ADuct HW 2.1

Apply the decision procedure of T_E for deciding the satisfiability of the following formula

$$g(a) \neq b \wedge f(a) = b \wedge g(b) = a \wedge g(f(a)) = b \wedge f(g(b)) = a$$

where f, g are unary functions and a, b are constants.

We want to apply congruence closure. Therefore we first have to find the set of all subterms S.

$$S = \{a, b, f(a), g(a), g(b), f(g(b)), g(f(a))\}$$

We start the congruence closure algorithm by giving each subterm its own partition.

$$[a], [b], [f(a)], [g(a)], [g(b)], [f(g(b))], [g(f(a))]$$

Now we look at any equality. Let's start with $f(a)=b$. We have to union the two partitions $[f(a)]$ and $[b]$ and do function propagation which gives $g(f(a)) = g(b)$ as $f(a)=b$. Therefore we also union $[g(f(a))]$ and $[g(b)]$.

$$[a], [b, f(a)], [g(a)], [g(b), g(f(a))], [f(g(b))]$$

We look at the next equality, namely $g(b)=a$ and union the partitions of a and $g(b)$. Function propagation also gives us $f(g(b)) = f(a)$ so we also union these.

$$[a, g(b), g(f(a))], [b, f(a), f(g(b))], [g(a)]$$

The next equality $g(f(a))=b$ lets us union $[a, g(b), g(f(a))]$ and $[b, f(a), f(g(b))]$. This time there is no function propagation as neither $f(g(f(a)))$ nor $g(g(f(a)))$ are in S.

$$[a, b, f(a), g(b), f(g(b)), g(f(a))], [g(a)]$$

Now for the last equality: $f(g(b)) = a$. These two subterms are already in the same partition, so nothing changes. We now build the congruence closure and look if any inequalities do not hold. The only inequality given is $g(a) \neq b$ and indeed $g(a)$ and b are in two different partitions. Therefore the given formula is satisfiable.

ADvct HW 2.2.

Let X denote a vector of integer-valued variables.

A linear integer inequality, or simply inequality, over X is a formula $A \cdot X \leq k$, where A is a vector of integer constants and k is an integer constant. For example, $(2, 0, -1) \cdot (x_1, x_2, x_3) \leq 4$ represents the inequality $2 \cdot x_1 - x_3 \leq 4$.

A linear integer inequality clause, or simply inequality clause, over X is a disjunction of inequalities over X. For example, $2 \cdot x_1 - x_3 \leq 4 \vee -x_2 - x_3 \leq 0$ is a clause with two inequalities.

Let C be the following inequality clause over X: $C: a \cdot X \leq k_1 \vee b \cdot X \leq k_2$, with a, b be integer constants (e.g. vectors with only one element) and k_1, k_2 integer constants.

Translate C to a formula D such that: • D is a conjunction of linear integer inequalities over X
• the solutions to X in C and D are the same (that is, C, D are equisatisfiable). Prove the correctness of your translation.

Set D: $(a \cdot w) X \leq (k_1 \cdot w) \wedge (b \cdot (-w+1)) X \leq (k_2 \cdot (-w+1))$

where $w \in \{0, 1\}$ and a, b, k_1, k_2 are as above.

We note that $w = 0 \iff -w+1 = 1$ and $w = 1 \iff -w+1 = 0$.

To show that the solutions to X in C and D are the same we start by showing

X is a solution to $C \Rightarrow X$ is a solution to D:

As X is a solution to C we have that either $a \cdot X \leq k_1$ or $b \cdot X \leq k_2$.

Case $a \cdot X \leq k_1$: We look at the w-variant in which $w = 1$. By simplifying D we get $aX \leq k_1 \wedge 0 \cdot X \leq 0$ which is true as $aX \leq k_1$ is given and $0 \cdot X \leq 0$ is a tautology.

Case $b \cdot X \leq k_2$: Same as above with $w = 0$.

X is solution to $D \Rightarrow X$ is solution to C:

As $w \in \{0, 1\}$ we have that either $w = 0$ or $w = 1$.

Case $w = 0$: X is solution to $D \Rightarrow X$ is solution to $(b(-w+1))X \leq (k_2(-w+1))$ which simplifies to $bX \leq k_2$. Therefore X is a solution to C.

Case $w = 1$: As in case $w = 0$.

We have now showed that the solutions in C and D are the same.

ADuct HW 2.3

Consider the following two formulas

(F1) $b-1=c+3 \wedge f(b)\neq b+1 \wedge read(A, f(c+4)) = c+3 \wedge$

$(read(A, f(b)) = b+2 \vee read(write(A, b+1, f(c+3)), f(c+4)) = c+5)$

(F2) $b=c+3 \wedge f(b)=c-1 \wedge read(A, f(c+3)) = b+1 \wedge$

$(read(A, f(b)) = c \vee read(write(A, b, f(c+3)), f(b)) = c+4)$

where b, c are constants, f is a unary function symbol, A is an array constant, read, write are interpreted in the array theory, and +, −, -1, 1, 2, 3, 4, 5 are interpreted in the standard way over the integers. For each formula (F1) and (F2) above,

(a) Use the Nelson-Oppen decision procedure in conjunction with DPLL-based reasoning in the combination of the theories of arrays, uninterpreted functions, and linear integer arithmetic. Use the decision procedure for the theory of arrays and the theory of uninterpreted functions and use simple mathematical reasoning for deriving new equalities among the constants in the theory of linear integer arithmetics. If the formula is satisfiable, give an interpretation that satisfies the formula.

