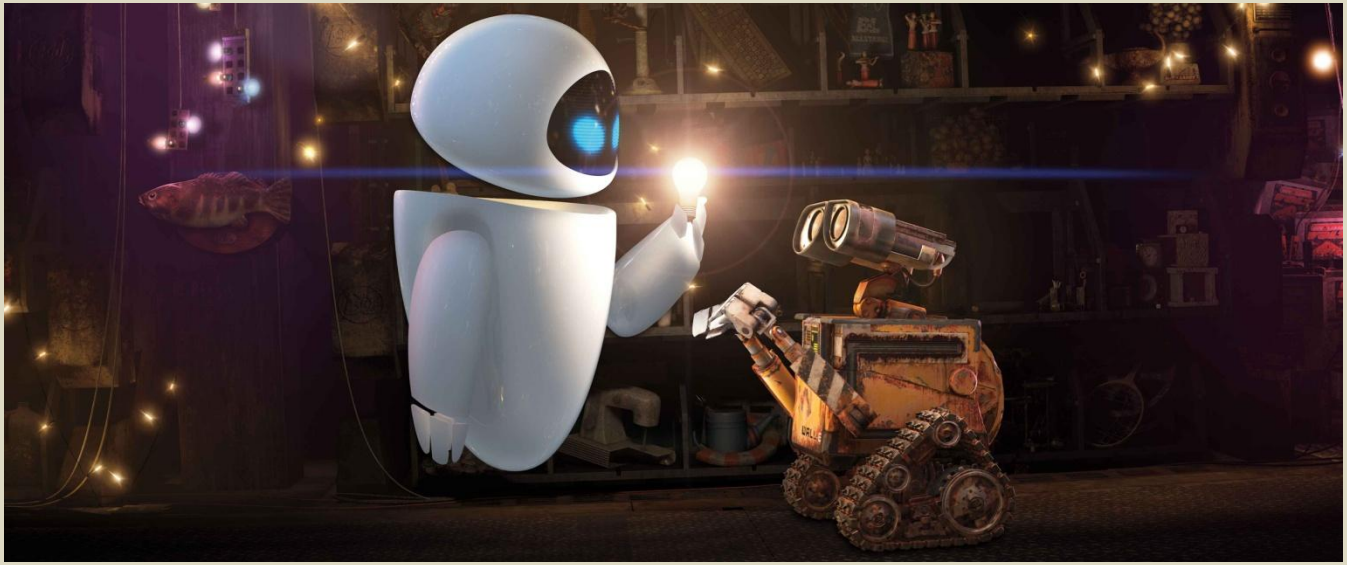
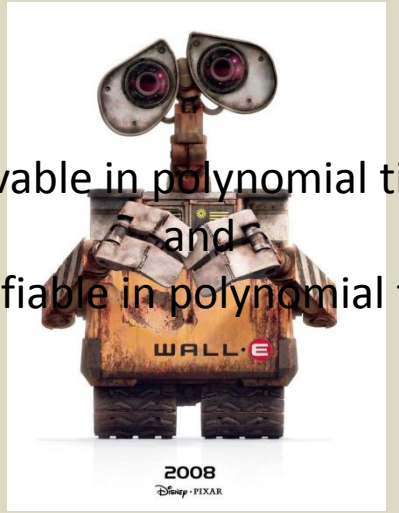
Zero Knowledge Proofs (1)



