

**Theorem 9.3.3** Let  $\mathcal{A} = (A_1, A_2, \dots, A_n)$  be a family of subsets of a set  $Y$ . Then the largest number  $\rho$  of sets of  $\mathcal{A}$  which can be chosen so that they have an SDR equals the smallest value taken on by the expression

$$|A_{i_1} \cup A_{i_2} \cup \dots \cup A_{i_k}| + n - k$$

over all choices of  $k = 1, 2, \dots, n$  and all choices of  $k$  distinct indices  $i_1, i_2, \dots, i_k$  from  $\{1, 2, \dots, n\}$ .

The number  $\rho$  defined in Theorem 9.3.3 is the matching number  $\rho(G)$  of the bipartite graph  $G$  that we have associated with the family  $\mathcal{A}$ .

**Example.** We define a family  $\mathcal{A} = (A_1, A_2, A_3, A_4, A_5, A_6)$  of subsets of  $\{a, b, c, d, e, f\}$  by

$$\begin{aligned} A_1 &= \{a, b, c\}, & A_2 &= \{b, c\}, & A_3 &= \{b, c\}, \\ A_4 &= \{b, c\}, & A_5 &= \{c\}, & A_6 &= \{a, b, c, d\}. \end{aligned}$$

We have

$$|A_2 \cup A_3 \cup A_4 \cup A_5| = |\{b, c\}| = 2;$$

hence,

$$|A_2 \cup A_3 \cup A_4 \cup A_5| + 6 - 4 = 4.$$

Thus, with  $n = 6$  and  $k = 4$ , we see by Theorem 9.3.3 that, at most, four of the sets  $\mathcal{A}$  can be chosen so that they have an SDR. Since  $(A_1, A_2, A_5, A_6)$  has  $(a, b, c, d)$  as an SDR, it follows that 4 is the largest number of sets with an SDR. In terms of marriage, 4 is the largest number of gentlemen that can marry if each gentleman is to marry an acceptable woman.  $\square$

## 9.4 Stable Marriages

In this section<sup>8</sup> we consider a variation of the marriage problem discussed in the previous section.

There are  $n$  women and  $n$  men in a community. Each woman ranks each man in accordance with her preference for that man as a spouse. No ties are allowed, so that if a woman is indifferent between two men, we nonetheless require that she express some preference. The

<sup>8</sup>This section is partly based on the article "College admissions and the stability of marriage" by D. Gale and L.S. Shapely, *American Mathematical Monthly*, 69(1962), 9-15. A comprehensive treatment of the questions considered here can be found in the book *The stable marriage problem: Structure and algorithms* by D. Gusfield and R.W. Irving, The MIT Press, Cambridge (1989).

preferences are to be purely ordinal, and thus each woman ranks the men in the order  $1, 2, \dots, n$ . Similarly, each man ranks the women in the order  $1, 2, \dots, n$ . There are  $n!$  ways in which the women and men can be paired so that a *complete marriage* takes place. We say that a complete marriage is *unstable*, provided that there exist two women  $A$  and  $B$  and two men  $a$  and  $b$  such that

- (i)  $A$  and  $a$  get married;
- (ii)  $B$  and  $b$  get married;
- (iii)  $A$  prefers (i.e., ranks higher)  $b$  to  $a$ ;
- (iv)  $b$  prefers  $A$  to  $B$ .

Thus, in an unstable complete marriage,  $A$  and  $b$  could act independently of the others and run off with each other, since both would regard their new partner as more preferable than their current spouse. Thus, the complete marriage is "unstable" in the sense that it can be upset by a man and a woman acting together in a manner that is beneficial to both. A complete marriage is called *stable*, provided it is not unstable. The question that arises first is *Does there always exist a stable, complete marriage?*

We set up a mathematical model for this problem by using a bipartite graph again. Let  $G = (X, \Delta, Y)$  be a bipartite graph in which

$$X = \{w_1, w_2, \dots, w_n\}$$

is the set of  $n$  women and

$$Y = \{m_1, m_2, \dots, m_n\}$$

is the set of  $n$  men. We join each woman-vertex (left is now woman) to each man-vertex (right is now man). The resulting bipartite graph is *complete* in the sense that it contains all possible edges between its two sets of vertices.<sup>9</sup> Corresponding to each edge  $\{w_i, m_j\}$ , there is a pair  $p, q$  of numbers where  $p$  denotes the position of  $m_j$  in  $w_i$ 's ranking of the men, and  $q$  denotes the position of  $w_i$  in  $m_j$ 's ranking of the women. A complete marriage of the women and men corresponds to a perfect matching (of  $n$  edges) in this bipartite graph  $G$ .

