3.4 Der Erwartungswert für die lineare Komplexität

... lässt sich exakt bestimmen (ohne Beweis):

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.