CSE 20
DISCRETE MATH

Fall 2017

http://cseweb.ucsd.edu/classes/fa17/cse20-ab/

Reminders + goals

- Midterm Exam on Tuesday October 31 – in class
  - One note card can be used. Bring photo ID to *your* lecture.
  - Assigned seats: seat map on Piazza (tonight)
  - Review session Sunday morning – CENTR 101 podcast

- HW 4 due Saturday 11pm material included on exam

- Today's review: more CNF/DNF/circuit examples, proofs
- Review sheet: **also** algorithms + number representations

Implement a proposition

What combinatorial logic circuit (with AND, OR, NOT, XOR gates) implements the compound proposition

$$(p \to q) \leftrightarrow (r \to p) \quad ?$$

Implement a proposition

What combinatorial logic circuit (with AND, OR, NOT, XOR gates) implements the compound proposition

$$(p \to q) \leftrightarrow (r \to p) \quad ?$$

Strategy: Find equivalent proposition and then implement.

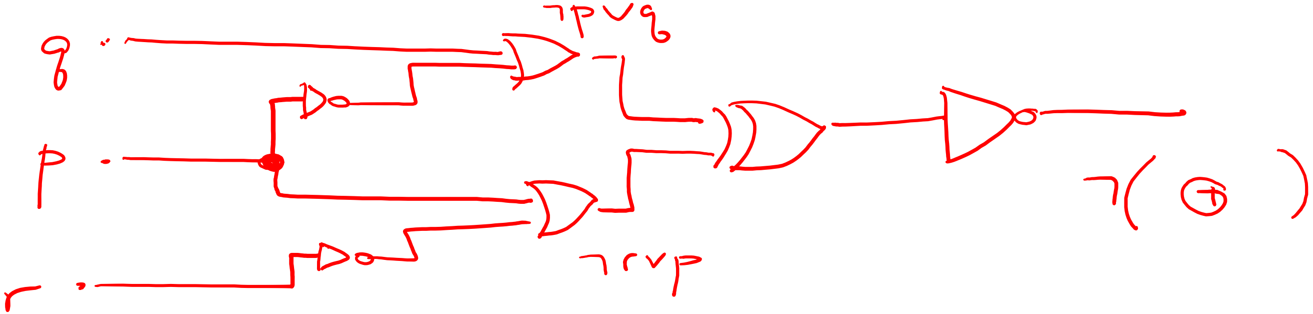
- Via logical equivalences
- Via truth table algorithm for CNF / DNF

Via logical equivalences

$$(p \to q) \leftrightarrow (r \to p)$$

$$\equiv \neg((p \to q) \oplus (r \to p))$$

$$\equiv \neg((\neg p \vee q) \oplus (\neg r \vee p))$$



Via truth table

intermediate

	p	q	r	$(p \to q)$	$(r \to p)$	$\boxed{(p \to q) \leftrightarrow (r \to p)}$
$(111)_2 = 7$	T	T	T			
6	T	T	F			
5	T	F	T			
4	T	F	F			
3	F	T	T			
2	F	T	F			
1	F	F	T			
$(000)_2 = 0$	F	F	F			

Via truth table

p	q	r	$(p \to q)$	$(r \to p)$	$(p \to q) \leftrightarrow (r \to p)$
T	T	T	T		
T	T	F	T		
T	F	T	F		
T	F	F	F		
F	T	T	T		
F	T	F	T		
F	F	T	T		
F	F	F	T		

Via truth table

p	q	r	$(p \to q)$	$(r \to p)$	$(p \to q) \leftrightarrow (r \to p)$
T	T	T	T	T	
T	T	F	T	T	
T	F	T	F	T	
T	F	F	F	T	
F	T	T	T	F	
F	T	F	T	T	
F	F	T	T	F	
F	F	F	T	T	

Via truth table

p	q	r	$(p \rightarrow q)$	$(r \rightarrow p)$	$(p \rightarrow q) \leftrightarrow (r \rightarrow p)$
T	T	T	T	T	T
T	T	F	T	T	T
T	F	T	F	T	F
T	F	F	F	T	F
F	T	T	T	F	F
F	T	F	T	T	T
F	F	T	T	F	F
F	F	F	T	T	T

Via truth table

A DNF
B CNF

p	q	r	$(p \rightarrow q) \leftrightarrow (r \rightarrow p)$
T	T	T	T
T	T	F	√ T
T	F	T	F
T	F	F	F
F	T	T	F
F	T	F	√ T
F	F	T	F
F	F	F	√ T

LAND IN THESE ROWS!

