldots, A_n$ be a collection of sets such that $|\cup_{i\in I} A_i| \geq |I| - d$ for every $I \subseteq \{1,2,\ldots,n\}$. Prove that some sub-collection of $n-d$ of the sets $A_1, A_2, \ldots, A_n$ has a SDR. (*Hint:* Form a new collection of sets by adding d new elements to each set, and use Hall's Theorem.)

6. A team of four executives from the Halifax office of Coast Combinatorial Services flies out to Victoria to meet with their four counterparts from the Victoria office. There are a number of topics about which each pair of executives from the different offices must meet. These are summarised in the matrix A below, whose (i,j) entry is the number of topics about which Victoria executive i and Halifax executive j must meet:
$$A = \begin{bmatrix} 4 & 1 & 2 & 1 \\ 3 & 2 & 2 & 1 \\ 1 & 3 & 2 & 2 \\ 0 & 2 & 2 & 4 \end{bmatrix}.$$
Each meeting takes one hour, involves two people, and covers one topic. Is it possible for all meetings to be scheduled in a single eight hour work day?

7. Let $k > 0$ and let $A_1, A_2, \ldots, A_n$ be a collection of k-subsets of a finite set X such that every element of X appears in exactly k sets in the collection. Prove that $|X| = n$.

8. Use König's Theorem to prove Hall's Theorem.

   (*Hint*: Let $X = \cup_{i \in I} A_i = \{x_1, x_2, \ldots, x_m\}$, and let A be the $m \times n$ 0-1 matrix in which
$$a_{ij} = \begin{cases} 0 & \text{if } x_j \notin A_i, \\ 1 & \text{if } x_j \in A_i. \end{cases}$$
   Show that Hall's condition implies that n lines are needed to contain all ones of A.)

9. Analyze the extremal cases for the number of distinct SDRs for a family $A_1, \ldots, A_n$ of k-sets. In other words, what is the maximum possible number of SDRs, and when does equality occur in Theorem 2.5?

10. (a) Call two SDRs $(x_1, x_2, \ldots, x_n)$ and $(y_1, y_2, \ldots, y_n)$ *disjoint* if $x_i \neq y_i$ for each $i = 1, 2, \ldots, n$. Suppose $A_1, A_2, \ldots, A_n$ are each k-subsets of $\{1, 2, \ldots, n\}$, and that every element in $\{1, 2, \ldots, n\}$ belongs to exactly k of the A_i. Prove that these sets have k SDRs, any two of which are disjoint.

    (b) An $n \times n$ matrix is a *permutation matrix* if it can be obtained from the $n \times n$ identity matrix by some rearrangement of the rows. Suppose A is a 0-1 matrix with the sum of entries on each line equal to k. Show that A is a sum of k permutation matrices.

11. Show that Theorem 2.4 is actually true more generally if every element of X appears in exactly l sets in the collection, where $0 < l \leq k$.

Chapter 3

Posets and extremal set theory

Recall that a *(binary) relation* on a set P is a subset R of the Cartesian product $P \times P$. When $(x, y) \in R$ the infix notation $x\,R\,y$ is often adopted, and we say that x and y are *related* under R.

We will drop the adjective "binary", as all of the relations we study will involve pairs of objects. Sometimes a symbol which is not a letter is used, as in $x \leq y$.

A binary relation is abstracted from the idea of forming ordered pairs of elements of a set that are "related" in some way. Instead of trying to formulate what it means for two objects to be "related", we instead declare a relation to be any collection of ordered pairs of objects, and then study relations that have various additional properties (a mathematician's solution for sure!).

A relation $\preceq$ on P is called a *partial order* if it satisfies the three conditions:

- ($\preceq$ is *reflexive*) $x \preceq x$ for all $x \in P$.
- ($\preceq$ is *anti-symmetric*) if $x \preceq y$ and $y \preceq x$, then $x = y$ for all $x, y \in P$.
- ($\preceq$ is *transitive*) if $x \preceq y$ and $y \preceq z$ then $x \preceq z$ for all $x, y, z \in P$.

Here are some examples (verification that each of these is a partial order is left as an exercise):

1. The relation $\leq$ is a partial order on any set P of real numbers.

2. The relation *divides* defined by $x \mid y$ if and only if there is an integer k such that $kx = y$ is a partial order on any set P of positive integers. (What goes wrong with allowing all integers?)

3. The relation $\subseteq$ is a partial order on $\mathcal{P}(X)$, the set of all subsets of X.

There is a sense in which "is a subset of" is a better model of a partial order then "less than or equal to". Given two sets B and C, three possibilities can arise: it could be that $B \subseteq C$, it could be that $C \subseteq B$, or it could be that neither set is a subset of the other. If $\preceq$ is a partial order on P, then for any two elements $x, y \in P$ one of the three possibilities $x \preceq y$, $y \preceq x$, or $x \not\preceq y$ and $y \not\preceq x$ must arise (the symbol $\not\preceq$ is intended to mean that x and y are not related under $\preceq$). The less than or equal to relation has an additional property in the sense that the third case above can not arise. Given any two numbers it is guaranteed that one is less than or equal to the other (if they are equal, then each is less than or equal to the other).

Let $\preceq$ be a partial order on a set P. We say $x, y \in P$ are *comparable* if either $x \preceq y$ or $y \preceq x$, and *incomparable* if neither possibility holds. A *total order* (or *linear order*) is a partial order in which every pair of elements are comparable.

Less than or equal to is a total order on any set of real numbers. The subset relation is a total order on $\mathcal{P}(\{1\}) = \{\emptyset, \{1\}\}$ but not on $\mathcal{P}(\{1,2\}) = \{\emptyset, \{1\}, \{2\}, \{1,2\}\}$ (because $\{1\}$ and $\{2\}$ are incomparable. Similarly, the divides relation is a total order on $\{1, 2, 4, 8, 16\}$ but not on $\{1, 2, 3\}$ (because neither $2 \mid 3$ nor $3 \mid 2$).

A *partially ordered set*, or *poset*, is an ordered pair $(P, \preceq)$, where P is a set and $\preceq$ is a partial order on P. When the relation $\preceq$ is understood (or just some abstract partial order), we talk about the poset P. A *totally ordered set* is defined similarly.

For example, $(\mathbb{Z}, \geq)$, $(\mathcal{P}(\{a, b, c\}), \subseteq)$, and $(\{1, 2, \ldots, 12\}, |)$ are all posets.

Let $\preceq$ be a partial order on P. For $x, y \in P$ we write $x \prec y$ if $x \preceq y$ and $x \neq y$.

The *Hasse diagram* gives a pictorial representation of a poset $(P, \preceq)$. Let u and v be distinct elements of P. We say that v *covers* u if $u \prec v$ and there is no element w such that $u \prec w \prec v$. The Hasse diagram of P is a graph drawn in the plane as follows:

- each vertex corresponds to a point in P,

- if v covers u then the point corresponding to u is "below" (has a smaller y-coordinate than) the point corresponding to v, and the points u and v are joined by an edge.

The Hasse diagram tells us everything about the poset P. It tells us what the points are (provided the vertices are labelled – but the names of the points are not really important) and, by definition of "covers", $x \prec y$ if and only if there is a path from x to y in which every edge goes upwards.

Let $(P, \preceq)$ be a poset. An element $x \in P$ is a *maximal element* is there is no element $y \in P$ such that $x \prec y$. A *minimal element* is defined similarly. Equivalently, an element x of a poset P is a maximal (respectively, minimal) element if $x \preceq y$ (respectively, $y \preceq x$) implies $x = y$.

A *chain* in a poset $(P, \preceq)$ is a subset $C \subseteq P$ such that any two elements of C are comparable. Note that P itself is a chain if and only if $\preceq$ is a total order on P.

If C is a chain containing n elements then, by anti-symmetry and transitivity of $\preceq$, the elements of C can be listed as

$$x_1 \prec x_2 \prec \cdots \prec x_n.$$

We will sometimes specify a chain by listing its elements in this way. The *length* of a chain is the number of elements it contains. The element x_1 is the *least* element of the chain, and x_n is the *greatest* element of the chain.

Proposition 3.1. *A non-empty finite poset has both a maximal element and a minimal element.*

Proof: Let $(P, \preceq)$ be a non-empty finite poset and let $x_1 \prec x_2 \prec \cdots \prec x_k$ be a longest chain in P. Then $1 \leq k \leq |P|$. If x_k is not a maximal element, then there is an element x_{k+1} such that $x_k \prec x_{k+1}$. But then (by transitivity) $x_1 \prec x_2 \prec \cdots \prec x_k \prec x_{k+1}$ is a longer chain than our longest chain, a contradiction. A similar argument shows that x_1 is a minimal element in $(P, \preceq)$. □

An *antichain* in a poset $(P, \preceq)$ is a subset $A \subseteq P$ such that no two elements of A are comparable.

Let $\preceq$ be a partial order on P. According to the definition of partial order, $\preceq$ is technically not a partial order on any proper subset $Q \subset P$, since it is not a subset of $Q \times Q$. (if $x \in P - Q$, then $(x, x) \in \preceq$ but $(x, x) \notin Q \times Q$. Nevertheless, the intersection of $\preceq$ and

$Q \times Q$ is a partial order on Q (see Exercise 5). Since little confusion can arise, if $Q \subseteq P$ we will denote the poset obtained by this restriction of $\preceq$ to elements of Q by $(Q, \preceq)$. Furthermore, it follows from its definition that every chain in the poset Q is a chain in P and every antichain in Q is an antichain in P.

Theorem 3.2. (Mirsky, 1971) *Let $(P, \preceq)$ be a poset. If the longest chain in P has length m, then P can be partitioned into m antichains.*

Proof: We proceed by induction on m. If $m = 1$ then P itself is an antichain, since '$\preceq$' is just '$=$'. Suppose, for some $m \geq 2$, that if the longest chain in P has length $m-1$, then P can be partitioned into $m-1$ antichains.

Consider a poset P in which the maximum length of a chain is m. Let T be the set of maximal elements of P. By Proposition 3.1, $T \neq \emptyset$ and, by definition of maximal element, T is an antichain.

We claim that any longest chain in the poset $(P - T, \preceq)$ has length $m - 1$. Suppose not. Then the poset $(P - T, \preceq)$ has a chain of length m, say

$$x_1 \prec x_2 \prec \cdots \prec x_m.$$

Since this is also a chain of length m in P, we have $x_m \in T$, contradicting $x_m \in P - T$. Therefore, any longest chain in $P - T$ has length at most $m - 1$. But since P has a chain of length m, and T contains at most one element from each chain, $P - T$ has a chain of length $m - 1$.

By the induction hypothesis, $P - T$ can be partitioned into $m - 1$ antichains. Adding T to this collection give a partition of P into m antichains. □

Suppose P is a finite poset. Then Theorem 3.2 can be stated as: *The maximum length of a chain in P equals the minimum number of antichains into which P can be partitioned.* Compare this with Theorem 3.4 below.

Corollary 3.3. *Let $(P, \preceq)$ be a poset with at least $mn + 1$ elements. Then either P has a chain of length $m + 1$ or an antichain of size $n + 1$.*

Proof: Suppose P has neither a chain of length $m+1$ nor an antichain of size $n+1$. Then, the length of a longest chain in P is $k \leq m$, and by Theorem 3.2 P can be partitioned into k antichains. By assumption each antichain has size at most n, so $|P| \leq kn \leq mn < mn+1$, a contradiction. □

As an example of Corollary 3.3, we prove a result of Erdös and Szekeres from 1935: *In any sequence of $mn+1$ distinct integers, there is either an increasing subsequence of length $m+1$ or a decreasing subsequence of length $n+1$.* Suppose the sequence is $x_1, x_2, \ldots, x_{mn+1}$. The relation $\preceq$ on the set $\{x_1, x_2, \ldots, x_{mn+1}\}$ defined by $x_i \preceq x_j$ if and only if $i \leq j$ and $x_i \leq x_j$ is a partial order (check this). By Corollary 3.3, there is either a chain of length $m+1$, or an antichain of size $n+1$. These two possibilities correspond to an increasing subsequence of length $m+1$ or a decreasing subsequence of length $n+1$, respectively.

Theorem 3.2 can be viewed as a "dual" of an earlier (and more important) theorem.

Theorem 3.4. (Dilworth's Theorem, 1950) *Let $(P, \preceq)$ be a finite poset. Then, the minimum number of chains into which P can be partitioned equals the maximum size of an antichain in P.*

Proof: Suppose P can be partitioned into m chains. Then, since an antichain can contain at most one element from each of these chains, the size of a largest antichain is at most m.

We use induction on $n = |P|$ to prove the converse implication that if the largest size of an antichain is M, then P can be partitioned into M chains. The statement is true if $n = 0$, as there is nothing to prove. Suppose it is true for all posets with at most $n-1$ elements, for some $n \geq 1$. Let $(P, \preceq)$ be a poset with n elements.

Let C be a longest chain in P, and consider the poset $(P - C, \preceq)$. Since C is a chain, a largest antichain in $P - C$ must have size at least $M - 1$. Since every antichain in $P - C$ is an antichain in P, a largest antichain in $P - C$ has size at most M.

Suppose a largest antichain in $P - C$ has size $M - 1$. By the induction hypothesis, $P - C$ can be partitioned into $M - 1$ chains. Thus, C together with a partition of $P - C$ into $M - 1$ chains constitutes a partition of P into M chains.

Now suppose that $P - C$ has an antichain $Y = \{y_1, y_2, \ldots, y_M\}$ of size M. Define

$$A = \{x \in P : y_i \preceq x \text{ for some } i\} \quad \text{and} \quad B = \{x \in P : x \preceq y_i \text{ for some } i\}.$$

(The letters A and B are meant to suggest Above and Below the antichain, in the sense of the Hasse diagram.) Note that both $Y \subseteq A$ and $Y \subseteq B$. Since Y is a largest antichain, $A \cup B = P$ (if some element $y \in P - Y$ is incomparable with every element of Y, then $Y \cup \{y\}$ is a larger antichain).

We claim that A and B are proper subsets of P (this will allow the induction hypothesis to be applied to the posets $(A, \preceq)$ and $(B, \preceq)$). We show that $B \neq P$. Since C is a finite chain, it has a greatest element g. Suppose $g \in B$. Then $g \preceq y$ for some $y \in Y$. Since $Y \subseteq P - C,\ g \neq y$. Thus, in P, the set $C \cup \{y\}$ is a longer chain than C, a contradiction. Similarly, $A \neq P$.

Since each element $y_i \in B$, the poset $(B, \preceq)$ has an antichain of size M. By the induction hypothesis, B can be partitioned into M chains $B_1, B_2, \ldots, B_M$, where $y_i \in B_i,\ 1 \leq i \leq M$.

We claim that y_i is the greatest element of B_i. Suppose not. Then there exists $x \in B_i$ such that $y_i \prec x$. Since $x \in B$, we have $x \preceq y_j$ for some j. By transitivity this implies $y_i \prec y_j$, contrary to $\{y_1, y_2, \ldots, y_M\}$ being an antichain. This proves the claim.

Similarly, A can be partitioned into M chains $A_1, A_2, \ldots, A_m$ with y_i being the least element in $A_i,\ 1 \leq i \leq M$.

It follows from the results above that for $i = 1, 2, \ldots, M$ the set $A_i \cup B_i$ is a chain in P. Hence $A_1 \cup B_1, A_2 \cup B_2, \ldots, A_M \cup B_M$ is a partition of P into M chains. □

It turns out that Dilworth's Theorem is equivalent to Hall's Theorem, and therefore also to König's Theorem (in the sense that the truth of any one of them implies the truth of the others). There are other theorems in discrete mathematics that are also equivalent to these three. They include the Max-Flow Min-Cut Theorem (graph theory: network flows), and Menger's Theorem (graph theory: connectivity).

We show here that Dilworth's Theorem implies Hall's Theorem. Let $A_1, A_2, \ldots, A_n$ be a collection of subsets of $X = \{x_1, x_2, \ldots, x_m\}$ that satisfy Hall's condition:

$$\left| \bigcup_{i \in I} A_i \right| \geq |I| \text{ for all } I \subseteq \{1, 2, \ldots, n\}.$$

Let $P = \{x_1, x_2, \ldots, x_m, A_1, A_2, \ldots, A_n\}$, where the symbols $A_1, A_2, \ldots, A_n$ are considered to be distinct even if the corresponding sets are identical. Define a relation $\preceq$ on P by $a \preceq C$ if and only if $a = C$, or $a \in X,\ C \in Y = \{A_1, A_2, \ldots, A_n\}$ and $a \in C$. Then $\preceq$ is a partial order (check this).

We claim that a largest antichain in P has size m. Consider an antichain consisting of $p \geq 0$ elements $y_1, y_2, \ldots, y_p \in X$ and $q \geq 0$ elements $B_1, B_2, \ldots, B_q \in Y$. Then none of the elements $y_1, y_2, \ldots, y_p$ can belong to the union $\bigcup_{i=1}^{q} B_i$, so that $|\bigcup_{i=1}^{q} B_i| \leq m - p$.

Using Hall's condition, this implies $q \leq m - p$, or $p + q \leq m$. Thus no antichain in P has size greater than m. The set X is an antichain of size m, which proves the claim.

By Dilworth's Theorem, the set P can be partitioned into m chains. Some n of these must have length two and involve elements $x \in X$ and $y \in Y$ such that $x \in y$. These n elements of X form a SDR of $A_1, A_2, \ldots, A_n$.

Since Hall's condition is easily seen to be necessary for the existence of a SDR, the proof is complete.

We complete this chapter by considering some properties of antichains in the poset of subsets of X ordered by containment.

Theorem 3.5. (Sperner's Theorem) *Let X be an n-set. If $A_1, A_2, \ldots, A_m$ are subsets of X such that A_i is not a subset of A_j when $i \neq j$, then $m \leq \binom{n}{\lfloor n/2 \rfloor}$.*

Proof: Some helpful notation is to use $\binom{X}{t}$ for the set of all t-subsets of X. These are antichains for each t.

By Dilworth's Theorem, to show the largest antichain in $(\mathcal{P}(X), \subseteq)$ has size $M = \binom{n}{\lfloor n/2 \rfloor}$, it suffices to construct a partition of $(\mathcal{P}(X), \subseteq)$ into chains $C_1, \ldots, C_M$. Initially, set these chains to be empty. Place each element of $\binom{X}{\lfloor n/2 \rfloor}$ into distinct chains, so that now each chain has a single set in it.

Suppose for induction that all sets of size between t and u have been covered by chains $C_1, \ldots, C_M$. We may assume $t \leq \lfloor n/2 \rfloor \leq u$.

Consider the sets in $\binom{X}{t-1}$. For each such set Z, define a set $\text{Ext}(Z) = \{Y \in \binom{X}{t} : Y \supset X\}$. This is the set of all extensions of Z to a t-set. We have $|\text{Ext}(Z)| = n - t + 1$, since there are this many choices for an element of $X - Z$. Moreover, any $Y \in \binom{X}{t}$ belongs to exactly t such sets, since there are t possible elements in Y to delete. Since $n - t + 1 \geq t$, we have by Exercise 2.11 an SDR of the sets $\text{Ext}(Z)$, $Z \in \binom{X}{t-1}$. If Y represents Z, place Z in the same chain as Y. This extends the chains to cover all sets in $\binom{X}{t-1}$.

Similarly, we may extend the chains to cover all sets in $\binom{X}{u+1}$. By induction, we construct $C_1, \ldots, C_M$ covering all of $\mathcal{P}(X)$. □

Corollary 3.6. *Let $X = \{1, 2, \ldots, n\}$, where n is even. Then $(\mathcal{P}(X), \subseteq)$ has exactly one antichain of maximum size: $\binom{X}{\lfloor n/2 \rfloor}$.*

Proof: Exercise. □

In fact, when n is odd there are only two possible antichains, as expected. Details of the proof are omitted.

Theorem 3.7. *Let $X = \{1, 2, \ldots, n\}$, where n is odd. Then $(\mathcal{P}(X), \subseteq)$ has exactly two antichains of maximum size: $\binom{X}{\lfloor n/2 \rfloor}$ and $\binom{X}{\lceil n/2 \rceil}$.*

Exercises

1. Prove that each of the following is a partial order:

   (a) the relation 'divides' on the set of positive integers.

   (b) the relation $\subseteq$ on the power set of a set X.

2. Let $P = \{1, \ldots, n\}$, and consider the poset $(P, |)$, where as usual $x \mid y$ if and only if $kx = y$ for some integer k.

   (a) What is the length of a longest chain in $(P, |)$?

   (b) Describe a partition of this poset into the same number of antichains.

3. Let $P = (V, \preceq)$ be a poset. The *digraph of P* has vertex set V and a directed arc from x to y whenever $x \preceq y$.

   (a) Show that the digraph of P has no directed cycles of length greater than one.

   (b) Show that if $\preceq$ is a total order, then the digraph of P has a vertex with an arc to all other vertices.

   (c) Use (b) to show that if C is a chain containing n elements then, the elements of C can be listed as $x_1 \prec x_2 \prec \cdots \prec x_n$.

4. Draw the Hasse diagram of

   (a) a finite poset with two different minimal elements.

   (b) an infinite poset with two different minimal elements.

5. Let $(P, \preceq)$ be a poset, and $Q \subseteq P$. Let $\preceq' = \preceq \cap (Q \times Q)$. Prove that $(Q, \preceq')$ is a poset. (We have been using $(Q, \preceq)$ to denote this poset.) Prove further that every chain in Q is a chain in P and every antichain in Q is an antichain in P.

6. Show that among a group of $pq + 1$ rats there is either a sequence of $p + 1$ rats each of which is a descendant of the next, or a collection of $q + 1$ rats none of which is a descendant of another.

7. (a) How many longest chains are there in $(\mathcal{P}(X), \subseteq)$?

   (b) Given any set $A \in \binom{X}{t}$, how many longest chains contain A?

8. Let $\mathcal{A}$ be an antichain in $(\mathcal{P}(X), \subseteq)$, and let α_t denote the number of elements of $\mathcal{A}$ of size t. Prove that

$$\sum_{t=0}^{n} \alpha_t \, t!(n-t)! \leq n! \quad \text{or, equivalently,} \qquad \sum_{k=0}^{n} \frac{\alpha_t}{\binom{n}{t}} \leq 1.$$

   (*Hint:* Use the exercise above.)

9. Let α_t be as in the previous exercise. Prove that if $\mathcal{A}$ is an antichain of size $\binom{n}{\lfloor n/2 \rfloor}$ in $(\mathcal{P}(X), \subseteq)$, then

   (a) every longest chain contains an element of $\mathcal{A}$, and

   (b) $\alpha_t = 0$ unless $t = \lceil n/2 \rceil$ or $t = \lfloor n/2 \rfloor$.

