One-Sided-$\mathcal{AM}$ und Kollaps-Theorem für $\mathcal{AM}$

Lars Siggelkow

13. Juli 2002

Inhaltsverzeichnis

1 Einleitung

Im vorherigen Vortrag wurden Arthur-Merlin-Spiele ($\mathcal{AM}$) als eine spezielle Klasse interaktiver Beweissysteme einführt. In diesem Vortrag werde ich zwei wichtige Eigenschaften dieser Klasse vorstellen: Das *One-Sided-Error-$\mathcal{AM}$-Theorem* besagt, dass es für jede Arthur-Merlin-Sprache ein Protokoll mit nur einseitigem Fehler gibt. Nach dem *Kollapstheorem* für Arthur-Merlin-Spiele kollabiert die $\mathcal{AM}$-Hierarchie auf $\mathcal{AM}_2$.

2 ...zur Erinnerung: Arthur-Merlin-Spiele

Im folgenden werde ich noch einmal kurz vorstellen, worum es sich bei Arthur-Merlin-Spielen handelt. Für die Details sei auf den vorhergehenden Vortrag verwiesen.

2.1 Die Idee

Der König Arthur muß qua Amtes Entscheidungen treffen. Da sein Urteilsvermögen jedoch begrenzt ist, benötigt er den Rat des weisen Zauberers Merlin. Da jedoch letztlich Arthur seine Entscheidungen selbst zu verantworten hat, erwartet er von Merlin außer einer Antwort auch eine plausible Begründung. Mit anderen Worten: Merlin soll ihm die Richtigkeit der Antwort beweisen. Nur wenn Merlin dies gelingt, akzeptiert Arthur den Rat.

2.2 Das Interaktive Beweissystem

Ein Arthur-Merlin-Game ($\mathcal{AM}$) ist ein interaktives Beweissystem bei dem Arthur der Verifier und Merlin der Proover ist. Arthur verfügt über Zufallsbits, die er jedoch –im Gegensatz zur Klasse $\mathcal{IP}$– Merlin mitteilen muß.

2.3 ...und formal

Arthur läßt sich durch eine polynomialzeitbeschränkte probabilistische Turingmaschine mit einem Orakel f (M_A^f) formalisieren, wobei Merlin hier als die Orakelfunktion f beschrieben wird.

Definition ($\mathcal{AM}$)**.** *Eine Sprache L ist in der Klasse $\mathcal{AM}$ enthalten gdw. eine OPTM M_A^f mit Oraklefunktion f und eine Konstante $0 < \epsilon < 1/2$ existiert, so dass für alle Wörter x gilt:*

$$x \in L \quad \Rightarrow \quad \exists f \; \Pr[M_A^f(x) = 1] > 1 - \epsilon \tag{1}$$

$$x \notin L \quad \Rightarrow \quad \forall f \; \Pr[M_A^f(x) = 1] < \epsilon \tag{2}$$

3 Merlin-Maschinen

3.1 Die Idee

Bei der vorherigen Formalisierung von Arthur-Merlin-Games haben wir die Perspektive von Arthur eingenommen: Die Maschine M_A^f modellierte die Rolle von Arthur. Merlin erscheint dabei als Orakel, also eine Art *Black Box*. Für den folgenden Beweis brauchen wir jedoch die Möglichkeit einzelne Runden eines Arthur-Merlin-Spiels zu simulieren. Dazu reicht eine solche *black box*-Betrachung von Merlin nicht aus.Vielmehr müssen wir die Strategie Merlins, i.e. sein Verhalten beurteilen können.

Was ist also Merlins Sicht auf das Spiel? Merlin kennt Arthur inkl. seiner Zufallsbits. D.h. Merlin kann mit seinen unbegrenzten Ressourcen Arthur´s Verhalten vollständig simulieren. Insbesondere kann Merlin also auch Arthur's Fragen vorherberechnen. Arthur's Funktion in dem Spiel läßt sich also auf das Generieren von

Zufallsbits und die abschließende Entscheidung (i.e. die Akzeptanz des Beweises, die aber auch durch Merlin simuliert werden kann) reduzieren. Nachdem Arthur in einem Zug eine Sequenz von Zufallsbits geschickt hat, versucht Merlin nun einen Zug zu machen, der seine Gewinnchancen maximiert.[1] Dies erreicht Merlin dadurch, dass er eine optimale Reaktion auf die Zufallsbits *rät*. Die entscheidene Idee ist nun, dass dieses Raten eines optimalen Schrittes als nichtdeterministische Entscheidung modelliert werden kann.

