# Day 12

Thursday June 7, 2012

## 1 A Word on Well-Ordering

We talked about the principle of induction. Given a formula $\varphi(n)$ then to prove $\forall n.\varphi(n)$ then it is sufficent to prove

- $\varphi(0)$.
- $\forall n.\varphi(n) \to \varphi(n+1)$

We mentioned that $\mathbb{N}$ is a **well-ordering**, that is that $\leq$ is a linear ordering (total, transitive, reflexive, anti-symmetric) on $\mathbb{N}$ and that it is well-founded (no infinite descending chains). All of these properties are obvious on $\mathbb{N}$. There is another property that is quite useful:

**Definition 1** (The Well-Ordering Property)**.** A set $A$ with a linear ordering $\preceq$ has the **well-ordering property** if and only if for every $S \subseteq A$, where $S \neq \emptyset$, there is an $a \in S$ which is minimum with respect to $\preceq$, that is every $b \in S$ is such that $a \preceq b$.

As it turns out, a set is a well-ordering if and only if it has the well-ordering property.

*Proof.* Suppose that $A$ with $\succeq$ is well ordered. Then it is a linear order and there are no infinite descending chains. We want to show that it has the well-ordering property. So take $S \subseteq A$ nonempty. We want to show that $S$ has a least element.

We go by contradiction. Suppose not. Then take $x_1 \in S$, which is possible as $S$ is nonempty. As $x_1$ is not minimal, we can find $x_2 \in S$ such that $x_1 \succeq x_2$. Similarly, $x_2$ is not minimal, so we can find $x_3$ such that $x_1 \succeq x_2 \succeq x_3$ continuing in this way we get a infinite descending chain, which contradicts well-foundedness.

Conversely, suppose that we have the well-ordering property. Suppose for contradiction, the set was no well-founded. So take an infinite descending chains

$$a_1 \succeq a_2 \succeq a_3 \succeq \cdots$$

Take the set of all elements in this chain $\{\, a_i \mid i \in \mathbb{Z}^+ \,\}$. By the well-ordering property, this has a least element, which is $a_k$ for some $k \in \mathbb{Z}^+$. So then the infinite descending chain must just be $a_k$ past $k$, which contradicts the chain is strictly descending. □

Why is this important? It illustrates an important characteristic of $\mathbb{N}$: every nonempty subset of $\mathbb{N}$ has a least element. Now, using this property, we can prove induction.

*Proof.* We want to show that induction is valid. That is

$$(\varphi(0) \wedge (\forall n.\varphi(n) \to \varphi(n+1))) \to (\forall n.\varphi(n))$$

Suppose this is false. So we have

$$(\varphi(0) \wedge (\forall n.\varphi(n) \to \varphi(n+1))) \wedge (\exists n.\neg\varphi(n))$$

Well, as $\exists n.\neg\varphi(n)$ we have an $m$ that satisfies $\neg\varphi(m)$. In fact, we may have lots of counterexamples. Let $S$ be the set of counterexamples, ie. like $m \in S$ if and only if $\neg\varphi(m)$. As $\exists n.\neg\varphi(n)$ we know $S$ is nonempty.

By the well-ordering property $S$ has a least element, call it $m$. We now do cases:

If $m = 0$, we get a contradiction, because we have $\varphi(0)$.

Otherwise, $m = k+1$ for some $k$. Instantiating the universal statement we are assuming at $k$ and we get $\varphi(k) \to \varphi(k+1)$. As $m$ is least, we know $\varphi(k)$ holds, and thus we know $\varphi(k+1)$, ie. we know $\varphi(m)$. □

As an application, anytime we take natural numbers, we can assume that they are the smallest such.

**Theorem 1.** *$\sqrt{2}$ is irrational.*

*Proof.* Suppose not; then we can find $n$ and $m$ naturals such that $\sqrt{2} = \frac{n}{m}$. We may assume that $n$ and $m$ are the least such. Then we have that $2m^2 = n^2$. Thus $n$ is even, so $n = 2k$ for some $k \in \mathbb{N}$. And so $2m^2 = 4k^2$, ie. $m^2 = 2k^2$.

Then $m$ is even, so $m = 2l$ for some $l \in \mathbb{N}$.

