Beweisverifikation und Nichtapproximierbarkeit

Thorsten Hübschen

Arbeitsgruppe 4
Sommerakademie St. Johann 1998
Studienstiftung des deutschen Volkes

Vortragsübersicht

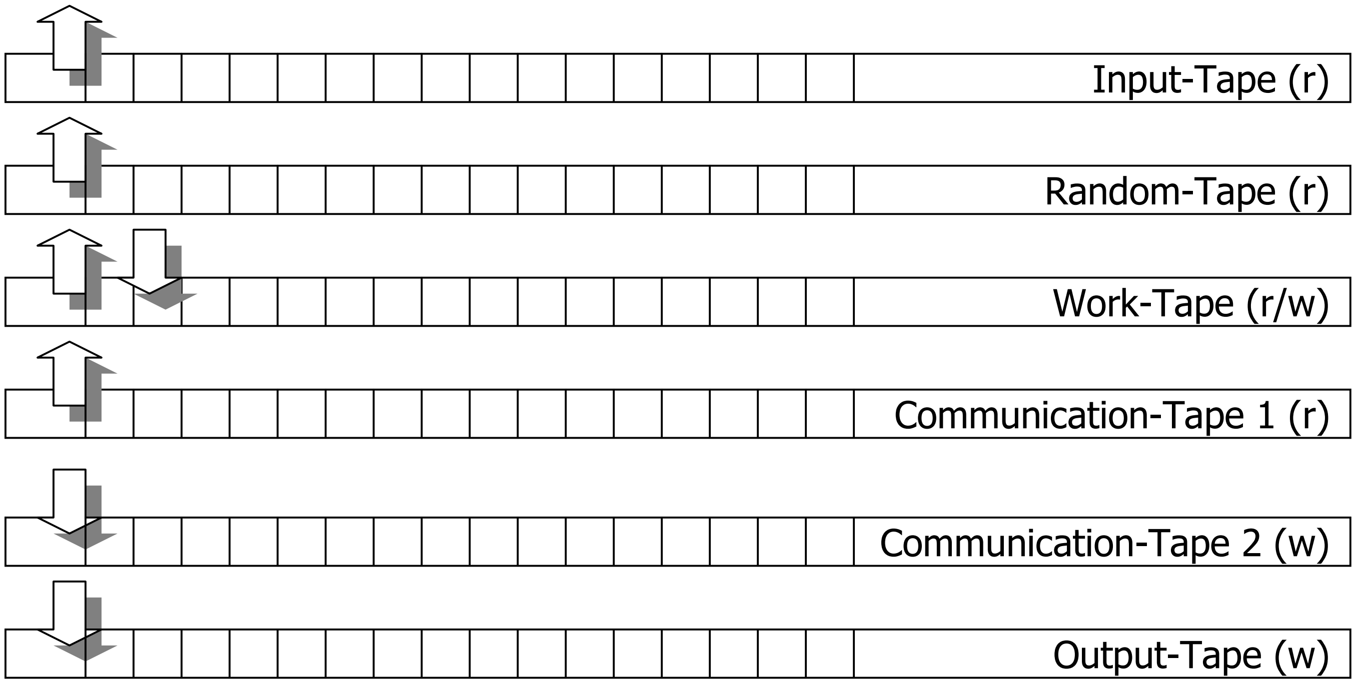
Teil I : Beweisverifikation

- Interaktive Beweissysteme
  - Definitionen
  - Bemerkungen
  - Beispiel: Interaktiver Beweis für Graph Non-Isomorphism
  - Diskussionen
- Probabilistisch überprüfbare Beweisssysteme
  - Definitionen
  - Bemerkungen
- Das PCP-Theorem

