Lecture 7

Monday, February 10, 2020 4:58 PM

Unit 1 : How to prove properties of programs?

Statements about programs (assertions, termination, etc.)

$\Downarrow$ various techniques

Statements about mathematics

```
int x=0; int lim = input();
while (x<lim) {
    x := x+2
}
assert (x % 2 == 0)
```

Program about which we want to prove something

$\Downarrow$ Technique: come up with invariant

"Always x % 2 == 0".

$\Downarrow$ Proof obligation

Show that this invariant is inductive.

Show that $\forall x$,

if $\underbrace{x \% 2 == 0}_{\text{invariant holds now}}$

then $\underbrace{(x+2) \% 2 == 0}_{\text{invariant will hold in the next step.}}$

Statement in logic/math. If this stmt is true, then orig. prog has the desired property.

Unsaid belief so far

I trust in your ability to prove mathematical statements.

But : no programmer is willing to prove things by hand.

Q : How do we automate the discharging of proof obligations?

discharging of proof obligations?

SAT solvers: propositional logic

SMT solvers: programs are not just about logic.

Also handle data.

Numbers, strings, uninterpreted functions

black boxes.

Propositional Logic

Proposition: A statement about the world.

It rained yesterday.

There was a taxi at the station.

- Michael Phelps is the best swimmer in the world.
- Michael Phelps was faster in the 2012 100m Olympic swimming event than all competitors.

---

① If the train arrives late p

and there are no taxis at the station, $\neg q$ $\quad p \wedge \neg q \Rightarrow r$

then John is late for the meeting. r

② John is not late for the meeting $\quad \neg r$

③ But the train also arrived late. $\quad p$

Conclusion: There must have been taxis at the station. $\quad q$

① If it is raining p

& Jane does not have an umbrella, $\neg q$

then she will get wet : r

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

② Jane is not wet $\qquad \neg r$

③ And it was raining $\qquad p$

Conclusion : She must have had an umbrella with her. $\qquad q$

Claim : For all propositions p, q, r,

if $p \wedge \neg q \Rightarrow r$ $\qquad r \vee \neg(p \wedge \neg q)$

$\neg r$ $\qquad r \vee (\neg p \vee q)$

p

then it must be the case that q.

Proof : $p \wedge \neg q \Rightarrow r$ is the same as $\neg p \vee q \vee r$.

We know p. We know $\neg r$.

Therefore q.

"Sequent calculus" "Natural deduction" systems

$$\frac{p \Rightarrow q \qquad p}{q} \text{ Modus ponens} \qquad \frac{p \Rightarrow q \qquad \neg q}{\neg p} \text{ Modus tollens.}$$

Can a system prove everything which is true? Completeness

Can a system only prove things which are true? Consistency / ~~Soundness~~

Proof $\rightleftarrows$ vs. Truth vs. Expressible

$\downarrow$

Truth tables.

a	b	$a \wedge b$ "a and b"
T	T	T
T	F	F
F	T	F
F	F	F

2^n rows for a formula with n variables

$\wedge$	$\vee$	$\neg$
and	or	not
$\cdot$	$+$	$\overline{a}$

a	b	$a \vee b$
T	T	T
T	F	T
F	T	T
F	F	F

a	$\overline{a}$
T	F
F	T

a	b	$a \Rightarrow b$	$a \wedge b$
T	T	T	T
T	F	F	F
F	T	T	F
F	F	T	F

$\boxed{A}$ $\boxed{1}$ $\boxed{B}$ $\boxed{3}$

<u>Claim</u>: If number on one side, then letter on the other.

other.

Question: which cards to turn over to verify claim?

Given a propositional formula φ,

is it satisfiable?

validity?

how many models does it have?

a	b	c ...	φ
T	T	F	T
T	F	F	F
⋮	⋮	⋮	⋮

Satisfiability: Is there a row where the output is true?

NP-complete

Validity: Is the output always true?

(co-NP complete)

Model counting: How many rows evaluat

Model counting : How many rows evaluate

(#P-complete) to true.

Decision problems

Given φ, is it satisfiable? Y/N.

- Witness to Y : simply give the row which satisfies

  If φ has n variables, then witness has n bits.

  Witness can be checked in poly time.

- Witness to N. : Nobody knows how to do this efficiently.

