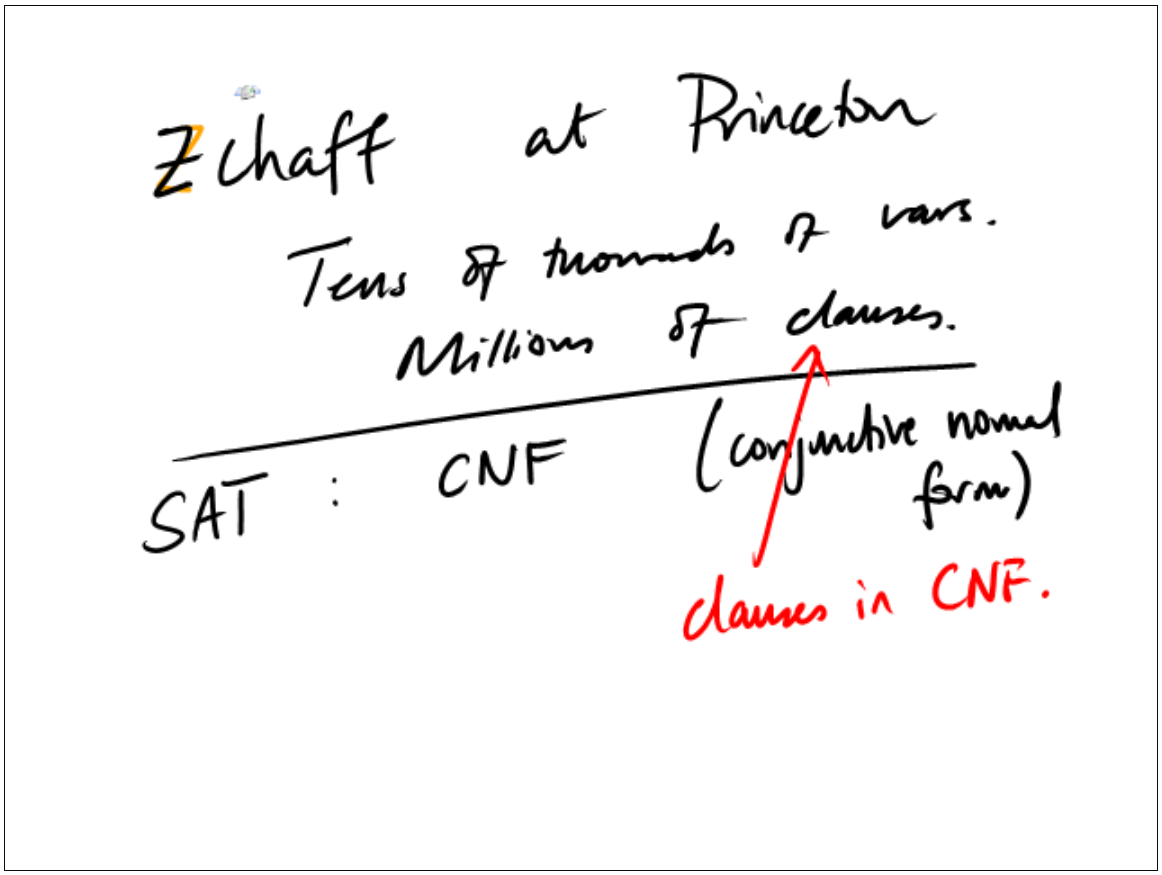
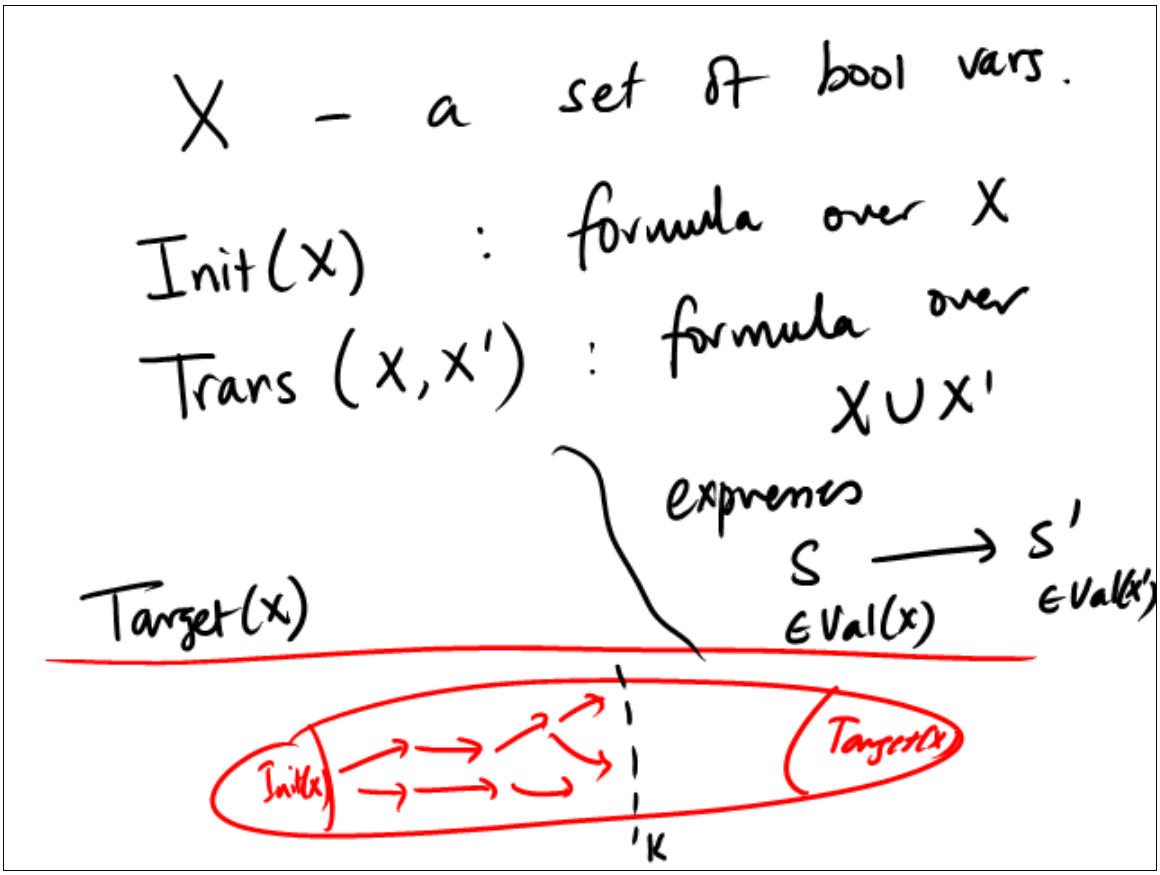
Bounded Model-checking

