## Post'sche Korrespondenzproblem

Reservoir von k Spielkartentypen

| 1 | 10 | 011 | 10 |
|---|---|---|---|
| 101 | 00 | 11 | 111 |

Frage: Kann man Spielkarten (mit möglichen Wiederholungen) so nebeneinanderlegen, dass sich oben und <u>unten</u> das gleiche Wort ergibt ?

| 1 | 011 | 10 | 011 |
|---|---|---|---|
| 101 | 11 | 00 | 11 |



## Post'sche Korrespondenzproblem $PCP_\Sigma$

Gegeben: $k \in \mathbb{N}$, $((x_1,y_1),(x_2,y_2),\cdots,(x_k,y_k)) \in (\Sigma^*)^{2k}$

Frage: Gibt es $I \in \{1,\cdots,k\}^*$ mit $X[I] = Y[I]$

$I = (i_1,i_2,\cdots,i_n)$

$X[I] = x_{i_1} x_{i_2} \cdots x_{i_n}$

$Y[I] = y_{i_1} y_{i_2} \cdots y_{i_n}$



**Satz:** PCP ist nicht entscheidbar.

**Beweis:**

UNIV $\preceq$ WORT $\preceq$ MPCP $\preceq$ PCP,

also

UNIV $\preceq$ PCP .

Da UNIV unentscheidbar, ist also auch PCP unentscheidbar.



## Modifiziertes Post'sche Korrespondenzproblem $MPCP_\Sigma$

Gegeben: $k \in \mathbb{N}$, $((x_1,y_1),(x_2,y_2),\cdots,(x_k,y_k)) \in (\Sigma^*)^{2k}$

Frage: Gibt es $I \in \{1,\cdots,k\}^*$ mit $X[I] = Y[I]$

**und** $i_1 = 1$

$I = (i_1,i_2,\cdots,i_n)$

$X[I] = x_{i_1} x_{i_2} \cdots x_{i_n}$

$Y[I] = y_{i_1} y_{i_2} \cdots y_{i_n}$



**Beh:** $MPCP_\Sigma \preceq PCP_{\Sigma\cup\{\#,\$\}}$



**Beh:** $MPCP_\Sigma \preceq PCP_{\Sigma\cup\{\#,\$\}}$

Beweis:

$( k , ((x_1,y_1),\cdots,(x_k,y_k)) )$

**Beh:** $MPCP_\Sigma \preceq PCP_{\Sigma\cup\{\#,\$\}}$

Beweis:

$$( k , ((x_1,y_1),\cdots,(x_k,y_k)) ) \quad\rightarrow\quad ( k+2, ((\bar{x}_1,\grave{y}_1), (\acute{x}_1,\grave{y}_1),\cdots, (\acute{x}_k,\grave{y}_k), (\$,\#\$)) )$$



**Beh:** $MPCP_\Sigma \preceq PCP_{\Sigma\cup\{\#,\$\}}$

Beweis:

$$( k , ((x_1,y_1),\cdots,(x_k,y_k)) ) \quad\rightarrow\quad ( k+2, ((\bar{x}_1,\grave{y}_1), (\acute{x}_1,\grave{y}_1),\cdots, (\acute{x}_k,\grave{y}_k), (\$,\#\$)) )$$

$$a = a_1a_2\cdots a_m$$
$$\bar{a} = \#a_1\#a_2\#\cdots\#a_m\#$$
$$\acute{a} = a_1\#a_2\#\cdots\#a_m\#$$
$$\grave{a} = \#a_1\#a_2\#\cdots\#a_m$$



## WORT: Das Wortproblem

**Gegeben:** Eine Grammatik $G = (\Sigma,V,S,P)$ und ein Wort $w\in\Sigma^*$

**Frage:** Ist $w\in L(G)$ ? Also, wird $w$ von $G$ generiert?



## WORT: Das Wortproblem

**Gegeben:** Eine Grammatik $G = (\Sigma,V,S,P)$ und ein Wort $w\in\Sigma^*$

**Frage:** Ist $w\in L(G)$ ? Also, wird $w$ von $G$ generiert?

Als Sprache ausgedrückt:

WORT = { cod(G)\$cod(w) | $w\in L(G)$ }



## WORT: Das Wortproblem

**Gegeben:** Eine Grammatik $G = (\Sigma,V,S,P)$ und ein Wort $w\in\Sigma^*$

**Frage:** Ist $w\in L(G)$ ? Also, wird $w$ von $G$ generiert?

Als Sprache ausgedrückt:

WORT = { cod(G)\$cod(w) | $w\in L(G)$ }

**Beh:** UNIV $\preceq$ WORT



## WORT: Das Wortproblem

**Gegeben:** Eine Grammatik $G = (\Sigma,V,S,P)$ und ein Wort $w\in\Sigma^*$

**Frage:** Ist $w\in L(G)$ ? Also, wird $w$ von $G$ generiert?

Als Sprache ausgedrückt:

WORT = { cod(G)\$cod(w) | $w\in L(G)$ }

**Beh:** UNIV $\preceq$ WORT

Beweis schon bei Äquivalenz von TM und Grammatiken gegeben.

**Beh:** WORT $\preceq$ MPCP



**Beh:** WORT $\preceq$ MPCP

Beweisidee: Gegeben Grammatik $G=(\Sigma,V,S,P)$ und Wort $w$,
baue MPCP, dessen Lösung eine Derivation $S \Rightarrow_G w$ darstellt.

$$w \Leftarrow U_m \Leftarrow U_{m-1} \Leftarrow U_{m-2} \Leftarrow \cdots \Leftarrow U_2 \Leftarrow U_1 \Leftarrow S$$



**Beh:** WORT $\preceq$ MPCP

Beweisidee: Gegeben Grammatik $G=(\Sigma,V,S,P)$ und Wort $w$,
baue MPCP, dessen Lösung eine Derivation $S \Rightarrow_G w$ darstellt.

$$w \Leftarrow U_m \Leftarrow U_{m-1} \Leftarrow U_{m-2} \Leftarrow \cdots \Leftarrow U_2 \Leftarrow U_1 \Leftarrow S$$

$$w \Leftarrow U_m \Leftarrow U_{m-1} \Leftarrow U_{m-2} \Leftarrow \cdots \Leftarrow U_2 \Leftarrow U_1 \Leftarrow S$$



**Beh:** WORT $\preceq$ MPCP

Beweisidee: Gegeben Grammatik $G=(\Sigma,V,S,P)$ und Wort $w$,
baue MPCP, dessen Lösung eine Derivation $S \Rightarrow_G w$ darstellt.

$$€w \Leftarrow U_m \Leftarrow U_{m-1} \Leftarrow U_{m-2} \Leftarrow \cdots \Leftarrow U_2 \Leftarrow U_1 \Leftarrow S \quad \$$$

$$€ \quad w \Leftarrow U_m \Leftarrow U_{m-1} \Leftarrow U_{m-2} \Leftarrow \cdots \Leftarrow U_2 \Leftarrow U_1 \Leftarrow S\$$$



**Beh:** WORT $\preceq$ MPCP

Beweisidee: Gegeben Grammatik $G=(\Sigma,V,S,P)$ und Wort $w$,
baue MPCP, dessen Lösung eine Derivation $S \Rightarrow_G w$ darstellt.

$$\boxed{\begin{matrix}€w \Leftarrow \\ €\end{matrix}}\, U_m \boxed{\begin{matrix}\Leftarrow \\ w \Leftarrow\end{matrix}} U_{m-1} \boxed{\begin{matrix}\Leftarrow \\ \Leftarrow\end{matrix}} \begin{matrix}U_{m-2} \\ U_{m-1}\end{matrix} \boxed{\begin{matrix}\Leftarrow \\ \Leftarrow\end{matrix}} \cdots \boxed{\begin{matrix}\Leftarrow \\ \Leftarrow\end{matrix}} U_2 \boxed{\begin{matrix}\Leftarrow \\ \Leftarrow\end{matrix}} U_1 \boxed{\begin{matrix}\Leftarrow \\ \Leftarrow\end{matrix}} S \boxed{\begin{matrix}\$ \\ \Leftarrow S\$\end{matrix}}$$

| 0 | 0 | 1 | A | 0 | 0 | 1 | B | 1 | 1 |
|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 1 | A | 0 | 0 | 1 | A0 | 1 | 1 |

