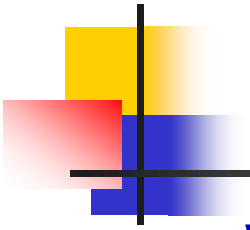
Normal Forms



- Well formed formula (wff) – also called formula, is a string consists of propositional variables, connectives, and parenthesis used in the proper manner. E.g. ((p $\vee$ q) $\wedge$ ($\neg$ p $\vee$ r))
- p$\vee$q$\vee\neg$r is a disjunction expression, and p$\wedge\neg$q $\wedge$ r is a conjunction expression.
- Product for conjunction, sum for disjunction.
- An elementary product (sum)is a product (sum) of the variables and their negations in a formula.
- An elementary sum is a disjunction of literals.

Disjunction/Conjunction Normal Form

- Disjunctive normal form (DNF) – a formula which is equivalent to a given formula and consists of a sum of elementary products
- E.g. $(p \rightarrow q) \wedge \neg q \equiv (\neg p \wedge \neg q) \vee (q \wedge \neg q)$ is in DNF.
- Conjunctive normal form (CNF) - a formula which is equivalent to a given formula and consists of a product of elementary sums
- E.g $(p \rightarrow q) \wedge \neg q \equiv (\neg p \vee q) \wedge \neg q$ is in CNF.

Sufficient and Necessary Condition

- A necessary and sufficient condition for an elementary product to be false – it contains at least one pair of literals in which one "is" the negation of the other.
- A necessary and sufficient condition for an elementary sum to be true – it contains at least one pair of liters in which one "is" the negation of the other.
- $p \wedge \neg p \wedge \ldots \equiv F \wedge \ldots = F$
- $p \vee \neg p \vee \ldots \equiv T \vee \ldots = T$

Fallacy or Tautology

- A given formula is identically false (a contradiction), if every elementary product appearing in its disjunctive normal form is identically false.
- A given formula in a given formula is identically true (a tautology), if every elementary sum appearing in the formula has at least two literals, of which one is the negation of the other.

Principal Disjunctive Normal Form

- Minterms of p and q – $p \wedge q$, $\neg p \wedge q$, $p \wedge \neg q$, $\neg p \wedge \neg q$

  each variable occurs either negated or nonnegated but not both occur together in the conjunction.
- Principal disjunctive normal form – for a given formula, an equivalent formula consisting of disjunctions of minterms only, also called sum of products normal form.
- $p \rightarrow q = \neg p \vee q = (p \wedge q) \vee (p \wedge \neg q) \vee (\neg p \wedge \neg q)$
- What is the principal disjunctive normal form for $(p \wedge q) \vee (\neg p \wedge r) \vee (q \wedge r)$? (see example 4)

Principal Conjunctive Normal Form

- Maxterms of p and q – $p \vee q$, $\neg p \vee q$, $p \vee \neg q$, $\neg p \vee \neg q$

  each variable occurs either negated or nonnegated but not both, appears only once.
- Principal disjunctive normal form – for a given formula, an equivalent formula consisting of disjunctions of maxterms only, also called product-of-sums canonical form.
- $p \rightarrow q = \neg p \vee q$ is in PDNF.
- What is the principal conjunctive normal form for $[(p \vee q) \wedge \neg p \rightarrow \neg q]$? (see example 6)

Examples of PDNF & PCNF

- $p \leftrightarrow q = (p \wedge q) \vee (\neg p \wedge \neg q)$ in PDNF.
- $p \vee \neg q = [p \wedge (q \vee \neg q)] \vee [\neg q \wedge (p \vee \neg p)]$
  $= (p \wedge q) \vee (p \wedge \neg q) \vee (\neg q \wedge p) \vee (\neg q \wedge \neg p)$
  $= (p \wedge q) \vee (p \wedge \neg q) \vee (\neg p \wedge \neg q)$ in PDNF
- $p \leftrightarrow q = (\neg p \vee q) \wedge (\neg q \vee p)$ in PCNF
- $(p \rightarrow q) \rightarrow (q \rightarrow p) = (\neg p \vee q) \rightarrow (\neg q \vee p)$
  $= \neg(\neg p \vee q) \vee (\neg q \vee p)$
  $= \ldots = (p \vee \neg q)$ in PCNF

