October 1995

VERSA: Verification, Execution and Rewrite System for ASCR

Duncan Clarke
University of Pennsylvania

Follow this and additional works at: http://repository.upenn.edu/cis_reports

Recommended Citation
http://repository.upenn.edu/cis_reports/196


This paper is posted at ScholarlyCommons, http://repository.upenn.edu/cis_reports/196
For more information, please contact repository@pobox.upenn.edu.
VERSA: Verification, Execution and Rewrite System for ACSR

Abstract
VERSA is a tool for the automated analysis of resource-bound real-time systems using the Algebra of Communicating Shared Resources (ACSR). This document serves as an introduction to the tool for beginning users, and as a reference for process and command syntax, examples of usage, and tables of operators, built-in functions and algebraic laws. Two detailed examples demonstrate the application of VERSA to canonical examples from the literature.

This version of the VERSA user's guide reflects the 95.09.10 version of the tool.

Comments
VERSA: Verification, Execution and Rewrite System for ACSR \(^1\)

MS-CIS-95-34

Duncan Clarke

1995

\(^1\)This research was supported in part by ONR N00014-89-J-1131s1, NSF CCR-9415346, and AFOSR F49620-95-1-0508
VERSA: Verification, Execution and Rewrite System for ACSR *

Duncan Clarke
Department of Computer and Information Science
University of Pennsylvania
Philadelphia, PA 19104-6389

October 30, 1995

Abstract

VERSA is a tool for the automated analysis of resource-bound real-time systems using the Algebra of Communicating Shared Resources (ACSR). This document serves as an introduction to the tool for beginning users, and as a reference for process and command syntax for users of all experience levels. Coverage includes a complete description of process and command syntax, examples of usage, and tables of operators, built-in functions and algebraic laws. Two detailed examples demonstrate the application of VERSA to canonical examples from the literature.

This version of the VERSA user’s guide reflects the 95.09.10 version of the tool. The latest version of VERSA is available by anonymous ftp from ftp.cis.upenn.edu in directory pub/rtg, and through the World-Wide Web via the Penn Real-Time Group home page http://www.cis.upenn.edu/~rtg/home.html.

*This research was supported in part by ONR N00014-89-J-1131S1, NSF CCR-9415346, and AFOSR F49620-95-1-0508.
## Contents

1 Introduction

2 General Syntax
   2.1 Format
   2.2 Comments
   2.3 Identifiers
   2.4 Reserved Words

3 Basic Data Types
   3.1 Integer Constants
   3.2 Event Label Constants
   3.3 Resource Name Constants
   3.4 Process Constants

4 Composite Data Types
   4.1 Set Constants
   4.2 Action Constants
   4.3 Event Constants
   4.4 Pair Constants

5 Operators and Expressions
   5.1 Expressions
   5.2 Index Definitions
   5.3 Operand Notation
   5.4 Arithmetic (+integer)
   5.5 Relational (+integer)
   5.6 Boolean (+integer)
   5.7 Miscellaneous (+integer)
   5.8 Sets (-set)
   5.9 Prefix (-process)
   5.10 Composition (-process)
   5.11 Context (-process)
   5.12 Miscellaneous (-process)
   5.13 Precedence and Associativity

6 Commands
   6.1 Miscellaneous
   6.2 Binding Process Variables
   6.3 Queries
   6.4 Process Equivalence Checking
   6.5 Process Interpretation
   6.6 Interpreter Commands

7 Preprocessor
   7.1 Token Replacement
   7.2 Macros
   7.3 File Inclusion
   7.4 Conditional Compilation
   7.5 Pragmas

A X-Windows Interface

B Built-In Functions
   min(ie1,...,ien)
   max(ie1,...,ien)
   sqrt(ie)
   sqrt(ie,round)
   UniqueDigits(n,radix)
   LeadingDigit(n,radix)
   TrailingDigit(n,radix)
   HasDigit(n,d,radix)
   rand(ceil)

C Algebraic Laws
   Choice1...Choice7
   Par1...Par6
   Scope1...Scope6
   Res1...Res6
   Close1...Close6
   Rec1

D Examples
   D.1 Two Bit Buffers
   D.2 The Jobshop

<table>
<thead>
<tr>
<th>Operator</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>min(ie1,...,ien)</td>
<td>14</td>
</tr>
<tr>
<td>max(ie1,...,ien)</td>
<td>14</td>
</tr>
<tr>
<td>sqrt(ie)</td>
<td>14</td>
</tr>
<tr>
<td>sqrt(ie,round)</td>
<td>14</td>
</tr>
<tr>
<td>UniqueDigits(n,radix)</td>
<td>14</td>
</tr>
<tr>
<td>LeadingDigit(n,radix)</td>
<td>14</td>
</tr>
<tr>
<td>TrailingDigit(n,radix)</td>
<td>14</td>
</tr>
<tr>
<td>HasDigit(n,d,radix)</td>
<td>14</td>
</tr>
<tr>
<td>rand(ceil)</td>
<td>14</td>
</tr>
<tr>
<td>Choice1...Choice7</td>
<td></td>
</tr>
<tr>
<td>Par1...Par6</td>
<td></td>
</tr>
<tr>
<td>Scope1...Scope6</td>
<td></td>
</tr>
<tr>
<td>Res1...Res6</td>
<td></td>
</tr>
<tr>
<td>Close1...Close6</td>
<td></td>
</tr>
<tr>
<td>Rec1</td>
<td></td>
</tr>
</tbody>
</table>

2
1 Introduction

This paper is intended as an introduction to the VERSA system for beginning users and a reference for advanced users. VERSA is a toolkit for modeling systems using ACSR, the Algebra of Communicating Shared Resources. ACSR is a real-time process algebra that incorporates the interleaved event synchronization model of CCS and a synchronous semantics for time passage steps. Novel aspects of ACSR include explicit notions of resources, time, and priority.

