Synthetic Undecidability of MSELL via FRACTRAN mechanised in Coq

Dominique Larchey-Wendling

FSCD 2021
July 22

Introduction

Motivations for studying MSELL

- MELL decidability
  - most important LL open decidability question
  - some proof attempts (Bimbo 2015)
  - later refuted (Strassburger 2019)
  - MELL encodes Petri nets reachability
- Petri nets, VASS reachability is decidable
  - major results from 80's (Mayr 1981, et al)
  - proof still revisted in the 2010's (Leroux)
  - non-elementary (Czerwinski et al 2019)
  - (possibly) Ackermann complete (Czerwinski 2021, Leroux 2021)
- MSELL simple extension of MELL
  - 3 modalities, one of them exponential
  - modalities interact in the promotion rule
- MSELL is undecidable (Chaudhuri 2018)
  - unlike ILL, proof *does not use forking* via &
  - instead exploits interaction of modalities

Approach and main focus of the talk

- The proof of Chaudhuri 2018
  - undecidability of (classical) MSELL
  - many-one reduction from *two counters* Minsky machines
  - completeness of the reduction via focussing
- Revisit the proof for (intuitionistic) IMSELL
  - compare with the ILL proof (CPP'19)
  - completeness via (trivial) phase semantics
- A synthetic framework for mechanized undecidability in Coq
  - need to add undecidability for two counters machines $\mathrm{MMA0}_2$
  - we plug from the FRACTRAN seed instead of many counters machines
  - we introduce a sequent formulation of counter machines $\mathrm{MM}_{\mathrm{nd}}$
- In this talk, we focus on:
  - comparing the reductions from $\mathrm{MM}_{\mathrm{nd}}$ to ILL vs. IMSELL
  - explain some details for the FRACTRAN to $\mathrm{MMA0}_2$

A library for synthetic undecidability in Coq

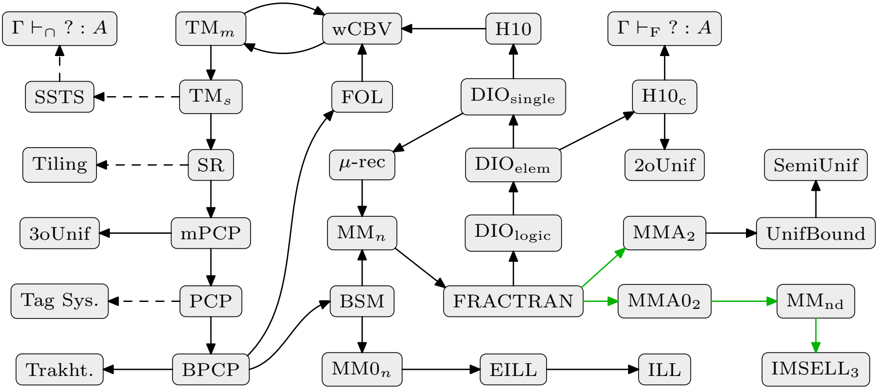
`https://github.com/uds-psl/coq-library-undecidability`

Definition (Synthetic undecidability)

P undecidable $:=$ Halting problem reduces to P

- a decision problem $(X, P) : \Sigma(X : \texttt{Type}), X \to \mathbb{P}$
- Many-one reduction from (X, P) to (Y, Q)
  - computable function $f : X \to Y$ s.t. $\forall x,\ P\,x \leftrightarrow Q(f\,x)$
  - "computable" requirement replaced by "defined in CTT"
  - We write $P \preceq Q$ when such reduction exists
- Coq terms are computable (axiom-free)
- Undecidability in Coq by many-one reductions
  - if P undecidable and $P \preceq Q$ then Q undecidable

Overview of the library of Undecidability (CoqPL'20)



- Y. Forster, DLW, A. Dudenhefner, F. Kunze, D. Kirst, G. Smolka ...
- ITP'18'19'21, CPP'19'20, FSCD'19'20'21, IJCAR'20, LICS'21
- Mechanizing undecidability for logics was my main initial motivation

Intuitionistic Linear Logic

Intuitionistic Linear Logic (ILL)

$$\frac{}{A \vdash A} \qquad \frac{A, \Gamma \vdash B}{\Gamma \vdash A \multimap B}$$

$$\frac{\Gamma \vdash A \qquad B, \Delta \vdash C}{A \multimap B, \Gamma, \Delta \vdash C}$$

$$\frac{\Gamma \vdash A \qquad \Gamma \vdash B}{\Gamma \vdash A \,\&\, B}$$

$$\frac{A, \Gamma \vdash C}{A \,\&\, B, \Gamma \vdash C} \qquad \frac{B, \Gamma \vdash C}{A \,\&\, B, \Gamma \vdash C}$$

$$\frac{!\Gamma \vdash B}{!\Gamma \vdash !B}\ \text{promotion}$$

$$\frac{A, \Gamma \vdash B}{!A, \Gamma \vdash B}\ \text{dereliction}$$

$$\frac{\Gamma \vdash B}{!A, \Gamma \vdash B}\ \text{Weak}$$

$$\frac{!A, !A, \Gamma \vdash B}{!A, \Gamma \vdash B}\ \text{Contr}$$

Intui. Multiplicative and Exponential LL (IMELL)

$$\frac{}{A \vdash A} \qquad \frac{A, \Gamma \vdash B}{\Gamma \vdash A \multimap B}$$

