Verification of PCP-Related Computational Reductions in Coq

Yannick Forster, Edith Heiter, Gert Smolka

ITP 2018
July 12

Decidability

A problem $P : X \to \mathbb{P}$ is decidable if . . .

Classically

Fix a model of computation M:
there is a decider in M

Decidability

A problem $P : X \to \mathbb{P}$ is decidable if ...

Classically

Fix a model of computation M:
there is a decider in M

For the cbv λ-calculus

$$\exists u : \mathbf{T}. \forall x : X. \ (u\overline{x} \triangleright T \land Px) \lor (u\overline{x} \triangleright F \land \neg Px)$$

Decidability

A problem $P : X \to \mathbb{P}$ is decidable if ...

Classically	Fix a model of computation M: there is a decider in M
For the cbv λ-calculus	$\exists u : \mathbf{T}. \forall x : X.\ (u\overline{x} \triangleright T \land Px) \lor (u\overline{x} \triangleright F \land \neg Px)$
Type Theory	$\exists f : X \to \mathbb{B}.\ \forall x : X.\ Px \leftrightarrow fx = \mathsf{true}$

Decidability

A problem $P : X \to \mathbb{P}$ is decidable if ...

Classically	Fix a model of computation M: there is a decider in M
For the cbv λ-calculus	$\exists u : \mathbf{T}. \forall x : X.\ (u\overline{x} \triangleright T \land Px) \lor (u\overline{x} \triangleright F \land \neg Px)$
Type Theory	$\exists f : X \to \mathbb{B}.\ \forall x : X.\ Px \leftrightarrow fx = \mathsf{true}$
dependent version (Coq, Agda, Lean, ...)	$\forall x : X.\ \{Px\} + \{\neg Px\}$

Undecidability

A problem $P : X \to \mathbb{P}$ is undecidable if . . .

Classically

If there is no decider u in M

Undecidability

A problem $P : X \to \mathbb{P}$ is undecidable if ...

Classically — If there is no decider u in M

For the cbv λ-calculus — $\neg\exists u : \mathbf{T}.\forall x : X.\ (u\overline{x} \triangleright T \land Px) \lor (u\overline{x} \triangleright F \land \neg Px)$

Undecidability

A problem $P : X \to \mathbb{P}$ is undecidable if ...

Classically	If there is no decider u in M
For the cbv λ-calculus	$\neg\exists u : \mathbf{T}.\forall x : X.\ (u\overline{x} \triangleright T \wedge Px) \vee (u\overline{x} \triangleright F \wedge \neg Px)$
Type Theory	$\neg(\forall x : X.\ \{Px\} + \{\neg Px\})$

Undecidability

A problem $P : X \to \mathbb{P}$ is undecidable if ...

Classically — If there is no decider u in M

For the cbv λ-calculus — $\neg\exists u : \mathbf{T}.\forall x : X.\ (u\overline{x} \triangleright T \land Px) \lor (u\overline{x} \triangleright F \land \neg Px)$

Type Theory — ~~$\neg(\forall x : X.\ \{Px\} + \{\neg Px\})$~~

Undecidability

SAARLAND UNIVERSITY
COMPUTER SCIENCE

A problem $P : X \to \mathbb{P}$ is undecidable if ...

Classically — If there is no decider u in M

For the cbv λ-calculus — $\neg\exists u : \mathbf{T}.\forall x : X.\ (u\overline{x} \triangleright T \wedge Px) \vee (u\overline{x} \triangleright F \wedge \neg Px)$

Type Theory — ~~$\neg(\forall x : X.\ \{Px\} + \{\neg Px\})$~~

In practice: most proofs are by reduction

Definition

P undecidable := Halting problem reduces to P

Reduction

A problem is a type X and a unary predicate $P : X \to \mathbb{P}$

A reduction of (X, P) to (Y, Q) is a function $f : X \to Y$ s.t.
$\forall x.\ Px \leftrightarrow Q(fx)$

Write

$P \preceq Q$

Post correspondence problem

From Wikipedia, the free encyclopedia

The **Post correspondence problem** is an undecidable decision problem that was introduced by Emil Post in 1946.[1] Because it is simpler than the halting problem and the *Entscheidungsproblem* it is often used in proofs of undecidability.

PCP

SAARLAND UNIVERSITY
COMPUTER SCIENCE

$$\boxed{\frac{C2}{LoC2018}}\ \boxed{\overline{xfor}}\ \boxed{\frac{nf}{d}}\ \boxed{\frac{FLo}{F}}\ \boxed{\frac{d}{ord}}\ \boxed{\frac{018inO}{inOxf}}$$

PCP

SAARLAND UNIVERSITY
COMPUTER SCIENCE

$$\boxed{\frac{C2}{LoC2018}} \quad \boxed{\overline{xfor}} \quad \boxed{\frac{nf}{d}} \quad \boxed{\frac{FLo}{F}} \quad \boxed{\frac{d}{ord}} \quad \boxed{\frac{018inO}{inOxf}}$$

$$\boxed{\frac{FLo}{F}}$$

PCP

SAARLAND UNIVERSITY
COMPUTER SCIENCE

$$\boxed{\frac{C2}{LoC2018}}\ \boxed{\overline{xfor}}\ \boxed{\frac{nf}{d}}\ \boxed{\frac{FLo}{F}}\ \boxed{\frac{d}{ord}}\ \boxed{\frac{018inO}{inOxf}}$$

$$\boxed{\frac{FLo}{F}}\ \boxed{\frac{C2}{LoC2018}}$$

PCP

$$\boxed{\frac{C2}{LoC2018}}\ \boxed{\overline{xfor}}\ \boxed{\frac{nf}{d}}\ \boxed{\frac{FLo}{F}}\ \boxed{\frac{d}{ord}}\ \boxed{\frac{018inO}{inOxf}}$$

$$\boxed{\frac{FLo}{F}}\ \boxed{\frac{C2}{LoC2018}}\ \boxed{\frac{018inO}{inOxf}}$$

PCP

SAARLAND UNIVERSITY
COMPUTER SCIENCE

$$\left[\frac{C2}{LoC2018}\right]\left[\overline{xfor}\right]\left[\frac{nf}{d}\right]\left[\frac{FLo}{F}\right]\left[\frac{d}{ord}\right]\left[\frac{018inO}{inOxf}\right]$$

$$\left[\frac{FLo}{F}\right]\left[\frac{C2}{LoC2018}\right]\left[\frac{018inO}{inOxf}\right]\left[\overline{xfor}\right]$$

PCP

$$\left[\frac{C2}{LoC2018}\right] \left[\overline{xfor}\right] \left[\frac{nf}{d}\right] \left[\frac{FLo}{F}\right] \left[\frac{d}{ord}\right] \left[\frac{018inO}{inOxf}\right]$$

$$\left[\frac{FLo}{F}\right] \left[\frac{C2}{LoC2018}\right] \left[\frac{018inO}{inOxf}\right] \left[\overline{xfor}\right] \left[\frac{d}{ord}\right]$$

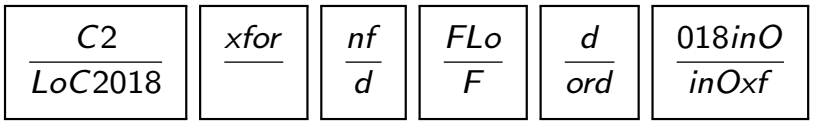
PCP

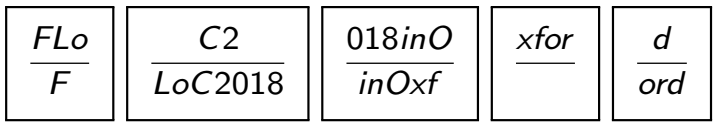
$$\boxed{\frac{C2}{LoC2018}}\ \boxed{\frac{xfor}{}}\ \boxed{\frac{nf}{d}}\ \boxed{\frac{FLo}{F}}\ \boxed{\frac{d}{ord}}\ \boxed{\frac{018inO}{inOxf}}$$

$$\boxed{\frac{FLo}{F}}\ \boxed{\frac{C2}{LoC2018}}\ \boxed{\frac{018inO}{inOxf}}\ \boxed{\frac{xfor}{}}\ \boxed{\frac{d}{ord}}$$

$$\frac{FLoC2018inOxford}{FLoC2018inOxford}$$

PCP

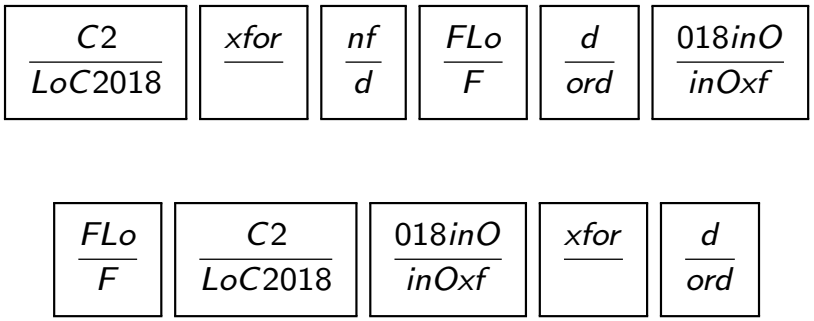




$$\frac{FLoC2018inOxford}{FLoC2018inOxford}$$

- Symbols a, b, c: $\mathbb{N}$
- Strings x, y, z: lists of symbols
- Card c: pairs of strings
- Stacks A, P: lists of cards
- $A \subseteq P$: list inclusion