Teil II: Nicht-Approximierbarkeit

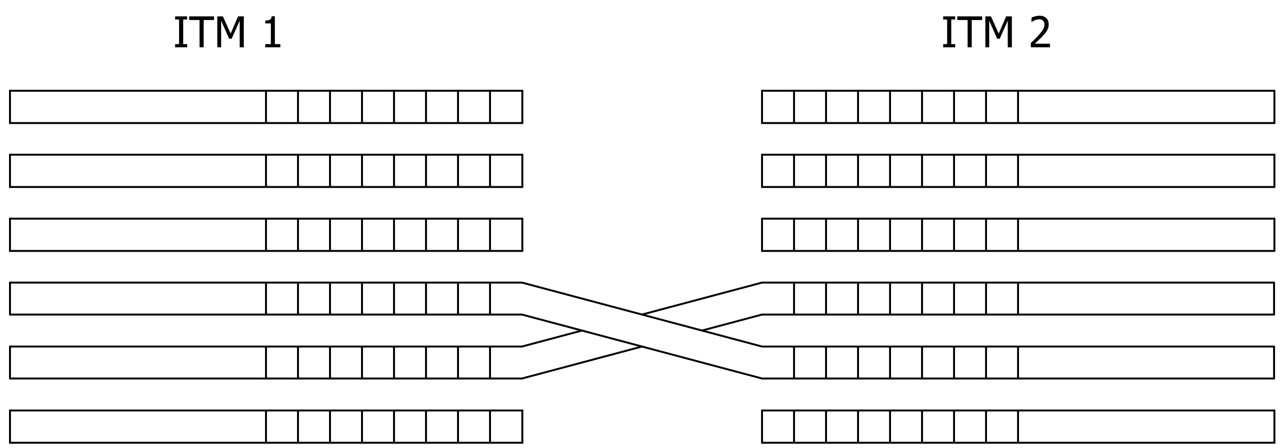
Interaktive Turing-Maschinen

Def. Eine *interaktive Turing-Maschine (ITM)* ist eine 6-bändige deterministische Turing-Maschine mit folgender Konfiguration:



Interaktive Paare von TMs

Def. Ein *interaktives Paar von Turing-Maschinen* ist ein Paar von interaktiven Turing-Maschinen, welche ihre Kommunikationsbänder gemeinsam benutzen, so daß das Kommunikationsband 1 (read-only) der ersten Turing-Maschine gleichzeitig das Kommunikationsband 2 (write-only) der zweiten ist und umgekehrt.



Interaktive Beweissysteme

- Ein *interaktives Beweissystem (interactive proof system)* für eine Sprache L ist ein interaktives Paar von Turing-Maschinen (P,V), so daß der *Verifier* V eine probabilistische Polynomialzeit-Maschine ist, für die gilt:

  - *Vollständigkeit:* Jedes $x \in L$ wird von dem Verifier nach Interaktion mit dem *Prover* P über den gemeinsamen Input x akzeptiert.
  - *Robustheit:* Für jeden potentiellen Prover P* weist der Verifier V jedes $x \notin L$ nach Interaktion mit P* über den gemeinsamen Input x mit einer Wahrscheinlichkeit von mindestens ½ zurück.

- Es seien r und m Ganzzahl-Funktionen. Die Komplexitätsklasse **IP**$(m(\cdot),r(\cdot))$ besteht aus genau den Sprachen, die ein interaktives Beweissystem besitzen, in welchem V bei gemeinsamen Input x höchstens $r(|x|)$ Münzen wirft und in dem höchstens $m(|x|)$ Nachrichten zwischen V und P ausgetauscht werden.
- Wir setzen insbesondere **IP**$(m(\cdot))$:= **IP**$(m(\cdot)$, `poly`) und **IP :=** **IP**(`poly`) .