$$\frac{\Gamma \vdash A \qquad B, \Delta \vdash C}{A \multimap B, \Gamma, \Delta \vdash C}$$

$$\frac{!\Gamma \vdash B}{!\Gamma \vdash !B} \text{ promotion}$$

$$\frac{A, \Gamma \vdash B}{!A, \Gamma \vdash B} \text{ dereliction}$$

$$\frac{\Gamma \vdash B}{!A, \Gamma \vdash B} \text{ Weak}$$

$$\frac{!A, !A, \Gamma \vdash B}{!A, \Gamma \vdash B} \text{ Contr}$$

Intui. Mult. Sub-Exponential LL (IMSELL)

$$\frac{}{A \vdash A} \qquad \frac{A, \Gamma \vdash B}{\Gamma \vdash A \multimap B}$$

$$\frac{\Gamma \vdash A \qquad B, \Delta \vdash C}{A \multimap B, \Gamma, \Delta \vdash C}$$

$$\frac{!^{\star}\Gamma \vdash B}{!^{\star}\Gamma \vdash !^{m} B}\ m \preccurlyeq \star$$

$$\frac{A, \Gamma \vdash B}{!^{m} A, \Gamma \vdash B}$$

$$\frac{\Gamma \vdash B}{!^{u} A, \Gamma \vdash B}\ u \in \mathcal{U}$$

$$\frac{!^{u} A, !^{u} A, \Gamma \vdash B}{!^{u} A, \Gamma \vdash B}\ u \in \mathcal{U}$$

IMSELL$_\Lambda$ (the modal structure)

- Compared to ILL: multiplicatives only (no &, like IMELL)
- Compared to IMELL: modal rules are refined
  - Contr./Weak. limited to unbounded modalities
- Modal structure $\Lambda = (\Lambda, \preccurlyeq, \mathcal{U})$:
  - with a *pre-order* $\preccurlyeq : \Lambda \to \Lambda \to \mathbb{P}$
  - a sub-set of *unbounded* modalities $u \in \mathcal{U}$, with $\mathcal{U} : \Lambda \to \mathbb{P}$
  - $\mathcal{U}$ is $\preccurlyeq$*-upward closed*
- Promotion: *interaction* between modalities $\star = \{k_1, \dots, k_n\}$

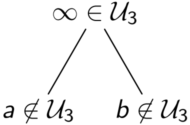
$$\frac{!^\star\Gamma \vdash B}{!^\star\Gamma \vdash !^m B}\ m \preccurlyeq \star \qquad \Bigg| \qquad \frac{!^{k_1}A_1, \dots, !^{k_n}A_n \vdash B}{!^{k_1}A_1, \dots, !^{k_n}A_n \vdash !^m B}\ m \preccurlyeq k_1, \dots, k_n$$

- Uniform case $m = k_1 = \cdots = k_n$ same as (regular) promotion

$$\frac{!^m\Gamma \vdash B}{!^m\Gamma \vdash !^m B}$$

IMSELL$_\Lambda$ and IMSELL$_3$ (undecidability)

- Decidability of IMSELL$_\Lambda$ depending on Λ
- IMSELL$_3$ = IMSELL$_{\Lambda_3}$ is undecidable:
  - $\Lambda_3 = \{a, b, \infty\}$, $\mathcal{U}_3 = \{\infty\}$
  - $a \preccurlyeq \infty$ and $b \preccurlyeq \infty$
  - $a \not\preccurlyeq b$ and $b \not\preccurlyeq a$



- Also IMSELL$_\Lambda$ undecidable when Λ embeds Λ_3
- IMSELL$_\infty$ is isomorphic to IMELL
  - $\Lambda_\infty = \mathcal{U}_\infty = \{\infty\}$
  - IMSELL$_\Lambda$ contains IMELL when $\mathcal{U} \neq \emptyset$
- IMSELL$_\Lambda$ decidable?
  - yes if $\mathcal{U} = \emptyset$
  - IMELL $\simeq$ IMSELL$_\infty$ is unknown
- Undecidability for IMSELL$_3$:
  - by many-one reduction from two-counters Minsky machines

Reducing Minsky machines to ILL and IMSELL_3

$\mathrm{MM}_{\mathrm{nd}}$: sequent style Minsky machines

- Σ finite list/set of instructions ($\mathtt{STOP}_{\mathrm{n}}$, $\mathtt{INC}_{\mathrm{n}}$, $\mathtt{DEC}_{\mathrm{n}}$, $\boxed{\mathtt{ZERO}_{\mathrm{n}}}$)
- Sequents: $\Sigma \mathbin{/\!\!/_{\mathrm{n}}} x \oplus y \vdash p$
- x/y values (in $\mathbb{N}$) of *two counters* α/β
- $p, q, \ldots$ are labels (in e.g. $\mathbb{N}$)
- Computation as proof-search, Halting as $\boxed{\text{derivability}}$

$$\frac{}{\Sigma \mathbin{/\!\!/_{\mathrm{n}}} 0 \oplus 0 \vdash p}\ \mathtt{STOP}_{\mathrm{n}}\, p \in \Sigma$$

$$\frac{\Sigma \mathbin{/\!\!/_{\mathrm{n}}} 1{+}x \oplus y \vdash q}{\Sigma \mathbin{/\!\!/_{\mathrm{n}}} x \oplus y \vdash p}\ \mathtt{INC}_{\mathrm{n}}\, \alpha\, p\, q \in \Sigma \qquad \frac{\Sigma \mathbin{/\!\!/_{\mathrm{n}}} x \oplus 1{+}y \vdash q}{\Sigma \mathbin{/\!\!/_{\mathrm{n}}} x \oplus y \vdash p}\ \mathtt{INC}_{\mathrm{n}}\, \beta\, p\, q \in \Sigma$$