10. Prove Corollary 3.6.

11. Is it true that in an arbitrary finite poset, every longest chain contains an element of every largest antichain?

12. An international firm has 250 employees, each of whom speaks several languages. For each pair of employees (A, B), there is a language spoken by A and not by B, and there is another language spoken by B and not by A. Prove that at least 10 different languages must be spoken at the firm.

13. An *intersecting family* of sets is a collection of distinct sets, no two of which are disjoint. Prove that an intersecting family of subsets of $\{1, 2, \ldots, n\}$ has size at most 2^{n-1}, and describe an example to show that equality can hold.

14. Christi has 199 wooden boxes. In any collection of 13 boxes, there are two such that one fits completely inside the other. She wants to store her collection by putting a box inside another box, and then putting that box inside another, and so on, so that each larger box has exactly one smaller box (and its contents) placed inside it. Can she store all of her boxes inside 12 of the boxes in her collection?

Chapter 4

Finite geometries

A *projective plane* is an ordered pair $(\mathcal{P}, \mathcal{L})$, where $\mathcal{P}$ is a set of *points* and $\mathcal{L}$ is a set of *lines* satisfying the following five postulates:

P1. There exists at least one line.

P2. There are at least three points on every line.

P3. Not all points are on the same line.

P4. There is exactly one line on any two distinct points.

P5. There is exactly one point on any two distinct lines.

These postulates are given in terms of the primitive (undefined) terms "point" and "line". It is helpful to think of "on" as an incidence relation between points and lines (a subset of $\mathcal{P} \times \mathcal{L}$). We will sometimes denote by pq the unique line on the points p and q, whose existence is guaranteed by P4.

Perhaps surprisingly, these postulates can be satisfied for finite sets of points and lines. Two examples are given below.

Example 4.1. (The Fano plane) Here, the point set is $\mathcal{P} = \mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$ and the lines are the sets belonging to

$$\mathcal{L} = \{\{0, 1, 3\}, \{1, 2, 4\}, \{2, 3, 5\}, \{3, 4, 6\}, \{0, 4, 5\}, \{1, 5, 6\}, \{0, 2, 6\}\} .$$

Point p is on line L if and only if $p \in L$.

Example 4.2. Here, the point set is $\mathcal{P} = \mathbb{Z}_{13}$ and the line set is $\mathcal{L} = \{\{0, 1, 3, 9\} + x : x \in \mathbb{Z}_{13}\}$, where we interpret the translate $S + x = \{s + x : s \in S\}$, and addition is performed mod 13. Point p is on line L if and only if $p \in L$.

Proposition 4.3. *The following statements hold for any projective plane* $(\mathcal{P}, \mathcal{L})$*:*

P1′. *There exists at least one point.*

P2′. *There are at least three lines on every point.*

P3′. *Not all lines are on the same point.*

Proof: We prove P1′ and P3′, and leave P2′ as an exercise. Note that by P1, $\mathcal{L} \neq \emptyset$.

To prove P1′, note that by P2 there are at least three points on any line L. Therefore, there exists at least one point.

To prove P3′, let p be a point (the existence of p is guaranteed by what we have just proved). We must show there exists a line not on p. Let L be a line. If L is not on p, the desired line has been found. Suppose, then, that L is on p. By P2 there is a point $q \neq p$ on L, and by P3 there is a point r not on L. By P4 there is exactly one line H on the points q and r. Since q is on both L and H, P5 guarantees that H is not on p. □

For any proposition concerning projective planes that contains only the terms “point”, “line”, and “on”, we can form a second proposition called its *dual* by interchanging the words “point” and “line” wherever they occur. Note that P1′, P2′ and P3′ are duals of P1, P2, and P3, respectively. Since postulates P4 and P5 are duals of each other, any proof using P1 through P5 can be “dualized”.

Principle of duality for projective planes. *If a proposition can be derived from postulates P1 through P5, then its dual can also be derived from these postulates.*

A *finite projective plane* is a projective plane $(\mathcal{P}, \mathcal{L})$ in which the set $\mathcal{P}$ of points is finite. Since two lines are the same if they are on exactly the same points, this implies that the set $\mathcal{L}$ of lines is also finite.

Proposition 4.4. *Let* $(\mathcal{P}, \mathcal{L})$ *be a finite projective plane. Then, there is an integer* $n \geq 2$ *such that:*

- *There are* $n + 1$ *lines on each point and* $n + 1$ *points on each line.*

- *There are $n^2 + n + 1$ points and $n^2 + n + 1$ lines.*

Proof: Since $\mathcal{P}$ is finite, each line contains a finite number of points. Let L be a line, and suppose there are $n + 1$ points on L. By P2, $n + 1 \geq 3$, so that $n \geq 2$.

Let p be a point not on L. By P5, for any line H on p there is exactly one point on both H and L and, by P4, no two of these points are the same. Thus, there are at most $n + 1$ lines on p. On the other hand, for each point q on L, P4 asserts that there is a line on p and q. By P5, no two of these lines are the same. Thus, there are exactly $n + 1$ lines on any point p not on L.

Fix a point p not on L and let H be a line not on p (H exists by P3$'$). For each line K on p there is a unique point on both K and H, and no two such points are the same. Since there are $n + 1$ lines on p, there are at least $n + 1$ points on H. On the other hand, for every point q on H there is a line on p and q, and no two such lines are the same, so there are at most $n + 1$ points on H. Therefore, any line not on p is on exactly $n + 1$ points.

We now show that any line on p is also on $n + 1$ points. Let K be a line on p. By P5 there is a point ℓ on both K and L, and by P2 there is a point m on L and not on K. Similarly, there is a point j, different from p and m, on the line pm. Then, by P4, j is not on L so that there are exactly $n + 1$ lines on j. By a similar argument as in the previous paragraph, there are exactly $n + 1$ points on K.

We now show that any point on L is on $n + 1$ lines. Let r be on L, and let $K \neq rp$ be a line on p (the line K exists because $n + 1 \geq 3$). For each line R on r there is a unique point on both R and K, and no two such points are the same. Since K is on $n+1$ points, there are at most $n + 1$ lines on r. On the other hand, for each of the $n + 1$ points t on K, there is a line rt, so there are at least $n + 1$ lines on r. Thus, any point on L is on $n + 1$ lines.

This proves the first statement.

Now, fix any point p. There are $n + 1$ lines on p, each of which contains $n + 1$ points, including p. Since p is the only point on any two of these lines (and it is on every two of them), the number of points is $(n+1)n+1 = n^2+n+1$. To determine the number of lines, we count the pairs (p, L), where p is a point on the line L. On the one hand, there are n^2+n+1 choices for p, and for each of these there are $n+1$ choices for L, so the number of pairs is $(n+1)(n^2+n+1)$. On the other hand, for each choice of L there are $n+1$ choices for p, so the number of pairs is $(n + 1)|\mathcal{L}|$. Therefore, $(n + 1)(n^2 + n + 1) = (n + 1)|\mathcal{L}|$, or $|\mathcal{L}| = n^2 + n + 1$. □

A finite projective plane is said to have *order* n if it has $n+1$ points on each line and $n+1$ lines on each point. An important question that arises is: for which values of n does there exist a projective plane of order n? Later, we describe a construction (Theorem 4.8) that shows they exist whenever n is prime, or a power of a prime. No projective plane of order n, where n is neither a prime nor a power of a prime prime, is known to exist. On the other hand, there are very few tools for proving that such structures can not exist. The main theorem that can be used for proving non-existence of projective planes of certain orders is the following, which we state without proof.

Theorem 4.5. (Bruck-Ryser Theorem) *Suppose* $n \equiv 1$ *or* $2 \pmod 4$. *If there exists a projective plane of order* n, *then* n *can be written as a sum of two squares.*

To use the Bruck-Ryser Theorem to prove non-existence of certain projective planes, consider the contrapositive: For $n \equiv 1$ or $2 \pmod 4$, if n can not be expressed as a sum of two squares, then there is no projective plane of order n.

Example 4.6. Let $n = 30$. We have that $30 \equiv 2 \pmod 4$, and that 30 can not be expressed as a sum of two squares (either by subtracting each of $0^2, 1^2, \ldots, 5^2$ from 30 and noting that the result is not a square, or by appealing to Lemma 4.7 below). Thus, there is no projective plane of order 30.

A well-known theorem due to Lagrange (in the sense that gave the first published proof) characterises the integers that can be written as a sum of two squares. Euler, Fermat and Diophantus made all important contributions to finding the characterisation, so it is a bit unfair to call it “Lagrange’s Theorem”. In any case, we state it without proof, too.

Lemma 4.7. *The positive integer* n *can be written as a sum of two squares if and only if the prime factorisation of* n *contains no prime congruent to 3 modulo 4 to an odd power.*

As examples of Lemma 4.7, consider 40 and 1575. The prime factorisation of 40 is $2^3 5$, which contains no prime congruent to 3 modulo 4 to an odd power. Thus, by the lemma, 40 is a sum of two squares. In fact, $40 = 2^2 + 6^2$. On the other hand, we have 1575 has prime factorisation $3^2 5^2 7$, in which the integer 7 is congruent to 3 modulo 4 and appears to an odd power. Thus, by the lemma, the integer 1575 is not a sum of two squares.

We now show how to construct projective planes of prime power order. The construction makes use of some tools from abstract algebra and linear algebra. If you unfamiliar with vector spaces and finite fields, try to visualise the construction taking place in $\mathbb{R}^3$. Everything is pretty much the same, except that the resulting projective plane is not finite.

Theorem 4.8. *Let $n > 1$ be a prime power. Then, there exists a projective plane of order n.*

Proof: From abstract algebra, since n is a prime power, there is a field $GF(n)$ with n elements. Let V be the set of all 3-tuples with elements from $GF(n)$. For $\alpha \in GF(n)$ and $(x_1, x_2, x_3) \in V$, define $\alpha(x_1, x_2, x_3) = (\alpha x_1, \alpha x_2, \alpha x_3)$. From linear algebra we know that V, together with this *scalar multiplication* and componentwise addition of 3-tuples (also called *vectors*), is a 3-dimensional vector space.

For convenience, write $V^* = V - \{(0, 0, 0)\}$

The point set $\mathcal{P}$ of our projective plane is the set of 1-dimensional subspaces of V. That is,

$$\mathcal{P} = \{P_{\mathbf{v}} : \mathbf{v} \in V^*\},$$

where

$$P_{\mathbf{v}} = \{\alpha\mathbf{v} : \alpha \in GF(n)\}.$$

These are lines through the origin in V.

The line set $\mathcal{L}$ of our projective plane is the set of all 2-dimensional subspaces of V. That is

$$\mathcal{L} = \{L_{\mathbf{u},\mathbf{v}} : \mathbf{u}, \mathbf{v} \in V^* \text{ with } \mathbf{u} \notin P_{\mathbf{v}}\},$$

where

$$L_{\mathbf{u},\mathbf{v}} = \{\alpha\,\mathbf{u} + \beta\,\mathbf{v} : \alpha, \beta \in GF(n)\}.$$

These are planes through the origin in V. (The last condition in the definition of $\mathcal{L}$ says that $\mathbf{u}$ and $\mathbf{v}$ are linearly independent vectors.) The phrase "point P is on line L" means that $P \subseteq L$.

We now sketch an argument that postulates P1 through P5 hold.

Postulate P1 holds because there is a plane through the origin in V – for example the one determined by the set of all triples with third component equal to 0.

To see that P2 holds, notice that a plane through the origin, say $L_{\mathbf{u},\mathbf{v}}$ contains the distinct lines through the origin $P_{\mathbf{u}}$, $P_{\mathbf{v}}$, and $P_{\mathbf{u}+\mathbf{v}}$.

Postulate P3 holds since a plane through the origin is a 2-dimensional subspace and therefore does not contain every non-zero vector in V.

Since two distinct lines through the origin determine a unique plane through the origin, P4 holds.

P5 holds since the intersection of two distinct planes through the origin is a line through the origin.

Finally, we must justify the claim that the projective plane has order n. Let $L_{\mathbf{u},\mathbf{v}} \in \mathcal{L}$. Each choice for α and β, not both zero, gives a non-zero vector $\alpha\mathbf{u} + \beta\mathbf{v}$ in the plane L, and the set of all scalar multiples of any such vector is a line through the origin in $L_{\mathbf{u},\mathbf{v}}$. There are $n^2 - 1$ choices for α and β, not both zero. For each non-zero vector $\mathbf{z}$ in $L_{\mathbf{u},\mathbf{v}}$, all $n - 1$ non-zero scalar multiples of $\mathbf{z}$ are on the same one-dimensional subspace. Thus, each one-dimensional subspace is counted $n - 1$ times, and hence each plane through the origin in V contains $(n^2 - 1)/(n - 1) = n + 1$, lines through the origin. Hence each line of the projective plane is on $n + 1$ points. □

Illustration of the construction. Let $n = 2$. Then $GF(2) = \{0, 1\}$ and we can write V as $V = \{000, 100, 010, 001, 110, 101, 011, 111\}$. Imagine V on the cube Q_3. The 1-dimensional subspaces through the origin (000) in V are identifiable with the 7 nonzero points in V. So let's say $\mathcal{P} = V - \{000\}$. The line set $\mathcal{L}$ corresponds to seven planes through 000:

$\{100, 010, 110\}$ (front face)

$\{100, 001, 101\}$ (left face)

$\{010, 001, 011\}$ (bottom face)

$\{110, 001, 111\}$ (diag. to front face)

$\{101, 010, 111\}$ (diag. to left face)

$\{011, 100, 111\}$ (diag. to bottom face)

$\{110, 101, 011\}$ (diag. to all faces)

There is a renaming of the nonzero triples over $GF(2)$ to $\{1, \ldots, 7\}$ which recovers exactly the points and lines of our first example in this section.

More formally, two projective planes $(\mathcal{P}_1, \mathcal{L}_1)$ and $(\mathcal{P}_2, \mathcal{L}_2)$ are *isomorphic* (the same up to renaming the points) if there is a 1-1 and onto correspondence $\phi : \mathcal{P}_1 \to \mathcal{P}_2$ such that:

- $\phi(L_1) \in \mathcal{L}_2$ for each line $L_1 \in \mathcal{L}_1$

(where lines are regarded as the set of points they are "on"). Not all projective planes of the same order are isomorphic. It is known that there are exactly four non-isomorphic (different) projective planes of order nine.

Theorem 4.8 gives the existence of projective planes of order 2, 3, 4, 5, 7, 8, 9, and 11. By the Bruck-Ryser Theorem, there is no projective plane of order 6. The Bruck-Ryser Theorem does not rule out the existence of a projective plane of order 10. However, it is known that no such plane exists. This was the conclusion from a massive computer search by Lam, Thiel, Swiercz and McKay (all from Concordia University) – the final part of the computation ran as a low priority job on a Cray supercomputer for over two years. It is presently unknown whether there is a projective plane of order 12. This is the smallest undecided case.

An *affine plane* is an ordered pair $(\mathcal{P}, \mathcal{L})$, where $\mathcal{P}$ is a set of *points* and $\mathcal{L}$ is a set of *lines* satisfying the following five postulates:

A1. There exists at least one line.

A2. There are at least two points on every line.

A3. Not all points are on the same line.

A4. There is exactly one line on any two distinct points.

A5. Given a line L and a point p not on L, there is exactly one line on p and not on any point of L.

The classical example of an affine plane is given by $\mathbb{R}^2$, the ordinary Euclidean plane. (Think about the meaning of A5 for $\mathbb{R}^2$.)

A *finite affine plane* is an affine plane in which the point set $\mathcal{P}$ is finite. (Since lines are on points, and two lines are the same if they are on the same collection of points, this implies that $\mathcal{L}$ is also finite.) Here are two examples of finite affine planes:

Example 4.9. The point set is $\mathcal{P} = \{1, 2, 3, 4\}$ the line set $\mathcal{L}$ is the set of all 2-subsets of $\mathcal{P}$, and point p is on line L if and only if $p \in L$.

Example 4.10. The point set is $\mathcal{P} = \{1, 2, \ldots, 9\}$ and the line set is

$$\mathcal{L} = \big\{\{1,2,3\}, \{4,5,6\}, \{7,8,9\}, \{1,4,7\}, \{2,5,8\}, \{3,6,9\},$$

$$\{1,5,9\}, \{2,6,7\}, \{3,4,8\}, \{3,5,7\}, \{2,4,9\}, \{1,6,8\}\big\},$$

and point p is on line L if and only if $p \in L$. The lines can be regarded as the set of all rows, columns and diagonals of the matrix

$$M = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{bmatrix}.$$

A similar result as Proposition 4.4 holds for affine planes. It may be derived from postulates A1 through A5. We leave the proof as an exercise.

Proposition 4.11. *Let $(\mathcal{P}, \mathcal{L})$ be a finite affine plane. Then, there is an integer $n \geq 2$ such that:*

- *There are n points on each line and $n+1$ lines on each point.*
- *There are n^2 points and $n(n+1)$ lines.*

A finite affine plane is said to have *order n* if it has n points on each line (and $n+1$ lines on each point).

As mentioned earlier, A5 is often called the *parallel postulate*. We define two lines in an affine plane to be *parallel* if they are either identical, or are on disjoint sets of points.

Let $(\mathcal{P}, \mathcal{L})$ be an affine plane. Define a relation $\|$ on $\mathcal{L}$ by $L_1 \| L_2$ if and only if L_1 and L_2 are parallel. Then $\|$ is an equivalence relation. (The proof of this fact is an exercise.) We denote by $[L]$ the equivalence class of L – the set of lines consisting of L and all lines parallel to L – and call $[L]$ the *parallel class* of L.

Proposition 4.12. *For each line $L \in \mathcal{L}$ in an affine plane of order n, the parallel class $[L]$ has exactly n members.*

Proof: We claim first that each parallel class contains exactly one line on any point. To see this, let $[L]$ be a parallel class and p be a point not on L (any point on L is on a line in $[L]$). By postulate A5, there is a line H on p parallel to L. Since $\|$ is an equivalence relation, lines parallel to the same line are parallel to each other. Thus, $H \in [L]$. This proves the claim.

By Theorem 4.11, there are n^2 points and each line contains n points. Since $[L]$ contains a line on every point and no two lines in L are on the same point, $[L]$ must contain exactly n lines. □

The question of which values of n there exists an affine plane of order n is closely related to the same problem for projective planes.

Theorem 4.13. *There exists a projective plane of order n if and only if there exists an affine plane of order n.*

Proof: ($\Rightarrow$) Suppose that $\Pi = (\mathcal{P}, \mathcal{L})$ is a projective plane of order n, and regard each line as the set of points that it is on. The main idea is that the result of deleting any line and all of its points from Π leaves an affine plane. Let $L \in \mathcal{L}$. Our affine plane will have for its point set $\mathcal{Q}$ the set $\mathcal{P} - L$ of points not on L, and for its line set $\mathcal{K}$ the set $\big\{H - L : H \in \mathcal{L} - \{L\}\big\}$ of lines in $\mathcal{L}$ with the point in common with L deleted. We must show that A1 through A5 hold for $(\mathcal{Q}, \mathcal{K})$.

By P2$'$ (Proposition 3.1) $|\mathcal{L}| \geq 3$. Thus, $|\mathcal{K}| \geq 2$, so A1 holds.

Let $H \in \mathcal{L} - \{L\}$ be a line of Π. Since L is on at least three points (by P2), and there is exactly one point on both H and L (by P5), there are at least two points on $H - L$. Hence, A2 holds.

Let $H - L \in \mathcal{K}$. By exercise 14, there is a point p of Π on neither H nor L. Thus, $p \in \mathcal{Q}$ and is not on $H - L$, so that A3 holds.

Let p and q be distinct points in $\mathcal{Q}$. Then, $p, q \in \mathcal{P}$ so, by P4, there is exactly on line K one these two points. Since no point of L belongs to $\mathcal{Q}$, $K \neq L$. Thus $K - L \in \mathcal{K}$, so there is a line in $\mathcal{K}$ on p and q. Each line in $\mathcal{K}$ arises from a line in $\mathcal{L}$, so $K - L$ is the only line in $\mathcal{K}$ on these two points. Thus, A4 holds.

Let $K - L \in \mathcal{K}$ (so that $K \in \mathcal{L}$) and let $p \in \mathcal{Q}$ be a point not on K. Let q be the point on both K and L in Π. By P4 there is a unique line $J \in \mathcal{L}$ on p and q. Since p is not on L, $J \neq L$. Thus, $J - L = J - \{q\}$ is a line in $\mathcal{K}$ that is on p but not on any point of K. Suppose $H - L \in \mathcal{K}$ is a line on p but not on any point of $K - L$. Then, since there is a point on H and K in Π but no point on $H - L$ and $K - L$, we must have that q is the point on H and K in Π. Hence H and J are both lines in Π that are on the points p and q, so $H = J$. Consequently, $H - L = J - L$ and A5 holds.

Therefore, $(\mathcal{Q}, \mathcal{K})$ is an affine plane. Since each line in $\mathcal{K}$ contains $(n+1) - 1 = n$ points, it has order n.

($\Leftarrow$) Let $\Omega = (\mathcal{Q}, \mathcal{K})$ be an affine plane of order n, and regard each line as the set of points it is on. The main idea is to add a new line consisting of one new point for each parallel class, and extend each of the lines to contain the new point corresponding to its parallel class.

Since $\|$ is an equivalence relation, the parallel classes partition $\mathcal{K}$. By exercise 3(b), there are $n+1$ parallel classes. For each parallel class $[K]$, $K \in \mathcal{K}$, let $p_{[K]}$ be a new point (*i.e.* one that is not in $\mathcal{Q}$), and define $L_\infty = \{p_{[K]} : K \in \mathcal{K}\}$. Our projective plane will have point set

$$\mathcal{P} = \mathcal{Q} \cup L_\infty$$

and line set

$$\mathcal{L} = \big\{K \cup \{p_{[K]}\} : K \in \mathcal{K}\big\} \cup \{L_\infty\}.$$

We must show that P1 through P5 hold for $\Pi = (\mathcal{P}, \mathcal{L})$.

By A1, there is at least one line in Ω. Thus, there is at least one line in Π, and P1 holds.

To see that P2 holds, note first that L_∞ contains $n+1 \geq 3$ points. Secondly, since each line in $\mathcal{K}$ is on n points, by construction every other in $\mathcal{L} - \{\mathcal{L}_\infty\}$ also contains $n+1$ points.

