7.4 Probabilistische Schaltnetze

Nun zur Formalisierung probabilistischer Algorithmen. Das sieht im Ansatz etwa so aus: Gegeben sei eine Funktion

$$f\colon A \longrightarrow \mathbb{F}_2^s$$

auf einer Menge A. Ein probabilistischer Algorithmus über dem Wahrscheinlichkeitsraum Ω soll eine Funktion

$$C\colon A \times \Omega \longrightarrow \mathbb{F}_2^s$$

definieren; er dient zur (probabilistischen) Berechnung von $f(x)$ bzw. f, wenn die Wahrscheinlickeit

$$P(\{\omega \mid C(x,\omega) = f(x)\}) \quad (\text{„lokal“}) \text{ bzw.}$$

$$P(\{(x,\omega) \mid C(x,\omega) = f(x)\}) \quad (\text{„global“})$$

genügend groß ist (signifikant $> \frac{1}{2^s}$). Im lokalen Fall wird bei festem x über Ω gemittelt, im globalen Fall auch über A. Dabei sollen im allgemeinen die Wahrscheinlichkeitsräume Ω und $A \times \Omega$ endlich und mit der Gleichverteilung versehen sein.

Um probabilistische Algorithmen beschreiben zu können, muss man Schaltnetze mit *drei* verschiedenen Typen von Eingängen betrachten:

- r **deterministische Eingänge**, die mit einer Eingabe $x \in \mathbb{F}_2^r$ – oder aus einer Teilmenge $A \subseteq \mathbb{F}_2^r$ – belegt werden,
- einige konstante Eingänge
- und k **probabilistische Eingänge**, die mit einem Element des LAPLACEschen Wahrscheinlichkeitsraums $\Omega = \mathbb{F}_2^k$ belegt werden (k „Münzenwürfe“), oder mit einem Element eines Teilraums $\Omega \subseteq \mathbb{F}_2^k$. – Natürlich sind auch andere Wahrscheinlichkeitsverteilungen als die Gleichverteilung auf Ω möglich und manchmal sinnvoll.

Über die Ausgabe $y \in \mathbb{F}_2^s$ werden dann Wahrscheinlichkeitsaussagen der oben beschriebenen Art gemacht.

Beispiele

1. Die Suche nach einem Nicht-Quadratrest für einen Primzahlmodul p: Dabei sei p eine n-Bitzahl. Dazu wurde $b \in [1 \ldots p-1]$ zufällig gewählt und $(\frac{b}{p})$ (das LEGENDRE-Symbol, das für Quadratreste 1, für Nichtquadratreste -1 ist) berechnet. Die Wahrscheinlichkeit für einen Erfolg ist dabei $\frac{1}{2}$, der Aufwand $\mathrm{O}(n^2)$ (siehe Anhang A.9). Betrachten wir allgemeiner die Frage, ob in einem unabhängig gewählten h-Tupel

$(b_1, \ldots, b_h) \in \Omega = [1 \ldots p-1]^h$ ein Nicht-Quadratrest vorkommt. Es gibt (für das fest gewählte p) ein Schaltnetz ohne deterministische Eingänge (aber mit konstanten Eingängen zur Einspeisung von p),

$$C : \mathbb{F}_2^{hn} \longrightarrow \mathbb{F}_2^n,$$

$$C(\omega) = \begin{cases} b_i, & \text{das erste } b_i\text{, das Nicht-Quadratrest ist,} \\ 0, & \text{falls kein Nicht-Quadratrest gefunden wurde,} \end{cases}$$

das die Größe $\mathrm{O}(hn^2)$ hat und mit der Wahrscheinlichkeit $1 - \frac{1}{2^h}$ einen Nichtquadratrest ausgibt.

2. Der strenge Pseudoprimzahltest: Hier entstammen die Eingaben der Menge A der ungeraden Zahlen in $[3 \ldots 2^n - 1]$. Berechnet werden soll die Funktion

$$f : A \longrightarrow \mathbb{F}_2, \quad f(m) = \begin{cases} 1, & \text{falls } m \text{ zusammengesetzt,} \\ 0, & \text{falls } m \text{ prim.} \end{cases}$$

Die zufälligen Eingänge werden durch die Wahl eines Basiselements $a \in \Omega = [2 \ldots 2^n - 1]$ besetzt. Der strenge Pseudoprimzahltest liefert ein Schaltnetz

$$C : \mathbb{F}_2^n \times \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$$

der Größe $\mathrm{O}(n^3)$ mit dem Ergebnis 1, wenn m durchfällt (dann ist m sicher zusammengesetzt), oder 0, wenn m besteht (dann ist m möglicherweise prim).

Die Eigenschaft eines (probabilistischen) Schaltnetzes C mit r deterministischen Eingängen, eine Entscheidung mit einer Wahrscheinlichkeit richtig zu treffen, die signifikant vom zufälligen Erraten des Wertes $f(x) \in \mathbb{F}_2^s$ abweicht, wird so formalisiert: Ein Schaltnetz

$$C : \mathbb{F}_2^r \times \Omega \longrightarrow \mathbb{F}_2^s$$

hat einen **ε-Vorteil** mit $\varepsilon \geq 0$ bei der Berechnung von $f(x)$ bzw. f, wenn

$$P(\{\omega \in \Omega \mid C(x, \omega) = f(x)\}) \geq \frac{1}{2^s} + \varepsilon \quad \text{(„lokal“) bzw.}$$

$$P(\{(x, \omega) \in A \times \Omega \mid C(x, \omega) = f(x)\}) \geq \frac{1}{2^s} + \varepsilon \quad \text{(„global“).}$$

Die Wahrscheinlichkeit bezüglich ω für das richtige Ergebnis wird also im globalen Fall noch über $x \in A$ gemittelt. Der Vorteil 0, also die Wahrscheinlichkeit $\frac{1}{2^s}$, entspricht dem puren Raten des Ergebnisses.

C hat eine **Irrtumswahrscheinlichkeit** ε bei der Berechnung von $f(x)$ bzw. f, wenn

$$P(\{\omega \in \Omega \mid C(x, \omega) = f(x)\}) \geq 1 - \varepsilon \quad \text{bzw.}$$

$$P(\{(x,\omega) \in A \times \Omega \mid C(x,\omega) = f(x)\}) \geq 1 - \varepsilon.$$

Beispiele

1. Bei der Suche nach einem Nicht-Quadratrest mod p ist

$$P(\{\omega \in \Omega \mid C(\omega) \text{ ist Nichtquadratrest}\}) = 1 - \frac{1}{2^h}.$$

Das Schaltnetz hat also einen $(\frac{1}{2} - \frac{1}{2^h})$-Vorteil und eine Irrtumswahrscheinlichkeit von $\frac{1}{2^h}$.

2. Beim strengen Pseudoprimzahltest ist für festes m

$$P(\{\omega \in \Omega \mid C(m,\omega) = f(m)\}) \begin{cases} \geq \frac{3}{4}, & \text{wenn } m \text{ zusammengestzt}, \\ = 1, & \text{wenn } m \text{ prim.} \end{cases}$$

Das ergibt über alle m gemittelt

$$P(\{(m,\omega) \in A \times \Omega \mid C(m,\omega) = f(m\}) \geq \frac{3}{4},$$

also einen $\frac{1}{4}$-Vorteil und eine Irrtumswahrscheinlichkeit $\frac{1}{4}$. (Da es wesentlich mehr zusammengesetzte Zahlen als Primzahlen gibt, wird bei der Mittelung über m der Wert $\frac{1}{4}$ nicht wesentlich erhöht.)