So we have $m = 2l$ and $n = 2k$, so $\sqrt{2} = \frac{2l}{2k} = \frac{l}{k}$; as $l < m$ and $k < n$, we have a contradiction, as we chose these numbers as small as possible! □

This style of proof is called **proof by infinite descent**

# 2 Equivalence Relations

Now, we begin talking about equivalence relations. This will occupy our time for the rest of the week, essentially.

**Definition 2.** Equivalence relations are meant to capture the properties of equality on sets. $\sim$ is an equivalence relation on a set $A$ if and only if it is

- Reflexive: $\forall a \in A \,.\, a \sim a$.
- Symmetric: $\forall a, b \in A \,.\, (a \sim b) \to (b \sim a)$.
- Transitive: $\forall a, b, c \in A \,.\, ((a \sim b) \wedge (b \sim c)) \to (a \sim c)$.

**Example 1.** There are many examples of equivalence relations. We will use the following toy relation to begin.

Define $\sim$ on the real numbers by

$$a \sim b \iff a = b + 2\pi k \text{ for some } k \in \mathbb{Z}$$

Geometrically, $a$ and $b$ are related if $a$ and $b$ represent the same angle.

We first prove this is an equivalence relation.

*Proof.* First we show that it is reflexive. Let $a \in \mathbb{R}$ be arbitrary. We seek to show that $a \sim a$. Well, this is clear, as $a = a + 2\pi \cdot 0$.

Next, we show that it is symmetric. Like $a, b \in \mathbb{R}$, and take $k$ such that $a = b + 2\pi k$. Then of course, $b = a + 2\pi(-k)$, so $b \sim a$.

Finally, suppose that $a \sim b$ and $b \sim c$. Then take $k, l \in \mathbb{Z}$ such that $a = b + 2\pi k$ and $b = c + 2\pi l$. Then we have $a - 2\pi k = c + 2\pi l$, an so $a = c + 2\pi(k + l)$ □

**Definition 3.** Let $\sim$ be a an equivalence relation on a set $A$. Then if $a \in A$ the **equivalence class of $a$ with respect to $\sim$**, which we denote $[a]_\sim$ is:

$$[a]_\sim = \{\, b \in A \mid a \sim b \,\}$$

That is, the equivalence class of $a$ is all of the things in $a$ that are related to $a$.

We say $a$ is the **representative** of the class $[a]_\sim$.

**Example 2.** Consider the above equivalence class.

$$[0]_\sim = \{\, \ldots, -4\pi, -2\pi, 0, 2\pi, 4\pi, \ldots \,\}$$

Note then that $[0]_\sim = [2\pi]_\sim$. Can you write down what $[\frac{\pi}{2}]_\sim$ is?

The set of equivalence classes form a partition of a set.

**Definition 4.** If $A$ is a set then a family of sets $\{\, \mathscr{F}_\alpha \mid \alpha \in \Lambda \,\}$ is a **partition** if

- The sets span $A$: that is for every $a \in A$, there is some $\alpha$ such that $a \in F_\alpha$. More concisely

$$A = \bigcup_{\alpha \in \Lambda} \mathscr{F}_\alpha$$

- The sets are pairwise disjoint: that is, for each $\alpha, \beta \in \Lambda$ we have $\mathscr{F}_\alpha \cap \mathscr{F}_\beta = \emptyset$.
- The sets are nonempty: that is for each $\alpha \in \Lambda$, $\mathscr{F}_\alpha \neq \emptyset$.

**Theorem 2.** *If $A$ is a set and $\sim$ is an equivalence relation on $A$ then the set of equivalence classes $\{ [a]_\sim \mid a \in A \}$ is a partition.*

*Proof.* First we show that the sets span $A$. Take $a \in A$. Want to show that $a$ is in some equivalence class. Well, by reflexivity, $a \sim a$, so $a \in [a]_\sim$.

Clearly each equivalence class is nonempty as it at least has the representative in there.

