

# Pseudozufallszahlen

Vorlesungsskript von Arne Winterhof

31. Januar 2005

Dieses Skript ist die schriftliche Ausarbeitung einer Vorlesung, die ich im Wintersemester 2004/2005 an der Kepler Universität Linz gehalten habe.

Arne Winterhof

## Inhaltsverzeichnis

<b>1</b>	<b>Einleitung</b>	<b>1</b>
1.1	Anwendungsbeispiele . . . . .	1
1.2	Beispiele für Pseudozufallszahlengeneratoren . . . . .	2
<b>2</b>	<b>Bitfolgen</b>	<b>4</b>
2.1	Bitverteilung . . . . .	4
2.2	Autokorrelation . . . . .	7
<b>3</b>	<b>Lineare Komplexität</b>	<b>9</b>
3.1	Berlekamp-Massey Algorithmus . . . . .	10
3.2	Legendre-Folge . . . . .	12
3.3	Erwartungswert . . . . .	16
<b>4</b>	<b>Gittertest</b>	<b>18</b>
4.1	Lineare Komplexität und Gittertest . . . . .	19
4.2	Expliziter Inversionsgenerator . . . . .	23
4.3	Rekursiver Inversionsgenerator . . . . .	24
<b>5</b>	<b>Diskrepanz</b>	<b>26</b>
5.1	Allgemeine Diskrepanzschranke . . . . .	28
5.2	Exkurs über Exponentialsummen . . . . .	30
5.3	Linearer Kongruenzgenerator . . . . .	32
5.4	Expliziter Inversionsgenerator . . . . .	34
5.5	Rekursiver Inversionsgenerator . . . . .	36

<b>6</b>	<b>Weitere Bemerkungen zu Inversionsgenerator und Legendre-Folge</b>	<b>38</b>
6.1	Maximale Periode des rekursiven Inversionsgenerators . . . . .	38
6.2	Berechnung . . . . .	39
<b>7</b>	<b>Weitere Generatoren</b>	<b>40</b>
7.1	Explizite inverse und nichtlineare Generatoren . . . . .	40
7.2	Verallgemeinerungen von Legendre-Folgen und Sidelnikov-Folgen .	40
7.3	Potenzgenerator und quadratischer Kongruenzgenerator . . . . .	41
7.4	Nichtlineare Generatoren höherer Ordnung . . . . .	41
7.5	Exponentialgenerator und quadratischer Exponentialgenerator . .	41
7.6	Folgen über elliptischen Kurven . . . . .	42
<b>8</b>	<b>Lineare Komplexität von Sidelnikov-Folgen</b>	<b>42</b>
8.1	Maximale Lineare Komplexität über $\mathbb{F}_2$ . . . . .	42
8.2	Lineare Komplexität über $\mathbb{F}_p$ . . . . .	44
<b>9</b>	<b>Lineare Komplexität über verschiedenen Moduln</b>	<b>45</b>
<b>10</b>	<b>Lineare Komplexität weiterer Generatoren</b>	<b>47</b>
10.1	Explizit nichtlinearer Generator der Periode $p$ . . . . .	47
10.2	Legendre Folge über $\mathbb{F}_p$ . . . . .	48
10.3	Quadratischer Exponentialgenerator . . . . .	48
<b>11</b>	<b><math>k</math>-Fehler lineare Komplexität</b>	<b>48</b>
11.1	1-Fehler lineare Komplexität der Legendre-Folge über $\mathbb{F}_p$ . . . . .	49
11.2	1-Fehler lineare Komplexität der Sidelnikov-Folge über $\mathbb{F}_p$ . . . . .	49
<b>12</b>	<b>Literatur</b>	<b>50</b>

# 1 Einleitung

Als *Pseudozufallszahlen* bezeichnet man Zahlenfolgen, die durch einen deterministischen Algorithmus (*Pseudozufallszahlengenerator*) berechnet werden aber 'zufällig' aussehen. (Deterministisch heißt, dass bei jedem Start der Zufallszahlenberechnung mit gleichem Startwert die gleiche Zahlenfolge erzeugt wird.)

Die 'Zufälligkeit' wird durch statistische Eigenschaften der Zahlenfolge bestimmt wie Gleichwahrscheinlichkeit der einzelnen Zahlen und statistische Unabhängigkeit verschiedener Zahlen der Folge.

Man unterscheidet zwischen periodischen und nicht-periodischen Pseudozufallszahlengeneratoren. (Eine Folge  $(x_n)$  heißt *periodisch mit Periode  $t$* , wenn  $x_{n+t} = x_n$  für  $n = 0, 1, \dots$  gilt.)

Beispiele:

1. Sei  $p$  eine Primzahl,  $x_0$  ein ganzzahliger Startwert und  $a$  ein ganzzahliger Multiplikator, so dass  $x_0$  und  $a$  beide nicht durch  $p$  teilbar sind. Dann ist die durch

$$x_{n+1} = ax_n \text{ mod } p$$

definierte Folge periodisch. (Für eine ganze Zahl  $x$  ist  $x \text{ mod } p$  definiert als die eindeutige ganze Zahl  $y$  mit  $0 \leq y \leq p - 1$ , für die  $x - y$  durch  $p$  teilbar ist.) Z.B. die Wahl  $p = 5$ ,  $x_0 = 1$  und  $a = 2$  liefert eine Folge der Periode 4.

2. Sei  $m > 1$  eine quadratfreie natürliche Zahl. Dann ist die Folge  $(x_n)$  der Nachkommastellen von  $\sqrt{m}$ , d.h.

$$\sqrt{m} = a, x_0x_1x_2 \dots,$$

nicht-periodisch.

Da periodische Generatoren oft deutlich schneller als nicht-periodische sind, beschränken wir uns im Folgenden auf periodische Pseudozufallszahlengeneratoren.

## 1.1 Anwendungsbeispiele

Die Qualität von Pseudozufallszahlen hängt von der jeweiligen Anwendung ab. Das sollen die folgenden beiden Beispiele verdeutlichen.

Monte-Carlo Berechnung von  $\pi$ :

1. Wähle  $N$  Paare von Pseudozufallszahlen

$$(x_n, x_{n+1}) \in [0, 1)^2, \quad n = 0, \dots, N - 1.$$

2. Zähle die Anzahl  $K$  der Paare  $(x_n, x_{n+1})$  innerhalb des Einheitskreises (d.h.  $x_n^2 + x_{n+1}^2 \leq 1$ ).
3. Bestimme als Näherungswert  $\pi \approx \frac{4K}{N}$ .

Die Qualität der Pseudozufallszahlen bezüglich dieser Anwendung hängt von der Verteilung der Paare  $(x_n, x_{n+1})$  im Einheitsquadrat ab.

Stromchiffren:

Wir betrachten eine als  $(0, 1)$ -Folge (Bitfolge) dargestellte Nachricht  $m_0, m_1, \dots$ . Ein *Stromchiffre* verschlüsselt jedes Bit  $m_j$  der Nachricht mit dem Element  $x_j$  einer binären Pseudozufallszahlenfolge  $x_0, x_1, \dots$  durch

$$c_j = m_j + x_j \text{ mod } 2.$$

Der verschlüsselte Text  $c_0, c_1, \dots$  kann durch erneutes Addieren der Pseudozufallszahlenfolge zurück erhalten werden:

$$m_j = c_j + x_j \text{ mod } 2.$$

Die Sicherheit eines Stromchiffres hängt von der 'Zufälligkeit' der Pseudozufallszahlenfolge, insbesondere von ihrer Vorhersagbarkeit, ab.

Das erste Beispiel soll uns als Fundamentalbeispiel für sogenannte Monte-Carlo-Methoden dienen, das zweite für kryptografische Anwendungen.

## 1.2 Beispiele für Pseudozufallszahlengeneratoren

Wir unterscheiden im Folgenden zwischen Pseudozufallsbits, d.h.  $(0, 1)$ -Folgen, und Folgen im Einheitsintervall  $[0, 1)$ .

Beispiel: (Bitgenerator, Legendre-Folge)

Sei  $p > 2$  eine Primzahl. Für eine ganze Zahl  $n$  ist das Legendre-Symbol  $\left(\frac{n}{p}\right)$  definiert durch

$$\left(\frac{n}{p}\right) = \begin{cases} 0, & n \text{ ist durch } p \text{ teilbar,} \\ 1, & n \text{ ist nicht durch } p \text{ teilbar und} \\ & \text{es gibt eine ganze Zahl } x \text{ mit } x^2 \equiv n \pmod{p}, \\ -1, & \text{sonst.} \end{cases}$$

(Die Bezeichnung  $a \equiv b \pmod p$  bedeutet, dass  $a - b$  durch  $p$  teilbar ist.) Das Legendre-Symbol hat die Eigenschaften

$$\left(\frac{n}{p}\right) \left(\frac{m}{p}\right) = \left(\frac{nm}{p}\right)$$

und

$$\left(\frac{n}{p}\right) \equiv n^{(p-1)/2} \pmod p.$$

Die Legendre-Folge  $(l_n)$  ist definiert durch

$$l_n := \begin{cases} 1, & \left(\frac{n}{p}\right) = -1, \\ 0, & \text{sonst,} \end{cases} \quad n = 0, 1, \dots$$

und hat Periode  $p$ .

Beispiele: (Pseudozufallszahlen im Einheitsintervall)

1. Linearer Kongruenzgenerator

Sei  $p$  eine Primzahl, sowie  $1 \leq y_0 \leq p - 1$  und  $1 \leq a \leq p - 1$  ganze Zahlen. Sei

$$y_{n+1} = ay_n \pmod p, \quad n = 0, 1, \dots$$

Dann erhalten wir lineare Pseudozufallszahlen  $(x_n)$  im Intervall  $[0, 1)$  durch

$$x_n = y_n/p, \quad n = 0, 1, \dots$$

Die Folge  $(x_n)$  ist  $t$ -periodisch, wobei  $t$  die Ordnung von  $a$  modulo  $p$  ist, d.h.  $t$  ist die kleinste natürlich Zahl mit  $a^t \equiv 1 \pmod p$ .

Da man mit Hilfe von lediglich zwei Folgegliedern  $y_n, y_{n+1}$  das Bildungsgesetz der Folge berechnen kann, sind lineare Kongruenzgeneratoren für kryptografische Anwendungen ungeeignet.

2. Nichtlinearer Kongruenzgenerator

Sei  $p$  eine Primzahl,  $0 \leq y_0 \leq p - 1$ ,  $f$  ein Polynom vom Grad größer gleich 2 mit ganzzahligen Koeffizienten und Hauptkoeffizient  $1 \leq a \leq p - 1$ . Sei

$$y_{n+1} = f(y_n) \pmod p, \quad n = 0, 1, \dots$$

(Wegen  $x^p \equiv x \pmod p$  dürfen wir  $\text{grad}(f) \leq p - 1$  annehmen.) Dann erhalten wir nichtlineare Pseudozufallszahlen  $(x_n)$  im Intervall  $[0, 1)$  durch  $x_n = y_n/p$ ,  $n = 0, 1, \dots$ . Die Folge  $(x_n)$  ist schließlich, d.h. evtl. nach einer Vorperiode, periodisch. Durch Wahl eines geeigneten Startwertes  $y_0$  können wir annehmen, dass  $(x_n)$  rein periodisch, d.h. ohne Vorperiode, ist. Ist  $f$  modulo  $p$  bijektiv, so ist  $(x_n)$  rein periodisch.

### 3. Inversionsgenerator

Sei  $p$  eine Primzahl, sowie  $0 \leq y_0, b \leq p-1$  und  $1 \leq a \leq p-1$  ganze Zahlen. Sei

$$y_{n+1} = a\bar{y}_n + b \pmod{p}, \quad n = 0, 1, \dots,$$

wobei  $\bar{x}$  das Inverse  $x^{-1}$  von  $x$  modulo  $p$  bezeichnet, wenn  $x$  nicht durch  $p$  teilbar ist und anderenfalls 0 ist. (Das Inverse  $x^{-1}$  von  $x$  erfüllt  $xx^{-1} \equiv 1 \pmod{p}$ .) Dann erhalten wir inverse Pseudozufallszahlen  $(x_n)$  im Intervall  $[0, 1)$  durch  $x_n = y_n/p$ ,  $n = 0, 1, \dots$ . Die Folge  $(x_n)$  ist rein periodisch.

### 4. Expliziter nichtlinearer Kongruenzgenerator

Seien  $p$  und  $f$  wie in 2.. Dann definieren wir die  $p$ -periodische Folge  $(y_n)$  durch

$$y_n = f(n) \pmod{p}, \quad n = 0, 1, \dots$$

Explizite nichtlineare Pseudozufallszahlen erhalten wir durch Division mit  $p$ .

### 5. Expliziter Inversionsgenerator

Wir benutzen die Bezeichnungen aus 3. und definieren die  $p$ -periodische Folge  $(y_n)$  durch

$$y_n = \overline{an + b} \pmod{p}, \quad n = 0, 1, \dots$$

## 2 Bitfolgen

In diesem Kapitel analysieren wir Zufälligkeitskriterien für Pseudozufallsbitfolgen am Beispiel der Legendre-Folge.

### 2.1 Bitverteilung

Ein erstes Kriterium für eine 'gute' Pseudozufallsbitfolge ist, dass die Anzahl der Einsen und die Anzahl der Nullen in etwa gleich ist. Z.B. besteht eine Periode der Legendre-Folge aus  $(p-1)/2$  Einsen und  $(p+1)/2$  Nullen. Neben dieser globalen Verteilungseigenschaft ist auch eine entsprechende lokale Eigenschaften für Periodenabschnitte wünschenswert.

**Satz 1** Für  $1 \leq N \leq p-1$  und  $0 \leq b \leq p-1$  sei  $l_b, l_{b+1}, \dots, l_{b+N-1}$  ein Periodenabschnitt der Legendre-Folge der Länge  $N$ . So gilt für die Anzahlen  $A_0$  und  $A_1$  der Nullen und Einsen in diesem Abschnitt:

$$|A_0 - A_1| < 1 + p^{1/2}(1 + \ln p).$$

Beweis: Wir haben

$$A_1 = \sum_{n=b}^{b+N-1} l_n \quad \text{und} \quad A_0 = N - A_1$$

und somit

$$|A_0 - A_1| = \left| \sum_{n=b}^{b+N-1} (1 - 2l_n) \right| \leq 1 + \left| \sum_{n=b}^{b+N-1} \binom{n}{p} \right|.$$

Setze

$$e_p(x) := e^{2\pi i x/p} = \cos(2\pi x/p) + i \sin(2\pi x/p)$$

und

$$S(a) := \sum_{n=0}^{p-1} \binom{n}{p} e_p(an), \quad 0 \leq a \leq p-1.$$

Sei  $x$  eine Zahl mit  $\left(\frac{x}{p}\right) = -1$ . Dann durchläuft  $xn \bmod p$  alle Werte  $0, 1, \dots, p-1$ , wenn  $n \bmod p$  alle Werte  $0, 1, \dots, p-1$  durchläuft, und es gilt

$$S(0) = \sum_{n=0}^{p-1} \binom{xn}{p} = \left(\frac{x}{p}\right) S(0) = -S(0),$$

woraus

$$S(0) = 0 \tag{1}$$

folgt. Als nächstes zeigen wir

$$|S(a)| = p^{1/2}, \quad 1 \leq a \leq p-1. \tag{2}$$

Sei  $\bar{z} = x - iy$  das konjugiert Komplexe der komplexen Zahl  $z = x + iy$ . Verifiziere außerdem

$$\begin{aligned} e_p(x)e_p(y) &= e_p(x+y), \\ \overline{e_p(x)} &= e_p(-x) \end{aligned}$$

und

$$\binom{n}{p} = \binom{n^{-1}}{p}, \quad n \not\equiv 0 \pmod{p}.$$

Für  $1 \leq a \leq p-1$  gilt

$$\begin{aligned} |S(a)|^2 &= S(a)\overline{S(a)} \\ &= \left( \sum_{n=1}^{p-1} \binom{n}{p} e_p(an) \right) \left( \sum_{m=1}^{p-1} \binom{m^{-1}}{p} e_p(-am) \right) \\ &= \sum_{n=1}^{p-1} \sum_{m=1}^{p-1} \binom{nm^{-1}}{p} e_p(a(n-m)). \end{aligned}$$

In der inneren Summe ersetzen wir  $k := nm^{-1}$  und erhalten

$$|S(a)|^2 = \sum_{k=1}^{p-1} \sum_{m=1}^{p-1} \binom{k}{p} e_p(am(k-1))$$

$$\begin{aligned}
&= \sum_{k=1}^{p-1} \binom{k}{p} \left( -1 + \sum_{m=0}^{p-1} e_p(am(k-1)) \right) \\
&= -S(0) + \sum_{k=1}^{p-1} \binom{k}{p} \sum_{m=0}^{p-1} e_p(am(k-1)).
\end{aligned}$$

Für  $k = 1$  ist die innere Summe gleich  $p$  und für  $k \neq 1$  haben wir

$$\sum_{m=0}^{p-1} e_p(am(k-1)) = \sum_{m=0}^{p-1} e_p(a(k-1))^m = \frac{e_p(a(k-1))^p - 1}{e_p(a(k-1)) - 1} = 0,$$

woraus (2) folgt. Nun gilt

$$\begin{aligned}
\left| \sum_{n=b}^{b+N-1} \binom{n}{p} \right| &= \left| \sum_{n=0}^{p-1} \binom{n}{p} \frac{1}{p} \sum_{a=0}^{p-1} \sum_{m=b}^{b+N-1} e_p(a(n-m)) \right| \\
&= \frac{1}{p} \left| \sum_{a=0}^{p-1} S(a) \sum_{m=b}^{b+N-1} e_p(-am) \right| \\
&\leq \frac{1}{p} \sum_{a=0}^{p-1} |S(a)| \left| \sum_{m=b}^{b+N-1} e_p(-am) \right| \\
&= \frac{1}{p^{1/2}} \sum_{a=1}^{p-1} \left| \sum_{n=0}^{N-1} e_p(an) \right|.
\end{aligned}$$

Schließlich beweisen wir noch

$$T := \sum_{a=1}^{p-1} \left| \sum_{n=0}^{N-1} e_p(an) \right| < p(1 + \ln p). \quad (3)$$

Wir haben

$$\left| \sum_{n=0}^{N-1} e_p(an) \right| = \left| \frac{e_p(a)^N - 1}{e_p(a) - 1} \right| \leq \frac{2}{|e_p(a) - 1|}.$$

Weiterhin gilt

$$|e_p(a) - 1| = |e_p(a/2) - e_p(-a/2)| = 2|\sin(a\pi/p)|, \quad 1 \leq a \leq p-1.$$

Wegen

$$\sin(x) \geq \frac{2x}{\pi}, \quad 0 \leq x \leq \frac{\pi}{2}$$

erhält man

$$|\sin(a\pi/p)| = |\sin(\min(a, p-a)\pi/p)| \geq \frac{2 \min(a, p-a)}{p}$$

und damit

$$\begin{aligned} T &\leq \frac{p}{2} \sum_{a=1}^{p-1} \frac{1}{\min(a, p-a)} = p \sum_{a=1}^{(p-1)/2} \frac{1}{a} \\ &\leq p \left( 1 + \int_1^{(p-1)/2} \frac{dx}{x} \right) = p \left( 1 + \ln \frac{p-1}{2} \right) < p(1 + \ln p) \end{aligned}$$

und das Ergebnis folgt.  $\square$

## 2.2 Autokorrelation

**Definition 1** Sei  $(x_n)$  eine  $t$ -periodische  $(0, 1)$ -Folge. Dann ist die (periodische) Autokorrelationsfunktion  $A(l)$  von  $(x_n)$  definiert durch

$$A(l) := \sum_{n=0}^{t-1} (-1)^{x_n - x_{n+l}}, \quad 1 \leq l \leq t-1.$$

Der Wert  $A(l)$  ist ein Maß für die Gleichheit zwischen der ursprünglichen Folge und einer verschobenen Folge.

