Notes for Tutorial 8

6.042 - April 4 and April 7, 2003

The topics this week are well-ordering and the pigeonhole principle, with a side order of graph theory. These notes cover:

1. A quick review of the "divides" relation.
2. Well-ordering versus induction. (well-ordering)
3. The Halting Problem. (pigeonhole)
4. Euler's Formula. (well-ordering)

This should be plenty. If you somehow have extra time, you could give the problem of showing that every sequence of $n^2 + 1$ distinct numbers has either a subsequence of length $n + 1$ that is either strictly increasing or strictly decreasing. The proof is in Rosen.

1 Review of the "divides" relation

The relation $a \mid b$ ("a divides b") holds if there is an integer k such that $ak = b$.

This relation is reflexive and transitive. It is not symmetric because $2 \mid 4$, but it is not true that $4 \mid 2$. If the relation is over the natural numbers, it is also antisymmetric ($a \mid b$ and $b \mid a$ implies $a = b$). However, if the relation is over the integers, it is not antisymmetric ($3 \mid 3$ and $3 \mid -3$, but $3 \neq -3$.)

Here are two simple properties of the "divides" relation that we'll need shortly.

1. If $a \mid b$, then $a \mid cb$ for every integer c.
2. If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$.

Prove these if you like. In any case, leave them on a corner of the board for the next section.

2 Well-Ordering versus Induction

Everything provable by induction is provable via well-ordering and vice-versa. One can show this equivalence formally, but an example may be more persuasive. Have students prove the following simple claim by both induction and well-ordering. Leave "parallel proofs" on the board so students can compare them.

Claim 1 *For all $n \in \mathbb{N}$, $8 \mid (9^n - 1)$.*

Proof. The proof is by induction. Let $P(n)$ be the proposition that $8 \mid (9^n - 1)$. First, note that $P(0)$ is true because 8 divides $9^0 - 1 = 0$. Next, we must show that for all $n \geq 0$, $P(n)$ implies $P(n+1)$. Assume that $P(n)$ is true, where $n \geq 0$. Then we can reason as follows:

$$\begin{aligned}
& 8 \mid (9^n - 1) \\
\Rightarrow \quad & 8 \mid (9 \cdot (9^n - 1)) \\
\Rightarrow \quad & 8 \mid (9 \cdot (9^n - 1) + 8) \\
\Rightarrow \quad & 8 \mid 9^{n+1} - 1
\end{aligned}$$

The initial statement is $P(n)$. The first implication uses property 1, the second uses property 2, and the last follows by simplifying the right side. Thus, $P(n)$ implies $P(n+1)$ and the claim follows by induction. □

Proof. Assume that the claim is false; we'll show that this leads to a contradiction. Let S be the set of all $n \in \mathbb{N}$ such that 8 does not divide $9^n - 1$. By assumption, the set S is nonempty and thus, by the well-ordering principle, S has a smallest element m.

Note that m can not be zero, because 8 divides $9^0 - 1 = 0$. Then, since $m - 1$ is a natural number not in S, we know that 8 divides $9^{m-1} - 1$. We can then reason as follows.

$$\begin{aligned}
& 8 \mid (9^{m-1} - 1) \\
\Rightarrow \quad & 8 \mid (9 \cdot (9^{m-1} - 1)) \\
\Rightarrow \quad & 8 \mid (9 \cdot (9^{m-1} - 1) + 8) \\
\Rightarrow \quad & 8 \mid 9^{m} - 1
\end{aligned}$$

The first implication uses property 1, the second uses property 2, and the last uses simplification on the right side. The result is a contradiction, since m is defined to be an element of S. Therefore, our original assumption was false, and the claim is true. □

3 The Halting Problem

In general, determining whether a program will eventually stop is hopelessly difficult. This is called "the halting problem", and should not be confused with the Laboratory for Computer Science D-league hockey team. To see why the halting problem is so hard, suppose we wrote program to exhaustively search for integral solutions to the equation:

$$a^n + b^n = c^n \qquad \text{(where } a, b, c > 0 \text{ and } n > 2\text{)}$$

Suppose that the program only stops if it finds a solution. Does it eventually stop? The answer is "no". But this assertion is equivalent to Fermat's Last Theorem, which took 350 years to prove! In fact, there is no general way to determine whether a program eventually stops— *on a computer with infinite memory.*

But on a computer with finite memory— say, one gigabyte— we can solve the halting problem by using the pigeonhole principle! Does anyone see how?

Part of the value of this question is that it raises a lot of modelling issues. Try to accept student modelling decisions that don't break the basic argument; e.g., they might include a 60-gig hard drive, they might want to model internal register and caches, etc. Be sure to preclude external inputs and random numbers (unless you're prepared for that complexity!)

Be patient, but here are some hints you can give students if they're going nowhere.

- Let's say a *state* of the computer is a particular setting of its memory bits. How many states does a computer with one gigabyte of memory have?