Suzanne van Wijk & Maaike Zwart

Last time

- Turing Machines
- P and NP

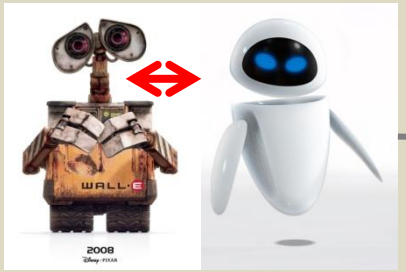


Solvable in polynomial time

and

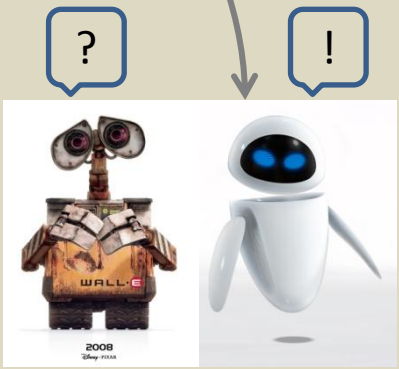
Verifiable in polynomial time

Today



Interactive machines

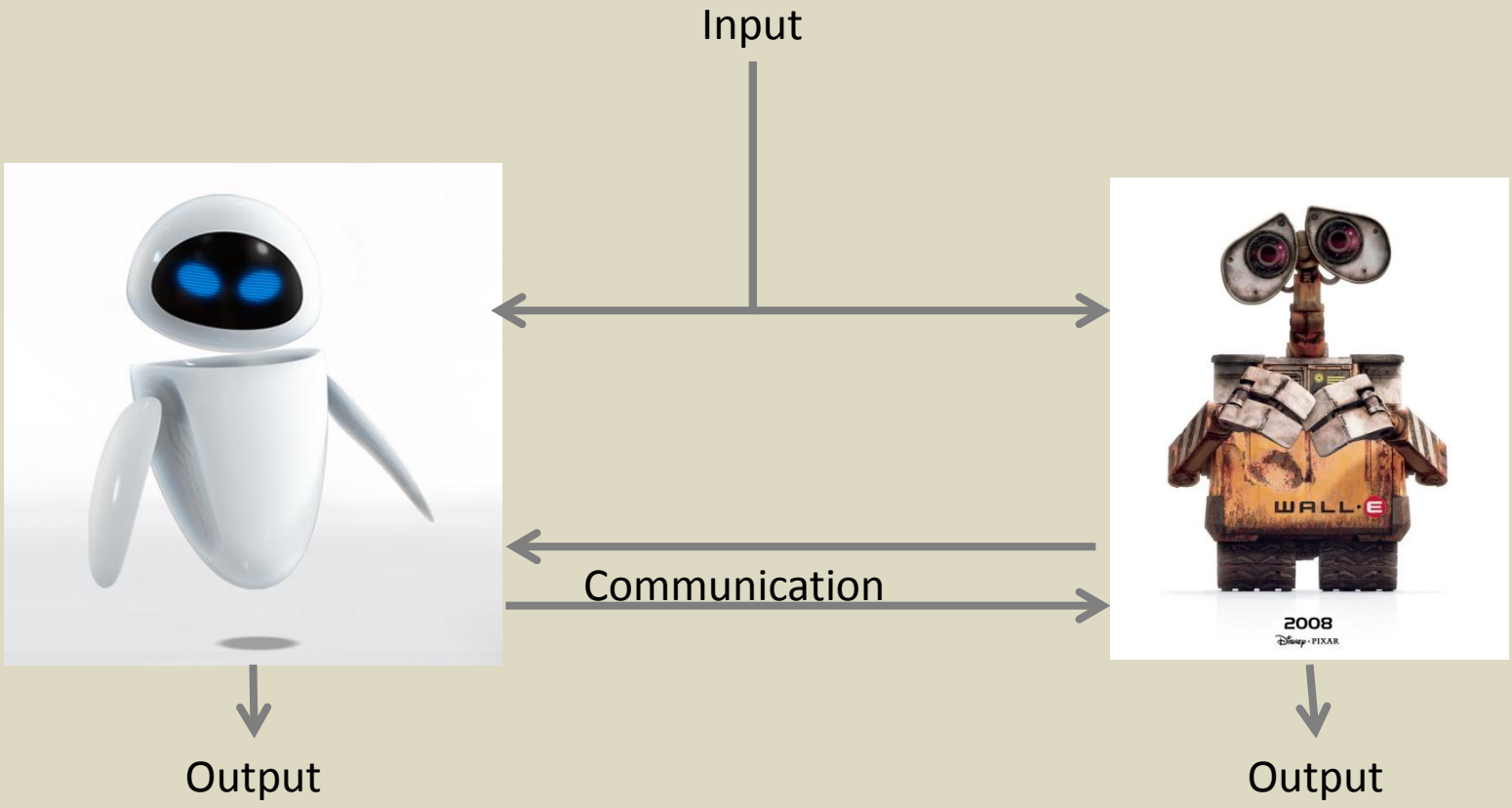
Turing Machines



Interactive Proof Systems

