Neuigkeiten zum PCP

Johannes Waldmann & Heiko Stamer

Inhalt

Motivation, Ziele

- Faszination: Einfachheit vs. Komplexität !
- Betrachtung „schwieriger“ PCPs
- Entscheidbarkeit von Teilklassen z.B. $PCP(3)$
- kürzerer Beweis für Entscheidbarkeit von $PCP(2)$
- Beispiele für Grundvorlesung, Übungen *Berechenbarkeits- und Komplexitätstheorie*
- Austausch von Erfahrungen und Ergebnissen mit internationaler Forschergemeinde

Notationen, Voraussetzungen

endliche Alphabete: $\Sigma = \{\sigma_1, \sigma_2, \ldots, \sigma_n\}$ und $\Delta = \{\delta_1, \delta_2, \ldots, \delta_m\}$

- Verkettung von Elementen bildet Wort-Monoide Σ^*, Δ^*
- neutrales Element, „leeres Wort“: ε
- Halbgruppen: $\Sigma^+ = \Sigma^* \setminus \{\varepsilon\}$, $\Delta^+ = \Delta^* \setminus \{\varepsilon\}$

Elementare Bezeichnungen über Wörtern $w \in \Sigma^*$ bzw. $w \in \Delta^*$:

- Länge eines Wortes: $|w|$
- Anzahl der δ's im Wort w: $|w|_\delta$

Definition 1 (Morphismus)

Abbildung $h: \Sigma^* \to \Delta^*$ ist **Morphismus**, *wenn $\forall u, v \in \Sigma^*: h(uv) = h(u)h(v)$ gilt.*

Definition 2 (PCP-Instanz)

Das Tupel (h, g) heißt **PCP-Instanz**.

$h, g: \Sigma^* \to \Delta^*$ Morphismen, aber $h', g': \Sigma \to \Delta^*$ ausreichend.

Notationen, Voraussetzungen

Notation 1 (PCP-Instanz)

$$\Psi \quad = \quad ((u_1, v_1), (u_2, v_2), \ldots, (u_n, v_n))$$

$$\textit{mit} \quad u_i = h'(\sigma_i), v_i = g'(\sigma_i)$$

oder

$$\begin{array}{c|cccc} \Psi & \sigma_1 & \sigma_2 & \ldots & \sigma_n \\ \hline h' & u_1 & u_2 & \ldots & u_n \\ g' & v_1 & v_2 & \ldots & v_n \end{array}$$

Beispiel 1 $\Sigma = \{A, B, C\}$, $\Delta = \{0, 1\}$

$$\begin{aligned} \Psi_1 &= ((110, 1), (0, 1), (1, 01)) \\ &= \begin{array}{c|ccc} & A & B & C \\ \hline h' & 110 & 0 & 1 \\ g' & 1 & 1 & 01 \end{array} \\ &\overset{\textit{kurz}}{=} \begin{pmatrix} 110 & 0 & 1 \\ 1 & 1 & 01 \end{pmatrix} \end{aligned}$$

Notationen, Voraussetzungen

Definition 3 (Lösung, Lösungsmengen)

Ein Wort $w \in \Sigma^+$ *mit* $h(w) = g(w)$ *heißt nicht-triviale* **Lösung der Instanz**.

Gleichheitsmenge, Lösungsmenge:

$$\mathbb{E}(h,g) \;=\; \{w \in \Sigma^+ \;:\; h(w) = g(w)\}$$

Menge der Lösungslängen (Spektrum):

$$\mathbb{L}(h,g) \;=\; \{|w| \;:\; w \in \mathbb{E}(h,g)\}$$

kürzeste Lösungen:

$$\mathbb{E}_{\leq}(h,g) \;=\; \{w \in \mathbb{E}(h,g) \;:\; \forall z \in \mathbb{E}(h,g) :\; |w| \leq |z|\}$$

Anzahl kürzester Lösungen: $|\mathbb{E}_{\leq}(h,g)|$

Notation 2 (Lösungsmengen)