VERSA facilitates the construction and analysis of real-time systems using ACSR with the following features:

- Support for ACSR’s full syntax and semantics.
- Syntax and semantic checking of process expressions.
- Support for indexed process names, event labels, and resource names.
- Generalized operators for economically expressing operations on indexed process names, event labels, and resource names.
- Manipulation of ACSR process terms according to a set of laws preserving strong bisimulation.
- Equivalence checking and refutation for pairs of processes.
- Interactive execution of the labeled transition system corresponding to an ACSR process.

The sections that follow present a complete description of VERSA’s input syntax. ACSR and VERSA semantics are treated informally. This paper is a quick reference for VERSA. It is not intended as a tutorial or formal treatment of ACSR.

2 General Syntax

2.1 Format

- Spaces, tabs, newlines and formfeeds are used as separators. Extra such characters are legal and can be used to improve readability.

2.2 Comments

- Two types:

1. Begin with /*, end with */.
2. Begin with //, end with newline.
- Legal anywhere a space is legal.

2.3 Identifiers

- Identifiers are used as the names of process variables, event labels, resource names, index variables, and functions.
- Legal characters — a-z A-Z 0-9 underscore (_), apostrophe (’)
  - First character must be alphabetic.
  - There is no limit on identifier length.
  - Any apostrophes must occur last.
- Examples — P P2 P_i Delay P’ P2’’

2.4 Reserved Words

- Process Components

  and idle inf infinite
  infinity infty NIL or
  rec scope t tau

  The sequence of characters NIL is reserved for every capitalization of its individual letters.
- Generalized Process and Set Operators

  Choice Parallel Set
  Union Intersect Complement

- Algebraic Law Names

  Choice# Par# Scope# Res#
  Close# Rec# Rhide# Relab#

  The # symbol denotes any sequence of digits. The first letter may be upper or lower case.
- Commands

  bindings bye ctsmp
debug echo exit
fold guarded quit
terse unbind unbindall
unfold unwind verbose
whynot
3 Basic Data Types

The basic data types are integer (decimal), event label, resource name, and process. This section presents the syntax for constants.

3.1 Integer Constants
- Digits 0-9 or the keyword infty.
- Keyword infty is a special symbol representing infinity. Only allowed context is the time bound in a scope() operator.
- Keyword infty has aliases inf, infinite, and infinity.
- Examples — 007 12 scope(P,e,infty,Pe,NIL,Pi)

3.2 Event Label Constants
- Identifiers.
- Optionally prefixed with an apostrophe ('). Corresponds to bar over events in traditional process algebra notation, as in $\bar{e}$.
- Optionally suffixed by a comma separated list of integer indices enclosed in square brackets ([ and ]).
- The keywords tau and t represent the distinguished event label $\tau$.
- Examples — in 'Out tau e[1,1]

3.3 Resource Name Constants
- Identifiers.
- Optionally suffixed by a comma separated list of integer indices enclosed in square brackets ([ and ]).
- Examples — cpu Printer cell[34]

3.4 Process Constants
- NIL is the only process constant.
- Deadlocked process; performs no events or actions.

4 Composite Data Types

The built-in composite data types are set, action, event, and pair. This section presents the syntax for constants.

4.1 Set Constants
- Unordered comma separated list of homogeneous elements.
- Allowed element types are event labels, resource names, pairs, and resource, priority pairs.
- Examples — {rd,wrt} {} {(r1),(s,1)}

4.2 Action Constants
- Set of parenthesis enclosed resource name, priority pairs.
- Priority is expressed as an integer value.
- The keyword idle is an alias for the action {}.
- Examples — idle {} {(r1,5),(r2,7)}

4.3 Event Constants
- Parenthesis enclosed event label, priority pair.
- Priority is expressed as an integer value.
- Examples — (e,1) (in[34],27) (tau,0)

4.4 Pair Constants
- Slash (/) separated pair of event labels or resource names.
- Examples — P/p[34] R/R'

5 Operators and Expressions

5.1 Expressions
- An expression consists of one or more operands with an operator.
- Parenthesis may be used freely to improve readability or override default operator precedences.
- Examples —
  - i+7
  - P+NIL
  - R[x=(y*z)/w] || S
5.2 Index Definitions

- An index is an identifier that represents an integer variable.
- The range of an index is defined by an index definition.

**Syntax**

\( \{var, (max | min, max[, step[, cond]])\} \)

<table>
<thead>
<tr>
<th>var</th>
<th>The index being defined.</th>
</tr>
</thead>
<tbody>
<tr>
<td>min</td>
<td>An integer expression for the initial value. (Default is 1).</td>
</tr>
<tr>
<td>max</td>
<td>An integer expression for the maximum value.</td>
</tr>
<tr>
<td>step</td>
<td>An integer expression for the value by which the index is incremented. (Default is 1).</td>
</tr>
<tr>
<td>cond</td>
<td>Boolean conditional evaluated for each value of the index. If cond is false the index value is not used. (Default is 1).</td>
</tr>
</tbody>
</table>

- **Example** — \{i, i, 100, j, i%2 == 0\}
  This index ranges from 1 to 100 by steps of j. (Index i is a sub-index of an index j, the value of which is used for the increment of i.) Only even values of i will be available to the context of this index definition.

- An index definition can define multiple indices. A comma-separated list of individual index definitions is used. Index values are initialized and computed from left-to-right.

