A NEW RELATIONAL SOLVER FOR THE ALLOY ANALYZER

Mudathir Mohamed, Baoluo Meng, Andrew Reynolds and Cesare Tinelli

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

\[
\text{sig} \ B \ () \\
// f: A \to B \text{ is injective}
\text{sig} \ A \{ \ f: \text{disj} \ \text{one} \ B \} \\
// f \text{ is surjective}
\text{fact} \ { \ f[A] = B } \\
// \text{ different elements have different images}
\text{assert} \ \text{assertion} \ { \ \forall \ x,y: A | x \neq y \implies f[x] \neq f[y] \}
\text{check} \ \text{assertion for} \ 5 \ A, 5 \ B
\]

Example 2

\[
\text{sig} \ A, B, C \text{ in Int} \ ()
\]

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

\[
\text{fact} \ { \ // \ A = \{1\} \cup \{2\}, \ B = \{4\} \cup \{5\} \\
A = 1 + 2 \text{ and } B = 4 + 5 \\
C = \text{plus}[A, B] \}
\]

\text{run} \ () \text{ for } 6 \ \text{Int}

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

Semantics of arithmetic operations on integer signatures

• Kodkod interprets \( \text{plus}[A, B] \) where \( A, B \) are integer signatures as \( \text{plus}[\text{sum}[A], \text{sum}[B]] \). Other operations (\( \text{minus}, \text{mul}, \text{div}, \text{rem} \)) are similar
• Kodkod interprets inequalities \( A \leftrightarrow B \) where \( op \in \{<, \leq, >, \geq\} \) as \( \text{sum}[A] \leftrightarrow \text{sum}[B] \)
• CRS interprets \( \text{plus}[A, B] \) as \( \{z | \exists x \in A, y \in B | x + y = z\} \). Other operations (\( \text{minus}, \text{mul}, \text{div}, \text{rem} \)) are similar
• CRS interprets inequalities \( A \leftrightarrow B \) where \( op \in \{<, \leq, >, \geq\} \) as \( \exists x, y \in \mathbb{Z} | A = \{x\} \land B = \{y\} \land (x \leftrightarrow op \ y) \)