Solving Bit-Vector Equations

Concepts for Fixed and Non-Fixed Length

M. Oliver Möller* and Harald Rueß**

* BRICS

BRICS PhD School
University of Aarhus
DK - 8000 Århus C, Denmark

** SRI International

SRI International
Computer Science Laboratory
Menlo Park, CA, 94025, USA

Abstract of this Talk

1. How Difficult is "Solving" in the Theory of Bit-Vectors?
2. Equational Transformation Systems
3. Solving Fixed-Sized Equations - a Paradigm
4. Extension of this Paradigm to Variable Length

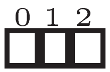
Bit-Vectors

The Core Theory

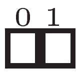
- $x_{[n]}$ denotes a bit-vector with n bits. $x_{[n]} : bvec_n$, n a fixed constant.
- The bits are numered from left to right, starting with 0.
- Constants are $\mathbf{0}_{[n]}$ and $\mathbf{1}_{[n]}$.
- Concatenation:

$x_{[3]}$ $\quad y_{[3]}$ $\quad x_{[3]} \otimes y_{[3]}$

- Extraction:



$[0 : 1] \rightarrow$



$x_{[3]}$ $\quad x_{[3]}[0 : 1]$

Extensions

- Boolean operations

$$x_{[3]} \wedge y_{[3]}$$

- Arithmetic (modulo 2^n)

$$x_{[3]} \ +_{[3]} \ y_{[3]}$$

- Variable length

$$x_{[n]} \quad : \quad bvec_n$$
$$n \quad : \quad I\!N$$

- Variable Extraction

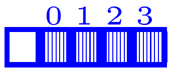
$$x_{[3]}[\text{i:j}] \quad : \quad bvec_{j-i+1}$$
$$i, j \quad : \quad I\!N$$

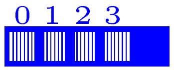
Solving Bit-Vector Equations

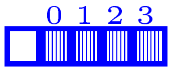
$x_{[4]} : bvec_4, \quad y_{[2]} : bvec_2$

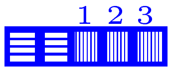
- valid: $x_{[4]}[0:2] \otimes x_{[4]}[3:3] = x_{[4]}$

  $\rightsquigarrow \; x_{[4]} = x_{[4]}$

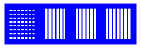
- unsatisfiable: $\mathbf{0}_{[1]} \otimes x_{[4]} =$ 

