CS202 Discrete Mathematics

Topics I teach:

Set theory: sets, relations, functions, countability; Logic: formulae, interpretations, methods of proof, soundness and completeness in propositional and predicate logic; Number theory: division algorithm, Euclid's algorithm, fundamental theorem of arithmetic, Chinese remainder theorem, special numbers like Catalan, Fibonacci, harmonic and Stirling;

Lecture 1: 31 Jul 2014

A function with a signature of $\{0,1\}^n \to \{0,1\}$ is called a boolean function. There are four 1-variable boolean functions, and sixteen 2-variable boolean functions. See the tables below.

x	0	x	$\neg x$	1
0	0	0	1	1
1	0	1	0	1

x	y	0	$\wedge$	$\not\rightarrow$	x	$\not\leftarrow$	y	$\oplus$	$\vee$	$\downarrow$	$\leftrightarrow$	$\neg y$	$\leftarrow$	$\neg x$	$\rightarrow$	$\uparrow$	1
0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
0	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
1	0	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
1	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1

Negation of x is represented variously as $\neg x$, $\bar{x}$, x'. OR of x and y is represented as either $x \vee y$ or $x + y$. AND of x and y is represented as either $x \wedge y$ or xy.

The truth table of an n-variable boolean function is a table with 2^n rows, one corresponding to each possible assignment of boolean (or truth) values (false=0 or true=1) to the input variables. A boolean function is fully specified by its truth table. For example, see function f defined below using its truth table.

A boolean expression is an expression constructed from boolean variables (that take boolean values) and boolean functions (operators/connectives). Negation is a unary operator because it operates on one argument. $\wedge$, $\not\rightarrow$, $\not\leftarrow$, $\oplus$, $\vee$, $\downarrow$, $\leftrightarrow$, $\leftarrow$, $\rightarrow$, and $\uparrow$ are binary operators because each of them takes two arguments.

Given a boolean expression, its truth table can be constructed from the truth tables of its constituents. For boolean expressions e_1 and e_2, $e_1 \equiv e_2$ iff they have the same truth table. For example, the truth tables below establish that $\overline{x+y} \equiv \bar{x}\bar{y}$, and $\overline{xy} \equiv \bar{x} + \bar{y}$; these are called De Morgan's laws. Two boolean expressions are logically equivalent, if they have the same truth table.

x	y	z	f	f
0	0	0	0	1
0	0	1	0	1
0	1	0	1	0
0	1	1	0	1
1	0	0	0	1
1	0	1	1	0
1	1	0	0	1
1	1	1	1	0

x	y	$\bar{x}$	$\bar{y}$	$x+y$	xy	$\bar{x}+\bar{y}$	$\bar{x}\bar{y}$	$\overline{x+y}$	$\overline{xy}$
0	0	1	1	0	0	1	1	1	1
0	1	1	0	1	0	1	0	0	1
1	0	0	1	1	0	1	0	0	1
1	1	0	0	1	1	0	0	0	0

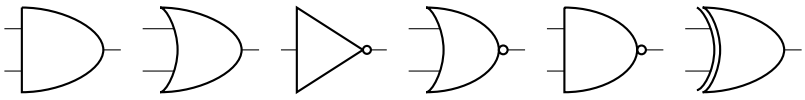
De Morgan's laws can be extended to many variables: $\overline{x+y+z} \equiv \bar{x}\bar{y}\bar{z}$, and $\overline{xyz} \equiv \bar{x} + \bar{y} + \bar{z}$.

Using the rows of the truth table in which $f \equiv 1$, we can write that $f \equiv \bar{x}y\bar{z} + x\bar{y}z + xyz$. This is a "sum of products" (SoP) form for f. Using the remaining rows of the truth table, we can write that $\bar{f} \equiv \bar{x}\bar{y}\bar{z} + \bar{x}\bar{y}z + \bar{x}yz + x\bar{y}\bar{z} + xy\bar{z}$. By De Morgan's laws, therefore, $f \equiv (x+y+z)(x+y+\bar{z})(x+\bar{y}+\bar{z})(\bar{x}+y+z)(\bar{x}+\bar{y}+z)$. This is a "Product of Sums" (PoS) form for f.

That is, given the truth table of f, a SoP, as well as a PoS form of f can be readily found. These expressions use only $\neg$, $\wedge$ and $\vee$ among the logical connectives. Therefore, $\{\neg, \wedge, \vee\}$ is a complete set of connectives.

Using De Morgan's laws $\wedge$ can be synthesized using $\vee$ and $\neg$. Hence, $\{\neg, \vee\}$ is a complete set of connectives. Similarly, $\vee$ can be synthesized using $\wedge$ and $\neg$. Hence, $\{\neg, \wedge\}$ too is a complete set of connectives.

A boolean expression can be converted into a "circuit diagram" using "logic gates". The following logic gates represent AND, OR, NOT, NOR, NAND, XOR respectively.



For $x \in \{0, 1\}$, $x \uparrow x \equiv \bar{x}$, and $\overline{x \uparrow y} \equiv x \wedge y$.
For $x \in \{0, 1\}$, $x \downarrow x \equiv \bar{x}$, and $\overline{x \downarrow y} \equiv x \vee y$.

Therefore, $\{\uparrow\}$ and $\{\downarrow\}$ are also complete sets of connectives. NAND and NOR are, therefore, called universal logic gates.

NAND and NOR are the only universal logic gates. This can be proved as follows. Suppose $h(x, y)$ is a logic gate. Consider a 2-input circuit made up of h-gates. If $h(0, 0)$ were 0, then forcing both the inputs of the circuit to 0 will force the output of the circuit to 0 because a 1 will not be generated at any point inside the circuit. Therefore, the circuit cannot be equivalent to, for example, NAND. Remember, $0 \uparrow 0 \equiv 1$. That is, for h to be universal, it must be that $h(0, 0) \equiv 1$. Similarly, it can be argued that if h is universal, then $h(1, 1) \equiv 0$. $h(0, 1)$ and $h(1, 0)$ can now be filled in four ways. The four functions we get are $\bar{x}$, $\bar{y}$, NAND and NOR. The former two cannot be universal as they depend only on one input.

Note that $\{\wedge, \vee\}$ is not a complete set of connectives. Any 2-input circuit made of AND and OR gates will produce 0 when the inputs are both 0.

Boolean expression $x \rightarrow y$ is called an implication; x is its antecedent and y is its consequent; it evaluates to 0 iff $x \equiv 1$ and $y \equiv 0$. In other words, when the antecedent is false, an implication is true. For example, "If $2 + 2 \equiv 5$, then Bertrand Russell is the Pope" is trivially true.

For an implication $x \rightarrow y$, $\bar{y} \rightarrow \bar{x}$ is its contrapositive, $y \rightarrow x$ is its converse, and $\bar{x} \rightarrow \bar{y}$ is its inverse. An implication and its contrapositive are logically equivalent. Therefore, the converse and inverse of an implication are logically equivalent.

Lecture 2: 5 Aug 2014

An implication $p \to q$ can be expressed in English in many ways. Some are: "if p, then q", "p is sufficient for q", "q when p", "a necessary condition for p is q", "q unless $\neg p$", "p implies q", "p only if q", "q follows from p". A double implication $p \leftrightarrow q$ can be expressed in English in many ways. Some are: "p is necessary and sufficient for q", "p iff q", "p if and only if q".

Logical connectives have the following precedence:

$\neg$ (highest)

$\wedge$ and $\uparrow$ (left to right association)

$\vee$ and $\downarrow$ and $\oplus$ (left to right association)

$\to$ (right to left association)

$\leftrightarrow$ (right to left association) (lowest).

Therefore, $p \vee q \to r \leftrightarrow s \vee t \wedge u$ must be parenthesized like this: $((p \vee q) \to r) \leftrightarrow (s \vee (t \wedge u))$. $p \to q \to r$ means $p \to (q \to r)$. $p \vee q \oplus r$ means $(p \vee q) \oplus r$

A boolean expression is a tautology if the rightmost column of its truth table has only 1's. A boolean expression is a contradiction if the rightmost column of its truth table has only 0's.

Recall, two boolean expressions are logically equivalent if they have the same truth table. Verify that the following equivalences hold: (Read $\bar{x}$ as $\neg x$, $x + y$ as $x \vee y$, xy as $x \wedge y$, 0 as false and 1 as true.)

Identity laws: $p1 \equiv p$; $p + 0 \equiv p$

Domination laws: $p + 1 \equiv 1$; $p0 \equiv 0$

Idempotent laws: $p + p \equiv p$; $pp \equiv p$

Double negation law: $\bar{\bar{p}} \equiv p$

Commutative laws: $p + q \equiv q + p$; $pq \equiv qp$

Associative laws: $(p + q) + r \equiv p + (q + r)$; $(pq)r \equiv p(qr)$

Distributive laws: $p + qr \equiv (p + q)(p + r)$; $p(q + r) \equiv pq + pr$

De Morgans laws: $\overline{pq} \equiv \bar{p} + \bar{q}$; $\overline{p + q} \equiv \bar{p}\bar{q}$

Absorption laws: $p + pq \equiv p$; $p(p + q) \equiv p$

Negation laws: $p + \bar{p} \equiv 1$; $p\bar{p} \equiv 0$

These laws can be used to simplify boolean expressions. For example, consider the following puzzle (Smullyan, Rossen): An island has two kinds of inhabitants, knights, who always tell the truth, and knaves, who always lie. You encounter two persons A and B. What are A and B, if A says "B is a knight" and B says "The two of us are of opposite types"?

Let p denote "A is a knight" and q denote "B is a knight". A is a knight if and only if what A said is true, namely q. That is, $p \leftrightarrow q$. B is a knight if and only if what B said is true, namely $p\bar{q} + \bar{p}q$. That is, $q \leftrightarrow p\bar{q} + \bar{p}q$. Putting the two together we have: $(p \leftrightarrow q)(q \leftrightarrow p\bar{q} + \bar{p}q) \equiv (pq + \bar{p}\bar{q})(q(p\bar{q} + \bar{p}q) + \bar{q}(pq + \bar{p}\bar{q})) \equiv (pq + \bar{p}\bar{q})(\bar{p}q + \bar{p}\bar{q}) \equiv (pq + \bar{p}\bar{q})\bar{p} \equiv \bar{p}\bar{q}$. That is, both A and B are knaves.

Note that $\overline{\bar{p}q + p\bar{q}} \equiv (p + \bar{q})(\bar{p} + q) \equiv pq + \bar{p}\bar{q}$

Another puzzle. A says "At least one of us is a knave" and B says nothing. As before, let p denote "A is a knight" and q denote "B is a knight". A is a knight if and only

if what A said is true, namely $\bar{p}\bar{q} + \bar{p}q + p\bar{q}$. That is, $p \leftrightarrow \bar{p}\bar{q} + \bar{p}q + p\bar{q}$, which is equivalent to $p(\bar{p}\bar{q} + \bar{p}q + p\bar{q}) + \bar{p}(pq) \equiv 0 + 0 + p\bar{q} + 0 \equiv p\bar{q}$. Therefore, A is a knight, but B is a knave.

Note that $\overline{\bar{p}\bar{q} + \bar{p}q + p\bar{q}} \equiv (p + q)(p + \bar{q})(\bar{p} + q) \equiv (p + q)(pq + \bar{p}\bar{q}) \equiv pq$

Lecture 3: 6 Aug 2014

Arguments like "All men are mortal. Socrates is a man. So, Socrates is mortal." cannot be expressed using propositional formulae (boolean expressions). For this we need a richer logic called Predicate/First Order Logic.

In the statement "$4 > 3$", 4 is the subject and "> 3" is the predicate. The subject can be abstracted away using a variable as in "$x > 3$". Let $P(x)$ denote the predicate "$x > 3$". Then $P(5)$ denotes the statement "$5 > 3$". $P(2)$ denotes "$2 > 3$".

More than one noun can be abstracted away using variables. For example, let $Q(x, y)$ be the predicate "$x > y$". Then $Q(5, 7)$ denotes "$5 > 7$". Let $R(x, y, z)$ denote the predicate "$x + y > z$". Then $R(2, 3, 4)$ denotes the statement "$2 + 3 > 4$".

First Order Logic allows for quantification over variables; $\forall$ and $\exists$ are the two quantifiers, called the universal quantifier and existential quantifier respectively. $\forall x P(x)$ reads as "for all x, it is the case that $P(x)$". $\exists x P(x)$ reads as "there exists an x such that $P(x)$". The quantification is over a set D called the domain of discourse. D is fixed at the start of the discourse. If D is the set of all natural numbers, then $P(x)$ could be interpreted as "$x > 3$". If D is the set of all human beings, then $P(x)$ could be interpreted as "x is at least 50 inches tall". $\forall x P(x)$ asserts that for every $x \in D$, $P(x)$. $\exists x P(x)$ asserts that for some $x \in D$, $P(x)$.

Sometimes we want to make statements on restrictions on D. For example, we may want to say "For every $x > 11$, $P(x)$". This can be expressed as "$\forall x(x > 11 \rightarrow P(x))$". Note that "$\forall x(x > 11 \wedge P(x))$" will not do, as that would mean "For every x, $x > 11$ and $P(x)$", which is not the same thing at all. Similarly, "There exists $x > 11$ such that $P(x)$" can be expressed as "$\exists x(x > 11 \wedge P(x))$". Note that "$\exists x(x > 11 \rightarrow P(x))$" will not do, as that paraphrases "There exists x such that either $x \leq 11$ or $P(x)$".

The quantifiers have higher precedence than logical connectives. For example, $\forall x P(x) \vee Q(x)$ stands for $(\forall x P(x)) \vee Q(x)$. That is, the scope of a quantifier, unless modified by parentheses extends only over the nearest predicate. Compare the above to $\forall x(P(x) \vee Q(x))$.

x is free in "$x > 3$", but is bound in "$\forall x(x > 3)$". x is both bound and free in "$x < 100 \wedge \forall x(x > 3)$"; the first occurance is free, while the second is bound to the quantification $\forall x$. This is analogous to the occurances of "he" in "*He* is attacking, and now it is everyone for *himself*."

Two formulae are logically equivalent iff they evaluate to the same truth values irrespective of the interpretations of the predicate symbols and free variables in them.

For example, $\neg\forall x P(x)$ and $\exists x \neg P(x)$ are equivalent formulae. Similarly, $\neg\exists x P(x)$ and $\forall x \neg P(x)$ are equivalent formulae. These are called De Morgan's laws for quantifiers.

Nested quantifiers: $\forall x \exists y(x + y = 0)$ and $\exists y \forall x(x + y = 0)$ do not mean the same. When D is the set of natural numbers, the former says that every number has an additive inverse, while the latter says that there is a number that is the additive inverse of all numbers. The former is true. The latter is false. The order of $\forall$ and $\exists$ is important. In a sequence of $\forall$s, the order is not important. Permuting them does not change the meaning of the formula. $\forall x \forall y(x + y = y + x)$ and $\forall y \forall x(x + y = y + x)$ both assert the commutativity of addition. Similarly, a sequence of $\exists$s can be permuted too, without changing the meaning.

A formula is logically valid iff it evaluates to true irrespective of the interpretations of the predicate symbols and free variables in it.

$\forall x(P(x) \rightarrow Q(x)) \rightarrow (\forall x P(x) \rightarrow \forall x Q(x))$ is a logically valid formula. This can be argued as follows. If the antecedent is false, the implication is true. So let us consider the case where the antecedent is true. Suppose, $\forall x P(x)$. Then for every $x \in D$, $P(x) \rightarrow Q(x)$ and $P(x)$ hold. Therefore, for every $x \in D$, $Q(x)$ must hold. In other words, $\forall x Q(x)$ holds. We conclude that the consequent is true, whenever the antecedent is true, and so the statement is always true.

$(\forall x P(x) \rightarrow \forall x Q(x)) \rightarrow \forall x(P(x) \rightarrow Q(x))$ is not logically valid. This can be shown by setting up a choice of D, P and Q that makes the statement false. If D is the set of all people, P stands for "x is peaceful", and Q stands are for "x is happy", then the statement reads "If all are peaceful, then all are happy. Therefore, anyone who is peaceful must be happy." Not everyone is peaceful. So the antecedent is trivially true. The consequent is false because even if an individual is peaceful, she might be surrounded by quarrelsome people, and consequently may be unhappy.

Lecture 4: 7 Aug 2014

If $\alpha(x)$ is a first order formula with a single free variable x, then let $\exists!x(\alpha(x))$ stand for $\exists x(\alpha(x)) \wedge \forall x \forall y(\alpha(x) \wedge \alpha(y) \rightarrow x = y)$. It reads "There exists a unique x such that $\alpha(x)$.

In the following, *equality* is a special predicate satisfying

(1) $\forall x(x = x)$

(2) $(x = y) \rightarrow (\alpha(x, x) \rightarrow \alpha(x, y))$

where x and y are variables, $\alpha(x, x)$ is any formula, and $\alpha(x, y)$ can be obtained from $\alpha(x, x)$ by substituting some free occurances of x by y, provided that in none of the substitutions y is captured by a quantifier.

Consider a first order logic with equality that has three predicate symbols P, L and O, where the first two are unary and the third is binary. (The predicate symbols P, L and O stand for "point", "line", and "lies on" respectively.)

For brevity, let us exclude brackets and write Px for $P(x)$, Lx for $L(x)$ and Oxz for $O(x, z)$.

Let Γ be the following set of formulae:

(P1) $\forall x \forall y[Px \wedge Py \wedge x \neq y \rightarrow \exists! z(Lz \wedge Oxz \wedge Oyz)]$

P1 asserts that there is a unique line passing through any pair of distinct points.

(P2) $\forall z[Lz \rightarrow \exists x \exists y(Px \wedge Py \wedge x \neq y \wedge Oxz \wedge Oyz)]$

P2 asserts that every line has at least two distinct points lying on it.

(P3) $\exists w \exists x \exists y(Pw \wedge Px \wedge Py \wedge w \neq x \wedge x \neq y \wedge y \neq w \wedge \forall z(Lz \rightarrow \neg(Owz \wedge Oxz \wedge Oyz)))$

P3 asserts that there are three distinct non-collinear points.

The above three formulae together with their logical consequences constitute Incidence Geometry.

Now consider the following assertion, called the Euclidean Parallel Property (EuP) "Given a line x, and a point y not on x, there exists a unique line z passing through y so that z and x do not intersect." Let α be the formula that represents EuP:

$\forall x \forall y[Lx \wedge Py \wedge \neg Oyx \rightarrow \exists! z(Lz \wedge \neg \exists w(Pw \wedge Owx \wedge Owz))]$

Let β and γ be the first order formulae that represent, respectively, the following: the Elliptic Parallel Property (ElP)— "Given a line x, and a point y not on x, there exists no line z passing through y so that z and x do not intersect", and the Hyperbolic Parallel Property (HyP)— "Given a line x, and a point y not on x, there exist more than one line z passing through y so that z and x do not intersect". Clearly, $\neg\alpha$ is logically equivalent to $\beta \vee \gamma$. (Exercise: What are β and γ?)

Now consider the following interpretations:

($\mathcal{I}_1$) The domain is the set consisting of and only of three individuals A, B, C, and all the three two-member subsets of $\{A, B, C\}$. P is mapped to the set $\{A, B, C\}$. L is mapped to the set of the three two-member subsets of $\{A, B, C\}$. O is mapped to $\{(x, y) | P(x) \wedge L(y) \wedge x \in y\}$. P1, P2 and P3 are all true in this interpretation. So, we say, this interpretation is a **model** of incidence geometry. Note that β is true in this interpretaion.