PCP



- Symbols a, b, c: $\mathbb{N}$
- Strings x, y, z: lists of symbols
- Card c: pairs of strings
- Stacks A, P: lists of cards
- $A \subseteq P$: list inclusion

$$[\,]^1 := \epsilon \qquad [\,]^2 := \epsilon$$

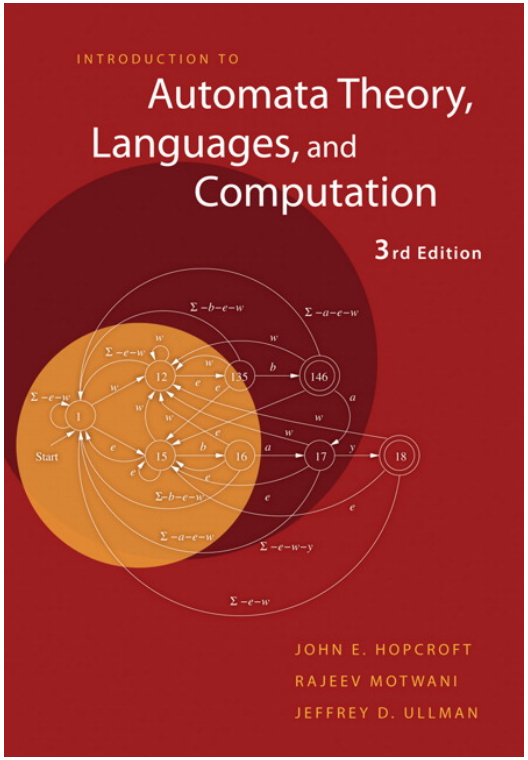
$$(x/y :: A)^1 := x(A^1) \qquad (x/y :: A)^2 := y(A^2)$$

$$PCP\,(P) \;:=\; \exists A \subseteq P.\; A \neq [\,] \wedge A^1 = A^2$$

History

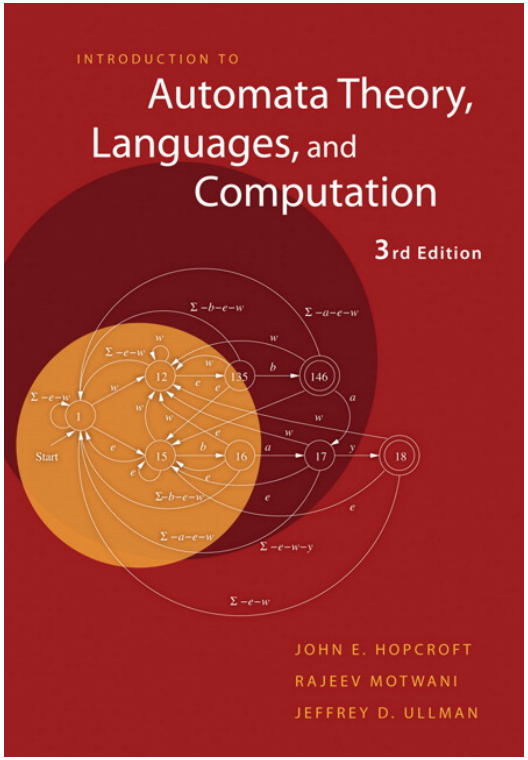
SAARLAND UNIVERSITY
COMPUTER SCIENCE

TM halting $\preceq$ MPCP

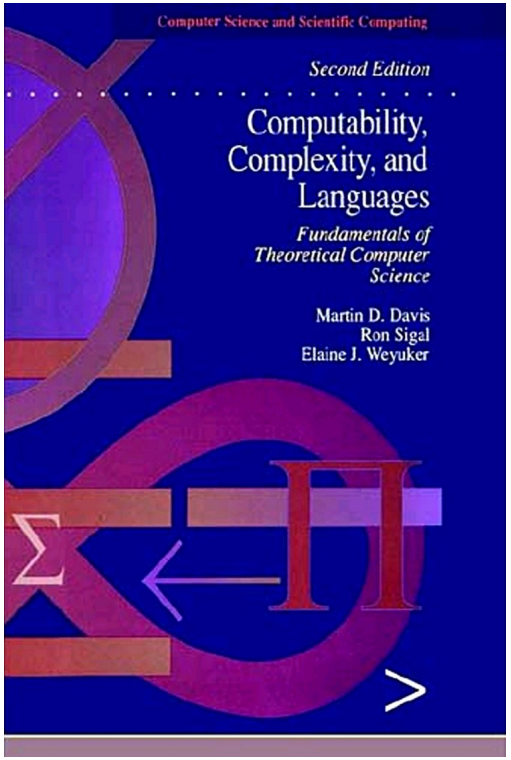


History

TM halting $\preceq$ MPCP



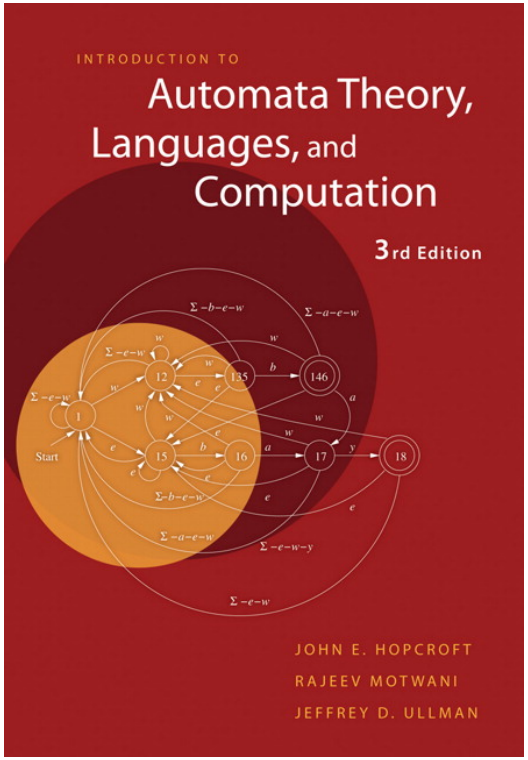
SR $\preceq$ PCP



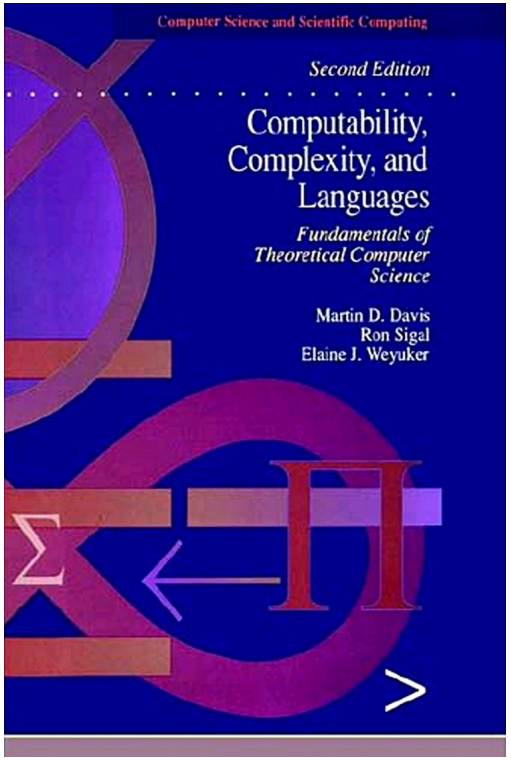
History

SAARLAND UNIVERSITY
COMPUTER SCIENCE

TM halting $\preceq$ MPCP



SR $\preceq$ PCP



PCP $\preceq$ CFI

Post's Correspondence Problem and
the Undecidability of Context-Free Intersection

Wim H. Hesselink

July 28, 2015

1 Introduction

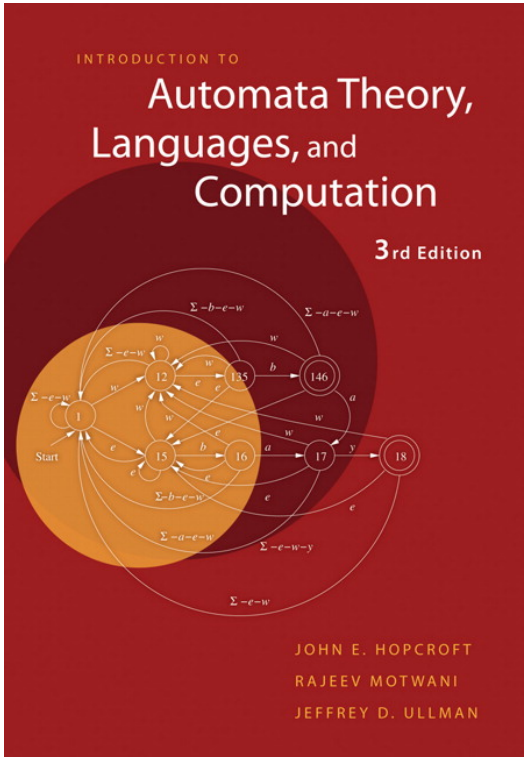
Our starting point is the undecidability of nullability of a string in a rewrite system. This is used to prove undecidability of Post's Modified Correspondence Problem, and of the disjointness of context-free languages. These results are not new but the presentation differs from the book [HU79].

In courses on languages, one usually omits the operator for concatenation of strings or concatenation of elements to strings or strings to elements. Strings are finite sequences of symbols, but in this note we also need to concatenate sequences of pairs. We here therefore decided to use the operator : to concatenate finite sequences, and elements to finite sequences, and finite sequences to elements. We also use them for strings, but we omit them when they become confusing, in particular, between concrete symbols.

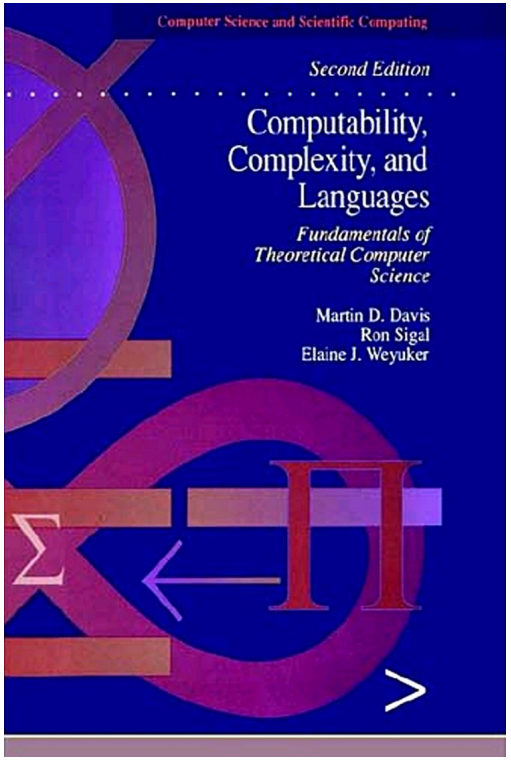
An *alphabet* is a finite set; its elements are called *symbols*. A *string* over alphabet Σ is a finite sequence of elements of Σ. The empty string is denoted by ε. For a string x and a symbol a, we write $n_a(x)$ to denote the number of occurrences of symbol a in sequence x. The reversal of a string x is denoted by x^R. Recall that $(x : y)^R = y^R : x^R$ for arbitrary strings x and y.