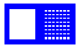
  $x_{[4]} \otimes \mathbf{1}_{[1]}$ 

- or neither: $\mathbf{0}_{[1]} \otimes x_{[4]} =$ 

  $y_{[2]} \otimes x_{[4]}[1:3]$ 

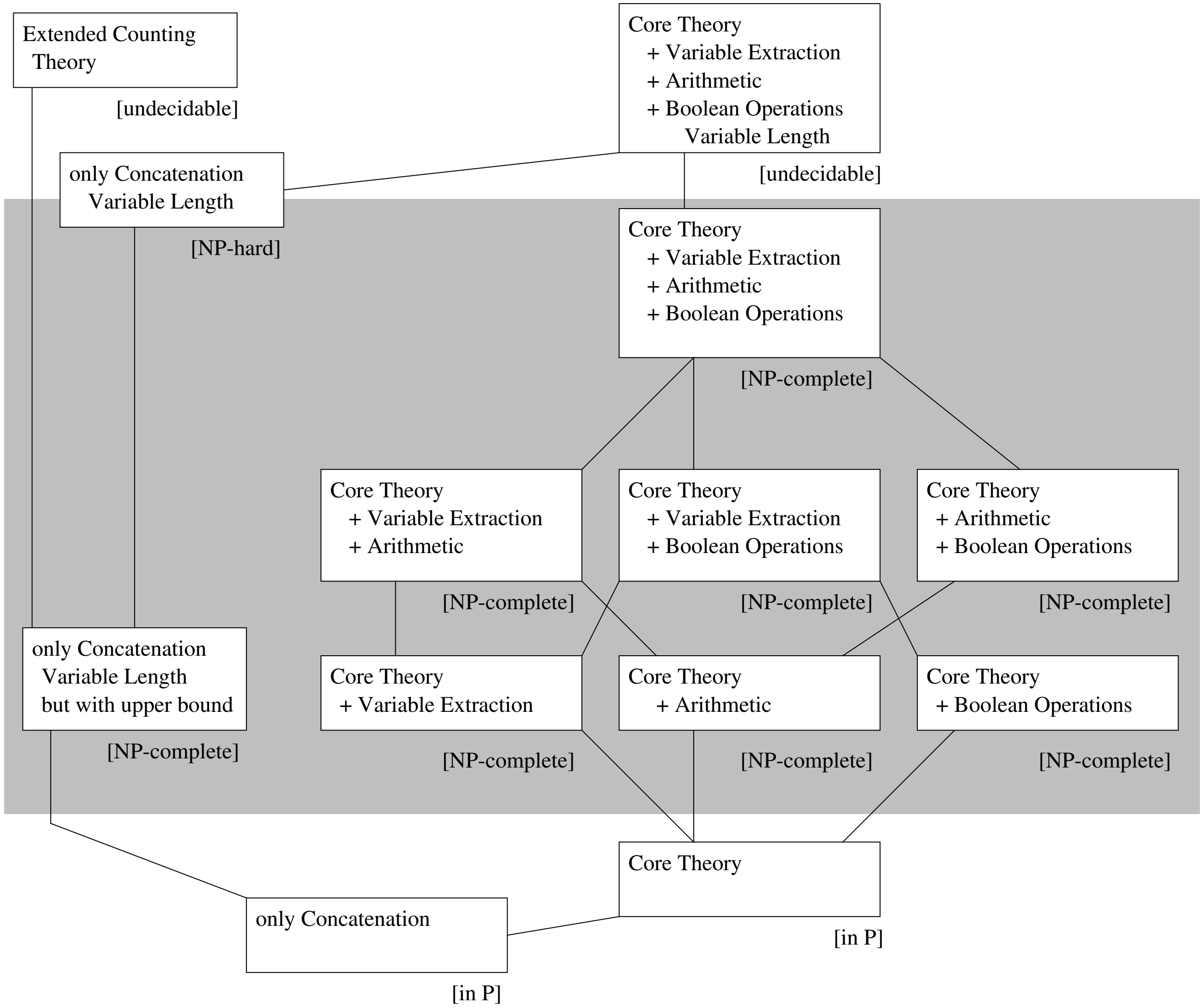
  $\rightsquigarrow$

  $x_{[4]} = a_{[1]} \otimes b_{[3]}$ x = 

  $y_{[4]} = \mathbf{0}_{[1]} a_{[1]}$ y = 

  $\Rightarrow$ $\left.\begin{array}{l}\text{complete}\\ \text{explicit}\end{array}\right\}$ set of witnesses

A View on Complexity



Equational Transformation Systems

- Rules:

$$R \equiv \quad \underbrace{\{\underline{p = q}\}, \quad cond(\underline{p}, \underline{q})}_{lhs(R)} \quad \rightarrowtail \quad \underbrace{\{\underline{l = r}\}}_{rhs(R)}$$

- Set of equations:

$$\Upsilon \equiv \{\underline{t = s}\}$$

- Matching (M, τ, R):

$$M \subseteq \Upsilon$$

$$\tau(M) \doteq lhs(R) \ \wedge \ cond(M)$$

- Application of rule R:

$$\Upsilon \leftarrow \Big(\Upsilon \setminus \tau\big(lhs(R)\big) \ \cup \ \tau\big(rhs(R)\big)\Big)$$

Solving by Bitwise Splitting

$$(1) \quad t_{[n]} = u_{[n]},\ 1 < n \rightarrowtail \left\{ \begin{array}{l} t[0:0] = u[0:0] \\ t[1:n-1] = u[1:n-1] \end{array} \right\}$$

. . . .

$$(2) \quad c_{[n]} = c'_{[n]},\ c \neq c' \rightarrowtail \textbf{FAIL}$$

$$(3) \quad t = t \rightarrowtail \{\}$$

$$(4) \quad \left\{ \begin{array}{c} p = q \\ q = r \end{array} \right\} \rightarrowtail \left\{ \begin{array}{c} p = r \\ q = r \end{array} \right\}$$

$$(5) \quad \left\{ \begin{array}{c} p = q \\ q = p \end{array} \right\} \rightarrowtail \{\ p = q\ \}$$

$$(6) \quad \left\{ \begin{array}{c} p = t \\ p = u \end{array} \right\} \rightarrowtail \left\{ \begin{array}{c} p = t \\ u = t \end{array} \right\}$$

$$(7) \quad c = t,\quad t \neq c \rightarrowtail \{\ t = c\ \}$$

Example

$x : bvec_{2n}, \qquad y, z : bvec_n$

Start: $\{\ x[0:n\text{-}1] \otimes y = y \otimes z\ \}$

$$\overset{(1)^n}{\rightarrowtail} \left\{ \begin{array}{rcl} x[0:0] & = & y[0:0] \\ & \vdots & \\ x[n\text{-}1:n\text{-}1] & = & y[n\text{-}1:n\text{-}1] \\ y & = & z \end{array} \right\} \overset{(1)^n}{\rightarrowtail} \left\{ \begin{array}{rcl} x[0:0] & = & y[0:0] \\ & \vdots & \\ x[n\text{-}1:n\text{-}1] & = & y[n\text{-}1:n\text{-}1] \\ y[0:0] & = & z[0:0] \\ & \vdots & \\ y[n\text{-}1:n\text{-}1] & = & z[n\text{-}1:n\text{-}1] \end{array} \right\}$$

$$\overset{(5)^n}{\rightarrowtail} \left\{ \begin{array}{rcl} x[0:0] & = & z[0:0] \\ & \vdots & \\ x[n\text{-}1:n\text{-}1] & = & z[n\text{-}1:n\text{-}1] \\ y[0:0] & = & z[0:0] \\ & \vdots & \\ y[n\text{-}1:n\text{-}1] & = & z[n\text{-}1:n\text{-}1] \end{array} \right\}$$

$\Rightarrow$ Total: $3n$ steps.

