Veriopt

August 25, 2022

Abstract

The Veriopt project aims to prove the optimization pass of the GraalVM compiler. The GraalVM compiler includes a sophisticated Intermediate Representation (IR) in the form of a sea-of-nodes based graph structure. We first define the IR graph structure in the Isabelle/HOL interactive theorem prover. We subsequently give the evaluation of the structure a semantics based on the current understanding of the purpose of each IR graph node. Optimization phases are then encoded including the static analysis passes required for an optimization. Each optimization phase is proved to be correct by proving that a bisimulation exists between the unoptimized and optimized graphs. The following document has been automatically generated from the Isabelle/HOL source to provide a very comprehensive definition of the semantics and optimizations introduced by the Veriopt project.

Contents

1 Runtime Values and Arithmetic

theory *Values*
  imports
    HOL−Library.Word
    HOL−Library.Signed-Division
    HOL−Library.Float
    HOL−Library.LaTeXsugar
begin

lemma $-((x::float)-y) = (y-x)$
  by *simp*

In order to properly implement the IR semantics we first introduce a type that represents runtime values. These runtime values represent the full range of primitive types currently allowed by our semantics, ranging from basic integer types to object references and arrays.

Note that Java supports 64, 32, 16, 8 signed ints, plus 1 bit (boolean) ints, but during calculations the smaller sizes are sign-extended to 32 bits, so here we model just 32 and 64 bit values.

An object reference is an option type where the *None* object reference points to the static fields. This is examined more closely in our definition of the heap.

type-synonym *int64 = 64 word* — long
type-synonym *int32 = 32 word* — int
type-synonym *int16 = 16 word* — short
type-synonym *int8 = 8 word* — char
type-synonym *int1 = 1 word* — boolean

abbreviation *valid-int-widths* :: *nat set* **where**
  valid-int-widths ≡ *{ 1, 8, 16, 32, 64}*

type-synonym *objref = nat option*

datatype (*discs-sels*) *Value =*
  UndefVal |
  IntVal32 32 word |
  IntVal64 64 word |

  ObjRef objref |
  ObjStr string

Characterise integer values, covering both 32 and 64 bit. If a node has a stamp smaller than 32 bits (16, 8, or 1 bit), then the value will be sign-extended to 32 bits. This is necessary to match what the stamps specify E.g. an 8-bit stamp has a default range of -128..+127. And a 1-bit stamp has a default range of -1..0, surprisingly.

definition *logic-negate* :: (′*a::len*) *word* ⇒ ′*a word* **where**
  logic-negate x = (if x = 0 then 1 else 0)

definition *is-IntVal* :: *Value* ⇒ *bool* **where**
  is-IntVal v = (is-IntVal32 v ∨ is-IntVal64 v)

Extract signed integer values from both 32 and 64 bit.

fun *intval* :: *Value* ⇒ *int* **where**
  intval (IntVal32 v) = sint v |
  intval (IntVal64 v) = sint v

fun *wf-bool* :: *Value* ⇒ *bool* **where**
  wf-bool (IntVal32 v) = (v = 0 ∨ v = 1) |
  wf-bool - = False

fun *val-to-bool* :: *Value* ⇒ *bool* **where**
  val-to-bool (IntVal32 val) = (if val = 0 then False else True) |
  val-to-bool (IntVal64 val) = (if val = 0 then False else True) |
  val-to-bool v = False

fun *bool-to-val* :: *bool* ⇒ *Value* **where**
  bool-to-val True = (IntVal32 1) |
  bool-to-val False = (IntVal32 0)

value *sint(word-of-int (1) :: int1)*

fun *is-int-val* :: *Value* ⇒ *bool* **where**
  is-int-val (IntVal32 v) = True |
  is-int-val (IntVal64 v) = True |
  is-int-val - = False

1.1 Arithmetic Operators

We need to introduce arithmetic operations which agree with the JVM.

Within the JVM, bytecode arithmetic operations are performed on 32 or 64 bit integers, unboxing where appropriate.

The following collection of intval functions correspond to the JVM arithmetic operations. We merge the 32 and 64 bit operations into a single function, even though the stamp of each IRNode tells us exactly what the bit widths will be. These merged functions know to make it easier to do the instantiation of Value as 'plus', etc. It might be worse for reasoning, because it could cause more case analysis, but this does not seem to be a problem in practice.

fun *intval-add* :: *Value* ⇒ *Value* ⇒ *Value* **where**
  intval-add (IntVal32 v1) (IntVal32 v2) = (IntVal32 (v1+v2)) |
  intval-add (IntVal64 v1) (IntVal64 v2) = (IntVal64 (v1+v2)) |

intval-add - - = UndefVal

instantiation *Value* :: *ab-semigroup-add*
begin

definition *plus-Value* :: *Value* ⇒ *Value* ⇒ *Value* **where**
  plus-Value = intval-add

print-locale! *ab-semigroup-add*

instance proof
  fix *a b c* :: *Value*
  show *a + b + c = a + (b + c)*
    apply (*simp add: plus-Value-def*)
    apply (*induction a*; *induction b*; *induction c*; *auto*)
    done
  show *a + b = b + a*
    apply (*simp add: plus-Value-def*)
    apply (*induction a*; *induction b*; *auto*)
    done
qed
end

fun *intval-sub* :: *Value* ⇒ *Value* ⇒ *Value* **where**
  intval-sub (*IntVal32 v1*) (*IntVal32 v2*) = (*IntVal32 (v1−v2)*) |
  intval-sub (*IntVal64 v1*) (*IntVal64 v2*) = (*IntVal64 (v1−v2)*) |
  intval-sub - - = UndefVal

instantiation *Value* :: *minus*
begin

definition *minus-Value* :: *Value* ⇒ *Value* ⇒ *Value* **where**
  minus-Value = intval-sub

instance proof qed
end

fun *intval-mul* :: *Value* ⇒ *Value* ⇒ *Value* **where**
  intval-mul (*IntVal32 v1*) (*IntVal32 v2*) = (*IntVal32 (v1∗v2)*) |
  intval-mul (*IntVal64 v1*) (*IntVal64 v2*) = (*IntVal64 (v1∗v2)*) |
  intval-mul - - = UndefVal

instantiation *Value* :: *times*
begin

definition *times-Value* :: *Value* ⇒ *Value* ⇒ *Value* **where**
  times-Value = intval-mul

instance proof qed
end

fun *intval-div* :: *Value* ⇒ *Value* ⇒ *Value* **where**
  intval-div (*IntVal32 v1*) (*IntVal32 v2*) = (*IntVal32* (*word-of-int*((*sint v1*) *sdiv* (*sint v2*)))) |
  intval-div (*IntVal64 v1*) (*IntVal64 v2*) = (*IntVal64* (*word-of-int*((*sint v1*) *sdiv* (*sint v2*)))) |
  intval-div - - = UndefVal

instantiation *Value* :: *divide*
begin

definition *divide-Value* :: *Value* ⇒ *Value* ⇒ *Value* **where**
  divide-Value = intval-div

instance proof qed
end

fun *intval-mod* :: *Value* ⇒ *Value* ⇒ *Value* **where**
  intval-mod (*IntVal32 v1*) (*IntVal32 v2*) = (*IntVal32* (*word-of-int*((*sint v1*) *smod* (*sint v2*)))) |
  intval-mod (*IntVal64 v1*) (*IntVal64 v2*) = (*IntVal64* (*word-of-int*((*sint v1*) *smod* (*sint v2*)))) |
  intval-mod - - = UndefVal

instantiation *Value* :: *modulo*
begin

definition *modulo-Value* :: *Value* ⇒ *Value* ⇒ *Value* **where**
  modulo-Value = intval-mod

instance proof qed
end

1.2   Bitwise Operators and Comparisons

context
  includes *bit-operations-syntax*
begin

fun *intval-and* :: *Value* ⇒ *Value* ⇒ *Value* **where**

intval-and (*IntVal32 v1*) (*IntVal32 v2*) = (*IntVal32* (*v1 AND v2*)) |
intval-and (*IntVal64 v1*) (*IntVal64 v2*) = (*IntVal64* (*v1 AND v2*)) |
intval-and - - = UndefVal

fun *intval-or* :: *Value* ⇒ *Value* ⇒ *Value* **where**
intval-or (*IntVal32 v1*) (*IntVal32 v2*) = (*IntVal32* (*v1 OR v2*)) |
intval-or (*IntVal64 v1*) (*IntVal64 v2*) = (*IntVal64* (*v1 OR v2*)) |
intval-or - - = UndefVal

fun *intval-xor* :: *Value* ⇒ *Value* ⇒ *Value* **where**
intval-xor (*IntVal32 v1*) (*IntVal32 v2*) = (*IntVal32* (*v1 XOR v2*)) |
intval-xor (*IntVal64 v1*) (*IntVal64 v2*) = (*IntVal64* (*v1 XOR v2*)) |
intval-xor - - = UndefVal

fun *intval-short-circuit-or* :: *Value* ⇒ *Value* ⇒ *Value* **where**
intval-short-circuit-or (*IntVal32 v1*) (*IntVal32 v2*) = *bool-to-val* ((*v1* ≠ *0*) ∨ (*v2* ≠ *0*)) |
intval-short-circuit-or (*IntVal64 v1*) (*IntVal64 v2*) = *bool-to-val* ((*v1* ≠ *0*) ∨ (*v2* ≠ *0*)) |
intval-short-circuit-or - - = UndefVal

fun *intval-equals* :: *Value* ⇒ *Value* ⇒ *Value* **where**
intval-equals (*IntVal32 v1*) (*IntVal32 v2*) = *bool-to-val* (*v1* = *v2*) |
intval-equals (*IntVal64 v1*) (*IntVal64 v2*) = *bool-to-val* (*v1* = *v2*) |
intval-equals - - = UndefVal

fun *intval-less-than* :: *Value* ⇒ *Value* ⇒ *Value* **where**
intval-less-than (*IntVal32 v1*) (*IntVal32 v2*) = *bool-to-val* (*v1* <s *v2*) |
intval-less-than (*IntVal64 v1*) (*IntVal64 v2*) = *bool-to-val* (*v1* <s *v2*) |
intval-less-than - - = UndefVal

fun *intval-below* :: *Value* ⇒ *Value* ⇒ *Value* **where**
intval-below (*IntVal32 v1*) (*IntVal32 v2*) = *bool-to-val* (*v1* < *v2*) |
intval-below (*IntVal64 v1*) (*IntVal64 v2*) = *bool-to-val* (*v1* < *v2*) |
intval-below - - = UndefVal

fun *intval-not* :: *Value* ⇒ *Value* **where**
intval-not (*IntVal32 v*) = (*IntVal32* (*NOT v*)) |
intval-not (*IntVal64 v*) = (*IntVal64* (*NOT v*)) |
intval-not - = UndefVal

fun *intval-negate* :: *Value* ⇒ *Value* **where**
intval-negate (*IntVal32 v*) = *IntVal32* (− *v*) |
intval-negate (*IntVal64 v*) = *IntVal64* (− *v*) |
intval-negate - = UndefVal

fun *intval-abs* :: *Value* ⇒ *Value* **where**
intval-abs (*IntVal32 v*) = (*if* (*v*) <s *0 then* (*IntVal32* (− *v*)) *else* (*IntVal32 v*)) |
intval-abs (*IntVal64 v*) = (*if* (*v*) <s *0 then* (*IntVal64* (− *v*)) *else* (*IntVal64 v*)) |

intval-abs - = UndefVal

fun *intval-conditional* :: *Value* ⇒ *Value* ⇒ *Value* ⇒ *Value* **where**
  intval-conditional cond tv fv = (if (val-to-bool cond) then tv else fv)

fun *intval-logic-negation* :: *Value* ⇒ *Value* **where**
  intval-logic-negation (IntVal32 v) = (IntVal32 (logic-negate v)) |
  intval-logic-negation (IntVal64 v) = (IntVal64 (logic-negate v)) |
  intval-logic-negation - = UndefVal

lemma *intval-eq32*:
  assumes *intval-equals (IntVal32 v1) v2 ≠ UndefVal*
  shows *is-IntVal32 v2*
 by (*metis Value.exhaust-disc assms intval-equals.simps(10) intval-equals.simps(12)*
intval-equals.simps(15) intval-equals.simps(16) is-IntVal64-def is-ObjRef-def is-ObjStr-def)

lemma *intval-eq32-simp*:
  assumes *intval-equals (IntVal32 v1) v2 ≠ UndefVal*
  shows *intval-equals (IntVal32 v1) v2 = bool-to-val (v1 = un-IntVal32 v2)*
  by (*metis Value.collapse(1) assms intval-eq32 intval-equals.simps(1)*)

1.3   Narrowing and Widening Operators

Note: we allow these operators to have inBits=outBits, because the Graal compiler also seems to allow that case, even though it should rarely / never arise in practice.

When narrowing to less than 32 bits, we sign extend back to 32 bits, because we always represent integer values as either 32 or 64 bits.

fun *narrow-helper* :: *nat* ⇒ *nat* ⇒ *int32* ⇒ *Value* **where**
  narrow-helper inBits outBits val =
    (if outBits ≤ inBits ∧ outBits ≤ 32 ∧
      outBits ∈ valid-int-widths ∧
      inBits ∈ valid-int-widths
    then IntVal32 (signed-take-bit (outBits − 1) val)
    else UndefVal)

value *sint(signed-take-bit 0 (1 :: int32))*

fun *intval-narrow* :: *nat* ⇒ *nat* ⇒ *Value* ⇒ *Value* **where**
  intval-narrow inBits outBits (IntVal32 v) =
    (if inBits = 64
     then UndefVal
     else narrow-helper inBits outBits v) |
  intval-narrow inBits outBits (IntVal64 v) =
    (if inBits = 64
     then (if outBits = 64
        then IntVal64 v
        else narrow-helper inBits outBits (scast v))

else UndefVal) |
  intval-narrow - - - = UndefVal

value *intval*(*intval-narrow 16 8* (*IntVal32* (*512* − *2*)))

fun *choose-32-64* :: *nat* ⇒ *int64* ⇒ *Value* **where**
  choose-32-64 outBits v = (*if outBits = 64 then* (*IntVal64 v*) *else* (*IntVal32* (*scast v*)))

value *sint* (*signed-take-bit 7* ((*256* + *128*) :: *int64*))

fun *sign-extend-helper* :: *nat* ⇒ *nat* ⇒ *int32* ⇒ *Value* **where**
  sign-extend-helper inBits outBits val =
    (*if inBits ≤ outBits ∧ inBits ≤ 32 ∧*
        outBits ∈ valid-int-widths ∧
        inBits ∈ valid-int-widths
      then
        (*if outBits = 64*
          then IntVal64 (*scast* (*signed-take-bit* (*inBits* − *1*) *val*))
          else IntVal32 (*signed-take-bit* (*inBits* − *1*) *val*))
      else UndefVal)

fun *intval-sign-extend* :: *nat* ⇒ *nat* ⇒ *Value* ⇒ *Value* **where**
  intval-sign-extend inBits outBits (*IntVal32 v*) *=*
    sign-extend-helper inBits outBits v |
  intval-sign-extend inBits outBits (*IntVal64 v*) *=*
    (*if inBits=64 ∧ outBits=64 then IntVal64 v else UndefVal*) |
  intval-sign-extend - - - = UndefVal

fun *zero-extend-helper* :: *nat* ⇒ *nat* ⇒ *int32* ⇒ *Value* **where**
  zero-extend-helper inBits outBits val =
    (*if inBits ≤ outBits ∧ inBits ≤ 32 ∧*
        outBits ∈ valid-int-widths ∧
        inBits ∈ valid-int-widths
      then
        (*if outBits = 64*
          then IntVal64 (*ucast* (*take-bit inBits val*))
          else IntVal32 (*take-bit inBits val*))
      else UndefVal)

fun *intval-zero-extend* :: *nat* ⇒ *nat* ⇒ *Value* ⇒ *Value* **where**
  intval-zero-extend inBits outBits (*IntVal32 v*) *=*
    zero-extend-helper inBits outBits v |
  intval-zero-extend inBits outBits (*IntVal64 v*) *=*
    (*if inBits=64 ∧ outBits=64 then IntVal64 v else UndefVal*) |
  intval-zero-extend - - - = UndefVal

10

Some well-formedness results to help reasoning about narrowing and widening operators

lemma *narrow-helper-ok*:
  assumes *narrow-helper inBits outBits val $\neq$ UndefVal*
  shows *$0 <$ outBits $\wedge$ outBits $\leq$ 32 $\wedge$*
      outBits $\leq$ inBits $\wedge$
      outBits $\in$ valid-int-widths $\wedge$
      inBits $\in$ valid-int-widths
  using *assms narrow-helper.simps neq0-conv* **by** *fastforce*

lemma *intval-narrow-ok*:
  assumes *intval-narrow inBits outBits val $\neq$ UndefVal*
  shows *$0 <$ outBits $\wedge$*
      outBits $\leq$ inBits $\wedge$
      outBits $\in$ valid-int-widths $\wedge$
      inBits $\in$ valid-int-widths
  using *assms narrow-helper-ok intval-narrow.simps neq0-conv*
 by *(smt (verit, best) insertCI intval-sign-extend.elims order-le-less zero-neq-numeral)*

lemma *narrow-takes-64*:
  assumes *result = intval-narrow inBits outBits value*
  assumes *result $\neq$ UndefVal*
  shows *is-IntVal64 value = (inBits = 64)*
  using *assms* **by** *(cases value; simp; presburger)*

lemma *narrow-gives-64*:
  assumes *result = intval-narrow inBits outBits value*
  assumes *result $\neq$ UndefVal*
  shows *is-IntVal64 result = (outBits = 64)*
  using *assms*
 by *(smt (verit, best) Value.case-eq-if Value.discI(1) Value.discI(2) Value.disc-eq-case(3) add-diff-cancel-left' diff-is-0-eq intval-narrow.elims narrow-helper.simps numeral-Bit0 zero-neq-numeral)*

lemma *sign-extend-helper-ok*:
  assumes *sign-extend-helper inBits outBits val $\neq$ UndefVal*
  shows *$0 <$ inBits $\wedge$ inBits $\leq$ 32 $\wedge$*
      inBits $\leq$ outBits $\wedge$
      outBits $\in$ valid-int-widths $\wedge$
      inBits $\in$ valid-int-widths
  using *assms sign-extend-helper.simps neq0-conv* **by** *fastforce*

lemma *intval-sign-extend-ok*:
  assumes *intval-sign-extend inBits outBits val $\neq$ UndefVal*
  shows *$0 <$ inBits $\wedge$*
      inBits $\leq$ outBits $\wedge$
      outBits $\in$ valid-int-widths $\wedge$

$inBits \in valid\text{-}int\text{-}widths$
using *assms sign-extend-helper-ok intval-sign-extend.simps neq0-conv*
by (*smt* (*verit, best*) *insertCI intval-sign-extend.elims order-le-less zero-neq-numeral*)

lemma *zero-extend-helper-ok*:
  assumes *zero-extend-helper inBits outBits val* $\neq$ *UndefVal*
  shows $0 < inBits \wedge inBits \leq 32 \wedge$
      $inBits \leq outBits \wedge$
      $outBits \in valid\text{-}int\text{-}widths \wedge$
      $inBits \in valid\text{-}int\text{-}widths$
  using *assms zero-extend-helper.simps neq0-conv* **by** *fastforce*

lemma *intval-zero-extend-ok*:
  assumes *intval-zero-extend inBits outBits val* $\neq$ *UndefVal*
  shows $0 < inBits \wedge$
      $inBits \leq outBits \wedge$
      $outBits \in valid\text{-}int\text{-}widths \wedge$
      $inBits \in valid\text{-}int\text{-}widths$
  using *assms zero-extend-helper-ok intval-zero-extend.simps neq0-conv*
  by (*smt* (*verit, best*) *insertCI intval-zero-extend.elims order-le-less zero-neq-numeral*)

1.4 Bit-Shifting Operators

definition *shiftl* (**infix** $<<$ *75*) **where**
  shiftl w n = (*push-bit n*) *w*

lemma *shiftl-power*[*simp*]: $(x::('a::len)\ word) * (2\ \hat{}\ j) = x << j$
  unfolding *shiftl-def* **apply** (*induction j*)
   apply *simp* **unfolding** *funpow-Suc-right*
  by (*metis* (*no-types, opaque-lifting*) *push-bit-eq-mult*)

lemma $(x::('a::len)\ word) * ((2\ \hat{}\ j) + 1) = x << j + x$
  by (*simp add: distrib-left*)

lemma $(x::('a::len)\ word) * ((2\ \hat{}\ j) - 1) = x << j - x$
  by (*simp add: right-diff-distrib*)

lemma $(x::('a::len)\ word) * ((2\hat{}j) + (2\hat{}k)) = x << j + x << k$
  by (*simp add: distrib-left*)

lemma $(x::('a::len)\ word) * ((2\hat{}j) - (2\hat{}k)) = x << j - x << k$
  by (*simp add: right-diff-distrib*)

definition *shiftr* (**infix** $>>>$ *75*) **where**
  shiftr w n = (*drop-bit n*) *w*

value $(255 :: 8\ word) >>> (2 :: nat)$

definition *signed-shiftr* :: *′a* :: *len word* ⇒ *nat* ⇒ *′a* :: *len word* (**infix** *>> 75*)
where
  signed-shiftr w n = word-of-int ((sint w) div (2 ^ n))

value (*128* :: *8 word*) *>> 2*

Note that Java shift operators use unary numeric promotion, unlike other
binary operators, which use binary numeric promotion (see the Java lan-
guage reference manual). This means that the left-hand input determines
the output size, while the right-hand input can be any size.

fun *intval-left-shift* :: *Value* ⇒ *Value* ⇒ *Value* **where**
  intval-left-shift (*IntVal32 v1*) (*IntVal32 v2*) = *IntVal32* (*v1 << unat (v2 AND*
0x1f)) |
  intval-left-shift (*IntVal32 v1*) (*IntVal64 v2*) = *IntVal32* (*v1 << unat (v2 AND*
0x1f)) |
  intval-left-shift (*IntVal64 v1*) (*IntVal32 v2*) = *IntVal64* (*v1 << unat (v2 AND*
0x3f)) |
  intval-left-shift (*IntVal64 v1*) (*IntVal64 v2*) = *IntVal64* (*v1 << unat (v2 AND*
0x3f)) |
  intval-left-shift - - = UndefVal

fun *intval-right-shift* :: *Value* ⇒ *Value* ⇒ *Value* **where**
  intval-right-shift (*IntVal32 v1*) (*IntVal32 v2*) = *IntVal32* (*v1 >> unat (v2 AND*
0x1f)) |
  intval-right-shift (*IntVal32 v1*) (*IntVal64 v2*) = *IntVal32* (*v1 >> unat (v2 AND*
0x1f)) |
  intval-right-shift (*IntVal64 v1*) (*IntVal32 v2*) = *IntVal64* (*v1 >> unat (v2 AND*
0x3f)) |
  intval-right-shift (*IntVal64 v1*) (*IntVal64 v2*) = *IntVal64* (*v1 >> unat (v2 AND*
0x3f)) |
  intval-right-shift - - = UndefVal

fun *intval-uright-shift* :: *Value* ⇒ *Value* ⇒ *Value* **where**
  intval-uright-shift (*IntVal32 v1*) (*IntVal32 v2*) = *IntVal32* (*v1 >>> unat (v2*
AND 0x1f)) |
  intval-uright-shift (*IntVal32 v1*) (*IntVal64 v2*) = *IntVal32* (*v1 >>> unat (v2*
AND 0x1f)) |
  intval-uright-shift (*IntVal64 v1*) (*IntVal32 v2*) = *IntVal64* (*v1 >>> unat (v2*
AND 0x3f)) |
  intval-uright-shift (*IntVal64 v1*) (*IntVal64 v2*) = *IntVal64* (*v1 >>> unat (v2*
AND 0x3f)) |
  intval-uright-shift - - = UndefVal

end

2 Examples of Narrowing / Widening Functions

experiment begin
corollary *intval-narrow 32 8 (IntVal32 (256 + 128)) = IntVal32 (−128)* **by** *simp*
corollary *intval-narrow 32 8 (IntVal32 (−2)) = IntVal32 (−2)* **by** *simp*
corollary *intval-narrow 32 1 (IntVal32 (−2)) = IntVal32 0*   **by** *simp*
corollary *intval-narrow 32 1 (IntVal32 (−3)) = IntVal32 (−1)* **by** *simp*

corollary *intval-narrow 32 8 (IntVal64 (−2)) = UndefVal* **by** *simp*
corollary *intval-narrow 64 8 (IntVal32 (−2)) = UndefVal* **by** *simp*
corollary *intval-narrow 64 8 (IntVal64 (−2)) = IntVal32 (−2)* **by** *simp*
corollary *intval-narrow 64 8 (IntVal64 (256+127)) = IntVal32 127* **by** *simp*
corollary *intval-narrow 64 32 (IntVal64 (−2)) = IntVal32 (−2)* **by** *simp*
corollary *intval-narrow 64 64 (IntVal64 (−2)) = IntVal64 (−2)* **by** *simp*
end

experiment begin
corollary *intval-sign-extend 8 32 (IntVal32 (256 + 128)) = IntVal32 (−128)* **by** *simp*
corollary *intval-sign-extend 8 32 (IntVal32 (−2)) = IntVal32 (−2)* **by** *simp*
corollary *intval-sign-extend 1 32 (IntVal32 (−2)) = IntVal32 0*   **by** *simp*
corollary *intval-sign-extend 1 32 (IntVal32 (−3)) = IntVal32 (−1)* **by** *simp*

corollary *intval-sign-extend 8 32 (IntVal64 (−2)) = UndefVal* **by** *simp*
corollary *intval-sign-extend 8 64 (IntVal64 (−2)) = UndefVal* **by** *simp*
corollary *intval-sign-extend 8 64 (IntVal32 (−2)) = IntVal64 (−2)* **by** *simp*
corollary *intval-sign-extend 32 64 (IntVal32 (−2)) = IntVal64 (−2)* **by** *simp*
corollary *intval-sign-extend 64 64 (IntVal64 (−2)) = IntVal64 (−2)* **by** *simp*
end

experiment begin
corollary *intval-zero-extend 8 32 (IntVal32 (256 + 128)) = IntVal32 128* **by** *simp*
corollary *intval-zero-extend 8 32 (IntVal32 (−2)) = IntVal32 254* **by** *simp*
corollary *intval-zero-extend 1 32 (IntVal32 (−1)) = IntVal32 1*   **by** *simp*
corollary *intval-zero-extend 1 32 (IntVal32 (−2)) = IntVal32 0*   **by** *simp*

corollary *intval-zero-extend 8 32 (IntVal64 (−2)) = UndefVal* **by** *simp*
corollary *intval-zero-extend 8 64 (IntVal64 (−2)) = UndefVal* **by** *simp*
corollary *intval-zero-extend 8 64 (IntVal32 (−2)) = IntVal64 254* **by** *simp*
corollary *intval-zero-extend 32 64 (IntVal32 (−2)) = IntVal64 4294967294* **by** *simp*
end

lemma *intval-add-sym*:
  shows *intval-add a b = intval-add b a*
  by (*induction a*; *induction b*; *auto*)

code-deps *intval-add*
code-thms *intval-add*

lemma *intval-add* (*IntVal32* (*2^31−1*)) (*IntVal32* (*2^31−1*)) = *IntVal32* (*−2*)
  by *eval*
lemma *intval-add* (*IntVal64* (*2^31−1*)) (*IntVal64* (*2^31−1*)) = *IntVal64 4294967294*
  by *eval*

end

3 Nodes

3.1 Types of Nodes

theory *IRNodes*
  imports
    Values
begin

The GraalVM IR is represented using a graph data structure. Here we define the nodes that are contained within the graph. Each node represents a Node subclass in the GraalVM compiler, the node classes have annotated fields to indicate input and successor edges.

We represent these classes with each IRNode constructor explicitly labelling a reference to the node IDs that it stores as inputs and successors.

The inputs_of and successors_of functions partition those labelled references into input edges and successor edges of a node.

To identify each Node, we use a simple natural number index. Zero is always the start node in a graph. For human readability, within nodes we write INPUT (or special case thereof) instead of ID for input edges, and SUCC instead of ID for control-flow successor edges. Optional edges are handled as "INPUT option" etc.

type-synonym *ID = nat*
type-synonym *INPUT = ID*
type-synonym *INPUT-ASSOC = ID*
type-synonym *INPUT-STATE = ID*
type-synonym *INPUT-GUARD = ID*
type-synonym *INPUT-COND = ID*

type-synonym *INPUT-EXT = ID*
type-synonym *SUCC = ID*

datatype (*discs-sels*) *IRNode =*
  AbsNode (*ir-value*: *INPUT*)
  | *AddNode* (*ir-x*: *INPUT*) (*ir-y*: *INPUT*)
  | *AndNode* (*ir-x*: *INPUT*) (*ir-y*: *INPUT*)
  | *BeginNode* (*ir-next*: *SUCC*)
  | *BytecodeExceptionNode* (*ir-arguments*: *INPUT list*) (*ir-stateAfter-opt*: *INPUT-STATE option*) (*ir-next*: *SUCC*)
  | *ConditionalNode* (*ir-condition*: *INPUT-COND*) (*ir-trueValue*: *INPUT*) (*ir-falseValue*: *INPUT*)
  | *ConstantNode* (*ir-const*: *Value*)
  | *DynamicNewArrayNode* (*ir-elementType*: *INPUT*) (*ir-length*: *INPUT*) (*ir-voidClass-opt*: *INPUT option*) (*ir-stateBefore-opt*: *INPUT-STATE option*) (*ir-next*: *SUCC*)
  | *EndNode*
  | *ExceptionObjectNode* (*ir-stateAfter-opt*: *INPUT-STATE option*) (*ir-next*: *SUCC*)

  | *FrameState* (*ir-monitorIds*: *INPUT-ASSOC list*) (*ir-outerFrameState-opt*: *INPUT-STATE option*) (*ir-values-opt*: *INPUT list option*) (*ir-virtualObjectMappings-opt*: *INPUT-STATE list option*)
  | *IfNode* (*ir-condition*: *INPUT-COND*) (*ir-trueSuccessor*: *SUCC*) (*ir-falseSuccessor*: *SUCC*)
  | *IntegerBelowNode* (*ir-x*: *INPUT*) (*ir-y*: *INPUT*)
  | *IntegerEqualsNode* (*ir-x*: *INPUT*) (*ir-y*: *INPUT*)
  | *IntegerLessThanNode* (*ir-x*: *INPUT*) (*ir-y*: *INPUT*)
  | *InvokeNode* (*ir-nid*: *ID*) (*ir-callTarget*: *INPUT-EXT*) (*ir-classInit-opt*: *INPUT option*) (*ir-stateDuring-opt*: *INPUT-STATE option*) (*ir-stateAfter-opt*: *INPUT-STATE option*) (*ir-next*: *SUCC*)
  | *InvokeWithExceptionNode* (*ir-nid*: *ID*) (*ir-callTarget*: *INPUT-EXT*) (*ir-classInit-opt*: *INPUT option*) (*ir-stateDuring-opt*: *INPUT-STATE option*) (*ir-stateAfter-opt*: *INPUT-STATE option*) (*ir-next*: *SUCC*) (*ir-exceptionEdge*: *SUCC*)
  | *IsNullNode* (*ir-value*: *INPUT*)
  | *KillingBeginNode* (*ir-next*: *SUCC*)
  | *LeftShiftNode* (*ir-x*: *INPUT*) (*ir-y*: *INPUT*)
  | *LoadFieldNode* (*ir-nid*: *ID*) (*ir-field*: *string*) (*ir-object-opt*: *INPUT option*) (*ir-next*: *SUCC*)
  | *LogicNegationNode* (*ir-value*: *INPUT-COND*)
  | *LoopBeginNode* (*ir-ends*: *INPUT-ASSOC list*) (*ir-overflowGuard-opt*: *INPUT-GUARD option*) (*ir-stateAfter-opt*: *INPUT-STATE option*) (*ir-next*: *SUCC*)
  | *LoopEndNode* (*ir-loopBegin*: *INPUT-ASSOC*)
  | *LoopExitNode* (*ir-loopBegin*: *INPUT-ASSOC*) (*ir-stateAfter-opt*: *INPUT-STATE option*) (*ir-next*: *SUCC*)
  | *MergeNode* (*ir-ends*: *INPUT-ASSOC list*) (*ir-stateAfter-opt*: *INPUT-STATE option*) (*ir-next*: *SUCC*)
  | *MethodCallTargetNode* (*ir-targetMethod*: *string*) (*ir-arguments*: *INPUT list*)
  | *MulNode* (*ir-x*: *INPUT*) (*ir-y*: *INPUT*)
  | *NarrowNode* (*ir-inputBits*: *nat*) (*ir-resultBits*: *nat*) (*ir-value*: *INPUT*)

| *NegateNode* (*ir-value*: *INPUT*)
| *NewArrayNode* (*ir-length*: *INPUT*) (*ir-stateBefore-opt*: *INPUT-STATE option*)
(*ir-next*: *SUCC*)
| *NewInstanceNode* (*ir-nid*: *ID*) (*ir-instanceClass*: *string*) (*ir-stateBefore-opt*: *IN-PUT-STATE option*) (*ir-next*: *SUCC*)
| *NotNode* (*ir-value*: *INPUT*)
| *OrNode* (*ir-x*: *INPUT*) (*ir-y*: *INPUT*)
| *ParameterNode* (*ir-index*: *nat*)
| *PiNode* (*ir-object*: *INPUT*) (*ir-guard-opt*: *INPUT-GUARD option*)
| *ReturnNode* (*ir-result-opt*: *INPUT option*) (*ir-memoryMap-opt*: *INPUT-EXT option*)
| *RightShiftNode* (*ir-x*: *INPUT*) (*ir-y*: *INPUT*)
| *ShortCircuitOrNode* (*ir-x*: *INPUT-COND*) (*ir-y*: *INPUT-COND*)
| *SignExtendNode* (*ir-inputBits*: *nat*) (*ir-resultBits*: *nat*) (*ir-value*: *INPUT*)
| *SignedDivNode* (*ir-nid*: *ID*) (*ir-x*: *INPUT*) (*ir-y*: *INPUT*) (*ir-zeroCheck-opt*: *IN-PUT-GUARD option*) (*ir-stateBefore-opt*: *INPUT-STATE option*) (*ir-next*: *SUCC*)

| *SignedRemNode* (*ir-nid*: *ID*) (*ir-x*: *INPUT*) (*ir-y*: *INPUT*) (*ir-zeroCheck-opt*: *INPUT-GUARD option*) (*ir-stateBefore-opt*: *INPUT-STATE option*) (*ir-next*: *SUCC*)

| *StartNode* (*ir-stateAfter-opt*: *INPUT-STATE option*) (*ir-next*: *SUCC*)
| *StoreFieldNode* (*ir-nid*: *ID*) (*ir-field*: *string*) (*ir-value*: *INPUT*) (*ir-stateAfter-opt*: *INPUT-STATE option*) (*ir-object-opt*: *INPUT option*) (*ir-next*: *SUCC*)
| *SubNode* (*ir-x*: *INPUT*) (*ir-y*: *INPUT*)
| *UnsignedRightShiftNode* (*ir-x*: *INPUT*) (*ir-y*: *INPUT*)
| *UnwindNode* (*ir-exception*: *INPUT*)
| *ValuePhiNode* (*ir-nid*: *ID*) (*ir-values*: *INPUT list*) (*ir-merge*: *INPUT-ASSOC*)
| *ValueProxyNode* (*ir-value*: *INPUT*) (*ir-loopExit*: *INPUT-ASSOC*)
| *XorNode* (*ir-x*: *INPUT*) (*ir-y*: *INPUT*)
| *ZeroExtendNode* (*ir-inputBits*: *nat*) (*ir-resultBits*: *nat*) (*ir-value*: *INPUT*)
| *NoNode*

| *RefNode* (*ir-ref*:*ID*)

fun *opt-to-list* :: $'a$ *option* $\Rightarrow$ $'a$ *list* **where**
  opt-to-list None = [] |
  opt-to-list (*Some v*) = [*v*]

fun *opt-list-to-list* :: $'a$ *list option* $\Rightarrow$ $'a$ *list* **where**
  opt-list-to-list None = [] |
  opt-list-to-list (*Some x*) = *x*

The following functions, inputs_of and successors_of, are automatically generated from the GraalVM compiler. Their purpose is to partition the node edges into input or successor edges.