Zero-Knowledge Proofs

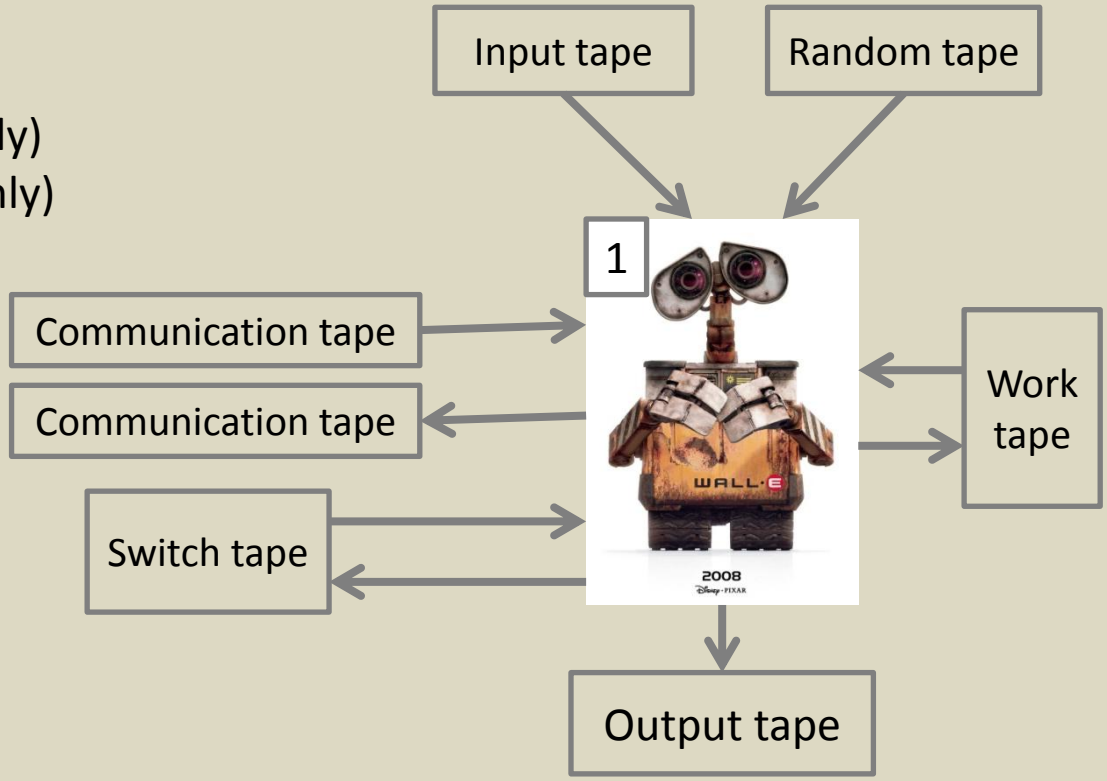
Interactive Machines



Interactive Machines - Formally

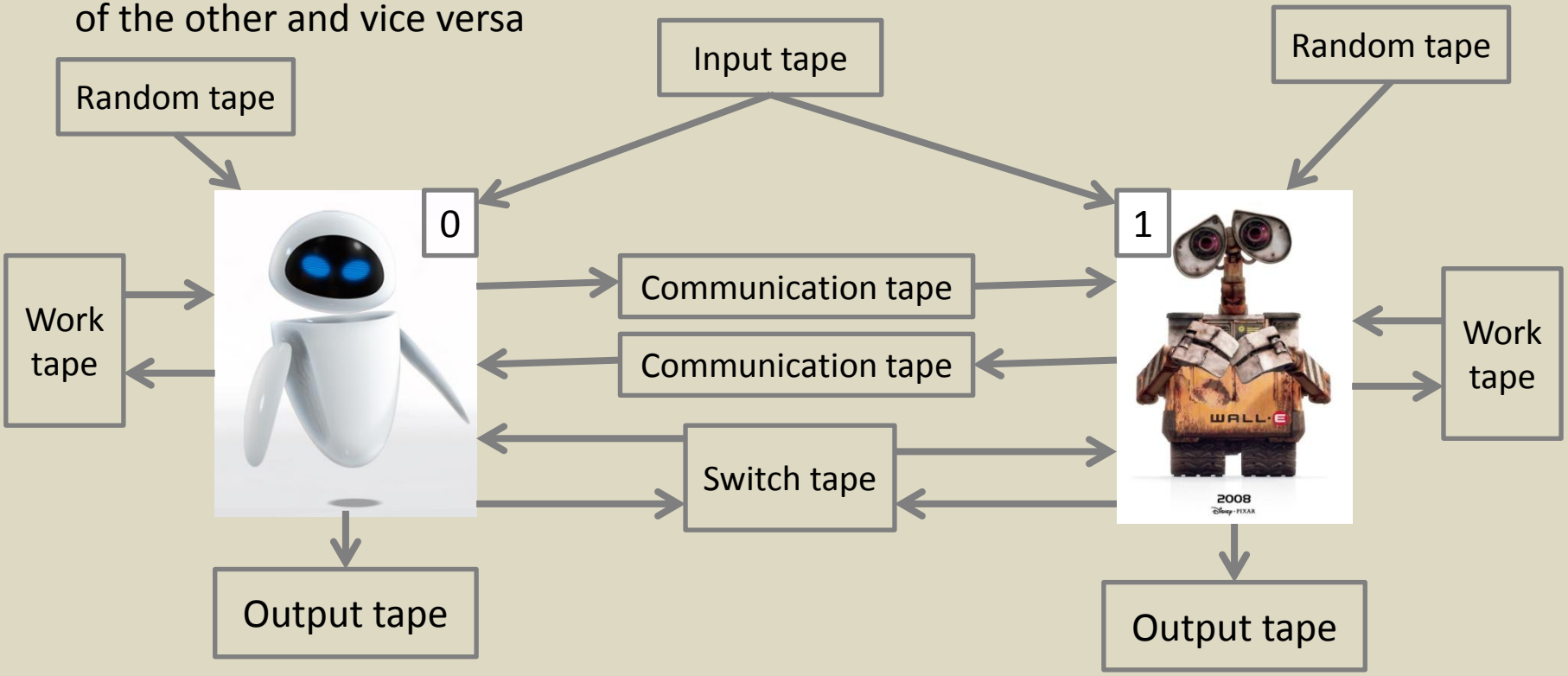
Interactive Turing Machine

- Identity in {0,1}
- Input tape (read-only)
- Random tape (read-only)
- Work tape (read and write)
- Output tape (write-only)
- Communication tape (read-only)
- Communication tape (write-only)
- Switch tape (read and write)



Interactive Machines

Two ITM's are *linked* if
- Their identities are opposite
- They share their input tape and switch tape
- The read-only communication tape of the one is the write-only communication tape of the other and vice versa