Abbkürzung für gegebene PCP-Instanz Ψ*:*

$$\mathbb{E}(\Psi) \qquad \mathbb{L}(\Psi) \qquad \mathbb{E}_{\leq}(\Psi)$$

Beispiel 2 (Lösungsmengen zum Beispiel 1)
$\Sigma = \{A, B, C\},\ \Delta = \{0, 1\}$

$$\Psi_1 = \begin{pmatrix} 110 & 0 & 1 \\ 1 & 1 & 01 \end{pmatrix}$$

$$\mathbb{E}(\Psi_1) = \left\{ \begin{array}{l} AACBCCBC, \\ AACBCCBCAACBCCBC, \\ AACACBACCBCBCCBC, \ldots \end{array} \right\}$$

$$\begin{aligned} h(AACBCCBC) &= 110\ 110\ 1\ 0 \ldots \\ &= 1101101 \ldots \\ g(AACBCCBC) &= 1\ 1\ 01\ 1 \ldots \end{aligned}$$

$$\mathbb{L}(\Psi_1) = \{8, 16, 24, 32, 40, 48, 56, 64, \ldots\}$$

$$\mathbb{E}_{\leq}(\Psi_1) = \{AACBCCBC\}$$

Post Correspondence Problem

Definition 4 (Post Correspondence Problem)
Eingabe: *PCP-Instanz* Ψ
Fragestellung: $\mathbb{E}(\Psi) \stackrel{?}{=} \emptyset$

- Problem rekursiv unentscheidbar [Post1946]
- alternative Definition des PCP über Wortpaare und Indexfolge
- $\mathbb{E}(\Psi) \neq \emptyset$, dann $\mathbb{E}(\Psi)$ unendlich (Verkettung von Lösungen)
- $\mathbb{L}(\Psi) \stackrel{?}{=} \emptyset$ ist äquivalent zum PCP

Beispiel 3 (keine Lösungen) $\Sigma = \{A, B\},\ \Delta = \{0, 1\}$

$$\Psi_3 = \begin{pmatrix} 000 & 1 \\ 0 & 01 \end{pmatrix} \qquad \mathbb{E}(\Psi_3) = \emptyset$$

Beispiel 4 (einfache Lösungen) $\Sigma = \{A, B\},\ \Delta = \{0, 1\}$

$$\Psi_4 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \qquad \mathbb{E}(\Psi_4) = \{B, BB, BBB, \ldots\}$$

Beispiel 5 (komplexe Lösungen) $\Sigma = \{A, B, C\},\ \Delta = \{0, 1\}$

$$\Psi_5 = \begin{pmatrix} 01000 & 0 & 100 \\ 0 & 01001 & 0010 \end{pmatrix} \qquad \mathbb{L}(\Psi_5) = \{182, 245, 252, \ldots\}$$

Eigenschaften von PCP-Instanzen

Definition 5

Größe *der PCP-Instanz* Ψ*:* $\mathtt{size}(\Psi) = |\Sigma|$

Definition 6

Weite: $\mathtt{width}(\Psi) = \max\limits_{1 \leq i \leq n} (|h'(\sigma_i)|, |g'(\sigma_i)|)$

Beispiel 6 (Größe und Weite)

Bsp.	Instanz	Größe	Weite
Ψ_1	$\begin{pmatrix} 110 & 0 & 1 \\ 1 & 1 & 01 \end{pmatrix}$	3	3
Ψ_3	$\begin{pmatrix} 000 & 1 \\ 0 & 01 \end{pmatrix}$	2	3
Ψ_4	$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$	2	1
Ψ_5	$\begin{pmatrix} 01000 & 0 & 100 \\ 0 & 01001 & 0010 \end{pmatrix}$	3	5

Einschränkung des Zielalphabets

- Für PCP-Instanzen Ψ mit $|\Delta| = 1$ ist die Frage $\mathbb{E}(\Psi) \stackrel{?}{=} \emptyset$ rekursiv **entscheidbar**.