History

TM halting $\preceq$ MPCP



SR $\preceq$ PCP



PCP $\preceq$ CFI

Post's Correspondence Problem and the Undecidability of Context-Free Intersection

Wim H. Hesselink

July 28, 2015

1 Introduction

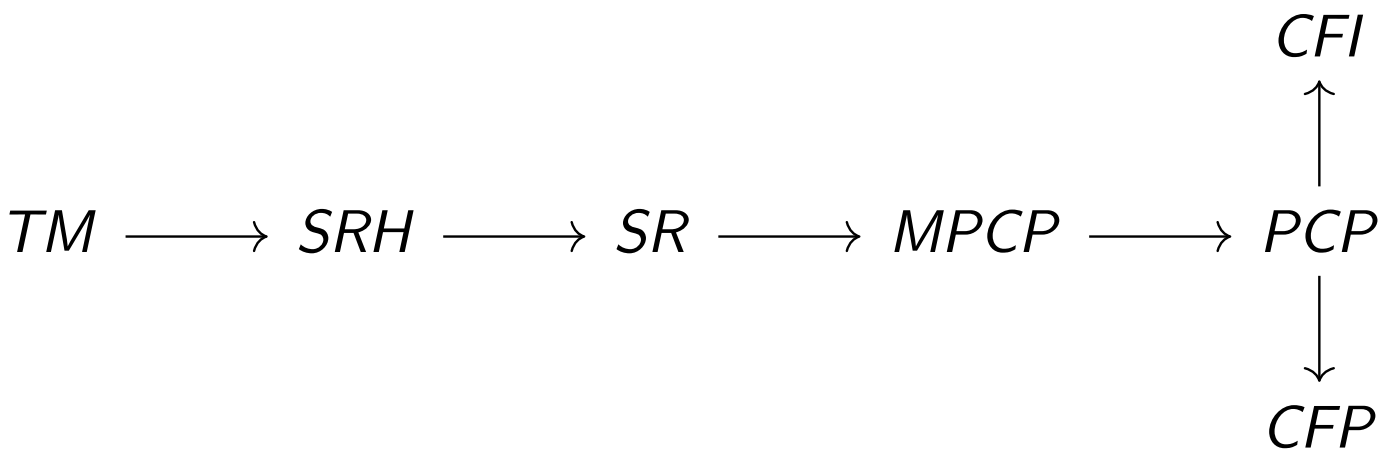
Our starting point is the undecidability of nullability of a string in a rewrite system. This is used to prove undecidability of Post's Modified Correspondence Problem, and of the disjointness of context-free languages. These results are not new but the presentation differs from the book [HU79].

In courses on languages, one usually omits the operator for concatenation of strings or concatenation of elements to strings or strings to elements. Strings are finite sequences of symbols, but in this note we also need to concatenate sequences of pairs. We here therefore decided to use the operator : to concatenate finite sequences, and elements to finite sequences, and finite sequences to elements. We also use them for strings, but we omit them when they become confusing, in particular, between concrete symbols.

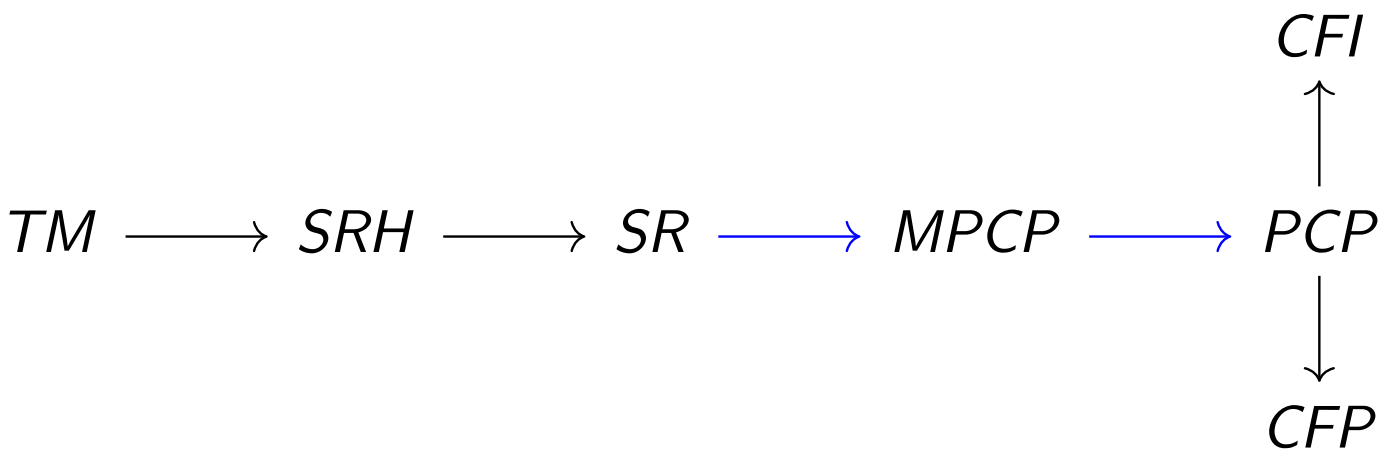
An *alphabet* is a finite set; its elements are called *symbols*. A *string* over alphabet Σ is a finite sequence of elements of Σ. The empty string is denoted by ε. For a string x and a symbol a, we write $n_a(x)$ to denote the number of occurrences of symbol a in sequence x. The reversal of a string x is denoted by x^R. Recall that $(x : y)^R = y^R : x^R$ for arbitrary strings x and y.

At best proof sketches, no inductions are given

Contribution



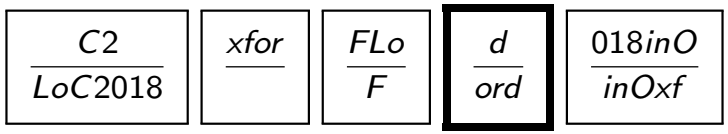
Contribution



MPCP $\preceq$ PCP

MPCP

SAARLAND UNIVERSITY
COMPUTER SCIENCE



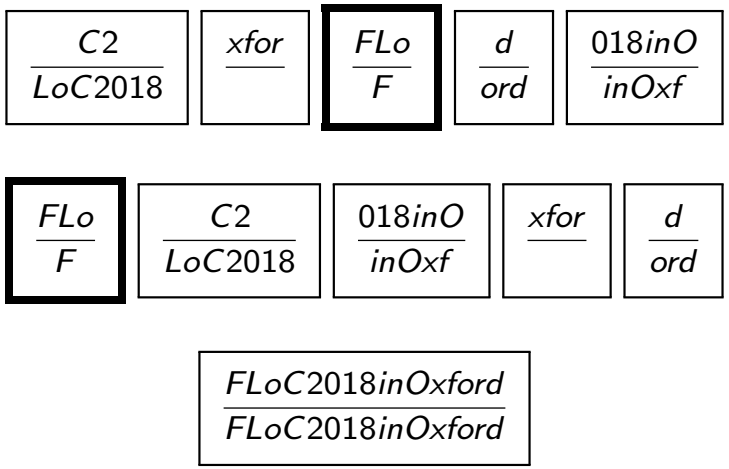
MPCP

SAARLAND UNIVERSITY
COMPUTER SCIENCE

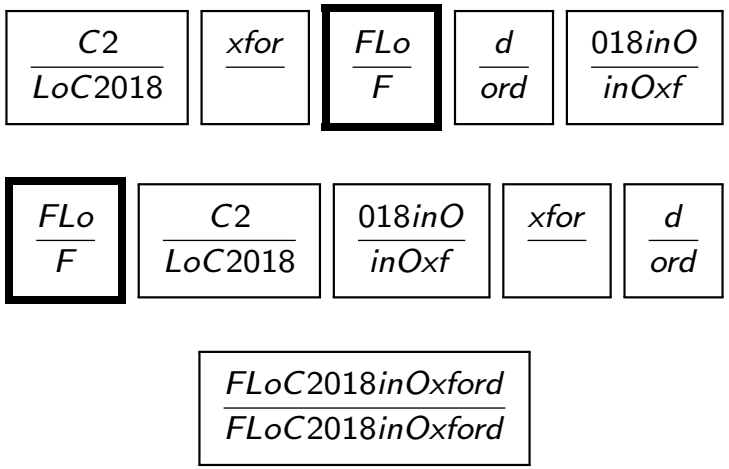
$$\frac{C2}{LoC2018} \quad \frac{xfor}{} \quad \frac{FLo}{F} \quad \frac{d}{ord} \quad \frac{018inO}{inOxf}$$

MPCP

SAARLAND UNIVERSITY
COMPUTER SCIENCE

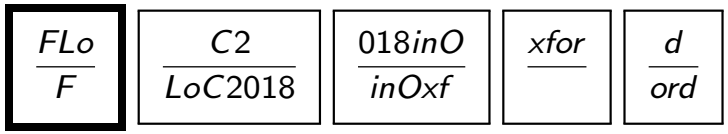


MPCP



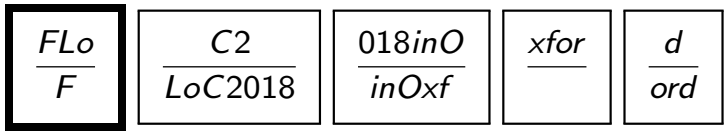
$$MPCP\,(x/y, P) \;:=\; \exists A \subseteq x/y :: P.\; xA^1 = yA^2$$

MPCP $\preceq$ PCP



$$\frac{FLoC2018inOxford}{FLoC2018inOxford}$$

MPCP $\preceq$ PCP



$$\frac{FLoC2018inOxford}{FLoC2018inOxford}$$

$$\frac{\$\#F\#L\#o\#C\#2\#0\#1\#8\#i\#n\#O\#x\#f\#o\#r\#d\#\$}{\$\#F\#L\#o\#C\#2\#0\#1\#8\#i\#n\#O\#x\#f\#o\#r\#d\#\$}$$

MPCP $\preceq$ PCP

SAARLAND UNIVERSITY
COMPUTER SCIENCE

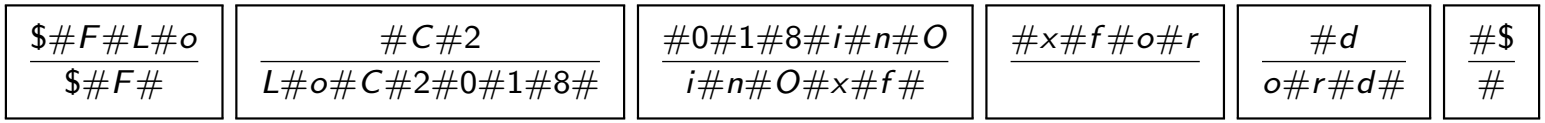
$$\boxed{\frac{FLo}{F}}\ \boxed{\frac{C2}{LoC2018}}\ \boxed{\frac{018inO}{inOxf}}\ \boxed{\frac{xfor}{}}\ \boxed{\frac{d}{ord}}$$

$$\frac{FLoC2018inOxford}{FLoC2018inOxford}$$

$$\frac{\$\#F\#L\#o\#C\#2\#0\#1\#8\#i\#n\#O\#x\#f\#o\#r\#d\#\$}{\$\#F\#L\#o\#C\#2\#0\#1\#8\#i\#n\#O\#x\#f\#o\#r\#d\#\$}$$

$$\boxed{\frac{\$\#F\#L\#o}{\$\#F\#}}\ \boxed{\frac{\#C\#2}{L\#o\#C\#2\#0\#1\#8\#}}\ \boxed{\frac{\#0\#1\#8\#i\#n\#O}{i\#n\#O\#x\#f\#}}\ \boxed{\frac{\#x\#f\#o\#r}{}}\ \boxed{\frac{\#d}{o\#r\#d\#}}\ \boxed{\frac{\#\$}{\$}}$$