- **Example** — \{i, i, 10\}, \{j, 1, i\}
  Index i ranges from one to ten, and for each value of i, index j ranges from one up to the value of i.

5.3 Operand Notation

- Some operators require specific kinds of operands. The following notation is used to indicate differences.
  - \( e \) Any expression or constant.
  - \( v \) Any expression that refers to a variable to which a value can be assigned.

- A prefix indicates expression type. For example, \( ie \) is any integer expression. The complete list of type prefixes follows:
  - \( i \) — integer
  - \( p \) — process
  - \( l \) — event label
  - \( e \) — event
  - \( r \) — resource name
  - \( a \) — action
  - \( d \) — index definition

- Pairs of a given label type are indicated by a \( p \) suffix, for example \( lep \) for an event label pair or \( rep \) for a resource name pair.

- Sets of a given base type are indicated by an \( s \) suffix, for example \( les \) for an event label set.

- If several operands appear in an expression, then they may be distinguished by appending numbers, for example \( p1 + p2 \).

5.4 Arithmetic \((\rightarrow \text{integer})\)

**Addition**: +

- **Usage** — \( ie1 + ie2 \)
- **Example** — \( i1 + i2 \)

**Subtraction**: -

- **Usage** — \( ie1 - ie2 \)
- **Example** — \( j - 1 \)

**Negation**: -

- **Usage** — \( -ie \)
- **Example** — \( -j \)

**Multiplication**: *

- **Usage** — \( ie1 \times ie2 \)
- **Example** — \( i \times 2 \)

**Division**: /

- **Usage** — \( ie1 / ie2 \)
- **Example** — \( j / 2 \)

**Remainder**: %

- **Usage** — \( ie1 \% ie2 \)
- **Example** — \( k \% 2 \)

**Exponentiation**: **

- **Usage** — \( ie1 \times ie2 \)
- **Example** — \( m \times 3 \)
5.5 Relational (→integer)

The logical value “false” is represented by integer 0, and “true” by any non-zero value. The values of relational and boolean expressions are 0 for false and 1 for true.

Equal: ==
- Usage — \(i_1 == i_2\)
- Example — \(\{i,0,10,1,(j\%2)==0\}\)

Not Equal: !=
- Usage — \(i_1 != i_2\)
- Example — \(\{i,0,10,1,i!=j\}\)

Less Than: <
- Usage — \(i_1 < i_2\)
- Example — \(\{i,0,10,1,i<j\}\)

Less Than or Equal: <=
- Usage — \(i_1 <= i_2\)
- Example — \(\{i,0,10,1,i<=j-1\}\)

Greater Than: >
- Usage — \(i_1 > i_2\)
- Example — \(\{i,0,10,1,2*i>j\}\)

Greater Than or Equal: >=
- Usage — \(i_1 >= i_2\)
- Example — \(\{i,0,10,1,2*i>=j-1\}\)

5.6 Boolean (→integer)

Negation: !
- Usage — ! \(i\)
- Example — \(\{i,0,10,1,(i<j+k)\}\)

Disjunction: or
- Usage — \(i_1 \text{ or } i_2\)
- Example — \(\{i,0,10,1,(i<3) \text{ or } (i>6)\}\)

Conjunction: and
- Usage — \(i_1 \text{ and } i_2\)
- Example — \(\{i,1,9,1,(i\%2) \text{ and } (i<j)\}\)

5.7 Miscellaneous (→integer)

Function Call: \(\text{FuncName(\ldots)}\)
- Usage — \(\text{FuncName}(i_1, \ldots, i_n)\)
  The built-in function indicated by \(\text{FuncName}\) (see Appendix B) is applied to the argument list.
- Example — \(\text{Set}[\text{sqrt}(i)] \{i,1,100\}\)

5.8 Sets (→set)

Set Generator: \(\text{Set}[\ldots]\)
- Usage — \(\text{Set}[e_1, \ldots, len nd]\)
  Generates a set of event labels.
- Example — \(\text{Set}[e[i] \{i,1,5]\}\)

- Usage — \(\text{Set}[r_1, \ldots, ren nd]\)
  Generates a set of resource names.
- Example — \(\text{Set}[r[i,j], s[i] \{i,1,5], \{j,1,5]\}\)

- Usage — \(\text{Set}[epl, \ldots, lepn nd]\)
  Generates a set of event label pairs.
- Example — \(\text{Set}[in[i+2]/e[i] \{i,1,5]\}\)

- Usage — \(\text{Set}[rep1, \ldots, repn nd]\)
  Generates a set of resource name pairs.
- Example — \(\text{Set}[cpu[i*2]/r[i] \{i,1,5]\}\)

Union: \(\text{Union}[\ldots]\)
- Usage — \(\text{Union}[e_1, \ldots, esn]\)
  Forms the union of two or more sets containing elements of the same base type.
- Example — \(\text{Union}\{r\}, \text{Set}[s[i] \{i,1,5]\}\)

Intersection: \(\text{Intersect}[\ldots]\)
- Usage — \(\text{Intersect}[e_1, \ldots, esn]\)
  Forms the intersection of two or more sets containing elements of the same base type.
- Example — \(\text{Intersect}\{r[1], r[2], r[3]\}, \{r[2], s\}\)

Complement: \(\text{Complement}[\ldots]\)
• Usage — Complement[es1,es2]
  Forms the complement of set es1 with respect to universe es2. The elements of es1 and es2 must be of the same base type.

• Example — Complement[\{r[3]\},Set[r[1] \{i,1,5]\}]

5.9 Prefix (→process)

Event Prefix: .

• Usage — ee.pe
  A process that synchronizes on ee and continues as the process pe.

