MA251 Combinatorics

1. Binomial coefficients

1A The definitions For integers r, n with $0 \le r \le n$ we have four possible definitions of the binomial coefficient ${}^nC_r$:

(i) ${}^nC_r = \frac{n!}{r!(n-r)!}$;

(ii) ${}^nC_r$ is the number of subsets of size r of a given set of size n;

(iii) ${}^nC_r$ is the number appearing in Pascal's triangle

$$\begin{array}{ccccccccc} &&&&1&&&& \\ &&&1&&1&&& \\ &&1&&2&&1&& \\ &1&&3&&3&&1& \\ 1&&4&&6&&4&&1 \\ &&&&\ldots&&&& \end{array}$$

(as the $(r+1)$-st number in the $(n+1)$-st line);

(iv) ${}^nC_r$ is the coefficient of a^rb^{n-r} in the binomial expansion of $(a+b)^n$.

The importance of these numbers is signalled by this variety of different ways in which they can be described. My own preference is for (ii); I believe that this is really the root reason why binomial coefficients turn up so often.

1B Proof of equality We must check that the definitions (i)-(iv) in 1A do indeed all give the same numbers; possible arguments are as follows.

(a) Equivalence of (i) and (ii) Suppose we have a set X with n elements, listed as $\{x_1,\ldots,x_n\}$. Let us count the number of ways of putting these in order. This is just $n!$, because we have n choices for which element we take first, then $n-1$ choices for the second, $n-2$ choices for the third, $\ldots$, finishing with just one choice for the last, making $n(n-1)(n-2)\ldots 1 = n!$ possibilities altogether.

On the other hand, we could do the ordering by the following method:

(α) pick out a set A of r elements of X, to be the first r elements in the final ordering;

(β) put these in order at the front;

(γ) put the elements of $X \setminus A$ in order at the back.

If we followed this scheme, we should have $\#([X]^r)$ choices at step (α), where

$$[X]^r = \{A : A \subseteq X,\ \#(A) = r\}$$

is the set of r-element subsets of X; $r!$ choices at step (β), because $\#(A) = r$; and $(n-r)!$ choices at step (γ), because $\#(X \setminus A) = n-r$. So this makes $r!(n-r)!\#([X]^r)$ ways of doing it altogether, and this must be equal to $n!$, got by counting the same set in a different way. Thus

$$n! = r!(n-r)!\#([X]^r), \quad \#([X]^r) = \frac{n!}{r!(n-r)!},$$

which is what we had to prove, since 1A(i) defines ${}^nC_r$ to be $\frac{n!}{r!(n-r)!}$, while 1B(ii) defines it to be $\#([X]^r)$.

Equivalence of (i) and (iii) Induce on n. For this argument, write ${}^nC_r$ for $\frac{n!}{r!(n-r)!}$ and $P_{n,r}$ for the corresponding number in Pascal's triangle. Then

$$P_{0,0} = 1 = \frac{0!}{0!0!} = {}^0C_0,$$

These notes are made available to students on the understanding that they have not been properly checked for errors, nor do they necessarily cover the topics to be examined in the course, which are determined by the material covered in lectures.

and if $n = 0$ this is the only thing to check, so the induction starts. For the inductive step to $n \geq 1$,

$$P_{n,0} = 1 = \frac{n!}{0!n!} = {}^0C_n, \quad P_{0,n} = 1 = \frac{n!}{n!0!} = {}^nC_n,$$

and if $0 < r < n$,

$$P_{n,r} = P_{n-1,r-1} + P_{n-1,r}$$

(because that's how Pascal's triangle works – you get $P_{n,r}$ by adding up the two numbers above it)

$$= {}^{n-1}C_{r-1} + {}^{n-1}C_r = \frac{(n-1)!}{(r-1)!((n-1)-(r-1))!} + \frac{(n-1)!}{r!(n-1-r)!}$$

(by the inductive hypothesis)

$$= \frac{(n-1)!}{r!(n-r)!}(r + n - r) = \frac{n!}{r!(n-r)!} = {}^nC_r$$

as required, and the induction proceeds.

Equivalence of (iii) and (iv) Induce on n. For $n = 0$,

$$(a+b)^n = 1 = P_{0,0}a^0b^0;$$

for $n = 1$,

$$(a+b)^1 = b + a = P_{1,0}a^0b^1 + P_{1,1}a^1b^0.$$

For the inductive step to $n \geq 2$,

$$(a+b)^n = (a+b)(a+b)^{n-1} = (a+b)\sum_{r=0}^{n-1} P_{n-1,r}a^rb^{n-1-r}$$

(by the inductive hypothesis)

$$= \sum_{r=0}^{n-1} P_{n-1,r}a^{r+1}b^{n-1-r} + \sum_{r=0}^{n-1} P_{n-1,r}a^rb^{n-r}$$

$$= \sum_{k=1}^{n} P_{n-1,k-1}a^kb^{n-k} + \sum_{r=0}^{n-1} P_{n-1,r}a^rb^{n-r}$$

(substituting $k = r+1$, $r = k-1$)

$$= \sum_{r=1}^{n} P_{n-1,r-1}a^rb^{n-r} + \sum_{r=0}^{n-1} P_{n-1,r}a^rb^{n-r}$$

$$= P_{n-1,0}a^0b^n + \sum_{r=1}^{n-1}(P_{n-1,r-1} + P_{n-1,r})a^rb^{n-r} + P_{n-1,n-1}a^nb^0$$

$$= b^n + \sum_{r=1}^{n-1} P_{n,r}a^rb^{n-r} + a^n = \sum_{r=0}^{n} P_{n,r}a^rb^{n-r},$$

and the induction proceeds.

Remarks (a) There are two not-quite-standard notations above. (i) I use $\#(X)$ for the number of elements in X. Algebraists (e.g., Dr Higgins) tend to write $|X|$. I'm an analyst, and when I see $|\ |$ I think of the absolute value of a real number, or the modulus of a complex number: $|-2| = 2$, $|3+4i| = 5$. I think that counting is important enough to have its own symbol not used for anything else. (ii) The notation $[X]^r$ for the collection of subsets of X of size r is becoming standard at research level, but hasn't percolated to elementary textbooks yet. I think it's jolly convenient.

(b) In the proof of the equivalence of (i) and (ii), I used the ' double-counting' method: write down an appropriate set and count it in two different ways. This is one of the most important techniques in combinatorics.

1C Some identities I suppose there must be literally hundreds of useful formulae which have been found connecting binomial coefficients. The great majority correspond to different ways of counting particular sets. I give here just a handful of the most important ones. (Some others are in the problem sheet.)

(a) ${}^nC_r = {}^nC_{n-r}$ whenever $0 \le r \le n$.
(b) $\sum_{r=0}^{n} {}^nC_r = 2^n$ for every $n \ge 0$.
(c) $\sum_{r=0}^{n} (-1)^r\, {}^nC_r = 0$ for every $n \ge 1$.
(d) $\sum_{r=0}^{n} r\, {}^nC_r = 2^{n-1}n$ for every $n \ge 0$.

proofs (a) $\frac{n!}{r!(n-r)!} = \frac{n!}{(n-r)!r!}$.

(a)$'$ If $\#(X) = n$, we have a bijection $a \mapsto X \setminus a$ from $[X]^r$ to $[X]^{n-r}$. So $[X]^r$ and $[X]^{n-r}$ must have the same number of members.

(b) $\sum_{r=0}^{n} {}^nC_r = \sum_{r=0}^{n} {}^nC_r 1^r 1^{n-r} = (1+1)^n = 2^n$.

(b)$'$ If $\#(X) = n$, then

$$\sum_{r=0}^{n} \#([X]^r) = \#(\mathcal{P}X) = 2^n,$$

writing $\mathcal{P}X$ for the family of subsets of X.

(c) $\sum_{r=0}^{n} (-1)^r\, {}^nC_r = \sum_{r=0}^{n} {}^nC_r (-1)^r 1^{n-r} = (-1+1)^n = 0$.

(c)$'$ If $\#(X) = n$, then

$$\begin{aligned}\sum_{r=0}^{n} (-1)^r \#([X]^r) &= \sum_{r \text{ is odd}} \#([X]^r) - \sum_{r \text{ is even}} \#([X]^r) \\ &= \#(\mathcal{A}_{\text{even}}) - \#(\mathcal{A}_{\text{odd}}),\end{aligned}$$

writing $\mathcal{A}_{\text{even}}$ for the family of subsets of X with an even number of members, $\mathcal{A}_{\text{odd}}$ for the family of subsets of X with an odd number of members. But if we fix any particular $x \in X$, we have a bijection $a \mapsto a \triangle \{x\} : \mathcal{A}_{\text{even}} \to \mathcal{A}_{\text{odd}}$, so these two sets must have the same number of members.

(d) If $n = 0$,

$$0.\frac{0!}{0!0!} = 0 = 2^{-1} \times 0.$$

If $n \ge 1$,

$$\sum_{r=0}^{n} r \frac{n!}{r!(n-r)!} = \sum_{r=1}^{n} r \frac{n!}{r!(n-r)!} = \sum_{r=1}^{n} \frac{n!}{(r-1)!(n-r)!} = \sum_{k=0}^{n-1} \frac{n!}{k!(n-k-1)!}$$

(substituting $k = r-1$, $r = k+1$)

$$= n \sum_{k=0}^{n-1} \frac{(n-1)!}{k!(n-1-k)!} = 2^{n-1}n$$

using (b).

(d)$'$ Let X be a set with n elements, and consider the set $R = \{(x, a) : x \in a \subseteq X\}$. We can calculate $\#(R)$ in two ways:

(α) There are n ways of choosing x; having chosen x, there are 2^{n-1} ways of choosing A, since we have to put x into A, and there are then $n-1$ other points to decide.

(β) If we set $R_r = \{(x, A) : x \in A \in [X]^r\}$, then $\#(R) = \sum_{r=1}^{n} \#(R_r)$, because $R = R_1 \cup R_2 \cup \ldots R_n$ and the different R_r don't overlap. Now to count each R_r, we choose first $A \in [X]^r$ – there are $\#([X]^r)$ ways of doing this – and then x, for which we shall have r different choices. So

$$\#(R_r) = r\#([X]^r) \text{ for each } r,$$

$$2^{n-1}n = \#(R) = \sum_{r=1}^{n} \#(R_r) = \sum_{r=1}^{n} r\#([X]^r) = \sum_{r=0}^{n} r\#([X]^r).$$

(d)″

$$2\sum_{r=0}^{n} r\ {}^nC_r = \sum_{r=0}^{n} r\ {}^nC_r + \sum_{r=0}^{n} r\ {}^nC_{n-r}$$

(using (a))

$$= \sum_{r=0}^{n} r\ {}^nC_r + \sum_{k=0}^{n} (n-k)\ {}^nC_k$$

(substituting $k = n - r$, $r = n - k$ in the second sum)

$$= \sum_{r=0}^{n} r\ {}^nC_r + \sum_{r=0}^{n} (n-r)\ {}^nC_r = \sum_{r=0}^{n} n\ {}^nC_r = 2^n n$$

using (b).

