7.5 Polynomiale Schaltnetzfamilien

Ein Schaltnetz hat eine festgelegte Zahl von Eingängen, kann also (im Gegensatz zu einer TURING-Maschine) nur Eingaben bestimmter Länge verarbeiten. Bei Effizienzuntersuchungen will man aber meist das Wachstum des Aufwandes bei immer weiterer Vergrößerung der Eingabelänge abschätzen. Dazu unterstellt man eine ganze Familie $(C_n)_{n\in\mathbb{N}}$ von Schaltnetzen mit wachsender Zahl deterministischer Eingänge, deren Größe $\#C_n$ kontrolliert wächst; damit kann man dann das Wachstum des Aufwandes als Funktion der Länge der Eingabe ausdrücken. Genauer wird definiert: Eine **polynomiale (probabilistische) Schaltnetzfamilie (PPS)** ist eine Familie $C = (C_n)_{n\in\mathbb{N}}$,

$$C_n \colon \mathbb{F}_2^{r(n)} \times \mathbb{F}_2^{k(n)} \longrightarrow \mathbb{F}_2^{s(n)}, \tag{1}$$

von (probabilistischen) Schaltnetzen mit $r(n)$ deterministischen und $k(n)$ probabilistischen Eingängen, so dass es ein Polynom $\alpha \in \mathbb{N}[X]$ (nichtnegative ganzzahlige Koeffizienten) gibt mit $\#C_n \leq \alpha(n)$ für alle $n \in \mathbb{N}$. Insbesondere ist die Zahl der Eingänge aller Arten und die Zahl $s(n)$ der Ausgänge polynomial beschränkt.

Bemerkung. Das bedeutet nicht notwendig, dass die Funktionen r, k, s selbst Polynome sind.

Sind alle $k(n) = 0$, so spricht man selbstverständlich von einer deterministischen polynomialen Schaltnetzfamilie.

Durch dieses Berechnungsmodell (im deterministischen Fall) könnten mehr Probleme berechenbar sein als durch das gebräuchliche Modell der TURING-Maschinen (und sind es tatsächlich), da für jede Eingabelänge ein anderer Algorithmus gewählt werden kann. Man spricht daher auch von einem „nicht-gleichmäßigen Berechnungsmodell“. Das erscheint auf den ersten Blick vielleicht als Nachteil dieses Berechnungsmodells, ist aber für die Kryptoanalyse sogar besonders realistisch: Nach Wahl der Inputlänge n hat der Kryptoanalytiker die Möglichkeit, einen passenden Algorithmus zu wählen. Das heisst, Aussagen über Nichteffizienz, die unter diesem Berechnungsmodell bewiesen werden, erlauben, die Inputlänge als öffentlich bekannt anzunehmen.

Ist eine TURING-Berechnung in polynomialer Zeit möglich, so gibt es für das gleiche Problem auch eine polynomiale Schaltnetzfamilie. Die Umkehrung davon gilt nicht; es sind allerdings nur „künstliche“ Beispiele bekannt. Gäbe es für irgendein NP-vollständiges Problem eine polynomiale Schaltnetzfamilie, so für alle. Nichtgleichmäßige Komplexität kann man allerdings auch mit TURING-Maschinen modellieren, indem man für jede Eingabelänge eine andere TURING-Maschine zulässt. Analog kann man natürlich auch probabilistische TURING-Maschinen zulassen.

Ein Problem soll **hart** heissen, wenn es kein PPS gibt, das es mit signifikanter Wahrscheinlichkeit löst. Die früher behandelten „harten zahlen-

theoretischen Probleme“ sind vermutlich in diesem Sinne hart, z. B. die Primzerlegung; präzisiert wird das später.

Wir wissen bereits, dass die Grundoperationen für ganze Zahlen mit polynomialen Schaltnetzfamilien berechenbar sind (sogar deterministisch).