Circuits: Depth and Size

TECHNISCHE UNIVERSITÄT DARMSTADT

Complexity Theory

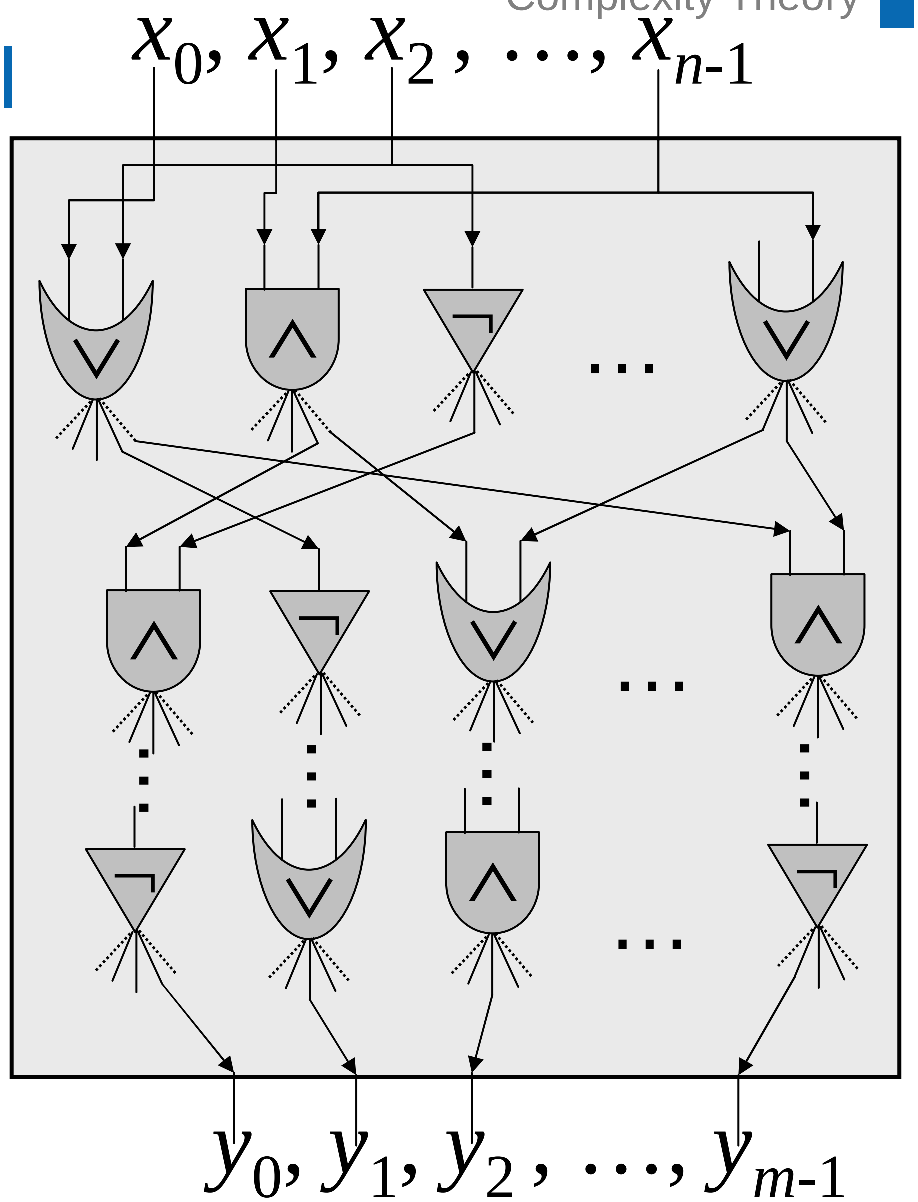
Gates ∨,∧,¬ are universal

unbounded fan-out

fan-in: binary/unary

N-ary: simulate
in depth O(log *N*)

- *n* inputs, *m* outputs
- depth *d* $\Rightarrow$ size $\leq m \cdot 2^d$
- If sorted topologically, evaluation on a TM in time O(size)



Uniformity

Each circuit C has a fixed number of inputs

→ for deciding $L \subseteq \{0,1\}^*$, consider a family (C_n)

$\{1^n : n = \langle M \rangle$ for terminating TM $M\}$ undecidable
to TM, but decidable by some family of circuits:

F. Meyer auf der Heide (1984): knapsack can be
decided by circuit family C_n of polynom.size

New circuit for each n: nonuniform algorithm

Def: Call family C_n of circuits uniform
if some logspace-DTM can,
on input 1^n, output $\langle C_n \rangle$

