Mathematics for Computer Science/Software Engineering

Notes for the course MSM1F3

Dr. R. A. Wilson

October 1996

Chapter 1

Logic

Lecture no. 1.

We introduce the concept of a *proposition*, which is a statement which is either true or false (that is, it has a definite *truth value*). Questions, instructions, interjections, etc. are not propositions.

Compound propositions can be formed by *conjunction*, that is $p \wedge q$, read 'p and q', which is understood to be true when both p and q are true, and false otherwise. Similarly the *disjunction* of p and q is $p \vee q$, read 'p or q', which is defined to be true when either p or q is true (or both). This is the so-called *inclusive or*, as opposed to the *exclusive or* more often used in computing, which means 'p or q but not both'.

All these things are defined by *truth tables*, which list all possible truth values for the simple propositions p, q, etc., and the corresponding truth values for the compound proposition. Similarly, we can define the *negation* of p, written $\overline{p}$ and read 'not p', to be true if p is false and false if p is true.

Examples such as $(p \wedge q) \vee r$ and $p \wedge (q \vee r)$ show that brackets are essential, as these two propositions have different truth values in some circumstances. They can both be read as 'p and q or r', but with the comma in different places, thus: 'p and q, or r' versus 'p, and q or r'. Alternatively, you can think of it as the distinction between 'either p and q, or r' and 'p and either q or r'.

Conditional propositions are statements of the form 'if p then q'. In order to give this a truth value in all circumstances, we define it by the following truth table.

p	q	$p \to q$
T	T	T
T	F	F
F	T	T
F	F	T

Lecture no. 2.

Heuristic justification for this definition: if p is true and q is false, then the statement 'if p is true then q is true' obviously cannot be true, and therefore must be false. On the other hand, if p is false, then the statement 'if p is true then ...' is an empty statement—it is saying nothing at all, and therefore cannot be false. So it must be true.

If you work out the truth table of $\overline{p} \vee q$, you will see that it is identical to the truth table for $p \to q$. Thus from a logical point of view there is no difference between them: one is just a re-wording of the other. We say they are *logically equivalent*, and write $p \to q \equiv \overline{p} \vee q$.

Other useful examples include DeMorgan's laws: $\overline{p \vee q} \equiv \overline{p} \wedge \overline{q}$ and $\overline{p \wedge q} \equiv \overline{p} \vee \overline{q}$. These can easily be proved by working out the truth tables. Similarly $\overline{\overline{p}} \equiv p$.

One very important result is that $p \to q \equiv \overline{q} \to \overline{p}$. The statement $\overline{q} \to \overline{p}$ is called the *contrapositive* of $p \to q$. This result can be proved by truth tables as before, or alternatively we can argue as follows.

$$\overline{q} \to \overline{p} \equiv \overline{\overline{q}} \vee \overline{p} \equiv q \vee \overline{p} \equiv p \vee q \equiv p \to q.$$

Warning: the statement $q \to p$ (called the *converse* of $p \to q$) is not logically equivalent to $p \to q$.

In order to be able to dispense with truth tables altogether, you need also the *distributive laws* $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$ and $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$.

Introduce quantifiers: '$x > 3$' is not a proposition, since its truth value depends on the value of x. But we want to talk about mathematical statements of the form 'if $x > 3$ then $x^2 > 9$', which is undoubtedly a true statement! It really means 'for any x, if $x > 3$ then $x^2 > 9$'. We introduce *propositional functions* such as $P(x)$ to denote statements which become propositions when we give a particular value to the variable x. Thus if $P(x)$ denotes '$x > 3$', we can see that $P(1)$ is false, while $P(5)$ is true. Now let $Q(x)$ denote '$x^2 > 9$', so we can write our full statement as $\forall x(P(x) \to Q(x))$, which we read as 'for any x, if $P(x)$ is true then $Q(x)$ is true'.

Lecture no. 3.