Basic Idea

A *chunk* is a term of the form

$$
\begin{array}{ll}
 & c_{[n]} \\
\text{or} & x_{[n]} \\
\text{or} & x_{[n]}[i:j].
\end{array}
$$

Paradigm: $\boxed{\text{Treat only chunks with maximal size as distinct objects.}}$

Advantages:

+ Speedup.

+ Facilitates the extension of the theory to variable length.

Where to Split ?

This can be computed (1) in advance

or (2) incrementally.

Preferable: (2).

Problem:

The information where to split has to be stored somewhere.

Solution:

Store it inside the set of equations.

Example: $t = u \quad \equiv \quad x_{[16]}[0:7] \otimes y_{[8]} = y_{[8]} \otimes z_{[8]}$

$$\Rightarrow \quad \mathcal{SE}(t = u) \quad \equiv \quad \{\ x_{[16]} = x_{[16]}[0:7] \otimes x_{[16]}[8:15]\ \}$$

Split Rules of the Equational Transformation System $\mathcal{C}_{\Re}$

$$(1) \qquad p_{[n]} \otimes t = q_{[n]} \otimes u \quad \rightarrowtail \left\{ \begin{array}{l} p = q \\ t = u \end{array} \right\}$$

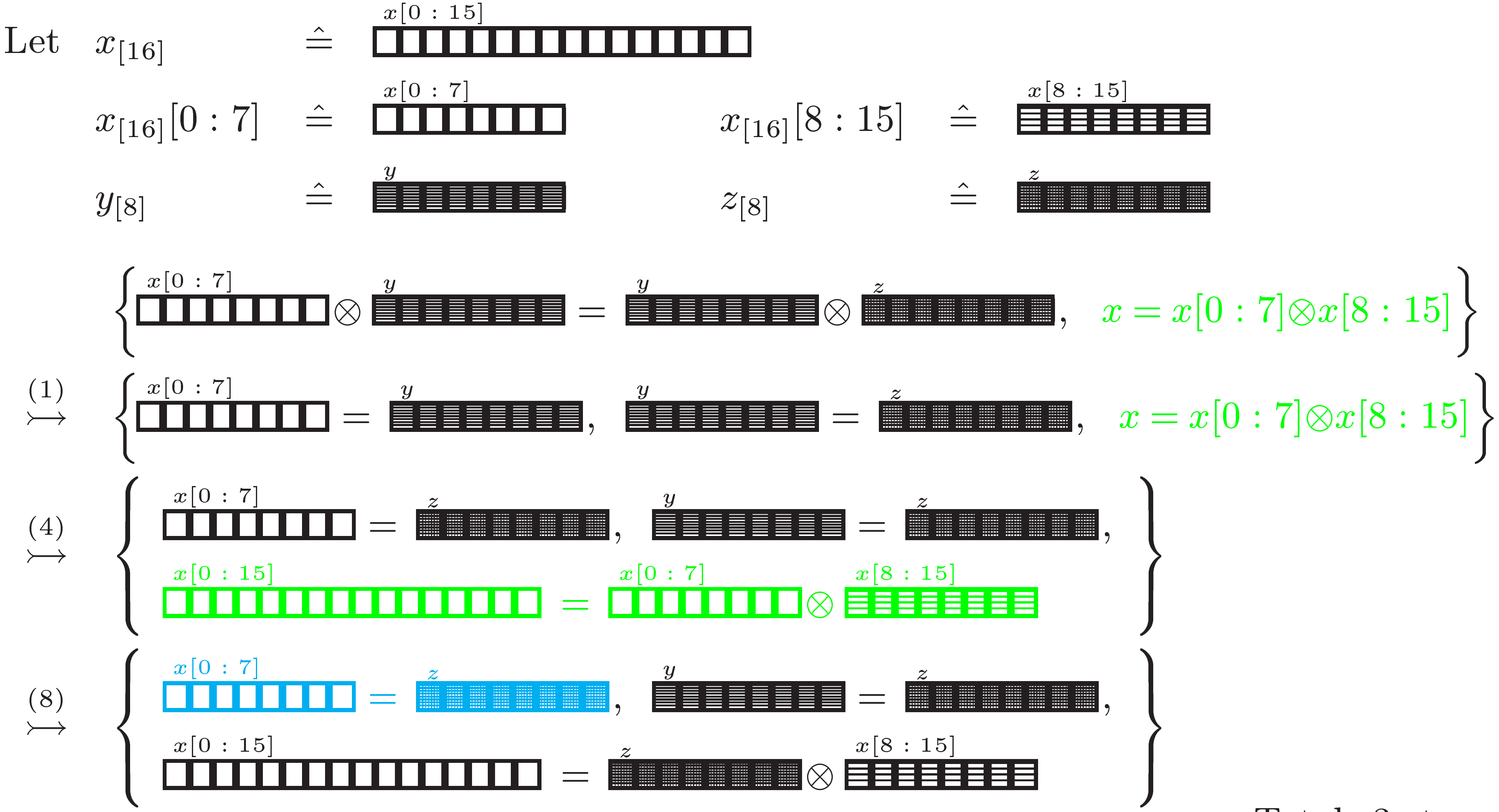
$$(1') \qquad p_{[n]} \otimes t = q_{[m]} \otimes u, \; n < m \quad \rightarrowtail \left\{ \begin{array}{l} p = q[0:n\text{-}1] \\ q[n:m\text{-}1] \otimes u = t \\ q = q[0:n\text{-}1] \otimes q[n:m\text{-}1] \end{array} \right\}$$

