3. Goppa Codes

3.1. Einleitung

Goppa Codes sind für Kryptosysteme von besonderer Bedeutung, da für sie im Gegensatz zu vielen anderen Codeklassen weiterhin die Annahme der Ununterscheidbarkeit von zufälligen linearen Codes gilt. Kombiniert mit der zweiten Annahme, dass zufällige lineare Codes aufgrund des General-Decoding-Problems (sowohl auf Digitalrechnern als auch mithilfe von Quantencomputern) nicht effizient decodiert werden können,[1] ist es möglich, mit einem effizienten Decodierverfahren für Goppa Codes eine quantensichere Einwegfunktion und damit ein quantensicheres Kryptosystem zu konstruieren. Der Kern dieses Kapitels ist es ein effizientes Decodierverfahren für Goppa Codes herzuleiten. Dazu werden Goppa Codes definiert und grundlegende Eigenschaften bewiesen. Das Kapitel ist angelehnt an die Arbeiten von Goppa [12], Huffman et al. [13], Baldoni et al. [1] und MacWilliams et al. [16].

Goppa Codes wurden 1970 vom russischen Mathematiker Valery Goppa in seinem Paper „A new class of linear correcting codes“ eingeführt [12]. Nach Goppa hat diese Codeklasse die besonderen Vorteile, wie zyklische Codes durch ein Generatorpolynom spezifiziert zu sein. Doch im Gegensatz zu zyklischen Codes erlaube der Grad des Generatorpolynoms eine Abschätzung der Parameter eines Goppa Codes. Die einzigen zyklischen Codes, die nach Goppa ebenfalls diese Eigenschaft aufweisen, seien BCH-Codes, die durch Goppa Codes verallgemeinert würden (vgl. [12]).

[1] Da es sich hierbei um Annahmen handelt, sind die beiden Aussagen bisher nicht bewiesen oder widerlegt worden. Sie bilden die Grundlage für die Sicherheit des McEliece Kryptosystems.

3.2. Definition und Parameter von Goppa Codes

Goppa Codes der Länge n über $\mathbb{F}_q$ sind wie folgt definiert:[2]

Definition 3.1 (Goppa Codes)**.** Sei $\mathbb{F}_q$ ein endlicher Körper und $m \in \mathbb{N}$ beliebig.

Es seien $L = (\alpha_1, \ldots, \alpha_n)$ ein n-Tupel paarweise verschiedener Elemente aus $\mathbb{F}_{q^m}$ und $g(x) \in \mathbb{F}_{q^m}[x]$ ein normiertes Polynom mit $g(\alpha_i) \neq 0$ für $i = 1, \ldots, n$. Dann heißt der lineare Code

$$\Gamma(L, g) := \left\{ c = (c_1, \ldots, c_n) \in \mathbb{F}_q^n : R_c(x) = \sum_{i=1}^{n} \frac{c_i}{x - \alpha_i} \equiv 0 \bmod g(x) \right\}$$

über $\mathbb{F}_q$ (klassischer) *Goppa Code* der Länge n zum *Goppa-Polynom* $g(x)$. L wird auch *Support* des Goppa Codes genannt.

Ist $g(x)$ zudem irreduzibel, so wird $\Gamma(L, g)$ als *irreduzibler Goppa Code* bezeichnet.

Es ist zu bemerken, dass das Inverse von $x - \alpha_i \bmod g(x)$ existiert, da aus $g(\alpha_i) \neq 0$ folgt, dass der ggT von $(x - \alpha_i)$ und $g(x)$ gleich 1 ist. Aus dem Lemma von Bézout folgt dann die Existenz.

Satz 3.2 (Goppa Codes sind lineare Codes)**.** Goppa Codes sind lineare Codes, da

$$R_{ac}(x) = \sum_{i=1}^{n} \frac{ac_i}{x - \alpha_i} = a \sum_{i=1}^{n} \frac{c_i}{x - \alpha_i} \equiv a \cdot 0 \equiv 0 \bmod g(x)$$

für alle $a \in \mathbb{F}_q, c \in \Gamma(L, g)$ gilt und

$$R_{c_1+c_2}(x) = \sum_{i=1}^{n} \frac{c_1 + c_2}{x - \alpha_i} = \sum_{i=1}^{n} \frac{c_1}{x - \alpha_i} + \sum_{i=1}^{n} \frac{c_2}{x - \alpha_i} \equiv 0 + 0 \equiv 0 \bmod g(x)$$

für alle $c_1, c_2 \in \Gamma(L, g)$ gilt.

[2] Beachte, dass im Originalpaper nur binäre Goppa Codes betrachtet werden, die erst in späteren Papern generalisiert wurden. Hier wird eine Definition über beliebigen Galoiskörpern gegeben.

3.2.1. Kontrollmatrix (und Generatormatrix)

Im vorherigen Abschnitt wurde gezeigt, dass Goppa Codes lineare Codes sind. Da für jeden linearen Code eine Generator- und Kontrollmatrix existiert, wird im Folgenden die Kontrollmatrix von Goppa Codes hergeleitet.[3]

Die Existenz von $(x - \alpha_i)^{-1}$ aus der Definition von Goppa Codes wurde bereits gezeigt. Das Inverse Element zu $(x - \alpha_i)^{-1}$ lässt sich mittels des erweiterten euklidischen Algorithmus herleiten und ist nach Huffman et al. [13] wie folgt angeben

$$\frac{1}{x-\alpha_i} = 1 \cdot \frac{1}{x-\alpha_i} \equiv \left(\frac{g(\alpha_i)}{g(\alpha_i)} - \frac{g(x)}{g(\alpha_i)}\right) \frac{1}{x-\alpha_i} \equiv -\frac{1}{g(\alpha_i)} \frac{g(x) - g(\alpha_i)}{x-\alpha_i} \bmod g(x). \tag{3.1}$$

Ersetzt man in Definition 3.1 den Bruch $\frac{1}{x-\alpha_i}$ gemäß Gleichung 3.1, so ist c genau dann ein Codewort, wenn[4]

$$R_c(x) = \sum_{i=1}^{n} \frac{c_i}{x-\alpha_i} \equiv \sum_{i=1}^{n} c_i \frac{g(x) - g(\alpha_i)}{x-\alpha_i} g(\alpha_i)^{-1} \equiv 0 \bmod g(x) \tag{3.2}$$

gilt. In Gleichung 3.2 kann die modulo Operation weggelassen werden, da der Grad von

$$\sum_{i=1}^{n} c_i \frac{g(x) - g(\alpha_i)}{x-\alpha_i} g(\alpha_i)^{-1}$$

durch die Division von $g(x)$ durch $x - \alpha_i$ stets kleiner ist als der von $g(x)$. Ein Codewort c ist also genau dann in $\Gamma(L, g)$ enthalten, wenn

$$\sum_{i=1}^{n} c_i \frac{g(x) - g(\alpha_i)}{x-\alpha_i} g(\alpha_i)^{-1} = 0 \tag{3.3}$$

gilt. Nun wird der Bruch

$$\frac{g(x) - g(\alpha_i)}{x-\alpha_i}$$

genauer analysiert, indem ein Goppa-Polynom eines spezifischen Grades ange-

[3] Die Kontrollmatrix statt der Generatormatrix herzuleiten ist durch die Definition von Goppa Codes motiviert.

[4] Man kann das Minus weglassen, da $0 \equiv -0$ gilt.