Sipser–Gács–Lautemann

Theorem: $\mathbf{BPP} \subseteq \Sigma_2 \cap \Pi_2$ *„Derandomization“*

Notation: $\underline{y},\underline{z} \in \{0,1\}^m \Rightarrow \underline{y} \oplus \underline{z}$:= componentw. xor

Now fix $p(n)$-time NTM M for $L \in \mathbf{BPP}$.

For input $\underline{x}$, M guesses a random string $\underline{r} \in \{0,1\}^{p(n)}$.

$R_M(\underline{x})$:= { all $\underline{r} \in \{0,1\}^{p(n)}$ leading M to accept $\underline{x}$ } $\in \mathbf{P}$

$\underline{x} \in L \Rightarrow \mathrm{Card}\left(R_M(\underline{x})\right) \geq (1-2^{-n}) \cdot 2^{p(n)}$

$\underline{x} \notin L \Rightarrow \mathrm{Card}\left(R_M(\underline{x})\right) \leq 2^{-n} \cdot 2^{p(n)}$

→Exercise

Goal: $L = \{ \underline{x} \mid \exists \underline{t}_1,\ldots,\underline{t}_{p(|\underline{x}|)} \in \{0,1\}^{p(|\underline{x}|)} :$

$\forall \underline{y} \in \{0,1\}^{p(|\underline{x}|)} : \exists i=1,\ldots,p(|\underline{x}|): \underline{y} \oplus \underline{t}_i \in R_M(\underline{x}) \}$ $\in \Sigma_2$

$\Leftrightarrow \{0,1\}^p \subseteq \bigcup_i (R_M(\underline{x}) \oplus \underline{t}_i)$

Erdős' Probabilistic Method

TECHNISCHE UNIVERSITÄT DARMSTADT
Complexity Theory

Hypothesis: $R \subseteq \{0,1\}^p$, $\mathrm{Card}(R) \geq (1-2^{-n}) \cdot 2^p$

Claim: $\exists \underline{t}_1,\ldots,\underline{t}_p \in \{0,1\}^p : \forall \underline{y} \in \{0,1\}^p \quad \exists j \leq p: \ \underline{y} \oplus \underline{t}_j \in R$

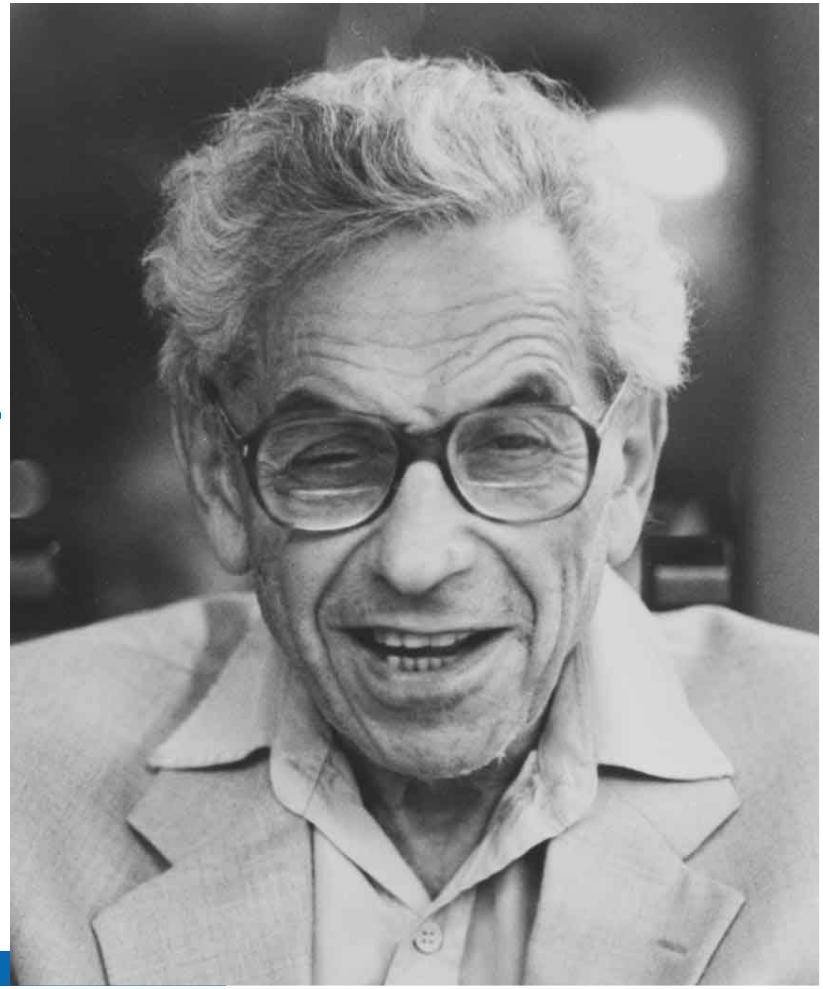
Probablistic proof:

Consider random $\underline{t}_1,\ldots,\underline{t}_p$.

For any fixed $\underline{y} \in \{0,1\}^p$:

- $\Pr_{\underline{t}}[\ \underline{y} \oplus \underline{t} \notin R\ ] \leq 2^{-n}$
- $\Pr_{\underline{t}_1,\ldots,\underline{t}_p}[\ \forall j \leq p: \underline{y} \oplus \underline{t}_j \notin R\ ] \leq (2^{-n})^p$
- $\Pr_{\underline{t}_1,\ldots,\underline{t}_p}[\ \exists \underline{y} \in \{0,1\}^p: \forall j \leq p: \underline{y} \oplus \underline{t}_j \notin R\ ] \leq 2^p \cdot (2^{-n})^p < 1$ ■

↓ Exercise



Zusammenfassung I

- Asymptotik, Rechenmodelle, Ressourcen
- Vergleich von Problemen: Reduktion
- Turingmaschinen und ihre Programmierung
- polynom. Laufzeit und Speicher: **P** und **PSPACE**
- Beispielprobleme: Eulerkreis, Hamiltonkreis (EC), Kantenüberdeckung, Knotenüberdeckung (VC), TSP, Clique, Independent Set, Erfüllbarkeit (SAT, 3SAT)
- polynomielle Reduktionen zwischen ihnen
- **NP**-Vollständigkeit, Satz von Cook-Levin
- Approximationsalgorithmen und Güte (VC, metr. TSP, Knapsack); Grenzen der Approximierbarkeit

Zusammenfassung II

- **PSPACE**-Vollständigkeit und QBF
- Gewinnstrategien für ein 2-Player Spiel
- nichtdeterministischer Platz**:** Satz von Savitch
- und Satz von Immerman&Szelepcsényi
- **NL** und Parallelcomputing; Schaltkreise
- Komplexität und Kryptographie (**UP**)
- Probabilistische Komplexitätsklassen **RP**, **BPP**
- polynomielle Hierarchie $\mathbf{P}^{\mathbf{NP}}$, $\mathbf{NP}^{\mathbf{NP}}$, $\mathbf{P}^{\mathbf{NP}^{\mathbf{NP}}}$ etc
- $\mathbf{BPP} \subseteq \mathbf{NP}^{\mathbf{NP}} \cap \mathbf{coNP}^{\mathbf{NP}}$

Complexity Zoo

no lower bounds proven!

only 'relative' ones:

e.g. „If **SAT**$\in$**P**, then **NP**=**P**“

Method: reduction,

i.e. algorithm design + analysis (again).

Sequel: „*Advanced Complexity Theory*“

time versus space

hierarchy theorems

Baker, Gill & Solovay

- Kolmogorov Complexity
- 1-tape DTMs

(strong) Church-Turing Hypothesis:

Anything that should be considered efficiently *computable in practice can be computed by a Turing machine.* polytime

- Sound upper and lower bounds for simulation problems in physics
- Topological and algebraic lower bounds for computational problems over real numbers