- $\forall \Psi : \exists$ äquivalentes Ψ' mit $|\Delta_{\Psi'}| = 2$

  Insbesondere lassen sich alle PCP-Instanzen mit $|\Delta_\Psi| > 2$ durch geeignete Kodierung auf ein zweielementiges Zielalphabet reduzieren.

Beispiel 7 (Kodierung)

$\Sigma = \{A, B, C\}$, $\Delta_{\Psi_7} = \{0, 1, 2, 3\}$, $\Delta_{\Psi_7'} = \{0, 1\}$

$$\Psi_7 = \begin{pmatrix} 02 & 30 & 1 \\ 23 & 0 & 10 \end{pmatrix} \overset{\text{binäre Kodierung}}{\rightleftharpoons} \Psi_7' = \begin{pmatrix} 0010 & 1100 & 01 \\ 1011 & 00 & 0100 \end{pmatrix}$$

$$\mathbb{E}(\Psi_7) = \mathbb{E}(\Psi_7') = \{CAB, CABCAB, \ldots\}$$

Klassifizierung

Definition 7 (Größen)

$$PCP(k) = \{\Psi \ : \ \texttt{size}(\Psi) = k\}$$

Definition 8 (Größen, Weiten)

$$PCP(k,l) = \{\Psi \in PCP(k) \ : \ \texttt{width}(\Psi) = l\}$$

Beispiel 8 (PCP Klassen)

$$\begin{array}{rcl}
PCP(1) & = & \left\{ \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 00 \\ 0 \end{pmatrix}, \ldots \right\} \\
|PCP(1)| & = & \infty \\
PCP(1,1) & = & \left\{ \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\} \\
|PCP(1,1)| & = & 4 \\
PCP(3,3) & = & \left\{ \begin{pmatrix} 000 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \ldots, \begin{pmatrix} 111 & 111 & 111 \\ 111 & 111 & 111 \end{pmatrix} \right\} \\
|PCP(3,3)| & = & 7\,482\,880
\end{array}$$

- $PCP(n)$ mit $n \in \{1,2\}$ ist **entscheidbar**

- $PCP(n)$ mit $n \geq 7$ ist **unentscheidbar**
  ($PCP(7)$: [Matiyasevich,Sénizergues1996])

Lösungssuche

- PCP ist allgemein nur **semi-entscheidbar**

  ⇝ zusätzliche Abbruchbedingungen für Lösungsalgorithmus
  z.B. maximale Suchtiefe, maximale Knotenanzahl, ...

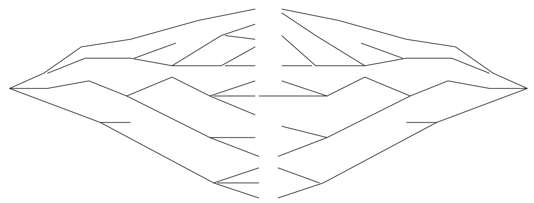
- **Tiefensuche:** ungeeignet
  unendliche Pfade, nicht unbedingt kürzeste Lösung

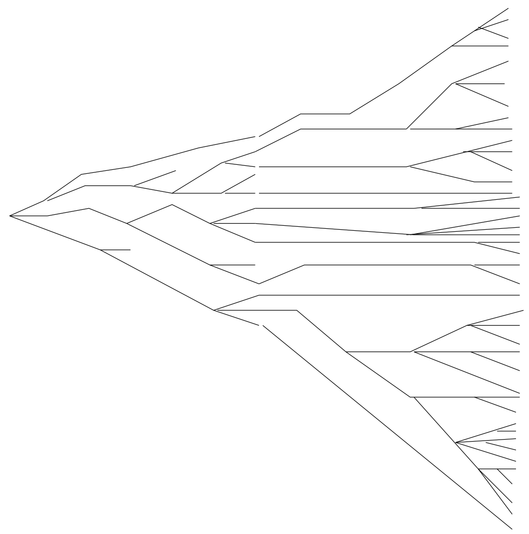
- **Breitensuche:** besser, aber höherer Speicherplatzbedarf