**Satz 2** Für die Autokorrelationsfunktion der Legendre-Folge gilt

$$A(l) = \begin{cases} -1, & p \equiv 3 \pmod{4}, \\ 2 \left( \frac{l}{p} \right) - 1, & p \equiv 1 \pmod{4}, \end{cases} \quad 1 \leq l \leq p-1.$$

Beweis: Wir bemerken, dass

$$(-1)^{ln} = \left( \frac{n}{p} \right), \quad n \not\equiv 0 \pmod{p}$$

und somit für  $l = 1, \dots, p-1$

$$\begin{aligned} A(l) &= \left( \frac{l}{p} \right) + \left( \frac{-l}{p} \right) + \sum_{\substack{n=1 \\ n \neq p-l}}^{p-1} \left( \frac{n}{p} \right) \left( \frac{n+l}{p} \right)^{-1} \\ &= \left( \frac{l}{p} \right) \left( 1 + \left( \frac{-1}{p} \right) \right) + \sum_{\substack{n=1 \\ n \neq p-l}}^{p-1} \left( \frac{n/(n+l)}{p} \right) \\ &= \left( \frac{l}{p} \right) (1 + (-1)^{(p-1)/2}) + \sum_{m=2}^{p-1} \left( \frac{m}{p} \right) \\ &= \left( \frac{l}{p} \right) (1 + (-1)^{(p-1)/2}) + S(0) - 1, \end{aligned}$$

da  $n(n+l)^{-1} \pmod{p}$  alle Werte  $0, \dots, p-1$  außer 1 durchläuft, wenn  $n \pmod{p}$  alle Werte außer  $p-l$  durchläuft, und das Ergebnis folgt nach (1).  $\square$

**Definition 2** Sei  $(x_n)$  eine  $t$ -periodische  $(0, 1)$ -Folge. Dann ist die aperiodische Autokorrelationsfunktion  $A(l, b, N)$  von  $(x_n)$  definiert durch

$$A(l, b, N) := \sum_{n=b}^{b+N-1} (-1)^{x_n - x_{n+l}}, \quad 1 \leq l, N \leq t-1, \quad 0 \leq b \leq t-1.$$

Die periodische Autokorrelation ist ein Maß für die 'globale Zufälligkeit' und die aperiodische Autokorrelation für die 'lokale Zufälligkeit' einer Folge.

**Satz 3** Für die aperiodische Autokorrelationsfunktion der Legendre-Folge gilt

$$|A(l, b, N)| < 3 + 2p^{1/2}(1 + \ln p), \quad 1 \leq l, N \leq p-1, \quad 0 \leq b \leq p-1.$$

Beweisskizze: Das Resultat ergibt sich analog zu dem Beweis von Satz 1 mit dem folgenden Ergebnis von A. Weil anstelle von (2):

**Hilfssatz 1** Sei  $f(X)$  ein ganzzahliges Polynom vom Grad  $D$  und  $a$  eine nicht durch  $p$  teilbare ganze Zahl, so gilt

$$\left| \sum_{n=0}^{p-1} \left( \frac{f(n)}{p} \right) e_p(an) \right| \leq Dp^{1/2}.$$

Für einen Beweis siehe W.M. Schmidt: Equations over Finite Fields. Zunächst haben wir

$$\begin{aligned} |A(l, b, N)| &\leq 2 + \left| \sum_{n=b}^{b+N-1} \left( \frac{n}{p} \right) \left( \frac{n+l}{p} \right) \right| \\ &\leq 2 + \frac{1}{p} \sum_{a=0}^{p-1} \left| \sum_{n=0}^{p-1} \left( \frac{n}{p} \right) \left( \frac{n+l}{p} \right) e_p(an) \right| \left| \sum_{m=b}^{b+N-1} e_p(-am) \right|. \end{aligned}$$

Im Beweis von Satz 2 haben wir

$$\sum_{n=0}^{p-1} \left( \frac{n}{p} \right) \left( \frac{n+l}{p} \right) = -1$$

gezeigt. Mit Hilfssatz 1 und (3) ergibt sich

$$|A(l, b, N)| < 2 + \frac{1}{p}(N + 2p^{1/2}p(1 + \ln p))$$

und daraus die Behauptung. □

### 3 Lineare Komplexität

**Definition 3** Sei  $(s_n)$  eine ganzzahlige Folge und  $p$  eine Primzahl. Die lineare Komplexität von  $(s_n)$  modulo  $p$  ist die kleinste natürliche Zahl  $L = L(s_n)$ , so dass es ganze Zahlen  $c_0, \dots, c_{L-1}$  gibt mit

$$s_{n+L} \equiv c_{L-1}s_{n+L-1} + \dots + c_0s_n \pmod{p}, \quad n = 0, 1, \dots$$

Für  $N \geq 2$  ist die lineare Komplexität von  $(s_n)$  bei  $N$  die kleinste natürliche Zahl  $L = L(s_n, N)$ , so dass es ganze Zahlen  $c_0, \dots, c_{L-1}$  gibt mit

$$s_{n+L} \equiv c_{L-1}s_{n+L-1} + \dots + c_0s_n \pmod{p}, \quad n = 0, 1, \dots, N - L - 1. \quad (4)$$

Die Abbildung  $N \mapsto L(s_n, N)$  heißt lineares Komplexitätsprofil von  $(s_n)$ .

Ist  $s_n \equiv 0 \pmod{p}$  für  $n = 0, \dots, N - 1$ , so definieren wir  $L(s_n, N) = 0$ ,  $N \geq 1$ .

Weiterhin definieren wir  $L(s_n, 1) = 1$ , falls  $s_0 \not\equiv 0 \pmod{p}$ .

Allgemein gilt:

1.  $L(s_n) = \sup_{N \geq 1} L(s_n, N)$ .
2.  $L(s_n, N + 1) \geq L(s_n, N)$ ,  $N \geq 1$ .

Ist  $(s_n)$  periodisch mit Periode  $t$ , so gilt:

1.  $L(s_n) \leq t$ .
2.  $L(s_n) = L(s_n, 2t)$ .

Beispiel: Sei  $(s_n)$  eine ganzzahlige Folge mit  $s_n \equiv 0 \pmod{p}$  für  $n = 0, \dots, M - 2$  und  $s_{M-1} \not\equiv 0 \pmod{p}$ , so gilt

$$L(s_n, N) = \begin{cases} 0, & N = 1, \dots, M - 1, \\ N, & N = M. \end{cases}$$

**Hilfssatz 2** Für zwei ganzzahlige Folgen  $(a_n)$  und  $(b_n)$  gilt

$$L(a_n + b_n, N) \leq L(a_n, N) + L(b_n, N), \quad N \geq 1.$$

Beweis: Setze  $M := L(a_n, N)$  und  $K := L(b_n, N)$ . Gelte also

$$a_{n+M} \equiv d_{M-1}a_{n+M-1} + \dots + d_0a_n \pmod{p}, \quad 0 \leq n \leq N - M - 1,$$

und

$$b_{n+K} \equiv e_{K-1}b_{n+K-1} + \dots + e_0b_n \pmod{p}, \quad 0 \leq n \leq N - K - 1,$$

so auch

$$a_{n+M+K} \equiv d_{M-1}a_{n+M+K-1} + \dots + d_0a_{n+K} \pmod{p}, \quad 0 \leq n \leq N - M - K - 1,$$

und

$$b_{n+M+K} \equiv e_{K-1}b_{n+M+K-1} + \dots + e_0b_{n+M} \pmod{p}, \quad 0 \leq n \leq N - M - K - 1.$$

Addition der beiden letzten Gleichungen ergibt

$$\begin{aligned} & (a_{n+M+K} + b_{n+M+K}) \\ = & \sum_{m=0}^{M-1} d_m(a_{n+K+m} + b_{n+K+m}) + \sum_{k=0}^{K-1} e_k(a_{n+M+k} + b_{n+M+k}) \\ & - \sum_{m=0}^{M-1} d_m b_{n+K+m} - \sum_{k=0}^{K-1} e_k a_{n+M+k} \\ = & \sum_{m=0}^{M-1} d_m(a_{n+K+m} + b_{n+K+m}) + \sum_{k=0}^{K-1} e_k(a_{n+M+k} + b_{n+M+k}) \\ & - \sum_{m=0}^{M-1} d_m \sum_{k=0}^{K-1} e_k b_{n+k+m} - \sum_{k=0}^{K-1} e_k \sum_{m=0}^{M-1} d_m a_{n+k+m} \end{aligned}$$

also eine lineare Rekursion für die ersten  $N$  Glieder der Summenfolge und somit die Behauptung.  $\square$

### 3.1 Berlekamp-Massey Algorithmus

**Satz 4** Ist  $L(s_n, N) > N/2$ , so gilt

$$L(s_n, N+1) = L(s_n, N).$$

Ist  $L(s_n, N) \leq N/2$ , so gilt entweder

$$L(s_n, N+1) = L(s_n, N)$$

oder

$$L(s_n, N+1) = N+1 - L(s_n, N).$$

Beweis: Setze  $L := L(s_n, N)$ . Dann existieren  $c_0, \dots, c_{L-1}$  mit

$$s_{n+L} \equiv c_{L-1}s_{n+L-1} + \dots + c_0s_n \pmod{p}, \quad 0 \leq n \leq N - L - 1.$$

Gilt dieselbe Rekursion auch für  $n = N - L$ , so haben wir  $L(s_n, N+1) = L(s_n, N)$ . Anderenfalls setze

$$\lambda := s_N - c_{L-1}s_{N-1} - \dots - c_0s_{N-L} \pmod{p} \neq 0.$$

Sei  $a_n := s_n$  für  $n = 0, \dots, N-1$  und  $a_N := s_N - \lambda$ , so gilt

$$\begin{aligned} N+1 &= L(s_n - a_n, N+1) \leq L(s_n, N+1) + L(-a_n, N+1) \\ &= L(s_n, N+1) + L(a_n, N+1) = L(s_n, N+1) + L(s_n, N). \end{aligned}$$

Somit haben wir

$$L(s_n, N + 1) \geq \max(L(s_n, N), N + 1 - L(s_n, N)).$$

Wir beweisen die Gleichheit induktiv. Für  $N = 1$  gilt offensichtlich Gleichheit und wir nehmen  $N > 1$  an.

Ist  $L(s_n, N) = L(s_n, N - 1) = \dots = L(s_n, 1) = 0$ , so gilt  $s_n \equiv 0 \pmod p$  für  $0 \leq n \leq N - 1$ . Wegen der Annahme  $s_N \not\equiv 0 \pmod p$  folgt  $L(s_n, N + 1) = N + 1$ .

Ist  $L(s_n, N) = L(s_n, N - 1) = \dots = L(s_n, 1) = 1$ , so ist  $s_{n+N} \equiv s_N s_0^{-1} s_n \pmod p$  die gewünschte Rekursionsgleichung.

Wir können also annehmen, dass ein  $1 \leq M \leq N - 1$  existiert mit

$$L(s_n, N) = L(s_n, N - 1) = \dots = L(s_n, M + 1) > L(s_n, M).$$

Nach Induktionsvoraussetzung gilt also  $L(s_n, M) = M + 1 - L$ . Sei

$$s_{n+M+1-L} \equiv d_{M-L}s_{n+M-L} + \dots + d_0 s_n \pmod p, \quad 0 \leq n \leq L - 2,$$

und setze

$$\mu := s_M - d_{M-L}s_{M-1} - \dots - d_0 s_{L-1} \pmod p \neq 0.$$

Im Fall  $L > N/2$  ist

$$\begin{aligned} s_{n+L} &\equiv c_{L-1}s_{n+L-1} + \dots + c_0 s_n \\ &\quad + \lambda \mu^{-1} (s_{n+M-N+L} - d_{M-L}s_{n+M-N+L-1} - \dots - d_0 s_{n-N+2L-1}) \pmod p, \\ &\quad 0 \leq n \leq N - L, \end{aligned}$$

eine Rekursionsgleichung der Länge  $L$  und im Fall  $L \leq N/2$  ist

$$\begin{aligned} s_{n+N+1-L} &\equiv c_{L-1}s_{n+N-L} + \dots + c_0 s_{n+N-2L+1} \\ &\quad + \lambda \mu^{-1} (s_{n+M-L+1} - d_{M-L}s_{n+M-L} - \dots - d_0 s_n) \pmod p, \\ &\quad 0 \leq n \leq L - 1, \end{aligned}$$

eine Rekursionsgleichung der Länge  $N + 1 - L$  für die ersten  $N + 1$  Folgenglieder und die Behauptung folgt.  $\square$

Der Beweis ist konstruktiv und liefert einen Algorithmus zur Bestimmung des linearen Komplexitätsprofils einschließlich der zugehörigen Rekursionsvorschriften.

Beispiel:  $(s_0, \dots, s_9) = (1101011101)$ :

$N$	$L(s_n, N)$	
1	1	— — —
2	1	$s_{n+1} \equiv s_n \pmod{2}$
3	2	$s_{n+2} \equiv s_{n+1} + s_n \pmod{2}$ oder $s_{n+2} \equiv 0 \pmod{2}$
4	2	$s_{n+2} \equiv s_{n+1} + s_n \pmod{2}$
5	3	$s_{n+3} \equiv s_{n+1} \pmod{2}$ oder $s_{n+3} \equiv s_{n+2} + s_n \pmod{2}$
6	3	$s_{n+3} \equiv s_{n+1} \pmod{2}$
7	4	$s_{n+4} \equiv s_{n+1} + s_n \pmod{2}$ oder $s_{n+4} \equiv s_{n+3} + s_n \pmod{2}$
8	4	$s_{n+4} \equiv s_{n+1} + s_n \pmod{2}$
9	5	$s_{n+5} \equiv s_{n+4} + s_{n+3} + s_{n+2} + s_{n+1} + s_n \pmod{2}$ oder $s_{n+5} \equiv s_{n+3} + s_{n+2} \pmod{2}$
10	5	$s_{n+5} \equiv s_{n+4} + s_{n+3} + s_{n+2} + s_{n+1} + s_n \pmod{2}$

### 3.2 Legendre-Folge

**Satz 5** Für die lineare Komplexität modulo 2 der Legendre-Folge  $(l_n)$  bei  $1 \leq N \leq p-1$  gilt:

$$L(l_n, N) > \frac{N}{1 + p^{1/2}(1.5 + \ln p)} - 1.$$

Beweis: Sei  $L := L(l_n, N)$  und gelte

$$l_{n+L} \equiv c_{L-1}l_{n+L-1} + \dots + c_0l_n \pmod{2}, \quad 1 \leq n \leq N - L - 1.$$

Wegen  $(-1)^{l_n} = \left(\frac{n}{p}\right)$ ,  $1 \leq n \leq p-1$ , gilt mit  $c_L := 1$ :

$$1 = (-1)^{\sum_{j=0}^L c_j l_{n+j}} = \left(\frac{\prod_{j=0}^L (n+j)^{c_j}}{p}\right)$$

und daher

$$N - L - 1 = \sum_{n=1}^{N-L-1} \left(\frac{\prod_{j=0}^L (n+j)^{c_j}}{p}\right) =: S.$$

Andererseits kann man analog dem Beweis von Satz 3

$$|S| < (L+1)p^{1/2}(1.5 + \ln p)$$

zeigen, woraus

$$N - (L+1) < (L+1)p^{1/2}(1.5 + \ln p)$$

und die Behauptung folgt. □

**Satz 6** Für die lineare Komplexität modulo 2 der Legendre-Folge  $(l_n)$  gilt:

$$L(l_n) = \begin{cases} (p-1)/2, & p \equiv 1 \pmod{8}, \\ p, & p \equiv 3 \pmod{8}, \\ p-1, & p \equiv 5 \pmod{8}, \\ (p+1)/2, & p \equiv 7 \pmod{8}. \end{cases}$$

Der Beweis folgt nach einigen vorbereitenden Hilfssätzen.

**Hilfssatz 3** Für eine  $t$ -periodische Folge  $(s_n)$  modulo  $p$  definiere

$$S^t(X) := \sum_{n=0}^{t-1} s_n X^n.$$

Dann gilt für die lineare Komplexität modulo  $p$

$$L(s_n) = t - \text{grad}(\text{ggT}(S^t(X), 1 - X^t)).$$

Beweis: Zunächst gilt

$$(1 - X^t) \sum_{n=0}^{\infty} s_n X^n = \sum_{n=0}^{\infty} s_n X^n - \sum_{n=t}^{\infty} s_{n-t} X^n = S^t(X)$$

und somit

$$\frac{1 - X^t}{\text{ggT}(1 - X^t, S^t(X))} \sum_{n=0}^{\infty} s_n X^n = \frac{S^t(X)}{\text{ggT}(1 - X^t, S^t(X))}. \quad (5)$$

Durch Koeffizientenvergleich erhält man eine lineare Rekursionsgleichung für  $(s_n)$  der Länge  $t - \text{grad}(\text{ggT}(1 - X^t, S^t(X)))$ .