$$(1'') \qquad p_{[n]} \otimes t = q_{[m]} \quad \rightarrowtail \left\{ \begin{array}{l} p = q[0:n\text{-}1] \\ q[n:m\text{-}1] = t \\ q = q[0:n\text{-}1] \otimes q[n:m\text{-}1] \end{array} \right\}$$

Non-Split Rules of the Equational Transformation System $\mathcal{C}_{\Re}$

(2)	$c_{[n]} = c'_{[n]}$,	$c \neq c'$	$\rightarrowtail$	**FAIL**
(3)	$t = t$		$\rightarrowtail$	$\{\}$
(4)	$\left\{ \begin{array}{c} p = q \\ q = r \end{array} \right\}$		$\rightarrowtail$	$\left\{ \begin{array}{c} p = r \\ q = r \end{array} \right\}$
(5)	$\left\{ \begin{array}{c} p = q \\ q = p \end{array} \right\}$		$\rightarrowtail$	$\{\ p = q\ \}$
(6)	$\left\{ \begin{array}{c} p = t \\ p = u \end{array} \right\}$		$\rightarrowtail$	$\left\{ \begin{array}{c} p = t \\ u = t \end{array} \right\}$
(7)	$c = t,$	$t \neq const$	$\rightarrowtail$	$\{\ t = c\ \}$
(8)	$\left\{ \begin{array}{c} p = t \\ q = u \end{array} \right\}$,	$q \preceq t$	$\rightarrowtail$	$\left\{ \begin{array}{l} p = t[q/u] \\ q = u \end{array} \right\}$
(9)	$p_{[n]} = q_{[m]} \otimes t,$	$p_{[n]} \dot{\neq} \sigma(q_{[m]} \otimes t)$	$\rightarrowtail$	$\{\ q_{[m]} \otimes t = p_{[n]}\ \}$

Solving the Equation $x_{[16]}[0:7] \otimes y_{[8]} = y_{[8]} \otimes z_{[8]}$ via $\mathcal{C}_{\Re}$



$\Rightarrow$ Total: 3 steps.

Bit-Vectors with Variable Length

Example:

$$x_{[n]} \otimes \mathbf{0}_{[1]} \otimes y_{[m]} \;=\; z_{[2]} \otimes \mathbf{1}_{[1]} \otimes w_{[2]}$$

Two solutions:

$$\begin{array}{llrcl}
(i) & n=1,\ m=3, & y_{[3]} & = & \mathbf{1}_{[1]} \otimes w_{[2]}, \\
 & & z_{[2]} & = & x_{[1]} \otimes \mathbf{1}_{[1]} \\
(ii) & n=3,\ m=1, & x_{[3]} & = & z_{[2]} \otimes \mathbf{1}_{[1]}, \\
 & & w_{[2]} & = & \mathbf{0}_{[1]} \otimes y_{[1]}
\end{array}$$

$\Rightarrow$
- A solution in general is a *disjunction* of conjunctions.
- Some reasoning about integers is necessary.

Frames

A *frame* is a pair (Υ, Ψ), where

- $\Upsilon \;\equiv\; \{s = t,\; s' = t', \ldots\}$ is a set of equations.
- Ψ is a set of integer constraints of the form

  $n < m$

  $n = m$

  $n \mid m$ (divisibility)

  or $n \not\mid m$ (non-divisibility).

A *frame transformation system* operates on a set of frames

$$\Xi \;\equiv\; \big\{(\Upsilon_1, \Psi_1),\; (\Upsilon_2, \Psi_2), \ldots\big\}.$$

Ξ is called *disjoint*, if for each (Υ_i, Ψ_i), $(\Upsilon_j, \Psi_j) \in \Xi$, $i \neq j$: $\quad \Psi_i \wedge \Psi_j \;\models\; \bot$.

This is decidable.