($\mathcal{I}_2$) The domain is the set consisting of and only of four individuals A, B, C, D and all the six two-member subsets of $\{A, B, C, D\}$. P is mapped to the set $\{A, B, C, D\}$. L is mapped to the set of the six two-member subsets of $\{A, B, C, D\}$. O is mapped to

$\{(x,y)|P(x) \wedge L(y) \wedge x \in y\}$. P1, P2 and P3 are all true in this interpretation. So, this interpretation also is a model of incidence geometry. Note that α is true in this interpretaion.

($\mathcal{I}_3$) The domain is the set consisting of and only of five individuals A, B, C, D, E and all the ten two-member subsets of $\{A,B,C,D,E\}$. P is mapped to the set $\{A,B,C,D,E\}$. L is mapped to the set of the ten two-member subsets of $\{A,B,C,D,E\}$. O is mapped to $\{(x,y)|P(x) \wedge L(y) \wedge x \in y\}$. P1, P2 and P3 are all true in this interpretation. So, this interpretation also is a model of incidence geometry. Note that γ is true in this interpretaion.

($\mathcal{I}_4$) The domain is the set of all points on the surface of a sphere S, together with all the great circles of S. (A great circle of a sphere S is any circle on S that has the same diameter as S.) P is mapped to the set of all points on S. L is mapped to the set of all the great circles of S. O is mapped to $\{(x,y)|P(x) \wedge L(y) \wedge y$ passes through $x\}$. P1 is not true in this interpretation because, any two diametrically opposite points on S have an infinite number of great circles passing through them. So, this interpretation is not a model of incidence geometry.

From the above, it is clear that neither α nor $(\neg\alpha)$ is a logical consequence of Γ. A formula α is a logical consequence of a set of formulae Γ ($\Gamma \vDash \alpha$), if every interpretation that makes every formula of Γ true also makes α true. It is also said that Γ logically imples α ($\Gamma \Rightarrow \alpha$).

Lecture 5: 8 Aug 2014

A system of logic (such as Propositional Calculus or First Order Predicate Calculus) consists of (i) syntax: the language of the logic, specified by a grammar (ii) semantics: possible meanings of the syntactic entities, specified by functions that map them to semantic entities (iii) a proof system: a rewriting mechanism for generating syntactic entities that satisfy certain semantic requirements.

The language of Propositional Calculus (Propcal for short) is generated by the following grammar G_0 over the alphabet $\{(,), \neg, \rightarrow, a_1, \ldots\}$.

$S : (\neg S)|(S \rightarrow S)|A$

$A : a_1|\ldots$

(The production "$S : (\neg S)|(S \rightarrow S)|A$" says that a formula, belonging to the syntactic class of S, can be produced by either negating another formula, or making up an implication from two other formulae, unless it is an atomic proposition. The production "$A : a_1|\ldots$" says that an atomic proposition is one among $a_1|\ldots$. We could have one or more atomic propositions, possibly even an infinite number.)

The strings in $L(G_0)$, the language of G_0, are the *well formed formulae* (wff for short) of Propcal. (We need not worry about the potentially infinite number of atomic formulae we use. If we agree to write, for example, a_8 as $a\_11111111$, we need only a finite alphabet.)

Consider functions of the form $\sigma : \{a_n | n > 0\} \rightarrow \{0, 1\}$; we call them *assignments*. The semantics of the wffs of Propcal under σ is defined inductively as follows:

$[\![a_n]\!]^\sigma = \sigma(a_n)$ for all $n > 0$

$[\![(\neg\alpha)]\!]^\sigma = 1 - [\![\alpha]\!]^\sigma$ for every wff α

$[\![(\alpha \rightarrow \beta)]\!]^\sigma = 1 - [\![\alpha]\!]^\sigma(1 - [\![\beta]\!]^\sigma)$ for every wffs α and β

- α *logically implies* β (denoted $\alpha \Rightarrow \beta$), if for every assignment σ, $[\![\beta]\!]^\sigma = 1$ whenever $[\![\alpha]\!]^\sigma = 1$.
- β is a *logical consequence* of α (denoted $\alpha \vDash \beta$), if $\alpha \Rightarrow \beta$.
- β is a *logical consequence* of a set of wffs Γ (denoted $\Gamma \vDash \beta$), if for every assignment σ, $[\![\beta]\!]^\sigma = 1$, whenever for all α in Γ, $[\![\alpha]\!]^\sigma = 1$.
- A wff α is a tautology (denoted $\vDash \alpha$), if for every assignment σ, $[\![\alpha]\!]^\sigma = 1$.

Theorem 1 *If* $\Gamma \vDash \alpha$ *and* $\Gamma \vDash (\alpha \rightarrow \beta)$ *then* $\Gamma \vDash \beta$.

Proof: Assume that $\Gamma \vDash \alpha$ and $\Gamma \vDash (\alpha \rightarrow \beta)$. Say, $\Gamma \nvDash \beta$. Then there exists an assignment σ that satisfies Γ, but such that $[\![\beta]\!]^\sigma = 0$. But $[\![\alpha]\!]^\sigma = 1$. So, $[\![(\alpha \rightarrow \beta)]\!]^\sigma = 0$, a contradiction. ■

Corollary 1 *If* $\vDash \alpha$ *and* $\vDash (\alpha \rightarrow \beta)$ *then* $\vDash \beta$.

We want algorithms for recognising tautologies, and logical consequences of given sets of wffs. A proof system is an answer. The truth table method is an answer as well, unless we are seeking the logical consequences of an infinite set of wffs.

A proof system $\mathcal{P}$ consists of a set of axioms (which are nothing but a set of chosen wffs), and a finite set of rules of inference (which are relations over wffs). A proof in $\mathcal{P}$ is a sequence $\beta_1, \ldots, \beta_n$ of wffs such that each β_i is either an axiom, or follows from some of the earlier wffs in the sequence by some rule of inference. A wff is a theorem of $\mathcal{P}$, if there is a proof culminating in it.

Now let us consider a proof system $\mathcal{P}_0$ for Propcal. (There are many proof systems for Propcal. $\mathcal{P}_0$ is only one of them.)

If α, β, γ are any three wffs, the following wffs are axioms:

(A1) $(\alpha \to (\beta \to \alpha))$

(A2) $(\alpha \to (\beta \to \gamma)) \to ((\alpha \to \beta) \to (\alpha \to \gamma))$

(A3) $(\neg\alpha \to \neg\beta) \to ((\neg\alpha \to \beta) \to \alpha)$

A1, A2 and A3 are called axiom schemas, because they provide templates for forming axioms.

Any axiom that is an instance of the above schemas will be called a logical axiom. Note that we have an infinite number of logical axioms. Let us use the symbol Γ_0 to denote the set of logical axioms.

In addition to the logical axioms, we can also have a set of *proper axioms*. (Note that all logical axioms are tautologies. But the proper axioms need not be tautologies. As we shall see, all tautologies can be proved from Γ_0 alone; so there is no need to adopt a tautology as a proper axiom.)

$\mathcal{P}_0$ has only one rule of inference, a relation called *modus ponens* (MP):

$\{\langle \alpha, (\alpha \to \beta), \beta \rangle | \alpha \text{ and } \beta \text{ are wffs } \}$

MP suggests that, if α and $(\alpha \to \beta)$ have already been proved then it is fine to deduce β.

We write $\Gamma \vdash \alpha$, when Γ is the set of proper axioms of $\mathcal{P}_0$, and α is a theorem of $\mathcal{P}_0$. In particular, when $\Gamma = \phi$, we write $\vdash \alpha$.

Here is a proof in $\mathcal{P}_0$:

Proof 1: $\vdash \alpha \to \alpha$

$\vdash (\alpha \to ((\alpha \to \alpha) \to \alpha)) \to ((\alpha \to (\alpha \to \alpha)) \to (\alpha \to \alpha))$	by (A2)	(1)
$\vdash \alpha \to ((\alpha \to \alpha) \to \alpha)$	by (A1)	(2)
$\vdash (\alpha \to (\alpha \to \alpha)) \to (\alpha \to \alpha)$	by MP 1,2	(3)
$\vdash \alpha \to (\alpha \to \alpha)$	by (A1)	(4)
$\vdash \alpha \to \alpha$	by MP 3,4	(5)

Lecture 6: 14 Aug 2014

Theorem 2 *(Soundness of Propcal) If* $\Gamma \vdash \alpha$*, then* $\Gamma \vDash \alpha$.

Proof: If $\Gamma \vdash \alpha$, then there exists a proof $\beta_1, \ldots, \beta_n = \alpha$ in $\mathcal{P}_0$.

Clearly, β_1 is an axiom. So, any assignment that satisfies Γ satisfies β_1 also. Hence, $\Gamma \vDash \beta_1$. This is the basis.

Assume that $\Gamma \vDash \beta_j$, for all $j < i$. Consider β_i; it is either an axiom (in which case $\Gamma \vDash \beta_i$ as in the basis), or it follows from β_j and $\beta_k = (\beta_j \to \beta_i)$ by MP, for some $j, k < i$ (in which case, by induction hypothesis, $\Gamma \vDash \beta_j$ and $\Gamma \vDash \beta_k = (\beta_j \to \beta_i)$, and so by Theorem 1, $\Gamma \vDash \beta_i$). So by induction, for all i, $\Gamma \vDash \beta_i$. In particualar, $\Gamma \vDash \beta_n = \alpha$. □

Corollary 2 *If* $\vdash \alpha$*, then* $\vDash \alpha$.

Theorem 3 *(Deduction Theorem) If* $\Gamma, \alpha \vdash \beta$*, then* $\Gamma \vdash (\alpha \to \beta)$.

Proof: If $\Gamma, \alpha \vdash \beta$, then there exists a proof $\beta_1, \ldots, \beta_n = \beta$ in $\mathcal{P}_0$. We prove that $\Gamma \vdash (\alpha \to \beta_i)$, for all i.

Basis: (1) β_1 is a logical axiom: Trivially, $\vdash \beta_1$. Also, by (A1), $\vdash \beta_1 \to (\alpha \to \beta_1)$. Hence by MP, $\vdash (\alpha \to \beta_1)$. Thus, $\Gamma \vdash (\alpha \to \beta_1)$.

(2) β_1 is from Γ: Trivially, $\Gamma \vdash \beta_1$. Also, by (A1), $\Gamma \vdash \beta_1 \to (\alpha \to \beta_1)$. Thus, by MP, $\Gamma \vdash (\alpha \to \beta_1)$.

(3) $\beta_1 = \alpha : \vdash (\alpha \to \alpha)$ (Proof 1). Hence, $\Gamma \vdash (\alpha \to \alpha)$.

Induction Step: (i) β_i is a logical axiom/is the same as α/from Γ: As above

(ii) β_i follows from β_j and $\beta_k = (\beta_j \to \beta_i)$ by MP, for some $j, k < i$: By inductive hypothesis, $\Gamma \vdash (\alpha \to \beta_j)$ and $\Gamma \vdash (\alpha \to (\beta_j \to \beta_i))$. Also, by (A2), $\vdash (\alpha \to (\beta_j \to \beta_i)) \to ((\alpha \to \beta_j) \to (\alpha \to \beta_i))$. Now, two applications of MP give $\Gamma \vdash (\alpha \to \beta_i)$. ■

Here are some proofs in $\mathcal{P}_0$.

Proof 2: $\alpha \to \beta, \beta \to \gamma \vdash \alpha \to \gamma$

$\alpha \to \beta, \beta \to \gamma, \alpha \vdash \alpha$	Proper Axiom	(6)
$\vdash \alpha \to \beta$	Proper Axiom	(7)
$\vdash \beta$	MP 6,7	(8)
$\vdash \beta \to \gamma$	Proper Axiom	(9)
$\vdash \gamma$	MP 8,9	(10)
$\alpha \to \beta, \beta \to \gamma \vdash \alpha \to \gamma$	by DT	(11)

Proof 3: $\alpha \to (\beta \to \gamma), \beta \vdash \alpha \to \gamma$

$\alpha \to (\beta \to \gamma), \beta, \alpha \vdash \alpha$	Proper Axiom	(12)
$\vdash \alpha \to (\beta \to \gamma)$	Proper Axiom	(13)
$\vdash \beta \to \gamma$	MP 12,13	(14)
$\vdash \beta$	Proper Axiom	(15)
$\vdash \gamma$	MP 14,15	(16)
$\alpha \to (\beta \to \gamma), \beta \vdash \alpha \to \gamma$	by DT	(17)

Proof 4: $\vdash \neg\neg\beta \to \beta$

$\vdash (\neg\beta \to \neg\neg\beta) \to ((\neg\beta \to \neg\beta) \to \beta)$	A3	(18)
$\vdash (\neg\beta \to \neg\beta)$	Proof 1	(19)
$\vdash (\neg\beta \to \neg\neg\beta) \to \beta$	18, 19, Proof 3	(20)
$\vdash \neg\neg\beta \to (\neg\beta \to \neg\neg\beta)$	A1	(21)
$\vdash \neg\neg\beta \to \beta$	20, 21, Proof 2	(22)

Proof 5: $\vdash \beta \to \neg\neg\beta$

$\vdash (\neg\neg\neg\beta \to \neg\beta) \to ((\neg\neg\neg\beta \to \beta) \to \neg\neg\beta)$	A3	(23)
$\vdash \neg\neg\neg\beta \to \neg\beta$	Proof 4	(24)
$\vdash (\neg\neg\neg\beta \to \beta) \to \neg\neg\beta$	MP 23, 24	(25)
$\vdash \beta \to (\neg\neg\neg\beta \to \beta)$	A1	(26)
$\vdash \beta \to \neg\neg\beta$	25, 26, Proof 2	(27)

Proof 6: $\vdash \neg\beta \to (\beta \to \gamma)$

$\neg\beta, \beta \vdash \beta \to (\neg\gamma \to \beta)$	A1	(28)
$\vdash \neg\beta \to (\neg\gamma \to \neg\beta)$	A1	(29)
$\vdash \beta$	Proper Axiom	(30)
$\vdash \neg\beta$	Proper Axiom	(31)
$\vdash \neg\gamma \to \beta$	MP 28,30	(32)
$\vdash \neg\gamma \to \neg\beta$	MP 29, 31	(33)
$\vdash (\neg\gamma \to \neg\beta) \to ((\neg\gamma \to \beta) \to \gamma)$	A3	(34)
$\vdash \gamma$	MPs 32, 33, 34	(35)

That is, starting with β and $\neg\beta$ as proper axioms, we can prove anything. Substitute γ in the above with $\neg\gamma$, and we have a proof of $\neg\gamma$ as well. In particular,

$\vdash \neg\beta \to (\beta \to \gamma)$	By DT	(36)

Proof 7: $\neg\beta \to \neg\alpha \vdash \alpha \to \beta$

$\neg\beta \to \neg\alpha, \alpha \vdash (\neg\beta \to \neg\alpha) \to ((\neg\beta \to \alpha) \to \beta)$	A3	(37)
$\vdash \alpha \to (\neg\beta \to \alpha)$	A1	(38)
$\vdash \alpha$	Proper Axiom	(39)
$\vdash \neg\beta \to \neg\alpha$	Proper Axiom	(40)
$\vdash \neg\beta \to \alpha$	MP 38, 39	(41)
$\vdash \beta$	MPs 37, 40, 41	(42)
$\neg\beta \to \neg\alpha \vdash \alpha \to \beta$	by DT	(43)

Lecture 7: 21 Aug 2014

Proof 8: $\vdash (\alpha \to \beta) \to (\neg\beta \to \neg\alpha)$

$\alpha \to \beta \vdash \neg\neg\alpha \to \alpha$	Proof 4	(44)
$\vdash \alpha \to \beta$	Proper Axiom	(45)
$\vdash \neg\neg\alpha \to \beta$	44, 45, Proof 2	(46)
$\vdash \beta \to \neg\neg\beta$	Proof 5	(47)
$\vdash \neg\neg\alpha \to \neg\neg\beta$	46, 47, Proof 2	(48)
$\vdash (\neg\neg\alpha \to \neg\neg\beta) \to (\neg\beta \to \neg\alpha)$	Proof 7	(49)
$\vdash \neg\beta \to \neg\alpha$	MP, 48, 49	(50)
$\varnothing \vdash (\alpha \to \beta) \to (\neg\beta \to \neg\alpha)$	by DT	(51)

Proof 9: $\vdash \alpha \to (\neg\beta \to \neg(\alpha \to \beta))$

$\alpha, \alpha \to \beta \vdash \alpha$	Proper Axiom	(52)
$\vdash \alpha \to \beta$	Proper Axiom	(53)
$\vdash \beta$	MP, 52, 53	(54)
$\varnothing \vdash \alpha \to ((\alpha \to \beta) \to \beta)$	by DT	(55)
$\vdash ((\alpha \to \beta) \to \beta) \to (\neg\beta \to \neg(\alpha \to \beta))$	Proof 8	(56)
$\vdash \alpha \to (\neg\beta \to \neg(\alpha \to \beta))$	Proof 2	(57)

Theorem 4 *For every wff α, the atomic propositions of which are say $a_{i_1}, \ldots, a_{i_k}$, and every assignment σ, if we define*

$\alpha_{i_j}^{\sigma}$ as a_{i_j} or $\neg a_{i_j}$ depending respectively on whether $\sigma(a_{i_j}) = 1$ or 0, for $1 \le j \le k$, and

α^{σ} as α or $\neg\alpha$ depending respectively on whether $[\![\alpha]\!]^{\sigma} = 1$ or 0,

then it is the case that $\alpha_{i_1}^{\sigma}, \ldots, \alpha_{i_k}^{\sigma} \vdash \alpha^{\sigma}$.

Proof: Induction on the number of operators in α.

Basis: Zero operators. Then α must be just an atomic proposition, a_{i_1}. So, it is enough to show that $a_{i_1} \vdash a_{i_1}$ and $\neg a_{i_1} \vdash \neg a_{i_1}$. But this is easy because for any wff β, $\beta \vdash \beta$.

Induction step: (a) Say $\alpha = \neg\beta$. Then by hypothesis, $\alpha_{i_1}^{\sigma}, \ldots, \alpha_{i_k}^{\sigma} \vdash \beta^{\sigma}$. If $[\![\alpha]\!]^{\sigma} = 1$, then $[\![\beta]\!]^{\sigma} = 0$; $\alpha^{\sigma} = \alpha = \neg\beta = \beta^{\sigma}$, and we are done. If $[\![\alpha]\!]^{\sigma} = 0$, then $[\![\beta]\!]^{\sigma} = 1$; $\alpha^{\sigma} = \neg\alpha = \neg\neg\beta$; but, $\vdash \beta \to \neg\neg\beta$ (Proof 5), and that does it because $\beta^{\sigma} = \beta$.

(b) Say $\alpha = (\beta \to \gamma)$. Then by hypothesis, $\alpha_{i_1}^{\sigma}, \ldots, \alpha_{i_k}^{\sigma} \vdash \beta^{\sigma}$, and $\alpha_{i_1}^{\sigma}, \ldots, \alpha_{i_k}^{\sigma} \vdash \gamma^{\sigma}$. If $[\![\beta]\!]^{\sigma} = 0$, or $[\![\gamma]\!]^{\sigma} = 1$, then $\alpha^{\sigma} = \alpha$; but, $\vdash (\neg\beta \to (\beta \to \gamma))$ (Proof 6), and $\vdash (\gamma \to (\beta \to \gamma))$, (Axiom 1); QED. If $[\![\beta]\!]^{\sigma} = 1$, or $[\![\gamma]\!]^{\sigma} = 0$, then $\alpha^{\sigma} = \neg\alpha$; but, $\vdash (\beta \to (\neg\gamma \to \neg(\beta \to \gamma)))$, (Proof 9); QED. ■.

