MATHEMATICS 300 — SPRING 2001

Introduction to Mathematical Reasoning — H. J. Sussmann

HANDOUT NO. 11—April 30, 2001

1 A COUPLE OF REMARKS ON THE FINAL EXAM

The final exam will have approximately the same structure as the second midterm (but will be longer, of course).

In particular, it will contain lots of questions about definitions and proofs that were given in class or in the book or in the handouts. *Make sure you study all this material carefully and systematically. Just reading things once or twice in a hurry is not enough.*

For the final exam there will definitely be formal proofs. They will be short, but they will be there. And I will try hard not to have typos such as the one in Problem 1 of the second midterm.

THE BINOMIAL THEOREM

THEOREM. Let a, b be real numbers. Let n be a natural number. Then

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}\,.$$

PROOF. We let S be the set of all natural numbers n for which the formula is not true. We want to prove that S is empty.

Assume S is not empty. Then, by the Well Ordering Principle, S has a smallest member. Call it q. Then q is a natural number,

$$(a+b)^q \neq \sum_{k=0}^{q} \binom{q}{k} a^k b^{q-k}\,,$$

and q is the smallest natural number for which this happens.

For $n = 0$, the formula says that $1 = 1$ (because $(a+b)^0 = 1$, since $x^0 = 1$ for every x, and $\sum_{k=0}^{0} \binom{0}{k} a^k b^{0-k} = \binom{0}{0} a^0 b^0 = 1$). So q cannot be 0, because the formula is true for $n = 0$, so $0 \notin S$.

Therefore $q > 0$, so $q-1$ is a natural number, and $q-1 \notin S$. This means that

$$(a+b)^{q-1} = \sum_{k=0}^{q-1} \binom{q-1}{k} a^k b^{q-1-k}\,.$$

Then

$$\begin{aligned}
(a+b)^q &= (a+b)(a+b)^{q-1} \\
&= (a+b)\sum_{k=0}^{q-1}\binom{q-1}{k}a^k b^{q-1-k} \\
&= a\left(\sum_{k=0}^{q-1}\binom{q-1}{k}a^k b^{q-1-k}\right) + b\left(\sum_{k=0}^{q-1}\binom{q-1}{k}a^k b^{q-1-k}\right) \\
&= \left(\sum_{k=0}^{q-1}\binom{q-1}{k}a^{k+1} b^{q-1-k}\right) + \left(\sum_{k=0}^{q-1}\binom{q-1}{k}a^k b^{q-k}\right).
\end{aligned}$$

We now observe that

$$\sum_{k=0}^{q-1}\binom{q-1}{k}a^{k+1}b^{q-1-k} = \sum_{k=1}^{q}\binom{q-1}{k-1}a^k b^{q-k}.$$

(REASON: in the sum $\sum_{k=0}^{q-1}\binom{q-1}{k}a^{k+1}b^{q-1-k}$, relabel the indices by using "j" for $k+1$. Then, as k ranges from 0 to $q-1$, $k+1$ ranges from 1 to q, so j ranges from 1 to q. Also, $\binom{q-1}{k}a^{k+1}b^{q-1-k}$ becomes $\binom{q-1}{j-1}a^j b^{q-j}$, because $k=j-1$. So

$$\sum_{k=0}^{q-1}\binom{q-1}{k}a^{k+1}b^{q-1-k} = \sum_{j=1}^{q}\binom{q-1}{j-1}a^j b^{q-j}.$$

But the variable of summation is a dummy variable, so we can call it anything we like, and in particular we can substitute k for j, obtaining:

$$\sum_{j=1}^{q}\binom{q-1}{j-1}a^j b^{q-j} = \sum_{k=1}^{q}\binom{q-1}{k-1}a^k b^{q-k}.$$

Therefore

$$\sum_{k=0}^{q-1}\binom{q-1}{k}a^{k+1}b^{q-1-k} = \sum_{k=1}^{q}\binom{q-1}{k-1}a^k b^{q-k},$$

as stated.)

It follows that

$$(a+b)^q = \left(\sum_{k=1}^{q}\binom{q-1}{k-1}a^k b^{q-k}\right) + \left(\sum_{k=0}^{q-1}\binom{q-1}{k}a^k b^{q-k}\right).$$

But

$$\begin{aligned}
\sum_{k=1}^{q}\binom{q-1}{k-1}a^k b^{q-k} &= \binom{q-1}{q-1}a^q b^{q-q} + \sum_{k=1}^{q-1}\binom{q-1}{k-1}a^k b^{q-k} \\
&= a^q + \sum_{k=1}^{q-1}\binom{q-1}{k-1}a^k b^{q-k},
\end{aligned}$$

and

$$\sum_{k=0}^{q-1} \binom{q-1}{k} a^k b^{q-k} = \binom{q-1}{0} a^0 b^{q-0} + \sum_{k=1}^{q-1} \binom{q-1}{k} a^k b^{q-k}$$
$$= b^q + \sum_{k=1}^{q-1} \binom{q-1}{k} a^k b^{q-k}.$$

