3.5 Der Erwartungswert für die lineare Komplexität

Nachdem nun die Verteilung der linearen Komplexität exakt bestimmt ist, lassen sich auch Erwartungswert und Varianz bei fester Länge exakt bestimmen:

Hauptsatz 1 (Rueppel) *Für den Mittelwert*

$$E_N = \frac{1}{2^N} \cdot \sum_{u \in \mathbb{F}_2^N} \lambda(u)$$

und die Varianz V_N der linearen Komplexität aller Bitfolgen der Länge N gilt:

$$\begin{aligned} E_N &= \frac{N}{2} + \frac{2}{9} + \frac{\varepsilon}{18} - \frac{N}{3 \cdot 2^N} - \frac{2}{9 \cdot 2^N} \approx \frac{N}{2}, \\ V_N &= \frac{86}{81} - \frac{14-\varepsilon}{27} \cdot \frac{N}{2^N} - \frac{82-2\varepsilon}{81} \cdot \frac{1}{2^N} - \frac{9N^2+12N+4}{81} \cdot \frac{1}{2^{2N}} \approx \frac{86}{81} \end{aligned}$$

mit $\varepsilon = 0$ für gerades, $\varepsilon = 1$ für ungerades N.

Bemerkenswert ist, dass die Varianz von N praktisch unabhängig ist.

Zum Beweis muss man etwas ausholen; dabei treten Summen auf, die mit einem Trick aus der Analysis geschlossen ausgewertet werden können.

Hilfssatz 5 *Für die Funktion*

$$f\colon \mathbb{R} - \{1\} \longrightarrow \mathbb{R}, \quad f(x) = \frac{x^{r+1} - x}{x-1},$$

gilt:

$$\begin{aligned} f'(x) &= \frac{1}{(x-1)^2} \cdot \left[r x^{r+1} - (r+1)x^r + 1 \right], \\ f''(x) &= \frac{1}{(x-1)^3} \cdot \left[(r^2-r)x^{r+1} - 2(r^2-1)x^r + (r^2+r)x^{r-1} - 2 \right], \\ x^2 f''(x) + x f'(x) &= \frac{x}{(x-1)^3} \cdot \left[r^2 x^{r+2} - (2r^2+2r-1)x^{r+1} + (r+1)^2 x^r - x - 1 \right]. \end{aligned}$$

Beweis. Das folgt durch direkte Rechnung. $\diamond$

Mit Hilfe von f lassen sich folgende Summen berechnen:

Korollar 1 *Für alle $x \in \mathbb{R}$, $x \neq 1$, gilt:*

$$\begin{aligned} \sum_{i=1}^{r} x^i &= \frac{1}{x-1} \cdot \left[x^{r+1} - x \right], \\ \sum_{i=1}^{r} i x^i &= \frac{x}{(x-1)^2} \cdot \left[r x^{r+1} - (r+1)x^r + 1 \right], \\ \sum_{i=1}^{r} i^2 x^i &= \frac{x}{(x-1)^3} \cdot \left[r^2 x^{r+2} - (2r^2+2r-1)x^{r+1} + (r+1)^2 x^r - x - 1 \right]. \end{aligned}$$

Beweis. Aus der bekannten Formel für die geometrische Reihe folgt

$$\sum_{i=1}^{r} x^i = x \cdot \sum_{i=0}^{r-1} x^i = x \cdot \frac{x^r - 1}{x - 1} = f(x),$$

$$\sum_{i=1}^{r} i x^i = x \cdot \sum_{i=1}^{r} i x^{i-1} = x \cdot f'(x),$$

$$\sum_{i=1}^{r} i^2 x^i = \sum_{i=1}^{r} i(i-1)x^i + \sum_{i=1}^{r} i x^i = x^2 \cdot f''(x) + x \cdot f'(x).$$

Die behaupteten Formeln folgen also aus dem Hilfssatz 5. $\diamond$

Korollar 2

$$\begin{aligned} \sum_{i=1}^{r} i\, 2^{2i-1} &= \frac{3r-1}{9} \cdot 2^{2r+1} + \frac{2}{9}, \\ \sum_{i=1}^{r} i^2\, 2^{2i-1} &= \frac{3r^2 - 2r}{9} \cdot 2^{2r+1} + \frac{5}{27} \cdot 2^{2r+1} - \frac{10}{27}. \end{aligned}$$