The symbol $\forall$ is called the *universal quantifier*. Similarly there is the *existential quantifier* $\exists$, which can be read as 'there exists'. Thus the statement $\exists x P(x)$ is true if there is some value of x for which $P(x)$ is true.

Now to show in a given instance that $\forall x P(x)$ is false, we need only find one value of x for which $P(x)$ is false. Such an x is called a *counterexample*. This leads us to another form of DeMorgan's laws: $\overline{\forall x P(x)} \equiv \exists x \overline{P(x)}$. Similarly, if $\exists x P(x)$ is false, then there is no x for which $P(x)$ is true, so for all x, $P(x)$ is false, and we obtain the other of DeMorgan's laws: $\overline{\exists x P(x)} \equiv \forall x \overline{P(x)}$.

In all these examples, we need to understand the context of a given statement: that is, if we say there exists an x with $P(x)$ true, we are only talking about x

being within a certain *domain of discourse*, typically the set of real numbers, or the set of integers.

Mathematical results are often of the form $\forall x(P(x) \to Q(x))$. To prove something like this, all we need to do is to consider all those values of x for which $P(x)$ is actually true, and show that in these cases $Q(x)$ is also true. Such a proof is called a *direct proof*.

But just as $p \to q$ is logically equivalent to $\overline{q} \to \overline{p}$, we can see that $\forall x(P(x) \to Q(x))$ is logically equivalent to $\forall x(\overline{Q(x)} \to \overline{P(x)})$. Thus an alternative strategy is to consider all those values of x for which $Q(x)$ is false, and show that in these cases $P(x)$ is also false. This is called a *proof by contrapositive*.

For example, let the domain of discourse be the set of integers, and let $P(n)$ be 'n^2 is an even number', and $Q(n)$ be 'n is an even number'. In this case a direct proof of $\forall n(P(n) \to Q(n))$ is hard to find, but a proof by contrapositive is easier: we consider all values of n for which $Q(n)$ is false, that is all n such that n is not even, so is odd. Then $n = 2k+1$ for some integer k, so $n^2 = (2k+1)^2 = 4k^2+4k+1$, which is odd. In other words we have proved that $P(n)$ is false in all circumstances where $Q(n)$ is false. Thus we have given a proof by contrapositive of the proposition 'if n is an integer such that n^2 is an even number, then n is an even number'.

Lecture no. 4.

A more powerful method of proof than either a direct proof or a proof by contrapositive, is a *proof by contradiction*. This uses the fact that $p \to q \equiv p \wedge \overline{q} \to r \wedge \overline{r}$. As usual, we prove this equivalence by examining a truth-table, or we can argue heuristically by saying that to prove that p implies q, it is enough to prove that you cannot have p true and q false—that is, $p \wedge \overline{q}$ is a contradiction.

For example, to prove that is m and n are positive integers, then $\left(\frac{m}{n}\right)^2 \neq 2$, we assume $p \wedge \overline{q}$ and try to deduce a contradiction. That is, we assume that m and n are positive integers, and $\left(\frac{m}{n}\right)^2 = 2$. Now, if such positive integers exist, then $n < m$, and we can assume that m and n are as small as possible. Then $m^2 = 2n^2$, so m^2 is even, so m is even, so $m = 2k$ for some integer k. Therefore $2n^2 = m^2 = (2k)^2 = 4k^2$, and so $n^2 = 2k^2$. This implies that $\left(\frac{n}{k}\right)^2 = 2$, with smaller numbers than before since $n < m$. This is a contradiction, and therefore we have proved the required result.

