Lecture 2 Elements of Propositional Logic

Announcement: Homework 1 has been uploaded to Piazza.

A simple verification problem

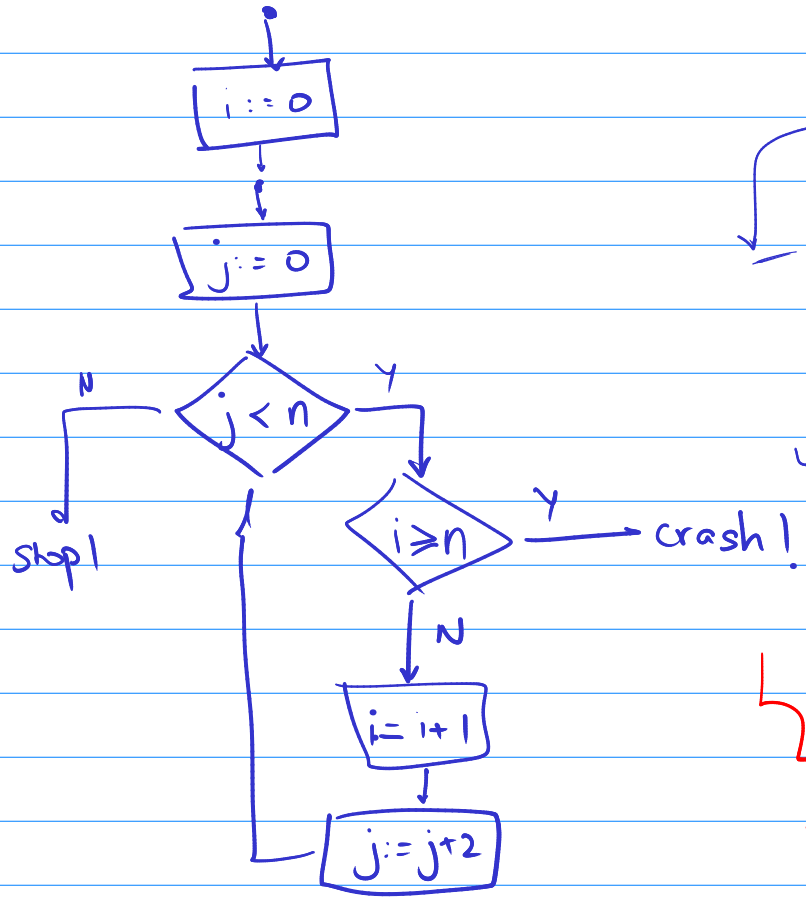
```
CountBy2(n)
    i := 0   j := 0
    while j < n
    |   if (i ≥ n) crash!
    |   i := i + 1
    |
    |   j := j + 2
```

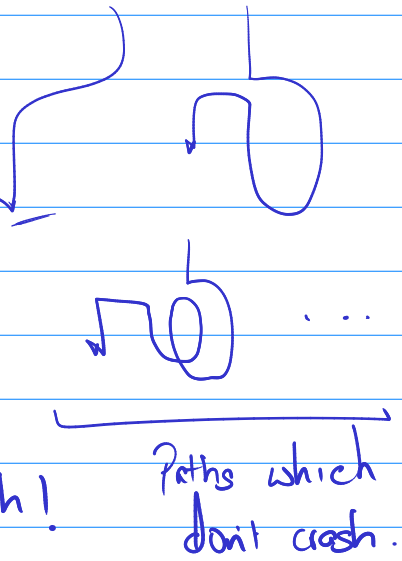
Property: $\forall n \in \mathbb{Z}$ CountBy2(n) doesn't crash.

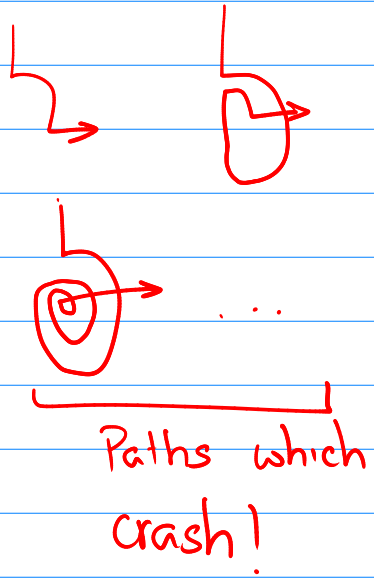
Invariant: At the beginning of the loop body, in every iteration, $0 \leq i \leq j < n$.

