# PCP ohne Vorverweise
# Oder: It's all linear algebra

Klaus Aehlig  Markus Latte  Dimitri Scheftelowitsch

Der Tragödie erster Teil (Rest wird später nachgeliefert)

**Zusammenfassung**

Dies ist der Versuch der Autoren, einen Beweis des PCP-Theorems aufzuschreiben, ohne erst später bewiesene Sätze zu verwenden.

## Vorwort

Dieses Skript stellt die Ausarbeitung des Workshops "Probabilistically Checkable Proofs" auf der Winterakademie 2012/13 des Clubs der Ehemaligen der Deutschen Schülerakademie e.V. (CdE) da. Hauptvorlage des 3-tägigen Workshops in Windischleuba (Thüringen) bildete das Lehrbuch von Arora und Barak [AB09].

## Konventionen

- Vektoren sind Spaltenvektoren.
- Ist $A$ eine Matrix (zum Beispiel ein Vektor), so bezeichnet $A^t$ die transponierte Matrix.
- Alle Wahrscheinlichkeiten beziehen sich auf die Gleichverteilung, es sei denn, es ist explizit etwas anderes zugesichert.
- $\cdot \circ \cdot$ ist die Funktionskomposition. Es gilt $(f \circ g)(x) = f(g(x))$.
- $f^{-1}$ is die inverse Funktion zu $f$, falls existent.

## 1 Zeugen für die Lösbarkeit linearer Gleichungssysteme

**Definition 1.1.** Für $u = (u_1, \ldots, u_n)^t$ und $v = (v_1, \ldots, v_n)^t$ aus $\mathbb{F}_2^n$ setzen wir $\langle u, v\rangle_{\mathbb{F}_2} = \sum_i u_i v_i$.

**Bemerkung 1.2.** Aus Definition 1.1 folgt unmittelbar $\langle u, v\rangle_{\mathbb{F}_2} = \langle v, u\rangle_{\mathbb{F}_2}$.

**Bemerkung 1.3.** Für $u \in \mathbb{F}_2^n$ ist die Abbildung $\mathbb{F}_2^n \to \mathbb{F}_2$, $x \mapsto \langle u, x\rangle_{\mathbb{F}_2}$ linear mit darstellender Matrix $u^t$. Umgekehrt gibt es zu jeder linearen Abbildung $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$ einen Vektor $u$, so dass $f(x) = \langle u, x\rangle_{\mathbb{F}_2}$ ist, nämlich das Transponierte der darstellenden Matrix.

**Theorem 1.4.** *Sei $0 \neq u \in \mathbb{F}_2^n$, so gilt für die Hälfte aller $x \in \mathbb{F}_2^n$, dass $\langle u, x\rangle_{\mathbb{F}_2} \neq 0$.*

*Beweis.* Sei $u = (u_1, \ldots, u_n)^t$ mit $u_j \neq 0$. Für $x = (x_1, \ldots, x_n)^t$ gilt $\langle u, x\rangle_{\mathbb{F}_2} = \sum_{i \neq j} u_i x_i + u_j x_j = C + x_j$ für ein von $x_j$ unabhängiges $C \in \mathbb{F}_2$. Es gilt also für genau einen der beiden Vektoren $(x_1, \ldots, x_{j-1}, 0, x_{j+1}, \ldots, x_n)^t$ und $(x_1, \ldots, x_{j-1}, 1, x_{j+1}, \ldots, x_n)^t$, dass das Produkt nicht 0 ist. □

**Korollar 1.5.** *Sind $u, v \in \mathbb{F}_2^n$ mit $u \neq v$, so gilt für die Hälfte aller $x \in \mathbb{F}_2^n$ dass $\langle u, x\rangle_{\mathbb{F}_2} \neq \langle v, x\rangle_{\mathbb{F}_2}$.*

*Beweis.* Ist $u \neq v$, so ist $u - v \neq 0$. Ferner ist $\langle u, x\rangle_{\mathbb{F}_2} - \langle v, x\rangle_{\mathbb{F}_2} = \langle u - v, x\rangle_{\mathbb{F}_2}$. Theorem 1.4 liefert die Behauptung. □

**Bemerkung 1.6.** Korollar 1.5 ist der Ort, an dem die Reduktion des Betrachtens geschieht: um zwei Vektoren in $\mathbb{F}_2^n$ mit hoher Wahrscheinlichkeit richtig zu vergleichen, genügt es, nur zwei Bits statt $2n$ Bits zu lesen. Dazu ist ein Vektor $w$ als (Wertetabelle der) Funktion $\mathbb{F}_2^n \to \mathbb{F}_2$, $x \mapsto \langle w, x\rangle_{\mathbb{F}_2}$ gegeben statt als Folge seiner Komponenten. In den weiteren Schritten wird diese Funktion in den Zeugen ausgelagert, der letztendlich die Lösbarkeit eines gegebenen linearen Gleichungssystem attestiert.

**Korollar 1.7.** *Seien $A, B \in \mathbb{F}_2^{m \times n}$ mit $A \neq B$. Dann gilt für die Hälfte aller $v \in \mathbb{F}_2^n$, dass $Av \neq Bv$.*

*Beweis.* Da $A \neq B$, gibt es ein $i$ so dass sich die $i$-te Zeile $a_i$ von $A$ von der $i$-ten Zeile $b_i$ von $B$ unterscheidet. Der $i$-te Eintrag von $Av$ ist dann gerade $\langle a_i, v\rangle_{\mathbb{F}_2}$ und der $i$-te Eintrag von $Bv$ ist $\langle b_i, v\rangle_{\mathbb{F}_2}$. Die Behauptung folgt aus Korollar 1.5. □

**Definition 1.8.** Sei $\rho \in \mathbb{R}$. Zwei Funktionen $f, g\colon \mathbb{F}_2^n \to \mathbb{F}_2$ heißen *$\rho$-nahe*, falls $\mathsf{Pr}_x[f(x) = g(x)] \geq \rho$.