(d)‴ If $n \ge 1$,

$$\frac{1}{\#(\mathcal{P}X)} \sum_{r=0}^{n} r\#([X]^r)$$

is the average size of a randomly chosen subset of X, which is just $\frac{n}{2}$.

Remark I used the notation '$A\triangle\{x\}$' above. Recall that for any sets A, B,

$$A \setminus B = \{y : y \in A, y \notin B\}, \quad A\triangle B = (A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B).$$

So $A\triangle\{x\}$ is $A \cup \{x\}$ if $x \notin A$, and $A \setminus \{x\}$, that is, A with the point x thrown away, if $x \in A$.

1D Induction I have used 'induction' in some of the arguments above; perhaps I ought to run very quickly through the material (covered by MA181, which you're supposed to have done) which you need to know.

Recall that a **partially ordered set** is a set X together with a relation $\le$ such that

$x \le x$ for every $x \in X$ ($\le$ is 'reflexive')

if $x \le y$ and $y \le z$ then $x \le z$ ($\le$ is 'transitive')

if $x \le y$ and $y \le x$ then $x = y$ ($\le$ is 'antisymmetric').

A **totally ordered set** is a partially ordered set $(X, \le)$ such that for any $x, y \in X$ either $x \le y$ or $y \le x$. A **well-ordered set** is a totally ordered set $(X, \le)$ such that every non-empty subset of X has a least member.

The basic principle of induction is this: if X is a well-ordered set, and $P(.)$ is some property of members of X, then either $P(x)$ for every $x \in X$, or $A = \{x : P(x) \text{ is false}\}$ is non-empty, and in the latter case there is a least $x \in X$ for which $P(x)$ is false. So if you can prove that there isn't a *least* $x \in X$ for which $P(x)$ is false, then you've proved that $P(x)$ is true for every x.

The most important well-ordered sets, and practically the only ones we need for this course, are the sets

$$\mathbb{N} = \{1, 2, 3, \dots\},$$

$$\mathbb{N} \cup \{0\} = \{0, 1, 2, \dots\}.$$

These correspond directly to the

1E Second Principle of Induction Suppose that $P(.)$ is a property of natural numbers, and $P(n)$ is true whenever $P(i)$ is true for every $i < n$, then in fact $P(n)$ is true for every n.

proof ? If there were any n for which $P(n)$ was false, then there would be a least one, and then we should have an n such that $P(n)$ is false but $P(i)$ is true for every $i < n$; which is what the hypothesis says can't happen. **X**

1F An alternative principle which many people find a bit easier to grasp is the

First Principle of Induction Suppose that $P(.)$ is a property of natural numbers, that $P(1)$ is true and that $P(n+1)$ is true whenever $P(n)$ is true. Then in fact $P(n)$ is true for every n.

proof ? If it weren't, then there would be a first k for which $P(k)$ was false. We can't have $k = 1$, because we checked that $P(1)$ was true. So we must have $k \geq 2$ and $n = k-1 \in \mathbb{N}$. But now $P(n)$ is true (because $n < k$) and $P(n+1)$ is false, which is also supposed to be impossible. **X**

Remarks (a) You will see that I put the Second Principle of Induction first. This is because of the direction I approached from. Of course 'well-ordered sets' are a relatively modern invention (late 1800s I think), while 'induction' goes back to the ancient Greeks.

It's my own experience that in practice it's usually right to think in terms of the Second Principle, as being the more powerful one. In 1B-1C above, I used the phrase 'inductive step to n'; what I mean by this is, assuming that $P(i)$ is true for every $i < n$, let's try to prove $P(n)$. In fact I think the arguments there could be done with the First Principle, because I think we only needed to know $P(n-1)$ in each case.

(b) I have stated both the First and Second Principles of Induction in terms of the set $\mathbb{N} = \{1, 2, \dots\}$, but that's only because we have a simple name for it. I hope it is obvious that exactly the same ideas apply to $\{0, 1, 2, \dots\}$; the only difference is that at the 'base step' when applying the First Principle we have to check $P(0)$ rather than $P(1)$. Indeed, for the work of this course, inductions will start at 0 as often as they start at 1. I expect there will also be inductions starting at 2, corresponding to the well-ordered set $\{2, 3, 4, \dots\}$.

1G A computation Let me show you how to calculate

$$k = \sum_{r\equiv 0 \bmod 3}^{n} C_r = \#(\{a : a \subseteq X, \#(a) \text{ is divisible by} 3\}$$

if $\#(X) = 3$.

Set $\omega = e^{2\pi i/3} = -\frac{1}{2} + \frac{i\sqrt{3}}{2}$, so that $1 + \omega = \frac{1}{2} + \frac{i\sqrt{3}}{2} = e^{\pi i/3}$. Consider

$$\gamma_n = \mathcal{R}\mathrm{e}((1+\omega)^n) = \sum_{r=0}^{n} \frac{n!}{}^{n} C_r \, \mathcal{R}\mathrm{e}(\omega^r)$$

$$= \sum_{a\subseteq X} \mathcal{R}\mathrm{e}(\omega^{\#(a)}) = k - \tfrac{1}{2}(2^n - k)$$

(because if $\#(a)$ is divisible by 3 then $\omega^{\#(a)} = 1 = \mathcal{R}\mathrm{e}(\omega^{\#(a)}$, and this happens k times, while if $\#(a)$ is not divisible by 3 then $\mathcal{R}\mathrm{e}(\omega^{\#(a)}) = -\frac{1}{2}$, and this happens $2^n - k$ times)

$$= \tfrac{3}{2}k - 2^{n-1},$$

so that $k = \frac{1}{3}2^n + \frac{2}{3}\gamma_n$. Now this means that

if $n \equiv 0 \bmod 6$, $\gamma_n = 1$ and $k = \frac{1}{3}2^n + \frac{2}{3}$,

if $n \equiv 1$ or $n \equiv 5 \bmod 6$, $\gamma_n = \frac{1}{2}$ and $k = \frac{1}{3}2^n + \frac{1}{3}$,

if $n \equiv 2$ or $n \equiv 4 \bmod 6$, $\gamma_n = -\frac{1}{2}$ and $k = \frac{1}{3}2^n - \frac{1}{3}$,

if $n \equiv 3 \bmod 6$, $\gamma_n = -1$ and $k = \frac{1}{3}2^n - 1$.

1H Similarly, we can compute

$$k = \textstyle\sum_{r\equiv 0 \bmod 4}^{n} C_r$$

by taking

$$\gamma_n = \mathcal{R}\mathrm{e}((1+i)^n) = \sum_{r=0}^{n} {}^nC_r i^r$$

$$= \sum_{r\equiv 0 \bmod 4}^{n} C_r - \sum_{r\equiv 2 \bmod 4}^{n} C_r = k - (2^{n-1} - k)$$

(because

$$\sum_{r\equiv 0 \bmod 4}^{n} C_r + \sum_{r\equiv 2 \bmod 4}^{n} C_r = \sum_{r\equiv 0 \bmod 2}^{n} C_r = 2^{n-1}$$

if $n \geq 1$). So $k = 2^{n-2} + \frac{1}{2}\gamma_n$, and

if $n \equiv 0 \bmod 8$, $\gamma_n = 2^{n/2}$, $k = 2^{n-2} + 2^{(n-2)/2}$,
if $n \equiv 1$ or $n \equiv 7 \bmod 8$, $\gamma_n = 2^{(n-1)/2}$, $k = 2^{n-2} + 2^{(n-3)/2}$,
if $n \equiv 2$ or $n \equiv 6 \bmod 8$, $\gamma_n = 0$, $k = 2^{n-2}$,
if $n \equiv 3$ or $n \equiv 5 \bmod 8$, $\gamma_n = -2^{(n-1)/2}$, $k = 2^{n-2} - 2^{(n-3)/2}$,
if $n \equiv 4 \bmod 8$, $\gamma_n = -2^{n/2}$, $k = 2^{n-2} - 2^{n/2}$.

amsppt.styma251b2.tex Version of 2.3.96

2. Graphs

2A Definition By a **graph** I will mean, in this course, an object $G = (V, E)$ where V is a set of **vertices**, E is a set of **edges**, and

(i) each edge links two distinct vertices, its **endpoints**,
(ii) each pair of vertices is linked by at most one edge.

If you like, you can think of an edge e as being actually the doubleton set $\{a, b\}$ where a and b are its endpoints, so that $E \subseteq [V]^2$. This makes it a little more difficult to move across to other related concepts such as *directed graphs* and *multigraphs*; but I'm not going to discuss these in this course anyway.

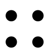
2B Small graphs (a) If $V = \emptyset$ we must have $E = \emptyset$; end of story. The picture is

(b) If $\#(V) = 1$ then again we must have $E = \emptyset$.

(c) If $\#(V) = 2$ there are two possibilities. Either the two vertices are linked by an edge, or they aren't. So the pictures are

(d) If $\#(V) = 3$ there are four possibilities, according to what $\#(E)$ is:

(e) If $\#(V) = 4$ things are more complicated, because even when we know the number of edges there may be more than one possibility. If there are no edges then we must have



If there is just one edge we must have

If there are two edges, they may be separate, or they may share a vertex

If there are three edges, they may form a line, or a three-pointed star, or a triangle

If there are four edges, they may form a square or a triangle with a handle

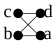
If there are five edges, there is just one missing

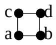
and if there are six edges, there isn't

2C Making sense of the lists (a) It takes care and discipline to get every single graph, once and once only – I mean, noticing that

are the 'same' graph, because you get one from the other just by exchanging a couple of points and pulling the edges across with them. These graphs are **isomorphic**, that is, can be turned into each other by re-labelling the vertices

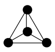




Similarly,

are isomorphic, and

are isomorphic.

(b) There are some standard tricks for checking that our lists are right, or at least for avoiding some kinds of mistake. The first idea is that of 'degree' of a vertex. If $G = (V, E)$ is any graph and $v \in V$ is a vertex, then the **degree** of v is the number of edges of which v is an endpoint. Now if two graphs are isomorphic, the lists of degrees of their vertices must be the same. For instance, among the three graphs with four vertices and three edges, only one of them (the middle one) has a vertex of degree 3 and only one (the right-hand one) has a vertex of degree 0; so that these three are certainly not isomorphic.

(c) Another way of testing the lists is through the idea of 'complement'. If $G = (V, E)$ is a graph, its **complement** is the graph $\overline{G} = (V, \overline{E})$ with the same set of vertices but with exactly the opposite set of edges, so that the two graphs

are complements of each other. (Of course

are isomorphic.) This is why there are two 'different' graphs with four vertices and two edges, and also two different graphs with four vertices and four edges; they are in complementary pairs

One of the graphs with four vertices and three edges is isomorphic to its own complement:

When listing graphs, you should always check your lists to see that you have the complements of the graphs you have found.

(d) While giving definitions, let me add a word which I shall be using a great deal: the **order** of a graph $G = (V, E)$ is just the number of its vertices, $\#(V)$. Thus in 2B above I have listed all the graphs of order 4 or less, or rather, I have listed 19 graphs such that every graph of order 4 or less is isomorphic to exactly one of them.