Equational Transformation Systems

- Rules:

$$R \;\equiv\; \{\underline{p = q}\} \;,\; cond\;(\underline{p}, \underline{q}) \;\rightarrowtail\; \{\underline{l' = r'}\}$$

- Set of equations:

$$\Upsilon \;\equiv\; \{\underline{t \;\; = s \;\;}\}$$

- Matching (M, τ, R):

$$M \subseteq \Upsilon$$

$$\tau(M) \doteq lhs(R) \;\wedge\; cond(M \quad)$$

- Application of rule R:

$$\Upsilon \;\leftarrow\; \Big(\Upsilon \setminus \tau\big(lhs(R)\big) \quad \cup \quad \tau\big(rhs(R)\big)\Big)$$

Frame

$$(\quad , \Psi) \qquad (\quad , \Psi) \qquad \left\{ \begin{array}{l} (\quad , \Psi'), \\ (\{\underline{l'' = r''}\}, \Psi''), \ldots \end{array} \right\}$$

frames:

$$\Xi \qquad \{(\quad _1 \quad _1 , \Psi_1), \ (\underline{s_2 = t_2}, \Psi_2), \ldots \}$$

$$_{\hat{i}} \text{ for } (\Upsilon_{\hat{i}}, \Psi_{\hat{i}}) \in \Xi$$

$$, \Psi$$

$$\Xi \quad \leftarrow \quad \Big(\Xi \setminus \{(\Upsilon_{\hat{i}}, \Psi_{\hat{i}})\}\Big) \quad \cup \quad \tau\Big(\{(\Upsilon', \Psi'), \ (\Upsilon'', \Psi''), \ldots\}\Big)$$

The Context Split Rule (1) of $\mathcal{S}_{\Re}$

$$
(1) \quad \left(\{p_{[n]} \otimes t = q_{[m]} \otimes u\} \cup E,\ \Psi\right) \quad \rightarrowtail \quad
\left[
\begin{array}{l}
\left(
\begin{array}{l}
\left\{
\begin{array}{l}
p_{[n]} = q_{[m]}[0 : n-1], \\
q_{[m]}[n : m-1] \otimes u = t, \\
q_{[m]} = q_{[m]}[0 : n-1] \otimes q_{[m]}[n : m-1]
\end{array}
\right\} \cup E, \\
\{n < m\} \cup \Psi
\end{array}
\right) \\
\left(
\begin{array}{l}
\left\{
\begin{array}{l}
p_{[n]} = q_{[m]}, \\
t = u
\end{array}
\right\} \cup E, \\
\{n = m\} \cup \Psi
\end{array}
\right) \\
\left(
\begin{array}{l}
\left\{
\begin{array}{l}
q_{[m]} = p_{[n]}[0 : m-1], \\
p_{[n]}[m : n-1] \otimes t = u, \\
p_{[n]} = p_{[n]}[0 : m-1] \otimes p_{[n]}[m : n-1]
\end{array}
\right\} \cup E, \\
\{n > m\} \cup \Psi
\end{array}
\right)
\end{array}
\right]
$$

The Same-Variable Rule $(1)^*$ of $\mathcal{S}_{\Re}$

$$(1)^* \qquad \Big(\{x_{[n]}[i:j] = x_{[n]}[k:l]\} \cup E, \Psi\Big) \qquad \rightarrowtail \qquad \left[\begin{array}{l} \left(\begin{array}{l} \left\{x_{[n]}[i:l] = {a_{[k-i]}}^{\frac{l-i+1}{k-i}}\right\} \cup E, \\ \{(l-i+1) \mid (k-i)\} \cup \Psi \end{array}\right) \\ \left(\begin{array}{l} \left\{x_{[n]}[i:l] = a_{[h]} \otimes (b_{[h']} \otimes a_{[h]})^{\frac{l-i-h+1}{k-i}}\right\} \cup E, \\ \{(l-i+1) \nmid (k-i)\} \cup \Psi \end{array}\right) \\ \\ \text{where} \quad \begin{array}{l} h = (l-i+1)\mathrm{MOD}(k-i), \\ h' = k-i-h, \\ a,\ b \text{ fresh variables.} \end{array} \end{array}\right]$$

where $i < k$

Simple Rules of $\mathcal{S}_{\Re}$

$$(1'') \quad \left(\{p_{[n]} \otimes t = q_{[m]}\} \cup E,\ \Psi\right) \quad \rightarrowtail \quad \left(\left\{\begin{array}{l} p_{[n]} = q_{[m]}[0:n\text{-}1], \\ q_{[m]}[n:m\text{-}1] = t, \\ q_{[m]} = q_{[m]}[0:n\text{-}1] \otimes q_{[m]}[n:m\text{-}1] \end{array}\right\} \cup E,\ \Psi\right)$$

. . . .