It is more convenient, for notational purposes, to use the model afforded by the *preferential ranking matrix*. This matrix is an  $n$ -by- $n$  array of  $n$  rows, one for each of the women  $w_1, w_2, \dots, w_n$ , and  $n$

<sup>9</sup>In Chapter 11, this graph is called the complete bipartite graph  $K_{n,n}$ .

columns, one for each of the  $n$  men  $m_1, m_2, \dots, m_n$ . In the position at the intersection of row  $i$  and column  $j$ , we place the pair  $p, q$  of numbers representing, respectively, the ranking of  $m_j$  by  $w_i$  and the ranking of  $w_i$  by  $m_j$ . A complete marriage corresponds to a set of  $n$  positions of the matrix that includes exactly one position from each row and one position from each column.<sup>10</sup>

**Example.** Let  $n = 2$ , and let the preferential ranking matrix be

$$\begin{array}{c} \\ w_1 \\ w_2 \end{array} \begin{array}{cc} m_1 & m_2 \\ \left[ \begin{array}{cc} 1, 2 & 2, 2 \\ 2, 1 & 1, 1 \end{array} \right] \end{array}.$$

Thus, for instance, the entry 1, 2 in the first row and first column means that  $w_1$  has put  $m_1$  first on her list and  $m_1$  has put  $w_1$  second on his list. There are two possible complete marriages:

$$(1) w_1 \leftrightarrow m_1, w_2 \leftrightarrow m_2,$$

$$(2) w_1 \leftrightarrow m_2, w_2 \leftrightarrow m_1.$$

The first is readily seen to be stable. The second is unstable since  $w_2$  prefers  $m_2$  to her spouse  $m_1$ , and similarly  $m_2$  prefers  $w_2$  to his spouse  $w_1$ .  $\square$

**Example.** Let  $n = 3$ , and let the preferential ranking matrix be

$$\begin{array}{c} \\ \\ \\ \end{array} \begin{array}{ccc} m_1 & m_2 & m_3 \\ \left[ \begin{array}{ccc} 1, 3 & 2, 2 & 3, 1 \\ 3, 1 & 1, 3 & 2, 2 \\ 2, 2 & 3, 1 & 1, 3 \end{array} \right] \end{array}. \quad (9.11)$$

There are  $3! = 6$  possible complete marriages. One is

$$w_1 \leftrightarrow m_1, w_2 \leftrightarrow m_2, w_3 \leftrightarrow m_3.$$

Since each woman gets her first choice, the complete marriage is stable, even though each man gets his last choice! Another stable complete marriage is obtained by giving each man his first choice. But note that, in general, there may not be a complete marriage in which every man (or every woman) gets first choice. For example, this happens when all the women have the same first choice and all the men have the same first choice.  $\square$

We now show that a stable complete marriage always exists and, in doing so, obtain an algorithm for determining a stable complete marriage. Thus, complete chaos can be avoided!

**Theorem 9.4.1** For each preferential ranking matrix, there is a stable complete marriage.

**Proof.** We define an algorithm, the *deferred acceptance algorithm*,<sup>11</sup> for determining a complete marriage:

### Deferred Acceptance Algorithm

Begin with every woman marked as rejected.

While there exists a rejected woman, do the following:

- (1) Each woman marked as rejected chooses the man whom she ranks highest among all those men who have not yet rejected her.
- (2) Each man picks out the woman he ranks highest among all those women who have chosen him and whom he has not yet rejected, defers decision on her, and now rejects the others.

Thus, during the execution of the algorithm,<sup>12</sup> the women propose to the men, and some men and some women become *engaged*, but the men are able to break engagements if they receive a better offer. Once a man becomes engaged, he remains engaged throughout the execution of the algorithm, but his fiancée may change; in his eyes, a change is always an improvement. A woman, however, may be engaged and disengaged several times during the execution of the algorithm; however, each new engagement results in a less desirable partner for her. It follows from the description of the algorithm that, as soon as there are no rejected women, then each man is engaged to exactly one woman, and since there are as many men as women, each woman is engaged to exactly one man. We now pair each man with the woman to whom he is engaged and obtain a complete marriage. We now show that this marriage is stable.