2D More definitions Let $G = (V, E)$ be a graph. A **path** in G is a string $(v_0\, v_1\, v_2\, \ldots\, v_n)$ of vertices such that every successive pair v_{i-1}, v_i are linked by an edge in G. We say that the path is **simple** if all the v_i are distinct, except possibly that $v_0 = v_n$, and **closed** if indeed $v_0 = v_n$ (so that the path returns to its starting point). The **length** of the path is the number of edges (so that the length of $(a\,b\,c)$ is 2). It is convenient to allow a singleton vertex (v_0) to count as a path of length 0. A **cycle** is a simple closed path of length at least 3. G is **connected** if any two vertices can be linked by a path. Thus the connected graphs of order 4 are

G is a **tree** if it is connected and has no cycles; thus the trees of order 4 are

2E Lemma Suppose that $G = (V, E)$ is a graph and a, b two vertices of G which can be joined by a path in G. Then they can be joined by a simple path.

proof Since there is a path from a to b, there is a shortest path. (If we write A for the set of lengths of paths from a to b, this is a non-empty subset of $\mathbb{N} \cup \{0\}$, so has a least member.) Call such a path P. (Of course there might be more than one path of the same length; if so, it won't matter which we take.) Then P is simple. **P?** If it weren't, say $P = (v_0\, v_1\, \dots\, v_n)$ where $a = v_0$ and $b = v_n$, then there would be $i < j$ such that $v_i = v_j$. But in this case

$$P' = (v_0\, \dots\, v_i\, v_{j+1}\, \dots\, v_n)$$

would be a strictly shorter path from a to b. **XQ**

Remark The formula for P' is a little misleading if $j = n$; in this case what we want is just $(v_0\, \dots\, v_i)$, since $v_i = v_n = b$. But we still get a strictly shorter path.

2F Components Let $G = (V, E)$ be a graph. For $x, y \in V$ write $x \sim y$ if there is a path from x to y in G. Then $\sim$ is an equivalence relation on V. **P** (i) Since I allow paths of zero length, $x \sim x$ for every $x \in V$, and the relation is reflexive. (ii) If $(x\, v_1\, \dots\, v_{n-1}\, y)$ is a path from x to y, then $(y\, v_{n-1}\, \dots\, , v_1\, x)$ is a path from y to x. So $\sim$ is symmetric. (iii) If $(x\, v_1\, \dots\, v_{n-1}\, y)$ is a path from x to y, and $(y\, w_1\, \dots\, w_{m-1}\, z)$ is a path from y to z, then

$$(x\, v_1\, \dots\, v_{n-1}\, y\, w_1\, \dots\, w_{m-1}\, z)$$

is a path from x to z, so $\sim$ is transitive. **Q**

The equivalence classes in V under this relation are called the **components** of the graph G. For each $x \in V$, the component containing x is just the set of points which can be reached from x by paths.

If $W \subseteq V$ is any set, the **restriction** of G to W, $G{\restriction}W$, is the graph (W, E_W) where E_W consists of those edges in E such that both ends belong to W. Now if C is a component of G, $G{\restriction}C$ is connected. The graph G is defined by these restrictions to its components, because we know that there are no edges between different components, so that if we know all the $G{\restriction}C$ we shall know G. For most of the problems of graph theory, indeed, once we understand connected graphs we're home, since general graphs are got just by putting connected graphs side by side.

2G Which graphs are trees? There is an elegant characterization of 'trees' in terms of numbers of edges and vertices, which I approach through the following proposition.

Propostion Let $G = (V, E)$ be a finite graph, and $\mathcal{C}$ the set of its components (see 2F). Then

$$\#(E) + \#(\mathcal{C}) \geq \#(V),$$

with equality iff G has no cycles.

Remark If you like, you can think of the formula above as

$$e + c \geq v,$$

so long as you don't get into a muddle by using the letters e, v for the numbers $\#(E)$, $\#(V)$ of edges and vertices when we generally use them to represent individual edges and vertices.

proof Induce on $m = \#(E)$. If $m = 0$, then G has no edges, so no two distinct vertices are connected by a path, and every component is a singleton $\{v\}$; thus

$$\#(V) = \#(\mathcal{C}) = \#(\mathcal{C}) + \#(E).$$

Also, of course, there are no cycles.

For the inductive step to $m \geq 1$, take any edge $e \in E$ and consider $G' = G - e = (V, E')$, where $E' = E \setminus \{e\}$. Let a, b be the endpoints of e, and write $\mathcal{C}'$ for the set of components of G'. We have to consider two cases:

case 1 Suppose that a and b belong to different components V_1 and V_2 of G'. In this case, because a and b are linked in G by the edge e, $V_1 \cup V_2$ becomes a component of G, while all the other components of G' remain components in G. So $\#(\mathcal{C}) = \#(\mathcal{C}') - 1$, while $\#(E) = \#(E') + 1$. By the inductive hypothesis, because $\#(E') = m - 1$,

$$\#(V) \leq \#(E') + \#(\mathcal{C}') = \#(E) + \#(\mathcal{C}).$$

As for cycles, any cycle of G' is surely a cycle in G; but also, any cycle in G is a cycle in G'. **P?** If not, it would have to have the edge e as one of its links. But now the rest of the cycle would be a path between a and b in G', which is impossible, because a and b are in different components of G'. **XQ** So we get

$$\begin{aligned} G \text{ has a cycle} &\iff G' \text{ has a cycle} \\ &\iff \#(V) < \#(E') + \#(\mathcal{C}') \end{aligned}$$

(by the inductive hypothesis)

$$\iff \#(V) < \#(E) + \#(\mathcal{C}).$$

Thus the induction continues.

case 2 Suppose a and b belong to the same component V_0 of G'. Then V_0 remains a component of G, and so do all other components of G', so $\mathcal{C}' = \mathcal{C}$ and

$$\#(E) + \#(\mathcal{C}) = \#(E') + 1 + \#(\mathcal{C}') \geq \#(V) + 1 > \#(V)$$

by the inductive hypothesis. Moreover, there is a path from a to b in G', and therefore a simple path (2E); suppose it is $(a \ldots b)$; then we can add a at the end to make a cycle $(a \ldots b\, a)$ in G, as required. Thus in this case also the induction continues.

2H Corollary Let $G = (V, E)$ be a non-empty finite graph. Then the following are equiveridical:
(i) G is a tree;
(ii) G is connected and $\#(V) \geq \#(E) + 1$;
(iii) G has no cycles and $\#(V) \leq \#(E) + 1$;
and in this case $\#(V) = \#(E) + 1$.

proof (a) If G is a tree, then (by definition) it is connected and has no cycles, so (because it is not empty) it has exactly one component, and

$$\#(V) = \#(E) + 1$$

by 2G. Thus (i) implies (ii) and (iii).

(b) If (ii) is true, then again $\#(V) \leq \#(E) + 1$, by 2G, and since we must in this case have equality, 2G tells us that there are no cycles, that is, that G is a tree.

(c) Finally, if (iii) is true, then by 2G we have $\#(V) = \#(E) + \#(\mathcal{C})$, where $\mathcal{C}$ is the set of components of G, so $\#(\mathcal{C}) \leq 1$; thus G is connected and must be a tree.

2I Adding degrees: Lemma In any finite graph $G = (V, E)$,

$$\textstyle\sum_{v \in V} d(v) = 2\#(E).$$

proof Consider the set

$$R = \{(v, e) : v \in V,\ e \in E,\ v \text{ is an endpoint of } e\}.$$

Then

$$\begin{aligned} \#(R) &= \sum_{v \in V} \#(\{e : (v, e) \in R\}) = \sum_{v \in V} d(v) \\ &= \sum_{e \in E} \#(\{v : (v, e) \in R\}) = 2\#(E). \end{aligned}$$

2J Proposition Suppose that $G = (V, E)$ is a non-empty finite graph in which every vertex has degree at least 2. Then G has a cycle of length at least 3.

proof By 2I,

$$\#(E) = \tfrac{1}{2} \textstyle\sum_{v \in V} d(v) \geq \#(V).$$

Also, because $V \neq \emptyset$, the set $\mathcal{C}$ of components of G is also not empty, so $\#(E) + \#(\mathcal{C}) > \#(V)$; by 2G, G has a cycle.

***2K Counting trees** There is a beautiful result (Theorem 2M below) giving the total number of trees which can be formed on a given set of vertices; unfortunately it must be regarded as outside the syllabus of this course, but I write it out anyway. First a definition: if $G = (V, E)$ is a graph, a **leaf** in G is a vertex of degree precisely 1.

***2L Lemma** If $L \subseteq V$, write $\mathcal{T}_{VL}$ for the set of trees with vertex set V in which L is the set of leaves. If W is any set and $n \in \mathbb{N}$, write F_{nW} for the set of surjective functions from $\{1, \ldots, n\}$ onto W. Then whenever $n \geq 3$, V is a set of size n, and $L \subseteq V$,

$$\#(F_{n-2,V \setminus L}) = \#(\mathcal{T}_{VL}).$$

proof (a) Note first that any tree on a set of two or more vertices must have a leaf. **P** Because it is connected, every vertex has degree at least 1. Because there is no cycle, there must be a vertex of degree less than 2, by 2J. **Q**

So if $\#(V) = n \geq 3$ and $L = \emptyset$, $\mathcal{T}_{VL} = \emptyset$; but also $F_{n-2,V \setminus L} = \emptyset$ because $\#(V \setminus L) > n - 2$. So in this case

$$\#(F_{n-2,V \setminus L}) = 0 = \#(\mathcal{T}_{VL}).$$

(b) Now induce on n.

(i) If $n = 3$, then the only trees on V are simple chains with two leaves, and there is just one of them for each doubleton set of leaves; while $F_{1,V \setminus L} = \emptyset$ unless $V \setminus L$ is a singleton, and in this case has just one element. So we have

$$\begin{aligned} \#(F_{1,V \setminus L}) = \#(\mathcal{T}_{VL}) &= 0 \text{ if } \#(L) \neq 2, \\ &= 1 \text{ if } \#(L) = 2. \end{aligned}$$

(ii) For the inductive step to $n > 3$, take $L \subseteq V$ where $\#(V) = n$. If $L = \emptyset$ then $\#(F_{n-2,V}) = \#(\mathcal{T}_{V\emptyset}) = 0$, by (a). If $L \neq \emptyset$, take any $v \in L$.