(b) Encode the formula as an input to the Z3 SMT solver and evaluate Z3 on your encoding. Interpret the result of Z3. Provide the electronic version of your Z3 encoding together with your solution.

ADuct HW 2.3.

(F1) $b-1=c+3 \wedge f(b)\neq b+1 \wedge read(A,f(c+4))=c+3 \wedge (read(A,f(b))=b+2 \vee$

$read(write(A, b+1, f(c+3)), f(c+4)) = c+5)$

a) The formula is of the form $p_1 \wedge p_2 \wedge p_3 \wedge (p_4 \vee p_5)$. Using a SAT solver (or simple reasoning) we get $p_1 \mapsto 1, p_2 \mapsto 1, p_3 \mapsto 1, p_4 \mapsto 0, p_5 \mapsto 1$ as a possible model.

This gives us the following literals in $T_E \cup T_A \cup T_Q$:

$b-1=c+3$; $f(b)\neq b+1$; $read(A,f(c+4))=c+3$; $read(A,f(b))\neq b+2$;

$read(write(A, b+1, f(c+3)), f(c+4)) = c+5$

Now we separate into the three theories:

T_Q: $b-1=c+3$; $x_1=b+1$; $x_2=c+4$; $x_3=c+3$; $x_4=b+2$; $x_5=c+5$

T_E: $f(b)\neq x_1$; $x_6=f(x_2)$; $x_7=f(b)$; $x_8=f(x_3)$

T_A: $read(A, x_6)=x_3$; $read(A, x_7)\neq x_4$; $read(write(A, x_1, x_8), x_6)=x_5$

We rewrite the read as a new function g_A:

T_Q: $b-1=c+3$; $x_1=b+1$; $x_2=c+4$; $x_3=c+3$; $x_4=b+2$; $x_5=c+5$

T_E: $f(b)\neq x_1$; $x_6=f(x_2)$; $x_7=f(b)$; $x_8=f(x_3)$; $g_A(x_6)=x_3$; $g_A(x_7)\neq x_4$

T_A: $read(write(A, x_1, x_8), x_6)=x_5$

Now we derive shared equalities:

$b-1=c+3$ & $x_2=c+4$ $\rightsquigarrow$ $\boxed{x_2=b}$ further we get $x_6=f(x_2)$ & $x_7=f(b)$ $\rightsquigarrow$ $\boxed{x_6=x_7}$

$b-1=c+3$ & $x_5=c+5$ & $x_1=b+1$ $\rightsquigarrow$ $\boxed{x_1=x_5}$

Now we split upon $x_1=x_6$ and $x_1\neq x_6$. We start with $\boxed{x_1=x_6}$:

As $b=x_2$ we have $f(b)=f(x_2)$ with $f(b)\neq x_1=x_6=f(x_2)$ we get a contradiction.

Now for the case $x_1\neq x_6$ we get from $read(write(A,x_1,x_8),x_6)=x_5$ that $g_A(x_6)=x_5$ with $g_A(x_6)\neq x_3$ $\rightsquigarrow$ $\boxed{x_3=x_5}$. This contradicts $x_3=c+3$ & $x_5=c+5$.

Back to the SAT solver! We choose $p_1 \mapsto 1, p_2 \mapsto 1, p_3 \mapsto 1, p_4 \mapsto 1, p_5 \mapsto 0$ as the next model.

$b-1=c+3$; $f(b)\neq b+1$; $read(A,f(c+4))=c+3$; $read(A,f(b))=b+2$;

$read(write(A, b+1, f(c+3)), f(c+4)) \neq c+5$

...

ADuct HW 2.3.

... $T_Q: b-1=c+3;\ x_1=b+1;\ x_2=c+4;\ x_3=c+3;\ x_4=b+2;\ x_5=c+5$

$T_E: f(b)\neq x_1;\ x_6=f(x_2);\ x_7=f(b);\ x_8=f(x_3);\ g_A(x_6)=x_3;\ g_A(x_7)=x_4;\ x_9\neq x_5$

$T_A: read(write(A,x_1,x_8),x_6)=x_9$

Shared Equalities: $\boxed{x_2=b}$; $\boxed{x_6=x_7}$; $\boxed{x_1=x_5}$ as above and $\boxed{x_3=x_4}$ from $x_6=x_7$ & $g_A(x_6)=x_3$ & $g_A(x_7)=x_4$. This however contradicts $x_3=c+3$, $x_4=b+2$ and $b-1=c+3$.

