G. Holzmann	80	PAN
	87	Supertime
	89	SPIN
Pnueli	77	temporal logic
Kripke	63	modal logic
Clarke + Emerson, Sifakis + Queille	81	Model checking 10^6 states
Ken McMillan	89	BDD allow 10^{60} states

what about... (DNJ)

data structures?
unbounded system?
non-temporal?

MC + Z → Alloy, a model finder

Does O preserve I?

$\forall s,s' \mid O(s,s') \wedge I(s) \Rightarrow I(s')$

negate & solve

$\exists s,s' \mid O(s,s') \wedge I(s) \wedge \neg I(s')$

model finding problem instance

- analysis constraint
- vars
- instance = binding of vars to vals

run P facts ∧ decls ∧ P

check A facts ∧ decls ∧ ¬A

vars = sigs, fields, pred args

Skolemization

$\exists x: X \mid F$, $X = \{X_0, X_1, X_2\}$

$\equiv F[x \leftarrow X_0] \vee F[x \leftarrow X_1] \vee F[x \leftarrow X_2]$

$\exists = \infty \vee$
$\forall = \infty \wedge$

instances found won't contain x

but...

$\exists x \mid F \approx F[x \leftarrow X_3]$

↖ Fresh

$\exists x \mid x > y$ soln: $y=1$

$X_3 > y$ soln: $y=1, X_3=2$

Alloy: some x: X | F

⇓

$(x:X) \wedge F[x \leftarrow X_3]$