Theorem 5 *If α is a tautology, then $\vdash \alpha$.*

Proof: Let $a_{i_1}, \ldots, a_{i_k}$ be the atomic propositions of α. Consider 2^k assignments so that any two of them differ in atleast one of the a_i's. Consider two assignments σ_1 and σ_2 so that they agree on all of a_i's except a_{i_k}; say $\sigma_1(a_{i_k}) = 1$, and $\sigma_2(a_{i_k}) = 0$. Then by Theorem 4, $\alpha_{i_1}^{\sigma_1}, \ldots, \alpha_{i_{k-1}}^{\sigma_1}, \alpha_{i_k}^{\sigma_1} \vdash \alpha^{\sigma_1} = \alpha$ and $\alpha_{i_1}^{\sigma_1}, \ldots, \alpha_{i_{k-1}}^{\sigma_1}, \neg\alpha_{i_k}^{\sigma_1} \vdash \alpha^{\sigma_2} = \alpha$. Hence by Deduction Theorem, $\alpha_{i_1}^{\sigma_1}, \ldots, \alpha_{i_{k-1}}^{\sigma_1} \vdash \alpha_{i_k}^{\sigma_1} \to \alpha$, and $\alpha_{i_1}^{\sigma_1}, \ldots, \alpha_{i_{k-1}}^{\sigma_1} \vdash \neg\alpha_{i_k}^{\sigma_1} \to \alpha$. So by (A3) and Proof 8, $\alpha_{i_1}^{\sigma_1}, \ldots, \alpha_{i_{k-1}}^{\sigma_1} \vdash \alpha$. Now we have gotten rid of a_{i_k}.

Next, consider 2^{k-1} assignments so that any two of them differ in atleast one of the first $(k-1)$ a_i's. Pair the assignments and repeat the process; we can get rid of $a_{i_{k-1}}$.

Repeating this k times we can get rid of all a_i's. We will be left with $\vdash \alpha$. ■

Lecture 8: 22 Aug 2014

Theorem 6 *If Γ is a finite set of wffs, then $\Gamma \vDash \alpha$ implies $\Gamma \vdash \alpha$.*

Proof: Say, $\Gamma = \{\beta_1, \ldots, \beta_n\}$. If $\{\beta_1, \ldots, \beta_n\} \vDash \alpha$, then $\vDash (\beta_1 \to (\cdots(\beta_n \to \alpha)\cdots))$. So by Theorem 5, $\vdash (\beta_1 \to (\cdots(\beta_n \to \alpha)\cdots))$. Hence, $\{\beta_1, \ldots, \beta_n\} \vdash (\beta_1 \to (\cdots(\beta_n \to \alpha)\cdots))$. Apply MP n times, and we have $\{\beta_1, \ldots, \beta_n\} \vdash \alpha$. □

Definition 1 *A set Γ of wffs is said to be consistent, if for no wff α it is the case that both $\vdash \alpha$ and $\vdash \neg\alpha$.*

In other words, Γ inconsistent, if for some wff α, $\vdash \alpha$ and $\vdash \neg\alpha$. By Proof 6, anything can be proved from an inconsistent set.

Theorem 7 *If Γ is a consistent set of wffs, then there exists a set of wffs Σ such that*
(a) $\Gamma \subseteq \Sigma$,
(b) Σ is consistent,
(c) For any wff α, either $\alpha \in \Sigma$ XOR $\neg\alpha \in \Sigma$.

Proof: The set of all strings from the alphabet $\{(,), \to, \neg, a, \_, 1\}$ can be enumerated in lexicographic order. For example, the lexicographic ordering of the strings from $\{a, b\}$ is

$\epsilon, a, b, aa, ab, ba, bb, aaa, aab, aba, abb, baa, bab, bba, bbb, aaaa, \ldots,$

where ϵ is the string of length zero. Each string of this alphabet can be easily checked to see if it is a wff. (Exercise: Devise an algorithm using a stack.) Juxtaposing these two algorithms allows us to enumerate the wffs in Propcal.

Let α_i be the i-th in the enumeration. Let $\Sigma_0 = \Gamma$. For $i \geq 1$ define Σ_i as follows:
$\Sigma_i = \Sigma_{i-1} \cup \{\alpha_i\}$ if this set is consistent
$= \Sigma_{i-1} \cup \{\neg\alpha_i\}$ otherwise.

I claim that Σ_i is consistent. Let me prove this using induction. Σ_0 is consistent, because it is the same as Γ. Hypothesis: Σ_{i-1} is consistent. But assume that neither $\Sigma_{i-1} \cup \{\alpha_i\}$ nor $\Sigma_{i-1} \cup \{\neg\alpha_i\}$ is consistent. Then $\Sigma_{i-1} \cup \{\alpha_i\} \vdash \beta \vdash \neg\beta$ for some β. But these proofs use only a finite subset of $\Sigma_{i-1} \cup \{\alpha_i\}$. Hence $\Sigma_{i-1} \cup \{\alpha_i\}$ has a finite inconsistent subset. This subset must contain α_i. (Why?) Let this subset be $\{\gamma_1, \ldots, \gamma_n, \alpha_i\}$. Similarly, $\Sigma_{i-1} \cup \{\neg\alpha_i\}$ has a finite inconsistent subset; say, $\{\delta_1, \ldots, \delta_m, \neg\alpha_i\}$. So, $\{\gamma_1, \ldots, \gamma_n\} \vdash (\alpha_i \to \beta) \vdash (\alpha_i \to \neg\beta) \vdash \neg\alpha_i$. (**Exercise**). Similarly, $\{\delta_1, \ldots, \delta_m\} \vdash (\neg\alpha_i \to \beta) \vdash (\neg\alpha_i \to \neg\beta) \vdash \alpha_i$. (**Exercise**). Hence, $\{\gamma_1, \ldots, \gamma_n, \delta_1, \ldots, \delta_m\} \vdash \alpha_i \vdash \neg\alpha_i$. Thus, Σ_{i-1} has an inconsistent subset. Contardiction. So one of $\Sigma_{i-1} \cup \{\alpha_i\}$ or $\Sigma_{i-1} \cup \{\neg\alpha_i\}$ must be consistent. So Σ_i is consistent.

Now define $\sigma = \bigcup_{n>0} \Sigma_n$. Σ is consistent, because otherwise $\Sigma \vdash \beta \vdash \neg\beta$, for some β; but a proof can use only a finite number of wffs; so for some finite $\Sigma' \subset \Sigma$, $\Sigma' \vdash \beta \vdash \neg\beta$; this Σ' must be contained in some Σ_n; that Σ_n would then be inconsistent; contradiction.

Clearly, $\Sigma_0 = \Gamma \subset \Sigma$.

Since Σ_i is consistent, for any wff α, both α and $\neg\alpha$ cannot be in Σ. For any wff α, there exists an n so that $\alpha = \alpha_n$. So, either $\alpha \in \Sigma_n$ or $\neg\alpha \in \Sigma_n$. Thus, either $\alpha \in \Sigma$ XOR $\neg\alpha \in \Sigma$. □

Definition 2 *A set Γ of wffs is said to be satisfiable, if there exists an an assignment that saisfies each wff of Γ.*

Lecture 9: 28 Aug 2014

Theorem 8 *If a set of wffs* Γ *is consistent, then it is satisfiable.*

Proof: If Γ is consistent, then by Theorem 7, there is a *maximal consistent superset* Σ of Γ. Define an assignment σ as follows:

$\sigma(a_i) = 1$ if $a_i \in \Sigma$

$= 0$ otherwise.

Consider a wff $\alpha \in \Sigma$. If $a_{i_1}, \ldots, a_{i_k}$ are the atomic propositions in α, then by Theorem 4, $\alpha^\sigma_{i_1}, \ldots, \alpha^\sigma_{i_k} \vdash \alpha^\sigma$. By the definition of α^σ_i's, all of them must be in Σ. If $[\![\alpha]\!]^\sigma = 0$, then $\alpha^\sigma = \neg\alpha$. Then $\alpha^\sigma_{i_1}, \ldots, \alpha^\sigma_{i_k} \vdash \neg\alpha$. Hence $\alpha^\sigma_{i_1}, \ldots, \alpha^\sigma_{i_k}, \alpha \vdash \neg\alpha \vdash \alpha$. That is, Σ has an inconsistent finite subset. Contradiction. □

Theorem 9 *The following statements are equivalent*

(a) If a set of wffs Γ *is consistent, then it is satisfiable.*

(b) For a set Γ *of wffs and a wff* α*, if* $\Gamma \vDash \alpha$*, then* $\Gamma \vdash \alpha$*.*

Proof: $\Rightarrow$: Say, $\Gamma \vDash \alpha$. Any assignment that satisfies Γ satisifies α too, and hence does not satisfy $\neg\alpha$. So, $\Gamma \cup \{\neg\alpha\}$ is unsatisfiable, and hence is inconsistent. That is, $\Gamma \cup \{\neg\alpha\} \vdash \beta \vdash \neg\beta$ for some β. So, $\Gamma \vdash (\neg\alpha \rightarrow \beta) \vdash (\neg\alpha \rightarrow \neg\beta) \vdash \alpha$. (**Exercise**).

$\Leftarrow$: Say, Γ is unsatisfiable. Then it is trivially true that $\Gamma \vDash \alpha$, for any α. Hence $\Gamma \vdash \alpha$. Similarly, $\Gamma \vdash \neg\alpha$. Γ is inconsistent. □

Corollary 3 *(Completeness of Propcal) For a set* Γ *of wffs and a wff* α*, if* $\Gamma \vDash \alpha$*, then* $\Gamma \vdash \alpha$*.*

First Order Logic

The alphabet of a first order logic is made up of the following: logical connectives ($\rightarrow$, $\neg$), quantifier ($\forall$), variables (x_i, for $i \geq 0$), function symbols (f^n_i, for $n \geq 0$ and $i \geq 0$, where f^n_i is the i-th n-ary function symbol), predicate symbols (P^n_i, for $n > 0$ and $i \geq 0$, where f^n_i is the i-th n-ary predicate symbol); 0-ary function symbols are also called individual constants; let us use a_i as alternate represenation for f^0_i.

Now we define the following syntactic entities:

Term For each $i \geq 0$, there is a term that consists of just a_i. For each $i \geq 0$, there is a term that consists of just x_i. For each $n > 0$ and $i \geq 0$, $f^n_i(\text{term}_1, \ldots, \text{term}_n)$ is a term, where $\text{term}_1, \ldots, \text{term}_n$ are terms.

Atomic Formula For each $n > 0$ and $i \geq 0$, $P^n_i(\text{term}_1, \ldots, \text{term}_n)$ is an atomic formula, where $\text{term}_1, \ldots, \text{term}_n$ are terms.

Well Formed Formula An atomic formula is a wff. If α and β are wffs, and x_i is a variable, then $(\neg\alpha)$, $(\alpha \rightarrow \beta)$, and $\forall x_i(\alpha)$ are also wffs.

Definition 3 *A term* t *is free for* x_i *in a wff* α*, if no variable in* t *will be "captured" by a quantifier in* α *when* t *is substituted for every occurance of* x_i *in* α*.*

The sematics of a first order logic is specified by an interpretation (also called a structure) $\mathcal{I} = \langle \mathcal{D}, \mathcal{F}, \mathcal{R} \rangle$, where $\mathcal{D}$ is a set of inviduals called the domain of discourse, $\mathcal{F}$ is a mapping from function symbols to functions over the domain of discourse such that each n-ary function symbol f_i^n is mapped to an n-ary function $\mathcal{I}(f_i^n)$, and $\mathcal{R}$ is a mapping from predicate symbols to relations over the domain of discourse such that each n-ary predicate symbol P_i^n is mapped to an n-ary relation $\mathcal{I}(P_i^n)$.

An interpretation itself is not sufficient to specify the meaning of all syntactic entities, because the meaning of the variables are as yet unspecified. This we do through a context, which is a function from the set of variables to $\mathcal{D}$.

The semantics of the terms under an interpretation-context pair (I, c) is defined inductively as follows:

$s^{\mathcal{I},c}(x_i) = c(x_i)$

$s^{\mathcal{I},c}(a_i) = \mathcal{I}(a_i)$

For each $n > 0$ and $i \geq 0$, $s^{\mathcal{I},c}(f_i^n(\text{term}_1, \ldots, \text{term}_n)) = \mathcal{I}(f_i^n)(s^{\mathcal{I},c}(\text{term}_1), \ldots, s^{\mathcal{I},c}(\text{term}_n))$

Lecture 10: 29 Aug 2014

The semantics of the wffs under an interpretation-context pair $(\mathcal{I}, c)$ is defined inductively as follows:
For each $n > 0$ and $i \geq 0$, $[\![P_i^n(\text{term}_1, \ldots, \text{term}_n)]\!]^{\mathcal{I},c} = 1$ iff $(s^{\mathcal{I},c}(\text{term}_1), \ldots, s^{\mathcal{I},c}(\text{term}_n))$ is a member of $\mathcal{I}(P_i^n)$.
$[\![(\neg\alpha)]\!]^{\mathcal{I},c} = 1 - [\![\alpha]\!]^{\mathcal{I},c}$ for every wff α
$[\![(\alpha \to \beta)]\!]^{\mathcal{I},c} = 1 - [\![\alpha]\!]^{\mathcal{I},c}(1 - [\![\beta]\!]^{\mathcal{I},c})$ for every wffs α and β
$[\![\forall x_i(\alpha)]\!]^{\mathcal{I},c} = 1$ iff for every context c' such that $c'(x_j) \neq c(x_j)$ implies $j = i$, $[\![\alpha]\!]^{\mathcal{I},c'} = 1$.

$(\mathcal{I}, c')$ such that $c'(x_j) \neq c(x_j)$ implies $j = i$ is called a one-change-world of $(\mathcal{I}, c)$, because they differ atmost on x_i.

Definition 4 *A wff α is* true *in an interpretation $\mathcal{I}$ if for every context c, $[\![\alpha]\!]^{\mathcal{I},c} = 1$. Similarly, a wff α is* false *in an interpretation $\mathcal{I}$ if for every context c, $[\![\alpha]\!]^{\mathcal{I},c} = 0$.*

Definition 5 *A wff α is said to be satisfiable, if there exists an interpretation-context pair $(\mathcal{I}, c)$ such that $[\![\alpha]\!]^{\mathcal{I},c} = 1$. A set Γ of wffs is said to be satisfiable, if there exists an interpretation-context pair $(\mathcal{I}, c)$ that saisfies each wff of Γ.*

Note that it is not necessary for a wff to be either false or true in an interpretation. Some contexts may satisfy it, and some may not.

Definition 6
1. α logically implies β *(denoted $\alpha \Rightarrow \beta$), if for every interpretation-context pair $(\mathcal{I}, c)$, $[\![\beta]\!]^{\mathcal{I},c} = 1$ whenever $[\![\alpha]\!]^{\mathcal{I},c}$=1.*
2. *β is a* logical consequence *of α (denoted $\alpha \vDash \beta$), if $\alpha \Rightarrow \beta$.*
3. *β is a* logical consequence *of a set of wffs Γ (denoted $\Gamma \vDash \beta$), if for every interpretation-context pair $(\mathcal{I}, c)$, $[\![\beta]\!]^{\mathcal{I},c} = 1$, whenever for all α in Γ $[\![\alpha]\!]^{\mathcal{I},c}$=1.*

Definition 7 *A wff α is logically vaid (denoted $\vDash \alpha$), if for every interpretation-context pair $(\mathcal{I}, c)$, $[\![\alpha]\!]^{\mathcal{I},c} = 1$.*

Theorem 10 *If $\Gamma \vDash \alpha$ and $\Gamma \vDash (\alpha \to \beta)$ then $\Gamma \vDash \beta$.*

Proof: DIY. □

Corollary 4 *If $\vDash \alpha$ and $\vDash (\alpha \to \beta)$ then $\vDash \beta$.*

As in the case of Propcal, we want algorithms for recognising logically valid wffs and logical consequences of given sets of wffs. But in the case of FOL, we do not have any effective procedure like the truth table method. So we have to resort to developing a proof system.

Let us consider a proof system $\mathcal{P}_1$ for first order logic.

If α, β, γ are any three wffs, the following wffs and all generalisations of them are axioms: (If α is a formula and x_i is a variable $\forall x_i(\alpha)$ is a generalisation of α.

(A1) $(\alpha \rightarrow (\beta \rightarrow \alpha))$
(A2) $(\alpha \rightarrow (\beta \rightarrow \gamma)) \rightarrow ((\alpha \rightarrow \beta) \rightarrow (\alpha \rightarrow \gamma))$
(A3) $(\neg\alpha \rightarrow \neg\beta) \rightarrow ((\neg\alpha \rightarrow \beta) \rightarrow \alpha)$
(A4) $\forall x_i(\alpha(x_i)) \rightarrow \alpha(t)$, where t is a term that is free for x_i in $\alpha(x_i)$
(A5) $\forall x_i(\alpha \rightarrow \beta) \rightarrow (\forall x_i(\alpha) \rightarrow \forall x_i(\beta))$
(A6) $\alpha \rightarrow \forall x_i(\alpha)$, where x_i is not free in α

Any wff that is an instance of the above schemas or is a generalization of one will be called a logical axiom. In addition to the logical axioms, we can also have a set of *proper axioms*.

Lecture 11: 4 Sep 2014

Rule of inference

$\mathcal{P}_1$ has only one rule of inference, a relation called *modus ponens* (MP):

$\{\langle \alpha, (\alpha \to \beta), \beta \rangle | \alpha$ and β are wffs $\}$

Notation 1 *We write $\Gamma \vdash \alpha$, when Γ is the set of proper axioms of $\mathcal{P}_1$, and α is a theorem of $\mathcal{P}_1$. In particular, when $\Gamma = \phi$, we write $\vdash \alpha$.*

Theorem 11 *(Generalisation theorem) If $\Gamma \vdash \alpha$, and x_i does not occur free in any wff in Γ, then $\Gamma \vdash \forall x_i(\alpha)$.*

Proof: Use induction on the length of the proof of α from Γ.

(1) If α is a logical axiom, then $\forall x_i(\alpha)$ is also a logical axiom. So, $\vdash \forall x_i(\alpha)$, and in particular, $\Gamma \vdash \forall x_i(\alpha)$.

(2) If $\alpha \in \Gamma$, then x_i does not occur free in α, and hence by axiom schema (A6), $\alpha \to \forall x_i(\alpha)$ is a logical axiom. So, $\Gamma \vdash \alpha \to \forall x_i(\alpha) \vdash \alpha \vdash \forall x_i(\alpha)$.

(3) Say, α is obtained by MP from β and $\beta \to \alpha$. By induction hypothesis, $\Gamma \vdash \forall x_i(\beta)$ and $\Gamma \vdash \forall x_i(\beta \to \alpha)$. So, by axiom schema (A5), $\Gamma \vdash \forall x_i(\beta) \to \forall x_i(\alpha)$. Hence, $\Gamma \vdash \forall x_i(\alpha)$. □

The next two theorems are easy to prove.

Theorem 12 *(Soundness of First Order Logic) If $\Gamma \vdash \alpha$, then $\Gamma \vDash \alpha$.*

Theorem 13 *(Deduction Theorem for First Order Logic) If $\Gamma, \alpha \vdash \beta$, then $\Gamma \vdash (\alpha \to \beta)$.*

Definition 8 *A set Γ of wffs in First Order Logic is said to be consistent, if for no wff α it is the case that both $\vdash \alpha$ and $\vdash \neg\alpha$.*

As in the case of Propcal, albeit using longer proofs, it can be shown that:

Theorem 14 *If Γ is a consistent set of wffs in First Order Logic, then there exists a set of wffs Σ such that*

(a) $\Gamma \subseteq \Sigma$,

(b) Σ is consistent,

(c) For any wff α, either $\alpha \in \Sigma$ XOR $\neg\alpha \in \Sigma$.