**Bemerkung 1.9.** Zwei Funktionen $f, g\colon \mathbb{F}_2^n \to \mathbb{F}_2$ sind 1-nahe genau dann, wenn sie identisch sind.

**Lemma 1.10.** *Seien $f, g\colon \mathbb{F}_2^n \to \mathbb{F}_2$ linear und $\rho$-nahe für ein $\rho > 1/2$. Dann ist $f = g$.*

*Beweis.* Seien $u^t, v^t$ die darstellenden Matrizen von $f$ und $g$. Die Behauptung folgt aus Korollar 1.5. □

**Korollar 1.11.** *Ist $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$ schon $(1-\delta)$-nahe zu einer linearen Funktion für ein $\delta < 1/4$, so ist die lineare Funktion eindeutig.*

*Beweis.* Sind $g, h\colon \mathbb{F}_2^n \to \mathbb{F}_2$ beide linear und $\delta$-nahe zu $f$, so sind $g, h$ schon $(1-2\delta)$-nahe. Die Behauptung folgt aus Lemma 1.10. $\square$

**Theorem 1.12.** *Sei $\delta < 1/4$. Es gibt einen Algorithmus für das folgende Problem, der mit mindestens Wahrscheinlichkeit $1-2\delta$ das richtige Ergebnis liefert.*

> *Gegeben eine Funktion $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$, die $(1-\delta)$-nahe einer linearen Funktion $\tilde{f}\colon \mathbb{F}_2^n \to \mathbb{F}_2$ ist, und gegeben $x \in \mathbb{F}_2^n$. Bestimme $\tilde{f}(x)$.*

*Ferner betrachtet der Algorithmus für beliebige $f$ und $x$ nur konstant viele Stellen von $f$.*

*Beweis.* Zunächst bemerken wir, dass $\tilde{f}$ nach Korollar 1.11 eindeutig bestimmt ist. Der Algorithmus funktioniert wie folgt.

> Wähle $x' \in \mathbb{F}_2^n$ zufällig und setze $x'' = x' + x$. Bestimme $y' = f(x')$ und $y'' = f(x'')$. Antworte $y'' - y'$.

Wir sehen, dass sowohl $y'$, als auch $y''$ gleichverteilt auf $\mathbb{F}_2^n$ sind. Da $f, \tilde{f}$ schon $(1-\delta)$-nahe sind, gilt mit Wahrscheinlichkeit jeweils mindestens $1-\delta$, dass $y' = \tilde{f}(x')$ und $y'' = \tilde{f}(x'')$. Mit Wahrscheinlichkeit mindestens $1-2\delta$ gilt also beides. In diesem Fall ist $y'' - y' = \tilde{f}(x'+x) - \tilde{f}(x') = \tilde{f}(x'+x-x') = \tilde{f}(x)$. $\square$

**Theorem 1.13.** *Es gibt einen probabilistischen Algorithmus für das folgende Problem, der korrekte Eingaben stets akzeptiert und falsche mit Wahrscheinlichkeit mindestens $1/2$ zurückweist.*

> *Gegeben $A \in \mathbb{F}_2^{m\times n}$ und $b \in \mathbb{F}_2^m$. Entscheide für $u \in \mathbb{F}_2^n$, ob $Au = b$.*

*Dabei sind $A$ und $b$ explizit gegeben und $u$ in Form einer Abbildung $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$, $x \mapsto \langle u, x\rangle_{\mathbb{F}_2}$, die der Algoritmus nur an einer Stelle auswertet.*

*Beweis.* Der Algorithmus funktioniert wie folgt.

> Wähle $v \in \mathbb{F}_2^m$ zufällig und akzeptiere, wenn $\langle u, A^t v\rangle_{\mathbb{F}_2} = \langle b, v\rangle_{\mathbb{F}_2}$.

Für die Richtigkeit bemerken wir, dass $\langle Au, v\rangle_{\mathbb{F}_2} = \langle u, A^t v\rangle_{\mathbb{F}_2}$ und wenden Korrolar 1.5 an.

Da $A$ und $b$ gegeben sind (und $v$ selbst gewählt), muss der Algoritmus $f$ in der Tat nur an einer Stelle auswerten und kann alle anderen Rechnungen selbst durchführen. $\square$

**Korollar 1.14.** *Sei $\delta < 1/4$ fest. Es gibt einen probabilistischen Algorithmus mit einer Fehlerwahrscheinlichkeit von höchstens $\frac{1}{2} + 2\delta$ für das folgende Problem.*

> *Gegeben $A \in \mathbb{F}_2^{m\times n}$, $b \in \mathbb{F}_2^m$ sowie eine Funktion $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$, die schon $(1-\delta)$-nahe an $\tilde{f}\colon \mathbb{F}_2^n \to \mathbb{F}_2$ linear ist. Entscheide, ob die darstellende Matrix $u$ von $\tilde{f}$ Lösung der Gleichung $Au^t = b$ ist.*

*Darüberhinaus akzeptiert der Algorithmus immer, falls $\delta = 0$ und $Au^t = b$, und wertet $f$ nur an konstant vielen Stellen aus.*

*Beweis.* Bemerkung 1.3 und Theorem 1.13, wobei die eine Stelle von $\tilde{f}$ mittels Theorem 1.12 mit einer Irrtumswahrscheinlichkeit von höchstens $2\delta$ bestimmt wird. $\square$

$$\begin{array}{ccccccc}
\{\alpha \mid \alpha \subseteq [n]\} & \cong & \mathbb{F}_2^n & \cong & (\mathbb{F}_2^n)^* & \hookrightarrow & \{f\colon \{\pm 1\}^n \to \{\pm 1\}\} \subseteq \{f\colon \{\pm 1\}^n \to \mathbb{R}\} \\
 & \text{als Menge} & & u \mapsto \langle u, \cdot \rangle_{\mathbb{F}_2} & & & \\
 & \alpha \mapsto \underline{\alpha} & & & & f \mapsto \uparrow f &
\end{array}$$

Abbildung 1: Überblick über die in Abschnitt 2 verwendeten Vektorräume.