Therefore

$$(a+b)^q = a^q + \left(\sum_{k=1}^{q-1} \binom{q-1}{k-1} a^k b^{q-k} \right) + b^q + \left(\sum_{k=1}^{q-1} \binom{q-1}{k} a^k b^{q-k} \right).$$

Now,

$$\left(\sum_{k=1}^{q-1} \binom{q-1}{k-1} a^k b^{q-k} \right) + \left(\sum_{k=1}^{q-1} \binom{q-1}{k} a^k b^{q-k} \right) = \sum_{k=1}^{q-1} \left(\binom{q-1}{k-1} + \binom{q-1}{k} \right) a^k b^{q-k}$$
$$= \sum_{k=1}^{q-1} \binom{q}{k} a^k b^{q-k},$$

using the identity

$$\binom{q-1}{k-1} + \binom{q-1}{k} = \binom{q}{k}.$$

It follows that

$$(a+b)^q = a^q + b^q + \Big(\sum_{k=1}^{q-1} \binom{q}{k} a^k b^{q-k} \Big).$$

On the other hand,

$$\sum_{k=0}^{q} \binom{q}{k} a^k b^{q-k} = \binom{q}{0} a^0 b^{q-0} + \Big(\sum_{k=1}^{q-1} \binom{q}{k} a^k b^{q-k} \Big) + \binom{q}{q} a^q b^{q-q}$$
$$= b^q + \Big(\sum_{k=1}^{q-1} \binom{q}{k} a^k b^{q-k} \Big) + a^q.$$

Then

$$(a+b)^q = \sum_{k=0}^{q} \binom{q}{k} a^k b^{q-k}.$$

But we established before that

$$(a+b)^q \neq \sum_{k=0}^{q} \binom{q}{k} a^k b^{q-k}.$$

So we have reached a contradiction, and our proof is complete.

THE SIZE OF A FINITE SET

What is the precise definition of "size" (also called "cardinality") of a finite set?

Recall that

> A set A is *finite* if there exists a matching between A and the set I_n for some natural number n.

Recall also that

> If n is a natural number, then $I_n = \{m : m \in \mathbb{N} \wedge 1 \leq m \leq n\}$.

It is then reasonable to guess that the definition of "size of a finite set" will be as follows:

> Let A be a finite set. Then the *size* of A (written $|A|$) is the natural number n such that there exists a matching between A and the set I_n.

This definition, however, poses a problem. We have talked about "the" natural number n such that .... But, how do we know that there is only one such number? Couldn't it happen, for example, that a set A can be matched both with I_{235} and with I_{346}, in which case we would have to say that "the number of elements of A is 235," and also that "the number of elements of A is 346"?

You don't believe that this can happen, right? I don't believe it either, but in mathematics saying that "I don't believe something" is not a proof. So let us give a real proof.

THEOREM. Let A be a set. Let n, m be natural numbers such that there is a matching between A and I_n and there is a matching between A and I_m. Then $n = m$.

PROOF. Suppose M is a matching between A and I_n, and M' is a matching between A and I_m. Then one can easily construct a matching between I_n and I_m. (This is a good exercise for you; prove it! *This would make a wonderful question for the final exam.*) So we can forget about the set A. Our problem really is to show that *if there is a matching between I_n and I_m then n and m must be equal.* Let us relabel the numbers, if necessary, so that n is the smaller of the two. (For example, if $n = 6$ and $m = 5$, we change their names so that n becomes 5 and m becomes 6.) So what we have to do is prove the following.

THEOREM. Let n, m be natural numbers such that $n \leq m$. Assume that there is a matching between I_n and I_m. Then $n = m$.

PROOF. Let us call a natural number n "bad" if there is a matching between I_n and I_m for some natural number m such that $n < m$. We want to prove that there aren't any bad numbers.

Suppose there exist bad numbers. Then, by the well ordering principle, there exists a smallest bad number. Call it ν.

Can ν be zero? Let us see. For 0 to be bad, there would have to exist a matching between I_0 and I_m for some natural number m such that $m > 0$. Suppose M is such a matching. This means, to begin with, that M is a set of ordered pairs (x, y) such that $x \in I_0$ and $y \in I_m$. Since I_0 is the empty set, there do not exist any ordered pairs (x, y) such that $x \in I_0$ and $y \in I_m$. So $M = \emptyset$. Now, a second condition for M to be a matching between I_0 and I_m is that if we pick any member y of I_m there exists an $x \in I_0$ such that $(x, y) \in M$. Pick $y = 1$. (This is possible because we are assuming that $m > 0$, so $1 \in I_m$.) Then there would have to exist an $x \in I_0$ such that $(x, y) \in M$. But such an x does not exist, because $I_0 = \emptyset$. So we have arrived at a contradiction. ("There exists an $x \in I_0$ such that $(x, y) \in M$ and there does not exist an $x \in I_0$ such that $(x, y) \in M$.") Therefore 0 is not bad. So $\nu \neq 0$.

Since ν is a natural number and $\nu \neq 0$, $\nu - 1$ is a natural number. Since ν was the smallest bad number, $\nu - 1$ is not bad.