Theorem 15 *If a set of First Order Logic wffs Γ is consistent, then it is satisfiable.*

Theorem 16 *The following statements are equivalent*

(a) If a set of First Order Logic wffs Γ is consistent, then it is satisfiable.

(b) For a set Γ of First Order Logic wffs and a First Order Logic wff α, if $\Gamma \vDash \alpha$, then $\Gamma \vdash \alpha$.

Corollary 5 *(Completeness of First Order Logic; Gödel's Completeness Theorem) For a set Γ of wffs and a wff α, if $\Gamma \vDash \alpha$, then $\Gamma \vdash \alpha$.*

Lecture 12: 11 Sep 2014

Consider a first order theory S with one binary predicate symbol (=), one individual constant (0), three function symbols ($'$,+,$*$), and the following proper axioms (called Peano's axioms, though they were first formulated by Dedekind):

(S1) $\forall x_1 \forall x_2 \forall x_3 (x_1 = x_2 \rightarrow (x_1 = x_3 \rightarrow x_2 = x_3))$
(S2) $\forall x_1 \forall x_2 (x_1 = x_2 \rightarrow x_1' = x_2')$
(S3) $\forall x_1 (0 \neq x_1')$
(S4) $\forall x_1 \forall x_2 (x_1' = x_2' \rightarrow x_1 = x_2)$
(S5) $\forall x_1 (x_1 + 0 = x_1)$
(S6) $\forall x_1 \forall x_2 (x_1 + x_2' = (x_1 + x_2)')$
(S7) $\forall x_1 (x_1 * 0 = 0)$
(S8) $\forall x_1 \forall x_2 (x_1 * (x_2') = (x_1 * x_2) + x_1)$
(S9) for any wff $\alpha(x)$ of S, $\alpha(0) \rightarrow [\forall x(\alpha(x) \rightarrow \alpha(x')) \rightarrow \forall x \alpha(x)]$

(S9) is an axiom-schema, from which we can spawn a countably infinite numebr of axioms. (S1) and (S2) are necessary to make S a first order theory with equality; it can be shown that they are sufficient also.

The standard model

(An interpretation in which all the proper axioms of a theory are true is said to be a model of the theory. If Γ is the set of proper axioms, and $\Gamma \vDash \alpha$, then α is true in every model of the theory.)

Consider the following interpretation for S: $\mathcal{I}_0 = \langle \mathcal{D}_0, \mathcal{F}_0, \mathcal{R}_0 \rangle$, where $\mathcal{D}_0$ is $\mathbb{N}$ the set of natural numbers; $\mathcal{F}_0$ maps 0 to natural number zero, $'$ to the successor function, + to the addition function and $*$ to the multiplication function; $\mathcal{R}_0$ maps = to the identity relation. As can be readily verified, all the proper axioms are true in $\mathcal{I}_0$; so $\mathcal{I}_0$ is a model of S. Any interpretation of S whose domain is isomorphic to $\mathcal{D}_0$ is called a standard model of S.

Theorem 17 *Any model of S that has a countably infinite domain is standard.*

Gödel's completeness theorem tells us that any wff that is true in every model of S is provable in S. But can there be wffs that are true in $\mathcal{I}_0$, but not in some other model of S? If there exists such a wff, then it cannot be a logical consequence of the proper axioms and hence must be unprovable in S; that would mean that though S, on the face of it, seems to capture our intuitive understanding of natural numbers, is unable to prove every true statement on natural numbers. The so called "Gödel's incompleteness theorem" demonstrtes the existence of such a wff.

Representability of functions and relations in S

Definition 9 *A number theoretic relation $R \subseteq \mathbb{N}^k$ is said to be representable in S iff there exists a wff $\alpha(x_1, \ldots, x_k)$ in S with k free variables such that for any $\langle n_1, \ldots, n_k \rangle$,*

(1) if $\langle n_1, \ldots, n_k \rangle \in R$, then $\vdash_S \alpha(n_1, \ldots, n_k)$
(2) if $\langle n_1, \ldots, n_k \rangle \notin R$, then $\vdash_S \neg\alpha(n_1, \ldots, n_k)$

Note that *numerals* (terms denoting numbers) are represented as follows: 0 by 0, $0'$ by 1, $0''$ by 2, $0'''$ by 3 etc.

Informally, a relation R is representable in S, when S is capable of "describing" R in a manner consistent with our intuitive number-theoretic understanding of R. Note that, S being a formal system, all the "describing" done by S is syntactic (see the definition above); ofcourse, by virtue of Gödel's completeness theorem, all that is "described" will have to be a logical consequence of Peano's Axioms as well.

Definition 10 *A number theoretic function $f : \mathbb{N}^k \to \mathbb{N}$ is said to be representable in S iff there exists a wff $\alpha(x_1, \ldots, x_{k+1})$ in S with $k+1$ free variables such that for any $\langle n_1, \ldots, n_{k+1} \rangle$,*

(1) if $f(n_1, \ldots, n_k) = n_{k+1}$, then $\vdash_S \alpha(n_1, \ldots, n_k, n_{k+1})$

(2) $\vdash_S \exists! x_{n+1} \alpha(n_1, \ldots, n_k, x_{n+1})$

Lecture 13: 12 Sep 2014

The one-argument zero function ζ that returns zero for every argument is represented by the wff $x_1 = x_1 \wedge x_2 = 0$.

The one-argument successor function σ that returns "the argument plus one" is represented by the wff $x_2 = x_1'$.

The i-th k-arguments projection function π_i^k that returns the i-th argument is represented by the wff $x_1 = x_1 \wedge x_2 = x_2 \wedge \ldots \wedge x_k = x_k \wedge x_{k+1} = x_i$.

The class of functions that are representable in S is very rich. A function is computable iff it is representable in S.

Gödel numbering

Choose an appropriate Gödel numbering scheme so that every symbol, expression, and sequence of expressions of S gets a unique Gödel number (GN). One such numbering is described now.

Let the GN of each symbol of S be an odd number. Say, $\rightarrow$, $\neg$, $\forall$, (,), 0, $'$, +, $*$, = get GNs of 3, 5, 7, 9, 11, 13, 15, 17, 19, 21 respectively. Say, the i-th variable x_i, for $i \geq 0$, gets $23 + 2i$. Let the GN of a string "$a_1 \ldots a_n$" be $gn(a_1 \ldots a_n) = \Pi_{i>0} p_i^{gn(a_i)}$, where p_i is the i-th prime number. For example $p_1 = 2$; $p_2 = 3$; $p_3 = 5$, and $gn(0 + x_1 = x_2) = 2^{13}3^{17}5^{25}7^{21}11^{27}$. Let the GN of a sequence of strings $\langle s_1, \ldots, s_n \rangle$" be $\Pi_{i>0} p_i^{gn(s_i)}$, where p_i is the i-th prime number.

It is easy to see that no two syntactic entities get the same GN. Every symbol gets an odd number. In the prime factorization of the GN of a string, the exponent of 2 is an odd number. In the prime factorization of the GN of a sequence of strings, the exponent of 2 is an even number.

Given a syntactic entity (symbol, string, sequnce of strings), we can easily compute its GN. Given a number, we can easily check if it is a valid GN, and if it is decode it into the corresponding syntactic entity.

With the help of GNs, we can treat every syntactic entity as a number.

Incompleteness

Using this scheme we can synthesise a sequence of representable-in-S functions and predicates about S, a sample of which is given below:

- Variable-Expression(n) : true iff n is (the GN of) an expression containing a single variable.
- Term(n) : true iff n is a term of S; let us drop "the GN of" hereafter; that is, let us assume that synatactic entities and their GNs are one and the same.
- Formula(n) : true iff n is a wff of S
- MP(m, n, p) : true iff p is the result of applying MP on m and n

- Substitution(m, n, p, q) : true iff wff m is the result of substituting term p for every free occurance of variable q in wff n.
- Logical-Axiom(n) : true iff n is an instance of a logical axiom of S.
- Proper-Axiom(n) : true iff n is an instance of a proper axiom of S.
- Axiom(n) : true iff n is an instance of an axiom of S.
- Proof(n, m) : true iff n is a proof m in S.
- Neg(n, m) : true iff either n is a negation of m or m is a negation of n.
- Proves-an-instance$_\alpha(n_1, \ldots, n_k, m)$: true iff m is a proof of $\alpha(n_1, \ldots, n_k)$ in S; note that this predicate is parameterised on α; that is for each α there is a different predicate.
- Proves-an-assertion-on-self(n, m) : true iff n is a wff with one free variable, and m is the proof in S of $n(n)$; "$n(n)$" formally means "the GN of the wff obtained by applying $\text{GN}^{-1}(n)$ (the one-free-variable-wff corresponding to n) to the numeral n.

The standard model of S makes S "speak" about numbers. That is under this model we can visualise each wff of S as an assertion about numbers. In particular, each wff with exactly one free variable can be thought as an assertion about a number, which may be true or false depending on tthe number. For example, consider the wff "$x > 3$"; this is true for $x = 4$, but false for $x = 1$.

Now, if we were to identify each synatactic entity of S with a number, then we would be able to visualise each wff-with-exactly-one-free-variable (which is itself a syntactic entity) as an assertion about a syntactic entity. Gödel numbering is one such trick; it identifes each symbol, string and sequence of strings of S with a unique number. Once we have syntactic entities that make general assertions about syntactic entities, by particularisation, we can form syntactic entities that make assertions about themselves.

Recall the following representable-in-S predicate we saw earlier.

Proves-an-assertion-on-self(n, m) : true iff n is a wff with one free variable, and m is the proof in S of $n(n)$

Say this is represented in S by $\alpha(x, y)$. Now consider the wff $\forall y \neg\alpha(x, y)$; m be the GN of this wff; this is a one free variable wff; hence it can be visualised as stating that "$x(x)$ cannot be proved". By plugging in m for x we can make m talk about itself; that is, make it assert that "$m(m)$ is not provable"; but this is nothing but $m(m)$ itself. Let us call this γ. γ, according to the semantics of the standard model, asserts that "I am not provable"; this wff cannot be false, because if its is then it must be provable, and then by Soundness of S it must be true; so it must be true, in which case it cannot be provable.

This means we have found an assertion that is true according to our intuitive under standing of numbers, but will not be proved by the formal system that we laid out. That is to say that our proof system does not capture all the truths of number theory. It may seem that this can be remedied by adopting a stronger proof system. But such is not the case, because for the new proof system P' again, the above construction can be carried out to

obtain a wff that asserts its on non-provability in P'; one only has to plug in new primitive recursive predicates for the axioms and the rules of inference. This shows up the inherent inability of proof systems to match our intuitive understanding of Mathematics.

Lecture 14: 18 Sep 2014

Number Theory

Reference: Niven, Zuckerman and Montgomery, An Introduction to the Theory of Numbers.

$\mathbb{Z}$ denotes the set of integers.

For two integers $a \neq 0$ and b, $a \mid b$ (a divides b, a is a divisor of b, b is a multiple of b), if for some integer x, $b = ax$. Its negation is denoted $a \nmid b$.

Theorem 18 *(i) if $a \mid b$, then for any $c \in \mathbb{Z}$, $a \mid bc$ (ii) if $a \mid b$ and $b \mid c$, then $a \mid c$ (iii) if $a \mid b$ and $a \mid c$, then for any $p, q \in \mathbb{Z}$, $a \mid (bp + cq)$ (iv) if $a \mid b$ and $b \mid a$, then $a = \pm b$ (v) if $a \mid b$ for positive a and b, then $a \leq b$ (vi) if $x \in \mathbb{Z}$, $x \neq 0$ and $a \mid b$, then $xa \mid xb$*

Proof: (iii) $(a \mid b \wedge a \mid c) \Rightarrow \exists x, y \in \mathbb{Z}(b = ax \wedge c = ay) \Rightarrow \exists x, y \in \mathbb{Z}\ \forall p, q \in \mathbb{Z}(bp + cq = a(px + yq)) \Rightarrow \forall p, q \in \mathbb{Z}\ \exists x, y \in \mathbb{Z}(bp + cq = a(px + yq)) \Rightarrow \forall p, q \in \mathbb{Z}\ \exists z \in \mathbb{Z}(bp + cq = az) \Rightarrow \forall p, q \in \mathbb{Z}\ a \mid (bp + cq)$

Prove the rest yourself. □

Theorem 19 *(The division algorithm.) For any two integers $a > 0$ and b, there exist unique integers q and r such that $b = qa + r$ and $0 \leq r < a$. If $a \nmid b$, then $0 < r < a$.*

Proof: Consider the arithmetic progression $\ldots, b - 3a, b - 2a, b - a, b, b + a, b + 2a, b + 3a, \ldots$. Let the smallest non-negative member of this AP be r. Then, $r = b - qa$ for some integer q. That establishes the existence of at least one pair (r, q) satisfying $b = qa + r$ and $0 \leq r < a$.

Suppose $(r', q') \neq (r, q)$ satisfies $b = q'a + r'$ and $0 \leq r$. Then, $r' \neq r$ and $r' = b - q'a$. So, r' is a nonnegative member of the AP. That is $r' \geq b - qa + a \geq a$. Therefore, there is a unique pair (r, q) satisfying $b = qa + r$ and $0 \leq r < a$.

If $a \nmid b$, then the smallest non-negative member of the AP is nonzero. □

Prove the following theorem.

Theorem 20 *For any two integers $a \neq 0$ and b, there exist unique integers q and r such that $b = qa + r$ and $0 \leq r < |a|$.*

Integer a is a common divisor (CD) of integers b and c, if $a \mid b$ and $a \mid c$. Every nonzero integer has only a finite number of divisors. That is, unless $b = c = 0$, there is only a finite number CDs of b and c. If $b \neq 0$ or $c \neq 0$, then the greatest of their CDs is their GCD (greatest common divisor). The notion can be extended to more than two integers.

Theorem 21 *If $g = \text{GCD}(b, c)$, then there exist integers x_0 and y_0 such that $g = bx_0 + cy_0$.*

Proof: Consider $S = \{bx + cy \mid x, y \in \mathbb{Z}\}$. Let d be the least positive member of S. Say, $d = bx_0 + cy_0$.

If $d \nmid b$, then by the division algorithm, there exist unique integers r and q such that $b = qd + r$ and $0 < r < d$. So, $r = b - qd = b - q(bx_0 + cy_0) = b(1 - qx_0) + c(-qy_0)$. That is, $r \in S$. So d is not the least positive member of S. Contradiction.

Since $g \mid b$, $g \mid c$ and $d = bx_0 + cy_0$, we have that $g \mid d$. As g and d are both positive, by Theorem 18, $g \leq d$. But g is the GCD and d is a CD of b and c. So $d \leq g$. That is, $g = d$. □

Corollary 6 $\text{GCD}(b, c)$ *is the least positive member of* $\{bx + cy \mid x, y \in \mathbb{Z}\}$.

Theorem 22 *For any two integers b and c, not both zero, the GCD is the positive CD that is a multiple of every CD.*

Proof: If d is a CD of b and c, then by (iii) of Theorem 18, d divides every member of $\{bx + cy \mid x, y \in \mathbb{Z}\}$, and g in particular. So, the GCD is a multiple of every CD.

If g and g' are both positive CDs that are multiples of all CDs, then $g \mid g'$ and $g' \mid g$ and hence $g = g'$. So the GCD is the only positive CD that is a multiple of every CD. □

Lecture 15: 19 Sep 2014

Theorem 23 *For every positive integer d, $\text{GCD}(bd, cd) = \text{GCD}(b, c).d$*

Proof: $\text{GCD}(bd, cd)$ is the least positive member of $\{bdx + cdy \mid x, y \in \mathbb{Z}\}$, which is d times the least positive member of $\{bx + cy \mid x, y \in \mathbb{Z}\}$. □

Theorem 24 *For every positive CD d of b and c, $\text{GCD}(b/d, c/d) = \text{GCD}(b, c)/d$.*

Proof: Set $d \leftarrow d$, $b \leftarrow b/d$ and $c \leftarrow c/d$ in the above theorem. □

Theorem 25 *If $\text{GCD}(a, d) = \text{GCD}(b, d) = 1$, then $\text{GCD}(ab, d) = 1$.*

Proof: By Theorem 21, there exist integers x_0, y_0, x_1, y_1 such that $1 = ax_0 + dy_0 = bx_1 + dy_1$. Therefore, for $z_1 = dy_0y_1 - y_0 - y_1$, and $z_0 = x_0x_1$, $ab(z_0) = (1 - dy_0)(1 - dy_1) = 1 + dz_1$. That is, $ab(z_0) + d(-z_1) = 1$. Thus, 1 is the least positive member of $\{abx + dy \mid x, y \in \mathbb{Z}\}$. Hence, $\text{GCD}(ab, d) = 1$. □

When $\text{GCD}(a, b) = 1$, a and b are called relatively prime or co-prime.

Theorem 26 *For any integers a, b and x, $\text{GCD}(a, b) = \text{GCD}(a, b + ax)$.*

Proof: $\text{GCD}(a, b + ax)$ is the least positive member of $S = \{ay + (b + ax)z \mid y, z \in \mathbb{Z}\} = \{a(y + xz) + bz \mid y, z \in \mathbb{Z}\} = \{au + bz \mid y, z \in \mathbb{Z}\}$. Given integers u and z, choose $y = u - xz$. □

Theorem 27 *If a and c are co-prime, and $a \mid bc$, then $a \mid b$.*

Proof: $\text{GCD}(ab, bc) = b.\text{GCD}(a, c) = b$. Thus, all CDs of ab and bc divide b. But a is a CD of bc and ab. □

Theorem 28 *(Euclid's algorithm.) For any two integers r_0 and $r_1 > 0$, if we apply the division algorithm repeatedly as follows:*

$i = 1$;
do {
$(r_{i+1}, q_{i+1}) \leftarrow$ Division_Algorithm(r_{i-1}, r_i); $i = i + 1$;
} while ($r_i \neq 0$);

The GCD of r_0 and r_1 is r_{i-1}, the last nonzero remainder in the division process. Integers x_0 and y_0 such that $r_{i-1} = r_0x_0 + r_1y_0$ can be obtained by writing each r_j, $2 \leq j < i$ as a linear combination of r_0 and r_1.

Proof: By Theorem 26, $\text{GCD}(r_0, r_1) = \text{GCD}(r_1, r_0 - r_1q_2) = \text{GCD}(r_1, r_2)$. Continuing like this, we find that this is equal to $\text{GCD}(r_{i-1}, r_{i-2} - r_{i-1}q_i) = \text{GCD}(r_{i-1}, 0) = r_{i-1}$.

It is easy to show by induction that each r_j is a linear combination of r_0 and r_1. The basis is formed by r_0 and r_1 themselves. If r_{j-1} and r_{j-2} are linear combinations of r_0 and r_1, then so is r_j. □

For integers a and b, $a \mid ab$ and $b \mid ab$; ab is a common multiple (CM) of a and b. The least of the positive CMs of a and b is called the LCM (least common multiple) of a and b.

Theorem 29 *Let $l = \text{LCM}(a, b)$. If c is a CM of a and b, then $l \mid c$. Also, $0, \pm l, \pm 2l, \pm 3l, \ldots$ are all the CMs of a and b.*

Proof: Let c be a CM of a and b. There exists a unique pair (r, q) of integers such that $c = ql + r$ and $0 \leq r < l$. If $r \neq 0$, then as $a \mid l$ and $a \mid c$ and $b \mid l$ and $b \mid c$, we have that $a \mid r$ and $b \mid r$. That is, r is a CM of a and b. So $l \neq \text{LCM}(a, b)$. Contradiction. Thus, $r = 0$ and $l \mid c$. That is, every CM is among $0, \pm l, \pm 2l, \pm 3l, \ldots$, all of which are CMs. □

Theorem 30 *For every positive integer d, $\text{LCM}(bd, cd) = \text{LCM}(b, c).d$*

Proof: Let $l = \text{LCM}(b, c)$ and $L = \text{LCM}(bd, cd)$. Then $bd \mid ld$ and $cd \mid ld$; ld is a CM of bd and cd; $L \mid ld$. Also, $b \mid L/d$ and $c \mid L/d$; L/d is a CM of b and c; $l \mid L/d$. That is, $L = l$. □

Theorem 31 $\text{GCD}(a, b).\text{LCM}(a, b) = \mid ab \mid$

Proof: First assume that $a, b > 0$.