• Example — (e,1).P

Action Prefix: :

• Usage — ae:pe
  A process that executes the time-consuming action ae and continues as the process pe.

• Example — \{(r,1),(s,2)\}:Q

5.10 Composition (→process)

Choice: +

• Usage — pe1 + pe2
  A process that chooses to continue as pe1 or pe2 depending on one or more of the following: (1) event and resource offerings of the environment; (2) priority arbitration; and (3) nondeterministic choice among alternatives.

• Example — (e,1).P + Q

Generalized Choice: Choice[

• Usage — Choice[pe de]
  The choice process that results from composing the process expressions pe that result for index values defined by de. Similar to the following ACSR notation: $\prod_{i=\text{min}}^{\text{max}} P_i$.

• Example — Choice[P[i] \{i,1,10\}]

Parallel Composition: || (or |)

• Usage — pe1 || pe2
  The process that result from executing pe1 and pe2 simultaneously. Events are interleaved or synchronize to produce $\tau$ events. Time consuming actions must execute concurrently.

• Example — ((e,1).P+\{}:P2)||Q

Generalized Parallel Composition: Parallel[

• Usage — Parallel[pe de]
  The choice process that results from composing the process expressions pe that result for index values defined by de. Similar to the following ACSR notation: $\prod_{i=\text{min}}^{\text{max}} P_i$.

• Example — Parallel[\{(e[i],1).Q \{i,1,10\}\]}

5.11 Context (→process)

Temporal Scope: Scope()

• Usage — scope(pe1,le,ie,pe2,pe3,pe4)
  Process pe1 is executed for up to ie time units. If pe1 executes an event labeled with le before ie time units elapse then the scope is terminated and the process continues as pe2. If pe1 is executed for exactly ie time units without the scope being terminated the scope is terminated and the process continues as pe3. The scope can be terminated at any time before ie time units elapse by executing an event or action offered by pe4. In that case, the process continues as pe4.

• Example — scope(rec X.{}:X, dummy,10, NIL,TimesUp,NIL)

Resource Closure: [ ]

• Usage — [pe] res
  The process formed by augmenting every action a of pe with \{r,0\} for every \(r \in \text{res}\) such that a has no resource name, priority pair with resource r.

• Example — [\{(r,1),(t,3)\}:P]\{r,s,t\}
  The first action of this process would be \{(r,1),(t,3),(s,0)\}. Subsequent actions of P would be augmented in the same way.

Event Restriction: \(~\)

• Usage — pe \ les
  The process formed by prohibiting pe from executing events labeled with event labels from les.
Example —

\[((e,1).P \parallel (e,1).Q)\{e,f,g}\]

The process can only perform the action \((r,2)\) and continue as \((P\mid Q)\{e,f,g\}\) because the offered events are restricted.

Resource Hiding: \(\backslash\)

- Usage — \(pe \backslash rns\)
  The process formed by eliminating all resource, priority pairs labeled with resource names from \(rns\) from the actions of \(pe\).
- Example — \(\{(r,1),(s,1)\}:P\backslash\{s\}\)
  The first action of this process would be \(\{(r,1)\}\). Subsequent actions of \(P\) would be modified in the same way.

Total Resource Hiding: \(\backslash\{\ast\}\)

- Usage — \(pe \backslash \{\ast\}\)
  The process formed by eliminating all resource, priority pairs from the actions of \(pe\).
- Example — \(\{(r,1),(s,1)\}:P\backslash\{\ast\}\)
  The first action of this process would be \\{\}. Subsequent actions of \(P\) would be modified in the same way.

Relabeling: \%

- Usage — \(pe \% [leps, reps]\)
  The events of \(pe\) are relabeled according to the pairs of \(leps\) and the resources names appearing in actions of \(pe\) are relabeled according to the pairs of \(reps\).
- Example — \(\{(r,1)\}:X\%[\{(init/e),(cpu/r)\}\]
  The first event of this process would be \((init,1)\). The action following this event would be \{(CPU,1)\}. Subsequent events and actions of \(P\) would be modified in the same way.

5.12 Miscellaneous \((\rightarrow process)\)

Recursion: \(\text{rec}\)

- Usage — \(\text{rec} \ pv. pe\)
  Standard recursion on process variable \(pv\).
- Example — \(\text{rec} X.((\text{again},1).X \ + \ (\text{stop},1).\text{NIL})\)

Law Application: \(\text{LawName()}\)

5.13 Precedence and Associativity

- Precedence — In the chart below, the operators within a group have equal precedence. Higher precedence operator groups are higher in the chart.

  - Associativity — In the absence of explicit parentheses, associativity rules are used to determine how to group operators and operands (left-to-right, or right-to-left), when the operators are in the same group.

  - Examples —
    - \(a \ast b/c\) is equivalent to \((a \ast b)/c\) because of left-to-right associativity.
    - \(e,(2)\).\{\}::P and \(e,(2)\).\{\}:P\) are equivalent because of right-to-left associativity.
Exponentiation

<table>
<thead>
<tr>
<th>Usage</th>
<th>pv = pe ;</th>
</tr>
</thead>
<tbody>
<tr>
<td>The process pe is bound to the process variable pv. If pv is already bound the old binding is saved and can be restored with an unbind command.</td>
<td></td>
</tr>
</tbody>
</table>

Example — P = (e1)P ;

Generative:

<table>
<thead>
<tr>
<th>Usage</th>
<th>pv = pe de ;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multiple bindings may be registered, depending on how many index values are generated by de. Process variable pv must be indexed by exactly the index variables defined by de.</td>
<td></td>
</tr>
</tbody>
</table>

Example — Q[i] = (psYes,1).NIL { i, i, i, 100, i, sqrt(i)*sqrt(i)==i };
| This process generator binds only those 9[i] for which i is a perfect square. |

Unbinding:

<table>
<thead>
<tr>
<th>Usage</th>
<th>unbind pv ;</th>
</tr>
</thead>
<tbody>
<tr>
<td>The current binding of process variable pv is removed. If pv was already bound at the time of its most recent binding, the old binding is restored. Binding and unbinding implement push and pop operations on a LIFO stack of bindings with its head bound to pv.</td>
<td></td>
</tr>
</tbody>
</table>

The keyword unwind is an alias for unbind.

