RUHR UNIVERSITÄT BOCHUM RUB

Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Enrico Thomae

Lösungsblatt zur Vorlesung

Quantenalgorithmen

WS 2011/2012

Blatt 2 / 31. Oktober 2011

Abgabe bis 14. November 2011, 14 Uhr (vor der Übung)

AUFGABE 1 (4 Punkte)**:**
Seien $A \in \mathbb{C}^{m\times m}$ und $B \in \mathbb{C}^{n\times n}$ zwei unitäre Matrizen. Beweisen Sie, dass auch $A \otimes B$ eine unitäre Matrix ist.

Lösungsvorschlag:

Zeige: $(A\otimes B)\overline{(A\otimes B)}^T = I_{mn}$.
Es gilt:

$$\overline{(A\otimes B)}^T = \overline{\begin{pmatrix} a_{11}B & \dots & a_{1m}B \\ \vdots & \ddots & \vdots \\ a_{m1}B & \dots & a_{mm}B \end{pmatrix}}^T = \begin{pmatrix} \overline{a_{11}B} & \dots & \overline{a_{1m}B} \\ \vdots & \ddots & \vdots \\ \overline{a_{m1}B} & \dots & \overline{a_{mm}B} \end{pmatrix}^T = \begin{pmatrix} \overline{a_{11}}\,\overline{B} & \dots & \overline{a_{1m}}\,\overline{B} \\ \vdots & \ddots & \vdots \\ \overline{a_{m1}}\,\overline{B} & \dots & \overline{a_{mm}}\,\overline{B} \end{pmatrix}^T$$

$$= \begin{pmatrix} \overline{a_{11}}\,\overline{B}^T & \dots & \overline{a_{m1}}\,\overline{B}^T \\ \vdots & \ddots & \vdots \\ \overline{a_{1m}}\,\overline{B}^T & \dots & \overline{a_{mm}}\,\overline{B}^T \end{pmatrix}.$$

Es folgt:

$$(A\otimes B)\overline{(A\otimes B)}^T = \begin{pmatrix} a_{11} & \dots & a_{1m} \\ \vdots & \ddots & \vdots \\ a_{m1} & \dots & a_{mm} \end{pmatrix} \cdot \begin{pmatrix} \overline{a_{11}}\,\overline{B}^T & \dots & \overline{a_{m1}}\,\overline{B}^T \\ \vdots & \ddots & \vdots \\ \overline{a_{1m}}\,\overline{B}^T & \dots & \overline{a_{mm}}\,\overline{B}^T \end{pmatrix} = \left(\sum_{k=0}^{m} a_{ik}\overline{a_{jk}}B\overline{B}^T\right)_{1\le i,j\le m}$$

$= \left(\sum_{k=0}^{m} a_{ik}\overline{a_{jk}}I_n\right)_{1\le i,j\le m}$ da B unitär. Auch gilt $\sum_{k=0}^{m} a_{ik}\overline{a_{jk}} = 1 \Leftrightarrow i = j$, da A unitär, d.h. $\sum_{k=0}^{m} a_{ik}\overline{a_{jk}} = \delta_{i,j}$, mit $\delta_{i,j}$ Kronecker-Delta. Also folgt:

$$\left(\sum_{k=0}^{m} a_{ik}\overline{a_{jk}}I_n\right)_{1\le i,j\le m} = (\delta_{i,j}I_n)_{1\le i,j\le m} = I_{mn}.$$

AUFGABE 2 (5 Punkte)**:**
Sei $H_n := \bigotimes_{i=1}^{n} W_2$ und $y \in \{0,1\}^n$. Zeigen Sie, dass

$$H_n|y\rangle = 2^{-\frac{n}{2}} \sum_{x\in\{0,1\}^n} (-1)^{x\cdot y}|x\rangle,$$

wobei $x \cdot y$ das Skalarprodukt von x und y ist.

