Geheime Botschaften

Sommersemester 2017

Dr. T. Moede
t.moede@tu-bs.de
Universitätsplatz 2, Raum 426
0531 391-7527

Technische Universität Braunschweig

Übungsblatt 5

Aufgabe 1. (LFSR - Nullzustand)
Zeigen oder widerlegen Sie: Es gibt ein linear rückgekoppeltes Schieberegister der Länge 4, welches einen Nicht-Nullzustand in den Nullzustand überführt.

Aufgabe 2. (LFSR - maximale Periode)
Machen Sie sich klar, dass für ein LFSR maximaler Periode die ganz rechte Zelle zur Rückkopplung beitragen muss.

Aufgabe 3. (LFSR - Rekonstruktion)
Sie wissen, das ein LFSR der Länge 3 verwendet wurde, um die Folge

$$010\ 110$$

zu erzeugen. Konstruieren Sie aus diesen Daten das LFSR vollständig, d.h. bestimmen Sie die **Initialisierung** und die **Rückkopplungskoeffizienten** c_i.

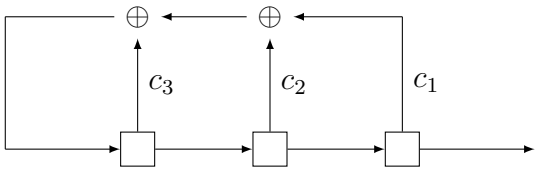

Abbildung 1: Allgemeines LFSR der Länge 3

Aufgabe 4. (LFSR - Primitive Polynome I)
Sie ordnen dem allgemeinen LFSR aus Aufgabe 3 das Polynom

$$1 + c_3x + c_2x^2 + c_1x^3$$

zu. Dieses hat Koeffizienten (nicht Exponenten!) in der Menge $\{0, 1\}$. Ihnen wird erzählt, dass ein solches LFSR genau dann maximale Periode hat, wenn dieses Polynom primitiv ist. Außerdem erhalten Sie die Information, dass ein primitives Polynom immer irreduzibel ist. Natürlich wissen Sie, dass ein Polynom vom Grad 3 genau dann irreduzibel ist, wenn es keine Nullstelle über dem betrachteten Körper hat, d.h. in diesem Fall keine Nullstellen modulo 2 betrachtet hat. Kann dann das LFSR, welches zum Polynom

$$1 + x + x^2 + x^3$$

gehört, maximale Periode haben?

Aufgabe 5. (LFSR - Primitive Polynome II)
Für ein Polynom $p \in \mathbb{F}_2[x]$ vom Grad n mit $p(0) \neq 0$ definieren wir den **Exponenten** als die kleinste Zahl e, so dass p das Polynom $x^e + 1$ teilt. Das Polynom wird **primitiv** genannt, wenn der Exponent gerade $2^n - 1$ ist. Zeigen Sie, dass das Polynom

$$1 + x + x^3 \in \mathbb{F}_2[x]$$

primitiv ist. Beachten Sie hierbei, dass Sie die Koeffizienten modulo 2 reduzieren müssen. Nach Aufgabe 4 liefert dies ein LFSR der Länge 3 von maximaler Periode.