Consider women  $A$  and  $B$  and men  $a$  and  $b$  such that  $A$  is paired with  $a$  and  $B$  is paired with  $b$ , but  $A$  prefers  $b$  to  $a$ . We show that  $b$  cannot prefer  $A$  to  $B$ . Since  $A$  prefers  $b$  to  $a$ , during some stage of the algorithm  $A$  chose  $b$ , but  $A$  was rejected by  $b$  for some woman he ranked higher. But the woman  $b$  eventually gets paired with is at least as high on his list as any woman that he rejected during the course of the algorithm. Since  $A$  was rejected by  $b$ ,  $b$  must prefer  $B$  to  $A$ . Thus, there is no unstable pair, and this complete marriage is stable.  $\square$

<sup>11</sup>Also called the Gale–Shapley algorithm.

<sup>12</sup>Note that we have reversed the traditional roles of men and women in which

<sup>10</sup>The astute reader has no doubt noticed that a complete marriage corresponds

**Example.** We apply the deferred acceptance algorithm to the preferential ranking matrix in (9.11), designating the women as  $A, B, C$ , respectively, and the men as  $a, b, c$ , respectively.<sup>13</sup> In (1),  $A$  chooses  $a$ ,  $B$  chooses  $b$ , and  $C$  chooses  $c$ . There are no rejections, the algorithm halts, and  $A$  marries  $a$ ,  $B$  marries  $b$ ,  $C$  marries  $c$ , and they live happily ever after.  $\square$

**Example.** We apply the deferred acceptance algorithm to the preferential ranking matrix

$$\begin{array}{c} \\ A \\ B \\ C \\ D \end{array} \begin{array}{cccc} a & b & c & d \\ \left[ \begin{array}{cccc} 1, 2 & 2, 1 & 3, 2 & 4, 1 \\ 2, 4 & 1, 2 & 3, 1 & 4, 2 \\ 2, 1 & 3, 3 & 4, 3 & 1, 4 \\ 1, 3 & 4, 4 & 3, 4 & 2, 3 \end{array} \right] \end{array} . \quad (9.12)$$

The results of the algorithm are as follows:

- (i)  $A$  chooses  $a$ ,  $B$  chooses  $b$ ,  $C$  chooses  $d$ ,  $D$  chooses  $a$ ;  $a$  rejects  $D$ .
- (ii)  $D$  chooses  $d$ ;  $d$  rejects  $C$ .
- (iii)  $C$  chooses  $a$ ;  $a$  rejects  $A$ .
- (iv)  $A$  chooses  $b$ ;  $b$  rejects  $B$ .
- (v)  $B$  chooses  $a$ ;  $a$  rejects  $B$ .
- (vi)  $B$  chooses  $c$ .

In (vi), there are no rejections, and

$$A \leftrightarrow b, B \leftrightarrow c, C \leftrightarrow a, D \leftrightarrow d$$

is a stable complete marriage.  $\square$

If, in the deferred acceptance algorithm, we interchange the roles of the women and men and have the men choose women according to their rank preferences, we obtain a stable complete marriage which may, but need not, differ from the one obtained by having the women choose men.

**Example.** We apply the deferred acceptance algorithm to the preferential ranking matrix in (9.12), where the men choose the women. The results are as follows:

<sup>13</sup>The BIG guys versus the little guys.

- (i)  $a$  chooses  $C$ ,  $b$  chooses  $A$ ,  $c$  chooses  $B$ ,  $d$  chooses  $A$ ;  $A$  rejects  $d$ .
- (ii)  $d$  chooses  $B$ ;  $B$  rejects  $d$ .
- (iii)  $d$  chooses  $D$ .

The complete marriage

$$a \leftrightarrow C, b \leftrightarrow A, c \leftrightarrow B, d \leftrightarrow D$$

is stable. This is the same complete marriage obtained by applying the algorithm the other way around.  $\square$

**Example.** We apply the deferred acceptance algorithm to the preferential ranking matrix in (9.11), where the men choose the women. The results are as follows:

- (i)  $a$  chooses  $B$ ,  $b$  chooses  $C$ ,  $c$  chooses  $A$ .