Having examined the overall outline of a proof, let us look more closely at the detailed *deductions* or *arguments* used as individual steps in the proof. Each of these is essentially of the same form: we know some propositions p, q, ... (called the *hypotheses*) to be true already, and we deduce a *conclusion* r, say. This argument may be written in the form

$$\begin{array}{c} p \\ q \\ \vdots \\ \hline \therefore\ r \end{array}$$

Such an argument is said to be *valid* if whenever the hypotheses are all true, the conclusion is also true. Otherwise, it is *invalid*, which means that under some circumstances, all the hypotheses can be true, but the conclusion is not true. For example, the argument

$$\begin{array}{c} p \to q \\ p \\ \hline \therefore\ q \end{array}$$

is valid. We can prove this using a truth table: the only case where both of the hypotheses are true is the case when both p and q are true, and in particular the conclusion is true. On the other hand, the argument

$$\begin{array}{c} p \to q \\ q \\ \hline \therefore\ p \end{array}$$

is invalid. To see this, we find one case where the hypotheses are both true but the conclusion is false, such as the case p is false and q is true.

Lecture no. 5.

More complicated examples can be analysed with truth tables.

The first example above can be extended to

$$\begin{array}{c} p \\ p \to q \\ q \to r \\ \hline \therefore\ r \end{array}$$

or

$$\begin{array}{c} p \\ p \to q \\ q \to r \\ \hline \therefore\ p \wedge q \wedge r \end{array}$$

which is again a valid argument. Indeed, if we have a whole series of propositions

$P(1)$, $P(2)$, and so on, we can construct a valid argument in the form

$$\begin{array}{c} P(1) \\ P(1) \to P(2) \\ P(2) \to P(3) \\ \vdots \\ \hline \therefore P(1) \land P(2) \land P(3) \ldots \end{array}$$

which can also be written more compactly as

$$\begin{array}{c} P(1) \\ \forall k(P(k) \to P(k+1)) \\ \hline \therefore \forall n P(n) \end{array}$$

This form of argument is called the *Principle of Mathematical Induction.* It is understood that the domain of discourse for these quantifiers is the set of positive integers.

Example: prove that for all positive integers n,

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$$

We let $P(n)$ denote the given statement $1+2+3+\cdots+n = \frac{n(n+1)}{2}$, so that $P(1)$ is the statement $1 = \frac{1\times 2}{2}$, which is true. Now we assume that $P(k)$ is true, that is $1+2+3+\cdots+k = \frac{k(k+1)}{2}$ and deduce that $1+2+3+\cdots+k+(k+1) = \frac{k(k+1)}{2} + (k+1) = \frac{(k+1)(k+2)}{2}$, in other words $P(k+1)$ is true. Thus we have proved mathematically that $P(1)$ is true, and that for all k, if $P(k)$ is true then $P(k+1)$ is true. Hence by the Principle of Mathematical Induction, it follows that $\forall n P(n)$ is true.

Lecture no. 6.

More examples of induction:

1. Prove that for all integers n, $5^n - 1$ is divisible by 4.

   For $n = 1$, the statement is '$5 - 1$ is divisible by 4', which is true. Now if $5^k - 1$ is divisible by 4, then $5^{k+1} - 1 = 5 \times 5^k - 1 = (4+1) \times 5^k - 1 = 4 \times 5^k + 5^k - 1$, which is divisible by 4, since both parts 4×5^k and $5^k - 1$ are divisible by 4.

2. Prove that for all integers $n \geq 4$, $n! > 2^n$. (Here we first define $n! = 1 \times 2 \times 3 \times \cdots \times n$, called *n factorial.*)

   For $n = 4$, the statement is $4! > 2^4$, i.e. $24 > 16$, which is true. Now if $k! > 2^k$, then $(k+1)! = (k+1) \times k! > (k+1) \times 2^k > 2 \times 2^k = 2^{k+1}$.

The Principle of Mathematical Induction can also be expressed in the so-called *strong form*:

$$\frac{\forall k((\forall j(j < k \rightarrow P(j)) \rightarrow P(k))}{\therefore \forall n P(n)},$$

which is a shorthand for

$$\begin{array}{c} T \rightarrow P(1) \\ P(1) \rightarrow P(2) \\ P(1) \wedge P(2) \rightarrow P(3) \\ P(1) \wedge P(2) \wedge P(3) \rightarrow P(4) \\ \vdots \\ \hline \therefore P(1) \wedge P(2) \wedge P(3) \ldots \end{array}$$

One example where we need the strong form is the following: prove that every positive integer (is either 1, or a prime, or) can be factorised as a product of primes. (Here we do not count 1 as a prime.)