(α) If $T \in \mathcal{T}_{VL}$, then v is linked by an edge in T to exactly one $u \in V$, and $u \notin L$, because otherwise $\{u, v\}$ would be a component of T. So

$$\#(\mathcal{T}_{VL}) = \textstyle\sum_{u \in V \setminus L} \#(\{T : T \in \mathcal{T}_{VL},\ v \text{ is linked to } u \text{ in } T\}).$$

On the other hand, if $T \in \mathcal{T}_{VL}$ and v is linked to u by an edge in T, then $T - v$, the graph obtained from T by deleting the vertex v and the edge $(u\,v)$, is again a tree. The set of leaves of $T - v$ must be either $L' = L \setminus \{v\}$ or $L' \cup \{u\}$; that is, $T - v$ belongs either to $\mathcal{T}_{V',L'}$ or to $\mathcal{T}_{V',L' \cup \{u\}}$, where $V' = V \setminus \{v\}$. Accordingly

$$\#(\mathcal{T}_{VL}) = \textstyle\sum_{u \in V \setminus L} \#(\mathcal{T}_{V'L'}) + \#(\mathcal{T}_{V',L' \cup \{u\}}).$$

(β) Now look at $F_{n-2,V \setminus L}$. Every $f \in F_{n-2,V \setminus L}$ can be identified with a pair (g, u), where $u = f(n-2)$ and g is the restriction of f to $\{1, \ldots, n-3\}$. Moreover, in this case, the set of values of g must be either $V \setminus L = V' \setminus L'$ or $V' \setminus (L' \cup \{u\})$. So the total number of such pairs is

$$\textstyle\sum_{u \in V \setminus L} \#(F_{n-3,V' \setminus L'}) + \#(F_{n-3,V' \setminus (L' \cup \{u\})}),$$

and this is $\#(F_{n-2,V \setminus L})$.

(γ) Putting these together,

$$\begin{aligned} \#(\mathcal{T}_{VL}) &= \sum_{u \in V \setminus L} \#(\mathcal{T}_{V'L'}) + \#(\mathcal{T}_{V',L' \cup \{u\}}) \\ &= \sum_{u \in V \setminus L} \#(F_{n-3,V' \setminus L'}) + \#(F_{n-3,V' \setminus (L' \cup \{u\})}) \end{aligned}$$

(by the inductive hypothesis, since $\#(V') = n - 1 < n$)

$$= \#(F_{n-2,V \setminus L}),$$

as required. Thus the induction proceeds.

*__2M Theorem__ For any $n \geq 1$, the number of trees on a given vertex set V of size n is just n^{n-2}.

proof If $\#(V) = 1$ then the only graph on V is a tree, so the number of trees is $1 = 1^{-1}$. If $\#(V) = 2$ then again there is exactly one tree on V, and $1 = 2^0$. If $\#(V) = n \geq 3$, then the number of trees is

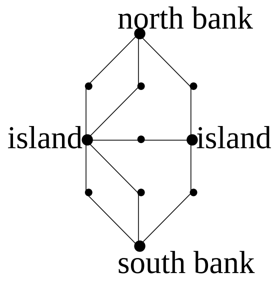
$$\sum_{L \subseteq V} \#(\mathcal{T}_{VL}) = \sum_{L \subseteq V} \#(F_{n-2,V \setminus L}),$$

which is the number of functions from $\{1, \ldots, n-2\}$ to V, since for any such function f there is exactly one set $L \subseteq V$ such that $V \setminus L$ is the set of values of f. But the number of these functions is n^{n-2}, as claimed.

amsppt.styma251b3.tex Version of 31.1.96

3. Eulerian and Hamiltonian Paths

3A Königsberg bridges The river Pregelarme (now Pregelya) in Königsberg (now Kaliningrad) has, or at least in 1735 had, two islands in the middle, with seven bridges: one island connected by a single bridge to each bank, the other island connected by two bridges to each bank, and the two islands joined by a bridge. In those happy days it was the custom of the bourgeoisie to go for evening walks along the river, and the question arose: could one find a walk which crossed every bridge exactly once? Leonhard Euler (1707-1783) showed that you couldn't. He observed that what matters is the graph



with a vertex for each bank, each bridge and each island, and an edge for each end of each bridge. Then a walk which crossed every bridge exactly once would correspond to a path in the graph which used every edge exactly once. Now look at the vertex which corresponds to the north bank. This has degree 3. But that means that you can't manage the three edges at that vertex except by either starting or finishing there; because if you start and finish elsewhere, then every arrival at the north bank must be matched by a departure, and you will be able to use only two of the three edges. The same applies to the south bank and the eastern island, and indeed to the western island as well, since this has degree 5, also an odd number. But this means that the two vertices corresponding to the beginning and end of your walk must somehow cover four vertices, which can't be done.

Euler (being a mathematician) immediately generalized the argument to what, in modern language, becomes the following.

3B Definition Let G be a finite graph. An **Eulerian path** in G is a path using every edge of G exactly once. An **Eulerian circuit** is a closed Eulerian path.

3C Proposition Let $G = (V, E)$ be a connected graph.

(a) If G has an Eulerian circuit then it has no vertices of odd degree, and for any $a \in V$ there is an Eulerian circuit starting and finishing at a.

(b) If G has an Eulerian path which is not a circuit, then G has exactly two vertices of odd degree, and any Eulerian path in G must start at one of these and end at the other.

proof Suppose that $(v_0\, v_1\, \ldots\, v_n)$ is an Eulerian path in G. Then for any $v \in V$, the degree of v is just

$$\#(\{i : i < n,\, v = v_i\}) + \#(\{i : i > 0,\, v = v_i\}),$$

because the first counts the number of steps in the path which start at v, and the second counts the number of steps finishing at v; and every edge with v as an endpoint must appear exactly once as one or other of these. But this sum is necessarily even if v is not equal to v_0 or v_n, odd if $v = v_0 \neq v_n$ or $v = v_n \neq v_0$, and even again if $v = v_0 = v_n$. So if the path is closed, every vertex has even degree, while if it is not closed then v_0 and v_n have odd degree and all other vertices have even degree. Since this marks out v_0 and v_n as the only vertices of odd degree, any other Eulerian path must start at one and end at the other.

If the path is closed, then (because G is connected) it passes through any given vertex a, so we can start and finish the circuit at a.

3D Theorem Suppose that $G = (V, E)$ is a non-empty finite connected graph in which every vertex has even degree. Then it has an Eulerian circuit.

proof Induce on $m = \#(E)$. If $m = 0$ then V must be a singleton $\{v\}$ (because G is non-empty and connected), so that (v) is a trivial Eulerian circuit.

For the inductive step to $m > 0$, we know that G has more than one vertex; because it is connected, $d_G(v) \geq 1$ for every $v \in V$; because every vertex has even degree, $d_G(v) \geq 2$ for every v; so G has a non-trivial cycle $(v_0\, v_1\, \ldots\, v_n)$, where $v_n = v_0$ (2J). Let $G' = (V, E')$ be the graph obtained by deleting all the edges used in this cycle. Then $d_{G'}(v)$ is either $d_G(v) - 2$ (if $v = v_i$ for some i) or $d_G(v)$, and in either case is even, for every $v \in V$. Of course G' need not be connected; let $V_1, \ldots, V_r$ be its components. Then for every $k \leq r$ there is a $j(k)$ such that $v_{j(k)} \in V_k$. **P** Starting from any $a \in V_k$, there is a path Q from a to v_0 in G, because G is connected. This meets the set $\{v_1, \ldots, v_n\}$ in some first point v_i (possibly a itself); now the segment of Q from a to v_i is a path in G', so v_i belongs to the same component of G' as a does, and we can take $j(k) = i$. **Q** Note that if $k < k' \leq r$ then $j(k) \neq j(k')$, because V_k and $V_{k'}$ are disjoint.

For each i with $1 \leq i \leq n$, construct a path P_i as follows. If $i \neq j(k)$ for every k, then P_i will be the trivial path (v_i). If $i = j(k)$, then let G_k be the restriction of G' to V_k (see 2F). This is a connected graph in which every vertex has even degree, and it has at most $m - 3$ edges (because we used at least 3 edges in the cycle $(v_0\, \ldots\, v_n)$). By the inductive hypothesis, G_k has an Eulerian circuit, which we may take as starting and finishing at $v_i = v_{j(k)}$ (see 3Ca); take this circuit for the path P_i.

Now consider the path

$$P = (v_0\, P_1\, P_2\, \ldots\, P_n)$$

in G obtained by putting these paths together, remembering that each P_i ends at v_i, which is linked by an edge in G to the starting vertex v_{i+1} of P_{i+1}. This is an Eulerian circuit in G, because every edge in G is either of the form $(v_{i-1}\, v_i)$ or is an edge in some G_k and therefore appears just once in the corresponding $P_{j(k)}$. Thus the induction continues.

3E Corollary Let $G = (V, E)$ be a connected finite graph in which just two vertices have odd degree. Then G has an Eulerian path.

proof Suppose the two vertices with odd degree are a and b. Take any $c \notin V$ and let G' be the graph (V', E') where $V' = V \cup \{c\}$ and $E' = E \cup \{(a\, c), (b\, c)\}$, that is, the graph got by adding a new vertex c with edges from c to a and b. Then every vertex of G' has even degree in G', so G' has an Eulerian circuit. We may take it that this circuit starts at c, so that it must be one of

$$(c\, a\, v_1\, \ldots\, v_r\, b\, c), \quad (c\, b\, v_1\, \ldots\, v_r\, a\, c),$$

because there's no other way of getting to and from c without using some edge more than once. But this means that the central section, $(a\, v_1\, \ldots\, v_r\, b)$ or $(b\, v_1\, \ldots\, v_r\, a)$, is an Eulerian path in G.

3F Hamiltonian paths and circuits Having sorted out Eulerian paths, I think the next definition is a very natural one. If $G = (V, E)$ is a finite graph, a **Hamiltonian path** in G is a path which uses every vertex exactly once; except that we allow it to start and finish at the same vertex, in which case it is a **Hamiltonian circuit**. Of course a graph with a Hamiltonian path must be connected. Among the graphs of order 4, those with Hamiltonian paths are

The graph

is connected, but has no Hamiltonian path.

Now the extraordinary fact is this: there is *no* effective general way to determine whether a given graph has a Hamiltonian path or not. I must be careful here about the meaning of the phrase 'effective general way'. What we should like is a computer package which would take a description of a graph, as a list of vertices and edges, and after not more than a few seconds' pause reply with a statement of whether a path exists and, preferably, a listing of such a path if there is one. Now of course the graph will have to be of a size the machine can be expected to cope with. But one would certainly expect a modern computer to manage a graph with a thousand vertices and ten thousand edges. And no program has ever been written which, running on all the computers of the world put together till the end of the century, could be guaranteed to solve such a problem. Of course you could write a program which would get there in the end, just by trying every possible path – after all, there can't be more than 1000! of them, and most of them will die very quickly. But if every vertex has degree 20, which is perfectly possible, you will be searching in a tree with around 20^{1000} possible paths, and this is out of our reach.

I said 'no program has ever been written'. Of course your natural reaction is to say that perhaps nobody has seriously tried. But people have tried very seriously; not only pure mathematicians seeking honour, but applied mathematicians seeking profit. Because not only do Hamiltonian-path problems sometimes turn up in commercially important contexts, but it has been shown that an efficient program to find Hamiltonian paths could be converted into efficient programs for any of a wide variety of extremely important problems. And it is indeed generally believed that *there is no efficient program.* The abstract problem of determining whether this is actually true is one of the great challenges of modern combinatorics and modern theoretical computing.

