Asymptotic Analysis of Sequences Defined by Automata

Sara Kropf

Um eine kryptographische Verschlüsselung zu optimieren, ist es sinnvoll, Zahlen nicht im Dezimalsystem darzustellen. Dadurch können bestimmte Operationen, wie die Multiplikation großer Zahlen, schneller durchgeführt werden. Insgesamt wird die Verschlüsselung damit sicherer, da größere Schlüssel benutzt werden können.

Die Größe von bestimmten Parametern des Ziffernsystems beeinflusst die Laufzeit der Verschlüsselung. Ein Beispiel für einen solchen Parameter ist die Ziffernsumme. Um genaue Angaben zur Laufzeit eines Verschlüsselungsalgorithmus zu geben, ist eine asymptotische Analyse dieser Parameter notwendig. Dazu werden sogenannte Automaten verwendet: Das sind einfache Modelle für einen Computer mit einem endlichen Speicher. In Abbildung 1 ist ein Beispiel für einen solchen Automaten gegeben, wobei die Knoten die endlich vielen Speicherzustände symbolisieren und die Kanten die Übergänge zwischen den Zuständen. Dabei ist die Beschriftung der Übergänge als „Input Label | Output Label“ zu lesen.

Die gesuchten Parameter des Ziffernsystems können als der Output von Automaten dargestellt werden. Um solche Parameter asymptotisch zu analysieren, werden in dieser Dissertation grundlegende Resultate bewiesen.

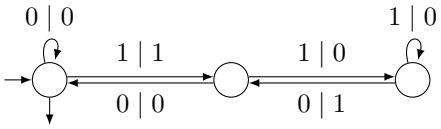

Abbildung 1: Beispiel für einen Automaten mit Output.

Die asymptotischen Resultate beinhalten zum Beispiel den erwarteten durchschnittlichen Output in der Form

$$\frac{8}{13}\log_2 N + \Psi(\log_2 N) + o(1)$$

bei einem zufälligen Input kleiner als N. Diese Formel setzt sich zusammen aus einem logarithmischen Hauptterm plus einer periodischen Fluktuation Ψ (siehe Abbildung 2) plus einem Fehlerterm, der gegen 0 konvergiert.

In dieser Dissertation werden die grundlegenden Resultate bewiesen, damit im Endeffekt eine solche asymptotische Analyse mit der Berechnung aller Konstanten automatisiert von einem Computer durchgeführt werden kann.

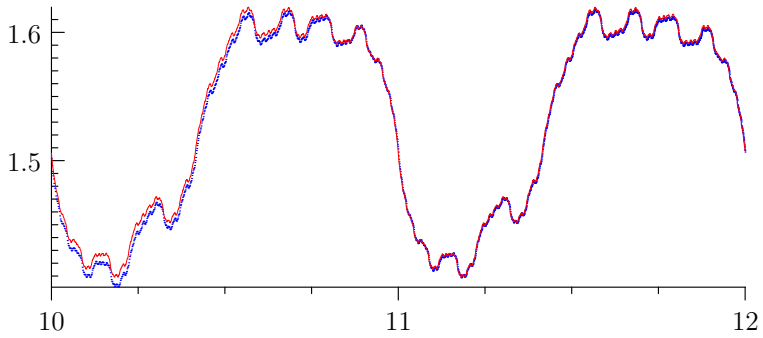

Abbildung 2: Periodische Fluktuation Ψ (rot) mit empirischen Werten (blau).