Verifying countBy2 is hard because of

- number of states is large (infinite)







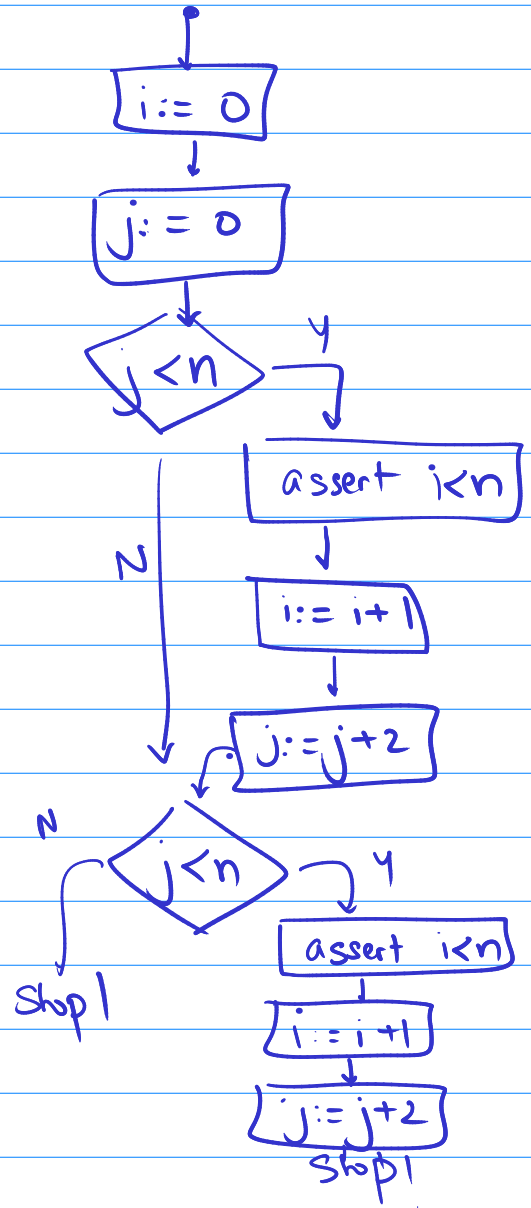
Claim: Verifyng countBy2 is hard because there are infinitely many paths through the program.

A simpler program without loops

countBy2-Fin(n) ⇝ { Unrolled countBy2 program twice

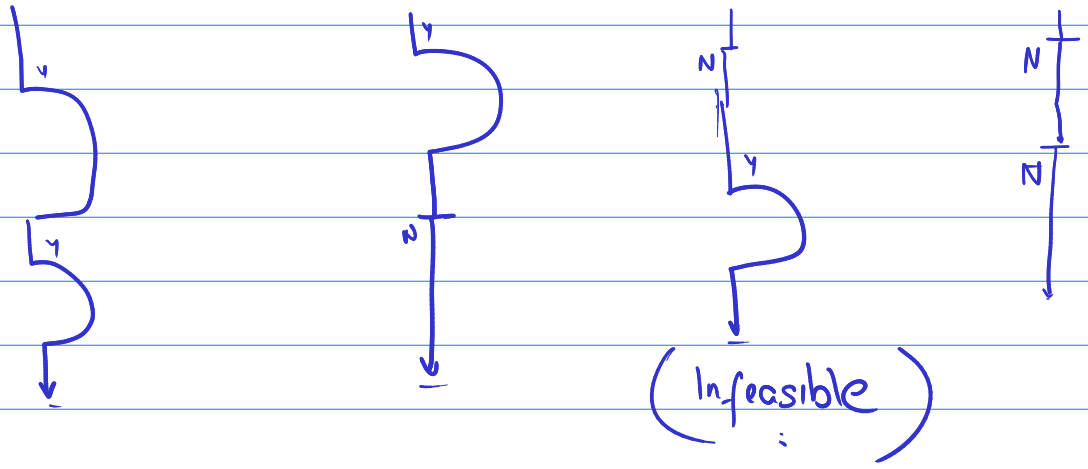
```
i := 0   j := 0

if j < n
    assert (i < n)
    i := i + 1
    j := j + 2

if j < n
    assert (i < n)
    i := i + 1
    j := j + 2
```

If i ≠ n then crash!

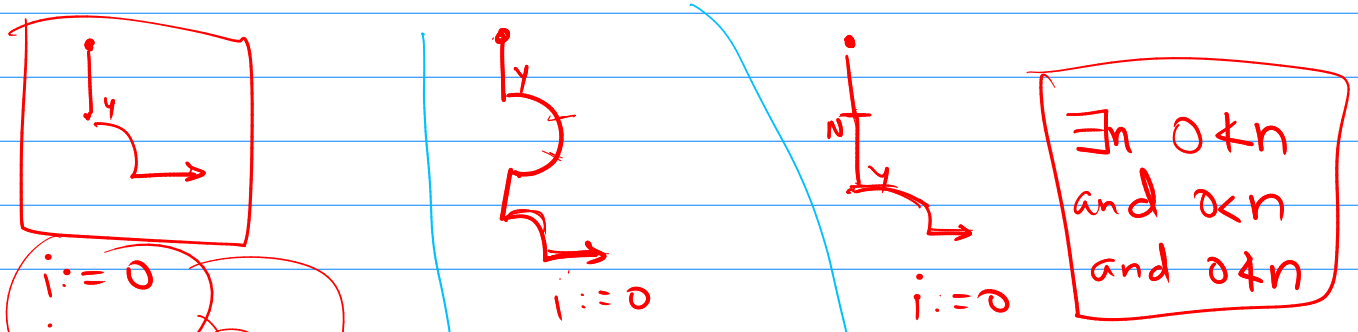


Property: $\forall n \in \mathbb{Z}$, countBy2-Fin does not crash.

