2.7. Untere Schranken für PHP

Definition (PHP_n^m)

Variablen: x_{ij} $1 \le i \le m$, $1 \le j \le n$

(Bedeutung Taube $i \to$ Loch j)

Klauseln: - $\{x_{i1}, \dots, x_{in}\}$ für alle $1 \le i \le m$

- $\{\overline{x_{ij}}, \overline{x_{i'j}}\}$ für alle $1 \le i < i' \le m$, $1 \le j \le n$

Beobachtung: - PHP_n^m unerfüllbar $\Leftrightarrow m > n$

- $\| PHP_n^m \| = O(nm^2)$

PHP_n^{n+1} war die erste unerfüllbare Klauselmenge, für die nachgewiesen wurde, dass sie keine Resolutionswiderlegungen polynomieller Länge besitzt.

Satz 2.25 (Haken '85)

$$L(PHP_n^{n+1} \vdash \emptyset) \geq 2^{\Omega(n)} = 2^{\Omega(\sqrt[3]{\|F\|})}$$

Korollar 2.26 (Haken 85)

Resolution ist nicht p-beschränkt.

Für einen sehr hübschen Beweis (mit einem Spielargument) von Hakens Ergebnis siehe Pavel Pudlák "Proofs as Games" (2000).
In der Vorlesung beweisen wir ein stärkeres Ergebnis (mittels Satz 2.24), welches uns auch eine $2^{\Omega(\|F\|)}$ untere Schranke für Graph-PHP liefert.

Definition (G-PHP)

Sei $G = (V \dot\cup U, E)$ ein bipartiter Graph, $|V| = m$, $|U| = n$. G-PHP enthält die Variablen x_e, $e \in E$.

Klauseln: $C_v = \{ x_{\{v,u\}} \mid u \in N(v) \}$ für $v \in V$

$$H = \left\{ \{ \overline{x_{\{v,u\}}}, \overline{x_{\{v',u\}}} \} \,\middle|\, \text{für } v,v' \in V,\ v \neq v',\ u \in U \right\}$$

Beobachtung: $K_{m,n}\text{-PHP} = PHP^m_n$

Expandergraphen

Sei $G = (V \dot\cup U, E)$ ein bipartiter Graph mit $|V| = m$ und $|U| = n$ und $\max\{|N(v)| \mid v \in V\} \leq \Delta$.

$N(V') := \{u \in U \mid \text{es gibt } v \in V' \text{ mit } \{v,u\} \in E\}$

- G ist ein <u>$m \times n$ (Δ, s, c)-Expander</u>, falls

$$|N(V')| \geq c \cdot |V'| \quad \text{für alle } V' \subseteq V \text{ mit } |V'| \leq s.$$

Sei $\partial(V') := \{u \in U \mid \text{es gibt } \underline{\text{genau ein}}\ v \in V' \text{ mit } \{v,u\} \in E\}$

- G ist ein <u>$m \times n$ (Δ, s, c)-Boundary-Expander</u>, falls
$$|\partial(V')| \geq c \cdot |V'| \quad \text{für alle } V' \subseteq V \text{ mit } |V'| \leq s.$$

Für die untere Schranke für G-PHP benötigen wir gute Boundary-Expander. Das folgende Lemma garantiert deren Existenz.

Lemma 2.27

Es gibt $n_0 \in \mathbb{N}$ und $\alpha > 0$, sodass es für alle $n \geq n_0$ ein $(n+1) \times n$ $(5, \alpha \cdot n, 1)$-Boundary-Expander gibt.

$\Rightarrow$ Den Beweis des Lemmas verschieben wir zunächst.

Lemma 2.28

Sei G ein $(n+1)\times n$ (Δ, s, c)-Boundary-Expander.

Dann ist $w(G\text{-PHP} \vdash \emptyset) \geq \frac{s \cdot c}{2}$.

Aus Lemma 2.28, Lemma 2.27 und Satz 2.24 folgt:

Satz 2.29

Es gibt eine Familie von Graphen G_n mit

$$L(G_n\text{-PHP} \vdash \emptyset) = 2^{\Omega(\| G_n\text{-PHP} \|)}.$$

Korollar 2.30

Resolution ist nicht p-beschränkt.

- Außerdem folgt Satz 2.25, da für $G = (V \dot\cup U, E)$ und $G'(V \dot\cup U, E')$ mit $E' \subseteq E$ gilt: $G'\text{-PHP} = G\text{-PHP}|_\alpha$ für ein geeignetes α.

  Nach Lemma 2.21 folgt dann

  $$L(PHP_n^{n+1} \vdash \emptyset) \geq L(G\text{-PHP} \vdash \emptyset)$$

  für alle $G = (V \dot\cup U, E)$ mit $|V| = n+1$ und $|U| = n$.