- **Nutzung der Struktur:** Suche von beiden Seiten

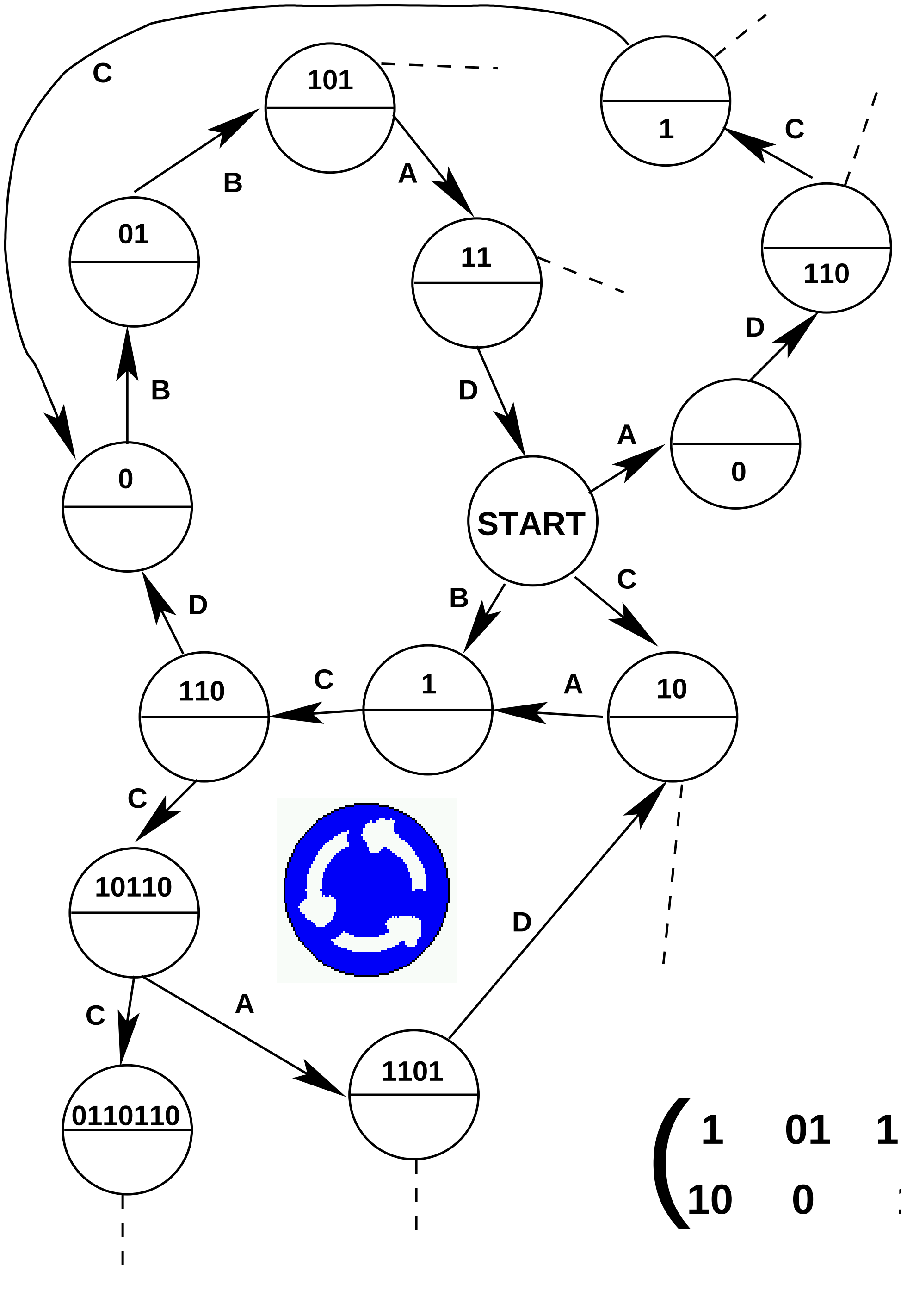
  ⇝ **effiziente** Aufbewahrung in einem Binärbaum