# 2 Linearitätstest

**Definition 2.1.** Für eine natürliche Zahl $n$ sei $[n]$ die Menge $\{0, 1, \ldots, n-1\}$. In der Sprache der Mengenlehre ist also $[n] = n$.

**Definition 2.2.** Für $\alpha \subseteq [n]$ sei $\underline{\alpha} \in \mathbb{F}_2^n$ derjenige Vektor, der genau an den Stellen $i \in [n]$ den Wert 1 stehen hat, an denen $i \in \alpha$.

**Bemerkung 2.3.** $\underline{\cdot}\colon \{\alpha \mid \alpha \subseteq [n]\} \to \mathbb{F}_2^n$ ist ein Isomorphismus von Mengen.

**Definition 2.4.** $\{\pm 1\} := \{-1, 1\}$.

**Definition 2.5.** Die Bijektion $\uparrow\colon \mathbb{F}_2 \to \{\pm 1\}$ ist definiert durch $0 \mapsto 1$ und $1 \mapsto -1$.

**Bemerkung 2.6.** Für $a, b \in \mathbb{F}_2$ gilt $\uparrow(a+b) = (\uparrow a)(\uparrow b)$. Mithin ist $\uparrow\colon (\mathbb{F}_2, +) \to \mathbb{Z}^*$ sogar ein Isomorphismus von Gruppen.

**Definition 2.7.** Für eine Funktion $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$ bezeichnet $\uparrow f$ die Funktion

$$\uparrow \circ f \circ \Big( (x_1, \ldots, x_n) \mapsto (\uparrow^{-1} x_1, \ldots, \uparrow^{-1} x_n) \Big)\colon \{\pm 1\}^n \to \{\pm 1\}\,.$$

**Definition 2.8.** $\mathcal{H}$ ist der Vektorraum über $\mathbb{R}$ der Funktionen

$$\{f \mid f\colon \{\pm 1\}^n \to \mathbb{R}\}$$

mit punktweiser Addition und Muliplikation.

$$\begin{array}{rcl}
(f+g) & := & x \mapsto f(x) + g(x) \\
a \cdot f & := & x \mapsto a f(x)
\end{array}$$

für alle obigen Funktionen und alle $a \in \mathbb{R}$. Vermöge

$$\langle f, g \rangle_{\mathcal{H}} \quad := \quad \mathop{\mathsf{Ex}}_{x \in \{\pm 1\}^n} [f(x) g(x)]$$

wird $\mathcal{H}$ zu einen euklidischen Vektorraum.

**Bemerkung 2.9.** $\mathcal{H}$ ist sogar ein Hilbertraum, aber Vollständigkeit benötigen wir hier nicht.

**Definition 2.10.** Für $\alpha \subseteq [n]$ setze $\chi_\alpha \colon \{\pm 1\}^n \to \{\pm 1\}$ mit $(x_0, \ldots, x_{n-1}) \mapsto \prod_{i \in \alpha} x_i$.

In der Tat sind die $\chi_\alpha$ die Bilder der $\alpha$ unter der Abbildung in Abbildung 1.

**Lemma 2.11.** *Für $\alpha \subseteq [n]$ ist $\uparrow(\langle \underline{\alpha}, \cdot \rangle_{\mathbb{F}_2}) = \chi_\alpha$.*

*Beweis.* Sei $\alpha \subseteq [n]$. Für alle $x = (x_i)_i \in \{\pm 1\}^n$ gilt nun $\uparrow(\langle \underline{\alpha}, \cdot \rangle_{\mathbb{F}_2})(x) = \uparrow(\langle \underline{\alpha}, (\uparrow^{-1} x_i)_i \rangle_{\mathbb{F}_2}) = \uparrow(\sum_{i \in \alpha} \uparrow^{-1} x_i) = \prod_{i \in \alpha} \uparrow(\uparrow^{-1} x_i) = \prod_{i \in \alpha} x_i = \chi_\alpha(x)$. $\square$

**Lemma 2.12.** *Die Familie $\{\chi_\alpha \mid \alpha \subseteq [n]\}$ ist eine Orthonormalbasis in $\mathcal{H}$.*

*Beweis.* Seien $\alpha, \beta \subseteq [n]$ und sei $\delta$ ihre symmetrische Differenz, diese ist $(\alpha \setminus \beta) \cup (\beta \setminus \alpha)$. Die Gleichverteilung wählt jedes Element in $\{\pm 1\}^n$ mit der Wahrscheinlichkeit $p = |\{\pm 1\}^n|^{-1}$. So gilt

$$\langle \chi_\alpha, \chi_\beta \rangle_{\mathcal{H}} \quad = \quad \sum_{\substack{(x_0,\ldots,x_{n-1}) \\ \in \{\pm 1\}^n}} p \prod_{i \in \alpha} x_i \prod_{i \in \beta} x_i \quad = \quad p \sum_{\substack{(x_0,\ldots,x_{n-1}) \\ \in \{\pm 1\}^n}} \prod_{i \in \delta} x_i \prod_{i \in \alpha \cap \beta} \underbrace{x_i^2}_{=1}$$

Falls $\delta$ die leere Menge ist, so ist $\langle \chi_\alpha, \chi_\beta \rangle_{\mathcal{H}} = 1$, da das leere Produkt $p^{-1}$-mal summiert wird. Andernfalls gibt es ein $i \in \delta$ und wir können die Summation über $x_i$ vorziehen. Die verbleibende innere Summe über $(x_0, \ldots, x_{n-1})$ ohne $x_i$ wird einmal mit $-1$ und einmal mit 1 gewichtet. Also ist in diesem Fall $\langle \chi_\alpha, \chi_\beta \rangle_{\mathcal{H}} = 0$. Da jede Funktion in $\mathcal{H}$ von nur $2^n$ Eingaben abhängt, ist die Dimension von $\mathcal{H}$ höchstens $2^n$. Weil die betrachte Familie die Größe $2^n$ hat, bildet sie auch eine Basis. $\square$