IPS: Bemerkungen I

- Die IP-Hierarchie ist äquivalent zu einer entsprechenden Hierarchie, in der die Vollständigkeitsbedingung in soweit gelockert wird, daß jedes $x \in L$ nur mit einer Wahrscheinlichkeit von mindestens 2/3 akzeptiert werden muß.
- Das Zulassen einer von Null verschiedenen Fehlerwahrscheinlichkeit in der Robustheitsbedingung ist hingegen entscheidend, ansonsten wären IPS nur für Sprachen aus **NP** möglich.
- Schränkt man das IPS in soweit ein, daß dem Verifier nur noch erlaubt wird, dem Prover die Ergebnisse seiner Münzwürfe, d.h. die Bits seines Random-Tapes, zu übermitteln, (sog. *Arthur-Merlin-Games*) erhält man trotzdem noch die vollständige IP-Hierarchie.
- Nach k-maligem sequenziellen oder parallelen Ausführen eines interaktiven Beweises mit gegebener Fehlerwahrscheinlichkeit von jeweils $\varepsilon > 0$ beträgt die kummulierte Fehlerwahrscheinlichkeit ε^k und kann daher unter jede beliebige positive Schranke gedrückt werden. Die Wahl der Fehlerwahrscheinlichkeit ½ in der Definition ist daher relativ willkürlich.

IPS : Bemerkungen II

- Es gilt **IP**(0,`poly`) = co**RP** und **IP**(1,0) = **NP**. Ferner gilt **IP**(0,`log`) = **IP**(0,0) = **P** und **IP**(`poly`,`log`) = **IP**(1,0) = **NP**.

- Für jede Ganzzahl-Funktion f, so daß f(n) $\geq$ 2 für alle n gilt, kollabiert die Klasse **IP**(O(f($\cdot$))) zu der Klasse **IP**(f($\cdot$)). Insbesondere gilt damit **IP**(O(1)) = **IP**(2).

- Die Klasse IP(2) enthält Sprachen, von denen nicht bekannt ist, ob diese in **NP** enthalten sind, z.B. das Problem Graph Non-Isomorphism.

Ein interaktiver Beweis für Graph Non-Isomorphism

Instanz: Zwei Graphen G_1 und G_2

Frage: Gibt es keine bijektive Kanten-invariante Abbildung der Eckpunkte von G_1 auf die Eckpunkte von G_2 ?

Bemerkungen:

- Eine Abbildung π von G_1 nach G_2 heißt Kanten-invariant, wenn zwei Eckpunkte u und v des Graphen G_1 genau dann benachbart sind, wenn die Eckpunkte $\pi(u)$ und $\pi(v)$ des Graphen G_2 benachbart sind.
- Es ist nicht bekannt, ob das Problem Graph Non-Isomorphism in **NP** enthalten ist.

Ein interaktiver Beweis für Graph Non-Isomorphism (cont.)

Algorithmus:

- Der Verifier wählt zufällig einen der beiden Graphen G_1 oder G_2 aus. Dieser sei mit G_α, $\alpha \in \{1,2\}$, bezeichnet.
- Der Verifier erzeugt eine zufällige isomorphe Kopie von G_α und sendet diese an den Prover.
- Der Prover antwortet darauf mit einer Zahl $\beta \in \{1,2\}$.
- Der Verifier interpretiert den Fall $\beta=\alpha$ als Hinweis dafür, daß die beiden Graphen nicht isomorph sind. Im Fall $\beta\neq\alpha$ bricht der Verifier sofort ab und weist den Input zurück.
- Diese 4 Schritte werden mehrmals wiederholt, um stochastische Evidenz zu sammeln. Der Verifier akzeptiert den Input dann und nur dann, wenn alle Antworten des Provers korrekt sind.

Ein interaktiver Beweis für Graph Non-Isomorphism (cont.)

Korrektheit des Algorithmus

- Wenn die beiden Graphen nicht isomorph sind, ist der vom Verifier vorgelegte Graph G_α zu genau einem der beiden Graphen isomorph, welches der Prover durch exhaustive search leicht herausfinden und somit immer die korrekte Antwort geben kann. Damit ist die Vollständigkeitsbedingung erfüllt.
- Wenn die beiden Graphen dagegen isomorph sind, ist es unmöglich, zwischen einer zufälligen Kopie des ersten und einer zufälligen Kopie des zweiten zu unterscheiden. Daher ist die Wahrscheinlichkeit, daß der Prover auf eine Nachfrage des Verifier korrekt antwortet höchstens gleich 1/2. Somit ist die Wahrscheinlichkeit, daß der Prover auf alle k Nachfragen korrekt antwortet höchstens gleich 2^{-k} und damit ist auch die Robustheitsbedingung erfüllt.

