Sei A Alphabet und $P = f_1, \ldots, f_k \subset A^* \times A^*$. Wir betrachten das von P in $A^* \times A^*$ erzeugte Untermonoid $\langle P \rangle$ und bilden

$$\mathfrak{K} = \langle P \rangle \cap \{(w, w) \mid w \in A^*\}.$$

Der zweite Teil des Ausdrucks enthält das Untermonoid von $A^* \times A^*$, dessen Elemente auf der „Diagonale" liegen. $\mathfrak{K}$ ist offensichtlich auch ein Untermonoid von $A^* \times A^*$.

Problem: Enthält $\mathfrak{K}$ mehr als nur die Einheit ε, in anderen Worten: Gibt es Indizes $i_1, \ldots, i_j$, so daß

$$p_{i_1} \cdot p_{i_2} \cdot \ldots \cdot p_{i_j} = q_{i_1} \cdot q_{i_2} \cdot \ldots \cdot q_{i_j}, \; j > 0.$$

gilt, wenn $f_i = (p_i, q_i)$ ist.

Definition: P heißt **kombinierbar** $\iff \mathfrak{K} \neq \varepsilon$.

Das Problem „P kombinierbar?" ist das **Post'sche Korrespondenzproblem**.

Satz: Das Korrespondenzproblem ist nicht entscheidbar.

Beweis: Zum Beweis gehen wir von einem Semi-Thue-System $\mathfrak{S} = (\mathcal{A}^*, P, \rightarrow)$ und reduzieren das Wortproblem $u \xrightarrow{\mathfrak{S}} v$ auf das Korrespondenzproblem. Hieraus ergibt sich dann die Nichtentscheidbarkeit.

Zunächst ordnen wir P ein Produktionensystem P' zu. Wir bedienen uns hierbei der folgenden Schreibweise

$$\underline{u} = (u, u) \quad , \quad \underline{u}^\beta = (u^\beta, {}^\beta u)$$

$$\begin{aligned} (u_1, \ldots, u_n)^\beta &= u_1 \beta u_2 \beta u_3 \ldots \beta u_n \beta, \\ {}^\beta(u_1, \ldots, u_n) &= \beta u_1 \beta u_2 \ldots \beta u_n \end{aligned}$$

Wir führen zwei neue Hilfssymbole $\beta, \gamma \notin \mathcal{A}$ ein und setzen

$${}^\beta g_u = (\gamma\gamma\beta, \gamma\gamma^\beta(u\gamma)), \;\; g_v^\beta = ((\gamma v)^\beta \gamma, \beta\gamma).$$

Nun setzen wir

$$P' = \{\underline{a}^\beta \mid a \in \mathcal{A}\} \cup \{\underline{\gamma}^\beta\} \cup \{f^\beta \mid f \in P\} \cup \{{}^\beta g_u, g_v^\beta\}$$

Das Element γ dient als Trennzeichen zwischen den Wörtern, die in Ableitungen erzeugt werden. Das Zeichen β dient zum Sperren trivialer Kombinationen (a, a).

Sei nun also

$$\begin{aligned} F = (\underline{u_1} \times f_1 \times \underline{v_1}) \circ (\underline{u_2} \times f_2 \times v_2) \\ \circ \ldots \circ (\underline{u_m} \times f_m \times \underline{v_m}) \end{aligned}$$

eine Ableitung

$$u \xrightarrow{F} v,\ \ f_i \in P \text{ für } i = 1, \ldots, m.$$

Wir ordnen F das Produkt

$$\begin{aligned} F' = {}^\beta g_u \cdot (\underline{u_1}^\beta \cdot f_1^\beta \cdot \underline{v_1}^\beta) \cdot \underline{\gamma}^\beta \cdot (\underline{u_2}^\beta \cdot f_2^\beta \cdot \underline{v_3}^\beta) \\ \cdot \ldots \cdot \underline{\gamma}^\beta \cdot (\underline{u_m}^\beta \cdot f_m^\beta \cdot v_m^\beta) \cdot g_v^\beta \end{aligned}$$

zu. Das Produkt liegt in dem Monoid $(\mathcal{A} \cup \{\beta, \gamma\})^* \times (\mathcal{A} \cup \{\beta, \gamma\})^*$.

Wir zeigen: F' liegt genau dann auf der Diagonale, wenn $u \xrightarrow{F} v$ gilt.

Zum Beweis bezeichnen wir mit F_i das i-te Präfix von F. Wir setzen also

$$
\begin{aligned}
F'_0 &= {}^{\beta}g_u,\ F_1 = F'_0 \cdot (\underline{u_1}^{\beta} \cdot f_1^{\beta} \cdot \underline{v_1}^{\beta}) \cdot \underline{\gamma}^{\beta} \\
F'_{i+1} &= F'_i \cdot (\underline{u_{i+1}^{\beta}} \cdot f_{i+1}^{\beta} \cdot \underline{v_{i+1}^{\beta}}) \cdot \underline{\gamma}^{\beta} \\
&\qquad \text{für } i = 1, \ldots, m-2, \\
F'_m &= F'_{m-1} \cdot (\underline{u_m^{\beta}} \cdot f_m^{\beta} \cdot \underline{v_m^{\beta}}) \cdot g_v^{\beta}
\end{aligned}
$$

Mit $Q(F'_i)$ bezeichnen wir die erste, mit $Z(F'_i)$ die zweite Komponente. Wir haben dann mit $f = (p, q)$:

$$
Z(F'_0) = Q(F'_0) \cdot u^{\beta} \cdot \gamma,
$$
$$
Z(F'_i) = Q(F'_i) \cdot (u_i, q_i, v_i)^{\beta} \cdot \gamma.
$$