Notations of Σ and Π (mutually excluded)

- maxterms of p and q – $p \vee q$, $\neg p \vee q$, $p \vee \neg q$, $\neg p \vee \neg q$ represented by 00, 10, 01, 11, or Π 0, Π 2, Π 1, Π 3
- Minterms of p and q – $p \wedge q$, $\neg p \wedge q$, $p \wedge \neg q$, $\neg p \wedge \neg q$ represented by 11, 01, 10, 00, or Σ 3, Σ 1, Σ 2, Σ 0
- $[(p \vee q) \wedge \neg p \rightarrow \neg q] = [(p \wedge \neg p) \vee (q \wedge \neg p)] \rightarrow \neg q$
  $= (q \wedge \neg p) \rightarrow \neg q = \neg (q \wedge \neg p) \vee \neg q$
  $= \neg q \vee p \vee \neg q = p \vee \neg q =$ Π 1
- $(p \rightarrow q) \rightarrow (q \rightarrow p) = (\neg p \vee q) \rightarrow (\neg q \vee p)$
  $= \neg (\neg p \vee q) \vee (\neg q \vee p)$
  $= (p \wedge \neg q) \vee (\neg q \wedge (p \vee \neg p)) \vee (p \wedge (q \vee \neg q))$
  $= (p \wedge q) \vee (p \wedge \neg q) \vee (\neg p \wedge \neg q) =$ Σ0,2,3

First Order Logic

- Clause form – statements whose elementary components are connected by the operation OR ($\vee$)
- First-order logic
  - Objects: cs4701, fred, ph219, emptylist …
  - Relations/Predicates: is_Man(fred), Located(cs4701, ph219), is_kind_of(apple, fruit)…
  - Note: Relations typically correspond to verbs
  - Functions: Best_friend(), beginning_of() : Returns object(s)
  - Connectives: $\neg$, $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$
  - Quantifiers: Universal $\forall$ and Existential $\exists$
- Any statement expressed in the first-order logic can be expressed in clause form.

Prenex Normal Forms

- A formula F is called a Prenex normal form – iff F is a first order logic and is in the form of $(Q_1x_1, \ldots, Q_nx_n)(M)$ where every (Q_ix_i), i=1,…,n is either $(\forall x_i)$ or $(\exists x_i)$ and M is a formula containing no quantifiers. $(Q_1x_1, \ldots, Q_nx_n)$ is called the prenex, and M is called the matrix of F.
- Convert a first order logic into prenex normal form
  1. Replace → and ↔ using ¬, ∧, ∨
  2. Use double negation and De Morgan's law repeatedly
  3. Rename the variables if necessary
  4. Use rules of (i) ∀ distributes over ∧, ∃ distributes over ∨ (ii) ∀ doesn't distribute over ∨, ∃ doesn't distribute over ∧ to bring the quantifiers to the left.

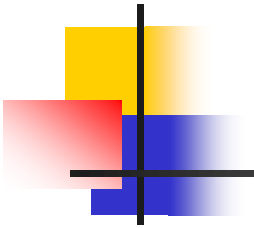
Examples of Prenex Normal Forms

- $\neg\forall x\ P(x) \leftrightarrow \exists x\ \neg P(x)$
- $\neg\exists x\ P(x) \leftrightarrow \forall x\ \neg P(x)$
- $(Qx)\ F(x) \vee G \leftrightarrow Qx\ (F(x) \vee G)$, if G doesn't contain x
- $(Qx)\ F(x) \wedge G \leftrightarrow Qx\ (F(x) \wedge G)$, if G doesn't contain x