IPS: Diskussionen

- **IP** = „Alles, was effizient verifiziert werden kann“.

- Beim Übergang vom **NP** zu **IP** löst man sich von zwei Aspekten von „Beweisen“, die mit dem ursprünglichen Begriff des Beweises untrennbar verbunden waren:
  - *Absolute Korrektheit*: Bei probabilistischen Beweisen wird eine, wenn auch beliebig kleine, Fehlerwahrscheinlichkeit akzeptiert.
  - *Objektivität/Übertragbarkeit:* Ein interaktiver Beweis „überzeugt“ nur einen Beobachter, der entweder selbst aktiv als Verifier an dem interaktiven Beweis teilgenommen hat oder der „glaubt“, daß die Münzwürfe des Verifiers für den Prover wirklich unvorhersehbar waren. (Kann beispielsweise in dem vorgestellten IPS für Graph Non-Isomorphism der Prover die Münzwürfe des Verifiers vorhersagen, so kann er immer korrekt antworten, selbst wenn die Graphen isomorph sind.)

Probabilistisch prüfbare Beweise

- Ein *probabilistisch überprüfbares Beweissystem (probabilistic checkable proof system)* für eine Sprache L ist eine probabilistische Polynomialzeit-Orakelmaschine V, welche als *Verifier* bezeichnet wird und für die gilt:

  - *Vollständigkeit:* Für jedes $x \in L$ existiert eine Orakelmenge π_x, so daß V den Input x mit Zugriff auf das Orakel π_x immer akzeptiert.

  - *Robustheit:* Für jedes $x \notin L$ und für jede Orakelmenge π_x weist der Verifier V den Input x mit Zugriff auf π_x mit einer Wahrscheinlichkeit von mindestens 1/2 zurück.

- Es seien r und q Ganzzahl-Funktionen. Die Komplexitätsklasse **PCP**$(r(\cdot),q(\cdot))$ besteht aus genau den Sprachen, für die ein probabilistisch überprüfbares Beweissystem existiert, in welchem der Verifier für jeden Input der Länge n höchstens r(n) Münzwürfe durchführt und höchstens q(n) Fragen an das Orakel stellt.

PCP : Bemerkungen

- Das Orakel π_x in einem PCP-System konstituiert einen Beweis im strengen mathematischen Sinn.
- Im Gegensatz zu NP-Beweisen hat das PCP-Orakel die zusätzliche Eigenschaft, es dem Verifier zu ermöglichen, wahlfrei auf beliebige kleine Abschnitte des Beweises zuzugreifen.
- Ein PCP-System ist ein Spezialfall eines IPS, in dem die Antworten des Prover unabhängig von seinen vorherigen Antworten sind, wo der Prover also „gedächtnislos“ ist.
- **PCP**(`poly`, 0) = co**RP**
- **PCP**(0,`poly`) = **NP**
- **PCP**(`poly`,`poly`) = **NEXP**

Das PCP-Theorem

Theorem Es gilt:

$$\mathbf{NP} \subseteq \mathbf{PCP}(\mathtt{log}, O(1))$$

Corollar Es gilt:

$$\mathbf{NP} = \mathbf{PCP}(\mathtt{log}, O(1))$$

Corollar Es gilt:

$$\mathbf{NEXP} = \mathbf{PCP}(\mathtt{poly}, O(1))$$

Proposition Es existieren Konstanten α, $\beta > 0$, so daß für jede Ganzzahl-Funktion $l(\cdot)$ mit $0 \leq l(n) \leq \alpha \log_2 n$ gilt:

$$\mathbf{NP} = \mathbf{PCP}(r(\cdot), q(\cdot)),$$

mit $r(n) = \alpha \log_2 n - l(n)$ und $q(n) = \beta\, 2^{l(n)}$.