fun *inputs-of* :: *IRNode* ⇒ *ID list* **where**
  inputs-of-AbsNode:
  inputs-of (*AbsNode value*) = [*value*] |
  inputs-of-AddNode:
  inputs-of (*AddNode x y*) = [*x, y*] |
  inputs-of-AndNode:
  inputs-of (*AndNode x y*) = [*x, y*] |
  inputs-of-BeginNode:
  inputs-of (*BeginNode next*) = [] |
  inputs-of-BytecodeExceptionNode:
   inputs-of (*BytecodeExceptionNode arguments stateAfter next*) = *arguments* @
(*opt-to-list stateAfter*) |
  inputs-of-ConditionalNode:
   inputs-of (*ConditionalNode condition trueValue falseValue*) = [*condition, true-
Value, falseValue*] |
  inputs-of-ConstantNode:
  inputs-of (*ConstantNode const*) = [] |
  inputs-of-DynamicNewArrayNode:
   inputs-of (*DynamicNewArrayNode elementType length0 voidClass stateBefore
next*) = [*elementType, length0*] @ (*opt-to-list voidClass*) @ (*opt-to-list stateBefore*)
|
  inputs-of-EndNode:
  inputs-of (*EndNode*) = [] |
  inputs-of-ExceptionObjectNode:
  inputs-of (*ExceptionObjectNode stateAfter next*) = (*opt-to-list stateAfter*) |
  inputs-of-FrameState:
   inputs-of (*FrameState monitorIds outerFrameState values virtualObjectMappings*)
= *monitorIds* @ (*opt-to-list outerFrameState*) @ (*opt-list-to-list values*) @ (*opt-list-to-list
virtualObjectMappings*) |
  inputs-of-IfNode:
  inputs-of (*IfNode condition trueSuccessor falseSuccessor*) = [*condition*] |
  inputs-of-IntegerBelowNode:
  inputs-of (*IntegerBelowNode x y*) = [*x, y*] |
  inputs-of-IntegerEqualsNode:
  inputs-of (*IntegerEqualsNode x y*) = [*x, y*] |
  inputs-of-IntegerLessThanNode:
  inputs-of (*IntegerLessThanNode x y*) = [*x, y*] |
  inputs-of-InvokeNode:
   inputs-of (*InvokeNode nid0 callTarget classInit stateDuring stateAfter next*)
= *callTarget* # (*opt-to-list classInit*) @ (*opt-to-list stateDuring*) @ (*opt-to-list
stateAfter*) |
  inputs-of-InvokeWithExceptionNode:
  inputs-of (*InvokeWithExceptionNode nid0 callTarget classInit stateDuring stateAfter
next exceptionEdge*) = *callTarget* # (*opt-to-list classInit*) @ (*opt-to-list stateDur-
ing*) @ (*opt-to-list stateAfter*) |
  inputs-of-IsNullNode:
  inputs-of (*IsNullNode value*) = [*value*] |
  inputs-of-KillingBeginNode:
  inputs-of (*KillingBeginNode next*) = [] |

inputs-of-LeftShiftNode:
inputs-of (*LeftShiftNode x y*) = [*x, y*] |
inputs-of-LoadFieldNode:
inputs-of (*LoadFieldNode nid0 field object next*) = (*opt-to-list object*) |
inputs-of-LogicNegationNode:
inputs-of (*LogicNegationNode value*) = [*value*] |
inputs-of-LoopBeginNode:
inputs-of (*LoopBeginNode ends overflowGuard stateAfter next*) = *ends* @ (*opt-to-list overflowGuard*) @ (*opt-to-list stateAfter*) |
inputs-of-LoopEndNode:
inputs-of (*LoopEndNode loopBegin*) = [*loopBegin*] |
inputs-of-LoopExitNode:
inputs-of (*LoopExitNode loopBegin stateAfter next*) = *loopBegin* # (*opt-to-list stateAfter*) |
inputs-of-MergeNode:
inputs-of (*MergeNode ends stateAfter next*) = *ends* @ (*opt-to-list stateAfter*) |
inputs-of-MethodCallTargetNode:
inputs-of (*MethodCallTargetNode targetMethod arguments*) = *arguments* |
inputs-of-MulNode:
inputs-of (*MulNode x y*) = [*x, y*] |
inputs-of-NarrowNode:
inputs-of (*NarrowNode inputBits resultBits value*) = [*value*] |
inputs-of-NegateNode:
inputs-of (*NegateNode value*) = [*value*] |
inputs-of-NewArrayNode:
inputs-of (*NewArrayNode length0 stateBefore next*) = *length0* # (*opt-to-list stateBefore*) |
inputs-of-NewInstanceNode:
inputs-of (*NewInstanceNode nid0 instanceClass stateBefore next*) = (*opt-to-list stateBefore*) |
inputs-of-NotNode:
inputs-of (*NotNode value*) = [*value*] |
inputs-of-OrNode:
inputs-of (*OrNode x y*) = [*x, y*] |
inputs-of-ParameterNode:
inputs-of (*ParameterNode index*) = [] |
inputs-of-PiNode:
inputs-of (*PiNode object guard*) = *object* # (*opt-to-list guard*) |
inputs-of-ReturnNode:
inputs-of (*ReturnNode result memoryMap*) = (*opt-to-list result*) @ (*opt-to-list memoryMap*) |
inputs-of-RightShiftNode:
inputs-of (*RightShiftNode x y*) = [*x, y*] |
inputs-of-ShortCircuitOrNode:
inputs-of (*ShortCircuitOrNode x y*) = [*x, y*] |
inputs-of-SignExtendNode:
inputs-of (*SignExtendNode inputBits resultBits value*) = [*value*] |
inputs-of-SignedDivNode:
inputs-of (*SignedDivNode nid0 x y zeroCheck stateBefore next*) = [*x, y*] @

(*opt-to-list zeroCheck*) @ (*opt-to-list stateBefore*) |
  inputs-of-SignedRemNode:
   inputs-of (*SignedRemNode nid0 x y zeroCheck stateBefore next*) = [*x*, *y*] @
(*opt-to-list zeroCheck*) @ (*opt-to-list stateBefore*) |
  inputs-of-StartNode:
  inputs-of (*StartNode stateAfter next*) = (*opt-to-list stateAfter*) |
  inputs-of-StoreFieldNode:
   inputs-of (*StoreFieldNode nid0 field value stateAfter object next*) = *value* #
(*opt-to-list stateAfter*) @ (*opt-to-list object*) |
  inputs-of-SubNode:
  inputs-of (*SubNode x y*) = [*x*, *y*] |
  inputs-of-UnsignedRightShiftNode:
  inputs-of (*UnsignedRightShiftNode x y*) = [*x*, *y*] |
  inputs-of-UnwindNode:
  inputs-of (*UnwindNode exception*) = [*exception*] |
  inputs-of-ValuePhiNode:
  inputs-of (*ValuePhiNode nid0 values merge*) = *merge* # *values* |
  inputs-of-ValueProxyNode:
  inputs-of (*ValueProxyNode value loopExit*) = [*value*, *loopExit*] |
  inputs-of-XorNode:
  inputs-of (*XorNode x y*) = [*x*, *y*] |
  inputs-of-ZeroExtendNode:
  inputs-of (*ZeroExtendNode inputBits resultBits value*) = [*value*] |
  inputs-of-NoNode: *inputs-of* (*NoNode*) = [] |

  inputs-of-RefNode: *inputs-of* (*RefNode ref*) = [*ref*]

fun *successors-of* :: *IRNode* ⇒ *ID list* **where**
  successors-of-AbsNode:
  successors-of (*AbsNode value*) = [] |
  successors-of-AddNode:
  successors-of (*AddNode x y*) = [] |
  successors-of-AndNode:
  successors-of (*AndNode x y*) = [] |
  successors-of-BeginNode:
  successors-of (*BeginNode next*) = [*next*] |
  successors-of-BytecodeExceptionNode:
  successors-of (*BytecodeExceptionNode arguments stateAfter next*) = [*next*] |
  successors-of-ConditionalNode:
  successors-of (*ConditionalNode condition trueValue falseValue*) = [] |
  successors-of-ConstantNode:
  successors-of (*ConstantNode const*) = [] |
  successors-of-DynamicNewArrayNode:
  successors-of (*DynamicNewArrayNode elementType length0 voidClass stateBefore
next*) = [*next*] |
  successors-of-EndNode:
  successors-of (*EndNode*) = [] |

successors-of-ExceptionObjectNode:
successors-of (*ExceptionObjectNode stateAfter next*) = [*next*] |
successors-of-FrameState:
successors-of (*FrameState monitorIds outerFrameState values virtualObjectMappings*) = [] |
successors-of-IfNode:
successors-of (*IfNode condition trueSuccessor falseSuccessor*) = [*trueSuccessor, falseSuccessor*] |
successors-of-IntegerBelowNode:
successors-of (*IntegerBelowNode x y*) = [] |
successors-of-IntegerEqualsNode:
successors-of (*IntegerEqualsNode x y*) = [] |
successors-of-IntegerLessThanNode:
successors-of (*IntegerLessThanNode x y*) = [] |
successors-of-InvokeNode:
successors-of (*InvokeNode nid0 callTarget classInit stateDuring stateAfter next*) = [*next*] |
successors-of-InvokeWithExceptionNode:
successors-of (*InvokeWithExceptionNode nid0 callTarget classInit stateDuring stateAfter next exceptionEdge*) = [*next, exceptionEdge*] |
successors-of-IsNullNode:
successors-of (*IsNullNode value*) = [] |
successors-of-KillingBeginNode:
successors-of (*KillingBeginNode next*) = [*next*] |
successors-of-LeftShiftNode:
successors-of (*LeftShiftNode x y*) = [] |
successors-of-LoadFieldNode:
successors-of (*LoadFieldNode nid0 field object next*) = [*next*] |
successors-of-LogicNegationNode:
successors-of (*LogicNegationNode value*) = [] |
successors-of-LoopBeginNode:
successors-of (*LoopBeginNode ends overflowGuard stateAfter next*) = [*next*] |
successors-of-LoopEndNode:
successors-of (*LoopEndNode loopBegin*) = [] |
successors-of-LoopExitNode:
successors-of (*LoopExitNode loopBegin stateAfter next*) = [*next*] |
successors-of-MergeNode:
successors-of (*MergeNode ends stateAfter next*) = [*next*] |
successors-of-MethodCallTargetNode:
successors-of (*MethodCallTargetNode targetMethod arguments*) = [] |
successors-of-MulNode:
successors-of (*MulNode x y*) = [] |
successors-of-NarrowNode:
successors-of (*NarrowNode inputBits resultBits value*) = [] |
successors-of-NegateNode:
successors-of (*NegateNode value*) = [] |
successors-of-NewArrayNode:
successors-of (*NewArrayNode length0 stateBefore next*) = [*next*] |
successors-of-NewInstanceNode:

successors-of (*NewInstanceNode nid0 instanceClass stateBefore next*) = [*next*] |
successors-of-NotNode:
successors-of (*NotNode value*) = [] |
successors-of-OrNode:
successors-of (*OrNode x y*) = [] |
successors-of-ParameterNode:
successors-of (*ParameterNode index*) = [] |
successors-of-PiNode:
successors-of (*PiNode object guard*) = [] |
successors-of-ReturnNode:
successors-of (*ReturnNode result memoryMap*) = [] |
successors-of-RightShiftNode:
successors-of (*RightShiftNode x y*) = [] |
successors-of-ShortCircuitOrNode:
successors-of (*ShortCircuitOrNode x y*) = [] |
successors-of-SignExtendNode:
successors-of (*SignExtendNode inputBits resultBits value*) = [] |
successors-of-SignedDivNode:
successors-of (*SignedDivNode nid0 x y zeroCheck stateBefore next*) = [*next*] |
successors-of-SignedRemNode:
successors-of (*SignedRemNode nid0 x y zeroCheck stateBefore next*) = [*next*] |
successors-of-StartNode:
successors-of (*StartNode stateAfter next*) = [*next*] |
successors-of-StoreFieldNode:
successors-of (*StoreFieldNode nid0 field value stateAfter object next*) = [*next*] |
successors-of-SubNode:
successors-of (*SubNode x y*) = [] |
successors-of-UnsignedRightShiftNode:
successors-of (*UnsignedRightShiftNode x y*) = [] |
successors-of-UnwindNode:
successors-of (*UnwindNode exception*) = [] |
successors-of-ValuePhiNode:
successors-of (*ValuePhiNode nid0 values merge*) = [] |
successors-of-ValueProxyNode:
successors-of (*ValueProxyNode value loopExit*) = [] |
successors-of-XorNode:
successors-of (*XorNode x y*) = [] |
successors-of-ZeroExtendNode:
successors-of (*ZeroExtendNode inputBits resultBits value*) = [] |
successors-of-NoNode: *successors-of* (*NoNode*) = [] |

successors-of-RefNode: *successors-of* (*RefNode ref*) = [*ref*]

lemma *inputs-of* (*FrameState x* (*Some y*) (*Some z*) *None*) = *x* @ [*y*] @ *z*
  unfolding *inputs-of-FrameState* **by** *simp*
lemma *successors-of* (*FrameState x* (*Some y*) (*Some z*) *None*) = []

unfolding *inputs-of-FrameState* **by** *simp*

lemma *inputs-of* (*IfNode c t f*) = [*c*]
  unfolding *inputs-of-IfNode* **by** *simp*
lemma *successors-of* (*IfNode c t f*) = [*t, f*]
  unfolding *successors-of-IfNode* **by** *simp*

lemma *inputs-of* (*EndNode*) = [] ∧ *successors-of* (*EndNode*) = []
  unfolding *inputs-of-EndNode successors-of-EndNode* **by** *simp*

end

3.2 Hierarchy of Nodes

theory *IRNodeHierarchy*
imports *IRNodes*
begin

It is helpful to introduce a node hierarchy into our formalization. Often the GraalVM compiler relies on explicit type checks to determine which operations to perform on a given node, we try to mimic the same functionality by using a suite of predicate functions over the IRNode class to determine inheritance.

As one would expect, the function is<ClassName>Type will be true if the node parameter is a subclass of the ClassName within the GraalVM compiler.

These functions have been automatically generated from the compiler.

fun *is-EndNode* :: *IRNode* ⇒ *bool* **where**
  is-EndNode EndNode = *True* |
  is-EndNode - = *False*

fun *is-VirtualState* :: *IRNode* ⇒ *bool* **where**
  is-VirtualState n = ((*is-FrameState n*))

fun *is-BinaryArithmeticNode* :: *IRNode* ⇒ *bool* **where**
  is-BinaryArithmeticNode n = ((*is-AddNode n*) ∨ (*is-AndNode n*) ∨ (*is-MulNode n*) ∨ (*is-OrNode n*) ∨ (*is-SubNode n*) ∨ (*is-XorNode n*))

fun *is-ShiftNode* :: *IRNode* ⇒ *bool* **where**
  is-ShiftNode n = ((*is-LeftShiftNode n*) ∨ (*is-RightShiftNode n*) ∨ (*is-UnsignedRightShiftNode n*))

fun *is-BinaryNode* :: *IRNode* ⇒ *bool* **where**
  is-BinaryNode n = ((*is-BinaryArithmeticNode n*) ∨ (*is-ShiftNode n*))

fun *is-AbstractLocalNode* :: *IRNode* ⇒ *bool* **where**
  is-AbstractLocalNode n = ((*is-ParameterNode n*))

fun *is-IntegerConvertNode* :: *IRNode* ⇒ *bool* **where**
  is-IntegerConvertNode n = ((*is-NarrowNode n*) ∨ (*is-SignExtendNode n*) ∨
(*is-ZeroExtendNode n*))

fun *is-UnaryArithmeticNode* :: *IRNode* ⇒ *bool* **where**
  is-UnaryArithmeticNode n = ((*is-AbsNode n*) ∨ (*is-NegateNode n*) ∨ (*is-NotNode
n*))

fun *is-UnaryNode* :: *IRNode* ⇒ *bool* **where**
  is-UnaryNode n = ((*is-IntegerConvertNode n*) ∨ (*is-UnaryArithmeticNode n*))

fun *is-PhiNode* :: *IRNode* ⇒ *bool* **where**
  is-PhiNode n = ((*is-ValuePhiNode n*))

fun *is-FloatingGuardedNode* :: *IRNode* ⇒ *bool* **where**
  is-FloatingGuardedNode n = ((*is-PiNode n*))

fun *is-UnaryOpLogicNode* :: *IRNode* ⇒ *bool* **where**
  is-UnaryOpLogicNode n = ((*is-IsNullNode n*))

fun *is-IntegerLowerThanNode* :: *IRNode* ⇒ *bool* **where**
  is-IntegerLowerThanNode n = ((*is-IntegerBelowNode n*) ∨ (*is-IntegerLessThanNode
n*))

fun *is-CompareNode* :: *IRNode* ⇒ *bool* **where**
  is-CompareNode n = ((*is-IntegerEqualsNode n*) ∨ (*is-IntegerLowerThanNode n*))

fun *is-BinaryOpLogicNode* :: *IRNode* ⇒ *bool* **where**
  is-BinaryOpLogicNode n = ((*is-CompareNode n*))

fun *is-LogicNode* :: *IRNode* ⇒ *bool* **where**
  is-LogicNode n = ((*is-BinaryOpLogicNode n*) ∨ (*is-LogicNegationNode n*) ∨
(*is-ShortCircuitOrNode n*) ∨ (*is-UnaryOpLogicNode n*))

fun *is-ProxyNode* :: *IRNode* ⇒ *bool* **where**
  is-ProxyNode n = ((*is-ValueProxyNode n*))

fun *is-FloatingNode* :: *IRNode* ⇒ *bool* **where**
  is-FloatingNode n = ((*is-AbstractLocalNode n*) ∨ (*is-BinaryNode n*) ∨ (*is-ConditionalNode
n*) ∨ (*is-ConstantNode n*) ∨ (*is-FloatingGuardedNode n*) ∨ (*is-LogicNode n*) ∨
(*is-PhiNode n*) ∨ (*is-ProxyNode n*) ∨ (*is-UnaryNode n*))

fun *is-AccessFieldNode* :: *IRNode* ⇒ *bool* **where**
  is-AccessFieldNode n = ((*is-LoadFieldNode n*) ∨ (*is-StoreFieldNode n*))

fun *is-AbstractNewArrayNode* :: *IRNode* ⇒ *bool* **where**
  is-AbstractNewArrayNode n = ((*is-DynamicNewArrayNode n*) ∨ (*is-NewArrayNode
n*))

fun *is-AbstractNewObjectNode* :: *IRNode* ⇒ *bool* **where**
 is-AbstractNewObjectNode n = ((*is-AbstractNewArrayNode n*) ∨ (*is-NewInstanceNode n*))

fun *is-IntegerDivRemNode* :: *IRNode* ⇒ *bool* **where**
 is-IntegerDivRemNode n = ((*is-SignedDivNode n*) ∨ (*is-SignedRemNode n*))

fun *is-FixedBinaryNode* :: *IRNode* ⇒ *bool* **where**
 is-FixedBinaryNode n = ((*is-IntegerDivRemNode n*))

fun *is-DeoptimizingFixedWithNextNode* :: *IRNode* ⇒ *bool* **where**
 is-DeoptimizingFixedWithNextNode n = ((*is-AbstractNewObjectNode n*) ∨ (*is-FixedBinaryNode n*))

fun *is-AbstractMemoryCheckpoint* :: *IRNode* ⇒ *bool* **where**
 is-AbstractMemoryCheckpoint n = ((*is-BytecodeExceptionNode n*) ∨ (*is-InvokeNode n*))

fun *is-AbstractStateSplit* :: *IRNode* ⇒ *bool* **where**
 is-AbstractStateSplit n = ((*is-AbstractMemoryCheckpoint n*))

fun *is-AbstractMergeNode* :: *IRNode* ⇒ *bool* **where**
 is-AbstractMergeNode n = ((*is-LoopBeginNode n*) ∨ (*is-MergeNode n*))

fun *is-BeginStateSplitNode* :: *IRNode* ⇒ *bool* **where**
 is-BeginStateSplitNode n = ((*is-AbstractMergeNode n*) ∨ (*is-ExceptionObjectNode n*) ∨ (*is-LoopExitNode n*) ∨ (*is-StartNode n*))

fun *is-AbstractBeginNode* :: *IRNode* ⇒ *bool* **where**
  is-AbstractBeginNode n = ((*is-BeginNode n*) ∨ (*is-BeginStateSplitNode n*) ∨ (*is-KillingBeginNode n*))

fun *is-FixedWithNextNode* :: *IRNode* ⇒ *bool* **where**
 is-FixedWithNextNode n = ((*is-AbstractBeginNode n*) ∨ (*is-AbstractStateSplit n*) ∨ (*is-AccessFieldNode n*) ∨ (*is-DeoptimizingFixedWithNextNode n*))

fun *is-WithExceptionNode* :: *IRNode* ⇒ *bool* **where**
 is-WithExceptionNode n = ((*is-InvokeWithExceptionNode n*))

fun *is-ControlSplitNode* :: *IRNode* ⇒ *bool* **where**
 is-ControlSplitNode n = ((*is-IfNode n*) ∨ (*is-WithExceptionNode n*))

fun *is-ControlSinkNode* :: *IRNode* ⇒ *bool* **where**
 is-ControlSinkNode n = ((*is-ReturnNode n*) ∨ (*is-UnwindNode n*))

fun *is-AbstractEndNode* :: *IRNode* ⇒ *bool* **where**
 is-AbstractEndNode n = ((*is-EndNode n*) ∨ (*is-LoopEndNode n*))

fun *is-FixedNode* :: *IRNode* $\Rightarrow$ *bool* **where**
 is-FixedNode n = ((*is-AbstractEndNode n*) $\vee$ (*is-ControlSinkNode n*) $\vee$ (*is-ControlSplitNode n*) $\vee$ (*is-FixedWithNextNode n*))

fun *is-CallTargetNode* :: *IRNode* $\Rightarrow$ *bool* **where**
 is-CallTargetNode n = ((*is-MethodCallTargetNode n*))

fun *is-ValueNode* :: *IRNode* $\Rightarrow$ *bool* **where**
 is-ValueNode n = ((*is-CallTargetNode n*) $\vee$ (*is-FixedNode n*) $\vee$ (*is-FloatingNode n*))

fun *is-Node* :: *IRNode* $\Rightarrow$ *bool* **where**
 is-Node n = ((*is-ValueNode n*) $\vee$ (*is-VirtualState n*))

fun *is-MemoryKill* :: *IRNode* $\Rightarrow$ *bool* **where**
 is-MemoryKill n = ((*is-AbstractMemoryCheckpoint n*))

fun *is-NarrowableArithmeticNode* :: *IRNode* $\Rightarrow$ *bool* **where**
 is-NarrowableArithmeticNode n = ((*is-AbsNode n*) $\vee$ (*is-AddNode n*) $\vee$ (*is-AndNode n*) $\vee$ (*is-MulNode n*) $\vee$ (*is-NegateNode n*) $\vee$ (*is-NotNode n*) $\vee$ (*is-OrNode n*) $\vee$ (*is-ShiftNode n*) $\vee$ (*is-SubNode n*) $\vee$ (*is-XorNode n*))

fun *is-AnchoringNode* :: *IRNode* $\Rightarrow$ *bool* **where**
 is-AnchoringNode n = ((*is-AbstractBeginNode n*))

fun *is-DeoptBefore* :: *IRNode* $\Rightarrow$ *bool* **where**
 is-DeoptBefore n = ((*is-DeoptimizingFixedWithNextNode n*))

fun *is-IndirectCanonicalization* :: *IRNode* $\Rightarrow$ *bool* **where**
 is-IndirectCanonicalization n = ((*is-LogicNode n*))

fun *is-IterableNodeType* :: *IRNode* $\Rightarrow$ *bool* **where**
 is-IterableNodeType n = ((*is-AbstractBeginNode n*) $\vee$ (*is-AbstractMergeNode n*) $\vee$ (*is-FrameState n*) $\vee$ (*is-IfNode n*) $\vee$ (*is-IntegerDivRemNode n*) $\vee$ (*is-InvokeWithExceptionNode n*) $\vee$ (*is-LoopBeginNode n*) $\vee$ (*is-LoopExitNode n*) $\vee$ (*is-MethodCallTargetNode n*) $\vee$ (*is-ParameterNode n*) $\vee$ (*is-ReturnNode n*) $\vee$ (*is-ShortCircuitOrNode n*))

fun *is-Invoke* :: *IRNode* $\Rightarrow$ *bool* **where**
 is-Invoke n = ((*is-InvokeNode n*) $\vee$ (*is-InvokeWithExceptionNode n*))

fun *is-Proxy* :: *IRNode* $\Rightarrow$ *bool* **where**
 is-Proxy n = ((*is-ProxyNode n*))

fun *is-ValueProxy* :: *IRNode* $\Rightarrow$ *bool* **where**
 is-ValueProxy n = ((*is-PiNode n*) $\vee$ (*is-ValueProxyNode n*))

fun *is-ValueNodeInterface* :: *IRNode* $\Rightarrow$ *bool* **where**
 is-ValueNodeInterface n = ((*is-ValueNode n*))

fun *is-ArrayLengthProvider* :: *IRNode* ⇒ *bool* **where**
  is-ArrayLengthProvider n = ((*is-AbstractNewArrayNode n*) ∨ (*is-ConstantNode n*))

fun *is-StampInverter* :: *IRNode* ⇒ *bool* **where**
  is-StampInverter n = ((*is-IntegerConvertNode n*) ∨ (*is-NegateNode n*) ∨ (*is-NotNode n*))

fun *is-GuardingNode* :: *IRNode* ⇒ *bool* **where**
  is-GuardingNode n = ((*is-AbstractBeginNode n*))

fun *is-SingleMemoryKill* :: *IRNode* ⇒ *bool* **where**
  is-SingleMemoryKill n = ((*is-BytecodeExceptionNode n*) ∨ (*is-ExceptionObjectNode n*) ∨ (*is-InvokeNode n*) ∨ (*is-InvokeWithExceptionNode n*) ∨ (*is-KillingBeginNode n*) ∨ (*is-StartNode n*))

fun *is-LIRLowerable* :: *IRNode* ⇒ *bool* **where**
  is-LIRLowerable n = ((*is-AbstractBeginNode n*) ∨ (*is-AbstractEndNode n*) ∨ (*is-AbstractMergeNode n*) ∨ (*is-BinaryOpLogicNode n*) ∨ (*is-CallTargetNode n*) ∨ (*is-ConditionalNode n*) ∨ (*is-ConstantNode n*) ∨ (*is-IfNode n*) ∨ (*is-InvokeNode n*) ∨ (*is-InvokeWithExceptionNode n*) ∨ (*is-IsNullNode n*) ∨ (*is-LoopBeginNode n*) ∨ (*is-PiNode n*) ∨ (*is-ReturnNode n*) ∨ (*is-SignedDivNode n*) ∨ (*is-SignedRemNode n*) ∨ (*is-UnaryOpLogicNode n*) ∨ (*is-UnwindNode n*))

fun *is-GuardedNode* :: *IRNode* ⇒ *bool* **where**
  is-GuardedNode n = ((*is-FloatingGuardedNode n*))

fun *is-ArithmeticLIRLowerable* :: *IRNode* ⇒ *bool* **where**
  is-ArithmeticLIRLowerable n = ((*is-AbsNode n*) ∨ (*is-BinaryArithmeticNode n*) ∨ (*is-IntegerConvertNode n*) ∨ (*is-NotNode n*) ∨ (*is-ShiftNode n*) ∨ (*is-UnaryArithmeticNode n*))

fun *is-SwitchFoldable* :: *IRNode* ⇒ *bool* **where**
  is-SwitchFoldable n = ((*is-IfNode n*))

fun *is-VirtualizableAllocation* :: *IRNode* ⇒ *bool* **where**
  is-VirtualizableAllocation n = ((*is-NewArrayNode n*) ∨ (*is-NewInstanceNode n*))

fun *is-Unary* :: *IRNode* ⇒ *bool* **where**
  is-Unary n = ((*is-LoadFieldNode n*) ∨ (*is-LogicNegationNode n*) ∨ (*is-UnaryNode n*) ∨ (*is-UnaryOpLogicNode n*))

fun *is-FixedNodeInterface* :: *IRNode* ⇒ *bool* **where**
  is-FixedNodeInterface n = ((*is-FixedNode n*))

fun *is-BinaryCommutative* :: *IRNode* ⇒ *bool* **where**
  is-BinaryCommutative n = ((*is-AddNode n*) ∨ (*is-AndNode n*) ∨ (*is-IntegerEqualsNode n*) ∨ (*is-MulNode n*) ∨ (*is-OrNode n*) ∨ (*is-XorNode n*))

fun *is-Canonicalizable* :: *IRNode* ⇒ *bool* **where**
  is-Canonicalizable n = ((*is-BytecodeExceptionNode n*) ∨ (*is-ConditionalNode n*) ∨
(*is-DynamicNewArrayNode n*) ∨ (*is-PhiNode n*) ∨ (*is-PiNode n*) ∨ (*is-ProxyNode
n*) ∨ (*is-StoreFieldNode n*) ∨ (*is-ValueProxyNode n*))

fun *is-UncheckedInterfaceProvider* :: *IRNode* ⇒ *bool* **where**
  is-UncheckedInterfaceProvider n = ((*is-InvokeNode n*) ∨ (*is-InvokeWithExceptionNode
n*) ∨ (*is-LoadFieldNode n*) ∨ (*is-ParameterNode n*))

fun *is-Binary* :: *IRNode* ⇒ *bool* **where**
  is-Binary n = ((*is-BinaryArithmeticNode n*) ∨ (*is-BinaryNode n*) ∨ (*is-BinaryOpLogicNode
n*) ∨ (*is-CompareNode n*) ∨ (*is-FixedBinaryNode n*) ∨ (*is-ShortCircuitOrNode n*))

fun *is-ArithmeticOperation* :: *IRNode* ⇒ *bool* **where**
  is-ArithmeticOperation n = ((*is-BinaryArithmeticNode n*) ∨ (*is-IntegerConvertNode
n*) ∨ (*is-ShiftNode n*) ∨ (*is-UnaryArithmeticNode n*))

fun *is-ValueNumberable* :: *IRNode* ⇒ *bool* **where**
  is-ValueNumberable n = ((*is-FloatingNode n*) ∨ (*is-ProxyNode n*))

fun *is-Lowerable* :: *IRNode* ⇒ *bool* **where**
  is-Lowerable n = ((*is-AbstractNewObjectNode n*) ∨ (*is-AccessFieldNode n*) ∨
(*is-BytecodeExceptionNode n*) ∨ (*is-ExceptionObjectNode n*) ∨ (*is-IntegerDivRemNode
n*) ∨ (*is-UnwindNode n*))

fun *is-Virtualizable* :: *IRNode* ⇒ *bool* **where**
  is-Virtualizable n = ((*is-IsNullNode n*) ∨ (*is-LoadFieldNode n*) ∨ (*is-PiNode n*)
∨ (*is-StoreFieldNode n*) ∨ (*is-ValueProxyNode n*))

fun *is-Simplifiable* :: *IRNode* ⇒ *bool* **where**
  is-Simplifiable n = ((*is-AbstractMergeNode n*) ∨ (*is-BeginNode n*) ∨ (*is-IfNode
n*) ∨ (*is-LoopExitNode n*) ∨ (*is-MethodCallTargetNode n*) ∨ (*is-NewArrayNode n*))

fun *is-StateSplit* :: *IRNode* ⇒ *bool* **where**
  is-StateSplit n = ((*is-AbstractStateSplit n*) ∨ (*is-BeginStateSplitNode n*) ∨ (*is-StoreFieldNode
n*))

fun *is-ConvertNode* :: *IRNode* ⇒ *bool* **where**
  is-ConvertNode n = ((*is-IntegerConvertNode n*))

fun *is-sequential-node* :: *IRNode* ⇒ *bool* **where**
  is-sequential-node (*StartNode - -*) = *True* |
  is-sequential-node (*BeginNode -*) = *True* |
  is-sequential-node (*KillingBeginNode -*) = *True* |
  is-sequential-node (*LoopBeginNode - - - -*) = *True* |
  is-sequential-node (*LoopExitNode - - -*) = *True* |
  is-sequential-node (*MergeNode - - -*) = *True* |
  is-sequential-node (*RefNode -*) = *True* |

is-sequential-node - = False

The following convenience function is useful in determining if two IRNodes are of the same type irregardless of their edges. It will return true if both the node parameters are the same node class.

fun *is-same-ir-node-type* :: *IRNode* ⇒ *IRNode* ⇒ *bool* **where**
is-same-ir-node-type n1 n2 = (
  ((*is-AbsNode n1*) ∧ (*is-AbsNode n2*)) ∨
  ((*is-AddNode n1*) ∧ (*is-AddNode n2*)) ∨
  ((*is-AndNode n1*) ∧ (*is-AndNode n2*)) ∨
  ((*is-BeginNode n1*) ∧ (*is-BeginNode n2*)) ∨
  ((*is-BytecodeExceptionNode n1*) ∧ (*is-BytecodeExceptionNode n2*)) ∨
  ((*is-ConditionalNode n1*) ∧ (*is-ConditionalNode n2*)) ∨
  ((*is-ConstantNode n1*) ∧ (*is-ConstantNode n2*)) ∨
  ((*is-DynamicNewArrayNode n1*) ∧ (*is-DynamicNewArrayNode n2*)) ∨
  ((*is-EndNode n1*) ∧ (*is-EndNode n2*)) ∨
  ((*is-ExceptionObjectNode n1*) ∧ (*is-ExceptionObjectNode n2*)) ∨
  ((*is-FrameState n1*) ∧ (*is-FrameState n2*)) ∨
  ((*is-IfNode n1*) ∧ (*is-IfNode n2*)) ∨
  ((*is-IntegerBelowNode n1*) ∧ (*is-IntegerBelowNode n2*)) ∨
  ((*is-IntegerEqualsNode n1*) ∧ (*is-IntegerEqualsNode n2*)) ∨
  ((*is-IntegerLessThanNode n1*) ∧ (*is-IntegerLessThanNode n2*)) ∨
  ((*is-InvokeNode n1*) ∧ (*is-InvokeNode n2*)) ∨
  ((*is-InvokeWithExceptionNode n1*) ∧ (*is-InvokeWithExceptionNode n2*)) ∨
  ((*is-IsNullNode n1*) ∧ (*is-IsNullNode n2*)) ∨
  ((*is-KillingBeginNode n1*) ∧ (*is-KillingBeginNode n2*)) ∨
  ((*is-LoadFieldNode n1*) ∧ (*is-LoadFieldNode n2*)) ∨
  ((*is-LogicNegationNode n1*) ∧ (*is-LogicNegationNode n2*)) ∨
  ((*is-LoopBeginNode n1*) ∧ (*is-LoopBeginNode n2*)) ∨
  ((*is-LoopEndNode n1*) ∧ (*is-LoopEndNode n2*)) ∨
  ((*is-LoopExitNode n1*) ∧ (*is-LoopExitNode n2*)) ∨
  ((*is-MergeNode n1*) ∧ (*is-MergeNode n2*)) ∨
  ((*is-MethodCallTargetNode n1*) ∧ (*is-MethodCallTargetNode n2*)) ∨
  ((*is-MulNode n1*) ∧ (*is-MulNode n2*)) ∨
  ((*is-NegateNode n1*) ∧ (*is-NegateNode n2*)) ∨
  ((*is-NewArrayNode n1*) ∧ (*is-NewArrayNode n2*)) ∨
  ((*is-NewInstanceNode n1*) ∧ (*is-NewInstanceNode n2*)) ∨
  ((*is-NotNode n1*) ∧ (*is-NotNode n2*)) ∨
  ((*is-OrNode n1*) ∧ (*is-OrNode n2*)) ∨
  ((*is-ParameterNode n1*) ∧ (*is-ParameterNode n2*)) ∨
  ((*is-PiNode n1*) ∧ (*is-PiNode n2*)) ∨
  ((*is-ReturnNode n1*) ∧ (*is-ReturnNode n2*)) ∨
  ((*is-ShortCircuitOrNode n1*) ∧ (*is-ShortCircuitOrNode n2*)) ∨
  ((*is-SignedDivNode n1*) ∧ (*is-SignedDivNode n2*)) ∨
  ((*is-StartNode n1*) ∧ (*is-StartNode n2*)) ∨
  ((*is-StoreFieldNode n1*) ∧ (*is-StoreFieldNode n2*)) ∨
  ((*is-SubNode n1*) ∧ (*is-SubNode n2*)) ∨
  ((*is-UnwindNode n1*) ∧ (*is-UnwindNode n2*)) ∨
  ((*is-ValuePhiNode n1*) ∧ (*is-ValuePhiNode n2*)) ∨

$((\textit{is-ValueProxyNode n1}) \wedge (\textit{is-ValueProxyNode n2})) \vee$
$((\textit{is-XorNode n1}) \wedge (\textit{is-XorNode n2})))$

end

4 Stamp Typing

theory *Stamp*
  imports *Values*
begin

The GraalVM compiler uses the Stamp class to store range and type information for a given node in the IR graph. We model the Stamp class as a datatype, Stamp, and provide a number of functions on the datatype which correspond to the class methods within the compiler.