Lösungsvorschlag:

Betrachte zunächst $H_1|y_i\rangle$ für ein einzelnes Bit $y_i \in \{0,1\}$:
$H_1|0\rangle = W_2|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ und $H_1|1\rangle = W_2|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.
Also gilt für $H_1|y_i\rangle$:

$$H_1|y_i\rangle = \frac{1}{\sqrt{2}}(|0\rangle + (-1)^{y_i}|1\rangle)$$

Scharfes Hinsehen liefert, dass sich $H_1|y_i\rangle$ somit auch als:

$$H_1|y_i\rangle = W_2|y_i\rangle = \frac{1}{\sqrt{2}} \sum_{x \in \{0,1\}} (-1)^{y_i \cdot x}|x\rangle \tag{1}$$

schreiben lässt.
Sei nun $y \in \{0,1\}^n$. Es gilt:

$$H_n|y\rangle = \left(\bigotimes_{i=1}^{n} W_2\right)|y\rangle = \bigotimes_{i=1}^{n}(W_2|y_i\rangle) \overset{(1)}{=} \bigotimes_{i=1}^{n}\left(\frac{1}{\sqrt{2}}\sum_{x_i \in \{0,1\}}(-1)^{x_i \cdot y_i}|x_i\rangle\right)$$

$$= 2^{-\frac{n}{2}} \bigotimes_{i=1}^{n}\left(\sum_{x_i \in \{0,1\}}(-1)^{x_i \cdot y_i}|x_i\rangle\right) = 2^{-\frac{n}{2}} \sum_{x \in \{0,1\}^n} \bigotimes_{i=1}^{n}((-1)^{x_i \cdot y_i}|x_i\rangle)$$

$$= 2^{-\frac{n}{2}} \sum_{x \in \{0,1\}^n} \prod_{i=1}^{n}(-1)^{x_i \cdot y_i} \bigotimes_{i=1}^{n}|x_i\rangle = 2^{-\frac{n}{2}} \sum_{x \in \{0,1\}^n}(-1)^{\sum_{i=1}^{n} x_i \cdot y_i} \bigotimes_{i=1}^{n}|x_i\rangle = 2^{-\frac{n}{2}} \sum_{x \in \{0,1\}^n}(-1)^{\langle x|y\rangle}|x\rangle.$$

AUFGABE 3 (5 Punkte)**:**
Gegeben seien

$$\begin{aligned}
|\beta_{00}\rangle &= \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right), \\
|\beta_{01}\rangle &= \frac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right), \\
|\beta_{10}\rangle &= \frac{1}{\sqrt{2}}\left(|00\rangle - |11\rangle\right), \\
|\beta_{11}\rangle &= \frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right).
\end{aligned}$$

a) Zeigen Sie, dass $\{|\beta_{00}\rangle, |\beta_{01}\rangle, |\beta_{10}\rangle, |\beta_{11}\rangle\}$ eine orthonormale Basis bildet (die sogenannte Bell Basis).

b) Zeigen Sie folgende Identität für $|z\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$.

$$|z\rangle \otimes |\beta_{00}\rangle = \frac{1}{2}|\beta_{00}\rangle \otimes |z\rangle + \frac{1}{2}|\beta_{01}\rangle \otimes (M_1|z\rangle) + \frac{1}{2}|\beta_{10}\rangle \otimes (F|z\rangle) + \frac{1}{2}|\beta_{11}\rangle \otimes (M_1F|z\rangle)$$

Dabei bezeichnet $M_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ das Quanten Not und $F = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ den Flip.

c) Beschreiben Sie einen Algorithmus zur Quanten Teleportation, in dem Alice lediglich in der Bell Basis misst.

Lösungsvorschlag:

(a) Zeige, dass die Vektoren der Bell-Basis normiert sind. Betrachte:
$|\langle\beta_{00}||^2 = \langle\beta_{00}|\beta_{00}\rangle = \frac{1}{2}\langle|00\rangle+|11\rangle||00\rangle+|11\rangle\rangle = \frac{1}{2}(\underbrace{\langle 00|00\rangle}_{1}+\underbrace{\langle 00|11\rangle}_{0}+\underbrace{\langle 11|00\rangle}_{0}+\underbrace{\langle 11|11\rangle}_{1}) = 1.$