$$\frac{\Sigma \mathbin{/\!\!/_{\mathrm{n}}} x \oplus y \vdash q}{\Sigma \mathbin{/\!\!/_{\mathrm{n}}} 1{+}x \oplus y \vdash p}\ \mathtt{DEC}_{\mathrm{n}}\, \alpha\, p\, q \in \Sigma \qquad \frac{\Sigma \mathbin{/\!\!/_{\mathrm{n}}} x \oplus y \vdash q}{\Sigma \mathbin{/\!\!/_{\mathrm{n}}} x \oplus 1{+}y \vdash p}\ \mathtt{DEC}_{\mathrm{n}}\, \beta\, p\, q \in \Sigma$$

$$\frac{\Sigma \mathbin{/\!\!/_{\mathrm{n}}} 0 \oplus y \vdash q}{\Sigma \mathbin{/\!\!/_{\mathrm{n}}} 0 \oplus y \vdash p}\ \mathtt{ZERO}_{\mathrm{n}}\, \alpha\, p\, q \in \Sigma \qquad \frac{\Sigma \mathbin{/\!\!/_{\mathrm{n}}} x \oplus 0 \vdash q}{\Sigma \mathbin{/\!\!/_{\mathrm{n}}} x \oplus 0 \vdash p}\ \mathtt{ZERO}_{\mathrm{n}}\, \beta\, p\, q \in \Sigma$$

Basics of the encoding of $\mathrm{MM}_{\mathrm{nd}}$ in ILL/IMSELL$_3$

- Admissible rules in IMELL, IMSELL$_3$ and ILL

$$\frac{\Delta \vdash B}{!^\infty\Sigma, \Delta \vdash B}\ \text{(gen. weak.)} \qquad \frac{A, !^\infty\Sigma, \Delta \vdash B}{!^\infty\Sigma, \Delta \vdash B}\ A \in \Sigma\ \text{(absorption)}$$

- We identify $!^\infty$ and $!$
  - IMELL is a fragment of both ILL and IMSELL$_3$
- From $\mathrm{MM}_{\mathrm{nd}}$ sequents to LL sequents

$$\Sigma \mathbin{/\!\!/_{\mathrm{n}}} x \oplus y \vdash p \qquad \rightsquigarrow \qquad !^\infty\overline{\Sigma}, x\overline{\alpha}, y\overline{\beta} \vdash \overline{p}$$

- We below denote $\Delta = x\overline{\alpha}, y\overline{\beta} = \underbrace{\overline{\alpha}, \ldots, \overline{\alpha}}_{x\ \text{times}}, \underbrace{\overline{\beta}, \ldots, \overline{\beta}}_{y\ \text{times}}$
- $\overline{\Sigma}$, $\overline{\alpha}$ and $\overline{\beta}$ depend on ILL vs. IMSELL$_3$

Increment $\mathtt{INC}_{\mathrm{n}}\, \alpha\, p\, q$ (already in IMELL)

$$\frac{\Sigma \mathbin{/\!\!/_{\mathrm{n}}} 1{+}x \oplus y \vdash q}{\Sigma \mathbin{/\!\!/_{\mathrm{n}}} x \oplus y \vdash p}\ \mathtt{INC}_{\mathrm{n}}\, \alpha\, p\, q \in \Sigma$$

$$\cfrac{\cfrac{\cfrac{!^{\infty}\overline{\Sigma}, \overline{\alpha}, \Delta \vdash \overline{q}}{!^{\infty}\overline{\Sigma}, \Delta \vdash \overline{\alpha} \multimap \overline{q}}\ \multimap\text{-right} \qquad \cfrac{}{\overline{p} \vdash \overline{p}}}{(\overline{\alpha} \multimap \overline{q}) \multimap \overline{p}, !^{\infty}\overline{\Sigma}, \Delta \vdash \overline{p}}\ \multimap\text{-left}}{!^{\infty}\overline{\Sigma}, \Delta \vdash \overline{p}}\ (\overline{\alpha} \multimap \overline{q}) \multimap \overline{p} \in \overline{\Sigma}$$

Decrement $\mathtt{DEC}_\mathrm{n}\,\alpha\,p\,q$ (already in IMELL)

$$\frac{\Sigma \mathbin{/\!\!/_{\mathrm{n}}} x \oplus y \vdash q}{\Sigma \mathbin{/\!\!/_{\mathrm{n}}} 1{+}x \oplus y \vdash p}\ \mathtt{DEC}_\mathrm{n}\,\alpha\,p\,q \in \Sigma$$

$$\dfrac{\dfrac{}{\overline{\alpha} \vdash \overline{\alpha}} \qquad \dfrac{!^\infty\overline{\Sigma}, \Delta \vdash \overline{q} \qquad \dfrac{}{\overline{p} \vdash \overline{p}}}{\overline{q} \multimap \overline{p}, !^\infty\overline{\Sigma}, \Delta \vdash \overline{p}}\,\multimap\text{-left}}{\dfrac{\overline{\alpha} \multimap (\overline{q} \multimap \overline{p}), !^\infty\overline{\Sigma}, \overline{\alpha}, \Delta \vdash \overline{p}}{!^\infty\overline{\Sigma}, \overline{\alpha}, \Delta \vdash \overline{p}}\ \overline{\alpha} \multimap (\overline{q} \multimap \overline{p}) \in \overline{\Sigma}}\,\multimap\text{-left}$$