Given φ, is it valid? Y/N.

- Witness to $\mathcal{Y}$: Nobody knows how to do this efficiently

- Witness to $\mathcal{N}$: Row which evaluates to false.

Connection b/w satisfiability & validity.

Theorem: φ is valid iff $\neg\varphi$ is unsat.

Given a formula φ, how many models does it have?

Valiant 1979: Complexity

#P-complete the per

$$\det\begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - b$$

$$\text{perm}\begin{pmatrix} a & b \end{pmatrix} = a \ldots$$

s

of computing

rmanent.

C

$$\mathrm{perm}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad + b$$

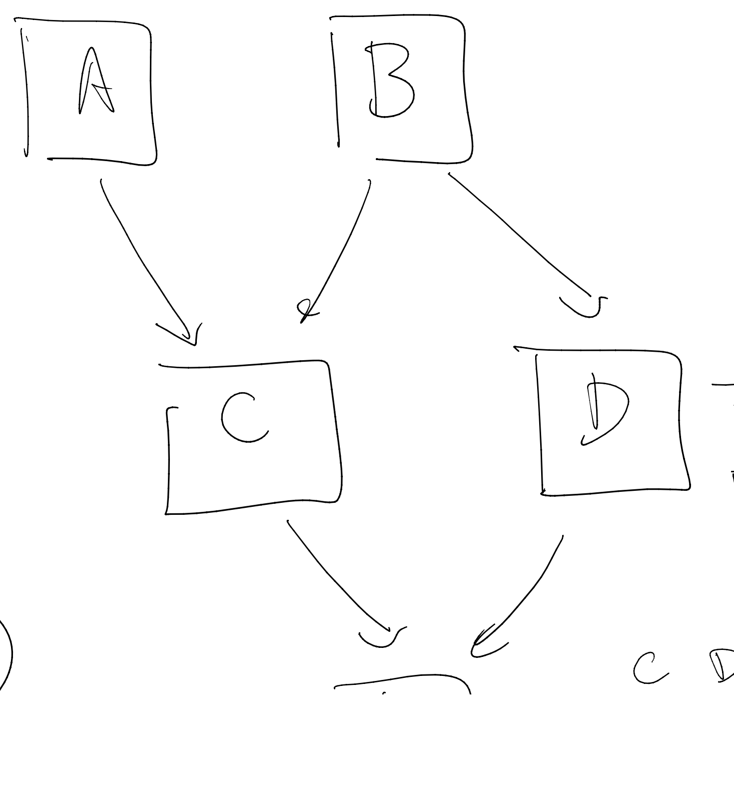
Counting SAT

Horn SAT | 2-SAT :

linear

Inference in Bayesian net

#P-complete.



$$\Pr(A \wedge E \mid \overline{D})$$

$$= \Pr(A \wedge E \wedge C \mid \overline{D})$$

$$= \Pr(A \wedge E \wedge \overline{C} \mid \overline{D})$$

C

solvable in

time.

works is

B	D
T	0.8
F	0.4

$|E$

$+\Pr(A \wedge E \wedge C \mid D)$

$\boxed{E}$

C	D
T	T
T	F
F	F
F	

$$|A \cup B| = |A| + |B| - |A$$

Preve

C

Connections between

model counting & r

How is φ represented

	E
T	0.8
F	0.2
T	0.1
F	0.5

$\cap B|$

ent double
counting.

random sampling

?

	Circuits	Formul
sat	NP-C	NP-C
validity	CO-NP-C	CO-N
Model counting	#P-comp	#P-

$$(a \wedge b) \vee (\bar{c} \wedge d$$

Circuits

las	CNF	DNF	ROBDD
E	NP-C.	trivial	triv
PC	trivial	co-NPC	triv
-comp.	#P-comp	#P-comp	trivi