$$(2) \quad \left(\{c_{[n]} = d_{[n]}\} \cup E,\ \Psi\right), \quad c \mathrel{\dot{\neq}} d \quad \rightarrowtail \quad \textbf{FAIL}$$

$$(3) \quad (\{t = t\} \cup E,\ \Psi) \quad \rightarrowtail \quad (E,\ \Psi)$$

$$(4) \quad \left(\left\{\begin{array}{l} p = q \\ q = r \end{array}\right\} \cup E,\ \Psi\right), \quad a \text{ fresh} \quad \rightarrowtail \quad \left(\left\{\begin{array}{l} p = a \\ q = a \\ r = a \end{array}\right\} \cup E,\ \Psi\right)$$

$$(5) \quad \left(\left\{\begin{array}{l} p = q \\ q = p \end{array}\right\} \cup E,\ \Psi\right), \quad a \text{ fresh} \quad \rightarrowtail \quad \left(\left\{\begin{array}{l} p = a \\ q = a \end{array}\right\} \cup E,\ \Psi\right)$$

$$(6) \quad \left(\left\{\begin{array}{l} p = t \\ p = u \end{array}\right\} \cup E,\ \Psi\right) \quad \rightarrowtail \quad \left(\left\{\begin{array}{l} p = t \\ u = t \end{array}\right\} \cup E,\ \Psi\right)$$

$$(7) \quad (\{c = t\} \cup E,\ \Psi), \quad t \notin \mathcal{C} \quad \rightarrowtail \quad (\{t = c\} \cup E,\ \Psi)$$

$$(8) \quad \left(\left\{\begin{array}{l} p = t \\ q = u \end{array}\right\} \cup E,\ \Psi\right), \quad q \preceq t \quad \rightarrowtail \quad \left(\left\{\begin{array}{l} p = t[q/u] \\ q = u \end{array}\right\} \cup E,\ \Psi\right)$$

$$(9) \quad (\{p = q \otimes t\} \cup E,\ \Psi), \quad p \mathrel{\dot{\neq}} \sigma(q \otimes t) \quad \rightarrowtail \quad (\{q \otimes t = p\} \cup E,\ \Psi)$$

$$(10) \quad (\Upsilon,\ \Psi), \quad \Psi \models \perp \quad \rightarrowtail \quad \textbf{FAIL}$$

The Frame Transformation System $\mathcal{S}_{\Re}$

- A straightforward extension of $\mathcal{C}_{\Re}$.
- $\mathcal{S}_{\Re}$ follows the paradigm of the largest chunks.
- Let $t = u$ be the original equation. Then $\mathcal{S}_{\Re}$ starts with

$$\Xi_0 \equiv (\{t = u\} \cup \mathcal{SE}(t = u),\ wf(t = u)),$$

where $wf(t = u)$ denote some well-formdness constraints.

An Example (1)

Consider

$$x_{[l]} \otimes \mathbf{1}_{[1]} \otimes \mathbf{0}_{[1]} = \mathbf{1}_{[1]} \otimes \mathbf{0}_{[1]} \otimes x_{[l]}.$$

Start:

$$\Xi_0 \equiv \left\{ (\{ x_{[l]} \otimes \mathbf{1}_{[1]} \otimes \mathbf{0}_{[1]} = \mathbf{1}_{[1]} \otimes \mathbf{0}_{[1]} \otimes x_{[l]} \}, \{1 \le l\}) \right\}.$$

$$\downarrow_{(1)}$$

$$\Xi_1 \equiv \left\{ \begin{array}{ll} (\{\ldots\}, & \{1 \le l, l < 1\}), \\ (\{x_{[l]} = \mathbf{1}_{[1]},\ \mathbf{1}_{[1]} \otimes \mathbf{0}_{[1]} = \mathbf{0}_{[1]} \otimes x_{[l]}\}, & \{1 \le l, l = 1\}), \\ (\{x_{[l]}[0:0] = \mathbf{1}_{[1]},\ x_{[l]}[1:l\text{-}1] \otimes \mathbf{1}_{[1]} \otimes \mathbf{0}_{[1]} = \mathbf{0}_{[1]} \otimes x_{[l]}\}, & \{1 \le l, l > 1\}) \end{array} \right\}.$$

First frame:	triggers rule (10) immediately.
Second frame:	triggers rule (2) after one more split step.
Third frame:	remains to process.

An Example (2)

$$\Xi_2 \equiv \{(\{x_{[l]}[0:0] = \mathbf{1}_{[1]},\ x_{[l]}[1:l\text{-}1] \otimes \mathbf{1}_{[1]} \otimes \mathbf{0}_{[1]} = \mathbf{0}_{[1]} \otimes x_{[l]}\}, \{l > 1\})\}.$$

$$\downarrow_{(1)}$$

$$\Xi_3 \equiv \left\{ \begin{array}{ll} (.., & \{l > 1, l < 2\}) \\ (\{..,\ x_{[l]}[1:1] = \mathbf{0}_{[1]},\ \mathbf{1}_{[1]} \otimes \mathbf{0}_{[1]} = x_{[l]}\}, & \{l > 1, l = 2\}) \\ (\{..,\ x_{[l]}[2:l\text{-}1] \otimes \mathbf{1}_{[1]} \otimes \mathbf{0}_{[1]} = x_{[l]}\}, & \{l > 1, l > 2\}) \end{array} \right\}$$

First frame: triggers rule (10) immediately.