<table>
<thead>
<tr>
<th>Usage</th>
<th>unbindall ;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remove all bindings.</td>
<td></td>
</tr>
</tbody>
</table>

6.1 Miscellaneous

** Termination:
- Usage: quit, exit, or bye.

** Display Mode:
- Usage: terse
  Set terse output mode. Eliminates all non-essential messages.
- Usage: verbose
  Set verbose output mode. Enable all user-oriented messages.
- Usage: debug
  Set debug output mode. Enables all user-oriented messages and generates copious amounts of data useful for debugging the VERSA system.
- Usage: echo
  Toggles echoing of input lines. If echo mode is on all input is copied to standard output. If echo mode is off input lines read from #include 'ed files will not be displayed.

6.3 Queries

** General Information:
- Usage — ?
  Displays a general help message summarizing commands and syntax.

** Bindings:
- Usage — bindings ?
  Displays all current process bindings.

** Identifier Types:
• Usage — *ident*?
  Displays the type (if any) of the identifier. If the identifier is a bound process variable its binding is displayed.

Event/Action Comparisons:

• Comparison operators (cop) are ==, ! =, <, <=, >, and >=.

• Usage — (ee1 | ae1) cop (ee2 | ae2) ?
  The preemption relation is applied to the pair of operands to determine whether one preempts the other. That result is conditioned by the comparison operator and an appropriate message is output.

• Example — (e,3) > (e,1)
  A message is output indicating that the query is true. Event (e,3) preempts event (e,1).

Guardedness:

• Usage — guarded( pe , pv ) ?
  Tests whether all occurrences of process variable pv are guarded by prefix operators in process pe and outputs an appropriate message.

• Usage — guarded( pe ) ?
  Tests whether every process variable that occurs in pe is guarded by a prefix operator and outputs an appropriate message.

### 6.4 Process Equivalence Checking

Equivalence:

• Usage — pv1 == pv2 ?
  The processes bound to pv1 and pv2 are compared to determine whether they are equivalent according to any of the following notions of equivalence:

  1. *Identity:* The abstract syntax tree representations of the two processes are compared node by node to determine whether the two processes have identical syntax. Time to complete is linear in the size of the abstract syntax trees.

  2. *Unique Fixpoint Induction:* The abstract syntax tree representations of the two processes are compared to determine whether the two processes have identical structure with the exception of process variable naming and referencing. Time to complete is proportional to the size of the abstract syntax trees.

3. *Prioritized Strong Equivalence:* Labeled Transition System (LTS) models are constructed for each of the processes and a state minimization algorithm is applied to the two state machines to determine whether or not they are bisimilar. Time to complete is exponential in the size of the abstract syntax trees for finite state processes. For infinite state processes the test does not terminate.

4. *Prioritized Weak Equivalence:* LTS models are constructed for each of the processes. All τ-labeled event edges are removed according to an algorithm that mimics the algorithm for computing the ε-closure of a finite state automaton. A state minimization algorithm is applied to the two τ-free LTS’s to determine whether or not they are bisimilar. Time to complete is exponential in the size of the abstract syntax trees for finite state processes. For infinite state processes the test does not terminate.

Refutation:

• Usage — *whynot* ?
  If the most recent equivalence test returned a result of false for the prioritized strong equivalence test this command will output a shortest path to the first state in each LTS where the processes diverge.

• Usage — *whynot* ?
  If the most recent equivalence test returned a result of false for the prioritized weak equivalence test this command will output a shortest path to the first state in each τ-free LTS where the processes diverge.

### 6.5 Process Interpretation

Executing the LTS:
- **Usage** — *pv* !
  An LTS is constructed for the process bound to *pv* and interpreter mode is entered. The commands accepted in interpreter mode are described in Section 6.6.

Executing the τ-free LTS:

- **Usage** — *pvτ* !
  An LTS is constructed for the process bound to *pv*. All τ-labeled event edges are removed according to an algorithm that mimics the algorithm for computing the ε-closure of a finite state automaton. Interpreter mode is entered for the τ-free LTS. The commands accepted in interpreter mode are described in Section 6.6.

### 6.6 Interpreter Commands

Interpreter commands are accepted in a special mode that is activated by the commands listed in Section 6.5. Interpreter mode allows the user to interactively step through the LTS (or τ-free LTS) corresponding to a process. The commands available in interpreter mode are listed below. The default value for optional numeric parameters is one.

**General:**

- `?` or `help` — Display a general help message summarizing commands and syntax.
- `quit` — Exit interpreter mode.

**Edge Traversal:**

- `step [edge]` — Advance along edge number *edge* to a new node.
- `back [steps]` — Backtrack by *steps* edge traversals.
- `cont [edge]` — Starting with *edge*, advance along edges until a choice arises or the trace length limit is met.
- `rand` — Advance along edges making choices according to a uniformly distributed random variable whenever a node with multiple output edges is encountered. Continue until the trace length limit is met.
- `seed seedval` — Seed the random number generator with *seedval*.
- `limit steps` — Set the trace length limit to *steps*.

- **limit** — Set the trace length limit to ∞.

