SAARLAND UNIVERSITY
COMPUTER SCIENCE

Undecidability of the Post Correspondence Problem

Second Bachelor Seminar Talk

Edith Heiter

Advisors: Prof. Dr. Gert Smolka, Yannick Forster

May 12, 2017

Post Correspondence Problem

$A_{TM} = \{(M, w) \in TM \times \Sigma^* \mid \text{M accepts w }\}$

$$A_{TM} \quad \leq_m \quad PCP$$

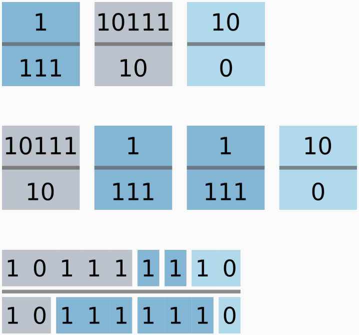
Σ : discrete type

domino := $\Sigma^* \times \Sigma^*$

pcp := finite set of dominos

A list S is a solution of a PCP instance P if

$S \neq \emptyset \wedge S \subseteq P \wedge match\, S$



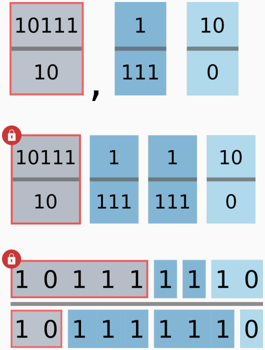
Modified Post Correspondence Problem

$A_{TM} = \{(M, w) \in TM \times \Sigma^* \mid \text{M accepts w } \}$
$PCP = \{P : pcp \mid \exists\, S \,.\, S \neq \emptyset \wedge S \subseteq P \wedge match\, S\}$

$$A_{TM} \quad \leq_m \quad MPCP \quad \leq_m \quad PCP$$

mpcp := domino $\times$ *pcp*

A list S is a solution of an MPCP instance (f, P) if
$S \subseteq P \cup \{F\} \wedge \text{match } (f :: S)$



Modified Post Correspondence ProblemReduction

$$A_{TM} = \{(M, w) \in TM \times \Sigma^* \mid \text{M accepts w } \}$$

$$PCP = \{P : pcp \mid \exists\, S \,.\, S \neq \emptyset \,\wedge\, S \subseteq P \,\wedge\, match\, S\}$$

$$MPCP = \{(f, P) : mpcp \mid \exists\, S \,.\, S \subseteq P \cup \{f\} \,\wedge\, match\,(f :: S)\}$$

$$A_{TM} \quad \leq_m \quad \boxed{MPCP \quad \leq_m \quad PCP}$$

$$f(P) = \left\{ \left[\frac{\star x_1}{y_1 \star}\right], \left[\frac{\star x_2}{y_2 \star}\right], \ldots, \left[\frac{\star x_k}{y_k \star}\right], \left[\frac{\star x_1}{\star y_1 \star}\right], \left[\frac{\#\$}{\$}\right] \right\}$$

Modified Post Correspondence ProblemReduction

$A_{TM} = \{(M, w) \in TM \times \Sigma^* \mid \text{M accepts w } \}$

$PCP = \{P : \mathit{pcp} \mid \exists\, S \,.\, S \neq \emptyset \,\wedge\, S \subseteq P \,\wedge\, \mathit{match}\, S\}$

$MPCP = \{(f, P) : \mathit{mpcp} \mid \exists\, S \,.\, S \subseteq P \cup \{f\} \,\wedge\, \mathit{match}\,(f :: S)\}$

$$\boxed{A_{TM} \qquad \leq_m \quad MPCP} \quad \leq_m \qquad PCP$$

Define a reduction g and prove its correctness

$(M, w) \in A_{TM} \Leftrightarrow g(M, w) \in MPCP$

Formalization of Turing Machines

Turing machine over finite alphabet Σ

$TM := (Q, \delta, q_0, F)$ with

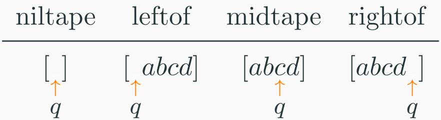
Q : finite type of states

$\delta : Q \times \Sigma_\perp \to$
$Q \times \Sigma_\perp \times \{L, N, R\}$

$q_0 : Q$ initial state

$F \subseteq Q$ set of halting states

```
Inductive tape : Type :=
|niltape : tape
|leftof : Σ → list Σ → tape
|rightof : Σ → list Σ → tape
|midtape : list Σ → Σ → list Σ → tape.
```



niltape	leftof	midtape	rightof
$[\ ]$	$[\ abcd]$	$[abcd]$	$[abcd\ ]$
$\uparrow$ q	$\uparrow$ q	$\uparrow$ q	$\uparrow$ q

A **configuration** consists of the current state and the tape.