Second frame: terminates with $(\{x_{[2]} = \mathbf{1}_{[1]} \otimes \mathbf{0}_{[1]}\},\ \{l = 2\})$.

Third frame: triggers $(1)^*$:

$$\Xi_4 \equiv \left\{ \begin{array}{ll} (\{.., x_{[l]} = (a_{[2]})^{\frac{l}{2}}\}, & \{l > 2, 2 \mid l\}) \\ (\{.., x_{[l]} = b_{[1]} \otimes (d_{[1]} \otimes b_{[1]})^{\frac{l-1}{2}}\}, & \{l > 2, 2 \not| \ l\}) \end{array} \right\}$$

An Example (3)

Note that both frames in Ξ_4 contain the equations

$$x_{[l]}[0:0] = \mathbf{1}_{[1]}, \qquad x_{[l]}[1:1] = \mathbf{0}_{[1]}$$

$\Rightarrow$ First frame:

$$(\{x_{[l]} = (\mathbf{1}_{[1]} \otimes \mathbf{0}_{[1]})^{\frac{l}{2}}\}, \{l > 2, 2 \mid l\}).$$

Second frame: yields a **FAIL**.

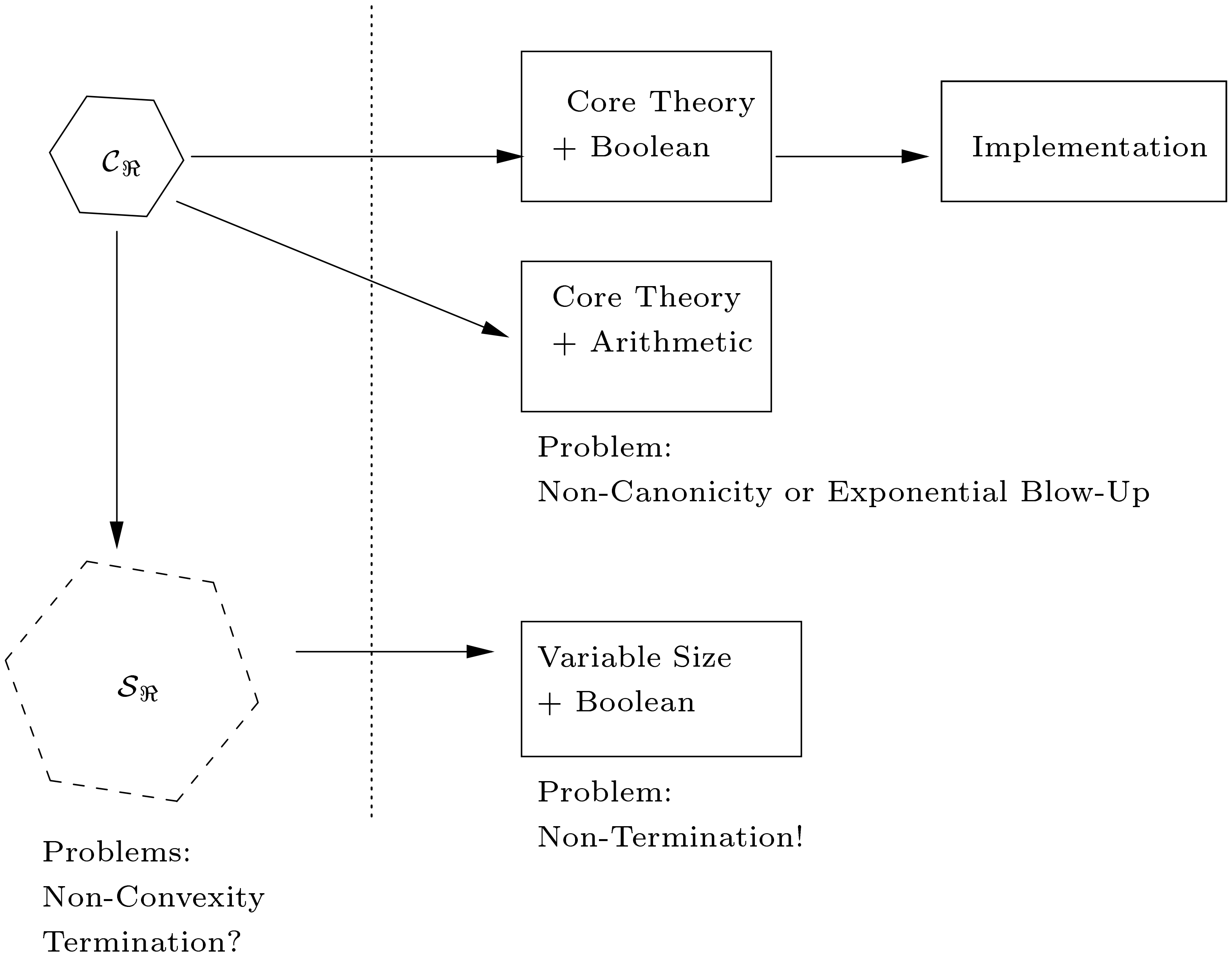
$\mathcal{S}_{\Re}$ terminates with

$$\Xi_5 \equiv \left\{ \begin{array}{ll} (\{x_{[2]} = \mathbf{1}_{[1]} \otimes \mathbf{0}_{[1]}\}, & \{l = 2\}) \\ (\{x_{[l]} = (\mathbf{1}_{[1]} \otimes \mathbf{0}_{[1]})^{\frac{l}{2}}\}, & \{l > 2, 2 \mid l\}) \end{array} \right\}.$$

What have we Gained?

1. An abstract description of an algorithm for fixed length, that follows the paradigm of the largest chunks.
2. An intuitive way to enhance this algorithm to a bit-vector theory allowing variable length.