Chapter 2

Basic concepts

Lecture no. 7.

The idea of a *set* as a collection of *elements*, without regard to ordering or repetitions. Examples $\{1, 2, 3, 4\}$ and $\{x|x \text{ is an even integer }\}$. If a is an element of the set A we write $a \in A$. The *cardinality* of set X is the number of elements in it, written $|X|$. The *empty set* $\emptyset = \{\}$ has no elements in it. Two sets are *equal* if they have the same elements, that is, $X = Y$ if and only if $\forall x(x \in X \rightarrow x \in Y \text{ and } x \in Y \rightarrow x \in X)$. A set X is a *subset* of a set Y, written $X \subseteq Y$, if all elements of X are elements of Y. If also $X \neq Y$, then X is a *proper* subset of Y, written $X \subset Y$ or sometimes $X \underset{\neq}{\subset} Y$. For example, $\emptyset \subseteq A$ and $A \subseteq A$ for any set A. The set of all subsets of a set X is called the *power set* of X, written $\mathcal{P}(X)$. If $|X| = n$ then $|\mathcal{P}(X)| = 2^n$—this can be proved by induction.

Lecture no. 8.

There are various ways of combining sets: the *union* $X \cup Y$ of X and Y is the set of elements that are either in X or in Y, or both, $X \cup Y = \{x|x \in X \text{ or } x \in Y\}$. Similarly the *intersection* $X \cap Y$ consists of those elements that are in both, $X \cap Y = \{x|x \in X \text{ and } x \in Y\}$. These operations obey many rules analogous to the rules of logic we studied earlier. For example, $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ for the same reason that in logic $p \vee (q \wedge r) = (p \vee q) \wedge (p \vee r)$.

To introduce an analogue of negation, we need to introduce first the notion of a *universal set* U (cf. domain of discourse) which all elements of all our sets are supposed to belong to. Then the *complement* $\overline{A}$ of a set A is the set of all elements which are not elements in A, that is $\overline{A} = \{x|x \in U \text{ and } x \notin A\}$.

Then we can write down DeMorgan's laws for sets: $\overline{A \cap B} = \overline{A} \cup \overline{B}$ and $\overline{A \cup B} = \overline{A} \cap \overline{B}$.

Moreover, we can identify the empty set with a *contradiction* (something that is always false), and the universal set with a *tautology* (something that is always true). Then there are several other useful rules such as $A \cap \overline{A} = \emptyset$ corresponding to $p \wedge \overline{p} = F$, and $A \cup \overline{A} = U$ corresponding to $p \vee \overline{p} = T$.

All these things can be illustrated in *Venn diagrams*.

If we have infinitely many sets, we may take the union (or intersection) of all of them, as follows. Suppose $\mathcal{S}$ is a set whose elements are themselves sets. We define $\bigcup\mathcal{S} = \{x|x \in S \text{ for some } S \in \mathcal{S}\}$ and $\bigcap\mathcal{S} = \{x|x \in S \text{ for all } S \in \mathcal{S}\}$. Thus we obtain analogues of the two quantifiers also. In particular, if $\mathcal{S} = \{A_1, A_2, \ldots\}$, we write $\bigcup\mathcal{S} = \bigcup_{i=1}^{\infty} A_i = A_1 \cup A_2 \cup \cdots$ and similarly for intersections.

Lecture no. 9.

The *difference* or *relative complement* of two sets A and B is $A - B = \{x|x \in A \text{ and } x \notin B\}$. This is a generalisation of the complement $\overline{B} = U - B$ where U is the universal set. The *symmetric difference* $A \triangle B = (A - B) \cup (B - A)$ is the set of elements in one or other (but not both) of A and B. Two sets are called *disjoint* if their intersection is the empty set.