Sei jetzt

$$s_{n+L} = \sum_{l=0}^{L-1} c_l s_{n+L-l}, \quad n \geq 0.$$

So ist

$$f(X) := \left( 1 - \sum_{l=0}^{L-1} c_l X^{L-l} \right) \sum_{n=0}^{\infty} s_n X^n \quad (6)$$

ein Polynom vom Grad kleiner als  $L$ . Aus (5) und (6) folgt

$$f(X) \frac{1 - X^t}{\text{ggT}(1 - X^t, S^t(X))} = \left( 1 - \sum_{l=0}^{L-1} c_l X^{L-l} \right) \frac{S^t(X)}{\text{ggT}(1 - X^t, S^t(X))}.$$

Da

$$\frac{S^t(X)}{\text{ggT}(1 - X^t, S^t(X))} \quad \text{und} \quad \frac{1 - X^t}{\text{ggT}(1 - X^t, S^t(X))}$$

teilerfremd sind, ist  $\frac{S^t(X)}{\text{ggT}(1 - X^t, S^t(X))}$  ein Teiler von  $f(X)$  und insbesondere

$$L - 1 \geq \text{grad}(f) \geq t - 1 - \text{grad}(\text{ggT}(1 - X^t, S^t(X))),$$

woraus die Behauptung folgt. □

**Hilfssatz 4** Sei  $(l_n)$  die Legendre-Folge,

$$S^p(X) := \sum_{n=0}^{p-1} l_n X^n$$

und  $\beta \neq 1$  eine  $p$ -te Einheitswurzel modulo 2 (d.h. eine Lösung der Gleichung  $X^p \equiv 1 \pmod{2}$  in einem Erweiterungskörper). Dann gilt

$$S^p(\beta^q) \equiv S^p(\beta) \pmod{2}, \quad \left(\frac{q}{p}\right) = 1,$$

$$S^p(\beta^m) \equiv 1 + S^p(\beta) \pmod{2}, \quad \left(\frac{m}{p}\right) = -1,$$

und

$$S^p(\beta) \pmod{2} \in \{0, 1\} \text{ genau dann, wenn } \left(\frac{2}{p}\right) = 1.$$

Beweis: Für  $q$  mit  $\left(\frac{q}{p}\right) = 1$  haben wir

$$S^p(\beta^q) \equiv \sum_{n=0}^{p-1} s_n \beta^{nq} = \sum_{\left(\frac{n}{p}\right)=-1} \beta^{nq} \equiv \sum_{\left(\frac{n}{p}\right)=-1} \beta^n \equiv S(\beta) \pmod{2}$$

und für  $m$  mit  $\left(\frac{m}{p}\right) = -1$

$$\begin{aligned} S^p(\beta^m) &\equiv \sum_{\left(\frac{n}{p}\right)=-1} \beta^{nm} \equiv \sum_{\left(\frac{n}{p}\right)=1} \beta^n \\ &\equiv \sum_{n=1}^{p-1} (1 + s_n) \beta^n \equiv \frac{\beta^p - \beta}{\beta - 1} + S(\beta) \equiv 1 + S(\beta) \pmod{2}. \end{aligned}$$

Außerdem gilt  $S^p(\beta) \pmod{2} \in \{0, 1\}$  genau dann, wenn  $S^p(\beta)^2 \equiv S^p(\beta^2) \equiv S^p(\beta) \pmod{2}$ . Dies ist genau dann der Fall, wenn  $\left(\frac{2}{p}\right) = 1$ . □

**Hilfssatz 5**

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}.$$

Beweis: Sei  $\xi$  eine primitive achte Einheitswurzel modulo  $p$  (d. h.  $\xi^8 \equiv 1 \pmod{p}$  aber  $\xi^4 \not\equiv 1 \pmod{p}$ ). Dann folgt wegen  $\xi^4 \equiv -1 \pmod{p}$  sofort  $\xi^2 + \xi^{-2} \equiv 0 \pmod{p}$ , damit

$$(\xi + \xi^{-1})^2 \equiv \xi^2 + \xi^{-2} + 2 \equiv 2 \pmod{p}$$

und schließlich wegen  $(\xi + \xi^{-1})^p \equiv \xi^p + \xi^{-p} \pmod{p}$  im Fall  $p \equiv \pm 1 \pmod{8}$ , dass

$$\left(\frac{2}{p}\right) \equiv 2^{(p-1)/2} \equiv (\xi + \xi^{-1})^{p-1} \equiv \frac{\xi^p + \xi^{-p}}{\xi + \xi^{-1}} \equiv 1 \pmod{p},$$

und analog im Fall  $p \equiv \pm 3 \pmod{8}$ , dass

$$\left(\frac{2}{p}\right) \equiv -1 \pmod{p},$$

woraus der Hilfssatz folgt. □

Beweis von Satz 6: Nach Hilfssatz 3 gilt

$$L = p - |\{j : S^p(\beta^j) \equiv 0 \pmod{2}, 0 \leq j \leq p-1\}|.$$

Zunächst gilt

$$S^p(1) \equiv \sum_{\left(\frac{n}{p}\right)=-1} 1 \equiv \frac{p-1}{2} \equiv \begin{cases} 0 \pmod{2}, & p \equiv 1 \pmod{4}, \\ 1 \pmod{2}, & p \equiv 3 \pmod{4}. \end{cases}$$

Ist  $\left(\frac{2}{p}\right) = 1$  und somit  $p \equiv 1$  oder  $7 \pmod{8}$ , so ist  $S^p(\beta) \pmod{2}$  entweder 0 oder 1. Im ersten Fall gilt  $S^p(\beta^q) \equiv 0 \pmod{2}$  für die  $(p-1)/2$  modulo  $p$  verschiedenen Zahlen mit  $\left(\frac{q}{p}\right) = 1$  und im zweiten Fall  $S^p(\beta^m) \equiv 0 \pmod{2}$  für die  $m$  mit  $\left(\frac{m}{p}\right) = -1$ , woraus der Satz folgt. □

**Hilfssatz 6** *Das lineare Komplexitätsprofil  $L(s_n, N)$  modulo  $p$  einer Folge  $(s_n)$  mit linearer Komplexität  $L$  erfüllt*

$$L(s_n, N) \geq \min(N + 1 - L, L), \quad N \geq 1.$$

Beweis: Wir nehmen an, dass  $L(s_n, N) < L$ . Dann existiert eine ganze Zahl  $k \geq 1$  mit

$$L(s_n, N) = L(s_n, N + 1) = \dots = L(s_n, N + k - 1) < L(s_n, N + k) \leq L(s_n) = L.$$

Nach Satz 4 gilt

$$L(s_n, N + k) = N + k - L(s_n, N).$$

Falls  $L(s_n, N) < N + 1 - L$ , so erhalten wir

$$L \geq L(s_n, N + k) = N + k - L(s_n, N) > N + k - (N + 1 - L) = L + k - 1 \geq L$$

und somit einen Widerspruch.  $\square$

Für große  $N$  liefern Satz 6 und Hilfssatz 6 eine Verbesserung von Satz 5.

### 3.3 Erwartungswert

**Hilfssatz 7** *Ist  $L(s_n, N) \leq N/2$ , dann existiert eine eindeutige lineare Rekursion kürzester Länge für die ersten  $N$  Folgenglieder von  $(s_n)$ , d.h. für  $L = L(s_n, N)$  sind die Koeffizienten  $c_0, \dots, c_{L-1}$  in (4) eindeutig bestimmt.*

Beweis: Setze  $L := L(s_n, N)$ . Angenommen, es gäbe zwei verschiedene Rekursionsgleichungen der Form (4) für die ersten  $N$  Folgenglieder von  $(s_n)$  mit Koeffizienten  $c_0, \dots, c_{L-1}$  bzw.  $d_0, \dots, d_{L-1}$ . Sei

$$k := \max\{j \mid c_j \not\equiv d_j \pmod{p}\},$$

so dass  $0 \leq k \leq L - 1$ . Ein Vergleich der rechten Seiten in (4) ergibt

$$(c_0 - d_0)s_n + \dots + (c_k - d_k)s_{n+k} \equiv 0 \pmod{p}, \quad 0 \leq n \leq N - L - 1.$$

Da  $c_k - d_k \not\equiv 0 \pmod{p}$  ist dies eine lineare Rekursionsgleichung der Länge  $k$  für die ersten  $N - (L - k)$  Folgenglieder von  $(s_n)$  und daher

$$L(s_n, N - (L - k)) \leq k. \tag{7}$$

Daher gilt  $L(s_n, N - (L - k)) < L(s_n, N)$  und es existiert ein kleinster positiver Index  $j \leq L - k$  mit  $L(s_n, N - (L - k) + j) > L(s_n, N - (L - k))$ . Anwendung des zweiten Teiles von Satz 4 ergibt

$$L(s_n, N - (L - k) + j) = N - (L - k) + j - L(s_n, N - (L - k)).$$

Aus (7) und  $L \leq N/2$  bekommen wir

$$L(s_n, N - (L - k) + j) \geq N - L + j \geq \frac{N}{2} + j.$$

Wegen  $N - (L - k) + j \leq N$  erhalten wir  $L(s_n, N) = L \geq N/2 + j$  im Widerspruch zu  $L \leq N/2$ .  $\square$

Für eine Primzahl  $p$  bezeichnen wir ab jetzt mit  $\mathbb{F}_p := \{0, 1, \dots, p-1\}$  den Körper mit  $p$  Elementen mit Addition und Multiplikation modulo  $p$ .

Sei  $A(N, L)$  die Anzahl der Folgenabschnitte  $s_0, \dots, s_{N-1} \in \mathbb{F}_p$  der Länge  $N$  mit  $L(s_n, N) = L$ .

**Hilfssatz 8**

$$A(N, 0) = 1$$

und

$$A(N, L) = (p - 1)p^{\min(2L-1, 2N-2L)}$$

für  $1 \leq L \leq N$ .

Beweis: Wir beweisen die Aussage mit vollständiger Induktion über  $N$ . Für  $N = 1$  ist die Aussage trivial. Wir nehmen an das die Behauptung für  $N$  gelte und leiten die Formel für  $N + 1$  her.

Sei zunächst  $L \leq N/2$ .

Nach Satz 4 ist  $L(s_n, N + 1) \leq N/2$  nur möglich, wenn  $L(s_n, N + 1) = L(s_n, N)$ . D.h. zu einem Folgenabschnitt  $(s_0, \dots, s_{N-1})$  mit  $L(s_n, N) = L$  existiert eine eindeutige lineare Rekursionsgleichung, die sich mit genau einem  $s_N$  fortsetzen läßt. Wir haben also

$$A(N + 1, L) = A(N, L)$$

und die Behauptung folgt nach Induktionsvoraussetzung.

Für  $L > N/2$  haben wir nach Satz 4

$$L = L(s_n, N + 1) = L(s_n, N) = \dots = L(s_n, L + j) = L + j - L = j$$

mit einem  $0 \leq j \leq N + 1 - L$ . Somit erhalten wir

$$\begin{aligned} & A(N + 1, L) \\ &= (p - 1)A(N, N + 1 - L) + (p - 1)pA(N, N - L) + \dots \\ & \quad + (p - 1)p^{N-L}A(L, 1) + (p - 1)p^{N-L+1}A(L, 0) \\ &= (p - 1)^2p^{2N+1-2L} + (p - 1)^2p^{2N-2L} + \dots + (p - 1)^2p^{N-L+1} + (p - 1)p^{N-L+1}, \end{aligned}$$

woraus die Behauptung folgt.  $\square$

**Satz 7** Der Erwartungswert für  $L(s_n, N)$  ist

$$\frac{1}{p^N} \sum_{L=0}^N A(N, L)L = \begin{cases} \frac{N}{2} + \frac{p}{(p+1)^2} - p^{-N} \frac{N(p+1)+p}{(p+1)^2} & \text{für gerade } N, \\ \frac{N}{2} + \frac{p^2+1}{2(p+1)^2} - p^{-N} \frac{N(p+1)+p}{(p+1)^2} & \text{für ungerade } N. \end{cases}$$

Beweis: Nach dem vorherigen Hilfssatz gilt

$$\begin{aligned} & \sum_{L=1}^N A(N, L)L \\ &= (p - 1) \sum_{L=1}^N p^{\min(2L-1, 2N-2L)} L \end{aligned}$$

$$\begin{aligned}
&= (p-1) \left( \sum_{L=1}^{\lfloor N/2 \rfloor} p^{2L-1} L + \sum_{L=\lfloor N/2 \rfloor+1}^N p^{2N-2L} L \right) \\
&= (p-1) \left( \sum_{L=1}^{\lfloor N/2 \rfloor} p^{2L-1} \sum_{k=1}^L 1 + \sum_{L=\lfloor N/2 \rfloor+1}^N p^{2N-2L} \left( \lfloor N/2 \rfloor + \sum_{k=\lfloor N/2 \rfloor+1}^L 1 \right) \right) \\
&= (p-1) \left( \sum_{k=1}^{\lfloor N/2 \rfloor} \sum_{L=k}^{\lfloor N/2 \rfloor} p^{2L-1} + \left\lfloor \frac{N}{2} \right\rfloor \sum_{L=\lfloor N/2 \rfloor+1}^N p^{2N-2L} + \sum_{k=\lfloor N/2 \rfloor+1}^N \sum_{L=k}^N p^{2N-2L} \right) \\
&= \sum_{k=1}^{\lfloor N/2 \rfloor} \frac{p^{2\lfloor N/2 \rfloor+2} - p^{2k}}{p^2 + p} + \left\lfloor \frac{N}{2} \right\rfloor \frac{p^{2(N-\lfloor N/2 \rfloor)} - 1}{p+1} + \sum_{k=\lfloor N/2 \rfloor+1}^N \frac{p^{2(N-k+1)} - 1}{p+1} \\
&= \left\lfloor \frac{N}{2} \right\rfloor \frac{p}{p+1} p^{2\lfloor N/2 \rfloor} - \frac{p}{p+1} \frac{p^{2\lfloor N/2 \rfloor} - 1}{p^2 - 1} + \left\lfloor \frac{N}{2} \right\rfloor \frac{p^{2(N-\lfloor N/2 \rfloor)} - 1}{p+1} \\
&\quad + \frac{p^{2(N-\lfloor N/2 \rfloor+1)} - p^2}{(p+1)(p^2-1)} - \frac{N - \lfloor N/2 \rfloor}{p+1},
\end{aligned}$$

woraus die Behauptung folgt.  $\square$

## 4 Gittertest

**Definition 4** Für  $s \geq 1$  und  $N \geq 2$  besteht ein Folge  $(s_n)$  über  $\mathbb{F}_p$  den  $s$ -dimensionalen  $N$ -Gittertest, wenn die Vektoren  $\{\mathbf{s}_n - \mathbf{s}_0 \mid 1 \leq n \leq N - s\}$  den ganzen Raum  $\mathbb{F}_p^s$  aufspannen, wobei

$$\mathbf{s}_n = (s_n, s_{n+1}, \dots, s_{n+s-1}), \quad 0 \leq n \leq N - s.$$

Falls  $(s_n)$  den  $s$ -dimensionalen  $N$ -Gittertest besteht so auch alle  $s'$ -dimensionalen  $N$ -Gittertests mit  $s' \leq s$  und falls  $(s_n)$  den  $s$ -dimensionalen  $N$ -Gittertest nicht besteht so auch nicht alle  $s'$ -dimensionalen  $N$ -Gittertest mit  $s' \geq s$ . Das größte  $s$ , für das  $(s_n)$  den  $s$ -dimensionalen  $N$ -Gittertest besteht bezeichnen wir mit  $S(s_n, N)$ .

**Hilfssatz 9** (i)  $S(s_n, N) \leq S(s_n, N+1) \leq S(s_n, N) + 1$ .

(ii)  $S(s_n, N) \leq N/2$ .

Beweis: (i) Falls für eine natürliche Zahl  $s$  die  $s$ -dimensionalen Vektoren  $\mathbf{s}_n - \mathbf{s}_0$ ,  $n = 1, \dots, N - s$ , den Raum  $\mathbb{F}_p^s$  aufspannen, so bleibt dies wahr, wenn wir den Vektor  $\mathbf{s}_{N+1-s} - \mathbf{s}_0$  dazu nehmen und wir erhalten  $S(s_n, N) \leq S(s_n, N+1)$ .

Setze  $S := S(s_n, N+1)$ . Der Rank der Matrix

$$\begin{pmatrix}
s_1 - s_0 & \cdots & s_{N+1-S} - s_0 \\
\vdots & & \vdots \\
s_S - s_{S-1} & \cdots & s_N - s_{S-1}
\end{pmatrix}$$

ist  $S$ , d.h. die  $S$  Zeilen dieser Matrix sind linear unabhängig. Also sind auch die ersten  $S-1$  Zeilen linear unabhängig, woraus  $S(s_n, N) \geq S-1 = S(s_n, N+1) - 1$  folgt.

(ii) Falls  $N-s$  Vektoren  $\mathbb{F}_p^s$  aufspannen, so gilt  $N-s \geq s$  und daher  $S(s_n, N) \leq N/2$ .  $\square$

## 4.1 Lineare Komplexität und Gittertest

**Satz 8** *Es gilt entweder*

$$S(s_n, N) = \min(L(s_n, N), N+1 - L(s_n, N))$$

oder

$$S(s_n, N) = \min(L(s_n, N), N+1 - L(s_n, N)) - 1.$$

Beweis: 1.  $S(s_n, N) \leq L(s_n, N)$ :

Setze  $L := L(s_n, N)$ . Wir dürfen  $L \leq N/2$  annehmen. Sei

$$s_{n+L} \equiv c_0 s_n + c_1 s_{n+1} + \dots + c_{L-1} s_{n+L-1} \pmod{p}, \quad (8)$$

$0 \leq n \leq N-L-1$ . Wir zeigen, dass  $(s_n)$  den  $(L+1)$ -dimensional  $N$ -Gittertest nicht besteht. Für  $\mathbf{s}_n = (s_n, \dots, s_{n+L})$ ,  $n = 0, \dots, N-L-1$ , haben wir nach (8)

$$\underline{c} := (c_0, \dots, c_{L-1}, -1) \perp \mathbf{s}_n$$

bezüglich des Standard inneren Produktes in  $\mathbb{F}_p^{L+1}$ . Daher gilt  $\underline{c} \perp (\mathbf{s}_n - \mathbf{s}_0)$ ,  $n = 1, \dots, N-L-1$ . Wegen  $\underline{c} \neq \underline{0}$  schließen wir, dass die lineare Hülle  $V$  von  $\{\mathbf{s}_n - \mathbf{s}_0 \mid 1 \leq n \leq N-L-1\}$  nicht  $\mathbb{F}_p^{L+1}$  ist. (Grund:  $\dim V < \dim V + \dim V^\perp = L+1$ .)