**Definition 2.13.** Für $x = (x_i), y = (y_i) \in \mathbb{F}_2^n$ setzen wir $x \odot y = (x_i y_i)_i$.

**Lemma 2.14.** *Für $\alpha \subseteq [n]$ und $x, y \in \{\pm 1\}^n$ gilt $\chi_\alpha(x \odot y) = \chi_\alpha(x)\chi_\alpha(y)$.*

*Beweis.* Sei $x = (x_i)_i$ und $y = (y_i)_i$. Dann ist $\chi_\alpha(x \odot y) = \prod_{i \in \alpha} x_i y_i = (\prod_{i \in \alpha} x_i)(\prod_{i \in \alpha} y_i) = \chi_\alpha(x)\chi_\alpha(y)$. $\square$

**Lemma 2.15.** *Sei $f \colon \{\pm 1\}^n \to \{\pm 1\}$ und $\varepsilon \in \mathbb{R}$. Falls*

$$\Pr_{x,y \in \{\pm 1\}^n}[f(x \odot y) = f(x)f(y)] \quad \geq \quad \frac{1}{2} + \varepsilon\,, \tag{1}$$

*dann gibt es ein $\alpha \subseteq [n]$ mit der Eigenschaft*

$$\langle f, \chi_\alpha \rangle_{\mathcal{H}} \quad \geq \quad 2\varepsilon\,.$$

*Beweis.* Aus der Vorausetzung (1) ergibt sich

$$\Pr_{x,y \in \{\pm 1\}^n}[f(x \odot y) \neq f(x)f(y)] \quad \leq \quad \frac{1}{2} - \varepsilon\,. \tag{2}$$

Da $f(xy)f(x)f(y) \in \{\pm 1\}$, können wir nachfolgenden Erwartungswert abschätzen.

$$\begin{aligned} & \mathop{\mathsf{Ex}}_{x,y\in\{\pm 1\}^n}[f(x\odot y)f(x)f(y)] \\ = \quad & 1\cdot \mathop{\mathsf{Pr}}_{x,y}[f(x\odot y)=f(x)f(y)] + (-1)\cdot \mathop{\mathsf{Pr}}_{x,y}[f(x\odot y)\neq f(x)f(y)] \\ \geq \quad & (\frac{1}{2}+\varepsilon) - (\frac{1}{2}-\varepsilon) = 2\varepsilon\,. \end{aligned}$$

Es sei $f = \sum_{\alpha\subseteq[n]} f_\alpha\chi_\alpha$ mit den $f_\alpha \in \mathbb{R}$ die Basisdarstellung von $f$ in der Orthonormalbasis aus Lemma 2.12. Wir verwenden Lemma 2.14 und erhalten

$$\begin{aligned} 2\varepsilon &\leq \mathop{\mathsf{Ex}}_{x,y}[f(xy)f(x)f(y)] \\ &= \mathop{\mathsf{Ex}}_{x,y}[\sum_{\alpha,\beta,\gamma} f_\alpha\chi_\alpha(xy)f_\beta\chi_\beta(x)f_\gamma\chi_\gamma(y)] \\ &= \mathop{\mathsf{Ex}}_{x,y}[\sum_{\alpha,\beta,\gamma} f_\alpha f_\beta f_\gamma\chi_\alpha(x)\chi_\alpha(y)\chi_\beta(x)\chi_\gamma(y)] \\ &= \sum_{\alpha,\beta,\gamma} f_\alpha f_\beta f_\gamma \mathop{\mathsf{Ex}}_{x}[\chi_\alpha(x)\chi_\beta(x)] \mathop{\mathsf{Ex}}_{y}[\chi_\alpha(y)\chi_\gamma(y)] \\ &= \sum_{\alpha,\beta,\gamma} f_\alpha f_\beta f_\gamma\langle\chi_\alpha,\chi_\beta\rangle_{\mathcal{H}}\langle\chi_\alpha,\chi_\gamma\rangle_{\mathcal{H}} \\ &= \sum_\alpha f_\alpha^3 \\ &\leq \max_\alpha f_\alpha \sum_\alpha f_\alpha^2 \end{aligned}$$

Da $f\colon \{\pm 1\}^n \to \{\pm 1\}$, ist $1 = \langle f, f\rangle_{\mathcal{H}} = \sum_\alpha f_\alpha^2$. Wegen $f_\alpha = \langle f,\chi_\alpha\rangle_{\mathcal{H}}$ ergibt sich die Behauptung. □

**Lemma 2.16.** *Seien $f, g\colon \mathbb{F}_2^n \to \mathbb{F}_2$ und $\delta \in \mathbb{R}$. Dann sind folgende Eigenschaften äquivalent.*

- *$f$ und $g$ sind $\frac{1+\delta}{2}$-nahe.*
- *$\langle\uparrow f, \uparrow g\rangle_{\mathcal{H}} \geq \delta$.*

*Beweis.* Offenbar gilt

$$\frac{1\ +\ \uparrow u \uparrow v}{2} \quad = \quad \begin{cases} 1 & \text{wenn } u = v \\ 0 & \text{sonst,} \end{cases} \qquad \text{für alle } u, v \in \mathbb{F}_2. \tag{3}$$

Die Mengen $\{\pm 1\}^n$ und $\mathbb{F}_2^n$ haben die selben Kardinalität vermöge der Bijektion $\uparrow$. Damit sind ihre jeweiligen Elemente mit der Wahrscheinlichkeit $p := |\{\pm 1\}^n|^{-1} =$

$|\mathbb{F}_2^n|^{-1}$ gleichverteilt. Wir ziehen die Aussage (3) nun hoch, denn die Werte $(\uparrow f)(\cdot)$ haben die Form $\uparrow\cdot$.