3.2 Definition

Die folgende Formailisierung des Sachverhaltes und die anschließenden Sätze und deren Beweise beruhen auf dem der Darstellung in [DlK00].

Definition (Merlin-Maschine). *Eine Merlin-Maschine ist eine polynomialzeitbeschränkte nichtdeterministische probabilistische 3-Band-Turingmaschine M_M mit zwei zusätzlichen Zuständen q_A und q_M. Im einzelnen gilt:*

Besondere Zustände:

q_A: *M_M verhält sich probabilistisch*

q_M: *M_M verhält sich nichtdeterministisch*

Bandbenutzung:

B_n:	*Arbeitsband*	*r/w*
B_A:	*Arthurband (Zufallsbits)*	*lesen in q_A*
B_M:	*Merlinband (Dokumentation nichtdeter. Entscheidungen)*	*schreiben in q_M*

Wenn die Maschine in den Nichtdeterminismus-Zustand q_M übergeht, rät sie nichtdeterministisch einen von zwei möglichen Folgezuständen und dokumentiert die Entscheidung durch Schreiben des entsprechenden Bits auf das Merlin-Band. Wenn die Maschine in den Zufalls-Zustand q_A übergeht, liest sie das nächste Zufallsbit auf dem Arthur-Band und wählt abhängig davon ihren Folgezustand.

Eine Konfiguration einer Merlin-Maschine wird durch das 5-Tupel $c = (q, s, t, \alpha, \beta)$ angegeben, wobei

q der aktuelle Zustand ist,

s die Zeichenkette auf dem Arbeitsband links von der aktuellen Position,

t die Zeichenkette auf dem Arbeitsband an und rechts von der aktuellen Position,

α der bis zum aktuellen Zeitpunkt gelesene Inhalt des Merlin-Bandes ist und

β der bis zum aktuellen Zeitpunkt gelesene Inhalt des Arthur-Bandes ist.

[1] Man kann sich vorstellen, daß Merlin Solitär spielt, wobei Arthur –gänzlich willkürlich– jede Runde ein paar Spielsteine umsetzt.

3.3 Akzeptanzwahrscheinlichkeit einer Merlin-Maschine

Die Akzeptanzwahrscheinlichkeit einer Merlin-Maschine wird induktiv über die Akzeptanzwahrscheinlichkeit für jede einzelne Konfiguration einer Berechnung definiert.

Definition (Akzeptanzwahrscheinlichkeit einer Merlin-Maschine). *Sei M_M eine Merlin-Maschine. Sei $c = (q, s, t, \alpha, \beta)$ eine Konfiguration von $M_M(x)$. Seien c_0, c_1 eventuell vorhandene Folgezustände von c.*

Die Akzeptanzwahrscheinlichkeit für die Konfiguration c (kurz: $\mathrm{acc}(c)$) ist wie folgt definiert:

$$\mathrm{acc}(c) = \begin{cases} 1 & \textit{gdw. } q = q_{ja} \\ 0 & \textit{gdw. } q = q_{nein} \\ \frac{\mathrm{acc}(c_0)+\mathrm{acc}(c_1)}{2} & \textit{gdw. } q = q_A \\ \max\{\mathrm{acc}(c_0), \mathrm{acc}(c_1)\} & \textit{gdw. } q = q_M \\ \mathrm{acc}(c_0) & \textit{sonst} \end{cases}$$

Sei c_{init} die Startkonfiguration von $M_M(x)$, dann gilt für die Akzeptanzwarhscheinlichkeit von M_M bei Eingabe x ($\Pr[M_M(x) = 1]$):

$$\Pr[M_M(x) = 1] = \mathrm{acc}(c_{init})$$

3.4 Charakterisierung von $\mathcal{AM}$ durch Merlin-Maschinen

Auf der Grundlage der vorangegangenen Definitionen kann man die Klasse $\mathcal{AM}$ nun wie folgt charakterisieren.

