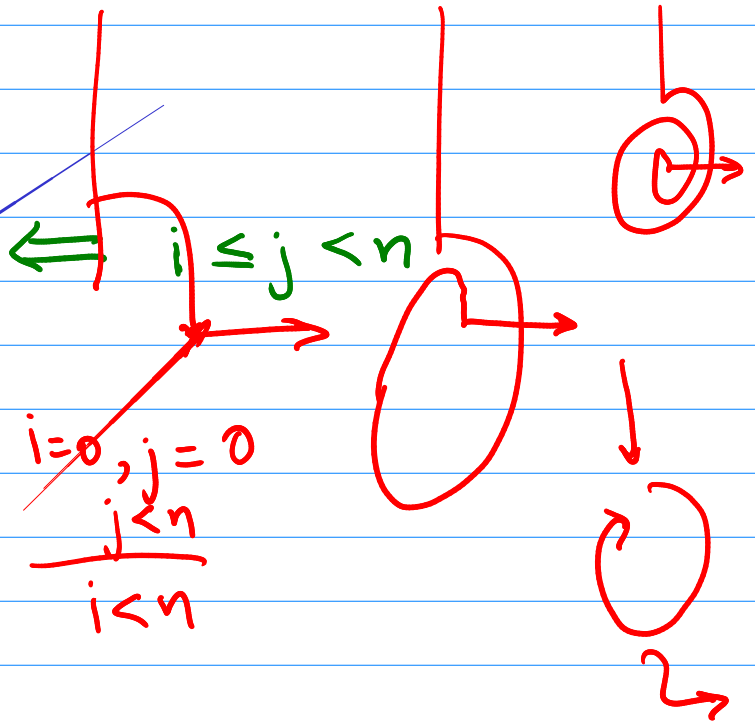
countBy2 (n)

```
i := 0 , j := 0
while j < n :
    if i ≥ n : crash
    i := i + 1
    j := j + 2
```



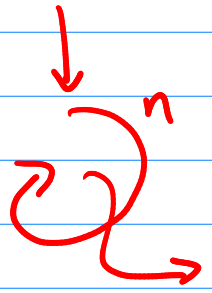
Property: $\forall n \in \mathbb{Z}$, countBy2 (n) doesn't crash.

Not the only kind of property

1. Program always halts
2. Program doesn't leak information
3. Program always computes the correct output
4. Whenever request, program eventually responds

Temporal reasoning

Claim: No matter how many times we take the loop, n is infeasible.



Challenge 1: Automatic invariant synthesis

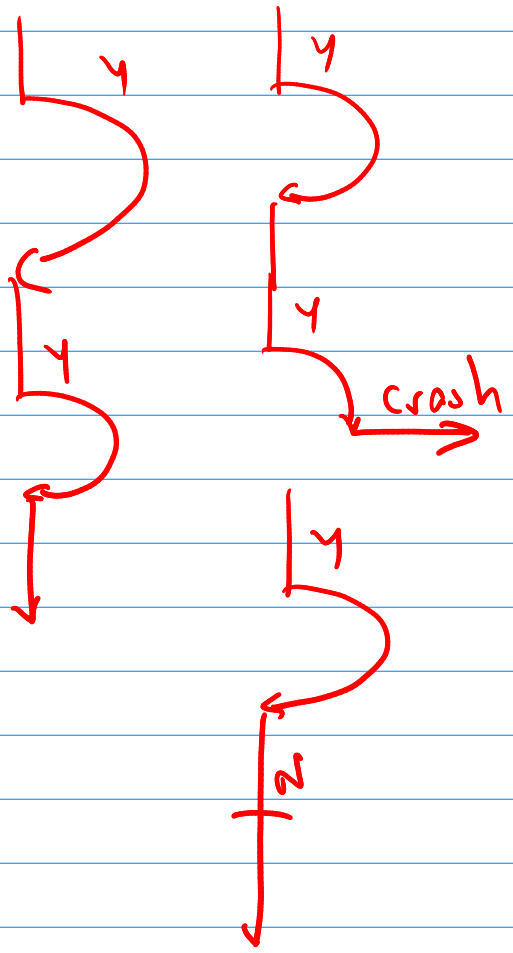
Challenge 2: Discharging verification conditions

$$\exists_{i,j,n} \left(i \leq j \text{ and } j < n \right) \text{ and } i \geq n$$

