Ein $\#\mathrm{P}$-vollständiges Problem: Die Permanente

Seminar Komplexitätstheorie

Leo Kayser

Wintersemester 2021/22

Institut für Theoretische Informatik

$\#\mathrm{P}$ und Zählprobleme

Definition 1: (Die Funktionenklassen FP und $\#\mathrm{P}$)

(i) $\mathrm{FP} = \{\, f\colon \Sigma^* \to \Delta^* \mid f \text{ ist in Polynomialzeit berechenbar} \,\}$

(ii) $$\#\mathrm{P} = \left\{ f\colon \Sigma^* \to \mathbb{N}_0 \;\middle|\; \begin{array}{c} \text{Es gibt eine Polynomialzeit-NTM } M \text{ mit} \\ f(x) = \#\,\mathrm{acc}_M(x) \text{ für alle } x \in \Sigma^* \end{array} \right\}$$

Beobachtung: $A \in \mathrm{NP}$ via polynomiellem Verifizierer V, d. h.

$$x \in A \quad \Longleftrightarrow \quad \exists y \text{ mit } |y| \leq p(|x|) \text{ und } V(\langle x, y \rangle) = 1,$$

für ein Polynom p, dann liegt das dazugehörige *Zählproblem* in $\#\mathrm{P}$:

$$\#A\colon \Sigma^* \to \mathbb{N}_0, \qquad x \mapsto \#\{\, y \mid |y| \leq p(|x|) \text{ und } V(\langle x, y \rangle) = 1 \,\}$$

Reduktionsbegriffe für Funktionenklassen

Definition 2: ($\leq_{\mathrm{m}}^{\mathrm{P}}$, $\leq_{\mathrm{met}}^{\mathrm{P}}$, $\leq_{\mathrm{T}}^{\mathrm{P}}$, Vollständigkeit)

Es seien $f_1\colon \Sigma^* \to \mathbb{N}_0$, $f_2\colon \Delta^* \to \mathbb{N}_0$ Funktionen. Wir definieren

(i) $f_1 \leq_{\mathrm{m}}^{\mathrm{P}} f_2$ gdw. es gibt $g \in \mathrm{FP}$ in mit $f_1(x) = f_2(g(x))$;

(ii) $f_1 \leq_{\mathrm{met}}^{\mathrm{P}} f_2$ gdw. es gibt $g, h \in \mathrm{FP}$ mit $f_1(x) = h(x, f_2(g(x)))$;

(iii) $f_1 \leq_{\mathrm{T}}^{\mathrm{P}} f_2$ gdw. $f_1 \in \mathrm{FP}^{f_2}$;

(iv) f_1 ist $\#\mathrm{P}$-*vollständig bezüglich* $\leq \in \{\leq_m^P, \leq_{met}^P, \leq_T^P\}$, gdw. $f_1 \in \#\mathrm{P}$ und für alle $f_0 \in \#\mathrm{P}$ gilt $f_0 \leq f_1$.

Beobachtung:

$$f_1 \leq_{\mathrm{m}}^{\mathrm{P}} f_2 \quad\Longrightarrow\quad f_1 \leq_{\mathrm{met}}^{\mathrm{P}} f_2 \quad\Longrightarrow\quad f_1 \leq_{\mathrm{T}}^{\mathrm{P}} f_2.$$

Der Satz von Cook-Levin für $\#\mathrm{P}$

Satz 3: ($\#\mathrm{P}$-Vollständigkeit von $\#\mathtt{SAT}$)

Das Zählproblem $\#\mathtt{SAT}(\langle\varphi\rangle) = \#\{\text{Erfüllende Belegungen von } \varphi\}$ ist vollständig für $\#\mathrm{P}$ bezüglich $\leq_{\mathrm{m}}^{\mathrm{P}}$. Die analoge Aussage gilt für $\#\mathtt{3SAT}$.

Beweis.

- Es sei $f \in \#\mathrm{P}$ mit $f(x) = \mathrm{acc}_M(x)$ für eine Polynomialzeit-NTM M
- Es sei g die Reduktionsfunktion für $L(M) \leq_{\mathrm{m}}^{\mathrm{P}} \mathtt{SAT}$ aus dem Satzes von Cook-Levin
- $\{\text{Akzept. Berechnungspfade von } M(x)\} \longleftrightarrow \{\text{Erfüllende Belegungen von } g(x)\}$

$\rightsquigarrow$ $f(x) = \#\mathtt{SAT}(g(x))$ für alle x. $\square$

Die Permanente

Definition 4: (Permanente, $\mathtt{PERM}$)

Die *Permanente* eine Matrix $A = [a_{i,j}] \in \mathrm{Mat}(n \times n, \mathbb{Z})$ ist

$$\operatorname{perm} A = \sum_{\sigma \in \mathcal{S}_n} a_{1,\sigma(1)} \cdots a_{n,\sigma(n)}.$$

Das dazugehörige Zählproblem bezeichnen wir mit $\mathtt{PERM}$, oder $\mathtt{PERM}_S$, wenn wir die Matrixeinträge auf eine Teilmenge $S \subseteq \mathbb{Z}$ einschränken.