$) \wedge (erf)$

But

ord

s

ial

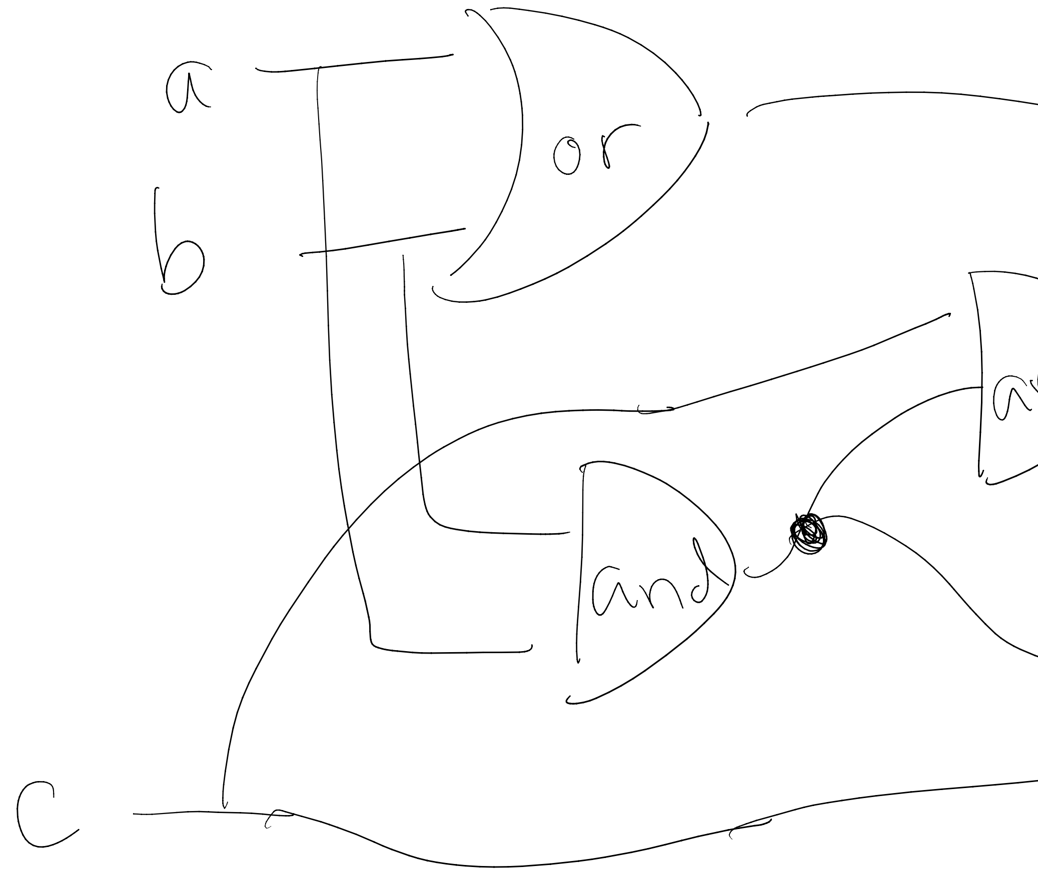
ial

ial

variable

ering is