Via truth table

p	q	r	$(p \to q) \leftrightarrow (r \to p)$	$p \vee q \vee r$	$p \wedge q \wedge r$
T	T	T	T	T	T
T	T	F	T	T	F
T	F	T	F	T	F
T	F	F	F	T	F
F	T	T	F	T	F
F	T	F	T	T	F
F	F	T	F	T	F
F	F	F	T	F	F

What compound proposition describes the first row?

A. $p \vee q \vee r$
B. $p \wedge q \wedge r$
C. $\neg p \vee \neg q \vee \neg r$
D. $\neg p \wedge \neg q \wedge \neg r$
E. None of the above

Via truth table

p	q	r	$(p \to q) \leftrightarrow (r \to p)$
T	T	T	T
T	T	F	T
T	F	T	F
T	F	F	F
F	T	T	F
F	T	F	T
F	F	T	F
F	F	F	T

p is T
q is T
r is T

$p \wedge q \wedge r$

$p \wedge q \wedge \neg r$

r is F

$\neg p \wedge q \wedge \neg r$

$\neg p \wedge \neg q \wedge \neg r$

Via truth table

p	q	r	$(p \to q) \leftrightarrow (r \to p)$	
T	T	T	T	$p \wedge q \wedge r$
T	T	F	T	$p \wedge q \wedge \neg r$
T	F	T	F	
T	F	F	F	
F	T	T	F	
F	T	F	T	$\neg p \wedge q \wedge \neg r$
F	F	T	F	
F	F	F	T	$\neg p \wedge \neg q \wedge \neg r$

$(p \wedge q \wedge r)$, $(p \wedge q \wedge \neg r)$ $\equiv p \wedge q$

DNF: $(p \wedge q \wedge r) \vee (p \wedge q \wedge \neg r) \vee (\neg p \wedge q \wedge \neg r) \vee (\neg p \wedge \neg q \wedge \neg r)$

As a circuit (assume 3 and 4 input gates are available; otherwise cascade)

DNF: $(p \wedge q \wedge r) \vee (p \wedge q \wedge \neg r) \vee (\neg p \wedge q \wedge \neg r) \vee (\neg p \wedge \neg q \wedge \neg r)$

Via truth table

CNF

p	q	r	$(p \to q) \leftrightarrow (r \to p)$
T	T	T	T
T	T	F	T
T	F	T	F
T	F	F	F
F	T	T	F
F	T	F	T
F	F	T	F
F	F	F	T

AVOID THESE ROWS!

Via truth table

p	q	r	$(p \to q) \leftrightarrow (r \to p)$
T	T	T	T
T	T	F	T
T	F	T	F
T	F	F	F
F	T	T	F
F	T	F	T
F	F	T	F
F	F	F	T

What compound proposition describes avoiding the third row?

A. $p \wedge \neg q \wedge r$
B. $\neg(p \wedge \neg q \wedge r)$
C. $p \vee \neg q \vee r$
D. $\neg(p \vee \neg q \vee r)$
E. None of the above

Via truth table

p	q	r	$(p \to q) \leftrightarrow (r \to p)$
T	T	T	T
T	T	F	T
T	F	T	F
T	F	F	F
F	T	T	F
F	T	F	T
F	F	T	F
F	F	F	T

$\neg(p \wedge \neg q \wedge r) \equiv \neg p \vee q \vee \neg r$

$\neg(p \wedge \neg q \wedge \neg r) \equiv \neg p \vee q \vee r$

$\neg(\neg p \wedge q \wedge r) \equiv p \vee \neg q \vee \neg r$

$\neg(\neg p \wedge \neg q \wedge r) \equiv p \vee q \vee \neg r$

Via truth table

p	q	r	$(p \to q) \leftrightarrow (r \to p)$
T	T	T	T
T	T	F	T
T	F	T	F
T	F	F	F
F	T	T	F
F	T	F	T
F	F	T	F
F	F	F	T

