Mathematisch-Naturwissenschaftliche Fakultät

Institut für Mathematik

Fachgebiet: Mathematik

Betreuer: Prof. Gohar Kyureghyan
Björn Kriepke
(e-mail: bjoern.kriepke@uni-rostock.de)

Shift-invariant functions with the polynomial composition property

Englische Zusammenfassung

Cryptographic algorithms rely on mathematical functions with special properties. One example is the function χ used in SHA-3, a widely used cryptographic hash standard. We show that repeatedly applying this function reveals an interesting algebraic behavior: it can be described with a special family of functions which behaves like polynomials. This raises the question of whether a more general mathematical principle explains this behavior.

In this thesis, we identify such a principle for a broader class of functions. We characterize precisely when repeated application of these functions exhibits this polynomial-like behavior and classify the algebraic structures that arise. This provides a unified framework for understanding patterns previously observed in χ and its generalizations. Finally, we study the cycles that arise when χ is repeatedly applied. We derive new formulas for counting these cycles and use them to describe how their number grows as the system becomes larger.

Deutsche Zusammenfassung

Kryptographische Algorithmen beruhen auf mathematischen Funktionen mit besonderen Eigenschaften. Ein Beispiel ist die Funktion χ aus SHA-3, einem weitverbreiteten kryptographischen Hashstandard. Wir zeigen, dass die wiederholte Anwendung dieser Funktion ein interessantes algebraisches Verhalten zeigt: Es lässt sich mithilfe einer speziellen Familie von Funktionen beschreiben, die sich ähnlich wie Polynome verhält. Dies wirft die Frage auf, ob diesem Verhalten ein allgemeineres mathematisches Prinzip zugrunde liegt.

In dieser Arbeit identifizieren wir ein solches Prinzip für eine allgemeinere Klasse von Funktionen. Wir charakterisieren präzise, unter welchen Bedingungen die wiederholte Anwendung dieser Funktionen dieses polynomähnliche Verhalten aufweist, und klassifizieren die dabei entstehenden algebraischen Strukturen. Dadurch schaffen wir einen einheitlichen Rahmen, um die zuvor bei χ und Verallgemeinerungen dieser Funktion beobachtete Muster zu verstehen. Abschließend untersuchen wir die Zyklen, die bei der wiederholten Anwendung von χ entstehen. Wir leiten neue Formeln zum Zählen dieser Zyklen her und analysieren, wie ihre Anzahl mit zunehmender Systemgröße wächst.