Now comes the main part of the proof. Let us first discuss a (hypothetical) example, before we actually do the real proof. Imagine, for example, that ν was equal to 38. The fact that ν is bad means that I_{38} can be matched with I_m for some m such that $m > 38$. Imagine, for example, that m was equal to 42. So we have a matching between I_{38} and I_{42} and our goal is to get a contradiction. The way we will do that is by showing that there must exist a matching between I_{37} and I_{41}. This will give us a contradiction, because it would show that 37 is bad, even though 38 was supposed to be the *smallest* bad number.

How do we get our matching between I_{37} and I_{41}? Easy!! Just pick our (hypothetical) matching M between I_{38} and I_{42}, pick one member a of I_{38}, look at the member b of I_{42} that is matched with a under M, and remove the pair (a, b) from M. But this is not as easy as it seems! Suppose, for example, that a was 23. Then, after we remove the pair (a, b) from M, we will be left with a matching between $I_{38} - \{23\}$ (the set of all natural numbers up to 38 with 23 removed) and something. This is not what we want! (What we want is a matching between I_{37} and something, and the set $I_{38} - \{23\}$ is *not* I_{37}.) Part of the problem can be remedied by choosing a to be not just any member of I_{38}, but being much more specific and choosing $a = 38$. We then look at the member b of I_{42} that is matched with 38 under M, and remove the pair $(38, b)$ from M. Now we are definitely left with a matching between I_{37} and "something." But we are still in trouble! The "something" with which I_{37} is matched is going to be $I_{42} - \{b\}$ (the set of all natural numbers up to 42 with b removed), and there is no reason for this set to be the one we want, namely, I_{41}. (Of course it *could* happen that we are lucky and b is precisely 42, in which case we would be doing fine. But this would be an extremely unlikely coincidence. For all we know, M is just a matching between I_{38} and I_{42}, and this by no means implies that under M the number matched with 38 is precisely 42.)

To remedy this problem, we first "fix" M. Suppose, for example, that b was 21 (that is, that the pair $(38, 21)$ belongs to M.) On the other hand, there is some number $u \in I_{38}$ which is matched with 42 under M. Say this number was 15. This means that the pairs $(38, 21)$ and $(15, 42)$ are in M. Now construct a new matching M' by letting M' be the same as M, except that instead of the pairs $(38, 21)$ and $(15, 42)$ we put in M' the pairs $(38, 42)$ and $(15, 21)$. Then one has to prove that M' is also a matching between I_{38} and I_{42}. (This is easy, and a good exercise for you; do it! *This would make a wonderful question for the final exam.*) And M' has this extra feature that we wanted M to have: under M', 38 *is* matched to 42.

Summarizing: we need a matching M between I_{38} and I_{42} with the special additional property that under M 38 is matched to 42. If we pick just any matching M, it will not necessarily have this special property. But we can modify M so as to produce a *new* matching M' having the special property. So *if there is a matching between* I_{38} *and* I_{42} *then there is one having the special property that under this matching* 38 *is matched to* 42. And, once we have such a matching, we can proceed and the rest is smooth sailing.

Now let us go back to our *real* proof. We first prove a lemma.

LEMMA. Let n, m be natural numbers such that $n \leq m$. Assume that there exists a matching between I_n and I_m. Then there exists a matching M between I_n and I_m such that $(n, m) \in M$.

PROOF. Let Q be a matching between I_n and I_m. If $(n, m) \in Q$, then we can take $M = Q$ and we are done.

Now suppose $(n, m) \notin Q$. The definition of matching implies that there exist u, v such that $u \in I_n$, $v \in I_m$, $(u, m) \in Q$, and $(n, v) \in Q$. Moreover, $v \neq m$. (Reason: we are assuming that $(n, m) \notin Q$; therefore, if $(n, v) \in Q$, v cannot be m.) Similarly, $u \neq n$.

Define M by letting

$$M = \Big(Q - \{(n, v), (u, m)\}\Big) \cup \{(u, v), (n, m)\}\,.$$

(That is, M is constructed from Q by removing the pairs (n, v) and (u, m) from Q, and putting in their place the pairs (n, m) and (u, v).)

Then M is a matching between I_n and I_m. (This needs proof. It's a recommended exercise for you. Do it! *This would make a very nice question for the final exam.*) Moreover, $(n, m) \in M$. So the proof of the lemma is complete.

We now return to the proof of our theorem. We have ν, the smallest bad number, and we know that $\nu > 0$. So $\nu - 1$ is a natural number, and $\nu - 1$ is not bad. The fact that ν is bad means that there is a natural number m such that $m > \nu$ for which there exists a matching between I_ν and I_m. But then the lemma tells us that there exists a matching M between I_ν and I_m having the special property that $(\nu, m) \in M$. Let $M' = M - \{(\nu, m)\}$. Then M' is a matching between $I_{\nu-1}$ and I_{m-1}. (This needs proof. It's a recommended exercise for you. Do it! *This would make a very nice question for the final exam.*) Since $\nu < m$, it follows that $\nu - 1 < m - 1$. But we have shown that there exists a matching between $I_{\nu-1}$ and I_{m-1}. Therefore $\nu - 1$ is bad. But this contradicts the fact that ν was the smallest bad number. This contradiction completes our proof. c