**Interpreter State Management:**

- `trace` — Display the current trace.
- `trace*` — Display the current trace without listing τ labeled events.
- `clear` — Clear the current trace without changing the interpreter’s current node.
- `save` — Save a pointer to the current node and a copy of the current trace to a LIFO stack.
- `restore` — Reset the execution state to the state and trace saved most recently.

**Queries:**

- `show` — Display the outgoing edges of the current node.
- `show edge` — Display the outgoing edges of the node reachable via edge number *edge*.
- `show limit` — Display the current value of the trace length limit.
- `show stack` — Display stack of saved nodes and traces.
- `show stats` — Display statistics for the reachable state space of the LTS including node count, edge count, counts of deadlocked states, zeno states, states capable of stopping the clock, and CPU time to compute the LTS.
- `show time` — Display a count of time consuming steps contained in the current trace.
- `show deadlock*[s]` — Display the process term for each deadlocked node and a shortest path from the start node to each deadlocked node.

### 7 Preprocessor

A # as the first character on a line designates a preprocessor control line. Control lines are terminated by a newline. Use a backslash just before the newline to continue a control line.
7.1 Token Replacement

#define identifier string
- Example — #define DELAY 10
  Substitutes 10 for every occurrence of DELAY as a token.

#undef identifier
- Example — #undef DELAY
  Cancels previous #define for identifier DELAY, if any.

7.2 Macros

Note — To avoid precedence conflicts, enclose a macro parameter in parenthesis everywhere it occurs in a macro definition.

#define identifier1(identifier2,...) string
- Example — #define isodd(N) (((N)%2)==1)
  Substitutes (((arg)%2)==1) for isodd(arg), replacing each occurrence of N by arg.

  Example — #define pause(T,NEXT) \
  scope(rec X.{X}, \ 
  dummy,(T), \ 
  NIL,(NEXT),NIL)

  The backslashes are used to continue the macro definition across multiple lines. This macro creates a process expression that executes the time consuming action 0 for T time units and continues as NEXT.

7.3 File Inclusion

#include <filename>
- Example — #include <stdlib.acsr>
  Replaces this line with the contents of the file stdlib.acsr. The angle brackets specify that stdlib.acsr should be found in a directory found in the path defined by the ACSRLIB environment variable. Does not search the current working directory.

#include "filename"
- Example — #include "spec.acsr"
  Replaces this line with the contents of the file spec.acsr. When "spec.acsr" is used instead of <spec.acsr>, spec.acsr is sought in the current working directory.

7.4 Conditional Compilation

Conditional compilation control lines are used to compile different code depending on externally defined conditions. Conditional compilation blocks can be nested freely.

#if def identifier
- Example — #ifdef MODE
  True if MODE is currently defined by #define.
#endif

#ifdef identifier
- Example — #ifndef MODE
  True if MODE is not currently defined by #define.
#else
  ...
#endif

- If preceding #ifdef or #ifndef test is —
  - True — Lines between #else and #endif are ignored.
  - False — Lines between the test and a #else or, lacking a #else, the #endif, are ignored.

  #endif terminates the conditional compilation.

- Example —
  #ifndef STDLIB_ACSR
  #include <stdlib.acsr>
  #endif

7.5 Pragmas

Pragmas implement debugging directives that produce printed output describing the internal state of the lexical analyzer or parser.

#pragma identifier string

- The following identifiers are recognized:
  symtab_dump — Display the contents of the symbol table.
  macstab_dump — Display the contents of the macro table.
  text — Parse string as though it were regular input.
  sanity_test — Test integrity of processes.
  msg — Copy string to standard error output.
References


A  X-Windows Interface

An X-Windows interface has been implemented on top of the VERSA implementation described in the main body of this paper. It supports only the un-indexed portion of the ACSR process syntax.

The most valuable features of the X-Windows interface are (1) a point-and-click rewrite system that significantly improves the usability of the law application operators described in the main body of this paper; and (2) a point-and-click interface to the interpreter that displays a small portion of the LTS and allows the user to select the edges that are traversed with the mouse pointer.

The X-Windows interface includes a help function that provides complete information on its use.

B  Built-In Functions

This section describes the VERSA system’s built-in functions for operating on integer values.

- Minimum: \( \text{min}( \text{iel}, \ldots, \text{ien} ) \)
  Computes the minimum of its list of two or more arguments.
- Maximum: \( \text{max}( \text{iel}, \ldots, \text{ien} ) \)
  Computes the maximum of its list of two or more arguments.
- Square: \( \text{sqr}( \text{ie} ) \)
  Computes the square of \( \text{ie} \).
- Square Root: \( \text{sqrt}( \text{ie} \, \text{[round]} ) \)
  Computes the integer square root of \( \text{ie} \), rounding according to \( \text{round} \). If \( \text{round} \) is zero \( \lfloor \sqrt{\text{ie}} \rfloor \) is returned. If \( \text{round} \) is one \( \lceil \sqrt{\text{ie}} \rceil \) is returned. If \( \text{round} \) is not specified \( \text{ie} \) is truncated.
- Count Unique Digits: \( \text{UniqueDigits}(\text{iel}, \text{ie2}) \)
  Computes the count of unique digits in \( \text{iel} \) interpreted as a radix \( \text{ie2} \) integer.
- Leading Digit: \( \text{LeadingDigit}(\text{iel}, \text{ie2}) \)
  Computes the leading digit of \( \text{iel} \) interpreted as a radix \( \text{ie2} \) integer.
- Trailing Digits: \( \text{TrailingDigits}(\text{iel}, \text{ie2}) \)
  Interprets \( \text{iel} \) as a radix \( \text{ie2} \) integer and returns all but the first digit.
- Test for Digit: \( \text{HasDigit}(\text{iel}, \text{ie2}, \text{ie3}) \)
  Interprets \( \text{iel} \) as a radix \( \text{ie3} \) integer and checks whether it contains digit \( \text{ie2} \). Returns one if true, zero if false.
- Uniform Random Number: \( \text{rand}(\text{iel}) \)
  Returns a uniformly distributed random integer from the interval \( [0, \text{iel}) \).
C Algebraic Laws

