

4.6 Der IMPAGLIAZZO-NAOR-Generator

Das Rucksack-Problem (knapsack problem, subset sum problem) ist bekanntlich das folgende:

Gegeben: Natürliche Zahlen $a_1, \dots, a_n \in \mathbb{N}$ und $T \in \mathbb{N}$.

Gesucht: Eine Teilmenge $S \subseteq \{1, \dots, n\}$ mit

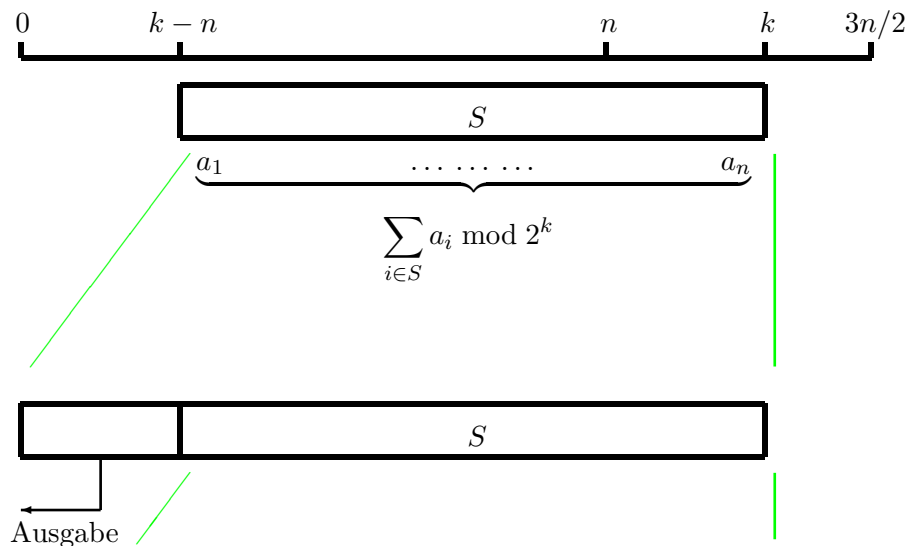
$$\sum_{i \in S} a_i = T.$$

Dieses Problem gilt als hart; es ist sogar NP-vollständig. Aufbauend darauf haben IMPAGLIAZZO und NAOR den folgenden Zufallsgenerator entwickelt:

Seien k und n (genügend große) natürliche Zahlen mit $n < k < \frac{3n}{2}$; als Parameter werden $a_1, \dots, a_n \in [1 \dots 2^k]$ zufällig gewählt. [Achtung: Das sind viele große Zahlen.] Der Zustandsraum besteht aus der Potenzmenge von $\{1, \dots, n\}$; die Zustände sind also Teilmengen $S \subseteq \{1, \dots, n\}$ und werden durch Bitfolgen in \mathbb{F}_2^n auf natürliche Weise repräsentiert. In jedem einzelnen Schritt wird die Summe

$$\sum_{i \in S} a_i \pmod{2^k}$$

gebildet. Das ist eine k -Bit-Zahl. Die ersten $k - n$ Bits werden ausgegeben, die letzten n Bits als neuer Zustand zurückbehalten, siehe die Abbildung.



Transformation und Outputfunktion sind also:

$$T(S) = \sum_{i \in S} a_i \bmod 2^n$$

(rechte n Bits weiterverwenden),

$$U(S) = \lfloor \frac{\sum_{i \in S} a_i \bmod 2^k}{2^n} \rfloor$$

linke $k - n$ Bits ausgeben.

Falls dieser Zufallsgenerator nicht perfekt ist, ist das Rucksack-Problem effizient lösbar.