Safe Autonomy

Lec - 3

- Spec & Verif
- Control theory 101.

Verification

$S \models \phi$ → M_ϕ : Most general automata that captures all behaviors that satisfy ϕ.

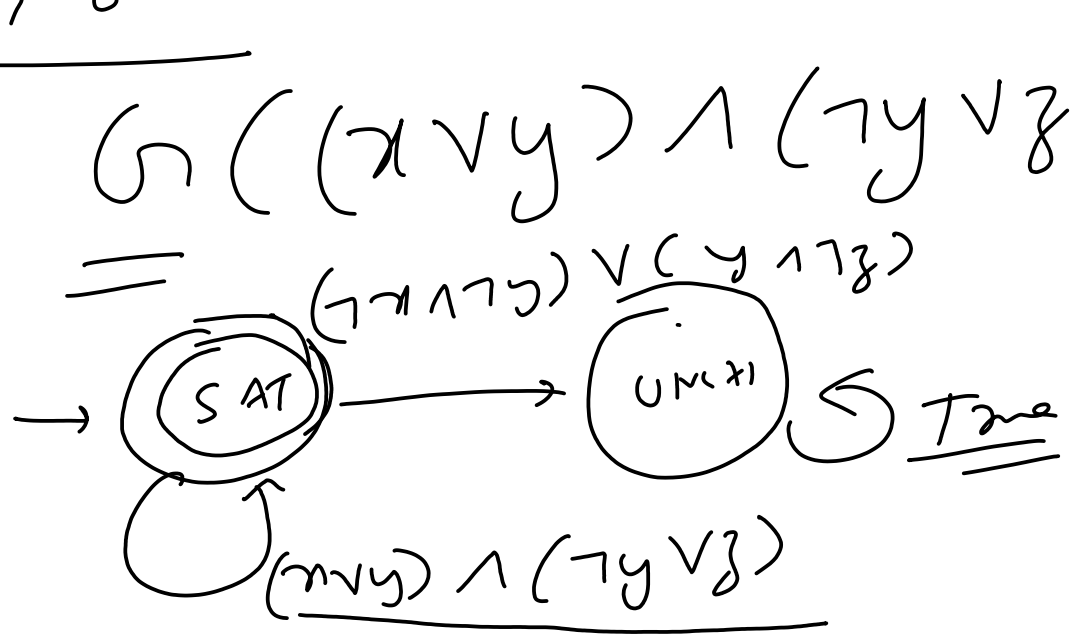
ϕ → Temporal logic

- LTL — linear temporal logic
- CTL — Computational Tree Logic
- CTL*
- Finite Model Theory → Modal logics.