- SAT solvers
- BMC / Reachability
- BMC / LTL


Zchaff at Princeton
Tens of thousands of vars.
Millions of clauses.
SAT : CNF (conjunctive normal form)
clauses in CNF.


X - a set of bool vars.
Init(X) : formula over X
Trans (X, X') : formula over X ∪ X'
expresses
S → S'
∈ Val(X) ∈ Val(X')
Target(X)
Init(X)
Target(X)
K

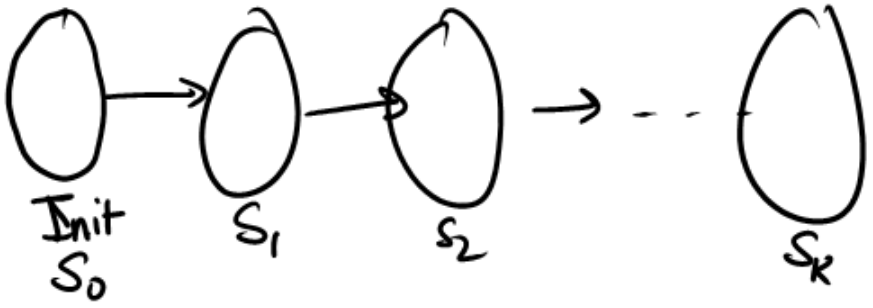
Bounded model checking.

Given $K \in \mathbb{N}$, is the Target reachable in K steps.