(With regard to Eulerian paths, the position is relatively simple. If you have a description of a graph, you only have to scan through the data once to calculate the degree of every vertex, and then to run through the vertices once to find out how many of them have odd degree. You also need to know whether your graph is connected; this takes a little longer, but if your list has n vertices and m edges, you won't have to read the list of edges more than n times to decide whether the graph is connected. So now you know whether you have an Eulerian path. To actually generate one, you can use the idea of the proof of 3D. Start by finding a cycle; you can do this just by wandering at random until you cross your path. Put this to one side and start again with the simpler graph got by deleting those edges. For each new cycle you find, check whether it shares a vertex with an older one, and if so amalgamate them to form a new closed path. This will produce an Eulerian circuit within $m/3$ repetitions of the process.)

3G Of course there are many special cases in which it is possible to be sure that there is, or is not, a Hamiltonian path. I give one result of this kind, partly because the proof uses a new kind of induction.

Proposition Let $G = (V, E)$ be a finite graph of order $n \geq 3$ such that $d(v) \geq \frac{1}{2}n$ for every $v \in V$. Then G has a Hamiltonian path.

proof Induce on $m = \frac{n(n-1)}{2} - \#(E)$ (the number of edges of the *complement* of G). If $m = 0$, then G is the complete graph on V, and if we list its vertices as $v_1, \dots, v_n$ then $(v_n\, v_1\, \dots\, v_n)$ is a Hamiltonian path in G. For the inductive step to $m \geq 1$, let v, w be any pair of vertices of G not linked by an edge, and let $G' = G + e = (V, E \cup \{e\})$ be the graph obtained by adding one edge e linking v and w. Now

$$d_{G'}(u) \geq d_G(u) \geq \frac{1}{2}n \text{ for every } u \in V,$$

$$\frac{n(n-1)}{2} - \#(E \cup \{e\}) = m - 1 < m,$$

so by the inductive hypothesis G' has a Hamiltonian path. If this path doesn't use the edge e it is already a Hamiltonian path for G. If it does use the edge e then we can start the path at any vertex and go in either direction, so we have a Hamiltonian path for G' of the form

$$(v\, v_2\, \dots\, v_{n-1}\, w\, v).$$

Set $v_1 = v$, $v_n = w$. Now consider the sets

$$S = \{i : 1 \leq i < n,\ v \text{ is linked to } v_{i+1} \text{ by an edge in } G,$$

$$T = \{i : 1 \leq i < n,\ w \text{ is linked to } v_i \text{ by an edge in } G.$$

Then $\#(S) = d(v)$ and $\#(T) = d(w)$. So

$$\#(S) + \#(T) \geq \frac{1}{2}n + \frac{1}{2}n = n > \#(S \cup T)$$

and S, T must overlap; say $j \in S \cap T$. Note that $1 \notin T$ and $n - 1 \notin S$, so $1 < j < n - 1$. Now look at

$$(v\, v_{j+1}\, v_{j+2}\, \ldots\, v_{n-1}\, w\, v_j\, v_{j-1}\, \ldots\, v_2\, v);$$

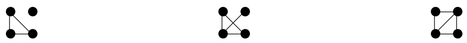
this is a Hamiltonian path in G. Thus the induction continues.

3H Colourings Let $G = (V, E)$ be any graph. A **colouring** of G is a function $f : V \to C$, where C is a set of 'colours', such that $f(v) \neq f(v')$ whenever v, $v' \in V$ are linked by an edge. The **colouring number** χG of G is the smallest size of any set C such that there is a colouring $f : V \to C$.

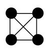
Among the graphs of order 4,

has colouring number 1,

have colouring number 2,



have colouring number 3, and



has colouring number 4.

We say that G is 'n-colourable' if it can be coloured with a set C of size n, that is, $\chi G \leq n$.

3I Colouring algorithms Once again, no efficient general procedures are known for determining the colouring number of a graph, and it is believed that no such procedure exists. (It is known that the colouring problem is equivalent to the Hamiltonian-path problem in the sense that if you had a magician who could solve one of these problems for you, then you would be able to use his answers in a program to solve the other.) There are one or two straightforward facts. For instance, $\chi G = 0$ iff G is the empty graph, $\chi G \leq 1$ iff G has no edges. If $G = K_n$, the **complete graph on n vertices**, then $\chi G = n$ (since every vertex must have a different colour); for any other graph of order n, $\chi G < n$ (since if there are two vertices not linked by an edge, we can give them the same colour, and then colour the others as we please). Also we have the following.

3J Proposition Let $G = (V, E)$ be a graph. Then $\chi G \leq 2$ iff G has no cycles of odd length.

proof (a) Suppose first that G is 2-colourable, that is, that we have a colouring $f : V \to C$ where $\#(C) \leq 2$. If $(v_0\, v_1\, \ldots\, v_n)$ is a cycle in G, then $f(v_0) \neq f(v_1)$, $f(v_1) \neq f(v_2)$; but this means that $f(v_2) = f(v_0)$. Similarly $f(v_4) = f(v_2) = f(v_0)$, $f(v_6) = f(v_4) = f(v_0)$, and so on. But since $f(v_{n-1}) \neq f(v_n)$ and $f(v_n) = f(v_0)$, $n - 1$ cannot be even, that is, n cannot be odd. Thus any cycles in G are of even length.

(b) Now suppose that G has no cycles of odd length.

(i) If G is empty then $\chi G = 0 \le 2$ and we can stop.

(ii) Suppose next that G is non-empty and connected. Start from any $v_0 \in V$ and for each $v \in V$ say that $r(v)$ is the shortest length of any path from v_0 to v in V. (Because G is connected, there always is at least one path from v_0 to v, so there is a shortest one. Of course $r(v_0) = 0$, while $r(v) = 1$ iff there is an edge linking v and v_0.) Now define $f : V \to \{0,1\}$ by setting $f(v) = 0$ if $r(v)$ is even, 1 if $r(v)$ is odd. In this case f is a colouring. **P** Suppose that v, $w \in V$ are linked by an edge. Re-label them, if necessary, so that $r(v) \le r(w)$. There is a path $(v_0\, v_1\, \ldots\, v_{r(v)})$ of length $r(v)$ from v_0 to $v = v_{r(v)}$; similarly, there is a path $(w_0\, w_1\, \ldots\, w_{r(w)})$ from $v_0 = w_0$ to $w_{r(w)}$. For each $i \le r(v)$, $r(v) \le r(v_i) + r(v) - i$, so $r(v_i) \ge i$; but also $r(v_i) \le i$, so $r(v_i) = i$ exactly. Similarly $r(w_i) = i$ for every $i \le r(w)$. But this means that we can't have $v_i = w_j$ unless $i = j$. Now take the largest i such that $v_i = w_i$. (α) It could be that $i = r(v)$, so that $v_i = v$. In this case, since $w \ne v$, we must have $r(w) > r(v)$. Also $(v_0\, \ldots\, v_{r-1}\, v\, w)$ is a path from v_0 to w, so $r(w) \le r(v) + 1$; but this means that $r(w) = r(v) + 1$ and $f(w) \ne f(v)$. (β) Otherwise, $i < r(v)$. In this case, all of v_i, $v_{i+1}, \ldots, v_{r(v)}, w_{i+1}, \ldots, w_{r(w)}$ are distinct, and we have a cycle

$$(v_i\, v_{i+1}\, \ldots\, v_{r(v)}\, w_{r(w)}\, w_{r(w)-1}\, \ldots\, w_{i+1}\, w_i)$$

of length $k = r(v) - i + 1 + r(w) - i$. Now, by hypothesis, k cannot be odd; but this means that $r(v) + r(w)$ cannot be even, that is, $r(v) - r(w)$ cannot be even, and $f(v) \ne f(w)$. Thus $f(v) \ne f(w)$ in both cases; as v, w are arbitrary, f is a colouring. **Q**

(iii) Finally, if G is not connected, let $V_1, \ldots, V_k$ be its components. For each $j \le k$, $G_j = G{\restriction}V_j$ is a connected graph with no cycles of odd order, so has a colouring $f_j : V_j \to \{0,1\}$; now set $f(v) = f_j(v)$ for every $v \in V_j$, $j \le k$. Since there are no edges linking vertices in different V_j, f is a 2-colouring for G.

Remark Observe that this colouring is found by a practicable algorithm; we have an effectively computable method of determining whether $\chi G \le 2$, and if it is of finding a colouring with χG colours. But the question of whether $\chi G = 3$ is already 'hard'.

3K The greedy algorithm Colourings are sufficiently important so that it's worth developing methods of colouring graphs even if you can't be sure that they give best possible results. (For example, consider the problem the examinations office has been tackling: schedule the examinations so that (at the very least) nobody has to sit two exams at once. If you take the examination papers as the vertices, and say that two papers are linked by an edge iff there is a student taking both, then a scheduling is a colouring, that is, a function f from the set V of papers to the set C of examination times such that $f(v) \ne f(w)$ whenever v, w are linked by an edge.)

One algorithm which, intelligently used, can give reasonably good results is the **greedy algorithm**. Here you have to start by picking an ordering $v_1, \ldots, v_n$ of the vertices. Now define $f : V \to \mathbb{N}$ inductively, setting

$$f(v_i) = \min\{k : k \in \mathbb{N},\ f(v_j) \ne k \text{ whenever } j < i \text{ and } v_i,\ v_j \text{ are linked by an edge}\}.$$

Provided you put the vertices in a good order – generally speaking, 'most difficult first' – the number of colours used by the greedy algorithm is likely to be not far off the colouring number of G. But I repeat: there is *no* algorithm of this type which always gives the right answer, at least, not unless you have a magician to tell you what order to put the vertices in.

3L Remark Observe that if we use the greedy algorithm, as above, then $f(v) \le 1 + d(v)$ for every vertex v (since there can't possibly be more than $d(v)$ colours forbidden to us when we come to colour v). So generally $\chi G \le 1 + \max_{v \in V} d(v)$ for any (finite) graph $G = (V, E)$.

3M Remarks (a) The original colouring problems referred to maps rather than graphs. If you imagine the old-fashioned kind of political map, showing countries or counties or whatever, coloured to show the boundaries clearly, then of course countries with a common frontier will need different colours. If you think of the countries as the vertices of your graph, linked by an edge iff they have a common border, then you get the corresponding graph-colouring problem.

(b) Of course you can also ask: is there a colouring of the *edges* of your graph $G = (V, E)$ so that two edges meeting at a vertex always have different colours? This can also be converted into an ordinary graph-colouring problem if you set $G' = (E, E^*)$, where e, $e' \in E$ (now thought of as vertices in G') are linked by an edge in G' iff they share an endpoint in G.