- Suppose we model the computer's behavior using a directed graph. For each state, create a vertex. If the computer moves from state s to state t when the clock ticks, put an edge $s \to t$. If the computer is halted in a particular state, it has no outgoing edges.

- In these terms, how could a computer *avoid* ever halting?

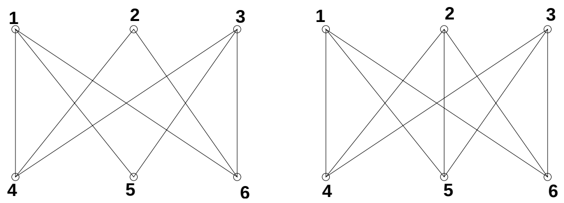
- Suppose you run the computer for a really long time and it hasn't halted. Must it be in a loop?

Here is the solution. The computer has $N = 2^{2^{30}}$ states. Suppose that we run the computer for $N + 1$ clock cycles. If the computer halts, then we certainly know whether it halts eventually. Otherwise, the computer visits states $s_1, \ldots, s_{N+1}$. By the pigeonhole principle, at least two of these states are the same; say, states s_i and s_j where $i < j$. Then the computer is will forever after loop through the states $s_i, \ldots, s_{j-1}$. Thus, if the computer has not halted after $N + 1$ clock cycles, it never halts.

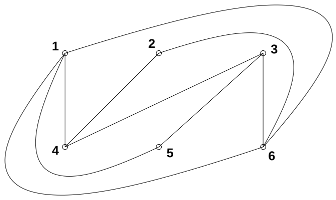
Of course, N is a big number...

4 Euler's Formula

A graph is *planar* if there is a way to draw it on a piece of paper so that no edges cross. For example, are either of these graphs planar?



The graph on the left is planar, because it can be redrawn so that no edges cross:



The graph on the right is not.

If a graph is drawn so that no edges cross, then the edges divide the plane into regions called *faces*. For example, the graph above has five faces, four bounded by edges and one surrounding the whole figure.

A graph is *connected* if there is a path between every pair of vertices. (Obviously, there are all sort of definitional issues involving paths. Avoid them as much as possible and stay on an intuitive level; this will be the least of our crimes in this argument. The points of this problem are (1) to get some feel for proofs involving graphs and (2) to apply well-ordering.)

Ask students to draw some planar graphs on their own paper.

Let V be the number of vertices in a planar graph, let E be the number of edges, and let F be the number of faces. Use well-ordering to prove that for every *connected* planar graph:

$$V - E + F \quad = \quad 2$$

This is called *Euler's formula*. Have students check that their graphs obey this formula. In the example above, there are $V = 6$ vertices, $E = 9$ edges, and $F = 5$ faces, and $6-9+5 = 2$.

Ask students to prove that Euler's formula holds for every connected, planar graph. Many different proofs are possible.

Claim 2 *The following equation holds for every connected, planar graph:*

$$V - E + F \quad = \quad 2$$

Here V is the number of vertices, E is the number of edges, and F is the number of faces.

I think that the following proof will be much more convincing if you work through a concrete example as you explain the argument.

Proof. Supose that the claim is false; we'll show that this leads to a contradiction. Let G be a graph that violates Euler's formula and has the smallest possible number of edges. Suppose that G has V vertices, E edges, and F faces.

It can not be that $E = 0$. In that case, the only connected graph consists of a single vertex. Then we have $V = 1$, $E = 0$, $F = 1$ and so Euler's formula is satisfied.

Therefore, $E > 0$ and so G contains a least one edge (u, v). Consider the graph G' which is obtained by removing edge (u, v) from G.

There are now two cases to consider.

1. Suppose that there is a path from u to v in G'. Then deleting the edge (u, v) decreases both the number of edges and the number of faces by one, and yields a connected planar graph for which Euler's formula holds. Therefore, Euler's formula must have held for G as well, contradicting the definition of G.

2. Suppose that there is no path from u to v in G'. Then we are left with two connected, planar graphs. Suppose the first has parameters E_1, V_1, and F_1 and the second has E_2, V_2, and F_2. Since Euler's formula holds for both, we have:

$$\begin{aligned} V_1 - E_1 + F_1 &= 2 \\ V_2 - E_2 + F_2 &= 2 \\ \Rightarrow \quad (V_1 + V_2) - (E_1 + E_2) + (F_1 + F_2) &= 4 \end{aligned}$$

   Since we deleted one edge, we have $E_1+E_2 = E-1$. Since no vertices have been deleted, we have $V_1 + V_2 = V$. The two graphs share one face, so we have $F_1 + F_2 = F + 1$. Substituting and simplifying gives:

$$\begin{aligned} V - (E - 1) + (F + 1) &= 4 \\ V - E + F &= 2 \end{aligned}$$

   This implies that Euler's formula holds for G, contradicting the definition of G.

In both cases, we obtain a contradiction. Our original supposition was wrong, and the claim is true. □

Claim 3 *The following equation holds for every connected, planar graph:*

$$V - E + F = 2$$

Here V is the number of vertices, E is the number of edges, and F is the number of faces.