Since $\mathcal{Q} \neq \emptyset$, there is a point not on L_∞. For any line in $H \in \mathcal{L} - \{L_\infty\}$ there is exactly one point on both H and L_∞ (by construction). Since L_∞ is on at least three points, there is a point not on H. Thus, P3 holds.

Let p and q be points in $\mathcal{P}$. Suppose first that $p, q \in \mathcal{Q}$. Then, by A4 there is a line $K \in \mathcal{K}$ on p and q. By construction, the line $K \cup \{p_{[K]}\}$ of Π is on p and q. Since L_∞ is not on p and q, and every other line of Π arises from adding a new point to a line of Ω, $K \cup \{p_{[K]}\}$ is the only line of Π on p and q. Next, suppose that neither p nor q is in $\mathcal{Q}$. Then p and q are on L_∞, and no line $K \cup \{p_{[K]}\}$, $K \in \mathcal{K}$, is on both of these points. Finally, suppose $p \in \mathcal{Q}$ and $q \notin \mathcal{Q}$ (the argument is similar if $q \in \mathcal{Q}$ and $p \notin \mathcal{Q}$). Then, $q \in L_\infty$ so that $q = p_{[K]}$ for some parallel class $[K]$ of Ω. Since $[K]$ contains a line on every point, there exists $H \in [K]$ such that p is on H. Thus, the line $H \cup \{q\}$ of Π is on p and q. The only lines of Π on q are L_∞ and those in $\{J \cup \{q\} : J \in [K]\}$, and only one of these is on p. Thus, in this case (too) there is a unique line on p and q. Therefore, P4 holds.

Finally, we show P5 holds. By construction, if $K \cup \{p_{[K]}\} \in \mathcal{L} - \{L_\infty\}$, then there is a unique point on both $K \cup \{p_{[K]}\}$ and L_∞. If J and K are different lines that belong to the same parallel class in Ω, then $p_{[K]}$ is the unique point on Π on $J \cup \{p_{[K]}\}$ and $K \cup \{p_{[K]}\}$. (Recall that $[J] = [K]$.) If J and K are lines that belong to different parallel classes in Ω, then by A4 and the definition of parallel, there is a unique point $q \in \mathcal{Q}$ on both of these lines. Further, $p_{[J]} \neq p_{[K]}$, so q is the only point of Π on $J \cup \{p_{[J]}\}$ and $K \cup \{p_{[K]}\}$. Hence, P5 holds.

Therefore $(\mathcal{P}, \mathcal{L})$ is a projective plane. Since, by construction, there are $n+1$ points on each line, it has order n. □

Isomorphism of affine planes is defined exactly the same way as isomorphism of projective planes.

Exercises

1. Prove statement P2′ of Proposition 4.3.

2. A dinner club has 16 members. Club nights are held five times per year. On each club night, some four members each host three other club members for dinner. Show that it is possible to schedule who dines together on these nights so that each pair of club members dines together exactly once each year. Is it possible to create such a schedule so that each member also hosts at least one dinner per year?

3. Prove that if $n \equiv 3 \pmod 4$, then n can not be written as a sum of two squares.

   (*Hint*: If $p \equiv 3 \pmod 4$, then determine $p^k \pmod 4$ for $k = 1, 2, \ldots$.)

4. Describe an infinite sequence $n_1, n_2, \ldots$ of distinct positive integers such that there is no projective plane of order n_i for any $i \geq 1$.

5. The *dual* of a projective plane $(\mathcal{P}, \mathcal{L})$ is the ordered pair $(\mathcal{P}', \mathcal{L}')$, where $\mathcal{P}' = \mathcal{L}$ and $\mathcal{L}' = \mathcal{P}$.

   (a) Show that the dual of a projective plane is also a projective plane.

   (b) Show that the Fano plane is isomorphic to its dual.

6. Let $\Pi = (\mathcal{P}, \mathcal{L})$ be a collection of points and lines that satisfies P2 and P4. If there are exactly $k+1$ points on every line and $k^2 + k + 1$ lines in all, must Π be a projective plane?

7. Show that the three postulates P1, P2, and P3 can be replaced by the single postulate Q: *there exists a set of four points, no three collinear* (on the same line).

8. Show that the following set of three self-dual postulates is equivalent to P1 through P5:

- Q1. There is exactly one line on any two distinct points and exactly one point on any two distinct lines.
- Q2. There exist two points and two lines such that each of the points is on exactly one of the lines and each of the lines is on exactly one of the points.
- Q3. There exist two points and two lines, the points not on the lines, such that the point on the two lines is on the line on the two points.

9. Prove that, given two lines H and L of a projective plane $(\mathcal{P}, \mathcal{L})$, there exists a point in $\mathcal{P}$ which is on neither H nor L.

10. Let $\Pi = (\mathcal{P}, \mathcal{L})$ be a projective plane of order n. A *subplane* $\Pi' = (\mathcal{P}', \mathcal{L}')$ of Π is a projective plane with $\mathcal{P}' \subseteq \mathcal{P}$, $\mathcal{L}' \subseteq \mathcal{L}$, and $x \in \mathcal{P}'$ is on $L \in \mathcal{L}'$ in Π' if and only if x is on L in Π. Prove that if Π' has order m, and $m < n$, then $m^2 \leq n$. (*Hint*: Consider a point $y \in \mathcal{P} - \mathcal{P}'$ which is on some line $L \in \mathcal{L}'$.)

11. (a) Show that the affine plane of order 2 is unique, up to isomorphism. (*Hint*: what are the lines?)

    (b) Use the construction in Theorem 4.13 and part (a) above to show that the Fano plane is the unique projective plane of order 2, up to isomorphism.

    (c) Explicitly find an isomorphism from the projective plane in the illustration following Theorem 4.8 to that given in Example 4.1

12. Show that the affine plane of order 3 in Example 4.10 is unique up to isomorphism. (*Hint*: argue that, by renaming points if necessary, the rows and columns of the matrix M in that example are two parallel classes in any such plane.)

13. Prove Theorem 4.11.

14. Let $(\mathcal{Q}, \mathcal{K})$ be a affine plane. Prove that $\|$ is an equivalence relation on $\mathcal{K}$.

15. Show that an affine plane of order n has exactly $n + 1$ parallel classes.

Chapter 5

Latin squares

We begin with *Euler's 36 Officers Problem*:

> Is it possible for thirty-six officers, of six different ranks and from six different regiments, to march in a 6×6 array so that in any line every rank and regiment occurs exactly once?

Notes:

- Each of the 36 pairs (rank, regiment) belongs to exactly one officer.
- Recall that a *line* of an array is a row or column of the array.

For any $n \geq 2$, the question can be asked for n^2 officers. It turns out that the "n^2 officers problem" has a solution if and only if $n \neq 2, 6$.

If the ranks and regiments are each numbered $1, 2, 3$, then the array below gives a solution to the 9-officers problem:

$$\begin{bmatrix} (1,1) & (2,2) & (3,3) \\ (2,3) & (3,1) & (1,2) \\ (3,2) & (1,3) & (2,1) \end{bmatrix}.$$

Notice that, in each line of the array, each rank occurs exactly once and similarly for each regiment.

A *Latin square* of *order* n is an $n \times n$ array with elements taken from an n element set $X = \{x_1, x_2, \ldots, x_n\}$, such that every element of X occurs exactly once in each row and each column.

Notes:

- We assume throughout this section that $X = \{1, 2, \ldots, n\}$.
- Each row and each column of a Latin square is a permutation of X.
- The name "Latin square" originates with Euler, who use Latin letters for the entries of the array.
- For any $n \geq 2$, the addition table for $\mathbb{Z}_n$ is a Latin square.
- The "multiplication table" for any group is a Latin square. (The converse is false.)
- In general, a Latin square is the multiplication table for an algebraic structure called a *quasigroup*. (We will not pursue these.)

The n^2 officers problem asks for two Latin squares of order n such that the n^2 pairs of (i, j)-entries comprise all n^2 pairs (rank, regiment). This implies that each such pair occurs exactly once. We will consider the problem of finding such pairs of Latin squares later.

Latin squares arise in the context of schedules and designs. Suppose, for example, that a badminton club consists of eight (mixed-gender) couples, and meets once per week to play mixed doubles. They desire a schedule such that, over the course of eight weeks, every possible combination of partners occurs. To construct such a schedule, let the females be $f_1, f_2, \ldots, f_8$, and the males be $m_1, m_2, \ldots, m_8$. Let L be a Latin square of order 8, say

$$L = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 7 & 8 & 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 6 & 7 & 8 & 1 & 2 \\ 5 & 6 & 7 & 8 & 1 & 2 & 3 & 4 \\ 7 & 8 & 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 5 & 6 & 7 & 8 & 1 \\ 4 & 5 & 6 & 7 & 8 & 1 & 2 & 3 \\ 8 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{bmatrix}.$$

The (i, j)-entry of L is the week on which female f_i is partnered with male m_j. Since L is a Latin square, there are eight pairs on each week, and every possible combination of mixed-gender partners occurs on some week.

We now estimate a count for the number of Latin squares. In this counting, two Latin squares L_1 and L_2 will be considered to be different if there exists a pair (i,j) such that the (i,j)-entry of L_1 is different from the (i,j)-entry of L_2. Our approach will make use of our previous work on SDRs and the idea of a Latin rectangle, defined below. The main idea is to build the squares one row at a time, and estimate the number of ways each new row can be added.

A $k \times n$ *Latin rectangle* is an $k \times n$ array $(1 \leq k \leq n)$ such that every element of $\{1,2,\ldots,n\}$ occurs exactly once in each row and at most once in each column.

A 3×5 Latin rectangle is shown below.

$$\begin{bmatrix} 2 & 5 & 4 & 3 & 1 \\ 3 & 1 & 2 & 5 & 4 \\ 5 & 2 & 1 & 4 & 3 \end{bmatrix}$$

Notes:

- Each row of a Latin rectangle is a permutation of $\{1,2,\ldots,n\}$.
- Each column of a Latin rectangle is a k-permutation of $\{1,2,\ldots,n\}$.
- A Latin square is an $n \times n$ Latin rectangle.
- A $1 \times n$ Latin rectangle is a permutation of $\{1,2,\ldots,n\}$. Thus, the number of $1 \times n$ Latin rectangles is $n!$.

Proposition 5.1. *Let R be a $k \times n$ Latin rectangle with $k < n$. There are at least $(n-k)!$ ways to add a row to R so that the result is a $(k+1) \times n$ Latin rectangle.*

Proof: For $i = 1,2,\ldots,n$, let A_i be the set of elements that do not appear in the i-th column of R. Then $|A_i| = n-k$. Further, since each of the first k rows of R is a permutation of $\{1,2,\ldots,n\}$, each element appears in some k columns of R. Therefore, each element of $\{1,2,\ldots,n\}$ belongs to exactly $n-k$ of the sets $A_1, A_2, \ldots, A_n$.

Every SDR of $A_1, A_2, \ldots, A_n$ gives rise to a row that can be used to extend R to a $(k+1)\times n$ Latin rectangle, and conversely. So the number of ways to extend R to a $(k+1) \times n$ Latin rectangle equals the number of SDRs of $A_1, A_2, \ldots, A_n$. By Corollary 2.6, this is at least $(n-k)!$. This completes the proof. □

Corollary 5.2. *For $1 \leq k \leq n$, the number of $k \times n$ Latin rectangles is at least*

$$n!(n-1)!\cdots(n-k+1)! = \prod_{i=1}^{k}(n-(i-1))!.$$

Proof: By induction on k. The number of $1 \times n$ Latin rectangles is $n!$. Suppose, for some $t \geq 1$, the the number of $t \times n$ Latin rectangles is at least $\prod_{i=1}^{t}(n-(i-1))!$. By Proposition 5.1, each $t \times n$ Latin rectangle can be extended to a $(t+1) \times n$ Latin rectangle in at least $(n-t)!$ ways. Further, any two $(t+1) \times n$ Latin rectangles that arise in this way differ either in the first t rows (if they arose from different $t \times n$ Latin rectangles), or in the $(t+1)$st row (if they arose from the same $t \times n$ Latin rectangle). Thus, by the induction hypothesis, the number of $(t+1) \times n$ Latin rectangles is at least $(n-t)! \cdot \Pi_{i=1}^{t}(n-(i-1))! = \Pi_{i=1}^{t+1}(n-(i-1))!$. The result now follows by induction. □

Corollary 5.3. *There are at least $\Pi_{k=1}^{n} k!$ Latin squares of order n.*

We now return to the "n^2 officers problem", and consider issues that arise from it.

Two Latin squares L and M of order n having entries from $\{1, 2, \ldots, n\}$ are called *orthogonal* if the n^2 ordered pairs (ℓ_{ij}, m_{ij}) of (i, j)-entries from L and M respectively are all different.

Notes:

- Only Latin squares of the same order can be orthogonal.
- The set of the n^2 ordered pairs (ℓ_{ij}, m_{ij}) of (i, j)-entries is $\{1, 2, \ldots, n\} \times \{1, 2, \ldots, n\}$.
- A solution to the n^2 officers problem corresponds to an pair of orthogonal Latin squares, one having the n ranks as entries, and the other having the n regiments as entries.
- There is no pair of orthogonal Latin squares of order 2.

A set of *mutually orthogonal Latin squares* (MOLS) is a set $\{L_1, L_2, \ldots, L_k\}$ of Latin squares, any two of which are orthogonal.

A set of three MOLS of order 5 is shown below.

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \\ 3 & 4 & 5 & 1 & 2 \\ 4 & 5 & 1 & 2 & 3 \\ 5 & 1 & 2 & 3 & 4 \end{bmatrix} \quad \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \\ 5 & 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 5 & 1 \\ 4 & 5 & 1 & 2 & 3 \end{bmatrix} \quad \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 3 & 4 \\ 4 & 5 & 1 & 2 & 3 \\ 3 & 4 & 5 & 1 & 2 \\ 2 & 3 & 4 & 5 & 1 \end{bmatrix}.$$

We now determine an upper bound on the maximum size of a set of pairwise orthogonal Latin squares. This will follow easily once we have made a few observations.

Lemma 5.4. *Let L be a Latin square. Let π be a permutation of $\{1, 2, \ldots, n\}$, and let L' be the array obtained from L by replacing each occurrence of i by $\pi(i)$, $1 \leq i \leq n$. Then L' is a Latin square.*

Proof: Exercise. □

Proposition 5.5. *Suppose L and M are orthogonal Latin squares. Let π be a permutation of $\{1, 2, \ldots, n\}$. If the Latin square L' is obtained from L by replacing each occurrence of i by $\pi(i)$, $1 \leq i \leq n$, then L' and M are orthogonal.*

Proof: Exercise. □

Proposition 5.6. *For any $n \geq 2$, any set of MOLS of order n has at most $n-1$ elements.*

Proof: Consider a set of MOLS. By Proposition 5.5, we may also assume that the first row of each Latin square is $[1, 2, \ldots, n]$. For any pair of these squares, the ordered pairs (x, x), $1 \leq x \leq n$ all arise from pairing corresponding entries in the first row. Thus, no two of the $(2, 1)$-entries can be equal. Further, no two of the $(2, 1)$-entries can equal 1 (the $(1, 1)$-entry). Hence there are $n - 1$ possibilities for the $(2, 1)$-entry of a square belonging to our set of MOLS, so the set can contain at most $n - 1$ Latin squares. □

It is not true that a set of $n - 1$ MOLS of Latin squares exists for every n. For example, there is not even a *pair* of orthogonal Latin squares of order 6. This was proved around 1900 by Tarry, by exhaustive search, meaning that he considered all cases (not that he was overtired at the end). This showed that the answer to Euler's 36 officers problem is "no". For order 10, it is known that there is no set of nine MOLS, that there is a pair of orthogonal Latin squares, and the existence of a set of three MOLS is still in question.

We will consider next the existence of sets of $n-1$ MOLS of order n, and after that the existence of pairs of orthogonal Latin squares of order n.

The occurrence of the numbers 6 and 10 with regard to the non-existence of sets of $n-1$ MOLS of order n, in the previous paragraph, hints that there may be a connection between such sets and affine (or projective) planes of order n. The connection is, in fact, very strong.

Let L be a Latin square of order n with entries from X. A *transversal of* L is set of n entries of L, one from each row and column. (Note: no two entries are equal.)

Lemma 5.7. *Let L and M be Latin squares with entries ℓ_{ij} and m_{ij}, respectively, from $\{1, 2, \ldots, n\}$. Then, L and M are orthogonal if and only if for every $x \in \{1, 2, \ldots, n\}$, the set $\{m_{ij} : \ell_{ij} = x\}$ is a transversal of M.*

Proof: Exercise. □

Theorem 5.8. *For $n \geq 2$, there exists a set of $n-1$ MOLS of order n if and only if there exists a affine plane of order n.*

Proof: ($\Rightarrow$) Let $\{L_1, L_2, \ldots, L_{n-1}\}$ be a set of $n-1$ MOLS of order n. The points of our affine plane will be the n^2 ordered pairs (i, j), $1 \leq i, j \leq n$. The lines of our affine plane fall into three categories:

- *horizontal*: for each $r \in \{1, 2, \ldots, n\}$, the set $H_r = \{(r, j) : j = 1, 2, \ldots, n\}$ is a line,
- *vertical*: for each $c \in \{1, 2, \ldots, n\}$, the set $V_c = \{(i, c) : i = 1, 2, \ldots, n\}$ is a line, and
- *transversal*: for each Latin square L_k, $1 \leq k \leq n-1$ and each $m \in \{1, 2, \ldots, n\}$, the set $T_{km} = \{(i, j) : \text{the } (i, j)\text{-entry of } L_k \text{ is } m\}$ is a line.

By construction each line contains n points. Thus, if A1 through A5 hold, then the affine plane we have constructed has order n.

It is clear from the construction that A1, A2, and A3 hold.

To establish A4, we must show that any two points are on exactly one line. There are $n(n+1)$ lines and each line contains n points. Since each line accounts for $\binom{n}{2}$ pairs of points, the collection of all lines accounts for

$$n(n+1)\binom{n}{2} = n(n+1)\frac{n(n-1)}{2} = \frac{n^2(n+1)(n-1)}{2} = \frac{n^2(n^2-1)}{2} = \binom{n^2}{2}$$

pairs of points. It therefore suffices to show that any two points are on at most one line. Observe that in each transversal line no two points agree in either coordinate. Consider the two distinct points (i, j) and (r, s). If $i = r$ these points are on H_i and no other line. If $j = s$ these points are on V_j and no other line. Hence assume $i \neq r$ and $j \neq s$, so that these two points are not on the same horizontal line or the same vertical line. If (i, j) and (r, s) belong to the same transversal line T_{km}, then L_k has entry m in both of these positions. Since any two Latin squares in our collection are orthogonal, no Latin square $L_t,\ t \neq j$ has the same entry in both of these positions. Thus, (i, j) and (r, s) can belong to no other transversal line. Therefore A4 holds.

To prove A5 holds, let K be a line and p a point not on K. By construction, there are $n + 1$ lines on p. Since A4 holds, exactly n of these intersect K. Thus, there is a unique line on p that is not on any point of K, which completes the proof.

($\Leftarrow$) Suppose that $(\mathcal{P}, \mathcal{L})$ is an affine plane of order n. This plane has n^2 points, and $n+1$ parallel classes each containing n lines. Let $\{H_1, H_2, \ldots, H_n\}$ and $\{V_1, V_2, \ldots, V_n\}$ be two (different) parallel classes. Any point $p \in \mathcal{P}$ belongs to exactly one line H_i and exactly one line V_j. Assign the coordinates (i, j) to p.

We use the remaining $n - 1$ parallel classes $C_1, C_2, \ldots, C_{n-1}$ to define our Latin squares. Suppose $C_k = \{K_1, K_2, \ldots, K_n\}$. Define an $n \times n$ array by putting the entry x in the (i, j) position if and only if the point with coordinates (i, j) is on K_x. Since the lines in C_k are parallel, this defines a Latin square.

It remains to show that the Latin squares L and M obtained from different parallel classes C_ℓ and C_m, respectively, are orthogonal. Any line of C_r intersects each line of C_s in exactly one point. Thus, for every $x \in \{1, 2, \ldots, n\}$, the set $\{m_{ij} : \ell_{ij} = x\}$ is a transversal of M. The result now follows from Lemma 5.7. □

Corollary 5.9. *For $n \geq 2$, there exists a set of $n - 1$ MOLS of order n if and only if there exists a projective plane of order n.*

To illustrate the construction of an affine plane of order n from a set of $n - 1$ MOLS of order n, consider the set $\{L_1, L_2\}$ of two MOLS of order three:

$$L_1 = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{bmatrix} \qquad L_2 = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{bmatrix}.$$

The point set of our affine plane is the set of nine ordered pairs

$$\mathcal{P} = \{(1, 1), (1, 2), (1, 3), (2, 1), (2, 2), (2, 3), (3, 1), (3, 2), (3, 3)\}.$$

The horizontal lines are

$$H_1 = \{(1,1),(1,2),(1,3)\}, \quad H_2 = \{(2,1),(2,2),(2,3)\}, \quad H_3 = \{(3,1),(3,2),(3,3)\}.$$

The vertical lines are

$$V_1 = \{(1,1),(2,1),(3,1)\}, \quad V_2 = \{(1,2),(2,2),(3,2)\}, \quad V_3 = \{(1,3),(2,3),(3,3)\}.$$

The transversal lines arising from L_1 are

$$T_{1,1} = \{(1,1),(2,2),(3,3)\}, \quad T_{1,2} = \{(1,2),(2,3),(3,1)\}, \quad T_{1,3} = \{(1,3),(2,1),(3,2)\}.$$

Finally, the transversal lines arising from L_2 are,

$$T_{2,1} = \{(1,1),(2,3),(3,2)\}, \quad T_{2,2} = \{(1,2),(2,1),(3,3)\}, \quad T_{2,3} = \{(1,3),(2,2),(3,1)\}.$$

These four parallel classes of lines give the affine plane of order 3 described in Section 3.