(c) While there is no useful theory for the calculation of chromatic numbers, there is a good deal which can be said about them; a particularly important concept is that of *chromatic polynomial*, mentioned in one of the problems of the problem sheet; for any finite graph $G = (V, E)$ there is a polynomial $p_G(x)$, of degree the order of G, such that for integers k the number of ways of colouring G with k colours is $p_G(k)$. (The trouble is that there's no effective way of calculating the coefficients of $p_G(x)$ for general graphs G!)

amsppt.styma251b4.tex Version of 2.3.96

4. Menger's Theorem

I come now to a theorem which is genuinely 'modern', or at any rate twentieth-century. It is definitely more difficult than what has gone before, and 4E especially is hard (the hardest thing in the course, I think). However I hope that if you concentrate hard on some examples then you will at least be able to understand what the theorem is trying to say.

4A We need a couple of definitions, one straightforward, the other less obvious.

Definition Let $G = (V, E)$ be a graph and a, b two vertices of G not linked by an edge.

(a) A set $S \subseteq V \setminus \{a, b\}$ **separates** a from b in G if every path from a to b in G uses at least one vertex in S; that is, if a and b cannot be joined by a path in $G - S$; that is, if a and b belong to different components of $G - S$.

(If a and b belong to different components of G, then $\emptyset$ separates a from b,)

(b) Two paths P_1, P_2 from a to b are **independent** if they share no vertices other than a and b.

4B Menger's Theorem Let $G = (V, E)$ be any finite graph, and a, $b \in V$ two distinct vertices not linked by an edge in G. Write p for the largest number of independent paths $P_1, \dots, P_p$ that we can find from a to b. (If there are no paths from a to b in G, set $p = 0$.) Write s for the smallest size of any set $S \subseteq V \setminus \{a, b\}$ which separates a from b. Then $p = s$.

4C Proof of Menger's Theorem: easy part The proof works by showing that $p \leq s$ and that $s \leq p$. The first is much easier, so I do it first. Take a $S \subseteq V \setminus \{a, b\}$, separating a from b, with $\#(S) = s$, and independent paths $P_1, \dots, P_p$ from a to b. Now every P_i must use at least one vertex $v_i \in S$, by the definition of 'separating'. But all the vertices $v_1, \dots, v_p$ must be different, by the definition of 'independent path'. So we have p distinct points in S and $p \leq \#(S) = s$.

4D Proof of Menger's Theorem: hard part There are various proofs of the second half, that $s \leq p$. What this says is that we can find a set S and a set $P_1, \dots, P_r$ of independent paths from a to b such that S separates a from b and $\#(S) \leq r$ (and therefore, of course, $\#(S) = s = p = r$, since we must have $r \leq p \leq s \leq \#(S)$).

The proof I will try to explain is an 'algorithmic' one, that is, one which can be used as the basis of a reasonably efficient computer program to exhibit S and $P_1, \dots, P_r$.

The centre of the algorithm is a method for improving on a given string $P_1, \dots, P_r$ of independent paths, by giving a constructive proof of the following lemma.

4E Lemma Let $G = (V, E)$ be a finite graph, and a, b two distinct vertices of G not linked by an edge. Let $P_1, \dots, P_r$ be independent simple paths from a to b. Then *either* a can be separated from b by a set with just r members *or* we can find independent simple paths $P'_1, \dots, P'_{r+1}$ from a to b in G.

Remark What I mean by 'constructive' is that the proof shows us exactly what to do in order to find either an S or a list $P'_1, \dots, P'_{r+1}$ in any particular case.

proof Let us say that a set $W \subseteq V$ is a 'good' set with 'critical points' $v_1, \dots, v_r$ if

$a \in W$, $b \notin W$;

for each $i \leq n$, the vertices of P_i belonging to W form an initial segment of P_i, containing at least one vertex other than a, and v_i is the last vertex of P_i belonging to W;

for every $x \in W \setminus \{v_1, \dots, v_n\}$ there are independent simple paths Q, $Q_1, \dots, Q_n$, all within W, such that Q runs from a to x and Q_i runs from a to v_i for each i.

(Allow Q to be the trivial path if $x = a$.) The simplest 'good' set is just $\{a, u_1, \dots, u_r\}$ where each u_i is the first point of P_i after a, so that its critical points are the u_i.

Now starting from a 'good' set W with critical points $v_1, \dots, v_r$, three things can happen.

case 1 There may be a $w \in W \setminus \{v_1, \dots, v_r\}$ which is linked to b by an edge. In this case, we can find independent simple paths $P'_1, \dots, P'_{r+1}$ from a to b, as follows. Because W is 'good', there are independent simple paths $Q_1, \dots, Q_r, Q$, all lying within w, joining a to $v_1, \dots, v_r, w$. For $i \le r$, take P'_i to be the path Q_i from a to v_i, followed by the segment of P_i from v_i to b. Now take P_{r+1} to be the path Q from a to w, followed by the link $(w\,b)$. Then the P'_i are all independent because no two of $Q_1, \dots, Q_r, Q$ share any vertices other than a, no two of $P_1, \dots, P_r$ share any vertices other than a and b, and the segments of P_i from v_i to b use no vertices of W other than v_i, so can't collide with Q or any of the Q_j. So now we have $r+1$ independent simple paths.

case 2 It may be that no $x \in W \setminus \{v_1, \dots, v_r\}$ is linked by an edge to any $y \in V \setminus W$. In this case $S = \{v_1, \dots, v_r\}$ separates a from b in G. **P** Let P be any path from a to b. Since $a \in W$, there must be a last vertex x of P which belongs to W; since $b \notin W$, $x \ne b$. But now the next vertex y of P after x belongs to $V \setminus W$ and is linked to x by an edge. This means that $x \in S$, by the hypothesis of this case. Thus every path from a to b in G passes through S, and S separates a from b.
So in this case we have a separating set of size r. **Q**

case 3 In any other case, there must be a $w \in W \setminus \{v_1, \dots, v_r\}$ linked to some $v \in V \setminus W$ with $v \ne b$. In this case there is a strictly larger 'good' set $W' \supseteq W$. **P**

case 3a Suppose that v does not lie on any of the P_j. In this case we can just take $W' = W \cup \{v\}$. Its critical points are still $v_1, \dots, v_r$. To see that it has enough independent paths in it, take any $x \in W' \setminus \{v_1, \dots, v_r\}$. If $x \in W$, then surely we have independent simple paths $Q_1, \dots, Q_r, Q$ from a to $v_1, \dots, v_r, x$ lying in W and therefore in W'. If $x = v$, then take independent simple paths $Q_1, \dots, Q_r, Q$ from a to $v_1, \dots, v_r, w$ lying in W, and extent Q to a path Q' from a to v by adding the link $(u\,v)$; then $Q_1, \dots, Q_r, Q'$ are independent paths from a to $v_1, \dots, v_r, v$.

case 3b Suppose that v lies on P_j. In this case (because the P_i are independent) it does not lie on any of the P_i for $i \ne j$. v lies further along P_j than v_j; take W' to be W together with all the vertices of P_j between v_j and v, including v. The new critical points of W' will be $v'_i = v_i$ for $i \ne j$, $v'_j = v$.
To see that W' has the independent-path property, take any $x \in W' \setminus \{v'_1, \dots, v'_r\}$. **(i)** If $x \in W \setminus \{v_1, \dots, v_r\}$, then there are independent simple paths $Q_1, \dots, Q_r, Q$ from a to $v_1, \dots, v_r, x$ in W. Set $Q'_i = Q_i$ for $i \ne j$ and let Q'_j be Q_j with the segment of P_j from v_j to $v'_j = v$ added, so that Q'_j is a path from a to v'_j in W'. Now $Q'_1, \dots, Q'_r, Q$ are independent paths in W' from a to $v'_1, \dots, v'_r$. **(ii)** Otherwise, x must lie on the path P_j somewhere between v_j and $v = v'_j$, including v_j but not v'_j. In this case, let $Q_1, \dots, Q_r, Q$ be independent simple paths from a to $v_1, \dots, v_r, w$ in W. Set $Q'_i = Q_i$ for $i \ne j$. Let Q'_j be the path Q extended by the link $(u\,v) = (u\,v'_j)$, and let Q' be the path Q_j extended by the segment of P_j between v_j and x. (If $x = v_j$ then $Q' = Q_j$, of course.) In this case $Q'_1, \dots, Q'_r, Q'$ will be independent paths in W' from a to $v'_1, \dots, v'_r, x$.
Thus in all cases we can find a strictly larger 'good' set W'. **Q**

construction Now the proof of the lemma as stated goes as follows. We start with the elementary 'good' set $W_0 = \{a, u_1, \dots, u_r\}$, and progressively build larger and lardge 'good' sets W_k, with $W_0 \subset W_1 \subset W_2 \dots$, using the methods of case 3 above, until we either find ourselves in case 1, and can build a new set of $r+1$ independent paths, or get stuck in case 2, so that we have a separating set of size r.

4F Conclusion of proof of Menger's theorem Let us return to the original problem: given a graph $G = (V, E)$ and distinct points a, $b \in V$ not linked by an edge in G, we want to find independent paths $P_1, \dots, P_r$ from a to b and a set $S \subseteq V \setminus \{a, b\}$ of size r separating a from b. If there is no path from a to b in G, we take $r = 0$ and $S = \emptyset$ and stop. If there is a path, there is a simple path; take it and call it P_{11}. Now apply the construction of 4E to find *either* a set S of size 1 separating a from b *or* two independent simple paths P_{21}, P_{22} from a to b. Repeat to find *either* a set S of size 2 separating a from b *or* three independent simple paths P_{31}, P_{32}, P_{33} from a to b. Keep going until you finally get a separating set of the same size as your family of independent paths.

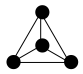
4G Remark In order to actually write my computer program, I had to do some more work. The point is that just knowing, in the abstract, that your set W is 'good' isn't enough to tell you how to build the paths you need in it. The subroutine corresponding to the arguments in 4E must therefore keep careful records of how the ‘good’ sets were built, so that when and if you finally get a link to b you can reconstruct the paths. It turns out that the records needed are minimal – really, all you need is an arrow from each point of W to one of its neighbours, and a marker for ‘ex-critical’ points – so the program can be made very fast.

amsppt.styma251b5.tex Version of 22.2.96

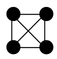
5. Planar graphs

5A (a) Definition A finite graph $G = (V, E)$ is **planar** if it can be drawn in the plane in the sense that each vertex corresponds to a (different) point in the plane and each edge is drawn as a continuous line (possibly curved) from one endpoint to another, and no two edges cross, nor does any edge pass through a vertex.

(b) Examples (i) The complete graph K_4 on 4 vertices is planar, because it can be drawn as

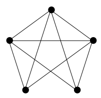


Note that the same graph can also be drawn as

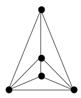


with two edges crossing; you may have to think a bit to decide whether a given graph is planar, because your first picture may miss it.

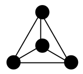
(ii) For instance, if we take the graph with 5 vertices and 9 edges – that is, K_5 with one edge deleted – then the straightforward picture



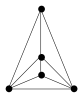
doesn’t look promising. But in fact this graph is planar:



(c) Given a drawing of a planar graph, then in the drawing we can identify its **faces**, that is, the regions into which the plane is divided by the edges of the drawing. Thus in the drawing



there are four faces; three inside and one outside. In the drawing



there are six faces, five inside and one outside. In each of the drawings

there is just one face, because in these pictures the edges don't separate the plane. But in

there are two faces, and in

there are three.