Since there are no rejections, the stable complete marriage obtained is

$$a \leftrightarrow B, b \leftrightarrow C, c \leftrightarrow A.$$

This is different from the complete marriage obtained by applying the algorithm the other way around.  $\square$

A stable complete marriage is called *optimal for a woman*, provided that a woman gets as a spouse a man whom she ranks at least as high as the spouse she obtains in every other stable complete marriage. In other words, there is no stable complete marriage in which the woman gets a spouse who is higher on her list. A stable complete marriage is called *women-optimal* provided that it is optimal for each woman. In a similar way, we define a *men-optimal* stable complete marriage. It is not obvious that there exist women-optimal and men-optimal stable complete marriages. In fact, it is not even obvious that, if each woman is independently given the best partner that she has in all the stable complete marriages, then this results in a pairing of the women and the men (it is conceivable that two women might end up with the same man in this way). Clearly, there can be only one women-optimal complete marriage and only one men-optimal complete marriage.

**Theorem 9.4.2** *The stable complete marriage obtained from the deferred acceptance algorithm, with the women choosing the men, is women-optimal. If the men choose the women in the deferred acceptance algorithm, the resulting complete marriage is men-optimal.*

**Proof.** A man  $M$  is called *feasible* for a woman  $W$ , provided that there is some stable complete marriage in which  $M$  is  $W$ 's spouse. We shall prove by induction that the complete marriage obtained by applying the deferred acceptance algorithm has the property that the men who reject a particular woman are not feasible for that woman. Because of the nature of the algorithm, this implies that each woman obtains as a spouse the man she ranks highest among all the men that are feasible for her, and hence the complete marriage is women-optimal.

The induction is on the number of rounds of the algorithm. To start the induction, we show that, at the end of the first round, no woman has been rejected by a man that is feasible for her. Suppose that both woman  $A$  and woman  $B$  choose man  $a$ , and  $a$  rejects  $A$  in favor of  $B$ . Then any complete marriage in which  $A$  is paired with  $a$  is not stable because  $a$  prefers  $B$  and  $B$  prefers  $a$  to whichever man she is eventually paired with.

We now proceed by induction and assume that at the end of some round  $k \geq 1$ , no woman has been rejected by a man who is feasible for her. Suppose that at the end of the  $(k + 1)$ st round, woman  $A$  is rejected by man  $a$  in favor of woman  $B$ . Then  $B$  prefers  $a$  over all those men that have not yet rejected her. By the induction assumption, none of the men who have rejected  $B$  in the first  $k$  rounds is feasible for  $B$ , and so there is no stable complete marriage in which  $B$  is paired with one of them. Thus, in any stable marriage,  $B$  is paired with a man who is no higher on her list than  $a$ .

Now suppose that there is a stable complete marriage in which  $A$  is paired with  $a$ . Then  $a$  prefers  $B$  to  $A$  and, by the last remark,  $B$  prefers  $a$  to whomever she is paired with. This contradicts the fact that the complete marriage is stable. The inductive step is now complete and we conclude that the stable complete marriage obtained from the deferred acceptance algorithm is optimal for the women.  $\square$

We now show that in the women-optimal complete marriage, each man has the *worst* partner he can have in any stable complete marriage.

**Corollary 9.4.3** *In the women-optimal stable complete marriage, each man is paired with the woman he ranks lowest among all the partners that are possible for him in a stable complete marriage.*

**Proof.** Let man  $a$  be paired with woman  $A$  in the women-optimal stable complete marriage. By Theorem 9.4.2  $A$  prefers  $a$  to all other men that are possible for her in a stable complete marriage. Suppose there is a stable complete marriage in which  $a$  is paired with woman  $B$ , where  $a$  ranks  $B$  lower than  $A$ . In this stable marriage,  $A$  is paired

with some man  $b$  different from  $a$  whom she therefore ranks lower than  $a$ . But then  $A$  prefers  $a$ , and  $a$  prefers  $A$ , and this complete marriage is not stable contrary to assumption. Hence, there is no stable complete marriage in which  $a$  gets a worse partner than  $A$ .  $\square$

Suppose the men-optimal and women-optimal stable complete marriages are identical. Then, by Corollary 9.4.3, in the woman-optimal complete marriage, each man gets both his best and worst partner taken over all stable complete marriages. (A similar conclusion holds for the women.) It thus follows in this case that there is exactly one stable complete marriage. Of course, the converse holds as well: if there is only one stable complete marriage, then the men-optimal and women-optimal stable complete marriages are identical.