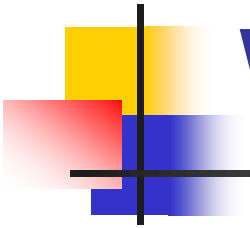
- E.g. 1 $\forall x\ P(x) \rightarrow \exists x\ Q(x)$
  sol: $\exists x\ (\neg P(x) \vee Q(x))$

- E.g. 2 $\forall x\ \forall y\ \exists z\ (P(x,z) \wedge P(y,z)) \rightarrow \exists u Q(x,y,u)$
  sol: $\forall x\ \forall y\ \forall z\ \exists u\ (\neg P(x,z) \vee \neg P(x,z) \vee Q(x,y,u))$

Terminology for Proof



- Axioms – statements we assume to be true
- Proposition, Lemma, Theorem – statement that can be shown to be true.
- Corollary – theorem that can be established directly from a proven theorem
- Conjecture – statement that is being proposed to be a true statement, usually based on the basis of some partial evidence, a heuristic argument, or an intuition of an expert.



Why Proof?

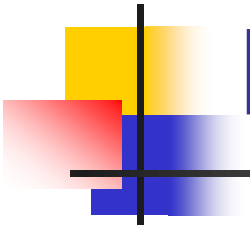
- Introduction to Proofs.
- What is a (valid) proof?
- Why are proofs necessary?

Introduction to Proof techniques

- In a proof, one uses axioms/definitions, premises and proven theorems
- Proof methods: direct, indirect, trivial, contradiction, proof by cases (exhaustive proof), proof of equivalence, existence proofs (constructive or non-constructive), proof by counterexamples, backward/forward reasoning
- Open Problems – famous unsolved problems

Direct/Indirect Proof

- A direct proof of a conditional statement p → q is constructed when the first step is the assumption that p is true, subsequent steps using rules of inference, with the final step showing q must also be true.
- Indirect proof – if we prove the theorem without starting with the premises and end with the conclusion.
- E.g. If n is an odd integer, then n^2 is odd.
- E.g. If n is an integer and 3n+2 is odd, then n is odd. (using indirect proof)



Proof by Contraposition

If $\sqrt{(pq)} \neq (p+q)/2$, then $p \neq q$

Direct proof ?? (not trivial)

Contrapositive:

If $p = q$, then $\sqrt{(pq)} = (p+q)/2$

It follows by:

$\sqrt{(pq)} = \sqrt{(pp)} = \sqrt{(p^2)} = p$

$(p+p)/2 = (p+q)/2 = p.$

Vacuous and Trivial Proof

- Vacuous proof – in p → q, if we know p is false already, the conditional statement must be true.
- Trivial proof – in p → q, if we know q is already true.
- E.g. P(n) is "if n > 1, then $n^2 > n$". Prove P(0) is true.
- E.g. P(n) is "If a and b are positive integers with $a \geqq b$, then $a^2 \geqq b^2$ ". Prove P(0) is true.

Proof by cases

If n is an integer, then n(n+1)/2 is an integer

- Case 1: n is even.

  or n = 2a, for some integer a

  So n(n+1)/2 = 2a*(n+1)/2 = a*(n+1),

  which is an integer.

- Case 2: n is odd.

  n+1 is even, or n+1 = 2a, for an integer a

  So n(n+1)/2 = n*2a/2 = n*a,

  which is an integer.

Proof by Contradiction

$\sqrt{2}$ is irrational

- Suppose $\sqrt{2}$ is rational. Then $\sqrt{2} = p/q$,
  such that p, q have no common factors.
  Squaring and transposing,
  $p^2 = 2q^2$ (even number)
  So, p is even (if x^2 is even, then x is even)
  that is, $p = 2x$ for some integer x
  hence, $4x^2 = 2q^2$ or $q^2 = 2x^2$
  So, q is even (if x^2 is even, then x is even)
  So, p,q are both even – they have a common factor of 2. CONTRADICTION.
  So $\sqrt{2}$ is NOT rational. Q.E.D.