Verifying Loop-Free Code

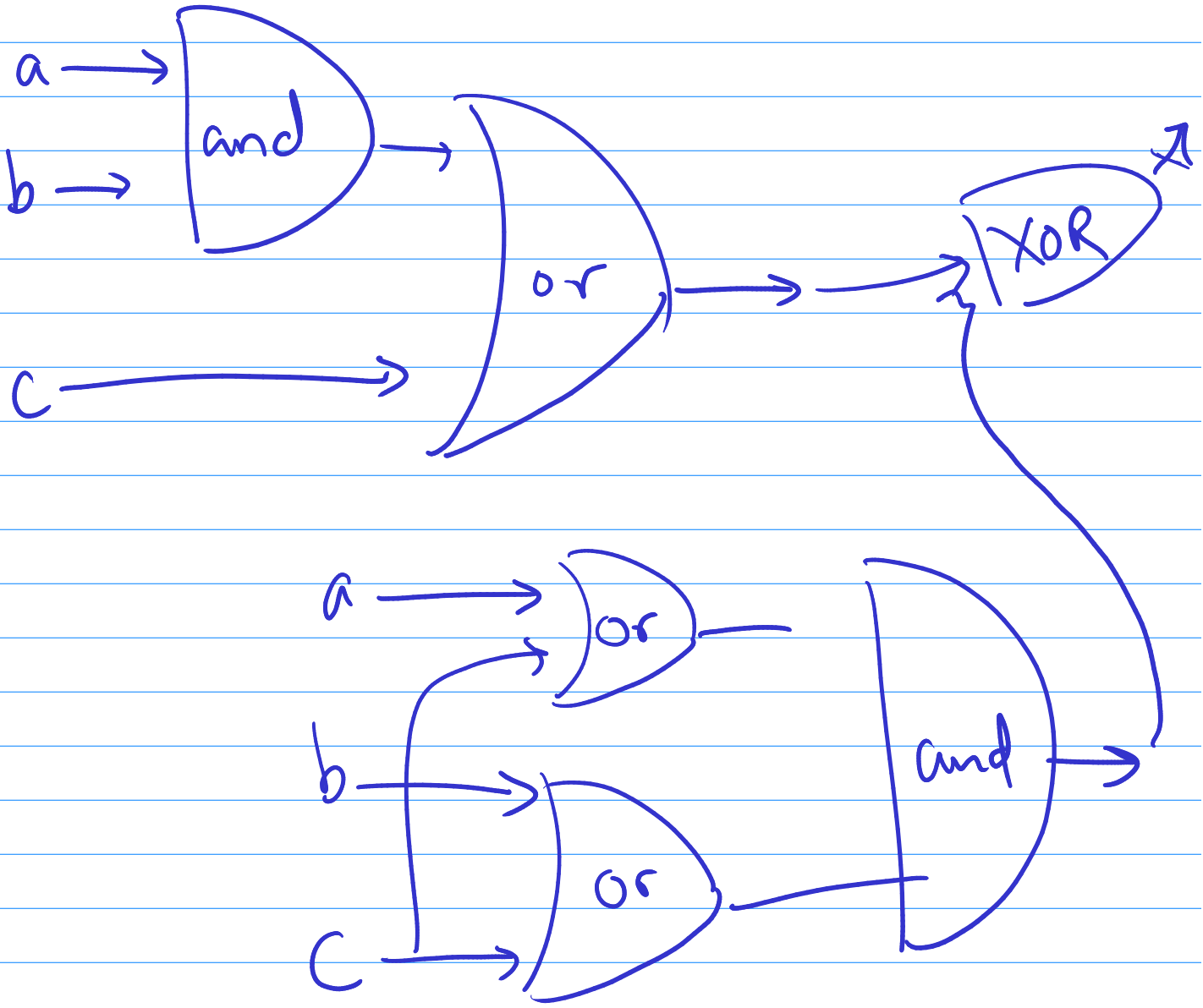
Bounded symbolic execution

```
count By 2 Fun (n):
    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
```



What if we remove if-conditions too?