Stop instruction $\mathtt{STOP}_{\mathrm{n}}\, p$ (already in IMELL)

$$\cfrac{}{\Sigma \mathbin{/\!\!/_{\mathrm{n}}} 0 \oplus 0 \vdash p}\ \mathtt{STOP}_{\mathrm{n}}\, p \in \Sigma$$

$$\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{}{\overline{p} \vdash \overline{p}}}{\vdash \overline{p} \multimap \overline{p}}\ \multimap\text{-right} \qquad \cfrac{}{\overline{p} \vdash \overline{p}}}{(\overline{p} \multimap \overline{p}) \multimap \overline{p} \vdash \overline{p}}\ \multimap\text{-left}}{(\overline{p} \multimap \overline{p}) \multimap \overline{p}, !^{\infty}\overline{\overline{\Sigma}} \vdash \overline{p}}\ \text{gen. weak.}}{!^{\infty}\overline{\overline{\Sigma}}, \emptyset \vdash \overline{p}}\ (\overline{p} \multimap \overline{p}) \multimap \overline{p} \in \overline{\overline{\Sigma}}$$

The conditional jump $\mathtt{ZERO}_{\mathrm{n}}\,\alpha\,p\,q$ (part 1, ILL only)

$$\frac{\Sigma \mathbin{/\!\!/_{\mathrm{n}}} 0 \oplus y \ \vdash\ q}{\Sigma \mathbin{/\!\!/_{\mathrm{n}}} 0 \oplus y \ \vdash\ p}\ \mathtt{ZERO}_{\mathrm{n}}\,\alpha\,p\,q \in \Sigma$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\boxed{\text{zero test on } \overline{\alpha}}}{!^{\infty}\overline{\Sigma}, y\overline{\beta} \vdash \underline{\alpha}} \qquad !^{\infty}\overline{\Sigma}, y\overline{\beta} \vdash \overline{q}}{!^{\infty}\overline{\Sigma}, y\overline{\beta} \vdash \underline{\alpha} \,\&\, \overline{q}}\ \&\text{-right} \qquad \dfrac{}{\overline{p} \vdash \overline{p}}}{(\underline{\alpha} \,\&\, \overline{q}) \multimap \overline{p}, !^{\infty}\overline{\Sigma}, y\overline{\beta} \vdash \overline{p}}\ \multimap\text{-left}}{!^{\infty}\overline{\Sigma}, y\overline{\beta} \vdash \overline{p}}\ (\underline{\alpha} \,\&\, \overline{q}) \multimap \overline{p} \in \overline{\Sigma}$$

- $\underline{\alpha}$ and $\underline{\beta}$ are fresh variables
  - $\underline{\alpha}$ implements a zero test of $\overline{\alpha}$, i.e. $x =^{?} 0$

The $\boxed{\text{zero test on } \overline{\alpha}}$ (part 2, already in IMELL)

$$
\begin{prooftree}
\AxiomC{}
\UnaryInfC{$\overline{\beta} \vdash \overline{\beta}$}
\AxiomC{}
\UnaryInfC{$\underline{\alpha} \vdash \underline{\alpha}$}
\RightLabel{$\multimap$-right}
\UnaryInfC{$\vdash \underline{\alpha} \multimap \underline{\alpha}$}
\AxiomC{}
\UnaryInfC{$\underline{\alpha} \vdash \underline{\alpha}$}
\RightLabel{$\multimap$-left}
\BinaryInfC{$(\underline{\alpha} \multimap \underline{\alpha}) \multimap \underline{\alpha}, \emptyset \vdash \underline{\alpha}$}
\RightLabel{gen. weak.}
\UnaryInfC{$(\underline{\alpha} \multimap \underline{\alpha}) \multimap \underline{\alpha}, !^{\infty}\overline{\Sigma}, \emptyset \vdash \underline{\alpha}$}
\RightLabel{$(\underline{\alpha} \multimap \underline{\alpha}) \multimap \underline{\alpha} \in \overline{\Sigma}$}
\UnaryInfC{$!^{\infty}\overline{\Sigma}, \emptyset \vdash \underline{\alpha}$}
\UnaryInfC{$\dots$}
\RightLabel{repeat y times}
\UnaryInfC{$!^{\infty}\overline{\Sigma}, y\overline{\beta} \vdash \underline{\alpha}$}
\AxiomC{}
\UnaryInfC{$\underline{\alpha} \vdash \underline{\alpha}$}
\RightLabel{$\multimap$-left}
\BinaryInfC{$\underline{\alpha} \multimap \underline{\alpha}, !^{\infty}\overline{\Sigma}, y\overline{\beta} \vdash \underline{\alpha}$}
\RightLabel{$\multimap$-left}
\BinaryInfC{$\overline{\beta} \multimap (\underline{\alpha} \multimap \underline{\alpha}), !^{\infty}\overline{\Sigma}, \overline{\beta}, y\overline{\beta} \vdash \underline{\alpha}$}
\RightLabel{$\overline{\beta} \multimap (\underline{\alpha} \multimap \underline{\alpha}) \in \overline{\Sigma}$}
\UnaryInfC{$!^{\infty}\overline{\Sigma}, (1+y)\overline{\beta} \vdash \underline{\alpha}$}
\end{prooftree}
$$