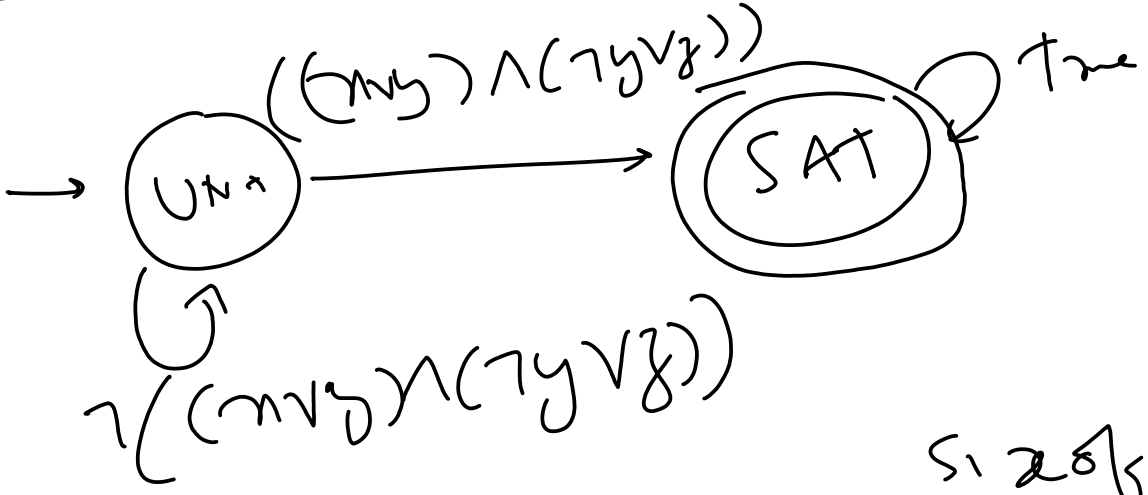
x, y, z

$G((x \vee y) \wedge (\neg y \vee z))$

$=$



$F((x \vee y) \wedge (\neg y \vee z))$



Size of Monitor ↝ $O(2^{|\phi|})$

Monitor for LTL

→ Kupferman & Vardi

Automata theoretic Model checking 1987

LTL → 1977, CTL - 1983,

Special Cases

Safety Prop

$G(\phi)$ ϕ only has G

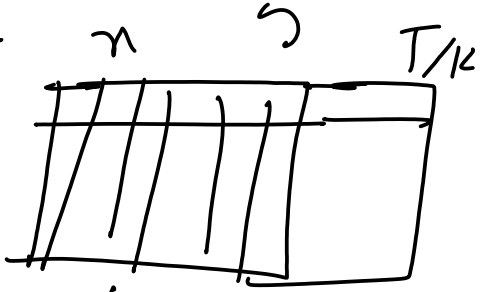
Eventually

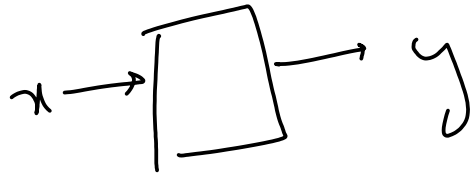
$F(\phi)$ ϕ only has F

1987 - 2003

Symbolic Representation

30 Sith



① 

$\exists x \; S_S(x,y) \wedge \neg R(I,\phi)$

Symbolic rep

1993

BDDs

Binary decision Diagrams

100-1000 Sith

② Program Verf

{Input} Pgm {output}

Polyhedral / Decomposed polyhedral

2017

SMT

2003

SAT

Symbolically exp of paths

10^6

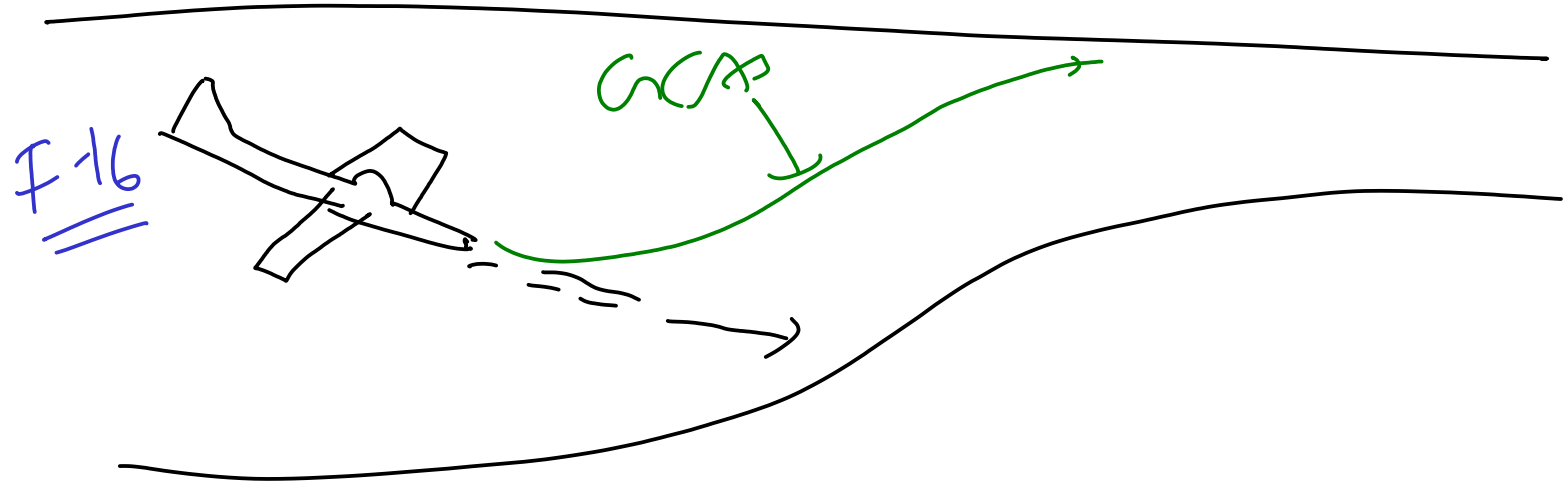
2^{10^6}

- ✗ Details of model checking / SAT / —
- ✗ theoretical aspects of spec
- ✗ Z, Petrinets, Concurrent Sys,

