7.7 Harte Probleme

Etwas kniffliger ist die exakte Definition eines harten Problems. Es ist klar, dass die Forderung, das Problem solle für fast alle Eingaben nicht effizient lösbar sein, durch die schlichte Negierung der Eigenschaft „effizient“ nicht erfüllt wird. Näher kommt dem schon die Forderung, der Vorteil des Algorithmus solle mit wachsendem n gegen 0 gehen; aber auch das ist keine geeignete Definition, da der Vorteil nur eine untere Schranke ist. Der beste Ansatz ist, zu verlangen, dass es keinen Vorteil gibt, der „zu langsam“ gegen 0 geht. „Zu langsam“ soll bedeuten

$$\frac{1}{\eta(n)} \quad \text{mit einem beliebigen Polynom } \eta \in \mathbb{N}[X],$$

und es soll „fast keine“ Eingaben geben, die Ausnahmen sind – die Ausnahmemenge soll „dünn“ sein. Diese Vorstellung wird jetzt in eine exakte Definition umgesetzt.

Für $x \in L_{r(n)}$ betrachten wir die Wahrscheinlichkeit

$$p_x := P(\{\omega \in \Omega_{k(n)} \mid C_n(x,\omega) = f(x)\}),$$

ferner die Menge der Eingaben x, für die C_n einen ε-Vorteil hat:

$$L_{r(n)}(\varepsilon) := \{x \in L_{r(n)} \mid p_x \geq \frac{1}{2^{s(n)}} + \varepsilon\}.$$

Für ein Polynom $\eta \in \mathbb{N}[X]$ ist dann $L_{r(n)}(\frac{1}{\eta(n)})$ die Menge von Eingaben x, für die $f(x)$ von C mit Vorteil $\frac{1}{\eta(n)}$ berechnet wird. Die Ausnahmemenge für η ist damit

$$L^{[f,C,\eta]} := \bigcup_{n\in\mathbb{N}} L_{r(n)}(\frac{1}{\eta(n)}).$$

Wir bezeichnen sie als „**Vorteilsmenge für f, C und η**“. Ihre Bestandteile sollen mit wachsendem n immer unbedeutender werden, und das wird so definiert:

Definition 2. Eine Teilmenge $A \subseteq L$ heisst **dünn**, wenn für alle nichtkonstanten Polynome $\varphi \in \mathbb{N}[X]$ mit $A_n = A \cap L_n$ gilt

$$\#A_n \leq \frac{\#L_n}{\varphi(n)} \quad (\text{also } \varphi(n) \cdot \#A_n \leq \#L_n) \quad \text{für fast alle } n \in \mathbb{N}.$$

Bemerkungen und Beispiele

1. Ist $\#A_n = c$ konstant und $L_n = \mathbb{F}_2^n$, so ist A dünn in L, denn die verlangte Ungleichung ist $c \cdot \varphi(n) \leq 2^n$.

2. Wächst $\#A_n$ höchstens wie ein Polynom, aber $\#L_n$ schneller als jedes Polynom, so ist A dünn in L.

3. Ist $\#A_n = c \cdot \#L_n$ ein fester Anteil, so ist A nicht dünn in L.

4. Ist $L = \mathbb{N}$ und A die Menge der Primzahlen (beides binär codiert), so ist nach dem Primzahlsatz

$$\#A_n \approx \frac{2^{n-1}}{n \cdot \ln(2)} = \frac{\#L_n}{n \cdot \ln(2)}.$$

   Die Menge der Primzahlen ist also nicht dünn in $\mathbb{N}$.

5. Es ist kein effizienter Algorithmus bekannt, der mehr als eine dünne Teilmenge der Menge M aller Produkte von zwei Primzahlen, die sich in der Länge um höchstens ein Bit unterscheiden, faktorisieren kann.

Definition 3. Sei f wie in (2). Dann heißt f **hart**, wenn für jede PPS wie in (1) und für jedes Polynom $\eta \in \mathbb{N}[X]$ die Vorteilsmenge $L^{[f,C,\eta]}$ dünne Teilmenge von L ist.

Beispiele

1. Nach Bemerkung 5 ist die Primzerlegung vermutlich hart.

2. **Quadratrest-Vermutung:** Sei B die Menge von Produkten zweier Primzahlen $\equiv 3 \pmod 4$ (BLUM-Zahlen),

$$L = \{(m, a) \mid m \in B, 1 \leq a \leq m-1\},$$

$$f : L \longrightarrow \mathbb{F}_2$$

   die Funktion

$$f(m,a) = \begin{cases} 1, & \text{wenn } a \text{ Quadratrest mod } m, \\ 0 & \text{sonst.} \end{cases}$$

   Dann ist f hart.