$$\begin{aligned}
& \frac{1+\langle \uparrow f, \uparrow g\rangle_{\mathcal{H}}}{2} \\
= \quad & \frac{1 \; + \; \sum_{x\in\{\pm 1\}^n} p(\uparrow f)(x)\;(\uparrow g)(x)}{2} && \text{(Definition 2.8)} \\
= \quad & \sum_{x\in\{\pm 1\}^n} p \frac{1 \; + \; (\uparrow f)(x)\;(\uparrow g)(x)}{2} && (\textstyle\sum_x p = 1) \\
= \quad & \sum_{x\in\{\pm 1\}^n} p \begin{cases} 1 & \text{wenn } (\uparrow f)(x) = (\uparrow f)(y) \\ 0 & \text{sonst} \end{cases} && \text{(Aussage (3))} \\
= \quad & \sum_{x\in\mathbb{F}_2^n} p \begin{cases} 1 & \text{wenn } x = y \\ 0 & \text{sonst} \end{cases} && (\uparrow \text{ ist bijektiv}) \\
= \quad & \mathop{\mathsf{Ex}}_{x\in\mathbb{F}_2^n} [f(x) = g(x)] && \text{(Gleichverteilung)}
\end{aligned}$$

Damit sind $f$ und $g$ $\frac{1+\delta}{2}$-nahe gdw. $\mathsf{Ex}_{x\in\mathbb{F}_2^n}[f(x) = g(x)] \geq \frac{1+\delta}{2}$ gdw. $\frac{1+\langle\uparrow f,\uparrow g\rangle_{\mathcal{H}}}{2} \geq \frac{1+\delta}{2}$ gdw. $\langle\uparrow f,\uparrow g\rangle_{\mathcal{H}} \geq \delta$. □

**Theorem 2.17.** *Seien $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$ und $\rho > 0.5$. Falls*

$$\mathop{\mathsf{Pr}}_{x,y\in\mathbb{F}_2^n}[f(x) + f(y) = f(x+y)] \quad \geq \quad \rho\,,$$

*so ist $f$ $\rho$-nahe an einer linearen Funktion.*

*Beweis.* Mittels Bemerkung 2.6 gilt

$$\mathop{\mathsf{Pr}}_{x,y\in\mathbb{F}_2^n}[f(x) + f(y) = f(x+y)] \quad = \quad \mathop{\mathsf{Pr}}_{x,y\in\{\pm 1\}^n}[\uparrow f(x\odot y) = \uparrow f(x)\uparrow f(y)]\,.$$

Setze $\varepsilon := \rho - 0.5$. Da $\varepsilon \geq 0$, liefert Lemma 2.15 für $\uparrow f$ und $\varepsilon$ eine Menge $\alpha \subseteq [n]$ mit $\langle\uparrow f, \chi_\alpha\rangle_{\mathcal{H}} \geq 2\varepsilon$. Mit Lemma 2.16 für $\delta := 2\varepsilon$ sind $f$ und $\uparrow^{-1}\chi_\alpha$ damit $\frac{1+2\varepsilon}{2}$-nahe. Also sind die beiden Funktionen nach Setzung von $\varepsilon$ auch $\rho$-nahe. Die Funktion $\uparrow^{-1}\chi_\alpha$ ist eine lineare Funktion in $\mathbb{F}_2^n \to \mathbb{F}_2$. □

**Korollar 2.18.** *Sei $1 > \rho > 0.5$. Dann gibt es ein $C \in \mathbb{N}$ und einen probabilistischen Algorithmus, der ein gegebenes $f\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ an höchstens $C$ Stellen auswertet und folgende Eigenschaften hat.*

- *Ist $f$ linear, so akzeptiert der Algorithmus stets.*
- *Ist $f$ zu keiner linearen Funktion $\rho$-nahe, so lehnt der Algorithmus mit Wahrscheinlichkeit mindestens $\rho$ ab.*

*Beweis.* Der Algorithmus wählt $N$ mal Werte $x, y \in \mathbb{F}_2^n$ zufällig und akzeptiert, falls stets $f(x) + f(y) = f(x+y)$ gilt. Lineare Funktionen werden also stets akzeptiert. Ist umgekehrt $f$ zu keiner linearen Funktion $\rho$-nahe, so ist nach Theorem 2.17 $\mathsf{Pr}_{x,y\in\mathbb{F}_2^n}[f(x)+f(y)=f(x+y)]<\rho$. Die Wahrscheinlichkeit, dass der Algorithmus $f$ ablehnt, ist also mindestens $1-\rho^N$. Für $N=\lceil\frac{\ln(1-\rho)}{\ln(\rho)}\rceil$ folgt die Behauptung. □

# 3 Von quadratischen Gleichungen zu linearen

**Definition 3.1.** Für $u\in\mathbb{F}_2^m$ und $v\in\mathbb{F}_2^n$ setzen wir $u\otimes v=uv^t\in\mathbb{F}_2^{m\times n}$.

**Bemerkung 3.2.** Ist $u=(u_1,\dots,u_m)$ und $v=(v_1,\dots,v_n)$, so ist $u\otimes v=(u_iv_j)_{i,j}$.

**Definition 3.3.** Für $A\in\mathbb{F}_2^{m\times n}$ sei $\ulcorner A\urcorner\in\mathbb{F}_2^{mn}$ derjenige $nm$-dimensionale Vektor der durch spaltenweises Hintereinanderschreiben der Einträge von $A$ entsteht.

**Bemerkung 3.4.** Es ist $\ulcorner\cdot\urcorner\colon\mathbb{F}_2^{m\times n}\to\mathbb{F}_2^{mn}$ ein linearer Isomorphismus.

