Natürliche Beweise

Nicht-uniforme Berechnungsmodelle

Ist die $\mathtt{P} \stackrel{?}{=} \mathtt{NP}$ Frage vielleicht deshalb so schwer, weil wir sie mit „**gängigen**" Methoden gar nicht beantworten können?

- Es ist $\mathtt{P} \subseteq \mathtt{P/poly}$, denn jede Sprache in $\mathtt{P}$ kann von Schaltkreisen polynomieller Größe erkannt werden: Es genügt der Nachweis, dass (irgend)eine $\mathtt{NP}$-vollständige Sprache nicht zu $\mathtt{P/poly}$ gehört.

Was weiß man über die Größe oder Tiefe von Schaltkreisen für boolesche Funktionen $f : \{0,1\}^n \to \{0,1\}$?

Größe und Tiefe von Schaltkreisen (1/2)

(a) Für jede Funktion $f : \{0,1\}^n \to \{0,1\}$ gilt

$$\mathtt{DEPTH}(f) \leqslant n + \lceil \log_2 n \rceil \text{ sowie } \mathtt{SIZE}(f) \overset{\text{Lupanov}}{\leqslant} (1 + o(1)) \cdot \frac{2^n}{n}$$

(b) Für mehr als die Hälfte aller Funktionen $g : \{0,1\}^n \to \{0,1\}$ ist

$$\mathtt{DEPTH}(g) \geqslant n - \mathcal{O}(\log_2 n) \text{ und } \mathtt{SIZE}(g) = \Omega(\frac{2^n}{n}).$$

Die meisten Sprachen sind „hammer-hart“.

Benutze ein **Abzählargument**:

- Zähle die Anzahl der Schaltkreise vorgegebener Größe oder Tiefe
- und zähle die Anzahl boolescher Funktionen!

Größe und Tiefe von Schaltkreisen (2/2)

Welche **unteren** Schranken sind für *konkrete* boolesche Funktionen bekannt?

- Lineare untere Größen-Schranken und logarithmische untere Tiefen-Schranken.
  - Z.B. für alle Funktionen f, die von jeder Eingabe abhängen, wenn es also für jedes $i \in \{1, \ldots, n\}$ eine Eingabe $x \in \{0,1\}^n$ mit
    $$f(x) \neq f(x \oplus e_i)$$
    gibt, wobei $e_i \in \{0,1\}^n$ das Wort mit einer Eins nur in Position i ist.
  - Gegenwärtiger Weltrekord: Die untere Größenschranke $5n - o(n)$.
- Für eine Boolesche Funktion $f : \{0,1\}^n \to \{0,1\}$ ist
  (a) die Empfindlichkeit e_x für Eingabe x die Anzahl der Bitpositionen i für die $f(x) \neq f(x \oplus e_i)$ gilt.
  (b) Die **Empfindlichkeit** von f ist die durchschnittliche Empfindlichkeit $e = \frac{1}{2^n} \sum_{x \in \{0,1\}^n} e_x$ einer Eingabe.

  Bekannt: $f \in \mathrm{AC}^0 \implies$ die Empfindlichkeit von f ist höchstens poly-log(n).
- Für monotone Schaltkreise – $\{\vee, \wedge\}$-Schaltkreise ohne Negationsgatter – sind exponentielle untere Größenschranken und lineare Tiefenschranken bekannt.

Wie könnten Argumente aussehen, die für eine Familie

$$f = (f_n \mid n \in \mathbb{N})$$

boolescher Funktionen nachweisen, dass f *keine* Schaltkreise der Größe $\mathcal{O}(n^c)$ hat?

$\mathbf{B_n}$ bezeichnet die Menge der Booleschen Funktionen mit n Eingabebits.

(a) $\mathcal{C} = (C_n \mid n \in \mathbb{N})$ heißt **kombinatorische Eigenschaft**, falls $C_n \subseteq B_n$.

(b) $\mathcal{C} = (C_n \mid n \in \mathbb{N})$ ist **natürlich** (gegen $\mathtt{SIZE}(n^c)$), falls

   (1) $\mathcal{C}$ **konstruktiv** ist: Wenn $f_n \in B_n$ durch ihre Funktionstabelle spezifiziert ist, dann kann in Zeit polynomiell in 2^n entschieden werden, ob $f_n \in C_n$, d.h. ob f die Eigenschaft $\mathcal{C}$ besitzt.

   (2) $\mathcal{C}$ **hinreichend groß ist**: Es ist $|C_n| \geqslant 2^{-n} \cdot |B_n|$ für alle $n \in \mathbb{N}$.