To illustrate the reverse construction of $n-1$ MOLS of order n from an affine plane of order n, consider the affine plane of order three with point set $\mathcal{P} = \{1,2,\ldots,9\}$ and line set

$$\begin{aligned}\mathcal{L} = \{&\{1,2,3\},\{4,5,6\},\{7,8,9\},\{1,4,7\},\{2,5,8\},\{3,6,9\},\\ &\{1,5,9\},\{2,6,7\},\{3,4,8\},\{1,6,8\},\{2,4,9\},\{3,5,7\}\}.\end{aligned}$$

The parallel classes are

$$C_H = \{\{1,2,3\},\{4,5,6\},\{7,8,9\}\}, \quad C_V = \{\{1,4,7\},\{2,5,8\},\{3,6,9\}\},$$

$$C_1 = \{\{1,5,9\},\{2,6,7\},\{3,4,8\}\}, \quad C_2 = \{\{1,6,8\},\{2,4,9\},\{3,5,7\}\}.$$

Let the lines in C_H be H_1, H_2, and H_3 in the order listed above, and let the lines in C_V be V_1, V_2, and V_3 in the order listed above. This gives the following assignment of coordinates to points:

$$\begin{gathered}1 = (1,1),\ 2 = (1,2),\ 3 = (1,3),\ 4 = (2,1),\ 5 = (2,2),\\ 6 = (2,3),\ 7 = (3,1),\ 8 = (3,2),\ 9 = (3,3).\end{gathered}$$

The parallel classes C_1 and C_2 give rise, respectively, to the Latin squares

$$L_1 = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{bmatrix}, \quad L_2 = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{bmatrix},$$

our original pair of orthogonal Latin squares of order 3.

The question of for which values of n there exists a set of $n-1$ MOLS of order n is not completely solved at present, just as with the existence problem for affine planes of order n. By Theorem 4.8, we know that there exists a set of $n-1$ MOLS of order n whenever n is a prime power. From our discussion about projective planes, we also know that there is no other value of n for which such a set of $n-1$ MOLS is known to exist, and that in some of these cases the existence of $n-1$ MOLS of order n is ruled out by the Bruck-Ryser Theorem.

Euler knew how to construct a pair of orthogonal Latin squares of order n whenever $n \not\equiv 2 \pmod 4$, and conjectured that no pair of orthogonal Latin squares existed when $n \equiv 2 \pmod 4$. As mentioned before, around 1900 Tarry showed that there is no pair of orthogonal Latin squares of order 6. Thus, Euler was right that the 36 officers problem has no solution. However, in a paper published in the *Canadian Journal of Mathematics* in 1960, R.C. Bose, E.T. Parker, and S.S. Srikhande showed that Euler's conjecture was false by giving a construction for a pair of orthogonal Latin squares in all remaining cases. We conclude this section by showing how to construct a pair of orthogonal Latin squares of order n whenever $n \not\equiv 2 \pmod 4$.

Let L and M be Latin squares of order n_1 and n_2, respectively. The *composition* (or direct product) of L and M is the $n_1n_2 \times n_1n_2$ array $L \times M$ constructed by taking n_1 copies of M, no two having a common entry, and replacing each entry of L by the corresponding copy of M. An example is shown below. The three copies of $\begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix}$ involved are itself, $\begin{bmatrix} 3 & 4 \\ 4 & 3 \end{bmatrix}$, and $\begin{bmatrix} 5 & 6 \\ 6 & 5 \end{bmatrix}$.

$$\begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{bmatrix} \times \begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 4 & 3 & 6 & 5 \\ 5 & 6 & 1 & 2 & 3 & 4 \\ 6 & 5 & 2 & 1 & 4 & 3 \\ 3 & 4 & 5 & 6 & 1 & 2 \\ 4 & 3 & 6 & 5 & 2 & 1 \end{bmatrix}$$

Proposition 5.10. *The composition of two Latin squares L and M is also a Latin square.*

Proof: Exercise. □

Lemma 5.11. *Let L_1 and L_2 be orthogonal Latin squares of order n_1, and M_1 and M_2 be orthogonal Latin squares of order n_2. Then, $L_1 \times M_1$ and $L_2 \times M_2$ are orthogonal Latin squares of order n_1n_2.*

Proof: By Proposition 5.10, both $L_1 \times M_1$ and $L_2 \times M_2$ are Latin squares, and by construction they have order n_1n_2. Since exactly $(n_1n_2)^2$ ordered pairs arise from pairing corresponding elements in these two Latin squares, it suffices to show that each ordered pair occurs at least once.

Suppose x is an entry in the r-th copy of M_1 and y is an entry in the s-th copy of M_2. Since L_1 and L_2 are orthogonal, the ordered pair (r, s) arises when corresponding elements of L_1 and L_2 are paired. Thus, there is a subarray of $L_1 \times M_1$ that contains the elements of the r-th copy of M_1 and is such that the subarray of $L_2 \times M_2$ occupying the same positions contains the elements of the s-th copy of M_2. Since M_1 and M_2 are orthogonal, the ordered pair (x, y) arises when the ordered pairs of corresponding elements are formed. □

Theorem 5.12. *Let* $n \geq 3$. *If* $n \not\equiv 2 \pmod 4$, *then there exists a pair of orthogonal Latin squares of order* n.

Proof: By induction on n. For the basis, note that every $n \leq 8$ which is not congruent to 2 modulo 4 is either prime or a prime power, so the result follows from Corollary 5.9 and Theorem 4.8. Suppose that for some $n \geq 9$ and all k such that $3 \leq k < n$ and $k \not\equiv 2 \pmod 4$ there exists a pair of orthogonal Latin squares of order k.

Consider n. If $n \equiv 2 \pmod 4$, the statement holds. If n is prime, then the existence of a pair of orthogonal Latin squares of order n follows from Corollary 5.9 and Theorem 4.8. Suppose, then, that n is neither prime nor congruent to 2 modulo 4. Then (by Exercise 12), we can write $n = n_1n_2$, where each $n_i \geq 3$ is either odd or divisible by 4. By the induction hypothesis there exist two orthogonal Latin squares L_1 and L_2 of order n_1 and two orthogonal Latin squares M_1 and M_2 of order n_2. By Lemma 5.11, $L_1 \times M_1$ and $L_2 \times M_2$ are orthogonal Latin squares of order $n = n_1n_2$. The result now follows by induction. □

We illustrate the proof of Theorem 5.12 by constructing a pair of orthogonal Latin squares of order $12 = 3 \times 4$. First, we need two orthogonal Latin squares of order 3:

$$L_1 = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{bmatrix} \qquad L_2 = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{bmatrix}.$$

Next, we need two orthogonal Latin squares of order 4:

$$M_1 = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \end{bmatrix}, \qquad M_2 = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \\ 2 & 1 & 4 & 3 \end{bmatrix}.$$

To construct $L_1 \times M_1$, we need three copies of M_1 with entries from $\{1,2,3,4\}$, $\{5,6,7,8\}$, and $\{9,10,11,12\}$, respectively:

$$\begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \end{bmatrix}, \quad \begin{bmatrix} 5 & 6 & 7 & 8 \\ 6 & 5 & 8 & 7 \\ 7 & 8 & 5 & 6 \\ 8 & 7 & 6 & 5 \end{bmatrix}, \quad \begin{bmatrix} 9 & 10 & 11 & 12 \\ 10 & 9 & 12 & 11 \\ 11 & 12 & 9 & 10 \\ 12 & 11 & 10 & 9 \end{bmatrix}.$$

Replacing the elements $1, 2$, and 3 in L_1 by these three squares (so that 1 is replaced by the first square, 2 by the second, etc.) gives:

$$L_1 \times M_1 = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 2 & 1 & 4 & 3 & 6 & 5 & 8 & 7 & 10 & 9 & 12 & 11 \\ 3 & 4 & 1 & 2 & 7 & 8 & 5 & 6 & 11 & 12 & 9 & 10 \\ 4 & 3 & 2 & 1 & 8 & 7 & 6 & 5 & 12 & 11 & 10 & 9 \\ 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 1 & 2 & 3 & 4 \\ 6 & 5 & 8 & 7 & 10 & 9 & 12 & 11 & 2 & 1 & 4 & 3 \\ 7 & 8 & 5 & 6 & 11 & 12 & 9 & 10 & 3 & 4 & 1 & 2 \\ 8 & 7 & 6 & 5 & 12 & 11 & 10 & 9 & 4 & 3 & 2 & 1 \\ 9 & 10 & 11 & 12 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 10 & 9 & 12 & 11 & 2 & 1 & 4 & 3 & 6 & 5 & 8 & 7 \\ 11 & 12 & 9 & 10 & 3 & 4 & 1 & 2 & 7 & 8 & 5 & 6 \\ 12 & 11 & 10 & 9 & 4 & 3 & 2 & 1 & 8 & 7 & 6 & 5 \end{bmatrix}.$$

Similarly, one constructs

$$L_2 \times M_2 = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 3 & 4 & 1 & 2 & 7 & 8 & 5 & 6 & 11 & 12 & 9 & 10 \\ 4 & 3 & 2 & 1 & 8 & 7 & 6 & 5 & 12 & 11 & 10 & 9 \\ 2 & 1 & 4 & 3 & 6 & 5 & 8 & 7 & 10 & 9 & 12 & 11 \\ 9 & 10 & 11 & 12 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 11 & 12 & 9 & 10 & 3 & 4 & 1 & 2 & 7 & 8 & 5 & 6 \\ 12 & 11 & 10 & 9 & 4 & 3 & 2 & 1 & 8 & 7 & 6 & 5 \\ 10 & 9 & 12 & 11 & 2 & 1 & 4 & 3 & 6 & 5 & 8 & 7 \\ 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 1 & 2 & 3 & 4 \\ 7 & 8 & 5 & 6 & 11 & 12 & 9 & 10 & 3 & 4 & 1 & 2 \\ 8 & 7 & 6 & 5 & 12 & 11 & 10 & 9 & 4 & 3 & 2 & 1 \\ 6 & 5 & 8 & 7 & 10 & 9 & 12 & 11 & 2 & 1 & 4 & 3 \end{bmatrix}.$$

These two Latin squares are orthogonal.

Let $N(n)$ denote the maximum size of a set of MOLS of order n. By combining Theorem 5.12 and the result of Bose, Parker and Srikhande mentioned earlier, the following result is obtained.

Theorem 5.13. *For all $n \geq 7$, we have $N(n) \geq 2$.*

In fact, it is known that the size of a largest set of MOLS of order n tends to infinity as n does. The following result of Beth in 1983 is the best-known general lower bound on $N(n)$. The proof is based on sieve techniques in number theory, and is beyond the scope of this course.

Theorem 5.14. *For sufficiently large n, $N(n) \geq n^{1/14.8}$.*

Exercises

1. Show that the number of $2 \times n$ Latin rectangles equals $d_n n!$, where d_n is the number of derangements of an n-set.

2. Find and prove a bound similar to Corollary 5.2 for the number of Latin squares with first row $[1, 2, \ldots, n]$.

3. A square dance club consists of 20 mixed gender couples and meets three times weekly for six weeks. The coordinator wants to assign opposite gender partners so that no female is partnered with the same male twice and, further, no female is ever partnered with her spouse. Is this possible? Why or why not? (If the answer is yes, you need only explain why the desired schedule exists - it is not necessary to produce it.)

4. (a) Prove Lemma 5.4.

   (b) Prove Proposition 5.5.

5. (a) Prove Lemma 5.7.

   (b) Let L be a Latin square. Show that there exists a Latin square M such that L and M are orthogonal if and only if L has n disjoint transversals.

   (c) Let n be an even integer and let L be the Latin square with entries $\ell_{ij} = i + j \pmod{n}$. Show that L has no transversal.

   (d) Can there be a Latin square M such that M and the Latin square L in part (c) are orthogonal? Why or why not?

(e) Let $A^\top$ denote the transpose of the Latin square A. Show that if A and $A^\top$ are orthogonal, then the diagonal positions are a transversal of A.

(f) Show that there is no Latin square L of order 3 such that L and $L^\top$ are orthogonal.

6. An $n \times n$ *semi-magic square* is a matrix in which each integer between 1 and n^2 appears exactly once, and such that each row and each column sum to the same constant. (In a *magic square*, the two diagonals also sum to the same constant.) Let L and M be Latin squares of order n with L having entries $\{1, \dots, n\}$ and M having entries $\{0, n, 2n, \dots, n(n-1)\}$. Prove that $L + M$ is a semi-magic square if and only if L and M are orthogonal Latin squares.

7. Let p be a prime number. Let $L_1, L_2, \dots, L_{p-1}$ be the $p \times p$ arrays defined by setting the (i, j) entry of L_k equal to $i \cdot k + j \pmod p$. Show that $\{L_1, L_2, \dots, L_{p-1}\}$ is a set of $p - 1$ MOLS.

   (Note: we know from Number Theory that if $1 \leq x \leq p-1$ then there is a unique integer y, $1 \leq y \leq p-1$ such that $xy \equiv 1 \pmod p$.)

8. (a) A Latin square is called *symmetric* if it is identical to its transpose. For each $n \geq 1$ find a symmetric Latin square of order n.

   (b) A chess club with $2n$ members wants to schedule a round robin tournament (*i.e.* a tournament where every pair of members play a game). Show how such a schedule can be derived from a symmetric Latin square of order $2n$ with diagonal entries all equal to $2n$.

   (c) Explain how the Latin square from (b) corresponds to a partition $M_1, M_2, \dots, M_{2n-1}$ of the edges of the complete graph K_{2n} such that each set M_i contains n edges, no two of which have a vertex in common.

9. A scientist is studying the effect of soil, temperature and fertilizer on development of five different varieties of strawberries. She wants to compare the effects of five types of soil, five types of fertilizer, and five different temperatures on the growth of the strawberries. A comprehensive study would test each possible combination of variety, soil, temperature, and fertilizer, and would require $5^4 = 625$ different plots. Due to budget and space constraints she has only five small greenhouse units, each with five boxes in which plants can be grown, available for her study. Each greenhouse has its own heat control and can be kept at a different temperature. She decides that it is most important to that each pairing of strawberry variety and fertilizer is tested (at some temperature) and, further, each type of soil is tested at

least once at each temperature. Show how Latin squares can be used to obtain the desired experimental design.

10. Prove Proposition 5.10

11. Use the construction in the proof of Theorem 5.8 to construct an affine plane of order 4 from the following set of three MOLS:

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

12. Suppose that $n \geq 9$ is neither prime nor congruent to 2 modulo 4. Show that $n = n_1 n_2$, for some $n_1, n_2 \geq 3$, each of which is either odd or divisible by 4.

13. Use the construction of Lemma 5.11 to construct a pair of orthogonal Latin squares of order 9.

14. Let L_1 and L_2, and M_1 and M_2 be pairs of orthogonal Latin squares of order 200 and 100, respectively. Suppose that the $(94, 43)$-entries of L_1 and L_2 are 10 and 25, respectively. Suppose also that the $(5, 27)$-entries of M_1 and M_2 are 17 and 31, respectively. Assume that, in the construction from Lemma 5.11 the k-th copy of M_i has entries $(k-1)100+1, (k-1)100+2, \ldots, (k-1)100+100$. What are the $(9305, 4227)$ entries of $L_1 \times M_1$ and $L_2 \times M_2$?

15. Suppose $n = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$, where $p_1, p_2, \ldots, p_k$ are distinct primes and $e_i \geq 1$ for $i = 1, 2, \ldots, k$. Let $m = \min_{1 \leq i \leq k} \{p_i^{e_i}\}$. Prove that there exists a set of $m - 1$ MOLS of order n.

Chapter 6

Designs

6.1 Basic results and existence

A *balanced incomplete block design* (BIBD) with parameters (v, k, λ) is an ordered pair $(V, \mathcal{B})$ where

- V is a set of v objects called *points*,
- $\mathcal{B}$ is a collection of not necessarily distinct k-subsets of V called *blocks*, and
- every pair of distinct points are contained in exactly λ blocks.

Note: since the same k-subset can be a block more than once, $\mathcal{B}$ is not necessarily a set. This is why the generic term "collection" has been used in the definition.

There seems to be some disagreement among various writers as to the meaning of the terms "balanced" and "incomplete". The term balanced is held by some to mean that the blocks all have the same size, and by others to mean that each pair of points appears in the same number of blocks. The term incomplete is held by some to mean that (usually) $k < v$ (so that each block is somehow incomplete), and by others to mean that (usually) not all k subsets of V are blocks (so the collection is somehow incomplete). Thinking back to the origins of BIBDs in the (statistical) design of experiments, it seems likely that "balanced" should refer to the number of blocks containing each pair of points (so the interactions between things being tested are balanced), and that "incomplete" should mean that $k < v$.

In any case, we will usually abbreviate the terminology and say simply "(v, k, λ)-design". We use the word *design* as a generic term for (v, k, λ)-design. This can happen in two extreme senses: when the parameters are implied by the context, and when we have no parameters in mind at all. Sometimes the more descriptive terminology 2-(v, k, λ)-*design* is used. The '2' indicates that every 2 distinct elements are contained together in exactly λ blocks; these structures are sometimes generically referred to as 2-designs. This suggests that there is a more general definition, namely a *t-design* (or t-(v, k, λ)-design). These are defined as above except that every t-subset of V appears in exactly λ blocks. Apart from a couple of exercises, we will only be concerned with 2-designs.

Example 6.1. Let $(\mathcal{P}, \mathcal{L})$ be a projective plane of order n. If each line is regarded as the set of points it is on, then $(\mathcal{P}, \mathcal{L})$ is a $(n^2 + n + 1, n + 1, 1)$-design. Repeating each block of such a design λ times gives a $(n^2 + n + 1, n + 1, \lambda)$-design.

Example 6.2. Let $(\mathcal{Q}, \mathcal{K})$ be a affine plane of order n. If each line is regarded as the set of points it is on, then $(\mathcal{Q}, \mathcal{K})$ is a $(n^2, n, 1)$-design. Repeating each block of such a design λ times gives a (n^2, n, λ)-design.

Example 6.3. For $v \geq k \geq 2$, let $V = \{1, 2, \ldots, v\}$ and let $\mathcal{B} = \binom{V}{k}$, the collection of all k subsets of V. Then every pair of distinct elements in V is contained in exactly $\binom{v-2}{k-2}$ subsets in $\mathcal{B}$. Thus, $(V, \mathcal{B})$ is a $(v, k, \binom{v-2}{k-2})$-design. Designs of this type are called *trivial*.

Example 6.4. Let $V = \{1, 2, \ldots, 11\}$ and let $\mathcal{B}$ be the following collection of blocks:

$$\{1,3,4,5,9\}, \{2,4,5,6,10\}, \{3,5,6,7,11\}, \{1,4,6,7,8\}, \{2,5,7,8,9\}, \{3,6,8,9,10\},$$

$$\{4,7,9,10,11\}, \{1,5,8,10,11\}, \{1,2,6,9,11\}, \{1,2,3,7,10\}, \{2,3,4,8,11\}.$$

Every pair of distinct elements of V appears in exactly two blocks, so $(V, \mathcal{B})$ is an $(11, 5, 2)$-design. Repeating each block of this design m times gives a $(11, 5, 2m)$-design.

The main question regarding BIBDs is: For which triples (v, k, λ) does a (v, k, λ)-design exist? Enumeration and isomorphism of BIBDs are also interesting research topics, but we will not pursue these here. Check the references.

The existence question has an "asymptotic" answer. This is Wilson's Theorem, which we will state later.

Proposition 6.5. *Let $(V, \mathcal{B})$ be a (v, k, λ)-design. Then,*

1. *the number of blocks is* $b = \lambda\binom{v}{2}/\binom{k}{2} = \lambda v(v-1)/k(k-1)$, *and*

2. *every point belongs to exactly* $r = \lambda(v-1)/(k-1)$ *blocks.*

Proof: We prove (1) first. There are $\binom{v}{2}$ pairs of points, and each pair occurs together in λ blocks. Thus, the total number of pairs of points, counting repetitions, is $\lambda\binom{v}{2}$. On the other hand, there are b blocks each of which contains $\binom{k}{2}$ pairs of points, so the total number of pairs of points, counting repetitions, is $b\binom{k}{2}$. Therefore $b\binom{k}{2} = \lambda\binom{v}{2}$, or $b = \lambda\binom{v}{2}/\binom{k}{2}$.

We now prove (2). Let x be a point, and suppose x is contained in r_x blocks. Each of the $v-1$ elements of $V - \{x\}$ belongs to λ pairs containing x, so the total number of pairs containing x is $\lambda(v-1)$. On the other hand, each block containing x gives $k-1$ pairs containing x, so that the total number of pairs containing x is $r_x(k-1)$. Therefore $r_x(k-1) = \lambda(v-1)$, or $r_x = \lambda(v-1)/(k-1)$. Since the RHS of the latter expression is independent of x, the proof is complete. □

The definition of a (v, k, λ)-design is sometimes stated with the list of five parameters (v, b, r, k, λ). Proposition 6.5 says that b and r are determined by v, k and λ. We will continue to use b and r to denote the number of blocks and the number of blocks containing each point, respectively. Since these quantities are integers, we have the following. (Recall "|" is notation for "divides".)

Corollary 6.6. *If there exists a* (v, k, λ)*-design, then*

1. $k(k-1) \mid \lambda v(v-1)$, *and*

2. $(k-1) \mid \lambda(v-1)$.

The conditions in Corollary 6.6 are necessary for the existence of a BIBD with parameters (v, k, λ). A good way to see this is to consider the contrapositive of the statement: *If either* (1) *or* (2) *is false, then a* (v, k, λ)*-design does not exist.* The conditions are not sufficient: it is false that if v, k and λ are such that $(k-1) \mid \lambda(v-1)$ and $k(k-1) \mid \lambda v(v-1)$, then a (v, k, λ)-design exists. An example will be given following Corollary 6.7.

Corollary 6.7. *For any* (v, k, λ)*-design,* $bk = vr$.

Proof: Exercise. □

Recall the dinner club of Section 4, Exercise 2. Suppose it grows from 16 members to 20. They still wish to dine in groups of four on club nights in such a way that each pair of people dines together once per year. A schedule for the dinners corresponds to a $(20, 4, 1)$-design with the additional property that the blocks can be partitioned into sets of size five ("parallel classes") such that no two blocks in the same set intersect. Ignoring the second (important) condition for a moment, the first step is to check whether a $(20, 4, 1)$-design can exist. Necessary condition (2) of Corollary 6.6 requires that $3 \mid 1 \cdot 19$, which is not true. Therefore, no such design exists.

Continuing with the example from the previous paragraph, the club might instead seek a schedule running over a period of time so that each pair of people dine together the same number of times, λ. Thus, they want a $(20, 4, \lambda)$-design with the same partitionability property as above. From Example 3 we know that a $(20, 4, \binom{18}{2})$-design exists. By Proposition 6.5, the number of blocks in such a design is $\binom{18}{2}\binom{20}{2}/\binom{4}{2} = 4845$, so the schedule, if it exists (the partitioning problem would still need to be addressed) would cover 969 club nights. This is not realistic, so we check a few smaller values of λ. The case $\lambda = 2$ is ruled out by necessary condition (2) of Corollary 6.6 as 3 is not a divisor of $2 \cdot 19$. Check that the case $\lambda = 3$ satisfies divisibility conditions (1) and (2). Thus, a $(20, 4, 3)$-design is not ruled out by the Corollary 6.6, and *might* exist. (It turns out that a design with these parameters and with the required partitionability property does in fact exist.)