The conditional jump $\mathtt{ZERO}_{\mathrm{n}}\,\alpha\,p\,q$ (case of IMSELL$_3$)

$$\frac{\Sigma \,/\!\!/_{\mathrm{n}}\, 0 \oplus y \;\vdash\; q}{\Sigma \,/\!\!/_{\mathrm{n}}\, 0 \oplus y \;\vdash\; p}\;\mathtt{ZERO}_{\mathrm{n}}\,\alpha\,p\,q \in \Sigma$$

$$\dfrac{\dfrac{\dfrac{!^{\infty}\overline{\Sigma}, y\overline{\beta} \vdash \overline{q}}{!^{\infty}\overline{\Sigma}, y\overline{\beta} \vdash\, !^{b}\overline{q}}\; b \preccurlyeq \infty, b \qquad \dfrac{}{\overline{p} \vdash \overline{p}}}{!^{b}\overline{q} \multimap \overline{p}, !^{\infty}\overline{\Sigma}, y\overline{\beta} \vdash \overline{p}}\;\multimap\text{-left}}{!^{\infty}\overline{\Sigma}, y\overline{\beta} \vdash \overline{p}}\; !^{b}\overline{q} \multimap \overline{p} \in \overline{\Sigma}$$

- for IMSELL$_3$, $\overline{\alpha}$ and $\overline{\beta}$ not just fresh variables
  - $\overline{\alpha} := !^{a}\alpha_0$ and $\overline{\beta} := !^{b}\beta_0$ (with α_0, β_0 fresh)
  - exploit the interaction between $!^{\infty}$, $!^{a}$ and $!^{b}$
- the promotion rule $(b \preccurlyeq \infty, b)$ would not apply if $x > 0$
  - $\overline{\alpha} = !^{a}\alpha_0$ would occur on the left of $\vdash$
  - and $b \not\preccurlyeq a$ in the modal structure Λ_3

Soundness of the reduction from $\mathrm{MM}_{\mathrm{nd}}$

- $\alpha_0 := 0$, $\beta_0 := 1$, $\overline{p} := 2 + p$, $\overline{\alpha} := !^a\alpha_0$ and $\overline{\beta} := !^b\beta_0$

$$\begin{aligned}
\overline{\mathtt{STOP}_{\mathrm{n}}\, p} &:= (\overline{p} \multimap \overline{p}) \multimap \overline{p} \\
\overline{\mathtt{INC}_{\mathrm{n}}\, \alpha\, p\, q} &:= (\overline{\alpha} \multimap \overline{q}) \multimap \overline{p} & \qquad \overline{\mathtt{INC}_{\mathrm{n}}\, \beta\, p\, q} &:= (\overline{\beta} \multimap \overline{q}) \multimap \overline{p} \\
\overline{\mathtt{DEC}_{\mathrm{n}}\, \alpha\, p\, q} &:= \overline{\alpha} \multimap (\overline{q} \multimap \overline{p}) & \qquad \overline{\mathtt{DEC}_{\mathrm{n}}\, \beta\, p\, q} &:= \overline{\beta} \multimap (\overline{q} \multimap \overline{p}) \\
\overline{\mathtt{ZERO}_{\mathrm{n}}\, \alpha\, p\, q} &:= !^b\overline{q} \multimap \overline{p} & \qquad \overline{\mathtt{ZERO}_{\mathrm{n}}\, \beta\, p\, q} &:= !^a\overline{q} \multimap \overline{p}
\end{aligned}$$

- $\overline{\Sigma} = \overline{[\sigma_1; \ldots ; \sigma_n]} := \overline{\sigma_1}, \ldots , \overline{\sigma_n}$

Theorem (Soundness)

If $\Sigma \mathbin{/\!\!/_{\mathrm{n}}} x \oplus y \vdash p$ *is derivable in* $\mathrm{MM}_{\mathrm{nd}}$ *then* $!^\infty\overline{\Sigma}, x\overline{\alpha}, y\overline{\beta} \vdash \overline{p}$ *is provable in* $IMSELL_3$

- completeness by semantics in place of focusing (Chaudhuri 2018)

Trivial Phase Semantics for IMSELL_Λ

- Start from a commutative monoid $(M, \bullet, \epsilon)$ e.g. $(\mathbb{N}^2, +, [0;0])$
- for $X, Y \subseteq M$ define:
  - extended composition: $X \bullet Y := \{x \bullet y \mid x \in X \wedge y \in Y\}$
  - linear map: $X \multimap\!\!\bullet\, Y := \{k \in M \mid \{k\} \bullet X \subseteq Y\}$
- trivial means the closure is the *identity closure*
- interpret $(\Lambda, \mathcal{U}, \preccurlyeq)$, for $m : \Lambda$, $K_m \subseteq M$ s.t.
  - decreasing: $\forall m\, k,\ m \preccurlyeq k \to K_k \subseteq K_m$
  - sub-monoid: $\forall m,\ \epsilon \in K_m \wedge K_m \bullet K_m \subseteq K_m$
  - unbounded: $\forall u \in \mathcal{U},\ K_u = \{\epsilon\}$
- for $[\![\cdot]\!] \subseteq M$ defined on logical variable, we extend

$$[\![A \multimap B]\!] := [\![A]\!] \multimap\!\!\bullet\, [\![B]\!] \qquad [\![!^m A]\!] := [\![A]\!] \cap K_m$$

$$[\![A_1, \dots, A_n]\!] := [\![A_1]\!] \bullet \cdots \bullet [\![A_n]\!]$$

Theorem (Soundness)