2.  $S(s_n, N) \leq N+1 - L(s_n, N)$ :

Setze  $S := S(s_n, N)$ . Dann spannen die  $S$ -dimensionalen Vektoren  $\mathbf{s}_1 - \mathbf{s}_0, \dots, \mathbf{s}_{N-S} - \mathbf{s}_0$  den Raum  $\mathbb{F}_p^S$  auf. Daher existieren  $c_1, \dots, c_{N-S} \in \mathbb{F}_p$  mit

$$c_1(\mathbf{s}_1 - \mathbf{s}_0) + \dots + c_{N-S}(\mathbf{s}_{N-S} - \mathbf{s}_0) \equiv \mathbf{s}_{N+1-S} \pmod{p}.$$

Umordnung der linken Seite der Gleichung ergibt

$$-(c_1 + \dots + c_{N-S})\mathbf{s}_0 + c_1\mathbf{s}_1 + \dots + c_{N-S}\mathbf{s}_{N-S} \equiv \mathbf{s}_{N+1-S} \pmod{p}$$

und wir erhalten  $L(s_n, N+1) \leq N+1 - S$  bzw.

$$S(s_n, N) \leq N+1 - L(s_n, N+1) \leq N+1 - L(s_n, N).$$

Für die untere Schranke benötigen wir einige Hilfssätze.

**Hilfssatz 10** Ist  $L := L(s_n, N) \leq N/2$  und

$$s_{n+L} \equiv c_0 s_n + c_1 s_{n+1} + \dots + c_{L-1} s_{n+L-1} \pmod{p}, \quad 0 \leq n \leq N - L - 1, \quad (9)$$

die kürzeste lineare Rekursionsgleichung für die ersten  $N$  Folgglieder von  $(s_n)$ , so gilt

$$S(s_n, N) < L(s_n, N)$$

genau dann, wenn

$$c_0 + c_1 + \dots + c_{L-1} \equiv 1 \pmod{p}.$$

Beweis: Zunächst zeigen wir, dass die Bedingung  $c_0 + c_1 + \dots + c_{L-1} \equiv 1 \pmod{p}$  hinreichend ist. Wir addieren

$$c_0 s_{n+1} + (c_0 + c_1) s_{n+2} + \dots + (c_0 + \dots + c_{L-2}) s_{n+L-1}$$

auf beiden Seiten von (9) und bekommen

$$\begin{aligned} c_0 s_{n+1} + (c_0 + c_1) s_{n+2} + \dots + (c_0 + \dots + c_{L-1}) s_{n+L} &\equiv \\ c_0 s_n + (c_0 + c_1) s_{n+1} + \dots + (c_0 + \dots + c_{L-1}) s_{n+L-1} &\pmod{p}. \end{aligned}$$

Das heißt

$$\underline{0} \neq (c_0, c_0 + c_1, \dots, c_0 + \dots + c_{L-1}) \perp (\mathbf{s}_{n+1} - \mathbf{s}_n), \quad 0 \leq n \leq N - L - 1,$$

und  $(s_n)$  besteht den  $L$ -dimensionalen  $N$ -Gittertest nicht, d.h.  $S(s_n, N) < L$ , da

$$\langle \{\mathbf{s}_n - \mathbf{s}_0 \mid 1 \leq n \leq N - s\} \rangle = \langle \{\mathbf{s}_n - \mathbf{s}_{n-1} \mid 1 \leq n \leq N - s\} \rangle,$$

wobei  $\langle M \rangle$  die lineare Hülle von  $M$  bezeichnet.

Jetzt beweisen wir die Notwendigkeit der Bedingung. Wegen  $S(s_n, N) < L$  existiert ein  $L$ -dimensionaler Vektor  $(d_0, \dots, d_{L-1})$  mit

$$\underline{0} \neq (d_0, \dots, d_{L-1}) \perp (\mathbf{s}_{n+1} - \mathbf{s}_n), \quad 0 \leq n \leq N - L - 1.$$

Zunächst nehmen wir  $d_{L-1} \neq 0$  an. Aus der obigen Orthogonalitätsrelation bekommen wir eine lineare Rekursionsgleichung der Länge  $L$ :

$$s_{n+L} \equiv d_{L-1}^{-1} (d_0 s_n + (d_1 - d_0) s_{n+1} + \dots + (d_{L-1} - d_{L-2}) s_{n+L-1}) \pmod{p},$$

$0 \leq n \leq N - L - 1$ . Da nach Hilfssatz 7 für  $L(s_n, N) \leq N/2$  die zugehörige (normierte) lineare Rekursionsgleichung minimaler Länge eindeutig ist, bekommt man

$$c_0 + c_1 + \dots + c_{L-1} \equiv d_{L-1}^{-1} (d_0 + (d_1 - d_0) + \dots + (d_{L-1} - d_{L-2})) \equiv 1 \pmod{p}.$$

Schließlich beweisen wir, dass  $d_{L-1} = 0$  der Bedingung  $L(s_n, N) \leq N/2$  widerspricht. Sei  $k := \max\{j \mid d_j \neq 0\} < L - 1$ . Dann bekommen wir wieder von der

Orthogonalitätsrelation eine lineare Rekursionsgleichung der Länge  $k + 1$  für die ersten  $N - (L - 1 - k)$  Folgenglieder von  $(s_n)$  und daher

$$L(s_n, N - (L - 1 - k)) \leq k + 1 < L.$$

Jetzt verfahren wir wie im Beweis von Hilfssatz 7 im Teil hinter (7) und erhalten  $L(s_n, N) = L \geq N/2 + j$  mit einer natürlichen Zahl  $j$  im Widerspruch zu  $L \leq N/2$ .  $\square$

**Korollar 1** Setze  $L := L(s_n, N)$ . Falls  $S(s_n, N) < L \leq N/2$ , so gilt

$$\dim \langle \{s_n - s_0 \mid 1 \leq n \leq N - L\} \rangle = L - 1$$

und  $(s_L - s_{L-1}, \dots, s_{N-1} - s_{L-1})$  ist eine Linearkombination der Vektoren

$$(s_{i+1} - s_i, \dots, s_{N-L+i} - s_i), \quad i = 0, \dots, L - 2.$$

Beweis: Die Behauptung folgt sofort aus  $d_{L-1} \neq 0$  für alle

$$(d_0, \dots, d_{L-1}) \in \langle \{s_n - s_0 \mid 1 \leq n \leq N - L\} \rangle^\perp \setminus \{\mathbf{0}\},$$

was wir aus dem Beweis von Hilfssatz 10 erhalten.  $\square$

**Hilfssatz 11** Ist  $L(s_n, N + 1) \leq (N + 1)/2$ , so gilt

$$S(s_n, N) \geq L(s_n, N + 1) - 1.$$

Beweis: Setze  $L := L(s_n, N + 1)$ . Falls  $(s_n)$  den  $L$ -dimensionalen  $(N + 1)$ -Gittertest besteht, d.h.  $S(s_n, N + 1) \geq L(s_n, N + 1)$ , so gilt nach Hilfssatz 9  $S(s_n, N) \geq L(s_n, N + 1) - 1$ .

Falls  $(s_n)$  den  $L$ -dimensionalen  $(N + 1)$ -Gittertest nicht besteht, so liefert die Annahme  $L(s_n, N + 1) \leq (N + 1)/2$  mit Korollar 1, dass der Rank der Matrix

$$A := \begin{pmatrix} s_1 - s_0 & \cdots & s_{N+1-L} - s_0 \\ \vdots & & \vdots \\ s_L - s_{L-1} & \cdots & s_N - s_{L-1} \end{pmatrix}$$

gleich  $L - 1$  ist und die letzte Zeile von  $A$  eine Linearkombination der ersten  $L - 1$  Zeilen ist. Also ist der Rank der Matrix, die aus den ersten  $L - 1$  Zeilen von  $A$  besteht gleich  $L - 1$ . Das bedeutet, dass  $(s_n)$  den  $(L - 1)$ -dimensionalen  $N$ -Gittertest besteht, d.h.  $S(s_n, N) \geq L(s_n, N + 1) - 1$ .  $\square$

**Hilfssatz 12** Ist  $L(s_n, N + 1) > (N + 1)/2$ , so gilt

$$S(s_n, N) \geq N - L(s_n, N + 1).$$

Beweis: Sei  $L(s_n, N + 1) = (N + k + 1)/2$  mit  $k \geq 1$ . Nach Satz 4 gilt

$$L(s_n, N + 1) = L(s_n, N + 2) = \dots = L(s_n, N + k + 1) = \frac{N + k + 1}{2}.$$

Nach Hilfssatz 9 haben wir  $S(s_n, N) \geq S(s_n, N + k) - k$  und wegen  $L(s_n, N + k + 1) = (N + k + 1)/2$  dürfen wir Hilfssatz 11 anwenden, um  $S(s_n, N + k) \geq L(s_n, N + k + 1) - 1$  zu erhalten. Aus diesen Ungleichungen folgt

$$\begin{aligned} S(s_n, N) &\geq L(s_n, N + k + 1) - k - 1 = \frac{N + k + 1}{2} - k - 1 \\ &= N - \left( \frac{N + k + 1}{2} \right) = N - L(s_n, N + 1). \end{aligned}$$

□

Fortsetzung des Beweises von Satz 8:

3. Aus  $L(s_n, N) \leq (N + 1)/2$  folgt  $S(s_n, N) \geq L(s_n, N) - 1$ :

Ist  $L(s_n, N) \leq N/2$ , so erhalten wir Hilfssatz 11  $S(s_n, N) \geq S(s_n, N - 1) \geq L(s_n, N) - 1$ .

Ist  $L(s_n, N) = (N + 1)/2$ , so gilt  $L(s_n, N + 1) = (N + 1)/2$  und die Behauptung folgt aus Hilfssatz 11.

4. Aus  $L(s_n, N) > (N + 1)/2$  folgt  $S(s_n, N) \geq N - L(s_n, N)$ :

Aus  $L(s_n, N) > (N + 1)/2$  folgt  $L(s_n, N) = L(s_n, N + 1) > (N + 1)/2$  und Hilfssatz 12 liefert die untere Schranke  $N - L(s_n, N)$  für  $S(s_n, N)$ . □

Beispiel:  $(s_n)$ :

$$1 \ 1 \ 1 \ 0 \ -1 \ -1 \ 0 \ 1 \ 0.$$

Die ersten drei Folgeglieder genügen  $s_{n+1} = s_n$ , weswegen  $L(s_n, 2) = L(s_n, 3) = 1$  und Hilfssatz 10 liefert  $S(s_n, 2) = S(s_n, 3) = 0$ .

Dann wächst  $L$  zu  $L(s_n, 4) = \dots = L(s_n, 8) = 3$  und die Rekursionsgleichung der für die ersten acht Folgeglieder ist  $s_{n+3} = -s_{n+1} + s_{n+2}$ . Hilfssatz 10 liefert  $S(s_n, 6) = S(s_n, 7) = S(s_n, 8) = 3$ . Wegen  $S(s_n, N) \leq S(s_n, N + 1) \leq S(s_n, N) + 1$  (Hilfssatz 9) ergibt das  $S(s_n, 4) = 1$  und  $S(s_n, 5) = 2$ .

Die gesamte Folge erfüllt keine Rekursionsgleichung der Länge 3. Daher gilt  $L(s_n, 9) = 6$  und eine einfache Rechnung zeigt  $S(s_n, 9) = 4$ .

$N$	2	3	4	5	6	7	8	9
$L(s_n, N)$	1	1	3	3	3	3	3	6
$S(s_n, N)$	0	0	1	2	3	3	3	4

**Hilfssatz 13** Sei  $(l_N)$  eine Folge mit  $l_1 \leq 0$  und  $l_N \leq l_{N-1} + 1$  für  $N \geq 2$ . Gilt

$$L(s_n, N) \geq l_N \quad \text{für } N \geq 2,$$

so haben wir

$$L(s_n, N) \leq N - l_{N-1} \quad \text{für } N \geq 2.$$

Beweis: Für  $N = 2$  gilt

$$L(s_n, 2) \leq 2 \leq 2 - l_1$$

und für  $N > 2$  nach Satz 4

$$\begin{aligned} L(s_n, N) &\leq \max(L(s_n, N-1), N - L(s_n, N-1)) \\ &\leq \max(N-1 - l_{N-2}, N - l_{N-1}) = N - l_{N-1} \end{aligned}$$

nach Induktionsvoraussetzung. □

**Satz 9** *Unter den Voraussetzungen von Hilfssatz 13 gilt*

$$l_N - 1 \leq S(s_n, N) \leq \frac{N}{2} \quad \text{für } N \geq 2.$$

Beweis: Kombiniert man Satz 8 und Hilfssatz 13, erhält man

$$\begin{aligned} S(s_n, N) &\geq \min(L(s_n, N), N + 1 - L(s_n, N)) - 1 \\ &\geq \min(l_N, l_{N-1} + 1) - 1 = l_N - 1. \end{aligned}$$

$S(s_n, N) \leq N/2$  folgt direkt aus der Definition. □

## 4.2 Expliziter Inversionsgenerator

**Satz 10** *Seien  $a, b \in \mathbb{F}_p$ ,  $a \neq 0$  und sei  $(y_n)$  die durch  $y_n \equiv \overline{an + b} \pmod{p}$ ,  $n \geq 0$ , definierte Folge, wobei  $\bar{x} = x^{-1}$ ,  $x \not\equiv 0 \pmod{p}$  und  $\bar{0} = 0$  ist. Dann gilt*

$$L(y_n, N) \geq \min\left(\frac{N-1}{3}, \frac{p-1}{2}\right).$$

Beweis: Gelte

$$y_{n+L} \equiv c_{L-1}y_{n+L-1} + \dots + c_0y_n \pmod{p}, \quad 0 \leq n \leq N - L - 1, \quad (10)$$

mit  $c_0, \dots, c_{L-1} \in \mathbb{F}_p$ . Wir können  $L \leq p-1$  annehmen. Wenigstens

$$\min(p, N-L) - (L+1)$$

verschiedene  $n$  erfüllen  $0 \leq n \leq \min(N-L, p) - 1$  und

$$a(n+t) + b \not\equiv 0 \pmod{p} \quad \text{für alle } 0 \leq t \leq L.$$

Für diese  $n$  ist (10) äquivalent zu

$$(a(n+L) + b)^{-1} \equiv c_{L-1}(a(n+L-1) + b)^{-1} + \dots + (an + b)^{-1} \pmod{p}.$$

Multiplikation mit

$$\prod_{j=0}^L (a(n+j) + b)$$

ergibt

$$\prod_{j=0}^{L-1} (a(n+j) + b) \equiv \sum_{l=0}^{L-1} c_l \prod_{\substack{j=0 \\ j \neq l}}^L (a(n+j) + b) \pmod{p}$$

für alle  $n$  mit  $0 \leq n \leq N - L - 1$  und  $a(n+t) + b \not\equiv 0 \pmod{p}$  für alle  $0 \leq t \leq L$ . Daher hat das Polynom

$$F(X) := - \prod_{j=0}^{L-1} (a(X+j) + b) + \sum_{l=0}^{L-1} c_l \prod_{\substack{j=0 \\ j \neq l}}^L (a(X+j) + b)$$

vom Grad höchstens  $L$  wenigstens  $\min(p, N - L) - (L + 1)$  Nullstellen. Wegen

$$F(-a^{-1}b - L) \equiv -a^L \prod_{j=0}^{L-1} (j - L) \not\equiv 0 \pmod{p}$$

ist  $F(X)$  nicht das Nullpolynom und wir erhalten

$$L \geq \text{grad}(F) \geq \min(p, N - L) - (L + 1),$$

woraus die Behauptung folgt.  $\square$

## Korollar 2

$$S(y_n, N) \geq \min\left(\frac{N-4}{3}, \frac{p-3}{2}\right).$$

Beweis: Satz 9 und Satz 10.  $\square$

## 4.3 Rekursiver Inversionsgenerator

Wir betrachten die folgende Folge rationaler Funktionen über  $\mathbb{F}_p$ :

$$H_0(X) := X, \quad H_j(X) := H_{j-1}(aX^{-1} + b), \quad j = 1, 2, \dots, \quad (11)$$

mit Koeffizienten  $1 \leq a \leq p - 1$ ,  $0 \leq b \leq p - 1$ . Offensichtlich ist diese Folge rein periodisch. Bezeichne  $T$  die kleinste Periode. Wir beobachten, dass  $H_j(X) = f_j(X)/g_j(X)$  nichtkonstante rationale Funktionen mit Polynomen  $f_j, g_j \in \mathbb{F}_p[X]$  und  $\max\{\text{grad}(f_j), \text{grad}(g_j)\} = 1$ , d.h.  $\text{ggT}(f_j, g_j) = 1$ , sind. (Wir können jeder rationalen Funktion der Form  $\frac{\alpha X + \beta}{\gamma X + \delta}$  die Matrix  $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$  zuordnen.  $H_j$  entspricht dann die reguläre Matrix  $\begin{pmatrix} b & a \\ 1 & 0 \end{pmatrix}^j$ .)

