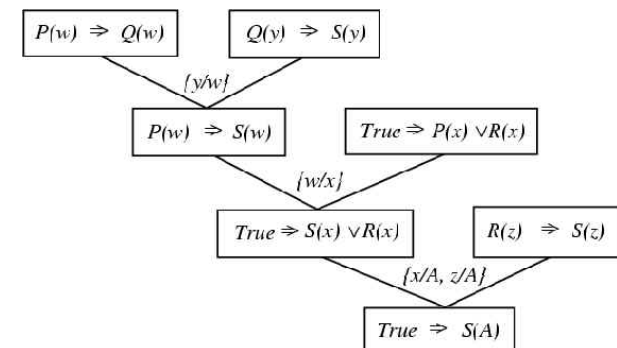


Beweissysteme

Hartmut Klauck
Universität Frankfurt
WS 06/07
10.1.



$$\text{NEXP} \subseteq \text{MIP}$$

- Wir betrachten weiter das MIP Protokoll für Orakel-3-SAT aus der letzten Vorlesung

Analyse des Protokolls

- Klar: Wenn zu akzeptieren ist, gibt es eine Strategie der Beweiser, mit der der Verifizierer mit Ws. 1 akzeptiert.
- Angenommen, die Formel ist nicht Orakel-erfüllbar
- Wenn p_A nicht s^{-k} -approximativ multilinear ist, wird mit hoher Ws. in Schritt 1 verworfen
- Nehmen wir also an, dass p_A s^{-k} -approximativ multilinear ist
- p'_A sei eine multilineare s^{-k} -Approximation von p_A
- Wenn der Verifizierer bis zum Schluss nicht verwirft, geht die Analyse wie beim TAUT Protokoll
- Der zu testende Ausdruck $\sum_{B_1, B_2, B_3, F, U \in \{0,1\}}^{3s+r} g(B_1, B_2, B_3, F, U, p_A(B_1), p_A(B_2), p_A(B_3)) = K$
ist für p'_A ein Polynom vom Grad $d = \text{poly}(n)$

Analyse des Protokolls

- Wenn der Ausdruck nicht gleich K ist, und der Beweiser sendet in einer Runde das „richtige“ Polynom, wird mit Sicherheit verworfen, da dann $s(0)+s(1) \neq K$
- Wenn der Beweiser ein anderes Polynom sendet, wird mit Ws. $(1-d/q)$ vom Verifizierer ein Körperelement gewählt, auf dem der reduzierte Ausdruck nicht den richtigen Wert hat usw.
- Zum Schluss erhalten wir mit hoher Ws. dass $g(B_1, B_2, B_3, F, U, p'_A(B_1), p'_A(B_2), p'_A(B_3))$ den falschen Wert hat.
- Dies prüfen wir mittels 3 Fragen an P_2
- Da B_1, B_2, B_3 zufällig sind, testen wir 3 zufällige Positionen von p_A .
- Mit Wahrscheinlichkeit $\geq 1-3/s^k$ stimmen p_A und p'_A an diesen Positionen überein
- Damit wird insgesamt mit hoher Wahrscheinlichkeit verworfen.

Bemerkung

- Das obige MIP Protokoll ist nichtadaptiv
- Tatsächlich ist auch das TAUT Protokoll nichtadaptiv: die Fragen des Verifizierers sind zufällige Körperelemente
- Damit können wir leicht das ganze in ein 1-Runden MIP Protokoll übersetzen
- Allerdings können wir TAUT nicht in einem 1-Runden IP Protokoll beweisen.
Nichtadaptivität hilft nur bei MIP, die Rundenzahl zu senken

Multilinearitätstest

- Wir betrachten jetzt den Test auf Multilinearität
- **Theorem 10.5**
Es gibt einen Algorithmus, der zu einer als Orakel gegebenen Funktion A in s Variablen folgendes leistet:
 - Sei $I=\{0,\dots,q-1\}$, k eine Konstante
 - Wenn A multilinear ist und ganzzahlige Werte hat, dann akzeptiert der Algorithmus immer
 - Wenn A nicht s^{-k} -approximativ multilinear ist, verwirft der Algorithmus mit hoher Ws .
 - Der Algorithmus stellt $\text{poly}(s)$ viele Fragen
- Dies ist ein Beispiel für einen Property Tester