Say, a and b are co-prime. Let $\text{LCM}(a, b) = da$. Then $b \mid da$. As $\text{GCD}(a, b) = 1$, by Theorem 27, $b \mid d$. Hence $b \leq d$ and so, $ba \leq da$. But $ba > 0$, is a CM of b and a. So $ba \geq da$. That is, $ba = da$. In other words, $\text{LCM}(a, b) = ab$.

When a and b are not co-prime, that is, say $\text{GCD}(a, b) = g > 1$, $\text{GCD}(a/g, b/g) = 1$, and therefore, $\text{GCD}(a/g, b/g).\text{LCM}(a/g, b/g) = ab/g^2$. That is, $(g.\text{GCD}(a/g, b/g))(g.\text{LCM}(a/g, b/g)) = \text{GCD}(a, b).\text{LCM}(a, b) = ab$.

When a or b is negative, $\text{GCD}(a, b) = \text{GCD}(\mid a \mid, \mid b \mid)$ and $\text{LCM}(a, b) = \text{LCM}(\mid a \mid, \mid b \mid)$. □

Lecture 16: 3 Oct 2014

An integer $p > 1$ is a prime, if 1 and p are the only positive divisors of p. A non-prime integer is called a composite.

Theorem 32 *Every integer $n > 1$ is a product of one or more primes.*

Proof: If n is prime, then "n" itself is the product we seek. If n is composite, then n is the product of two numbers n_1 and n_2 both less than n. Inductively assume that n_1 and n_2 satisfy the theorem. Then, combining the products, we have the theorem. □

A representation of an integer n as a product $p_1^{e_1} \dots p_k^{e_k}$ where each p_i is a prime, $p_i < p_{i+1}$, and e_i is an integer is called a canonical factoring of n into prime powers.

Theorem 33 *For prime p and integers a and b, if $p \mid ab$, then $p \mid a$ or $p \mid b$*

Proof: If $p \nmid a$ then, p and a are co-prime, and so by Theorem 27, $p \mid b$. □

Theorem 34 *For prime p and integers $a_1, \dots, a_n$, if $p \mid a_1 \dots a_n$, then $p \mid a_i$ for some i, $1 \le i \le n$.*

Proof: Use induction on n. Theorem 33 forms the basis. For $n > 2$, let $a = a_1$, and $b = a_2 \dots a_n$. Then by Theorem 33, $p \mid a$ or $p \mid b$. By induction hypothesis, if $p \mid a_2 \dots a_n$, then $p \mid a_i$ for some i, $2 \le i \le n$. Hence the theorem. □

Theorem 35 *(The fundamental theorem of arithmetic) Every integer $n > 1$ has a unique canonical prime factorization.*

Proof: Suppose n is an integer with two canonical prime factorizations. Cancel the common primes from these two. Some primes must remain on either side. The remaining primes form an equation: $q_1 \dots q_k = s_1 \dots s_l$. All $k + l$ primes in the equation must be distinct. But, $q_1 \mid s_1 \dots s_l$ and so by Theorem 34, q_1 equals some s_i. Contradiction. □

The fundamental theorem of arithmetic holds for integers. But it need not hold in general. For example, consider the set E of even integers. E is closed under addition and multiplication. In this system, 50 is a prime, but $12 = 2 \times 6$ is not. 100 has two canonical prime factorizations; $100 = 10^2 = 2 \times 50$.

As another example, consider the set $C = \{a + i\sqrt{6}b \mid a, b \in \mathbb{Z}\}$ of complex numbers. C is closed under addition and multiplication. Define the norm of $a + i\sqrt{6}b$ as $N(a + i\sqrt{6}b) = a^2 + 6b^2$, the square of its absolute value. 0, 1 and -1 are the only members of C with a norm ≤ 1. We say thet $a + i\sqrt{6}b$ is a prime, if it can be expressed as the product of two members of C, each of norm > 1. Note that $N(n_1 n_2) = N(n_1)N(n_2)$. So a composite number factorizes into two numbers of smaller norms. Since the norm of every number is an integer, the factorization tree has finite levels. A proper complex number in C has norm ≥ 6. So 5 is a prime because it doesn't have real factors in C, and if $5 = n_1 n_2$, then $25 = N(n_1)N(n_2) \ge 36$. $10 = 2 \times 5 = (2 + i\sqrt{6}b)(2 - i\sqrt{6}b)$ has two prime factorizations.

Let $\exp(a,p)$ denote the exponent of prime p in the prime facorization of integer $a > 1$. Then

$$a = \prod_{\text{prime } p} p^{\exp(a,p)}$$

. If $c = ab$, then

$$c = \prod_{\text{prime } p} p^{\exp(c,p)} = ab = \prod_{\text{prime } p} p^{\exp(a,p)+\exp(b,p)}$$

. For every prime p, $\exp(c,p) = \exp(a,p) + \exp(b,p)$.

It is easy to see that

$$\text{GCD}(a,b) = \prod_{\text{prime } p} p^{\max\{\exp(a,p),\exp(b,p)\}}$$

and

$$\text{LCM}(a,b) = \prod_{\text{prime } p} p^{\min\{\exp(a,p),\exp(b,p)\}}$$

As $x + y = \max\{x,y\} + \min\{x,y\}$, this proves that $\text{GCD}(a,b)\text{LCM}(a,b) = ab$.

An integer is a square if it can be written as n^2 for some integer n. If a is a square, then $\exp(a,p)$ is even for every prime p.

An integer is square-free if one is the largest square dividing it. If a is square-free, then $\exp(a,p)$ is either 0 or 1 for every prime p.

Lecture 17: 9 Oct 2014

Theorem 36 *(Euclid's Theorem) The number of primes is infinite.*

Proof: If $p_1, \ldots, p_r$ are the first r primes, then none of them divides $n = 1+p_1 \ldots p_r$. Therefore, either n is a prime, or n has a prime factor that is larger than $p_1, \ldots, p_r$. Either way, we have a larger prime. So primes never exhaust. □

Theorem 37 *There are arbitrarily long gaps in the series of primes. That is, for any integer k, there exist k consecutive integers, all of which are composite.*

Proof: Consider integers $(k+1)! + j$, for $2 \leq j \leq k+1$. All these numbers are composite because if $2 \leq j \leq k+1$, then $j \mid (k+1)!$ and so $j \mid (k+1)! + j$. □

Let $\pi(x)$ denote the number of primes not larger than x. Then,

Theorem 38 *(the Prime Number Theorem)*

$$\lim_{x \to \infty} \frac{\pi(x)}{x/\ln x} = 1$$

Congruences

If an integer $m \neq 0$ divides $a-b$, for any two integers a and b, then we say that a is congruent to b modulo m (denoted $a \equiv b \mod m$). Its negation (a is not congruent to b modulo m) is denoted $a \not\equiv b \mod m$.

Theorem 39 *For any integers a, b, c, d, x, y, and a non-zero integer m,*
(i) $(a \equiv b \mod m)$, $(b \equiv a \mod m)$, and $(a - b \equiv 0 \mod m)$ are equivalent statements
(ii) if $(a \equiv b \mod m)$, and $(b \equiv c \mod m)$, then $(a \equiv c \mod m)$
(iii) if $(a \equiv b \mod m)$, and $(c \equiv d \mod m)$, then $(ax + cy \equiv bx + dy \mod m)$
(iv) if $(a \equiv b \mod m)$, and $(c \equiv d \mod m)$, then $(ac \equiv bd \mod m)$
(v) if $(a \equiv b \mod m)$, and $d \mid m$, and $d > 0$, then $(a \equiv b \mod d)$
(vi) if $(a \equiv b \mod m)$, then $(ac \equiv bc \mod mc)$, for $c > 0$

Proof: (i)-(ii) DY.
(iii) $(a-b) = mk$ and $(c-d) = mj$, for some integers j and k. Then $(ax + cy - bx - dy) = (a-b)x + (c-d)y = m(k+j) \equiv 0 \mod m$.
(iv) Let $a = q_1 m + r_1$, $b = q_1' m + r_1$, $c = q_2 m + r_2$, $d = q_2' m + r_2$, where $0 \leq r_1, r_2 < m$. Then $ac = q_1 q_2 m^2 + (q_1 r_2 + r_1 q_2)m + r_1 r_2 \equiv r_1 r_2 \mod m$. Similarly, $bd \equiv r_1 r_2 \mod m$.
(v) $d \mid m$ and $m \mid (a-b)$ implies that $d \mid (a-b)$
(vi) if $a = qm + r$ and $b = q'm + r$, for $0 \leq r < m$, then $ac = qmc + rc$ and $bc = q'mc + rc$. If $c > 0$, then $0 \leq rc < mc$. □

Theorem 40 *Let f be a polynomial with integer coefficients. For any two integers a, b, and a non-zero integer m, if $(a \equiv b \mod m)$, then $(f(a) \equiv f(b) \mod m)$.*

Proof: Let $f(x) = c_0 x^n + c_1 x^{n-1} + \ldots + c_n$, for some integers $c_0, \ldots, c_n$. If $(a \equiv b \mod m)$, then $(a^2 \equiv b^2 \mod m)$ and $(a^3 \equiv b^3 \mod m)$ etc. Then $(c_{n-1} a \equiv c_{n-1} b \mod m)$ and $(c_{n-2} a^2 \equiv c_{n-2} b^2 \mod m)$ and $(c_{n-3} a^3 \equiv c_{n-3} b^3 \mod m)$ etc. Therefore, $(f(a) \equiv f(b) \mod m)$. □

Lecture 18: 10 Oct 2014

Theorem 41 *For integers a, m, x, y, $(ax \equiv ay \mod m)$ if and only if $(x \equiv y \mod m/\text{GCD}(a, m))$*

Proof: $(ax \equiv ay \mod m)$ iff $ax - ay = mz$ for some integer z
iff $\frac{a}{\text{GCD}(a,m)}(y - x) = \frac{m}{\text{GCD}(a,m)}z$ for some integer z
iff $\frac{m}{\text{GCD}(a,m)} \mid \frac{a}{\text{GCD}(a,m)}(y - x)$
iff $\frac{m}{\text{GCD}(a,m)} \mid (y - x)$ (because $\text{GCD}(a/g, m/g) = 1$)
iff $\left(x \equiv y \mod \frac{m}{\text{GCD}(a,m)}\right)$ □

Corollary 7 *For integers a, m, x, y, when $\text{GCD}(a, m) = 1$, $(ax \equiv ay \mod m)$ if and only if $(x \equiv y \mod m)$*

Theorem 42 *For integers $x, y, m_1, \ldots, m_r$, $(x \equiv y \mod m_i)$ for every i, $1 \le i \le r$, if and only if $(x \equiv y \mod \text{LCM}(m_1, \ldots, m_r))$*

Proof: If $(x \equiv y \mod m_i)$, then $(m_i \mid (y - x))$. Therefore, $(y - x)$ is a common multiple of $m_1, \ldots, m_r$. That is, $\text{LCM}(m_1, \ldots, m_r)) \mid (y - x)$. So, $(x \equiv y \mod \text{LCM}(m_1, \ldots, m_r))$. Conversely, if $(x \equiv y \mod \text{LCM}(m_1, \ldots, m_r))$, then $(x \equiv y \mod m_i)$ because $m_i \mid \text{LCM}(m_1, \ldots, m_r))$. □

If $(x \equiv y \mod m)$, then x is a residue of y modulo m. 1, 13, 31, 43 are all residues modulo 3 of 10. A set of integers $\{x_1, \ldots, x_m\}$ is a complete residue system (CRS) modulo m if for every integer y, there is a unique x_i so that $(x_i \equiv y \mod m)$. $\{0, 1, 2\}, \{2, 15, 10\}, \{100, 101, 102\}$ are all CRSs modulo 3.

A set of integers $\{r_1, \ldots, r_n\}$ is a reduced residue system (RRS) modulo m if each r_i is relatively prime to m, $(r_i \not\equiv r_j \mod m)$ whenever $i \neq j$, and for every integer y relatively prime to m, there is a unique r_i so that $(r_i \equiv y \mod m)$.

Take a CRS modulo m, and delete from it all members not relatively prime to m to get an RRS modulo m. All RRSs modulo m have the same size: $\phi(m)$ – Euler's ϕ function or totient of m. That is , $\phi(m)$ is the number of positive integers $< m$ that are relatively prime to m.

$\{1\}, \{1\}, \{1, 2\}, \{1, 3\}, \{1, 2, 3, 4\}, \{1, 5\}, \{1, 2, 3, 4, 5, 6\}, \{1, 3, 5, 7\}$ are all RRSs, respectively, modulo 1-8. That is, $\phi(1)$ to $\phi(8)$ are, respectively, 1, 1, 2, 2, 4, 2, 6, 4.

Theorem 43 *If $\text{GCD}(a, m) = 1$ and $\{r_1, \ldots, r_n\}$ is a CRS (resp., RRS) modulo m, then $\{ar_1, \ldots, ar_n\}$ is a CRS (resp., RRS) modulo m.*

Proof: Let $S = \{r_1, \ldots, r_n\}$ and $T = \{ar_1, \ldots, ar_n\}$. If S is a CRS or RRS modulo m, then $(r_i \not\equiv r_j \mod m)$ whenever $i \neq j$. If $(ar_i \equiv ar_j \mod m)$ then $(r_i \equiv r_j \mod m)$. Therefore, $(ar_i \not\equiv ar_j \mod m)$ whenever $i \neq j$. Hence, T is also a set of distinct residues modulo m. If S is a CRS modulo m, then T is a CRS modulo m. S is an RRS modulo m implies each r_i in it is co-prime with m implies each ar_i is coprime with m (because a is also co-pime with m) implies T is an RRS modulo m. □

Theorem 44 *(Fermat's Theorem) For any prime p and any integer a, if $p \nmid a$, then* ($a^{p-1} \equiv 1 \mod p$)

First let us prove Euler's generalization.

Theorem 45 *(Euler's Generalization of Fermat's Theorem) For any two integers a and m, if* $\text{GCD}(a, m) = 1$, *then* ($a^{\phi(m)} \equiv 1 \mod m$)

Proof: If $S = \{r_1, \ldots, r_{\phi(m)}\}$ is an RRS modulo m, then so is $\{ar_1, \ldots, ar_{\phi(m)}\}$, by Theorem 43. For each i, $1 \leq i \leq \phi(m)$, there exists a unique j, $1 \leq j \leq \phi(m)$, such that ($r_i \equiv ar_j \mod m$). Hence,

$$a^{\phi(m)} \prod_{j=1}^{\phi(m)} r_j \equiv \prod_{j=1}^{\phi(m)} ar_j \equiv \prod_{i=1}^{\phi(m)} r_i \mod m$$

Each r_i is co-prime with m. So is $\prod_{i=1}^{\phi(m)} r_i$, which can therefore be cancelled from the two sides. The theorem follows. □

If p is a prime and a is an integer such that $p \nmid a$, then $\text{GCD}(a, p) = 1$. $\phi(p) = p - 1$. Fermat's theorem now follows.

Lecture 19: 11 Oct 2014

Theorem 46 *If* $\text{GCD}(a, m) = 1$*, then* $(ax \equiv b \mod m)$ *has a solution* $x = x_1$*. All solutions are given by* $x = x_1 + jm$*, for* $j \in \mathbb{Z}$*.*

Proof: Set $x_1 = a^{\phi(m)-1}b$. Then $ax_1 = a^{\phi(m)}b \equiv b \mod m$; x_1 is indeed a solution. If $x = x_1 + jm$, then $ax = ax_1 + ajm \equiv ax_1 \equiv b \mod m$; x is also a solution.

If y is a solution, then $ay - ax_1 \equiv b - b = 0 \mod m$. That is, $a(y - x_1) \equiv 0 \mod m$. As $\text{GCD}(a, m) = 1$, $(y - x_1) \equiv 0 \mod m$ too. Hence, $y = x_1 + jm$, for some $j \in \mathbb{Z}$. □

Example: $353x \equiv 254 \mod 400$. $\text{GCD}(353, 400) = 1$. $\phi(400) = 160$. (Ref. Lecture 21.) So $353^{159} * 254 \equiv 318 \mod 400$ is a solution. 318 is the only solution in $[0, 399]$. All solutions: $\ldots, -882, -482, -82, 318, 718, 1118, 1518, \ldots$. As you can see, finding large exponents is not easy. So this method is not very practical.

Theorem 47 *(Wilson's Theorem) If* p *is a prime, then* $(p-1)! \equiv -1 \mod p$

Proof: The proof is by induction. For $p = 2$, $(p-1)! = 1! = 1 \equiv -1 \mod 2$; this forms the basis. Assume that the theorem holds for all primes $< p$. For any a, $1 \le a \le p-1$, $\text{GCD}(a, p) = 1$, and so $(ax \equiv 1 \mod p)$ has exactly one integer solution in $[0, p-1]$, by Theorem 46; as $x = 0$ cannot be a solution, the solution must be one of $1, \ldots, p-1$; a and x pair off giving $1 \mod p$. $1 * 1 \equiv 1 \mod p$ and $(p-1)(p-1) \equiv 1 \mod p$. For $2 \le a \le p-1$, $\text{GCD}(a-1, p) = \text{GCD}(a+1, p) = 1$ and hence, $(a-1)(a+1) = a^2 - 1$ is relatively prime to p; that is, $a^2 - 1 \not\equiv 0 \mod p$; in other words, $a^2 \not\equiv 1 \mod p$. No number other than 1 and $p-1$ pairs off with itself. So,

$$1.(2.3.\ldots.(p-2))(p-1) \equiv 1(p-1) \equiv (p-1) \equiv -1 \mod p$$

Solutions of congruences

Let $f(x)$ be a polynomial with constant coeffients. For any two integers u and v, if $(f(u) \equiv 0 \mod m)$, and $(u \equiv v \mod m)$, then $(f(v) \equiv 0 \mod m)$. So we do not count u and v as two separate solutions modulo $m$of the congruence $(f(x) \equiv 0 \mod m)$.

For example, consider $x^2 - x + 4 \equiv 0 \mod 10$. 3, 8, 13, 18, 23, 28, etc. are all its solutions. But $3 \equiv 13 \equiv 23 \equiv \ldots \mod 10$ and $8 \equiv 18 \equiv 28 \equiv \ldots \mod 10$. So we say this congruence has only two solutions.

In general, if S is a CRS modulo m, then $|\{u \mid (f(u) \equiv 0 \mod m) \wedge u \in S\}|$ is the number of solutions of $(f(x) \equiv 0 \mod m)$.

Let $f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n$. Let j be the largest integer such that $a_j \not\equiv 0 \mod m$. Then the degree of the congruence $(f(x) \equiv 0 \mod m)$ is j. If there is no j, then the degree of the congruence is undefined.

Here we consider congruences of degree 1. These are of the form $ax \equiv b \mod m$. By Theorem 46, if $\text{GCD}(a, m) = 1$, then $ax \equiv b \mod m$ has exactly one solution modulo m. Let $\text{GCD}(a, m) = g \not\equiv 1$. Suppose the congruence has a solution x. For some integer z, $ax = mz + b$; $g \mid a$; $g \mid m$; so, g divides $ax - mz = b$. In other words, if $g \nmid b$, then the congruence has no solution.