**Hilfssatz 14** Für jedes  $1 \leq k < T$  und  $a_0, \dots, a_{k-1} \in \mathbb{F}_p$  haben wir

$$H_k(X) \neq a_{k-1}H_{k-1}(X) + \dots + a_0H_0(X).$$

Beweis: Mit vollständiger Induktion sieht man mit  $g_j(X) := c_jX + d_j$ , dass

$$f_j(X) = (bc_j + d_j)X + ac_j. \quad (12)$$

Insbesondere, wenn  $c_j = 0$  dann gilt  $H_j(X) = X$  und  $j = 0$  oder  $j \geq T$ . Es folgt ebenfalls, dass für alle ganzen Zahlen  $j_1$  und  $j_2$  mit  $0 \leq j_1 < j_2 < T$  gilt:

$$\text{ggT}(g_{j_1}, g_{j_2}) = 1.$$

Falls  $\text{ggT}(g_{j_1}, g_{j_2}) > 1$  für ein Paar  $0 \leq j_1 < j_2 < T$ , so gilt

$$g_{j_1}(X) = \kappa g_{j_2}(X) \quad \text{mit} \quad 1 \leq \kappa \leq p-1,$$

$f_{j_1}(X) = \kappa f_{j_2}(X)$  nach (12) und daher  $H_{j_1}(X) = H_{j_2}(X)$ . Das impliziert

$$H_{j_1+1}(X) = H_{j_1}(aX^{-1} + b) = H_{j_2}(aX^{-1} + b) = H_{j_2+1}(X)$$

und iterativ

$$H_{j_1+T-j_2}(X) = H_T(X) = H_0(X)$$

im Widerspruch zu  $0 \leq j_1 + T - j_2 < T$ .

Für  $k = 1$  impliziert eine Gleichung der Form

$$H_k(X) = a_0H_0(X) = a_0X,$$

dass

$$f_k(X) = a_0Xg_k(X).$$

Das irreduzible Polynom  $g_k(X)$  teilt also das Polynom  $f_k(X)$ . Da  $H_k(X)$  nicht konstant ist und  $\max\{\text{grad}(f_k), \text{grad}(g_k)\} = 1$ , bekommen wir  $\text{grad}(f_k) = 1$  und  $\text{grad}(g_k) = 0$  im Widerspruch zu  $c_k \neq 0$ .

Für  $k > 1$  haben wir eine Gleichung der Form

$$H_k(X) = a_{k-1}H_{k-1}(X) + \dots + a_0H_0(X).$$

Bereinigung der Nenner liefert eine Gleichung der Form

$$g_{k-1}(X)^{s_j} \cdots g_1(X)^{s_1} f_k(X) = g_k(X) \Psi_0(X)$$

mit nichtnegativen ganzen Zahlen  $s_1, \dots, s_j$  und einem nicht verschwindenden Polynom  $\Psi_0(X)$ . Der irreduzible Factor  $g_k(X)$  auf der rechten Seite obiger Gleichung taucht auf der linken Seite nicht auf, da  $\text{ggT}(f_k, g_k) = \text{ggT}(g_j, g_k) = 1$  für alle  $1 \leq j < k < T$ . Dieser Widerspruch vervollständigt den Beweis.  $\square$

**Satz 11** Die lineare Komplexität bei  $N$  einer Folge  $(v_n)$ , die von einem Inversionsgenerator der Periode  $t$  erzeugt wird, genügt

$$L(v_n, N) \geq \min\left(\frac{N-1}{3}, \frac{t-1}{2}\right).$$

Beweis: Sei  $L$  die kleinste natürliche Zahl mit

$$v_{n+L} \equiv a_{L-1}v_{n+L-1} + \dots + a_0v_n \pmod{p}, \quad 0 \leq n \leq N-L-1$$

mit  $a_0, \dots, a_{L-1} \in \mathbb{F}_p$ . Für  $j \geq 0$  bezeichne  $E_j$  die Menge der Pole der rationalen Funktionen  $H_0, \dots, H_j$  definiert durch (11). D.h.  $|E_j| \leq j$ . Dann gilt

$$v_{n+j} = H_j(v_n), \quad v_n \notin E_j,$$

und deshalb

$$H_L(v_n) = a_{L-1}H_{L-1}(v_n) + \dots + a_0H_0(v_n), \quad 0 \leq n \leq \min(N-L, t) - 1, \quad v_n \notin E_L. \quad (13)$$

Offensichtlich gilt  $T \geq t$ . Wir dürfen  $L < t \leq T$  annehmen. Dann ist nach Hilfssatz 14

$$H(X) = -H_L(X) + a_{L-1}H_{L-1}(X) + \dots + a_0H_0(X)$$

eine rationale Funktion, die nicht identisch Null ist. Die  $H_j(X) = f_j(X)/g_j(X)$  sind nicht konstante rationale Funktionen, wobei  $f_j(X), g_j(X) \in \mathbb{F}_p[X]$  mit

$$\max\{\text{grad}(f_j), \text{grad}(g_j)\} = 1.$$

Daher gilt  $H(X) = F(X)/G(X)$  mit Polynomen  $F(X), G(X) \in \mathbb{F}_p[X]$  und  $\text{grad}(F) \leq L+1$ . Andererseits gilt nach (13), dass das Polynom  $F(X)$  wenigstens  $\min\{N-2L, t-L\}$  Nullstellen hat, nämlich alle  $v_n$ ,  $0 \leq n \leq \min(N-L, t) - 1$ , mit  $v_n \notin E_L$ , und daher  $\text{grad}(F) \geq \min\{N-2L, t-L\}$ . Somit haben wir  $L \geq \min\{N-2L, t-L\} - 1$ .  $\square$

**Korollar 3**

$$S(v_n, N) \geq \min\left(\frac{N-4}{3}, \frac{t-3}{2}\right).$$

## 5 Diskrepanz

**Definition 5** Sei  $N \geq 1$  und  $P$  eine Menge von Punkten  $\mathbf{x}_0, \dots, \mathbf{x}_{N-1} \in [0, 1]^s$  im  $s$ -dimensionalen Einheitsintervall. Die  $s$ -dimensionale (extreme) Diskrepanz  $D_s(N, P)$  von  $P$  ist

$$D_s(N, P) := \sup_J \left| \frac{A_N(J)}{N} - V(J) \right|,$$

wobei das Supremum über alle Teilintervalle  $J$  von  $[0, 1]^s$  betrachtet wird,  $A_N(J)$  die Anzahl der Punkte  $\mathbf{x}_0, \dots, \mathbf{x}_{N-1}$  die in  $J$  liegen ist und  $V(J)$  das  $s$ -dimensionale Volumen von  $J$  ist.

Die Diskrepanz ist ein Maß für die Gleichverteilung der Punktmenge. Für die eindimensionale Diskrepanz gilt das folgende Ergebnis.

**Hilfssatz 15** *Ist  $P = \{x_0, \dots, x_{N-1}\}$  mit  $0 < x_0 < x_1 < \dots < x_{N-1} < 1$ , so gilt*

$$D_1(N, P) = \frac{1}{N} + \max_{1 \leq n \leq N} \left( \frac{n}{N} - x_{n-1} \right) - \min_{1 \leq n \leq N} \left( \frac{n}{N} - x_{n-1} \right).$$

Beweis: Setze  $x_{-1} := 0$  und  $x_N := 1$ . Dann gilt

$$\begin{aligned} D_1(N, P) &= \max_{0 \leq i \leq j \leq N} \sup_{\substack{x_{i-1} < u \leq x_i \\ x_{j-1} < v \leq x_j \\ u < v}} \left| \frac{A_N([u, v))}{N} - (v - u) \right| \\ &= \max_{0 \leq i \leq j \leq N} \sup_{\substack{x_{i-1} < u \leq x_i \\ x_{j-1} < v \leq x_j \\ u < v}} \left| \frac{j-i}{N} - (v - u) \right| \\ &= \max_{0 \leq i \leq j \leq N} \max \left( \left| \frac{j-i}{N} - (x_j - x_{i-1}) \right|, \left| \frac{j-i}{N} - (x_{j-1} - x_i) \right| \right). \end{aligned}$$

Mit  $r_n := (n+1)/N - x_n$  für  $-1 \leq n \leq N$  ergibt sich

$$\begin{aligned} D_1(N, P) &= \max_{0 \leq i \leq j \leq N} \max \left( \left| r_j - r_{i-1} - \frac{1}{N} \right|, \left| r_{j-1} - r_i + \frac{1}{N} \right| \right) \\ &= \max_{0 \leq i, j \leq N} \left| \frac{1}{N} + r_{i-1} - r_j \right|. \end{aligned}$$

Für das Maximum über alle  $i \neq 0$  und  $j \neq N$  ergibt sich das Ergebnis. Die Werte für  $i = 0$  oder  $j = N$  sind kleiner.  $\square$

**Korollar 4** *Für einen linearen Kongruenzgenerator  $(x_n)$  mit einem primitiven Element  $a$  von  $\mathbb{F}_p$  (d.h.  $a$  hat die Ordnung  $p-1$ ) gilt*

$$D_1(p-1, \{x_0, \dots, x_{p-2}\}) = \frac{2}{p}.$$

Beweis: Der lineare Kongruenzgenerator erzeugt die Punktmenge  $\{x_0, \dots, x_{p-2}\} = \{\frac{1}{p}, \dots, \frac{p-1}{p}\}$  und das Ergebnis folgt nach dem Hilfssatz.  $\square$

**Korollar 5** *Die Punktmenge*

$$P = \left\{ \frac{1}{2N}, \frac{3}{2N}, \dots, \frac{2N-1}{2N} \right\}$$

*hat minimale Diskrepanz*

$$D_1(N, P) = \frac{1}{N}.$$

## 5.1 Allgemeine Diskrepanzschranke

Der folgende Satz führt das Problem der Diskrepanzabschätzung auf das Problem der Abschätzung bestimmter Exponentialsummen zurück. Für zwei Vektoren  $\mathbf{x} = (x_1, \dots, x_s)$  und  $\mathbf{y} = (y_1, \dots, y_s)$  bezeichne

$$\mathbf{x} \cdot \mathbf{y} = \sum_{j=1}^s x_j y_j$$

das gewöhnliche innere Produkt.

Sei  $p \geq 2$  eine natürliche Zahl,

$$C(p) := (-p/2, p/2] \cap \mathbb{Z}, \quad C^*(p) := C(p) \setminus \{0\},$$

$$C_s(p) := C(p)^s \quad \text{und} \quad C_s^*(p) := C_s(p) \setminus \{\mathbf{0}\}.$$

**Satz 12** Sei

$$\mathbf{y}_0, \dots, \mathbf{y}_{N-1} \in \mathbb{F}_p^s.$$

Sei  $P$  die Punktmenge  $\mathbf{y}_0/p, \dots, \mathbf{y}_{N-1}/p$ . Dann gilt

$$D_s(N, P) < 1 - \left(1 - \frac{1}{p}\right)^s + \frac{1}{N} (2 + \ln p)^s \max_{\mathbf{h} \in C_s^*(p)} \left| \sum_{n=0}^{N-1} e_p(\mathbf{h} \cdot \mathbf{y}_n) \right|.$$

Zum Beweis benötigen wir ein vorbereitendes Ergebnis.

**Hilfssatz 16** Seien  $t_j, u_j \in [0, 1]$ ,  $j = 1, \dots, s$ , und  $v \in [0, 1]$  mit  $|t_j - u_j| \leq v$ ,  $j = 1, \dots, s$ , so gilt

$$\left| \prod_{j=1}^s t_j - \prod_{j=1}^s u_j \right| \leq 1 - (1 - v)^s.$$

Beweis: Für  $s = 1$  ist die Aussage trivial. Wir nehmen  $t_{s+1} \geq u_{s+1}$  an. Dann gilt nach Induktionsvoraussetzung

$$\begin{aligned} \left| \prod_{j=1}^{s+1} t_j - \prod_{j=1}^{s+1} u_j \right| &\leq (t_{s+1} - u_{s+1}) \prod_{j=1}^s t_j + u_{s+1} \left| \prod_{j=1}^s t_j - \prod_{j=1}^s u_j \right| \\ &\leq t_{s+1} - u_{s+1} + u_{s+1} (1 - (1 - v)^s) \\ &= t_{s+1} (1 - (1 - v)^s) + (t_{s+1} - u_{s+1}) (1 - v)^s \\ &\leq 1 - (1 - v)^s + v (1 - v)^s = 1 - (1 - v)^{s+1}, \end{aligned}$$

und somit die zu zeigende Behauptung. □

Beweis (Satz 12): Für  $\mathbf{k} = (k_1, \dots, k_s) \in \mathbb{Z}^s$  sei  $A(\mathbf{k})$  die Anzahl der  $0 \leq n \leq N-1$  mit  $\mathbf{y}_n \equiv \mathbf{k} \pmod{p}$ . (Die Kongruenz ist koordinatenweise zu verstehen.) Dann gilt

$$A(\mathbf{k}) = \sum_{n=0}^{N-1} \frac{1}{p^s} \sum_{\mathbf{h} \in C_s(p)} e_p(\mathbf{h} \cdot (\mathbf{y}_n - \mathbf{k}))$$

und somit

$$A(\mathbf{k}) - \frac{N}{p^s} = \frac{1}{p^s} \sum_{\mathbf{h} \in C_s^*(p)} e_p(-\mathbf{h} \cdot \mathbf{k}) \sum_{n=0}^{N-1} e_p(\mathbf{h} \cdot \mathbf{y}_n).$$

Sei jetzt

$$J := \prod_{j=1}^s [u_j, v_j)$$

ein Teilintervall von  $[0, 1)^s$ . Für jedes  $1 \leq j \leq s$  wählen wir das größte abgeschlossene Teilintervall von  $[u_j, v_j)$  der Form  $[a_j/p, b_j/p]$  mit ganzen Zahlen  $a_j \leq b_j$ . Existiert für irgendein  $j$  kein solches Teilintervall, so haben wir  $A_N(J) = 0$  und  $v_j - u_j < 1/p$  und daher

$$\left| \frac{A_N(J)}{N} - V(J) \right| = V(J) < \frac{1}{p} \leq 1 - \left(1 - \frac{1}{p}\right)^s.$$

Wir nehmen also jetzt an, dass für alle  $j$  solche Zahlen  $a_j, b_j$  existieren und erhalten

$$\begin{aligned} \frac{A_N(J)}{N} - V(J) &= \sum_{\substack{\mathbf{k} \\ a_j \leq k_j \leq b_j}} \left( \frac{A(\mathbf{k})}{N} - \frac{1}{p^s} \right) + \frac{1}{p^s} \prod_{j=1}^s (b_j - a_j + 1) - V(J) \\ &= \frac{1}{p^s} \sum_{\mathbf{h} \in C_s^*(p)} \left( \sum_{\substack{\mathbf{k} \\ a_j \leq k_j \leq b_j}} e_p(-\mathbf{h} \cdot \mathbf{k}) \right) \left( \frac{1}{N} \sum_{n=0}^{N-1} e_p(\mathbf{h} \cdot \mathbf{y}_n) \right) \\ &\quad + \frac{1}{p^s} \prod_{j=1}^s (b_j - a_j + 1) - V(J). \end{aligned}$$

Wegen

$$\left| \frac{b_j - a_j + 1}{p} - (v_j - u_j) \right| < \frac{1}{p}, \quad 1 \leq j \leq s,$$

liefert Hilfssatz 16

$$\begin{aligned} &\left| \frac{A_N(J)}{N} - V(J) \right| \\ &< 1 - \left(1 - \frac{1}{p}\right)^s + \frac{1}{p^s} \sum_{\mathbf{h} \in C_s^*(p)} \left| \sum_{\substack{\mathbf{k} \\ a_j \leq k_j \leq b_j}} e_p(\mathbf{h} \cdot \mathbf{k}) \right| \left| \frac{1}{N} \sum_{n=0}^{N-1} e_p(\mathbf{h} \cdot \mathbf{y}_n) \right|. \end{aligned}$$

Für fixes  $\mathbf{h} = (h_1, \dots, h_s) \in C_s^*(p)$  gilt

$$\left| \sum_{\substack{\mathbf{k} \\ a_j \leq k_j \leq b_j}} e_p(\mathbf{h} \cdot \mathbf{k}) \right| = \left| \sum_{\substack{\mathbf{k} \\ 0 \leq k_j \leq b_j - a_j}} e_p(\mathbf{h} \cdot \mathbf{k}) \right| = \prod_{j=1}^s \left| \sum_{k_j=0}^{b_j - a_j} e_p(h_j k_j) \right|.$$

Ist  $h_j = 0$ , so gilt

$$\left| \sum_{k_j=0}^{b_j - a_j} e_p(\mathbf{h} \cdot \mathbf{k}) \right| = b_j - a_j + 1 \leq p.$$

Damit ergibt sich

$$\begin{aligned} \sum_{\mathbf{h} \in C_s^*(p)} \left| \sum_{\substack{\mathbf{k} \\ a_j \leq k_j \leq b_j}} e_p(\mathbf{h} \cdot \mathbf{k}) \right| &< \sum_{\mathbf{h} \in C_s(p)} \prod_{j=1}^s \left| \sum_{k_j=0}^{b_j - a_j} e_p(h_j k_j) \right| \\ &= \prod_{j=1}^s \left( \sum_{h \in C(p)} \left| \sum_{k_j=0}^{b_j - a_j} e_p(h k_j) \right| \right) \\ &\leq \prod_{j=1}^s \left( p + \sum_{h=1}^{p-1} \left| \sum_{k_j=0}^{b_j - a_j} e_p(h k_j) \right| \right) \\ &< \prod_{j=1}^s (p + p(1 + \ln p)) \end{aligned}$$

nach Gleichung (3). Somit bekommen wir

$$\begin{aligned} &\left| \frac{A_N(J)}{N} - V(J) \right| \\ &< 1 - \left(1 - \frac{1}{p}\right)^s + \frac{(2 + \ln p)^s}{N} \left| \sum_{n=0}^{N-1} e_p(\mathbf{h} \cdot \mathbf{y}_n) \right|, \end{aligned}$$

was den Beweis abschließt. □

## 5.2 Exkurs über Exponentialsummen

**Satz 13** Sei  $f(X) \in \mathbb{F}_p[X]$  ein Polynom vom Grad 2, dann gilt

$$\left| \sum_{n=0}^{p-1} e_p(f(n)) \right| \leq 2p^{1/2}.$$

Beweis: Wir benutzen die Abkürzung  $S(f) := \sum_{n=0}^{p-1} e_p(f(n))$ . Wegen  $|S(f)| = |S(f+c)|$  für jede Konstante  $c$  können wir  $f(0) = 0$  annehmen.