**Lemma 3.5.** *$\langle u,v\rangle_{\mathbb{F}_2}\langle x,y\rangle_{\mathbb{F}_2}=\langle\ulcorner u\otimes x\urcorner,\ulcorner v\otimes y\urcorner\rangle_{\mathbb{F}_2}$ gilt für $u,v\in\mathbb{F}_2^m$ und $x,y\in\mathbb{F}_2^n$.*

*Beweis.* Sei $u=(u_i)_i$, $v=(v_i)_i$, $x=(x_j)_j$, $y=(y_j)_j$. Dann ist $\langle u,v\rangle_{\mathbb{F}_2}\langle x,y\rangle_{\mathbb{F}_2}=(\sum_i u_iv_i)(\sum_j x_jy_j)=\sum_{i,j}(u_iv_ix_jy_j)=\sum_{i,j}((u_ix_j)(v_iy_j))$. □

**Lemma 3.6.** *Seien $A,B\in\mathbb{F}_2^{m\times n}$ mit $A\neq B$. Für $r\in\mathbb{F}_2^m$, $r'\in\mathbb{F}_2^n$ zufällig gilt mit Wahrscheinlichkeit $1/4$, dass $\langle\ulcorner A\urcorner,\ulcorner r\otimes r'\urcorner\rangle_{\mathbb{F}_2}\neq\langle\ulcorner B\urcorner,\ulcorner r\otimes r'\urcorner\rangle_{\mathbb{F}_2}$.*

*Beweis.* Sei $r=(r_i)_i$ und $r'=(r'_j)_j$. Für $X=(x_{ij})_{ij}$ gilt $\langle\ulcorner X\urcorner,\ulcorner r\otimes r'\urcorner\rangle_{\mathbb{F}_2}=\sum_{ij}x_{ij}r_ir'_j=\sum_j(x_{ij}r_i)r'_j=\langle X^tr,r'\rangle_{\mathbb{F}_2}$. Da $A\neq B$, gilt nach Korollar 1.7 in der Hälfte der Fälle $A^tr\neq B^tr$. Nach Korollar 1.5 folgt die Behauptung. □

**Theorem 3.7.** *Es gibt einen probabilistischen Algorithmus für das folgende Problem, der korrekte Eingaben stets akzeptiert und falsche mit Wahrscheinlichkeit $1/4$ zurückweist.*

> *Gegeben $u\in\mathbb{F}_2^n$ und $v\in\mathbb{F}_2^{n^2}$. Entscheide ob $v=\ulcorner u\otimes u\urcorner$.*

*Dabei sind $u$ und $v$ als Abbildungen $f\colon\mathbb{F}_2^n\to\mathbb{F}_2$, $x\mapsto\langle u,x\rangle_{\mathbb{F}_2}$ und $g\colon\mathbb{F}_2^{n^2}\to\mathbb{F}_2$, $x\mapsto\langle v,x\rangle_{\mathbb{F}_2}$ gegeben und der Algorithmus wertet $f$ an höchstens zwei Stellen und $g$ an einer Stelle aus.*

*Beweis.* Der Algorithmus arbeitet wie folgt.

> Wähle $r,r'\in\mathbb{F}_2^n$ zufällig. Akzeptiere, falls $\langle u,r\rangle_{\mathbb{F}_2}\langle u,r'\rangle_{\mathbb{F}_2}=\langle v,\ulcorner r\otimes r'\urcorner\rangle_{\mathbb{F}_2}$.

Die Korrektheit ergibt sich aus Lemma 3.5. Die Rückweisewahrscheinlichkeit ergibt sich aus Lemma 3.6. □

**Korollar 3.8.** *Sei $\delta < 1/4$ fest. Es gibt einen probabilistischen Algorithmus, der das folgende Problem mit einer Irrtumswahrscheinlichkeit von höchstens $3/4 + 6\delta$ entscheidet.*

> *Gegeben eine Funktion $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$, die schon $(1-\delta)$-nahe an einer linearen Funktion $\tilde{f}\colon \mathbb{F}_2^n \to \mathbb{F}_2$ ist, sowie eine Funktion $g\colon \mathbb{F}_2^{n^2} \to \mathbb{F}_2$, die schon $(1-\delta)$-nahe an einer linearen Funktion $\tilde{g}\colon \mathbb{F}_2^{n^2} \to \mathbb{F}_2$ ist. Entscheide, ob $v = \ulcorner u \otimes u \urcorner$ gilt, wobei $u^t$ die darstellende Matrix von $\tilde{f}$ und $v^t$ die darstellende Matrix von $\tilde{g}$ ist.*

*Darüberhinaus akzeptiert der Algorithmus immer, falls $\delta = 0$ und $v = \ulcorner u \otimes u \urcorner$, und wertet $f$ und $g$ nur an konstant vielen Stellen aus.*

*Beweis.* Theorem 3.7, wobei die drei Stellen von $\tilde{f}$ bzw. $\tilde{g}$ mit Theorem 1.12 jeweils mit einer Irrtumswahrscheinlichkeit von höchstens $2\delta$ bestimmt wird. $\square$

# 4 Die NP-Vollständigkeit quadratischer Gleichungssysteme

Für den Beweis des **PCP**-Theorems werden wir zeigen, dass ein **NP**-vollständiges Problem in der jeweiligen **PCP**-Klasse liegt. Für die einfache Variante des **PCP**-Theorems interessiert uns das folgende Problem.

**Definition 4.1** (QUADEQ)**.** Gegeben ist eine Menge quadratischer Gleichungen über $u_1, \ldots, u_n \in \mathbb{F}_2$. Entscheide, ob es eine Belegung der Variablen $u_1, \ldots, u_n$ gibt, sodass alle Gleichungen erfüllt sind.

**Beispiel 4.2.** Eine Instanz für QUADEQ mit vier Variablen wäre etwa

$$\begin{aligned} u_1u_2 + u_2u_3 &= 0 \\ u_1 + u_1u_4 &= 1 \\ u_3 + u_2u_4 &= 0 \end{aligned}$$

Man sieht leicht, dass $u_1 = 1, u_2 = 0, u_3 = 0, u_4 = 0$ eine mögliche Lösung ist.

Zunächst wollen wir zeigen, dass QUADEQ **NP**-vollständig ist. Es ist offenbar QUADEQ $\in$ **NP**, da quadratische Terme sich in Polynomialzeit auswerten lassen und damit eine mögliche Lösung in Polynomialzeit verifizierbar ist.

