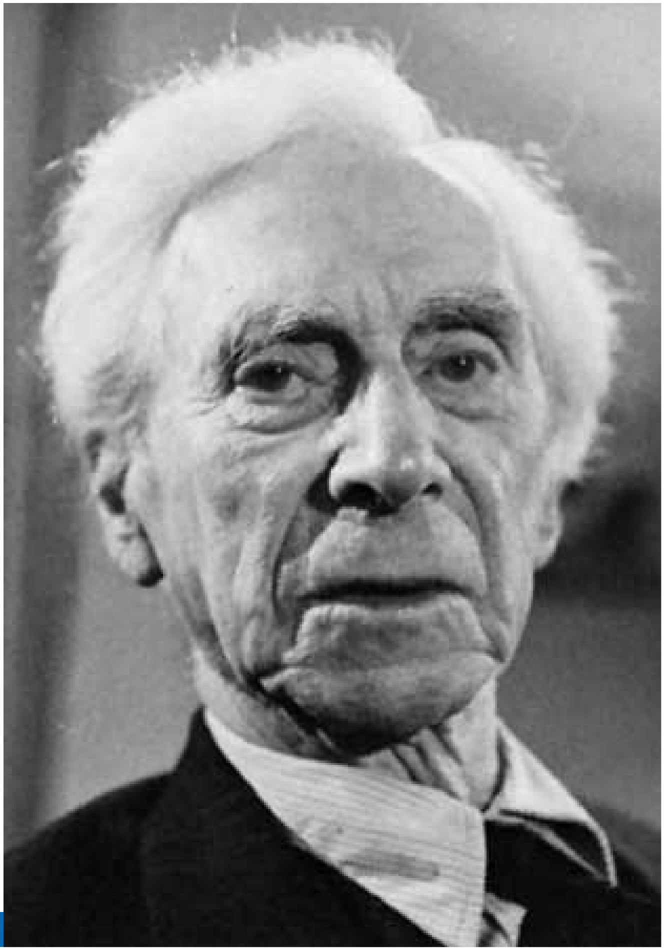
Bertrand Russel (1872-1970):

„Darin besteht das Wesen der Wissenschaft:
Zuerst denkt man an etwas, das wahr sein könnte.
Dann sieht man nach, ob es der Fall ist
und im allgemeinen ist es nicht der Fall.“



Erweiterung:

Oft kann man es nicht beweisen
noch widerlegen.

Damit muß man umgehen (lernen)!

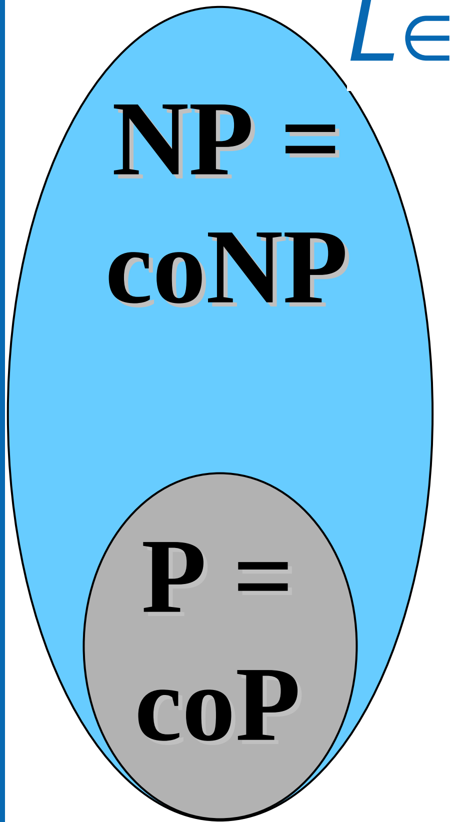
Szenarien für P≠NP

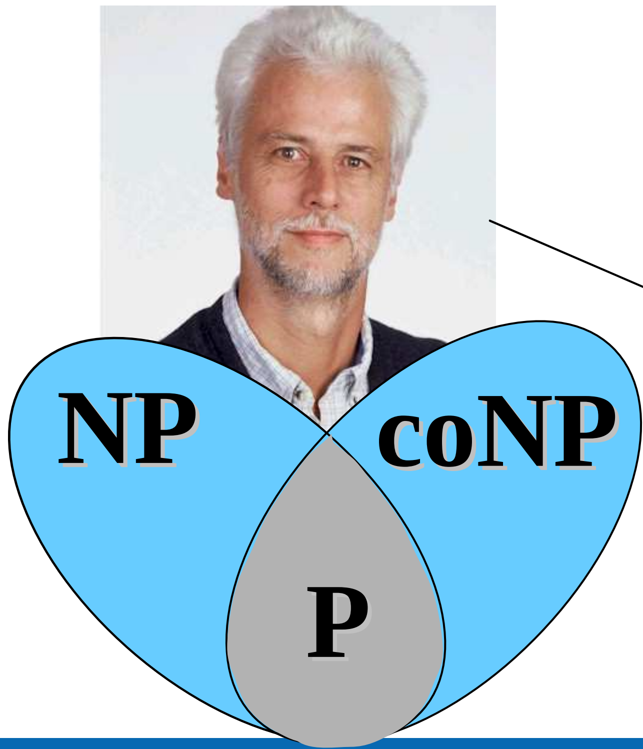
coNP := { L : das Komplement von L liegt in **NP** }