We will next give an example of parameters that satisfy the necessary conditions but for which the design in question does not exist. In order to do this, we need a fact.

Proposition 6.8. *Let $n \geq 2$. There exists a $(n^2, n, 1)$-design if and only if there exists an affine plane of order n.*

Proof: ($\Leftarrow$) This is clear (also, see Example 6.2).

($\Rightarrow$) We must show that postulates A1 - A5 hold. A1, A2, and A3 are clear. The truth of A4 follows from the definition of a design. To see A5, let B be a block and x a point not in B. By Proposition 6.5, the point x is in $r = 1(n^2 - 1)/(n - 1) = (n + 1)$ blocks. Since each pair of points is contained in only one block, exactly n of these intersect B. Thus, there is a unique block on x that does not meet B, so A5 holds. □

Since we know there is no affine plane of order 10, Proposition 6.8 implies that there is no $(100, 10, 1)$-design. But the necessary conditions hold for the parameter set: $9 \mid 1 \cdot 99$ and $10 \cdot 9 \mid 1 \cdot 100 \cdot 99$.

It is tempting to assert the corollary that a projective plane of order n exists if and only if a $(n^2+n+1, n+1, 1)$-design exists. But, we don't know that given a $(n^2+n+1, n+1, 1)$-design it is possible to delete a block and all points it contains and obtain a $(n^2, n, 1)$-design. (This also turns out to be true.) Suppose we try to prove directly that postulates P1-P5 hold. The first four are clear. To prove P5, we would need that there is exactly one point in the intersection of any two distinct blocks. This is the same thing needed to get a $(n^2, n, 1)$-design by deleting a block. We will eventually use some linear algebra to prove that in any design where $b = v$ any two distinct blocks intersect in exactly λ points. (See Corollary 6.13.) So the "corollary" is true, but we don't have enough tools to prove it just yet.

It follows from Proposition 6.8 that the Bruck-Ryser theorem can be used to rule out the existence of designs with certain parameter sets.

There is one further necessary condition that can be used to rule out the existence of designs with certain parameters. This is Fisher's inequality.

Theorem 6.9. (Fisher's Inequality, 1940) *In any (v, k, λ)-design with $1 < k < v$, it is necessary that $b \geq v$.*

We will give a proof of this inequality in the next section.

Plugging in the formula for b given in Proposition 6.5, Fisher's inequality says that if there exists a (v, k, λ)-design then $\frac{\lambda v(v-1)}{k(k-1)} \geq v$, or equivalently $\lambda(v-1) \geq k(k-1)$. The contrapositive of this statement is: *If $\lambda(v-1) < k(k-1)$ then there is no design with parameters (v, k, λ).* This statement can be used to rule out the existence of designs with certain parameters that satisfy the necessary conditions in Corollary 6.6. For example, consider $(46, 10, 1)$. Then, $(10-1) \mid 1(46-1)$ and $10(10-1) \mid 1(46)(46-1)$, so the divisibility conditions are satisfied. But, since $\lambda(v-1) = 1(46-1) = 45 < 90 = 10(10-1) = k(k-1)$, no design with these parameters can exist.

As seen above, the necessary condition arising from Fisher's inequality only rules out parameters where v is relatively small for a given k. This observation leads nicely into an important and famous existence theorem for designs.

Theorem 6.10. (Wilson's Theorem, 1972) *Given k and λ, there exists an integer $v_0(k, \lambda)$ such that a (v, k, λ)-design exists for all $v \geq v_0(k, \lambda)$ that satisfy the conditions of Corollary 6.6.*

Wilson's theorem can be phrased as: *The necessary conditions in Corollary 6.6 are asymptotically sufficient.* It is known that

$$v_0(k,\lambda) < e^{\left(e^{(k^{k^2})}\right)}.$$

For $k = 3$, the RHS is about e raised to $1.7 \cdot 10^{8548}$. This number has about $7 \cdot 10^{8547}$ digits!

Exercises

1. Suppose $k > 2$ and $k \equiv 2$ or $3 \pmod 4$. (a) Show that $\binom{k}{2}$ is odd.

   (b) Let $v = \binom{k}{2} + 1$. Does a $(v, k, 1)$-design exist?

2. Let M be the matrix

$$M = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & 16 \end{bmatrix}.$$

   For $i = 1, 2, \ldots, 16$, let B_i be the set of all elements different from i and in the same row or column as i. Show that $B_1, B_2, \ldots, B_{16}$ are the blocks of a design and find its parameters.

3. Prove that the following conditions on the parameters of a design are all equivalent:

   (a) $\lambda(v-1) = k(k-1)$,

   (b) $k^2 - \lambda v = k - \lambda$,

   (c) $(v-k)\lambda = (k-1)(k-\lambda)$,

   (d) $\lambda(v - 2k + \lambda) = (k-\lambda)^2$.

4. For each of the following, either fill in the missing values to obtain the full collection of parameters (v, b, r, k, λ) of a hypothetical design or demonstrate that no design with these parameters can exist.

   (a) $b = 35,\ k = 3, \lambda = 1.$

   (b) $v = 14,\ b = 7,\ r = 4.$

   (c) $r = 6,\ k = 4,\ \lambda = 2.$

(d) $v = 21,\ b = 28,\ k = 3.$

(e) $v = 17,\ r = 8,\ k = 5.$

(f) $v = 21,\ b = 30,\ k = 7.$

(g) $v = 10,\ r = 9,\ k = 3.$

(h) $b = 46,\ r = 9,\ k = 6.$

(i) $v = 19,\ k = 7,\ \lambda = 3.$

(j) $v = 22,\ r = 12,\ \lambda = 4.$

(k) $v = 25,\ k = 10,\ \lambda = 3.$

(l) $b = 15,\ k = 4,\ \lambda = 2.$

(m) $r = 7,\ k = 3,\ \lambda = 2.$

(n) $r = 13,\ k = 6,\ \lambda = 1.$

(o) $v = 21,\ b = 70,\ k = 3.$

(p) $v = 25,\ k = 5,\ \lambda = 3.$

5. Suppose $(V, \mathcal{B})$ is a (v, k, λ)-design such that no two blocks are the same and not every k-subset of V is a block. Let $\overline{\mathcal{B}}$ be the collection of k-subsets of V that do not belong to $\mathcal{B}$. Show that $(V, \overline{\mathcal{B}})$ is a design and find its parameters.

6. A t-(v, k, λ)-design is defined similarly to a (v, k, λ)-design, except that every t-subset of points is contained in exactly λ blocks (rather than every pair of points being contained in λ blocks). Ordinary designs are t-designs with $t = 2$.

   (a) What is a 1-design with $\lambda = 1$? (It has another name!)

   (b) Show that the number of blocks in a t-(v, k, λ)-design is $b = \lambda\binom{v}{t}/\binom{k}{t}$.

   (c) Show that for each $t = 1, 2, \ldots, k$, the collection of all k-subsets of $\{1, 2, \ldots, v\}$ are the blocks of a $t - (v, k, \lambda_t)$-design.

   (d) Let $(V, \mathcal{B})$ be a $t - (v, k, \lambda)$-design, and let $2 \le s \le t$. Show that there exists λ_s such that $(V, \mathcal{B})$ is a $s - (v, k, \lambda_s)$-design.

7. Find a value of x such that if $v > x\binom{k}{2}$, and the parameters (v, k, λ) satisfy the necessary conditions in Corollary 6.6, then $\frac{\lambda v(v-1)}{k(k-1)} \ge v$. (This explains why the condition arising from Fisher's inequality does not appear in Wilson's Theorem. Once v is large enough the condition is satisfied.)

6.2 Fisher's inequality and symmetric designs

Here, we begin with a beautiful proof of Fisher's inequality, stated in section 6.1 as Theorem 6.9. We first require some tools from linear algebra.

Let $\mathcal{D} = (V, \mathcal{B})$ be a design with $V = \{x_1, x_2, \ldots, x_v\}$ and blocks $B_1, B_2, \ldots, B_b$. The *incidence matrix* of $\mathcal{D}$ is the $v \times b$ matrix A with (i, j)-entry

$$a_{ij} = \begin{cases} 1 & \text{if } x_i \in B_j \\ 0 & \text{if } x_i \notin B_j. \end{cases}$$

Note: some authors define the incidence matrix to be $b \times v$ (the transpose of the matrix defined above) so be careful when searching through the literature.

Consider a $(4, 2, 1)$-design $(\mathcal{P}, \mathcal{B})$ with $\mathcal{P} = \{1, 2, 3, 4\}$ and blocks $\{1, 2\}, \{1, 3\}, \{1, 4\}, \{2, 3\}, \{2, 4\}, \{3, 4\}$. If we number the blocks $B_1, B_2, \ldots, B_6$ in the order they are listed, then the incidence matrix is

$$A = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}.$$

An incidence matrix tells you everything about a design, up to the names of the points and blocks. The number of points equals the number of rows, and the number of blocks equals the number of columns. The blocks in which a point is contained are indicated by the 1s in the corresponding row, and the elements of each block are given by the 1s in the corresponding column. Assigning different names to the points and/or blocks (for example, listing them in a different order) gives a different incidence matrix, but any two such matrices are equivalent in the sense that one can be obtained from the other by permuting rows and/or columns. Hence we talk about *the* incidence matrix of a design.

Notation: We use I to denote an identity matrix and J to denote a square matrix in which every entry equals 1.

Lemma 6.11. *Let A be the incidence matrix of a (v, k, λ)-design. Then,*

$$AA^\top = (r - \lambda)I + \lambda J.$$

Proof: Suppose the points of the design are $\{x_1, x_2, \ldots, x_v\}$. Then, $AA^\top$ is a $v \times v$ matrix.

The (i,j)-entry of $AA^\top$ is the dot product of the i-th row of A and the j-th column of $A^\top$, that is, of the i-th and j-th rows of A. If $i = j$ this is the number of blocks containing the point x_i, namely r. If $i \neq j$, then there is a contribution of 1 to the dot product for every block that contains both x_i and x_j. By definition of a (v, k, λ)-design, there are λ such blocks. The result now follows. □

Linear Algebraic Proof of Fisher's Inequality. Let A be the incidence matrix of the design. Suppose we know that $AA^\top$ is invertible, and hence has rank v (since it is $v \times v$). Given this, the following argument establishes the result. Since the rank of a product of two matrices is no larger than the smaller of their ranks, this implies that A has rank at least v. But A is a $v \times b$ matrix, so its rank can not be greater than b. Therefore, $b \geq v$.

Thus, we must show $AA^\top$ is invertible. We do so by showing its determinant is non-zero. From Lemma 6.11,

$$|AA^\top| = \begin{vmatrix} r & \lambda & \lambda & \cdots & \lambda \\ \lambda & r & \lambda & \cdots & \lambda \\ \lambda & \lambda & r & \cdots & \lambda \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \lambda & \lambda & \lambda & \cdots & r \end{vmatrix}.$$

Subtracting the first row from each other row (and remembering that this does not change the determinant) gives

$$|AA^\top| = \begin{vmatrix} r & \lambda & \lambda & \cdots & \lambda \\ \lambda - r & r - \lambda & 0 & \cdots & 0 \\ \lambda - r & 0 & r - \lambda & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \lambda - r & 0 & 0 & \cdots & r - \lambda \end{vmatrix}.$$

Adding each of columns 2 through v to column 1 (and remembering that this does not change the determinant either) gives

$$|AA^\top| = \begin{vmatrix} r + (v-1)\lambda & \lambda & \lambda & \cdots & \lambda \\ 0 & r - \lambda & 0 & \cdots & 0 \\ 0 & 0 & r - \lambda & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & r - \lambda \end{vmatrix}.$$

Since the determinant of an upper triangular matrix is the product of the entries on the main diagonal, $|AA^\top| = (r + (v-1)\lambda)(r-\lambda)^{v-1}$.

By hypothesis, $k < v$. Thus, by Proposition 6.5, $r > \lambda$. Since $v > 1$, we have $|AA^\top| > 0$. This completes the proof. □

A (v, k, λ)-design is called *symmetric* (or *square*) if $v = b$. This is when equality is obtained in Fisher's inequality.

By Corollary 6.7, $bk = vr$. Hence the parameters of a symmetric design also satisfy $k = r$.

By Fisher's inequality, symmetric designs have the smallest possible number of blocks of any design on v points. Although the incidence matrix of a symmetric design is square, it is typically not symmetric. The term "symmetric" arises because of a symmetry (or duality) between the points and blocks of such a design. This will become apparent shortly.

Note that for instance any design arising from a projective plane is symmetric.

The following theorem looks a lot like Lemma 6.11. Note, however, that the order of the matrices in the product is reversed.

Theorem 6.12. *Let A be the incidence matrix of a symmetric design. Then*

$$A^\top A = (k-\lambda)I + \lambda J.$$

Proof: Put $f = \sqrt{\frac{\lambda}{v}}$. Consider $(A - fJ)\left(A^\top + fJ\right) = AA^\top + f\left(AJ - JA^\top\right) - f^2J^2$. Now $AJ = rJ = kJ$ by definition of A and the fact that we have a symmetric design. Also, $JA^\top = (AJ)^\top = (kJ)^\top = kJ$. Since J is $v \times v$, $J^2 = vJ$ and therefore

$$AA^\top + f\left(AJ - JA^\top\right) - f^2J^2 = AA^\top - \lambda J.$$

By Lemma 6.11 and the fact that $k = r$, we have $AA^\top = (k-\lambda)I + \lambda J$. Thus, $AA^\top - \lambda J = (k-\lambda)I$. Therefore,

$$\left(A^\top + fJ\right)^{-1} = \frac{1}{k-\lambda}\left(A - fJ\right).$$

Since inverses commute, this implies

$$(k-\lambda)I = \left(A^\top + fJ\right)(A - fJ) = A^\top A + f\big(JA - A^\top J\big) - f^2J^2.$$

Since $JA = kJ$ and $A^\top J = (JA)^\top = (kJ)^\top = kJ$, the right hand side simplifies like before to $A^\top A - \lambda J$. Therefore, $A^\top A = (k-\lambda)I + \lambda J$. □

Corollary 6.13. *In a symmetric (v, k, λ)-design, every pair of distinct blocks intersect in exactly λ elements.*

Proof: Suppose the blocks of the design are $B_1, B_2, \ldots, B_b$. The number of elements in common to B_i and B_j is the (i, j)-entry of $A^\top A$. Since $i \neq j$, Theorem 6.12 asserts that this equals λ. □

Corollary 6.14. *Let $n \geq 2$. There exists a $(n^2 + n + 1, n + 1, 1)$-design if and only if there exists a projective plane of order n.*

Proof: Exercise. □

By Corollaries 6.7 and 6.13, for a symmetric design we have that the following statements are true:

- Every pair of distinct points are contained in exactly λ blocks and every pair of distinct blocks intersect in exactly λ points.
- Every block contains k points and every point is in k $(= r)$ blocks.

Some authors suggest that the symmetry of these statements is the reason underlying the term "symmetric design". The statements also suggest that there may be some sort of duality for symmetric designs that generalises duality of projective planes (which give rise to symmetric designs).

Suppose a symmetric design has points $x_1, x_2, \ldots, x_v$ and blocks $B_1, B_2, \ldots, B_v$. Its *dual* has points $B_1, B_2, \ldots, B_v$ and the blocks $X_1, X_2, \ldots, X_v$ defined by $B_i \in X_j \Leftrightarrow x_j \in B_i$.

Proposition 6.15. *The dual of a symmetric (v, k, λ)-design $\mathcal{D}$ is also a symmetric (v, k, λ)-design.*

Proof: By the definition, the dual has v points and v blocks. Since every point of $\mathcal{D}$ belongs to $r = k$ blocks, every block of the dual has size k. Let B_i and B_j be blocks of $\mathcal{D}$. By Corollary 6.13, these blocks have exactly λ points in common. Thus, B_i and B_j are contained in exactly λ blocks of the dual. This completes the proof. □

Up to notational difficulties, the dual of a symmetric design is obtained by reversing the role of the points and blocks while maintaining incidence. Indeed, the incidence matrix of the dual design is the transpose of the incidence matrix of the original symmetric design.

Notes:

- The dual design is defined only if the original design is symmetric.
- The dual design is symmetric (too).
- The dual of the dual is identical to the original design apart from the names of the points and blocks (*i.e.* they are isomorphic, where isomorphism is defined in the natural way).

Example 6.16. Consider the $(7, 3, 1)$-design with blocks $B_1 = \{2, 3, 5\}$, $B_2 = \{3, 4, 6\}$, $B_3 = \{4, 5, 7\}$, $B_4 = \{1, 5, 6\}$, $B_5 = \{2, 6, 7\}$, $B_6 = \{1, 3, 7\}$, $B_7 = \{1, 2, 4\}$. The dual design has points $B_1, B_2, \ldots, B_7$ and blocks

$$X_1 = \{B_4, B_6, B_7\}, X_2 = \{B_1, B_5, B_7\}, X_3 = \{B_1, B_2, B_6\}, X_4 = \{B_2, B_3, B_7\},$$

$$X_5 = \{B_1, B_3, B_4\}, X_6 = \{B_2, B_4, B_5\}, X_7 = \{B_3, B_5, B_6\}.$$

To construct an affine plane of order n from a projective plane of order n we choose any line of the projective plane and delete it and all points on it. The same idea allows new designs to be constructed from symmetric designs.

Let $\mathcal{D}$ be a symmetric (v, k, λ)-design, with point set V and blocks $B_1, B_2, \ldots, B_v$. Let $B = B_i$ be any fixed block of $\mathcal{D}$. The *residual* of $\mathcal{D}$ with respect to block B has points $V - B$ and blocks $B_j - B$, $j \neq i$.

Proposition 6.17. *The residual of a symmetric (v, k, λ)-design with respect to any block is a $(v - k, k - \lambda, \lambda)$-design.*

Proof: Exercise. □

Note that the residual design is defined with respect to symmetric designs only, but the residual design is not symmetric. The name residual suggests, correctly, that its what's left when all points in a particular block are deleted.

Example 6.18. Consider the $(11, 5, 2)$-design of Example 6.4. The residual with respect to the block $\{1, 3, 4, 5, 9\}$ is the $(6, 3, 2)$-design with point set $\{2, 6, 7, 8, 10, 11\}$ and blocks

$$\{2, 6, 10\}, \{6, 7, 11\}, \{6, 7, 8\}, \{2, 7, 8\}, \{6, 8, 10\},$$

$$\{7, 10, 11\}, \{8, 10, 11\}, \{2, 6, 11\}, \{2, 7, 10\}, \{2, 8, 11\}.$$

Let $\mathcal{D}$ be a symmetric (v, k, λ)-design, with point set V and blocks $B_1, B_2, \ldots, B_v$. Let $B = B_i$ be any fixed block of $\mathcal{D}$. The *restriction* of $\mathcal{D}$ to B has point set B_i and blocks $B_j \cap B$, $j \neq i$.

Proposition 6.19. *The restriction of a symmetric design to a block B is a $(k, \lambda, \lambda - 1)$-design.*

Proof: Exercise. □

The restriction of a symmetric design is more commonly called the *derived design*. Note that the derived design is only defined when the original design is symmetric, but the derived design is not symmetric.

Example 6.20. Consider again the $(11, 5, 2)$-design of Example 6.4. The derived design with respect to the block $\{1, 3, 4, 5, 9\}$ is the $(5, 2, 1)$-design with point set $\{1, 3, 4, 5, 9\}$ and blocks

$$\{4, 5\}, \{3, 5\}, \{1, 4\}, \{5, 9\}, \{3, 9\}, \{4, 9\}, \{1, 5\}, \{1, 9\}, \{1, 3\}, \{3, 4\}.$$

Exercises

1. Prove Corollary 6.7 by arguing that the LHS and RHS both count the number of 1s in the incidence matrix.

2. Let v, b, r, k, and λ be integers with $k < v$. Let A be a $v \times b$ 0-1 matrix. Prove that A is the incidence matrix of a (v, k, λ)-design if and only if $AA^\top = (r - \lambda)I + \lambda J_{v\times v}$ and $J_{v\times v}A = kJ_{v\times b}$, where $J_{s\times t}$ is an $s \times t$ matrix with every entry equal to 1.

3. It is known that if $v > k$ and there is some block in a (v, k, λ) design which is repeated m times, then $b \geq mv$. (This is known as 'Mann's Inequality'.) Give a direct proof of this for the simple case $k = 3$, $\lambda = 2$, $m = 2$. (*Hint*: Use an expression for b to rewrite the inequality.)

4. Show that in a symmetric design, if v is even then λ is even.

5. Prove Corollary 6.14

6. Determine all possible values of k and λ such that there exists a symmetric $(11, k, \lambda)$ design, and show how to construct these designs.

7. Let $(V, \mathcal{B})$ be a (v, k, λ)-design with blocks $B_1, B_2, \ldots, B_b$.

(a) Let x and y be distinct points in V. Prove that the number of blocks containing at least one of x or y is $2r - \lambda$.

(b) Prove that if $b-2r+\lambda > 0$ then the sets $\overline{B}_1, \overline{B}_2, \ldots, \overline{B}_b$ defined by $\overline{B}_i = V - B_i$ are the blocks of a $(v, v-k, b-2r+\lambda)$-dsign.

(c) Prove that if $v = b$ and $k < v-1$, then $b - 2r + \lambda > 0$.

8. Prove Proposition 6.17 and determine b and r for this design.

9. Prove Proposition 6.19 and determine b and r for this design.

10. (a) Make a formal definition of isomorphism of BIBDs $(V_1, \mathcal{B}_1)$ and $(V_2, \mathcal{B}_2)$.

    (b) Let $\mathcal{D}^d$ denote the dual of the symmetric design $\mathcal{D}$. Prove that $(\mathcal{D}^d)^d$ and $\mathcal{D}$ are isomorphic.

    (c) Prove that, up to isomorphism, there is only one $(v, 2, 1)$-design.

    (d) Let $\mathcal{D}$ be the $(15, 7, 3)$-design with $V = \{0, 1, \ldots, 9, A, B, C, D, E\}$ whose blocks (with brackets and commas omitted) are:

$$0123456, 012789A, 012BCDE, 03478BC, 0349ADE,$$

$$05678DE, 0569ABC, 13579BD, 1367ACE, 1458ABE,$$

$$14689CD, 2358ACD, 23689BE, 24579CE, 2467ABD.$$

    Construct the dual design $\mathcal{D}^d$ and show that $\mathcal{D}$ and $\mathcal{D}^d$ are not isomorphic. (*Hint*: look at the number of triples of blocks that intersect in three elements.)

