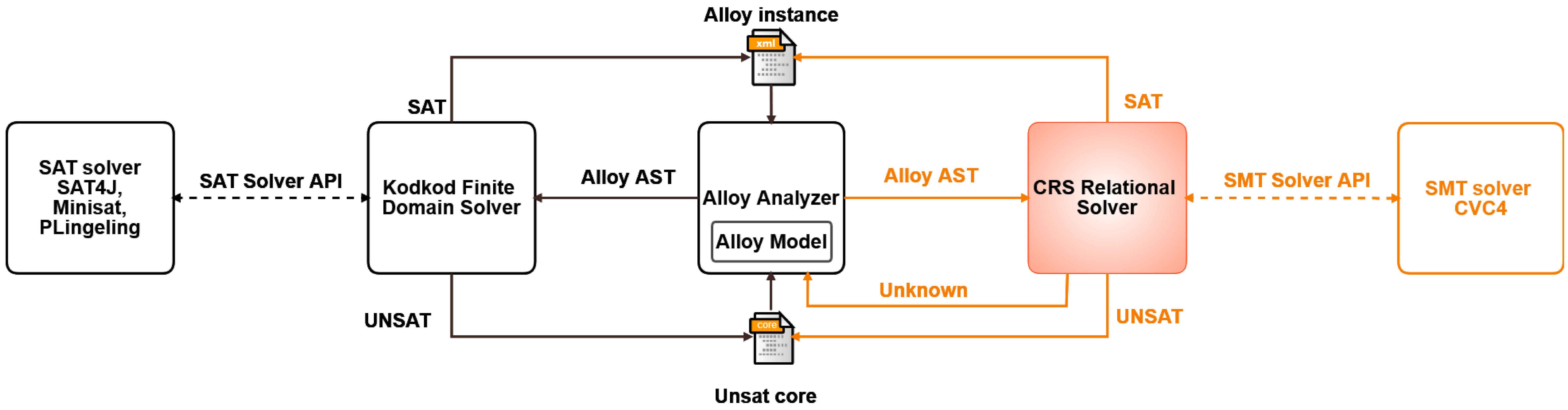
A new relational solver for the Alloy Analyzer

Mudathir Mohamed, Baoluo Meng, Andrew Reynolds and Cesare Tinelli

The University of Iowa

What is CRS?

- New relational solver from Alloy models to SMT formulas over the theory of finite relations
- It can prove properties on unbounded domains, including integers



Example 1

```
sig B {}
// f: A → B is injective
sig A{ f: disj one B }
// f is surjective
fact { f[A] = B }
// different elements have different images
assert assertion {
all x, y : A | x != y implies f[x] != f[y]}
check assertion for 5 A , 5 B
```

- Kodkod can prove valid assertions only in bounded scopes (e.g. 5 elements)
- CRS does not have this restriction

Example 2

```
sig A, B, C in Int {}
```

- Kodkod returns $C = \{12\} = \{sum[A] + sum[B]\}$
- CRS returns $C = \{5,6,7\}$ where $plus = \{(1,4,5),(1,5,6),(2,4,6),(2,5,7)\}$

```
fact {
  // A = {1}∪{2}, B = {4}∪{5}
  A = 1 + 2 and B = 4 + 5
  C = plus[A, B]   }
run {} for 6 Int
```

- Kodkod only supports fixed-bitwidth integers (e.g. $length = 6 \Rightarrow [-32, +31]$)
- CRS supports unbounded integers

CRS translation of non-integer signatures

Alloy Language	CRS Translation

univ	// Atom is a new uninterpreted sort
	$Atom$: TYPE
	// the universe set of [$Atom$]
	$atomUniv$: SET OF [$Atom$]

iden	atomIden : SET OF [$Atom, Atom$] $\forall x, y : Atom \,.\, \langle x, y\rangle \in atomIden \Leftrightarrow x = y$
sig A, B {}	A, B : SET OF [$Atom$] $A \cap B = \phi$
sig A_1, ..., A_n **extends** A {}	$A_1, \cdots, A_n$: SET OF [$Atom$] $A_1 \subseteq A, \cdots, A_n \subseteq A$ $A_i \cap A_j = \phi \;, 1 \le i < j \le n$
sig C { f: $A_1 \to \cdots \to A_n$ }	C : SET OF [$Atom$] f : SET OF [$\underbrace{Atom, \cdots, Atom}_{n+1}$] $f \subseteq C \times A_1 \times \cdots \times A_n$

CRS translation of integer signatures

Alloy Language	CRS Translation

sig univInt **in Int** { intIden: univInt }	// UInt is a new uninterpreted sort
	$UInt$: TYPE
	$intUniv$: SET OF [$UInt$]
	// one-to-one mapping from UInt to $\mathbb{Z}$
	$^{-} : UInt \to \mathbb{Z}$
	$intIden$: SET OF [$UInt, UInt$]
	$\forall x, y : UInt \,.\, \langle x, y\rangle \in intIden \Leftrightarrow x = y$

sig A, B **in Int** {}	A, B : SET OF [$UInt$]

// B = {4}∪{5}
B = 4 + 5
	$B = \{u_1\} \cup \{u_2\}$ where $u_1, u_2 \in UInt$
	$\overline{u_1} = 4 \wedge \overline{u_2} = 5$

C = plus[A,B]	C : SET OF [$UInt$] $\forall z : UInt \,.\, z \in C \Rightarrow$ $\exists x, y : UInt \,.\, x \in A \wedge y \in B \wedge \overline{x} + \overline{y} = \overline{z}$ $\forall x, y : UInt \,.\, x \in A \wedge y \in B \Rightarrow$ $\exists z : UInt \,.\, z \in C \wedge \overline{x} + \overline{y} = \overline{z}$

Semantics of arithmetic operations on integer signatures

- Kodkod interprets $plus[A, B]$ where A, B are integer signatures as $plus[sum[A], sum[B]]$. Other operations ($minus, mul, div, rem$) are similar
- Kodkod interprets inequalities $A \; op \; B$ where $op \in \{<, \le, >, \ge\}$ as $sum[A] \; op \; sum[B]$
- CRS interprets $plus[A, B]$ as $\{z \mid \exists\, x \in A, y \in B \,.\, x + y = z\}$. Other operations ($minus, mul, div, rem$) are similar
- CRS interprets inequalities $A \; op \; B$ where $op \in \{<, \le, >, \ge\}$ as $\exists\, x, y \in \mathbb{Z}.\; A = \{x\} \wedge B = \{y\} \wedge (x \; op \; y)$

LaTeX TikZposter