If $\Gamma \vdash A$ has a proof in IMSELL_Λ then $[\![\Gamma]\!] \subseteq [\![A]\!]$

Completeness of the reduction from $\mathrm{MM_{nd}}$

- Assume $!^\infty\overline{\Sigma}, x\overline{\alpha}, y\overline{\beta} \vdash \overline{p}$ is provable in IMSELL_3
- We use a trivial phase interpretation in $(\mathbb{N}^2, +, [0;0])$

$$K_m\,[x;y] := (a \preccurlyeq m \to y = 0) \wedge (b \preccurlyeq m \to x = 0) \wedge (m \in \mathcal{U} \to x = y = 0)$$

- hence: $K_a = \mathbb{N} \times \{0\}$, $K_b = \{0\} \times \mathbb{N}$, and $K_\infty = \big\{[0;0]\big\}$
- we interpret variables as:

$$[\![\alpha_0]\!] := \big\{[1;0]\big\} \quad [\![\beta_0]\!] := \big\{[0;1]\big\} \quad [\![\overline{p}]\!] = \big\{[x;y] \mid \Sigma \mathbin{/\!\!/_{\mathrm{n}}} x \oplus y \vdash p\big\}$$

- remember: $[\![\overline{\alpha}]\!] = [\![!^a\alpha_0]\!] = [\![\alpha_0]\!] \cap K_a = \big\{[1;0]\big\}$
- we check: $[0;0] \in [\![!^\infty\overline{\Sigma}]\!]$ and $[x;y] \in [\![x\overline{\alpha}, y\overline{\beta}]\!]$
- by soundness, from $\overline{\Sigma}, x\overline{\alpha}, y\overline{\beta} \vdash \overline{p}$ we deduce $[x;y] \in [\![\overline{p}]\!]$

Theorem (Completeness)

If $!^\infty\overline{\Sigma}, x\overline{\alpha}, y\overline{\beta} \vdash \overline{p}$ is provable in IMSELL_3 then $\Sigma \mathbin{/\!\!/_{\mathrm{n}}} x \oplus y \vdash p$ is derivable in $\mathrm{MM_{nd}}$

Undecidability for IMSELL_Λ and IMSELL_3

- Assume either $\Lambda = \Lambda_3$ or Λ_3 embeds into Λ
- We get a many-one reduction $\mathrm{MM}_{\mathrm{nd}} \preceq \mathsf{IMSELL}_\Lambda$:

$$\Sigma \mathbin{/\!\!/_{\mathrm{n}}} x \oplus y \vdash p \in \mathrm{MM}_{\mathrm{nd}} \quad \text{iff} \quad !^{\infty}\overline{\Sigma}, x\overline{\alpha}, y\overline{\beta} \vdash \overline{p} \in \mathsf{IMSELL}_\Lambda$$

Corollary (Undecidability)

If Λ_3 embeds into Λ then $\mathrm{MM}_{\mathrm{nd}}$ many-one reduces to IMSELL_Λ. In particular, provability in IMSELL$_3$ is undecidable

From FRACTRAN$_{\mathrm{reg}}$ to MMA0$_2$

The FRACTRAN language

Example (FRACTRAN program: list of (regular) fractions)

$$\left[\frac{455}{33}; \frac{11}{13}; \frac{1}{11}; \frac{3}{7}; \frac{11}{2}; \frac{1}{3}\right]$$

- Designed by J.H. Conway 1987
- Program: list of $\mathbb{N} \times \mathbb{N}^*$; State: a single $x \in \mathbb{N}$
- Step relation is simple to describe
  - pick the $\boxed{\text{first}}$ p/q s.t. $x \cdot p/q \in \mathbb{N}$, and this is the new state
  - inductively, characterized by two rules:

$$\frac{qy = px}{p/q :: Q \;/\!/_{\mathrm{F}}\, x \succ y} \qquad \frac{q \nmid px \qquad Q \;/\!/_{\mathrm{F}}\, x \succ y}{p/q :: Q \;/\!/_{\mathrm{F}}\, x \succ y}$$

The FRACTRAN$_{\mathrm{reg}}$ seed

- Here we only consider regular fractions, i.e. no $p/0$
- Termination: $Q /\!\!/_{\mathrm{F}}\, x\downarrow := \exists y,\ Q /\!\!/_{\mathrm{F}}\, x \succ^* y \wedge \forall z, \neg(Q /\!\!/_{\mathrm{F}}\, y \succ z)$
- Decision problem: $\boxed{\mathrm{FRACTRAN}_{\mathrm{reg}}(Q, x) := Q /\!\!/_{\mathrm{F}}\, x\downarrow}$
- Via a Gödel coding of many counters Minsky machines (Conway)
  - reduction from Minsky machines Halting to FRACTRAN$_{\mathrm{reg}}$

Theorem (mechanized by DLW&Forster, FSCD2019)

There is a many-one reduction from the Halting problem for single tape Turing machines to termination of regular FRACTRAN programs, i.e. Halt $\preceq$ FRACTRAN$_{\mathrm{reg}}$, *and thus* FRACTRAN$_{\mathrm{reg}}$ *is undecidable.*