Satz. *Eine Sprache L ist in der Klasse $\mathcal{AM}$ enthalten gdw. eine Merlin-Maschine M_M und eine Konstante $0 < \epsilon < 1/2$ existiert, so dass für alle Wörter x gilt:*

$$x \in L \Rightarrow \Pr[M_M(x) = 1] > 1 - \epsilon$$
$$x \notin L \Rightarrow \Pr[M_M(x) = 1] < \epsilon$$

Beweisidee. Eine Funktion $f(x) =$ "Inhalt von B_M für $M_M(x)$" entspricht der Orakelfunktion einer Arthur-Maschine. Im Falle $x \in L$ existiert ein f, so dass die Arthur-Maschine mit Orakel f mit hoher Wahrscheinlichkeit akzeptiert. Für die Merlin-Maschine beschreibt diese Funktion f einen Berechnungspfad mit einer hohen Akzeptanzwahrscheinlichkeit. Im Falle $x \notin L$ ist für alle Orakel, bzw. für alle Berechnungpfade, die Akzeptanzwahrscheinlichkeit entsprechend gering. □

4 Komplementäre $\mathcal{AM}_k(r)$-Prädikate

Schließlich kann man ausgehend von dem Modell der Merlin-Maschine noch eine weitere Charakterisierung von $\mathcal{AM}$ auf der Grundlage von in Polynomialzeit entscheidbaren Prädikaten angeben. Dieser Formalismus wird sich als besonders geeignet für die folgenden Beweise erweisen.

Definition (P-Prädikat). *Ein Prädikat $R(x_0, \ldots, x_k)$ heißt P-Prädikat, wenn*

1. *$R(x_0, \ldots, x_k) \quad \Rightarrow \quad$ es ex. ein Polynom p, mit $\|x_i\| = p(\|x_0\|)$, $1 \leq i \leq k$.*

2. *R ist in P entscheidbar.*

Im folgenden werde ich $\exists_r^+$ als Quantorensymbol verwenden. Dabei hat der Ausdruck $\exists_r^+ x$ die Bedeutung: "für den r-ten Teil aller x gilt ...". Zudem gilt $\exists^+ \equiv \exists_{2/3}^+$.

Definition (Komplementäre $\mathcal{AM}_k(r)$-Prädikate). *Sei $k \geq 0$ und $1/2 < r \leq 1$. R_0 und R_1 heißen* komplementäre $\mathcal{AM}_k(r)$-Prädikate, *wenn ein P-Prädikat R existiert, so dass für jedes x gilt:*

$$\begin{array}{lllllll} R_1(x) & \equiv & \exists_r^+ y_1 & \exists y_2 & \exists_r^+ y_3 & \ldots & Q_k y_k \quad R(x, y_1, \ldots, y_k) \\ R_0(x) & \equiv & \exists_r^+ y_1 & \forall y_2 & \exists_r^+ y_3 & \ldots & Q'_k y_k \quad \neg R(x, y_1, \ldots, y_k), \end{array}$$

wobei über $\{0,1\}^{p(\|x\|)}$, mit p aus der Definition von P-Prädikat, quantifiziert wird.

Für $\mathcal{MA}$ gilt ganz analog:

Definition (Komplementäre $\mathcal{MA}_k(r)$-Prädikate).
Sei $k \geq 0$ und $1/2 < r \leq 1$. R_0 und R_1 heißen komplementäre $\mathcal{MA}_k(r)$-Prädikate, *wenn ein P-Prädikat R existiert, so dass für jedes x gilt:*

$$\begin{array}{lllllll} R_1(x) & \equiv & \exists y_1 & \exists_r^+ y_2 & \exists y_3 & \ldots & Q_k y_k \quad R(x, y_1, \ldots, y_k) \\ R_0(x) & \equiv & \forall y_1 & \exists_{1/2}^+ y_2 & \forall y_3 & \ldots & Q'_k y_k \quad \neg R(x, y_1, \ldots, y_k), \end{array}$$

wobei über $\{0,1\}^{p(\|x\|)}$, mit p aus der Definition von P-Prädikat, quantifiziert wird.

Lemma (Wahrscheinlichkeitsverstärkung). *Sei $k \geq 0$. Die folgenden Aussagen sind äquivalent:*

1. *R_1 und R_0 sind komplementäre $\mathcal{AM}_k(c)$-Prädikate für ein $c > 1/2$.*
2. *R_1 und R_0 sind komplementäre $\mathcal{AM}_k(c)$-Prädikate für jedes $c > 1/2$.*
3. *R_1 und R_0 sind komplementäre $\mathcal{AM}_k(1 - 2^{-p(n)})$-Prädikate für ein Polynom p.*

Ohne Beweis. □

Satz (Charakterisierung von $\mathcal{AM}$ durch Komplementäre $\mathcal{AM}_k$-Prädikate). *Sei $k \geq 0$.*