BMC $\xleftarrow{\text{encoded}}$ SAT

X, $Init(x)$, $Trans(x, x')$, $Target(x)$, k $\longrightarrow$ φ_k

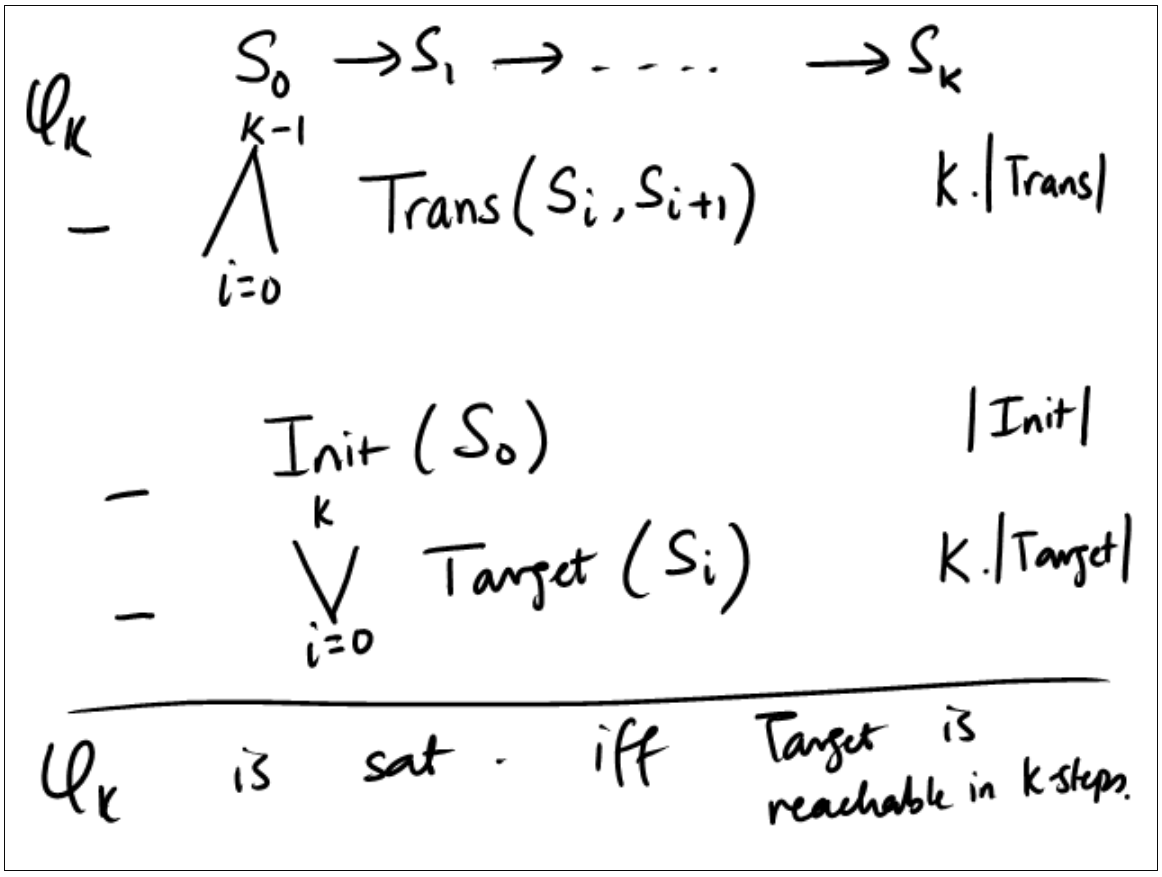
φ_k is sat iff Target is reachable in K steps