Für  $0 \neq \lambda \in \mathbb{F}_p$ ,  $\mu \in \mathbb{F}_p$ , sei

$$f_{\lambda,\mu}(X) := f(\lambda X + \mu) - f(\mu).$$

Da  $X \mapsto \lambda X + \mu$  eine Permutation von  $\mathbb{F}_p$  ist, gilt

$$S(f_{\lambda,\mu}) = S(f).$$

Koeffizientenvergleich liefert, dass mindestens  $p(p-1)/2$  der  $f_{\lambda,\mu}$  verschieden sind. Es gilt also

$$\begin{aligned} \frac{p(p-1)}{2} |S(f)|^2 &\leq \sum_{a,b=0}^{p-1} |S(aX^2 + bX)|^2 = \sum_{a,b=0}^{p-1} S(aX^2 + bX)S(-aX^2 - bX) \\ &= \sum_{x,y=0}^{p-1} \sum_{a,b=0}^{p-1} e_p(ax^2 + bx)e_p(-ay^2 - by) \\ &= \sum_{x,y=0}^{p-1} \left( \sum_{a=0}^{p-1} e_p(a(x^2 - y^2)) \right) \left( \sum_{b=0}^{p-1} e_p(b(x - y)) \right) = p^3, \end{aligned}$$

woraus die Behauptung folgt.  $\square$

Ohne Beweis geben wir die folgende Verallgemeinerung an.

**Satz 14** Sei  $f/g$  eine rationale Funktion über  $\mathbb{F}_p$  und  $v$  die Anzahl der verschiedenen Nullstellen des Polynoms  $g$  (im algebraischen Abschluss von  $\mathbb{F}_p$ ). Ist  $f/g$  nicht konstant, so gilt

$$\left| \sum_{x \in \mathbb{F}_p, g(x) \neq 0} e_p \left( \frac{f(x)}{g(x)} \right) \right| \leq (\max(\text{grad}(f), \text{grad}(g)) + v^* - 2)p^{1/2} + \delta,$$

wobei  $v^* = v$  und  $\delta = 1$  im Fall  $\text{grad}(f) \leq \text{grad}(g)$  und  $v^* = v + 1$  und  $\delta = 0$  anderenfalls.

Beweis: Siehe C. Moreno und O. Moreno: Exponential sums and Goppa codes: I, Proc. Amer. Math. Soc. 111 (1991), 523–531.  $\square$

Wir benötigen noch ein weiteres verwandtes Ergebnis.

Sei  $g$  eine primitive Wurzel modulo  $p$ . Dann definieren wir für  $m = 1, \dots, p-2$

$$\chi_m(g^n) := e_{p-1}(mn), \quad n = 0, \dots, p-2,$$

und  $\chi_m(0) := 0$ .

**Satz 15** Für ein Polynom  $f(X) \in \mathbb{F}_p[X]$  gilt

$$\left| \sum_{x \in \mathbb{F}_p} e_p(f(x)) \chi_m(x) \right| \leq \text{grad}(f) p^{1/2}.$$

Beweis: Siehe W.M. Schmidt, Equations over finite fields. □

### 5.3 Linearer Kongruenzgenerator

Sei  $y_{n+1} \equiv ay_n \pmod{p}$ ,  $n \geq 0$ , mit  $a, y_0 \in \mathbb{F}_p^* := \mathbb{F}_p \setminus \{0\}$ , d.h.

$$y_n = a^n y_0, \quad n \geq 0,$$

und  $x_n = y_n/p$ ,  $n \geq 0$ , eine Folge von linearen Pseudozufallszahlen. Sei  $t$  die Ordnung von  $a$  modulo  $p$ . (D.h.  $(y_n)$  ist  $t$ -periodisch.) Für  $h \in \mathbb{F}_p$  und  $N$  mit  $1 \leq N \leq t$  betrachten wir die Exponentialsummen

$$S_N := \sum_{n=0}^{N-1} e_p(hy_n).$$

**Satz 16** Ist  $h \neq 0$ , so gilt

$$|S_t| < p^{1/2}.$$

Beweis: Es gilt

$$\begin{aligned} |S_t| &= \left| \sum_{n=0}^{t-1} e_p(hy_0 a^n) \right| \\ &= \frac{t}{p-1} \left| -1 + \sum_{x \in \mathbb{F}_p} e_p(hy_0 x^{(p-1)/t}) \right| \\ &\leq \frac{t}{p-1} \left( 1 + \left( \frac{p-1}{t} - 1 \right) p^{1/2} \right) < p^{1/2} \end{aligned}$$

nach Satz 14. □

**Satz 17** Ist  $h \neq 0$ , so gilt

$$|S_N| < (p^{1/2} + 1)(2 + \ln t) \quad \text{für } 1 \leq N < t.$$

Beweis: Wir haben

$$\begin{aligned}
S_N &= \sum_{n=0}^{t-1} e_p(hy_n) \sum_{k=0}^{N-1} \frac{1}{t} \sum_{m=0}^{t-1} e_t(m(n-k)) \\
&= \frac{1}{t} \sum_{m=0}^{t-1} \left( \sum_{k=0}^{N-1} e_t(-mk) \right) \left( \sum_{n=0}^{t-1} e_p(hy_n) e_t(mn) \right) \\
&= \frac{N}{t} \sum_{n=0}^{t-1} e_t(hy_n) + \frac{1}{t} \sum_{m=1}^{t-1} \left( \sum_{k=0}^{N-1} e_t(-mk) \right) \left( \sum_{n=0}^{t-1} e_p(hy_n) e_t(mn) \right)
\end{aligned}$$

und daher

$$|S_N| \leq \frac{N}{t} |S_t| + \frac{1}{t} \sum_{m=1}^{t-1} \left| \sum_{k=0}^{N-1} e_t(mk) \right| \left| \sum_{n=0}^{t-1} e_p(hy_n) e_t(mn) \right|. \quad (14)$$

Für  $1 \leq m \leq t-1$  gilt

$$\begin{aligned}
\left| \sum_{n=0}^{t-1} e_p(hy_n) e_t(mn) \right| &= \left| \sum_{n=0}^{t-1} e_p(ha^n y_0) e_t(mn) \right| \\
&\leq \frac{t}{p-1} \left( 1 + \left| \sum_{x \in \mathbb{F}_p} e_p(hx^{(p-1)/t} y_0) \chi_{m(p-1)/t}(x) \right| \right) \\
&\leq p^{1/2} + 1
\end{aligned}$$

nach Satz 15. Somit ergibt sich

$$\begin{aligned}
\sum_{m=1}^{t-1} \left| \sum_{k=0}^{N-1} e_t(mk) \right| \left| \sum_{n=0}^{t-1} e_p(hy_n) e_t(mn) \right| &\leq (p^{1/2} + 1) \sum_{m=1}^{t-1} \left| \sum_{k=0}^{N-1} e_t(mk) \right| \\
&\leq (p^{1/2} + 1) t (1 + \ln t)
\end{aligned}$$

nach (3). Mit Satz 16 erhalten wir aus einem analogen Ergebnis zu (14) mit  $t$  statt  $p$

$$|S_N| < \frac{N}{t} p^{1/2} + (p^{1/2} + 1) (1 + \ln t),$$

woraus der Satz folgt.  $\square$

**Korollar 6** Für  $P = \{x_n : 0 \leq n \leq t-1\}$  gilt

$$D_1(N, P) < \frac{1}{p} + N^{-1} (p^{1/2} + 1) (2 + \ln p) (2 + \ln t), \quad 1 \leq N \leq t.$$

Beweis: Satz 12 und Satz 17.  $\square$

## 5.4 Expliziter Inversionsgenerator

Sei  $y_n = \overline{an + b} \bmod p$ ,  $n \geq 0$ , und  $x_n = y_n/p$ ,  $n \geq 0$ , eine Folge von explizit inversen Pseudozufallszahlen. Für  $h_0, h_1, \dots, h_{s-1} \in \mathbb{F}_p$  und  $N$  mit  $1 \leq N \leq p$  betrachten wir die Exponentialsummen

$$S_N = \sum_{n=0}^{N-1} e_p \left( \sum_{j=0}^{s-1} h_j x_{n+j} \right).$$

**Satz 18** *Sind  $h_0, h_1, \dots, h_{s-1}$  nicht alle 0, so gilt*

$$|S_p| \leq (2s - 2)p^{1/2} + s + 1.$$

Beweis: Wir können  $s < p$  annehmen. Dann gilt

$$\begin{aligned} |S_p| &= \left| \sum_{n \in \mathbb{F}_p} e_p \left( \sum_{j=0}^{s-1} h_j \overline{a(n+j) + b} \right) \right| \\ &\leq s + \left| \sum_{n \in \mathbb{F}_p, g(n) \neq 0} e_p \left( \frac{f(n)}{g(n)} \right) \right|, \end{aligned}$$

mit

$$f(x) = \sum_{i=0}^{s-1} h_i \prod_{j=0, j \neq i}^{s-1} (a(x+j) + b)$$

und

$$g(x) = \prod_{j=0}^{s-1} (a(x+j) + b).$$

Nach Voraussetzung existiert ein  $0 \leq i \leq s-1$  mit  $h_i \neq 0$ . Wegen

$$f(-a^{-1}b - i) \neq 0$$

ist  $f/g$  nicht identisch 0. Daher gilt  $\text{grad}(f) < \text{grad}(g)$  und  $f/g$  ist nicht konstant. Wir können also Satz 14 anwenden, um die Behauptung zu erhalten.  $\square$

**Satz 19** *Sind  $h_0, h_1, \dots, h_{s-1}$  nicht alle 0, so gilt*

$$|S_N| < s(2p^{1/2} + 1)(2 + \ln p) \text{ für } 1 \leq N < p.$$

Beweis: Wir nehmen wieder  $s < p$  an. Mit  $\sigma_n := \sum_{i=0}^{s-1} h_i x_{n+i}$  haben wir

$$\begin{aligned} S_N &= \sum_{n=0}^{p-1} e_p(\sigma_n) \sum_{t=0}^{N-1} \frac{1}{p} \sum_{h=0}^{p-1} e_p(h(n-t)) \\ &= \frac{1}{p} \sum_{h=0}^{p-1} \left( \sum_{t=0}^{N-1} e_p(-ht) \right) \left( \sum_{n=0}^{p-1} e_p(\sigma_n + hn) \right) \\ &= \frac{N}{p} \sum_{n=0}^{p-1} e_p(\sigma_n) + \frac{1}{p} \sum_{h=1}^{p-1} \left( \sum_{t=0}^{N-1} e_p(-ht) \right) \left( \sum_{n=0}^{p-1} e_p(\sigma_n + hn) \right) \end{aligned}$$

und daher

$$|S_N| \leq \frac{N}{p} |S_p| + \frac{1}{p} \sum_{h=1}^{p-1} \left| \sum_{t=0}^{N-1} e_p(ht) \right| \left| \sum_{n=0}^{p-1} e_p(\sigma_n + hn) \right|.$$

Für  $h \neq 0$  gilt

$$\begin{aligned} \left| \sum_{n=0}^{p-1} e_p(\sigma_n + hn) \right| &= \left| \sum_{n=0}^{p-1} e_p \left( \sum_{i=0}^{s-1} h_i \overline{a(n+i) + b} + hn \right) \right| \\ &\leq s + \left| \sum_{n \in \mathbb{F}_p, g(n) \neq 0} e_p \left( \frac{f(n)}{g(n)} \right) \right| \end{aligned}$$

mit

$$f(x) = hx \prod_{j=0}^{s-1} (a(x+j) + b) + \sum_{i=0}^{s-1} h_i \prod_{j=0, j \neq i}^{s-1} (a(x+j) + b)$$

und

$$g(x) = \prod_{j=0}^{s-1} (a(x+j) + b).$$

Wir verifizieren wieder, dass  $f/g$  nicht konstant ist. Satz 14 ergibt

$$\begin{aligned} \sum_{h=1}^{p-1} \left| \sum_{t=0}^{N-1} e_p(ht) \right| \left| \sum_{n=0}^{p-1} e_p(\sigma_n + hn) \right| &\leq s(2p^{1/2} + 1) \sum_{h=1}^{p-1} \left| \sum_{t=0}^{N-1} e_p(ht) \right| \\ &\leq s(2p^{1/2} + 1)p(1 + \ln p) \end{aligned}$$

nach (3). Mit Satz 18 erhalten wir

$$|S_N| \leq \frac{N}{p} ((2s-2)p^{1/2} + s + 1) + s(2p^{1/2} + 1)(1 + \ln p).$$

Einfache Rechnungen ergeben den Satz. □

**Korollar 7** Für  $P = \{(x_n, x_{n+1}, \dots, x_{n+s-1}) : 0 \leq n \leq p-1\}$  gilt

$$D_s(N, P) < 1 - \left(1 - \frac{1}{p}\right)^s + N^{-1} s(2p^{1/2} + 1)(2 + \ln p)^{s+1}.$$

## 5.5 Rekursiver Inversionsgenerator

Sei  $y_{n+1} = a\overline{y_n} + b$ ,  $n \geq 0$ , ein rekursiver Inversionsgenerator mit Periode  $t$  und seien  $x_n = y_n/p$ ,  $n \geq 0$ , (rekursive) inverse Pseudozufallszahlen. Für  $1 \leq N \leq t$  und  $h_0, \dots, h_{s-1} \in \mathbb{F}_p$  definieren wir

$$S_N := \sum_{n=0}^{N-1} e_p \left( \sum_{j=0}^{s-1} h_j y_{n+j} \right).$$

**Satz 20** *Sind nicht alle  $h_0, \dots, h_{s-1}$  gleich 0, so gilt*

$$|S_N| \leq (\sqrt{5} + 1) s^{1/2} N^{1/2} p^{1/4}, \quad 1 \leq N \leq t.$$

Beweis: Definiere die Permutation  $\psi$  von  $\mathbb{F}_p$  durch

$$\psi(x) := \begin{cases} ax^{-1} + b, & x \neq 0, \\ b, & x = 0, \end{cases} \quad x \in \mathbb{F}_p.$$

Für eine ganze Zahl  $m$  sei  $\psi^m$  die  $m$ te Iteration von  $\psi$ . Dann gilt

$$y_n = \psi^n(y_0), \quad n \geq 0.$$

Für eine ganze Zahl  $k \geq 0$  gilt

$$\left| S_N - \sum_{n=0}^{N-1} e_p \left( \sum_{j=0}^{s-1} h_j y_{n+k+j} \right) \right| \leq 2k.$$

Für  $K \geq 1$  gilt

$$\sum_{k=0}^{K-1} k = (K-1)K/2$$

und somit

$$\begin{aligned} K|S_N| &= \left| \sum_{k=0}^{K-1} \left( S_N - \sum_{n=0}^{N-1} e_p \left( \sum_{j=0}^{s-1} h_j y_{n+k+j} \right) + \sum_{n=0}^{N-1} e_p \left( \sum_{j=0}^{s-1} h_j y_{n+k+j} \right) \right) \right| \\ &\leq W + (K-1)K \end{aligned} \tag{15}$$

mit

$$\begin{aligned} W &= \left| \sum_{n=0}^{N-1} \sum_{k=0}^{K-1} e_p \left( \sum_{j=0}^{s-1} h_j y_{n+k+j} \right) \right| \\ &\leq \sum_{n=0}^{N-1} \left| \sum_{k=0}^{K-1} e_p \left( \sum_{j=0}^{s-1} h_j y_{n+k+j} \right) \right| \\ &= \sum_{n=0}^{N-1} \left| \sum_{k=0}^{K-1} e_p \left( \sum_{j=0}^{s-1} h_j \psi^{k+j}(y_n) \right) \right|. \end{aligned}$$

Mit der Cauchy-Schwarz Ungleichung erhält man

$$\begin{aligned}
W^2 &\leq N \sum_{n=0}^{N-1} \left| \sum_{k=0}^{K-1} e_p \left( \sum_{j=0}^{s-1} h_j \psi^{k+j}(y_n) \right) \right|^2 \\
&\leq N \sum_{w=0}^{p-1} \left| \sum_{k=0}^{K-1} e_p \left( \sum_{j=0}^{s-1} h_j \psi^{k+j}(w) \right) \right|^2 \\
&= N \sum_{k,l=0}^{K-1} \sum_{w=0}^{p-1} e_p \left( \sum_{j=0}^{s-1} h_j (\psi^{k+j}(w) - \psi^{l+j}(w)) \right).
\end{aligned}$$

Sei  $r := \min\{j : h_j \neq 0\}$ . Da  $\psi^{r+\min(k,l)}$  eine Permutation ist gilt

$$W^2 \leq N \sum_{k,l=0}^{K-1} \sum_{w=0}^{p-1} e_p \left( \sum_{j=r}^{s-1} h_j (\psi^{k+j-r-\min(k,l)}(w) - \psi^{l+j-r-\min(k,l)}(w)) \right).$$

Für  $k = l$  ist die Summe über  $w$  gleich  $p$  und für  $k \neq l$  wenden wir Satz 14 an. Für  $m \geq 1$  existieren  $\alpha_m, \beta_m, \gamma_m (\neq 0), \delta_m$ , so dass

$$\psi^m(w) = \frac{\alpha_m w + \beta_m}{\gamma_m w + \delta_m}, \quad w \notin \{-\gamma_1^{-1}\delta_1, \dots, -\gamma_m^{-1}\delta_m\}$$

(vgl. Beweis von Hilfssatz 14). Somit lässt sich

$$\sum_{j=r}^{s-1} h_j (\psi^{k+j-r-\min(k,l)}(w) - \psi^{l+j-r-\min(k,l)}(w))$$

für alle bis auf höchstens  $K+s-1$  verschiedene  $w$  als rationale Funktion  $f(w)/g(w)$  schreiben mit Polynomen  $f, g$ , die  $\text{grad}(g) - 1 \leq \text{grad}(f) \leq 2s$  erfüllen. Zusammengefasst ergibt das

$$W^2 \leq N(Kp + K^2((4s-2)p^{1/2} + K + s - 1)).$$

Jetzt wählen wir  $K := \lceil p^{1/2} \rceil$  und erhalten

$$\frac{W^2}{K^2} \leq N(p^{1/2} + (4s-1)p^{1/2} + s).$$

Da das Ergebnis sonst trivial ist, dürfen wir  $s \leq p^{1/2}$  annehmen und bekommen mit (15)

$$|S_N| \leq (4s+1)^{1/2} N^{1/2} p^{1/4} + p^{1/2}.$$

Nehmen wir weiterhin  $N \geq p^{1/2}$  an, so folgt das Ergebnis.  $\square$

**Korollar 8** Für  $P = \{(x_n, x_{n+1}, \dots, x_{n+s-1}) : 0 \leq n \leq t-1\}$  gilt

$$D_s(N, P) < 1 - \left(1 - \frac{1}{p}\right)^s + (\sqrt{5} + 1) N^{-1/2} s^{1/2} p^{1/2} (2 + \ln p)^s.$$

## 6 Weitere Bemerkungen zu Inversionsgenerator und Legendre-Folge

### 6.1 Maximale Periode des rekursiven Inversionsgenerators

**Satz 21** *Ist  $\gamma$  ein primitives Element von  $\mathbb{F}_{p^2}$  (d.h.  $\gamma$  ist Lösung der Gleichung  $X^{p^2-1} \equiv 1 \pmod{p}$  aber keiner Gleichung  $X^n \equiv 1 \pmod{p}$  mit  $1 \leq n \leq p^2 - 2$ ). Für  $a = -\gamma^{p+1}$  und  $b = \gamma + \gamma^p$  hat die Folge  $y_{n+1} = a\bar{y}_n + b$  die Periode  $p$ .*

Beweis: 1. Die Folge  $c_0 = 0, c_1 = 1, c_{n+2} = bc_{n+1} + ac_n, n \geq 0$ , hat die kleinste Periode  $T = p^2 - 1$ . Wegen

$$(1 - Y^T) \sum_{n=0}^{\infty} c_n Y^n = \sum_{n=0}^{T-1} c_n Y^n$$

und

$$(1 - bY - aY^2) \sum_{n=0}^{\infty} c_n Y^n = Y$$

folgt

$$(1 - Y^T)Y = (1 - bY - aY^2) \sum_{n=0}^{T-1} c_n Y^n.$$

Daher muss  $1 - bY - aY^2$  das Polynom  $1 - Y^T$  teilen bzw. (Übergang von  $Y$  zu  $X = Y^{-1}$ )  $X^2 - bX - a$  teilt  $X^T - 1$ . D.h. die Nullstelle  $\gamma$  von  $X^2 - bX - a$  muss eine Nullstelle von  $X^T - 1$  sein. Da  $\gamma$  ein primitives Element von  $\mathbb{F}_{p^2}$  ist, muss  $T = p^2 - 1$  gelten.