$|\langle\beta_{01}||^2 = \langle\beta_{01}|\beta_{01}\rangle = \frac{1}{2}\langle|01\rangle+|10\rangle||01\rangle+|10\rangle\rangle = \frac{1}{2}(\overbrace{\langle 01|01\rangle}^{1}+\overbrace{\langle 01|10\rangle}^{0}+\overbrace{\langle 10|01\rangle}^{0}+\overbrace{\langle 10|10\rangle}^{1}) = 1.$

$|\langle\beta_{10}||^2 = \langle\beta_{10}|\beta_{10}\rangle = \frac{1}{2}\langle|00\rangle-|11\rangle||00\rangle-|11\rangle\rangle = \frac{1}{2}(\underbrace{\langle 00|00\rangle}_{1}-\underbrace{\langle 00|11\rangle}_{0}-\underbrace{\langle 11|00\rangle}_{0}+\underbrace{\langle 11|11\rangle}_{1}) = 1.$

$|\langle\beta_{11}||^2 = \langle\beta_{11}|\beta_{11}\rangle = \frac{1}{2}\langle|01\rangle-|10\rangle||01\rangle-|10\rangle\rangle = \frac{1}{2}(\overbrace{\langle 01|01\rangle}^{1}-\overbrace{\langle 01|10\rangle}^{0}-\overbrace{\langle 10|01\rangle}^{0}+\overbrace{\langle 10|10\rangle}^{1}) = 1.$

Zeige nun, dass alle Vektoren der Bell Basis paarweise orthongonal aufeinander stehen:
$\langle\beta_{00}|\beta_{01}\rangle = \frac{1}{2}\langle|00\rangle+|11\rangle||01\rangle+|10\rangle\rangle = \frac{1}{2}(\langle 00|01\rangle+\langle 00|10\rangle+\langle 11|01\rangle+\langle 11|10\rangle) = 0.$

$\langle\beta_{00}|\beta_{10}\rangle = \frac{1}{2}\langle|00\rangle+|11\rangle||00\rangle-|11\rangle\rangle = \frac{1}{2}(\langle 00|00\rangle-\langle 00|11\rangle+\langle 11|00\rangle-\langle 11|11\rangle) = 1-1 = 0.$

$\langle\beta_{00}|\beta_{11}\rangle = \frac{1}{2}\langle|00\rangle+|11\rangle||01\rangle-|10\rangle\rangle = \frac{1}{2}(\langle 00|01\rangle-\langle 00|10\rangle+\langle 11|01\rangle-\langle 11|10\rangle) = 0.$

$\langle\beta_{01}|\beta_{10}\rangle = \frac{1}{2}\langle|01\rangle+|10\rangle||00\rangle-|11\rangle\rangle = \frac{1}{2}(\langle 01|00\rangle-\langle 01|11\rangle+\langle 10|00\rangle-\langle 10|11\rangle) = 0.$

$\langle\beta_{01}|\beta_{11}\rangle = \frac{1}{2}\langle|01\rangle+|10\rangle||01\rangle-|10\rangle\rangle = \frac{1}{2}(\langle 01|01\rangle-\langle 01|10\rangle+\langle 10|01\rangle-\langle 10|10\rangle) = 1-1 = 0.$

$\langle\beta_{10}|\beta_{11}\rangle = \frac{1}{2}\langle|00\rangle-|11\rangle||01\rangle-|10\rangle\rangle = \frac{1}{2}(\langle 00|01\rangle-\langle 00|10\rangle-\langle 11|01\rangle+\langle 11|10\rangle) = 0.$
Da orthogonale Vektoren linear unabhängig sind, bilden die vier Vektoren der Bell Basis eine orthonormale Basis des $\mathbb{C}^4$.