Beweis.

$$\sum_{i=1}^{r} i 2^{2i-1} = \frac{1}{2} \cdot \sum_{i=1}^{r} i 4^i = \frac{1}{2} \cdot \frac{4}{9} \cdot \left[r 4^{r+1} - (r+1) 4^r + 1 \right] = \frac{2}{9} \cdot \left[3r 4^r - 4^r + 1 \right],$$

$$\begin{aligned} \sum_{i=1}^{r} i^2 2^{2i-1} &= \frac{1}{2} \cdot \sum_{i=1}^{r} i^2 4^i = \frac{1}{2} \cdot \frac{4}{27} \cdot \left[r^2 4^{r+2} - (2r^2 + 2r - 1) 4^{r+1} + (r+1)^2 4^r - 5 \right] \\ &= \frac{2}{27} \cdot \left[(9r^2 - 6r + 5) \cdot 4^r - 5 \right]. \end{aligned}$$

$\diamond$

Der Mittelwert über die lineare Komplexität ist nun

$$E_N = \frac{1}{2^N} \cdot \sum_{u \in \mathbb{F}_2^N} \lambda(u) = \frac{1}{2^N} \cdot \sum_{l=0}^{N} l \cdot \mu_N(l),$$

$$2^N E_N = \underbrace{\sum_{l=1}^{\lfloor \frac{N}{2} \rfloor} l \cdot 2^{2l-1}}_{S_1} + \underbrace{\sum_{l=\lceil \frac{N+1}{2} \rceil}^{N} l \cdot 2^{2(N-l)}}_{S_2}.$$

Sei zunächst N gerade. Dann ist

$$\begin{aligned}
S_1 &= \sum_{l=1}^{\frac{N}{2}} l \cdot 2^{2l-1} = \frac{3N-2}{18} \cdot 2^{N+1} + \frac{2}{9} = \frac{N}{3} \cdot 2^N - \frac{2}{9} \cdot 2^N + \frac{2}{9}\,, \\
S_2 &= \sum_{l=\frac{N}{2}+1}^{N} l \cdot 4^{N-l} \overset{k=N-l}{=} \sum_{k=0}^{\frac{N}{2}-1} (N-k) \cdot 4^k = N \cdot \sum_{k=0}^{\frac{N}{2}-1} 4^k - \sum_{k=0}^{\frac{N}{2}-1} k \cdot 4^k \\
&= N \cdot \frac{4^{N/2}-1}{3} - \frac{4}{9} \cdot \left[(\frac{N}{2} - 1) \cdot 4^{\frac{N}{2}} - \frac{N}{2} \cdot 4^{\frac{N}{2}-1} + 1 \right] \\
&= \frac{N}{3} \cdot 2^N - \frac{N}{3} - \frac{4}{9} \cdot \left[\frac{N}{2} \cdot 2^N - 2^N - \frac{N}{8} \cdot 2^N + 1 \right] \\
&= \left(\frac{N}{6} + \frac{4}{9} \right) \cdot 2^N - \frac{N}{3} - \frac{4}{9}.
\end{aligned}$$

Zusammen ergibt das

$$2^N E_N = \frac{N}{2} \cdot 2^N + \frac{2}{9} \cdot 2^N - \frac{N}{3} - \frac{2}{9}\,,$$

womit die erste Formel von Hauptsatz 1 für gerades N bewiesen ist.