Stamp information is used in a variety of ways in optimizations, and so, we additionally provide a number of lemmas which help to prove future optimizations.

datatype *Stamp =*
  VoidStamp
  | *IntegerStamp* (*stp-bits*: *nat*) (*stpi-lower*: *int*) (*stpi-upper*: *int*)

  | *KlassPointerStamp* (*stp-nonNull*: *bool*) (*stp-alwaysNull*: *bool*)
  | *MethodCountersPointerStamp* (*stp-nonNull*: *bool*) (*stp-alwaysNull*: *bool*)
  | *MethodPointersStamp* (*stp-nonNull*: *bool*) (*stp-alwaysNull*: *bool*)
 | *ObjectStamp* (*stp-type*: *string*) (*stp-exactType*: *bool*) (*stp-nonNull*: *bool*) (*stp-alwaysNull*: *bool*)
  | *RawPointerStamp* (*stp-nonNull*: *bool*) (*stp-alwaysNull*: *bool*)
  | *IllegalStamp*

fun *bit-bounds* :: *nat* $\Rightarrow$ (*int* $\times$ *int*) **where**
  bit-bounds bits = (((2 ^ *bits*) *div 2*) * −1, ((2 ^ *bits*) *div 2*) − 1)

experiment begin
corollary *bit-bounds 1* = (−1, 0) **by** *simp*
end

— A stamp which includes the full range of the type
fun *unrestricted-stamp* :: *Stamp* $\Rightarrow$ *Stamp* **where**
  unrestricted-stamp VoidStamp = *VoidStamp* |
  unrestricted-stamp (*IntegerStamp bits lower upper*) = (*IntegerStamp bits* (*fst* (*bit-bounds bits*)) (*snd* (*bit-bounds bits*))) |

unrestricted-stamp (*KlassPointerStamp nonNull alwaysNull*) = (*KlassPointerStamp
False False*) |
unrestricted-stamp (*MethodCountersPointerStamp nonNull alwaysNull*) = (*MethodCountersPointerStamp
False False*) |
unrestricted-stamp (*MethodPointersStamp nonNull alwaysNull*) = (*MethodPointersStamp
False False*) |
unrestricted-stamp (*ObjectStamp type exactType nonNull alwaysNull*) = (*ObjectStamp
'''' False False False*) |
unrestricted-stamp - = IllegalStamp

fun *is-stamp-unrestricted* :: *Stamp* ⇒ *bool* **where**
is-stamp-unrestricted s = (*s* = *unrestricted-stamp s*)

— A stamp which provides type information but has an empty range of values
fun *empty-stamp* :: *Stamp* ⇒ *Stamp* **where**
empty-stamp VoidStamp = *VoidStamp* |
empty-stamp (*IntegerStamp bits lower upper*) = (*IntegerStamp bits* (*snd* (*bit-bounds
bits*)) (*fst* (*bit-bounds bits*))) |

empty-stamp (*KlassPointerStamp nonNull alwaysNull*) = (*KlassPointerStamp
nonNull alwaysNull*) |
empty-stamp (*MethodCountersPointerStamp nonNull alwaysNull*) = (*MethodCountersPointerStamp
nonNull alwaysNull*) |
empty-stamp (*MethodPointersStamp nonNull alwaysNull*) = (*MethodPointersStamp
nonNull alwaysNull*) |
empty-stamp (*ObjectStamp type exactType nonNull alwaysNull*) = (*ObjectStamp
'''' True True False*) |
empty-stamp stamp = *IllegalStamp*

fun *is-stamp-empty* :: *Stamp* ⇒ *bool* **where**
is-stamp-empty (*IntegerStamp b lower upper*) = (*upper* < *lower*) |

is-stamp-empty x = *False*

— Calculate the meet stamp of two stamps
fun *meet* :: *Stamp* ⇒ *Stamp* ⇒ *Stamp* **where**
meet VoidStamp VoidStamp = *VoidStamp* |
meet (*IntegerStamp b1 l1 u1*) (*IntegerStamp b2 l2 u2*) = (
  if b1 ≠ *b2 then IllegalStamp else*
  (*IntegerStamp b1* (*min l1 l2*) (*max u1 u2*))
) |

meet (*KlassPointerStamp nn1 an1*) (*KlassPointerStamp nn2 an2*) = (
  KlassPointerStamp (*nn1* ∧ *nn2*) (*an1* ∧ *an2*)
) |
meet (*MethodCountersPointerStamp nn1 an1*) (*MethodCountersPointerStamp
nn2 an2*) = (
  MethodCountersPointerStamp (*nn1* ∧ *nn2*) (*an1* ∧ *an2*)
) |

meet (*MethodPointersStamp nn1 an1*) (*MethodPointersStamp nn2 an2*) = (
  MethodPointersStamp (*nn1* ∧ *nn2*) (*an1* ∧ *an2*)
) |
meet s1 s2 = *IllegalStamp*

— Calculate the join stamp of two stamps
fun *join* :: *Stamp* ⇒ *Stamp* ⇒ *Stamp* **where**
  join VoidStamp VoidStamp = *VoidStamp* |
  join (*IntegerStamp b1 l1 u1*) (*IntegerStamp b2 l2 u2*) = (
    if b1 ≠ *b2 then IllegalStamp else*
    (*IntegerStamp b1* (*max l1 l2*) (*min u1 u2*))
) |

  join (*KlassPointerStamp nn1 an1*) (*KlassPointerStamp nn2 an2*) = (
    if ((*nn1* ∨ *nn2*) ∧ (*an1* ∨ *an2*))
    then (*empty-stamp* (*KlassPointerStamp nn1 an1*))
    else (*KlassPointerStamp* (*nn1* ∨ *nn2*) (*an1* ∨ *an2*))
) |
  join (*MethodCountersPointerStamp nn1 an1*) (*MethodCountersPointerStamp nn2 an2*) = (
    if ((*nn1* ∨ *nn2*) ∧ (*an1* ∨ *an2*))
    then (*empty-stamp* (*MethodCountersPointerStamp nn1 an1*))
    else (*MethodCountersPointerStamp* (*nn1* ∨ *nn2*) (*an1* ∨ *an2*))
) |
  join (*MethodPointersStamp nn1 an1*) (*MethodPointersStamp nn2 an2*) = (
    if ((*nn1* ∨ *nn2*) ∧ (*an1* ∨ *an2*))
    then (*empty-stamp* (*MethodPointersStamp nn1 an1*))
    else (*MethodPointersStamp* (*nn1* ∨ *nn2*) (*an1* ∨ *an2*))
) |
  join s1 s2 = *IllegalStamp*

— In certain circumstances a stamp provides enough information to evaluate a value as a stamp, the asConstant function converts the stamp to a value where one can be inferred.

fun *asConstant* :: *Stamp* ⇒ *Value* **where**
  asConstant (*IntegerStamp b l h*) = (*if l* = *h then IntVal64* (*word-of-int l*) *else UndefVal*) |
  asConstant - = UndefVal

— Determine if two stamps never have value overlaps i.e. their join is empty
fun *alwaysDistinct* :: *Stamp* ⇒ *Stamp* ⇒ *bool* **where**
  alwaysDistinct stamp1 stamp2 = *is-stamp-empty* (*join stamp1 stamp2*)

— Determine if two stamps must always be the same value i.e. two equal constants
fun *neverDistinct* :: *Stamp* ⇒ *Stamp* ⇒ *bool* **where**
  neverDistinct stamp1 stamp2 = (*asConstant stamp1* = *asConstant stamp2* ∧ *asConstant stamp1* ≠ *UndefVal*)

fun *constantAsStamp* :: *Value ⇒ Stamp* **where**
  constantAsStamp (*IntVal32 v*) = (*IntegerStamp* (*nat 32*) (*sint v*) (*sint v*)) |
  constantAsStamp (*IntVal64 v*) = (*IntegerStamp* (*nat 64*) (*sint v*) (*sint v*)) |

  constantAsStamp - = IllegalStamp

— Define when a runtime value is valid for a stamp
fun *valid-value* :: *Value ⇒ Stamp ⇒ bool* **where**
  valid-value (*IntVal32 v*) (*IntegerStamp b l h*) = ((*b=32* ∨ *b=16* ∨ *b=8* ∨ *b=1*) ∧
(*sint v ≥ l*) ∧ (*sint v ≤ h*)) |
  valid-value (*IntVal64 v*) (*IntegerStamp b l h*) = (*b=64* ∧ (*sint v ≥ l*) ∧ (*sint v ≤
h*)) |

  valid-value (*ObjRef ref*) (*ObjectStamp klass exact nonNull alwaysNull*) =
    ((*alwaysNull* ⟶ *ref = None*) ∧ (*ref=None* ⟶ ¬ *nonNull*)) |
  valid-value stamp val = False

fun *compatible* :: *Stamp ⇒ Stamp ⇒ bool* **where**
  compatible (*IntegerStamp b1 - -*) (*IntegerStamp b2 - -*) = (*b1 = b2*) |
  compatible (*VoidStamp*) (*VoidStamp*) = *True* |
  compatible - - = False

fun *stamp-under* :: *Stamp ⇒ Stamp ⇒ bool* **where**
  stamp-under x y = ((*stpi-upper x*) < (*stpi-lower y*))

— The most common type of stamp within the compiler (apart from the Void-
Stamp) is a 32 bit integer stamp with an unrestricted range. We use *default-stamp*
as it is a frequently used stamp.
definition *default-stamp* :: *Stamp* **where**
  default-stamp = (*unrestricted-stamp* (*IntegerStamp 32 0 0*))

end

5   Graph Representation

theory *IRGraph*
  imports
    IRNodeHierarchy
    Stamp
    HOL−Library.FSet
    HOL.Relation
begin

This theory defines the main Graal data structure - an entire IR Graph.

IRGraph is defined as a partial map with a finite domain. The finite domain

is required to be able to generate code and produce an interpreter.

typedef *IRGraph* = {*g* :: *ID* ⇀ (*IRNode* × *Stamp*) . *finite* (*dom g*)}
proof −
  have *finite*(*dom*(*Map.empty*)) ∧ *ran Map.empty* = {} **by** *auto*
  then show *?thesis*
    by *fastforce*
qed

setup-lifting *type-definition-IRGraph*

lift-definition *ids* :: *IRGraph* ⇒ *ID set*
  is λ*g*. {*nid* ∈ *dom g* . ∄ *s*. *g nid* = (*Some* (*NoNode, s*))} **.**

fun *with-default* :: ′*c* ⇒ (′*b* ⇒ ′*c*) ⇒ ((′*a* ⇀ ′*b*) ⇒ ′*a* ⇒ ′*c*) **where**
  with-default def conv = (λ*m k*.
    (*case m k of None* ⇒ *def* | *Some v* ⇒ *conv v*))

lift-definition *kind* :: *IRGraph* ⇒ (*ID* ⇒ *IRNode*)
  is *with-default NoNode fst* **.**

lift-definition *stamp* :: *IRGraph* ⇒ *ID* ⇒ *Stamp*
  is *with-default IllegalStamp snd* **.**

lift-definition *add-node* :: *ID* ⇒ (*IRNode* × *Stamp*) ⇒ *IRGraph* ⇒ *IRGraph*
  is λ*nid k g*. *if fst k* = *NoNode then g else g*(*nid* ↦ *k*) **by** *simp*

lift-definition *remove-node* :: *ID* ⇒ *IRGraph* ⇒ *IRGraph*
  is λ*nid g*. *g*(*nid* := *None*) **by** *simp*

lift-definition *replace-node* :: *ID* ⇒ (*IRNode* × *Stamp*) ⇒ *IRGraph* ⇒ *IRGraph*
  is λ*nid k g*. *if fst k* = *NoNode then g else g*(*nid* ↦ *k*) **by** *simp*

lift-definition *as-list* :: *IRGraph* ⇒ (*ID* × *IRNode* × *Stamp*) *list*
  is λ*g*. *map* (λ*k*. (*k, the* (*g k*))) (*sorted-list-of-set* (*dom g*)) **.**

fun *no-node* :: (*ID* × (*IRNode* × *Stamp*)) *list* ⇒ (*ID* × (*IRNode* × *Stamp*)) *list*
where
  no-node g = *filter* (λ*n*. *fst* (*snd n*) ≠ *NoNode*) *g*

lift-definition *irgraph* :: (*ID* × (*IRNode* × *Stamp*)) *list* ⇒ *IRGraph*
  is *map-of* ∘ *no-node*
  by (*simp add*: *finite-dom-map-of*)

definition *as-set* :: *IRGraph* ⇒ (*ID* × (*IRNode* × *Stamp*)) *set* **where**
  as-set g = {(*n, kind g n, stamp g n*) | *n* . *n* ∈ *ids g*}

definition *true-ids* :: *IRGraph* ⇒ *ID set* **where**
  true-ids g = *ids g* − {*n* ∈ *ids g*. ∃ *n*′ . *kind g n* = *RefNode n*′}

definition *domain-subtraction* :: $'a$ *set* $\Rightarrow$ ($'a \times {'}b$) *set* $\Rightarrow$ ($'a \times {'}b$) *set*
  (**infix** $\unlhd$ *30*) **where**
  domain-subtraction s r = $\{(x, y) . (x, y) \in r \wedge x \notin s\}$

notation (*latex*)
  domain-subtraction (- $\lhd$ -)

code-datatype *irgraph*

fun *filter-none* **where**
  filter-none g = $\{nid \in dom\ g . \nexists s.\ g\ nid = (Some\ (NoNode, s))\}$

lemma *no-node-clears*:
  res = *no-node xs* $\longrightarrow$ ($\forall x \in set\ res.\ fst\ (snd\ x) \neq NoNode$)
  by *simp*

lemma *dom-eq*:
  assumes $\forall x \in set\ xs.\ fst\ (snd\ x) \neq NoNode$
  shows *filter-none* (*map-of xs*) = *dom* (*map-of xs*)
  unfolding *filter-none.simps* **using** *assms map-of-SomeD*
  by *fastforce*

lemma *fil-eq*:
  filter-none (*map-of* (*no-node xs*)) = *set* (*map fst* (*no-node xs*))
  using *no-node-clears*
  by (*metis dom-eq dom-map-of-conv-image-fst list.set-map*)

lemma *irgraph*[*code*]: *ids* (*irgraph m*) = *set* (*map fst* (*no-node m*))
  unfolding *irgraph-def ids-def* **using** *fil-eq*
  by (*smt Rep-IRGraph comp-apply eq-onp-same-args filter-none.simps ids.abs-eq*
ids-def irgraph.abs-eq irgraph.rep-eq irgraph-def mem-Collect-eq)

lemma [*code*]: *Rep-IRGraph* (*irgraph m*) = *map-of* (*no-node m*)
  using *Abs-IRGraph-inverse*
  by (*simp add*: *irgraph.rep-eq*)

— Get the inputs set of a given node ID
fun *inputs* :: *IRGraph* $\Rightarrow$ *ID* $\Rightarrow$ *ID set* **where**
  inputs g nid = *set* (*inputs-of* (*kind g nid*))
— Get the successor set of a given node ID
fun *succ* :: *IRGraph* $\Rightarrow$ *ID* $\Rightarrow$ *ID set* **where**
  succ g nid = *set* (*successors-of* (*kind g nid*))
— Gives a relation between node IDs - between a node and its input nodes
fun *input-edges* :: *IRGraph* $\Rightarrow$ *ID rel* **where**
  input-edges g = ($\bigcup\ i \in ids\ g.\ \{(i,j)|j.\ j \in (inputs\ g\ i)\}$)
— Find all the nodes in the graph that have nid as an input - the usages of nid
fun *usages* :: *IRGraph* $\Rightarrow$ *ID* $\Rightarrow$ *ID set* **where**

usages g nid = {i. i ∈ ids g ∧ nid ∈ inputs g i}
fun *successor-edges* :: *IRGraph ⇒ ID rel* **where**
  successor-edges g = (⋃ i ∈ ids g. {(i,j)|j . j ∈ (succ g i)})
fun *predecessors* :: *IRGraph ⇒ ID ⇒ ID set* **where**
  predecessors g nid = {i. i ∈ ids g ∧ nid ∈ succ g i}
fun *nodes-of* :: *IRGraph ⇒ (IRNode ⇒ bool) ⇒ ID set* **where**
  nodes-of g sel = {nid ∈ ids g . sel (kind g nid)}
fun *edge* :: *(IRNode ⇒ 'a) ⇒ ID ⇒ IRGraph ⇒ 'a* **where**
  edge sel nid g = sel (kind g nid)

fun *filtered-inputs* :: *IRGraph ⇒ ID ⇒ (IRNode ⇒ bool) ⇒ ID list* **where**
  filtered-inputs g nid f = filter (f ∘ (kind g)) (inputs-of (kind g nid))
fun *filtered-successors* :: *IRGraph ⇒ ID ⇒ (IRNode ⇒ bool) ⇒ ID list* **where**
  filtered-successors g nid f = filter (f ∘ (kind g)) (successors-of (kind g nid))
fun *filtered-usages* :: *IRGraph ⇒ ID ⇒ (IRNode ⇒ bool) ⇒ ID set* **where**
  filtered-usages g nid f = {n ∈ (usages g nid). f (kind g n)}

fun *is-empty* :: *IRGraph ⇒ bool* **where**
  is-empty g = (ids g = {})

fun *any-usage* :: *IRGraph ⇒ ID ⇒ ID* **where**
  any-usage g nid = hd (sorted-list-of-set (usages g nid))

lemma *ids-some*[*simp*]: *x ∈ ids g ⟷ kind g x ≠ NoNode*
proof −
  have *that*: *x ∈ ids g ⟶ kind g x ≠ NoNode*
    using *ids.rep-eq kind.rep-eq* **by** *force*
  have *kind g x ≠ NoNode ⟶ x ∈ ids g*
    unfolding *with-default.simps kind-def ids-def*
    by (*cases Rep-IRGraph g x = None; auto*)
  from *this that* **show** *?thesis* **by** *auto*
qed

lemma *not-in-g*:
  assumes *nid ∉ ids g*
  shows *kind g nid = NoNode*
  using *assms ids-some* **by** *blast*

lemma *valid-creation*[*simp*]:
  finite (dom g) ⟷ Rep-IRGraph (Abs-IRGraph g) = g
  using *Abs-IRGraph-inverse* **by** (*metis Rep-IRGraph mem-Collect-eq*)

lemma [*simp*]: *finite (ids g)*
  using *Rep-IRGraph ids.rep-eq* **by** *simp*

lemma [*simp*]: *finite (ids (irgraph g))*
  by (*simp add: finite-dom-map-of*)

lemma [*simp*]: *finite (dom g) ⟶ ids (Abs-IRGraph g) = {nid ∈ dom g . ∄s. g*

nid = Some (NoNode, s)}
  using *ids.rep-eq* **by** *simp*

lemma [*simp*]: *finite* (*dom g*) $\longrightarrow$ *kind* (*Abs-IRGraph g*) = (λx . (*case g x of None* $\Rightarrow$ *NoNode* | *Some n* $\Rightarrow$ *fst n*))
  by (*simp add: kind.rep-eq*)

lemma [*simp*]: *finite* (*dom g*) $\longrightarrow$ *stamp* (*Abs-IRGraph g*) = (λx . (*case g x of None* $\Rightarrow$ *IllegalStamp* | *Some n* $\Rightarrow$ *snd n*))
  using *stamp.abs-eq stamp.rep-eq* **by** *auto*

lemma [*simp*]: *ids* (*irgraph g*) = *set* (*map fst* (*no-node g*))
  using *irgraph* **by** *auto*

lemma [*simp*]: *kind* (*irgraph g*) = (λ*nid*. (*case* (*map-of* (*no-node g*)) *nid of None* $\Rightarrow$ *NoNode* | *Some n* $\Rightarrow$ *fst n*))
  using *irgraph.rep-eq kind.transfer kind.rep-eq* **by** *auto*

lemma [*simp*]: *stamp* (*irgraph g*) = (λ*nid*. (*case* (*map-of* (*no-node g*)) *nid of None* $\Rightarrow$ *IllegalStamp* | *Some n* $\Rightarrow$ *snd n*))
  using *irgraph.rep-eq stamp.transfer stamp.rep-eq* **by** *auto*

lemma *map-of-upd*: (*map-of g*)($k \mapsto v$) = (*map-of* ((k, v) # *g*))
  by *simp*

lemma [*code*]: *replace-node nid k* (*irgraph g*) = (*irgraph* (((*nid, k*) # *g*)))
proof (*cases fst k = NoNode*)
  case *True*
  then show *?thesis*
    by (*metis* (*mono-tags, lifting*) *Rep-IRGraph-inject filter.simps*(*2*) *irgraph.abs-eq no-node.simps replace-node.rep-eq snd-conv*)
next
  case *False*
  then show *?thesis* **unfolding** *irgraph-def replace-node-def no-node.simps*
    by (*smt* (*verit, best*) *Rep-IRGraph comp-apply eq-onp-same-args filter.simps*(*2*) *id-def irgraph.rep-eq map-fun-apply map-of-upd mem-Collect-eq no-node.elims replace-node.abs-eq replace-node-def snd-eqD*)
qed

lemma [*code*]: *add-node nid k* (*irgraph g*) = (*irgraph* (((*nid, k*) # *g*)))
  by (*smt* (*z3*) *Rep-IRGraph-inject add-node.rep-eq filter.simps*(*2*) *irgraph.rep-eq map-of-upd no-node.simps snd-conv*)

lemma *add-node-lookup*:
  gup = add-node nid (*k, s*) *g* $\longrightarrow$
  (*if k $\neq$ NoNode then kind gup nid = k $\wedge$ stamp gup nid = s else kind gup nid = kind g nid*)
proof (*cases k = NoNode*)

37

case *True*
then show *?thesis*
   by (*simp add*: *add-node.rep-eq kind.rep-eq*)
next
  case *False*
  then show *?thesis*
    by (*simp add*: *kind.rep-eq add-node.rep-eq stamp.rep-eq*)
qed

lemma *remove-node-lookup*:
  gup = remove-node nid g $\longrightarrow$ *kind gup nid = NoNode* $\land$ *stamp gup nid = IllegalStamp*
  by (*simp add*: *kind.rep-eq remove-node.rep-eq stamp.rep-eq*)

lemma *replace-node-lookup*[*simp*]:
  gup = replace-node nid (*k, s*) *g* $\land$ *k* $\neq$ *NoNode* $\longrightarrow$ *kind gup nid = k* $\land$ *stamp gup nid = s*
  by (*simp add*: *replace-node.rep-eq kind.rep-eq stamp.rep-eq*)

lemma *replace-node-unchanged*:
  gup = replace-node nid (*k, s*) *g* $\longrightarrow$ ($\forall$ *n* $\in$ (*ids g* $-$ {*nid*}) . *n* $\in$ *ids g* $\land$ *n* $\in$ *ids gup* $\land$ *kind g n = kind gup n*)
  by (*simp add*: *kind.rep-eq replace-node.rep-eq*)

5.0.1 Example Graphs

Example 1: empty graph (just a start and end node)

definition *start-end-graph*:: *IRGraph* **where**
  start-end-graph = irgraph [(*0, StartNode None 1, VoidStamp*), (*1, ReturnNode None None, VoidStamp*)]

Example 2: public static int sq(int x) return x * x;

[1 P(0)] / [0 Start] [4 *] | / V / [5 Return]

definition *eg2-sq* :: *IRGraph* **where**
  eg2-sq = irgraph [
   (*0, StartNode None 5, VoidStamp*),
   (*1, ParameterNode 0, default-stamp*),
   (*4, MulNode 1 1, default-stamp*),
   (*5, ReturnNode* (*Some 4*) *None, default-stamp*)
  ]

value *input-edges eg2-sq*
value *usages eg2-sq 1*

end

38

5.1 Control-flow Graph Traversal

theory
  Traversal
imports
  IRGraph
begin

type-synonym *Seen = ID set*

nextEdge helps determine which node to traverse next by returning the first successor edge that isn't in the set of already visited nodes. If there is not an appropriate successor, None is returned instead.

fun *nextEdge* :: *Seen ⇒ ID ⇒ IRGraph ⇒ ID option* **where**
  nextEdge seen nid g =
    (let nids = (filter (λnid′. nid′ ∉ seen) (successors-of (kind g nid))) in
    (if length nids > 0 then Some (hd nids) else None))

pred determines which node, if any, acts as the predecessor of another.

Merge nodes represent a special case where-in the predecessor exists as an input edge of the merge node, to simplify the traversal we treat only the first input end node as the predecessor, ignoring that multiple nodes may act as a successor.

For all other nodes, the predecessor is the first element of the predecessors set. Note that in a well-formed graph there should only be one element in the predecessor set.

fun *pred* :: *IRGraph ⇒ ID ⇒ ID option* **where**
  pred g nid = (case kind g nid of
    (MergeNode ends - -) ⇒ Some (hd ends) |
    - ⇒
      (if IRGraph.predecessors g nid = {}
        then None else
        Some (hd (sorted-list-of-set (IRGraph.predecessors g nid)))
)
)

Here we try to implement a generic fork of the control-flow traversal algorithm that was initially implemented for the ConditionalElimination phase

type-synonym *′a TraversalState = (ID × Seen × ′a)*

inductive *Step*
  :: *(′a TraversalState ⇒ ′a) ⇒ IRGraph ⇒ ′a TraversalState ⇒ ′a TraversalState option ⇒ bool*
  for *sa g* **where**
  — Hit a BeginNode with an IfNode predecessor which represents the start of a basic block for the IfNode. 1. nid' will be the successor of the begin node. 2. Find the first and only predecessor. 3. Extract condition from the preceding IfNode. 4.

39

Negate condition if the begin node is second branch (we've taken the else branch of the condition) 5. Add the condition or the negated condition to stack 6. Perform any stamp updates based on the condition using the registerNewCondition function and place them on the top of the stack of stamp information

$\llbracket$ *kind g nid = BeginNode nid′*;

 nid ∉ seen;
 seen′ = {nid} ∪ seen;

 Some ifcond = pred g nid;
 kind g ifcond = IfNode cond t f;

 analysis′ = sa (nid, seen, analysis) $\rrbracket$
 $\implies$ *Step sa g (nid, seen, analysis) (Some (nid′, seen′, analysis′))* |

— Hit an EndNode 1. nid' will be the usage of EndNode 2. pop the conditions and stamp stack

$\llbracket$ *kind g nid = EndNode*;

 nid ∉ seen;
 seen′ = {nid} ∪ seen;

 nid′ = any-usage g nid;

 analysis′ = sa (nid, seen, analysis) $\rrbracket$
 $\implies$ *Step sa g (nid, seen, analysis) (Some (nid′, seen′, analysis′))* |

— We can find a successor edge that is not in seen, go there
$\llbracket$ ¬(*is-EndNode (kind g nid)*);
 ¬(*is-BeginNode (kind g nid)*);

 nid ∉ seen;
 seen′ = {nid} ∪ seen;

 Some nid′ = nextEdge seen′ nid g;

 analysis′ = sa (nid, seen, analysis) $\rrbracket$
 $\implies$ *Step sa g (nid, seen, analysis) (Some (nid′, seen′, analysis′))* |

— We can cannot find a successor edge that is not in seen, give back None
$\llbracket$ ¬(*is-EndNode (kind g nid)*);
 ¬(*is-BeginNode (kind g nid)*);

 nid ∉ seen;
 seen′ = {nid} ∪ seen;

 None = nextEdge seen′ nid g $\rrbracket$
 $\implies$ *Step sa g (nid, seen, analysis) None* |

— We've already seen this node, give back None
⟦*nid* ∈ *seen*⟧ ⟹ *Step sa g* (*nid*, *seen*, *analysis*) *None*

code-pred (*modes*: $i \Rightarrow i \Rightarrow i \Rightarrow o \Rightarrow bool$) *Step* **.**

end

5.2 Structural Graph Comparison

theory
  Comparison
imports
  IRGraph
begin

We introduce a form of structural graph comparison that is able to assert structural equivalence of graphs which differ in zero or more reference node chains for any given nodes.

fun *find-ref-nodes* :: *IRGraph* ⇒ (*ID* ⇀ *ID*) **where**
find-ref-nodes g = map-of
 (*map* (λ*n*. (*n*, *ir-ref* (*kind g n*))) (*filter* (λ*id*. *is-RefNode* (*kind g id*)) (*sorted-list-of-set*
(*ids g*))))

fun *replace-ref-nodes* :: *IRGraph* ⇒ (*ID* ⇀ *ID*) ⇒ *ID list* ⇒ *ID list* **where**
replace-ref-nodes g m xs = map (λ*id*. (*case* (*m id*) *of Some other* ⇒ *other* | *None*
⇒ *id*)) *xs*

fun *find-next* :: *ID list* ⇒ *ID set* ⇒ *ID option* **where**
  find-next to-see seen = (*let l* = (*filter* (λ*nid*. *nid* ∉ *seen*) *to-see*)
    in (*case l of* [] ⇒ *None* | *xs* ⇒ *Some* (*hd xs*)))

inductive *reachables* :: *IRGraph* ⇒ *ID list* ⇒ *ID set* ⇒ *ID set* ⇒ *bool* **where**
reachables g [] {} {} |
⟦*None* = *find-next to-see seen*⟧ ⟹ *reachables g to-see seen seen* |
⟦*Some n* = *find-next to-see seen*;
  node = *kind g n*;
  new = (*inputs-of node*) @ (*successors-of node*);
  reachables g (*to-see* @ *new*) ({*n*} ∪ *seen*) *seen*′ ⟧ ⟹ *reachables g to-see seen*
seen′

code-pred (*modes*: $i \Rightarrow i \Rightarrow i \Rightarrow o \Rightarrow bool$) [*show-steps*,*show-mode-inference*,*show-intermediate-results*]

reachables **.**

inductive *nodeEq* :: (*ID* ⇀ *ID*) ⇒ *IRGraph* ⇒ *ID* ⇒ *IRGraph* ⇒ *ID* ⇒ *bool*
where
⟦ *kind g1 n1* = *RefNode ref*; *nodeEq m g1 ref g2 n2* ⟧ ⟹ *nodeEq m g1 n1 g2 n2* |
⟦ *x* = *kind g1 n1*;
  y = *kind g2 n2*;

41

is-same-ir-node-type x y;
replace-ref-nodes g1 m (*successors-of x*) = *successors-of y*;
replace-ref-nodes g1 m (*inputs-of x*) = *inputs-of y* ⟧
⟹ *nodeEq m g1 n1 g2 n2*

code-pred [*show-modes*] *nodeEq* **.**

fun *diffNodesGraph* :: *IRGraph* ⇒ *IRGraph* ⇒ *ID set* **where**
diffNodesGraph g1 g2 = (*let refNodes* = *find-ref-nodes g1 in*
    { *n . n* ∈ *Predicate.the* (*reachables-i-i-i-o g1* [*0*] {}) ∧ (*case refNodes n of Some*
- ⇒ False | - ⇒ True) ∧ ¬(*nodeEq refNodes g1 n g2 n*)})

fun *diffNodesInfo* :: *IRGraph* ⇒ *IRGraph* ⇒ (*ID* × *IRNode* × *IRNode*) *set* **where**
diffNodesInfo g1 g2 = {(*nid, kind g1 nid, kind g2 nid*) | *nid . nid* ∈ *diffNodesGraph g1 g2*}

fun *eqGraph* :: *IRGraph* ⇒ *IRGraph* ⇒ *bool* **where**
eqGraph isabelle-graph graal-graph = ((*diffNodesGraph isabelle-graph graal-graph*) = {})

end

6 Data-flow Semantics

theory *IRTreeEval*
  imports
    Graph.Stamp
begin

We define a tree representation of data-flow nodes, as an abstraction of the graph view.

Data-flow trees are evaluated in the context of a method state (currently called MapState in the theories for historical reasons).

The method state consists of the values for each method parameter, references to method parameters use an index of the parameter within the parameter list, as such we store a list of parameter values which are looked up at parameter references.

The method state also stores a mapping of node ids to values. The contents of this mapping is calculates during the traversal of the control flow graph.

As a concrete example, as the *SignedDivNode* can have side-effects (during division by zero), it is treated as part of the control-flow, since the data-flow phase is specified to be side-effect free. As a result, the control-flow semantics for *SignedDivNode* calculates the value of a node and maps the node identifier to the value within the method state. The data-flow semantics then just reads the value stored in the method state for the node.

type-synonym *ID = nat*
type-synonym *MapState = ID ⇒ Value*
type-synonym *Params = Value list*

definition *new-map-state* :: *MapState* **where**
  new-map-state = (λx. UndefVal)

6.1   Data-flow Tree Representation

datatype *IRUnaryOp =*
    UnaryAbs
  | *UnaryNeg*
  | *UnaryNot*
  | *UnaryLogicNegation*
  | *UnaryNarrow* (*ir-inputBits*: *nat*) (*ir-resultBits*: *nat*)
  | *UnarySignExtend* (*ir-inputBits*: *nat*) (*ir-resultBits*: *nat*)
  | *UnaryZeroExtend* (*ir-inputBits*: *nat*) (*ir-resultBits*: *nat*)

datatype *IRBinaryOp =*
    BinAdd
  | *BinMul*
  | *BinSub*
  | *BinAnd*
  | *BinOr*
  | *BinXor*
  | *BinShortCircuitOr*
  | *BinLeftShift*
  | *BinRightShift*
  | *BinURightShift*
  | *BinIntegerEquals*
  | *BinIntegerLessThan*
  | *BinIntegerBelow*

datatype (*discs-sels*) *IRExpr =*
    UnaryExpr (*ir-uop*: *IRUnaryOp*) (*ir-value*: *IRExpr*)
  | *BinaryExpr* (*ir-op*: *IRBinaryOp*) (*ir-x*: *IRExpr*) (*ir-y*: *IRExpr*)
  | *ConditionalExpr* (*ir-condition*: *IRExpr*) (*ir-trueValue*: *IRExpr*) (*ir-falseValue*:
IRExpr)

  | *ParameterExpr* (*ir-index*: *nat*) (*ir-stamp*: *Stamp*)

  | *LeafExpr* (*ir-nid*: *ID*) (*ir-stamp*: *Stamp*)

  | *ConstantExpr* (*ir-const*: *Value*)
  | *ConstantVar* (*ir-name*: *string*)
  | *VariableExpr* (*ir-name*: *string*) (*ir-stamp*: *Stamp*)

fun *is-ground* :: *IRExpr ⇒ bool* **where**

is-ground (*UnaryExpr op e*) = *is-ground e* |
is-ground (*BinaryExpr op e1 e2*) = (*is-ground e1* ∧ *is-ground e2*) |
is-ground (*ConditionalExpr b e1 e2*) = (*is-ground b* ∧ *is-ground e1* ∧ *is-ground e2*) |
is-ground (*ParameterExpr i s*) = *True* |
is-ground (*LeafExpr n s*) = *True* |
is-ground (*ConstantExpr v*) = *True* |
is-ground (*ConstantVar name*) = *False* |
is-ground (*VariableExpr name s*) = *False*

typedef *GroundExpr* = { *e* :: *IRExpr* . *is-ground e* }
  using *is-ground.simps*(*6*) **by** *blast*

6.2 Functions for re-calculating stamps

Note: all integer calculations are done as 32 or 64 bit calculations. Most operators have the same output bits as their inputs. But the following $fixed_32$ binary operators always output 32 bits. And the unary operators that are not $normal_unary$ are narrowing or widening operators, so the result bits is specified by the operator.

abbreviation *fixed-32* :: *IRBinaryOp set* **where**
  fixed-32 ≡ {*BinShortCircuitOr*, *BinIntegerEquals*, *BinIntegerLessThan*, *BinIntegerBelow*}

abbreviation *normal-unary* :: *IRUnaryOp set* **where**
  normal-unary ≡ {*UnaryAbs*, *UnaryNeg*, *UnaryNot*, *UnaryLogicNegation*}

fun *stamp-unary* :: *IRUnaryOp* ⇒ *Stamp* ⇒ *Stamp* **where**

  stamp-unary op (*IntegerStamp b lo hi*) =
    (*if op* ∈ *normal-unary*
     then unrestricted-stamp (*IntegerStamp* (*if b=64 then 64 else 32*) *lo hi*)
     else unrestricted-stamp (*IntegerStamp* (*ir-resultBits op*) *lo hi*)) |

  stamp-unary op - = *IllegalStamp*

fun *stamp-binary* :: *IRBinaryOp* ⇒ *Stamp* ⇒ *Stamp* ⇒ *Stamp* **where**
  stamp-binary op (*IntegerStamp b1 lo1 hi1*) (*IntegerStamp b2 lo2 hi2*) =
    (*if* (*b1* ≠ *b2*) *then IllegalStamp else*
      (*if op* ∉ *fixed-32* ∧ *b1=64*
       then unrestricted-stamp (*IntegerStamp 64 lo1 hi1*)
       else unrestricted-stamp (*IntegerStamp 32 lo1 hi1*))) |

  stamp-binary op - - = *IllegalStamp*

fun *stamp-expr* :: *IRExpr* ⇒ *Stamp* **where**
  stamp-expr (*UnaryExpr op x*) = *stamp-unary op* (*stamp-expr x*) |
  stamp-expr (*BinaryExpr bop x y*) = *stamp-binary bop* (*stamp-expr x*) (*stamp-expr*

y) |
  stamp-expr (*ConstantExpr val*) = *constantAsStamp val* |
  stamp-expr (*LeafExpr i s*) = *s* |
  stamp-expr (*ParameterExpr i s*) = *s* |
  stamp-expr (*ConditionalExpr c t f*) = *meet* (*stamp-expr t*) (*stamp-expr f*)

export-code *stamp-unary stamp-binary stamp-expr*

6.3 Data-flow Tree Evaluation

fun *unary-eval* :: *IRUnaryOp* ⇒ *Value* ⇒ *Value* **where**
  unary-eval UnaryAbs v = *intval-abs v* |
  unary-eval UnaryNeg v = *intval-negate v* |
  unary-eval UnaryNot v = *intval-not v* |
  unary-eval UnaryLogicNegation v = *intval-logic-negation v* |
  unary-eval (*UnaryNarrow inBits outBits*) *v* = *intval-narrow inBits outBits v* |
 unary-eval (*UnarySignExtend inBits outBits*) *v* = *intval-sign-extend inBits outBits v* |
 unary-eval (*UnaryZeroExtend inBits outBits*) *v* = *intval-zero-extend inBits outBits v*

fun *bin-eval* :: *IRBinaryOp* ⇒ *Value* ⇒ *Value* ⇒ *Value* **where**
  bin-eval BinAdd v1 v2 = *intval-add v1 v2* |
  bin-eval BinMul v1 v2 = *intval-mul v1 v2* |
  bin-eval BinSub v1 v2 = *intval-sub v1 v2* |
  bin-eval BinAnd v1 v2 = *intval-and v1 v2* |
  bin-eval BinOr v1 v2 = *intval-or v1 v2* |
  bin-eval BinXor v1 v2 = *intval-xor v1 v2* |
  bin-eval BinShortCircuitOr v1 v2 = *intval-short-circuit-or v1 v2* |
  bin-eval BinLeftShift v1 v2 = *intval-left-shift v1 v2* |
  bin-eval BinRightShift v1 v2 = *intval-right-shift v1 v2* |
  bin-eval BinURightShift v1 v2 = *intval-uright-shift v1 v2* |
  bin-eval BinIntegerEquals v1 v2 = *intval-equals v1 v2* |
  bin-eval BinIntegerLessThan v1 v2 = *intval-less-than v1 v2* |
  bin-eval BinIntegerBelow v1 v2 = *intval-below v1 v2*

lemmas *eval-thms* =
  intval-abs.simps intval-negate.simps intval-not.simps
  intval-logic-negation.simps intval-narrow.simps
  intval-sign-extend.simps intval-zero-extend.simps
  intval-add.simps intval-mul.simps intval-sub.simps
  intval-and.simps intval-or.simps intval-xor.simps
  intval-left-shift.simps intval-right-shift.simps
  intval-uright-shift.simps intval-equals.simps
  intval-less-than.simps intval-below.simps

inductive *not-undef-or-fail* :: *Value* ⇒ *Value* ⇒ *bool* **where**

$\llbracket value \neq\ UndefVal\rrbracket \Longrightarrow not\text{-}undef\text{-}or\text{-}fail\ value\ value$

notation (*latex* **output**)
  not-undef-or-fail (*- = -*)

inductive
  evaltree :: MapState ⇒ Params ⇒ IRExpr ⇒ Value ⇒ bool ([-,-] ⊢ - ↦ - *55*)
  for *m p* **where**