5B Euler's Formula Suppose that $G = (V, E)$ is any finite graph drawn in the plane with no edges crossing. Then

$$\#(V) + \#(\mathcal{F}) = \#(E) + \#(\mathcal{C}) + 1,$$

where $\mathcal{F}$ is the set of faces in the drawing and $\mathcal{C}$ is the set of components of G.

Remarks (a) You may prefer to remember this in the form

$$v + f = e + c + 1$$

(cf. 2G above).

(b) Note that in this expression, V, E and $\mathcal{C}$ are determined by the structure of the graph $G = (V, E)$, but $\mathcal{F}$ is not. One of the remarkable features of this theorem is that it tells us that if we have two different drawings of the same graph, then the number of faces in each drawing must be the same.

sketch of proof Induce on $m = \#(E)$.

(a) If $m = 0$, then $\mathcal{F}$ has just one member (because we have only n points in the picture, and they can't separate the plane), while the components of G are just the singleton subsets of V, so $\#(\mathcal{C}) = \#(V)$, and

$$\#(V) + \#(\mathcal{F}) = \#(V) + 1 = \#(E) + \#(\mathcal{C}) + 1.$$

Thus the induction starts.

(b) For the inductive step to $m \geq 1$, fix on some edge $e \in E$, and let a, b be its endpoints; let $G' = G - e = (V, E \setminus \{e\})$ be the graph with that edge deleted. If we rub the edge e out of our drawing of G, we obtain a drawing of G'; let $\mathcal{F}'$ be the set of faces of this drawing. Write $E' = E \setminus \{e\}$ for the set of edges of G' and $\mathcal{C}'$ for the set of its components. Then the inductive hypothesis tells us that

$$\#(V) + \#(\mathcal{F}') = \#(E') + \#(\mathcal{C}') + 1 = \#(E) + \#(\mathcal{C}'),$$

since $\#(E') = m - 1 < m$.

case 1 Suppose that a and b belong to different components V_1, V_2 of G'. Then $V_1 \cup V_2$ is a component of G, while all the other components of G' remain components of G (as in 2G). On the other hand, because V_1 and V_2 are not linked by an edge in G', the two sides of the new edge e can still be joined by paths in the plane not crossing any edge of the drawing of G – you just have to go the long way, around V_1 say. So $\#(\mathcal{F}) = \#(\mathcal{F}')$. Thus

$$\#(V) + \#(\mathcal{F}) = \#(V) + \#(\mathcal{F}') = \#(E) + \#(\mathcal{C}') = \#(E) + \#(\mathcal{C}) + 1.$$

case 2 Suppose that a and b belong to the same component C_0 of G'. Then G and G' have exactly the same components. On the other hand, there is a (simple) path from a to b in G' which, combined with the edge e, forms a cycle; so the two sides of the edge e are no longer in the same face of the drawing of G. Accordingly $\#(\mathcal{F}) = \#(\mathcal{F}') + 1$, and we get

$$\#(V) + \#(\mathcal{F}) = \#(V) + \#(\mathcal{F}') + 1 = \#(E) + \#(\mathcal{C}') + 1 = \#(E) + \#(\mathcal{C}) + 1.$$

Thus the induction continues in both cases.

Remark I call this a 'sketch' of a proof because the parts of the argument which keep count of the faces of G, G' depend on pictures in ways which most twentieth-century pure mathematicians would feel were dangerous; a modern account would spend a lot longer on these points.

5C Corollary If $G = (V, E)$ is any non-empty connected planar finite graph, then for any drawing of it in the plane

$$\#(V) + \#(\mathcal{F}) = \#(E) + 2,$$

because G has just one component.

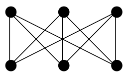
5D Two non-planar graphs (a) The complete graph K_5 on 5 vertices is not planar.

proof ? Suppose, if possible, that we had a planar drawing of K_5. Since $\#(V) = 5$, $\#(E) = 10$ and $\#(\mathcal{C}) = 1$, we must have just $10 + 1 + 1 - 5 = 7$ faces. But if we count the set

$$R = \{(e, F) : e \in E,\ F \in \mathcal{F},\ e \text{ is on the boundary of } F\},$$

every face must have at least 3 edges, so $\#(R) \geq 3\#(\mathcal{F}) = 21$, while each edge bounds at most 2 faces, so $\#(R) \leq 2\#(E) = 20$; and this is impossible. **X**

(b) Let $K_{3,3}$ be the **bipartite graph** with 6 vertices in two families of 3, the edges being all possible links between vertices of different families, thus:



Then $K_{3,3}$ is not planar.

proof Here we have $\#(V) = 6$, $\#(E) = 9$, $\#(\mathcal{C}) = 1$. **?** If $K_{3,3}$ could be drawn in the plane, then the number of faces would have to be $9+1+1-6 = 5$. But this time there are no triangles in the graph (indeed, it is 2-colourable), so that every face must be bounded by at least 4 edges. So if we count

$$R = \{(e, F) : e \in E,\ F \in \mathcal{F},\ e \text{ is on the boundary of } F\},$$

we must have

$$\#(R) \geq 4\#(\mathcal{F}) \geq 20, \quad \#(R) \leq 2\#(E) = 18,$$

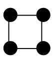
which again is impossible. **X**

Remark In the puzzle books of my youth this was the 'gas–water–electricity' problem. If you think of the top three vertices as three houses, and the bottom three vertices as the supply centres for the utilities, then the problem is to connect every house to every utility without any two conduits crossing (since this will risk damage when the second one is installed); and it can't be done, wherever the houses and supply centres are.

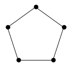
5E Definition If $G = (V, E)$ and $G' = (V', E')$ are graphs, a **topological embedding** of G in G' is an injective map $f : V \to V'$ together with a map $g : E \to \mathcal{P}$, where $\mathcal{P}$ is the set of simple paths in G', such that $g(e)$ is a path from $f(a)$ to $f(b)$ whenever e links a to b, and the paths $g(e)$ are independent in the strong sense that no vertex v' of G' can lie on more than one path $g(e)$ unless it is a common endpoint of both.

The idea is that if we have a drawing of G, we can turn it into a drawing of G' by adding some vertices in the middle of the edges, and then, if we wish, adding new vertices and edges anywhere we like.

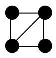
Examples (a)



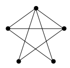
is topologically embedded in



(b)



is topologically embedded in



5F Kuratowski's Theorem A finite graph G is planar iff neither K_5 nor $K_{3,3}$ can be topologically embedded in G.

5G Theorem If $G = (V, E)$ is any finite planar graph, it can be drawn in the plane with every edge straight.

5H Four-colour theorem Every planar graph is 4-colourable.

5I Remarks (a) I give no proofs of these. 5F and 5G are within reach of an undergraduate course, but third- rather than second-year. 5H is another matter. After a century of being one of the most famous problems in topology and graph theory, it was finally proved in 1976 with the aid of a computer program; the problem was reduced to a matter of checking something between 1300 and 1400 configurations to show that none of them could appear in a minimal counter-example, and the check was done by a machine. There was for some time a residual doubt about the validity of the proof, as it seemed to depend on being sure that the program was correct, and there is no effective way of proving that any substantial chunk of computer code is actually right; but these doubts seem to have evaporated with time, and I don't think anybody now doubts that the 1976 argument is essentially right.

(b) All three of these are 'computable' in the sense that it is possible, in principle, to write a computer program which, given a description of a graph, will

either exhibit a topological embedding of one of K_5, $K_{3,3}$ into it (by listing the functions f, g of Definition 5E)

or draw the graph (with all edges represented as straight lines, as in 5G) and list a 4-colouring of its vertices.

I should remark that I do not think anybody has seriously contemplated actually writing a program to produce a 4-colouring of a given planar graph. But the 1976 proof of the four-colour theorem, with some refinements, makes it plain that such a program would be feasible.

amsppt.styma251b6.tex Version of 21.2.96

6. More combinatorics

6A Definitions Let X and Y be any sets, and $R \subseteq X \times Y$ any relation.

(a) For $I \subseteq X$, write

$$R[I] = \{y : (x, y) \in R \text{ for some } xinI\};$$

for $J \subseteq Y$, write

$$R^{-1}[J] = \{x : (x, y) \in R \text{ for some } y \in J\}.$$

(b) If $D \subseteq X$ is a set and $f : D \to Y$ is function, say that f is **covered** by R if $(x, f(x)) \in R$ for every $x \in \operatorname{dom} f = D$.

6B The marriage lemma Suppose that X and Y are finite sets and $R \subseteq X \times Y$ is a relation. Let m be the largest size of any set $D \subseteq X$ such that there is an injective function $f : D \to Y$ covered by R. Then

$$\max_{I \subseteq X}(\#(I) - \#(R[I])) = \#(X) - m.$$

proof Set $d = \max_{I \subseteq X}(\#(I) - \#(R[I]))$.

(a) Let $D \subseteq X$ be a set of size m and $f : D \to Y$ is an injective function covered by R. Then for any $I \subseteq X$,

$$\#(R[I]) \geq \#(f[I]) = \#(I \cap D),$$

because f is injective, so

$$\#(I) - \#(R[I]) \leq \#(I) - \#(I \cap D) = \#(I \setminus D) \leq \#(X \setminus D) = \#(X) - m.$$

As I is arbitrary, $d \leq \#(X) - m$.

(ii) To show that $\#(X) - m \leq d$, we may suppose that X and Y are disjoint. Take two new points a, b not in $X \cup Y$. Define a graph $G = (V, E)$ by setting $V = X \cup Y \cup \{a, b\}$ and say that the edges of G are just

all edges $(a\,x)$ where $x \in X$,

all edges $(b\,y)$ where $y \in Y$,

edges $(x\,y)$ for $(x, y) \in R$.

Now a and b are not linked by an edge so by Menger's theorem we have a family $P_1, \ldots, P_r$ of independent paths from a to b and a set $S \subset V \setminus \{a, b\} = X \cup Y$ separating a from b with $\#(S) = r$. Now we can take it that all the P_i are simple paths, in which case each must be of the form $(a\,x_i\,y_i\,b)$. Set $D = \{x_i : i \leq r\}$ and $f(x_i) = y_i$ for $i \in D$; because the P_i are independent, all the x_i, y_i are distinct, so f is an injective function. Also $(x_i\,y_i)$ is an edge of G, that is, $(x_i, y_i) \in R$ for each i, so f is covered by R, and $r = \#(D) \leq m$.

On the other hand, if we set $I = X \setminus S$, then $R[I] \subseteq S$, because if $x \in I$ and $(x, y) \in R$ then $(a\,x\,y\,b)$ is a path from a to b in G which must pass through S, and the only possible vertex of the path which can belong to S is y. So we get

$$r = \#(S) = \#(S \cap X) + \#(S \cap Y) \geq \#(X) - \#(I) + \#(R[I]),$$

and

$$d \geq \#(I) - \#(R[I]) \geq \#(X) - r \geq \#(X) - m.$$

Putting these together, we have $d = \#(X) - m$, as required.