If $g \mid b$, then $ax \equiv b \mod m$ iff $(a/g)x \equiv (b/g) \mod (m/g)$. So it is enough to solve the latter congruence.

Consider the congruence $(a/g)x \equiv 1 \mod (m/g)$. As $\text{GCD}(a/g, m/g) = 1$, this congruence has exactly one solution modulo m/g; suppose $(x_0 \mod (m/g))$ is that solution. Then $x_0(b/g) \mod (m/g)$ is the only solution-modulo-(m/g) of $(a/g)x \equiv (b/g) \mod (m/g)$. That means, $(x_0(b/g) + t(m/g) \mod m)$ are the g solutions-modulo-m of it, and therefore of $ax \equiv b \mod m$.

Example: $353x \equiv 254 \mod 400$. $\text{GCD}(353, 400) = 1$. Using Euclid's algorithm, we find that $1 = 17 \times 353 - 15 \times 400$. That is, 17 is the only solution-modulo-400 of $353x \equiv 1 \mod 400$. So, $17 \times 254 = 4318 \equiv 318 \mod 400$ is the only of $353x \equiv 254 \mod 400$.

Example: $15x \equiv 25 \mod 35$.

As $\text{GCD}(15, 35) = 5$, this is iff $3x \equiv 5 \mod 7$.

First consider $3x \equiv 1 \mod 7$. $\text{GCD}(3, 7) = 1 = 7 + 3 \times (-2)$. But $-2 \equiv 5 \mod 7$. So 5 is the only solution-modulo-7 of $3x \equiv 1 \mod 7$.

So $5 * 5 = 25$ is a solution of $3x \equiv 5 \mod 7$. But $25 \equiv 4 \mod 7$. So 4 is the only solution-modulo-7 of $3x \equiv 5 \mod 7$. Hence, $4, 11, 18, 25, 32$ are the solutions-modulo-35 of $15x \equiv 25 \mod 35$.

Lecture 20: 16 Oct 2014

Theorem 48 *(Chinese Remainder Theorem) Let $m_1, \ldots, m_r$ be r positive integers relatively prime in pairs. Let $a_1, \ldots, a_r$ be r integers. Congruences $x \equiv a_i \mod m_i$, for $1 \leq i \leq r$ have simultaneous solutions. Any two solutions are congruent modulo $m_1 \ldots m_r$*

Proof: Let $m = m_1 \ldots m_r$. Let $M_j = m/m_j$. Then $\text{GCD}(M_j, m_j) = 1$. Therefore, $M_j x \equiv 1 \mod m_j$ has exactly one solution among $0, \ldots, m_j - 1$; say, that is b_j. Then, $M_j b_j \equiv 1 \mod m_j$.

If $i \neq j$, $M_j b_j = (m_1 \ldots m_{j-1} m_{j+1} \ldots m_r) b_j \equiv 0 \mod m_i$.

Define $x_0 = \sum_{i=1}^{r} M_j b_j a_j$.

$x_0 = M_1 b_1 a_1 + (M_2 b_2 a_2 + \ldots + M_r b_r a_r) \equiv M_1 b_1 a_1 \equiv a_1 \mod m_1$.

Similarly, $x_0 \equiv a_i \mod m_i$, for each i.

So x_0 is a simultaneous solution.

If x_0 and x_1 are simultaneous solutions, then for each i, $x_0 \equiv x_1 \mod m_i$. Therefore $x_0 \equiv x_1 \mod \text{LCM}(m_1, \ldots, m_r)$. That is, $x_0 \equiv x_1 \mod m$. □

Example: $(353x \equiv 254 \mod 400)$ iff $(353x \equiv 254 \mod 16)$ and $(353x \equiv 254 \mod 25)$ iff $(x \equiv 14 \mod 16)$ and $(3x \equiv 4 \mod 25)$ because $(353 \equiv 1 \mod 16)$, $(353 \equiv 3 \mod 25)$, $(254 \equiv 14 \mod 16)$, $(254 \equiv 4 \mod 25)$.

Solving $(3x \equiv 4 \mod 25)$, first we consider $(3x \equiv 1 \mod 25)$. $1 = 25 - 8 \times 3$. $-8 \equiv 17 \mod 25$ is a solution. So $17 = 68 \equiv 18 \mod 25$ is a solution of $(3x \equiv 4 \mod 25)$.

We are left with $(x \equiv 14 \mod 16)$ and $(x \equiv 18 \mod 25)$. Applying Chinese Remainder Theorem, $a_1 = 14$, $m_1 = 16$, $a_2 = 18$, $m_2 = 25$, $M_1 = 25$, $M_2 = 25$. Let b_1 be the solution of $M_1 b_1 \equiv 1 \mod m_1$; i.e., $25 b_1 \equiv 1 \mod 16$; then $b_1 = 9$. Let b_2 be the solution of $M_2 b_2 \equiv 1 \mod m_2$; i.e., $16 b_2 \equiv 1 \mod 25$; then $b_2 = 11$. A simultaneous solution is $M_1 b_1 a_1 + M_2 b_2 a_2 = 6318 \equiv 318 \mod 400$. 318 is the only solution in $[0, 399]$.

Theorem 49 *If m and n are relatively prime integers, then $\phi(mn) = \phi(m)\phi(n)$.*

Proof:

Let A, B, C be RRS-s modulo m, n and mn respectively.

If $x \in C$, then $\text{GCD}(x, mn) = 1$, and so $\text{GCD}(x, m) = 1$ and $\text{GCD}(x, n) = 1$. So $(x \equiv r \mod m)$ and $(x \equiv s \mod n)$ for unique $r \in A$ and $s \in B$. That is, $|C| \leq |A \times B|$.

If $(r, s) \in A \times B$, then by Chinese Remainder Theorem, $(x \equiv r \mod m)$ and $(x \equiv s \mod n)$ have exactly one simultaneous solution in $[0, mn - 1]$. Let x_0 be that solution. Then x_0 is relatively prime to mn because $\text{GCD}(r, m) = 1$ and $\text{GCD}(s, n) = 1$. That is $x_0 \equiv x_0' \mod mn$, for some $x_0' \in C$. That is, $|C| \geq |A \times B|$. □

Lecture 21: 17 Oct 2014

Theorem 50 *If $n > 1$, then $\phi(n) = n \cdot \Pi_{p|n}(1 - 1/p)$*

Proof: $\phi(m)$ is the number of positive integers $\leq m$ that are relatively prime to m. So $\phi(1) = 1$.

Let $n = p_1^{e_1} p_2^{e_2} \ldots p_r^{e_r}$ be the canonical prime factorization of n. As $\text{GCD}(p_i^{e_i}, p_j^{e_j}) = 1$, for $i \neq j$, $\phi(n) = \Pi_{j=1}^{r} \phi(p_j^{e_j})$.

In $[1, p^e]$, p^e has exactly p^{e-1} divisors, namely, $1, p, p^2, \ldots, p^e$. Therefore, $\phi(p^e) = p^e - p^{e-1} = p^e(1 - 1/p)$.

That is, $\phi(n) = \Pi_{j=1}^{r} p_j^{e_j}(1 - 1/p_j) = n \cdot \Pi_{p|n}(1 - 1/p)$. □

Theorem 51 *If $n > 1$, then $\sum_{d|n} \phi(d) = n$. (The summation is over all divisors d of n.)*

Proof: First consider the case $n = p^e$, for some prime p. $\sum_{d|p^e} \phi(d) = \phi(1) + \phi(p) + \phi(p^2) + \ldots + \phi(p^e) = 1 + (p-1) + p(p-1) + p^2(p-1) + \ldots + p^{e-1}(p-1) = 1 + (p-1)(1 + p + p^2 + \ldots + p^{e-1}) = p^e = n$.

For general n, proceed by induction on the number of prime factors of n. Say $N = np^e$. $\sum_{d|N} \phi(d) = \sum_{d|n} \phi(d) + \sum_{d|n} \phi(pd) + \ldots + \sum_{d|n} \phi(p^e d) = \sum_{d|n} \phi(d) + \sum_{d|n} \phi(p)\phi(d) + \ldots + \sum_{d|n} \phi(p^e)\phi(d) = \sum_{d|n} \phi(d)[1 + \sum_{d|n} \phi(p) + \ldots + \sum_{d|n} \phi(p^e)] = \sum_{d|n} \phi(d)[\sum_{e|p^e} \phi(e)] = p^e \sum_{d|n} \phi(d) = p^e n$. The last equality is by induction hypothesis. □

Ceiling and Floor

For $x \in \mathbb{R}$, $\lfloor x \rfloor$, called the floor of x, is the greatest integer $\leq x$; $\lceil x \rceil$, called the ceiling of x, is the smallest integer $\geq x$.

Theorem 52 *(i) $\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$; $x - 1 < \lfloor x \rfloor \leq x$; $0 \leq x - \lfloor x \rfloor < 1$*
(ii) $\lfloor x \rfloor = \sum_{1 \leq i \leq x} 1$, for $x \geq 0$
(iii) $\lfloor x + j \rfloor = \lfloor x \rfloor + j$, if $j \in \mathbb{Z}$
(iv) $\lfloor x \rfloor + \lfloor y \rfloor \leq \lfloor x + y \rfloor \leq \lfloor x \rfloor + \lfloor y \rfloor + 1$
(v) $\lfloor x \rfloor + \lfloor -x \rfloor = 0$, if x is an integer, -1 otherwise
(vi) $\lfloor \lfloor x \rfloor / j \rfloor = \lfloor x/j \rfloor$, if j is a positive integer
(vii) $-\lfloor -x \rfloor = \lceil x \rceil$
(viii) $\lfloor x + (1/2) \rfloor = round(x)$, where halves are rounded upwards
(ix) $-\lfloor -x + (1/2) \rfloor = round(x)$, where halves are rounded downwards
(x) For $n, m \in \mathbb{Z}^+$, $\lfloor n/m \rfloor$ is the number of integers in $[1, n]$ divisible by m.

Proof: (i)-(iii) DY. (iv) If $x = n + \epsilon$ and $y = m + \delta$, where $n, m \in \mathbb{Z}$, and $0 \leq \epsilon, \delta < 1$, then $\lfloor x \rfloor + \lfloor y \rfloor = n + m \leq \lfloor x + y \rfloor = \lfloor n + m + \epsilon + \delta \rfloor = n + m$ or $n + m + 1 \leq \lfloor x \rfloor + \lfloor y \rfloor + 1$. (v) If x is an integer, then $\lfloor x \rfloor = x$ and $\lfloor -x \rfloor = -x$. If $x = n + \delta$, for $n \in \mathbb{Z}$, $0 \leq \delta < 1$, then $\lfloor x \rfloor = n$ and $\lfloor -x \rfloor = -(n + 1)$. (vi) Let $x = n + \delta$, for $n \in \mathbb{Z}$, $0 \leq \delta < 1$. Let $n = qj + r$, for $j, q, r \in \mathbb{Z}$, $0 \leq r < j$. Then $x = qj + r + \delta$. So, $\lfloor \lfloor x \rfloor / j \rfloor = \lfloor n/j \rfloor = q$, and $\lfloor x/j \rfloor = q$ because $r + \delta < j$. (vii)-(x) DY. □

Generating Functions

Consider a sequence $\mathbf{a} = \langle a_0, a_1, a_2, a_3, \ldots \rangle$ of complex numbers.

The function $A(z) = a_0 + a_1 z + a_2 z^2 + a_3 z^3 + \ldots$ is called the generating function of $\mathbf{a}$.

We assume that z is small enough for each of the following identities to hold. Beyond that we do not care what values z takes, as we shall not be evaluating generating functions for particular values of z.

The generating function of $\mathbf{b} = \langle \beta a_0, \beta a_1, \beta a_2, \beta a_3, \ldots \rangle$ is $\beta A(z)$, for any constant β.

If $\mathbf{a} = \langle 1, 1, 1, 1, \ldots \rangle$, then $A(z) = 1/(1-z)$. If $\mathbf{a} = \langle 1, \alpha, \alpha^2, \alpha^3, \ldots \rangle$, then $A(z) = 1/(1-\alpha z)$. In general, if $\mathbf{b} = \langle a_0, \alpha a_1, \alpha^2 a_2, \alpha^3 a_3, \ldots \rangle$, then $B(z) = A(\alpha z)$.

If $\mathbf{c} = \mathbf{a} + \mathbf{b}$, the position wise sum of $\mathbf{a}$ and $\mathbf{b}$, then $C(z) = A(z) + B(z)$.

S is the shift operation on sequences. S^i shifts every member of a sequence by i positions to the right, and fills the vacant positions with zero. For example, $S^2(\langle 1, 2, 3, 4, \ldots \rangle) = \langle 0, 0, 1, 2, 3, 4, \ldots \rangle$. When i is negative a left shift is indicated. For eaxample, $S^{-2}(\langle 1, 2, 3, 4, \ldots \rangle) = \langle 3, 4, 5, 6, \ldots \rangle$. The generating function of $S^i(\mathbf{a})$ is $z^i A(z)$, and that of $S^{-i}(\mathbf{a})$ is $(A(z) - a_0 - \ldots - a_{i-1} z^{i-1})/z^i$.

We say that $\mathbf{c}$ is $\mathbf{a} * \mathbf{b}$, the convolution of $\mathbf{a}$ and $\mathbf{b}$, if $c_r = a_0 b_r + a_1 b_{r-1} + \ldots + a_r b_0$. Verify that in that case, $C(z) = A(z)B(z)$. If $\mathbf{c} = \mathbf{a} * \langle 1, 1, 1, 1, \ldots \rangle$, then $c_r = \sum_{j=0}^{r} a_r$; $\mathbf{c}$ is the prefix sums sequence of $\mathbf{a}$.

If $\mathbf{a} = \langle 1, 0, 0, 0, \ldots \rangle$, then $A(z) = 1$. Its prefix sums sequence is $\mathbf{b} = \langle 1, 1, 1, 1, \ldots \rangle$; $B(z) = 1/(1-z)$. The prefix sums sequence of $\mathbf{b}$ is $\mathbf{c} = \langle 1, 2, 3, 4, \ldots \rangle$; $C(z) = 1/(1-z)^2$.

Generating functions can be used to establish many results on numbers. For example,

$1/(1-z)^2 = 1 + 2z + 3z^2 + 4z^3 + \ldots$

$z/(1-z)^2 = 0 + z + 2z^2 + 3z^3 + 4z^4 + \ldots$

Differentiating,

$d/dz(z/(1-z)^2) = (1+z)/(1-z)^3 = 1 + 2^2 z + 3^2 z^2 + 4^2 z^3 + \ldots$

$z(1+z)/(1-z)^3 = 0 + z + 2^2 z^2 + 3^2 z^3 + 4^2 z^4 + \ldots$

As dividing by $(1-z)$ is equivalent to taking prefix-sums

$z(1+z)/(1-z)^4 = 0 + (1^2)z + (1^2 + 2^2)z^2 + (1^2 + 2^2 + 3^2)z^3 + \ldots$

By Binomial Theorem, the coefficient of z^r in $(1-z)^{-4}$ is $\frac{(-4)(-5)(-6)\ldots(-4-r+1)}{r!}(-1)^r = \frac{4.5.6.\ldots.(r+3)}{r!} = \frac{(r+1)(r+2)(r+3)}{1.2.3}$. Therefore, the coefficient of z^r in $(z+z^2)(1-z)^{-4}$ is $\frac{(r)(r+1)(r+2)}{1.2.3} + \frac{(r-1)(r)(r+1)}{1.2.3} = \frac{r(r+1)(2r+1)}{6}$, which is the sum of the first r squares.

Fibonacci Numbers

Fibonacci numbers are defined as follows: $F_0 = 0$, $F_1 = 1$; for all $i \geq 0$, $F_{i+2} = F_{i+1} + F_i$. That is, $\langle 0, 1, 1, 2, 3, 5, 8, 13, 21, \ldots \rangle$ is the Fibonacci sequence.

$F(z) = 0 + 1z + 1z^2 + 2z^3 + 3z^4 + 5z^5 \ldots$ is its generating function. Then,

$zF(z) = 0 + 0z + 1z^2 + 1z^3 + 2z^4 + 3z^5 + 5z^6 \ldots$ and

$z^2 F(z) = 0 + 0z + 0z^2 + 1z^3 + 1z^4 + 2z^5 + 3z^6 + 5z^7 \ldots$.

Clearly, $(1 - z - z^2)F(z) = z$, and therefore, $F(z) = \frac{z}{1-z-z^2}$.

But then $F(z) = \frac{z}{(1-\phi_1 z)(1-\phi_2 z)}$, where $\phi_1 = (1+\sqrt{5})/2$ and $\phi_1 = (1-\sqrt{5})/2$.
That is, $F(z) = \frac{1/\sqrt{5}}{(1-\phi_1 z)} - \frac{1/\sqrt{5}}{(1-\phi_2 z)}$.
Therefore, $F_i = \frac{\phi_1^i}{\sqrt{5}} - \frac{\phi_2^i}{\sqrt{5}}$.

Theorem 53 *(Cassini's Theorem) For $n > 0$, $F_{n+1}F_{n-1} - F_n^2 = (-1)^n$.*

Proof: The proof is by induction on n. Basis: $F_2F_0 - F_1^2 = 1 * 0 - 1 = -1 = (-1)^1$.

Step: $F_{n+2}F_n - F_{n+1}^2 = (F_{n+1} + F_n)F_n - (F_n + F_{n-1})F_{n+1} = F_n^2 - F_{n-1}F_{n+1}$, which is the negative of $(-1)^n$, by the hypothesis. □

Lecture 22: 18 Oct 2014

Linear recurrences with constant coefficients

Some sequences can be represented using recurrence relations. A recurrence relation of the form

$$c_0 a_r + c_1 a_{r-1} + \ldots + c_{k-1} a_{r-k+1} + c_k a_{r-k} = f(r) \tag{58}$$

is called a linear recurrence with constant coefficients (LRCC) if each c_i is a constant. It is of the k-th order, if $c_0, c_k \neq 0$. Examples are $3a_r + 2a_{r-1} = r^2$ (of the first order), $7a_r - a_{r-2} = 3$ (of the second order).

Consider $3a_r - 5a_{r-1} + 2a_{r-2} = r^2 + 5$, an LRCC of the second order. If $a_3 = 0$ and $a_4 = 1$, then $a_5 = 35/5$, $a_6 = 292/9$, $a_2 = 9$, $a_1 = 59/2$. Every member of the sequence can be computed in this manner. If $a_3 = 4$ and $a_4 = 6$, then $a_5 = 18$, $a_6 = 119/3$, $a_2 = 9$, $a_1 = 25$.

In general, an LRCC can represent many sequences. But if an LRCC is given with k consecutive members of the sequence, then the rest of the sequence is uniquely defined. Note that less than k will not do. The k consecutive members form a valid boundary condition.

Let $\langle a_r = p_r \rangle$ be a particular solution of Eq. 58. Any solution $\langle a_r = h_r \rangle$ of the corresponding homogeneous-LRCC

$$c_0 a_r + c_1 a_{r-1} + \ldots + c_{k-1} a_{r-k+1} + c_k a_{r-k} = 0 \tag{59}$$

is called a homogeneous solution of the given LRCC (Eq. 58). Then $\langle a_r = p_r + h_r \rangle$ also is a solution of Eq. 58.