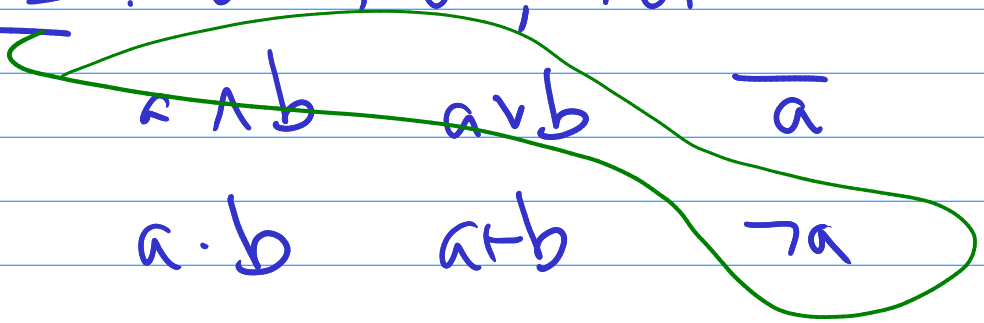
Stateless electrical circuits



Propositional logic

Atomic propositions : $a, b, c, \ldots$

Connectives : and, or, not



$a \Rightarrow b$ implication $\quad \overline{a} \vee b$

if a then b

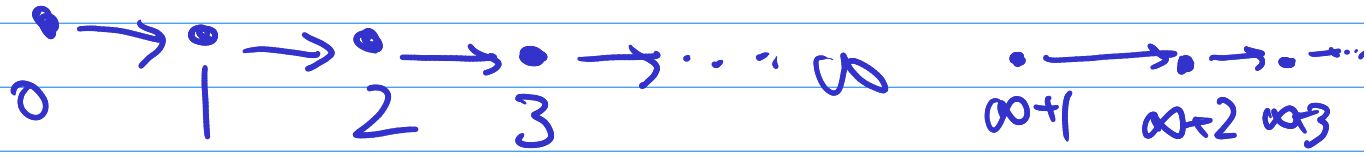
nand nor

What do these connectives mean?

Truth tables

a	b	$a \wedge b$	$a \vee b$	$\neg a$
T	T	T	T	F
T	F	F	T	F
F	T	F	T	T
F	F	F	F	T

Model



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

Modus ponens

$$\frac{p \Rightarrow q \quad \overline{q}}{\overline{p}}$$

Modus tollens

Truth proof expressiveness model

$a \vee \overline{a}$

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

Claim: $\exists$ irrational numbers a, b s.t a^b is rational.

Proof

Consider $a = \sqrt{2}^{\sqrt{2}}$ $\quad b = \sqrt{2}$

a is either rational, or it is not.

Case 1: a is rational

Let $a' = \sqrt{2}$ $\quad b' = \sqrt{2}$

$a'^{b'} = a$ is rational

Case 2: a is irrational

$$a^b = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^2 = 2$$

Completeness: Is everything which is true also provable?

Soundness: Is everything that is provable also true?

For verification engineers

Soundness: If the tool says that the program is bug-free, then it is really bug-free

Completeness: If the program is bug-free, then does the tool agree?

Algorithmic Questions

Given a propositional formula φ

Canonical NP-complete problem

(1) Is it satisfiable?

Is there a row in the TT where it evaluates to T?

→ Y Easy Y-witness

→ N No witnesses are hard Proof complexity

(2) Is it valid?

Canonical Co NP-complete problem

Do all rows in the TT evaluate to T?

→ Y seems hard to prove

→ N Easy N-witness

(3) How many Ts?

Canonical #P-complete problem

Model counting problem

Counting SAT problem

(4) Enumerate all models?

(5) Pick a random model uniformly