11. Consider exercise 2 from section 6.1. Show that this design is symmetric, and find the the dual, residual and restriction with respect to block B_1.

6.3 Difference sets and difference systems

A (v, k, λ)-*difference set* is a k-subset $D \subseteq \mathbb{Z}_v$ such that each non-zero element of $\mathbb{Z}_v$ occurs exactly λ times among the $k(k-1)$ differences of elements belonging to D.

For example, $\{1, 2, 4\}$ is a $(7, 3, 1)$-difference set as the six differences modulo 7 are

$$1-2 \equiv 6,\ 1-4 \equiv 4,\ 2-1 \equiv 1,\ 2-4 \equiv 5,\ 4-1 \equiv 3,\ 4-2 \equiv 2\ \ 2-1 \equiv 1.$$

Similarly, $\{1, 3, 4, 5, 9\}$ is a $(11, 5, 2)$-difference set.

Note: the group $\mathbb{Z}_v$ can be replaced by any Abelian group, so more general results than the ones we will consider are true.

Proposition 6.21. *If there exists a (v, k, λ)-difference set, then $k(k-1) = \lambda(v-1)$.*

Proof: There are $k(k-1)$ differences of elements in a k-set D, and each of the $v-1$ non-zero elements of $\mathbb{Z}_v$ must occur λ times as a difference. □

The above proposition is useful when phrased as its contrapositive:

If $k(k-1) \neq \lambda(v-1)$, then there is no (v, k, λ)-difference set.

Let D be a (v, k, λ)-difference set. For each $i \in \mathbb{Z}_v$, the set $D + i = \{d + i : d \in D\}$ is called a *translate* of D. To *develop D modulo v* means to construct the v translates of D.

Developing the $(7, 3, 1)$-difference set $\{1, 2, 4\}$ modulo 7 yields the (seven) translates

$$\{1, 2, 4\}, \{2, 3, 5\}, \{3, 4, 6\}, \{4, 5, 7\}, \{1, 5, 6\}, \{2, 6, 7\}, \{1, 3, 7\},$$

which are the blocks of a $(7, 3, 1)$-design. It turn out to be true in general that developing a (v, k, λ)-difference set yields the blocks of a (v, k, λ)-design (which accounts in part for the similarity in notation).

Proposition 6.22. *Every translate of a (v, k, λ)-difference set is also a (v, k, λ)-difference set.*

Proof: Exercise. □

Proposition 6.23. *Let D be a (v, k, λ)-difference set. Then the collection of translates of D is a (v, k, λ) design.*

Proof: Since each translate is a k-subset of $\{1, 2, \ldots, v\}$, it remains to show that each pair of distinct elements occur together in exactly λ translates.

Let $D = \{d_1, d_2, \ldots, d_k\}$. Let $x \in \{1, 2, \ldots, v\}$. Suppose $x \in D + j$. Then $x = d_\ell + j$ for some ℓ, so that $j = x - d_\ell$. Since $x = d_i + (x - d_i)$, the element x appears in the translates $D + (x - d_i)$, $1 \leq i \leq k$, and no others.

Let a and b be distinct elements of $\{1, 2, \ldots, v\}$. Then, by the above argument a and b both occur in a translate $D + t$ whenever $t = a - d_i = b - d_j$ for some integers i and j. But $a - d_i = b - d_j$ is equivalent to $a - b = d_i - d_j$. By definition of a a (v, k, λ)-difference set, there are exactly λ pairs of elements of D for which the condition on the RHS holds. Hence, a and b occur together in exactly λ translates of D. This completes the proof. □

Note: The design obtained by developing a difference set is necessarily symmetric, since there are v blocks.

Difference sets occur in pairs, though not necessarily for the same k or λ.

Proposition 6.24. *If D is a (v, k, λ)-difference set, then $\overline{D}$ is a $(v, v-k, v-2k+\lambda)$-difference set.*

Proof: Exercise. □

For example, since $\{1, 3, 4, 5, 9\}$ is a $(11, 5, 2)$-difference set, Proposition 6.24 says that its complement $\{2, 6, 7, 8, 10, 11\}$ is a $(11, 6, 3)$-difference set.

One method for finding (v, k, λ)-designs is to find (v, k, λ)-difference sets. There are two catches. First, not every design can be obtained via difference sets (or similar methods). Second, we presently have no methods other than trial and error for finding difference sets. The next two theorems give some methods for finding difference sets. They are stated without proof.

Theorem 6.25. (Paley, 1972) *Let $p \equiv 3 \pmod 4$ be prime. The set of non-zero squares modulo p is a $(p, \frac{p-1}{2}, \frac{p-3}{4})$-difference set.*

The squares modulo 7 are $1^2 \equiv 1, 2^2 \equiv 4$, and $3^2 \equiv 2$. Thus, $D_1 = \{1, 2, 4\}$ is a $(7, 3, 1)$-difference set, as we have already seen. Developing D_1 modulo 7 yields a $(7, 3, 1)$-design, the Fano plane. (It is only necessary to work out the squares up to $(7-1)/2$ because $4 \equiv (-3), 5 \equiv (-2), 6 \equiv (-1)$. In general it is only necessary to go up to $(p-1)/2$.) Here is a new example.

Example 6.26. The squares of the first 11 integers modulo 23 are (in order) 1, 4, 9, 16, 2, 13, 3, 18, 12, 8, 6. Thus,

$$D_2 = \{1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18\}$$

is a $(23, 11, 5)$-difference set. Developing D_2 modulo 23 yields a $(23, 11, 5)$-design.

Corollary 6.27. *Let $p \equiv 3 \pmod 4$ be prime. The set consisting of zero and the non-squares modulo p is a $(p, \frac{p+1}{2}, \frac{p+1}{4})$-difference set.*

Proof: The set of non-squares is the complement of the set of squares, so the result follows from Proposition 6.24. □

Referring to the examples above, this means $\{3, 5, 6, 7\}$ is a $(7, 4, 2)$-difference set, and $\{5, 7, 10, 11, 14, 15, 17, 19, 20, 21, 22, 23\}$ is a $(23, 12, 6)$-difference set.

Let D be a (v, k, λ)-difference set. The integer m is called a *multiplier* of D if the set $mD = \{md : d \in D\}$ is a translate of D (*i.e.* if there exists j such that $mD = D + j$).

A (v, k, λ)-difference set D is *fixed* by a multiplier m if $mD = D$.

For example, $D = \{1, 2, 4, 10\}$ is a $(13, 4, 1)$-difference set (check this!). The integer 3 is a multiplier of D because $3D = \{3, 6, 12, 4\} = D + 2$.

It is presently unknown whether every difference set must have a multiplier besides 1 (which always works). The following theorem gives some special conditions under which a multiplier exists.

Theorem 6.28. (Multiplier Theorem, Hall and Ryser, 1951) *Let D be a (v, k, λ)-difference set. If q is a prime number such that*

- $q > \lambda$,
- $q \nmid v$, *and*
- $q | (k - \lambda)$,

then q is a multiplier of D. Furthermore, there exists a translate of D that is fixed by every multiplier of D.

It is worth mentioning that the first part of the Multiplier Theorem gives conditions that are sufficient for the existence of a multiplier. It does *not* say that there is no multiplier if the conditions fail.

In the case where the Multiplier Theorem guarantees the existence of a multiplier, it can be used together with Proposition 6.22 to give a method for deciding existence or non-existence of difference sets:

Suppose we are looking for a $(21, 5, 1)$-difference set. Since $5 \cdot 4 = 1 \cdot (21 - 1)$, the necessary condition is satisfied (and hence does not rule out the existence of such a set). The integer 2 satisfies the three conditions of the Multiplier Theorem, and so is a multiplier of any

$(21, 5, 1)$-difference set. By Proposition 6.22, we can assume that such a difference set D is fixed by 2, *i.e.* $2D = D$. Thus, if $x \in D$, then $2x \in D$. Applying this argument over and over, $2x, 2^2x, 2^3x, \ldots$ are all in D. Now, repeated multiplication by 2 partitions the elements of $\mathbb{Z}_{21}$ into the following sets (called *orbits*):

$$\{1, 2, 4, 8, 16, 11\}, \{3, 6, 12\}, \{5, 10, 20, 19, 17, 13\}, \{7, 14\}, \{9, 18, 15\}, \{0\}.$$

The set D has size five and must be a union of sets from this collection. (Since D is fixed by the multiplier 2, it must contain either all or no elements from each orbit.) Thus, there are two possibilities for D, $\{3, 6, 12\} \cup \{7, 14\}$ and $\{7, 14\} \cup \{9, 18, 15\}$. Both of these work (check this), so **there exists a $(21, 5, 1)$-difference set, and the multiplier Theorem aids in finding it.**

Note that there is no guarantee that a set of the correct size formed from a union of orbits is a difference set. It could be that none are, in which case it can be concluded that no difference set exists.

Now suppose we are looking for a $(31, 10, 3)$-difference set D. The necessary condition $10 \cdot 9 = 3 \cdot (31 - 1)$ is satisfied. The integer 7 satisfies the three conditions of the Multiplier Theorem and so is a multiplier of D (if it exists). By Proposition 6.22, we can assume that D is fixed by 7. As in the previous example, if $x \in D$ then $7x, 7^2x, 7^3x, \ldots$ are also in D. This leads to the orbits:

$$\{0\}, \{1, 7, 18, 2, 14, 5, 4, 28, 10, 8, 25, 20, 16, 19, 9\},$$

$$\{3, 21, 23, 6, 11, 15, 12, 22, 30, 24, 13, 29, 17, 26, 27\}.$$

Now D must be a union of sets from this collection, but it is impossible to form a set of size 10 this way. **Hence no $(31, 10, 3)$-difference set exists.**

Let $D_1, D_2, \ldots, D_t$ be (not necessarily distinct) k-subsets of $\mathbb{Z}_v$. If the $t \cdot k(k-1)$ numbers arising from taking all possible differences of elements in each set include each non-zero element of $\mathbb{Z}_v$ exactly λ times, then $D_1, D_2, \ldots, D_t$ is called a (v, k, λ)-*difference system.*

For example, $\{1, 3, 9\}, \{2, 5, 6\}$ form a $(13, 3, 1)$-difference system (check this).

Proposition 6.29. *If the sets $D_1, D_2, \ldots, D_t$ form a (v, k, λ)-difference system, then $tk(k-1) = \lambda(v-1)$.*

Proof: Exercise. □

The contrapositive of the above proposition is: *If* $tk(k-1) \neq \lambda(v-1)$, *then there is no* (v, k, λ)*-difference system.*

Proposition 6.29 implies that the number t of sets in a (v, k, λ)-difference system is determined by v, k, and λ. It equals $\frac{\lambda(v-1)}{k(k-1)}$.

Proposition 6.30. *If* $D_1, D_2, \ldots, D_t$ *form a* (v, k, λ)*-difference system, then the* tv *sets* $D_i + j$, $i = 1, 2, \ldots, t$, $j \in \mathbb{Z}_v$, *are the blocks of a* (v, k, λ)*-design.*

Proof: Exercise. □

One use of difference systems is in scheduling round-robin tournaments, that is, tournaments in which every pair of entrants play exactly once. The sets

$$\{1, -1\}, \{2, -2\}, \ldots, \{n-1, n\}$$

are a $(2n-1, 2, 1)$-difference system: The differences are $\pm 2, \pm 4, \ldots, \pm(2n-2)$, respectively, and since $2n-1$ is odd, every non-zero element of $\mathbb{Z}_{2n-1}$ appears in this list exactly once. Since the initial blocks are disjoint, so is each translate obtained by adding the same number to each initial block. Thus, each such set of translates can be viewed as a round. Developing the initial blocks modulo $2n-1$ yields the following schedule:

Round				
1	1 plays $2n-2$	2 plays $2n-3$	...	$n-1$ plays n
2	2 plays 0	3 plays $2n-2$	...	n plays $n+1$
3	3 plays 1	4 plays 0	...	$n+1$ plays $n+2$
$\vdots$	$\vdots$	$\vdots$	...	$\vdots$
$2n-1$	0 plays $2n-3$	1 plays $2n-4$	...	$n-2$ plays $n-1$

This schedule is for a tournament with $2n-1$ entrants. Thus, one entrant sits out in each round. The way we have it set up, entrant i does not play in round i. In order to adapt the above to a schedule for a tournament with $2n$ entrants, add an extra team "∞" and the match "i plays ∞" to the $(i+1)$st round, $0 \leq i \leq 2n-2$. Even though it does not agree with our definition, you might conceptually regard the original $n-1$ sets and $\{0, \infty\}$ as a difference system in $\mathbb{Z}_{2n-1} \cup \{\infty\}$ (with the rule that $\infty + x = \infty$).

A similar result to Proposition 6.25 holds for primes congruent to 1 modulo 4. We state it without proof.

Theorem 6.31. *Let* $p \equiv 1 \pmod 4$ *be prime. Let* S *be the set of non-zero squares and* T *the set of non-squares modulo* p. *Then* S, T *is a* $(p, \frac{p-1}{2}, \frac{p-3}{2})$*-difference system.*

Example 6.32. Consider $p = 13$. The sets of non-zero squares and non-squares in $\mathbb{Z}_{13}$ are $S = \{1, 4, 9, 3, 12, 10\}$ and $T = \{2, 5, 6, 7, 8, 11\}$. So by Theorem 6.31, S, T is a $(13, 6, 5)$-difference system. Developing these initial blocks modulo 13 gives a $(13, 6, 5)$-design.

Exercises

1. (a) Prove Proposition 6.29.

   (b) Prove Proposition 6.30.

   (c) Suppose $D_1, D_2, \ldots, D_t$ is a (v, k, λ)-difference system. Prove that for each $i \in \mathbb{Z}_v$ the sets $D_1 + i, D_2 + i, \ldots, D_t + i$ are also a (v, k, λ)-difference system.

2. Let D be a (v, k, λ)-difference set. Prove that $\overline{D}$ is a $(v, v-k, v-2k+\lambda)$-difference set. (*Hint*: Prove that any non-zero element of $\mathbb{Z}_v$ occurs $2(k-\lambda)$ times as a difference of elements, one in D and one in $\overline{D}$.)

3. Use the Multiplier Theorem to decide whether there exists a difference set with the given parameters.

   (a) $(22, 7, 2)$.

   (b) $(73, 9, 1)$.

   (c) $(56, 11, 2)$.

   (d) $(79, 13, 2)$.

4. Is it true that the collection of sets obtained by complementing each set in a difference system is also a difference system?

5. Suppose a league schedule for $2n$ teams is to be constructed, with each pair of teams playing exactly once. It is desirable that each team should alternate home and away games as much as possible. Define a *break* in this pattern to be a repetition of being home, or of being away, in two consecutive games.

   (a) Show that the league schedule must contain at least $2n - 2$ breaks.

   (b) Show how to construct a schedule with exactly $2n - 2$ breaks.

6.4 Resolvable designs

A (v, k, λ)-design is called *resolvable* if its blocks can be partitioned into r groups (or parallel classes), each of which is a partition of the point set V.

For example, any affine plane is a resolvable $(n^2, n, 1)$-design.

Resolvable designs are inevitably what's required with scheduling problems that require members of a given group to be partitioned into subsets (of the same size) such that every pair of members are in the same group some fixed number of times. An example might be scheduling a golf tournament; the goal would be to partition the entrants into foursomes so that every pair of entrants play together exactly once, say. (Notice that this is the same as the diner club problem discussed earlier.)

Proposition 6.33. *Let $\mathcal{D}$ be a resolvable (v, k, λ)-design. Then $k \mid v$.*

Proof: Exercise. □

The contrapositive of this statement is: *If $k \not| v$, then there is no resolvable (v, k, λ)-design.* Thus, for example, there can not be a resolvable $(11, 5, 2)$-design (even though an $(11, 5, 2)$-design exists). The condition $k \mid v$ is therefore necessary for the existence of a resolvable (v, k, λ)-design. In fact, by Exercise 1, if this condition and $(k-1) \mid \lambda(v-1)$ are satisfied, then so is $k(k-1) \mid \lambda v(v-1)$ (so that the latter condition is not needed). Hence, the necessary conditions for the existence of a resolvable (v, k, λ)-design are $k \mid v$ and $(k-1) \mid \lambda(v-1)$.

The most famous problem about resolvable designs is *Kirkman's Schoolgirls Problem*:

> Fifteen schoolgirls walk each day in five groups of three. Arrange the girls walks for a seven day period so that, in that time, each pair of girls walks together in a group exactly once.

Kirkman posed this problem (and solved it) in 1847. Here is a solution:

Mon:	ABC	DEF	GHI	JKL	MNO
Tue:	ADH	BEK	CIO	FLN	GJM
Wed:	AEM	BHN	CGK	DIL	FJO
Thu:	AFI	BLO	CHJ	DKM	EGN
Fri:	AGL	BDJ	CFM	EHO	IKN
Sat:	AJN	BIM	CEL	DGO	FHK
Sun:	AKO	BFG	CDN	EIJ	HLM

A similar question could be asked in the more general context of resolvable designs. Kirkman's Schoolgirls Problem asks for a resolvable $(15, 3, 1)$-design. One generalisation asks for a resolvable $(3t, 3, 1)$-design. Checking the necessary conditions, we require that $2 \mid 1(3t-1)$. This implies that $3t-1$ is even, and so t is odd. So is possible for a resolvable $(v, 3, 1)$-design to exist only if $v \equiv 3 \pmod 6$. It turns out that they exist in all possible cases. We will not pursue this topic any further.

Exercises

1. Show that the condition $k \mid v$ is necessary for the existence of a resolvable (v, k, λ)-design and, if this condition and $(k-1) \mid \lambda(v-1)$ are satisfied, then so is $k(k-1) \mid \lambda v(v-1)$ (so that the latter condition is not needed).

2. Show that if a (v, k, λ)-design is resolvable and $v > k$, then $b \geq v + r - 1$.

   (*Hint*: in the incidence matrix A, the collections of columns corresponding to the parallel classes all have the same sum; now apply some results from linear algebra to reduce the upper bound on the rank of A.)

3. State and solve the "nine schoolgirls problem", if possible. Do the same for the "12 schoolgirls problem".

4. A group of n, $5 \leq n \leq 22$, golfers is planning a trip that will include one round of golf per day. They wish to schedule their games so that on each day they play in groups of groups of three, and and every pair of golfers plays together the same number of times – and at most twice – during the trip. For what values of n is there a chance that this is possible, and how many games would each golfer play on the trip?

5. Prove that, in a resolvable design, $r \mid b$.

6. A (v, k, λ) design is *affine resolvable* if it is resolvable such that any two blocks in different parallel classes intersect in the same number of points. Show that any resolvable $(2k, k, k-1)$ design is also affine resolvable.

6.5 Steiner triple systems

A *Steiner triple system* of *order* v is a $(v, 3, 1)$-design. (Blocks are often called *triples* in this case.) The purpose of this section is to show these exist whenever the necessary conditions are satisfied. Contrast this with the discussion following Wilson's Theorem. We begin by working out the necessary conditions for $(v, 3, 1)$ designs.

Proposition 6.34. *If there exists a Steiner triple system of order $v > 0$ then $v \equiv 1$ or $3 \pmod 6$.*

Proof: By Corollary 6.6, we must have $2 \mid v - 1$ (so v is odd) and $3 \cdot 2 \mid v(v - 1)$. Since 3 is prime, it divides either v or $v - 1$. So $v \equiv 0$ or $1 \pmod 3$.

So, modulo 6, the only possibilities in which v is odd are $1, 3, 5$. In addition, the case $5 \pmod 6$ can be ruled out by the second condition. □

The following construction is independently due to S. Schreiber (1973) and R.M. Wilson (1974). (This is the same Wilson as in Wilson's Theorem.) It is our first instance of a nontrivial general existence result for designs.

Theorem 6.35. *If $v \equiv 1$ or $3 \pmod 6$, then there exists a Steiner triple system of order v.*

Proof: We may assume $v \geq 3$, for otherwise $v = 1$ and $\mathcal{B} = \emptyset$ is trivially the block set of a Steiner triple system of order 1. Let $n = v - 2$, so that n is odd. To start the construction, take all triples $\{a, b, c\} \subseteq \{0, 1, \ldots, n - 1\}$ such that $a + b + c \equiv 0 \pmod n$. (Since we are selecting 3-subsets, it is required that $a, b,$ and c are all different. Note also that once two elements of a triple are selected, the third is determined.) The triples contain every pair of distinct integers from $\{0, 1, \ldots, n - 1\}$ except $\{x, -2x : x \neq 0\}$ (the third element would need to be x, and we wouldn't get a triple). It remains to add triples so that every element is in a triple with n and $n + 1$ ($v - 2$ and $v - 1$ – remember that the smallest symbol is zero), and all pairs of the form $\{x, -2x : x \neq 0\}$ arise.

The numbers $\{1, 2, \ldots, n - 1\}$ can be partitioned into orbits of the form

$$O_x = \{x, -2x, 4x, \ldots, (-2)^{t-1}x\}.$$

The cases t even and t odd are treated separately.

Suppose $|O_x| = t$ is even. For each orbit O_x, with $|O_x| = t \equiv 0 \pmod 2$, add the triples

$$\{x, -2x, n\}, \{-2x, 4x, n + 1\}, \{4x, -8x, n\}, \{-8x, 16x, n + 1\}, \ldots, \{(-2)^{t-1}x, x, n + 1\}.$$

(The fact that t is even implies that the last triple includes $n+1$ rather than n.)

We now consider the odd orbits. Observe O_{-x} (the orbit containing $-x$) is disjoint from O_x and has the same cardinality. (This is an easy exercise in algebra.) For each odd orbit O_x, add the triples

$$\{-2x, 4x, n\}, \{4x, -8x, n+1\}, \{-8x, 16x, n\}, \ldots, \{(-2)^{t-1}x, x, n+1\}$$

in such a way that if the pair $\{x, -2x\}$ does not occur, then neither does $\{-x, 2x\}$. This is possible since x and $-x$ never belong to the same orbit. (The fact that t is odd and that there is no triple containing x and $-2x$ implies that the last triple includes $n+1$ rather than n.) These triples do not contain some pairs of the form $\{y, -2y\}$. Further, any such y does not appear in a triple with n, and $-2y$ does not appear in a triple with $n+1$. For each such y, remove the triples $\{y, -y, 0\}$ and $\{2y, -2y, 0\}$ added earlier, add the triples $\{y, -2y, 0\}$, $\{-y, 2y, 0\}$ and also the triples $\{y, -y, n\}$, $\{2y, -2y, n+1\}$.