A homogeneous-LRCC, when it has a solution, has a solution of the form $\langle a_r = A\alpha^r \rangle$. Then

$$c_0 \alpha^r + c_1 \alpha^{r-1} + \ldots + c_{k-1} \alpha^{r-k+1} + c_k \alpha^{r-k} = 0 \tag{60}$$

That is,

$$c_0 \alpha^k + c_1 \alpha^{k-1} + \ldots + c_{k-1} \alpha + c_k = 0 \tag{61}$$

This is the characteristic equation of the LRCC. Suppose α_1 is a root of the characteristic equation; Then $\langle a_r = A_1 \alpha_1^r \rangle$, for any constant A_1, is indeed a solution of the homogeneous-LRCC.

If α_1 is a root of multiplicity > 1, then it is a root of Eq.60 and its first derivative equation

$$c_0 r\alpha^{r-1} + c_1 (r-1)\alpha^{r-2} + \ldots + c_{k-1}(r-k+1)\alpha^{r-k} + c_k (r-k)\alpha^{r-k-1} = 0$$

as well. Multiplying both sides by $A_2\alpha$,

$$c_0 A_2 r\alpha^r + c_1 A_2 (r-1)\alpha^{r-1} + \ldots + c_{k-1} A_2 (r-k+1)\alpha^{r-k+1} + c_k A_2 (r-k)\alpha^{r-k} = 0$$

That is, $\langle a_r = A_2 r \alpha_1^r \rangle$, for any constant A_2, also is a solution of the homogeneous-LRCC.

Continuing like this, we find that if α_1 is a root of multiplicity $> m-1$, then $\langle a_r = A_m r^{m-1} \alpha_1^r \rangle$, for any constant A_m, also is a solution of the homogeneous-LRCC.

Putting them together, $\langle a_r = (A_1 + A_2 r + \ldots + A_m r^{m-1})\alpha_1^r \rangle$ is a solution of the homogeneous-LRCC, when α_1 is a characteristic root of multiplicity m.

For example, if the characteristic equation is $4\alpha^3 - 20\alpha^2 + 17\alpha - 4 = 0$, then the characteristic roots are 0.5, 0.5 and 4. Therefore, $\langle a_r = (A_1 + A_2 r)(1/2)^r + A_3(4)^r \rangle$ is a homogeneous solution, for every A_1, A_2 and A_3.

Particular Solution

There is no general method for finding a particular solution. However, when $f(r)$ takes certain forms, we know what to do.

(i) If $f(r)$ is a polynomial of degree t then so is the particular solution.

(ii) When β is NOT a characteristic root, if $f(r)$ is a polynomial of degree t multiplied by β^r, then so is the particular solution.

(iii) When β is a characteristic root of multiplicity $m \geq 1$, if $f(r)$ is a polynomial of degree t multiplied by β^r, then the particular solution is a polynomial of degree t multiplied by $\beta^r r^m$.

Example 1: $a_r + 5a_{r-1} + 6a_{r-2} = 3r^2$. $f(r)$ is a polynomial of degree 2. So is the particular solution. Say the PS is $p_0 r^2 + p_1 r + p_2$.

Substituting in the recurrence, and equating the coefficients, $12p_0 = 3$, $34p_0 - 12p_1 = 0$, $29p_0 - 17p_1 + 12p_2 = 0$

Solving for the unknowns we find $p_0 = 1/4$, $p_1 = 17/24$, $p_2 = 115/288$.

So the PS is $r^2/4 + 17r/24 + 115/288$.

Example 2: $a_r + 5a_{r-1} + 6a_{r-2} = 42.4^2$. The characteric equation is $\alpha^2 + 5\alpha + 6 = 0$. The characteristic roots are -2 and -3. $f(r)$ is a polynomial of degree 0 multiplied by 4^r. So is the PS. It's of the form $p.4^r$.

Substituting in the recurrence, $p = 16$. So the PS is 16.4^r.

Example 3: $a_r - 2a_{r-1} = 3.2^r$. The characteric equation is $\alpha - 2 = 0$. 2 is a characteristic root of multiplicity 1. $f(r)$ is a polynomial of degree 0 multiplied by 2^r. So, the PS is a polynomial of degree 0 multiplied by $2^r.r$. That is, the PS is of the form $pr.2^r$.

Substituting in the recurrence, $p = 3$. So the PS is $3r.2^r$.

The total solution

The total solution of Eq.58 is obtained by adding the homogeneous solution and the particular solution. This has k unknowns, namely $A_1, \ldots, A_k$. Apply the boundary condition to obtain k linear equations in these k unknowns. Solve them to find the solution we seek.

Example 1: $a_r + 5a_{r-1} + 6a_{r-2} = 3r^2$; $a_0 = 0$, $a_1 = 1$. $A_1(-2)^r + A_2(-3)^r + r^2/4 + 17r/24 + 115/288$ is the total solution. Using the boundary conditions, we get two equations:

$A_1 + A_2 = -115/288$

$2A_1 + 3A_2 = 103/288$

Solving them, $A_1 = 37/32$ and $A_2 = -14/9$.

That is, the solution of the recurrence relation is: $-14(-2)^r/9 + 37(-3)^r/32 + r^2/4 + 17r/24 + 115/288$

Lecture 23: 30 Oct 2014

Harmonic numbers

For $n \geq 0$, the n-th harmonic number H_n is defined as follows:

$$H_n = \sum_{k=1}^{n} \frac{1}{k}$$

That is $H_0 = 0$, $H_1 = 1$, $H_2 = 1.5$, $H_3 = 1.8333$, $H_4 = 2.08333$, $H_5 = 2.28333$, etc. H_n can be expressed as:

$$H_n = 1 + \frac{1}{2} + \left(\frac{1}{3} + \frac{1}{4}\right) + \left(\frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8}\right) + \left(\frac{1}{9} + \frac{1}{10} + \frac{1}{11} + \frac{1}{12} + \frac{1}{13} + \frac{1}{14} + \frac{1}{15} + \frac{1}{16}\right) + \ldots + \left(\ldots + \frac{1}{n}\right)$$

Each group from the third has twice the number of terms as the previous one. Thus, each group, except the first and possibly the last, sums to strictly between 1/2 and 1. Here $1/n$ falls in group number $\lceil \log n \rceil$. That is, H_n is $> \lceil \log n \rceil / 2$ and $< \lceil \log n \rceil$.

A closer estimation is obtained as follows:

$$H_n - 1 < \int_1^n \frac{1}{x} dx = [\ln x]_1^n = \ln n = (\log n)/1.443 < H_n$$

That is, $\ln n < H_n < \ln n + 1$, for $n > 1$.

See Concrete Mathematics, Graham, Knuth and Patashnik.

For $n \geq 0$, the n-th 2-nd-order harmonic number $H_n^{(2)}$ is defined as follows:

$$H_n^{(2)} = \sum_{k=1}^{n} \frac{1}{k^2}$$

As $n \to \infty$, $H_n^{(2)} \to \zeta(2) = \pi^2/6 = 1.6449$.

For $n \geq 0$, the n-th 3-rd-order harmonic number $H_n^{(3)}$ is defined as follows:

$$H_n^{(3)} = \sum_{k=1}^{n} \frac{1}{k^3}$$

As $n \to \infty$, $H_n^{(3)} \to \zeta(3) = 1.20205$.

In general, for $r > 1$, for $n \geq 0$, the n-th r-th-order harmonic number $H_n^{(r)}$ is defined as follows:

$$H_n^{(r)} = \sum_{k=1}^{n} \frac{1}{k^r}$$

As $n \to \infty$, $H_n^{(r)} \to \zeta(r)$.

Consider

$$\ln\left(\frac{k}{k-1}\right) = \frac{1}{k} + \frac{1}{2k^2} + \frac{1}{3k^3} + \frac{1}{4k^4} + \ldots$$

Summing both sides for $2 \le k \le k$,

$$\ln n - \ln 1 = (H_n - 1) + (H_n^{(2)} - 1)/2 + (H_n^{(3)} - 1)/3 + (H_n^{(4)} - 1)/4 + \ldots$$

From this we get

$$H_n - \ln n = 1 - (H_n^{(2)} - 1)/2 - (H_n^{(3)} - 1)/3 - (H_n^{(4)} - 1)/4 + \ldots$$

When $n \to \infty$, the RHS tends to

$$1 - (\zeta(2) - 1)/2 - (\zeta(3) - 1)/3 - (\zeta(4) - 1)/4 + \ldots$$

which is called Euler's constant γ and can be shown to be approximately 0.577215665. That is, for large n, H_n is about $\ln n + 0.58$.

Stirling numbers of the second kind

$\left\{ {n \atop k} \right\}$ is the number of ways to partition a set of n items into k nonempty subsets.

For $n > 0$, $\left\{ {n \atop n} \right\} = 1$ because each nonempty subset must be a singleton in this case. The convention is to set $\left\{ {0 \atop 0} \right\} = 1$. For $n > 0$, $\left\{ {n \atop 0} \right\} = 0$. For $n > 0$, $\left\{ {n \atop 1} \right\} = 1$ because there is only one way to partition a set of n items into one nonempty subset.

Given $n > 0$ items, keep one of them, say x, aside. Suppose $1 < k < n$. (i) Partitioning of the $n-1$ items other than x into k nonempty subsets can be done in $\left\{ {n-1 \atop k} \right\}$ ways. Given one of those partitions, there are k subsets to choose to put x in. Note that the subset that ends up containing x is not a singleton. (ii) Put x in a subset on its own; this is a singleton subset. Partitioning of the remaining $n-1$ into $k-1$ nonempty subsets can be done in $\left\{ {n-1 \atop k-1} \right\}$ ways. Hence,

$$\left\{ {n \atop k} \right\} = k * \left\{ {n-1 \atop k} \right\} + \left\{ {n-1 \atop k-1} \right\}$$

Stirling numbers of the first kind

$\left[{n \atop k} \right]$ is the number of ways to arrange a set of n items into k nonempty cycles. In other words, we are given n distiguishable beads, and are required to make k garlands out of them; $\left[{n \atop k} \right]$ is the number of ways to do this.

For $n > 0$, $\left[{n \atop n} \right] = 1$ because each cycle has one item in this case. The convention is to set $\left[{0 \atop 0} \right] = 1$. For $n > 0$, $\left[{n \atop 0} \right] = 0$. For $n > 0$, $\left[{n \atop 1} \right] = n!/n = (n-1)!$ because n items can be permuted in $n!$ ways, each permutation when its ends are stuck together becomes a cycle, and for any permutation, all its cyclic shifts produce the same cycle.

Given $n > 0$ items, keep one of them, say x, aside. Suppose $1 < k < n$. (i) Partitioning of the $n-1$ items other than x into k cycles can be done in $\left[{n-1 \atop k} \right]$ ways. Given one of those partitions, there are k cycles to choose to put x in. If the cycle chosen has r elements in it, then x has r places to choose; it can be inserted between any two consecutive items in the cycle. Note that the cycle that ends up containing x is not a singleton. (ii) Put x in a cycle

on its own; this is a singleton cycle. Partitioning of the remaining $n-1$ into $k-1$ cycles can be done in $\begin{bmatrix} n-1 \\ k-1 \end{bmatrix}$ ways. Hence,

$$\begin{bmatrix} n \\ k \end{bmatrix} = (n-1) * \begin{bmatrix} n-1 \\ k \end{bmatrix} + \begin{bmatrix} n-1 \\ k-1 \end{bmatrix}$$

Lecture 24: 31 Oct 2014

Set Theory

A set is a collection of objects called its members. A set itself is an object and can be member of sets. Let "$a \in A$" denote "a is a member of A". Let "$a \notin A$" denote its negation.

For any two sets A and B, if for every object x, $x \in A$ iff $x \in B$, then $A = B$. This is called the **Principle of Extensionality**. It asserts that sets are defined by their memberships.

There is a set with no member. This is called the empty set and is denoted $\varnothing$. Note that $\varnothing \notin \{\varnothing\}$ because $\varnothing$ has no member, while $\{\varnothing\}$ has one member — namely, $\varnothing$.

If every member of A is also a member of B, then A is a subset of B ($A \subseteq B$), and B is a superset of A ($B \supseteq A$). $\varnothing$ is a subset of every set. If $A \subseteq B$ and $A \neq B$, then $A \subset B$.

The union $A \cup B$ of sets A and B: $x \in A \cup B$ iff $x \in A$ or $x \in B$.

The intersection $A \cap B$ of sets A and B: $x \in A \cap B$ iff $x \in A$ and $x \in B$.

The relative complement $U - A$ of set A in U: $x \in U - A$ iff $x \in U$ and $x \notin A$.

A set can be deemed a predicate on/property of objects. In this sense, $x \in A$ iff x has property A.

Suppose we need to deal only with the members and subsets of some universal set U. Then $A \cup B$ is the $\vee$ of properties A and B; $A \cap B$ is the $\wedge$ of properties A and B; $U - A$ is the $\neg$ of property A. It is easy to see that the algebra of sets is boolean. Thus the following laws hold.

Identity laws: $A \cap U = A$; $A \cup \varnothing = A$
Domination laws: $A \cup U = U$; $A \cap \varnothing = \varnothing$
Idempotent laws: $A \cup A = A$; $A \cap A = A$
Double negation law: $U - (U - A) = A$
Commutative laws: $A \cup B = B \cup A$; $A \cap B = q \cap A$
Associative laws: $(A \cup B) \cup C = A \cup (B \cup C)$; $(A \cap B) \cap C = A \cap (B \cap C)$
Distributive laws: $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$; $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
De Morgans laws: $U - (A \cap B) = (U - A) \cup (U - B)$; $U - (A \cup B) = (U - A) \cap (U - B)$
Absorption laws: $A \cup (A \cap B) = A$; $A \cap (A \cup B) = A$
Negation laws: $A \cup (U - A) = U$; $A \cap (U - A) = \varnothing$

The set of all subsets of A is the power set of A, denote 2^A. If A is finite, and has $|A| = n$ members, then $|2^A| = 2^n$.

Sets can be defined using abstractions. If $\alpha(x)$ is a one argument predicate, then $\{x \mid \alpha(x)\}$ is the set of objects x that satisfy $\alpha(x)$.

A set A may contain sets, along with other objects, as its members. $\bigcup A$ is defined as $\{x \mid \exists b(b \in A \wedge x \in b)\}$. For example, $\bigcup\{\{2,3\},4,\{5\}\} = \{2,3,5\}$. $x \in \bigcup A$ iff x is a member of a member of A.

$\bigcap A$ is defined as $\{x \mid \forall b(b \in A \rightarrow x \in b)\}$. $\bigcap \varnothing$ is undefined.

Embedding of Peano's system in Set Theory

Suppose that for each set a, the successor a^+ is defined as $a \cup \{a\}$. We say that a set A is inductive iff $\varnothing \in A$ and $\forall a(a \in A \rightarrow a^+ \in A)$ (that is, A is closed under the successor operator).

Define ω as $\bigcap\{A \mid A \text{ is inductive}\}$. That is, $x \in \omega$ iff x belongs to every inductive set.

Theorem 54 *ω is inductive. ω is a subset of every inductive set.*

Proof: $x \in \omega$ iff x belongs to every inductive set. Hence ω is a subset of every inductive set.

$\varnothing$ belongs to every inductive set. So, $\varnothing \in \omega$.

If $x \in \omega$, then x belongs to every inductive set, and therefore, by the closure property of inductive sets, x^+ belongs to every inductive set, which is iff $x^+ \in \omega$. That is, ω is closed under the successor operator.

Thus, ω is inductive. □

If $a \subseteq \omega$ is inductive, then $\omega \subseteq a$; that is, $a = \omega$. That means, no proper subset of ω is inductive.

Definition 11 $0 = \varnothing$, $1 = 0^+$, $2 = 1^+$, $3 = 2^+$, $4 = 3^+$, *etc.*

Then $0 = \varnothing$, $1 = \varnothing^+$, $2 = \varnothing^{++}$, $3 = \varnothing^{+++}$, $4 = \varnothing^{++++}$ etc. That is,
$1 = \varnothing \cup \{\varnothing\} = \{\varnothing\}$
$2 = \{\varnothing\} \cup \{\{\varnothing\}\} = \{\varnothing, \{\varnothing\}\}$
$3 = \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\}$
Note that $0 \in 1 \in 2 \in 3 \in \ldots$ and $0 \subset 1 \subset 2 \subset 3 \subset \ldots$

ω is the "smallest" inductive set containing 0. Let the set of natural numbers $\mathbb{N} = \omega$.

Suppose we want to show that a one variable predicate $\alpha(n)$ is true for every natural number n.

Let $T = \{n \in \mathbb{N} \mid \alpha(n)\}$.

Prove that T is inductive, and that $0 \in T$. Then $T = \mathbb{N}$.

For example, to show that every natural number except 0 is the successor of a natural number, let $T = \{n \in \mathbb{N} \mid n = 0 \text{ or } \exists p \in \mathbb{N}(n = p^+)\}$.

$0 \in T$. If $p \in T$, then $n = p^+ \in T$. So $T = \mathbb{N}$. Hence the proof.

Lecture 25: 1 Nov 2014

For any two objects x and y, there is a unique set that contains exactly these two: $\{x, y\}$. Such a set is called an unordered pair. Note that when $x = y$, this is a singleton set.

An ordered pair (x, y) can be defined as the set $\{x, \{x, y\}\}$. It has two members. One of them is a member of the other; that one is the first component of the ordered pair.

A relation is a set of ordered pairs. For a relation R, the domain of R (denoted dom R) is defined as follows: $x \in \text{dom } R$ iff $\exists y(\langle x, y\rangle \in R)$. The range of R (denoted ran R): $x \in \text{ran } R$ iff $\exists y(\langle y, x\rangle \in R)$. The field of R is the union of the domain and range of R: fld $R = \text{dom } R \cup \text{ran } R$.

$A \times B$ is the set of all ordered pairs with the first component from A and the second component from B. R is a relation from A to B, if $R \subseteq A \times B$. A binary relation on A is a subset of $A \times A$. An n-tuple is an ordered sequence of n objects. An n-tuple on set A can be thought of as an ordered pair, the first component of which is an $(n-1)$-tuple on A and the second component is a member of A. For example, $(x, y, z) = ((x, y), z)$. An n-ary relation is a set of n-tuples. Notation: $A^2 = A \times A$, $A^3 = A^2 \times A$, and so on. An n-ary relation on A is a subset of A^n, and hence, a relation from A^{n-1} to A.

If $(x, y) \in R$, then we write xRy.

A function F is a relation such that $(\forall x \in \text{dom } F)\exists! y(xFy)$. For $x \in \text{dom } F$, let $F(x)$ denote the unique y such that xFy. That is, $(x, F(x)) \in F$. We say that function F maps A **into** B, if dom $F = A$ and ran $F \subseteq B$, and that function F maps A **onto** B, if dom $F = A$ and ran $F = B$

A set R is single-rooted iff for each $y \in \text{ran } R$, $\exists! x(xRy)$. Note that even a non-relation can be called single-rooted. For example, $\{(2, 0), (2, 1), c\}$ is single-rooted. A function F is one-to-one iff it is single-rooted.

A bijection is a function that is one-to-one and onto. An injection is a function that is one-to-one and into, but need not be onto. A surjection is a function that is onto. A function is a bijection iff it is an injection and a surjection.

For any **sets** F, G, we define the inverse of F as $F^{-1} = \{(u, v) \mid vFu\}$, the composition of F and G as $F \circ G = \{(u, v) \mid \exists t(uGt \wedge tFv)\}$, the resitriction of F to A as $F \upharpoonright A = \{(u, v) \mid uFv \wedge u \in A\}$, the image of A under F as $F[[A]] = \text{ran } (F \upharpoonright A) = \{v \mid \exists u \in A(uFv)\}$.