Indirect or Contradiction

If n is an integer and $n^3 + 5$ is odd, then n is an even

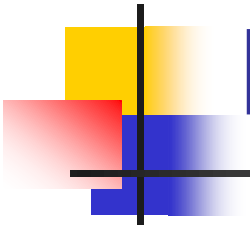
Indirect proof (contrapositive) :

Let $n = k+1$, $n^3 + 5 = 2(4k^3 + 6k^2 + 3k + 3)$

Proof by Contradiction:

Suppose that $n^3 + 5$ is odd and n is odd

$5 = (n^3 + 5) - n^3$ should be even, because of the difference of two odds, but it is an odd.



Existence Proofs (1/2)

E.g.1 There exists (distinct) integers x,y,z satisfying $x^2+y^2 = z^2$

Proof: x = 3, y = 4, z = 5. (by constructive existence proof)

E.g.2 There is a positive integer that can be written as the sum of cubes of positive integers in two different ways.

Proof: $1729 = 10^3+9^3 = 12^3+1^3$

Existence Proofs (2/2)

There exists irrational b,c, such that b^c is rational

By nonconstructive proof:

Consider $\sqrt{2}^{\sqrt{2}}$. Two cases are possible:

- Case 1: $\sqrt{2}^{\sqrt{2}}$ is rational – DONE ($b = c = \sqrt{2}$).

- Case 2: $\sqrt{2}^{\sqrt{2}}$ is **irrational** –

  Let $b = \sqrt{2}^{\sqrt{2}}$, $c = \sqrt{2}$.

  Then $b^c = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = (\sqrt{2})^{\sqrt{2}*\sqrt{2}} = (\sqrt{2})^2 = 2$

The Use of Counterexamples

EX1. All prime numbers are odd (false)

Proof: 2 is an even number and a prime.

EX2. Every prime number can be written as the difference of two squares, i.e. $a^2 - b^2$.

Proof: 2 can't be written as $a^2 - b^2$

Proof by Equivalence

- n is even iff n^2 is even

Proof (by equivalence)

Let P be "n is even", Q be "n^2 is even"

P and Q are equivalence can be proven by "P→ Q and Q → P"

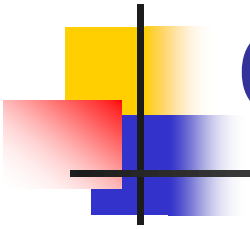
What is wrong with the proof ?

- If n^2 is positive, then n is positive.

Proof: Suppose that n^2 is positive. Because the conditional statement "If n is positive, then n^2 is positive" is true, hence we can conclude that n is positive.

- If is not positive, then n^2 is not positive.

Proof: Suppose that n is not positive. Because the conditional statement "If n is positive, then n^2 is positive" is true, hence we conclude that n^2 is not positive.



Conjectures

- Fermat's Last Theorem

  $x^n + y^n = z^n$ has no solution in (positive) integers x,y,z with xyz =! 0 whenever n is an integer and is greater than 2.

  $\exists x, \exists y, \exists z, \exists n$ such that $x^n + y^n = z^n$?

  domain of x, y, and z is Z^+, domain of n is $\{x \backslash x > 2, x \in Z\}$

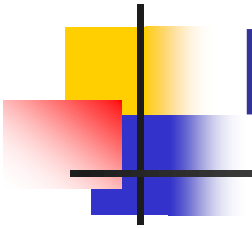
The 3X + 1 Conjecture

- 3x+1 conjecture

  Game: Start from a given integer n. If n is even, replace n by n/2. If n is odd, replace n with 3n+1. Keep doing this until you hit 1.

e.g. $n=5 \rightarrow 16 \rightarrow 8 \rightarrow 4 \rightarrow 2 \rightarrow 1$

Q: Does this game terminate for all n?



MEMO

- Read section 1.7, 1.8, and 1.9
- Get familiar with terminology of theorem proving
- Be familiar with proof methods of contrapositive, counterexample, exhaustive, and existence
- What is the Fermat's last theorem?
- HW #1-4 of §1.7, #5-8 of §1.8, #5,6,9,10,17,19 of §1.9.