Choice1 \( P + \text{NIL} = P \)
Choice2 \( P + P = P \)
Choice3 \( P + Q = Q + P \)
Choice4 \( (P + Q) + R = P + (Q + R) \)
Choice5 \( A_1 : P_1 + A_2 : P_2 = A_2 : P_2 \text{ if } A_1 \prec A_2 \)
Choice6 \( (a_1, n_1).P_1 + (a_2, n_2).P_2 = (a_2, n_2).P_2 \text{ if } (a_1, n_1) \prec (a_2, n_2) \)
Choice7 \( A : P + (\tau, n).Q = (\tau, n).Q \text{ if } n > 0 \)

\begin{align*}
\text{Par1:} & \quad \text{NIL}\|\text{NIL} = \text{NIL} \\
\text{Par2:} & \quad (A : P)\|\text{NIL} = \text{NIL} \\
\text{Par3:} & \quad (a, n).P\|\text{NIL} = (a, n).(P\|\text{NIL}) \\
\text{Par4:} & \quad P\|Q = Q\|P \\
\text{Par5:} & \quad (P\|Q)\|R = P\|(Q\|R) \\
\text{Par6:} & \quad \left( \sum_{i \in I} A_i : P_i + \sum_{j \in J} (a_j, n_j).Q_j \right) \| (\sum_{k \in K} B_k : R_k + \sum_{l \in L} (b_l, m_l).S_l) \\
& \quad = \sum_{i \in I, j \in J} (A_i \cup B_j) : (P_i\|Q_j) \\
& \quad + \sum_{j \in J} (a_j, n_j).(P_j\|(\sum_{k \in K} B_k : R_k + \sum_{l \in L} (b_l, m_l).S_l)) \\
& \quad + \sum_{l \in L} (b_l, m_l).(\sum_{i \in I} A_i : P_i + \sum_{j \in J} (a_j, n_j).Q_j)\|S_l \\
& \quad + \sum_{j \in J, j \in L, a_j = b_l} (\tau, n_j + m_l).(Q_j\|S_l)
\end{align*}

Table 1: ACSR Laws (Part 1 of 2)
Scope 1: \[ A : P \Delta_t^1 (Q, R, S) = A : (P \Delta_{t-1}^b (Q, R, S)) + S \text{ if } t > 0 \]

Scope 2: \[(a, n).P \Delta_t^1 (Q, R, S) = (a, n).((P \Delta_t^b (Q, R, S)) + S \text{ if } t > 0 \land a \neq b) \]

Scope 3: \[(a, n).P \Delta_t^1 (Q, R, S) = (\tau, n).Q + S \text{ if } t > 0 \land a = b \]

Scope 4: \[ P \Delta_t^0 (Q, R, S) = R \]

Scope 5: \[(P_1 + P_2) \Delta_t^1 (Q, R, S) = P_1 \Delta_t^b (Q, R, S) + P_2 \Delta_t^b (Q, R, S) \]

Scope 6: \[ \text{NIL} \Delta_t^1 (Q, R, S) = S \]

Res 1: \[ \text{NIL} \setminus F = \text{NIL} \]

Res 2: \[ (P + Q) \setminus F = (P \setminus F) + (Q \setminus F) \]

Res 3: \[ (A : P) \setminus F = A : (P \setminus F) \]

Res 4: \[ ((a, n).P) \setminus F = (a, n).(P \setminus F) \text{ if } a \notin F \land \overline{a} \notin F \]

Res 5: \[ (P \setminus F_1) \setminus F_2 = P \setminus (F_1 \cup F_2) \]

Res 6: \[ [(P)]_I \setminus F = [P \setminus F]_I \]

Close 1: \[ [\text{NIL}]_I = \text{NIL} \]

Close 2: \[ [P + Q]_I = [P]_I + [Q]_I \]

Close 3: \[ [A_1 : P]_I = (A_1 \cup A_2) : [P]_I \text{ where } A_2 = \{(r, 0) | r \in I - \rho(A_1)\} \]

Close 4: \[ [(a, n).P]_I = (a, n).[P]_I \]

Close 5: \[ [(P)]_I = [P]_{I \cup I} \]

Close 6: \[ [P \setminus F]_I = ([P]_I) \setminus F \]

Rec 1: \[ \text{rec}X.P = P[\text{rec}X.P/X] \]

Table 2: ACSR Laws (Part 2 of 2)
D Examples

D.1 Two Bit Buffers

\[
\begin{align*}
\text{TBB} &= (\text{in},1).\text{TBB1}; \\
\text{TBB1} &= (\text{in},1).\text{TBB2} + (\text{out},1).\text{TBB}; \\
\text{TBB2} &= (\text{out},1).\text{TBB1}; \\
\text{SYS} &= (\text{OBBL}|\text{OBBR})\{\text{sync}\}; \\
\text{OBBL} &= (\text{in},1).\text{(sync},2).\text{OBBL}; \\
\text{OBBR} &= ('\text{sync},2).(\text{out},1).\text{OBBR};
\end{align*}
\]

Processes TBB and SYS provide two alternative formulations of a two bit buffer. They are adapted from a CCS example found in [9]. TBB is a purely sequential formulation of a two bit buffer that receives one or two inputs by synchronizing on \text{in} and generates output by synchronizing on \text{out}. If zero bits are currently held only \text{in} is possible. If one bit is held either \text{in} or \text{out} is possible. If two bits are held the buffer is full so only \text{out} is possible. SYS is an alternative formulation that uses concurrency instead of explicit sequential structure to realize the buffer.