MPCP $\preceq$ PCP



$$
\begin{aligned}
{}^{\#}\epsilon &:= \epsilon & \epsilon^{\#} &:= \epsilon \\
{}^{\#}(ax) &:= \#a({}^{\#}x) & (ax)^{\#} &:= a\#(x^{\#})
\end{aligned}
$$

We define:

$$
\begin{aligned}
d &:= \$({}^{\#}x_0) \,/\, \$\#(y_0^{\#}) \\
e &:= \#\$ \,/\, \$ \\
P &:= \{d, e\} +\!\!+ \{{}^{\#}x \,/\, y^{\#} \mid x/y \in x_0/y_0 :: R \wedge (x/y) \neq (\epsilon/\epsilon)\}
\end{aligned}
$$

MPCP $\preceq$ PCP

Lemma 14. *There exists a stack $A \subseteq x_0/y_0 :: R$ such that $x_0 A^1 = y_0 A^2$ if and only if there exists a nonempty stack $B \subseteq P$ such that $B^1 = B^2$.*

Lemma 15. *Every nonempty match $B \subseteq P$ starts with d.*

Lemma 16. *The following hold:*

1. $({}^{\#}x)\# = \#(x^{\#})$.
2. ${}^{\#}(xy) = ({}^{\#}x)({}^{\#}y)$.
3. $(xy)^{\#} = (x^{\#})(y^{\#})$.
4. ${}^{\#}x \neq \#(y^{\#})$.
5. $x^{\#} = y^{\#} \to x = y$.

Lemma 17. *Let $A \subseteq x_0/y_0 :: R$ and $xA^1 = yA^2$. Then there exists a stack $B \subseteq P$ such that $({}^{\#}x)B^1 = \#(y^{\#})B^2$.*

Lemma 18. *Let $B \subseteq P$ such that $({}^{\#}x)B^1 = \#(y^{\#})B^2$ and $x, y \subseteq \Sigma$. Then there exists a stack $A \subseteq x_0/y_0 :: R$ such that $xA^1 = yA^2$.*

Theorem 19. *MPCP reduces to PCP.*

Proof. Follows with Lemma 14. □

$\mathrm{SR} \preceq \mathrm{MPCP}$

$\mathrm{SR} \preceq \mathrm{MPCP}$

Let $R = [\underbrace{ab/ba}_{1}, \underbrace{aa/ab}_{2}]$ and $aab \succ_R^* bab$ with

$$aab \succ_1 aba \succ_1 baa \succ_2 bab$$

SR $\preceq$ MPCP

Let $R = [\underbrace{ab/ba}_{1}, \underbrace{aa/ab}_{2}]$ and $aab \succ_R^* bab$ with

$$aab \succ_1 aba \succ_1 baa \succ_2 bab$$

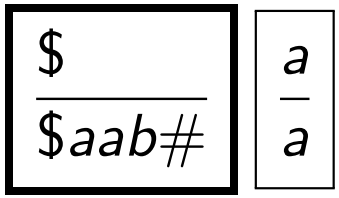
$$\boxed{\frac{\$}{\$aab\#}}$$

$$\frac{\$}{\$aab\#}$$

SR $\preceq$ MPCP

Let $R = [\underbrace{ab/ba}_{1}, \underbrace{aa/ab}_{2}]$ and $aab \succ_R^* bab$ with

$$aab \succ_1 aba \succ_1 baa \succ_2 bab$$



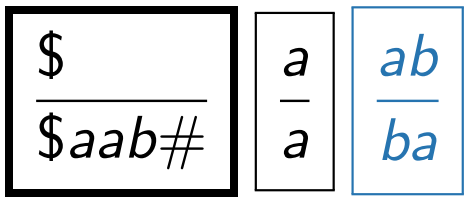
$$\frac{\$}{\$aab\#}$$

- *copy cards* transfer unchanged symbols to the next string

SR $\preceq$ MPCP

Let $R = [\underbrace{ab/ba}_{1}, \underbrace{aa/ab}_{2}]$ and $aab \succ_R^* bab$ with

$$aab \succ_1 aba \succ_1 baa \succ_2 bab$$



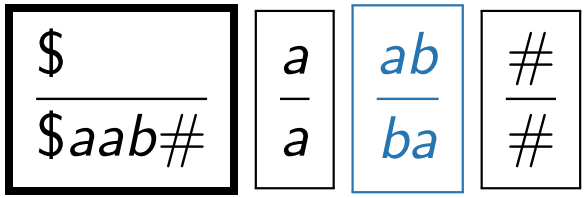
$$\frac{\$}{\$aab\#}$$

- *copy cards* transfer unchanged symbols to the next string
- *rewrite cards* simulate a single rewrite

SR $\preceq$ MPCP

Let $R = [\underbrace{ab/ba}_{1}, \underbrace{aa/ab}_{2}]$ and $aab \succ_R^* bab$ with

$$aab \succ_1 aba \succ_1 baa \succ_2 bab$$



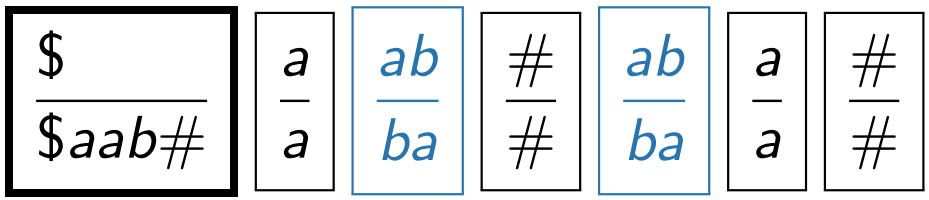
$$\frac{\$aab\#}{\$aab\#aba\#}$$

- *copy cards* transfer unchanged symbols to the next string
- *rewrite cards* simulate a single rewrite
- consecutive strings are separated by #

SR $\preceq$ MPCP

Let $R = [\underbrace{ab/ba}_{1}, \underbrace{aa/ab}_{2}]$ and $aab \succ_R^* bab$ with

$$aab \succ_1 aba \succ_1 baa \succ_2 bab$$



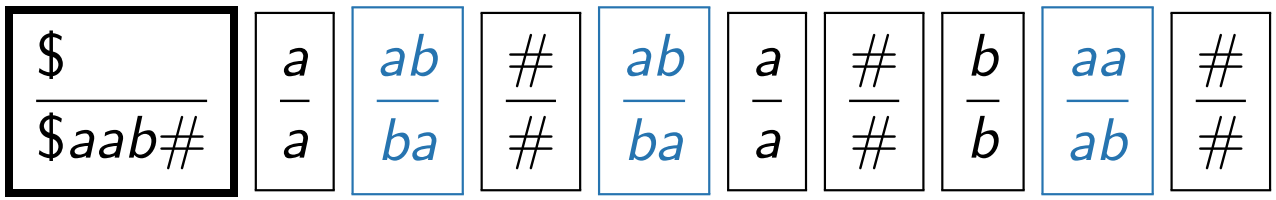
$$\frac{\$aab\#aba\#}{\$aab\#aba\#baa\#}$$

- *copy cards* transfer unchanged symbols to the next string
- *rewrite cards* simulate a single rewrite
- consecutive strings are separated by #

$\mathrm{SR} \preceq \mathrm{MPCP}$

Let $R = [\underbrace{ab/ba}_{1}, \underbrace{aa/ab}_{2}]$ and $aab \succ_R^* bab$ with

$$aab \succ_1 aba \succ_1 baa \succ_2 bab$$



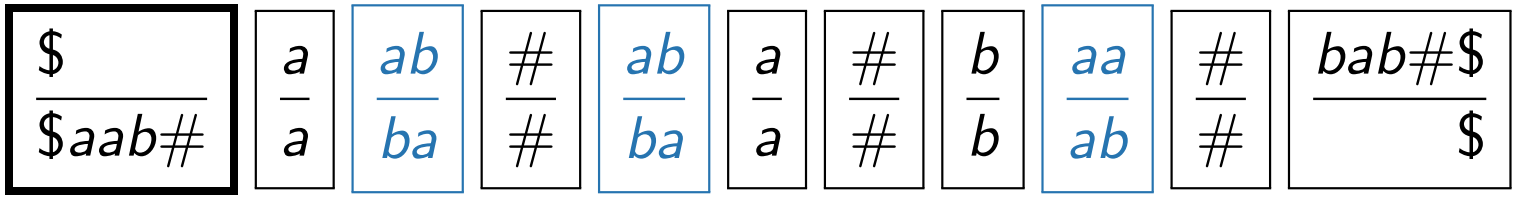
$$\frac{\$aab\#aba\#baa\#}{\$aab\#aba\#baa\#bab\#}$$

- *copy cards* transfer unchanged symbols to the next string
- *rewrite cards* simulate a single rewrite
- consecutive strings are separated by #

SR $\preceq$ MPCP

Let $R = [\underbrace{ab/ba}_{1}, \underbrace{aa/ab}_{2}]$ and $aab \succ_R^* bab$ with

$$aab \succ_1 aba \succ_1 baa \succ_2 bab$$



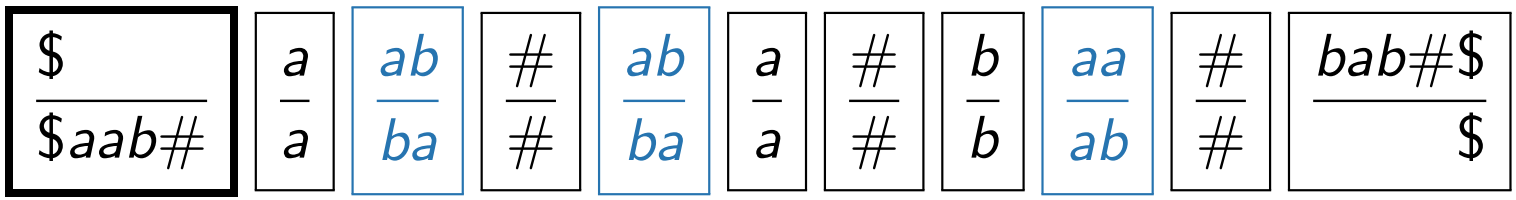
$$\frac{\$aab\#aba\#baa\#bab\#\$}{\$aab\#aba\#baa\#bab\#\$}$$