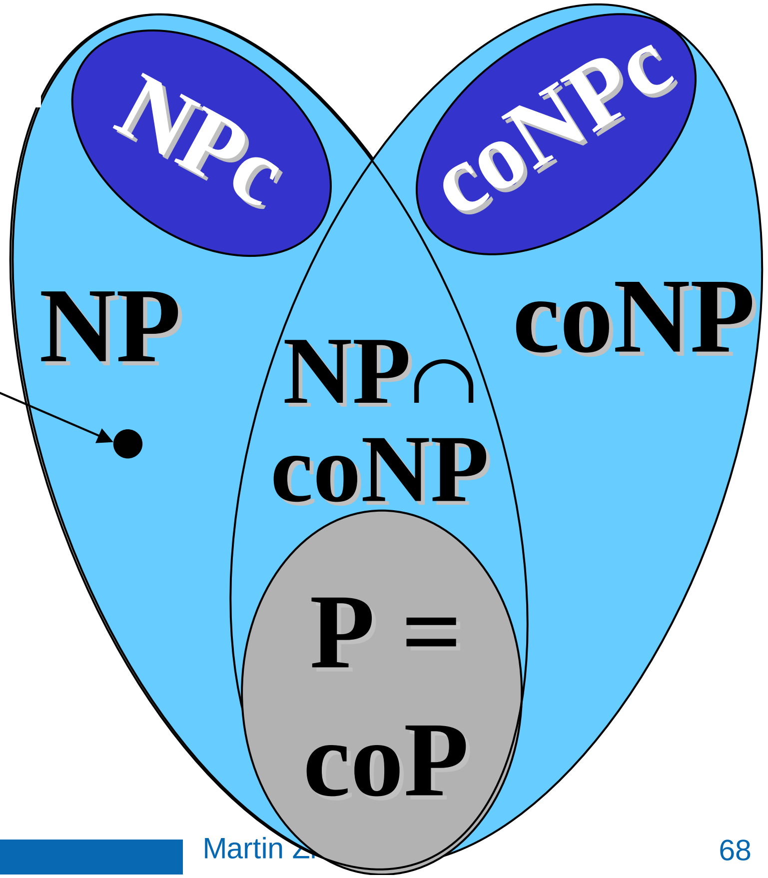
unSAT ={Bool'Formel $\varphi(x_1,\ldots,x_n)$ falsch $\forall x$} **coNPc**

Theorem (Ladner 1975): Falls **P≠NP**, so gibt es

$L \in$ **NP** \ (**P**∪**NPc**)







Zeit: $\mathbf{P} \subseteq \mathbf{NP}$ √ $\mathbf{P} = \mathbf{NP}$? \$1 Mio

Platz: $\mathbf{PSPACE} \subseteq \mathbf{NPSPACE}$ √

Walter Savitch (1970): $\mathbf{PSPACE} = \mathbf{NPSPACE}$

Genauer gilt:

$\mathbf{NSPACE}(s(n)) \subseteq \mathbf{DSPACE}(s(n)^2)$

sofern $s(n)$ konstruierbar ist.

Def: …d.h. wenn eine DTM bei Eingabe „1^n" Ausgabe „$1^{s(n)}$" produzieren kann in Zeit $O(s(n))$.

Beispiele: Polynome, Übung…

Sei M (nicht-/deterministische) TM,
$s(n)$-platzbeschränkt und $t(n)$-zeitbeschränkt.