VERSA can be used to demonstrate the equivalence of these two formulations as follows:

```
:- #include "2bb.acsr"
:- TBB == SYS?
   ufi failed--following pair could not be matched:
   <(\text{in},1).\text{TBB1},(\text{OBBL}|\text{OBBR})\{\text{sync}\}>
   --following pair was matched:
   <\text{TBB},\text{SYS}>
   false (by prioritized strong equivalence)
   true (by prioritized weak equivalence)
:- whynot?
prefix:  --(\text{in},1)-->
unmatched TBB:
   --(\text{in},1)-->
   --(\text{out},1)-->
unmatched SYS:
   --(\tau,(2+2))@\text{sync}-->
```

The "#include" command reads the process descriptions from a file named 2bb.acsr. The "TBB == SYS?" command initiates equivalence checking of the TBB and SYS processes. The first result that is printed is the outcome of the unique fixpoint induction test. The test fails because TBB and SYS disagree on their respective first operators. The next result is the outcome of the prioritized strong equivalence test. Since that test failed, the next result that is printed is the outcome of the prioritized weak equivalence test, which succeeded. Processes TBB and SYS are equivalent by prioritized weak equivalence (the notion of bisimulation that disregards internal \tau events).

The "whynot?" command demonstrates the equivalence refutation feature. It lists edges that can be traversed to arrive at states that are not bisimilar according to the definition of prioritized strong equivalence. The output shows that after an \text{in} event TBB and SYS differ because TBB is ready for another \text{in} or \text{out} immediately, but SYS must first synchronize internally on its \text{sync} event.
D.2 The Jobshop

#define JOBRANGE 1,3
#define EASY 1
#define HARD 2
#define OTHER 3
#define DONE(JOB) 0
#define IFELSE(PRED,P1,P2) ((tau,2*((PRED)!=0)+1).(P1) + (tau,2).(P2))

Sem = {Sem + (get,1).rec Sem'.(put,1).Sem + {(Semaphore,1)}:Sem'};
HamSem = Sem%[(geth/get,puth/put),{Hammer/Semaphore}];
MalSem = Sem%[(getm/get,putm/put),{Mallet/Semaphore}];

Jobber = Choice[(in[job],1).Start[job] {job,JOBRANGE}] + {}:Jobber;
Start[job] = IFELSE(job==EASY,{},Finish[job],
     IFELSE(job==HARD,Usehammer[job],
     Usehammer[job] = (geth,1).{}.:Usehammer[job] +
     (tau,1).{}.:Usehammer[job] {job,JOBRANGE};
Usemallet[job] = ('getm,1).{}.:('putm,1).Finish[job] +
     {}:Usemallet[job] {job,JOBRANGE};
Finish[job] = ('out[DONE(job)],1).Jobber
     {job,JOBRANGE};

Jobshop = [Jobshop']{Hammer,Mallet};
Jobshop' = (Jobber || Jobber || HamSem || MalSem){geth,puth,getm,putm};

Process Jobshop is an ACSR implementation of the job shop example found in [9]. The #define of
JOBRANGE defines the range of values that represent jobs. The next three #defines break JOBRANGE into
distinct types of jobs, EASY, HARD, and OTHER. The DONE macro translates a job into a completed job.

The IFELSE macro uses ACSR’s priority relation to define an if/then/else construct. If the value of the
boolean predicate PRED is non-zero (i.e. true) then process P1 is prefixed with a priority 2*1+1 = 3 internal
event. Otherwise process P1 is prefixed with priority 2*0+1 = 1 internal event. The “else” process P2 is
always prefixed with a priority 2 internal event. According to the semantics of the choice operator if PRED is
true (r,3).P1 will be executed, otherwise (r,2).P2 will be executed.

Process Sem is a general purpose binary semaphore with idling. Initially Sem can idle for one time unit
or receive a get request to allocate the semaphore. Once the semaphore is allocated it remains allocated
and any idling steps include the Semaphore resource until a put request is received. Process HamSem uses
renaming of events and resources to create a Hammer resources whose access is controlled by geth and puth
events. Process MalSem creates a similar Mallet resource.

Process Jobber describes a single worker in the job shop. A job is received by synchronizing on an
in[job] event, or the jobber idles for one time unit. If a job of type job was received, the process continues
as Start[job]. Note how generalized choice (i.e. Choice[····]) and indexing are used to simulate value
passing with indexed events. Start evaluates the job type and (1) completes “easy” jobs in one time unit
without the use of any tools; (2) proceeds as Usehammer if the job is “hard;” or (3) proceeds as Useoffset if
the job falls somewhere in between.
Process Usetool attempts to use either the hammer or the mallet to complete the job, depending on which tool (if any) is available. If no tool is available, Usetool idles for one time unit and tries again. Processes Usehammer and Usemallet allocate and use their respective tools, or idle one time unit if the tool is not immediately available. Process Finish marks the job as complete and outputs the job with an out event.

Process Jobshop creates a job shop with two jobbers by composing Jobber processes in parallel with Hammer and Mallet controlling processes. The get and put operations for the two resources are restricted to insure that the resources can only be allocated locally, and no external resources are allocated. The Jobshop is closed in the Hammer and Mallet resources to insure that Hammer and Mallet are used exclusively by the two Jobber processes.