1. *Eine Sprache L ist in $\mathcal{AM}_k$ gdw. die Prädikate $R_1(x) \equiv (x \in L)$ und $R_0 \equiv (x \notin L)$ komplementäre $\mathcal{AM}_k$-Prädikate sind.*
2. *(analog für $\mathcal{MA}_k$).*

Beweis. 1.Aussage

"$\Rightarrow$": Sei M eine Merlin-Maschine mit $L(M) = L$ und $\epsilon \leq 2^{-(k+3)}$. Sei $(y_1, \ldots, y_k)$ die Sequenz von Zufallsbits, und Nichtdeterminismusbits, die alternierend von M bei Eingabe x generiert/gelesen wird, wobei jedes y_i o.B.d.A exakt die Länge $p(\|x\|)$ für ein Polynom p hat. Sei $c(x, y_1, \ldots, y_i)$ die Konfiguration von $M(x)$ nachdem die Wörter $y_1, \ldots y_i$ generiert/gelesen wurden.

$x \in L$:

$\curvearrowright$ (Def. Merlin-Maschine)

$$\mathrm{acc}(c(x)) > 1 - \epsilon$$

$\curvearrowright$ (Def. acc, probabilistisches Verhalten, Stochastik)

$$\exists^+ y_1 \ \mathrm{acc}(c(x, y_1)) > 1 - 4\epsilon$$

$\curvearrowright$ (Def. acc, nichtdeterministisches Verhalten)

$$\exists^+ y_1 \ \exists y_2 \ \mathrm{acc}(c(x, y_1, y_2)) > 1 - 4\epsilon$$

$\curvearrowright$ (Iteration des Arguments)

$$\exists^+ y_1 \ \exists y_2 \dots Q_i y_i \, \mathrm{acc}(c(x, y_1, \dots, y_i)) > 1 - 2^{i+1}\epsilon, \quad i \leq k$$

$\curvearrowright$ (für $i = k$, Voraussetzung für ϵ)

$$\begin{aligned} \exists^+ y_1 \ \exists y_2 \dots Q_k y_k \, \mathrm{acc}(c(x, y_1, \dots, y_k)) &> 1 - 2^{k+1}\epsilon \\ &\geq 1 - 2^{(k+1)-(k+3)} = 3/4 \end{aligned}$$

$\curvearrowright$ (wenn c Haltekonfiguration gilt: $\mathrm{acc}(c) > 3/4 \ \Rightarrow \ \mathrm{acc}(c) = 1$)

$$\exists^+ y_1 \ \exists y_2 \dots Q_k y_k \, \mathrm{acc}(c(x, y_1, \dots, y_k)) = 1$$

$x \notin L$:

Ähnlich wie für $x \in L$ zeigt man:

$$x \notin L \quad \Rightarrow \quad \exists^+ y_1 \ \forall y_2 \dots Q_k y_k \, \mathrm{acc}(c(x, y_1, \dots, y_k)) = 0$$

“ $\Leftarrow''$:

Seien $[x \in L]$ und $[x \notin L]$ komplementäre $\mathcal{AM}_k(r)$-Prädikate mit $r = 1 - 1/4k$ (O.B.d.A wegen Wahrscheinlichkeitsverstärkung). Somit existiert ein P-Prädikat R, so dass:

$$\begin{aligned} x \in L \ &\equiv \ \exists^+ y_1 \ \exists y_2 \dots Q_k y_k R(x, y_1, \dots, y_k) \\ x \notin L \ &\equiv \ \exists^+ y_1 \ \forall y_2 \dots Q'_k y_k \neg R(x, y_1, \dots, y_k) \end{aligned}$$

Sei M eine Merlin-Maschine, die sich bei Eingabe x wie folgt verhält:

> In einer ungeraden Phase $1 \leq i \leq k$, geht M in den Zufallszustand q_A über und liest den Zufallsstring y_i, $\|y_i\| = p(n)$. In einer geraden Phase $2 \leq i \leq k$, geht M in den Nichtdeterminismuszustand q_M über und generiert nichtdeterministisch einen String y_i, $\|y_i\| = p(\|x\|)$. In der Endphase $k+1$ verifiziert M, ob $R(x, y_1, \dots, y_k)$ gilt.