- *copy cards* transfer unchanged symbols to the next string
- *rewrite cards* simulate a single rewrite
- consecutive strings are separated by #

SR $\preceq$ MPCP

Let $R = [\underbrace{ab/ba}_{1}, \underbrace{aa/ab}_{2}]$ and $aab \succ_R^* bab$ with

$$aab \succ_1 aba \succ_1 baa \succ_2 bab$$



$$\frac{\$aab\#aba\#baa\#bab\#\$}{\$aab\#aba\#baa\#bab\#\$}$$

- *copy cards* transfer unchanged symbols to the next string
- *rewrite cards* simulate a single rewrite
- consecutive strings are separated by #

$$\begin{aligned} d &:= \$ \,/\, \$x_0\# \\ e &:= y_0\#\$ \,/\, \$ \\ P &:= [d, e] +\!\!+ R +\!\!+ [\#/\#] +\!\!+ [a/a \mid a \in \Sigma] \end{aligned}$$

SR $\preceq$ MPCP

Given R and x_0, y_0 construct P such that $x_0 \succ^* y_0 \leftrightarrow \mathrm{PCP}(P)$:

$$
\begin{aligned}
d &:= \$ \,/\, \$x_0\# \\
e &:= y_0\#\$ \,/\, \$ \\
P &:= [d, e] +\!\!+ R +\!\!+ [\#/\#] +\!\!+ [a/a \mid a \in \Sigma]
\end{aligned}
$$

SR $\preceq$ MPCP

Given R and x_0, y_0 construct P such that $x_0 \succ^* y_0 \leftrightarrow \mathrm{PCP}(P)$:

$$\begin{aligned} d &:= \$ \,/\, \$x_0\# \\ e &:= y_0\#\$ \,/\, \$ \\ P &:= [d, e] +\!\!+ R +\!\!+ [\#/\#] +\!\!+ [a/a \mid a \in \Sigma] \end{aligned}$$

Theorem

$x_0 \succ_R^* y_0$ if and only if there exists a stack $A \subseteq P$ such that $d :: A$ matches.

SR $\preceq$ MPCP

Given R and x_0, y_0 construct P such that $x_0 \succ^* y_0 \leftrightarrow \mathrm{PCP}(P)$:

$$\begin{aligned} d &:= \$ \,/\, \$x_0\# \\ e &:= y_0\#\$ \,/\, \$ \\ P &:= [d, e] +\!\!+ R +\!\!+ [\#/\#] +\!\!+ [a/a \mid a \in \Sigma] \end{aligned}$$

Theorem

$x_0 \succ_R^* y_0$ if and only if there exists a stack $A \subseteq P$ such that $d :: A$ matches.

Lemma

Let $x \subseteq \Sigma$ and $x \succ_R^* y_0$. Then there exists $A \subseteq P$ such that $A^1 = x\#A^2$.

SR $\preceq$ MPCP

Given R and x_0, y_0 construct P such that $x_0 \succ^* y_0 \leftrightarrow \mathrm{PCP}(P)$:

$$\begin{aligned} d &:= \$ \,/\, \$x_0\# \\ e &:= y_0\#\$ \,/\, \$ \\ P &:= [d, e] +\!\!+ R +\!\!+ [\#/\#] +\!\!+ [a/a \mid a \in \Sigma] \end{aligned}$$

Theorem

$x_0 \succ_R^* y_0$ if and only if there exists a stack $A \subseteq P$ such that $d :: A$ matches.

Lemma

Let $x \subseteq \Sigma$ and $x \succ_R^* y_0$. Then there exists $A \subseteq P$ such that $A^1 = x\#A^2$.

Lemma

Let $A \subseteq P$, $A^1 = x\#yA^2$, and $x, y \subseteq \Sigma$. Then $yx \succ_R^* y_0$.

Post Correspondence Problems are special CFGs

SAARLAND UNIVERSITY
COMPUTER SCIENCE

$$\left[\frac{C2}{LoC2018}\right]\left[\frac{xfor}{}\right]\left[\frac{nf}{d}\right]\left[\frac{FLo}{F}\right]\left[\frac{d}{ord}\right]\left[\frac{018inO}{inOxf}\right]$$

Post Correspondence Problems are special CFGs

SAARLAND UNIVERSITY
COMPUTER SCIENCE

$$\left[\frac{C2}{LoC2018}\right] \left[\frac{xfor}{}\right] \left[\frac{nf}{d}\right] \left[\frac{FLo}{F}\right] \left[\frac{d}{ord}\right] \left[\frac{018inO}{inOxf}\right]$$

Produce grammars:

$G_1(P)$:

$N \to \text{C2 } M \text{ C2\#LoC2018\#}$
$N \to \text{xfor } M \text{ xfor\#\#}$
$N \to \text{nf } M \text{ nf\#d\#}$
$N \to \text{FLo } M \text{ FLo\#F\#}$
$N \to \text{d } M \text{ d\#ord\#}$
$N \to \text{018inO } M \text{ 018inO\#inOxf\#}$
$M \to N \mid \#$

$G_2(P)$:

$N \to \text{LoC2018 } M \text{ C2\#LoC2018\#}$
$N \to M \text{ xfor\#\#}$
$N \to \text{d } M \text{ nf\#d\#}$
$N \to \text{F } M \text{ FLo\#F\#}$
$N \to \text{ord } M \text{ d\#ord\#}$
$N \to \text{inOxf } M \text{ 018inO\#inOxf\#}$
$M \to N \mid \#$

Post Correspondence Problems are special CFGs

SAARLAND UNIVERSITY
COMPUTER SCIENCE

$$\left[\frac{C2}{LoC2018}\right] \left[\frac{xfor}{}\right] \left[\frac{nf}{d}\right] \left[\frac{FLo}{F}\right] \left[\frac{d}{ord}\right] \left[\frac{018inO}{inOxf}\right]$$

Produce grammars:

$G_1(P)$:

$N \to \text{C2 } M \text{ C2\#LoC2018\#}$
$N \to \text{xfor } M \text{ xfor\#\#}$
$N \to \text{nf } M \text{ nf\#d\#}$
$N \to \text{FLo } M \text{ FLo\#F\#}$
$N \to \text{d } M \text{ d\#ord\#}$
$N \to \text{018inO } M \text{ 018inO\#inOxf\#}$
$M \to N \mid \#$

$G_2(P)$:

$N \to \text{LoC2018 } M \text{ C2\#LoC2018\#}$
$N \to M \text{ xfor\#\#}$
$N \to \text{d } M \text{ nf\#d\#}$
$N \to \text{F } M \text{ FLo\#F\#}$
$N \to \text{ord } M \text{ d\#ord\#}$
$N \to \text{inOxf } M \text{ 018inO\#inOxf\#}$
$M \to N \mid \#$

$$\left[\frac{FLo}{F}\right]$$

$$\text{FLo } N \text{ FLo\#F\#}$$

$$\text{F } N \text{ FLo\#F\#}$$

$$\text{PCP}(P) \leftrightarrow \mathcal{L}(G_1(P)) \cap \mathcal{L}(G_2(P)) \neq \emptyset$$

Post Correspondence Problems are special CFGs

SAARLAND UNIVERSITY
COMPUTER SCIENCE

$$\left[\frac{C2}{LoC2018}\right] \left[\frac{xfor}{}\right] \left[\frac{nf}{d}\right] \left[\frac{FLo}{F}\right] \left[\frac{d}{ord}\right] \left[\frac{018inO}{inOxf}\right]$$

Produce grammars:

$G_1(P)$:

$N \to \text{C2 } M \text{ C2\#LoC2018\#}$
$N \to \text{xfor } M \text{ xfor\#\#}$
$N \to \text{nf } M \text{ nf\#d\#}$
$N \to \text{FLo } M \text{ FLo\#F\#}$
$N \to \text{d } M \text{ d\#ord\#}$
$N \to \text{018inO } M \text{ 018inO\#inOxf\#}$
$M \to N \mid \#$

$G_2(P)$:

$N \to \text{LoC2018 } M \text{ C2\#LoC2018\#}$
$N \to M \text{ xfor\#\#}$
$N \to \text{d } M \text{ nf\#d\#}$
$N \to \text{F } M \text{ FLo\#F\#}$
$N \to \text{ord } M \text{ d\#ord\#}$
$N \to \text{inOxf } M \text{ 018inO\#inOxf\#}$
$M \to N \mid \#$

$$\left[\frac{FLo}{F}\right] \left[\frac{C2}{LoC2018}\right]$$

FLoC2 N C2#LoC2018#FLo#F#

FLoC2018 N C2#LoC2018#FLo#F#

$$\text{PCP}(P) \leftrightarrow \mathcal{L}(G_1(P)) \cap \mathcal{L}(G_2(P)) \neq \emptyset$$

Post Correspondence Problems are special CFGs

SAARLAND UNIVERSITY
COMPUTER SCIENCE

$$\left[\frac{C2}{LoC2018}\right] \left[\frac{xfor}{}\right] \left[\frac{nf}{d}\right] \left[\frac{FLo}{F}\right] \left[\frac{d}{ord}\right] \left[\frac{018inO}{inOxf}\right]$$

Produce grammars:

$G_1(P)$:

$N \to$ C2 M C2#LoC2018#
$N \to$ xfor M xfor##
$N \to$ nf M nf#d#
$N \to$ FLo M FLo#F#
$N \to$ d M d#ord#
$N \to$ 018inO M 018inO#inOxf#
$M \to N \mid \#$

$G_2(P)$:

$N \to$ LoC2018 M C2#LoC2018#
$N \to$ M xfor##
$N \to$ d M nf#d#
$N \to$ F M FLo#F#
$N \to$ ord M d#ord#
$N \to$ inOxf M 018inO#inOxf#
$M \to N \mid \#$

$$\left[\frac{FLo}{F}\right] \left[\frac{C2}{LoC2018}\right] \left[\frac{018inO}{inOxf}\right]$$

FLoC2018InO N 018inO#inOxf#C2#LoC2018#FLo#F#

FLoC2018InOxf N 018inO#inOxf#C2#LoC2018#FLo#F#

$$\mathrm{PCP}(P) \leftrightarrow \mathcal{L}(G_1(P)) \cap \mathcal{L}(G_2(P)) \neq \emptyset$$

Post Correspondence Problems are special CFGs

SAARLAND UNIVERSITY
COMPUTER SCIENCE

$$\left[\frac{C2}{LoC2018}\right] \left[\frac{xfor}{}\right] \left[\frac{nf}{d}\right] \left[\frac{FLo}{F}\right] \left[\frac{d}{ord}\right] \left[\frac{018inO}{inOxf}\right]$$

Produce grammars:

$G_1(P)$:

$N \to \text{C2 } M \text{ C2\#LoC2018\#}$
$N \to \text{xfor } M \text{ xfor\#\#}$
$N \to \text{nf } M \text{ nf\#d\#}$
$N \to \text{FLo } M \text{ FLo\#F\#}$
$N \to \text{d } M \text{ d\#ord\#}$
$N \to \text{018inO } M \text{ 018inO\#inOxf\#}$
$M \to N \mid \#$

$G_2(P)$:

$N \to \text{LoC2018 } M \text{ C2\#LoC2018\#}$
$N \to M \text{ xfor\#\#}$
$N \to \text{d } M \text{ nf\#d\#}$
$N \to \text{F } M \text{ FLo\#F\#}$
$N \to \text{ord } M \text{ d\#ord\#}$
$N \to \text{inOxf } M \text{ 018inO\#inOxf\#}$
$M \to N \mid \#$

$$\left[\frac{FLo}{F}\right] \left[\frac{C2}{LoC2018}\right] \left[\frac{018inO}{inOxf}\right] \left[\frac{xfor}{}\right]$$

FLoC2018InOxfor N xfor#018inO#inOxf#C2#LoC2018#FLo#F#

FLoC2018InOxf N xfor#018inO#inOxf#C2#LoC2018#FLo#F#

$$\text{PCP}(P) \leftrightarrow \mathcal{L}(G_1(P)) \cap \mathcal{L}(G_2(P)) \neq \emptyset$$

Post Correspondence Problems are special CFGs

SAARLAND UNIVERSITY
COMPUTER SCIENCE

$$\left[\frac{C2}{LoC2018}\right]\left[\frac{xfor}{}\right]\left[\frac{nf}{d}\right]\left[\frac{FLo}{F}\right]\left[\frac{d}{ord}\right]\left[\frac{018inO}{inOxf}\right]$$

Produce grammars:

$G_1(P)$:

$N \to \text{C2 } M \text{ C2\#LoC2018\#}$
$N \to \text{xfor } M \text{ xfor\#\#}$
$N \to \text{nf } M \text{ nf\#d\#}$
$N \to \text{FLo } M \text{ FLo\#F\#}$
$N \to \text{d } M \text{ d\#ord\#}$
$N \to \text{018inO } M \text{ 018inO\#inOxf\#}$
$M \to N \mid \#$

$G_2(P)$:

$N \to \text{LoC2018 } M \text{ C2\#LoC2018\#}$
$N \to M \text{ xfor\#\#}$
$N \to \text{d } M \text{ nf\#d\#}$
$N \to \text{F } M \text{ FLo\#F\#}$
$N \to \text{ord } M \text{ d\#ord\#}$
$N \to \text{inOxf } M \text{ 018inO\#inOxf\#}$
$M \to N \mid \#$

$$\left[\frac{FLo}{F}\right]\left[\frac{C2}{LoC2018}\right]\left[\frac{018inO}{inOxf}\right]\left[\frac{xfor}{}\right]\left[\frac{d}{ord}\right]$$

FLoC2018InOxford # d#ord#xfor#018inO#inOxf#C2#LoC2018#FLo#F#

FLoC2018InOxford # d#ord#xfor#018inO#inOxf#C2#LoC2018#FLo#F#

$$\text{PCP}(P) \leftrightarrow \mathcal{L}(G_1(P)) \cap \mathcal{L}(G_2(P)) \neq \emptyset$$

TM halting $\preceq$ SR

We use the TM definition from Asperti, Ricciotti (2015, in Matita)

TM halting $\preceq$ SR

We use the TM definition from Asperti, Ricciotti (2015, in Matita)

Turing machines are special forms of rewriting systems:

TM halting $\preceq$ SR

We use the TM definition from Asperti, Ricciotti (2015, in Matita)

Turing machines are special forms of rewriting systems:

Read	Write	Move	x	y	x	y	x	y
$\bot$	$\bot$	L	$q_1 \langle$	$q_2 \langle$	$a\, q_1 \rangle$	$q_2\, a \rangle$		
$\bot$	$\bot$	N	$q_1 \langle$	$q_2 \langle$	$q_1 \rangle$	$q_2 \rangle$		
$\bot$	$\bot$	R	$q_1 \langle\rangle$	$q_2 \langle\rangle$	$q_1 \rangle$	$q_2 \rangle$	$q_1 \langle\, a$	$\langle\, q_1\, a$
$\bot$	$\lfloor b \rfloor$	L	$q_1 \langle$	$q_2 \langle b$	$a\, q_1 \rangle$	$q_2\, a\, b \rangle$		
$\bot$	$\lfloor b \rfloor$	N	$q_1 \langle$	$\langle q_2\, b$	$q_1 \rangle$	$q_2\, b \rangle$		
$\bot$	$\lfloor b \rfloor$	R	$q_1 \langle$	$\langle b\, q_2$	$q_1 \rangle$	$b\, q_2 \rangle$		
$\lfloor a \rfloor$	$\bot$	L	$\langle q_1\, a$	$q_2 \langle a$	$c\, q_1\, a$	$q_2\, c\, a$		
$\lfloor a \rfloor$	$\bot$	N	$q_1\, a$	$q_2\, a$				
$\lfloor a \rfloor$	$\bot$	R	$q_1\, a$	$a\, q_2$				
$\lfloor a \rfloor$	$\lfloor b \rfloor$	L	$\langle q_1\, a$	$q_2 \langle b$	$c\, q_1\, a$	$q_2\, c\, b$		
$\lfloor a \rfloor$	$\lfloor b \rfloor$	N	$q_1\, a$	$q_2\, b$				
$\lfloor a \rfloor$	$\lfloor b \rfloor$	R	$q_1\, a$	$b\, q_2$				

TM halting $\preceq$ SR

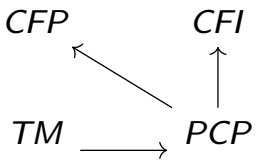
We use the TM definition from Asperti, Ricciotti (2015, in Matita)

Turing machines are special forms of rewriting systems:

Read	Write	Move	x	y	x	y	x	y
$\bot$	$\bot$	L	$q_1 \langle$	$q_2 \langle$	$a\, q_1 \rangle$	$q_2\, a \rangle$		
$\bot$	$\bot$	N	$q_1 \langle$	$q_2 \langle$	$q_1 \rangle$	$q_2 \rangle$		
$\bot$	$\bot$	R	$q_1 \langle\rangle$	$q_2 \langle\rangle$	$q_1 \rangle$	$q_2 \rangle$	$q_1 \langle\, a$	$\langle\, q_1\, a$
$\bot$	$\lfloor b \rfloor$	L	$q_1 \langle$	$q_2 \langle b$	$a\, q_1 \rangle$	$q_2\, a\, b \rangle$		
$\bot$	$\lfloor b \rfloor$	N	$q_1 \langle$	$\langle q_2\, b$	$q_1 \rangle$	$q_2\, b \rangle$		
$\bot$	$\lfloor b \rfloor$	R	$q_1 \langle$	$\langle b\, q_2$	$q_1 \rangle$	$b\, q_2 \rangle$		
$\lfloor a \rfloor$	$\bot$	L	$\langle q_1\, a$	$q_2 \langle a$	$c\, q_1\, a$	$q_2\, c\, a$		
$\lfloor a \rfloor$	$\bot$	N	$q_1\, a$	$q_2\, a$				
$\lfloor a \rfloor$	$\bot$	R	$q_1\, a$	$a\, q_2$				
$\lfloor a \rfloor$	$\lfloor b \rfloor$	L	$\langle q_1\, a$	$q_2 \langle b$	$c\, q_1\, a$	$q_2\, c\, b$		
$\lfloor a \rfloor$	$\lfloor b \rfloor$	N	$q_1\, a$	$q_2\, b$				
$\lfloor a \rfloor$	$\lfloor b \rfloor$	R	$q_1\, a$	$b\, q_2$				

Huge proof, essentially a big case distinction, no insight

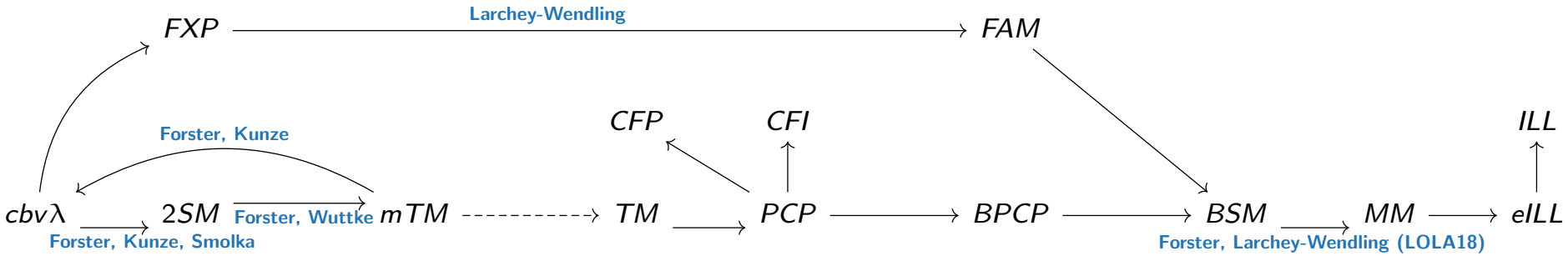
Future Work



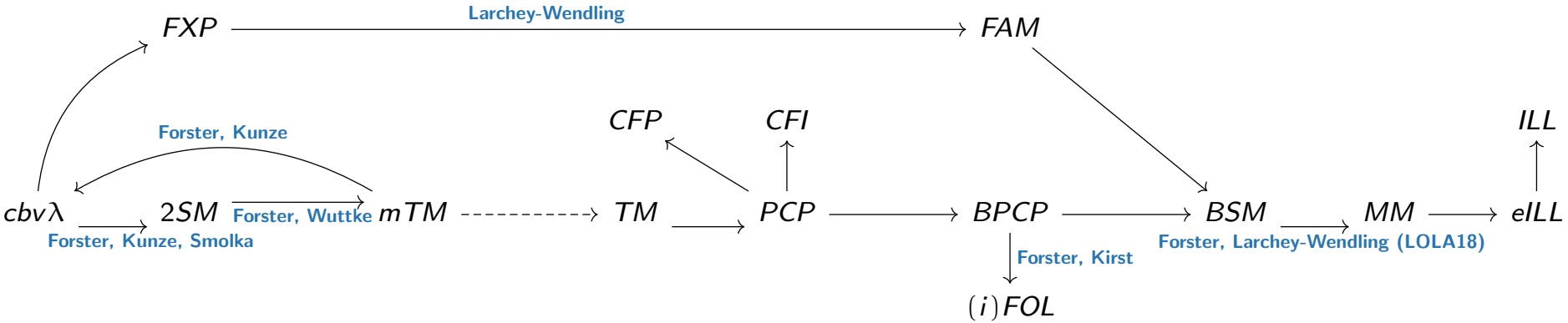
Future Work


CFP
CFI
ILL
TM
PCP
BPCP
BSM
MM
eILL
Forster, Larchey-Wendling (LOLA18)

