4.2 BBS-Generator und Quadratrest-Eigenschaft

Für einen Startwert $x \in \mathbb{M}_m$ sei $(b_1(x), \ldots, b_r(x))$ die vom BBS-Generator erzeugte Bitfolge. Ein probabilistisches Schaltnetz

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

hat einen ε-Vorteil bei der **BBS-Extrapolation** für m, wenn

$$P(\{(x,\omega) \in Q_m \times \Omega \mid C(b_1(x), \ldots, b_r(x), \omega) = \mathrm{lsb}(x)\}) \geq \frac{1}{2} + \varepsilon.$$

Das bedeutet: Der durch C gegebene Algorithmus sagt jeweils das Vorgängerbit zu einer Teilfolge mit ε-Vorteil „voraus".

Im folgenden Satz sei τ_n der Aufwand für die Operation $xy \bmod m$, wo m eine n-Bit-Zahl und $0 \leq x, y < m$ ist. Bekanntlich ist $\tau_n = \mathrm{O}(n^2)$.

Hilfssatz 1 *Sei m eine* Blum*-Zahl $< 2^n$. Das probabilistische Schaltnetz $C\colon \mathbb{F}_2^r \times \Omega \longrightarrow \mathbb{F}_2$ habe einen ε-Vorteil bei der BBS-Extrapolation für m. Dann gibt es ein probabilistisches Schaltnetz $C'\colon \mathbb{F}_2^n \times \Omega \longrightarrow \mathbb{F}_2$ der Größe $\#C' \leq \#C + r\tau_n + 4$, das einen ε-Vorteil bei der Bestimmung der Quadratrest-Eigenschaft auf $\mathbb{M}_m^+$ hat.*

Beweis. Zunächst wird mit Aufwand $r\tau_n$ die BBS-Folge $(b_1, \ldots, b_r)$ zum Startwert $x \in \mathbb{M}_m^+$ berechnet. Dann sagt C das Bit $\mathrm{lsb}(\sqrt{x}^2 \bmod m)$ mit Vorteil ε voraus. Setzt man also

$$C'(x,\omega) := \begin{cases} 1, & \text{wenn } C(b_1, \ldots, b_r, \omega) = \mathrm{lsb}(x), \\ 0 & \text{sonst,} \end{cases}$$

so hat man nach dem Abschnitt über Blum-Zahlen in Kapitel III die Quadratrest-Eigenschaft von x mit ε-Vorteil bestimmt. Der zusätzliche Aufwand für den Bitvergleich sind maximal 4 weitere Knoten im Schaltnetz. $\diamond$

Sei nun $C : \mathbb{F}_2^n \times \Omega \longrightarrow \mathbb{F}_2$ ein beliebiges probabilistisches Schaltnetz. Dann ist für $r \geq 1$ das **r-fache Schaltnetz** definiert durch

$$C^{(r)}\colon \mathbb{F}_2^n \times \Omega^r \longrightarrow \mathbb{F}_2,$$

$$C^{(r)}(x, \omega_1, \ldots, \omega_r) := \begin{cases} 1, & \text{wenn } \#\{i \mid C(x, \omega_i) = 1\} \geq \frac{r}{2}, \\ 0 & \text{sonst.} \end{cases}$$

Dieses Schaltnetz repräsentiert also die „Mehrheitsentscheidung"; es wird realisiert durch r-fache Parallelschaltung von C, eine Ganzzahl-Addition von r Bits und einen Größenvergleich von $\lceil {}^2\log r \rceil$-Bit-Zahlen, hat also eine Größe

$$\#C^{(r)} \leq r \cdot \#C + 2r^2.$$

Hilfssatz 2 (Verdichtung eines Vorteils) *Sei $A \subseteq \mathbb{F}_2^n$, und C berechne die* Boole*sche Funktion f auf A mit ε-Vorteil. Sei $r = 2s + 1$ ungerade.*

Dann berechnet $C^{(r)}$ die Funktion f mit einer Irrtumswahrscheinlichkeit

$$\leq \frac{(1-4\varepsilon^2)^s}{2}.$$

Ist $\delta > 0$ beliebig, so gibt es ein

$$r \leq 3 + \frac{1}{2\delta\varepsilon^2},$$

so dass $C^{(r)}$ die Funktion f mit einer Irrtumswahrscheinlichkeit $\leq \delta$ berechnet.

