1 Уравнения вида $A \circ X = B$

Рассмотрим уравнение $A \circ X = B$, где $\circ$ обозначает расширение любой бинарной операции на словах. Примеры таких операций является конкатенация и перетасовка ($\diamond$).

Утверждение 1.1. *Если уравнение $A \circ X = B$ имеет решение, то оно имеет единственное максимальное решение $X_{\max}$.*

Доказательство.

$$X_{max} = \{v \in \Sigma^* \mid A \circ \{v\} \subseteq B\}.$$

$\square$

Рассмотрим уравнение $AX = B$ с регулярными коэффициентами и конкатенацией.

Левой производной языка $L \subseteq \Sigma^*$ по слову $u \in \Sigma^*$ называется язык

$$u^{-1}L = \{w \in \Sigma^* \mid uw \in L\}.$$

Утверждение 1.2. *Регулярный язык имеет конечное число различных производных.*

Утверждение 1.3. *Если уравнение $AX = B$ имеет решение, то его максимальное решение $X_{\max}$ является регулярным языком.*

Доказательство.

$$X_{\max} = \bigcap_{u \in A} u^{-1}B.$$

$\square$

Как следствие имеем

Теорема 1.1. *Задача нахождения решения уравнения $AX = B$ алгоритмически разрешима.*

Утверждение 1.4. *Если уравнение $AX = B$ имеет решение, то оно имеет по крайней мере одно минимальное решение $X_{\min}$.*

Доказательство. Пусть $\mathcal{F} = \{X_i, i \in I\}$ есть множество всех решений уравнения. Интерес представляет случай, когда $\mathcal{F}$ бесконечно. Пусть в $\mathcal{F}$ существует бесконечная цепь $\mathcal{C} = \{X_j \mid j \in J\}$:

$$X \supseteq X_1 \supseteq \ldots \supset X_n \supset \ldots.$$

Рассмотрим язык $\overline{X} = \cap_{j \in J} X_j$ и докажем, что $\overline{X}$ является решением. Во-первых, $\overline{X} \neq \varnothing$ (рассмотрим разложение самого короткого слова в B). Далее, $\overline{X} \subseteq X$, а значит $A\overline{X} \subseteq B$. Осталось доказать обратное вложение $A\overline{X} \supseteq B$.

Пусть $w \in B$ и $P = \{(u_1, v_1), \ldots, (u_k, v_k)\}$ есть множество разложений слова w, т.е. $u_i \in A$, $v_i \in X$, $u_i v_i = w$. Тогда найдется такой элемент $(u, v) \in P$, что $v \in Y_j$ для всех $j \in J$. Предположим обратное. Для каждого $m = 1, \ldots, k$ выберем j_m таким, что $v_m \notin X_{j_m}$ и рассмотрим язык $T = \cap X_{j_m}$. Существует индекс $k \in J$ такой, что $T = X_k$, а значит $AT = B$ и слово w можно разложить. Противоречие. Существование минимального решения следует из леммы Цорна: если в частично упорядоченном множестве каждая цепь имеет нижнюю грань, то в этом множестве есть по крайней мере один минимальный элемент. $\square$

Доказательство существования минимального решения не гарантирует его регулярности и не дает алгоритма нахождения минимального решения.

Теорема 1.2. *Задача проверки минимальности заданного решения уравнения $AX = B$ алгоритмически разрешима.*

Доказательство. Решение F уравнения $AX = B$ является минимальным, если множество "лишних" слов языка F

$$E = \{v \in F \mid A(F \setminus \{v\}) = B\}$$

пусто, или $F - E = F$.

Покажем, что множество слов языка B, которые имеют единственное разложение по A и F

$$U(A, F) = \{w \in AF \mid \forall u_1, u_2 \in A\ u_1^{-1}w, u_2^{-1}w \in F \Rightarrow u_1 = u_2\}$$

регулярно и может быть эффективно построено. Пусть языки A и F распознаются детерминированными автоматами $\mathcal{A} = \langle \Sigma, Q, \delta, q_\circ, T \rangle$ и $\mathcal{F} = \langle \Sigma, S, \gamma, s_\circ, G \rangle$, соответственно.

Построим булев автомат $\mathbb{U} = \langle \Sigma, S \cup Q, \rho, q_\circ, G \rangle$ со следующей функцией переходов $(p \in S \cup Q,\ a \in \Sigma)$:

$$\rho(p, a) = \begin{cases} p', & p \in Q \setminus T \text{ и } \delta(p, a) = p' \\ (p'_a \wedge \neg p'_f) \vee (\neg p'_a \wedge p'_f), & p \in T, \delta(p, a) = p'_a, \gamma(s_\circ, a) = p'_f. \\ p', & p \in S \text{ и } \gamma(p, a) = p' \end{cases}$$

Этот автомат распознает однозначную конкатенацию языков A и F. Теперь построим искомое множество

$$F \setminus E = F \cap \left(\bigcup_{w \in U(A,F)} w^{-1} U(A, F) \right).$$

Проверка минимальности сводится к проверке равенства $F = F \setminus E$. □