These are *rough notes* based on my own notes I prepared for the Week 6 lecture. They go with the annotated lecture slides you can see on the "More" page of the course website. Although they are rough, I'm providing them here in case they help you remember what we did in lecture.

(In case you're curious: I don't follow these notes exactly in lecture. Once I'm in class, I try not to read them at all if I can avoid it. So why do I write them? Because writing these notes is like a practice run for the lecture. I find any presentation I give (like a lecture) goes a lot more smoothly if I've spent a bit of time thinking about every part of it.)

1 Legend

Text that should already be on slides.
Descriptions of other things that should already be on slides.

Text I should write during lecture.

Descriptions of other things I should draw or write or do.

2 Recursively defined functions

Recursively defined functions

Let F be the smallest set such that
- Base case: variables $A, B, \ldots, Z \in F$.
- Constructor cases: If $e, f \in F$, then $(e \text{ AND } f), \text{NOT } e \in F$.

(F = propositional formulas with AND and NOT.)

For $f \in F$, let
- $N_v(f) = \#$ occurrences of variables in f
- $N_{op}(f) = \#$ occurrences of operators in f

Give recursive (or "inductive") definitions of N_v and N_{op}.

We've talked about recursively defined sets. We can also define functions on those sets recursively.

Base case: If $e \in F$, $N_v(e) = 1$ and $N_{op}(e) = 0$.

Constructor cases: If $e, f \in F$,

- $N_v((e \text{ AND } f)) = N_v(e) + N_v(f)$
- $N_{op}(e \text{ AND } f) = 1 + N_{op}(e) + N_{op}(f)$
- $N_v(\text{NOT } e) = N_v(e)$

- $N_{op}(\text{NOT } e) = 1 + N_{op}(e)$

Let Bkt be the smallest set such that
- Base case: $\lambda \in \text{Bkt}$
- Constructor cases: If $s, t \in \text{Bkt}$, then $s \cdot t$, $\texttt{[}s\texttt{]} \in \text{Bkt}$.

Define $f : \text{Bkt} \to \mathbb{N}$ by
- Base case: $f(\lambda) = 1$.
- Constructor cases: for $s, t \in \text{Bkt}$, $f(s \cdot t) = f(s) + f(t)$ and $f(\texttt{[}s\texttt{]}) = f(s)$.

What is $f(\texttt{[]})$?

$\texttt{[]} = \texttt{[]} \cdot \lambda$, so $f(\texttt{[]}) = f(\texttt{[]}) + f(\lambda) = f(\texttt{[]}) + 1$.

The definition of Bkt is ambiguous.

Unambiguous definition of Bkt

Let Bkt be the smallest set such that
- Base case: $\lambda \in \text{Bkt}$
- Constructor case: If $s, t \in \text{Bkt}$, then $\texttt{[}s\texttt{]}t \in \text{Bkt}$.

(Exercise: prove this is the same set.)

(Exercise: prove no string can be constructed more than one way.)

What are these functions?

Define $N : \text{Bkt} \to \mathbb{N}$ by:
- Base case: $N(\lambda) = 0$
- Constructor case: for $s, t \in \text{Bkt}$, let $N(\texttt{[}s\texttt{]}t) = 2 + N(s) + N(t)$

Define $D : B \to \mathbb{N}$ by:
- Base case: $D(\lambda) = 0$
- Constructor case: for $s, t \in \text{Bkt}$, let $D(\texttt{[}s\texttt{]}t) = \max\{1 + D(s), D(t)\}$.

$N(s) = \#$ brackets in s

$D(s) =$ max depth of brackets in s

Use structural induction to prove $\forall s \in \text{Bkt}\,.\, N(s) \geq 2D(s)$.

Proof:

For $s \in \text{Bkt}$, let $P(s) =$ "$N(s) \geq 2D(s)$".

Base case: $N(\lambda) = 0$, $2D(\lambda) = 0$, so $N(\lambda) \geq 2D(\lambda)$, i.e. $P(\lambda)$.