2. Mit  $\vartheta := (\gamma - \gamma^p)^{-1}$  gilt

$$c_n = \vartheta \gamma^n + \vartheta^p \gamma^{pn}, \quad n \geq 0.$$

Für  $n = 0$  gilt  $c_0 = \vartheta + \vartheta^p = (\gamma - \gamma^p)^{-1} + (\gamma^p - \gamma)^{-1} = 0$ . Für  $n = 1$  gilt  $c_1 = \vartheta \gamma + \vartheta^p \gamma^p = (1 - \gamma^{p-1})^{-1} + (1 - \gamma^{1-p})^{-1} = 1$ . Gelte  $c_n = \vartheta \gamma^n + \vartheta^p \gamma^{pn}$  für  $n \geq 0$ , so erhalten wir

$$\begin{aligned} c_{n+2} &= bc_{n+1} + ac_n \\ &= b(\vartheta \gamma^{n+1} + \vartheta^p \gamma^{p(n+1)}) + a(\vartheta \gamma^n + \vartheta^p \gamma^{pn}) \\ &= (b\gamma^{-1} + a\gamma^{-2})\vartheta \gamma^{n+2} + (b\gamma^{-p} + a\gamma^{-2p})\vartheta^p \gamma^{p(n+2)} \\ &= \vartheta \gamma^{n+2} + \vartheta^p \gamma^{p(n+2)}. \end{aligned}$$

3. Wir haben  $c_m \neq 0, 1 \leq m \leq p$ .

Angenommen, es wäre  $c_m = 0$  mit  $1 \leq m \leq p$ . Dann würde nach 2.

$$\gamma^{(p-1)m} = -\vartheta^{1-p} = 1$$

und somit  $c_{n+(p-1)m} = c_n$ ,  $n \geq 0$ , gelten. Damit wäre die Periode von  $c_n$  aber höchstens  $(p-1)m \leq (p-1)p < p^2 - 1$  im Widerspruch zu 1.

4. Mit  $y_0 = 0$  gilt  $y_n = c_n^{-1}c_{n+1} \neq 0$ ,  $1 \leq n \leq p-1$ .  
Wir haben  $y_1 = b = c_1^{-1}c_2 \neq 0$  und induktiv

$$y_{n+1} = ay_n^{-1} + b = (ac_n + bc_{n+1})c_{n+1}^{-1} = c_{n+1}^{-1}c_{n+2} \neq 0.$$

Da  $y_0 = 0$  aber  $y_n \neq 0$  für  $n = 1, \dots, p-1$  muss die Periode gleich  $p$  sein.  $\square$

## 6.2 Berechnung

Das Legendre-Symbol kann man folgendermaßen berechnen:

$$\left(\frac{n}{p}\right) \equiv n^{(p-1)/2} \pmod{p}.$$

Nach dem kleinen Fermat lässt sich das Inverse von  $0 \neq x \in \mathbb{F}_p$  als

$$x^{-1} \equiv x^{p-2} \pmod{p}$$

berechnen. In beiden Fällen müssen wir also Potenzen modulo  $p$  finden. Dieses kann mit *wiederholtem Quadrieren* effizient durchgeführt werden.

Berechnung von  $n^k \pmod{p}$ :

Wir berechnen zunächst

$$n, n^2, n^4, \dots, n^{2^t} \pmod{p} \quad \text{mit } t = \lfloor \log_2 k \rfloor.$$

Sei  $k = b_0 + 2b_1 + \dots + b_t 2^t$ ,  $b_0, \dots, b_t \in \{0, 1\}$  die Bitdarstellung von  $k$ , so gilt

$$n^k \equiv n^{b_0} n^{2b_1} \dots n^{2^t b_t} \pmod{p},$$

d.h. wir benötigen höchstens  $t$  weitere Multiplikationen modulo  $p$ .

Zur Bestimmung des Inversen kann man alternativ den Euklidischen Algorithmus benutzen. Zur Berechnung des Legendre-Symbols ist das quadratische Reziprozitätsgesetz

$$\left(\frac{p}{q}\right) = (-1)^{(p-1)(q-1)/4} \left(\frac{q}{p}\right)$$

(zusammen mit dem Ergänzungsgesetz  $\left(\frac{2}{p}\right) = 1$  genau dann, wenn  $p \equiv \pm 1 \pmod{8}$ ) hilfreich.

## 7 Weitere Generatoren

### 7.1 Explizite inverse und nichtlineare Generatoren

Sei  $\mathbb{F}_q$  ein endlicher Körper mit  $q = p^r$  Elementen, wobei  $p$  eine Primzahl ist. Dann ist  $\mathbb{F}_q$  ein  $r$  dimensionaler Vektorraum über  $\mathbb{F}_p$ . Sei  $\{\beta_1, \dots, \beta_r\}$  eine Basis von  $\mathbb{F}_q$  über  $\mathbb{F}_p$ , so ordnen wir die Elemente  $\xi_0, \dots, \xi_{q-1}$  von  $\mathbb{F}_q$  auf folgende Art:

$$\xi_n = n_1\beta_1 + n_2\beta_2 + \dots + n_r\beta_r, \quad (16)$$

wenn

$$n = n_1 + n_2p + \dots + n_rp^{r-1}, \quad 0 \leq n_1, n_2, \dots, n_r \leq p-1.$$

Außerdem setzen wir  $\xi_{n+q} := \xi_n$ ,  $n \geq 0$ . Explizite inverse bzw. nichtlineare Generatoren sind dann von der Form

$$\eta_n = \overline{a\xi_n + b}, \quad n \geq 0, \quad 0 \neq a, b \in \mathbb{F}_q,$$

bzw.

$$\eta_n = f(\xi_n), \quad n \geq 0,$$

mit einem Polynom  $f$  über  $\mathbb{F}_q$  vom Grad höchstens  $q-1$ .

Ist  $t$  ein Teiler von  $q-1$ , so kann man auch  $t$ -periodische explizite inverse bzw. nichtlineare Generatoren definieren:

$$\eta_n = \overline{a\gamma^n + b}, \quad n \geq 0, \quad a, b \in \mathbb{F}_q, \quad ab \neq 0,$$

bzw.

$$\eta_n = f(\gamma^n), \quad n \geq 0,$$

mit einem Polynom über  $\mathbb{F}_q$  vom Grad höchstens  $t-1$ , wobei  $\gamma \in \mathbb{F}_q$  ein Element der Ordnung  $t$  ist.

Aus der Folge  $(\eta_n)$  über  $\mathbb{F}_q$  bekommt man dann eine Folge  $(x_n)$  im Einheitsintervall durch

$$x_n := \sum_{i=1}^r \eta_n^{(i)} p^{-i},$$

wenn

$$\eta_n = \eta_n^{(1)}\beta_1 + \eta_n^{(2)}\beta_2 + \dots + \eta_n^{(r)}\beta_r, \quad 0 \leq \eta_n^{(1)}, \dots, \eta_n^{(r)} \leq p-1.$$

### 7.2 Verallgemeinerungen von Legendre-Folgen und Sidelnikov-Folgen

Mit der Anordnung (16) können wir *verallgemeinerte Legendre-Folgen* definieren:

$$l_n := \begin{cases} 0, & \text{es gibt } \eta \in \mathbb{F}_q \text{ mit } \xi_n = \eta^2, \\ 1, & \text{sonst.} \end{cases}$$

Sind  $p$  und  $r$  verschiedene ungerade Primzahlen, so definieren wir den *Zwei-Primzahlen Generator* ( $z_n$ ) durch

$$z_n := \begin{cases} 1, & \left(\frac{n}{p}\right) \left(\frac{n}{r}\right) = -1 \text{ oder } p \text{ teilt } n \text{ u. } n \not\equiv 0 \pmod{pr}, \\ 0, & \text{sonst,} \end{cases} \quad n = 0, 1, \dots$$

Ist  $g$  eine primitive Wurzel modulo  $p$ , dann ist die *Sidelnikov-Folge* ( $s_n$ ) durch

$$s_n := \begin{cases} 1, & \left(\frac{g^{n+1}}{p}\right) = -1, \\ 0, & \text{sonst,} \end{cases} \quad n = 0, 1, \dots,$$

definiert. Sidelnikov-Folgen haben die Periode  $p - 1$ .

### 7.3 Potenzgenerator und quadratischer Kongruenzgenerator

Der *Potenzgenerator* ( $p_n$ ) wird rekursiv definiert durch

$$p_{n+1} \equiv p_n^e \pmod{m}, \quad n \geq 0,$$

mit einem Startwert  $p_0 \in \mathbb{Z}$  und einem ganzzahligen Exponenten  $e \geq 2$ . Im Fall  $e = 2$  wird dieser Generator auch *Blum-Blum-Shub Generator* genannt und im Fall  $\gcd(e, \varphi(m))=1$ , wobei  $\varphi$  die Euler-Funktion ist, heisst er *RSA Generator*. Der *quadratische Kongruenzgenerator* ist von der Form

$$q_{n+1} \equiv aq_n^2 + bq_n + c \pmod{m}, \quad n \geq 0,$$

mit einem Startwert  $q_0$ .

Beide Generatoren sind spezielle (rekursive) nichtlineare Kongruenzgeneratoren.

### 7.4 Nichtlineare Generatoren höherer Ordnung

Um längere Perioden zu erhalten, kann man auch (rekursive) *nichtlineare Kongruenzgeneratoren* der Ordnung  $k \geq 1$  definieren:

$$y_{n+1} = f(y_n, y_{n-1}, \dots, y_{n+1-k}), \quad n \geq 0,$$

mit Startwerten  $y_0, \dots, y_{k-1} \in \mathbb{F}_p$  und einem Polynom über  $\mathbb{F}_p$  in  $k$  Variablen.

### 7.5 Exponentialgenerator und quadratischer Exponentialgenerator

Der *Exponentialgenerator* ist durch

$$e_{n+1} = g^{e_n}, \quad n \geq 0,$$

mit einem  $g \in \mathbb{F}_p^*$  und einer natürlichen Zahl  $e_0$  definiert.  
 Der *quadratische Exponentialgenerator*  $(q_n)$  ist definiert als

$$q_n = g^{n^2}, \quad n \geq 0,$$

mit einem Element  $g \in \mathbb{F}_p^*$ .

## 7.6 Folgen über elliptischen Kurven

Ist  $E$  eine elliptische Kurve über  $\mathbb{F}_p$ ,  $p \geq 5$ , und  $P \in \mathbb{F}_p^2$  ein Punkt der Ordnung  $t$  auf  $E$ . Ist  $f$  ein bivariates Polynom über  $\mathbb{F}_p$ , so kann man folgendermaßen eine Folge über  $\mathbb{F}_p$  definieren:

$$y_n = f(nP), \quad n \geq 0.$$

Insbesondere wählt man  $f(x, y) = x$  oder  $f(x, y) = y$ .

# 8 Lineare Komplexität von Sidelnikov-Folgen

## 8.1 Maximale Lineare Komplexität über $\mathbb{F}_2$

Wir starten mit Hilfssatz 3. Ist  $p - 1 = 2^s r$  mit einem ungeraden  $r$ , so gilt

$$X^{p-1} - 1 \equiv (X^r - 1)^{2^s}.$$

D.h. zur Bestimmung der linearen Komplexität müssen wir die Anzahl (in Vielfachheiten gezählt) der gemeinsamen Nullstellen von  $X^r - 1$  und  $S^{p-1}(X) = \sum_{n=0}^{p-1} s_n X^n$  bestimmen. Wir beschränken uns auf einen Fall, in dem 1 die einzige gemeinsame Nullstelle ist.

**Hilfssatz 17** *Ist  $r$  eine ungerade Primzahl, so dass 2 eine primitive Wurzel modulo  $r$  ist, und  $\beta \neq 1$  eine Nullstelle von  $X^r - 1$ . Dann sind die Potenzen  $\beta, \beta^2, \dots, \beta^{r-1}$  linear unabhängig über  $\mathbb{F}_2$ .*

Beweis: Wir haben  $\mathbb{F}_2(\beta) = \mathbb{F}_{2^n}$ , wobei  $n$  die Ordnung von 2 modulo  $r$  ist, d.h. nach Voraussetzung  $n = r - 1$ . Eine (Polynomial-)Basis von  $\mathbb{F}_{2^{r-1}}$  ist dann  $\{1, \beta, \dots, \beta^{r-2}\}$ . Offensichtlich ist dann auch  $\{\beta, \beta^2, \dots, \beta^{r-1}\}$  linear unabhängig.  $\square$

**Hilfssatz 18** *Ist  $r \geq p^{1/2} + 1$  eine ungerade Primzahl, so dass 2 eine primitive Wurzel modulo  $r$  ist. Dann gilt für jede Nullstelle  $\beta \neq 1$  von  $X^r - 1$*

$$S^{p-1}(\beta) \neq 0.$$

*Proof.* Wegen  $\beta^r = 1$  gilt

$$S^{p-1}(\beta) = \sum_{n=0}^{p-2} s_n \beta^n = \sum_{h=0}^{r-1} \sum_{j=0}^{(p-1)/r-1} s_{h+jr} \beta^h.$$

Der kleinste Rest von  $(p-1)/2$  modulo  $r$  ist 0. Nach dem vorherigen Hilfssatz sind  $\beta, \dots, \beta^{r-1}$  linear unabhängig über  $\mathbb{F}_2$ . Dann folgt aus  $S^{p-1}(\beta) = 0$  und  $1 + \beta + \dots + \beta^{r-1} = 0$

$$\sum_{j=0}^{(p-1)/r-1} s_{h+jr} = \sum_{j=0}^{(p-1)/r-1} s_{jr}, \quad h = 1, \dots, r-1.$$

Nach Definition der Sidelnikov-Folge gilt

$$(-1)^{s_n} = \left( \frac{g^n + 1}{p} \right), \quad n \neq (p-1)/2,$$

und

$$\prod_{j=0}^{(p-1)/r-1} (g^{jr} X + 1) = 1 - X^{(p-1)/r}.$$

Daher hat

$$(-1)^{\sum_{j=0}^{(p-1)/r-1} s_{h+jr}} = \prod_{j=0}^{(p-1)/r-1} \left( \frac{g^{h+jr} + 1}{p} \right) = \left( \frac{1 - g^{h(p-1)/r}}{p} \right)$$

für alle  $h = 1, \dots, r-1$  den selben Wert. Summation über  $h$  ergibt

$$\begin{aligned} r-1 &= \left| \sum_{h=0}^{r-1} \left( \frac{1 - g^{h(p-1)/r}}{p} \right) \right| = \frac{r}{p-1} \left| \sum_{h=0}^{p-2} \left( \frac{1 - g^{h(p-1)/r}}{p} \right) \right| \\ &\leq \frac{r}{p-1} \left( \left( \frac{p-1}{r} - 1 \right) p^{1/2} + 1 \right) < p^{1/2} \end{aligned}$$

nach Weil's Schranke (Hilfssatz 1) im Widerspruch zur Annahme für  $r$ .  $\square$

Wir brauchen unter gewissen Voraussetzungen also nur noch die 1 als Nullstelle von  $S^{p-1}(X)$  zu untersuchen.