Durch einfache Induktion über die Phasen von $M(x)$ erhält

$$\begin{aligned} X \in L &\Rightarrow \Pr[(M(x) = 1] \geq r^{(k+1)/2} = (1 - \frac{1}{4k})^{(k+1)/2} > 3/4 \\ X \notin L &\Rightarrow \Pr[(M(x) = 1] \leq 1 - r^{(k+1)/2} < 1/4 \end{aligned}$$

<u>2.Aussage</u>

Der Beweis für $\mathcal{MA}_k$ geht analog. $\square$

5 Hilfssätze

Im folgenden werde ich zwei Hilfssätze beweisen. Diese Sätze stellen wichtige Argumente für die späteren Beweise des One-Sided-Error-$\mathcal{AM}$-Theorems und des Kollaps-Theorems bereit. Insbesondere der Beweis des ersten Hilfssatzes, des sogenannten *Swapping-Lemmas* hat als Argument für das Folgende eine entscheidende Bedeutung.

Lemma (Swapping-Lemma). *Sei $R(x, y, z)$ ein polynomiell balanciertes Prädikat für ein Polynom p. Sei $\|x\| = n$. Sei $\vec{w} = (w_1, \ldots, w_{p(n)})$, mit $\|w_i\| = p(n)$, $i = 1, \ldots, p(n)$. Dann gilt:*

1. $\forall y \quad \exists^+ z \quad R(x,y,z) \quad \Rightarrow \quad \exists^+ \vec{w} \quad \forall y \quad [\exists z \in \vec{w} \quad R(x,y,z)]$
2. $\forall z \quad \exists^+_{1-2^{-n}} y \quad R(x,y,z) \quad \Rightarrow \quad \forall \vec{w} \quad \exists^+ y \quad [\forall z \in \vec{w} \quad R(x,y,z)]$

Beweis.

Idee
Für ein festes x wird der Wert von $R(x, y, z)$ in einer $2^{p(n)} \times 2^{p(n)}$-Matrix M kodiert mit allen möglichen Werten für y als Zeilen und allen möglichen Werten für z als Spalten:

$$M := \quad \begin{array}{cc} & (z) \\ (y) & \begin{bmatrix} 1,1 & \cdots & 1,2^{p(n)} \\ \vdots & \ddots & \vdots \\ 2^{p(n)},1 & \cdots & 2^{p(n)},2^{p(n)} \end{bmatrix} \end{array}$$

Die erste Aussage stellt sich nun wie folgt dar:

Vor: In jeder Zeile sind mindestens $3/4 \cdot 2^{p(n)}$ Einsen.

Impl: Wähle $p(n)$ Spalten aus!
Pr[“in jeder Zeile gibt es mindestens eine Eins in einer der ausgewählten Spalten”] $\geq$ 3/4.

Für die zweite Aussage ergibt sich folgendes:

Vor: In jeder Spalte sind $1 - 2^{-p(n)}$ aller Einträge Einsen, bzw. in jeder Spalte sind $2^{p(n)-n}$ aller Einträge Nullen.

Impl: Wähle $p(n)$ Spalten! Wähle eine Zeile!
Pr[“in dieser Zeile stehen in allen der gewählten Spalten Einsen”] $\geq 3/4$

Beweis der ersten Aussage
Sei $\vec{w}$ zufällig gewählt. Dann läßt sich die Behauptung wie folgt ausdrücken und es

gilt:

$$\begin{aligned}
\Pr[\exists y\ \forall z \in \vec{w}\ \neg R(x,y,z)] &\leq \sum_{\|y\|=p(n)} \Pr[\forall z \in \vec{w}\ \neg R(x,y,z)] && \text{(ggf. wird doppelt gezählt)}\\
&= \sum_{\|y\|=p(n)} \prod_{z\in\vec{w}} \Pr[\neg R(x,y,z)] && \text{(alle } z \text{ sind unabhängig)}\\
&\leq \sum_{\|y\|=p(n)} \prod_{z\in\vec{w}} \frac{1}{4} && \text{(wegen Vor.)}\\
&= 2^{p(n)} \left(\frac{1}{4}\right)^{p(n)} = \left(\frac{1}{2}\right)^{p(n)}\\
&\leq \frac{1}{4} \quad \text{für } p(n) \geq 2
\end{aligned}$$

Beweis der zweiten Aussage

O.B.d.A gelte für n

$$2^n \geq 4p(n) \qquad \text{(d.h. } n \text{ ist hinreichend groß).} \tag{3}$$

Sei $y \in_R \{0,1\}^{p(n)}$. Nach Voraussetzung gilt nun

$$\forall z \in \{0,1\}^{p(n)}\ \Pr[\neg R(x,y,z)] \leq 2^{-n} \tag{4}$$

Für jede $\vec{w}$ gilt somit

$$\begin{aligned}
\Pr[\exists z \in \vec{w}\ \neg R(x,y,z)] &\leq \sum_{z\in\vec{w}} \Pr[\neg R(x,y,z)]\\
&\leq p(n)2^{-n} && \text{wegen (4)}\\
&\leq 1/4 && \text{wegen (3)}
\end{aligned}$$

□

Der zweite Hilfsatz, das *verallgemeinerte $\mathcal{BPP}$-Theorem* stellt im wesentlichen bereits eine Anwendung des Swapping-Lemmas dar.