Finally, we show they are disjoint. Suppose that $E_1$ and $E_2$ are two distinct equivalence classes. As they are distinct and nonempty (by last sentence) we can take $a \in E_1$ and $b \in E_2$ such that $a \not\sim b$. Want to show they are disjoint. Otherwise, there is a $c \in E_1 \cap E_2$. Then $a \sim c$ and $b \sim c$. By symmetry, we have $a \sim c$ and $c \sim b$. By transitive, we get $a \sim b$, which is a contradiction. $\square$

# 3 Group Work

Today, we will work in groups to talk about different relations. For each of the following relations, you should answer two questions:

- Prove that it is an equivalence relation.
- Describe it's equivalence classes

Some are easier than others, and they are presented in what I feel is increasing difficulty.

## 3.1 Complex Magnitude

Recall the complex numbers are numbers of the form $a + bi$ where $i = \sqrt{-1}$. The **magnitude** of a complex number $a + bi$ is

$$|a + bi| = \sqrt{a^2 + b^2}$$

Define the relation $\circ$ on $\mathbb{C}$ by : If $z_1, z_2 \in \mathbb{C}$ then $z_1 \circ z_2$ if and only if $|z_1| = |z_2|$

## 3.2 Odd Factors

Consider the positive integers (that is: natural numbers, without 0). We can write every positive integer $n$ uniquely as some odd number times a power of 2. This odd number is the largest odd number that divides $n$. For example, for 18, the largest odd number that divides it is 9.

So define the relation $\equiv$ on $\mathbb{Z}^+$ by $n \equiv m$ if and only if $n$ and $m$ have the same largest odd number factor (for example: $9 \equiv 18$, but $9 \not\equiv 27$).

## 3.3 Powers of Two

Similar as above, we have that every positive integer $n$ can be unique written as some odd numbers times a power of 2. So we define a relation $\frown$ on the positive integers $\mathbb{Z}^+$ by $n \frown m$ if and only if the $n$ and $m$ have the same largest power of two (eg. $2 \frown 6$, but $2 \not\frown 12$)

## 3.4 Periodic Sine

Recall that $\sin(x)$ is a function on the real numbers that takes in a real numbers, reads it as an angle, and then returns the $y$-coordinate of the point on the unit circle corresponding to that angle. This is a periodic function that has period $2\pi$. But besides its periodicity, it is still not 1-1, as $\sin(0) = \sin(\pi)$.

So, we make a relation $\approx$ on real numbers and say $x \approx y$ if and only if $\sin(x) = \sin(y)$.

## 3.5 Differing by a Rational

The real numbers $\mathbb{R}$ contain both rationals and irrationals. But, the rationals have nice closure properties (the sum and difference of two rationals is rational) where as the irrationals do not.

So, define a relation on $\mathbb{R}$ by relating two numbers if they differ by a rational; that is define $\cong$ on $\mathbb{R}$ by $x \cong y$ if and only if $x - y \in \mathbb{Q}$.

## 3.6 Infinite Binary Sequence

An **infinite sequence** is a sequence of numbers indexed by $\mathbb{Z}^+$. For example: $(2, 4, 6, 8, 10, \ldots)$ is a sequence. From the pattern, it looks like the 6th element of the sequence is 12.

An **infinite binary sequence** is a sequence of just 0's and 1′. For example $(1, 0, 1, 0, 1, 0, 1, \ldots)$ is a sequence, where it looks like the $i$th element of the sequence of 1 if $i$ is odd and 0 if $i$ is even.

We write sequence as $(a_n)_{n\in\mathbb{Z}^+}$, and then we say $a_i$ when referring to the $i$th element of the sequence. So, if we name the first sequence above $(b_i)_{i\in\mathbb{Z}^+}$, then we would say $b_1 = 2$ and $b_6 = 12$.

We define $\sim$ on the set of infinite binary sequences as follows:

$$(a_n)_{n\in\mathbb{Z}^+} \sim (b_n)_{n\in\mathbb{Z}^+} \iff \exists N \in \mathbb{Z}^+ . \forall m > N \, . \, a_m = b_m$$

That is, two binary sequences are equivalent if they are "eventually equal," ie. there is a point for which after then they are equal. For example,

$$(1, 0, 1, 1, 0, 0, 0, 0, 0, \ldots) \sim (1, 1, 0, 0, 0, 0, 0, 0, \ldots)$$

Where both of the above sequences continue to be 0's forever.