Theorem 55 *(i) For a set F, dom F^{-1} = ran F and ran F^{-1} = dom F. (ii) For a relation F, $(F^{-1})^{-1} = F$. (iii) For a set F, F^{-1} is a function iff F is single-rooted. (iv) A relation F is a function iff F^{-1} is single-rooted. (v) Assume that F is a one-to-one function. If $x \in$ dom F, then $F^{-1}(F(x)) = x$. If $y \in$ ran F, then $F(F^{-1}(y)) = y$. (vi) F and G are functions. $F \circ G$ is a function. Its domain is $\{x \in \text{dom } G \mid G(x) \in \text{dom } F\}$. For $x \in$ dom $F \circ G$, $(F \circ G)(x) = F(G(x))$. (vii) For any two sets F and F, $(F \circ G)^{-1} = G^{-1} \circ F^{-1}$.*

Proof: Exercise.

Lecture 26: 12 Nov 2014

A relation R on set A is called reflexive on A, if xRx for all $x \in A$. R is symmetric on A, if for every $x, y \in A$, xRy implies yRx. R is transitive on A, if for every $x, y, z \in A$, xRy and yRz imply xRz.

A binary relation R on set A is an equivalence relation, iff R is reflexive, symmetric and transitive on A. For an equivalence relation R, x and y are said to be in the same equivalence class iff xRy. In other words, an equivalence class of R on set A is a maximal subset of A such that any two members of it are in raltion R to each other. The equivalence class that contains $x \in A$ is denoted $[x]_R$. Thus, $[x]_R = \{t \mid xRt\}$. The quotient A/R of A under R is the set of equivalence classes $\{[x]_R \mid x \in A\}$.

A binary relation R on set A is a linear (total) ordering iff R is transitive on A and satisfies trichotomy. (R satisfies trichotomy on A iff for every x and y in A, exactly one of xRy, $x = y$, yRx holds.) For example, $<, >$ are linear orderings on $\mathbb{N}$.

Embedding of integers in set theory

Define a relation $\sim$ on $\mathbb{N} \times \mathbb{N}$ as follows: $(m, n) \sim (p, q)$ iff $m + q = n + p$. (We avoid using subtraction because $\mathbb{N}$ is not closed under subtraction.)

Theorem 56 *$\sim$ is an equivalence relation on $\mathbb{N} \times \mathbb{N}$.*

Definition 12 $\mathbb{Z} = (\mathbb{N} \times \mathbb{N})/\sim$

$2_Z = [(2,0)]_\sim = \{(2,0), (3,1), (4,2), \ldots\}$.
$-3_Z = [(0,3)]_\sim = \{(0,3), (1,4), (2,5), \ldots\}$.

Imagine the integral grid points on the real plane. Each line of slope one that passes through an integral point on the y-axis represents an equivalence class. For example, 2_Z corresponds to the line $x - y = 2$, and -3_Z corresponds to the line $x - y = -3$.

Theorem 57 *If $(m, n) \sim (m', n')$ and $(p, q) \sim (p', q')$, then $(m + p, n + q) \sim (m' + p', n' + q')$.*

Definition 13 *Addition ($+_Z$) of integers is defined as follows:* $[(m, n)]_\sim +_Z [(p, q)]_\sim = [(m + p, n + q)]_\sim$

Theorem 58 *$+_Z$ is commutative and associative on $\mathbb{Z}$. 0_Z is the identity of $+_Z$. Each integer has an additive inverse. In short, $(\mathbb{Z}, +_Z)$ is an Abelian group.*

Definition 14 *Multiplication ($*_Z$) of integers is defined as follows:* $[(m, n)]_\sim *_Z [(p, q)]_\sim = [(mp + nq, mq + np)]_\sim$

Theorem 59 *$*_Z$ is commutative and associative on $\mathbb{Z}$. It distributes over $+_Z$. 1_Z is the identity of $*_Z$. $0_Z \neq 1_Z$. Whenever $a *_Z b = 0$, either $a = 0_Z$ or $b = 0_Z$. In short, $(\mathbb{Z}, +_Z, *_Z, 0_Z, 1_Z)$ is an integral domain.*

Definition 15 *The less-than relation ($<_Z$) on integers is defined as follows:* $[(m,n)]_\sim <_Z [(p,q)]_\sim = m+q \in p+n$

Theorem 60 $<_Z$ *is a linear ordering on* $\mathbb{Z}$.

Note that $\mathbb{N}$ is not a subset of $\mathbb{Z}$, the way we have defined them. But if we define $\mathbb{N}_Z = \{[(n,0)]_\sim \mid n \in \mathbb{N}\}$, then $(\mathbb{N}_Z, +_Z, *_Z, 0_Z, 1_Z)$ is isomorphic to $(\mathbb{N}, +, *, 0, 1)$.

Definition 16 *A set S is countable iff there exists a one-to-mapping from S into* $\mathbb{N}$.

Theorem 61 $\mathbb{Z}$ *is countable.*

Proof: Integers can be counted in this order: $0, -1, 1, -2, 2, \ldots$

Embedding of rational numbers in set theory

Let $\mathbb{Z}' = \mathbb{Z} - \{0\}$. Define a relation $\bowtie$ on $\mathbb{Z} \times \mathbb{Z}'$ as follows: $(a,b) \bowtie (c,d)$ iff $ad = bc$. (We avoid using division because $\mathbb{Z}$ is not closed under division.)

Theorem 62 $\bowtie$ *is an equivalence relation on* $\mathbb{Z} \times \mathbb{Z}'$.

Definition 17 *The set of rational numbers* $\mathbb{Q} = (\mathbb{Z} \times \mathbb{Z}')/\bowtie$

$2_Q = [(2,1)]_\bowtie = \{(2,1), (-2,-1), (4,2), (-4,-2), (6,3), \ldots\}$.
$-\frac{1}{3}_Q = [(-1,3)]_\bowtie = \{(-1,3), (1,-3), (-2,6), (2,-6), (-3,9), \ldots\}$.
Imagine the integral grid points on the real plane. Each line that passes through the origin and some one grid point not on the x-axis represents an equivalence class. For example, 2_Q corresponds to the line $x/y = 2$, and $-\frac{1}{3}_Q$ corresponds to the line $x/y = -1/3$.

Definition 18 *Addition ($+_Q$) of rational numbers is defined as follows:* $[(a,b)]_\bowtie +_Q [(c,d)]_\bowtie = [(ad+cb, bd)]_\bowtie$

Theorem 63 $+_Q$ *is commutative and associative on* $\mathbb{Q}$. 0_Q *is the identity of* $+_Q$. *Each rational number has an additive inverse. In short,* $(\mathbb{Q}, +_Q)$ *is an Abelian group.*

Definition 19 *Multiplication ($*_Q$) of rational numbers is defined as follows:* $[(a,b)]_\bowtie *_Q [(c,d)]_\bowtie = [(ac, bd)]_\bowtie$

Theorem 64 $*_Q$ *is commutative and associative on* $\mathbb{Q}$. *It distributes over* $+_Q$. 1_Q *is the identity of* $*_Q$. $0_Q \neq 1_Q$. *Whenever* $a *_Q b = 0$, *either* $a = 0_Q$ *or* $b = 0_Q$. *Every non-zero rational number has a reciprocal. In short,* $(\mathbb{Q}, +_Q, *_Q, 0_Q, 1_Q)$ *is a field.*

Definition 20 *The less-than relation ($<_Q$) on rational numbers is defined as follows:* $[(a,b)]_\bowtie <_Q [(c,d)]_\bowtie = ad < bc$

Theorem 65 $<_Q$ *is a linear ordering on* $\mathbb{Q}$.

Note that $\mathbb{Z}$ is not a subset of $\mathbb{Q}$, the way we have defined them. But if we define $\mathbb{Z}_Q = \{[(n,1)]_\bowtie \mid n \in \mathbb{Z}\}$, then $(\mathbb{Z}_Q, +_Q, *_Q, 0_Q, 1_Q)$ is isomorphic to $(\mathbb{Z}, +_Z, *_Z, 0_Z, 1_Z)$.

Theorem 66 *$\mathbb{Q}$ is countable.*

Proof: Enumerate the members of $\mathbb{N} \times \mathbb{N}$ in the following manner:

$$(0,0),(0,1),(1,0),(2,0),(1,1),(0,2),(0,3),(1,2),\ldots$$

The algorithm is to enumerate the ordered pairs in the sorted order of the sum of the two components. This can be generalized into an enumeration of $\mathbb{Z} \times \mathbb{Z}'$. From this if we filter out the ordered pairs in which the two components have common factors, we have an enumeration of $\mathbb{Q}$. □

Theorem 67 *$\sqrt{2}$ is not a rational number.*

Proof: Assume the contrary. Let $\sqrt{2} = a/b$, where $\text{GCD}(a,b) = 1$. Then $2b^2 = a^2$. That is a^2 is an even square. So a is even. Let $a = 2k$. Hence, $2b^2 = 4k^2$, and so $b^2 = 2k^2$. That is, b^2 is an even square as well. So b is even. That is $\text{GCD}(a,b) \geq 2$. Contradiction. □

Embedding of real numbers in set theory

Definition 21 *A Dedekind cut is a subset x of $\mathbb{Q}$ such that (i) $\varnothing \neq x \neq \mathbb{Q}$; (ii) x is closed downwards; that is, $(q \in x) \wedge (r < q) \rightarrow (r \in x)$; (iii) x has no largest member.*

Definition 22 *The set of real numbers $\mathbb{R}$ is the set of all Dedekind cuts.*

Each real number r is thus equated to the set of all rational numbers less than r. For example, the set of all rational numbers less than 2 is not empty, does not contain all rational numbers, is closed downwards, and has no largest member. To see the last, consider the infinite sequence $1.9, 1.99, 1.999, 1.9999, \ldots$ that tends to 2.

Theorem 68 *Every real number has a decimal representation.*

Theorem 69 *$\mathbb{R}$ is not countable.*

Proof: Suppose the set of real numbers in $(0,1)$ is countable. Then each real number in $(0,1)$ maps to a unique natural number, called, say, its count. Imagine an enumeration of real numbers, using their counts, in this manner:

1 $0.a_1a_2a_3a_4a_5a_6\ldots$
2 $0.b_1b_2b_3b_4b_5b_6\ldots$
3 $0.c_1c_2c_3c_4c_5c_6\ldots$
4 $0.d_1d_2d_3d_4d_5d_6\ldots$

Form a real number $r = 0.a'_1b'_2c'_3d'_4\ldots$ where $x' = (x+1) \mod 10$. r differs from the i-th real number in the i-th decimal place. So r is not in the enumeration. That is, the enumeration is not exhaustive. Contradiction.

If the set of real numbers in $(0,1)$ is uncountable, so would be its superset $\mathbb{R}$. □

Definition 23 *The less-than relation ($<_R$) on real numbers is defined as follows: $r <_R s$ iff $r \subset s$*

Theorem 70 *$<_R$ is a linear ordering on $\mathbb{R}$.*

Definition 24 *Addition ($+_R$) of real numbers is defined as follows: $x +_R y = \{q + r \mid (q \in x) \wedge (r \in y)\}$*

Definition 25 *Multiplication ($*_R$) of real numbers is defined as follows:*
(i) if x and y are nonnegative real numbers, then $x *_R y = \{qr \mid (0 \leq q \in x) \wedge (0 \leq r \in y)\}$
(ii) if x and y are both negative real numbers, then $x *_R y = |x| *_R |y|$
(ii) if exactly one of x and y is negative, then $x *_R y = -|x| *_R |y|$

Theorem 71 *$(\mathbb{R}, +_R, *_R, 0_R, 1_R)$ is a field.*

Lecture 27: 13 Nov 2014

A set can be defined using an abstraction as in $\{x \mid \alpha(x)\}$, where $\alpha(.)$ is a property that x must satisfy in order to be in the set. An infinite set can be defined only with an abstraction.

If the abstraction is not specified precisely enough, the definition can lead to paradoxes. Consider the set $A = \{x \mid x$ is a natural number that can be defined in at most 100 characters$\}$. On any finite alphabet, there are only a finite number of strings of length at most 100. Therefore, there exists n, "the least natural number that cannot be defined in at most 100 characters". But then that is the definition of n in at most 100 characters. So, $n \in A$ and $n \notin A$.

To avoid this paradox, it is enough to specify the abstraction using a logical formula. But even with a "well-defined" abstraction $B = \{x \mid x \notin x\}$ is paradoxical. If $B \in B$, then $B \notin B$. If $B \notin B$, then $B \in B$.

This sort of pitfalls can be avoided if we agree that some collections of sets are not sets. (Examples are the set of all sets, and the set B above.) This is the approach taken by Zermelo-Fraenkel axiomatization of Set Theory.

The following are the axioms of the Zermelo-Fraenkel system.

Extensionality Axiom. If two sets have exactly the same members, then they are equal: $\forall x \forall y(\forall z(z \in x \leftrightarrow z \in y) \rightarrow x = y)$.

Empty Set Axiom. There is a set with no members: $\exists x \forall y(y \notin x)$.

Pairing Axiom. For any two sets, there is a set with exactly these two as members: $\forall x \forall y \exists z \forall u(u \in z \leftrightarrow u = x \vee u = y)$.

Power Set Axiom. For any set x, there is a set whose members are exactly the subsets of x: $\forall x \exists y \forall z(z \in y \leftrightarrow z \subseteq x)$.

Subset Axioms. (Axiom schema.) For each formula α with k free variable such that x is not free in α, the following is an axiom: $\forall t_1 \ldots \forall t_k \forall u \exists x \forall y(y \in x \leftrightarrow x \in u \wedge \alpha(t_1, \ldots, t_k))$.

For example, $\forall t \forall u \exists x \forall y(y \in x \leftrightarrow y \in t \wedge y \in u)$: there exists the intersection of t and u. Also, $\forall t \forall u \exists x \forall y(y \in x \leftrightarrow y \notin t \wedge y \in u)$: there exists a set that is the complement of t relative to u.

Union Axiom. For any set x, there exists a set y whose members are exactly the members of the members of x: $\forall x \exists y \forall z(z \in y \leftrightarrow \exists u(z \in u \wedge u \in x))$.

Axiom of Choice. For any relation R, there exists a function $F \subseteq R$ such that dom F = dom R.

Infinity Axiom. There exists an inductive set: $\exists x(\varnothing \in x \wedge \forall y(y \in x \rightarrow y^+ \in x))$.

Replacement Axioms. For any formula $\nu(x, y)$, in which z is not free, the following is an axiom: $\forall u[(\forall x \in u) \forall a \forall b(\nu(x, a) \wedge \nu(x, b) \rightarrow a = b) \rightarrow \exists z \forall y(y \in z \leftrightarrow (\exists x \in u)\nu(x, y))]$. In other words, if every member of u has a nominee, then there is a set that contains precisely the nominees of the members of u.

Regularity Axiom. Every nonempty set x has a member y with $x \cap y = \varnothing$.

Equinumerosity

We say that set A is equinumerous with set B ($A \approx B$) iff there exists a one-to-one mapping from A onto B.

We have seen that $\mathbb{N} \times \mathbb{N} \approx \mathbb{N}$ and $\mathbb{N} \approx \mathbb{N}_e$, where $\mathbb{N}_e$ is the set of even natural numbers.

It is easy to see that $(0,1) \approx \mathbb{R}$: Consider the real plane. Let O denote the origin. Bend the interval into a semi-circle about O that is below the x-axis. The semi-circle has a radius of $1/\pi$. Draw a tangent L to the semi-circle at $(0, -1/\pi)$. Every line segment that connects a point r on L to O intersects the semi-circle at a unique point $f(r)$. This mapping f is one-to-one and onto $(0,1)$.

Let ${}^AB$ denote the set of functions from A to B. Then 2^A, the power set of A, is equinumerous with ${}^A\{0,1\}$. This is because any function from A to $\{0,1\}$ is the characteristic function of a subset of A. But $\{0,1\} \approx 2$. So, ${}^A2 = 2^A$.

Theorem 72 $A \not\approx 2^A$

Proof: Let *own* be a mapping from A into 2^A. (Imagine that each member of A *own*s a subset of A.) Let $B = \{x \in A \mid x \notin own(x)\}$. ($B$ is the set of members of A that do not *own* themselves.) Then $B \subseteq A$. For each $x \in A$, $x \in B$ iff $x \notin own(x)$. For some $x \in A$, if $B = own(x)$, then $x \in B$ and $x \notin B$. Hence, $B \neq own(x)$ for any $x \in A$. That is *own* is not onto 2^A. □

Definition 26 *A set is finite iff it is equinumerous to a natural number.*

Theorem 73 *(Pigeonhole Principle) No natural number is equinumerous to a proper subset of itself.*

Corollary 8 *Any set equinumerous to a proper subset of itself is infinite.*

Lecture 28: 14 Nov 2014

For a finite set A, the unique natural number n that is equinumerous with n is called the cardinal number of A; card A, for short. For any two sets A and B (finite or infinite), card A = card B iff $A \approx B$. card $\mathbb{N}$ is denoted by $\aleph_0$.

cardinal arithmetic

If κ and λ are cardinal numbers, then (i) $\kappa + \lambda$ is the cardinal number of $K \cup L$, where K and L are two disjoint sets of cardinality κ and λ respectively; (ii) $\kappa.\lambda$ is the cardinal number of $K \times L$, where K and L are any two sets of cardinality κ and λ respectively; (iii) κ^λ is the cardinal number of ${}^L K$, where K and L are any two sets of cardinality κ and λ respectively.

We say that B dominates A ($A \preceq B$) iff there exists a one-to-one mapping from A into B, and that card $A \leq$ card B iff $A \preceq B$. Thus a set A is countable iff $A \preceq \mathbb{N}$; that is, card $A \leq \aleph_0$.

Theorem 74 *(Schröder-Bernstein Theorem) If $A \preceq B$ and $B \preceq A$, then $A \approx B$. (In other words, If card $A \leq$ card B and card $B \leq$ card A, then card A = card B.)*

Theorem 75 *A countable union of countable sets is countable.*

Theorem 76 *For a cardinal number κ, $\kappa < \aleph_0$ iff κ is finite.*

Cantor conjectured that there is no set of cardinality between $\aleph_0$ and $2^{\aleph_0}$, where the latter is the cardinality of $\mathbb{R}$. This conjecture is called the continuum hypothesis. In 1939, Gödel showed that the continuum hypothesis cannot be disproved from the axioms of Set Theory. In 1963, Cohen showed that the continuum hypothesis cannot be proved from the axioms of Set Theory. That means that either the continuum hypothesis or its negation is a true but unprovable statement of Set Theory.

Consistency

Continuing the discussion on Peano's system from Lecture 14, let Con_S be the following wff

$\forall w \forall x \forall y \forall z \neg(proof(w, y) \wedge proof(x, z) \wedge neg(y, z))$ where $proof(w, y)$ is true iff w is the proof of y, and $neg(y, z)$ is true iff y is the negation of z. Con_S asserts that no two provable wffs can be negations of each other. In other words, Con_S asserts the consistency of S.

Gödel proved the following theorem:

Theorem 77 $\vdash_S (Con_S \rightarrow \gamma)$

Here γ is the Gödel's proposition, the wff that asserts, "I am not provable." The upshot is that S cannot prove its own consistency; that is, $\nvdash_S Con_S$. (Assume otherwise. Then Con_S is a theorem of S. By the above Theorem, $Con_S \rightarrow \gamma$ is also a theorem of S. So by MP, γ is also a theorem of S. But we have already seen that γ is not provable in S. Contradiction.)

Fine, we cannot prove the consistency of S in S; assume it as an axiom, what then? Say the resultant system is S'; by a similar argument we get that we cannot prove the consistency of S' in S'.

Consistency of S can be proved using higher mathematics. But an essentially similar argument can be carried out about Set Theory, deemed a foundational system for all mathematics, to show that Set Theory cannot prove its own consistency. It seems that we are saddled with a formal system that cannot prove its own consistency.