Lemma (Verallgemeinertes $\mathcal{BPP}$-Theorem). *Seien R_0 und R_1 polynomiell balancierte komplementäre Prädikate für ein Polynom p. Sei $r = 1 - 2^{-\|x\|}$. Dann gilt für alle x:*

1. $\exists_r^+ y \quad R_1(x,y) \quad \Rightarrow \quad \forall \vec{w} \quad \exists^+ y \quad [\forall i \leq p(n) \quad R_1(x, y \oplus w_i)]$
2. $\exists_r^+ y \quad R_0(x,y) \quad \Rightarrow \quad \exists^+ \vec{w} \quad \forall y \quad [\exists i \leq p(n) \quad R_0(x, y \oplus w_i)]$

Beweis.

Beweis der ersten Aussage

$$\begin{aligned}
&\exists_r^+ y \quad R_1(x,y)\\
&\quad \Rightarrow \forall z \quad \exists_r^+ y \quad R_1(x, z \oplus y) && \text{(Eigenschaft des } \oplus\text{-Operators)}\\
&\quad \Rightarrow \exists^+ \vec{w} \quad \forall z \quad \left[\exists y \in \vec{w} \quad R_1(x, z \oplus y)\right] && \text{(Swapping Lemma)}\\
&\quad \Rightarrow \exists^+ \vec{w} \quad \forall z \quad \left[\exists i \leq p(n) \quad R_1(x, z \oplus w_i)\right] && \text{(Definition } \vec{w}\text{)}\\
&\quad \Rightarrow \exists^+ \vec{w} \quad \forall y \quad \left[\exists i \leq p(n) \quad R_1(x, y \oplus w_i)\right] && \text{(Umbenennung } z \to y\text{)}
\end{aligned}$$

Beweis der zweiten Aussage

$$
\begin{array}{llll}
\exists_r^+ y \quad R_0(x,y) & & & \\
\quad \Rightarrow & \forall z \quad \exists_r^+ y & R_0(x, z \oplus y) & \text{(Eigenschaft des $\oplus$-Operators)} \\
\quad \Rightarrow & \forall \vec{w} \quad \exists^+ y & \left[\forall z \in \vec{w} \quad R_0(x, z \oplus y)\right] & \text{(swapping Lemma)} \\
\quad \Rightarrow & \forall \vec{w} \quad \exists^+ y & \left[\forall i \leq p(n) \quad R_0(x, y \oplus w_i)\right] & \text{(Definiton von $\vec{w}$)}
\end{array}
$$

□

6 One-Sided-Error-$\mathcal{AM}$

Ich komme nun zu dem ersten wichtigen Theorem. Es besagt, dass es zu jeder Arthur-Merlin-Sprache L ein Arthur-Merlin-Protokoll mit einseitigem Fehler gibt. Das heißt, dass für $x \in L$, Arthur in jedem Fall akzepiert.

Theorem (One-Sided-Error-$\mathcal{AM}$). *Seine R_1 und R_0 komlementäre $\mathcal{AM}_2$-Prädikate. Dann existiert ein P-Prädikat R, so dass für jedes x gilt*

$$
\begin{array}{lllll}
R_1(x) & \Rightarrow & \forall z_1 \quad \exists z_2 & R(x, z_1, z_2) & \textit{(ohne Fehler)} \\
R_0(x) & \Rightarrow & \exists^+ z_1 \quad \forall z_2 & \neg R(x, z_1, z_2) & \textit{(einseitiger Fehler)}
\end{array}
$$

(Entsprechendes gilt für $\mathcal{MA}_2$).