$\neg(p \wedge \neg q \wedge r) \equiv \neg p \vee q \vee \neg r$

$\neg(p \wedge \neg q \wedge \neg r) \equiv \neg p \vee q \vee r$

$\neg(\neg p \wedge q \wedge r) \equiv p \vee \neg q \vee \neg r$

$\neg(\neg p \wedge \neg q \wedge r) \equiv p \vee q \vee \neg r$

CNF: $(\neg p \vee q \vee \neg r) \wedge (\neg p \vee q \vee r) \wedge (p \vee \neg q \vee \neg r) \wedge (p \vee q \vee \neg r)$

As a circuit (assume 3 and 4 input gates are available; otherwise cascade)

CNF: $(\neg p \vee q \vee \neg r) \wedge (\neg p \vee q \vee r) \wedge (p \vee \neg q \vee \neg r) \wedge (p \vee q \vee \neg r)$

Prime numbers

Which of these is the definition of n being **prime**?

Domain is positive integers, D(x,y) means x divides y

i.e. y is an int multiple of x

e.g. $D(2,4)$

$\neg D(4,2)$

A. $\forall x(\ D(x,n) \vee x = 1 \vee x = n\ )$

B. $\neg\exists x(\ 1 < x < n \wedge \cancel{\neg} D(x,n)\ )$ ✓ "There's no pos int strictly b/w 1 and n that divides n"

i.e. "There's no proper divisor of n"

C. $\exists x(\ (x = 1 \vee x = n) \wedge \neg D(x,n)\ )$

D. $\forall x(\ D(x,n) \to (x = 1 \vee x = n)\ )$ ≡ $\forall x((x \neq 1 \wedge x \neq n) \to \neg D(x,n))$

or

$\exists x(\ (x=1 \vee x=n) \to D(x,n))$ ✗

$\forall x\ (\ 1<x<n \to \neg D(x,n))$ ✓

E. None of the above

Overall strategy

- Do you believe the statement? its negation?
  - Try some small examples.
- Determine logical structure + main connective.
- Determine relevant definitions.
- Map out possible proof strategies.
  - For each strategy: what can we **assume**, what is the **goal**?
  - Start with simplest, move to more complicated if/when get stuck.

Direct proof, construction, exhaustive, etc.

Contradiction, hidden cases

Sample proofs

A set is called **closed under an operation** exactly when

No matter which input is chosen from the set → **Operation** → *Output is also in the set*

ints are closed under +

ints are closed under ·

x is rational means there are ints p, q ($q \neq 0$) such that $x = \frac{p}{q}$

Sets and operations

x is prime means there are no proper divisors of x

Which of the following sets are closed under the corresponding operations? Prove your answer.

The set of positive rational numbers under multiplication.

The set of integers under taking powers (i.e. x^y).

The set of prime numbers under addition.

The set of irrational numbers under division.

The set of rational numbers under subtraction.

Proof strategies so far

Assume? Goal?

- To prove a statement of the form All x have property P(x)
  - Consider an arbitrary (fixed but unknown) x in the domain. Prove P(x) holds for that element – only using facts true about "generic" elements in the domain.
- To prove a statement All x have property P(x) is false
  - Find a counterexample: a specific element in the domain where P(x) evaluates to False.
- To prove a statement of the form There is an x with property P(x)
  - Find an example: a specific element in the domain where P(x) evaluates to True.
- To prove a statement There is an x with property P(x) is false
  - Consider an arbitrary (fixed but unknown) x in the domain. Prove P(x) **fails**for that element – only using facts true about "generic" elements in the domain.

Proof strategies so far

Assume? Goal?

- To prove a statement of the form If P then Q
  - Assume P is true. Using this assumption (and definitions, etc.) prove Q.
  - OR Assume Q is false. Using this assignment (and defintiions, etc.) prove P is false.
- To prove a statement of the form Both X and Y
  - Step 1: Prove X. Step 2: Prove Y
- To prove a statement of the form At least one of X and Y
  - Convert to equivalent version: If not X then Y
  - OR convert to different equivalent version: If not Y then X

Proof by contradiction

Assume? Goal?

- To prove a statement of **any** **form**
  - Assume: the statement is false.
  - Using this assumption (and definitions, etc.) find X which must be both truth and false!
  - ????
  - Conclude: original assumption invalid, i.e. the statement is true.

Exam strategy

- Questions are listed by topic, not by difficulty.
- **Read all questions.**
- **Start with ones you know how to do.**
- Read directions carefully. (Need to justify? What's required?)
- Pace yourself (look at # points per question).
- Ask questions if needed.