To complete the construction, add the triple $\{0, n, n+1\}$. It is left to the reader to check that this set of triples contains every pair exactly once. □

We illustrate the construction with two examples.

Example 6.36. Suppose $v = 9$. Then $n = 7$. The construction begins with the triples (with brackets omitted): 016, 025, 034, 124, 356. The powers of $(-2) \equiv 5 \pmod 7$ are $5, 4, 6, 2, 3, 1$, so that the integer t in the proof is 6. Following the construction in this case, and using $x = 1$, we add the triples: 157, 548, 467, 628, 237, 318. Finally, we add 078 to obtain our Steiner triple system of order 9:

$$016, 025, 034, 124, 356, 157, 548, 467, 628, 237, 318, 078.$$

Example 6.37. Now suppose $v = 13$. Then $n = 11$. The construction begins with the triples (with brackets omitted and using A for 10):

$$01A, 029, 038, 047, 056, 128, 137, 146, 236, 245, 39A, 48A, 57A, 589, 679$$

The powers of $(-2) = 9 \pmod{11}$ are $9, 4, 3, 5, 1$ so that so that the integer t in the proof is 5. The sets in the partition of $\{1, 2, \ldots, 10\}$ are $\{1, 3, 4, 5, 9\}$ and $\{10, 2, 6, 7, 8\}$. Using $x = 1$ and $-x = 10$, we add the triples (where B is used for 11, and C is used for 12): $94B, 43C, 35B, 51C$ and then $27B, 78C, 86B, 6AC$. The pairs of the form $\{y, -2y\}$ that are missing are $\{1, 9\}$ and $\{2, 10\}$, so we delete the triples $01A$ and 029 added earlier, and add the triples $190, 20A, 1AB$, and $92C$. Finally, the triple $0BC$ is added to obtain the Steiner triple system of order 13:

$$038, 047, 056, 128, 137, 146, 236, 245, 39A, 48A, 57A, 589, 679,$$

$$94B, 43C, 35B, 51C, 27B, 78C, 86B, 6AC, 190, 02A, 1AB, 92C, 0BC.$$

In practice, a "random" Steiner triple system of large order v is often found on computer using a technique known as *hill-climbing.* In this algorithm, we repeatedly pick triples $\{x, y, z\}$ at random and add to the current collection of triples whenever none of the pairs $\{x, y\}$, $\{x, z\}$, $\{y, z\}$ are covered so far. If two or more of these pairs are covered, we reject $\{x, y, z\}$ and pick a new triple. However, if exactly one of these pairs, say $\{x, y\}$ is already covered, locate the unique block in our current collection containing this pair and *replace* it by the new triple $\{x, y, z\}$. Hill-climbing is remarkably successful in generating Steiner triple systems of large orders (at least $v \approx 10^4$) in no more than a few seconds on modern computers. However, the algorithm is probabilistic and has no guaranteed running time.

Let $(V, \mathcal{B})$ be a Steiner triple system. A *subsystem* of it is a Steiner triple system $(U, \mathcal{A})$ with $U \subseteq V$ and $\mathcal{A} \subseteq \mathcal{B}$. This next fact says that (proper) subsystems cannot be too large.

Proposition 6.38. *If any Steiner triple system of order v contains a subsystem of order u, then either $u = v$ or $2u < v$.*

Proof: Exercise. □

In fact, there is a converse to Proposition 6.38 known as the Doyen-Wilson Theorem. (yes, the same Wilson again!)

Exercises

1. In the beginning of the proof of Theorem 6.35, how many triples $\{a, b, c\} \subset \mathbb{Z}_n$ with $a + b + c \equiv 0 \pmod{n}$ are there?

2. Use the construction in Theorem 6.35 to give a Steiner triple system of order 15 and 19.

3. (a) Let $v \equiv 1$ or $3 \pmod{6}$, and let $\mathcal{S}$ be a Steiner triple system of order v. Define a $v \times v$ array L by setting its (i, j)-entry equal to i if $i = j$, and equal to the unique x such that $\{i, j, x\}$ is a block of $\mathcal{S}$. Prove that L is a *symmetric* Latin square (*i.e.* $L = L^\top$).

   (b) Can the construction in (a) be reversed to obtain a Steiner triple system of order v from a symmetric Latin square L of order v with $\ell_{ii} = i,\ 1 \leq i \leq v.$?

4. Prove Proposition 6.38.

5. Explain how to construct a Steiner triple system of order 21 which contains three subsystems of order 7 on disjoint sets of points. (*Hint*: use a Latin square of order 7.)

Chapter 7

Codes

7.1 Basic properties

In a basic model of a communication system there is a source that produces some sort of data that is to be sent to a receiver. A typical first step in this process is for the data to transformed into binary digits (*bits*), with strings of several bits representing one piece of data. If there are at most k different pieces of data, then $\lceil \log_2(k) \rceil$ bits are necessary in order for each of these to correspond to different binary strings. For example, $\lceil \log_2(26) \rceil = 5$ bits are required if the data is the 26 letters of the alphabet. In practice, we don't use the minimum possible number of bits to represent the data. More about this below.

We make the following assumptions about the communication system.

- If n bits are transmitted, then n (possibly different) bits are received.
- Each bit has exactly the same probability of being altered in transmission.

A *binary word* (or *word*) of *length* n is a finite sequence of bits $(b_1, b_2, \ldots, b_n)$, where $b_i \in \{0, 1\}$ for $i = 1, 2, \ldots, n$. We will normally drop the brackets and commas and simply write $b_1 b_2 \ldots b_n$. For example we will usually write 001101 instead of $(0, 0, 1, 1, 0, 1)$. Since we will be using some linear algebra it is important to bear in mind that words are really vectors.

A *code* is a set of words. The words belonging to some code we are talking about are usually called *codewords*.

We will only be concerned with *binary block codes*: sets of binary codewords all having the same length. (The number of symbols in each codeword is called the *length* of the code. This is the same as the length of a codeword, defined above.)

Suppose k pieces of data are to be transmitted. Then, a code C with at least k codewords is needed. Typically the codewords have more than $\lceil \log_2(k) \rceil$ bits, the extra bits being useful in handling errors that might occur in transmission. The "encoding" of the information to be transmitted amounts to forming a 1-1 correspondence between the binary data and a subset of the codewords in C. The exact means of doing this depends on the code and the application. Since there is a cost of transmitting extra information, one would like to use codes with as small a length as possible.

Suppose a codeword is transmitted. If the received word is not a codeword, then errors have definitely occurred. If the received word is a codeword, then it could be that no errors have occurred, or that several errors – changing the codeword into a different codeword – have occurred.

One simple way to add redundancy to help with error handling is to form the codewords by repeating each piece of data three times. For example, consider the repetition code

$$C_1 = \{000000, 010101, 101010, 111111\}.$$

Since at least three errors must occur to change one codeword into another, all combinations of two or fewer errors can be detected (because what's received is not a codeword). Combinations of three or more errors may not be detectable. If the received word is not a codeword, it can be decoded by breaking it into three pieces and using majority rule. This method will result in correct decoding if at most one error occurs in transmission, and may result in incorrect decoding if two or more errors occur in transmission. Suppose the codeword 101010 is sent. If one error occurs in transmission and 111010 is received, then comparing 11, 10, and 10 leads to it being correctly decoded as 101010. If two errors occur in transmission so that 011010 is received, it is still decoded correctly by this rule. But, if two errors occur so that 000010 is received, it is incorrectly decoded as 000000. Thus, with this decoding scheme, the code C_1 can be used to correct any single error but not combinations of two or more errors.

Consider starting with the four bit strings of length two and adding a third bit to make the number of 1s in each codeword even (this is an example of a *parity check* bit). This results in the code

$$C_2 = \{000, 011, 101, 110\}.$$

By inspection, no two codewords differ in exactly one bit. Thus, all single errors can be detected (and no more). The code C_2 can not correct any errors: if 010 is received then any of 000, 110, or 011 could have been sent with one error occurring in transmission.

If u and v are binary words of length n, we define $u + v$ to be the binary word obtained by componentwise addition modulo 2. For example $01101 + 11001 = 10100$.

The componentwise binary addition defined above can be interpreted as exclusive or. Note that $u + v$ is only defined in the case that u and v have the same length. Note also that this operation is commutative ($u + v = v + u$) and associative ($u + (v + w) = (u + v) + w$, hence we can omit the brackets and write $u + v + w$).

The (*Hamming*) *weight* of a binary word v, denoted $\mathrm{wt}(v)$ is the number of times the digit 1 occurs in v. For example, $\mathrm{wt}(110101) = 4$ and $\mathrm{wt}(00000) = 0$.

Let u and v be binary words of length n. The (*Hamming*) *distance* between u and v, denoted $d(u, v)$ is the number of positions in which u and v disagree.

Note that $d(u, v)$ is only defined in the case that u and v have the same length, and that $d(u, v) = \mathrm{wt}(u + v)$.

For example, $d(01011, 00111) = 2 = \mathrm{wt}(01011 + 00111) = \mathrm{wt}(01100)$.

Proposition 7.1. *Let u, v and w be binary words of length n. Then,*

1. $d(u, w) = 0$ *if and only if* $u = w$.

2. $d(u, w) = d(w, u)$.

3. $d(u, w) \leq d(u, v) + d(v, w)$.

Proof: Exercise. □

For a code C with at least two codewords, the *minimum distance* of C is the smallest of the numbers $d(u, w)$ over all pairs u, w of distinct codewords in C.

For example, let $C = \{0000, 1010, 0111\}$. Then, $d(0000, 1010) = 2$, $d(0000, 0111) = 3$, and $d(1010, 0111) = \mathrm{wt}(1101) = 3$, so the minimum distance of C is 2.

The minimum distance of a code is important with respect to error detection and correction since it is the minimum number of errors that must occur in order to transform one codeword into another.

Suppose a codeword u is sent and a word w, which may or may not be a codeword, is received. There is a question of how w should be interpreted (*decoded*). If the code is being used for error detection only, then a reasonable rule is: if w is a codeword, then assume that w was sent; otherwise, errors are detected so request retransmission. The rule most commonly employed when codes are used for error correction is called *incomplete maximum likelihood decoding* (IMLD): if there exists a (unique) codeword v such that $d(v, w) < d(x, w)$ for all codewords $x \neq v$, then assume that v was sent and decode w as v; otherwise (a tie occurs), request retransmission.

The protocols described in the previous paragraph make a distinction between error detection and error correction. Consider the code $C = \{000, 111\}$. Suppose 000 is sent and 110 is received, so that the two errors that occurred are detected. (More accurately, errors are detected. There is no way to know how many have occurred.) Since the receiver does not know which codeword was sent (if he did, the code is unnecessary!), there is no way to know how many errors have actually occurred. Using IMLD the received word is incorrectly decoded as 111, which implicitly assumes that only one error has occurred.

Let C be a code. If a codeword $v \in C$ is sent and a word w is received, then we say the *error pattern* $e = v + w$ has occurred. For instance, if $1100 \in C$ is sent and 1001 is received, then the error pattern is $e = 1100 + 1001 = 0101$. The error pattern is the binary word with 1s in the positions where errors have occurred and 0s elsewhere.

A code $C \subset \mathbb{Z}_2^n$ is said to *detect* error pattern e if for every $v \in C$, we have $v + e \notin C$. Say that a code C *detects all combinations of t or fewer errors* if it detects every non-zero error pattern e with $\mathrm{wt}(e) \leq t$.

Theorem 7.2. *A code C detects all combinations of t or fewer errors if and only if the minimum distance of C is at least $t + 1$.*

Proof: ($\Leftarrow$) Suppose the minimum distance of C is at least $t + 1$. If a codeword is sent and $1 \leq s \leq t$ errors occur, then the received word is not a codeword. Thus, the errors are detected.

($\Rightarrow$) Suppose C can detect all combinations of t or fewer errors. Then no combination of t or fewer errors can transform a codeword into a different codeword. This implies that no two different codewords differ in t or fewer positions. Therefore C has minimum distance at least $t+1$. □

A code C is called a *t-error detecting code* if it can detect all combinations of t or fewer errors, but not all combinations of $t+1$ errors.

Consider the code $C = \{0011, 0101, 1001, 0110, 1010, 1100\}$, which has minimum distance two (check this). By Theorem 7.2, the code C can detect all single errors. Since there exists a combination of two errors that will transform the codeword 0011 into the codeword 0101 (corresponding to the error pattern 0110), the code C is a 1-error detecting code.

Corollary 7.3. *A code C is t-error detecting if and only if its minimum distance equals $t+1$.*

A code C can *correct* error pattern e if, for all distinct $v, w \in C$, we have $d(v+e, v) < d(v+e, w)$. (Thus IMLD results in $v+e$ being correctly decoded as v.) A code C *corrects all combinations of t or fewer errors* if it corrects all error patterns e with $\mathrm{wt}(e) \leq t$.

Theorem 7.4. *A code C can correct all combinations of t or fewer errors if and only if the minimum distance of C is at least $2t+1$.*

Proof: ($\Rightarrow$) We prove the contrapositive. Suppose the minimum distance of C is $\ell \leq 2t$, and let u and v be codewords so that $d(u, v) = \mathrm{wt}(u+v) = \ell$. Let e be obtained from $u+v$ by changing some 1s to 0s, so that $\mathrm{wt}(e) = \lceil \ell/2 \rceil \leq t$. Suppose $u \in C$ is transmitted and $u+e$ is received. Then $d(u, u+e) = \lceil \ell/2 \rceil = \mathrm{wt}(e)$, and $d(v, u+e) = \mathrm{wt}(v+u+e) = \ell - \lceil \ell/2 \rceil = \lfloor \ell/2 \rfloor$. That is, the received word $u+e$ is at least as close to v as it is to u, so C does not correct the error pattern e.

($\Leftarrow$) Suppose C has minimum distance at least $2t+1$, and let e be a non-zero error pattern of weight at most t. Suppose $u \in C$ is transmitted and $u+e$ is received. Then, for any $w \in C$ with $w \neq u$,

$$d(u, u+e) \leq t < 2t + 1 - \mathrm{wt}(e) \leq d(w, u) - d(u+e, u) \leq d(u+e, w),$$

where the last step is from the triangle inequality. Thus, $u+e$ is closer to u than to any other codeword w, so C corrects the error pattern e. □

A code C is called a *t-error correcting code* if it can correct all combinations of t or fewer errors, but not all combinations of $t+1$ errors.

For example, the repetition code C_1 is a 1-error correcting code.

Corollary 7.5. *A code C is t-error correcting if and only if its minimum distance equals $2t+1$ or $2t+2$.*

The above results imply that large minimum distance is a desirable feature of a code. By repeating the data several times in forming the codewords (*i.e.* using a repetition code), the minimum distance can be made as large as desired. However, the length of such a code is large, and there is a cost associated with transmitting each bit. Thus, one would like codes with relatively small length (but still many codewords). So, one is led to searching for codes that somehow balance the conflicting goals of having large minimum distance and many codewords but small length.

For each word $v \in C$, define the set $B_t(v) = \{w \in \{0,1\}^n : d(v,w) \leq t\}$. This is usually called the *ball of radius t about v*. Observe that the number of words which differ from v in exactly i places is $\binom{n}{i}$ (choose i positions and complement those bits), so the number of words that differ from v in at most t positions is $|B_t(v)| = \binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{t}$. Notice that $|B_t(v)|$ is independent of the "centre" v.

Theorem 7.6. (The Hamming bound) *Suppose C is a code of length n with minimum distance $2t+1$ or $2t+2$. Then,*

$$|C| \leq \frac{2^n}{\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{t}}.$$

Proof: First, notice that no binary word w of length n is at distance less than or equal to t from two different codewords: if $u, v \in C$ with $d(w,u) \leq t$ and $d(w,v) \leq t$, then $d(u,v) \leq d(u,w) + d(w,v) \leq t + t = 2t$, a contradiction.

By the argument above, each word in $\mathbb{Z}_2^n$ belongs to at most one set $B_t(v)$, $v \in C$. Therefore,

$$|C| \cdot |B_t(0)| = \sum_{v \in C} |B_t(v)| \leq |\mathbb{Z}_2^n| = 2^n,$$

from which the result follows by division. □

For example, according to the Hamming bound a code with length 6 and minimum distance $3 = 2 \cdot 1 + 1$ has at most $2^6 / \left(\binom{6}{0} + \binom{6}{1}\right) \approx 9.14$ codewords. Since the number of codewords must be an integer, it has at most 9 codewords.

The Hamming bound gives an upper bound on the size of a code with given length and minimum distance. It does not say that the upper bound can be achieved.

A code C with length n and minimum distance $2t+1$ or $2t+2$ is called *perfect* if $|C| = \frac{2^n}{\binom{n}{0}+\binom{n}{1}+\cdots+\binom{n}{t}}$.

That is, a code is perfect if equality holds in the Hamming bound. A perfect code has the maximum possible number of codewords of any code of its length. Following the proof of the Hamming bound, this means that the balls of radius d about the codewords form a partition of $\{0,1\}^n$. Further, in order for equality to hold $\binom{n}{0}+\binom{n}{1}+\cdots+\binom{n}{d}$ must be a power of 2. It turns out that only codes of odd minimum distance can be perfect. The proof of this fact is an exercise.

The examples described in this paragraph are known as the *trivial perfect codes*. First, the set $\{0,1\}^n$ is a perfect code. Its minimum distance is $1 = 2\cdot 0+1$ and the number of codewords is $2^n/\binom{n}{0} = 2^n$. Second, when the length of the codewords is $n = 2t+1$, the code $C = \{00\cdots 0, 11\cdots 1\}$ is perfect as it has $2 = \frac{2^n}{2^{n-1}} = \frac{2^n}{\binom{n}{0}+\binom{n}{1}+\cdots+\binom{n}{t}}$ codewords. (The fact that when $n = 2t+1$, $\binom{n}{0}+\binom{n}{1}+\cdots+\binom{n}{t} = 2^{n-1} = \frac{1}{2}2^n$ follows from the binomial theorem and $\binom{n}{k} = \binom{n}{n-k}$.)

Theorem 7.7. (Tietävären and van Lint, 1973) *If C is a non-trivial perfect code of length n and minimum distance d, then either*

- $d = 3$ *and* $n = 2^r - 1$ *for some* $r \geq 3$, *or*
- $d = 7$ *and* $n = 23$.

Perfect codes with the parameters described in the theorem exist in all possible cases. The Hamming codes studied later have the parameters with $d = 3$. The Golay code, which we will not study, has $d = 7$ and $n = 23$.

Exercises

1. Let C be the set of characteristic vectors of the blocks of a $(v,k,1)$-design. Prove that C is a $(2k-3)$-error detecting code. (See chapter 1 for a definition of characteristic vector of a subset.)

2. Let C be a binary code of length n. We define the *information rate* of C to be the number $i(C) = \frac{1}{n}\log_2(|C|)$. (This quantity is a measure of the proportion of each codeword that is carrying the message, as opposed to redundancy that has been added to help deal with errors.) Prove that if C is a binary code, then $0 \leq i(C) \leq 1$.

3. Suppose the code C contains all of the binary words of length 11. Assume that bits are transmitted at the rate 10^7 bits per second and that each bit is received correctly with probability $p = 1 - 10^{-8}$, independently of what happens with any other bit.

   (a) What is the probability that a word is transmitted incorrectly and the errors are not detected?

   (b) If bits are transmitted all the time (the channel is in constant use), about how many words are (probably) transmitted incorrectly each day?

   Now suppose the code C' is obtained from C by adding an extra (parity check) digit to the words in C, so that the number of 1s in each codeword is even. Repeat (a) and (b) above for C'. If the channel is in constant use, about how long do you expect must pass between undetected incorrectly transmitted words? Express your answer as a number of days.

4. Establish the following three properties of the Hamming distance between words u, v, and w in a code C:

   (a) $d(u, w) = 0$ if and only if $u = w$.

   (b) $d(v, w) = d(w, v)$.

   (c) $d(v, w) \leq d(v, u) + d(u, w)$.

5. Suppose a code is being used for error correction, and also to detect errors that can not be unambiguously corrected. Prove that a it can correct all error patterns of weight at most s, and detect all non-zero error patterns of weight $s + 1$ to t (where $s \leq t$) if and only if it has minimum distance at least $s + t + 1$. (For example, consider $C = \{000, 111\}$. This single error correcting code detects all non-zero error patterns of weight at most 2. But, if 000 is sent and 110 is received, then only one error is detected and the received word is incorrectly decoded as 111. The ambiguity here is that it is not clear whether the error pattern is 110 or 001.)

6. Let $C = \{001, 101\}$. Suppose a codeword x is sent and the error pattern 011 occurs. Can the received word be decoded correctly? Explain.

7. Let C be the code that consists of all binary words of length 8 and even weight. Construct a code C' by adding two bits to each word in C so that the weight of each codeword is a multiple of 4. Is it true that C' is a 1-error correcting code? Explain your answer in detail.

8. Prove that no code with even minimum distance can be perfect.

9. Prove that there is a binary code C of length n and minimum distance d with
$$|C| \geq \frac{2^n}{\sum_{i=0}^{d-1} \binom{n}{i}}.$$
(*Hint:* think of a stupid algorithm for constructing such a code.)

7.2 Linear codes

Two more of the main issues in coding theory are easy encoding of data and fast decoding of messages. These are usually accomplished by using codes with some underlying algebraic structure.

A code C is called a *linear code* if $u + v \in C$ whenever u and v are in C.

The code $C_1 = \{0000, 1001, 0110, 1111\}$ is linear (check this). The code $C_2 = \{000, 111, 001, 101\}$ is not linear because $001, 101 \in C$ but $001 + 101 = 100 \notin C$.

It is easy to determine how many errors can are detected or corrected by a linear code.

Lemma 7.8. *The minimum distance of a linear code is the smallest weight of a non-zero codeword.*

Proof: Exercise. □

By the above theorem, the minimum distance can be determined by examining the weight of the $|C|$ codewords instead of checking the $\binom{|C|}{2}$ pairs of distances between distinct codewords.

Let $(b_1, b_2, \ldots, b_n)$ be a binary word. We define *scalar multiplication* by the elements of $\{0, 1\}_2$ by $1(b_1, b_2, \ldots, b_n) = (b_1, b_2, \ldots, b_n)$ and $0(b_1, b_2, \ldots, b_n) = (0, 0, \ldots, 0)$. (That is $1w = w$ and $0w$ is the word of all zeros.)