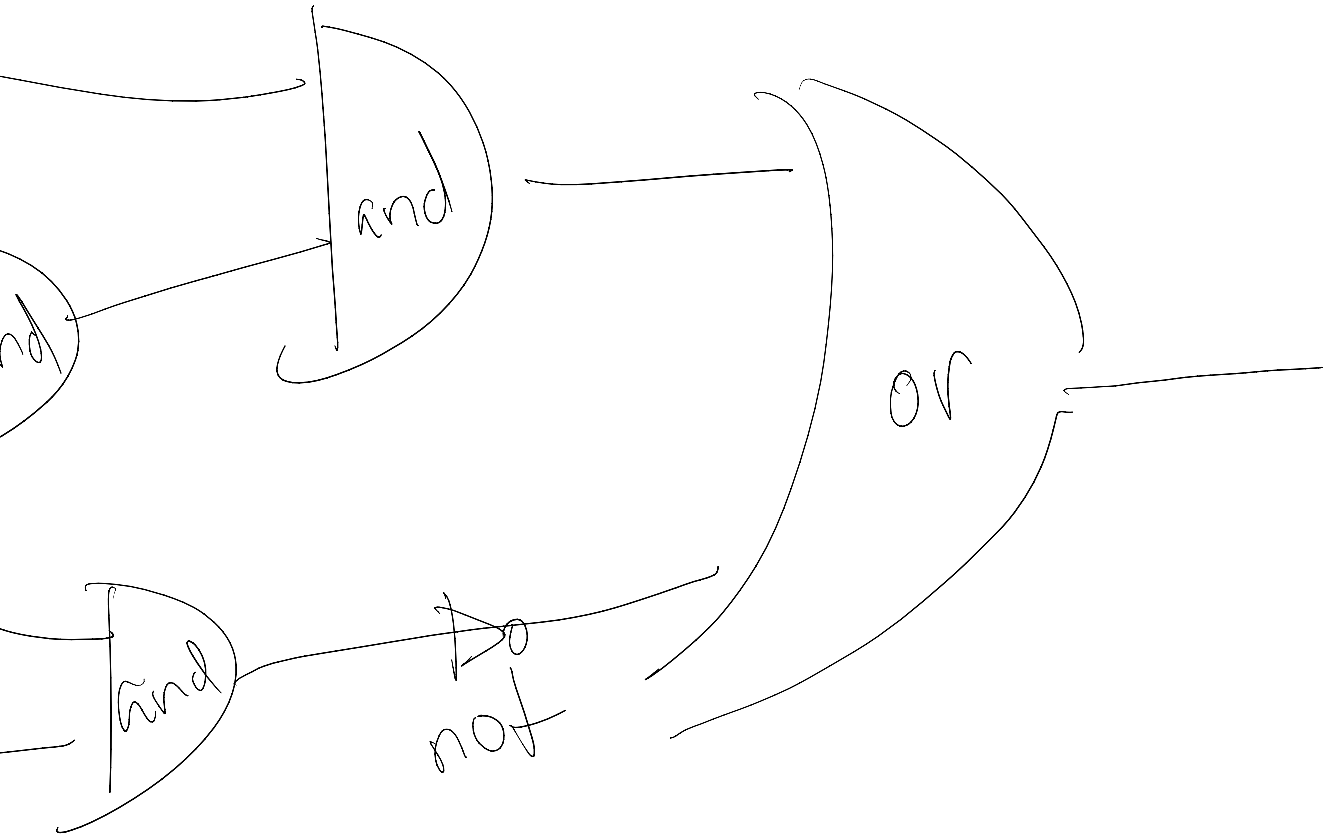
uper-hard!



Fan-out

Circuits are e

succinct



xponentially more
than formulas.