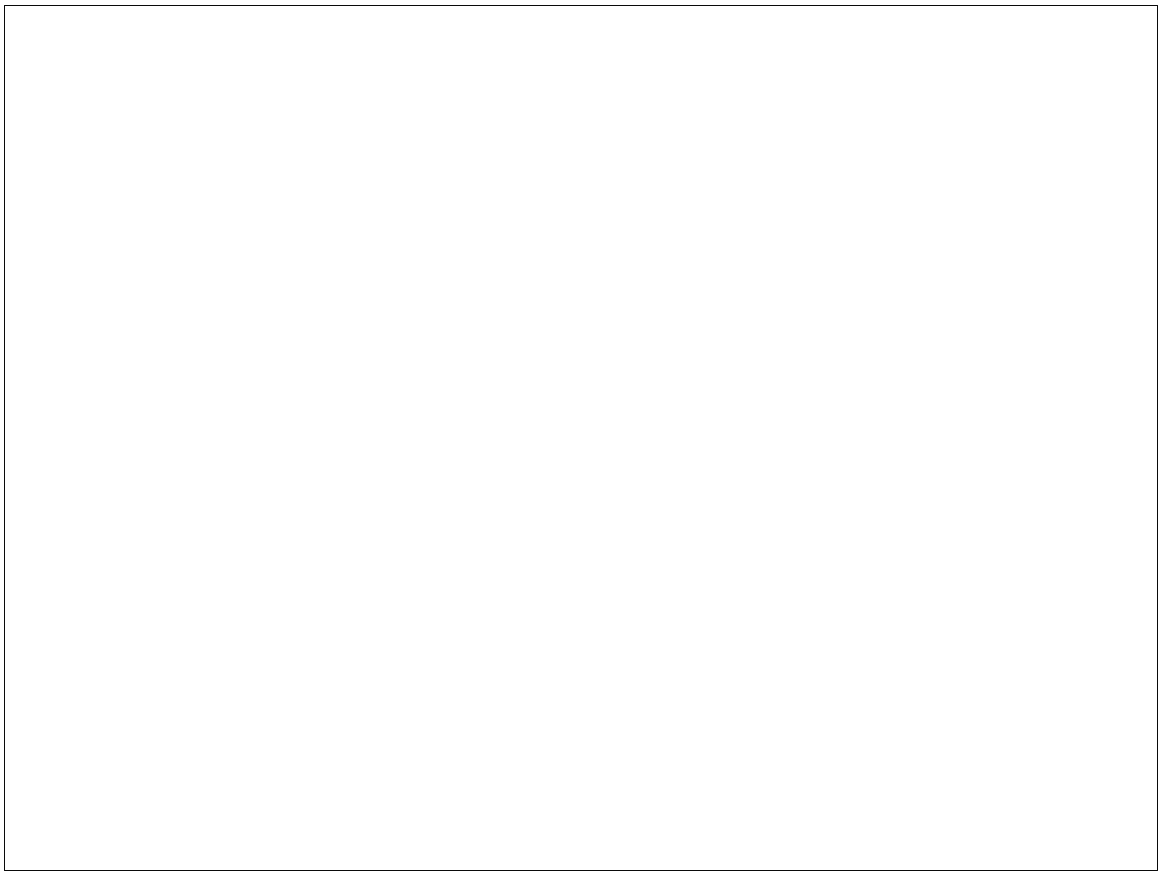


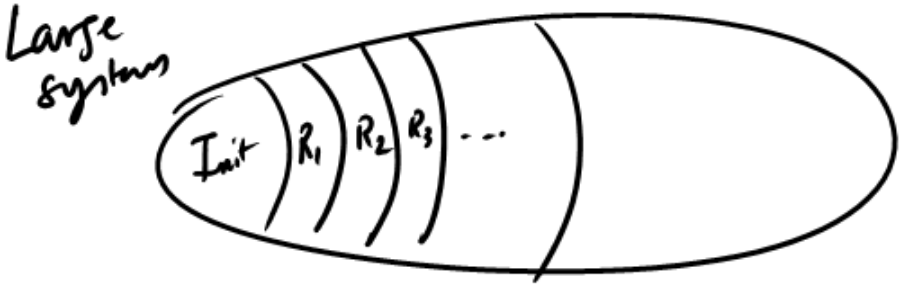
$S_0, S_1, \ldots S_k$ – copies of $X = \{x_1, \ldots x_n\}$

$S_0 = \{x_1^0, \ldots x_n^0\}$

$S_i = \{x_1^i, \ldots x_n^i\}$


$S_0 \to S_1 \to \cdots \to S_k$
φ_k
$\bigwedge_{i=0}^{k-1} Trans(S_i, S_{i+1})$
$k \cdot |Trans|$
$Init(S_0)$
$|Init|$
$\bigvee_{i=0}^{k} Target(S_i)$
$k \cdot |Target|$
φ_k is sat. iff Target is reachable in k steps.





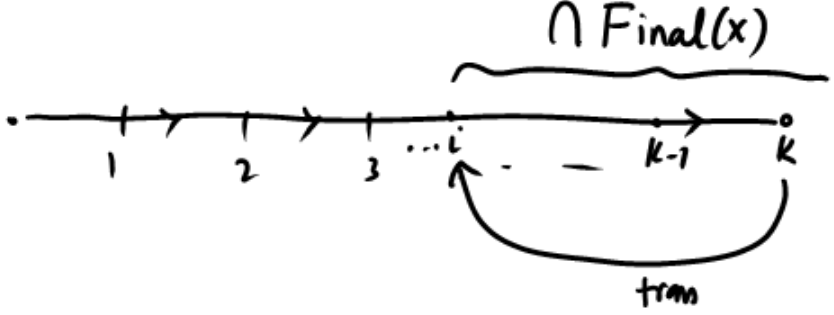
K_{BDD}

K_{SAT}

- BDD : space grows.
- SAT : ~~Constant~~ linear space.