(b) Es gilt:
$M_1|z\rangle = \alpha_1|0\rangle+\alpha_0|1\rangle$, sowie $F|z\rangle = \alpha_0|0\rangle-\alpha_1|1\rangle$ und $M_1F|z\rangle = \alpha_0|1\rangle-\alpha_1|0\rangle$. Für die rechte Seite ergibt sich:
$\frac{1}{2}|\beta_{00}\rangle\otimes|z\rangle+\frac{1}{2}|\beta_{01}\rangle\otimes(M_1|z\rangle)+\frac{1}{2}|\beta_{10}\rangle\otimes(F|z\rangle)+\frac{1}{2}|\beta_1 1\rangle\otimes(M_1F|z\rangle)$
$= \frac{\alpha_0}{2\sqrt{2}}|000\rangle+\frac{\alpha_1}{2\sqrt{2}}|001\rangle+\frac{\alpha_0}{2\sqrt{2}}|110\rangle+\frac{\alpha_1}{2\sqrt{2}}|111\rangle+\frac{\alpha_1}{2\sqrt{2}}|010\rangle+\frac{\alpha_0}{2\sqrt{2}}|011\rangle+\frac{\alpha_1}{2\sqrt{2}}|100\rangle+\frac{\alpha_0}{2\sqrt{2}}|101\rangle$
$+\frac{\alpha_0}{2\sqrt{2}}|000\rangle-\frac{\alpha_1}{2\sqrt{2}}|001\rangle-\frac{\alpha_0}{2\sqrt{2}}|110\rangle+\frac{\alpha_1}{2\sqrt{2}}|111\rangle+\frac{\alpha_0}{2\sqrt{2}}|011\rangle-\frac{\alpha_1}{2\sqrt{2}}|010\rangle-\frac{\alpha_0}{2\sqrt{2}}|101\rangle+\frac{\alpha_1}{2\sqrt{2}}|100\rangle$
$= \frac{\alpha_0}{\sqrt{2}}|000\rangle+\frac{\alpha_1}{\sqrt{2}}|111\rangle+\frac{\alpha_0}{\sqrt{2}}|011\rangle+\frac{\alpha_1}{\sqrt{2}}|100\rangle$
$= (\alpha_0|0\rangle+\alpha_1|1\rangle)\otimes(\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle))$
$= |z\rangle\otimes|\beta_{00}\rangle.$

(c) Alice und Bob teilen sich wieder ein EPR-Paar $|e\rangle$, wobei Alice das erste, Bob das zweite Qubit gehört.Alice kennt $|z\rangle = \alpha_0|0\rangle+\alpha_1|1\rangle$, welches an Bob gesendet werden soll. Alice berechnet $|z\rangle\otimes|e\rangle = |z\rangle\otimes|\beta_{00}\rangle$. Nach b) gilt nun

$$|z\rangle\otimes|e\rangle = \frac{1}{2}|\beta_{00}\rangle\otimes|z\rangle+\frac{1}{2}|\beta_{01}\rangle\otimes(M_1|z\rangle)+\frac{1}{2}|\beta_{10}\rangle\otimes(F|z\rangle)+\frac{1}{2}|\beta_{11}\rangle\otimes(M_1F|z\rangle).$$

Alice misst nun ihre Qubits in der Bell-Basis und erhält $|\beta_{ij}\rangle$. Alice sendet (i,j) über den klassischen Kanal an Bob der auf seinem Qubit (das letze) folgende Operation durchführt:

Messung von Alice	System im Zustand	Operation auf Bobs Qubit
(0,0)	$\|\beta_{00}\rangle \otimes \|z\rangle$	Nix
(0,1)	$\|\beta_{01}\rangle \otimes (M_1\|z\rangle)$	M_1, da $M_1M_1 = I_2$
(1,0)	$\|\beta_{10}\rangle \otimes (F\|z\rangle)$	F, da $FF = I_2$
(1,1)	$\|\beta_{11}\rangle \otimes (M_1F\|z\rangle)$	FM_1, da $FM_1M_1F = I_2$

Somit erhält Bob in seinem Qubit $|z\rangle$.

AUFGABE 4 (7 Punkte)**:**
Alice, Bob und Charlie teilen sich den folgenden 3-Qubit Zustand

$$\frac{1}{2}(|000\rangle - |110\rangle - |011\rangle - |101\rangle),$$

wobei Alice das 1. Qubit gehört, Bob das 2. und Charlie das 3. Qubit. Weiterhin hat jeder ein klassisches Bit b_A, b_B, b_C, so dass gilt $b_A \oplus b_B \oplus b_C = 0$.
Ziel von Alice, Bob und Charlie ist die Ausgabe von Bits a, b, c mit der Eigenschaft

$$b_A \vee b_B \vee b_C = a \oplus b \oplus c. \tag{2}$$

Dazu führen sie folgendes Protokoll durch:

- Jeder Teilnehmer dessen klassisches Bit Eins ist, führt W_2 auf seinem Qubit aus.
- Jeder misst sein Qubit und gibt das Ergebnis aus.