Induction step:

Let $s, t \in \text{Bkt}$.

Assume $P(s)$ and $P(t)$. (I.H.)

Then

$$\begin{aligned} N(\texttt{[}s\texttt{]}t) =& 2 + n(s) + N(t) \\ \geq& 2 + 2D(s) + 2D(t) \quad \text{by I.H.} \\ =& 2(1 + D(s) + D(t)) \\ \geq& 2 \cdot \max\{1 + D(s), D(t)\} \\ =& 2D(\texttt{[}s\texttt{]}t) \end{aligned}$$

By structural induction, $\forall s \in \text{Bkt}\,.\, P(s)$. □

3 Induction over $\mathbb{N} \times \mathbb{N}$

Suppose $P : \mathbb{N} \times \mathbb{N} \to \{\text{T}, \text{F}\}$ is a predicate, and we want to prove:

$$\forall x \in \mathbb{N}.\, \forall y \in \mathbb{N}.\, P(x, y)$$

(Ask for suggestions.)

Method 1:

Recursively define $\mathbb{N} \times \mathbb{N}$: smallest set s.t:

- $(0, 0) \in \mathbb{N} \times \mathbb{N}$
- If $(x, y) \in \mathbb{N} \times \mathbb{N}$, then $(x + 1, y), (x, y + 1) \in \mathbb{N} \times \mathbb{N}$.

Then use structural induction.

Method 2:

For $x \in \mathbb{N}$ let $Q(x) = \forall y \in \mathbb{N}.\, P(x, y)$. Prove $\forall x \in \mathbb{N}.\, Q(x)$ using complete induction.

Let $x \in \mathbb{N}$ and assume $\forall x' \in \mathbb{N}.\, (x' < x \text{ IMPLIES } Q(x))$.

$\vdots$

$\vdots$

$Q(x)$

$\forall x \in \mathbb{N}.\, Q(m)$ by complete induction.

We prove $Q(x)$ by induction

Fill in $\vdots$ with:

Let $y \in \mathbb{N}$. Assume $\forall y' \in \mathbb{N}.\, P(x, y')$.

$\vdots$

$P(x, y)$

By induction, $\forall y \in \mathbb{N}.\, P(x, y)$.
$Q(x)$ (by definition)

(Point to the remaining $\vdots$.) Okay, so this is going to be where the actual work of the proof goes. When we're trying to prove $P(x, y)$, what can we assume?

(Wait for answers.)

Fill in a grid, showing we can assume $P(x', y')$ for all $x' < x$ and all y', and we can assume $P(x, y')$ for all $y' < y$.

4 Order relations

Definition. A *partial order* on a set S is a binary predicate ("relation") $R : S \times S \to \{\mathrm{T}, \mathrm{F}\}$ such that for all $x, y, z \in S$:

- $R(x, x)$
- $(R(x, y)$ AND $R(y, x))$ IMPLIES $x = y$
- $(R(x, y)$ AND $R(y, z))$ IMPLIES $R(x, z)$

S	$R(x, y)$	Partial order?
$\mathbb{N}$	$x \leq y$	
$\mathbb{R}$	$x \leq y$	
$\mathbb{C}$	$\lvert x \rvert \leq \lvert y \rvert$	
$\mathcal{P}(\{1, 2, 3\})$	$x \subseteq y$	
players in a round-robin tournament	x beat y	
commits in a git repository	x is an ancestor of y *(drawing)*	

Beside the three items:

- (reflexive)

- (antisymmetric)
- (transitive)

With help, start filling in the table. Yes beside $\mathbb{N}$, $\mathbb{R}$.

Beside $\mathbb{C}$*:* not antisymmetric: $|i| \leq |1|$ and $|1| \leq |i|$.