  ConstantExpr:
  $\llbracket valid\text{-}value\ c\ (constantAsStamp\ c)\rrbracket$
    $\Longrightarrow [m,p] \vdash (ConstantExpr\ c) \mapsto c$ |

  ParameterExpr:
  $\llbracket i < length\ p;\ valid\text{-}value\ (p!i)\ s\rrbracket$
    $\Longrightarrow [m,p] \vdash (ParameterExpr\ i\ s) \mapsto p!i$ |

  ConditionalExpr:
  $\llbracket [m,p] \vdash ce \mapsto cond;$
    branch = (if val-to-bool cond then te else fe);
    $[m,p] \vdash branch \mapsto v;$
    $v \neq UndefVal\rrbracket$
    $\Longrightarrow [m,p] \vdash (ConditionalExpr\ ce\ te\ fe) \mapsto v$ |

  UnaryExpr:
  $\llbracket [m,p] \vdash xe \mapsto v;$
    result = (unary-eval op v);
    $result \neq UndefVal\rrbracket$
    $\Longrightarrow [m,p] \vdash (UnaryExpr\ op\ xe) \mapsto result$ |

  BinaryExpr:
  $\llbracket [m,p] \vdash xe \mapsto x;$
    $[m,p] \vdash ye \mapsto y;$
    result = (bin-eval op x y);
    $result \neq UndefVal\rrbracket$
    $\Longrightarrow [m,p] \vdash (BinaryExpr\ op\ xe\ ye) \mapsto result$ |

  LeafExpr:
  $\llbracket val = m\ n;$
    valid-value val s$\rrbracket$
    $\Longrightarrow [m,p] \vdash LeafExpr\ n\ s \mapsto val$

code-pred (*modes: i ⇒ i ⇒ i ⇒ o ⇒ bool as evalT*)
  [*show-steps,show-mode-inference,show-intermediate-results*]
  evaltree **.**

inductive
  evaltrees :: MapState ⇒ Params ⇒ IRExpr list ⇒ Value list ⇒ bool ([-,-] ⊢ - ↦$_L$

- 55)
  for *m p* **where**

  EvalNil:
  $[m,p] \vdash [] \mapsto_L []$ |

  EvalCons:
  $[\![m,p] \vdash x \mapsto xval;$
    $[m,p] \vdash yy \mapsto_L yyval]\!]$
    $\implies [m,p] \vdash (x\#yy) \mapsto_L (xval\#yyval)$

code-pred (*modes*: $i \Rightarrow i \Rightarrow i \Rightarrow o \Rightarrow bool$ *as evalTs*)
  evaltrees **.**

definition *sq-param0* :: *IRExpr* **where**
  sq-param0 = BinaryExpr BinMul
    (*ParameterExpr 0* (*IntegerStamp 32* ($-$ *2147483648*) *2147483647*))
    (*ParameterExpr 0* (*IntegerStamp 32* ($-$ *2147483648*) *2147483647*))

values {*v. evaltree new-map-state* [*IntVal32 5*] *sq-param0 v*}

declare *evaltree.intros* [*intro*]
declare *evaltrees.intros* [*intro*]

6.4   Data-flow Tree Refinement

We define the induced semantic equivalence relation between expressions. Note that syntactic equality implies semantic equivalence, but not vice versa.

definition *equiv-exprs* :: *IRExpr* $\Rightarrow$ *IRExpr* $\Rightarrow$ *bool* (*-* $\doteq$ *- 55*) **where**
  $(e1 \doteq e2) = (\forall\ m\ p\ v.\ (([m,p] \vdash e1 \mapsto v) \longleftrightarrow ([m,p] \vdash e2 \mapsto v)))$

We also prove that this is a total equivalence relation (*equivp equiv-exprs*) (HOL.Equiv_Relations), so that we can reuse standard results about equivalence relations.

lemma *equivp equiv-exprs*
  apply (*auto simp add*: *equivp-def equiv-exprs-def*)
  by (*metis equiv-exprs-def*)+

We define a refinement ordering over IRExpr and show that it is a preorder. Note that it is asymmetric because e2 may refer to fewer variables than e1.

instantiation *IRExpr* :: *preorder* **begin**

notation *less-eq* (**infix** $\sqsubseteq$ *65*)

definition

le-expr-def [*simp*]:
  $(e_2 \leq e_1) \longleftrightarrow (\forall\ m\ p\ v.\ (([m,p] \vdash e_1 \mapsto v) \longrightarrow ([m,p] \vdash e_2 \mapsto v)))$

definition
  lt-expr-def [*simp*]:
  $(e_1 < e_2) \longleftrightarrow (e_1 \leq e_2 \wedge \neg (e_1 \doteq e_2))$

instance proof
  fix x y z :: *IRExpr*
  show $x < y \longleftrightarrow x \leq y \wedge \neg (y \leq x)$ **by** (*simp add: equiv-exprs-def*; *auto*)
  show $x \leq x$ **by** *simp*
  show $x \leq y \Longrightarrow y \leq z \Longrightarrow x \leq z$ **by** *simp*
qed

end

abbreviation (**output**) *Refines* :: *IRExpr* $\Rightarrow$ *IRExpr* $\Rightarrow$ *bool* (**infix** $\sqsupseteq$ *64*)
  where $e_1 \sqsupseteq e_2 \equiv (e_2 \leq e_1)$

end

6.5   Data-flow Tree Theorems

theory *IRTreeEvalThms*
  imports
    IRTreeEval
begin

6.5.1   Deterministic Data-flow Evaluation

lemma *evalDet*:
  $[m,p] \vdash e \mapsto v_1 \Longrightarrow$
  $[m,p] \vdash e \mapsto v_2 \Longrightarrow$
  $v_1 = v_2$
  apply (*induction arbitrary*: v_2 *rule*: *evaltree.induct*)
  by (*elim EvalTreeE*; *auto*)+

lemma *evalAllDet*:
  $[m,p] \vdash e \mapsto_L v1 \Longrightarrow$
  $[m,p] \vdash e \mapsto_L v2 \Longrightarrow$
  $v1 = v2$
  apply (*induction arbitrary*: *v2 rule*: *evaltrees.induct*)
   apply (*elim EvalTreeE*; *auto*)
  using *evalDet* **by** *force*

6.5.2   Typing Properties for Integer Evaluation Functions

We use three simple typing properties on integer values: $is_IntVal32, is_IntVal64$ and the more general is_IntVal.

lemma *unary-eval-not-obj-ref*:
  shows *unary-eval op x $\neq$ ObjRef v*
  by (*cases op*; *cases x*; *auto*)

lemma *unary-eval-not-obj-str*:
  shows *unary-eval op x $\neq$ ObjStr v*
  by (*cases op*; *cases x*; *auto*)

lemma *unary-eval-int*:
  assumes *def*: *unary-eval op x $\neq$ UndefVal*
  shows *is-IntVal* (*unary-eval op x*)
  unfolding *is-IntVal-def* **using** *def*
  apply (*cases unary-eval op x*; *auto*)
  using *unary-eval-not-obj-ref unary-eval-not-obj-str* **by** *simp+*

lemma *bin-eval-int*:
  assumes *def*: *bin-eval op x y $\neq$ UndefVal*
  shows *is-IntVal* (*bin-eval op x y*)
  apply (*cases op*; *cases x*; *cases y*)
  unfolding *is-IntVal-def* **using** *def* **apply** *auto*
  by (*metis* (*full-types*) *bool-to-val.simps is-IntVal32-def*)+

lemma *int-stamp32*:
  assumes *i*: *is-IntVal32 v*
  shows *is-IntegerStamp* (*constantAsStamp v*)
  using *i* **unfolding** *is-IntegerStamp-def is-IntVal32-def* **by** *auto*

lemma *int-stamp64*:
  assumes *i*: *is-IntVal64 v*
  shows *is-IntegerStamp* (*constantAsStamp v*)
  using *i* **unfolding** *is-IntegerStamp-def is-IntVal64-def* **by** *auto*

lemma *int-stamp-both*:
  assumes *i*: *is-IntVal v*
  shows *is-IntegerStamp* (*constantAsStamp v*)
  using *i* **unfolding** *is-IntVal-def is-IntegerStamp-def*
  using *int-stamp32 int-stamp64 is-IntegerStamp-def* **by** *auto*

lemma *validDefIntConst*:
  assumes *v $\neq$ UndefVal*
  assumes *is-IntegerStamp* (*constantAsStamp v*)
  shows *valid-value v* (*constantAsStamp v*)
  using *assms* **by** (*cases v*; *auto*)

lemma *validIntConst*:
  assumes *i*: *is-IntVal v*
  shows *valid-value v* (*constantAsStamp v*)

using *i int-stamp-both is-IntVal-def validDefIntConst* **by** *auto*

6.5.3 Evaluation Results are Valid

A valid value cannot be *UndefVal*.

lemma *valid-not-undef*:
  assumes *a1*: *valid-value val s*
  assumes *a2*: *s* $\neq$ *VoidStamp*
  shows *val* $\neq$ *UndefVal*
  apply (*rule valid-value.elims(1)[of val s True]*)
  using *a1 a2* **by** *auto*

lemma *valid-VoidStamp*[*elim*]:
  shows *valid-value val VoidStamp* $\Longrightarrow$
    val = *UndefVal*
  using *valid-value.simps* **by** *metis*

lemma *valid-ObjStamp*[*elim*]:
  shows *valid-value val* (*ObjectStamp klass exact nonNull alwaysNull*) $\Longrightarrow$
    ($\exists v.$ *val* = *ObjRef v*)
  using *valid-value.simps* **by** (*metis val-to-bool.cases*)

lemma *valid-int1*[*elim*]:
  shows *valid-value val* (*IntegerStamp 1 lo hi*) $\Longrightarrow$
    ($\exists v.$ *val* = *IntVal32 v*)
  apply (*rule val-to-bool.cases[of val]*)
  using *Value.distinct* **by** *simp*+

lemma *valid-int8*[*elim*]:
  shows *valid-value val* (*IntegerStamp 8 l h*) $\Longrightarrow$
    ($\exists v.$ *val* = *IntVal32 v*)
  apply (*rule val-to-bool.cases[of val]*)
  using *Value.distinct* **by** *simp*+

lemma *valid-int16*[*elim*]:
  shows *valid-value val* (*IntegerStamp 16 l h*) $\Longrightarrow$
    ($\exists v.$ *val* = *IntVal32 v*)
  apply (*rule val-to-bool.cases[of val]*)
  using *Value.distinct* **by** *simp*+

lemma *valid-int32*[*elim*]:
  shows *valid-value val* (*IntegerStamp 32 l h*) $\Longrightarrow$
    ($\exists v.$ *val* = *IntVal32 v*)
  apply (*rule val-to-bool.cases[of val]*)
  using *Value.distinct* **by** *simp*+

lemma *valid-int64*[*elim*]:
  shows *valid-value val* (*IntegerStamp 64 l h*) $\Longrightarrow$

$(\exists\, v.\ val = IntVal64\ v)$

apply (*rule val-to-bool.cases*[*of val*])

using *Value.distinct* **by** *simp+*

lemmas *valid-value-elims* =
  valid-VoidStamp
  valid-ObjStamp
  valid-int1
  valid-int8
  valid-int16
  valid-int32
  valid-int64

lemma *evaltree-not-undef*:
  fixes *m p e v*
  shows $([m,p] \vdash e \mapsto v) \implies v \neq UndefVal$
  apply (*induction rule: evaltree.induct*)
  using *valid-not-undef* **by** *auto*

lemma *leafint32*:
  assumes *ev*: $[m,p] \vdash LeafExpr\ i\ (IntegerStamp\ 32\ lo\ hi) \mapsto val$
  shows $\exists\, v.\ val = (IntVal32\ v)$

proof −
  have *valid-value val* (*IntegerStamp 32 lo hi*)
    using *ev* **by** (*rule LeafExprE*; *simp*)
  then show *?thesis* **by** *auto*
qed

lemma *leafint64*:
  assumes *ev*: $[m,p] \vdash LeafExpr\ i\ (IntegerStamp\ 64\ lo\ hi) \mapsto val$
  shows $\exists\, v.\ val = (IntVal64\ v)$

proof −
  have *valid-value val* (*IntegerStamp 64 lo hi*)
    using *ev* **by** (*rule LeafExprE*; *simp*)
  then show *?thesis* **by** *auto*
qed

lemma *default-stamp* [*simp*]: *default-stamp* = *IntegerStamp* *32* (-2147483648)
2147483647
  using *default-stamp-def* **by** *auto*

lemma *valid32* [*simp*]:
  assumes *valid-value val* (*IntegerStamp 32 lo hi*)
  shows $\exists\, v.\ (val = (IntVal32\ v) \wedge lo \leq sint\ v \wedge sint\ v \leq hi)$

using *assms valid-int32* **by** *force*

lemma *valid64* [*simp*]:
  assumes *valid-value val* (*IntegerStamp 64 lo hi*)
  shows $\exists\, v.\ (val = (IntVal64\ v) \wedge lo \leq sint\ v \wedge sint\ v \leq hi)$
  using *assms valid-int64* **by** *force*

lemma *valid32or64*:
  assumes *valid-value x* (*IntegerStamp b lo hi*)
  shows $(\exists\ v1.\ (x = IntVal32\ v1)) \vee (\exists\ v2.\ (x = IntVal64\ v2))$
  using *valid32 valid64 assms valid-value.elims(2)* **by** *blast*

lemma *valid32or64-both*:
  assumes *valid-value x* (*IntegerStamp b lox hix*)
  and *valid-value y* (*IntegerStamp b loy hiy*)
  shows $(\exists\ v1\ v2.\ x = IntVal32\ v1 \wedge y = IntVal32\ v2) \vee (\exists\ v3\ v4.\ x = IntVal64\ v3 \wedge y = IntVal64\ v4)$
  using *assms valid32or64 valid32* **by** (*metis valid-int64 valid-value.simps(2)*)

6.5.4   Example Data-flow Optimisations

lemma *a0a-helper* [*simp*]:
  assumes *a*: *valid-value v* (*IntegerStamp 32 lo hi*)
  shows *intval-add v* (*IntVal32 0*) = *v*
proof −
  obtain *v32* :: *int32* **where** *v = (IntVal32 v32)* **using** *a valid32* **by** *blast*
  then show *?thesis* **by** *simp*
qed

lemma *a0a*: (*BinaryExpr BinAdd* (*LeafExpr 1 default-stamp*) (*ConstantExpr* (*IntVal32 0*)))
         $\geq$ (*LeafExpr 1 default-stamp*)
  by (*auto simp add*: *evaltree.LeafExpr*)

lemma *xyx-y-helper* [*simp*]:
  assumes *valid-value x* (*IntegerStamp 32 lox hix*)
  assumes *valid-value y* (*IntegerStamp 32 loy hiy*)
  shows *intval-add x* (*intval-sub y x*) = *y*
proof −
  obtain *x32* :: *int32* **where** *x*: *x = (IntVal32 x32)* **using** *assms valid32* **by** *blast*
  obtain *y32* :: *int32* **where** *y*: *y = (IntVal32 y32)* **using** *assms valid32* **by** *blast*
  show *?thesis* **using** *x y* **by** *simp*
qed

lemma *xyx-y*:
  (*BinaryExpr BinAdd*
    (*LeafExpr x* (*IntegerStamp 32 lox hix*))

```
      (BinaryExpr BinSub
        (LeafExpr y (IntegerStamp 32 loy hiy))
        (LeafExpr x (IntegerStamp 32 lox hix))))
 ≥ (LeafExpr y (IntegerStamp 32 loy hiy))
 by (auto simp add: LeafExpr)
```

6.5.5   Monotonicity of Expression Refinement

We prove that each subexpression position is monotonic. That is, optimizing
a subexpression anywhere deep inside a top-level expression also optimizes
that top-level expression.

Note that we might also be able to do this via reusing Isabelle's *mono* opera-
tor (HOL.Orderings theory), proving instantiations like *mono(UnaryExprop)*,
but it is not obvious how to do this for both arguments of the binary ex-
pressions.

lemma *mono-unary*:
  assumes $e \geq e'$
  shows ($UnaryExpr\ op\ e$) $\geq$ ($UnaryExpr\ op\ e'$)
  using *UnaryExpr assms* **by** *auto*

lemma *mono-binary*:
  assumes $x \geq x'$
  assumes $y \geq y'$
  shows ($BinaryExpr\ op\ x\ y$) $\geq$ ($BinaryExpr\ op\ x'\ y'$)
  using *BinaryExpr assms* **by** *auto*

lemma *never-void*:
  assumes $[m,\ p] \vdash x \mapsto xv$
  assumes *valid-value xv* ($stamp\text{-}expr\ xe$)
  shows $stamp\text{-}expr\ xe \neq VoidStamp$
  using *valid-value.simps*
  using *assms(2)* **by** *force*

lemma *compatible-trans*:
  compatible x y $\wedge$ *compatible y z* $\implies$ *compatible x z*
  by (*smt* (*verit, best*) *compatible.elims(2) compatible.simps(1)*)

lemma *compatible-refl*:
  compatible x y $\implies$ *compatible y x*
  using *compatible.elims(2)* **by** *fastforce*

lemma *mono-conditional*:

    assumes *ce* $\geq$ *ce$'$*
    assumes *te* $\geq$ *te$'$*
    assumes *fe* $\geq$ *fe$'$*
    shows (*ConditionalExpr ce te fe*) $\geq$ (*ConditionalExpr ce$'$ te$'$ fe$'$*)
proof (*simp only*: *le-expr-def*; (*rule allI*)+; *rule impI*)
  fix *m p v*
  assume *a*: [*m,p*] $\vdash$ *ConditionalExpr ce te fe* $\mapsto$ *v*
  then obtain *cond* **where** *ce*: [*m,p*] $\vdash$ *ce* $\mapsto$ *cond* **by** *auto*
  then have *ce$'$*: [*m,p*] $\vdash$ *ce$'$* $\mapsto$ *cond* **using** *assms* **by** *auto*

  define *branch* **where** *b*: *branch* = (*if val-to-bool cond then te else fe*)
  define *branch$'$* **where** *b$'$*: *branch$'$* = (*if val-to-bool cond then te$'$ else fe$'$*)
  then have *beval*: [*m,p*] $\vdash$ *branch* $\mapsto$ *v* **using** *a b ce evalDet* **by** *blast*

  from *beval* **have** [*m,p*] $\vdash$ *branch$'$* $\mapsto$ *v* **using** *assms b b$'$* **by** *auto*
  then show [*m,p*] $\vdash$ *ConditionalExpr ce$'$ te$'$ fe$'$* $\mapsto$ *v*
    using *ConditionalExpr ce$'$ b$'$*
    using *a* **by** *blast*
qed

6.6 Unfolding rules for evaltree quadruples down to bin-eval level

These rewrite rules can be useful when proving optimizations. They support top-down rewriting of each level of the tree into the lower-level *bin$_e$val* / *unary$_e$val* level, simply by saying *unfoldingunfold$_e$evaltree*.

lemma *unfold-valid32* [*simp*]:
  valid-value y (*constantAsStamp* (*IntVal32 v*)) = (*y* = *IntVal32 v*)
  by (*induction y*; *auto dest*: *signed-word-eqI*)

lemma *unfold-valid64* [*simp*]:
  valid-value y (*constantAsStamp* (*IntVal64 v*)) = (*y* = *IntVal64 v*)
  by (*induction y*; *auto dest*: *signed-word-eqI*)

lemma *unfold-const*:
  shows ([*m,p*] $\vdash$ *ConstantExpr c* $\mapsto$ *v*) = (*valid-value v* (*constantAsStamp c*) $\wedge$ *v* = *c*)
  by *blast*

corollary *unfold-const32*:
  shows ([*m,p*] $\vdash$ *ConstantExpr* (*IntVal32 c*) $\mapsto$ *v*) = (*v* = *IntVal32 c*)
  using *unfold-valid32* **by** *blast*

corollary *unfold-const64*:
  shows ([*m,p*] $\vdash$ *ConstantExpr* (*IntVal64 c*) $\mapsto$ *v*) = (*v* = *IntVal64 c*)
  using *unfold-valid64* **by** *blast*

lemma *unfold-binary*:
  shows $([m,p] \vdash BinaryExpr\ op\ xe\ ye \mapsto val) = (\exists\ x\ y.$
        $(([m,p] \vdash xe \mapsto x)\ \wedge$
        $([m,p] \vdash ye \mapsto y)\ \wedge$
        $(val = bin\text{-}eval\ op\ x\ y)\ \wedge$
        $(val \neq UndefVal)$
      $))$ (**is** *?L = ?R*)
proof (*intro iffI*)
  assume *3*: *?L*
  show *?R* **by** (*rule evaltree.cases*[*OF 3*]; *blast+*)
next
  assume *?R*
  then obtain *x y* **where** $[m,p] \vdash xe \mapsto x$
      and $[m,p] \vdash ye \mapsto y$
      and *val = bin-eval op x y*
      and $val \neq UndefVal$
    by *auto*
  then show *?L*
    by (*rule BinaryExpr*)
qed

lemma *unfold-unary*:
  shows $([m,p] \vdash UnaryExpr\ op\ xe \mapsto val)$
      $= (\exists\ x.$
        $(([m,p] \vdash xe \mapsto x)\ \wedge$
        $(val = unary\text{-}eval\ op\ x)\ \wedge$
        $(val \neq UndefVal)$
        $))$ (**is** *?L = ?R*)
  by *auto*

lemmas *unfold-evaltree =*
  unfold-binary
  unfold-unary
  unfold-const32
  unfold-const64
  unfold-valid32
  unfold-valid64

end

7   Tree to Graph

theory *TreeToGraph*
  imports
    Semantics.IRTreeEval

Graph.IRGraph
begin

7.1   Subgraph to Data-flow Tree

fun *find-node-and-stamp* :: *IRGraph* $\Rightarrow$ (*IRNode* $\times$ *Stamp*) $\Rightarrow$ *ID option* **where**
  find-node-and-stamp g (n,s) =
    find ($\lambda i.$ *kind g i = n* $\wedge$ *stamp g i = s*) (*sorted-list-of-set(ids g)*)

export-code *find-node-and-stamp*

fun *is-preevaluated* :: *IRNode* $\Rightarrow$ *bool* **where**
  is-preevaluated (*InvokeNode n - - - - -*) = *True* |
  is-preevaluated (*InvokeWithExceptionNode n - - - - - - -*) = *True* |
  is-preevaluated (*NewInstanceNode n - - -*) = *True* |
  is-preevaluated (*LoadFieldNode n - - -*) = *True* |
  is-preevaluated (*SignedDivNode n - - - - -*) = *True* |
  is-preevaluated (*SignedRemNode n - - - - -*) = *True* |
  is-preevaluated (*ValuePhiNode n - -*) = *True* |
  is-preevaluated - = False

inductive
  rep :: *IRGraph* $\Rightarrow$ *ID* $\Rightarrow$ *IRExpr* $\Rightarrow$ *bool* (*- $\vdash$ - $\simeq$ - 55*)
  for *g* **where**

  ConstantNode:
  $[\![$ *kind g n = ConstantNode c* $]\!]$
    $\Longrightarrow$ *g* $\vdash$ *n* $\simeq$ (*ConstantExpr c*) |

  ParameterNode:
  $[\![$ *kind g n = ParameterNode i*;
    stamp g n = s $]\!]$
    $\Longrightarrow$ *g* $\vdash$ *n* $\simeq$ (*ParameterExpr i s*) |

  ConditionalNode:
  $[\![$ *kind g n = ConditionalNode c t f*;
    g $\vdash$ *c* $\simeq$ *ce*;
    g $\vdash$ *t* $\simeq$ *te*;
    g $\vdash$ *f* $\simeq$ *fe* $]\!]$
    $\Longrightarrow$ *g* $\vdash$ *n* $\simeq$ (*ConditionalExpr ce te fe*) |

  AbsNode:
  $[\![$ *kind g n = AbsNode x*;
    g $\vdash$ *x* $\simeq$ *xe* $]\!]$
    $\Longrightarrow$ *g* $\vdash$ *n* $\simeq$ (*UnaryExpr UnaryAbs xe*) |

NotNode:
⟦*kind g n = NotNode x*;
  g ⊢ *x* ≃ *xe*⟧
  ⟹ *g* ⊢ *n* ≃ (*UnaryExpr UnaryNot xe*) |

NegateNode:
⟦*kind g n = NegateNode x*;
  g ⊢ *x* ≃ *xe*⟧
  ⟹ *g* ⊢ *n* ≃ (*UnaryExpr UnaryNeg xe*) |

LogicNegationNode:
⟦*kind g n = LogicNegationNode x*;
  g ⊢ *x* ≃ *xe*⟧
  ⟹ *g* ⊢ *n* ≃ (*UnaryExpr UnaryLogicNegation xe*) |

AddNode:
⟦*kind g n = AddNode x y*;
  g ⊢ *x* ≃ *xe*;
  g ⊢ *y* ≃ *ye*⟧
  ⟹ *g* ⊢ *n* ≃ (*BinaryExpr BinAdd xe ye*) |

MulNode:
⟦*kind g n = MulNode x y*;
  g ⊢ *x* ≃ *xe*;
  g ⊢ *y* ≃ *ye*⟧
  ⟹ *g* ⊢ *n* ≃ (*BinaryExpr BinMul xe ye*) |

SubNode:
⟦*kind g n = SubNode x y*;
  g ⊢ *x* ≃ *xe*;
  g ⊢ *y* ≃ *ye*⟧
  ⟹ *g* ⊢ *n* ≃ (*BinaryExpr BinSub xe ye*) |

AndNode:
⟦*kind g n = AndNode x y*;
  g ⊢ *x* ≃ *xe*;
  g ⊢ *y* ≃ *ye*⟧
  ⟹ *g* ⊢ *n* ≃ (*BinaryExpr BinAnd xe ye*) |

OrNode:
⟦*kind g n = OrNode x y*;
  g ⊢ *x* ≃ *xe*;
  g ⊢ *y* ≃ *ye*⟧
  ⟹ *g* ⊢ *n* ≃ (*BinaryExpr BinOr xe ye*) |

XorNode:
⟦*kind g n = XorNode x y*;
  g ⊢ *x* ≃ *xe*;

$g \vdash y \simeq ye$⟧
$\implies g \vdash n \simeq (BinaryExpr\ BinXor\ xe\ ye)\ |$

ShortCircuitOrNode:
⟦*kind g n = ShortCircuitOrNode x y*;
  $g \vdash x \simeq xe$;
  $g \vdash y \simeq ye$⟧
$\implies g \vdash n \simeq (BinaryExpr\ BinShortCircuitOr\ xe\ ye)\ |$

LeftShiftNode:
⟦*kind g n = LeftShiftNode x y*;
  $g \vdash x \simeq xe$;
  $g \vdash y \simeq ye$⟧
$\implies g \vdash n \simeq (BinaryExpr\ BinLeftShift\ xe\ ye)\ |$

RightShiftNode:
⟦*kind g n = RightShiftNode x y*;
  $g \vdash x \simeq xe$;
  $g \vdash y \simeq ye$⟧
$\implies g \vdash n \simeq (BinaryExpr\ BinRightShift\ xe\ ye)\ |$

UnsignedRightShiftNode:
⟦*kind g n = UnsignedRightShiftNode x y*;
  $g \vdash x \simeq xe$;
  $g \vdash y \simeq ye$⟧
$\implies g \vdash n \simeq (BinaryExpr\ BinURightShift\ xe\ ye)\ |$

IntegerBelowNode:
⟦*kind g n = IntegerBelowNode x y*;
  $g \vdash x \simeq xe$;
  $g \vdash y \simeq ye$⟧
$\implies g \vdash n \simeq (BinaryExpr\ BinIntegerBelow\ xe\ ye)\ |$

IntegerEqualsNode:
⟦*kind g n = IntegerEqualsNode x y*;
  $g \vdash x \simeq xe$;
  $g \vdash y \simeq ye$⟧
$\implies g \vdash n \simeq (BinaryExpr\ BinIntegerEquals\ xe\ ye)\ |$

IntegerLessThanNode:
⟦*kind g n = IntegerLessThanNode x y*;
  $g \vdash x \simeq xe$;
  $g \vdash y \simeq ye$⟧
$\implies g \vdash n \simeq (BinaryExpr\ BinIntegerLessThan\ xe\ ye)\ |$

NarrowNode:
⟦*kind g n = NarrowNode inputBits resultBits x*;
  $g \vdash x \simeq xe$⟧

$\implies g \vdash n \simeq (\mathit{UnaryExpr}\ (\mathit{UnaryNarrow}\ \mathit{inputBits}\ \mathit{resultBits})\ \mathit{xe})\ |$

SignExtendNode:
$[\![\mathit{kind}\ g\ n = \mathit{SignExtendNode}\ \mathit{inputBits}\ \mathit{resultBits}\ x;$
$\quad g \vdash x \simeq \mathit{xe}]\!]$
$\quad\quad \implies g \vdash n \simeq (\mathit{UnaryExpr}\ (\mathit{UnarySignExtend}\ \mathit{inputBits}\ \mathit{resultBits})\ \mathit{xe})\ |$

ZeroExtendNode:
$[\![\mathit{kind}\ g\ n = \mathit{ZeroExtendNode}\ \mathit{inputBits}\ \mathit{resultBits}\ x;$
$\quad g \vdash x \simeq \mathit{xe}]\!]$
$\quad\quad \implies g \vdash n \simeq (\mathit{UnaryExpr}\ (\mathit{UnaryZeroExtend}\ \mathit{inputBits}\ \mathit{resultBits})\ \mathit{xe})\ |$

LeafNode:
$[\![\mathit{is\text{-}preevaluated}\ (\mathit{kind}\ g\ n);$
$\quad \mathit{stamp}\ g\ n = s]\!]$
$\quad\quad \implies g \vdash n \simeq (\mathit{LeafExpr}\ n\ s)\ |$

RefNode:
$[\![\mathit{kind}\ g\ n = \mathit{RefNode}\ n';$
$\quad g \vdash n' \simeq e]\!]$
$\quad\quad \implies g \vdash n \simeq e$

code-pred (*modes*: $i \Rightarrow i \Rightarrow o \Rightarrow bool$ *as exprE*) *rep* **.**

inductive
$\quad replist :: \mathit{IRGraph} \Rightarrow \mathit{ID}\ list \Rightarrow \mathit{IRExpr}\ list \Rightarrow bool\ (\text{-} \vdash \text{-} \simeq_L \text{-}\ 55)$
$\quad$ **for** g **where**

RepNil:
$g \vdash [] \simeq_L []\ |$

RepCons:
$[\![g \vdash x \simeq \mathit{xe};$
$\quad g \vdash \mathit{xs} \simeq_L \mathit{xse}]\!]$
$\quad\quad \implies g \vdash x\#\mathit{xs} \simeq_L \mathit{xe}\#\mathit{xse}$

code-pred (*modes*: $i \Rightarrow i \Rightarrow o \Rightarrow bool$ *as exprListE*) *replist* **.**

definition *wf-term-graph* :: $\mathit{MapState} \Rightarrow \mathit{Params} \Rightarrow \mathit{IRGraph} \Rightarrow \mathit{ID} \Rightarrow bool$ **where**
$\quad \mathit{wf\text{-}term\text{-}graph}\ m\ p\ g\ n = (\exists\ e.\ (g \vdash n \simeq e) \land (\exists\ v.\ ([m,\ p] \vdash e \mapsto v)))$

values $\{t.\ \mathit{eg2\text{-}sq} \vdash 4 \simeq t\}$

7.2 Data-flow Tree to Subgraph

fun *unary-node :: IRUnaryOp ⇒ ID ⇒ IRNode* **where**
  unary-node UnaryAbs v = AbsNode v |
  unary-node UnaryNot v = NotNode v |
  unary-node UnaryNeg v = NegateNode v |
  unary-node UnaryLogicNegation v = LogicNegationNode v |
  unary-node (UnaryNarrow ib rb) v = NarrowNode ib rb v |
  unary-node (UnarySignExtend ib rb) v = SignExtendNode ib rb v |
  unary-node (UnaryZeroExtend ib rb) v = ZeroExtendNode ib rb v

fun *bin-node :: IRBinaryOp ⇒ ID ⇒ ID ⇒ IRNode* **where**
  bin-node BinAdd x y = AddNode x y |
  bin-node BinMul x y = MulNode x y |
  bin-node BinSub x y = SubNode x y |
  bin-node BinAnd x y = AndNode x y |
  bin-node BinOr x y = OrNode x y |
  bin-node BinXor x y = XorNode x y |
  bin-node BinShortCircuitOr x y = ShortCircuitOrNode x y |
  bin-node BinLeftShift x y = LeftShiftNode x y |
  bin-node BinRightShift x y = RightShiftNode x y |
  bin-node BinURightShift x y = UnsignedRightShiftNode x y |
  bin-node BinIntegerEquals x y = IntegerEqualsNode x y |
  bin-node BinIntegerLessThan x y = IntegerLessThanNode x y |
  bin-node BinIntegerBelow x y = IntegerBelowNode x y

fun *choose-32-64 :: int ⇒ int64 ⇒ Value* **where**
  choose-32-64 bits val =
    (if bits = 32
     then (IntVal32 (ucast val))
     else (IntVal64 (val)))

inductive *fresh-id :: IRGraph ⇒ ID ⇒ bool* **where**
  $n \notin ids\ g \implies fresh\text{-}id\ g\ n$

code-pred *fresh-id* **.**

fun *get-fresh-id :: IRGraph ⇒ ID* **where**

  get-fresh-id g = last(sorted-list-of-set(ids g)) + 1

export-code *get-fresh-id*

value *get-fresh-id eg2-sq*

value *get-fresh-id* (*add-node 6* (*ParameterNode 2, default-stamp*) *eg2-sq*)

inductive
  unrep :: IRGraph ⇒ IRExpr ⇒ (IRGraph × ID) ⇒ bool (*- ⊕ - ⤳ - 55*)
  where

  ConstantNodeSame:
  ⟦*find-node-and-stamp g* (*ConstantNode c, constantAsStamp c*) = *Some n*⟧
    ⟹ *g ⊕* (*ConstantExpr c*) ⤳ (*g, n*) |

  ConstantNodeNew:
  ⟦*find-node-and-stamp g* (*ConstantNode c, constantAsStamp c*) = *None*;
    n = get-fresh-id g;
    g′ = add-node n (*ConstantNode c, constantAsStamp c*) *g* ⟧
    ⟹ *g ⊕* (*ConstantExpr c*) ⤳ (*g′, n*) |

  ParameterNodeSame:
  ⟦*find-node-and-stamp g* (*ParameterNode i, s*) = *Some n*⟧
    ⟹ *g ⊕* (*ParameterExpr i s*) ⤳ (*g, n*) |

  ParameterNodeNew:
  ⟦*find-node-and-stamp g* (*ParameterNode i, s*) = *None*;
    n = get-fresh-id g;
    g′ = add-node n (*ParameterNode i, s*) *g*⟧
    ⟹ *g ⊕* (*ParameterExpr i s*) ⤳ (*g′, n*) |

  ConditionalNodeSame:
  ⟦*g ⊕ ce* ⤳ (*g2, c*);
    g2 ⊕ te ⤳ (*g3, t*);
    g3 ⊕ fe ⤳ (*g4, f*);
    s′ = meet (*stamp g4 t*) (*stamp g4 f*);
    find-node-and-stamp g4 (*ConditionalNode c t f, s′*) = *Some n*⟧
    ⟹ *g ⊕* (*ConditionalExpr ce te fe*) ⤳ (*g4, n*) |

  ConditionalNodeNew:
  ⟦*g ⊕ ce* ⤳ (*g2, c*);
    g2 ⊕ te ⤳ (*g3, t*);
    g3 ⊕ fe ⤳ (*g4, f*);
    s′ = meet (*stamp g4 t*) (*stamp g4 f*);
    find-node-and-stamp g4 (*ConditionalNode c t f, s′*) = *None*;
    n = get-fresh-id g4;
    g′ = add-node n (*ConditionalNode c t f, s′*) *g4*⟧
    ⟹ *g ⊕* (*ConditionalExpr ce te fe*) ⤳ (*g′, n*) |

  UnaryNodeSame:
  ⟦*g ⊕ xe* ⤳ (*g2, x*);
    s′ = stamp-unary op (*stamp g2 x*);
    find-node-and-stamp g2 (*unary-node op x, s′*) = *Some n*⟧

$\implies g \oplus (UnaryExpr\ op\ xe) \rightsquigarrow (g2,\ n)\ |$

UnaryNodeNew:
$[\![g \oplus xe \rightsquigarrow (g2,\ x);$
  $s' = stamp\text{-}unary\ op\ (stamp\ g2\ x);$
  $find\text{-}node\text{-}and\text{-}stamp\ g2\ (unary\text{-}node\ op\ x,\ s') = None;$
  $n = get\text{-}fresh\text{-}id\ g2;$
  $g' = add\text{-}node\ n\ (unary\text{-}node\ op\ x,\ s')\ g2]\!]$
  $\implies g \oplus (UnaryExpr\ op\ xe) \rightsquigarrow (g',\ n)\ |$