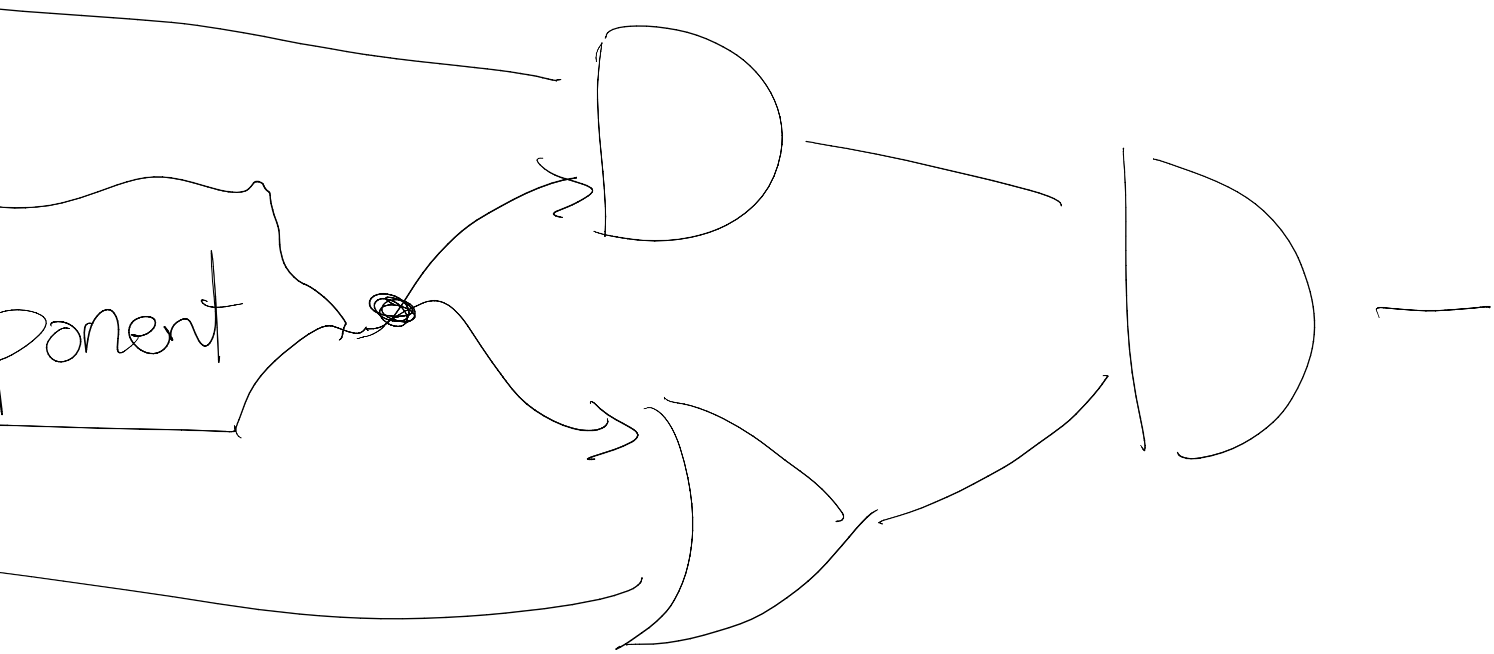
Fanouts and

Big comp

CNF : conjunctive

(a or $\bar{b}$ or c

able sharing



normal form.

c) and ($\bar{a}$ or b or e or f)

and (a

c

3-CNF : at m
clause

Cook's o

$\underbrace{\text{or } d \text{ or } \underbrace{\bar{e}}_{\text{literal}})}_{\text{clause}}$ and...

most 3 literals per

riginal NP-completeness

result. (3-SAT).