(a) Zeigen Sie, dass das Protokoll korrekt ist, d.h. dass Gleichung (2) erfüllt.

(b) Zeigen Sie, dass es keinen deterministischen Algorithmus gibt, der das Problem löst.

Lösungsvorschlag:

(a) Beobachte zunächst, dass es vier Wahlen von b_A, b_B, b_C gibt, die $b_A \oplus b_B \oplus b_C = 0$ genügen: $(b_A, b_B, b_C) \in \{(0,0,0), (1,1,0), (1,0,1), (0,1,1)\}$. Betrachte für dies Fälle den Protokollablauf:

$b_A = b_B = b_C = 0$:
Keiner führt W_2 auf seinem Qubit aus. Das System wird nicht verändert und die Messung liefert (0,0,0), (1,1,0), (0,1,1), oder (1,0,1). In allen Fällen gilt $b_A \vee b_B \vee b_C = 0 = a \oplus b \oplus c$.

$b_A = 1 = b_B, b_C = 0$:
Alice und Bob führen W_2 auf ihrem Qubit aus:
$(W_2 \otimes W_2 \otimes I_2)\frac{1}{2}(|000\rangle - |110\rangle - |011\rangle - |101\rangle)$
$= \frac{1}{2}(W_2|0\rangle \otimes W_2|0\rangle \otimes |0\rangle - W_2|1\rangle \otimes W_2|1\rangle \otimes |0\rangle - W_2|0\rangle \otimes W_2|1\rangle \otimes |1\rangle - W_2|1\rangle \otimes W_2|0\rangle \otimes |1\rangle)$
$= \frac{1}{4}((|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle) \otimes |0\rangle - (|0\rangle - |1\rangle) \otimes (|0\rangle - |1\rangle) \otimes |0\rangle - (|0\rangle + |1\rangle) \otimes (|0\rangle - |1\rangle) \otimes |1\rangle - (|0\rangle - |1\rangle) \otimes (|0\rangle + |1\rangle) \otimes |1\rangle)$
$= \frac{1}{4}(|000\rangle + |010\rangle + |100\rangle + |110\rangle - |000\rangle + |010\rangle + |100\rangle - |110\rangle - |001\rangle + |011\rangle - |101\rangle + |111\rangle - |001\rangle - |011\rangle + |101\rangle + |111\rangle)$
$= \frac{1}{2}(|010\rangle + |100\rangle - |001\rangle + |111\rangle)$
Die Messung der Qubits liefert hier $(0,1,0), (1,0,0), (0,0,1)$, oder $(1,1,1)$.

In allen Fällen gilt $b_A \vee b_B \vee b_C = 1 = a \oplus b \oplus c$.

$b_A = 1 = b_C, b_B = 0$:
Alice und Charlie führen W_2 auf ihrem Qubit aus:
$(W_2 \otimes I_2 \otimes W_2)\frac{1}{2}(|000\rangle - |110\rangle - |011\rangle - |101\rangle)$
$= \frac{1}{2}(W_2|0\rangle \otimes |0\rangle \otimes W_2|0\rangle - W_2|1\rangle \otimes |1\rangle \otimes W_2|0\rangle - W_2|0\rangle \otimes |1\rangle \otimes W_2|1\rangle - W_2|1\rangle \otimes |0\rangle \otimes W_2|1\rangle)$
$= \frac{1}{4}((|0\rangle + |1\rangle) \otimes |0\rangle \otimes (|0\rangle + |1\rangle) - (|0\rangle - |1\rangle) \otimes |1\rangle \otimes (|0\rangle + |1\rangle) - (|0\rangle + |1\rangle) \otimes |1\rangle \otimes (|0\rangle - |1\rangle) - (|0\rangle - |1\rangle) \otimes |0\rangle \otimes (|0\rangle - |1\rangle))$
$= \frac{1}{4}(|000\rangle + |001\rangle + |100\rangle + |101\rangle - |010\rangle - |011\rangle + |110\rangle + |111\rangle - |010\rangle + |011\rangle - |110\rangle + |111\rangle - |000\rangle + |001\rangle + |100\rangle - |101\rangle)$
$= \frac{1}{2}(+|001\rangle + |100\rangle - |010\rangle + |111\rangle)$
Die Messung der Qubits liefert hier $(0,0,1), (1,0,0), (0,1,0)$, oder $(1,1,1)$.
In allen Fällen gilt $b_A \vee b_B \vee b_C = 1 = a \oplus b \oplus c$.