The set $\mathbb{Z}_2^n$ of all binary words of length n, together with scalar multiplication by the elements of $\mathbb{Z}_2$ and componentwise addition modulo 2, is a vector space.

Proposition 7.9. *Let C be a linear code of length n. Then C, together with scalar multiplication and componentwise addition modulo 2, is a subspace of $\mathbb{Z}_2^n$. Conversely, any subspace of $\mathbb{Z}_2^n$ is a linear code.*

Proof: Exercise. □

By Proposition 7.9, a linear code C is a vector space, specifically a subspace of some $\mathbb{Z}_2^n$. We know from linear algebra that every vector space has a basis, and that any two bases contain the same number of elements.

The *dimension* of a linear code C, denoted by $dim(C)$, is the dimension of C as a vector space.

For example, the linear code C_1 above has dimension two and $\{1001, 0110\}$ is a basis.

Since we are talking only about scalar multiplication by elements of $\mathbb{Z}_2$, it follows that $dim(C) = k$ if there exists a subset $B = \{v_1, v_2, \ldots, v_k\} \subseteq C$ such that every element of C can be written as a sum of elements of B, and there is no smaller subset of C with this property.

Let $S = \{x_1, x_2, \ldots, x_t\} \subseteq \mathbb{Z}_2^n$. The *linear code generated by* S, denoted $\langle S \rangle$, is defined by

$$\langle S \rangle = \{w : w = \alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_t x_t,\ \alpha_i \in \mathbb{Z}_2,\ 1 \leq i \leq t\}.$$

(That is $\langle S \rangle$ is the set of all vectors (codewords) that can be written as a sum of vectors in S. We know from linear algebra that $\langle S \rangle$ is a subspace of $\mathbb{Z}_2^n$, so the use of the term "linear" is justified. Also, note that the dimension of $\langle S \rangle$ may be less than t – there is no requirement that S be a linearly independent set.)

The linear code $\langle S \rangle$ is the set of all vectors (codewords) that can be written as a sum of vectors in S. In order to find the dimension of $\langle S \rangle$, construct a matrix A whose rows are the elements of S and use Gaussian elimination to put A into row-echelon form. The non-zero rows of this matrix form a basis for $\langle S \rangle$, so $dim(C)$ is the number of non-zero rows. Here's an explanation of why that works. Each step of this process involves replacing a row by a linear combination of rows, *i.e.* by a vector in $\langle S \rangle$. Since the rows of A are the elements of S, the rows of any matrix obtained from A by elementary row operations are linear combinations of elements of S. Further, the elementary row operations tell how the elements of S are all obtainable as linear combinations of these rows. Thus, any vector that can be formed as a linear combination of elements of S can be formed as linear combinations of rows of any matrix constructed from A using elementary row operations. The rows of this matrix (in row-echelon form) are linearly independent, and are formed by taking linear combinations of elements of S. It follows that the set B of non-zero rows of the row-echelon form of A is a set of linearly independent elements of $\langle S \rangle$ with the property that every element of $\langle S \rangle$ is a linear combination of elements of B. That is, B is a basis for $\langle S \rangle$.

For example, let $S = \{11101, 10110, 01011, 11010\}$. Then, up to the order of the rows, the matrix A discussed above is

$$A = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 \end{bmatrix}.$$

Applying Gaussian elimination, we find

$$\begin{bmatrix} 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 \end{bmatrix} \to \begin{bmatrix} 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{bmatrix} \to \begin{bmatrix} 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

The last of these matrices is in row-echelon form. Thus, a basis for $\langle S \rangle$ is

$$B = \{11101, 01011, 00111\}$$

and $dim(\langle S \rangle) = 3$.

Proposition 7.10. *A linear code of dimension k contains exactly 2^k codewords.*

Proof: Suppose C has dimension k and let $B = \{v_1, v_2, \ldots, v_k\}$ be a basis for C. Then, each codeword $w \in C$ can be uniquely written as

$$w = \alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_k v_k,$$

where $\alpha_i \in \mathbb{Z}_2$ for $i = 1, 2, \ldots, k$. Since there are two choices for each scalar α_i, there are 2^k choices for the k-tuple $(\alpha_1, \alpha_2, \ldots, \alpha_k)$, and each of these gives rise to a different codeword. □

Suppose C is a linear code of length n and let $B = \{v_1, v_2, \ldots, v_k\}$ be a basis for C. A *generator matrix for* C is a $k \times n$ matrix G whose rows are the basis vectors (codewords) $v_1, v_2, \ldots, v_k$.

A linear code C can have many different generator matrices, hence we refer to "a" generator matrix (as opposed to "the" generator matrix). Note that the dimension of the code C equals the number of rows in a generator matrix, and the length of C equals the number of columns in a generator matrix.

A generator matrix provides an easy way to encode data. Let G be a generator matrix for C. Referring to the proof of Proposition 7.10, the word $w = (\alpha_1, \alpha_2, \ldots, \alpha_k)G$

and every codeword arises in this way for some choice of $(\alpha_1, \alpha_2, \ldots, \alpha_k)$. Thus, suppose the binary words of length k correspond to data (information). Then each piece of data $(\alpha_1, \alpha_2, \ldots, \alpha_k)$ can be encoded as a codeword in C via matrix multiplication by computing $(\alpha_1, \alpha_2, \ldots, \alpha_k)G$.

Continuing with the example just before Proposition 6.9, a generator matrix for $C = \langle S \rangle$ is

$$G = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{bmatrix}.$$

Now suppose we have the following correspondence between alphabetic characters and binary words of length three:

A: 000 E: 001 H: 010 K: 011 L: 100 M: 101 P: 110 X: 111

Then, the message HELP is encoded as a sequence of four codewords in C by computing

$$(0,1,0)G = 01011, \quad (0,0,1)G = 00111, \quad (1,0,0)G = 11101, \quad (1,1,0)G = 10110.$$

Since elementary row operations transform vectors in $\langle S \rangle$ to other vectors in $\langle S \rangle$, *any linear code has a generator matrix in reduced row echelon form* (RREF). For the example above, a generator matrix in RREF is

$$G' = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{bmatrix}.$$

It is important to notice that the choice of generator matrix determines the encoding of a message. The message HELP will be encoded differently if G' is taken as the generator matrix (for example, look at the codeword that represents "L").

Recall from linear algebra that two vectors $u = (u_1, u_2, \ldots, u_n)$ and $v = (v_1, v_2, \ldots, v_n)$ are called *orthogonal* if the *dot product* $u \cdot v = u_1v_1 + u_2v_2 + \cdots + u_nv_n$ equals zero. (The addition here takes place in $\mathbb{Z}_2$.)

For a subset $S \subseteq \mathbb{Z}_2^n$ we say that a vector w is *orthogonal to* S if it is orthogonal to every vector in S. The *orthogonal complement* of S, denoted $S^\perp$, is the set of all vectors orthogonal to S.

Recall from linear algebra that if V is a vector space and $S \subseteq V$, then $S^\perp$ is a subspace of V. So by Proposition 7.9, the orthogonal complement of any code is also a linear code. The *dual code* of a linear code C is the linear code $C^\perp$.

Example 7.11. Let $S = \{0100, 0101\}$. Then,

$$C = \langle S \rangle = \{0000, 0100, 0101, 0001\}.$$

To find $C^{\perp}$ we need to find all words $w = x_1x_2x_3x_4$ such that $w \cdot 0100 = 0$ and $w \cdot 0101 = 0$ (if w is orthogonal to every vector in S then it is orthogonal to every linear combination of vectors from S). The equation $w \cdot 0100 = 0$ implies $x_2 = 0$ and, using this, the equation $w \cdot 0101 = 0$ then implies that $x_4 = 0$. Thus, $C^{\perp}$ is the set of words where x_1 and x_3 are arbitrary and x_2 and x_4 are zero. That is

$$C^{\perp} = \{0000, 0010, 1000, 1010\}.$$

Proposition 7.12. *Let C be a linear code of length n. Then $(C^{\perp})^{\perp} = C$.*

Proof: Let $w \in C$. By definition of $C^{\perp}$, for any $x \in C^{\perp}$ the dot product $w \cdot x = 0$. Thus, w is orthogonal to every vector in $C^{\perp}$, so that $w \in (C^{\perp})^{\perp}$ and hence $C \subseteq (C^{\perp})^{\perp}$. We know from linear algebra that $dim(C) + dim(C^{\perp}) = n$. Thus $dim(C^{\perp}) + dim((C^{\perp})^{\perp}) = n$, so that $dim(C) = dim((C^{\perp})^{\perp})$. Since $C \subseteq (C^{\perp})^{\perp}$, it now follows that $C = (C^{\perp})^{\perp}$. □

Corollary 7.13. *Let C be a linear code, and let H be a generator matrix for $C^{\perp}$. Then $w \in C$ if and only if $Hw^{\top} = 0$ (the zero vector of length $n - k$).*

Proof: ($\Rightarrow$) Suppose $w \in C$. Then w is orthogonal to every word in $C^{\perp}$. Since the rows of H form a basis for $C^{\perp}$, and the i-th component of $Hw^{\top}$ is the dot product if w and the i-th row of H, we have that $Hw^{\top} = 0$.

($\Leftarrow$) Suppose $Hw^{\top} = 0$. Then (as above) w is orthogonal to every vector in a basis for $C^{\perp}$. Hence (by linearity of the dot product), w is orthogonal to every linear combination of these vectors, that is, to every vector in $C^{\perp}$. Thus $w \in (C^{\perp})^{\perp} = C$. □

A matrix H with the property that $Hw^{\top} = 0$ if and only if $w \in C$ is called a *parity check matrix for C*. (Note: Other formulations of this definition appear in various texts. Sometimes these involve the transpose of our matrix.)

By Corollary 7.13, every linear code has at least one parity check matrix – any generator matrix for $C^{\perp}$ will do. In the proof of Proposition 7.12 we used that if C has length n then $dim(C) + dim(C^{\perp}) = n$. The dimension of $C^{\perp}$ is the number of rows in a generator matrix for $C^{\perp}$. Thus, if C has dimension k (so that $C^{\perp}$ has dimension $n - k$), a parity check matrix for C has $n - k$ rows (and n columns).

Just as generator matrices provide a mechanism for easy encoding of data (via matrix multiplication), parity check matrices provide a simple mechanism for checking if a received word w is a codeword – just compute $Hw^\top$ and see if the result is zero.

Given either a generator matrix or a parity check matrix for a linear code, it is easy to obtain the other. (One procedure for doing this is described below.) Thus, *a linear code can be described by giving a generator matrix, or a parity check matrix.*

Two codes C_1 and C_2 (both of length n) are called *equivalent* if there exists a permutation of the n digits that, when applied to the words in C_1, gives C_2.

That is, two codes are equivalent if each can be obtained from the other by permuting the bit positions. The same permutation must be applied to each word. Equivalent codes are exactly the same, apart from the order of the digits. They have the same length, minimum distance, error correcting and detecting properties, etc.

For example, Let C_1 be the linear code with generator matrix $G_1 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$, so that $C_1 = \{000, 100, 001, 101\}$. Let C_2 be obtained from C_1 by exchanging the second and third digits. Thus, $C_2 = \{000, 100, 010, 110\}$. A generator matrix for C_2 can be obtained by exchanging the second and third columns of G_1, as this is equivalent to exchanging the second and third digits in the vectors in a basis (and hence all linear combinations of these vectors). It follows that $G_2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$ is a generator matrix for C_2.

Proposition 7.14. *Let C be a linear code. Then C is equivalent to a linear code with a generator matrix in the standard form $[I_k|X]$.*

Proof: The code C has a generator matrix G which can be put into RREF using Gaussian elimination. If G is in standard form, the proof is complete. Otherwise, the columns of G can be permuted to give a matrix G_1 in standard form. Since the code C_1 for which G_1 is the generator matrix is equivalent to C, the proof is compete. □

An advantage of having a generator matrix in standard form is easy encoding of data and easy interpretation of codewords. Suppose $G = [I_k|X]$ is a generator matrix for C. Then, for any k bit (data) word a, we have $aG = [aI_k|aX]$. (Hence only the second multiplication is necessary.) From this it is clear that the first k bits of the codeword carry the data (these are sometimes called the *data bits*), and the remaining $n-k$ bits are determined by the matrix X and are there to assist in error correction/detection (these are sometimes called the *parity check bits*). For example, consider the generator matrix

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{bmatrix}.$$

Then, $(\alpha_1, \alpha_2, \alpha_3)G$ is the vector

$$(\alpha_1, \alpha_2, \alpha_3, \alpha_2 + \alpha_3, \alpha_1 + \alpha_2 + \alpha_3).$$

The first three positions in this vector are just the data. The last two positions are determined by the 1s in the data. The fourth position is the parity of the number of 1s in the last two bits in the data (it equals 1 if and only if the number of 1s among α_2 and α_3 is odd), and the fifth position is the parity of the number of 1s in the data.

There is an easy algorithm for finding a parity check matrix given a generator matrix in standard form, and the process can be used in the other direction too. Suppose G is a generator matrix for C, in the standard form $G = [I_k|X]$ (where k is the dimension of C, so that X is a $k \times (n-k)$ matrix). Then $H = [X^\top|I_{n-k}]$ is a parity check matrix for C. To see this, observe that $HG^\top = X^\top I_k + I_{n-k}X^\top = 0$, so that if $w = aG \in C$, then $Hw^\top = H(aG)^\top = HG^\top a^\top = 0a^\top = 0$, where 0 denotes the zero matrix or zero vector, as appropriate.

The above construction is reversible: given a parity check matrix for C we can obtain a generator matrix for C. First, use Gaussian Elimination put the parity check matrix into the form $[X^\top|I_{n-k}]$ (if possible – a rearrangement of columns may be required; more on this below). This does not change the fact that it is a parity check matrix for C as it remains a generator matrix for $C^\perp$. Then, a generator matrix is $G = [I_k|X]$.

If the code C_1 does not have a generator matrix in standard form, the above procedure can still be used. Let G_1 be a generator matrix for C_1 in RREF. Permute the columns of G_1 to obtain a generator matrix G_2 (for an equivalent code) in standard form. Next, apply the construction to obtain a parity check matrix H_2 for the equivalent code. Now apply the inverse permutation to the columns of H_2 and obtain a parity check matrix H_1 for C_1. A similar construction can be applied to obtain a generator matrix when starting with a parity check matrix.

To illustrate this process, suppose C_1 is the code with generator matrix

$$G_1 = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \end{bmatrix}.$$

Listing the columns of G_1 in the order $7, 6, 3, 5, 4, 2, 1$ gives the matrix

$$G_2 = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix},$$

which is in standard form. A parity check matrix for this equivalent code is

$$H_2 = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}.$$

With respect to the original code C_1, the bits of the equivalent code are listed in the order $7, 6, 3, 5, 4, 2, 1$. Rearranging the columns of H_2 so that the bits are listed in the order $1, 2, 3, 4, 5, 6, 7$ gives a parity check matrix for C_1, namely:

$$H_1 = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}.$$

As a check on the above work, one could compute $HG^\top$. It should be the zero matrix because the rows of H and G are basis vectors in $C_1^\perp$ and C_1, respectively.

Exercises

1. Prove Lemma 7.8.

2. Prove that C is linear if and only if C detects precisely those error patterns in $\mathbb{Z}_2^n - C$.

3. Let H be a parity check matrix for a linear code C. Prove that C has minimum distance d if and only if any set of $d - 1$ columns of H is linearly independent and some set of d columns of H is linearly dependent.

4. Let $S = \{11000, 01111, 11110, 01010\}$, and $C = \langle S \rangle$.
   (a) Find a generator matrix, and also a parity check matrix for C.
   (b) What is the dimension of C, and of $C^\perp$?
   (c) Find the minimum distance of C, and of $C^\perp$.

5. Let C be the linear code with generator matrix

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}.$$

   Assign data to the words in $\mathbb{Z}_2^4$ by letting the letters $A, B, \ldots, P$ correspond to 0000, 0001, …, 1111, respectively. Encode the message CALL HOME (ignore the space).

6. Let C_1 and C_2 be the linear codes with parity check matrices

$$H_1 = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}, \qquad H_2 = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix},$$

   respectively.
   (a) Are C_1 and C_2 equivalent codes?
   (b) Find a generator matrix for C_2.

7. Let C be a linear code. Prove that either half the codewords in C have even weight, or every codeword in C has even weight. (*Hint*: assume there is a codeword w of odd weight, and start by explaining why the set $C + w$, obtained by adding w to each word in C, is equal to C.)

8. Prove that in a self-dual code all words have even weight. (A code C is *self-dual* if $C = C^\perp$.)

9. Prove Proposition 7.9.

10. Let C be a linear code of length n, dimension k and minimum distance $2t + 1$.
   (a) Prove that the number of error patterns that C detects is $2^n - 2^k$.

(b) Is the result in (a) consistent with the theorem that C detects all non-zero error patterns of weight at most d if and only if it has minimum distance at least $d+1$? Explain.

11. Suppose C is a single error correcting linear code with 5 parity check digits.

    (a) Prove that the length of C is at most $2^5 - 1$, and equality can hold. (*Hint*: consider a parity check matrix.)

    (b) Show that if equality holds in part (a), the resulting code is perfect.

    (c) Without appealing to some general result, prove that any two codes for which equality holds in part (a) are equivalent.

12. Prove that the maximum number of words in a t-error correcting linear code of length n is 2^t, where

$$t = n - \left\lfloor \log_2\left(\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{t}\right)\right\rfloor.$$

7.3 Hamming codes

For $r \geq 3$, the *Hamming code of length* $2^r - 1$ is the linear code with a parity check matrix which has as its columns the $2^r - 1$ non-zero binary words of length r.

A parity check matrix for the Hamming code of length 7 is

$$H = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}.$$

This is not in a form which permits one to immediately write down a generator matrix. But, it turns out that arranging the columns so that the i-th column is the binary representation of the number i permits a slick decoding algorithm. A generator matrix can easily be found using the method in the previous section.

Proposition 7.15. *For $r \geq 3$, the Hamming code of length $2^r - 1$ has minimum distance 3.*

Proof: Fix $r \geq 3$. Let C be the Hamming code of length $2^r - 1$, and let H be a parity check matrix for C as described in the definition. By Lemma 7.8 it suffices to prove that the smallest weight of a non-zero codeword equals three.

Note that the vector $Hx^\top$ is the sum of the columns of H corresponding to the positions in which x has 1s. Since H has no column of zeros, and no two identical columns, C contains no word of weight one or two. To see that C has a word of weight three, note that if w has 1s in the positions corresponding to the columns of H that are the binary representations of one, two and three, then $Hw^\top = 0$. Thus, C has minimum distance three. □

It is true in general that the minimum distance of a linear code C can be determined from its parity check matrix H. This was Exercise 2 of the previous section.

By Proposition 7.15 and Corollary 7.5 the Hamming code of length $2^r - 1$ is a single error correcting code. Suppose the columns of the parity check matrix H are arranged so that the i-th column of H is the binary representation of the number i. Suppose further that a codeword w is transmitted and that a single error occurs, so that the received word is $w = x + e$, where e has weight one. Then $Hw^\top = H(x+e)^\top = Hx^\top + He^\top = 0 + He^\top$. The vector $He^\top$ is the column of H corresponding to the position in which e has its 1. But the i-th column of H is the binary representation of the number i, so the vector $Hw^\top = He^\top$ is the binary representation of the position in which the error occurred. This establishes the correctness of the following decoding algorithm, in which w denoted the received word:

- If $Hw^\top = 0$, then accept that w was sent.
- Otherwise, complement the bit of w in position $Hw^\top$.

On the assumption that at most one error has occurred, the received word is decoded correctly.

Proposition 7.16. *For $r \geq 3$, the Hamming code of length $2^r - 1$ is a perfect (single error correcting) code.*

Proof: Fix $r \geq 3$ and let C denote the Hamming code of length $2^r - 1$. We have already seen that C is single error correcting. It remains to show that equality holds in the Hamming bound.

Since H has r rows, a generator matrix for C has $2^r - r - 1$ rows (the length of C is $2^r - 1$). Thus, C has dimension $2^r - r - 1$ and has $2^{2^r - r - 1}$ codewords. Since the minimum distance of C is $3 = 2 \cdot 1 + 1$, the RHS of the Hamming bound is

$$\frac{2^{2^r-1}}{\binom{2^r-1}{0} + \binom{2^r-1}{1}} = \frac{2^{2^r-1}}{1 + (2^r - 1)} = 2^{2^r-r-1} = |C|,$$

as required. This completes the proof. □

Exercises

1. Is it true that the codewords of weight three in the Hamming code of length 7 are the characteristic vectors of a $(7,3,1)$-design?

2. For the Hamming code of length 7, find a generator matrix corresponding to the partity check matrix whose i-th column is the binary representation of the number i.

3. Let C be a linear code of length n, with generator matrix G in standard form. Construct G^* from G by adding an extra column so that every row of G^* contains an even number of 1s. Let C^* be the linear code with generator matrix G^*. (The code C^* is called the *extended code* of C.)

   (a) Let H be a parity check matrix for C. Show that the matrix H^* obtained from H by adding a column of 0s, and then a row of 1s, is a parity check matrix for C^*.

   (b) Show that the words in C^* are obtained from the words in C by adding a parity check digit so that the number of 1s in each codeword is even.

   (c) Show that if the minimum distance of C is $2d+1$, then the minimum distance of C^* is $2d+2$ (so that C^* detects one more error that does C, but corrects no more errors than does C).

   (d) Construct the extended code for the Hamming code of length 7, and show that it is self-dual.

Bibliography

[1] I. Anderson, *Combinatorics of Finite Sets*, Oxford University Press, Oxford UK, 1987.

[2] L.M. Batten *Combinatorics of finite geometries*, Cambridge University Press, Cambridge UK, 1986.

[3] P. Cameron, *Combinatorics: Topics, Techniques, Algorithms*, Cambridge University Press, Cambridge UK, 1994.

[4] H. Eves, *A Survey of Geometry*, Allyn and Bacon, Boston, 1972.

[5] E. Gossett, *Discrete Mathematics with Proof*, Prentice-Hall, New Jersey, 2003.

[6] M. Hall Jr., *Combinatorial Theory*, Blaisdell, Waltham MA, 1967.

[7] F. S. Roberts and B. Tesman, *Applied Combinatorics* (2nd Ed.), Prentice Hall, New Jersey, 2005.

[8] H. J. Straight, *Combinatorics: An Invitation*, Brooks/Cole, Pacific Grove CA, 1993.

[9] J. H. van Lint and R. M. Wilson, *A Course in Combinatorics*, Cambridge University Press, Cambridge UK, 1992.