A *partition* is obtained by chopping up a set into non-empty, non-overlapping (i.e. pairwise disjoint) subsets. More formally, $\mathcal{S}$ is a partition of A if $\bigcup\mathcal{S} = A$, $\emptyset \notin \mathcal{S}$, and if $S \in \mathcal{S}$ and $T \in \mathcal{S}$ with $S \neq T$, then $S \cap T = \emptyset$. Examples: $\{\{1, 2, 4\}, \{3, 6\}, \{5, 7, 8\}\}$ is a partition of the set $\{1, 2, 3, 4, 5, 6, 7, 8\}$, and $\{\{\text{even integers}\}, \{\text{odd integers}\}\}$ is a partition of the set $\mathbb{Z}$ of all integers.

Lecture no. 10.

Ordered pairs, where order does matter, are written (a, b) to distinguish them from sets $\{a, b\}$ where order does not matter (cf. vector notation). The *Cartesian product* of two sets A and B is the set of all ordered pairs where the first element is in A and the second is in B: that is, $A \times B = \{(a, b)|a \in A \text{ and } b \in B\}$. We can generalise to ordered triples (a, b, c) and the Cartesian product of three sets $A \times B \times C = \{(a, b, c)|a \in A, b \in B, c \in C\}$, and so on.

Notion of a *string of length n*—an ordered n-tuple, but often written without the brackets and commas. Notation $\sum_{i=1}^{n} a_i = a_1 + a_2 + \cdots + a_n$ and $\prod_{i=1}^{n} a_i = a_1 \times a_2 \times \cdots \times a_n$. Compare also $\bigcup_{i=1}^{n} A_i = A_1 \cup A_2 \cup \cdots \cup A_n$, etc. *Concatenation* of two strings over an *alphabet* A: if $(a_1, a_2, \ldots, a_m)$ and $(b_1, b_2, \ldots, b_n)$ are two strings over A (i.e. $a_i \in A$ and $b_j \in A$), then their concatenation is $(a_1, a_2, \ldots, a_m, b_1, b_2, \ldots, b_n)$, of length $m + n$.

A *sequence* is like an infinite string, written $a_1, a_2, \ldots$ or sometimes $\{a_i\}_{i=1}^{\infty}$ (note that, confusingly, curly brackets are usually used instead of round brackets here).

Lecture no. 11.

Define *relations* between two sets as subsets of the Cartesian product. Informal discussion as tables. Examples. The special case of relations on a set: illustration in a *digraph*. A relation R on a set A is *reflexive* if everything is related to itself, i.e. $\forall x \in A(xRx)$. It is *anti-symmetric* if two things cannot be related both ways round, unless they are equal, i.e. $\forall x \in A \forall y \in A(xRy \wedge yRx \rightarrow x = y)$. It is *symmetric* if two things are always related both ways round or not at all, i.e. $\forall x \in A(xRy \rightarrow yRx)$. Examples in pictures.

Lecture no. 12.

Definition and examples of transitive relations. Examples of relations which are (i) symmetric and not anti-symmetric, (ii) anti-symmetric and not symmetric, (iii) both, (iv) neither. An *equivalence relation* is one which is reflexive, symmetric and transitive. Examples: 'is the same colour as'—corresponds to a partition into different colours. We will see later that an equivalence relation always corresponds to a partition. A *partial order* is a relation which is reflexive, anti-symmetric and transitive. Examples: '$\leq$' on $\mathbb{Z}$, and $\subseteq$ on $\mathcal{P}(X)$. First look at the example $X = \{1, 2\}$, then arbitrary sets. If we have a partial order relation we can simplify the digraph to a *Hasse diagram* by leaving out redundant information, i.e. loops, arrows (all assumed to go up the page), and all edges which can be deduced from transitivity.

Lecture no. 13.