BinaryNodeSame:
$[\![g \oplus xe \rightsquigarrow (g2,\ x);$
  $g2 \oplus ye \rightsquigarrow (g3,\ y);$
  $s' = stamp\text{-}binary\ op\ (stamp\ g3\ x)\ (stamp\ g3\ y);$
  $find\text{-}node\text{-}and\text{-}stamp\ g3\ (bin\text{-}node\ op\ x\ y,\ s') = Some\ n]\!]$
  $\implies g \oplus (BinaryExpr\ op\ xe\ ye) \rightsquigarrow (g3,\ n)\ |$

BinaryNodeNew:
$[\![g \oplus xe \rightsquigarrow (g2,\ x);$
  $g2 \oplus ye \rightsquigarrow (g3,\ y);$
  $s' = stamp\text{-}binary\ op\ (stamp\ g3\ x)\ (stamp\ g3\ y);$
  $find\text{-}node\text{-}and\text{-}stamp\ g3\ (bin\text{-}node\ op\ x\ y,\ s') = None;$
  $n = get\text{-}fresh\text{-}id\ g3;$
  $g' = add\text{-}node\ n\ (bin\text{-}node\ op\ x\ y,\ s')\ g3]\!]$
  $\implies g \oplus (BinaryExpr\ op\ xe\ ye) \rightsquigarrow (g',\ n)\ |$

AllLeafNodes:
$[\![stamp\ g\ n = s;$
  $is\text{-}preevaluated\ (kind\ g\ n)]\!]$
  $\implies g \oplus (LeafExpr\ n\ s) \rightsquigarrow (g,\ n)$

code-pred (*modes*: $i \Rightarrow i \Rightarrow o \Rightarrow bool\ as\ unrepE$)
  unrep **.**

unrepRules

$$\frac{\textit{find-node-and-stamp g (ConstantNode c, constantAsStamp c)} = \textit{Some n}}{g \oplus \textit{ConstantExpr c} \rightsquigarrow (g, n)}$$

$$\frac{\begin{array}{c}\textit{find-node-and-stamp g (ConstantNode c, constantAsStamp c)} = \textit{None} \\ n = \textit{get-fresh-id g} \\ g' = \textit{add-node n (ConstantNode c, constantAsStamp c) g}\end{array}}{g \oplus \textit{ConstantExpr c} \rightsquigarrow (g', n)}$$

$$\frac{\textit{find-node-and-stamp g (ParameterNode i, s)} = \textit{Some n}}{g \oplus \textit{ParameterExpr i s} \rightsquigarrow (g, n)}$$

$$\frac{\begin{array}{c}\textit{find-node-and-stamp g (ParameterNode i, s)} = \textit{None} \\ n = \textit{get-fresh-id g} \qquad g' = \textit{add-node n (ParameterNode i, s) g}\end{array}}{g \oplus \textit{ParameterExpr i s} \rightsquigarrow (g', n)}$$

$$\frac{\begin{array}{c}g \oplus \textit{ce} \rightsquigarrow (g2, c) \qquad g2 \oplus \textit{te} \rightsquigarrow (g3, t) \\ g3 \oplus \textit{fe} \rightsquigarrow (g4, f) \qquad s' = \textit{meet (stamp g4 t) (stamp g4 f)} \\ \textit{find-node-and-stamp g4 (ConditionalNode c t f, s')} = \textit{Some n}\end{array}}{g \oplus \textit{ConditionalExpr ce te fe} \rightsquigarrow (g4, n)}$$

$$\frac{\begin{array}{c}g \oplus \textit{ce} \rightsquigarrow (g2, c) \qquad g2 \oplus \textit{te} \rightsquigarrow (g3, t) \\ g3 \oplus \textit{fe} \rightsquigarrow (g4, f) \qquad s' = \textit{meet (stamp g4 t) (stamp g4 f)} \\ \textit{find-node-and-stamp g4 (ConditionalNode c t f, s')} = \textit{None} \\ n = \textit{get-fresh-id g4} \qquad g' = \textit{add-node n (ConditionalNode c t f, s') g4}\end{array}}{g \oplus \textit{ConditionalExpr ce te fe} \rightsquigarrow (g', n)}$$

$$\frac{\begin{array}{c}g \oplus \textit{xe} \rightsquigarrow (g2, x) \\ g2 \oplus \textit{ye} \rightsquigarrow (g3, y) \qquad s' = \textit{stamp-binary op (stamp g3 x) (stamp g3 y)} \\ \textit{find-node-and-stamp g3 (bin-node op x y, s')} = \textit{Some n}\end{array}}{g \oplus \textit{BinaryExpr op xe ye} \rightsquigarrow (g3, n)}$$

$$\frac{\begin{array}{c}g \oplus \textit{xe} \rightsquigarrow (g2, x) \\ g2 \oplus \textit{ye} \rightsquigarrow (g3, y) \qquad s' = \textit{stamp-binary op (stamp g3 x) (stamp g3 y)} \\ \textit{find-node-and-stamp g3 (bin-node op x y, s')} = \textit{None} \\ n = \textit{get-fresh-id g3} \qquad g' = \textit{add-node n (bin-node op x y, s') g3}\end{array}}{g \oplus \textit{BinaryExpr op xe ye} \rightsquigarrow (g', n)}$$

$$\frac{\begin{array}{c}g \oplus \textit{xe} \rightsquigarrow (g2, x) \qquad s' = \textit{stamp-unary op (stamp g2 x)} \\ \textit{find-node-and-stamp g2 (unary-node op x, s')} = \textit{Some n}\end{array}}{g \oplus \textit{UnaryExpr op xe} \rightsquigarrow (g2, n)}$$

$$\frac{\begin{array}{c}g \oplus \textit{xe} \rightsquigarrow (g2, x) \qquad s' = \textit{stamp-unary op (stamp g2 x)} \\ \textit{find-node-and-stamp g2 (unary-node op x, s')} = \textit{None} \\ n = \textit{get-fresh-id g2} \qquad g' = \textit{add-node n (unary-node op x, s') g2}\end{array}}{g \oplus \textit{UnaryExpr op xe} \rightsquigarrow (g', n)}$$

$$\frac{\textit{stamp g n} = s \qquad \textit{is-preevaluated (kind g n)}}{g \oplus \textit{LeafExpr n s} \rightsquigarrow (g, n)}$$

values {(n, g) . $(eg2\text{-}sq \oplus sq\text{-}param0 \rightsquigarrow (g, n))$}

7.3 Lift Data-flow Tree Semantics

definition *encodeeval* :: *IRGraph* $\Rightarrow$ *MapState* $\Rightarrow$ *Params* $\Rightarrow$ *ID* $\Rightarrow$ *Value* $\Rightarrow$ *bool*
  ([-,-,-] $\vdash$ - $\mapsto$ - *50*)
  where
  encodeeval g m p n v = ($\exists$ *e*. $(g \vdash n \simeq e) \land ([m,p] \vdash e \mapsto v))$

7.4 Graph Refinement

definition *graph-represents-expression* :: *IRGraph* $\Rightarrow$ *ID* $\Rightarrow$ *IRExpr* $\Rightarrow$ *bool*
  (- $\vdash$ - $\unlhd$ - *50*)
  where
  $(g \vdash n \unlhd e) = (\exists e'$. $(g \vdash n \simeq e') \land (e' \leq e))$

definition *graph-refinement* :: *IRGraph* $\Rightarrow$ *IRGraph* $\Rightarrow$ *bool* **where**
  graph-refinement g_1 g_2 =
      $((ids\ g_1 \subseteq ids\ g_2)\ \land$
      $(\forall\ n\ .\ n \in ids\ g_1 \longrightarrow (\forall e.\ (g_1 \vdash n \simeq e) \longrightarrow (g_2 \vdash n \unlhd e))))$

lemma *graph-refinement*:
  graph-refinement g1 g2 $\Longrightarrow$ $(\forall n\ m\ p\ v.\ n \in ids\ g1 \longrightarrow ([g1,\ m,\ p] \vdash n \mapsto v) \longrightarrow$
$([g2,\ m,\ p] \vdash n \mapsto v))$
   by (*meson encodeeval-def graph-refinement-def graph-represents-expression-def le-expr-def*)

7.5 Maximal Sharing

definition *maximal-sharing*:
  maximal-sharing g = $(\forall\ n_1\ n_2\ .\ n_1 \in true\text{-}ids\ g \land n_2 \in true\text{-}ids\ g \longrightarrow$
      $(\forall\ e.\ (g \vdash n_1 \simeq e) \land (g \vdash n_2 \simeq e) \land (stamp\ g\ n_1 = stamp\ g\ n_2) \longrightarrow n_1 =$
$n_2))$

end

7.6 Formedness Properties

theory *Form*
imports
  Semantics.TreeToGraph
begin

definition *wf-start* **where**
  wf-start g = $(0 \in ids\ g\ \land$
    is-StartNode (*kind g 0*))

definition *wf-closed* **where**
  wf-closed g =
    $(\forall\ n \in ids\ g$.

$inputs\ g\ n \subseteq ids\ g\ \wedge$
$succ\ g\ n \subseteq ids\ g\ \wedge$
$kind\ g\ n \neq NoNode)$

definition *wf-phis* **where**
  wf-phis g =
   $(\forall\ n \in ids\ g.$
    is-PhiNode (kind g n) $\longrightarrow$
    length (ir-values (kind g n))
     = length (ir-ends
      (kind g (ir-merge (kind g n))))))

definition *wf-ends* **where**
  wf-ends g =
   $(\forall\ n \in ids\ g\ .$
    is-AbstractEndNode (kind g n) $\longrightarrow$
    card (usages g n) > 0)

fun *wf-graph* :: *IRGraph* $\Rightarrow$ *bool* **where**
  wf-graph g = (wf-start g $\wedge$ *wf-closed g* $\wedge$ *wf-phis g* $\wedge$ *wf-ends g)*

lemmas *wf-folds =*
  wf-graph.simps
  wf-start-def
  wf-closed-def
  wf-phis-def
  wf-ends-def

fun *wf-stamps* :: *IRGraph* $\Rightarrow$ *bool* **where**
  wf-stamps g = $(\forall\ n \in ids\ g\ .$
   $(\forall\ v\ m\ p\ e\ .\ (g \vdash n \simeq e) \wedge ([m,\ p] \vdash e \mapsto v) \longrightarrow valid\text{-}value\ v\ (stamp\text{-}expr\ e)))$

fun *wf-stamp* :: *IRGraph* $\Rightarrow$ *(ID* $\Rightarrow$ *Stamp)* $\Rightarrow$ *bool* **where**
  wf-stamp g s = $(\forall\ n \in ids\ g\ .$
   $(\forall\ v\ m\ p\ e\ .\ (g \vdash n \simeq e) \wedge ([m,\ p] \vdash e \mapsto v) \longrightarrow valid\text{-}value\ v\ (s\ n)))$

lemma *wf-empty*: *wf-graph start-end-graph*
  unfolding *start-end-graph-def wf-folds* **by** *simp*

lemma *wf-eg2-sq*: *wf-graph eg2-sq*
  unfolding *eg2-sq-def wf-folds* **by** *simp*

fun *wf-logic-node-inputs* :: *IRGraph* $\Rightarrow$ *ID* $\Rightarrow$ *bool* **where**
wf-logic-node-inputs g n =
 $(\forall\ inp \in set\ (inputs\text{-}of\ (kind\ g\ n))\ .\ (\forall\ v\ m\ p\ .\ ([g,\ m,\ p] \vdash inp \mapsto v) \longrightarrow$ *wf-bool*
v))

fun *wf-values* :: *IRGraph* $\Rightarrow$ *bool* **where**
  wf-values g = $(\forall\ n \in ids\ g\ .$

$(\forall\ v\ m\ p\ .\ ([g,\ m,\ p] \vdash n \mapsto v) \longrightarrow$
   $(is\text{-}LogicNode\ (kind\ g\ n) \longrightarrow$
     $wf\text{-}bool\ v \wedge wf\text{-}logic\text{-}node\text{-}inputs\ g\ n)))$

end

7.7 Dynamic Frames

This theory defines two operators, 'unchanged' and 'changeonly', that are useful for specifying which nodes in an IRGraph can change. The dynamic framing idea originates from 'Dynamic Frames' in software verification, started by Ioannis T. Kassios in "Dynamic frames: Support for framing, dependencies and sharing without restrictions", In FM 2006.

theory *IRGraphFrames*
  imports
    Form
begin

fun *unchanged* :: *ID set $\Rightarrow$ IRGraph $\Rightarrow$ IRGraph $\Rightarrow$ bool* **where**
  unchanged ns g1 g2 = ($\forall$ n . n $\in$ ns $\longrightarrow$
  (n $\in$ ids g1 $\wedge$ n $\in$ ids g2 $\wedge$ kind g1 n = kind g2 n $\wedge$ stamp g1 n = stamp g2 n))

fun *changeonly* :: *ID set $\Rightarrow$ IRGraph $\Rightarrow$ IRGraph $\Rightarrow$ bool* **where**
  changeonly ns g1 g2 = ($\forall$ n . n $\in$ ids g1 $\wedge$ n $\notin$ ns $\longrightarrow$
  (n $\in$ ids g1 $\wedge$ n $\in$ ids g2 $\wedge$ kind g1 n = kind g2 n $\wedge$ stamp g1 n = stamp g2 n))

lemma *node-unchanged*:
  assumes *unchanged ns g1 g2*
  assumes *nid $\in$ ns*
  shows *kind g1 nid = kind g2 nid*
  using *assms* **by** *auto*

lemma *other-node-unchanged*:
  assumes *changeonly ns g1 g2*
  assumes *nid $\in$ ids g1*
  assumes *nid $\notin$ ns*
  shows *kind g1 nid = kind g2 nid*
  using *assms*
  using *changeonly.simps* **by** *blast*

Some notation for input nodes used

inductive *eval-uses*:: *IRGraph $\Rightarrow$ ID $\Rightarrow$ ID $\Rightarrow$ bool*
  for *g* **where**

  use0: *nid $\in$ ids g*
    $\Longrightarrow$ *eval-uses g nid nid |*

$use\text{-}inp$: $nid' \in inputs\ g\ n$
  $\implies eval\text{-}uses\ g\ nid\ nid'\ |$

$use\text{-}trans$: $[\![eval\text{-}uses\ g\ nid\ nid';$
  $eval\text{-}uses\ g\ nid'\ nid'']\!]$
  $\implies eval\text{-}uses\ g\ nid\ nid''$

fun *eval-usages* :: *IRGraph* $\Rightarrow$ *ID* $\Rightarrow$ *ID set* **where**
  eval-usages g nid = $\{n \in ids\ g\ .\ eval\text{-}uses\ g\ nid\ n\}$

lemma *eval-usages-self*:
  assumes $nid \in ids\ g$
  shows $nid \in eval\text{-}usages\ g\ nid$
  using *assms eval-usages.simps eval-uses.intros*(*1*)
  by (*simp add*: *ids.rep-eq*)

lemma *not-in-g-inputs*:
  assumes $nid \notin ids\ g$
  shows $inputs\ g\ nid = \{\}$
proof −
  have k: $kind\ g\ nid = NoNode$ **using** *assms not-in-g* **by** *blast*
  then show *?thesis* **by** (*simp add*: k)
qed

lemma *child-member*:
  assumes $n = kind\ g\ nid$
  assumes $n \neq NoNode$
  assumes *List.member* (*inputs-of n*) *child*
  shows $child \in inputs\ g\ nid$
  unfolding *inputs.simps* **using** *assms*
  by (*metis in-set-member*)

lemma *child-member-in*:
  assumes $nid \in ids\ g$
  assumes *List.member* (*inputs-of* (*kind g nid*)) *child*
  shows $child \in inputs\ g\ nid$
  unfolding *inputs.simps* **using** *assms*
  by (*metis child-member ids-some inputs.elims*)

lemma *inp-in-g*:
  assumes $n \in inputs\ g\ nid$
  shows $nid \in ids\ g$
proof −
  have $inputs\ g\ nid \neq \{\}$
    using *assms*
    by (*metis empty-iff empty-set*)

then have *kind g nid ≠ NoNode*
  using *not-in-g-inputs*
  using *ids-some* **by** *blast*
then show *?thesis*
  using *not-in-g*
  by *metis*
qed

lemma *inp-in-g-wf*:
  assumes *wf-graph g*
  assumes *n ∈ inputs g nid*
  shows *n ∈ ids g*
  using *assms* **unfolding** *wf-folds*
  using *inp-in-g* **by** *blast*

lemma *kind-unchanged*:
  assumes *nid ∈ ids g1*
  assumes *unchanged (eval-usages g1 nid) g1 g2*
  shows *kind g1 nid = kind g2 nid*
proof −
  show *?thesis*
    using *assms eval-usages-self*
    using *unchanged.simps* **by** *blast*
qed

lemma *stamp-unchanged*:
  assumes *nid ∈ ids g1*
  assumes *unchanged (eval-usages g1 nid) g1 g2*
  shows *stamp g1 nid = stamp g2 nid*
  by (*meson assms(1) assms(2) eval-usages-self unchanged.elims(2)*)

lemma *child-unchanged*:
  assumes *child ∈ inputs g1 nid*
  assumes *unchanged (eval-usages g1 nid) g1 g2*
  shows *unchanged (eval-usages g1 child) g1 g2*
  by (*smt assms(1) assms(2) eval-usages.simps mem-Collect-eq*
    unchanged.simps use-inp use-trans)

lemma *eval-usages*:
  assumes *us = eval-usages g nid*
  assumes *nid′ ∈ ids g*
  shows *eval-uses g nid nid′ ⟷ nid′ ∈ us* (**is** *?P ⟷ ?Q*)
  using *assms eval-usages.simps*
  by (*simp add: ids.rep-eq*)

lemma *inputs-are-uses*:
  assumes *nid′ ∈ inputs g nid*

shows *eval-uses g nid nid′*
by (*metis assms use-inp*)

lemma *inputs-are-usages*:
  assumes *nid′* ∈ *inputs g nid*
  assumes *nid′* ∈ *ids g*
  shows *nid′* ∈ *eval-usages g nid*
  using *assms*(*1*) *assms*(*2*) *eval-usages inputs-are-uses* **by** *blast*

lemma *inputs-of-are-usages*:
  assumes *List.member* (*inputs-of* (*kind g nid*)) *nid′*
  assumes *nid′* ∈ *ids g*
  shows *nid′* ∈ *eval-usages g nid*
  by (*metis assms*(*1*) *assms*(*2*) *in-set-member inputs.elims inputs-are-usages*)

lemma *usage-includes-inputs*:
  assumes *us* = *eval-usages g nid*
  assumes *ls* = *inputs g nid*
  assumes *ls* ⊆ *ids g*
  shows *ls* ⊆ *us*
  using *inputs-are-usages eval-usages*
  using *assms*(*1*) *assms*(*2*) *assms*(*3*) **by** *blast*

lemma *elim-inp-set*:
  assumes *k* = *kind g nid*
  assumes *k* ≠ *NoNode*
  assumes *child* ∈ *set* (*inputs-of k*)
  shows *child* ∈ *inputs g nid*
  using *assms* **by** *auto*

lemma *encode-in-ids*:
  assumes *g* ⊢ *nid* ≃ *e*
  shows *nid* ∈ *ids g*
  using *assms*
  apply (*induction rule*: *rep.induct*)
  apply *simp+*
  by *fastforce+*

lemma *eval-in-ids*:
  assumes [*g*, *m*, *p*] ⊢ *nid* ↦ *v*
  shows *nid* ∈ *ids g*
  using *assms* **using** *encodeeval-def encode-in-ids*
  by *auto*

lemma *transitive-kind-same*:
  assumes *unchanged* (*eval-usages g1 nid*) *g1 g2*
  shows ∀ *nid′* ∈ (*eval-usages g1 nid*) . *kind g1 nid′* = *kind g2 nid′*
  using *assms*
  by (*meson unchanged.elims*(*1*))

theorem *stay-same-encoding*:
  assumes *nc*: *unchanged* (*eval-usages g1 nid*) *g1 g2*
  assumes *g1*: *g1* ⊢ *nid* ≃ *e*
  assumes *wf*: *wf-graph g1*
  shows *g2* ⊢ *nid* ≃ *e*
proof −
  have *dom*: *nid* ∈ *ids g1*
    using *g1 encode-in-ids* **by** *simp*
  show *?thesis*
using *g1 nc wf dom* **proof** (*induction e rule: rep.induct*)
  case (*ConstantNode n c*)
  then have *kind g2 n = ConstantNode c*
    using *dom nc kind-unchanged*
    by *metis*
  then show *?case* **using** *rep.ConstantNode*
    by *presburger*
next
  case (*ParameterNode n i s*)
  then have *kind g2 n = ParameterNode i*
    by (*metis kind-unchanged*)
  then show *?case*
   by (*metis ParameterNode.hyps*(*2*) *ParameterNode.prems*(*1*) *ParameterNode.prems*(*3*)
rep.ParameterNode stamp-unchanged)
next
  case (*ConditionalNode n c t f ce te fe*)
  then have *kind g2 n = ConditionalNode c t f*
    by (*metis kind-unchanged*)
  have *c* ∈ *eval-usages g1 n* ∧ *t* ∈ *eval-usages g1 n* ∧ *f* ∈ *eval-usages g1 n*
    using *inputs-of-ConditionalNode*
      by (*metis ConditionalNode.hyps*(*1*) *ConditionalNode.hyps*(*2*) *ConditionalN-
ode.hyps*(*3*) *ConditionalNode.hyps*(*4*) *encode-in-ids inputs.simps inputs-are-usages
list.set-intros*(*1*) *set-subset-Cons subset-code*(*1*))
  then show *?case* **using** *transitive-kind-same*
   by (*metis ConditionalNode.hyps*(*1*) *ConditionalNode.prems*(*1*) *IRNodes.inputs-of-ConditionalNode*
⟨*kind g2 n = ConditionalNode c t f*⟩ *child-unchanged inputs.simps list.set-intros*(*1*)
local.ConditionalNode(*5*) *local.ConditionalNode*(*6*) *local.ConditionalNode*(*7*) *local.ConditionalNode*(*9*)
rep.ConditionalNode set-subset-Cons subset-code(*1*) *unchanged.elims*(*2*))
next
  case (*AbsNode n x xe*)
  then have *kind g2 n = AbsNode x*
    using *kind-unchanged*
    by *metis*
  then have *x* ∈ *eval-usages g1 n*
    using *inputs-of-AbsNode*
      by (*metis AbsNode.hyps*(*1*) *AbsNode.hyps*(*2*) *encode-in-ids inputs.simps in-
puts-are-usages list.set-intros*(*1*))
  then show *?case*
    by (*metis AbsNode.IH AbsNode.hyps*(*1*) *AbsNode.prems*(*1*) *AbsNode.prems*(*3*)

70

IRNodes.inputs-of-AbsNode ‹kind g2 n = AbsNode x› child-member-in child-unchanged
local.wf member-rec(*1*) *rep.AbsNode unchanged.simps*)
next
  case (*NotNode n x xe*)
  then have *kind g2 n = NotNode x*
    using *kind-unchanged*
    by *metis*
  then have $x \in$ *eval-usages g1 n*
    using *inputs-of-NotNode*
     by (*metis NotNode.hyps*(*1*) *NotNode.hyps*(*2*) *encode-in-ids inputs.simps inputs-are-usages list.set-intros*(*1*))
  then show *?case*
    by (*metis NotNode.IH NotNode.hyps*(*1*) *NotNode.prems*(*1*) *NotNode.prems*(*3*)
IRNodes.inputs-of-NotNode ‹kind g2 n = NotNode x› child-member-in child-unchanged
local.wf member-rec(*1*) *rep.NotNode unchanged.simps*)
next
  case (*NegateNode n x xe*)
  then have *kind g2 n = NegateNode x*
    using *kind-unchanged* **by** *metis*
  then have $x \in$ *eval-usages g1 n*
    using *inputs-of-NegateNode*
    by (*metis NegateNode.hyps*(*1*) *NegateNode.hyps*(*2*) *encode-in-ids inputs.simps inputs-are-usages list.set-intros*(*1*))
  then show *?case*
    by (*metis IRNodes.inputs-of-NegateNode NegateNode.IH NegateNode.hyps*(*1*)
NegateNode.prems(*1*) *NegateNode.prems*(*3*) *‹kind g2 n = NegateNode x› child-member-in*
child-unchanged local.wf member-rec(*1*) *rep.NegateNode unchanged.elims*(*1*))
next
  case (*LogicNegationNode n x xe*)
  then have *kind g2 n = LogicNegationNode x*
    using *kind-unchanged* **by** *metis*
  then have $x \in$ *eval-usages g1 n*
    using *inputs-of-LogicNegationNode inputs-of-are-usages*
    by (*metis LogicNegationNode.hyps*(*1*) *LogicNegationNode.hyps*(*2*) *encode-in-ids*
member-rec(*1*))
  then show *?case*
    by (*metis IRNodes.inputs-of-LogicNegationNode LogicNegationNode.IH Logic-*
NegationNode.hyps(*1*) *LogicNegationNode.hyps*(*2*) *LogicNegationNode.prems*(*1*) *‹kind*
g2 n = LogicNegationNode x› child-unchanged encode-in-ids inputs.simps list.set-intros(*1*)
local.wf rep.LogicNegationNode)
next
  case (*AddNode n x y xe ye*)
  then have *kind g2 n = AddNode x y*
    using *kind-unchanged* **by** *metis*
  then have $x \in$ *eval-usages g1 n* $\land$ $y \in$ *eval-usages g1 n*
    using *inputs-of-LogicNegationNode inputs-of-are-usages*
   by (*metis AddNode.hyps*(*1*) *AddNode.hyps*(*2*) *AddNode.hyps*(*3*) *IRNodes.inputs-of-AddNode*
encode-in-ids in-mono inputs.simps inputs-are-usages list.set-intros(*1*) *set-subset-Cons*)
  then show *?case*

by (*metis AddNode.IH*(*1*) *AddNode.IH*(*2*) *AddNode.hyps*(*1*) *AddNode.hyps*(*2*)
AddNode.hyps(*3*) *AddNode.prems*(*1*) *IRNodes.inputs-of-AddNode* ‹*kind g2 n = AddNode
x y*› *child-unchanged encode-in-ids in-set-member inputs.simps local.wf member-rec*(*1*)
rep.AddNode)
next
  case (*MulNode n x y xe ye*)
  then have *kind g2 n = MulNode x y*
    using *kind-unchanged* **by** *metis*
  then have *x ∈ eval-usages g1 n ∧ y ∈ eval-usages g1 n*
    using *inputs-of-LogicNegationNode inputs-of-are-usages*
  by (*metis MulNode.hyps*(*1*) *MulNode.hyps*(*2*) *MulNode.hyps*(*3*) *IRNodes.inputs-of-MulNode*
encode-in-ids in-mono inputs.simps inputs-are-usages list.set-intros(*1*) *set-subset-Cons*)
  then show *?case* **using** *MulNode inputs-of-MulNode*
  by (*metis* ‹*kind g2 n = MulNode x y*› *child-unchanged inputs.simps list.set-intros*(*1*)
rep.MulNode set-subset-Cons subset-iff unchanged.elims(*2*))
next
  case (*SubNode n x y xe ye*)
  then have *kind g2 n = SubNode x y*
    using *kind-unchanged* **by** *metis*
  then have *x ∈ eval-usages g1 n ∧ y ∈ eval-usages g1 n*
    using *inputs-of-LogicNegationNode inputs-of-are-usages*
  by (*metis SubNode.hyps*(*1*) *SubNode.hyps*(*2*) *SubNode.hyps*(*3*) *IRNodes.inputs-of-SubNode*
encode-in-ids in-mono inputs.simps inputs-are-usages list.set-intros(*1*) *set-subset-Cons*)
  then show *?case* **using** *SubNode inputs-of-SubNode*
  by (*metis* ‹*kind g2 n = SubNode x y*› *child-member child-unchanged encode-in-ids*
ids-some member-rec(*1*) *rep.SubNode*)
next
  case (*AndNode n x y xe ye*)
  then have *kind g2 n = AndNode x y*
    using *kind-unchanged* **by** *metis*
  then have *x ∈ eval-usages g1 n ∧ y ∈ eval-usages g1 n*
    using *inputs-of-LogicNegationNode inputs-of-are-usages*
  by (*metis AndNode.hyps*(*1*) *AndNode.hyps*(*2*) *AndNode.hyps*(*3*) *IRNodes.inputs-of-AndNode*
encode-in-ids in-mono inputs.simps inputs-are-usages list.set-intros(*1*) *set-subset-Cons*)
  then show *?case* **using** *AndNode inputs-of-AndNode*
  by (*metis* ‹*kind g2 n = AndNode x y*› *child-unchanged inputs.simps list.set-intros*(*1*)
rep.AndNode set-subset-Cons subset-iff unchanged.elims(*2*))
next
  case (*OrNode n x y xe ye*)
  then have *kind g2 n = OrNode x y*
    using *kind-unchanged* **by** *metis*
  then have *x ∈ eval-usages g1 n ∧ y ∈ eval-usages g1 n*
    using *inputs-of-OrNode inputs-of-are-usages*
  by (*metis OrNode.hyps*(*1*) *OrNode.hyps*(*2*) *OrNode.hyps*(*3*) *IRNodes.inputs-of-OrNode*
encode-in-ids in-mono inputs.simps inputs-are-usages list.set-intros(*1*) *set-subset-Cons*)
  then show *?case* **using** *OrNode inputs-of-OrNode*
  by (*metis* ‹*kind g2 n = OrNode x y*› *child-member child-unchanged encode-in-ids*
ids-some member-rec(*1*) *rep.OrNode*)
next

case (*XorNode n x y xe ye*)

  then have *kind g2 n = XorNode x y*

    using *kind-unchanged* **by** *metis*

  then have *x ∈ eval-usages g1 n ∧ y ∈ eval-usages g1 n*

    using *inputs-of-XorNode inputs-of-are-usages*

  by (*metis XorNode.hyps*(*1*) *XorNode.hyps*(*2*) *XorNode.hyps*(*3*) *IRNodes.inputs-of-XorNode encode-in-ids in-mono inputs.simps inputs-are-usages list.set-intros*(*1*) *set-subset-Cons*)

  then show *?case* **using** *XorNode inputs-of-XorNode*

  by (*metis ‹kind g2 n = XorNode x y› child-member child-unchanged encode-in-ids ids-some member-rec*(*1*) *rep.XorNode*)

next

  case (*ShortCircuitOrNode n x y xe ye*)

  then have *kind g2 n = ShortCircuitOrNode x y*

    using *kind-unchanged* **by** *metis*

  then have *x ∈ eval-usages g1 n ∧ y ∈ eval-usages g1 n*

    using *inputs-of-XorNode inputs-of-are-usages*

    by (*metis ShortCircuitOrNode.hyps*(*1*) *ShortCircuitOrNode.hyps*(*2*) *ShortCircuitOrNode.hyps*(*3*) *IRNodes.inputs-of-ShortCircuitOrNode encode-in-ids in-mono inputs.simps inputs-are-usages list.set-intros*(*1*) *set-subset-Cons*)

  then show *?case* **using** *ShortCircuitOrNode inputs-of-ShortCircuitOrNode*

  by (*metis ‹kind g2 n = ShortCircuitOrNode x y› child-member child-unchanged encode-in-ids ids-some member-rec*(*1*) *rep.ShortCircuitOrNode*)

next

case (*LeftShiftNode n x y xe ye*)

  then have *kind g2 n = LeftShiftNode x y*

    using *kind-unchanged* **by** *metis*

  then have *x ∈ eval-usages g1 n ∧ y ∈ eval-usages g1 n*

    using *inputs-of-XorNode inputs-of-are-usages*

    by (*metis LeftShiftNode.hyps*(*1*) *LeftShiftNode.hyps*(*2*) *LeftShiftNode.hyps*(*3*) *IRNodes.inputs-of-LeftShiftNode encode-in-ids in-mono inputs.simps inputs-are-usages list.set-intros*(*1*) *set-subset-Cons*)

  then show *?case* **using** *LeftShiftNode inputs-of-LeftShiftNode*

    by (*metis ‹kind g2 n = LeftShiftNode x y› child-member child-unchanged encode-in-ids ids-some member-rec*(*1*) *rep.LeftShiftNode*)

next

case (*RightShiftNode n x y xe ye*)

  then have *kind g2 n = RightShiftNode x y*

    using *kind-unchanged* **by** *metis*

  then have *x ∈ eval-usages g1 n ∧ y ∈ eval-usages g1 n*

    using *inputs-of-RightShiftNode inputs-of-are-usages*

  by (*metis RightShiftNode.hyps*(*1*) *RightShiftNode.hyps*(*2*) *RightShiftNode.hyps*(*3*) *IRNodes.inputs-of-RightShiftNode encode-in-ids in-mono inputs.simps inputs-are-usages list.set-intros*(*1*) *set-subset-Cons*)

  then show *?case* **using** *RightShiftNode inputs-of-RightShiftNode*

    by (*metis ‹kind g2 n = RightShiftNode x y› child-member child-unchanged encode-in-ids ids-some member-rec*(*1*) *rep.RightShiftNode*)

next

case (*UnsignedRightShiftNode n x y xe ye*)

  then have *kind g2 n = UnsignedRightShiftNode x y*

using *kind-unchanged* **by** *metis*

then have *x ∈ eval-usages g1 n ∧ y ∈ eval-usages g1 n*

  using *inputs-of-UnsignedRightShiftNode inputs-of-are-usages*

  by (*metis UnsignedRightShiftNode.hyps*(*1*) *UnsignedRightShiftNode.hyps*(*2*) *UnsignedRightShiftNode.hyps*(*3*) *IRNodes.inputs-of-UnsignedRightShiftNode encode-in-ids in-mono inputs.simps inputs-are-usages list.set-intros*(*1*) *set-subset-Cons*)

  then show *?case* **using** *UnsignedRightShiftNode inputs-of-UnsignedRightShiftNode*

  by (*metis ‹kind g2 n = UnsignedRightShiftNode x y› child-member child-unchanged encode-in-ids ids-some member-rec*(*1*) *rep.UnsignedRightShiftNode*)

next

  case (*IntegerBelowNode n x y xe ye*)

  then have *kind g2 n = IntegerBelowNode x y*

    using *kind-unchanged* **by** *metis*

  then have *x ∈ eval-usages g1 n ∧ y ∈ eval-usages g1 n*

    using *inputs-of-IntegerBelowNode inputs-of-are-usages*

    by (*metis IntegerBelowNode.hyps*(*1*) *IntegerBelowNode.hyps*(*2*) *IntegerBelowNode.hyps*(*3*) *IRNodes.inputs-of-IntegerBelowNode encode-in-ids in-mono inputs.simps inputs-are-usages list.set-intros*(*1*) *set-subset-Cons*)

  then show *?case* **using** *IntegerBelowNode inputs-of-IntegerBelowNode*

    by (*metis ‹kind g2 n = IntegerBelowNode x y› child-member child-unchanged encode-in-ids ids-some member-rec*(*1*) *rep.IntegerBelowNode*)

next

  case (*IntegerEqualsNode n x y xe ye*)

  then have *kind g2 n = IntegerEqualsNode x y*

    using *kind-unchanged* **by** *metis*

  then have *x ∈ eval-usages g1 n ∧ y ∈ eval-usages g1 n*

    using *inputs-of-IntegerEqualsNode inputs-of-are-usages*

    by (*metis IntegerEqualsNode.hyps*(*1*) *IntegerEqualsNode.hyps*(*2*) *IntegerEqualsNode.hyps*(*3*) *IRNodes.inputs-of-IntegerEqualsNode encode-in-ids in-mono inputs.simps inputs-are-usages list.set-intros*(*1*) *set-subset-Cons*)

  then show *?case* **using** *IntegerEqualsNode inputs-of-IntegerEqualsNode*

    by (*metis ‹kind g2 n = IntegerEqualsNode x y› child-member child-unchanged encode-in-ids ids-some member-rec*(*1*) *rep.IntegerEqualsNode*)

next

  case (*IntegerLessThanNode n x y xe ye*)

  then have *kind g2 n = IntegerLessThanNode x y*

    using *kind-unchanged* **by** *metis*

  then have *x ∈ eval-usages g1 n ∧ y ∈ eval-usages g1 n*

    using *inputs-of-IntegerLessThanNode inputs-of-are-usages*

     by (*metis IntegerLessThanNode.hyps*(*1*) *IntegerLessThanNode.hyps*(*2*) *IntegerLessThanNode.hyps*(*3*) *IRNodes.inputs-of-IntegerLessThanNode encode-in-ids in-mono inputs.simps inputs-are-usages list.set-intros*(*1*) *set-subset-Cons*)

  then show *?case* **using** *IntegerLessThanNode inputs-of-IntegerLessThanNode*

  by (*metis ‹kind g2 n = IntegerLessThanNode x y› child-member child-unchanged encode-in-ids ids-some member-rec*(*1*) *rep.IntegerLessThanNode*)

next

  case (*NarrowNode n ib rb x xe*)