Multilinearitätstest

- Idee: teste „lokal“ auf Verletzungen der Linearität
- $I = \{0, \dots, q-1\}$
- Wir betrachten k -dimensionale Unterräume $U \subseteq I^s$, bei denen es $s-k$ Koordinaten i_1, \dots, i_{s-k} und $s-k$ Elemente a_1, \dots, a_{s-k} gibt und $U = \{x_1, \dots, x_s : x_{i_j} = a_j \text{ für } j=1, \dots, s-k\}$
- 1-dimensionalen Unterräume dieser Form heissen *Linien*

Multilinearitätstest

- L sei die Menge aller Linien, L_i die Menge der Linien in Richtung i (d.h. Dimension i ist frei)
- **Definition 11.1:** Eine Funktion p auf I^s heisst *multilinear*, wenn ihre Einschränkung auf eine Linie l linear ist für alle $l \in L$.
- Eine Funktion ist δ -approximativ multilinear, wenn sie auf höchstens einem δ -Anteil aller Eingaben von einer multilinearen Funktion abweicht
- **Definition 11.2:** Für eine Funktion p heisst eine Linie l falsch, wenn p auf l nicht linear ist, sonst korrekt. l heisst δ -falsch, wenn p auf l nicht δ -approximativ linear ist

Multilinearitätstest

- Bemerkung: Wenn x aus I^s , und p multilinear, dann ist $|p(x)| \leq (2q)^s$
- Wenn der Tester also jemals zu große Werte, oder nicht ganzzahlige Werte findet, kann verworfen werden

Der Test

- Wir gehen davon aus, dass die meisten Werte $p(x)$ ganzzahlig und kleiner als $(2q)^s$ sind
- Test für eine Linie l :
 1. Ziehe m_1+2 zufällige Punkte auf der Linie
 2. Frage $p(x)$ an diesen Punkten
 3. Wenn $p(x)$ dort mit einer linearen Funktion übereinstimmt, akzeptiere, sonst verwirfe
- **Lemma 11.3:**
 - Wenn l korrekt ist, akzeptiert der Test
 - Wenn l δ -falsch ist, wird mit Wahrscheinlichkeit $1-\exp(-\delta m_1)$ verworfen

Beweis

- Wir fragen für m_1+2 Punkte x auf der Linie den Wert von $p(x)$
- 2 Punkte legen eine lineare Funktion h fest.
- Wenn für alle linearen Funktionen h zufällig gewählte Punkte x mit Wahrscheinlichkeit $\geq \delta$ von h abweichen, verwirft der Test mit Wahrscheinlichkeit mindestens

$$1-(1-\delta)^{m_1} \geq 1-\exp(-\delta m_1)$$

Der Tester

1. Ziehe m_2 zufällige Linien aus L_i für alle i
2. Überprüfe alle Linien wie beschrieben
3. Akzeptiere gdw für alle Linien akzeptiert wird
 - Wir erhalten leicht:
 - **Lemma 11.4:**
 - Wenn p multilinear ist, akzeptiert der Test
 - Wenn für ein i mindestens ein ε -Anteil aller Linien in L_i δ -falsch ist, dann wird mit Ws $1 - \exp(-\varepsilon m_2) - \exp(-\delta m_1)$ verworfen
 - **Theorem 11.5:**
 - Wenn p nicht α -approximativ multilinear ist, so gibt es ein i , so dass ein ε -Anteil der Linien in L_i δ -falsch ist, für $\alpha \approx s^2(\varepsilon + \delta)$

Bemerkung

- Theorem 11.5 ist nichttrivial
- Wir lassen den Beweis weg

Details

- Wir können nun die Parameter ε , $\delta=1/\text{poly}(n)$ wählen
- Dann reicht es $m_1, m_2 = \text{poly}(n)/(\varepsilon \cdot \delta)$ zu setzen, um mit hoher Ws. zu verwerfen
- Insgesamt brauchen wir $m_2 \cdot s \cdot (m_1 + 2) = \text{poly}(n)$ Fragen an das Orakel

Zusammenfassung

- Wir haben für Orakel-3-SAT ein MIP Beweissystem beschrieben
- Dieses ist äquivalent zu $\text{Orakel-3-SAT} \in \text{PCP}(\text{poly}, \text{poly})$
- Damit gilt $\text{MIP} = \text{NEXP} = \text{PCP}(\text{poly}, \text{poly})$
- Das MIP System benötigt nur 1 Runde
- Wir kombinieren das TAUT Beweissystem mit einem Property Tester für Multilinearität