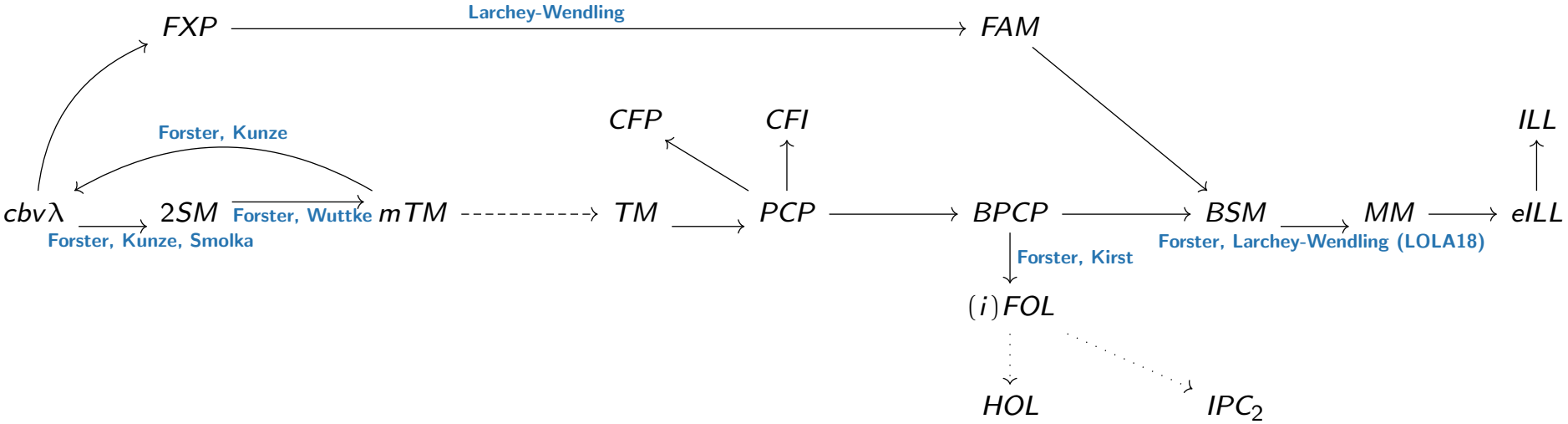
Future Work


FXP
Larchey-Wendling
FAM
CFP
CFI
ILL
Forster, Kunze
cbvλ
2SM
Forster, Wuttke
mTM
TM
PCP
BPCP
BSM
MM
eILL
Forster, Kunze, Smolka
Forster, Larchey-Wendling (LOLA18)

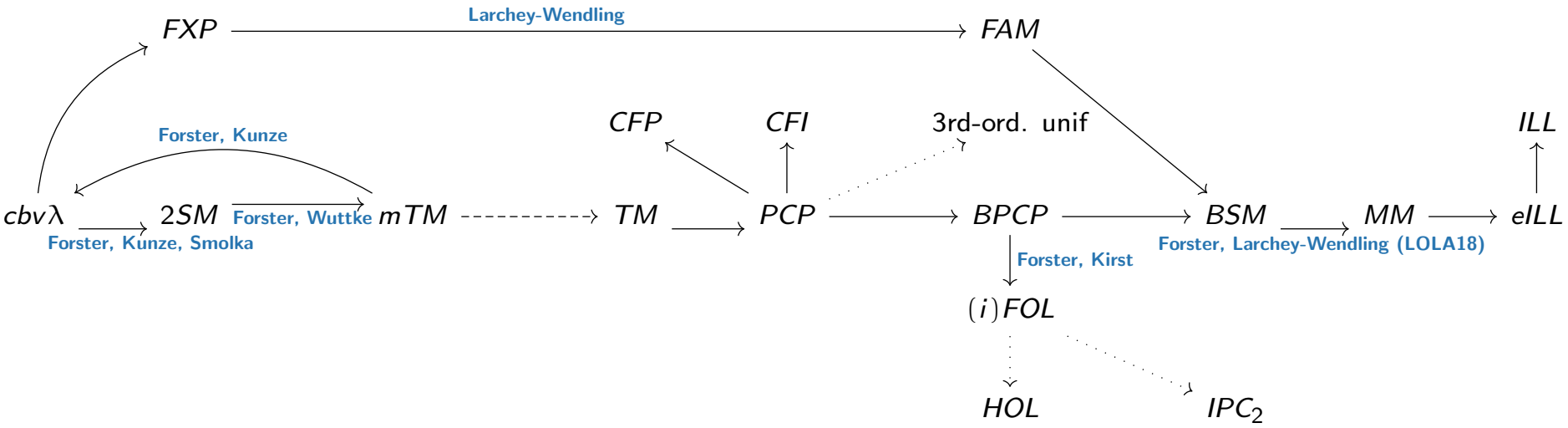
Future Work


FXP
Larchey-Wendling
FAM
CFP
CFI
ILL
Forster, Kunze
cbvλ
2SM
Forster, Wuttke
mTM
TM
PCP
BPCP
BSM
MM
eILL
Forster, Kunze, Smolka
Forster, Kirst
Forster, Larchey-Wendling (LOLA18)
(i)FOL

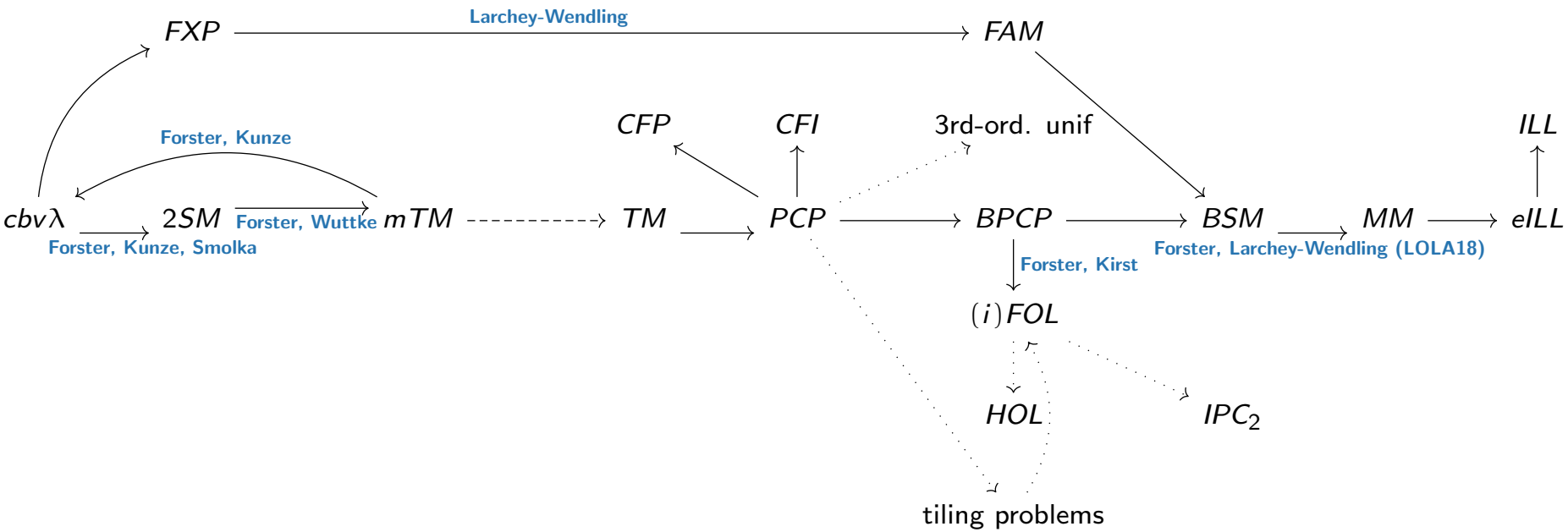
Future Work


FXP
Larchey-Wendling
FAM
CFP
CFI
ILL
Forster, Kunze
cbvλ
2SM
Forster, Wuttke
mTM
TM
PCP
BPCP
BSM
MM
eILL
Forster, Kunze, Smolka
Forster, Larchey-Wendling (LOLA18)
Forster, Kirst
(i)FOL
HOL
IPC2