Remark This is sometimes called the 'defect form' of the Marriage Lemma. The 'simple form' is the following:

6C Corollary Let X and Y be finite sets and $R \subseteq X \times Y$ a relation. Then the following are equiveridical:

(i) there is an injective function from X to Y covered by R

(ii) $\#(R[I]) \geq \#(I)$ for every $I \subseteq X$.

proof The point is that, in the language of 6B, (i) is true iff $m = \#(X)$, while (ii) is true iff $d \leq 0$; since we know that $0 \leq d = \#(X) - m$, these are equiveridical.

6D Remarks (a) The 'marriage lemma' takes that form because if you declare X to be a set of boys, Y a set of girls, and R to be the set

$$\{(x, y) : y \text{ will accept } x \text{ as a husband}\},$$

then it gives a necessary and sufficient condition for a pairing-off (satisfactory to the girls, anyway) to be achievable.

(b) Note that (because it is a straightforward development from Menger's theorem) the marriage lemma is effectively computable in the sense that a program can be written (I have done it) which, starting from X, Y and R, generates a set D, an injective function $f : D \to Y$ covered by R, and a set $I \subseteq X$ such that

$\#(I) - \#(R[I]) = \#(X \setminus D)$. (In fact, this is much easier than the program for Menger's theorem, mostly because all the paths we look at are guaranteed to be very short, so that we hardly have to think of them as paths.)

6E Dilworth's theorem Let $(P, \le)$ be a finite partially ordered set. Write

m for the largest size of any set $A \subseteq P$ of elements which is an antichain, that is, $p \not\le q$ for any distinct p, $q \in A$,

n for the smallest number of totally ordered subsets of P which can cover P.

Then $m = n$.

***proof (a)** (The easy half) To see that $m \le n$, note that if $C_1, \dots, C_n$ are totally ordered sets and A is an antichain, then $A \cap C_i$ can have at most one element for each i; so if $P = C_1 \cup \ldots \cup C_n$, $\#(A) \le n$.

(b) To see that $m \ge n$, consider the relation

$$R = \{(p, q) : p < q\} \subseteq P \times P.$$

By the Marriage Lemma, there are D, $I \subseteq P$ and an injective function $f : D \to P$ such that

f is covered by R, that is, $p < f(p)$ for every $p \in D$,

$\#(I) - \#(R[I]) = \#(P \setminus D)$.

(i) Set $A = I \setminus R[I]$. If p, $q \in A$, then $p \in I$ and $q \notin R[I]$ so $(p, q) \notin R$, that is, $p \not< q$; but this means that A is an antichain. Accordingly

$$m \ge \#(A) = \#(I) - \#(I \cap R[I]) \ge \#(I) - \#(R[I]).$$

(ii) For each $w \in P \setminus D$, let C_w be the set

$$\{w\} \cup \{p : p \in D, \exists\, k \in \mathbb{N} \text{ such that } f^k(p) = w\}.$$

Then C_w is a totally ordered subset of P. **P** If p, $q \in D$ and $f^j(p) = f^k(q) = w$, with $j \le k$, then

$$p < f(p) < f^2(p) < \ldots < f^j(p) = w,$$

so $p < w$. Moreover, because $f^j(f^{k-j}(q)) = f^j(p)$ and f is injective, $f^{k-j}(q) = p$ and $q \le p$. As p, q are arbitrary, C_w is a totally ordered subset of P. **Q**

Next, every element of P belongs to some C_w. **P** Starting from any $p \in P$, if $p \notin D$ then $p \in C_p$; while otherwise the chain $p < f(p) < f^2(p) < \ldots$ cannot be infinite, and must end with some $f^k(p) = w \notin D$, so that $p \in C_w$. **Q**

Consequently

$$n \le \#(P \setminus D) = \#(I) - \#(R[I]) \le m,$$

as claimed.

6F Ramsey's Theorem (finite form) Suppose that X is a set and $\#(X) \ge 2^{m_1+m_2}$, where m_1, $m_2 \in \mathbb{N} \cup \{0\}$. If $f : [X]^2 \to \{1, 2\}$ is any function, then there is a set $A \subseteq X$ such that, for some i, $\#(A) = m_i$ and $f(I) = i$ for every $I \in [A]^2$.

proof Induce on $m = m_1 + m_2$. If $m = 0$ then $m_1 = m_2 = 0$ and we can take $A = \emptyset$. For the inductive step to $m \ge 1$, take any $x \in X$ and consider

$$X_j = \{y : y \in X \setminus \{x\},\ f(\{x, y\}) = j\}$$

for $j = 1$, 2. Now

$$\#(X_1) + \#(X_2) = \#(X) - 1 \ge 2^{m_1+m_2} - 1 > 2(2^{m_1+m_2-1} - 1),$$

so there is some j such that $\#(X_j) > 2^{m_1+m_2-1} - 1$, that is, $\#(X_j) \ge 2^{m_1+m_2-1}$. Set $m'_j = m_j - 1$, $m'_i = m_i$ if $i \ne j$, so that $\#(X_j) \ge 2^{m'_1+m'_2}$. Look at $f_1 = f{\restriction}[X_j]^2 : [X_j]^2 \to \{1, 2\}$. By the inductive hypothesis, there is a set $A \subseteq X_j$ such that, for some i, $\#(A) = m'_i$ and $f_1(I) = i$ for every $I \in [A]^2$. If $i = j$, set $B = A \cup \{x\}$; if $i \ne j$, set $B = A$. Then $\#(B) = m_i$ and $f(I) = i$ for every $i \in [B]^2$. **P** (i) If $i = j$, then $\#(B) = m'_i + 1 = m_i$. If $I \in [B]^2$, either $I \subseteq A$ and $f(I) = f_1(I) = i$, or $I = \{x, y\}$ for some $y \in V_j$; but in this case $f(I) = j = i$ by the definition of V_j. (ii) If $i \neq j$ then $\#(B) = m'_i = m_i$ and $f(I) = f_1(I) = i$ for every $I \in [B]^2$. **Q**

Thus the induction proceeds.

6G Corollary Let $G = (V, E)$ be a finite graph of order at least 2^{m+n}. Then *either* K_m is a subgraph of G *or* K_n is a subgraph of $\overline{G}$.

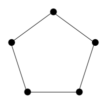
proof For $I \in [V]^2$, set $f(I) = 1$ if there is an edge in E linking the two vertices in I, 2 otherwise. By 6F, there is a set $A \subseteq V$ such that either $\#(A) = m$ and $f(I) = 1$ for every $I \in [A]^2$, or $\#(A) = n$ and $f(I) = 2$ for everyb $I \in [A]^2$. In the first case, $G \restriction A$ is a complete graph on m vertices; in the second case, $\overline{G} \restriction A$ is a complete graph on n vertices.

6H Ramsey numbers (a) The numbers $2^{m_1+m_2}$ in 6F, 2^{m+n} in 6G are certainly much larger than necessary. For instance, if G is a graph of order 6, at least one of G, $\overline{G}$ has K_3 as a subgraph. **P** (i) Suppose G has a vertex x of degree 3 or more. In this case, take a set A of 3 vertices linked to x by an edge. If no two vertices in A are linked by an edge in G, then $\overline{G} \restriction A$ is a complete graph on three vertices. If two vertices y, $z \in A$ are linked by an edge in G, then $G \restriction \{x, y, z\}$ is a complete graph on three vertices. (ii) Suppose G has a vertex x of degree 2 or less. Then x has degree at least 3 in $\overline{G}$, so we can use the same argument again. **Q**

(Another way of looking at it: if you have six people gathered together, either there are three people present who all know each other, or there are three people present none of whom know each other.)

(That assumes that the relation 'knowing each other' is symmetric. If you take your duties as a host seriously you will know very well that this isn't really true.)

(b) In fact 6 is the magic number here: if you consider the simple cycle on 5 vertices



then its complement is also a simple cycle and neither has K_3 as a subgraph.

(c) In general, we can talk about the **Ramsey numbers** $R(m, n)$: $R(m, n)$ is the smallest number such that whenever G is a graph of order $R(m, n)$, then either K_m is a subgraph of G or K_n is a subgraph of $\overline{G}$. Of course $R(m, n) = R(n, m)$. We have $R(0, n) = 0$, $R(1, n) = 1$, $R(2, n) = n$ (if K_2 is not a subgraph of G, then G has no edges, so K_n will be a subgraph of $\overline{G}$ provided there are n vertices). After this it gets difficult. I believe that very few of the $R(m, n)$ are known exactly; it may well be that the calculation is 'intractable' in the same sense that the travelling salesman problem is intractable.

(d) We can ask some of the same questions about infinite graphs; this leads into very deep water. But the first result is relatively easy.

6I Ramsey's theorem: infinite form Let $f : [\mathbb{N}]^2 \to \{1, 2\}$ be any function. Then there is an infinite set $A \subseteq \mathbb{N}$ such that f is constant on $[A]^2$.

proof Define $n_1 < n_2 < \ldots$, $C_1 \supset C_2 \supset \ldots$, $i_1, i_2 \ldots$ inductively, as follows. $C_1 = \mathbb{N}$. Given that C_k is an infinite subset of $\mathbb{N}$, take n_k to be the least member of C_k. Now set

$$C'_k = \{n : n \in C_k,\, n > n_k,\, f(\{n_k, n\}) = 1\}, \quad C''_k = \{n : n \in C_k,\, n > n_k,\, f(\{n_k, n\}) = 2\}.$$

If C'_k is infinite, set $i_k = 1$, $C_{k+1} = C'_k$. Otherwise, because $C'_k \cup C''_k = C_k \setminus \{n_k\}$ is infinite, C''_k must be infinite; set $i_k = 2$, $C_{k+1} = C''_k$. Continue.

Note that at each stage of the induction, $C_{k+1} \subseteq C_k \setminus \{n_k\}$, so that $n_k < n$ for every $n \in C_{k+1}$; in particular, $n_k < n_{k+1}$. Note also that $n_j \in C_j \subseteq C_{k+1}$, so that $f(\{n_k, n_j\}) = i_k$ whenever $k < j$.

Having completed this part of the induction, examine the i_k. There must be some $i \in \{1, 2\}$ such that $D = \{k : i_k = i\}$ is infinite. Set $A = \{n_k : k \in D\}$. Then A is an infinite subset of $\mathbb{N}$. If $I \in [A]^2$, then I must be expressible as $\{n_k, n_j\}$ where $k < j$ and k, $j \in D$; so that $f(I) = i_k = i$. Thus f is constant on $[A]^2$, as required.

6J Corollary Let $G = (V, E)$ be a graph in which V is a (countably) infinite set. Then one of G, $\overline{G}$ includes a complete graph on an infinite set of vertices.

Remark If, in this corollary, V is uncountable, the result will still be valid if V has a countably infinite subset; e.g., if V is the interval $[0, 1]$, it works because V includes the countably infinite set $\{\frac{1}{n} : n \in \mathbb{N}\}$.