  then have *kind g2 n = NarrowNode ib rb x*

    using *kind-unchanged* **by** *metis*

then have *x ∈ eval-usages g1 n*
  using *inputs-of-NarrowNode inputs-of-are-usages*
 by (*metis NarrowNode.hyps*(*1*) *NarrowNode.hyps*(*2*) *IRNodes.inputs-of-NarrowNode encode-in-ids inputs.simps inputs-are-usages list.set-intros*(*1*))
then show *?case* **using** *NarrowNode inputs-of-NarrowNode*
   by (*metis ‹kind g2 n = NarrowNode ib rb x› child-unchanged inputs.elims list.set-intros*(*1*) *rep.NarrowNode unchanged.simps*)
next
  case (*SignExtendNode n ib rb x xe*)
  then have *kind g2 n = SignExtendNode ib rb x*
    using *kind-unchanged* **by** *metis*
  then have *x ∈ eval-usages g1 n*
    using *inputs-of-SignExtendNode inputs-of-are-usages*
   by (*metis SignExtendNode.hyps*(*1*) *SignExtendNode.hyps*(*2*) *encode-in-ids inputs.simps inputs-are-usages list.set-intros*(*1*))
  then show *?case* **using** *SignExtendNode inputs-of-SignExtendNode*
  by (*metis ‹kind g2 n = SignExtendNode ib rb x› child-member-in child-unchanged in-set-member list.set-intros*(*1*) *rep.SignExtendNode unchanged.elims*(*2*))
next
  case (*ZeroExtendNode n ib rb x xe*)
  then have *kind g2 n = ZeroExtendNode ib rb x*
    using *kind-unchanged* **by** *metis*
  then have *x ∈ eval-usages g1 n*
    using *inputs-of-ZeroExtendNode inputs-of-are-usages*
  by (*metis ZeroExtendNode.hyps*(*1*) *ZeroExtendNode.hyps*(*2*) *IRNodes.inputs-of-ZeroExtendNode encode-in-ids inputs.simps inputs-are-usages list.set-intros*(*1*))
  then show *?case* **using** *ZeroExtendNode inputs-of-ZeroExtendNode*
  by (*metis ‹kind g2 n = ZeroExtendNode ib rb x› child-member-in child-unchanged member-rec*(*1*) *rep.ZeroExtendNode unchanged.simps*)
next
  case (*LeafNode n s*)
  then show *?case*
    by (*metis kind-unchanged rep.LeafNode stamp-unchanged*)
next
  case (*RefNode n n'*)
  then have *kind g2 n = RefNode n'*
    using *kind-unchanged* **by** *metis*
  then have *n' ∈ eval-usages g1 n*
     by (*metis IRNodes.inputs-of-RefNode RefNode.hyps*(*1*) *RefNode.hyps*(*2*) *encode-in-ids inputs.elims inputs-are-usages list.set-intros*(*1*))
  then show *?case*
  by (*metis IRNodes.inputs-of-RefNode RefNode.IH RefNode.hyps*(*1*) *RefNode.hyps*(*2*) *RefNode.prems*(*1*) *‹kind g2 n = RefNode n'› child-unchanged encode-in-ids inputs.elims list.set-intros*(*1*) *local.wf rep.RefNode*)
qed
qed

theorem *stay-same*:
  assumes *nc*: *unchanged* (*eval-usages g1 nid*) *g1 g2*
  assumes *g1*: [*g1*, *m*, *p*] ⊢ *nid* ↦ *v1*
  assumes *wf*: *wf-graph g1*
  shows [*g2*, *m*, *p*] ⊢ *nid* ↦ *v1*
proof −
  have *nid*: *nid* ∈ *ids g1*
    using *g1 eval-in-ids* **by** *simp*
  then have *nid* ∈ *eval-usages g1 nid*
    using *eval-usages-self* **by** *blast*
  then have *kind-same*: *kind g1 nid* = *kind g2 nid*
    using *nc node-unchanged* **by** *blast*
  obtain *e* **where** *e*: (*g1* ⊢ *nid* ≃ *e*) ∧ ([*m*,*p*] ⊢ *e* ↦ *v1*)
    using *encodeeval-def g1*
    by *auto*
  then have *val*: [*m*,*p*] ⊢ *e* ↦ *v1*
    using *g1 encodeeval-def*
    by *simp*
  then show *?thesis* **using** *e nid nc*
    unfolding *encodeeval-def*
  proof (*induct e v1 arbitrary*: *nid rule*: *evaltree.induct*)
    case (*ConstantExpr c*)
    then show *?case*
      by (*meson local.wf stay-same-encoding*)
  next
    case (*ParameterExpr i s*)
    have *g2* ⊢ *nid* ≃ *ParameterExpr i s*
      using *stay-same-encoding ParameterExpr*
      by (*meson local.wf*)
    then show *?case* **using** *evaltree.ParameterExpr*
      by (*meson ParameterExpr.hyps*)
  next
    case (*ConditionalExpr ce cond branch te fe v*)
    then have *g2* ⊢ *nid* ≃ *ConditionalExpr ce te fe*
    using *ConditionalExpr.prems*(*1*) *ConditionalExpr.prems*(*3*) *local.wf stay-same-encoding*
      by *presburger*
    then show *?case*
        by (*meson ConditionalExpr.prems*(*1*) *ConditionalExpr.prems*(*3*) *local.wf*
stay-same-encoding)
  next
    case (*UnaryExpr xe v op*)
    then show *?case*
      using *local.wf stay-same-encoding* **by** *blast*
  next
    case (*BinaryExpr xe x ye y op*)
    then show *?case*
      using *local.wf stay-same-encoding* **by** *blast*
  next
    case (*LeafExpr val nid s*)

    then show *?case*
      by (*metis local.wf stay-same-encoding*)
  qed
qed

lemma *add-changed*:
  assumes *gup = add-node new k g*
  shows *changeonly {new} g gup*
  using *assms* **unfolding** *add-node-def changeonly.simps*
  using *add-node.rep-eq add-node-def kind.rep-eq stamp.rep-eq* **by** *simp*

lemma *disjoint-change*:
  assumes *changeonly change g gup*
  assumes *nochange = ids g − change*
  shows *unchanged nochange g gup*
  using *assms* **unfolding** *changeonly.simps unchanged.simps*
  by *blast*

lemma *add-node-unchanged*:
  assumes *new ∉ ids g*
  assumes *nid ∈ ids g*
  assumes *gup = add-node new k g*
  assumes *wf-graph g*
  shows *unchanged (eval-usages g nid) g gup*
proof −
  have *new ∉ (eval-usages g nid)* **using** *assms*
    using *eval-usages.simps* **by** *blast*
  then have *changeonly {new} g gup*
    using *assms add-changed* **by** *blast*
  then show *?thesis* **using** *assms add-node-def disjoint-change*
    using *Diff-insert-absorb* **by** *auto*
qed

lemma *eval-uses-imp*:
  $((nid' ∈ ids\ g ∧ nid = nid')$
    $∨\ nid' ∈ inputs\ g\ nid$
    $∨\ (∃\,nid''\ .\ eval\text{-}uses\ g\ nid\ nid'' ∧ eval\text{-}uses\ g\ nid''\ nid'))$
    $⟷\ eval\text{-}uses\ g\ nid\ nid'$
  using *use0 use-inp use-trans*
  by (*meson eval-uses.simps*)

lemma *wf-use-ids*:
  assumes *wf-graph g*
  assumes *nid ∈ ids g*
  assumes *eval-uses g nid nid'*
  shows *nid' ∈ ids g*
  using *assms(3)*
proof (*induction rule*: *eval-uses.induct*)

```
  case use0
  then show ?case by simp
next
  case use-inp
  then show ?case
    using assms(1) inp-in-g-wf by blast
next
  case use-trans
  then show ?case by blast
qed

lemma no-external-use:
  assumes wf-graph g
  assumes nid′ ∉ ids g
  assumes nid ∈ ids g
  shows ¬(eval-uses g nid nid′)
proof −
  have 0: nid ≠ nid′
    using assms by blast
  have inp: nid′ ∉ inputs g nid
    using assms
    using inp-in-g-wf by blast
  have rec-0: ∄n . n ∈ ids g ∧ n = nid′
    using assms by blast
  have rec-inp: ∄n . n ∈ ids g ∧ n ∈ inputs g nid′
    using assms(2) inp-in-g by blast
  have rec: ∄nid″ . eval-uses g nid nid″ ∧ eval-uses g nid″ nid′
    using wf-use-ids assms(1) assms(2) assms(3) by blast
  from inp 0 rec show ?thesis
    using eval-uses-imp by blast
qed

end
```

7.8   Tree to Graph Theorems

```
theory TreeToGraphThms
imports
  IRTreeEvalThms
  IRGraphFrames
  HOL−Eisbach.Eisbach
  HOL−Eisbach.Eisbach-Tools
begin
```

7.8.1   Extraction and Evaluation of Expression Trees is Deterministic.

First, we prove some extra rules that relate each type of IRNode to the corresponding IRExpr type that 'rep' will produce. These are very helpful

for proving that 'rep' is deterministic.

named-theorems *rep*

lemma *rep-constant* [*rep*]:
  $g \vdash n \simeq e \Longrightarrow$
  kind g n = ConstantNode c $\Longrightarrow$
  e = ConstantExpr c
  by (*induction rule*: *rep.induct*; *auto*)

lemma *rep-parameter* [*rep*]:
  $g \vdash n \simeq e \Longrightarrow$
  kind g n = ParameterNode i $\Longrightarrow$
  $(\exists\, s.\ e = ParameterExpr\ i\ s)$
  by (*induction rule*: *rep.induct*; *auto*)

lemma *rep-conditional* [*rep*]:
  $g \vdash n \simeq e \Longrightarrow$
  kind g n = ConditionalNode c t f $\Longrightarrow$
  $(\exists\ ce\ te\ fe.\ e = ConditionalExpr\ ce\ te\ fe)$
  by (*induction rule*: *rep.induct*; *auto*)

lemma *rep-abs* [*rep*]:
  $g \vdash n \simeq e \Longrightarrow$
  kind g n = AbsNode x $\Longrightarrow$
  $(\exists\, xe.\ e = UnaryExpr\ UnaryAbs\ xe)$
  by (*induction rule*: *rep.induct*; *auto*)

lemma *rep-not* [*rep*]:
  $g \vdash n \simeq e \Longrightarrow$
  kind g n = NotNode x $\Longrightarrow$
  $(\exists\, xe.\ e = UnaryExpr\ UnaryNot\ xe)$
  by (*induction rule*: *rep.induct*; *auto*)

lemma *rep-negate* [*rep*]:
  $g \vdash n \simeq e \Longrightarrow$
  kind g n = NegateNode x $\Longrightarrow$
  $(\exists\, xe.\ e = UnaryExpr\ UnaryNeg\ xe)$
  by (*induction rule*: *rep.induct*; *auto*)

lemma *rep-logicnegation* [*rep*]:
  $g \vdash n \simeq e \Longrightarrow$
  kind g n = LogicNegationNode x $\Longrightarrow$
  $(\exists\, xe.\ e = UnaryExpr\ UnaryLogicNegation\ xe)$
  by (*induction rule*: *rep.induct*; *auto*)

lemma *rep-add* [*rep*]:
  $g \vdash n \simeq e \Longrightarrow$
  kind g n = AddNode x y $\Longrightarrow$
  $(\exists\, xe\ ye.\ e = BinaryExpr\ BinAdd\ xe\ ye)$

by (*induction rule*: *rep.induct*; *auto*)

lemma *rep-sub* [*rep*]:
  $g \vdash n \simeq e \Longrightarrow$
  kind g n = SubNode x y $\Longrightarrow$
  ($\exists$ *xe ye. e = BinaryExpr BinSub xe ye*)
  by (*induction rule*: *rep.induct*; *auto*)

lemma *rep-mul* [*rep*]:
  $g \vdash n \simeq e \Longrightarrow$
  kind g n = MulNode x y $\Longrightarrow$
  ($\exists$ *xe ye. e = BinaryExpr BinMul xe ye*)
  by (*induction rule*: *rep.induct*; *auto*)

lemma *rep-and* [*rep*]:
  $g \vdash n \simeq e \Longrightarrow$
  kind g n = AndNode x y $\Longrightarrow$
  ($\exists$ *xe ye. e = BinaryExpr BinAnd xe ye*)
  by (*induction rule*: *rep.induct*; *auto*)

lemma *rep-or* [*rep*]:
  $g \vdash n \simeq e \Longrightarrow$
  kind g n = OrNode x y $\Longrightarrow$
  ($\exists$ *xe ye. e = BinaryExpr BinOr xe ye*)
  by (*induction rule*: *rep.induct*; *auto*)

lemma *rep-xor* [*rep*]:
  $g \vdash n \simeq e \Longrightarrow$
  kind g n = XorNode x y $\Longrightarrow$
  ($\exists$ *xe ye. e = BinaryExpr BinXor xe ye*)
  by (*induction rule*: *rep.induct*; *auto*)

lemma *rep-short-circuit-or* [*rep*]:
  $g \vdash n \simeq e \Longrightarrow$
  kind g n = ShortCircuitOrNode x y $\Longrightarrow$
  ($\exists$ *xe ye. e = BinaryExpr BinShortCircuitOr xe ye*)
  by (*induction rule*: *rep.induct*; *auto*)

lemma *rep-left-shift* [*rep*]:
  $g \vdash n \simeq e \Longrightarrow$
  kind g n = LeftShiftNode x y $\Longrightarrow$
  ($\exists$ *xe ye. e = BinaryExpr BinLeftShift xe ye*)
  by (*induction rule*: *rep.induct*; *auto*)

lemma *rep-right-shift* [*rep*]:
  $g \vdash n \simeq e \Longrightarrow$
  kind g n = RightShiftNode x y $\Longrightarrow$
  ($\exists$ *xe ye. e = BinaryExpr BinRightShift xe ye*)
  by (*induction rule*: *rep.induct*; *auto*)

lemma *rep-unsigned-right-shift* [*rep*]:
  $g \vdash n \simeq e \Longrightarrow$
  kind g n = UnsignedRightShiftNode x y $\Longrightarrow$
  $(\exists\, xe\ ye.\ e = BinaryExpr\ BinURightShift\ xe\ ye)$
  by (*induction rule*: *rep.induct*; *auto*)

lemma *rep-integer-below* [*rep*]:
  $g \vdash n \simeq e \Longrightarrow$
  kind g n = IntegerBelowNode x y $\Longrightarrow$
  $(\exists\, xe\ ye.\ e = BinaryExpr\ BinIntegerBelow\ xe\ ye)$
  by (*induction rule*: *rep.induct*; *auto*)

lemma *rep-integer-equals* [*rep*]:
  $g \vdash n \simeq e \Longrightarrow$
  kind g n = IntegerEqualsNode x y $\Longrightarrow$
  $(\exists\, xe\ ye.\ e = BinaryExpr\ BinIntegerEquals\ xe\ ye)$
  by (*induction rule*: *rep.induct*; *auto*)

lemma *rep-integer-less-than* [*rep*]:
  $g \vdash n \simeq e \Longrightarrow$
  kind g n = IntegerLessThanNode x y $\Longrightarrow$
  $(\exists\, xe\ ye.\ e = BinaryExpr\ BinIntegerLessThan\ xe\ ye)$
  by (*induction rule*: *rep.induct*; *auto*)

lemma *rep-narrow* [*rep*]:
  $g \vdash n \simeq e \Longrightarrow$
  kind g n = NarrowNode ib rb x $\Longrightarrow$
  $(\exists\, x.\ e = UnaryExpr\ (UnaryNarrow\ ib\ rb)\ x)$
  by (*induction rule*: *rep.induct*; *auto*)

lemma *rep-sign-extend* [*rep*]:
  $g \vdash n \simeq e \Longrightarrow$
  kind g n = SignExtendNode ib rb x $\Longrightarrow$
  $(\exists\, x.\ e = UnaryExpr\ (UnarySignExtend\ ib\ rb)\ x)$
  by (*induction rule*: *rep.induct*; *auto*)

lemma *rep-zero-extend* [*rep*]:
  $g \vdash n \simeq e \Longrightarrow$
  kind g n = ZeroExtendNode ib rb x $\Longrightarrow$
  $(\exists\, x.\ e = UnaryExpr\ (UnaryZeroExtend\ ib\ rb)\ x)$
  by (*induction rule*: *rep.induct*; *auto*)

lemma *rep-load-field* [*rep*]:
  $g \vdash n \simeq e \Longrightarrow$
  is-preevaluated (*kind g n*) $\Longrightarrow$
  $(\exists\, s.\ e = LeafExpr\ n\ s)$
  by (*induction rule*: *rep.induct*; *auto*)

lemma *rep-ref* [*rep*]:
  $g \vdash n \simeq e \Longrightarrow$
  kind g n = RefNode n' $\Longrightarrow$
  $g \vdash n' \simeq e$
  by (*induction rule*: *rep.induct*; *auto*)

method *solve-det* **uses** *node* =
  (*match node* **in** *kind - - = node -* **for** *node* $\Rightarrow$
    ‹*match rep in r*: *-* $\Longrightarrow$ *- = node -* $\Longrightarrow$ *-* $\Rightarrow$
      ‹*match IRNode.inject in i*: (*node - = node -*) *= -* $\Rightarrow$
        ‹*match RepE in e*: *-* $\Longrightarrow$ ($\bigwedge$*x. - = node x* $\Longrightarrow$ *-*) $\Longrightarrow$ *-* $\Rightarrow$
          ‹*match IRNode.distinct in d*: *node -* $\neq$ *RefNode -* $\Rightarrow$
            ‹*metis i e r d*››››› |
  match node **in** *kind - - = node - -* **for** *node* $\Rightarrow$
    ‹*match rep in r*: *-* $\Longrightarrow$ *- = node - -* $\Longrightarrow$ *-* $\Rightarrow$
      ‹*match IRNode.inject in i*: (*node - - = node - -*) *= -* $\Rightarrow$
        ‹*match RepE in e*: *-* $\Longrightarrow$ ($\bigwedge$*x y. - = node x y* $\Longrightarrow$ *-*) $\Longrightarrow$ *-* $\Rightarrow$
          ‹*match IRNode.distinct in d*: *node - -* $\neq$ *RefNode -* $\Rightarrow$
            ‹*metis i e r d*››››› |
  match node **in** *kind - - = node - - -* **for** *node* $\Rightarrow$
    ‹*match rep in r*: *-* $\Longrightarrow$ *- = node - - -* $\Longrightarrow$ *-* $\Rightarrow$
      ‹*match IRNode.inject in i*: (*node - - - = node - - -*) *= -* $\Rightarrow$
        ‹*match RepE in e*: *-* $\Longrightarrow$ ($\bigwedge$*x y z. - = node x y z* $\Longrightarrow$ *-*) $\Longrightarrow$ *-* $\Rightarrow$
          ‹*match IRNode.distinct in d*: *node - - -* $\neq$ *RefNode -* $\Rightarrow$
            ‹*metis i e r d*››››› |
  match node **in** *kind - - = node - - -* **for** *node* $\Rightarrow$
    ‹*match rep in r*: *-* $\Longrightarrow$ *- = node - - -* $\Longrightarrow$ *-* $\Rightarrow$
      ‹*match IRNode.inject in i*: (*node - - - = node - - -*) *= -* $\Rightarrow$
        ‹*match RepE in e*: *-* $\Longrightarrow$ ($\bigwedge$*x. - = node - - x* $\Longrightarrow$ *-*) $\Longrightarrow$ *-* $\Rightarrow$
          ‹*match IRNode.distinct in d*: *node - - -* $\neq$ *RefNode -* $\Rightarrow$
            ‹*metis i e r d*›››››)

Now we can prove that 'rep' and 'eval', and their list versions, are deterministic.

lemma *repDet*:
  shows $(g \vdash n \simeq e_1) \Longrightarrow (g \vdash n \simeq e_2) \Longrightarrow e_1 = e_2$
proof (*induction arbitrary*: e_2 *rule*: *rep.induct*)
  case (*ConstantNode n c*)
  then show *?case* **using** *rep-constant* **by** *auto*
next
  case (*ParameterNode n i s*)
  then show *?case*
    by (*metis IRNode.disc*(*2685*) *ParameterNodeE is-RefNode-def rep-parameter*)
next
  case (*ConditionalNode n c t f ce te fe*)
  then show *?case*
    using *IRNode.distinct*(*593*)
    using *IRNode.inject*(*6*) *ConditionalNodeE rep-conditional*

    by *metis*
next
  case (*AbsNode n x xe*)
  then show *?case*
    by (*solve-det node*: *AbsNode*)
next
  case (*NotNode n x xe*)
  then show *?case*
    by (*solve-det node*: *NotNode*)
next
  case (*NegateNode n x xe*)
  then show *?case*
    by (*solve-det node*: *NegateNode*)
next
  case (*LogicNegationNode n x xe*)
  then show *?case*
    by (*solve-det node*: *LogicNegationNode*)
next
  case (*AddNode n x y xe ye*)
  then show *?case*
    by (*solve-det node*: *AddNode*)
next
  case (*MulNode n x y xe ye*)
  then show *?case*
    by (*solve-det node*: *MulNode*)
next
  case (*SubNode n x y xe ye*)
  then show *?case*
    by (*solve-det node*: *SubNode*)
next
  case (*AndNode n x y xe ye*)
  then show *?case*
    by (*solve-det node*: *AndNode*)
next
  case (*OrNode n x y xe ye*)
  then show *?case*
    by (*solve-det node*: *OrNode*)
next
  case (*XorNode n x y xe ye*)
  then show *?case*
    by (*solve-det node*: *XorNode*)
next
  case (*ShortCircuitOrNode n x y xe ye*)
  then show *?case*
    by (*solve-det node*: *ShortCircuitOrNode*)
next
  case (*LeftShiftNode n x y xe ye*)
  then show *?case*
    by (*solve-det node*: *LeftShiftNode*)

next
  case (*RightShiftNode n x y xe ye*)
  then show *?case*
    by (*solve-det node*: *RightShiftNode*)
next
  case (*UnsignedRightShiftNode n x y xe ye*)
  then show *?case*
    by (*solve-det node*: *UnsignedRightShiftNode*)
next
  case (*IntegerBelowNode n x y xe ye*)
  then show *?case*
    by (*solve-det node*: *IntegerBelowNode*)
next
  case (*IntegerEqualsNode n x y xe ye*)
  then show *?case*
    by (*solve-det node*: *IntegerEqualsNode*)
next
  case (*IntegerLessThanNode n x y xe ye*)
  then show *?case*
    by (*solve-det node*: *IntegerLessThanNode*)
next
  case (*NarrowNode n x xe*)
  then show *?case*
    by (*metis IRNode.distinct*(*2203*) *IRNode.inject*(*28*) *NarrowNodeE rep-narrow*)
next
  case (*SignExtendNode n x xe*)
  then show *?case*
  by (*metis IRNode.distinct*(*2599*) *IRNode.inject*(*39*) *SignExtendNodeE rep-sign-extend*)
next
  case (*ZeroExtendNode n x xe*)
  then show *?case*
  by (*metis IRNode.distinct*(*2753*) *IRNode.inject*(*50*) *ZeroExtendNodeE rep-zero-extend*)
next
  case (*LeafNode n s*)
  then show *?case* **using** *rep-load-field LeafNodeE*
    by (*metis is-preevaluated.simps*(*53*))
next
  case (*RefNode n′*)
  then show *?case*
    using *rep-ref* **by** *blast*
qed

lemma *repAllDet*:
  $g \vdash xs \simeq_L e1 \implies$
  $g \vdash xs \simeq_L e2 \implies$
  $e1 = e2$
proof (*induction arbitrary*: *e2 rule*: *replist.induct*)
  case *RepNil*
  then show *?case*

84

    using *replist.cases* **by** *auto*
next
  case (*RepCons x xe xs xse*)
  then show *?case*
    by (*metis list.distinct(1) list.sel(1) list.sel(3) repDet replist.cases*)
qed

lemma *encodeEvalDet*:
  $[g,m,p] \vdash e \mapsto v1 \Longrightarrow$
  $[g,m,p] \vdash e \mapsto v2 \Longrightarrow$
  $v1 = v2$
  by (*metis encodeeval-def evalDet repDet*)

lemma *graphDet*: $([g,m,p] \vdash n \mapsto v_1) \wedge ([g,m,p] \vdash n \mapsto v_2) \Longrightarrow v_1 = v_2$
  using *encodeEvalDet* **by** *blast*

7.8.2 Monotonicity of Graph Refinement

Lift refinement monotonicity to graph level. Hopefully these shouldn't really be required.

lemma *mono-abs*:
  assumes *kind g1 n = AbsNode x* $\wedge$ *kind g2 n = AbsNode x*
  assumes $(g1 \vdash x \simeq xe1) \wedge (g2 \vdash x \simeq xe2)$
  assumes $xe1 \geq xe2$
  assumes $(g1 \vdash n \simeq e1) \wedge (g2 \vdash n \simeq e2)$
  shows $e1 \geq e2$
  by (*metis AbsNode assms(1) assms(2) assms(3) assms(4) mono-unary repDet*)

lemma *mono-not*:
  assumes *kind g1 n = NotNode x* $\wedge$ *kind g2 n = NotNode x*
  assumes $(g1 \vdash x \simeq xe1) \wedge (g2 \vdash x \simeq xe2)$
  assumes $xe1 \geq xe2$
  assumes $(g1 \vdash n \simeq e1) \wedge (g2 \vdash n \simeq e2)$
  shows $e1 \geq e2$
  by (*metis NotNode assms(1) assms(2) assms(3) assms(4) mono-unary repDet*)

lemma *mono-negate*:
  assumes *kind g1 n = NegateNode x* $\wedge$ *kind g2 n = NegateNode x*
  assumes $(g1 \vdash x \simeq xe1) \wedge (g2 \vdash x \simeq xe2)$
  assumes $xe1 \geq xe2$
  assumes $(g1 \vdash n \simeq e1) \wedge (g2 \vdash n \simeq e2)$
  shows $e1 \geq e2$
  by (*metis NegateNode assms(1) assms(2) assms(3) assms(4) mono-unary repDet*)

lemma *mono-logic-negation*:
  assumes *kind g1 n = LogicNegationNode x* $\wedge$ *kind g2 n = LogicNegationNode x*
  assumes $(g1 \vdash x \simeq xe1) \wedge (g2 \vdash x \simeq xe2)$
  assumes $xe1 \geq xe2$
  assumes $(g1 \vdash n \simeq e1) \wedge (g2 \vdash n \simeq e2)$

shows $e1 \geq e2$
by (*metis LogicNegationNode assms*(*1*) *assms*(*2*) *assms*(*3*) *assms*(*4*) *mono-unary repDet*)

lemma *mono-narrow*:
  assumes *kind g1 n = NarrowNode ib rb x* $\wedge$ *kind g2 n = NarrowNode ib rb x*
  assumes (*g1* $\vdash$ *x* $\simeq$ *xe1*) $\wedge$ (*g2* $\vdash$ *x* $\simeq$ *xe2*)
  assumes *xe1* $\geq$ *xe2*
  assumes (*g1* $\vdash$ *n* $\simeq$ *e1*) $\wedge$ (*g2* $\vdash$ *n* $\simeq$ *e2*)
  shows $e1 \geq e2$
  using *assms mono-unary repDet NarrowNode*
  by *metis*

lemma *mono-sign-extend*:
  assumes *kind g1 n = SignExtendNode ib rb x* $\wedge$ *kind g2 n = SignExtendNode ib rb x*
  assumes (*g1* $\vdash$ *x* $\simeq$ *xe1*) $\wedge$ (*g2* $\vdash$ *x* $\simeq$ *xe2*)
  assumes *xe1* $\geq$ *xe2*
  assumes (*g1* $\vdash$ *n* $\simeq$ *e1*) $\wedge$ (*g2* $\vdash$ *n* $\simeq$ *e2*)
  shows $e1 \geq e2$
  by (*metis SignExtendNode assms*(*1*) *assms*(*2*) *assms*(*3*) *assms*(*4*) *mono-unary repDet*)

lemma *mono-zero-extend*:
  assumes *kind g1 n = ZeroExtendNode ib rb x* $\wedge$ *kind g2 n = ZeroExtendNode ib rb x*
  assumes (*g1* $\vdash$ *x* $\simeq$ *xe1*) $\wedge$ (*g2* $\vdash$ *x* $\simeq$ *xe2*)
  assumes *xe1* $\geq$ *xe2*
  assumes (*g1* $\vdash$ *n* $\simeq$ *e1*) $\wedge$ (*g2* $\vdash$ *n* $\simeq$ *e2*)
  shows $e1 \geq e2$
  using *assms mono-unary repDet ZeroExtendNode*
  by *metis*

lemma *mono-conditional-graph*:
  assumes *kind g1 n = ConditionalNode c t f* $\wedge$ *kind g2 n = ConditionalNode c t f*
  assumes (*g1* $\vdash$ *c* $\simeq$ *ce1*) $\wedge$ (*g2* $\vdash$ *c* $\simeq$ *ce2*)
  assumes (*g1* $\vdash$ *t* $\simeq$ *te1*) $\wedge$ (*g2* $\vdash$ *t* $\simeq$ *te2*)
  assumes (*g1* $\vdash$ *f* $\simeq$ *fe1*) $\wedge$ (*g2* $\vdash$ *f* $\simeq$ *fe2*)
  assumes *ce1* $\geq$ *ce2* $\wedge$ *te1* $\geq$ *te2* $\wedge$ *fe1* $\geq$ *fe2*
  assumes (*g1* $\vdash$ *n* $\simeq$ *e1*) $\wedge$ (*g2* $\vdash$ *n* $\simeq$ *e2*)
  shows $e1 \geq e2$
  using *ConditionalNodeE IRNode.inject*(*6*) *assms*(*1*) *assms*(*2*) *assms*(*3*) *assms*(*4*) *assms*(*5*) *assms*(*6*) *mono-conditional repDet rep-conditional*
  by (*smt* (*verit, best*) *ConditionalNode*)

lemma *mono-add*:
  assumes *kind g1 n = AddNode x y* $\wedge$ *kind g2 n = AddNode x y*
  assumes (*g1* $\vdash$ *x* $\simeq$ *xe1*) $\wedge$ (*g2* $\vdash$ *x* $\simeq$ *xe2*)
  assumes (*g1* $\vdash$ *y* $\simeq$ *ye1*) $\wedge$ (*g2* $\vdash$ *y* $\simeq$ *ye2*)

assumes *xe1 ≥ xe2 ∧ ye1 ≥ ye2*
assumes *(g1 ⊢ n ≃ e1) ∧ (g2 ⊢ n ≃ e2)*
shows *e1 ≥ e2*
using *mono-binary assms AddNodeE IRNode.inject(2) repDet rep-add*
by (*metis IRNode.distinct(205)*)

lemma *mono-mul*:
  assumes *kind g1 n = MulNode x y ∧ kind g2 n = MulNode x y*
  assumes *(g1 ⊢ x ≃ xe1) ∧ (g2 ⊢ x ≃ xe2)*
  assumes *(g1 ⊢ y ≃ ye1) ∧ (g2 ⊢ y ≃ ye2)*
  assumes *xe1 ≥ xe2 ∧ ye1 ≥ ye2*
  assumes *(g1 ⊢ n ≃ e1) ∧ (g2 ⊢ n ≃ e2)*
  shows *e1 ≥ e2*
  using *mono-binary assms IRNode.inject(27) MulNodeE repDet rep-mul*
  by (*smt (verit, best) MulNode*)

lemma *term-graph-evaluation*:
  (g ⊢ n ⊴ e) ⟹ (∀ m p v . ([m,p] ⊢ e ↦ v) ⟶ ([g,m,p] ⊢ n ↦ v))
  unfolding *graph-represents-expression-def* **apply** *auto*
  by (*meson encodeeval-def*)

lemma *encodes-contains*:
  g ⊢ n ≃ e ⟹
  kind g n ≠ NoNode
  apply (*induction rule: rep.induct*)
  apply (*match IRNode.distinct* **in** *e: ?n ≠ NoNode ⇒*
      ‹*presburger add: e*›)+
  apply *force*
  by *fastforce*

lemma *no-encoding*:
  assumes *n ∉ ids g*
  shows *¬(g ⊢ n ≃ e)*
   using *assms* **apply** *simp* **apply** (*rule notI*) **by** (*induction e; simp add: en-codes-contains*)

lemma *not-excluded-keep-type*:
  assumes *n ∈ ids g1*
  assumes *n ∉ excluded*
  assumes *(excluded ⊴ as-set g1) ⊆ as-set g2*
  shows *kind g1 n = kind g2 n ∧ stamp g1 n = stamp g2 n*
  using *assms* **unfolding** *as-set-def domain-subtraction-def* **by** *blast*

method *metis-node-eq-unary* **for** *node :: 'a ⇒ IRNode =*
  (*match IRNode.inject* **in** *i: (node - = node -) = - ⇒*
      ‹*metis i*›)
method *metis-node-eq-binary* **for** *node :: 'a ⇒ 'a ⇒ IRNode =*
  (*match IRNode.inject* **in** *i: (node - - = node - -) = - ⇒*

$\langle$*metis i*$\rangle$)

method *metis-node-eq-ternary* **for** *node* :: $'a \Rightarrow \, 'a \Rightarrow \, 'a \Rightarrow IRNode =$
  (*match IRNode.inject* **in** *i*: (*node* - - - = *node* - - -) = - $\Rightarrow$
    $\langle$*metis i*$\rangle$)

7.8.3   Lift Data-flow Tree Refinement to Graph Refinement

theorem *graph-semantics-preservation*:
  assumes *a*: $e1' \geq e2'$
  assumes *b*: $(\{n'\} \unlhd \textit{as-set } g1) \subseteq \textit{as-set } g2$
  assumes *c*: $g1 \vdash n' \simeq e1'$
  assumes *d*: $g2 \vdash n' \simeq e2'$
  shows *graph-refinement g1 g2*
  unfolding *graph-refinement-def* **apply** *rule*
   apply (*metis b d ids-some no-encoding not-excluded-keep-type singleton-iff sub-setI*)
  apply (*rule allI*) **apply** (*rule impI*) **apply** (*rule allI*) **apply** (*rule impI*)
  unfolding *graph-represents-expression-def*
proof −
  fix *n e1*
  assume *e*: $n \in ids\ g1$
  assume *f*: $(g1 \vdash n \simeq e1)$

  show $\exists\ e2.\ (g2 \vdash n \simeq e2) \wedge e1 \geq e2$
  proof (*cases n = n'*)
   case *True*
   have *g*: $e1 = e1'$ **using** *c f True repDet* **by** *simp*
   have *h*: $(g2 \vdash n \simeq e2') \wedge e1' \geq e2'$
     using *True a d* **by** *blast*
   then show *?thesis*
     using *g* **by** *blast*
  next
   case *False*
   have $n \notin \{n'\}$
     using *False* **by** *simp*
   then have *i*: *kind g1 n = kind g2 n* $\wedge$ *stamp g1 n = stamp g2 n*
     using *not-excluded-keep-type*
     using *b e* **by** *presburger*
   show *?thesis* **using** *f i*
   proof (*induction e1*)
    case (*ConstantNode n c*)
    then show *?case*
      by (*metis eq-refl rep.ConstantNode*)
   next
    case (*ParameterNode n i s*)
    then show *?case*
      by (*metis eq-refl rep.ParameterNode*)
   next
    case (*ConditionalNode n c t f ce1 te1 fe1*)

have k: *g1 ⊢ n ≃ ConditionalExpr ce1 te1 fe1* **using** *f ConditionalNode*
  by (*simp add*: *ConditionalNode.hyps*(*2*) *rep.ConditionalNode*)
obtain *cn tn fn* **where** *l*: *kind g1 n = ConditionalNode cn tn fn*
  using *ConditionalNode.hyps*(*1*) **by** *blast*
then have *mc*: *g1 ⊢ cn ≃ ce1*
  using *ConditionalNode.hyps*(*1*) *ConditionalNode.hyps*(*2*) **by** *fastforce*
from *l* **have** *mt*: *g1 ⊢ tn ≃ te1*
  using *ConditionalNode.hyps*(*1*) *ConditionalNode.hyps*(*3*) **by** *fastforce*
from *l* **have** *mf*: *g1 ⊢ fn ≃ fe1*
  using *ConditionalNode.hyps*(*1*) *ConditionalNode.hyps*(*4*) **by** *fastforce*
then show *?case*
proof −
  have *g1 ⊢ cn ≃ ce1* **using** *mc* **by** *simp*
  have *g1 ⊢ tn ≃ te1* **using** *mt* **by** *simp*
  have *g1 ⊢ fn ≃ fe1* **using** *mf* **by** *simp*
  have *cer*: ∃ *ce2.* (*g2 ⊢ cn ≃ ce2*) ∧ *ce1 ≥ ce2*
    using *ConditionalNode*
    using *a b c d l no-encoding not-excluded-keep-type repDet singletonD*
    by (*metis-node-eq-ternary ConditionalNode*)
  have *ter*: ∃ *te2.* (*g2 ⊢ tn ≃ te2*) ∧ *te1 ≥ te2*
    using *ConditionalNode a b c d l no-encoding not-excluded-keep-type repDet*
singletonD
    by (*metis-node-eq-ternary ConditionalNode*)
  have ∃ *fe2.* (*g2 ⊢ fn ≃ fe2*) ∧ *fe1 ≥ fe2*
    using *ConditionalNode a b c d l no-encoding not-excluded-keep-type repDet*
singletonD
    by (*metis-node-eq-ternary ConditionalNode*)
    then have ∃ *ce2 te2 fe2.* (*g2 ⊢ n ≃ ConditionalExpr ce2 te2 fe2*) ∧
ConditionalExpr ce1 te1 fe1 ≥ ConditionalExpr ce2 te2 fe2
    using *ConditionalNode.prems l rep.ConditionalNode cer ter*
    by (*smt* (*verit*) *mono-conditional*)
  then show *?thesis*
    by *meson*
 qed
next
  case (*AbsNode n x xe1*)
  have k: *g1 ⊢ n ≃ UnaryExpr UnaryAbs xe1* **using** *f AbsNode*
    by (*simp add*: *AbsNode.hyps*(*2*) *rep.AbsNode*)
  obtain *xn* **where** *l*: *kind g1 n = AbsNode xn*
    using *AbsNode.hyps*(*1*) **by** *blast*
  then have *m*: *g1 ⊢ xn ≃ xe1*
    using *AbsNode.hyps*(*1*) *AbsNode.hyps*(*2*) **by** *fastforce*
  then show *?case*
  proof (*cases xn = n′*)
    case *True*
    then have *n*: *xe1 = e1′* **using** *c m repDet* **by** *simp*
    then have *ev*: *g2 ⊢ n ≃ UnaryExpr UnaryAbs e2′* **using** *AbsNode.hyps*(*1*)
l m n
      using *AbsNode.prems True d rep.AbsNode* **by** *simp*