Bei Produktion
$B \rightarrow A0$
in $P$



**Beh:** WORT $\preceq$ MPCP

Beweisidee: Gegeben Grammatik $G=(\Sigma,V,S,P)$ und Wort $w$,
baue MPCP, dessen Lösung eine Derivation $S \Rightarrow_G w$ darstellt.

$$\boxed{\begin{matrix}€w \Leftarrow \\ €\end{matrix}}\, U_m \boxed{\begin{matrix}\Leftarrow \\ w \Leftarrow\end{matrix}} U_{m-1} \boxed{\begin{matrix}\Leftarrow \\ \Leftarrow\end{matrix}} \begin{matrix}U_{m-2} \\ U_{m-1}\end{matrix} \boxed{\begin{matrix}\Leftarrow \\ \Leftarrow\end{matrix}} \cdots \boxed{\begin{matrix}\Leftarrow \\ \Leftarrow\end{matrix}} U_2 \boxed{\begin{matrix}\Leftarrow \\ \Leftarrow\end{matrix}} U_1 \boxed{\begin{matrix}\Leftarrow \\ \Leftarrow\end{matrix}} S \boxed{\begin{matrix}\$ \\ \Leftarrow S\$\end{matrix}}$$

Grammatik $G = (\{a_1,\cdots,a_s\}, \{B_1,\cdots,B_t\}, B_1, \{\alpha_1 \rightarrow \beta_1, \cdots, \alpha_r \rightarrow \beta_r\})$, Wort $w$

**Beh:** WORT $\preceq$ MPCP

Beweisidee: Gegeben Grammatik $G=(\Sigma,V,S,P)$ und Wort $w$,
baue MPCP, dessen Lösung eine Derivation $S \Rightarrow_G w$ darstellt.

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| €w ⇐ | $U_m$ | ⇐ | $U_{m-1}$ | ⇐ | $U_{m-2}$ | ⇐ | ··· | ⇐ | $U_2$ | ⇐ | $U_1$ | ⇐ | S | $ |
| € | w | ⇐ | $U_m$ | ⇐ | $U_{m-1}$ | ⇐ | $U_{m-2}$ | ⇐ | ··· | ⇐ | $U_2$ | ⇐ | $U_1$ | ⇐ S$ |

Grammatik $G = ( \{a_1,\cdots,a_s\} ,\ \{B_1,\cdots,B_t\} ,\ B_1,\ \{\alpha_1\to\beta_1, \cdots , \alpha_r\to\beta_r\} )$, Wort $w$

**MPCP**

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| €w⇐ | ⇐ | $a_1$ | … | $a_s$ | $B_1$ | … | $B_t$ | $\alpha_1$ | … | $\alpha_r$ | $ |
| € | ⇐ | $a_1$ | … | $a_s$ | $B_1$ | … | $B_t$ | $\beta_1$ | … | $\beta_r$ | ⇐S$ |



**Satz:** PCP ist nicht entscheidbar.



**Satz:** PCP ist nicht entscheidbar.

**Beweis:**

UNIV $\preceq$ WORT $\preceq$ MPCP $\preceq$ PCP,

also

UNIV $\preceq$ PCP .

Da UNIV unentscheidbar, ist also auch PCP unentscheidbar.



## Der Rekursionssatz

**Ziel:** Turingmaschinen sollen ihre eigene Kodierung in ihren Berechnungen verwenden können

**Einfache Turingmaschine:** ein Band
anfangs Eingabeband,
dann Arbeitsband,
am Schluss Ausgabeband

$\langle M \rangle$ Kodierung von TM $M$

Komposition von TMen: $\langle A\rangle\#\langle B\rangle\#\langle C\rangle \ldots$
Turingmaschine $A$ läuft mit Eingabe $x$, hinterlässt $y$;
dann läuft TM $B$ mit Eingabe $y$, hinterlässt $z$;
dann läuft TM $C$ mit Eingabe $z$, usf.