The deferred acceptance algorithm has been in use since 1952 to match medical residents in the United States to hospitals.<sup>14</sup> We can think of the hospitals as being the women and the residents as being the men. But now, since a hospital generally has places for several residents, polyandrous marriages in which a woman can have several spouses are allowed.

We conclude this section with a discussion of a similar problem for which the existence of a stable marriage is no longer guaranteed.

**Example.** Suppose an even number  $2n$  of girls wish to pair up as roommates. Each girl ranks the other girls in the order  $1, 2, \dots, 2n - 1$  of preference. A *complete marriage* in this situation is a pairing of the girls into  $n$  pairs. A complete marriage is *unstable*, provided there exist two girls who are not roommates such that each of the girls prefers the other to her current roommate. A complete marriage is *stable*, provided it is not unstable. Does there always exist a stable complete marriage?

Consider the case of four girls,  $A, B, C, D$ , where  $A$  ranks  $B$  first,  $B$  ranks  $C$  first,  $C$  ranks  $A$  first, and each of  $A, B$ , and  $C$  ranks  $D$  last. Then, irrespective of the other rankings, there is no stable complete marriage as the following argument shows. Suppose  $A$  and  $D$  are roommates. Then  $B$  and  $C$  are also roommates. But  $C$  prefers  $A$  to  $B$ , and since  $A$  ranks  $D$  last,  $A$  prefers  $C$  to  $D$ . Thus, this complete marriage is not stable. A similar conclusion holds if  $B$  and  $D$  are roommates or if  $C$  and  $D$  are roommates. Since  $D$  has a roommate, there is no stable complete marriage.  $\square$

<sup>14</sup>It can also be used to match students to colleges, etc.

13. Let  $\mathcal{A} = (A_1, A_2, A_3, A_4, A_5, A_6)$ , where

$$\begin{aligned} A_1 &= \{1, 2\}, A_2 = \{2, 3\}, A_3 = \{3, 4\}, \\ A_4 &= \{4, 5\}, A_5 = \{5, 6\}, A_6 = \{6, 1\}. \end{aligned}$$

Determine the number of different SDR's that  $\mathcal{A}$  has. Generalize to  $n$  sets.

14. Let  $\mathcal{A} = (A_1, A_2, \dots, A_n)$  be a family of sets with an SDR. Let  $x$  be an element of  $A_1$ . Prove that there is an SDR containing  $x$ , but show by example that it may not be possible to find an SDR in which  $x$  represents  $A_1$ .

15. Suppose  $\mathcal{A} = (A_1, A_2, \dots, A_n)$  is a family of sets that "more than satisfies" the Marriage Condition. More precisely, suppose that

$$|A_{i_1} \cup A_{i_2} \cup \dots \cup A_{i_k}| \geq k + 1$$

for each  $k = 1, 2, \dots, n$  and each choice of  $k$  distinct indices  $i_1, i_2, \dots, i_k$ . Let  $x$  be an element of  $A_1$ . Prove that  $\mathcal{A}$  has an SDR in which  $x$  represents  $A_1$ .

16. Let  $n > 1$ , and let  $\mathcal{A} = (A_1, A_2, \dots, A_n)$  be the family of subsets of  $\{1, 2, \dots, n\}$ , where

$$A_i = \{1, 2, \dots, n\} - \{i\}, \quad (i = 1, 2, \dots, n).$$

Prove that  $\mathcal{A}$  has an SDR and that the number of SDR's is the  $n$ th derangement number  $D_n$ .

17. Consider a chessboard with forbidden positions which has the property that, if a square is forbidden, so is every square to its right and every square below it. Prove that the chessboard has a perfect cover by dominoes if and only if the number of allowable white squares equals the number of allowable black squares.

18. \* Let  $A$  be a matrix with  $n$  columns, with integer entries taken from the set  $S = \{1, 2, \dots, k\}$ . Assume that each integer  $i$  in  $S$  occurs exactly  $nr_i$  times in  $A$ , where  $r_i$  is an integer. Prove that it is possible to permute the entries in each row of  $A$  to obtain a matrix  $B$  in which each integer  $i$  in  $S$  appears  $r_i$  times in each column.<sup>15</sup>

<sup>15</sup>E. Kramer, S. Magliveras, T. van Trung, and Q. Wu: "Some perpendicular arrays for arbitrary large  $t$ ," *Discrete Math.*, 96 (1991), 101-110.