Beside $\mathcal{P}(\{1,2,3\})$. Yes

Beside chess players: not transitive

Beside commits in a git repository

Definition. A *total order* on S is a partial order R on S such that
- $\forall x \in S.\, \forall y \in S.\, (R(x,y)$ OR $R(y,x))$

(Beside the only item) (comparability)

E.g. $\leq$ on $\mathbb{Z}$, $\mathbb{N}$, $\mathbb{R}$.

$\subseteq$ on $\mathcal{P}(\{1,2,3\})$?

No, $\{1,2\}$ and $\{2,3\}$ not comparable.

Definition. A total order on a set S is a *well-ordering* if every non-empty subset of S has a minimum element.

Which of these total orders R are well-orderings?

S	$R(x,y)$	Well-ordering?
$\mathbb{Z}$	$x \leq y$	
$\mathbb{N}$	$x \leq y$	
$\mathbb{Q}^+$ (positive rationals $\frac{1}{2}, \frac{9}{7}, \frac{2}{3}, \ldots$)	$x \leq y$	

Beside $\mathbb{Z}$. No, take $S = \mathbb{Z} \subseteq \mathbb{Z}$: no minimum element.

Beside $\mathbb{Q}^+$. No. Also has no minimum element.

Beside $\mathbb{N}$. Yes

$\leq$ is not a well-ordering on $\mathbb{Z}$ or $\mathbb{Q}^+$. Is it possible to define any well-ordering on those sets?

$\mathbb{Z}$: order as $0, -1, 1, -2, 2, \ldots$.

$$R(x,y) = (|x| \leq |y|) \text{ AND } (|x| = |y| \text{ IMPLIES } x \leq y)$$

$\mathbb{Q}^+$: order by max{numerator, denominator} then numerator, in lowest terms. $\frac{1}{1}, \frac{1}{2}, \frac{2}{1}, \frac{1}{3}, \frac{2}{3}, \frac{3}{2}, \ldots$.

5 Well-ordering proofs

Well-ordering proofs

Theorem 1. Every positive rational number m/n can be expressed in lowest terms, i.e. as m'/n' where m' and n' in $\mathbb{Z}^+$ have no common factors other than 1.

Proof:

Let $m, n \in \mathbb{Z}^+$.

$24/20 \to 12/10 \to 6/5$

We want the smallest denominator n'.

Let $C = \{\text{possible denominators for } m/n\}$.

Given n', want $m'/n' = m/n$, so $m' = (m/n)n'$.

$C = \{n' \in \mathbb{Z}^+ | (m/n)n' \in \mathbb{Z}^+\}$.

C is nonempty because $n \in C$. Since $\leq$ is a well-ordering of $\mathbb{Z}^+$ and $C \subseteq \mathbb{Z}^+$, C has a smallest element. Call it n'.

Let $m' = (m/n)n' \in \mathbb{Z}^+$. Suppose for a contradiction that m' and n' have a common factor $k > 1$. Then $n'/k \in C$. But $n'/k < n'$ and n' is the smallest element of C. Contradiction.

So m' and n' have no common factors. □

Any complete induction proof can be turned into a well-ordering proof

E.g. from last week:

Theorem 2. Every integer greater than 1 is a product of (one or more) prime numbers.

(In class, we ran out of time, and I only wrote the definition of C.)

Proof:

Let $C = \{x \in \mathbb{N} | x > 1$ AND x is not a product of prime numbers$\}$. Enough to prove $C = \emptyset$.

Suppose for a contradiction that $C \neq \emptyset$.

Then since $\leq$ is a well-ordering on $\mathbb{N}$, there is a smallest element $x^* \in C$.

x^* is not prime (otherwise: product of just itself) and $x > 1$, so $\exists$ integers $y > 1, z > 1$ s.t. $x = yz$.

$y < x^*$ and $z < x^*$ so $y, z \notin C$. So y and z can be written as products of primes, so x^* can too. So $x^* \notin C$. Contradiction.

So $C = \emptyset$ (proof by contradiction). $\square$