**Proposition 4.3.** QUADEQ *is* **NP***-schwierig.*

*Beweis.* Wir geben eine Reduktion auf das Erfüllbarkeitsproblem für boolesche Schaltkreise mit Fan-In 2. Für einen gegebenen Schaltkreis definieren wir für jeden Ausgang eines Gatters und jeden Eingang des Schaltkreises $x$ eine Variable $v_x$ in $\mathbb{F}_2$. Dann kodieren wir die Gatter, sodass $\neg x$ auf $(1 - v_x)$, $x \vee y = 1$ auf $(1 - v_x)(1 - v_y) = 0$ und $x \wedge y = 1$ auf $v_x \cdot v_y = 1$ abgebildet werden. Offenbar lässt sich damit ein Schaltkreis vollständig in ein quadratisches Gleichungssystem umkodieren, sodass eine Lösung für ein quadratisches Gleichungssystem genau dann existiert, wenn der Schaltkreis erfüllbar ist. $\square$

**Korollar 4.4.** QUADEQ *eingeschränkt auf rein quadratische Gleichungen ist ebenfalls* **NP***-schwierig.*

*Beweis.* Folgt unmittelbar aus Proposition 4.3, da wir lineare Terme $z$ in $\mathbb{F}_2$ auch stetz als $z^2$ schreiben können. □

Im Folgenden wollen wir Lösungskandidaten für QUADEQ mit $m$ Gleichungen als Vektoren $u = (u_1, \ldots, u_n) \in \mathbb{F}_2^n$ darstellen. Dann ist es möglich, die Lösung mit einfachen Operationen aus der linearen Algebra zu verifizieren: Das Tensorprodukt $u \otimes u$ enthält genau die quadratischen Terme in $u_1, \ldots, u_n$, also reicht es nun, eine Koeffizientenmatrix $A \in \mathbb{F}_2^{n^2 \times m}$ mit $\ulcorner u \otimes u \urcorner$ zu multiplizieren und mit einem Ergebnisvektor $b \in \mathbb{F}_2^{n^2}$ zu vergleichen. Es sei angemerkt, dass diese Darstellung offenbar in Polynomialzeit berechenbar ist.

# 5 Das „kleine“ PCP-Theorem

In diesem Abschnitt wollen wir eine abgeschwächte Version des PCP-Theorems zeigen.

**Definition 5.1.** Mit $\mathfrak{n}$ bezeichnen wir die Identität auf den natürlichen Zahlen. Es gilt also $\mathfrak{n}(n) = n$.

**Definition 5.2.** Für $f, g \colon \mathbb{N} \to \mathbb{N}$ bezeichnen wir mit $f+g$, $fg$ und $f^g$ die punktweise Addition, Mulltiplikation und Exponentiation. Es gilt also $(f+g)(n) = f(n) + g(n)$, $(fg)(n) = f(n) \cdot g(n)$, $(f^g)(n) = f(n)^{g(n)}$. Ferner identifizieren wir Konstanten mit konstanten Funktionen.

**Definition 5.3.** Für $f, g \colon \mathbb{N} \to \mathbb{N}$ schreiben wir die Komposition auch als $f(g)$. Mit anderen Worten, $(f(g))(n) = f(g(n))$.

**Beispiel 5.4.** $f(\mathfrak{n}) = f$

**Definition 5.5.** Für $f \colon \mathbb{N} \to \mathbb{N}$ definieren wir $\mathcal{O}(f) = \{g \colon \mathbb{N} \to \mathbb{N} \mid \exists C \in \mathbb{N}. \exists N \in \mathbb{N} \forall n \geq N. g(n) \leq C f(n)\}$.

**Definition 5.6.** Wir verwenden den binären Logarithmus als Funktion auf den natürlichen Zahlen. Genauer definieren wir durch $\log(n) = \min\{k \mid 2^k \geq n\}$ eine Funktion $\log \colon \mathbb{N} \to \mathbb{N}$.

**Definition 5.7** ($(r,q)$-beschränkter Verifizierer)**.** Seien $r, q \colon \mathbb{N} \to \mathbb{N}$. Ein $(r,q)$-*beschränkter Verifizierer* für eine Sprache $L \subseteq \Sigma^*$ ist ein Algorithmus $A$, der für drei Eingaben $x, y, z$ mit $n = |x|$, folgende Eigenschaften hat.

- $A$ hat polynomielle Laufzeit in $n$.
- $A$ liest höchstens $q(n)$ Bits von $y$.
- $A$ liest höchstens die ersten $r(n)$ Bits von $z$.
- Falls $x \in L$, dann existiert ein $y$, sodass $\mathsf{Pr}_z[A(x,y,z) \text{ akzeptiert}] = 1$.

- Falls $x \notin L$, dann gilt für alle $y$, dass $\mathsf{Pr}_z[A(x,y,z)$ akzeptiert$] \leq \frac{1}{2}$.

**Bemerkung 5.8.** Das $y$ in Definition 5.7 heißt auch *Beweis* oder *Zeuge* und $z$ werden auch die *Zufallsbits* genannt.

**Bemerkung 5.9.** Offenbar gilt, dass ein $(r,q)$-beschränkten Verifizierer nur die Beweise der Länge $\mathcal{O}(2^{r(\mathfrak{n})})$ vollständig verwenden kann.

**Definition 5.10** (($R,Q$)-beschränkter Verifizierer)**.** Sind $R, Q \subseteq \{f : \mathbb{N} \to \mathbb{N}\}$, so heißt ein Algorithmus $A$ ein $(R,Q)$*-beschränkter Verifizierer*, wenn es $r \in R$ und $q \in Q$ gibt, so dass $A$ ein $(r,q)$-beschränkter Verifizierer ist.

**Definition 5.11** (**PCP**)**.** Die Komplexitätsklasse $\mathbf{PCP}(r,q)$ sei die Menge aller Probleme, die einen $(\mathcal{O}(r(\mathfrak{n})), \mathcal{O}(q(\mathfrak{n})))$-beschränkten Verifizierer haben.