2-SAT : Is

Can be

DNF : Disjunctive n

(_ and _ and _) or (

var or

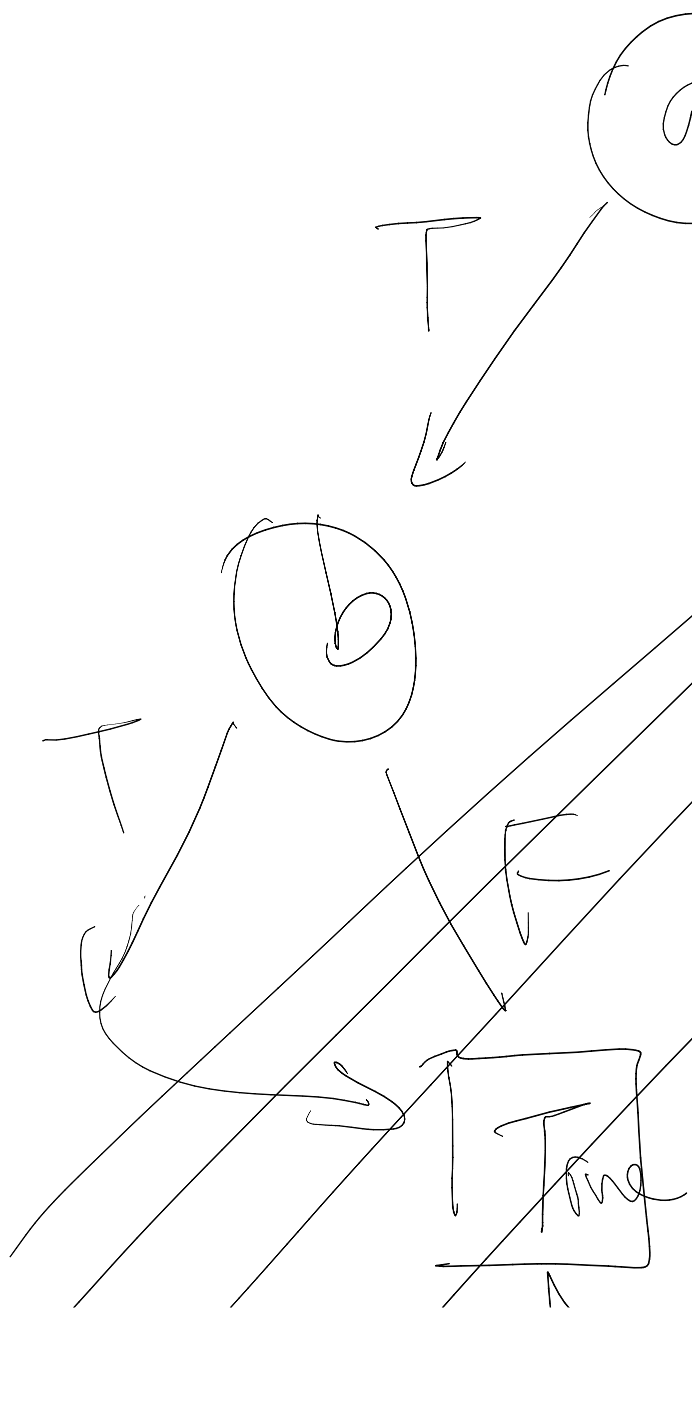
$\overline{var}$

a formula in 2-CNF
satisfiable?
done in linear time

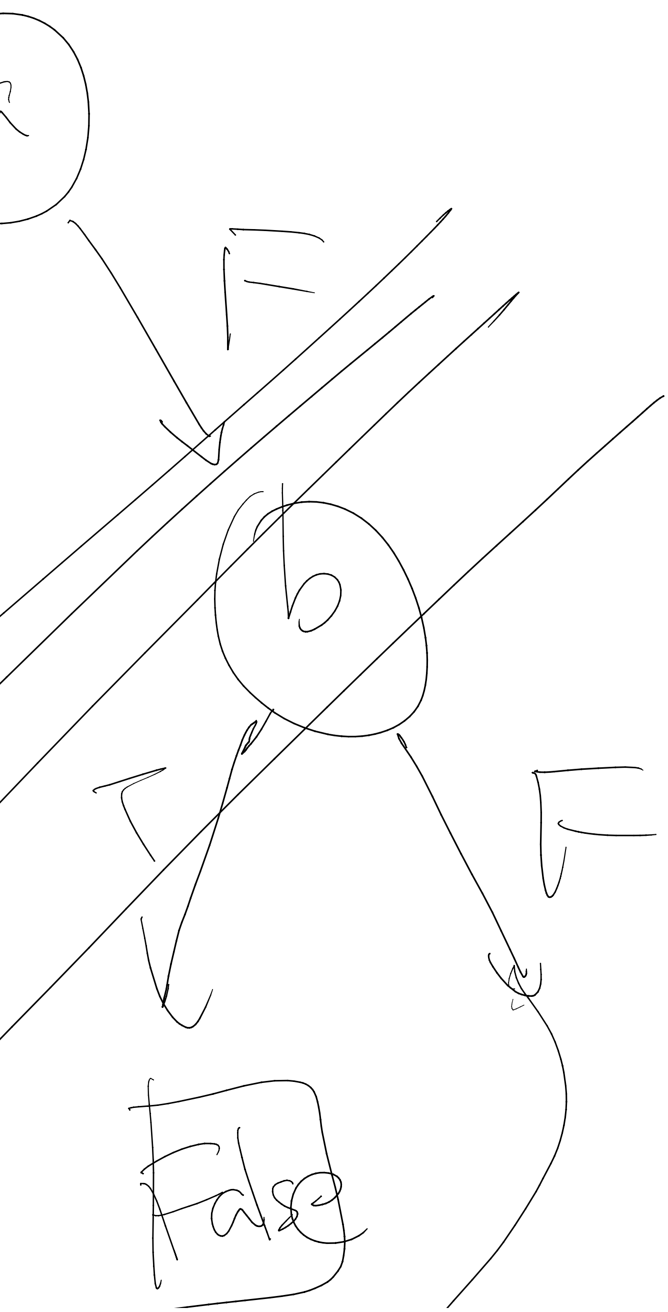
normal form

— and —) or (— and —) or ...

Binary dec



...sion diagrams (R...



Redu...