- FRACTRAN$_{\mathrm{reg}}$ as a seed of undecidability

Programming with $\mathrm{MM}_{\mathrm{nd}}$ vs. (classic) Minsky machines

- Minsky machines:
  - low-level model of computation
  - hundreds of instructions
  - correctness proofs require modular reasonning
- Modular reasonning:
  - programs inherit properties of sub-programs
- $\mathrm{MM}_{\mathrm{nd}}$, i.e. sequent style Minsky machines
  - great as a seed, especially for Linear logic
  - cumbersome as a target
- the issue is modular reasonning
  - merging $\mathrm{MM}_{\mathrm{nd}}$ programs lead namespace/labels conflicts
  - very bad for modular reasonning
- we use another (classic) representation
  - with a program counter PC
  - one sequence of contiguous instructions
  - concatenation avoid namespace conflicts

Minsky Machines ($\mathbb{N}$ valued register machines)

Example (transfers s to d in 3 instructions, with $s \neq d$)

$$\texttt{TRANSFER}_\mathrm{a}\, s\, d\, q := \;\; q : \texttt{INC}_\mathrm{a}\, d \quad q+1 : \texttt{DEC}_\mathrm{a}\, s\, q \quad q+2 : \texttt{DEC}_\mathrm{a}\, d\,(3+q)$$

- programs: $(q, [\iota_0; \ldots; \iota_k]) \;\leftrightsquigarrow\; q : \iota_0;\; \ldots \;;\; q+k : \iota_k$
- n registers of value in $\mathbb{N}$ for a fixed n
- state: $(\mathrm{PC}, \vec{v}) \in \mathbb{N} \times \mathbb{N}^n$
- instructions: $\quad \iota ::= \texttt{INC}_\mathrm{a}\, x \mid \texttt{DEC}_\mathrm{a}\, x\, j$
- Step semantics for $\texttt{INC}_\mathrm{a}\, x$ and $\texttt{DEC}_\mathrm{a}\, x\, j$ (pseudo code)

$$\begin{array}{ll} \texttt{INC}_\mathrm{a}\, x : & x \leftarrow x+1;\ \mathrm{PC} \leftarrow \mathrm{PC}+1 \\ \texttt{DEC}_\mathrm{a}\, x\, j : & \text{if } x = 0 \text{ then } \mathrm{PC} \leftarrow \mathrm{PC}+1 \\ & \text{if } x > 0 \text{ then } x \leftarrow x-1;\ \mathrm{PC} \leftarrow j \end{array}$$

- $(q, \texttt{TRANSFER}_\mathrm{a}\, s\, d\, q) \,/\!\!/_\mathrm{a}\, (q, \vec{v}) \succ^+ (3+q, \vec{v}\{0/s\}\{(\vec{v}_s + \vec{v}_d))/d\}$

Minsky machines semantics and termination

$$\frac{}{(i,P) /\!\!/_{\mathrm{a}}\, st \succ^0 st} \qquad \frac{i_1 = |L| + i \qquad P = L +\!\!+ \sigma :: R \qquad \sigma /\!\!/_{\mathrm{a}} (i_1, \vec{v}_1) \succ st_2 \qquad (i,P) /\!\!/_{\mathrm{a}}\, st_2 \succ^k st_3}{(i,P) /\!\!/_{\mathrm{a}} (i_1, \vec{v}_1) \succ^{1+k} st_3}$$

$$\begin{array}{rcll}
(i,P) /\!\!/_{\mathrm{a}}\, st_1 \succ^* st_2 & := & \exists k, (i,P) /\!\!/_{\mathrm{a}}\, st_1 \succ^k st_2 & \text{(computation)} \\
(i,P) /\!\!/_{\mathrm{a}}\, st_1 \succ^+ st_2 & := & \exists k > 0, (i,P) /\!\!/_{\mathrm{a}}\, st_1 \succ^k st_2 & \text{(progress)} \\
(i,P) /\!\!/_{\mathrm{a}}\, st_1 \leadsto (i_2, \vec{v}_2) & := & (i,P) /\!\!/_{\mathrm{a}}\, st_1 \succ^* (i_2, \vec{v}_2) \land \texttt{out}\ i_2\ (i,P) & \text{(output)} \\
(i,P) /\!\!/_{\mathrm{a}}\, st_1 \downarrow & := & \exists st_2, (i,P) /\!\!/_{\mathrm{a}}\, st_1 \leadsto st_2 & \text{(termination)}
\end{array}$$

Definition (Termination)

For MMA_n & $\mathrm{MMA0}_n$, instances are pairs $(P, \vec{v})$: P list of MMA_n instructions (starting at 1) and $\vec{v} : \mathbb{N}^n$ is the initial content of registers.

$$\begin{array}{lll}
\mathrm{MMA}_n & \text{(termination)} & (1,P) /\!\!/_{\mathrm{a}} (1, \vec{v}) \downarrow \\
\mathrm{MMA0}_n & \text{(term. on zero)} & (1,P) /\!\!/_{\mathrm{a}} (1, \vec{v}) \leadsto (0, [0; \ldots ; 0])
\end{array}$$