TM Acceptability

Inductive predicate $\rightarrow_M^i$ defining reachability

$$\frac{}{c \rightarrow_M^0 c} \qquad\qquad \frac{c_1 \rightarrow_M^i c_2 \qquad \text{state } c_2 \notin F}{c_1 \rightarrow_M^{(Si)} (\text{step } c_2)}$$

TM M accepts configuration c_0 if $\exists\, i\, c_f.\ c_0 \rightarrow_M^i c_f \ \wedge\ \text{state } c_f \in F$

String representation $\langle\cdot\rangle$ of configurations

tape	niltape	leftof	midtape	rightof
c	$[\underset{\underset{q}{\uparrow}}{\ }]$	$[\underset{\underset{q}{\uparrow}}{\ }abcd]$	$[ab\underset{\underset{q}{\uparrow}}{c}d]$	$[abcd\underset{\underset{q}{\uparrow}}{\ }]$
$\langle c\rangle$	$[\mathbf{q}\_]$	$[\mathbf{q}\_abcd]$	$[ab\mathbf{q}cd]$	$[abcd\mathbf{q}]$

Constructing an MPCP Match

Example: Turing machine T accepts all inputs with an even number of a-symbols, replacing them with x.

$$[\underset{\substack{\uparrow\\ q_0}}{a}\,ba] \to [x\,\underset{\substack{\uparrow\\ q_1}}{b}\,a] \to [xb\,\underset{\substack{\uparrow\\ q_1}}{a}\,] \to [xbx\,\underset{\substack{\uparrow\\ q_0}}{}\,] \to [xb\,\underset{\substack{\uparrow\\ q_f}}{x}\,]$$

C_I $\left[\frac{}{\star q_0 aba}\right]$

C_C $\left[\frac{\star}{\star}\right]$ and $\left[\frac{s}{s}\right]$ $\forall s \in \Sigma$

C_T $\left[\frac{q_0 a}{x q_1}\right], \left[\frac{q_1 b}{b q_1}\right], \left[\frac{q_1 a}{x q_0}\right], \left[\frac{x q_0 \star}{q_f x \star}\right], \ldots$

C_D $\left[\frac{s\, q_f}{q_f}\right], \left[\frac{q_f\, s}{q_f}\right]$ $\forall s \in \Sigma$

C_F $\left[\frac{q_f \star}{}\right]$

$$\left[\frac{}{\star q_0 aba}\right]\left[\frac{\star}{\star}\right]\left[\frac{q_0 a}{x q_1}\right]\left[\frac{b}{b}\right]\left[\frac{a}{a}\right]\left[\frac{\star}{\star}\right]\left[\frac{x}{x}\right]\left[\frac{q_1 b}{b q_1}\right]\left[\frac{a}{a}\right]\left[\frac{\star}{\star}\right]\left[\frac{x}{x}\right]\left[\frac{b}{b}\right]\left[\frac{q_1 a}{x q_0}\right]\left[\frac{\star}{\star}\right]\left[\frac{x}{x}\right]\left[\frac{b}{b}\right]\left[\frac{x q_0 \star}{q_f x \star}\right] \to$$

$$\to \left[\frac{\star}{\star}\right]\left[\frac{x}{x}\right]\left[\frac{b}{b}\right]\left[\frac{q_f\, x}{q_f}\right]\left[\frac{\star}{\star}\right]\left[\frac{x}{x}\right]\left[\frac{b q_f}{q_f}\right]\left[\frac{\star}{\star}\right]\left[\frac{x q_f}{q_f}\right]\left[\frac{\star}{\star}\right]\left[\frac{q_f \star}{}\right]$$

$$\frac{\star\, q_0 aba \star x q_1 ba \star x b q_1 a \star x b x q_0 \star x b q_f x \star x b q_f \star x q_f \star q_f \star}{\star\, q_0 aba \star x q_1 ba \star x b q_1 a \star x b x q_0 \star x b q_f x \star x b q_f \star x q_f \star q_f \star}$$

