Kurzfassung

Das Hauptziel dieser Arbeit ist, eine prägnante Einführung in das ursprüngliche McEliece-Verfahren von 1978 sowie in die Variante nach Niederreiter zu präsentieren. Das McEliece-Kryptosystem bietet nach heutigen Annahmen eine starke Sicherheit gegenüber bekannten Angriffen, insbesondere gegenüber Angriffen mit Quantencomputern. Zunächst werden die von Quantencomputern ausgehenden Risiken skizziert und das McEliece-Kryptosystem und seine Varianten innerhalb der Post-Quanten-Kryptografie eingeordnet. Zur Erklärung der Verfahren wird anschließend eine detaillierte Einführung in die verwendete Code-Klasse der Goppa Codes präsentiert. Im Anschluss daran werden Optimierungen und Schwächen sowohl des McEliece- als auch des Niederreiter-Systems aufgezeigt und jeweils ein Beispiel gegeben. Abschließend wird die aktuelle Classic McEliece-Variante des Systems vorgestellt.

Ergänzend zu diesem Buch steht im Github Repository 'GoppaCodes-and-McElieceKryptosystem' die Programmierung der Kryptosysteme als Jupyter Notebook zur Verfügung. Diese kann in cocalc ohne die Installation von Software ausprobiert werden.

Schlüsselwörter: Goppa Code, McEliece-Kryptosystem, asymmetrische Verschlüsselung, Fehlerkorrekturcodes, Post-Quanten-Kryptografie.

Abstract

The primary objective of this paper is to provide a concise introduction to the original McEliece scheme from 1978, as well as to the Niederreiter variant. The McEliece cryptosystem, under current assumptions, offers a high level of security against known attacks, particularly those involving quantum computers. Initially, the risks posed by quantum computers are outlined, and the McEliece cryptosystem and its variants are classified in the field of post-quantum cryptography. To explain the procedures, a detailed introduction to the class of codes used, known as Goppa codes, is presented.

Following that, optimizations and weaknesses of both the McEliece and Niederreiter systems are highlighted, with an example provided for each. Finally, the current Classic McEliece variant of the system is introduced.

In addition to this book, the Github repository 'GoppaCodes-and-McElieceKryptosystem' contains the programming of the crypto systems as a Jupyter notebook. This can be used in cocalc without the installation of software.

Keywords: Goppa code, McEliece cryptosystem, asymmetric encryption, error correction codes, post quantum cryptography.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Liste der Algorithmen