Beweis. Wegen der Definition komplemtärer $\mathcal{AM}_2$-Prädikate und Wahrscheinlichkeitsverstärkung kann man annehmen, dass ein P-Prädikat R^* existiert, so dass gilt

$$
\begin{array}{lll}
R_1(x) & \equiv & \exists_r^+ y_1 \quad \exists y_2 \quad R^*(x, y_1, y_2) \\
R_0(x) & \equiv & \exists_r^+ y_1 \quad \forall y_2 \; \neg R^*(x, y_1, y_2) \qquad \text{mit } r = 1 - 2^{-n}
\end{array}
$$

Somit erhält man für R_1

$$
\begin{array}{lll}
R_1(x) & & \\
\quad \Rightarrow & \forall \vec{w} \quad \exists^+ y_1 \quad \forall i \leq p(n) \quad \exists y_2 \quad R^*(x, y_1 \oplus w_i, y_2) & \text{($\mathcal{BPP}$-Theorem)} \\
\quad \Rightarrow & \forall \vec{w} \quad \exists^+ y_1 \quad \exists \vec{u} \quad \forall i \leq p(n) \quad R^*(x, y_1 \oplus w_i, u_i) & \text{(da über nur polyn. viele i quantifiziert wird, kann y_2 für “spätere” Wahl von i “parametierisiert” werden)} \\
\quad \Rightarrow & \forall \vec{w} \quad \exists \langle y_1, \vec{u} \rangle \quad \underbrace{\left(\forall i \leq p(n) \; R^*(x, y_1 \oplus w_i, u_i)\right)}_{\text{substituiere: } R(x, \vec{w}, \langle y_1, \vec{u} \rangle)} & \text{(“... wenn für viele erfüllt, dann auch für eins ...”)} \\
\quad \Rightarrow & \forall \vec{w} \quad \exists \langle y_1, \vec{u} \rangle \quad R(x, \vec{w}, \langle y_1, \vec{u} \rangle) & \text{(Beachte: R ist P-Prädikat!)}
\end{array}
$$

Für R_0 ergibt sich

$$
\begin{array}{lll}
R_0(x) & & \\
\quad \Rightarrow & \exists^+ \vec{w} \quad \forall y_1 \quad \exists i \leq p(n) \quad \forall y_2 \quad \neg R^*(x, y_1 \oplus w_i, y_2) & \text{($\mathcal{BPP}$-Theorem)} \\
\quad \Rightarrow & \exists^+ \vec{w} \quad \forall y_1 \quad \forall \vec{u} \quad \exists i \leq p(n) \quad \neg R^*(x, y_1 \oplus w_i, u_i) & \text{(s.o.)} \\
\quad \Rightarrow & \exists^+ \vec{w} \quad \forall \langle y_1, \vec{u} \rangle \quad \left(\exists i \leq p(n) \quad \neg R^*(x, y_1 \oplus w_i, u_i)\right) & \\
\quad \Rightarrow & \exists^+ \vec{w} \quad \forall \langle y_1, \vec{u} \rangle \quad \neg \underbrace{\left(\forall i \leq p(n) \quad R^*(x, y_1 \oplus w_i, u_i)\right)}_{R(x, \vec{w}, \langle y_1, \vec{u} \rangle)} & \\
\quad \Rightarrow & \exists^+ \vec{w} \quad \forall \langle y_1, \vec{u} \rangle \quad \neg R(x, \vec{w}, \langle y_1, \vec{u} \rangle) &
\end{array}
$$

$\square$

Durch Induktion wird dieses Ergebnis auf $\mathcal{AM}$ generalisiert. Der Beweis für $\mathcal{MA}$ geht analog.

7 Kollaps-Theorem für $\mathcal{AM}$

Das Kollaps-Theorem besagt nun, dass die Hierarchie der Arthur-Merlin Spiele auf $\mathcal{AM}_2$ kollabiert.

Theorem (Kollaps-Theorem).

1. *$\mathcal{MA}_3 \subseteq \mathcal{AM}_2$.*
2. *$\mathcal{AM}_{k+1} = \mathcal{AM}_k$, für $k \geq 2$.*

Beweis.