**Beh.:** Es gibt eine TM $Q$, die bei Eingabe $w \in \Sigma^*$
die Kodierung einer TM $\langle PRINT_w \rangle$ produziert,
die folgendes Eingabe/Ausgabe-Verhalten hat:
Eingabe $x$, Ausgabe $w$

$B$ TM mit folgendem Verhalten: $z \xrightarrow{B} \langle PRINT_z \rangle \# z$

$A$ TM $PRINT_{\langle B \rangle}$, also Verhalten: $x \xrightarrow{A} \langle B \rangle$

$\langle A\rangle\#\langle B\rangle$ , TM zuerst $A$ dann $B$ hat folgendes Verhalten:

$$x \xrightarrow{A} \langle B \rangle \xrightarrow{B} \underbrace{\langle PRINT_{\langle B \rangle} \rangle}_{A} \# \langle B \rangle$$

Also $\langle A\rangle\#\langle B\rangle$ ignoriert (und löscht) die Eingabe und produziert **seine eigene Beschreibung**



**Rekursionssatz** $t : \Sigma^* \times \Sigma^* \to \Sigma^*$ von TM $T$ berechnet
( Eingabe hat Form $u\$v$ )
$\exists$ TM $R$, die die Funktion $r : \Sigma^* \to \Sigma^*$ mit
$$r(x) = t( \langle R \rangle , x )$$
berechnet.

Man darf also annehmen, dass eine TM (oder auch ein Programm) auf seine eigene Beschreibung Zugriff hat.

**Rekursionssatz** $t : \Sigma^* \times \Sigma^* \to \Sigma^*$ von TM $T$ berechnet
( Eingabe hat Form $u\$v$ )
$\exists$ TM $R$, die die Funktion $r : \Sigma^* \to \Sigma^*$ mit
$r(x) = t(\langle R \rangle, x)$
berechnet.

Sei $T$ TM mit $u\$v \xrightarrow{T} t(u,v)$

$PREPRINT_z$ TM mit $x \xrightarrow{PREPRINT_z} zx$

$B$ TM mit $z\$w \xrightarrow{B} \langle PREPRINT_{z\$} \rangle\#z\$w$

$A$ TM $PREPRINT_{\langle B\rangle\#\langle T\rangle\$}$ $x \xrightarrow{A} \langle B \rangle\#\langle T \rangle\$x$



Sei $T$ TM mit $u\$v \xrightarrow{T} t(u,v)$

$PREPRINT_z$ TM mit $x \xrightarrow{PREPRINT_z} zx$

$B$ TM mit $z\$w \xrightarrow{B} \langle PREPRINT_{z\$} \rangle\#z\$w$

$A$ TM $PREPRINT_{\langle B\rangle\#\langle T\rangle\$}$ $x \xrightarrow{A} \langle B \rangle\#\langle T \rangle\$x$

Betrachte TM $R$ kodiert durch $\langle A \rangle\#\langle B \rangle\#\langle T \rangle$

$$x \xrightarrow{A} \langle B \rangle\#\langle T \rangle\$\,x \xrightarrow{B} \underbrace{\langle PREPRINT_{\langle B\rangle\#\langle T\rangle\,\$} \rangle}_{A}\#\langle B\rangle\#\langle T\rangle\$x$$

$$\langle A\rangle\#\langle B\rangle\#\langle T\rangle\ \$\,x \xrightarrow{T} t(\langle A\rangle\#\langle B\rangle\#\langle T\rangle, x)$$



Betrachte TM $R$ kodiert durch $\langle A \rangle\#\langle B \rangle\#\langle T \rangle$

$$x \xrightarrow{A} \langle B \rangle\#\langle T \rangle\$\,x \xrightarrow{B} \underbrace{\langle PREPRINT_{\langle B\rangle\#\langle T\rangle\,\$} \rangle}_{A}\#\langle B\rangle\#\langle T\rangle\$x$$

$$\underbrace{\langle A\rangle\#\langle B\rangle\#\langle T\rangle}_{\langle R\rangle}\ \$\,x \xrightarrow{T} t(\underbrace{\langle A\rangle\#\langle B\rangle\#\langle T\rangle}_{\langle R\rangle}, x)$$

**Rekursionssatz** $t : \Sigma^* \times \Sigma^* \to \Sigma^*$ von TM $T$ berechnet
( Eingabe hat Form $u\$v$ )
$\exists$ TM $R$, die die Funktion $r : \Sigma^* \to \Sigma^*$ mit
$r(x) = t(\langle R \rangle, x)$
berechnet.