One last time back to our SAT step and to the model $p_1,\dots,p_5\mapsto 1$

$T_Q: b-1=c+3;\ x_1=b+1;\ x_2=c+4;\ x_3=c+3;\ x_4=b+2;\ x_5=c+5$

$T_E: f(b)\neq x_1;\ x_6=f(x_2);\ x_7=f(b);\ x_8=f(x_3);\ g_A(x_6)=x_3;\ g_A(x_7)=x_4$

$T_A: read(write(A,x_1,x_8),x_6)=x_5$

Shared Equalities: $\boxed{x_2=b}$; $\boxed{x_6=x_7}$; $\boxed{x_1=x_5}$; $\boxed{x_3=x_4}$ as above. Same contradiction as above.

We rule out this model in the SAT solver as well and it now returns unsat.

Therefore the formula is unsat.

(F2) $b=c+3 \wedge f(b)=c-1 \wedge read(A,f(c+3))=b+1 \wedge$

$(read(A,f(b))=c \vee read(write(A,b,f(c+3)),f(b))=c+4)$

a) Formula has same form as first one. A possible sat model is $p_1\mapsto 1, p_2\mapsto 1, p_3\mapsto 1, p_4\mapsto 0, p_5\mapsto 1$.

This gives us $b=c+3;\ f(b)=c-1;\ read(A,f(c+3))=b+1;\ read(A,f(b))\neq c;\ read(write(A,b,f(c+3)),f(b))=c+4$

Separation gives us: $T_Q: b=c+3;\ x_1=c-1;\ x_2=c+3;\ x_3=b+1;\ x_4=c+4$

$T_E: f(b)=x_1;\ x_5=f(x_2);\ x_6=f(b);\ g_A(x_5)=x_3;\ g_A(x_6)\neq c$

$T_A: read(write(A,b,x_5),x_6)=x_4$

Shared Equalities: $b=c+3$ & $x_2=c+3 \rightsquigarrow \boxed{b=x_2}$ & $f(b)=x_1$ & $f(x_2)=x_5 \rightsquigarrow \boxed{x_1=x_5}$ $f(b)=x_1$ & $f(b)=x_6 \rightsquigarrow \boxed{x_1=x_6}$ & $x_1=x_5 \rightsquigarrow \boxed{x_5=x_6}$, $x_3=b+1$ & $x_4=c+4$ & $b=c+3$ $\rightsquigarrow \boxed{x_3=x_4}$. We split and consider $b\neq x_6$ first in T_A we now get $g_A(x_6)=x_4$. We get the congruence closure $[c], [x_1, x_5, x_6, f(b), f(x_2)], [x_2, b], [x_3, x_4, g_A(x_5), g_A(x_6)]$

and from T_Q we assign $[c]=0$, $[x_1,\dots]=-1$, $[x_2,b]=3$, $[x_3,\dots]=4$

to get the model $c\mapsto 0, x_1\mapsto -1, x_5\mapsto -1, \dots, f(x_2)\mapsto -1, x_2\mapsto 3, b\mapsto 3, x_3\mapsto 4, \dots, g_A(x_6)\mapsto 4$.

ADuct HW 2.4.

Consider the following formula: $x \neq y \rightarrow f(a) = x \vee f(a) = y$

where x, y are variables, a is a constant, and f is a unary function symbol.

Describe the class of interpretations that make this formula valid.

Consider any domain which contain exactly two elements. Let us name them 1 and 2 (they could have any names). We now consider all interpretations where $x, y, a \in \{1,2\}$ and $f: \{1,2\} \rightarrow \{1,2\}$. Let I be any of these interpretation.

If $I \models x = y$ then the formula is satisfied (by definition of implication).

If $I \models x \neq y$ then either $(x = 1 \wedge y = 2)$ or $(x = 2 \wedge y = 1)$.

Consider the case $x = 1$ and $y = 2$. As f maps to $\{1,2\}$ we have that

$f(a) = 1$, which gives us $f(a) = x$, or

$f(a) = 2$, which gives us $f(a) = y$. In both cases the formula holds.

Now consider the case $x = 2$ and $y = 1$. Once again either

$f(a) = 1$, therefore $f(a) = y$, or

$f(a) = 2$, therefore $f(a) = x$. Again the formula hols in both cases.

As the formula is satisfied for arbitrary interpretations the formula is valid.

Now consider interpretations with domain of only one element e.g. $\{1\}$.

If $x, y \in \{1\}$ we always have $x = 1 = y$, therefore all interpretations (actually there only is one) satisfy the formula, as $x \neq y$ is false.

However if we consider domains with at least three elements (e.g. $\{1,2,3,\ldots\}$) the formula is not valid. To see why we say $f(a) = 1$ (otherwise we rename the domain to set $f(a)$ to be 1). Let I be the interpretation in which $x \mapsto 2$, $y \mapsto 3$, $a \mapsto 1$, $f(a) \mapsto 1$. $x \neq y$ holds in I, but $f(a) = x \vee f(a) = y$ does not, therefore the formula can not be valid.

In summary the class of interpretations in which the formula is valid is the one in which the domain of elements has fewer than three elements.