Beispiel: $\operatorname{perm} \begin{bmatrix} 0 & 2 & 4 & 0 \\ 0 & 1 & 1 & 0 \\ 3 & 0 & 0 & 5 \\ 1 & 0 & 0 & 2 \end{bmatrix} = 66.$

Determinante und Permanente

- Formel ähnelt der Determinante:

$$\det A = \sum_{\sigma \in \mathcal{S}_n} \operatorname{sign} \sigma \cdot a_{1,\sigma(1)} \cdots a_{n,\sigma(n)}$$

- Determinante lässt sich effizient berechnen (Gauß-Elimination)
- Für Permanente *kein* effizienter Algorithmus bekannt
- Beste allgemeine Formel stammt von *Ryser*

$$\operatorname{perm} A = (-1)^n \sum_{S \subseteq \{1,\dots,n\}} (-1)^{|S|} \prod_{i=1}^{n} \sum_{j \in S} a_{i,j}$$

Herbert J. Ryser
(1923–1985)

Gewichtete Kreisüberdeckungen

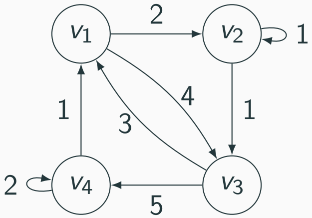
Es sei $G = (V, E)$ ein gerichteter gewichteter Graph mit Gewichten $w\colon E \to \mathbb{N}_0$.

Definition 5: (Kreisüberdeckung, $\#\mathtt{CC}$)

(i) Eine *Kreisüberdeckung* $\mathcal{C} \subseteq E$ von G ist eine Menge von knotendisjunkten Kreisen, die alle Knoten beinhaltet; das Gewicht sei $w(\mathcal{C}) = \prod_{e \in \mathcal{C}} w(e)$.

(ii) Das Zählproblem $\#\mathtt{CC}$ fragt nach der Summe der Gewichte *aller* Kreisüberdeckungen von G.

- Wie viele Kreisüberdeckungen besitzt folgender Graph?
- Was ist $\#\mathtt{CC}(G)$?



$$\begin{bmatrix} 0 & 2 & 4 & 0 \\ 0 & 1 & 1 & 0 \\ 3 & 0 & 0 & 5 \\ 1 & 0 & 0 & 2 \end{bmatrix}$$

Die kombinatorische Interpretation der Permanente

Lemma 6 Ist A die gewichtete Adjazenzmatrix von G, so ist

$$\#\mathtt{CC}(G) = \operatorname{perm} A.$$

Insbesondere sind $\#\mathtt{CC}$ und $\mathtt{PERM}_{\mathbb{N}_0}$ äquivalent bezüglich $\leq_{\mathrm{m}}^{\mathrm{P}}$.

- Gewichtete Graphen kann man mit ihren gewichteten Adjazenzmatrizen identifizieren (Nullen $\widehat{=}$ fehlende Kanten)
- Kreisüberdeckungen entsprechen Permutationen via

$$\mathcal{C} \mapsto \sigma_{\mathcal{C}}, \quad \sigma_{\mathcal{C}}(i) = j \text{ für } (v_i, v_j) \in \mathcal{C}.$$

- Somit ist $w(\mathcal{C}) = a_{1,\sigma_{\mathcal{C}}(1)} \cdots a_{n,\sigma_{\mathcal{C}}(n)}$ und die Identität folgt.

Eine weitere Interpretation

Definition 7: (Biadjazenzmatrix, $\texttt{PM}$, $\#\texttt{PM}$)

Es sei $G = (X, Y, E)$ ein bipartiter Graph, $X = Y = \{1, \dots, n\}$, $E \subseteq X \times Y$. Die *Biadjazenzmatrix* ist

$$M_G = [a_{i,j}], \qquad a_{i,j} = \begin{cases} 1 & \text{falls } (i,j) \in E; \\ 0 & \text{sonst.} \end{cases}$$

Das Entscheidungsproblem $\texttt{PM}$ fragt nach der Existenz eines perfekten Matchings in G. Das dazugehörige Zählproblem sei $\#\texttt{PM}$.