A FRACTRAN compiler using only two counters

- a critical brick in the construction with $s := 0$, $d := 1$
- tries fraction p/q on the contents of s, assuming d is void

$$(i_0, \texttt{FRAC\_ONE}_{\mathrm{a}}\, p\, q\, i_0\, j) \;:=\; \left[\begin{array}{ll} i_0\colon & \texttt{MULT\_CST}_{\mathrm{a}}\, s\, d\, p\, i_0; \\ i_1\colon & \texttt{MOD\_CST}_{\mathrm{a}}\, d\, s\, i_2\, i_5\, q\, i_1; \\ i_2\colon & \texttt{DIV\_CST}_{\mathrm{a}}\, s\, d\, q\, i_2; \\ i_3\colon & \texttt{TRANSFER}_{\mathrm{a}}\, d\, s\, i_3; \\ i_4\colon & \texttt{JUMP}_{\mathrm{a}}\, j\, d; \\ i_5\colon & \texttt{DIV\_CST}_{\mathrm{a}}\, s\, d\, p\, i_5; \\ i_6\colon & \texttt{TRANSFER}_{\mathrm{a}}\, d\, s\, i_6 \\ i_7\colon & \end{array}\right]$$

Lemma

If $qy = px$ then $(i_0, \texttt{FRAC\_ONE}_{\mathrm{a}}\, p\, q\, i_0\, j) /\!\!/_{\mathrm{a}} (i_0, [x; 0]) \succ^+ (j, [y; 0])$.
If $q \nmid px$ then $(i_0, \texttt{FRAC\_ONE}_{\mathrm{a}}\, p\, q\, i_0\, j) /\!\!/_{\mathrm{a}} (i_0, [x; 0]) \succ^+ (i_7, [x; 0])$.

- Then we chain those for the program $[p_1/q_1; \ldots; p_n/q_n]$, and loop

Reduction from FRACTRAN to $\mathsf{MMA}_2/\mathsf{MMA0}_2$

Theorem

For any regular FRACTRAN program $Q : \mathbb{L}(\mathbb{N} \times \mathbb{N}^*)$, *one can compute a* MMA_2 *program* $\texttt{FRAC\_MMA}_{\mathrm{a}}\, Q$ *such that for any* $x : \mathbb{N}$, *the three following properties are equivalent:*

1. $Q \mathbin{/\!\!/}_{\mathrm{F}} x \downarrow$;
2. $(1, \texttt{FRAC\_MMA}_{\mathrm{a}}\, Q) \mathbin{/\!\!/}_{\mathrm{a}} (1, [x; 0]) \rightsquigarrow (0, [0; 0])$;
3. $(1, \texttt{FRAC\_MMA}_{\mathrm{a}}\, Q) \mathbin{/\!\!/}_{\mathrm{a}} (1, [x; 0]) \downarrow$.

Corollary (Undecidability)

$\mathsf{FRACTRAN}_{\mathrm{reg}} \preceq \mathsf{MMA}_2$ *and* $\mathsf{FRACTRAN}_{\mathrm{reg}} \preceq \mathsf{MMA0}_2$ *hence* MMA_2 *and* $\mathsf{MMA0}_2$ *are both undecidable.*

Minsky machine termination as provability

Reduction from $\mathsf{MMA0}_2$ to $\mathrm{MM}_{\mathrm{nd}}$

- a quite straightforward translation

$$\overline{(\cdot)} : \mathbb{F}_2 \to \{\alpha, \beta\} \qquad \overline{0} := \alpha \quad \overline{1} := \beta$$

$$\begin{aligned}\langle i, \mathtt{INC}_{\mathrm{a}}\, x\rangle &:= [\mathtt{INC}_{\mathrm{n}}\, \overline{x}\, i\, (1{+}i)] \\ \langle i, \mathtt{DEC}_{\mathrm{a}}\, x\, j\rangle &:= [\mathtt{DEC}_{\mathrm{n}}\, \overline{x}\, i\, j; \mathtt{ZERO}_{\mathrm{n}}\, \overline{x}\, i\, (1{+}i)]\end{aligned}$$

$$\begin{aligned}\langle\!\langle i, [\,]\rangle\!\rangle &:= [\,] \\ \langle\!\langle i, \sigma :: P\rangle\!\rangle &:= \langle i, \sigma\rangle \mathbin{+\!\!+} \langle\!\langle 1{+}i, P\rangle\!\rangle\end{aligned}$$

Lemma (reduction)

With $\Sigma_P := \mathtt{STOP}_{\mathrm{n}}\, 0 :: \langle\!\langle 1, P\rangle\!\rangle$ *we have* $(1, P) \mathbin{/\!\!/_{\mathrm{a}}} (i, [x, y]) \succ^* (0, [0; 0])$ *iff* $\Sigma_P \mathbin{/\!\!/_{\mathrm{n}}} x \oplus y \vdash i$ *is derivable in* $\mathrm{MM}_{\mathrm{nd}}$.

Corollary

$\mathsf{MMA0}_2 \preceq \mathrm{MM}_{\mathrm{nd}}$ *hence* $\mathrm{MM}_{\mathrm{nd}}$ *is undecidable.*

Conclusion

Contributions and Perspectives

- Undecidability of IMSELL_3, a simpler proof:
  - via a proof-theoretic presentation of Minsky machines
  - that compares well with that of ILL
  - outlines the role played by the promotion rule
  - a short semantic proof for the completeness of the reduction
- Mechanisation in the Coq library of undecidability:
  - Two counters Minsky machines seed (from FRACTRAN)
  - Undecidability for IMSELL_Λ and IMSELL_3
  - Code available (+1200,+600 loc), included in the library

`https://github.com/uds-psl/coq-library-undecidability/releases/tag/FSCD-2021`

- Perspectives
  - (General) phase sem. for $\mathsf{IMSELL}_\Lambda \rightsquigarrow$ cut-elimination for IMSELL_Λ
  - If doable, implement Ackermann hardness for Petri nets/VASS
  - Insights for MELL, zero test at the end of computation?