3. If termination of $\mathcal{S}_{\mathfrak{R}}$ can be shown, it describes a conceptually simple algorithm for the word unification problem.

Scenario



$\mathcal{C}_{\Re}$
Core Theory
+ Boolean
Implementation
Core Theory
+ Arithmetic
Problem:
Non-Canonicity or Exponential Blow-Up
$\mathcal{S}_{\Re}$
Variable Size
+ Boolean
Problem:
Non-Termination!
Problems:
Non-Convexity
Termination?

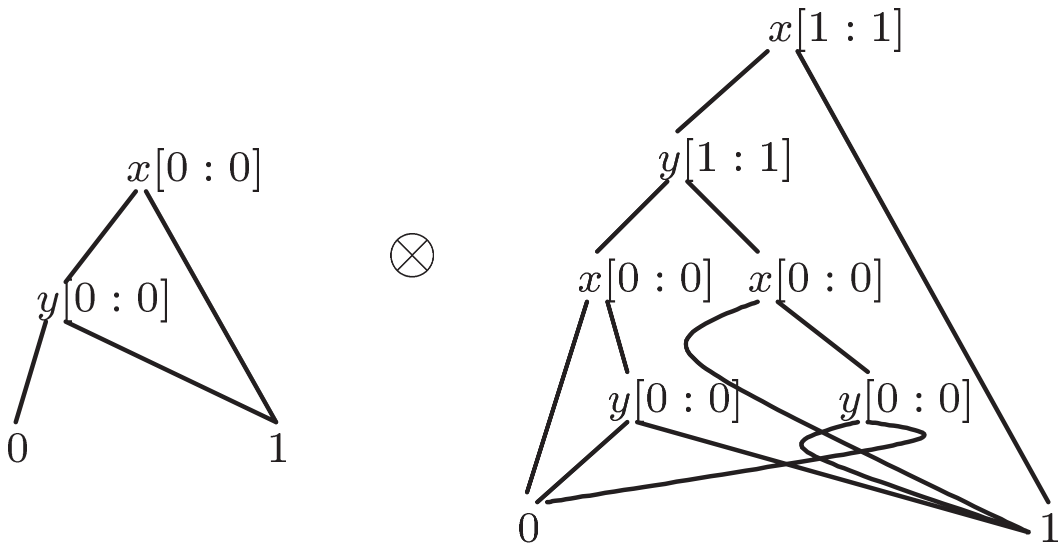
Questions & Discussion

Why canonization is expensive

Which is the canonical form?

$$(1) \quad x_{[n]} +_{[n]} x_{[n]} \equiv 2 \cdot x_{[n]} \equiv x_{[n]} \otimes \mathbf{0}_{[1]}$$

$$(2) \quad (x_{[2]} +_{[2]} y_{[2]}) \vee x_{[2]} \equiv$$



Canonical Form

canonical: well-defined and unique

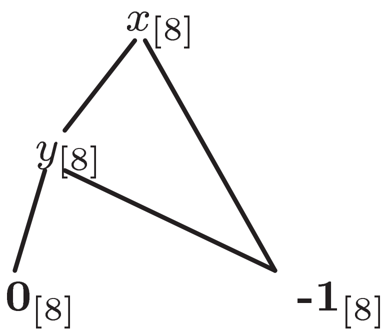
canonizer: a function σ with $t \equiv u \Leftrightarrow \sigma(t) \doteq \sigma(u)$

Canonical forms for bit-vectors

core theory: maximally connected concatenation of chunks

e.g. $x_{[8]} \otimes \mathbf{\text{-}1}_{[8]} \otimes y_{[16]}[0:3]$

+ Boolean: use ordered binary decision diagrams:
e.g.



$\otimes \ \mathbf{0}_{[4]}$

+ Arithmetic: split up to bits (!)