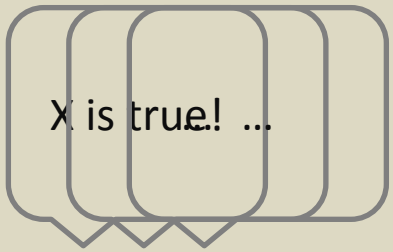
Interactive Proof Systems

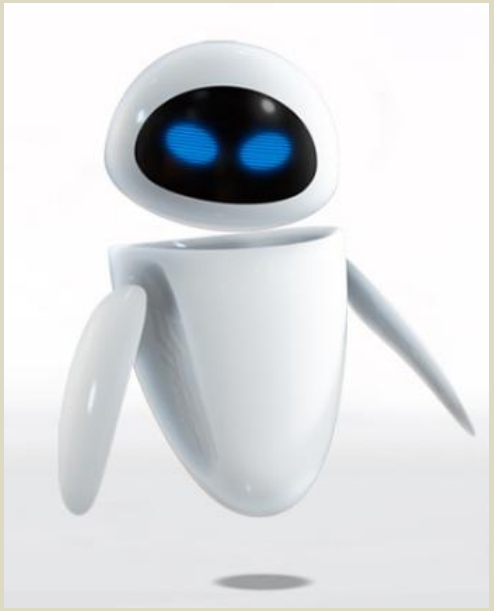
What is a *proof*?

A proof is whatever convinces me
- Shimon Even (1978)

Verification procedure to check the validity of a claim

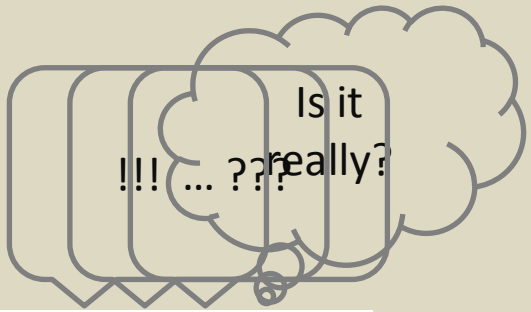
Interactive Proof Systems





Prover

Definition:
Polynomial-time



Verifier

Interactive Proof Systems

We want:
The prover can convince the verifier of a TRUE statement
The verifier cannot be convinced of a FALSE statement (by anyone)

Sounds like:
Completeness
Soundness

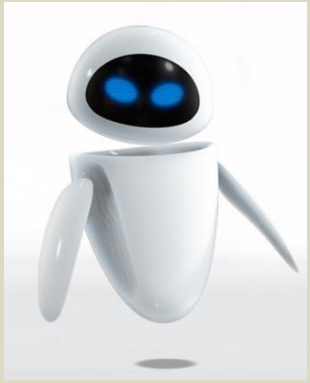
We get:
Since both machines are probabilistic (random tape), these conditions are too

Interactive Proof Systems - Formally

(this is the part where you might want to take some notes)

Interactive Proof Systems

I can tell the difference!



How can Eve prove her claim?

Prove it!

Zero-Knowledge Proofs

Proofs where the verifier *does not gain knowledge* besides that the claim is true

Naor et al. *Applied Kid Cryptography or How To Convince Your Children You Are Not Cheating.* Journal of Craptology. 1999

Knowledge

When do we speak of knowledge gain?

If Alice and Bob are having a conversation, then Bob gains knowledge if he can compute something *after* his conversation with Alice that he could not have computed *before*.

Note that *knowledge* and *information* are two different things!

Simulator

So how do we know whether the verifier doesn't gain knowledge?

If the output of the conversation between prover and verifier can be *simulated* without any interaction with the prover, so based only on the common input
Then the verifier does not gain knowledge

Simulator Ali Baba & the Magical Cave

(1) A forked cave with two dead ends (like so:)

(2) The thief got away fourty days in a row

(3) With the magic words, the dead end dissapears (like so:)

(4) Ali Baba shows the secret without revealing it

(5) His brother wants his 3 minutes of fame as well

(6) Who to believe?!

Quisquater et al. *How to Explain Zero-Knowledge Protocols to Your Children.* 1998

Zero-Knowledge

An interactive proof system is *zero-knowledge* if whatever can be efficiently computed from the input and the interaction with the prover, can also be efficiently computed from the input alone (by a simulator).

Zero-Knowledge - Formally

(again: you might want to take some notes!)

Zero-Knowledge

Next time:

Perfect Zero-Knowledge vs.
Computational Zero-Knowledge vs.
Almost Perfect Zero-Knowledge