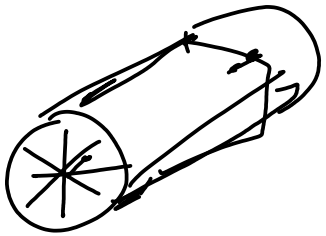
Foundation of Control

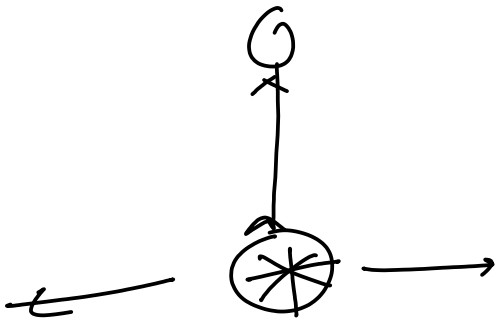
→ Easy to understand, but hard to achieve

- What is control
- Models
- Feedback control 101
- Various dimensions of control

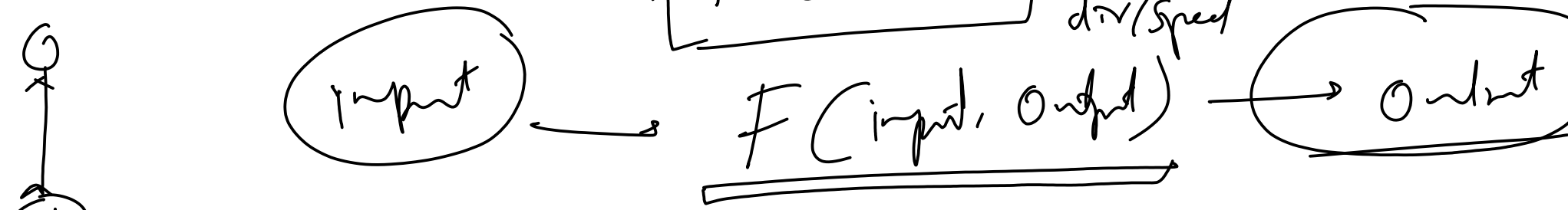


Hover board

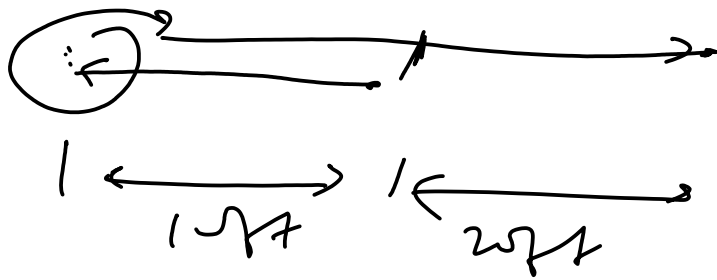




Control



What are the "inputs" to achieve a certain "output" given the system.



