3.5 The Mean Value of the Linear Complexity

From the exact distribution of the linear complexity we also can exactly determine the mean value and the variance (for fixed length N):

Theorem 3 (Rueppel) *Explicit formulas for the mean value*

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

and the variance V_N of the linear complexity of all bit sequences of length N are:

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

where $\varepsilon = 0$ for N even, $\varepsilon = 1$ for N odd (ε is the parity of N).

Remarkably the variance is almost independent of N. Thus almost all linear complexities vary around the mean value in a small strip only that is (almost) independent of N and becomes *relatively* more narrow with increasing N as illustrated by Figures 3.5 and 3.6.

For the proof we have to make a small detour. We'll encounter sums that have a nice expression using a well-known trick from calculus.

Lemma 15 *For the derivatives of the function*

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

we have the formulas:

$$f'(x) = \frac{1}{(x-1)^2} \cdot \left[r x^{r+1} - (r+1)x^r + 1 \right],$$

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

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

Proof. By direct calculation. ◇

Using these formulas for f we explicitly calculate some sums:

Corollary 1 *For all $x \in \mathbb{R}$, $x \neq 1$, we have:*

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

Proof. From the sum formula for the geometric series we conclude

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

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

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

Therefore the claimed formulas follow from Lemma 15. ◇

Corollary 2

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

Proof.

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

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

◇

Now the mean value of the linear complexity is

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

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

First let N be even. Then

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

Taken together this yields

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

proving the first formula of Theorem 3 for N even.

For odd N we have

$$\begin{aligned}
S_1 &= \sum_{l=1}^{\frac{N-1}{2}} l \cdot 2^{2l-1} = \frac{3(N-1)-2}{18} \cdot 2^N + \frac{2}{9} = \frac{3N-5}{18} \cdot 2^N + \frac{2}{9} \\
&= \frac{N}{6} \cdot 2^N - \frac{5}{18} \cdot 2^N + \frac{2}{9},
\end{aligned}$$

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

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

proving the first formula of Theorem 3 also for odd N.

Now let's calculate the variance V_N. We start with

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

Again we first treat the case of even N. Then the first sum evaluates as

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

We decompose the second sum:

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

and separately evaluate the summands:

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

We have to subtract

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

All this fragments together yield

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

proving the second formula of Theorem 3 for even N.

The corresponding calculation for odd N is:

$$\begin{aligned}
S_3 &= \sum_{l=1}^{\frac{N-1}{2}} l^2\cdot 2^{2l-1} = \frac{N^2}{12}\cdot 2^N - \frac{5N}{18}\cdot 2^N + \frac{41}{108}\cdot 2^N - \frac{10}{27}\,,\\
S_{4a} &= N^2\cdot\sum_{k=0}^{\frac{N-1}{2}} 4^k = \frac{2N^2}{3}\cdot 2^N - \frac{N^2}{3}\,,\\
S_{4b} &= N\cdot\sum_{k=0}^{\frac{N-1}{2}} k\cdot 4^k = \frac{N^2}{3}\cdot 2^N - \frac{5N}{9}\cdot 2^N + \frac{4N}{9}\,,\\
S_{4c} &= \sum_{k=0}^{\frac{N-1}{2}} k^2\cdot 4^k = \frac{N^2}{6}\cdot 2^N - \frac{5N}{9}\cdot 2^N + \frac{41}{54}\cdot 2^N - \frac{20}{27}\,,
\end{aligned}$$

$$\begin{aligned} 2^N \cdot E_N^2 &= \left[\frac{N}{2} + \frac{5}{18} - \frac{N}{3 \cdot 2^N} - \frac{2}{9 \cdot 2^N}\right]^2 \cdot 2^N \\ &= \frac{N^2}{4} \cdot 2^N + \frac{5N}{18} \cdot 2^N + \frac{25}{324} \cdot 2^N - \frac{N^2}{3} - \frac{11N}{27} - \frac{10}{81} \\ &\quad + \frac{N^2}{9 \cdot 2^N} + \frac{4N}{27 \cdot 2^N} + \frac{4}{81 \cdot 2^N}\,. \end{aligned}$$

Putting the fragments together we get

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

This completes the proof of Theorem 3.