  ⇝ Seitenauswahl wichtig (z.B. PCP-66 [Schöning1997])





„Kreise“



$$\begin{pmatrix} 1 & 01 & 110 & 0 \\ 10 & 0 & 1 & 110 \end{pmatrix}$$

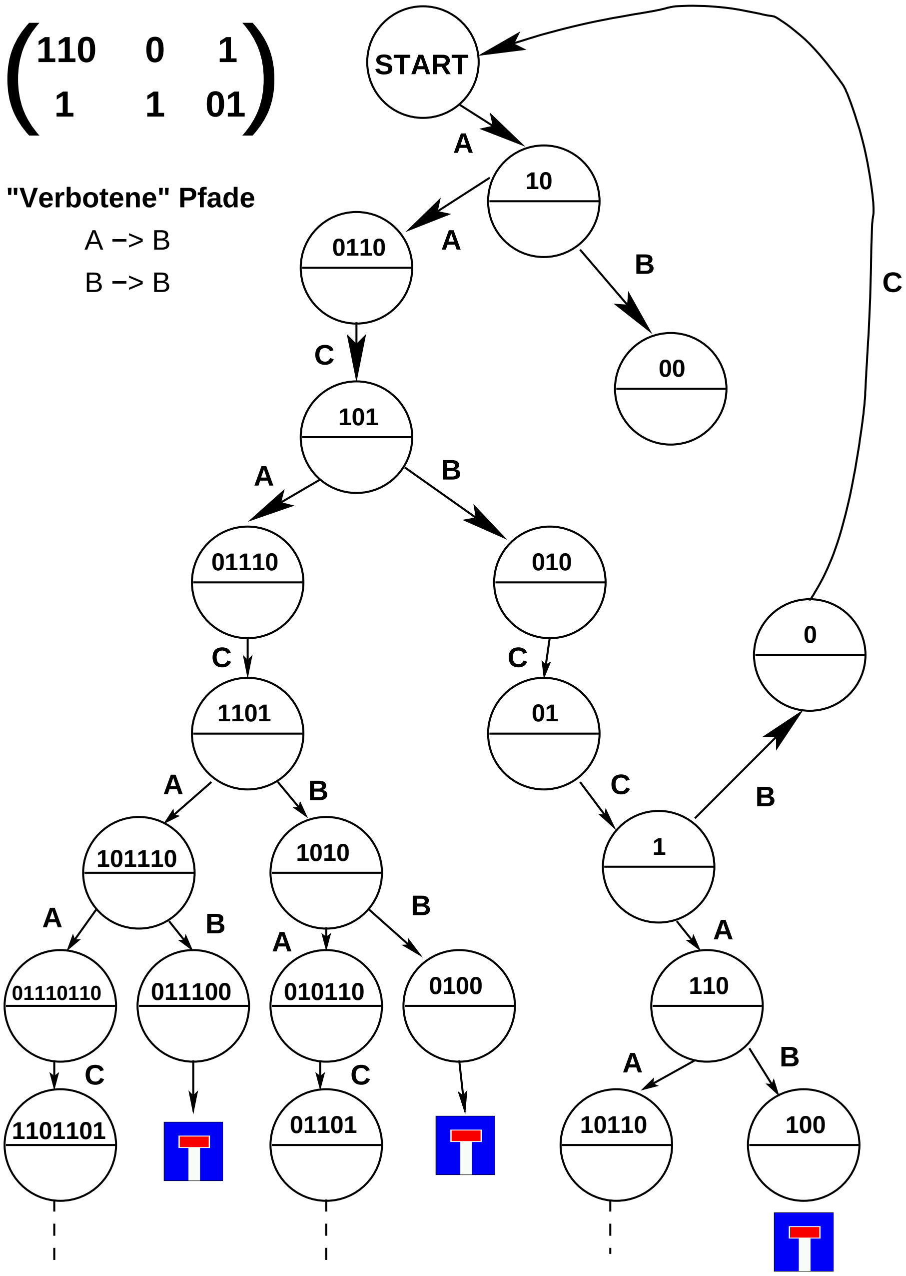
„Sackgassen“

$$\begin{pmatrix} 110 & 0 & 1 \\ 1 & 1 & 01 \end{pmatrix}$$

"Verbotene" Pfade

A –> B

B –> B



„schwierige“ PCPs, Rekorde

n	w	Ψ $\mathbb{L}(\Psi)$	$\lvert\mathbb{E}_{\leq}(\Psi)\rvert$	$\min \mathbb{L}(\Psi)$
3	3	$\begin{pmatrix} 0 & 01 & 1 \\ 1 & 0 & 101 \end{pmatrix}$ $\{44, 48, 52, 56, 60, 64, 68, \ldots\}$	1	44
		$\begin{pmatrix} 01 & 1 & 011 \\ 1 & 011 & 0 \end{pmatrix}$ $\{55, 60, 65, 70, 75, 80, 85, \ldots\}$	1	55