Für ungerades N ist

$$\begin{aligned}
S_1 &= \sum_{l=1}^{\frac{N-1}{2}} l \cdot 2^{2l-1} = \frac{3(N-1)-2}{18} \cdot 2^N + \frac{2}{9} = \frac{3N-5}{18} \cdot 2^N + \frac{2}{9} \\
&= \frac{N}{6} \cdot 2^N - \frac{5}{18} \cdot 2^N + \frac{2}{9}\,, \\
S_2 &= \sum_{l=\frac{N+1}{2}}^{N} l \cdot 4^{N-l} \overset{k=N-l}{=} \sum_{k=0}^{\frac{N-1}{2}} (N-k) \cdot 4^k = N \cdot \sum_{k=0}^{\frac{N-1}{2}} 4^k - \sum_{k=0}^{\frac{N-1}{2}} k \cdot 4^k \\
&= N \cdot \frac{4^{(N+1)/2}-1}{3} - \frac{4}{9} \cdot \left[\frac{N-1}{2} \cdot 4^{\frac{N+1}{2}} - \frac{N+1}{2} \cdot 4^{\frac{N-1}{2}} + 1 \right] \\
&= \frac{N}{3} \cdot 2^{N+1} - \frac{N}{3} - \frac{4}{9} \cdot \left[\frac{N-1}{2} \cdot 2^{N+1} - \frac{N+1}{2} \cdot 2^{N-1} + 1 \right] \\
&= \frac{2N}{3} \cdot 2^N - \frac{N}{3} - \frac{4N}{9} \cdot 2^N + \frac{4}{9} \cdot 2^N + \frac{N}{9} \cdot 2^N + \frac{1}{9} \cdot 2^N - \frac{4}{9} \\
&= \left(\frac{N}{3} + \frac{5}{9} \right) \cdot 2^N - \frac{N}{3} - \frac{4}{9}\,,
\end{aligned}$$

$$2^N E_N = \frac{N}{2} \cdot 2^N + \frac{5}{18} \cdot 2^N - \frac{N}{3} - \frac{2}{9}\,,$$

womit die erste Formel von Hauptsatz 1 auch für ungerades N bewiesen ist.

Nun zur Berechnung der Varianz V_N. Es ist

$$\begin{aligned} V_N + 2^N E_N^2 &= \frac{1}{2^N} \cdot \sum_{u \in \mathbb{F}_2^N} \lambda(u)^2 = \frac{1}{2^N} \cdot \sum_{l=0}^{N} l^2 \cdot \mu_N(l), \\ &= \underbrace{\sum_{l=1}^{\lfloor \frac{N}{2} \rfloor} l^2 \cdot 2^{2l-1}}_{S_3} + \underbrace{\sum_{l=\lceil \frac{N+1}{2} \rceil}^{N} l^2 \cdot 4^{N-l}}_{S_4}. \end{aligned}$$

Sei wieder zuerst N gerade. Dann ergibt die erste Summe

$$\begin{aligned} S_3 &= \sum_{l=1}^{\frac{N}{2}} l^2 \cdot 2^{2l-1} = \frac{3 \cdot \frac{N^2}{4} - 2 \cdot \frac{N}{2}}{9} \cdot 2^{N+1} + \frac{5}{27} \cdot 2^{N+1} - \frac{10}{27} \\ &= \frac{N^2}{6} \cdot 2^N - \frac{2N}{9} \cdot 2^N + \frac{10}{27} \cdot 2^N - \frac{10}{27}. \end{aligned}$$

Die zweite Summe wird weiter zerlegt:

$$\begin{aligned} S_4 &= \sum_{l=\frac{N}{2}+1}^{N} l^2 \cdot 4^{N-l} \overset{k=N-l}{=} \sum_{k=0}^{\frac{N}{2}-1} (N-k)^2 \cdot 4^k \\ &= \underbrace{N^2 \cdot \sum_{k=0}^{\frac{N}{2}-1} 4^k}_{S_{4a}} - 2 \underbrace{N \cdot \sum_{k=0}^{\frac{N}{2}-1} k \cdot 4^k}_{S_{4b}} + \underbrace{\sum_{k=0}^{\frac{N}{2}-1} k^2 \cdot 4^k}_{S_{4c}} \end{aligned}$$

Diese werden einzeln ausgewertet:

$$\begin{aligned} S_{4a} &= N^2 \cdot \frac{4^{\frac{N}{2}} - 1}{3} = \frac{N^2}{3} \cdot 2^N - \frac{N^2}{3}, \\ S_{4b} &= N \cdot \frac{4}{9} \cdot \left[(\frac{N}{2} - 1) \cdot 4^{\frac{N}{2}} - \frac{N}{2} \cdot 4^{\frac{N}{2}-1} + 1 \right] \\ &= \frac{4N}{9} \cdot \left[\frac{N}{2} \cdot 2^N - 2^N - \frac{N}{8} \cdot 2^N + 1 \right] = \frac{N^2}{6} \cdot 2^N - \frac{4N}{9} \cdot 2^N + \frac{4N}{9}, \\ S_{4c} &= \frac{4}{27} \cdot \left[(\frac{N}{2} - 1)^2 \cdot 4^{\frac{N}{2}+1} - \left(2 \cdot (\frac{N}{2} - 1)^2 + 2 \cdot (\frac{N}{2} - 1) - 1 \right) \cdot 4^{\frac{N}{2}} \right. \\ &\qquad \left. + (\frac{N}{2})^2 \cdot 4^{\frac{N}{2}-1} - 5 \right] \\ &= \frac{4}{27} \cdot \left[2 \cdot (\frac{N^2}{4} - N + 1) \cdot 2^N - N \cdot 2^N + 2 \cdot 2^N + 2^N + \frac{N^2}{16} \cdot 2^N - 5 \right] \\ &= \frac{1}{12} \cdot N^2 \cdot 2^N - \frac{4}{9} \cdot N \cdot 2^N + \frac{20}{27} \cdot 2^N - \frac{20}{27}. \end{aligned}$$

Dazu kommt noch

$$\begin{aligned} 2^N \cdot E_N^2 &= \left[\frac{N}{2} + \frac{2}{9} - \frac{N}{3 \cdot 2^N} - \frac{2}{9 \cdot 2^N}\right]^2 \cdot 2^N \\ &= \frac{N^2}{4} \cdot 2^N + \frac{2N}{9} \cdot 2^N + \frac{4}{81} \cdot 2^N - \frac{N^2}{3} - \frac{10N}{27} - \frac{8}{81} \\ &\quad + \frac{N^2}{9 \cdot 2^N} + \frac{4N}{27 \cdot 2^N} + \frac{4}{81 \cdot 2^N} . \end{aligned}$$

Alles zusammen ergibt

$$2^N \cdot V_N = \frac{86}{81} \cdot 2^N - \frac{14N}{27} - \frac{82}{81} - \frac{N^2}{9 \cdot 2^N} - \frac{4N}{27 \cdot 2^N} - \frac{4}{81 \cdot 2^N},$$

womit die zweite Formel von Hauptsatz 1 für gerades N bewiesen ist.

Die entsprechende Berechnung für ungerades N ist:

$$\begin{aligned} S_3 &= \sum_{l=1}^{\frac{N-1}{2}} l^2 \cdot 2^{2l-1} = \frac{N^2}{12} \cdot 2^N - \frac{5N}{18} \cdot 2^N + \frac{41}{108} \cdot 2^N - \frac{10}{27} , \\ S_{4a} &= N^2 \cdot \sum_{k=0}^{\frac{N-1}{2}} 4^k = \frac{2N^2}{3} \cdot 2^N - \frac{N^2}{3} , \\ S_{4b} &= N \cdot \sum_{k=0}^{\frac{N-1}{2}} k \cdot 4^k = \frac{N^2}{3} \cdot 2^N - \frac{5N}{9} \cdot 2^N + \frac{4N}{9} , \\ S_{4c} &= \sum_{k=0}^{\frac{N-1}{2}} k^2 \cdot 4^k = \frac{N^2}{6} \cdot 2^N - \frac{5N}{9} \cdot 2^N + \frac{41}{54} \cdot 2^N - \frac{20}{27} , \\ 2^N \cdot E_N^2 &= \left[\frac{N}{2} + \frac{5}{18} - \frac{N}{3 \cdot 2^N} - \frac{2}{9 \cdot 2^N}\right]^2 \cdot 2^N \\ &= \frac{N^2}{4} \cdot 2^N + \frac{5N}{18} \cdot 2^N + \frac{25}{324} \cdot 2^N - \frac{N^2}{3} - \frac{11N}{27} - \frac{10}{81} \\ &\quad + \frac{N^2}{9 \cdot 2^N} + \frac{4N}{27 \cdot 2^N} + \frac{4}{81 \cdot 2^N} . \end{aligned}$$

Alles zusammen ergibt

$$\begin{aligned} 2^N \cdot V_N &= S_3 + S_{4a} - 2 \cdot S_{4b} + S_{4c} - 2^N \cdot E_N^2 \\ &= \frac{86}{81} \cdot 2^N - \frac{13N}{27} - \frac{80}{81} - \frac{9N^2 + 12N + 4}{81 \cdot 2^N} , \end{aligned}$$

womit Hauptsatz 1 vollständig bewiesen ist.