   (3) $\mathcal{C}$ **nützlich** gegen $\mathtt{SIZE}(n^c)$ ist: Wenn $f = (f_n \mid n \in \mathbb{N})$ die Eigenschaft $\mathcal{C}$ für unendlich viele Eingabelängen n hat, gehört f **nicht** zu $\mathtt{SIZE}(n^c)$.

Natürliche Beweise (2/2)

Wir untersuchen also mögliche Beweise für

$$\mathtt{NP} \not\subseteq \mathtt{P/poly},$$

die

- konstruktiv-nachweisbare,
  - die Eigenschaft sollte überprüfbar sein
- von vielen Funktionen erfüllte Eigenschaften aufstellen,
  - die Eigenschaft sollte nicht exotisch sein
- wobei diese Eigenschaften nur von schwierigen Funktionen erfüllt wird.

Natürliche Beweise und AC^0

$\mathtt{SIZE}_{\mathbf{d}}(\mathbf{n^c})$ ist die Klasse aller Funktionen mit Schaltkreisen der Tiefe *höchstens d* und der Größe höchstens n^c.

Die Eigenschaft $\mathbf{C_n}$ treffe auf $f \in B_n$ genau dann zu, wenn die **Empfindlichkeit von f** mindestens $n/4$ ist. Es gelte $\mathcal{C} = (\mathbf{C_n} \mid \mathbf{n} \in \mathbb{N})$.

1. $\mathcal{C}$ ist **konstruktiv**, denn die Empfindlichkeit ist in Zeit $2^{O(n)}$ berechenbar.
2. $\mathcal{C}$ ist **hinreichend groß**, denn Funktionen haben hochwahrscheinlich eine Empfindlichkeit von mindestens $n/4$.
3. Man kann zeigen, dass $\mathcal{C}$ **nützlich** gegen $\mathtt{SIZE}_{\mathbf{d}}(\mathbf{n^c})$ für $c \in \mathbb{N}$ ist.

$\mathcal{C}$ ist ein **natürlicher Beweis** gegen $\mathtt{SIZE}_d(n^c)$, leider aber nicht gegen $\mathtt{SIZE}(n^c)$.

Haben wir die richtigen Eigenschaften gefordert?

- **Hinreichende Größe**.
  - Fast alle Funktionen in B_n sind Zufallssfunktionen und die Berechnung von Zufallsfunktionen ist schwierig.
  - Eine kombinatorische Eigenschaft $\mathcal{C}$, die von einer kleinen Minderheit angenommen wird, deckt nur exotische Schwierigkeitseigenschaften auf?!
    - Ausgeschlossen ist die Existenz einer solchen Eigenschaft aber nicht.
- **Konstruktivität**.
  - Idealerweise kann mit nicht zu großem Aufwand überprüft werden, ob eine boolesche Funktion Eigenschaft $\mathcal{C}$ besitzt.
  - Natürliche Beweise erfassen nur konstruktive Eigenschaften, aber
  - exponentielle Zeit $2^{O(n)}$, oder polynomielle Zeit in der Länge der Funktionstabelle erlaubt die Überprüfung vieler vernünftiger Eigenschaften?!

Natürliche Beweise unterscheiden boolesche PRFs und boolesche Zufallsfunktionen

Boolesche PRFs

Wie groß müssen Schaltkreise sein, die PRFs von Zufallsfunktionen unterscheiden?

(a) $\mathcal{F} = (f_\ell : \ell \in \{0,1\}^*)$ ist eine Familie von **PRFs** der **Komplexität** $s : \mathbb{N} \to \mathbb{N}$, wenn

- f_ℓ in Zeit polynomiell in $|\ell|$ auswertbar ist und
- $\mathcal{F}$ durch Schaltkreise der Größe $s(n)$ nur mit Vorteil $< \frac{1}{s(n)}$ von zufälligen Funktionen unterscheidbar ist.

(b) Im Folgenden betrachte nur boolesche Funktionen $f : \{0,1\}^n \to \{0,1\}$.

- Schränke PRFs z.B. auf das erste Ausgabebit ein.

Man vermutet sogar, dass z.B. der Blum-Micali Generator ($x \mapsto g^x \mod p$) boolesche PRFs der Komplexität

$$s(n) = 2^{n^\varepsilon}$$

für ein (genügend kleines) $\varepsilon > 0$ liefert.

Natürliche Beweise: Die zentrale Idee

1. Boolesche PRFs besitzen Schaltkreise polynomieller Größe, zufällige boolesche Funktionen benötigen Schaltkreise exponentieller Größe.
2. Ein natürlicher Beweis $\mathcal{C} = (\mathcal{C}_n \mid n \in \mathbb{N})$ muss deshalb boolesche PRFs und zufällige Funktionen unterscheiden.