Ways in which countBy2-Fin can execute normally



Ways in which countBy2-Fin can crash



Is there an n which causes the program to trace this path?

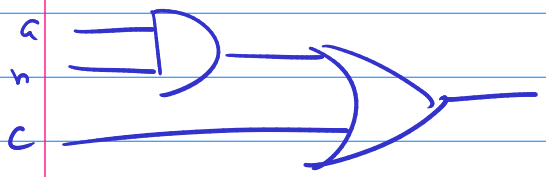
No. $\nexists n.\ 0<n$ and $0 \not< n$?

The path is infeasible.

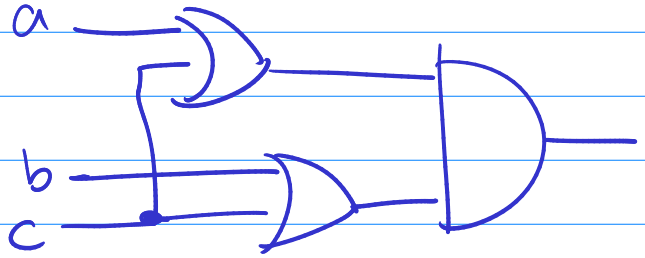
$\nexists n$ $0<n$ and $2<n$ and $1 \not< n$.

Therefore, this path is also infeasible.

Verifying stateless electrical circuits.



$a \cdot b + c$



$(a+c) \cdot (b+c)$

$L \Rightarrow R$

$L \Leftarrow R$

$L \Rightarrow \overline{R}$

Propositional Logic

- Propositional connectives: $\wedge$ $\cdot$ $\vee$ $+$ $\neg$ $-$

and	or	not
$\Rightarrow$	nand	nor

$a \Rightarrow b$ If a then b

(Not a) or b $\quad \bar{a} + b$

$\neg a \vee b$

- What do the connectives mean?

Truth tables

a	b	$a \wedge b$	$a \vee b$	$\bar{a}$
T	T	T	T	F
T	F	F	T	F
F	T	F	T	T
F	F	F	F	T

- Proof techniques

Modus Ponens (if, and, then)

$$\frac{p \Rightarrow q \qquad p}{q}$$

Modus Tollens

$$\frac{p \Rightarrow q \qquad \bar{q}}{\bar{p}}$$

- For example:

If it is raining (p) & Jane doesn't have an umbrella ($\bar{q}$)

then she will get wet (r) $\quad p \wedge \bar{q} \Rightarrow r$

Jane is not wet $\therefore \bar{r}$

But it is raining $\therefore p$

So she must have an umbrella $\therefore q$

$$\frac{p \wedge \bar{q} \Rightarrow r \qquad \bar{r}}{\overline{p \wedge \bar{q}}} \qquad \frac{\bar{p} \vee q \qquad p}{q}$$

$\equiv \quad \bar{p} \vee q$.

Logic : Connection between truth & prog.

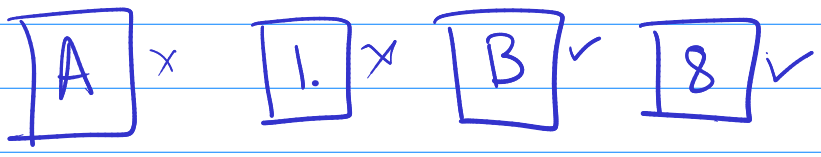
- truth tables

A model is a row in a truth table

Completeness : Can everything which is true be proved?

Soundness / Consistency : Are all provable statements true?

Puzzle



Guarantee : Every card has a letter on one side & a number on the other

Suspicion : If even number on one side then vowel on the other

Question: What cards should I turn over to confirm this suspicion?

✓ Proposal 1	B, 8	Proposal 3: (A)
- Proposal 2	8	

Algorithmic problems

Given a propositional logic formula φ

Q1: Is it satisfiable? Easy Y. witness

Some row in truth table which evaluates to true? Hard N witness

NP-complete

Q2: Is it valid? Easy N witness

Do all rows evaluate to true?

Hard Y witness

co-NP-complete

Q3: How many models? Model counting.

#P-complete

Q4: Enumerate models

Q5: Pick model uniformly at random.

Claim: φ is unsat iff $\neg\varphi$ is valid

Valiant 1979 Complexity of computing the permanent.

$$\det\begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc \qquad \text{perm}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad + bc$$

#P-complete

Bayesian Networks

Computing marginal probability is #P-complete.

Horn-SAT, 2-SAT: Solvable in linear time. Model counting is #P-complete