Beobachtung: $\#\texttt{PM}(G) = \operatorname{perm} M_G$. Es ist also $\#\texttt{PM} \equiv_{\mathrm{m}}^{\mathrm{P}} \texttt{PERM}_{\{0,1\}}$

Die große Überraschung

Leslie G. Valiant (*1949)

Satz 8: (Valiant [Val79])

$\mathtt{PERM}_{\{0,1\}}$ ist $\#\mathrm{P}$-vollständig bezüglich $\leq^{\mathsf{P}}_{\mathsf{met}}$.

Insbesondere ist $\#\mathtt{PM}$ $\#\mathrm{P}$-vollständig, *obwohl* $\mathtt{PM}$ in P liegt!

Beweisidee zum Satz von Valiant

1. $\mathtt{PERM}_{\{0,1\}} \in \#\mathrm{P}$, da $\#\mathtt{PM} \in \#\mathrm{P}$ (tatsächlich sogar $\mathtt{PERM}_{\mathbb{N}_0} \in \#\mathrm{P}$)
2. Reduziere zunächst $\#\mathtt{3SAT} \leq^{\mathrm{P}}_{\mathrm{met}} \mathtt{PERM}_{\{0,1\}}$ mit Zwischenergebnis in $\mathtt{PERM}_{\mathbb{Z}}$:

Konstruktion. Zu $\varphi(x_1, \ldots, x_n)$ in 3KNF mit m Klauseln konstruiere

- n Variablen-Gadgets, die je genau 2 Kreisüberdeckungen zulassen
- m Klausel Gadgets, verbunden mit den Variablen über
- $3m$ XOR-Gadgets, die Gewicht 4 bei korrekter Belegung liefern, 0 sonst.

3. Der so konstruierte Graph hat die Eigenschaft $\#\mathtt{CC}(G) = 4^{3m} \cdot \#\mathtt{3SAT}(\varphi)$
4. Durch Binärentwicklung werden $\pm a$-Kanten zu ± 1-Kanten
5. Da $\#\mathtt{CC}(G) \in \{0, \ldots, N = 4^{3m}2^n\}$, genügt es, mod $N + 1$ zu rechnen
   dann $-1 \equiv N \leadsto$ wiederhole 4.

$\leq_m^P$ ist (vermutlich) echt stärker als $\leq_{met}^P$

$\#\texttt{SAT}$ ist $\leq_m^P$-vollständig für $\#\mathrm{P}$. Gilt dasselbe für $\#\texttt{PM}$?

Satz 9: (Nein.)

Falls $\#\texttt{PM}$ $\#\mathrm{P}$-vollständig bzgl. $\leq_m^P$ ist, so ist $\mathrm{P} = \mathrm{NP}$.

Beweis.

- Sei $g \in \mathrm{FP}$ mit $\#\texttt{SAT}(\varphi) = \#\texttt{PM}(g(\varphi))$
- Sei M eine Polynomialzeit-DTM für $\texttt{PM}$.
- $M \circ g$ entscheidet $\texttt{SAT}$ in Polynomialzeit, also $\texttt{SAT} \in \mathrm{P}$. $\square$

Danke! Fragen?

Literaturquellen

[AB09] Sanjeev Arora und Boaz Barak. *Computational Complexity: A Modern Approach*. Cambridge: Cambridge University Press, 2009. ISBN: 9780521424264. DOI: 10.1017/CBO9780511804090. URL: https://www.cambridge.org/core/books/computational-complexity/3453CAFDEB0B4820B186FE69A64E1086.

[DK00] D.-Z. Du und K.-I. Ko. *Theory of Computational Complexity*. Wiley, 2000.

[Val79] Leslie G. Valiant. „The complexity of computing the permanent“. In: *Theoretical Computer Science* 8.2 (1979), S. 189–201. ISSN: 0304-3975. DOI: https://doi.org/10.1016/0304-3975(79)90044-6.

Bildquellen

- Folie 5: CC BY-SA 2.0 de, Konrad Jacobs - Oberwolfach Photo Collection.
  https://opc.mfo.de/detail?photo_id=3617
- Folie 9: CC BY-SA 2.0 de, Renate Schmid - Oberwolfach Photo Collection.
  https://opc.mfo.de/detail?photo_id=7074