**Bemerkung 5.12.** Man sieht leicht, dass $\mathbf{PCP}(r,q)$ gegenüber polynomiellen Reduktionen abgeschlossen ist; dies ist eine triviale Folgerung aus der Tatsache, dass der Verifizierer in der Definition von $\mathbf{PCP}(\cdot,\cdot)$ polynomielle Laufzeit hat.

**Definition 5.13.** Für $n \in \mathbb{N}$ sei $v_{\mathbb{F}_2^n} : [2^n] \to \mathbb{F}_2^n$ die Aufzählung der Elemente von $\mathbb{F}_2^n$ in lexikographischer Reihenfolge. Vermöge $v_{\mathbb{F}_2^n}$ werden $\mathbb{F}_2^n$-indizierte Familien von $\mathbb{F}_2$ zu Bitvektoren; mit anderen Worten, wir identifizieren $(a_v)_{v \in \mathbb{F}_2^n}$ mit dem Bitvektor $(a_{v_{\mathbb{F}_2^n}(i)})_{i \in [2^n]}$.

**Definition 5.14.** Die *Walsh-Hadamard-Kodierung* eines Vektors $u \in \mathbb{F}_2^n$ ist der Bitvektor

$$\mathrm{WH}(u) = (\langle u, v \rangle_{\mathbb{F}_2})_{v \in \mathbb{F}_2^n}$$

der Länge $2^n$. Ferner setzen wir für $A \in \mathbb{F}_2^{m \times n}$ noch $\mathrm{WH}(A) = \mathrm{WH}(\ulcorner A \urcorner)$.

**Bemerkung 5.15.** Die *Walsh-Hadamard-Kodierung* eines Objekts ist exponentiell länger als das Objekt selbst.

**Bemerkung 5.16.** Die Walsh-Hadamard-Kodierung ist die Wertetabelle der Funktion $v \mapsto \langle u, v \rangle_{\mathbb{F}_2}$ vom Typ $\mathbb{F}_2^n \to \mathbb{F}_2$ bzw. der Funktion $v \mapsto \langle \ulcorner A \urcorner, v \rangle_{\mathbb{F}_2}$ vom Typ $\mathbb{F}_2^{mn} \to \mathbb{F}_2$.

**Theorem 5.17** (kleiner **PCP**-Satz)**.** $\mathbf{NP} \subseteq \mathbf{PCP}(\mathfrak{n}^2, 1)$.

*Beweis.* Nach Korollar 4.4 ist QUADEQ **NP**-schwierig und kann als Gleichungssystem $A \ulcorner u \otimes u \urcorner = b$ mit Unbestimmter $u$ geschrieben werden. Für eine Lösung $u$ des Gleichungssystems soll der Zeuge $y$ die Konkakentation der Walsh-Hadamard-Kodierungen von $u$ und von $u \otimes u$ sein. Wir beschreiben nun einen $(\mathcal{O}(\mathfrak{n}^2), \mathcal{O}(1))$-beschränkten Verifizierer für diesen Zeugen.

- *Formatierung.* Der Zeuge, auf den der Verifizierer als Orakel zugreift, wird als Konkatentation eines Strings $\alpha$ der Länge $2^n$ und eines Strings $\beta$ der Länge $2^{n^2}$ aufgefasst.

- *Linearitätstests.* Mit Hilfe Korollar 2.18 wird mit konstant vielen gelesenen Bits des Zeugen überprüft, ob $\alpha$ schon $(1 - 1/2^8)$-nahe an einer linearen Funktion $\mathrm{WH}(u)$ ist und $\beta$ schon $(1-1/2^8)$-nahe an einer linearen Funktion $\mathrm{WH}(v)$ ist, und zwar jeweils so, dass der Fall, dass dem nicht so ist, mit Wahrscheinlichkeit mindestens $1 - 1/2^8$ erkannt wird.

- *Tensorprodukt-Verifikation.* Durch neun unabhängige Wiederholungen des Verfahrens in Korollar 3.8 wird überprüft, ob $v = \ulcorner u \otimes u \urcorner$. Ist das nicht der Fall, so wird dies mit Wahrscheinlichkeit mindestens $1-(3/4+6/2^8))^9 > 0.9$ erkannt.

- *Erfüllbarkeitstest.* Durch vier unabhängige Wiederholungen des Verfahrens aus Korollar 1.14 wird verifiziert, ob $v$ eine Lösung von $Av = b$ ist. Ist dies nicht der Fall, so wird dies mit Wahrscheinlichkeit mindestens $1 - (1/2 + 2/2^8)^4 > 0.9$ erkannt.

Falls $u$ eine Lösung des Gleichungssystems ist, wird offenbar der Bitstring $\mathrm{WH}(u)\,\mathrm{WH}(\ulcorner u \otimes u \urcorner)$ stets als Zeuge akzeptiert. Hat umgekehrt das Gleichungssystem keine Lösung, so muss für jeden String $y = \alpha\beta$ mindestens eine der folgenden Bedingungen verletzt sein.

- $\alpha$ und $\beta$ kodieren zwei Vektoren $u$ und $v$
- $v = \ulcorner u \otimes u \urcorner$
- $Av = b$

Wie oben argumentiert, bleibt dies mit einer Wahrscheinlichkeit von höchstens $\frac{1}{2^8} + \frac{1}{2^8} + \frac{1}{10} + \frac{1}{10} < \frac{1}{2}$ von dem Verifizierer unentdeckt.

Wir beobachten, dass wir im Laufe der Verifikation nur konstant viele Bits des Beweises gelesen haben. Weiterhin werden, für eine Konstante $C$, höchstens $C(\log 2^n + \log 2^{n^2}) \leq 2Cn^2$ Zufallsbits benötigt. $\square$

## Danksagungen

Die Autoren danken den Organisatoren der CdE Winterakademie 2012/2013, auf der dieses Skript entstanden ist.

## Literatur

[AB09] Sanjeev Arora and Boaz Barak. *Computational Complexity: A Modern Approach.* Cambridge University Press, 2009.