1. Maxim...

2. No vr...

Ordere...

o)

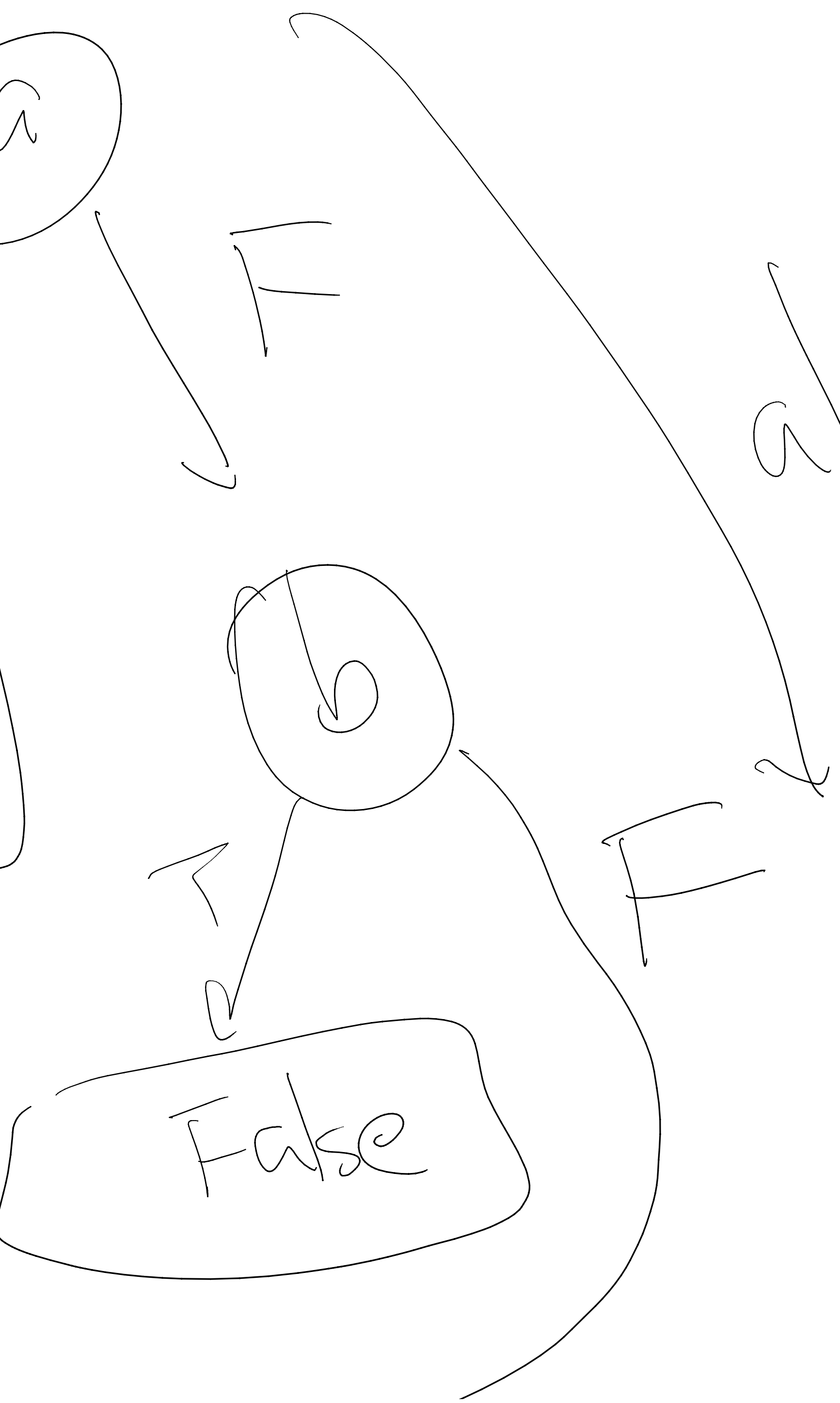
ced

nal sharing

nnecessary nodes

ed

ab



1 All br
the sam
orde

Randal
198
ROBDDs

anches share

me variable

r

---

l Bryant

56

s are canonical.

<u>Claim</u>: Every

equivalent

$(A \cdot B) +$

formula φ has an

CNF representati

$\overline{}$

$c = (A+C)(B$

$\overline{}$

n

on.

$+C)$,

$(A+B)\cdot C$

DeMorgan's

$$= \underline{A \cdot B} + AC$$

$$= A \cdot B + C($$

$$= A \cdot C + B \cdot C$$

Laws :

$+ BC + \underline{C}$

$\cancel{A + B + \text{true}}$

$= A \cdot B + C$

$$\overline{A \cdot B}$$

$$\overline{A + B}$$

$$= \overline{A} + \overline{B}$$

$$= \overline{A} \cdot \overline{B}$$