$b_B = 1 = b_C, b_A = 0$:
Bob und Charlie führen W_2 auf ihrem Qubit aus:
$(I_2 \otimes W_2 \otimes W_2)\frac{1}{2}(|000\rangle - |110\rangle - |011\rangle - |101\rangle)$
$= \frac{1}{4}(|0\rangle \otimes W_2|0\rangle \otimes W_2|0\rangle - |1\rangle \otimes W_2|1\rangle \otimes W_2|0\rangle - |0\rangle \otimes W_2|1\rangle \otimes W_2|1\rangle - |1\rangle \otimes W_2|0\rangle \otimes W_2|1\rangle)$
$= \frac{1}{4}(|0\rangle \otimes (|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle) - |1\rangle \otimes (|0\rangle - |1\rangle) \otimes (|0\rangle + |1\rangle) - |0\rangle \otimes (|0\rangle - |1\rangle) \otimes (|0\rangle - |1\rangle) - |1\rangle \otimes (|0\rangle + |1\rangle) \otimes (|0\rangle - |1\rangle))$
$= \frac{1}{4}(|000\rangle + |001\rangle + |010\rangle + |011\rangle - |100\rangle - |101\rangle + |110\rangle + |111\rangle - |000\rangle + |001\rangle + |010\rangle - |011\rangle - |100\rangle + |101\rangle - |110\rangle + |111\rangle)$
$= \frac{1}{2}(+|001\rangle + |010\rangle - |100\rangle + |111\rangle)$
Die Messung der Qubits liefert hier $(0,0,1), (0,1,0), (1,0,0)$, oder $(1,1,1)$.
In allen Fällen gilt $b_A \vee b_B \vee b_C = 1 = a \oplus b \oplus c$.
Somit ist das Protokoll korrekt.

(b) Annahme: Es existiert ein deterministischer Algorithmus, der das Problem löst.
Es existieren also deterministische Funktionen $D_A, D_B, D_C : \{0,1\} \to \{0,1\}$, mit denen das Protokoll korrekt ausgeführt werden kann.
Notation: $I_x := D_I(x)$, wobei $I \in A, B, C, x \in \{0,1\}$. Für alle Belegungen von b_A, b_B, b_C muss

$$b_A \vee b_B \vee b_C = a \oplus b \oplus c$$

gelten, d.h.

$$A_{b_A} \oplus B_{b_B} \oplus C_{b_C} = b_A \vee b_B \vee b_C \text{ für alle } b_i \in \{0,1\}.$$

Also gilt:

$$\begin{aligned}
A_0 \oplus B_0 \oplus C_0 &= 0 \vee 0 \vee 0 = 0 \\
A_0 \oplus B_1 \oplus C_1 &= 0 \vee 1 \vee 1 = 1 \\
A_1 \oplus B_0 \oplus C_1 &= 1 \vee 0 \vee 1 = 1 \\
A_1 \oplus B_1 \oplus C_0 &= 1 \vee 1 \vee 0 = 1
\end{aligned}$$

XORen aller vier Gleichungen führt zu:
$A_0 \oplus B_0 \oplus C_0 \oplus A_0 \oplus B_1 \oplus C_1 \oplus A_1 \oplus B_0 \oplus C_1 \oplus A_1 \oplus B_1 \oplus C_0 = 1 \oplus 1 \oplus 1$.
Da auf der linken Seite jede Belegung jeder Funktion genau zweimal vorkommt, folgt:

$$0 = 1.$$

Widerspruch,also falsche Annahme. Es gibt keinen det. Algorithmus, der das Problem löst.