		$\begin{pmatrix} 0 & 1 & 011 \\ 1 & 011 & 0 \end{pmatrix}$ $\{75, 78, 81, 84, 87, 90, 93, \ldots\}$	2	75
3	4	$\begin{pmatrix} 1 & 0 & 1011 \\ 0 & 011 & 1 \end{pmatrix}$ $\{112, \ldots\}$	2	112
		$\begin{pmatrix} 1 & 10 & 1101 \\ 0 & 1011 & 1 \end{pmatrix}$ $\{?, 119, \ldots\}$	?	?
		$\begin{pmatrix} 0011 & 00 & 1 \\ 0 & 1 & 001 \end{pmatrix}$ $\{132, 165, 176, 187, \ldots\}$	1	132
3	5	$\begin{pmatrix} 10101 & 10 & 1 \\ 1 & 01101 & 01 \end{pmatrix}$ $\{99, 102, 105, 108, 111, \ldots\}$	1	99
		$\begin{pmatrix} 11111 & 1 & 0011 \\ 0 & 1100 & 11 \end{pmatrix}$ $\{115, \ldots\}$	1	115
		$\begin{pmatrix} 01000 & 0 & 100 \\ 0 & 01001 & 0010 \end{pmatrix}$ $\{182, 245, \ldots\}$	1	182