**Hilfssatz 19** *Ist  $p \equiv 3 \pmod{4}$ , so gilt  $S^{p-1}(1) \neq 0$ .*

*Beweis:* Nach Definition der Sidelnikov-Folge gilt

$$S^{p-1}(1) = \sum_{\left(\frac{g^n+1}{p}\right)=-1} 1 = \frac{p-1}{2}.$$

Somit ist 1 genau dann eine Nullstelle, wenn  $p \equiv 1 \pmod{4}$ .  $\square$

**Satz 22** Ist  $p = 2r + 1$  mit einer ungeraden Primzahl  $r$ , so dass 2 eine primitive Wurzel modulo  $r$  ist, so hat die Sidelnikov-Folge die maximale lineare Komplexität über  $\mathbb{F}_2$

$$L = p - 1.$$

Beweis: Nach den vorherigen Hilfssätzen haben  $S^{p-1}(X)$  und  $X^{p-1} - 1$  keine gemeinsame Nullstelle, wenn  $r = (p - 1)/2 \geq p^{1/2} + 1$ . Dies ist erfüllt für  $p \geq 11$ . Der verbleibende Fall  $p = 7$  kann leicht direkt überprüft werden. (Für  $p = 3$  ist  $r = 1$  keine Primzahl).  $\square$

## 8.2 Lineare Komplexität über $\mathbb{F}_p$

**Hilfssatz 20** Sei  $g$  eine primitive Wurzel modulo  $p$ ,  $f \in \mathbb{F}_p[X]$  ein Polynom vom Grad höchsten  $p - 2$  und  $(y_n)$  definiert durch

$$y_n = f(g^n), \quad n \geq 0.$$

Die lineare Komplexität von  $(y_n)$  über  $\mathbb{F}_p$  ist mindestens gleich der Anzahl der von Null verschiedenen Koeffizienten von  $f$ .

Beweis: Sei  $w$  die Anzahl der von Null verschiedenen Koeffizienten von  $f$ . Wir nehmen an das  $L < w$ . Sei

$$y_{n+L} = c_{L-1}y_{n+L-1} + \dots + c_0y_n, \quad n \geq 0,$$

oder gleichwertig

$$f(g^L g^n) = c_{L-1}f(g^{L-1}g^n) + \dots + c_0f(g^n), \quad n \geq 0.$$

Somit hat mit  $c_L := -1$  das Polynom

$$F(X) := c_L f(g^L X) + c_{L-1} f(g^{L-1} X) + \dots + c_0 f(X)$$

mindestens  $p - 1$  Nullstellen  $(1, g, \dots, g^{p-2})$ . Wegen  $\text{grad}(F) \leq \text{grad}(f) \leq p - 2$  ist  $F$  identisch 0. Sei jetzt  $f(X) := \sum_{i=1}^w a_i X^{j_i}$  mit  $0 \leq j_1 < j_2 < \dots < j_w \leq p - 2$  und  $a_1 \cdots a_w \neq 0$ . Wir haben also

$$0 = F(X) = \sum_{l=0}^L c_l \sum_{i=1}^w a_i g^{lj_i} X^{j_i} = \sum_{i=1}^w a_i \left( \sum_{l=0}^L c_l g^{lj_i} \right) X^{j_i}.$$

Wegen  $a_i \neq 0$  liefert Koeffizientenvergleich

$$\sum_{l=0}^L c_l g^{lj_i} = 0, \quad i = 1, \dots, w.$$

Die Matrix  $(g^{lj_i})$ ,  $i = 1, \dots, L$ ,  $l = 0, \dots, L - 1$ , ist eine (reguläre) Vandermonde Matrix und somit  $c_0 = \dots = c_L = 0$  im Widerspruch zu  $c_L = -1$ .  $\square$

Die Sidelnikov-Folge aufgefasst als Folge über  $\mathbb{F}_p$  läßt sich folgendermaßen schreiben:

$$\begin{aligned} s_n &\equiv \frac{1}{2} ((g^n + 1)^{p-1} - (g^n + 1)^{(p-1)/2}) \\ &\equiv \frac{1}{2} \left( 1 + \sum_{j=1}^{(p-1)/2} \left( \binom{p-1}{j} - \binom{(p-1)/2}{j} \right) g^{nj} + \sum_{j=(p+1)/2}^{p-2} \binom{p-1}{j} g^{nj} \right) \\ &\quad \text{mod } p. \end{aligned}$$

Nach dem vorherigen Hilfssatz ist die lineare Komplexität über  $\mathbb{F}_p$  der Sidelnikov-Folge also

$$L \geq p - 1 - N,$$

wobei  $N$  die Anzahl der Lösungen  $j = 1, \dots, (p-1)/2$  von

$$\binom{p-1}{j} \equiv \binom{(p-1)/2}{j} \pmod{p}$$

ist.

**Satz 23** Die lineare Komplexität über  $\mathbb{F}_p$  einer Sidelnikov-Folge ist mindestens  $(p-1)/2$ .

## 9 Lineare Komplexität über verschiedenen Modulen

In diesem Abschnitt ist  $s_0, \dots, s_{N-1}$  ein ganzzahliger Folgenabschnitt. Analog zu Definition 3 kann man die lineare Komplexität dieses Folgenabschnittes über  $\mathbb{Z}$  und modulo  $m$  für eine (nicht notwendig prime) ganze Zahl  $m \geq 2$  definieren. Wir bezeichnen mit  $L$  die lineare Komplexität über  $\mathbb{Z}$  von  $(s_n)$  bei  $N$  und mit  $L_m$  die lineare Komplexität modulo  $m$  bei  $N$ .

**Satz 24** Sei  $h$  eine natürliche Zahl und

$$|s_i| \leq h, \quad i = 0, \dots, N - 1.$$

Dann gilt für  $m \geq 2$ ,

$$L_m \geq \frac{1}{2 \log_2 m} \min \{L, m/h - 1\}.$$

Beweis: Setze  $\mathbb{Z}_m := \{-\lceil m/2 \rceil + 1, \dots, \lfloor m/2 \rfloor\}$ . Wir dürfen  $m \geq h$  annehmen, da die Aussage sonst trivial ist. Sei  $l := L_m$  und

$$s_{n+l} \equiv c_{l-1}s_{n+l-1} + \dots + c_0s_n \pmod{m}, \quad n = 0, \dots, N-l-1.$$

Für jede ganze Zahl  $k \geq 0$  gilt

$$s_{n+k} \equiv \sum_{j=0}^{l-1} c_{j,k} s_{n+j} \pmod{m}, \quad n = 0, \dots, N-k-1, \quad (17)$$

mit einem Vektor  $\mathbf{c}_k := (c_{0,k}, \dots, c_{l-1,k}) \in \mathbb{Z}_m^l$ . Setze  $r := \lceil 2l \log_2 m \rceil$ . Wir dürfen  $r < m/h$  annehmen. Wir betrachten die folgenden  $2^r$  Linearkombinationen mit 0, 1-Koeffizienten

$$\sum_{k=0}^{r-1} e_k \mathbf{c}_k, \quad (e_0, \dots, e_{r-1}) \in \{0, 1\}^r. \quad (18)$$

Alle diese Vektoren sind im  $l$ -dimensionalen Würfel  $[-r(\lceil m/2 \rceil - 1), r\lfloor m/2 \rfloor]^l$  und haben daher höchstens

$$(r(m-1) + 1)^l \leq (rm)^l < (m^2/h)^l \leq m^{2l} \leq 2^r$$

verschiedene Werte. Daher müssen wenigstens zwei Vektoren (18) zusammenfallen. Die Differenz irgendeines Paares solcher Vektoren ergibtthat

$$\sum_{k=0}^{r-1} d_k \mathbf{c}_k \equiv \mathbf{0} \pmod{m}$$

mit einem Vektor  $(d_0, \dots, d_{r-1}) \in \{-1, 0, 1\}^r \setminus \{\mathbf{0}\}$ . Sei  $t \leq r-1$  der größte Wert von  $k$  mit  $d_k \neq 0$ . Mit (17) bekommen wir

$$\sum_{k=0}^t d_k s_{n+k} \equiv \sum_{k=0}^t d_k \sum_{j=0}^{l-1} c_{j,k} s_{n+j} \equiv \sum_{j=0}^{l-1} s_{n+j} \sum_{k=0}^t d_k c_{j,k} \equiv 0 \pmod{m}, \quad (19)$$

für jedes  $n = 0, \dots, N-t-1$ . Nach Wahl von  $r$  haben wir ebenfalls

$$\left| \sum_{k=0}^t d_k s_{n+k} \right| \leq rh < m, \quad n = 0, \dots, N-t-1,$$

und die Rekursionsgleichung (19) gilt über  $\mathbb{Z}$ . Benutzt man  $d_t = \pm 1$  und daher  $d_t^2 = 1$ , erhalten wir

$$s_{n+t} = - \sum_{k=0}^{t-1} d_t d_k s_{n+k}$$

für  $n = 0, \dots, N-t-1$ . Daher  $L \leq t \leq r-1 \leq 2l \log_2 m$ , was zum gewünschten Ergebnis führt.  $\square$

## 10 Lineare Komplexität weiterer Generatoren

### 10.1 Explizit nichtlinearer Generator der Periode $p$

Sei  $y_n = f(n)$ ,  $n \geq 0$ , mit einem Polynom  $f \in \mathbb{F}_p[X]$  vom Grad kleiner  $p$ .

**Satz 25** Die lineare Komplexität über  $\mathbb{F}_p$  der Folge  $(y_n)$  ist

$$L \geq \deg(f) + 1.$$

Beweis: Sei  $f(X) := \sum_{d=0}^D a_d X^d$  mit  $a_D \neq 0$ . Wir nehmen  $L \leq D$  an. Mit  $c_L := -1$  gelte

$$\sum_{l=0}^L c_l y_{n+l} = 0, \quad n \geq 0.$$

Also hat das Polynom

$$F(X) := \sum_{l=0}^L c_l f(X+l)$$

vom Grad höchstens  $D < p$  mindestens  $p$  Nullstellen und ist somit das Nullpolynom. Es gilt also

$$\begin{aligned} 0 &= \sum_{l=0}^L c_l \sum_{d=0}^D a_d (X+l)^d = \sum_{l=0}^L c_l \sum_{d=0}^D a_d \sum_{j=0}^d \binom{d}{j} l^{d-j} X^j \\ &= \sum_{j=0}^D \left( \sum_{d=j}^D a_d \binom{d}{j} \sum_{l=0}^L c_l l^{d-j} \right) X^j \end{aligned}$$

und somit

$$\sigma_{D-j} := \sum_{d=j}^D a_d \binom{d}{j} \sum_{l=0}^L c_l l^{d-j} = 0, \quad j = 0, \dots, D.$$

Wir definieren rekursiv  $\tau_0 := \sigma_0$  und

$$\tau_j := \sigma_j - a_D^{-1} \sum_{k=0}^{j-1} a_{D-j+k} \binom{D-j+k}{k} \binom{D}{k}^{-1} \tau_k, \quad 1 \leq j \leq D$$

und zeigen mit vollständiger Induktion

$$\tau_j = a_D \binom{D}{j} \sum_{l=0}^L c_l l^j = 0, \quad j = 0, \dots, D.$$

Wegen  $a_D \binom{D}{j} \neq 0$  folgt also  $\sum_{l=0}^L c_l l^j = 0$ ,  $j = 0, \dots, D$  und da die Vandermonde Matrix  $(n^j)$  regulär ist  $c_0 = \dots = c_L = 0$  im Widerspruch zu  $c_L = -1$ .  $\square$

## 10.2 Legendre Folge über $\mathbb{F}_p$

Für die Legendre-Folge gilt

$$l_n \equiv \frac{1}{2} (n^{p-1} - n^{(p-1)/2}) \pmod{p}, \quad n \geq 0,$$

und nach dem vorherigen Kapitel gilt für die lineare Komplexität modulo  $p$  der Legendre-Folge

$$L = p.$$

## 10.3 Quadratischer Exponentialgenerator

Sei  $g \in \mathbb{F}_p^*$  ein Element der Ordnung  $\tau$  und  $(u_n)$  die durch

$$u_n = g^{n^2}, \quad n \geq 0,$$

definierte Folge. Diese Folge ist rein periodisch mit Periode  $\tau/2 \leq t \leq \tau$ .

**Satz 26** Die lineare Komplexität  $L(N)$  modulo  $p$  bei  $N$  der Folge  $(u_n)$  erfüllt

$$L(N) \geq \left\lceil \frac{\min\{N, t\}}{2} \right\rceil, \quad N \geq 1.$$

Beweis: Sei  $L$  die kleinste natürliche Zahl mit

$$u_{n+L} = c_{L-1}u_{n+L-1} + \dots + c_0u_n, \quad 0 \leq n \leq N - L - 1.$$

Verifiziere

$$u_{n+l} = g^{l^2} u_n g^{2nl}, \quad l, n \geq 0. \quad (20)$$

Mit  $c_L := -1$  und  $b_l := g^{l^2} c_l$  für  $0 \leq l \leq L$  gilt

$$b_L g^{2nL} + \dots + b_0 = 0, \quad 0 \leq n \leq N - L - 1.$$

Ist  $\tau$  gerade, so sind die Elemente  $1, g^2, g^4, \dots, g^{\tau-2}$  verschieden, und ist  $\tau$  ungerade, so sind  $1, g^2, g^4, \dots, g^{2\tau-2}$  verschieden. Also hat das Polynom  $F(X) := b_L X^L + \dots + b_0$  vom Grad  $L$  mindestens  $\min\{N - L, \tau/2\}$  Nullstellen, wenn  $\tau$  gerade ist, und mindestens  $\min\{N - L, \tau\}$  Nullstellen, wenn  $\tau$  ungerade ist. Wegen  $t \leq \tau$  erhalten wir das Ergebnis.  $\square$

## 11 $k$ -Fehler lineare Komplexität

Sei  $(s_n)$  eine  $t$ -periodische Folge über  $\mathbb{F}_p$ . Das Gewicht  $w(s_n)$  der Folge ist die Anzahl der  $0 \leq n \leq t - 1$  mit  $s_n \neq 0$ . Die  $k$ -Fehler lineare Komplexität von  $(s_n)$  ist definiert als

$$L_k(s_n) = \min_{0 \leq w(z_n) \leq k} L(s_n + z_n), \quad 0 \leq k \leq t.$$

## 11.1 1-Fehler lineare Komplexität der Legendre-Folge über $\mathbb{F}_p$

**Satz 27** Für die Legendre-Folge  $(l_n)$  über  $\mathbb{F}_p$  gilt

$$L_1(l_n) \geq (p+1)/2, \quad p \geq 5.$$

Beweis: Sei  $z_n^{(k)}$  die  $p$ -periodische Folge mit

$$z_n^{(k)} := \begin{cases} 1, & n \equiv k \pmod{p}, \\ 0, & \text{sonst,} \end{cases} \quad k = 0, \dots, p-1.$$

Es gilt

$$z_n^{(k)} \equiv 1 - (n-k)^{p-1} \pmod{p}$$

und

$$l_n + xz_n^{(k)} \equiv \frac{1}{2}(n^{p-1} - n^{(p-1)/2}) + x - x(n-k)^{p-1}, \quad x \in \mathbb{F}_p.$$

Ist  $x \neq 1/2$ , so hat diese Summenfolge nach Satz 25 die maximale lineare Komplexität  $p$ . Ist  $x = 1/2$  und  $k \neq 0$ , so gilt

$$2(l_n + z_n^{(k)}) = -n^{(p-1)/2} + 1 - \sum_{j=0}^{p-2} \binom{p-1}{j} (-k)^{p-1-j} n^j.$$

Die Summenfolge lässt sich also für  $p \geq 5$  mit einem Polynom vom Grad  $p-2$  beschreiben und nach Satz 25 ist die lineare Komplexität mindestens  $p-1$ . Für  $x = 1/2$  und  $k = 0$  gilt

$$l_n + z_n^{(0)} \equiv \frac{1}{2} (1 - n^{(p-1)/2}) \pmod{p}$$

und die Folge hat lineare Komplexität  $L \geq (p+1)/2$ . □

## 11.2 1-Fehler lineare Komplexität der Sidelnikov-Folge über $\mathbb{F}_p$

**Satz 28** Für die Sidelnikov-Folge  $(s_n)$  über  $\mathbb{F}_p$  gilt

$$L_1(s_n) \geq \frac{p-3}{2}.$$

Beweis: Analog dem vorherigen Beweis definieren wir

$$z_n^{(k)} := 1 - (g^n - g^k)^{p-1}, \quad 0 \leq k \leq p-2, \quad n \geq 0.$$

Dann gilt

$$\begin{aligned} s_n + xz_n^{(k)} &= \frac{1}{2} ((g^n + 1)^{p-1} - (g^n + 1)^{(p-1)/2}) + x - x(g^n - g^k)^{p-1} \\ &= \left( \frac{1}{2} - x \right) + \sum_{j=1}^{(p-1)/2} \left( \binom{p-1}{j} \left( \frac{1}{2} - g^{-kj} x \right) - \frac{1}{2} \binom{(p-1)/2}{j} \right) g^{nj} \\ &\quad + \sum_{j=(p+1)/2}^{p-2} \binom{p-1}{j} \left( \frac{1}{2} - g^{-kj} x \right) g^{nj}. \end{aligned}$$

Ist  $x \neq g^{kj}/2$  für  $j = (p+1)/2, \dots, p-1$ , so gilt nach Hilfssatz 20

$$L(s_n + xz_n^{(k)}) \geq (p-1)/2.$$

Ist  $x = g^{kj_0}/2$  für ein  $(p+1)/2 \leq j_0 \leq p-1$ , so gilt  $(1/2 - g^{-kj}x) = 0$  genau dann, wenn  $kj \equiv kj_0 \pmod{p-1}$ . Mit  $d := \text{ggT}(k, p-1)$  ist das äquivalent zu

$$j \equiv j_0 \pmod{\frac{p-1}{d}}.$$

Dann sind höchstens

$$\left\lceil \frac{(p-1)/2}{(p-1)/d} \right\rceil = \lceil d/2 \rceil$$

Koeffizienten zu  $j = (p+1)/2, \dots, p-1$  gleich 0 bzw.

$$\frac{p-1}{2} - \left\lfloor \frac{d}{2} \right\rfloor$$

zu  $j = 1, \dots, (p-1)/2$  gleich 0. Daraus folgt

$$L(s_n + xz_n^{(k)}) \geq p-1 - ((p-1)/2 - \lfloor d/2 \rfloor + \lceil d/2 \rceil) \geq p-1 - (p+1)/2 = (p-3)/2$$

und somit der Satz. □

## 12 Literatur

1. Niederreiter: Random number generation and quasi-Monte Carlo methods, 1992.
2. Cusick/Ding/Renvall: Stream ciphers and number theory, 1999.
3. Shparlinski: Cryptographic applications of analytic number theory, 2003.
4. Knuth: The art of computer programming II, 1997.