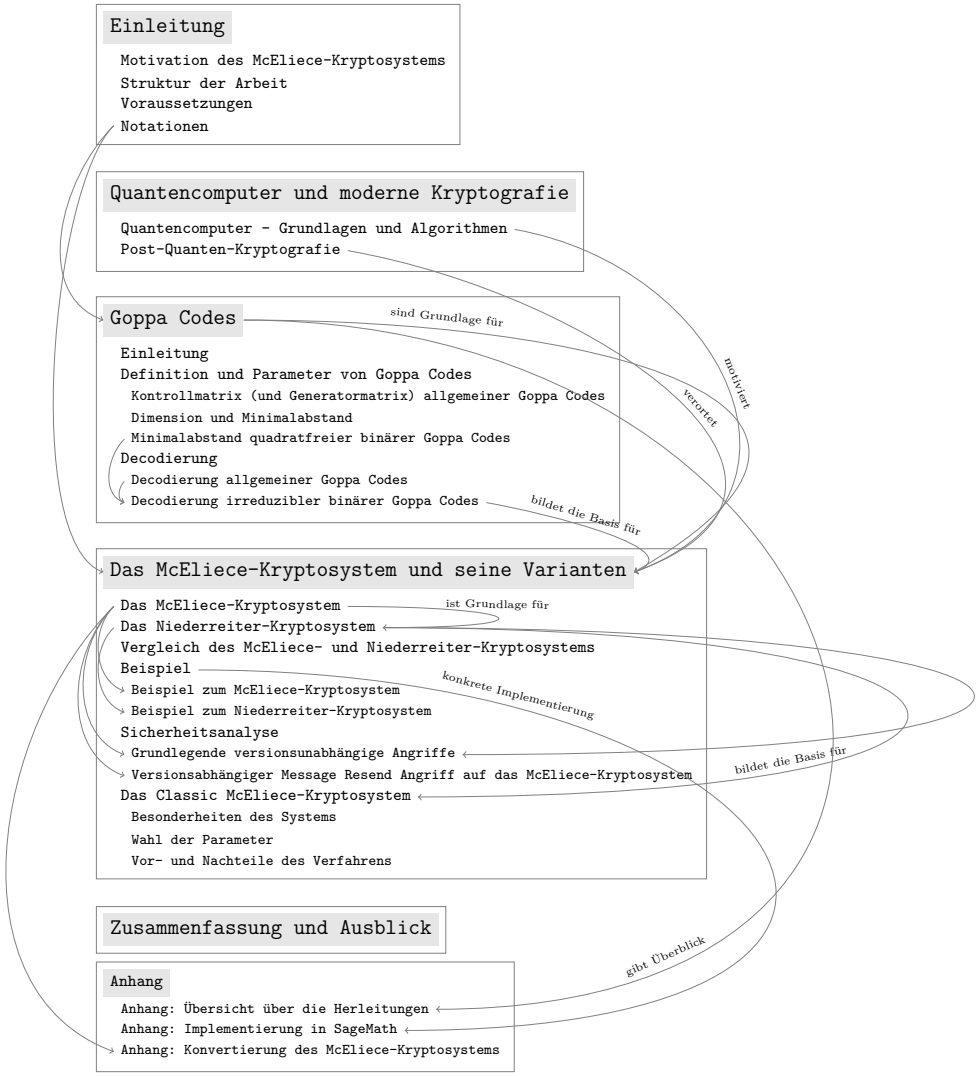

Abbildung 1.1.: Zusammenhang der Abschnitte und Kapitel
Aufeinanderfolgende Kapitel stehen immer in direktem Zusammenhang. Besondere Beziehungen sind durch die Pfeile hervorgehoben. Insbesondere der Zusammenhang der Kryptosysteme und die Einordnung, welcher Teil der Sicherheitsanalyse welches Kryptosystem betrifft, ist nochmal hervorgehoben.

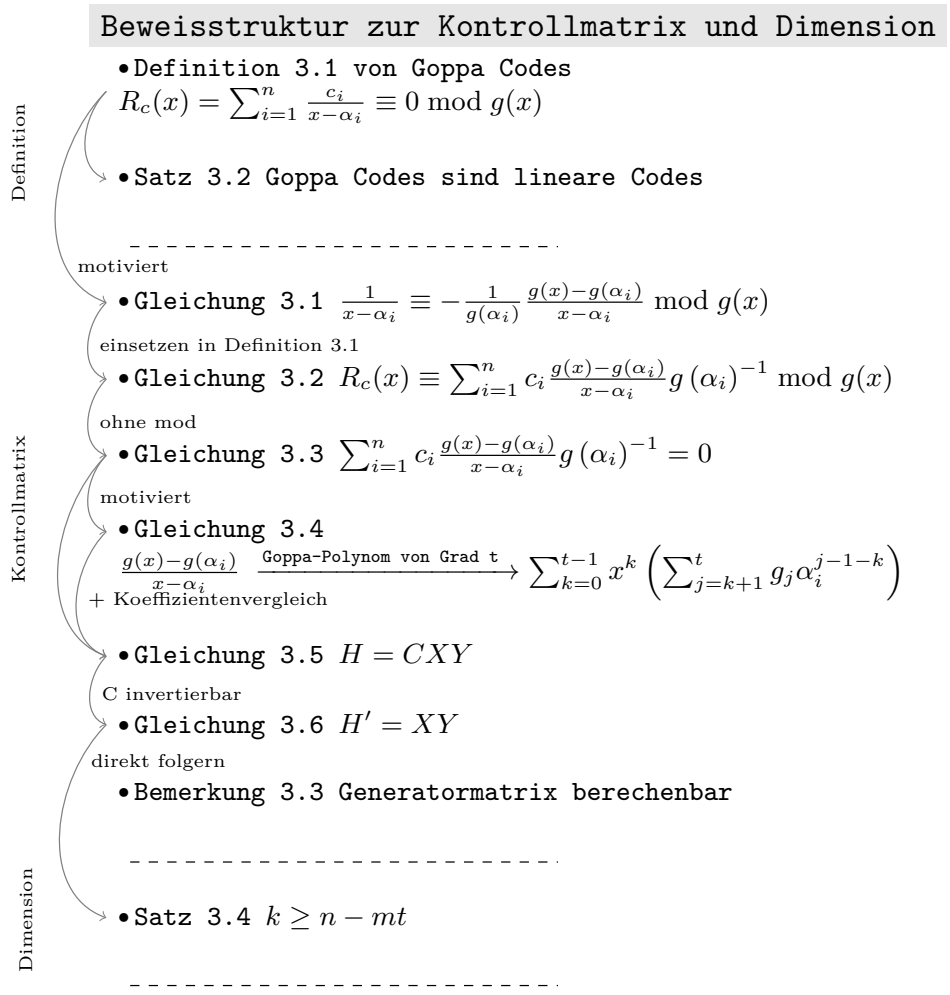

Abbildung A.1.: Übersicht über die Beweisstruktur zur Kontrollmatrix und Dimension von Goppa Codes