Ein natürlicher Beweis definiert also eine Attacke gegen PRfs. Aber:

- Während natürliche Beweise „Attacken“ mit Laufzeit $2^{\mathcal{O}(n)}$ erlauben, ist die Laufzeit von Attacken gegen Blum-Micali-PRFs durch $2^{n^{\varepsilon}}$ beschränkt.
- Auch ist der erreichte Vorteil ($|C_n| \geqslant 2^{-n}|B_n|$) klitzeklein!

Natürliche Beweise und PRFs (1/3)

Sei c eine hinreichend große Konstante und $\varepsilon > 0$ sei beliebig.

Wenn es eine Familie $\mathcal{F} = (f_\ell : \ell \in \{0,1\}^*)$ von PRFs der Komplexität mindestens 2^{n^ε} für $n = |\ell|$ gibt, dann gibt es *keine* natürlichen Beweise gegen $\mathtt{SIZE}(n^c)$.

- Sei $\mathcal{C} = (C_m \mid m \in \mathbb{N})$ ein natürlicher Beweis und die Funktionen $f_\ell : \{0,1\}^m \to \{0,1\}$ seien boolesche PRFs mit Komplexität mindestens $2^{|\ell|^\varepsilon}$.
  - Die Funktionen f_ℓ sind *effizient auswertbar* und $\mathcal{C}$ ist ein natürlicher Beweis gegen $\mathtt{SIZE}(n^c)$ für hinreichend großes $c \implies \mathbf{C_m(f_\ell) = 0}$.
  - Viele Funktionen erfüllen C_m, denn $|\mathbf{C_m}| \geqslant \frac{|\mathbf{B_m}|}{\mathbf{2^{O(m)}}}$.
- Für Zufallsfunktionen $f \in B_n$ und zufällige Wahlen von $\ell \in \{0,1\}^n$ folgt

$$|\ \mathrm{pr}_\mathbf{f}[\mathbf{C_n(f) = 1}] - \mathrm{pr}_\ell[\mathbf{C_n(f_\ell) = 1}]\ | = \mathrm{pr}_\mathbf{f}[\mathbf{C_n(f) = 1}] \geqslant \frac{\mathbf{1}}{\mathbf{2^{O(n)}}}.$$

C_m unterscheidet boolesche PRFs und RFs mit klitzekleiner W-keit.
Des weiteren wird Laufzeit $2^{\mathcal{O}(n)}$ benötigt, während nur Laufzeit $2^{\mathcal{O}(n^\epsilon)}$ erlaubt ist.

Setze $m := n^{\varepsilon/2}$.

1. Beide, $f_\ell(*0^{n-m})$ und $f(*0^{n-m})$, hängen nur von m Bits ab $\Longrightarrow$

$$\begin{aligned} & |\operatorname{pr}_f[C_m(f(*0^{n-m})) = 1] - \operatorname{pr}_\ell[C_m(f_\ell(*0^{n-m})) = 1]| \\ = \quad & \operatorname{pr}_f[C_m(f(*0^{n-m})) = 1] \geqslant \frac{1}{2^{\mathcal{O}(m)}}, \end{aligned}$$

   - denn werden die letzten $n-m$ Bits einer zufälligen Funktion $f \in B_n$ ausgenullt, erhält man eine zufällige Funktion $g \in B_m$.
   - $\operatorname{pr}_g[C_m(g) = 1] \geqslant 2^{-\mathcal{O}(m)}$ für eine zufällige Funktion g mit m Bits und
2. $C_m(f(*0^{n-m}))$ ist in Zeit höchstens $2^{\mathcal{O}(m)} = 2^{n^{\varepsilon/2}}$ auswertbar!

Betrachte die neue Eigenschaft

$$C_n^*(f) := C_m(f(*0^{n-m}))$$

für Funktionen $f \in B_n$.

Natürliche Beweise und PRFs (3/3)

Setze $C_n^*(f) := C_m(f(*0^{n-m}))$ für Funktionen $f \in B_n$.

- $C_n^*(f)$ ist in Zeit höchstens $2^{\mathcal{O}(m)} = 2^{\mathcal{O}(n^{\varepsilon/2})}$ auswertbar
- und erreicht die Trennung

$$|\operatorname{pr}_f[C_n^*(f) = 1] - \operatorname{pr}_\ell[C_n^*(f_t) = 1]| \geqslant \frac{1}{2^{\mathcal{O}(n^{\varepsilon/2})}}.$$

Widerspruch: PRFs der Komplexität 2^{n^ε} erlauben eine solche Trennung nicht $\Longrightarrow$ Es gibt keine natürlichen Beweise.