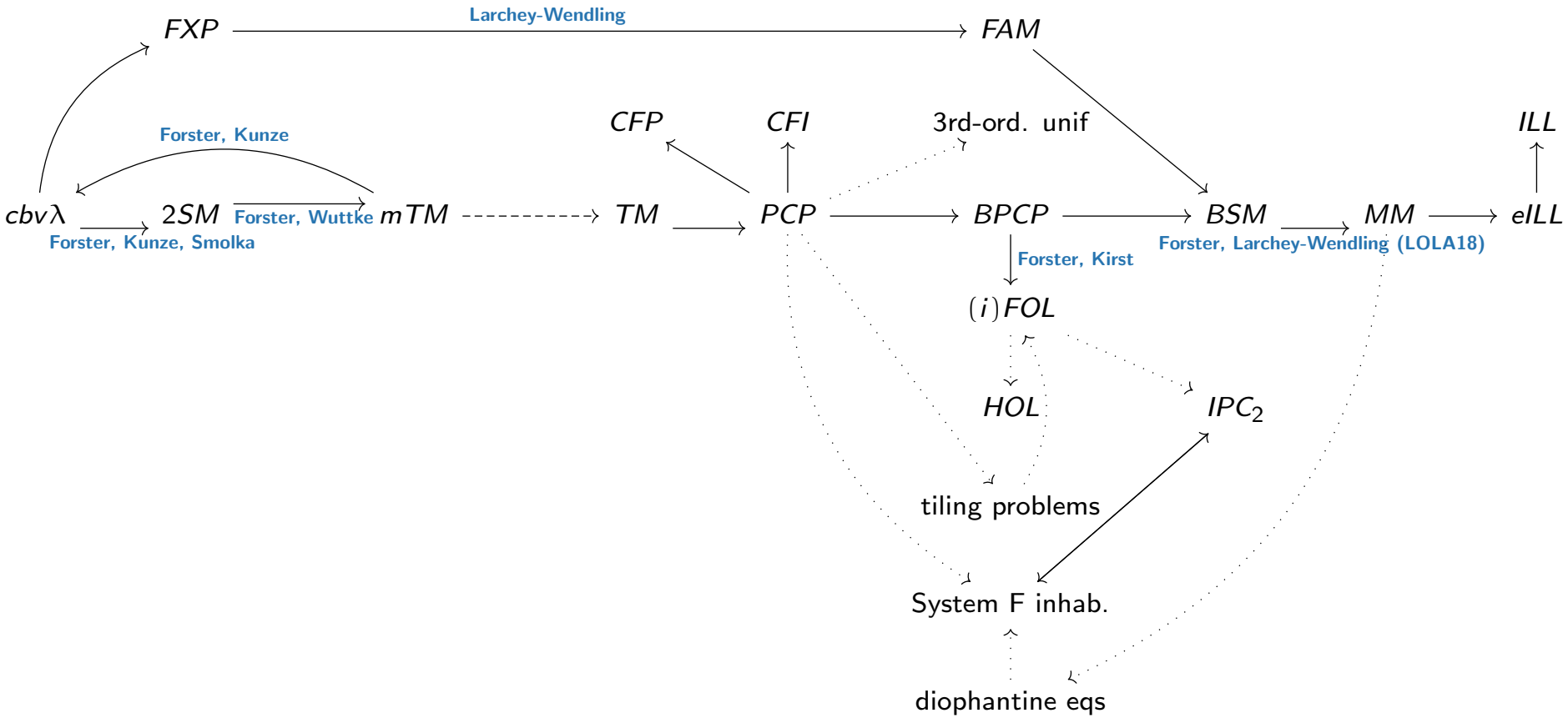
Future Work


FXP
Larchey-Wendling
FAM
CFP
CFI
3rd-ord. unif
ILL
Forster, Kunze
cbvλ
2SM
Forster, Wuttke
mTM
TM
PCP
BPCP
BSM
MM
eILL
Forster, Kunze, Smolka
Forster, Larchey-Wendling (LOLA18)
Forster, Kirst
(i)FOL
HOL
IPC2

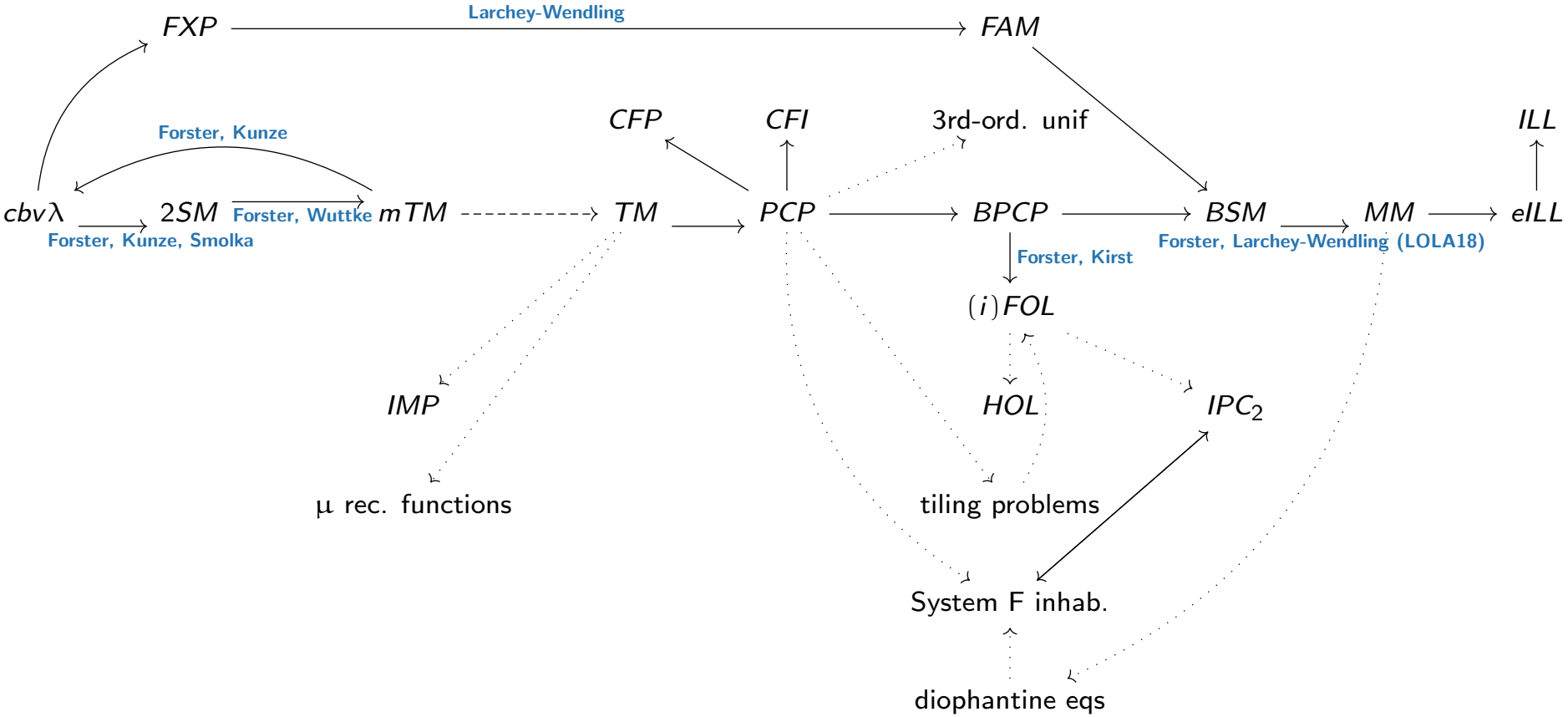
Future Work


FXP
Larchey-Wendling
FAM
CFP
CFI
3rd-ord. unif
ILL
Forster, Kunze
cbvλ
2SM
Forster, Wuttke
mTM
TM
PCP
BPCP
BSM
MM
eILL
Forster, Kunze, Smolka
Forster, Kirst
Forster, Larchey-Wendling (LOLA18)
(i)FOL
HOL
IPC2
tiling problems

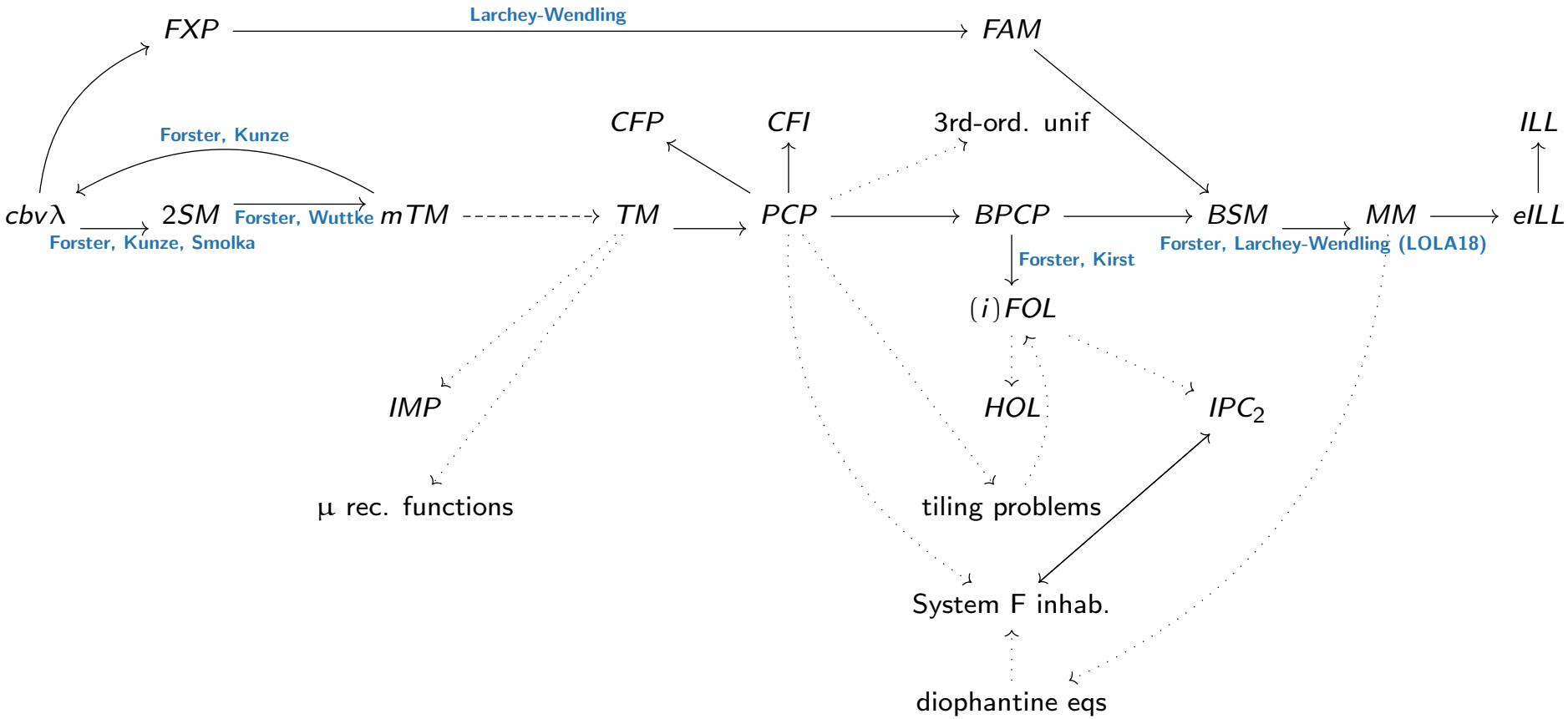
Future Work


FXP
Larchey-Wendling
FAM
CFP
CFI
3rd-ord. unif
ILL
Forster, Kunze
cbvλ
2SM
Forster, Wuttke
mTM
TM
PCP
BPCP
BSM
MM
eILL
Forster, Kunze, Smolka
Forster, Kirst
Forster, Larchey-Wendling (LOLA18)
(i)FOL
HOL
IPC2
tiling problems
System F inhab.
diophantine eqs

Future Work


FXP
Larchey-Wendling
FAM
Forster, Kunze
CFP
CFI
3rd-ord. unif
ILL
cbvλ
2SM
Forster, Wuttke
mTM
TM
PCP
BPCP
BSM
MM
eILL
Forster, Kunze, Smolka
Forster, Kirst
Forster, Larchey-Wendling (LOLA18)
(i)FOL
IMP
HOL
IPC2
μ rec. functions
tiling problems
System F inhab.
diophantine eqs

Future Work



Forster, Kunze: Automated extraction from Coq to cbv λ-calculus yields computability proofs for all reductions

Wrap-up

SAARLAND UNIVERSITY
COMPUTER SCIENCE

- A novel way to prove undecidability in Coq
- Transparent, explainable reduction from TM to PCP
- Enabling loads of future work. Add your own undecidable problems!

`https://www.ps.uni-saarland.de/extras/PCP/`