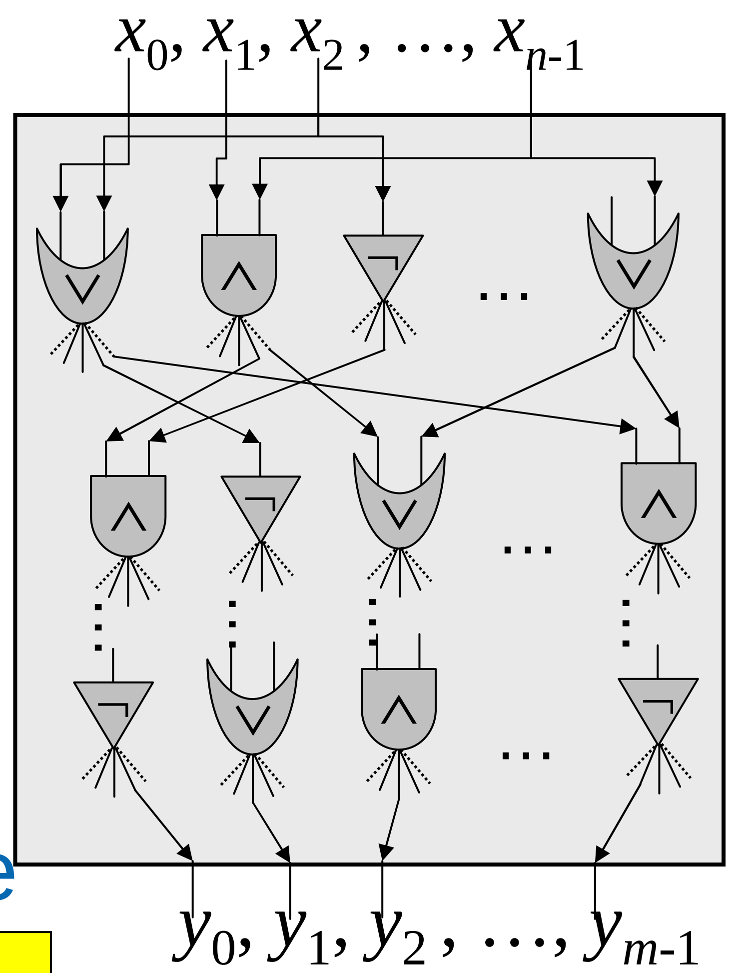
(sorted topologically).

evaluation on a TM
in time poly(size)

Circuit vs. Turing Complexity

Can evaluate a given circuit *C* on a TM
in time O(size) once sorted topologically
and in space O(*m*+depth):
for each gate on level *d*
recursively evaluate its 2
predecessors on levels<*d*

Can simulate a given TM *M*
with input $\underline{x}$ on a circuit
of depth $O\big(S_M(|\underline{x}|)^2\big)$
Reachability + Matrix Powering
of size $O\big(T_M(|\underline{x}|)^2\big)$
: next slide



size ≈ seq. time, depth ≈ space

n inputs, *m* outputs

$\mathcal{P}$-completeness

Reminder: Every $A \in \mathbf{NL} \subseteq \mathbf{P}$ can be solved in parallel time $O(\log^2 n)$ on polynomial size circuits. $\mathbf{NC}^2$

$B \in \mathcal{P}$ called $\mathcal{P}$-hard if $A \leqslant_L B$ holds for every $A \in \mathcal{P}$.

CircuitVal := { $\langle C,\underline{x}\rangle$: Circuit C evaluates to `true` on input assignment $\underline{x}$ } $\in \mathcal{P}$

Theorem: CircuitVal is $\mathcal{P}$-complete. Exercise

$\mathcal{P}$-vollständige Probleme lassen sich vermutlich nicht effizient parallelisieren.

Complexity and Cryptography

A **Public-Key System** with key-pair $(\underline{e},\underline{d})$ consists of two functions $E=E(\underline{e},\underline{x})$ and $D=D(\underline{d},\underline{y})$ such that $D(\underline{d},E(e,\underline{x}))=\underline{x}$ holds for all $\underline{x}$.