BMC for LTL

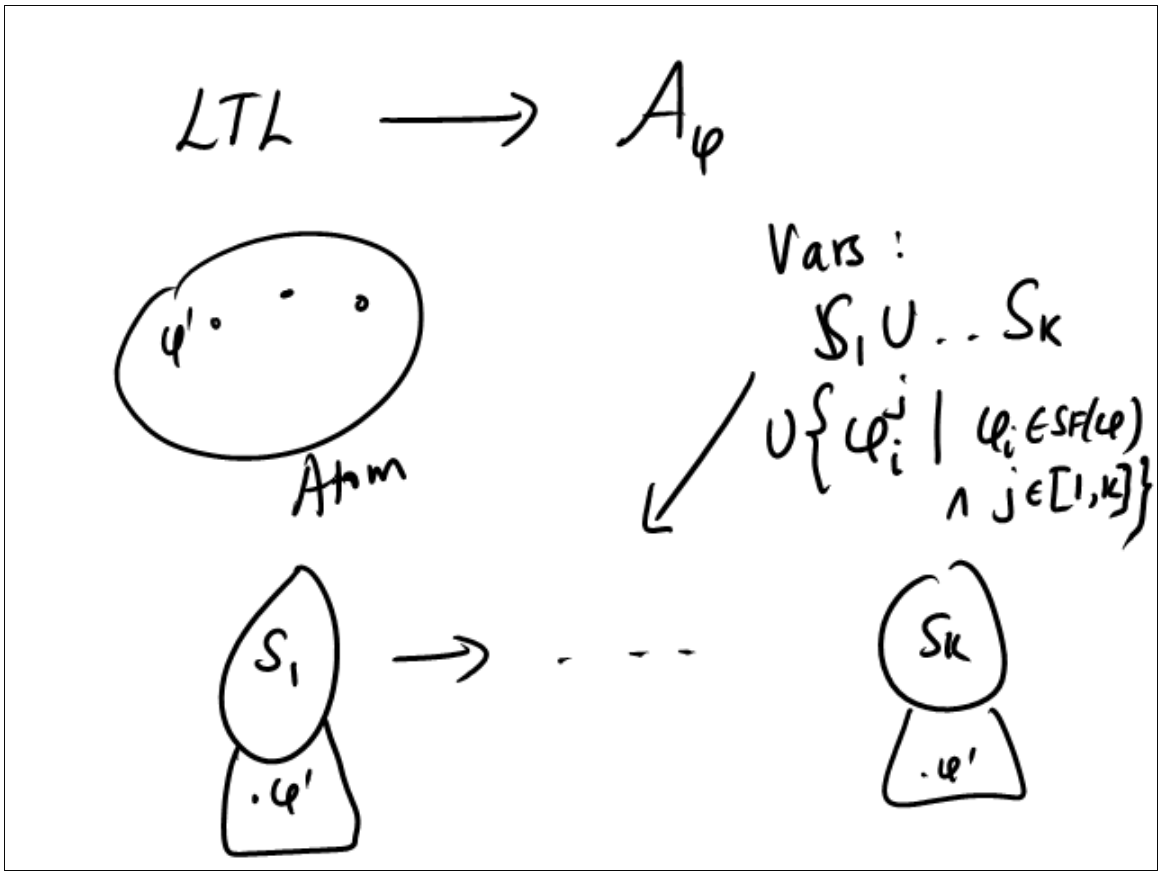
Init(x), Trans(x,x') , Final(x)



$$- \; Init(S_0)$$

$$- \; \bigwedge_{i=0}^{k-1} Trans(S_i, S_{i+1})$$

$$- \; \bigvee_{i=0}^{k-1} \left[Trans(S_k, S_i) \wedge \bigvee_{j=i}^{k} Final(S_j) \right]$$


LTL ⟶ A_φ
φ'
Atom
Vars :
$S_1 \cup \ldots S_K$
$\cup \{ \varphi_i^j \mid \varphi_i \in SF(\varphi) \wedge j \in [1,K] \}$
S_1
$.\varphi'$
S_K
$.\varphi'$

Also add transition constraints of A_φ.

Final(x) : defined to be the Büchi winning states of A_φ