<u>Beweis der ersten Aussage</u>
Seien R_1 und R_0 komplementäre $\mathcal{MA}_3$-Prädikate. Wegen des One-Sided-Error-Theorems und Wahrscheinlichkeitsverstärkung existiert ein P-Prädikat R, so dass gilt

$$\begin{array}{llllll} R_1(x) & \Rightarrow & \exists y_1 & \forall y_2 & \exists y_3 & R(x, y_1, y_2, y_3) \\ R_0(x) & \Rightarrow & \forall y_1 & \exists^+_r y_2 & \forall y_3 & \neg R(x, y_1, y_2, y_3) \quad \text{mit } r = 1 - 2^{-n}. \end{array}$$

Für R_1 ergibt sich nun

$$\begin{array}{ll} R_1(x) & \\ \Rightarrow \ \exists y_1 \quad \forall y_2 \quad \exists y_3 \quad R(x, y_1, y_2, y_3) & \\ \Rightarrow \ \forall \vec{w} \quad \exists y_1 \quad \forall i \leq p(n) \quad \exists y_3 \quad R(x, y_1, w_i, y_3) & \text{(sollte klar sein)} \\ \Rightarrow \ \forall \vec{w} \quad \exists y_1 \quad \exists \vec{u} \quad \forall i \leq p(n) \quad R(x, y_1, w_i, u_i) & \text{(s.o.)} \\ \Rightarrow \ \forall \vec{w} \quad \exists \langle y_1, \vec{u} \rangle \quad \underbrace{\big(\forall i \leq p(n) \quad R(x, y_q, w_i, u_i)\big)}_{(P\text{-Prädikat})} & \end{array}$$

Für R_2 erhält man nun

$$\begin{array}{ll} R_0(x) & \\ \Rightarrow \ \forall y_1 \quad \exists^+_r y_2 \quad \forall y_3 \quad \neg R(x, y_1, y_2, y_3) & \\ \Rightarrow \ \exists^+ \vec{w} \quad \forall y_1 \quad \exists i \leq p(n) \quad \forall y_3 \quad \neg R(x, y_1, w_i, y_3) & \text{(Swapping-Lemma)} \\ \Rightarrow \ \exists^+ \vec{w} \quad \forall y_1 \quad \forall \vec{u} \quad \exists i \leq p(n) \quad \neg R(x, y_1, w_i, u_i) & \text{(s.o.)} \\ \Rightarrow \ \exists^+ \vec{w} \quad \forall \langle y_1, \vec{u} \rangle \quad \big(\exists i \leq p(n) \quad \neg R(x, y_1, w_i, u_i)\big) & \\ \Rightarrow \ \exists^+ \vec{w} \quad \forall \langle y_1, \vec{u} \rangle \quad \neg \underbrace{\big(\forall i \leq p(n) \quad R(x, y_1, w_i, u_i)\big)} & \end{array}$$

Also sind R_0 und R_1 komplementäre $\mathcal{AM}_2$-Prädikate.

Beweis der zweiten Aussage
Sei $L \in \mathcal{AM}_{k+1},\ k \geq 2$; für gerades k sei $j = 2$, für ungerades k sei $j = 3$. Dann existieren komplementäre $\mathcal{MA}_j$-Prädikate R_1 und R_0, so dass für alle x ($\|x\| = n$) gilt

$$\begin{array}{lllllll} x \in L & \Rightarrow & \exists^+ y_1 & \exists y_2 & \dots & \exists^+ y_{k-j+1} & R_1(x, y_1, \dots, y_{k-j+1}) \\ x \notin L & \Rightarrow & \exists^+ y_1 & \forall y_2 & \dots & \exists^+ y_{k-j+1} & R_0(x, y_1, \dots, y_{k-j+1}) \end{array} \tag{5}$$

Aus 1 folgt, dass R_1 und R_0 komplementäre $\mathcal{AM}_2$-Prädikate sind und es gibt ein P-Prädikat R_2, so dass gilt

$$\begin{aligned} R_1(x, y_1, \dots, y_{k-j+1}) &\equiv \forall z_1 \quad \exists z_2 \quad R_2(x, y_1, \dots, y_{k-j+1}, z_1, z_2) \\ R_0(x, y_1, \dots, y_{k-j+1}) &\equiv \exists^+ z_1 \quad \forall z_2 \quad \neg R_2(x, y_1, \dots, y_{k-j+1}, z_1, z_2) \end{aligned} \tag{6}$$

Substituiert man nun (6) in (5) und fasst die Quantoren zu jeweils einem $\exists^+$-Quantor zusammen, so ergibt sich

$$L \in \mathcal{AM}_{k-j+2} \subseteq \mathcal{AM}_k$$

□

Korollar. *Für $k > 2$ gilt*

$$\mathcal{AM}_k = \mathcal{MA}_k = \mathcal{AM}_2$$

Literatur

[DlK00] Ding-Zhu Du and Ker l Ko. *Theory of Computational Complexity.* Wiley, 2000.