Classification

1960s

Panel 1920s

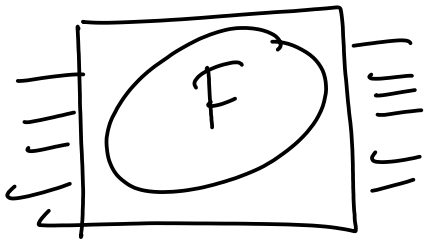
HCI

→ Discrete vs Continuous

→ SISO vs MIMO

Single input
Single output

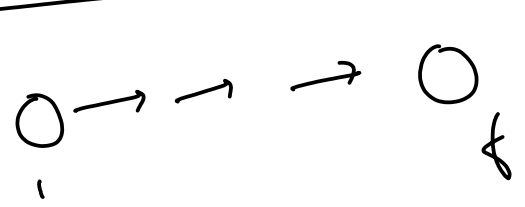
Multiple input
Multiple output

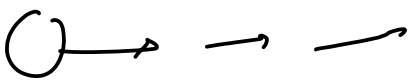


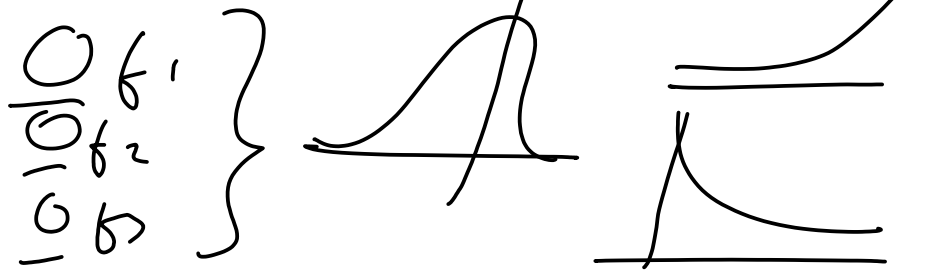
↑ Careful generation

→ Deterministic vs Stochastic

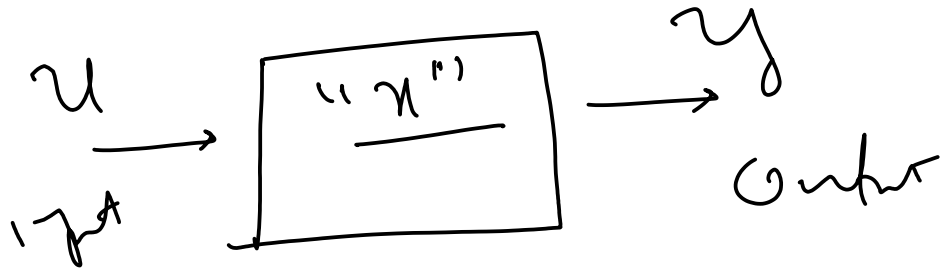
Non







Common Model for Control



$$\dot{x} = f(x, u)$$

$$y = g(x, u)$$

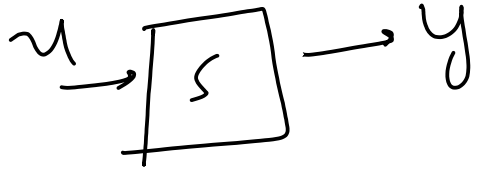
$g(x)$

State space model of Control

1960s

Kalmann

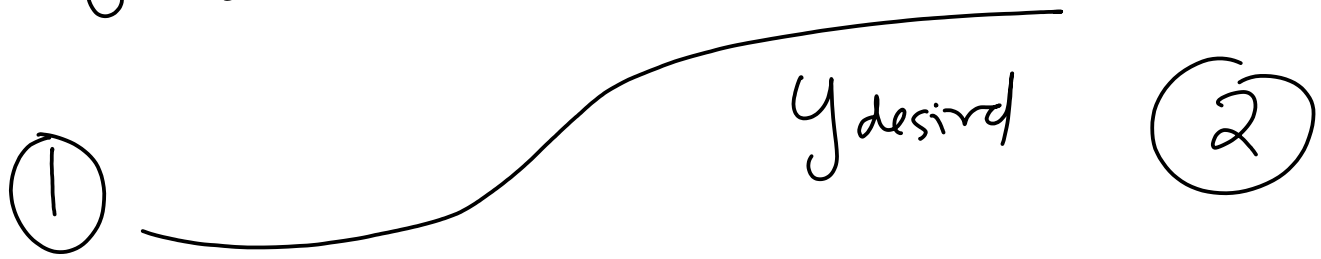