Beweis. Die Wahrscheinlichkeit, bei einer Anwendung von C die korrekte Antwort zu erhalten, ist

$$p := P(\{(x,\omega) \in A \times \Omega \mid C(x,\omega) = f(x)\}) \geq \frac{1}{2} + \varepsilon.$$

Da bei Vergrößerung von ε die Behauptung verschärft wird, kann man o. B. d. A. $p = \frac{1}{2} + \varepsilon$ annehmen. Der komplementäre Wert $q := 1 - p = \frac{1}{2} - \varepsilon$ ist die Wahrscheinlichkeit dafür, bei einer Anwendung von C die falsche Antwort zu erhalten. Also ist die Wahrscheinlichkeit dafür, bei r unabhängigen Anwendungen von C genau k richtige Antworten zu erhalten, $\binom{r}{k}p^k q^{r-k}$. Die gesuchte Irrtumswahrscheinlichkeit ist also

$$P(\{(x,\omega_1,\ldots,\omega_r) \in A \times \Omega^r \mid C^{(r)}(x,\omega_1,\ldots,\omega_r) = f(x)\})$$

$$\begin{aligned}
&= \sum_{k=0}^{s} \binom{r}{k} (\frac{1}{2}+\varepsilon)^k (\frac{1}{2}-\varepsilon)^{r-k} \\
&= (\frac{1}{2}+\varepsilon)^s (\frac{1}{2}-\varepsilon)^{s+1} \cdot \sum_{k=0}^{s} \binom{r}{k} (\frac{1}{2}+\varepsilon)^{k-s} (\frac{1}{2}-\varepsilon)^{s-k} \\
&= (\frac{1}{4}-\varepsilon^2)^s \cdot (\frac{1}{2}-\varepsilon) \cdot \underbrace{\sum_{k=0}^{s} \binom{r}{k} \underbrace{\left(\frac{\frac{1}{2}-\varepsilon}{\frac{1}{2}+\varepsilon}\right)^{s-k}}_{\leq 1}}_{\leq 2^{r-1} = 4^s} \\
&\leq (1-4\varepsilon^2)^s \cdot \frac{1}{2},
\end{aligned}$$

und die erste Aussage somit bewiesen.

Um eine Irrtumswahrscheinlichkeit $\leq \delta$ zu erreichen, ist hinreichend:

$$\begin{aligned}
(1-4\varepsilon^2)^s &\leq 2\delta, \\
s \cdot \ln(1-4\varepsilon^2) &\leq \ln 2 + \ln \delta, \\
s &\geq \frac{\ln 2 + \ln \delta}{\ln(1-4\varepsilon^2)}.
\end{aligned}$$

Wählt man also

$$s := \left\lceil \frac{\ln 2 + \ln \delta}{\ln(1-4\varepsilon^2)} \right\rceil,$$

so ist die Irrtumswahrscheinlichkeit von $C^{(r)}$ höchstens δ, ferner

$$\begin{aligned}
s &\leq 1 + \frac{\ln 2 + \ln \delta}{\ln(1-4\varepsilon^2)} = 1 + \frac{\ln \frac{1}{\delta} - \ln 2}{\ln \frac{1}{1-4\varepsilon^2}} \\
&\leq 1 + \frac{\frac{1}{\delta} - 1 - \ln 2}{4\varepsilon^2} \leq 1 + \frac{1}{4\delta\varepsilon^2}
\end{aligned}$$

und somit die zweite Aussage bewiesen. $\diamond$

$C^{(r)}$ hat dann übrigens die Größe

$$\#C^{(r)} \leq \left[3 + \frac{1}{2\delta\varepsilon^2}\right] \cdot \#C + 2 \cdot \left[3 + \frac{1}{2\delta\varepsilon^2}\right]^2.$$

Die Zusammenfassung der beiden Hilfssätze ergibt:

Satz 1 *Sei m eine* BLUM*-Zahl $< 2^n$. Das probabilistische Schaltnetz $C : \mathbb{F}_2^r \times \Omega \longrightarrow \mathbb{F}_2$ habe einen ε-Vorteil bei der BBS-Extrapolation für m. Dann gibt es für jedes $\delta > 0$ ein probabilistisches Schaltnetz $C' : \mathbb{F}_2^n \times \Omega' \longrightarrow \mathbb{F}_2$, das die Quadratrest-Eigenschaft auf $\mathbb{M}_m^+$ mit Irrtumswahrscheinlichkeit $\leq \delta$ bestimmt, mit*

$$\#C' \leq \left[3 + \frac{1}{2\delta\varepsilon^2}\right] \cdot [\#C + r\tau_n + 4] + 2 \cdot \left[3 + \frac{1}{2\delta\varepsilon^2}\right]^2.$$

Aus einer effizienten BBS-Extrapolation ließe sich also ein effizienter Entscheidungsalgorithmus für die Quadratrest-Eigenschaft konstruieren. Diese Aussage wird im folgenden Abschnitt präzisiert.