Noch einmal unäre Primzahlen

Jetzt betrachten wir wieder die Sprache der unären Primzahlen:

$$L = \{a^m \mid m \text{ ist eine Primzahl}\}$$

Wäre diese Sprache kontextfrei, dann gäbe es nach dem Pumping Lemma eine Zahl n, so dass insbesondere für jede Primzahl $p > n + 2$ das Wort a^p so in fünf Teile $uvwxy$ zerlegbar wäre, dass uv^iwx^iy für jedes $i \geq 0$ zu L gehören würde.

Aber mit $r = |vx|$ gilt offenbar $|uv^iwx^iy| = p + r(i-1)$.

Insbesondere ist also $uv^{p+1}wx^{p+1}y = a^s$, und dabei gilt die Gleichung $s = p + r(p+1-1) = p(r+1)$. Aber da $p > 2$ und $r \geq 1$ gilt, ist s mit Sicherheit keine Primzahl, d.h. $uv^{p+1}wx^{p+1}y \notin L$ – im Widerspruch zum Pumping Lemma.

Einelementiges Alphabet

Die letzten beiden Beispiele der vorigen Einheit haben gezeigt, dass man Pumping Lemma Beweise bei einelementigem Alphabet von Typ-3 direkt auf Typ-2 übertragen kann. Das ist kein Zufall.

Es gilt nämlich folgender Satz:

Satz: Alle Typ-2 Sprachen über einem einelementigen Alphabet sind bereits regulär.

Beweis:

Es sei L eine Typ-2 Sprache über dem Alphabet $\{a\}$. Ferner sei n die Zahl aus dem Pumping Lemma, und z ein Wort aus L mit $|z| \geq n$.

Einelementiges Alphabet, Beweis (1)

Das Wort z lässt sich darstellen als $z = uvwxy$ mit den drei Bedingungen des Pumping Lemmas, also

$$|vx| > 0, \quad |vwx| \leq n \quad \text{und} \quad uv^i wx^i y \in L \text{ für alle } i \geq 0.$$

Andererseits können wir z auch so schreiben:

$$z = a^{|u|} a^{|v|} a^{|w|} a^{|x|} a^{|y|} = a^{|u|+|v|+|w|+|x|+|y|}$$

oder mit $k = |u| + |w| + |y|$ und $m = |v| + |x|$:

$$z = a^{k+m}$$

Die dritte Bedingung des Pumping Lemmas liest sich nun so:

$$a^{k+i \cdot m} \in L \text{ für alle } i \geq 0$$

Man beachte, dass hierbei m die Bedingung $1 \leq m \leq n$ erfüllt.

Einelementiges Alphabet, Beweis (2)

Wir haben gesehen, dass es für jedes lange Wort $z \in L$ einen Wert m aus der Menge $\{1, \ldots, n\}$ gibt, für den alle Worte der Form $z\, a^{i \cdot m}$ auch zu L gehören. Den Wert m nennen wir in diesem Fall die *Periode* von z. Wenn wir $q = n!$ setzen, ist jede Periode ein Teiler von q.

Andererseits bedeutet das: Für jedes lange Wort $z \in L$ sind auch alle Worte der Form $z\, a^{i \cdot q}$ in L.

Nun zerlegen wir die Menge L in maximal $q + 1$ viele (disjunkte) Teilmengen, nämlich eine für alle kurzen Wörter aus L, sowie maximal q Teilmengen für Wörter aus L, deren Länge einen bestimmten Rest (aus der Menge $\{0, \ldots, q - 1\}$) bei der Division durch q lässt.

Einelementiges Alphabet, Beweis (3)

Die Menge der kurzen Wörter aus L ist

$$L_{kurz} := \{a^i \mid i < q \text{ und } a^i \in L\}$$

und die q anderen Mengen sind

$$L_r := \{a^{r+iq} \mid i > 0 \text{ und } a^{r+iq} \in L\}$$

für $r = 0, \ldots, q-1$.

Man kann sich leicht vergewissern, dass die definierten $q+1$ Mengen paarweise disjunkt sind, und dass ihre Vereinigung genau L ergibt:

$$L = L_{kurz} \cup L_0 \cup \cdots \cup L_{q-1}$$

L_{kurz} ist eine endliche Menge und daher regulär. Wenn wir zeigen können, dass auch die L_r alle regulär sind, ist der Beweis komplett.

Einelementiges Alphabet, Beweis (4)

Wie kann L_r für festes $r \in \{0, \ldots, q-1\}$ aussehen?

1. Fall: $L_r = \emptyset$. Dann ist L_r regulär, wie gewünscht.

2. Fall: $L_r \neq \emptyset$. Dann gibt es ein minimales s mit $a^s \in L_r$.

Beh.: In diesem Fall gilt $L_r = \{a^{s+iq} \mid i \geq 0\}$.

Begründung: a^s ist ein langes Wort, da $s \geq q > n$. Also ist mit a^s auch jedes Wort der Form a^{s+iq} in L, da die Periode von a^s jedenfalls ein Teiler von q ist. Nach Definition sind diese Worte dann aber auch alle in L_r. Andererseits sind alle Worte aus L_r von der Form a^{s+iq} oder a^{s-iq} für natürliche Zahl i. Letztere kommen aber nicht in Frage, da s minimal gewählt war. Damit ist die Behauptung bewiesen.

Abschluss des Beweises

Wir haben gesehen, dass L eine Vereinigung der endlichen Menge L_{kurz} und der q Mengen von der Form L_r ist, von denen einige leer sein können. Die nicht leeren L_r sind aber immer in der Form $\{a^{s+iq} \mid i \geq 0\}$ darstellbar und deshalb regulär.

Ein regulärer Ausdruck für L_r wäre z.B. $a^s(a^q)^*$.

Das vervollständigt den Beweis.