Transforming a TM into an MPCP Instance

TM M accepts configuration $c_0 \Leftrightarrow g(M, c_0) \in MPCP$

Definition of MPCP dominos

C_I	fixed initial card	$\left[\frac{}{\star\langle c_0\rangle}\right]$
C_C	copy cards	$\left[\frac{\star}{\star}\right]$ and $\left[\frac{s}{s}\right]$ $\forall s \in \Sigma$
C_T	transition cards	e.g. $\left[\frac{q_1 a}{x q_2}\right]$ if $q_1 \in Q \setminus F \wedge \delta(q_1, a) = (q_2, x, R)$
C_D	deletion cards	$\left[\frac{s\,q}{q}\right], \left[\frac{q\,s}{q}\right]$ $\forall s \in \Sigma \cup \{\_\}, \forall q \in F$
C_F	final card	$\left[\frac{q\star}{}\right]$ $\forall q \in F$

$g(M, c_0) := (C_I\ , C_C \cup C_T \cup C_D \cup C_F)$

Transition Dominos

$\forall\, q_1 \notin F,\ q_2 \in Q,\ a\ b\ z \in \Sigma$

$\delta(q_1, a) = (q_2, b, L)$ $\left[\dfrac{\star q_1 a}{\star q_2 \_ b}\right]$ and $\left[\dfrac{z q_1 a}{q_2 z b}\right]$

$\delta(q_1, \_) = (q_2, b, R)$ $\left[\dfrac{\star q_1 \_}{\star b q_2}\right]$ and $\left[\dfrac{q_1 \star}{b q_2 \star}\right]$

$\delta(q_1, \_) = (q_2, \_, N)$ $\ldots$

Correctness Proof

$$\forall M\, c_0.\ \exists\, c_f\, i\, .\, c_0 \rightarrow_M^i c_f \wedge (state\, c_f) \in F \ \Leftrightarrow \\ \exists P \subseteq TM_{cards}\, .\, match\left(\left[\frac{}{\star\langle c_0\rangle}\right] :: P\right)$$

Proof direction ⇒ with induction on i:

$i = 0 \wedge (state\, c_0) \in F$

We remove all symbols to the left and to the right of the state using deletion cards.

Example: $\langle c_0 \rangle = q_0\, a\, b$

$$\left[\frac{}{\star q_0 a b}\right] \left[\frac{\star}{\star}\right] \left[\frac{q_0\, a}{q_0}\right] \left[\frac{b}{b}\right] \left[\frac{\star}{\star}\right] \left[\frac{q_0\, b}{q_0}\right] \left[\frac{\star}{\star}\right] \left[\frac{q_0 \star}{}\right]$$

Correctness $\Rightarrow$ cont.

HAVE

IH: $match\left(\left[\frac{}{\star\langle step\ c_0\rangle}\right] :: A\right)$

IH': $\#_1 A = \star\langle step\ c_0\rangle :: \#_2 A$

$$\#_1(step\_cards\ c_0) = \star\,\langle c_0\rangle$$
$$\#_2(step\_cards\ c_0) = \star\,\langle step\ c_0\rangle$$

WANT

$\exists P,\ match\left(\left[\frac{}{\star\langle c_0\rangle}\right] :: P\right)$

$P := (step\_cards\ c_0) \mathbin{+\!\!+} A$

$$\frac{}{\star\langle c_0\rangle}\ \frac{\#_1(step\_cards\ c_0)}{\#_2(step\_cards\ c_0)}\ \frac{\#_1 A}{\#_2 A}$$

$$\frac{}{\star\langle c_0\rangle}\ \frac{\star\,\langle c_0\rangle}{\star\,\langle step\ c_0\rangle}\ \frac{\#_1 A}{\#_2 A}$$

$$\frac{}{\star\langle c_0\rangle}\ \frac{\star\,\langle c_0\rangle}{\star\,\langle step\ c_0\rangle}\ \frac{\star\langle step\ c_0\rangle\ \#_2 A}{\#_2 A}$$

$step\_cards :\ conf \to list\ domino$

Example: $\langle c_0\rangle = q_0\,a\,b\,c$ and $\delta(q_0, a) = (q_1, x, R)$

$$step\_cards\ c_0 = \left[\frac{\star}{\star}\right]\left[\frac{q_0\,a}{x\,q_1}\right]\left[\frac{b}{b}\right]\left[\frac{c}{c}\right]$$

Correctness $\Leftarrow$

$$\forall P\, c_0 . P \subseteq TM_{cards} \land match\left(\left[\frac{}{\star\langle c_0\rangle}\right] :: P\right) \to \exists\, c_f\, i\, .\, c_0 \to_M^i c_f \land (state\, c_f) \in F$$