Application



$\dot{x} = f(x,u)$

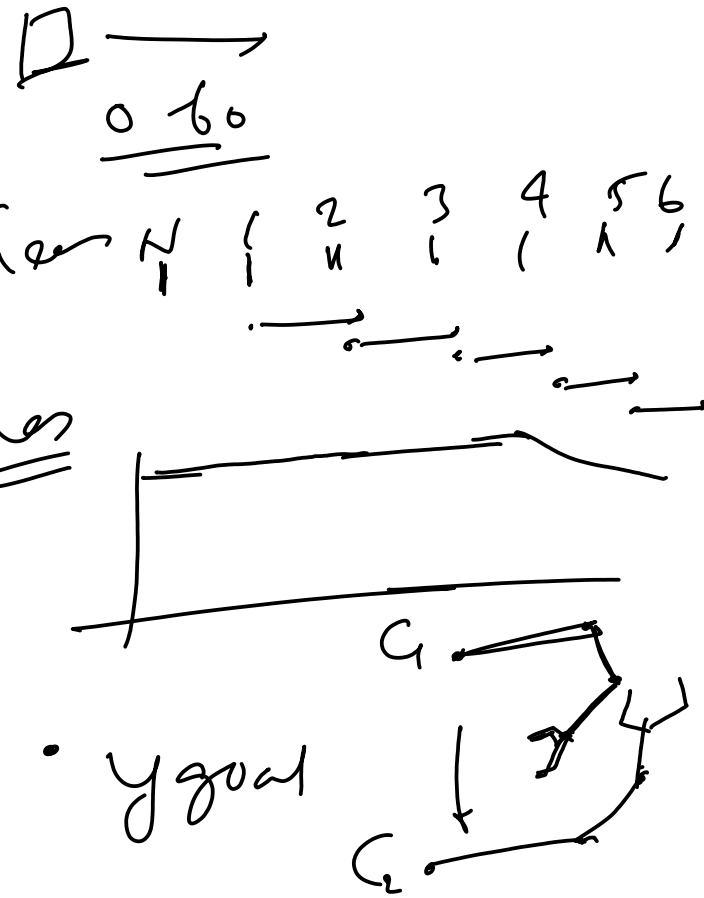
$y = g(x,u)$

1. Tracking
2. Regulation.



Synthesize the inputs ($\hat{u}$)

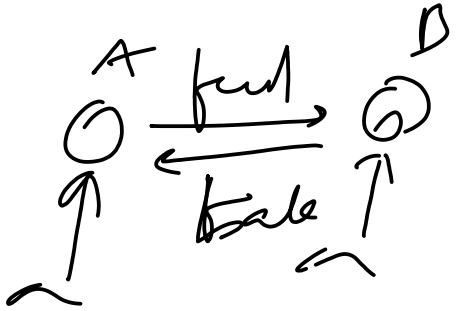
such $y = g(\hat{x}, \hat{u}) \sim y_{desired}$



Synthes. $\hat{u}$

such that $\hat{y}(t) = y_{goal}$

Feedback



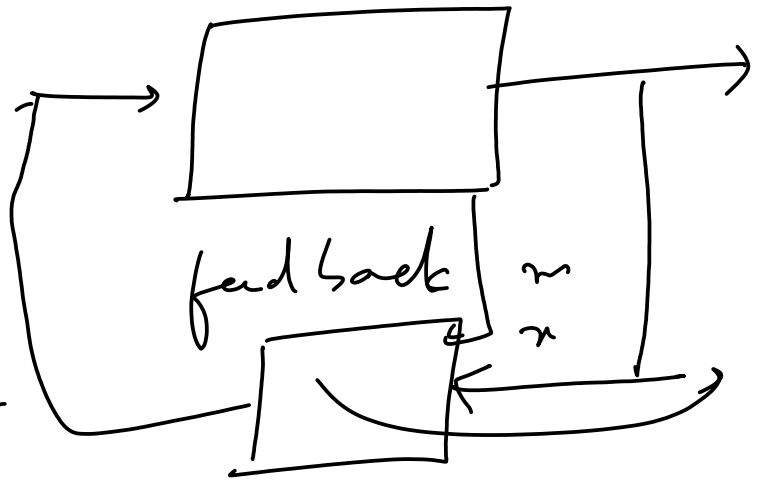
- ~~Suggestion~~
- ~~Mic / Speaker~~

→ Doesn't exist by itself

→ Reaction to an independent action that output feedback was performed.

closed loop

Autonomous Control System



Gear transmission CVT

$u = h(y, n)$

$u_1 = h(y)$

$u_2 = h(n)$ = state feedback