Example: the Hasse diagram of the relation '$\subseteq$' on $A = \mathcal{P}(X)$, where $X = \{1, 2, 3\}$.

Now equivalence relations correspond to partitions in the following way. If $\mathcal{S}$ is a partition of A, define a relation R on A by aRb whenever a and b are in the same part of the partition, i.e. whenever there is a set $T \in \mathcal{S}$ with $a \in T$ and $b \in T$. Then we show that R is an equivalence relation. Example: $\mathcal{S} = \{\{1, 3, 4\}, \{5\}, \{2, 6\}\}$. Conversely, if R is an equivalence relation on A, we first define $[a] = \{x \in A | aRx\}$, the *equivalence class of* a, for each $a \in A$. Then we prove that if aRb then $[a] = [b]$. For if aRb and $x \in [a]$, then aRx, so xRa, so xRb by transitivity, so bRx, i.e. $x \in [b]$. This gives $[a] \subseteq [b]$, and a similar argument gives $[b] \subseteq [a]$, and so $[a] = [b]$. This enables us to prove that the equivalence classes form a partition of A. So, let $\mathcal{S} = \{[a] | a \in A\}$. First, for any $a \in A$ we have aRa and so $a \in [a]$, so $a \in \bigcup \mathcal{S}$, whence $A = \bigcup \mathcal{S}$. Second, since $a \in [a]$, it is obvious that $[a] \neq \emptyset$. Third, if $[a] \cap [b] \neq \emptyset$, then there is some $x \in [a] \cap [b]$, so aRx and bRx, so xRb, so aRb, and by what we have already proved, $[a] = [b]$. These are the three conditions that define a partition, so we have proved that $\mathcal{S}$ is a partition of A.

Example: Let $A = \{1, 2, 3, 4, 5, 6, 7, 8\}$, and define R by aRb whenever $a - b$ is an integer multiple of 3. Then R is reflexive, since for all a, $a - a = 0$ is a multiple of 3; and R is symmetric, since if aRb, then $a - b = 3x$, so $b - a = 3(-x)$ and bRa; and R is transitive, since if aRb and bRc then $a - b = 3x$ and $b - c = 3y$, so $a - c = (a - b) + (b - c) = 3(x + y)$, and therefore aRc. The equivalence classes are $[1] = \{1, 4, 7\} = [4] = [7]$ and $[2] = \{2, 5, 8\} = [5] = [8]$ and $[3] = \{3, 6\} = [6]$, and the set of equivalence classes, $\mathcal{S} = \{\{1, 4, 7\}, \{2, 5, 8\}, \{3, 6\}\}$, forms a partition of A.

Lecture no. 14.

Return to considering more general relations. Define the *matrix of a relation*, useful for computer storage of some relations, and we can recognise reflexive and symmetric relations from the matrix. The *inverse* relation of $R \subseteq A \times B$ is

$R^{-1} = \{(b,a)|(a,b) \in R\} \subseteq B \times A$. If $R \subseteq A \times B$ and $S \subseteq B \times C$, then the *composition* of R and S is $S \circ R$ defined by $S \circ R = \{(a,c)|\exists b \in B$ such that $(a,b) \in R$ and $(b,c) \in S\}$.

So far we have only considered *binary* relations, that is subsets of Cartesian products $A \times B$. Similarly we can define *ternary* relations, which are subsets of $A \times B \times C$, or more generally, n-ary relations, which are subsets of $A_1 \times A_2 \times \cdots \times A_n$, say. Example: 'between' is a ternary relation on real numbers.

Informal definition of functions. Examples.

Lecture no. 15.

Also more formal: a relation $f \subseteq A \times B$ is a function if and only if for all $a \in A$, there is a unique $b \in B$ with $(a,b) \in f$. More normal notation for $(a,b) \in f$ is $f(a) = b$, and if $f \subseteq A \times B$ we prefer to write $f : A \to B$.