19. Find a 2-by-2 preferential ranking matrix for which both complete marriages are stable.

20. Consider a preferential ranking matrix in which woman  $A$  ranks man  $a$  first, and man  $a$  ranks  $A$  first. Show that, in every stable marriage,  $A$  is paired with  $a$ .

21. Consider the preferential ranking matrix

$$\begin{bmatrix} 1, n & 2, n-1 & 3, n-2 & \cdots & n, 1 \\ n, 1 & 1, n & 2, n-1 & \cdots & n-1, 2 \\ n-1, 2 & n, 1 & 1, n & \cdots & n-2, 3 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 3, n-3 & 4, n-3 & 5, n-4 & \cdots & 2, n-1 \\ 2, n-2 & 3, n-2 & 4, n-3 & \cdots & 1, n \end{bmatrix}$$

Prove that, for each  $k = 1, 2, \dots, n$ , the complete marriage in which each woman gets her  $k$ th choice is stable.

22. Use the deferred acceptance algorithm to obtain both the women-optimal and men-optimal stable complete marriages for the preferential ranking matrix

$$\begin{array}{c} a \quad b \quad c \quad d \\ A \quad \begin{bmatrix} 1, 3 & 2, 3 & 3, 2 & 4, 3 \\ 1, 4 & 4, 1 & 3, 3 & 2, 2 \\ 2, 2 & 1, 4 & 3, 4 & 4, 1 \\ 4, 1 & 2, 2 & 3, 1 & 1, 4 \end{bmatrix} \\ B \\ C \\ D \end{array}$$

Conclude that, for the given preferential ranking matrix, there is only one stable complete marriage.

23. Prove that in every application of the deferred acceptance algorithm with  $n$  women and  $n$  men, there are at most  $n^2 - n + 1$  proposals.

24. \* Extend the deferred acceptance algorithm to the case in which there are more men than women. In such a case, not all of the men will get partners.

25. Show, by using Exercise 22, that it is possible that in no complete marriage does any person get his or her first choice.

26. Apply the deferred acceptance algorithm to obtain a stable complete marriage for the preferential ranking matrix

$$\begin{array}{l} A \\ B \\ C \\ D \end{array} \begin{array}{cccc} a & b & c & d \\ \left[ \begin{array}{cccc} 1,3 & 2,2 & 3,1 & 4,3 \\ 1,4 & 2,3 & 3,2 & 4,4 \\ 3,1 & 1,4 & 2,3 & 4,2 \\ 2,2 & 3,1 & 1,4 & 4,1 \end{array} \right] . \end{array}$$

27. Consider an  $n$ -by- $n$  board in which there is a nonnegative number  $a_{ij}$  in the square in row  $i$  and column  $j$ , ( $1 \leq i, j \leq n$ ). Assume that the sum of the numbers in each row and in each column equals 1. Prove that it is possible to place  $n$  nonattacking rooks on the board at positions occupied by positive numbers.

## Chapter 10

# Combinatorial Designs

A *combinatorial design*, or simply a *design*, is an arrangement of the objects of a set into subsets satisfying certain prescribed properties. This is a very general definition and includes a vast amount of combinatorial theory. Many of the examples introduced in Chapter 1 can be viewed as designs: (i) perfect covers by dominoes of boards with forbidden positions, where we arrange the allowed squares into pairs so that each pair can be covered by one domino; (ii) magic squares, where we arrange the integers from 1 to  $n^2$  in an  $n$ -by- $n$  array so that certain sums are identical; (iii) Latin squares, where we arrange the integers from 1 to  $n$  in an  $n$ -by- $n$  array so that each integer occurs once in each row and once in each column. We shall treat Latin squares and the notion of orthogonality, briefly introduced in Chapter 1, more thoroughly in this chapter.

The area of combinatorial designs is highly developed, yet many interesting and fundamental questions remain unanswered. Many of the methods for constructing designs rely on the algebraic structure called a finite field and more general systems of arithmetic. In the first section we give a brief introduction to these "finite arithmetics," concentrating mainly on modular arithmetic. Our discussion will not be comprehensive, but should be sufficient to enable us to do arithmetic comfortably in these systems.

### 10.1 Modular Arithmetic

Let  $Z$  denote the set of integers

$$\{\dots, -2, -1, 0, 1, 2, \dots\},$$