Proof:

1. Size induction on $|P|$
2. Case analysis on $state\, c_0 \in F$

$$\begin{aligned}
state\, c_0 \in F :&\ \ c_f := c_0 \\
state\, c_0 \notin F :&\ \ \text{prove that } P \text{ can be split into } (step\_cards\, c_0) +\!\!+ P' \\
&\ \ \text{use IH with } P' \text{ and } step\, c_0 \text{ to get } i \text{ and } c_f \text{ with} \\
&\ \ step\, c_0 \to_M^i c_f \land (state\, c_f) \in F \\
&\ \ c_0 \to_M^1 step\, c_0 \to_M^i c_f \\
&\ \ \mathbf{c_0 \to_M^{(S\, i)} c_f}
\end{aligned}$$

Structure of the Solution List

Assumptions: $P \subseteq TM_{cards}$, $state\ c_0 \notin F$, $match\left(\left[\frac{\quad}{\star\langle c_0\rangle}\right] +\!\!+\, P\right)$

Goal: $P = (step\_cards\ c_0) :: P'$

Example: $c_0 = [\underset{\substack{\uparrow \\ q_0}}{a}\, ba]$ and $step\ c_0 = [x\, \underset{\substack{\uparrow \\ q_1}}{b}\, a]$ with $\delta(q_0, a) = (q_1, x, R)$

$$\left[\frac{\quad}{\star q_0 aba}\right]\left[\frac{\star}{\star}\right]\left[\frac{q_0 a}{x q_1}\right]\left[\frac{b}{b}\right]\left[\frac{a}{a}\right] :: P'$$

$$\frac{\star q_0 aba}{\star q_0 aba \star x q_1 ba}$$

$$P = \left[\frac{\star}{\star}\right]\left[\frac{q_0 a}{x q_1}\right]\left[\frac{b}{b}\right]\left[\frac{a}{a}\right] :: P'$$

$$P = (step\_cards\ c_0) +\!\!+ P'$$

C_I $\left[\frac{\$}{\$ \star \langle c_{start}\rangle}\right]$

C_C $\left[\frac{\star}{\star}\right]$ and $\left[\frac{s}{s}\right]$ $\forall s \in \Sigma$

C_T $\left[\frac{q_0 a}{x q_1}\right]$

C_D $\left[\frac{s\, q}{q}\right], \left[\frac{q\, s}{q}\right]$ $\forall s \in \Sigma \cup \{\_\}, \forall q \in F$

C_F $\left[\frac{q\star}{\quad}\right]$ $\forall q \in F$

Conclusion

What we have

- Formal definitions of single-tape Turing machines, MPCP and PCP
- Verified reductions from A_{TM} to $MPCP$ and $MPCP$ to PCP

Future work

- Undecidability of $\mathcal{L}(G_1) \cap \mathcal{L}(G_2) = \emptyset$ for CFG's G_1, G_2
- Reduction of A_{TM} to the word problem for string rewriting systems (SRS)
- Reduction of SRS to PCP

$$A_{TM} \leq SRS \leq PCP^{1}$$

[1] M. D. Davis and E. J. Weyuker. Computability, complexity, and languages - fundamentals of theoretical computer science. Computer science and applied mathematics. Academic Press, 1983,p.181-185

References

A. Asperti and W. Ricciotti.
Formalizing turing machines.
In *Logic, Language, Information and Computation - 19th International Workshop, WoLLIC 2012, Buenos Aires, Argentina, September 3-6, 2012. Proceedings*, pages 1–25, 2012.

J. E. Hopcroft, R. Motwani, and J. D. Ullman.
Introduction to Automata Theory, Languages, and Computation.
Pearson, third edition, 2006.

M. Sipser.
Introduction to the Theory of Computation.
Course Technology, second edition, 2006.

Coq Development

	Spec	Proof	Σ
MPCP $\leq$ PCP	130	180	310
$A_{TM} \leq$ MPCP	370	540	910
TM	170	110	280
Σ	670	830	1500

Formalization of TM Configurations

```
Variable Σ : finType.
Variable Q: finType.

Inductive tape : Type :=
  | niltape : tape
  | leftof : Σ → list Σ → tape
  | rightof : Σ → list Σ → tape
  | midtape : list Σ → Σ → list Σ → tape.

Definition tape' : Type := Σ* × Q × Σ*
```

Additional blank symbol needed to express $[\underset{\overset{\uparrow}{q}}{\ }abcd]$ vs. $(q, \mathit{leftof}\ a\, [b; c; d])$