Almost everything in computer programming can be considered to be a function: e.g. $+$ is a function from $\mathbb{R} \times \mathbb{R}$ to $\mathbb{R}$.

If f is a function from A to B, then (in the sense defined earlier for relations) the domain of f is A, and in general the range is a subset of B. If the range is actually the whole of B, then f is called *onto*, or *surjective*. This means that every element of B occurs as $f(a)$ for some a. In general it may occur as $f(a)$ for many different values of a: a function where this does not happen is called *one-to-one*, or *injective*. A function which is both injective and surjective is called *bijective*—in such a function, each element of A gives rise to a unique element of B, and *vice versa*, so this is sometimes called a *one-to-one-correspondence*.

Lecture no. 16.

Examples of functions which are or are not injective, surjective, bijective. Definition of inverse relation of a function f. Discussion of when it is an inverse function: we need f to be surjective and injective, i.e. bijective. In fact f has an inverse function if and only if it is bijective. Examples: $f = \{(1,c),(2,a),(3,b)\}$ is a bijection between $A = \{1,2,3\}$ and $B = \{a,b,c\}$ and has an inverse function $f^{-1} = \{(c,1),(a,2),(b,3)\}$. Similarly $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^3$ has inverse function $f^{-1}(y) = \sqrt[3]{y}$.

Lecture no. 17.

The idea of an *algorithm* as a precise set of instructions for computing a function. Thus it should have the properties of:

1. **Precision.** To enable a computer to follow the instructions.
2. **Input.**
3. **Output.**
4. **Uniqueness.** The output (and intermediate steps) are uniquely determined by the input.

5. **Generality.** It should apply to a whole set of possible inputs.

6. **Finiteness.** It must stop and output the answer after a finite nunber of steps.

Example: the Division Algorithm—If a and b are positive integers, to divide a by b and get a quotient q and remainder r (satisfying $a = bq + r$ and $0 \leq r < b$).

Example: Euclid's algorithm. If a and b are positive integers, then c is a *common divisor* if c divides a and c divides b. Define also the *greatest common divisor*, written g.c.d.(a, b). Then if $a = bq + r$ we can show that g.c.d.$(a, b) =$ g.c.d.(b, r). Hence by repeated application of the division algorithm we eventually get a remainder of 0, at which point b is the greatest common divisor. Working backwards, we can express g.c.d.(a, b) in the form $ax + by$ where x and y are integers (in fact one will be positive and the other negative). Examples.

Chapter 3

Counting methods

Lecture no. 18.

Multiplication principle. That is, $|A \times B| = |A| \times |B|$. Example: if a set has n elements, then it has 2^n subsets. Addition principle. That is, if A and B are disjoint sets, then $|A \cup B| = |A| + |B|$. In general, $|A \cup B| = |A| + |B| - |A \cap B|$, since the elements of $|A \cap B|$ have been counted twice. (This is the simplest case of *inclusion–exclusion*.) Generalize this to $|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$. First proof: how many times is each element counted? Second proof: formally from the previous result. Examples.

Lecture no. 19.

Permutations and combinations. Define: r-permutation of n things. The number of such is $P(n,r) = n(n-1)\dots(n-r+1)$. Define: r-combinations of n things. Here the ordering of the r things doesn't matter, so the number of such things is $C(n,r) = P(n,r)/n!$ Examples. (Poker hands, etc.)

Lecture no. 20.

Generalised permutations and combinations. Example: number of 'anagrams' of MISSISSIPPI is $\frac{11!}{4!4!2!1!}$. The general formula. Another example; number of ways of distributing six pints of beer between John, Fred and Tom. Another example: the coefficient of $x^2y^3z^4$ in the expansion of $(x+y+z)^9$.

Lecture no. 21.

Either some formulae like

$$\sum_{k=0}^{n} C(n,k) = 2^n$$

and the binomial theorem; or more examples of what we've just done; or revision.

Lecture no. 22.

Revision.

Unfortunately, the graph theory seems to have fallen off the end of the syllabus.