Beweis von Lemma 2.28

Wir definieren ein Komplexitätsmaß für Klauseln $\mu(C) \in \mathbb{N}$.

$$\mu(C) := \min \{ |V'| \mid V' \subseteq V,\ F_{V'} \models C \}$$

$C_v := \{ x_{v,u} \mid u \in N(v) \}$

Wobei $F_{V'} := \{ C_v \mid v \in V' \} \cup H$.

$H := \{ \{ \overline{x_{v,u}}, \overline{x_{v',u}} \} \mid v \neq v' \in V, u \in U \}$

(Beachte, dass $F_V = G\text{-}PHP$ die gesamte Klauselmenge ist.) Wir haben:

ⓐ $\mu(C) \leq 1$ für alle $C \in G\text{-}PHP$

ⓑ Wenn C Resolvente aus D und E ist, dann ist

$$\mu(C) \leq \mu(D) + \mu(E)$$

ⓒ $\mu(\emptyset) > s$

(Erläuterung: ⓐ ist trivial, ⓑ: Aus $F_{V'} \models D$ und $F_{V''} \models E$ folgt $F_{V' \cup V''} \models C$.

ⓒ: Für alle $V' \subseteq V$ mit $|V'| \leq s$ gibt es ein Matching zwischen V' und U, das jeden Knoten aus V' enthält. $\Rightarrow F_{V'}$ ist erfüllbar.)

Aus (a), (b), (c) folgt: In jeder Widerlegung Γ von G-PHP gibt es eine Klausel C mit

$$\frac{s}{2} \leq \mu(C) \leq s.$$

Sei C eine solche Klausel und $V' \subseteq V$ <u>minimal</u> mit $F_{V'} \models C$. $\Rightarrow |V'| \leq s$ und $|\partial(V')| \geq c \cdot |V'| \geq \frac{s \cdot c}{2}$.

Das Lemma folgt nun aus der folgenden Behauptung.

<u>Behauptung:</u> Für jedes $u \in \partial(V')$ gibt es eine Variable $x_{\{\hat{v},u\}}$ in C.

<u>Beweis der Behauptung:</u>

Angenommen kein $x_{\{\hat{v},u\}}$ ist in C enthalten für eine Variable $u \in \partial(V')$.

Sei $v \in V'$ mit $N(u) \cap V' = \{v\}$ der eindeutige Nachbar von u in V'.

Wegen der Minimalität von V' gilt $F_{V' \setminus \{v\}} \not\models C$

$\Rightarrow$ es gibt (totale) Belegung α mit $\alpha \models F_{V' \setminus \{v\}}$ und $\alpha \not\models C$.

Da für alle $\hat{v} \in N(u)$ die Variablen

$X_{\{\hat{v},u\}}$ weder in $F_{V' \setminus \{v\}}$ (wegen $N(u) \cap V' = \{v\}$)

noch in C (nach Annahme) vorkommen,

können wir annehmen, dass $\alpha(X_{\{v,u\}}) = 1$ und

$\alpha(X_{\{\hat{v},u\}}) = 0$ für alle $\hat{v} \in N(u) \setminus \{v\}$.

$\Rightarrow \alpha \models F_{V'}$, dies ist ein Widerspruch

zu $\alpha \not\models C$ und $F_{V'} \models C$. ↯

$\square$ (Behauptung)

$\square$ (Lemma 2.28)

2.8. Exkurs: Expandergraphen

An dieser Stelle geben wir ein probabilistisches Argument, das die Existenz von Expandergraphen zeigt.

$\boxed{\text{Lemma 2.31}}$ (Beweis aus (MO6))

Für $\Delta \geq 3$ und $c' < \Delta - 1$ gibt es ein $\alpha(\Delta, c') > 0$, sodass es für alle n ein $n \times n$ $(\Delta, \alpha \cdot n, c')$-Expander gibt.

Daraus erhalten wir dann für $\Delta = 5$ und $c' = \frac{7}{2}$ und dem folgenden Lemma die gewünschten Boundary-Expander aus Lemma 2.27 (welche für G-PHP verwendet wurden).

$\boxed{\text{Lemma 2.32}}$

(a) Wenn G ein $n \times n$ $(\Delta, \alpha \cdot n, c')$-Expander ist, dann ist G ein $n \times n$ $(\Delta, \alpha \cdot n, 2c' - \Delta)$-Boundary-Expander.

(b) Wenn G ein $n \times n$ $(\Delta, \alpha \cdot n, c)$-Boundary-Expander ist, dann ist G' ein $n \times (n-1)$ $(\Delta, \alpha n, c-1)$-Boundary-Expander, wobei G' aus G entsteht indem ein beliebiger Knoten aus der rechten Seite U gelöscht wurde.

(Beweis: Übung)