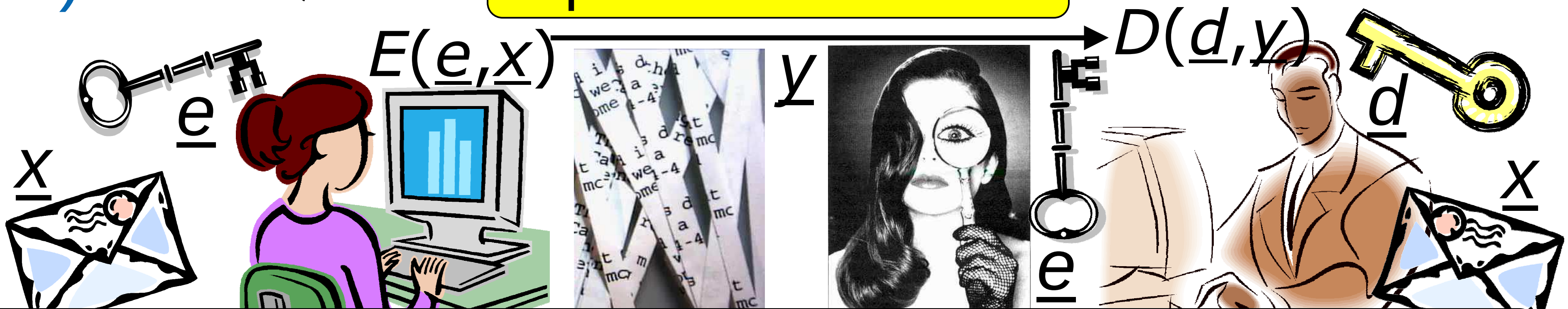
RSA

Call $f:\Sigma^*\to\Sigma^*$ a **one-way function** if

i) injective and $|\underline{x}|^k \geq |f(\underline{x})| \geq |\underline{x}|^{1/k}$ for some k

ii) computable in polynomial time (i.e. $f\in\mathfrak{FP}$)

iii) but $f^{-1}\notin\mathfrak{FP}$ impossible if $\mathfrak{P}=\mathfrak{NP}$! $\Rightarrow f^{-1}\in\mathfrak{FNP}$



encrypt with public key $\underline{e}$, decrypt with private key $\underline{d}$.

One-Way Functions and $\mathcal{UP}$

TECHNISCHE UNIVERSITÄT DARMSTADT
Complexity Theory

Definition: Call a NTM <u>unambiguous</u> if, for any input $\underline{x}$, it has at most one accepting computation.

$\mathcal{P} \subseteq \mathcal{UP} \subseteq \mathcal{NP}$

$\mathcal{UP}$ = {languages accepted by unambiguous polytime NTMs}

Theorem: $\mathcal{P} \neq \mathcal{UP}$ iff one-way functions exist.

Proof: a) For one-way f define $L := \{ (\underline{x},\underline{y}) \mid \exists \underline{z} \leq \underline{x}: f(\underline{z})=\underline{y} \}$

Then $L \in \mathcal{UP}$. And $\underline{y} \to f^{-1}(\underline{y})$ can be evaluated using binary search with polynomially many queries for L: $L \notin \mathcal{P}$

b) Let $L \in \mathcal{UP} \setminus \mathcal{P}$ be decided by unambiguous NTM U.

For $\underline{x}$ an accepting computation of U on $\underline{y}$, let $f(\underline{x}):=1\underline{y}$.

For other arguments let $f(\underline{x}):=0\underline{x}$.

This is one-way!

Call $f:\Sigma^* \to \Sigma^*$ a one-way function if injective and $|\underline{x}|^k \geq |f(\underline{x})| \geq |\underline{x}|^{1/k}$ and $f \in \mathcal{FP}$ ($\Rightarrow f^{-1} \in \mathcal{FNP}$) but $f^{-1} \notin \mathcal{FP}$

Issues with Cryptographic Complexity

Definition: Call a NTM unambiguous if, for any input $\underline{x}$, it has at most one accepting computation. $\mathcal{P} \subseteq \mathcal{UP} \subseteq \mathcal{NP}$

$\mathcal{UP}$ = {languages accepted by unambiguous polytime NTMs}

Theorem: $\mathcal{P} \neq \mathcal{UP}$ iff one-way functions exist.

- It might be $\mathcal{P} = \mathcal{UP} \neq \mathcal{NP}$
- No complete problem known for $\mathcal{UP}$
- *worst-case* complexity:

  f might be efficiently invertible on *many* practical inputs
- randomized algorithms are not deterministic yet practical

Cannot eff. check whether given NTM is unambiguous

Call $f:\Sigma^*\to\Sigma^*$ a one-way function if injective and $|\underline{x}|^k \geq |f(\underline{x})| \geq |\underline{x}|^{1/k}$ and $f\in\mathcal{FP}$ ($\Rightarrow f^{-1}\notin\mathcal{FNP}$) but $f^{-1}\notin\mathcal{FP}$