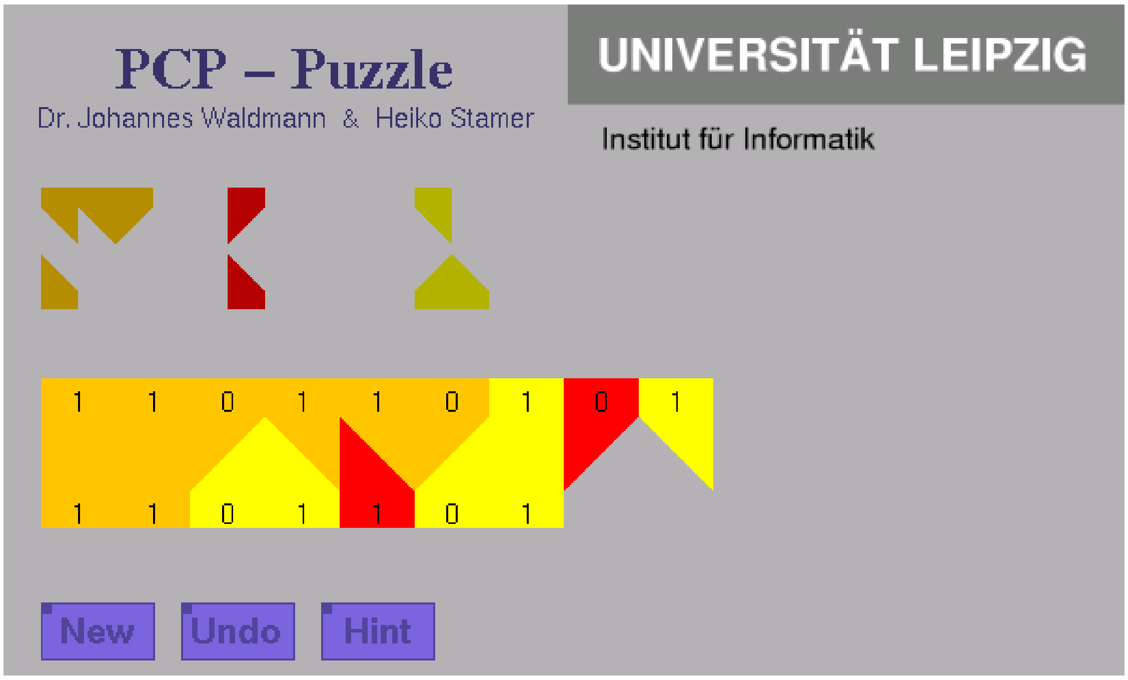
„schwierige“ PCPs, Rekorde

n	w	Ψ $\mathbb{L}(\Psi)$	$\lvert\mathbb{E}_{\leq}(\Psi)\rvert$	$\min \mathbb{L}(\Psi)$
4	3	$\begin{pmatrix} 0 & 01 & 101 & 100 \\ 001 & 0 & 1 & 101 \end{pmatrix}$ $\{88, \ldots\}$	1	88
		$\begin{pmatrix} 1 & 00 & 01 & 0 \\ 001 & 10 & 0 & 11 \end{pmatrix}$ $\left\{ \begin{array}{l} 92, 108, 119, 124, 127, 134, \\ 139, 141, 143, 146, 147, \ldots \end{array} \right\}$	1	92
		$\begin{pmatrix} 100 & 00 & 1 & 1 \\ 1 & 110 & 00 & 011 \end{pmatrix}^1$ $\{160, 184, \ldots\}$	1	160
		$\begin{pmatrix} 000 & 0 & 11 & 10 \\ 0 & 111 & 0 & 100 \end{pmatrix}^1$ $\{?, 204, \ldots\}$	?	?
4	4	$\begin{pmatrix} 1010 & 101 & 0 & 0 \\ 1 & 01 & 001 & 1010 \end{pmatrix}^2$ $\{104, 110, 116, 122, \ldots\}$	1	104
		$\begin{pmatrix} 0011 & 0 & 0100 & 1 \\ 11 & 01 & 110 & 0 \end{pmatrix}^2$ $\{144, 148, 152, 155, 161, \ldots\}$	1	144
		$\begin{pmatrix} 1011 & 10 & 1100 & 1 \\ 001 & 0 & 11 & 1011 \end{pmatrix}$ $\left\{ \begin{array}{l} 179, 215, 227, 250, 254, 263, \\ 269, 275, 280, 289, \ldots \end{array} \right\}$	1	179

[1] aus [Lorentz2000]

[2] Frank-Michael Schleif

PCP-Puzzle (virtuell)



- Implementierung in Java 1.1 als Applet
- leichte Benutzbarkeit mittels `WWW`-Browser
- aktuelle Version: `PcpPuzzle 0.0.1`
- Spielproblem durch Angabe von Parametern beim Aufruf des Applets in der `HTML`-Seite
- Vorgabe einer Lösung möglich (Hint-Funktion)
- Erweiterungen geplant (automatische Generierung, Punktwertung und Hiscore-Tabelle, etc.)

PCP@HOME

Was ist PCP@HOME ?

- Wettbewerb zur Suche „schwieriger“ PCP-Instanzen
- Projektseiten, Programme im Internet verfügbar

Ziele:

- „schwierige“ PCP-Instanzen für unsere Untersuchungen
- neue Anregungen für Lösungskriterien, Lösungssuche
- Motiviation zur Forschung am PCP
- weltweite Bereitstellung einer aktuellen Liste „schwieriger“ PCP-Instanzen