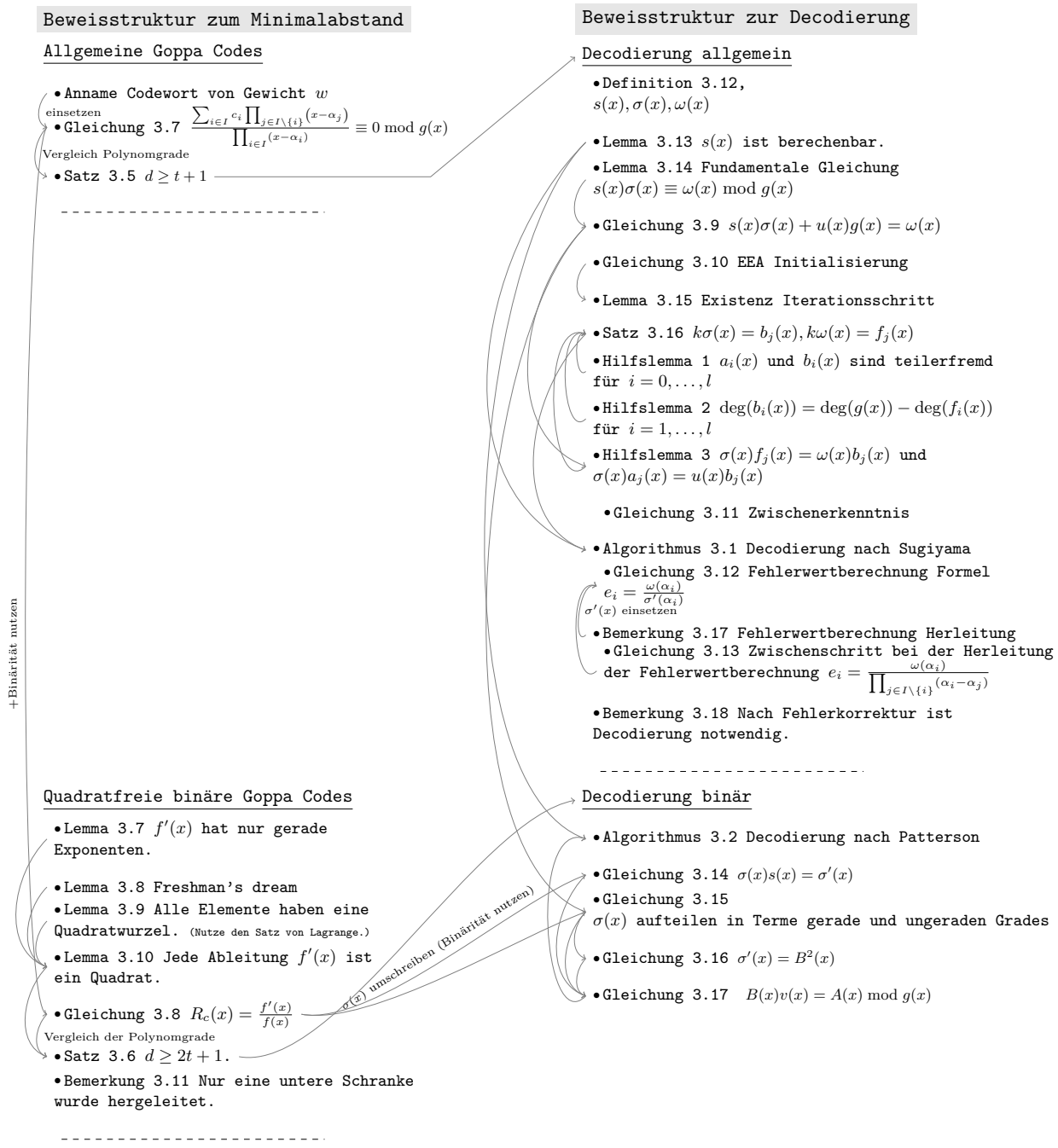

Abbildung A.2.: Übersicht über die Beweisstruktur zum Minimalabstand und der Decodierung von Goppa Codes