Erinnerung: $L(M) \leqslant_p \mathrm{QBF}$:

$\mathrm{succ}_\ell(U,U'')$:= «U'' ist Nachfolgekonfig. von U, die nach höchstens 2^ℓ Rechenschritten erreicht werden kann»

$\Leftrightarrow \exists U'\colon \mathrm{succ}_{\ell-1}(U,U') \wedge \mathrm{succ}_{\ell-1}(U',U'') \qquad \Leftrightarrow$

$\big(\exists U' \,\forall V,W\colon ((V=U \wedge W=U') \vee (V=U' \wedge W=U'')) \Rightarrow \mathrm{succ}_{\ell-1}(V,W)\big)$

Dann rekursiv weiter…

Hier: determin. $s(n)^2$-platzbeschränkter Algorithmus

Algorithmus „erreichbar“

erreichbar(U,U'',ℓ)

// Ist U'' von U aus

// in $\leq 2^\ell$ Schritten erreichbar?

Falls ℓ=0, **`return`**($U=U'' \vee U \vdash U''$)

Falls ℓ≥1, teste für alle U' rekursiv:

erreichbar(U,U',ℓ-1) <u>und</u>

erreichbar(U',U'',ℓ-1)

Falls beides ja, **`return(true)`**

`return(false)`

Platzbedarf: $f(\ell) \leq O(S) + f(\ell-1) \leq O(S\cdot\ell)$

NSPACE($s(n)$)$\subseteq$DSPACE($s(n)^2$)

NTM N sei $s(n)$-platzbeschränkt;

DTM M simuliert N auf Eingabe $\underline{w}$:

Berechne $S:=s(|\underline{w}|)$

und markiere so viel Platz auf dem Band.

[Nach Vor. „*platzkonstruierbar*" geht das!]

Berechne $\ell:=\log(T(|\underline{w}|)) \leq c\cdot S$

und U:=Startkonfig von N (S Zellen),

U'':=Endkonfig von N (o.B.d.A. eindeutig)

Aufruf: erreichbar(U,U'',ℓ). Platz O(S·ℓ)

3.2 Classes L, NL, and L-reductions

L ⊆ NL ⊆ P ⊆ NP ⊆ PSPACE=NPSPACE ⊆ EXP

L := { problems decidable using O(log *n*) tape cells }
but already the input uses $n=|\underline{x}|$ tape symbols.

Def: DTM/NTM with separate *read-only* input tape, count only working/output tape usage

→ **L**, **NL**

Exercise: NL ⊆ P

Example: $\{ 0^m 1^m : m \in \mathbb{N} \}$
- check the form 0*1*
- count #0s
- and #1s;
- compare these numbers:

only O(log m) tape cells *in addition* to the input!

Space-Bounded Computation

- Input tape: read-only, for free
- working tape: read/write, incurs cost
- output tape: write-only, one-way, for free

$\to$ *streaming computation*

Def: $A \leqslant_{\mathrm{L}} B$ iff there is some log-space computable $f:\Sigma^*\to\Sigma^*$ s.t. $\underline{x}\in A \Leftrightarrow f(\underline{x})\in B$.

Call A **NL**-hard if every $B\in$ **NL** satisfies $B \leqslant_{\mathrm{L}} A$,

NL-complete if in addition $A\in$ **NL** holds.

L $\subseteq$ NL $\subseteq$ P $\subseteq$ NP $\subseteq$ PSPACE=NPSPACE $\subseteq$ EXP

Example Problem in NL

- directed s-t-connectivity **dirPATH** :=

  $\{ \langle G,s,t\rangle : G=(V,E)$ directed graph,
  $s,t\in V$ with a path from s to t $\}$

  Algorithm directedReachable(V,E,s,t,ℓ):
  - while $\ell>0$ and $s\neq t$ do
    - follow some edge $(s,u)\in E$ leaving from s
    - let $s:=u$, $\ell:=\ell-1$
  - if $s=t$ return(`true`), else return(`false`).
- $\ell:=|V|-1$, s, u each use $O(\log|V|)$ bits.

Reductions

- polynomial-time *many-one*: $A \leqslant_p^m B$

  f:Σ*→Σ* **P**-computable s.t.: $\underline{x} \in A \;\Leftrightarrow\; f(\underline{x}) \in B$

  – in general $B \not\leqslant_p^m \Sigma^* \setminus B$ (example?)
- log-spacebounded *many-one*: $A \leqslant_L^m B$

  f:Σ*→Σ* **L**-computable s.t.: $\underline{x} \in A \;\Leftrightarrow\; f(\underline{x}) \in B$

  – $A \leqslant_L^m B \quad \Rightarrow \quad A \leqslant_p^m B$ (proof?)
- polynomial-time *Turing* Reduction: $A \leqslant_p^T B$

  A can be solved in polynomial time by aid of oracle queries to *B*: $A \in \mathbf{P}^B$

  – $A \leqslant_p^m B \Rightarrow A \leqslant_p^T B \Rightarrow A \leqslant_p^T \Sigma^* \setminus B$ (proof?)
- Further reductions: *truthtable*, parsimonious…