89

then have *r*: *UnaryExpr UnaryAbs e1'* ≥ *UnaryExpr UnaryAbs e2'*
  by (*meson a mono-unary*)
then show *?thesis* **using** *ev r*
  by (*metis n*)
next
  case *False*
  have *g1* ⊢ *xn* ≃ *xe1* **using** *m* **by** *simp*
  have ∃ *xe2*. (*g2* ⊢ *xn* ≃ *xe2*) ∧ *xe1* ≥ *xe2*
    using *AbsNode*
  using *False b encodes-contains l not-excluded-keep-type not-in-g singleton-iff*
    by (*metis-node-eq-unary AbsNode*)
    then have ∃ *xe2*. (*g2* ⊢ *n* ≃ *UnaryExpr UnaryAbs xe2*) ∧ *UnaryExpr*
UnaryAbs xe1 ≥ *UnaryExpr UnaryAbs xe2*
    by (*metis AbsNode.prems l mono-unary rep.AbsNode*)
  then show *?thesis*
    by *meson*
qed
next
  case (*NotNode n x xe1*)
  have *k*: *g1* ⊢ *n* ≃ *UnaryExpr UnaryNot xe1* **using** *f NotNode*
    by (*simp add*: *NotNode.hyps*(*2*) *rep.NotNode*)
  obtain *xn* **where** *l*: *kind g1 n* = *NotNode xn*
    using *NotNode.hyps*(*1*) **by** *blast*
  then have *m*: *g1* ⊢ *xn* ≃ *xe1*
    using *NotNode.hyps*(*1*) *NotNode.hyps*(*2*) **by** *fastforce*
  then show *?case*
  proof (*cases xn = n'*)
    case *True*
    then have *n*: *xe1* = *e1'* **using** *c m repDet* **by** *simp*
    then have *ev*: *g2* ⊢ *n* ≃ *UnaryExpr UnaryNot e2'* **using** *NotNode.hyps*(*1*)
l m n
      using *NotNode.prems True d rep.NotNode* **by** *simp*
    then have *r*: *UnaryExpr UnaryNot e1'* ≥ *UnaryExpr UnaryNot e2'*
      by (*meson a mono-unary*)
    then show *?thesis* **using** *ev r*
      by (*metis n*)
  next
    case *False*
    have *g1* ⊢ *xn* ≃ *xe1* **using** *m* **by** *simp*
    have ∃ *xe2*. (*g2* ⊢ *xn* ≃ *xe2*) ∧ *xe1* ≥ *xe2*
      using *NotNode*
      using *False i b l not-excluded-keep-type singletonD no-encoding*
      by (*metis-node-eq-unary NotNode*)
      then have ∃ *xe2*. (*g2* ⊢ *n* ≃ *UnaryExpr UnaryNot xe2*) ∧ *UnaryExpr*
UnaryNot xe1 ≥ *UnaryExpr UnaryNot xe2*
      by (*metis NotNode.prems l mono-unary rep.NotNode*)
    then show *?thesis*
      by *meson*
  qed

next
  case (*NegateNode n x xe1*)
  have *k*: $g1 \vdash n \simeq UnaryExpr\ UnaryNeg\ xe1$ **using** *f NegateNode*
    by (*simp add*: *NegateNode.hyps*(*2*) *rep.NegateNode*)
  obtain *xn* **where** *l*: *kind g1 n = NegateNode xn*
    using *NegateNode.hyps*(*1*) **by** *blast*
  then have *m*: $g1 \vdash xn \simeq xe1$
    using *NegateNode.hyps*(*1*) *NegateNode.hyps*(*2*) **by** *fastforce*
  then show *?case*
  proof (*cases xn = n'*)
    case *True*
    then have *n*: $xe1 = e1'$ **using** *c m repDet* **by** *simp*
    then have *ev*: $g2 \vdash n \simeq UnaryExpr\ UnaryNeg\ e2'$ **using** *NegateNode.hyps*(*1*)
l m n

      using *NegateNode.prems True d rep.NegateNode* **by** *simp*
    then have *r*: $UnaryExpr\ UnaryNeg\ e1' \geq UnaryExpr\ UnaryNeg\ e2'$
      by (*meson a mono-unary*)
    then show *?thesis* **using** *ev r*
      by (*metis n*)
  next
    case *False*
    have $g1 \vdash xn \simeq xe1$ **using** *m* **by** *simp*
    have $\exists\ xe2.\ (g2 \vdash xn \simeq xe2) \land xe1 \geq xe2$
      using *NegateNode*
      using *False i b l not-excluded-keep-type singletonD no-encoding*
      by (*metis-node-eq-unary NegateNode*)
      then have $\exists\ xe2.\ (g2 \vdash n \simeq UnaryExpr\ UnaryNeg\ xe2) \land UnaryExpr$
$UnaryNeg\ xe1 \geq UnaryExpr\ UnaryNeg\ xe2$
      by (*metis NegateNode.prems l mono-unary rep.NegateNode*)
    then show *?thesis*
      by *meson*
  qed
next
  case (*LogicNegationNode n x xe1*)
   have *k*: $g1 \vdash n \simeq UnaryExpr\ UnaryLogicNegation\ xe1$ **using** *f LogicNega-*
tionNode
    by (*simp add*: *LogicNegationNode.hyps*(*2*) *rep.LogicNegationNode*)
  obtain *xn* **where** *l*: *kind g1 n = LogicNegationNode xn*
    using *LogicNegationNode.hyps*(*1*) **by** *blast*
  then have *m*: $g1 \vdash xn \simeq xe1$
    using *LogicNegationNode.hyps*(*1*) *LogicNegationNode.hyps*(*2*) **by** *fastforce*
  then show *?case*
  proof (*cases xn = n'*)
    case *True*
    then have *n*: $xe1 = e1'$ **using** *c m repDet* **by** *simp*
      then have *ev*: $g2 \vdash n \simeq UnaryExpr\ UnaryLogicNegation\ e2'$ **using**
LogicNegationNode.hyps(*1*) *l m n*
      using *LogicNegationNode.prems True d rep.LogicNegationNode* **by** *simp*
    then have *r*: $UnaryExpr\ UnaryLogicNegation\ e1' \geq UnaryExpr\ UnaryLog\text{-}$

91

icNegation e2′
      by (*meson a mono-unary*)
    then show *?thesis* **using** *ev r*
      by (*metis n*)
  next
    case *False*
    have $g1 \vdash xn \simeq xe1$ **using** *m* **by** *simp*
    have $\exists\ xe2.\ (g2 \vdash xn \simeq xe2) \land xe1 \geq xe2$
      using *LogicNegationNode*
      using *False i b l not-excluded-keep-type singletonD no-encoding*
      by (*metis-node-eq-unary LogicNegationNode*)
      then have $\exists\ xe2.\ (g2 \vdash n \simeq UnaryExpr\ UnaryLogicNegation\ xe2) \land$
$UnaryExpr\ UnaryLogicNegation\ xe1 \geq UnaryExpr\ UnaryLogicNegation\ xe2$
      by (*metis LogicNegationNode.prems l mono-unary rep.LogicNegationNode*)
    then show *?thesis*
      by *meson*
  qed
  next
    case (*AddNode n x y xe1 ye1*)
    have *k*: $g1 \vdash n \simeq BinaryExpr\ BinAdd\ xe1\ ye1$ **using** *f AddNode*
      by (*simp add*: *AddNode.hyps*(*2*) *rep.AddNode*)
    obtain *xn yn* **where** *l*: *kind g1 n = AddNode xn yn*
      using *AddNode.hyps*(*1*) **by** *blast*
    then have *mx*: $g1 \vdash xn \simeq xe1$
      using *AddNode.hyps*(*1*) *AddNode.hyps*(*2*) **by** *fastforce*
    from *l* **have** *my*: $g1 \vdash yn \simeq ye1$
      using *AddNode.hyps*(*1*) *AddNode.hyps*(*3*) **by** *fastforce*
    then show *?case*
    proof −
      have $g1 \vdash xn \simeq xe1$ **using** *mx* **by** *simp*
      have $g1 \vdash yn \simeq ye1$ **using** *my* **by** *simp*
      have *xer*: $\exists\ xe2.\ (g2 \vdash xn \simeq xe2) \land xe1 \geq xe2$
        using *AddNode*
        using *a b c d l no-encoding not-excluded-keep-type repDet singletonD*
        by (*metis-node-eq-binary AddNode*)
      have $\exists\ ye2.\ (g2 \vdash yn \simeq ye2) \land ye1 \geq ye2$
        using *AddNode*
        using *a b c d l no-encoding not-excluded-keep-type repDet singletonD*
        by (*metis-node-eq-binary AddNode*)
     then have $\exists\ xe2\ ye2.\ (g2 \vdash n \simeq BinaryExpr\ BinAdd\ xe2\ ye2) \land BinaryExpr$
$BinAdd\ xe1\ ye1 \geq BinaryExpr\ BinAdd\ xe2\ ye2$
      by (*metis AddNode.prems l mono-binary rep.AddNode xer*)
     then show *?thesis*
      by *meson*
    qed
  next
    case (*MulNode n x y xe1 ye1*)
    have *k*: $g1 \vdash n \simeq BinaryExpr\ BinMul\ xe1\ ye1$ **using** *f MulNode*
      by (*simp add*: *MulNode.hyps*(*2*) *rep.MulNode*)

<div align="center">92</div>

obtain *xn yn* **where** *l*: *kind g1 n = MulNode xn yn*
  using *MulNode.hyps*(*1*) **by** *blast*
then have *mx*: *g1 ⊢ xn ≃ xe1*
  using *MulNode.hyps*(*1*) *MulNode.hyps*(*2*) **by** *fastforce*
from *l* **have** *my*: *g1 ⊢ yn ≃ ye1*
  using *MulNode.hyps*(*1*) *MulNode.hyps*(*3*) **by** *fastforce*
then show *?case*
proof −
  have *g1 ⊢ xn ≃ xe1* **using** *mx* **by** *simp*
  have *g1 ⊢ yn ≃ ye1* **using** *my* **by** *simp*
  have *xer*: ∃ *xe2*. (*g2 ⊢ xn ≃ xe2*) ∧ *xe1 ≥ xe2*
    using *MulNode*
    using *a b c d l no-encoding not-excluded-keep-type repDet singletonD*
    by (*metis-node-eq-binary MulNode*)
  have ∃ *ye2*. (*g2 ⊢ yn ≃ ye2*) ∧ *ye1 ≥ ye2*
    using *MulNode*
    using *a b c d l no-encoding not-excluded-keep-type repDet singletonD*
    by (*metis-node-eq-binary MulNode*)
 then have ∃ *xe2 ye2*. (*g2 ⊢ n ≃ BinaryExpr BinMul xe2 ye2*) ∧ *BinaryExpr*
BinMul xe1 ye1 ≥ BinaryExpr BinMul xe2 ye2
    by (*metis MulNode.prems l mono-binary rep.MulNode xer*)
  then show *?thesis*
    by *meson*
qed
next
 case (*SubNode n x y xe1 ye1*)
 have *k*: *g1 ⊢ n ≃ BinaryExpr BinSub xe1 ye1* **using** *f SubNode*
  by (*simp add*: *SubNode.hyps*(*2*) *rep.SubNode*)
 obtain *xn yn* **where** *l*: *kind g1 n = SubNode xn yn*
  using *SubNode.hyps*(*1*) **by** *blast*
 then have *mx*: *g1 ⊢ xn ≃ xe1*
  using *SubNode.hyps*(*1*) *SubNode.hyps*(*2*) **by** *fastforce*
 from *l* **have** *my*: *g1 ⊢ yn ≃ ye1*
  using *SubNode.hyps*(*1*) *SubNode.hyps*(*3*) **by** *fastforce*
 then show *?case*
 proof −
  have *g1 ⊢ xn ≃ xe1* **using** *mx* **by** *simp*
  have *g1 ⊢ yn ≃ ye1* **using** *my* **by** *simp*
  have *xer*: ∃ *xe2*. (*g2 ⊢ xn ≃ xe2*) ∧ *xe1 ≥ xe2*
    using *SubNode*
    using *a b c d l no-encoding not-excluded-keep-type repDet singletonD*
    by (*metis-node-eq-binary SubNode*)
  have ∃ *ye2*. (*g2 ⊢ yn ≃ ye2*) ∧ *ye1 ≥ ye2*
  using *SubNode a b c d l no-encoding not-excluded-keep-type repDet singletonD*
    by (*metis-node-eq-binary SubNode*)
 then have ∃ *xe2 ye2*. (*g2 ⊢ n ≃ BinaryExpr BinSub xe2 ye2*) ∧ *BinaryExpr*
BinSub xe1 ye1 ≥ BinaryExpr BinSub xe2 ye2
    by (*metis SubNode.prems l mono-binary rep.SubNode xer*)
  then show *?thesis*

by *meson*
  qed
next
  case (*AndNode n x y xe1 ye1*)
  have *k*: *g1* ⊢ *n* ≃ *BinaryExpr BinAnd xe1 ye1* **using** *f AndNode*
    by (*simp add*: *AndNode.hyps*(*2*) *rep.AndNode*)
  obtain *xn yn* **where** *l*: *kind g1 n* = *AndNode xn yn*
    using *AndNode.hyps*(*1*) **by** *blast*
  then have *mx*: *g1* ⊢ *xn* ≃ *xe1*
    using *AndNode.hyps*(*1*) *AndNode.hyps*(*2*) **by** *fastforce*
  from *l* **have** *my*: *g1* ⊢ *yn* ≃ *ye1*
    using *AndNode.hyps*(*1*) *AndNode.hyps*(*3*) **by** *fastforce*
  then show *?case*
  proof −
    have *g1* ⊢ *xn* ≃ *xe1* **using** *mx* **by** *simp*
    have *g1* ⊢ *yn* ≃ *ye1* **using** *my* **by** *simp*
    have *xer*: ∃ *xe2*. (*g2* ⊢ *xn* ≃ *xe2*) ∧ *xe1* ≥ *xe2*
      using *AndNode*
      using *a b c d l no-encoding not-excluded-keep-type repDet singletonD*
      by (*metis-node-eq-binary AndNode*)
    have ∃ *ye2*. (*g2* ⊢ *yn* ≃ *ye2*) ∧ *ye1* ≥ *ye2*
        using *AndNode a b c d l no-encoding not-excluded-keep-type repDet*
singletonD
      by (*metis-node-eq-binary AndNode*)
    then have ∃ *xe2 ye2*. (*g2* ⊢ *n* ≃ *BinaryExpr BinAnd xe2 ye2*) ∧ *BinaryExpr*
BinAnd xe1 ye1 ≥ *BinaryExpr BinAnd xe2 ye2*
      by (*metis AndNode.prems l mono-binary rep.AndNode xer*)
    then show *?thesis*
      by *meson*
  qed
next
  case (*OrNode n x y xe1 ye1*)
  have *k*: *g1* ⊢ *n* ≃ *BinaryExpr BinOr xe1 ye1* **using** *f OrNode*
    by (*simp add*: *OrNode.hyps*(*2*) *rep.OrNode*)
  obtain *xn yn* **where** *l*: *kind g1 n* = *OrNode xn yn*
    using *OrNode.hyps*(*1*) **by** *blast*
  then have *mx*: *g1* ⊢ *xn* ≃ *xe1*
    using *OrNode.hyps*(*1*) *OrNode.hyps*(*2*) **by** *fastforce*
  from *l* **have** *my*: *g1* ⊢ *yn* ≃ *ye1*
    using *OrNode.hyps*(*1*) *OrNode.hyps*(*3*) **by** *fastforce*
  then show *?case*
  proof −
    have *g1* ⊢ *xn* ≃ *xe1* **using** *mx* **by** *simp*
    have *g1* ⊢ *yn* ≃ *ye1* **using** *my* **by** *simp*
    have *xer*: ∃ *xe2*. (*g2* ⊢ *xn* ≃ *xe2*) ∧ *xe1* ≥ *xe2*
      using *OrNode*
      using *a b c d l no-encoding not-excluded-keep-type repDet singletonD*
      by (*metis-node-eq-binary OrNode*)
    have ∃ *ye2*. (*g2* ⊢ *yn* ≃ *ye2*) ∧ *ye1* ≥ *ye2*

using *OrNode a b c d l no-encoding not-excluded-keep-type repDet singletonD*
    by (*metis-node-eq-binary OrNode*)
then have $\exists\ xe2\ ye2.\ (g2 \vdash n \simeq BinaryExpr\ BinOr\ xe2\ ye2) \wedge BinaryExpr$
$BinOr\ xe1\ ye1 \geq BinaryExpr\ BinOr\ xe2\ ye2$
    by (*metis OrNode.prems l mono-binary rep.OrNode xer*)
then show *?thesis*
    by *meson*
  qed
next
  case (*XorNode n x y xe1 ye1*)
  have *k*: $g1 \vdash n \simeq BinaryExpr\ BinXor\ xe1\ ye1$ **using** *f XorNode*
    by (*simp add*: *XorNode.hyps*(*2*) *rep.XorNode*)
  obtain *xn yn* **where** *l*: *kind g1 n = XorNode xn yn*
    using *XorNode.hyps*(*1*) **by** *blast*
  then have *mx*: $g1 \vdash xn \simeq xe1$
    using *XorNode.hyps*(*1*) *XorNode.hyps*(*2*) **by** *fastforce*
  from *l* **have** *my*: $g1 \vdash yn \simeq ye1$
    using *XorNode.hyps*(*1*) *XorNode.hyps*(*3*) **by** *fastforce*
  then show *?case*
  proof −
    have $g1 \vdash xn \simeq xe1$ **using** *mx* **by** *simp*
    have $g1 \vdash yn \simeq ye1$ **using** *my* **by** *simp*
    have *xer*: $\exists\ xe2.\ (g2 \vdash xn \simeq xe2) \wedge xe1 \geq xe2$
      using *XorNode*
      using *a b c d l no-encoding not-excluded-keep-type repDet singletonD*
      by (*metis-node-eq-binary XorNode*)
    have $\exists\ ye2.\ (g2 \vdash yn \simeq ye2) \wedge ye1 \geq ye2$
        using *XorNode a b c d l no-encoding not-excluded-keep-type repDet*
singletonD
      by (*metis-node-eq-binary XorNode*)
    then have $\exists\ xe2\ ye2.\ (g2 \vdash n \simeq BinaryExpr\ BinXor\ xe2\ ye2) \wedge BinaryExpr$
$BinXor\ xe1\ ye1 \geq BinaryExpr\ BinXor\ xe2\ ye2$
      by (*metis XorNode.prems l mono-binary rep.XorNode xer*)
    then show *?thesis*
      by *meson*
  qed
next
  case (*ShortCircuitOrNode n x y xe1 ye1*)
  have *k*: $g1 \vdash n \simeq BinaryExpr\ BinShortCircuitOr\ xe1\ ye1$ **using** *f ShortCir-*
cuitOrNode
    by (*simp add*: *ShortCircuitOrNode.hyps*(*2*) *rep.ShortCircuitOrNode*)
  obtain *xn yn* **where** *l*: *kind g1 n = ShortCircuitOrNode xn yn*
    using *ShortCircuitOrNode.hyps*(*1*) **by** *blast*
  then have *mx*: $g1 \vdash xn \simeq xe1$
    using *ShortCircuitOrNode.hyps*(*1*) *ShortCircuitOrNode.hyps*(*2*) **by** *fastforce*
  from *l* **have** *my*: $g1 \vdash yn \simeq ye1$
    using *ShortCircuitOrNode.hyps*(*1*) *ShortCircuitOrNode.hyps*(*3*) **by** *fastforce*
  then show *?case*
  proof −

have *g1* ⊢ *xn* ≃ *xe1* **using** *mx* **by** *simp*
have *g1* ⊢ *yn* ≃ *ye1* **using** *my* **by** *simp*
have *xer*: ∃ *xe2*. (*g2* ⊢ *xn* ≃ *xe2*) ∧ *xe1* ≥ *xe2*
using *ShortCircuitOrNode*
using *a b c d l no-encoding not-excluded-keep-type repDet singletonD*
by (*metis-node-eq-binary ShortCircuitOrNode*)
have ∃ *ye2*. (*g2* ⊢ *yn* ≃ *ye2*) ∧ *ye1* ≥ *ye2*
using *ShortCircuitOrNode a b c d l no-encoding not-excluded-keep-type*
repDet singletonD
by (*metis-node-eq-binary ShortCircuitOrNode*)
then have ∃ *xe2 ye2*. (*g2* ⊢ *n* ≃ *BinaryExpr BinShortCircuitOr xe2 ye2*) ∧
BinaryExpr BinShortCircuitOr xe1 ye1 ≥ *BinaryExpr BinShortCircuitOr xe2 ye2*
by (*metis ShortCircuitOrNode.prems l mono-binary rep.ShortCircuitOrNode*
xer)
then show *?thesis*
by *meson*
qed
next
case (*LeftShiftNode n x y xe1 ye1*)
have *k*: *g1* ⊢ *n* ≃ *BinaryExpr BinLeftShift xe1 ye1* **using** *f LeftShiftNode*
by (*simp add*: *LeftShiftNode.hyps*(*2*) *rep.LeftShiftNode*)
obtain *xn yn* **where** *l*: *kind g1 n = LeftShiftNode xn yn*
using *LeftShiftNode.hyps*(*1*) **by** *blast*
then have *mx*: *g1* ⊢ *xn* ≃ *xe1*
using *LeftShiftNode.hyps*(*1*) *LeftShiftNode.hyps*(*2*) **by** *fastforce*
from *l* **have** *my*: *g1* ⊢ *yn* ≃ *ye1*
using *LeftShiftNode.hyps*(*1*) *LeftShiftNode.hyps*(*3*) **by** *fastforce*
then show *?case*
proof −
have *g1* ⊢ *xn* ≃ *xe1* **using** *mx* **by** *simp*
have *g1* ⊢ *yn* ≃ *ye1* **using** *my* **by** *simp*
have *xer*: ∃ *xe2*. (*g2* ⊢ *xn* ≃ *xe2*) ∧ *xe1* ≥ *xe2*
using *LeftShiftNode*
using *a b c d l no-encoding not-excluded-keep-type repDet singletonD*
by (*metis-node-eq-binary LeftShiftNode*)
have ∃ *ye2*. (*g2* ⊢ *yn* ≃ *ye2*) ∧ *ye1* ≥ *ye2*
using *LeftShiftNode a b c d l no-encoding not-excluded-keep-type repDet*
singletonD
by (*metis-node-eq-binary LeftShiftNode*)
then have ∃ *xe2 ye2*. (*g2* ⊢ *n* ≃ *BinaryExpr BinLeftShift xe2 ye2*) ∧
BinaryExpr BinLeftShift xe1 ye1 ≥ *BinaryExpr BinLeftShift xe2 ye2*
by (*metis LeftShiftNode.prems l mono-binary rep.LeftShiftNode xer*)
then show *?thesis*
by *meson*
qed
next
case (*RightShiftNode n x y xe1 ye1*)
have *k*: *g1* ⊢ *n* ≃ *BinaryExpr BinRightShift xe1 ye1* **using** *f RightShiftNode*
by (*simp add*: *RightShiftNode.hyps*(*2*) *rep.RightShiftNode*)

obtain *xn yn* **where** *l*: *kind g1 n = RightShiftNode xn yn*
  using *RightShiftNode.hyps*(*1*) **by** *blast*
then have *mx*: *g1 ⊢ xn ≃ xe1*
  using *RightShiftNode.hyps*(*1*) *RightShiftNode.hyps*(*2*) **by** *fastforce*
from *l* **have** *my*: *g1 ⊢ yn ≃ ye1*
  using *RightShiftNode.hyps*(*1*) *RightShiftNode.hyps*(*3*) **by** *fastforce*
then show *?case*
proof −
  have *g1 ⊢ xn ≃ xe1* **using** *mx* **by** *simp*
  have *g1 ⊢ yn ≃ ye1* **using** *my* **by** *simp*
  have *xer*: ∃ *xe2*. (*g2 ⊢ xn ≃ xe2*) ∧ *xe1 ≥ xe2*
    using *RightShiftNode*
    using *a b c d l no-encoding not-excluded-keep-type repDet singletonD*
    by (*metis-node-eq-binary RightShiftNode*)
  have ∃ *ye2*. (*g2 ⊢ yn ≃ ye2*) ∧ *ye1 ≥ ye2*
    using *RightShiftNode a b c d l no-encoding not-excluded-keep-type repDet*
singletonD
    by (*metis-node-eq-binary RightShiftNode*)
    then have ∃ *xe2 ye2*. (*g2 ⊢ n ≃ BinaryExpr BinRightShift xe2 ye2*) ∧
BinaryExpr BinRightShift xe1 ye1 ≥ BinaryExpr BinRightShift xe2 ye2
    by (*metis RightShiftNode.prems l mono-binary rep.RightShiftNode xer*)
  then show *?thesis*
    by *meson*
qed
next
  case (*UnsignedRightShiftNode n x y xe1 ye1*)
  have *k*: *g1 ⊢ n ≃ BinaryExpr BinURightShift xe1 ye1* **using** *f UnsignedRight-ShiftNode*
    by (*simp add*: *UnsignedRightShiftNode.hyps*(*2*) *rep.UnsignedRightShiftNode*)
  obtain *xn yn* **where** *l*: *kind g1 n = UnsignedRightShiftNode xn yn*
    using *UnsignedRightShiftNode.hyps*(*1*) **by** *blast*
  then have *mx*: *g1 ⊢ xn ≃ xe1*
    using *UnsignedRightShiftNode.hyps*(*1*) *UnsignedRightShiftNode.hyps*(*2*) **by**
fastforce
  from *l* **have** *my*: *g1 ⊢ yn ≃ ye1*
    using *UnsignedRightShiftNode.hyps*(*1*) *UnsignedRightShiftNode.hyps*(*3*) **by**
fastforce
  then show *?case*
  proof −
    have *g1 ⊢ xn ≃ xe1* **using** *mx* **by** *simp*
    have *g1 ⊢ yn ≃ ye1* **using** *my* **by** *simp*
    have *xer*: ∃ *xe2*. (*g2 ⊢ xn ≃ xe2*) ∧ *xe1 ≥ xe2*
      using *UnsignedRightShiftNode*
      using *a b c d l no-encoding not-excluded-keep-type repDet singletonD*
      by (*metis-node-eq-binary UnsignedRightShiftNode*)
    have ∃ *ye2*. (*g2 ⊢ yn ≃ ye2*) ∧ *ye1 ≥ ye2*
      using *UnsignedRightShiftNode a b c d l no-encoding not-excluded-keep-type*
repDet singletonD
      by (*metis-node-eq-binary UnsignedRightShiftNode*)

then have ∃ *xe2 ye2*. (*g2* ⊢ *n* ≃ *BinaryExpr BinURightShift xe2 ye2*) ∧ *BinaryExpr BinURightShift xe1 ye1* ≥ *BinaryExpr BinURightShift xe2 ye2*

    by (*metis UnsignedRightShiftNode.prems l mono-binary rep.UnsignedRightShiftNode xer*)

    then show *?thesis*

     by *meson*

  qed

next

  case (*IntegerBelowNode n x y xe1 ye1*)

  have *k*: *g1* ⊢ *n* ≃ *BinaryExpr BinIntegerBelow xe1 ye1* **using** *f IntegerBelowNode*

    by (*simp add*: *IntegerBelowNode.hyps*(*2*) *rep.IntegerBelowNode*)

  obtain *xn yn* **where** *l*: *kind g1 n = IntegerBelowNode xn yn*

    using *IntegerBelowNode.hyps*(*1*) **by** *blast*

  then have *mx*: *g1* ⊢ *xn* ≃ *xe1*

    using *IntegerBelowNode.hyps*(*1*) *IntegerBelowNode.hyps*(*2*) **by** *fastforce*

  from *l* **have** *my*: *g1* ⊢ *yn* ≃ *ye1*

    using *IntegerBelowNode.hyps*(*1*) *IntegerBelowNode.hyps*(*3*) **by** *fastforce*

  then show *?case*

  proof −

    have *g1* ⊢ *xn* ≃ *xe1* **using** *mx* **by** *simp*

    have *g1* ⊢ *yn* ≃ *ye1* **using** *my* **by** *simp*

    have *xer*: ∃ *xe2*. (*g2* ⊢ *xn* ≃ *xe2*) ∧ *xe1* ≥ *xe2*

     using *IntegerBelowNode*

     using *a b c d l no-encoding not-excluded-keep-type repDet singletonD*

     by (*metis-node-eq-binary IntegerBelowNode*)

    have ∃ *ye2*. (*g2* ⊢ *yn* ≃ *ye2*) ∧ *ye1* ≥ *ye2*

     using *IntegerBelowNode a b c d l no-encoding not-excluded-keep-type repDet singletonD*

     by (*metis-node-eq-binary IntegerBelowNode*)

     then have ∃ *xe2 ye2*. (*g2* ⊢ *n* ≃ *BinaryExpr BinIntegerBelow xe2 ye2*) ∧ *BinaryExpr BinIntegerBelow xe1 ye1* ≥ *BinaryExpr BinIntegerBelow xe2 ye2*

      by (*metis IntegerBelowNode.prems l mono-binary rep.IntegerBelowNode xer*)

    then show *?thesis*

     by *meson*

  qed

next

  case (*IntegerEqualsNode n x y xe1 ye1*)

  have *k*: *g1* ⊢ *n* ≃ *BinaryExpr BinIntegerEquals xe1 ye1* **using** *f IntegerEqualsNode*

    by (*simp add*: *IntegerEqualsNode.hyps*(*2*) *rep.IntegerEqualsNode*)

  obtain *xn yn* **where** *l*: *kind g1 n = IntegerEqualsNode xn yn*

    using *IntegerEqualsNode.hyps*(*1*) **by** *blast*

  then have *mx*: *g1* ⊢ *xn* ≃ *xe1*

    using *IntegerEqualsNode.hyps*(*1*) *IntegerEqualsNode.hyps*(*2*) **by** *fastforce*

  from *l* **have** *my*: *g1* ⊢ *yn* ≃ *ye1*

    using *IntegerEqualsNode.hyps*(*1*) *IntegerEqualsNode.hyps*(*3*) **by** *fastforce*

  then show *?case*

proof −
  have *g1 ⊢ xn ≃ xe1* **using** *mx* **by** *simp*
  have *g1 ⊢ yn ≃ ye1* **using** *my* **by** *simp*
  have *xer*: ∃ *xe2.* (*g2 ⊢ xn ≃ xe2*) ∧ *xe1 ≥ xe2*
    using *IntegerEqualsNode*
    using *a b c d l no-encoding not-excluded-keep-type repDet singletonD*
    by (*metis-node-eq-binary IntegerEqualsNode*)
  have ∃ *ye2.* (*g2 ⊢ yn ≃ ye2*) ∧ *ye1 ≥ ye2*
      using *IntegerEqualsNode a b c d l no-encoding not-excluded-keep-type*
repDet singletonD
      by (*metis-node-eq-binary IntegerEqualsNode*)
    then have ∃ *xe2 ye2.* (*g2 ⊢ n ≃ BinaryExpr BinIntegerEquals xe2 ye2*) ∧
BinaryExpr BinIntegerEquals xe1 ye1 ≥ BinaryExpr BinIntegerEquals xe2 ye2
      by (*metis IntegerEqualsNode.prems l mono-binary rep.IntegerEqualsNode*
xer)
    then show *?thesis*
      by *meson*
  qed
next
  case (*IntegerLessThanNode n x y xe1 ye1*)
    have *k*: *g1 ⊢ n ≃ BinaryExpr BinIntegerLessThan xe1 ye1* **using** *f IntegerLessThanNode*
    by (*simp add: IntegerLessThanNode.hyps*(*2*) *rep.IntegerLessThanNode*)
  obtain *xn yn* **where** *l*: *kind g1 n = IntegerLessThanNode xn yn*
    using *IntegerLessThanNode.hyps*(*1*) **by** *blast*
  then have *mx*: *g1 ⊢ xn ≃ xe1*
    using *IntegerLessThanNode.hyps*(*1*) *IntegerLessThanNode.hyps*(*2*) **by** *fast-force*
  from *l* **have** *my*: *g1 ⊢ yn ≃ ye1*
    using *IntegerLessThanNode.hyps*(*1*) *IntegerLessThanNode.hyps*(*3*) **by** *fast-force*
  then show *?case*
  proof −
    have *g1 ⊢ xn ≃ xe1* **using** *mx* **by** *simp*
    have *g1 ⊢ yn ≃ ye1* **using** *my* **by** *simp*
    have *xer*: ∃ *xe2.* (*g2 ⊢ xn ≃ xe2*) ∧ *xe1 ≥ xe2*
      using *IntegerLessThanNode*
      using *a b c d l no-encoding not-excluded-keep-type repDet singletonD*
      by (*metis-node-eq-binary IntegerLessThanNode*)
    have ∃ *ye2.* (*g2 ⊢ yn ≃ ye2*) ∧ *ye1 ≥ ye2*
        using *IntegerLessThanNode a b c d l no-encoding not-excluded-keep-type*
repDet singletonD
        by (*metis-node-eq-binary IntegerLessThanNode*)
      then have ∃ *xe2 ye2.* (*g2 ⊢ n ≃ BinaryExpr BinIntegerLessThan xe2 ye2*)
∧ *BinaryExpr BinIntegerLessThan xe1 ye1 ≥ BinaryExpr BinIntegerLessThan xe2*
ye2
      by (*metis IntegerLessThanNode.prems l mono-binary rep.IntegerLessThanNode*
xer)
      then show *?thesis*

    by *meson*
  qed
next
  case (*NarrowNode n inputBits resultBits x xe1*)
  have *k*: *g1 ⊢ n ≃ UnaryExpr* (*UnaryNarrow inputBits resultBits*) *xe1* **using**
f NarrowNode
    by (*simp add*: *NarrowNode.hyps*(*2*) *rep.NarrowNode*)
  obtain *xn* **where** *l*: *kind g1 n = NarrowNode inputBits resultBits xn*
   using *NarrowNode.hyps*(*1*) **by** *blast*
  then have *m*: *g1 ⊢ xn ≃ xe1*
   using *NarrowNode.hyps*(*1*) *NarrowNode.hyps*(*2*)
   by *auto*
  then show *?case*
  proof (*cases xn = n′*)
   case *True*
   then have *n*: *xe1 = e1′* **using** *c m repDet* **by** *simp*
   then have *ev*: *g2 ⊢ n ≃ UnaryExpr* (*UnaryNarrow inputBits resultBits*) *e2′*
using NarrowNode.hyps(*1*) *l m n*
    using *NarrowNode.prems True d rep.NarrowNode* **by** *simp*
   then have *r*: *UnaryExpr* (*UnaryNarrow inputBits resultBits*) *e1′ ≥ UnaryExpr*
(*UnaryNarrow inputBits resultBits*) *e2′*
    by (*meson a mono-unary*)
   then show *?thesis* **using** *ev r*
   by (*metis n*)
  next
   case *False*
   have *g1 ⊢ xn ≃ xe1* **using** *m* **by** *simp*
   have *∃ xe2.* (*g2 ⊢ xn ≃ xe2*) *∧ xe1 ≥ xe2*
    using *NarrowNode*
   using *False b encodes-contains l not-excluded-keep-type not-in-g singleton-iff*
    by (*metis-node-eq-ternary NarrowNode*)
    then have *∃ xe2.* (*g2 ⊢ n ≃ UnaryExpr* (*UnaryNarrow inputBits re-
sultBits*) *xe2*) *∧ UnaryExpr* (*UnaryNarrow inputBits resultBits*) *xe1 ≥ UnaryExpr*
(*UnaryNarrow inputBits resultBits*) *xe2*
    by (*metis NarrowNode.prems l mono-unary rep.NarrowNode*)
   then show *?thesis*
   by *meson*
  qed
next
  case (*SignExtendNode n inputBits resultBits x xe1*)
  have *k*: *g1 ⊢ n ≃ UnaryExpr* (*UnarySignExtend inputBits resultBits*) *xe1*
using f SignExtendNode
    by (*simp add*: *SignExtendNode.hyps*(*2*) *rep.SignExtendNode*)
  obtain *xn* **where** *l*: *kind g1 n = SignExtendNode inputBits resultBits xn*
   using *SignExtendNode.hyps*(*1*) **by** *blast*
  then have *m*: *g1 ⊢ xn ≃ xe1*
   using *SignExtendNode.hyps*(*1*) *SignExtendNode.hyps*(*2*)
   by *auto*
  then show *?case*

proof (*cases xn = n′*)
  case *True*
  then have *n*: *xe1 = e1′* **using** *c m repDet* **by** *simp*
  then have *ev*: *g2 ⊢ n ≃ UnaryExpr* (*UnarySignExtend inputBits resultBits*) *e2′* **using** *SignExtendNode.hyps*(*1*) *l m n*
    using *SignExtendNode.prems True d rep.SignExtendNode* **by** *simp*
    then have *r*: *UnaryExpr* (*UnarySignExtend inputBits resultBits*) *e1′ ≥ UnaryExpr* (*UnarySignExtend inputBits resultBits*) *e2′*
    by (*meson a mono-unary*)
    then show *?thesis* **using** *ev r*
    by (*metis n*)
  next
  case *False*
  have *g1 ⊢ xn ≃ xe1* **using** *m* **by** *simp*
  have *∃ xe2.* (*g2 ⊢ xn ≃ xe2*) *∧ xe1 ≥ xe2*
    using *SignExtendNode*
    using *False b encodes-contains l not-excluded-keep-type not-in-g singleton-iff*
    by (*metis-node-eq-ternary SignExtendNode*)
  then have *∃ xe2.* (*g2 ⊢ n ≃ UnaryExpr* (*UnarySignExtend inputBits result-Bits*) *xe2*) *∧ UnaryExpr* (*UnarySignExtend inputBits resultBits*) *xe1 ≥ UnaryExpr* (*UnarySignExtend inputBits resultBits*) *xe2*
    by (*metis SignExtendNode.prems l mono-unary rep.SignExtendNode*)
    then show *?thesis*
    by *meson*
  qed
next
  case (*ZeroExtendNode n inputBits resultBits x xe1*)
  have *k*: *g1 ⊢ n ≃ UnaryExpr* (*UnaryZeroExtend inputBits resultBits*) *xe1* **using** *f ZeroExtendNode*
    by (*simp add*: *ZeroExtendNode.hyps*(*2*) *rep.ZeroExtendNode*)
  obtain *xn* **where** *l*: *kind g1 n = ZeroExtendNode inputBits resultBits xn*
    using *ZeroExtendNode.hyps*(*1*) **by** *blast*
  then have *m*: *g1 ⊢ xn ≃ xe1*
    using *ZeroExtendNode.hyps*(*1*) *ZeroExtendNode.hyps*(*2*)
    by *auto*
  then show *?case*
  proof (*cases xn = n′*)
    case *True*
    then have *n*: *xe1 = e1′* **using** *c m repDet* **by** *simp*
    then have *ev*: *g2 ⊢ n ≃ UnaryExpr* (*UnaryZeroExtend inputBits resultBits*) *e2′* **using** *ZeroExtendNode.hyps*(*1*) *l m n*
      using *ZeroExtendNode.prems True d rep.ZeroExtendNode* **by** *simp*
      then have *r*: *UnaryExpr* (*UnaryZeroExtend inputBits resultBits*) *e1′ ≥ UnaryExpr* (*UnaryZeroExtend inputBits resultBits*) *e2′*
      by (*meson a mono-unary*)
      then show *?thesis* **using** *ev r*
      by (*metis n*)
    next
    case *False*

have *g1* ⊢ *xn* ≃ *xe1* **using** *m* **by** *simp*

have ∃ *xe2*. (*g2* ⊢ *xn* ≃ *xe2*) ∧ *xe1* ≥ *xe2*

using *ZeroExtendNode*

using *False b encodes-contains l not-excluded-keep-type not-in-g singleton-iff*

by (*metis-node-eq-ternary ZeroExtendNode*)

then have ∃ *xe2*. (*g2* ⊢ *n* ≃ *UnaryExpr* (*UnaryZeroExtend inputBits result-Bits*) *xe2*) ∧ *UnaryExpr* (*UnaryZeroExtend inputBits resultBits*) *xe1* ≥ *UnaryExpr* (*UnaryZeroExtend inputBits resultBits*) *xe2*

by (*metis ZeroExtendNode.prems l mono-unary rep.ZeroExtendNode*)

then show *?thesis*

by *meson*

qed

next

case (*LeafNode n s*)

then show *?case*

by (*metis eq-refl rep.LeafNode*)

next

case (*RefNode n′*)

then show *?case*

by (*metis a b c d no-encoding not-excluded-keep-type rep.RefNode repDet singletonD*)

qed

qed

qed

lemma *graph-semantics-preservation-subscript*:

assumes *a*: $e_1' \geq e_2'$

assumes *b*: ({*n*} ◁ *as-set* g_1) ⊆ *as-set* g_2

assumes *c*: g_1 ⊢ *n* ≃ e_1'

assumes *d*: g_2 ⊢ *n* ≃ e_2'

shows *graph-refinement* g_1 g_2

using *graph-semantics-preservation assms* **by** *simp*

lemma *tree-to-graph-rewriting*:

$e_1 \geq e_2$

∧ (g_1 ⊢ *n* ≃ e_1) ∧ *maximal-sharing* g_1

∧ ({*n*} ◁ *as-set* g_1) ⊆ *as-set* g_2

∧ (g_2 ⊢ *n* ≃ e_2) ∧ *maximal-sharing* g_2

⟹ *graph-refinement* g_1 g_2

using *graph-semantics-preservation*

by *auto*

declare [[*simp-trace*]]

lemma *equal-refines*:

fixes *e1 e2* :: *IRExpr*

assumes *e1* = *e2*

shows *e1* ≥ *e2*

using *assms*

by *simp*
declare [[*simp-trace=false*]]

lemma *eval-contains-id*[*simp*]: *g1* ⊢ *n* ≃ *e* ⟹ *n* ∈ *ids g1*
  using *no-encoding* **by** *blast*

lemma *subset-kind*[*simp*]: *as-set g1* ⊆ *as-set g2* ⟹ *g1* ⊢ *n* ≃ *e* ⟹ *kind g1 n* =
kind g2 n
  using *eval-contains-id* **unfolding** *as-set-def*
  by *blast*

lemma *subset-stamp*[*simp*]: *as-set g1* ⊆ *as-set g2* ⟹ *g1* ⊢ *n* ≃ *e* ⟹ *stamp g1 n*
= *stamp g2 n*
  using *eval-contains-id* **unfolding** *as-set-def*
  by *blast*

method *solve-subset-eval* **uses** *as-set eval* =
  (*metis eval as-set subset-kind subset-stamp* |
   metis eval as-set subset-kind)

lemma *subset-implies-evals*:
  assumes *as-set g1* ⊆ *as-set g2*
  assumes (*g1* ⊢ *n* ≃ *e*)
  shows (*g2* ⊢ *n* ≃ *e*)
  using *assms*(*2*)
  apply (*induction e*)
                    apply (*solve-subset-eval as-set*: *assms*(*1*) *eval*: *ConstantNode*)
                   apply (*solve-subset-eval as-set*: *assms*(*1*) *eval*: *ParameterNode*)
                  apply (*solve-subset-eval as-set*: *assms*(*1*) *eval*: *ConditionalNode*)
                  apply (*solve-subset-eval as-set*: *assms*(*1*) *eval*: *AbsNode*)
                 apply (*solve-subset-eval as-set*: *assms*(*1*) *eval*: *NotNode*)
                apply (*solve-subset-eval as-set*: *assms*(*1*) *eval*: *NegateNode*)
               apply (*solve-subset-eval as-set*: *assms*(*1*) *eval*: *LogicNegationNode*)
               apply (*solve-subset-eval as-set*: *assms*(*1*) *eval*: *AddNode*)
              apply (*solve-subset-eval as-set*: *assms*(*1*) *eval*: *MulNode*)
             apply (*solve-subset-eval as-set*: *assms*(*1*) *eval*: *SubNode*)
            apply (*solve-subset-eval as-set*: *assms*(*1*) *eval*: *AndNode*)
           apply (*solve-subset-eval as-set*: *assms*(*1*) *eval*: *OrNode*)
           apply (*solve-subset-eval as-set*: *assms*(*1*) *eval*: *XorNode*)
          apply (*solve-subset-eval as-set*: *assms*(*1*) *eval*: *ShortCircuitOrNode*)
         apply (*solve-subset-eval as-set*: *assms*(*1*) *eval*: *LeftShiftNode*)
        apply (*solve-subset-eval as-set*: *assms*(*1*) *eval*: *RightShiftNode*)
       apply (*solve-subset-eval as-set*: *assms*(*1*) *eval*: *UnsignedRightShiftNode*)
      apply (*solve-subset-eval as-set*: *assms*(*1*) *eval*: *IntegerBelowNode*)
     apply (*solve-subset-eval as-set*: *assms*(*1*) *eval*: *IntegerEqualsNode*)
    apply (*solve-subset-eval as-set*: *assms*(*1*) *eval*: *IntegerLessThanNode*)

apply (*solve-subset-eval as-set*: *assms*(*1*) *eval*: *NarrowNode*)
  apply (*solve-subset-eval as-set*: *assms*(*1*) *eval*: *SignExtendNode*)
  apply (*solve-subset-eval as-set*: *assms*(*1*) *eval*: *ZeroExtendNode*)
  apply (*solve-subset-eval as-set*: *assms*(*1*) *eval*: *LeafNode*)
by (*solve-subset-eval as-set*: *assms*(*1*) *eval*: *RefNode*)

lemma *subset-refines*:
  assumes *as-set g1* $\subseteq$ *as-set g2*
  shows *graph-refinement g1 g2*
proof −
  have *ids g1* $\subseteq$ *ids g2* **using** *assms* **unfolding** *as-set-def*
    by *blast*
  then show *?thesis* **unfolding** *graph-refinement-def* **apply** *rule*
    apply (*rule allI*) **apply** (*rule impI*) **apply** (*rule allI*) **apply** (*rule impI*)
    unfolding *graph-represents-expression-def*
    proof −
      fix *n e1*
      assume *1*:*n* $\in$ *ids g1*
      assume *2*:*g1* $\vdash$ *n* $\simeq$ *e1*

      show $\exists\, e2.\ (g2 \vdash n \simeq e2) \wedge e1 \geq e2$
        using *assms 1 2* **using** *subset-implies-evals*
        by (*meson equal-refines*)
    qed
  qed

lemma *graph-construction*:
  $e_1 \geq e_2$
  $\wedge$ *as-set* $g_1 \subseteq$ *as-set* g_2
  $\wedge$ $(g_2 \vdash n \simeq e_2)$
  $\Longrightarrow (g_2 \vdash n \trianglelefteq e_1) \wedge$ *graph-refinement* $g_1\ g_2$
  using *subset-refines*
  by (*meson encodeeval-def graph-represents-expression-def le-expr-def*)

7.8.4 Term Graph Reconstruction

lemma *find-exists-kind*:
  assumes *find-node-and-stamp g* (*node, s*) = *Some nid*
  shows *kind g nid* = *node*
  using *assms* **unfolding** *find-node-and-stamp.simps*
  by (*metis* (*mono-tags, lifting*) *find-Some-iff*)

lemma *find-exists-stamp*:
  assumes *find-node-and-stamp g* (*node, s*) = *Some nid*
  shows *stamp g nid* = *s*
  using *assms* **unfolding** *find-node-and-stamp.simps*
  by (*metis* (*mono-tags, lifting*) *find-Some-iff*)

lemma *find-new-kind*:

assumes $g' = \textit{add-node nid (node, s) g}$
assumes $\textit{node} \neq \textit{NoNode}$
shows $\textit{kind } g' \textit{ nid} = \textit{node}$
using *assms*
using *add-node-lookup* **by** *presburger*

lemma *find-new-stamp*:
assumes $g' = \textit{add-node nid (node, s) g}$
assumes $\textit{node} \neq \textit{NoNode}$
shows $\textit{stamp } g' \textit{ nid} = s$
using *assms*
using *add-node-lookup* **by** *presburger*

lemma *sorted-bottom*:
assumes *finite xs*
assumes $x \in xs$
shows $x \leq \textit{last}(\textit{sorted-list-of-set}(xs\text{::}\textit{nat set}))$
using *assms*
using *sorted2-simps(2) sorted-list-of-set(2)*
by (*smt* (*verit, del-insts*) *Diff-iff Max-ge Max-in empty-iff list.set(1) snoc-eq-iff-butlast*
sorted-insort-is-snoc sorted-list-of-set(1) sorted-list-of-set.fold-insort-key.infinite sorted-list-of-set.fold-insort-ke

lemma *fresh*: *finite xs* $\Longrightarrow \textit{last}(\textit{sorted-list-of-set}(xs\text{::}\textit{nat set})) + 1 \notin xs$
using *sorted-bottom*
using *not-le* **by** *auto*

lemma *fresh-ids*:
assumes $n = \textit{get-fresh-id } g$
shows $n \notin \textit{ids } g$
proof −
have *finite* ($\textit{ids } g$) **using** *Rep-IRGraph* **by** *auto*
then show *?thesis*
using *assms fresh* **unfolding** *get-fresh-id.simps*
by *blast*
qed

lemma *graph-unchanged-rep-unchanged*:
assumes $\forall\, n \in \textit{ids } g.\ \textit{kind } g\ n = \textit{kind } g'\ n$
assumes $\forall\, n \in \textit{ids } g.\ \textit{stamp } g\ n = \textit{stamp } g'\ n$
shows $(g \vdash n \simeq e) \longrightarrow (g' \vdash n \simeq e)$
apply (*rule impI*) **subgoal premises** e **using** e *assms*
apply (*induction n e*)
apply (*metis no-encoding rep.ConstantNode*)
apply (*metis no-encoding rep.ParameterNode*)
apply (*metis no-encoding rep.ConditionalNode*)
apply (*metis no-encoding rep.AbsNode*)
apply (*metis no-encoding rep.NotNode*)
apply (*metis no-encoding rep.NegateNode*)
apply (*metis no-encoding rep.LogicNegationNode*)

           apply (*metis no-encoding rep.AddNode*)
           apply (*metis no-encoding rep.MulNode*)
           apply (*metis no-encoding rep.SubNode*)
          apply (*metis no-encoding rep.AndNode*)
         apply (*metis no-encoding rep.OrNode*)
         apply (*metis no-encoding rep.XorNode*)
        apply (*metis no-encoding rep.ShortCircuitOrNode*)
       apply (*metis no-encoding rep.LeftShiftNode*)
       apply (*metis no-encoding rep.RightShiftNode*)
      apply (*metis no-encoding rep.UnsignedRightShiftNode*)
      apply (*metis no-encoding rep.IntegerBelowNode*)
     apply (*metis no-encoding rep.IntegerEqualsNode*)
     apply (*metis no-encoding rep.IntegerLessThanNode*)
    apply (*metis no-encoding rep.NarrowNode*)
   apply (*metis no-encoding rep.SignExtendNode*)
   apply (*metis no-encoding rep.ZeroExtendNode*)
   apply (*metis no-encoding rep.LeafNode*)
  by (*metis no-encoding rep.RefNode*)
 done

lemma *fresh-node-subset*:
  assumes $n \notin ids\ g$
  assumes $g' = add\text{-}node\ n\ (k,\ s)\ g$
  shows *as-set* $g \subseteq$ *as-set* g'
  using *assms*
 by (*smt* (*verit, del-insts*) *Collect-mono-iff Diff-idemp Diff-insert-absorb add-changed*
as-set-def disjoint-change unchanged.simps)

lemma *unrep-subset*:
  assumes $(g \oplus e \rightsquigarrow (g',\ n))$
  shows *as-set* $g \subseteq$ *as-set* g'
  using *assms* **proof** (*induction g e* $(g',\ n)$ *arbitrary:* $g'\ n$)
  case (*ConstantNodeSame g c n*)
  then show *?case* **by** *blast*
next
  case (*ConstantNodeNew g c n g'*)
  then show *?case* **using** *fresh-ids fresh-node-subset*
   by *presburger*
next
  case (*ParameterNodeSame g i s n*)
  then show *?case* **by** *blast*
next
  case (*ParameterNodeNew g i s n g'*)
  then show *?case* **using** *fresh-ids fresh-node-subset*
   by *presburger*
next
  case (*ConditionalNodeSame g ce g2 c te g3 t fe g4 f s' n*)
  then show *?case* **by** *blast*
next

case (*ConditionalNodeNew g ce g2 c te g3 t fe g4 f s' n g'*)
  then show *?case* **using** *fresh-ids fresh-node-subset*
    by (*meson subset-trans*)
next
  case (*UnaryNodeSame g xe g2 x s' op n*)
  then show *?case* **by** *blast*
next
  case (*UnaryNodeNew g xe g2 x s' op n g'*)
  then show *?case* **using** *fresh-ids fresh-node-subset*
    by (*meson subset-trans*)
next
  case (*BinaryNodeSame g xe g2 x ye g3 y s' op n*)
  then show *?case* **by** *blast*
next
  case (*BinaryNodeNew g xe g2 x ye g3 y s' op n g'*)
  then show *?case* **using** *fresh-ids fresh-node-subset*
    by (*meson subset-trans*)
next
  case (*AllLeafNodes g n s*)
  then show *?case* **by** *blast*
qed

lemma *fresh-node-preserves-other-nodes*:
  assumes $n' = get\text{-}fresh\text{-}id\ g$
  assumes $g' = add\text{-}node\ n'\ (k,\ s)\ g$
  shows $\forall\ n \in ids\ g\ .\ (g \vdash n \simeq e) \longrightarrow (g' \vdash n \simeq e)$
  using *assms*
 by (*smt* (*verit, ccfv-SIG*) *Diff-idemp Diff-insert-absorb add-changed disjoint-change*
fresh-ids graph-unchanged-rep-unchanged unchanged.elims(*2*))

lemma *found-node-preserves-other-nodes*:
  assumes *find-node-and-stamp g* (*k, s*) $=$ *Some n*
  shows $\forall\ n \in ids\ g.\ (g \vdash n \simeq e) \longleftrightarrow (g \vdash n \simeq e)$
  using *assms*
  by *blast*

lemma *unrep-ids-subset*[*simp*]:
  assumes $g \oplus e \rightsquigarrow (g',\ n)$
  shows $ids\ g \subseteq ids\ g'$
  using *assms unrep-subset*
  by (*meson graph-refinement-def subset-refines*)

lemma *unrep-unchanged*:
  assumes $g \oplus e \rightsquigarrow (g',\ n)$
  shows $\forall\ n \in ids\ g\ .\ \forall\ e.\ (g \vdash n \simeq e) \longrightarrow (g' \vdash n \simeq e)$
  using *assms unrep-subset fresh-node-preserves-other-nodes*
  by (*meson subset-implies-evals*)

theorem *term-graph-reconstruction*:

$g \oplus e \leadsto (g', n) \implies (g' \vdash n \simeq e) \land \textit{as-set } g \subseteq \textit{as-set } g'$

subgoal premises *e* **apply** (*rule conjI*) **defer**

  using *e unrep-subset* **apply** *blast* **using** *e*

proof (*induction g e (g', n) arbitrary: g' n*)

  case (*ConstantNodeSame g' c n*)

  then have *kind g' n = ConstantNode c*

    using *find-exists-kind local.ConstantNodeSame* **by** *blast*

  then show *?case* **using** *ConstantNode* **by** *blast*

next

  case (*ConstantNodeNew g c*)

  then show *?case*

    using *ConstantNode IRNode.distinct*(*683*) *add-node-lookup* **by** *presburger*

next

  case (*ParameterNodeSame i s*)

  then show *?case*

    by (*metis ParameterNode find-exists-kind find-exists-stamp*)

next

  case (*ParameterNodeNew g i s*)

  then show *?case*

    by (*metis IRNode.distinct*(*2447*) *ParameterNode add-node-lookup*)

next

  case (*ConditionalNodeSame g ce g2 c te g3 t fe g4 f s' n*)

  then have *k: kind g4 n = ConditionalNode c t f*

    using *find-exists-kind* **by** *blast*

  have *c: g4 ⊢ c ≃ ce* **using** *local.ConditionalNodeSame unrep-unchanged*

    using *no-encoding* **by** *blast*

  have *t: g4 ⊢ t ≃ te* **using** *local.ConditionalNodeSame unrep-unchanged*

    using *no-encoding* **by** *blast*

  have *f: g4 ⊢ f ≃ fe* **using** *local.ConditionalNodeSame unrep-unchanged*

    using *no-encoding* **by** *blast*

  then show *?case* **using** *c t f*

    using *ConditionalNode k* **by** *blast*

next

  case (*ConditionalNodeNew g ce g2 c te g3 t fe g4 f s' n g'*)

  moreover have *ConditionalNode c t f ≠ NoNode*

    using *unary-node.elims* **by** *blast*

  ultimately have *k: kind g' n = ConditionalNode c t f*

    using *find-new-kind local.ConditionalNodeNew*

    by *presburger*

  then have *c: g' ⊢ c ≃ ce* **using** *local.ConditionalNodeNew unrep-unchanged*

    using *no-encoding*

    by (*metis ConditionalNodeNew.hyps*(*9*) *fresh-node-preserves-other-nodes*)

  then have *t: g' ⊢ t ≃ te* **using** *local.ConditionalNodeNew unrep-unchanged*

    using *no-encoding fresh-node-preserves-other-nodes*

    by *metis*

  then have *f: g' ⊢ f ≃ fe* **using** *local.ConditionalNodeNew unrep-unchanged*

    using *no-encoding fresh-node-preserves-other-nodes*

    by *metis*

  then show *?case* **using** *c t f*

using *ConditionalNode k* **by** *blast*

next

  case (*UnaryNodeSame g xe g$'$ x s$'$ op n*)

  then have *k*: *kind g$'$ n = unary-node op x*

    using *find-exists-kind local.UnaryNodeSame* **by** *blast*

  then have *g$'$ ⊢ x ≃ xe* **using** *local.UnaryNodeSame* **by** *blast*

  then show *?case* **using** *k*

    apply (*cases op*)

    using *AbsNode unary-node.simps*(*1*) **apply** *presburger*

    using *NegateNode unary-node.simps*(*3*) **apply** *presburger*

    using *NotNode unary-node.simps*(*2*) **apply** *presburger*

    using *LogicNegationNode unary-node.simps*(*4*) **apply** *presburger*

    using *NarrowNode unary-node.simps*(*5*) **apply** *presburger*

    using *SignExtendNode unary-node.simps*(*6*) **apply** *presburger*

    using *ZeroExtendNode unary-node.simps*(*7*) **by** *presburger*

next

  case (*UnaryNodeNew g xe g2 x s$'$ op n g$'$*)

  moreover have *unary-node op x ≠ NoNode*

    using *unary-node.elims* **by** *blast*

  ultimately have *k*: *kind g$'$ n = unary-node op x*

    using *find-new-kind local.UnaryNodeNew*

    by *presburger*

  have *x ∈ ids g2* **using** *local.UnaryNodeNew*

    using *eval-contains-id* **by** *blast*

  then have *x ≠ n* **using** *local.UnaryNodeNew*(*5*) *fresh-ids* **by** *blast*

  have *g$'$ ⊢ x ≃ xe* **using** *local.UnaryNodeNew fresh-node-preserves-other-nodes*

    using ‹*x ∈ ids g2*› **by** *blast*

  then show *?case* **using** *k*

    apply (*cases op*)

    using *AbsNode unary-node.simps*(*1*) **apply** *presburger*

    using *NegateNode unary-node.simps*(*3*) **apply** *presburger*

    using *NotNode unary-node.simps*(*2*) **apply** *presburger*

    using *LogicNegationNode unary-node.simps*(*4*) **apply** *presburger*

    using *NarrowNode unary-node.simps*(*5*) **apply** *presburger*

    using *SignExtendNode unary-node.simps*(*6*) **apply** *presburger*

    using *ZeroExtendNode unary-node.simps*(*7*) **by** *presburger*

next

  case (*BinaryNodeSame g xe g2 x ye g3 y s$'$ op n*)

  then have *k*: *kind g3 n = bin-node op x y*

    using *find-exists-kind* **by** *blast*

  have *x*: *g3 ⊢ x ≃ xe* **using** *local.BinaryNodeSame unrep-unchanged*

    using *no-encoding* **by** *blast*

  have *y*: *g3 ⊢ y ≃ ye* **using** *local.BinaryNodeSame unrep-unchanged*

    using *no-encoding* **by** *blast*

  then show *?case* **using** *x y k* **apply** (*cases op*)

    using *AddNode bin-node.simps*(*1*) **apply** *presburger*

    using *MulNode bin-node.simps*(*2*) **apply** *presburger*

    using *SubNode bin-node.simps*(*3*) **apply** *presburger*

    using *AndNode bin-node.simps*(*4*) **apply** *presburger*

        using *OrNode bin-node.simps*(*5*) **apply** *presburger*
        using *XorNode bin-node.simps*(*6*) **apply** *presburger*
        using *ShortCircuitOrNode bin-node.simps*(*7*) **apply** *presburger*
        using *LeftShiftNode bin-node.simps*(*8*) **apply** *presburger*
        using *RightShiftNode bin-node.simps*(*9*) **apply** *presburger*
        using *UnsignedRightShiftNode bin-node.simps*(*10*) **apply** *presburger*
        using *IntegerEqualsNode bin-node.simps*(*11*) **apply** *presburger*
        using *IntegerLessThanNode bin-node.simps*(*12*) **apply** *presburger*
        using *IntegerBelowNode bin-node.simps*(*13*) **by** *presburger*
  next
    case (*BinaryNodeNew g xe g2 x ye g3 y s' op n g'*)
    moreover have *bin-node op x y $\neq$ NoNode*
      using *bin-node.elims* **by** *blast*
    ultimately have *k*: *kind g' n = bin-node op x y*
      using *find-new-kind local.BinaryNodeNew*
      by *presburger*
    then have *k*: *kind g' n = bin-node op x y*
      using *find-exists-kind* **by** *blast*
    have *x*: *g' $\vdash$ x $\simeq$ xe* **using** *local.BinaryNodeNew unrep-unchanged*
      using *no-encoding*
      by (*meson fresh-node-preserves-other-nodes*)
    have *y*: *g' $\vdash$ y $\simeq$ ye* **using** *local.BinaryNodeNew unrep-unchanged*
      using *no-encoding*
      by (*meson fresh-node-preserves-other-nodes*)
    then show *?case* **using** *x y k* **apply** (*cases op*)
      using *AddNode bin-node.simps*(*1*) **apply** *presburger*
      using *MulNode bin-node.simps*(*2*) **apply** *presburger*
      using *SubNode bin-node.simps*(*3*) **apply** *presburger*
      using *AndNode bin-node.simps*(*4*) **apply** *presburger*
      using *OrNode bin-node.simps*(*5*) **apply** *presburger*
      using *XorNode bin-node.simps*(*6*) **apply** *presburger*
      using *ShortCircuitOrNode bin-node.simps*(*7*) **apply** *presburger*
      using *LeftShiftNode bin-node.simps*(*8*) **apply** *presburger*
      using *RightShiftNode bin-node.simps*(*9*) **apply** *presburger*
      using *UnsignedRightShiftNode bin-node.simps*(*10*) **apply** *presburger*
      using *IntegerEqualsNode bin-node.simps*(*11*) **apply** *presburger*
      using *IntegerLessThanNode bin-node.simps*(*12*) **apply** *presburger*
      using *IntegerBelowNode bin-node.simps*(*13*) **by** *presburger*
  next
    case (*AllLeafNodes g n s*)
    then show *?case* **using** *rep.LeafNode* **by** *blast*
  qed
  done

lemma *ref-refinement*:
  assumes *g $\vdash$ n $\simeq$ e_1*
  assumes *kind g n' = RefNode n*
  shows *g $\vdash$ n' $\unlhd$ e_1*
  using *assms RefNode*

by (*meson equal-refines graph-represents-expression-def*)

lemma *unrep-refines*:
  assumes $g \oplus e \rightsquigarrow (g', n)$
  shows *graph-refinement g g'*
  using *assms*
  using *graph-refinement-def subset-refines unrep-subset* **by** *blast*

lemma *add-new-node-refines*:
  assumes $n \notin ids\ g$
  assumes $g' = add\text{-}node\ n\ (k,\ s)\ g$
  shows *graph-refinement g g'*
  using *assms* **unfolding** *graph-refinement*
  using *fresh-node-subset subset-refines* **by** *presburger*

lemma *add-node-as-set*:
  assumes $g' = add\text{-}node\ n\ (k,\ s)\ g$
  shows $(\{n\} \unlhd as\text{-}set\ g) \subseteq as\text{-}set\ g'$
  using *assms* **unfolding** *as-set-def domain-subtraction-def*
  using *add-changed*
  by (*smt* (*z3*) *case-prodE changeonly.simps mem-Collect-eq prod.sel*(*1*) *subsetI*)

theorem *refined-insert*:
  assumes $e_1 \geq e_2$
  assumes $g_1 \oplus e_2 \rightsquigarrow (g_2,\ n')$
  shows $(g_2 \vdash n' \unlhd e_1) \wedge graph\text{-}refinement\ g_1\ g_2$
  using *assms*
  using *graph-construction term-graph-reconstruction* **by** *blast*

lemma *ids-finite*: *finite* (*ids g*)
  using *Rep-IRGraph ids.rep-eq* **by** *simp*

lemma *unwrap-sorted*: *set* (*sorted-list-of-set* (*ids g*)) = *ids g*
  using *Rep-IRGraph set-sorted-list-of-set ids-finite*
  by *blast*

lemma *find-none*:
  assumes *find-node-and-stamp g* (*k, s*) = *None*
  shows $\forall\ n \in ids\ g.\ kind\ g\ n \neq k \vee stamp\ g\ n \neq s$
proof $-$
  have ($\nexists n.\ n \in ids\ g \wedge$ (*kind g n* = *k* $\wedge$ *stamp g n* = *s*))
      using *assms* **unfolding** *find-node-and-stamp.simps* **using** *find-None-iff un-*
wrap-sorted
    by (*metis* (*mono-tags, lifting*))
  then show *?thesis*
    by *blast*
qed

method *ref-represents* **uses** *node =*
(*metis IRNode.distinct*(*2755*) *RefNode dual-order.refl find-new-kind fresh-node-subset*
node subset-implies-evals)

7.8.5 Data-flow Tree to Subgraph Preserves Maximal Sharing

lemma *same-kind-stamp-encodes-equal*:
  assumes *kind g n = kind g n′*
  assumes *stamp g n = stamp g n′*
  assumes ¬(*is-preevaluated* (*kind g n*))
  shows ∀ *e.* $(g \vdash n \simeq e) \longrightarrow (g \vdash n′ \simeq e)$
  apply (*rule allI*)
  subgoal for *e*
    apply (*rule impI*)
    subgoal premises *eval* **using** *eval assms*
      apply (*induction e*)
    using *ConstantNode* **apply** *presburger*
    using *ParameterNode* **apply** *presburger*
                apply (*metis ConditionalNode*)
              apply (*metis AbsNode*)
             apply (*metis NotNode*)
            apply (*metis NegateNode*)
           apply (*metis LogicNegationNode*)
          apply (*metis AddNode*)
         apply (*metis MulNode*)
        apply (*metis SubNode*)
        apply (*metis AndNode*)
       apply (*metis OrNode*)
       apply (*metis XorNode*)
       apply (*metis ShortCircuitOrNode*)
      apply (*metis LeftShiftNode*)
     apply (*metis RightShiftNode*)
    apply (*metis UnsignedRightShiftNode*)
    apply (*metis IntegerBelowNode*)
    apply (*metis IntegerEqualsNode*)
   apply (*metis IntegerLessThanNode*)
  apply (*metis NarrowNode*)

apply (*metis SignExtendNode*)
      apply (*metis ZeroExtendNode*)
    defer
      apply (*metis RefNode*)
    by *blast*
    done
  done

lemma *new-node-not-present*:
  assumes *find-node-and-stamp g (node, s) = None*
  assumes *n = get-fresh-id g*
  assumes *g′ = add-node n (node, s) g*
  shows $\forall$ *n′* $\in$ *true-ids g.* ($\forall$ *e.* (($g \vdash n \simeq e$) $\wedge$ ($g \vdash n′ \simeq e$)) $\longrightarrow$ $n = n′$)
  using *assms*
  using *encode-in-ids fresh-ids* **by** *blast*

lemma *true-ids-def*:
  true-ids g = {*n* $\in$ *ids g.* $\neg$(*is-RefNode* (*kind g n*)) $\wedge$ ((*kind g n*) $\neq$ *NoNode*)}
  unfolding *true-ids-def ids-def*
  using *ids-def is-RefNode-def* **by** *fastforce*

lemma *add-node-some-node-def*:
  assumes *k* $\neq$ *NoNode*
  assumes *g′ = add-node nid (k, s) g*
  shows *g′ = Abs-IRGraph ((Rep-IRGraph g)(nid $\mapsto$ (k, s)))*
  using *assms*
  by (*metis Rep-IRGraph-inverse add-node.rep-eq fst-conv*)

lemma *ids-add-update-v1*:
  assumes *g′ = add-node nid (k, s) g*
  assumes *k* $\neq$ *NoNode*
  shows *dom (Rep-IRGraph g′) = dom (Rep-IRGraph g)* $\cup$ {*nid*}
  using *assms ids.rep-eq add-node-some-node-def*
  by (*simp add: add-node.rep-eq*)

lemma *ids-add-update-v2*:
  assumes *g′ = add-node nid (k, s) g*
  assumes *k* $\neq$ *NoNode*
  shows *nid* $\in$ *ids g′*
  using *assms*
  using *find-new-kind ids-some* **by** *presburger*

lemma *add-node-ids-subset*:
  assumes *n* $\in$ *ids g*
  assumes *g′ = add-node n node g*
  shows *ids g′ = ids g* $\cup$ {*n*}
  using *assms* **unfolding** *add-node-def*
  apply (*cases fst node = NoNode*)
  using *ids.rep-eq replace-node.rep-eq replace-node-def* **apply** *auto[1]*

unfolding *ids-def*
by (*smt* (*verit, best*) *Collect-cong Un-insert-right dom-fun-upd fst-conv fun-upd-apply ids.rep-eq ids-def insert-absorb mem-Collect-eq option.inject option.simps(3) replace-node.rep-eq replace-node-def sup-bot.right-neutral*)

lemma *convert-maximal*:
  assumes $\forall n\ n'.\ n \in$ *true-ids* $g \wedge n' \in$ *true-ids* $g \longrightarrow (\forall e\ e'.\ (g \vdash n \simeq e) \wedge (g \vdash n' \simeq e') \longrightarrow e \neq e')$
  shows *maximal-sharing* g
  using *assms*
  using *maximal-sharing* **by** *blast*

lemma *add-node-set-eq*:
  assumes $k \neq$ *NoNode*
  assumes $n \notin$ *ids* g
  shows *as-set* (*add-node* n $(k,\ s)$ g) $=$ *as-set* $g \cup \{(n,\ (k,\ s))\}$
  using *assms* **unfolding** *as-set-def add-node-def* **apply** *transfer* **apply** *simp*
  by *blast*

lemma *add-node-as-set-eq*:
  assumes $g' =$ *add-node* n $(k,\ s)$ g
  assumes $n \notin$ *ids* g
  shows $(\{n\} \unlhd$ *as-set* $g') =$ *as-set* g
  using *assms* **unfolding** *domain-subtraction-def*
  using *add-node-set-eq*
  by (*smt* (*z3*) *Collect-cong Rep-IRGraph-inverse UnCI UnE add-node.rep-eq as-set-def case-prodE2 case-prodI2 le-boolE le-boolI' mem-Collect-eq prod.sel(1) singletonD singletonI*)

lemma *true-ids*:
  true-ids $g =$ *ids* $g - \{n \in$ *ids* $g.\ $*is-RefNode* (*kind* g n)$\}$
  unfolding *true-ids-def*
  by *fastforce*

lemma *as-set-ids*:
  assumes *as-set* $g =$ *as-set* g'
  shows *ids* $g =$ *ids* g'
  using *assms*
  by (*metis antisym equalityD1 graph-refinement-def subset-refines*)

lemma *ids-add-update*:
  assumes $k \neq$ *NoNode*
  assumes $n \notin$ *ids* g
  assumes $g' =$ *add-node* n $(k,\ s)$ g
  shows *ids* $g' =$ *ids* $g \cup \{n\}$
  using *assms* **apply** (*subst assms(3)*) **using** *add-node-set-eq as-set-ids*
  by (*smt* (*verit, del-insts*) *Collect-cong Diff-idemp Diff-insert-absorb Un-commute add-node.rep-eq add-node-def ids.rep-eq ids-add-update-v1 ids-add-update-v2 insertE insert-Collect insert-is-Un map-upd-Some-unfold mem-Collect-eq replace-node-def*

replace-node-unchanged)

lemma *true-ids-add-update*:
  assumes $k \neq NoNode$
  assumes $n \notin ids\ g$
  assumes $g' = add\text{-}node\ n\ (k,\ s)\ g$
  assumes $\neg(is\text{-}RefNode\ k)$
  shows $true\text{-}ids\ g' = true\text{-}ids\ g \cup \{n\}$
  using *assms* **using** *true-ids ids-add-update*
  by (*smt* (*z3*) *Collect-cong Diff-iff Diff-insert-absorb Un-commute add-node-def*
find-new-kind insert-Diff-if insert-is-Un mem-Collect-eq replace-node-def replace-node-unchanged)

lemma *new-def*:
  assumes $(new \trianglelefteq as\text{-}set\ g') = as\text{-}set\ g$
  shows $n \in ids\ g \longrightarrow n \notin new$
  using *assms*
  by (*smt* (*z3*) *as-set-def case-prodD domain-subtraction-def mem-Collect-eq*)

lemma *add-preserves-rep*:
  assumes *unchanged*: $(new \trianglelefteq as\text{-}set\ g') = as\text{-}set\ g$
  assumes *closed*: *wf-closed g*
  assumes *existed*: $n \in ids\ g$
  assumes $g' \vdash n \simeq e$
  shows $g \vdash n \simeq e$
proof (*cases* $n \in new$)
  case *True*
  have $n \notin ids\ g$
    using *unchanged True* **unfolding** *as-set-def domain-subtraction-def*
    by *blast*
  then show *?thesis* **using** *existed* **by** *simp*
next
  case *False*
  then have *kind-eq*: $\forall\ n'\ .\ n' \notin new \longrightarrow kind\ g\ n' = kind\ g'\ n'$
    — can be more general than *stamp_eq* because NoNode default is equal
    using *unchanged not-excluded-keep-type*
    by (*smt* (*z3*) *case-prodE domain-subtraction-def ids-some mem-Collect-eq subsetI*)
  from *False* **have** *stamp-eq*: $\forall\ n' \in ids\ g'\ .\ n' \notin new \longrightarrow stamp\ g\ n' = stamp\ g'\ n'$
    using *unchanged not-excluded-keep-type*
    by (*metis equalityE*)
  show *?thesis* **using** *assms*(*4*) *kind-eq stamp-eq False*
  proof (*induction n e rule*: *rep.induct*)
    case (*ConstantNode n c*)
    then show *?case*
      using *rep.ConstantNode kind-eq* **by** *presburger*
  next

    case (*ParameterNode n i s*)
    then show *?case*
      using *rep.ParameterNode*
      by (*metis no-encoding*)
  next
    case (*ConditionalNode n c t f ce te fe*)
    have *kind*: *kind g n = ConditionalNode c t f*
      using *ConditionalNode.hyps*(*1*) *ConditionalNode.prems*(*3*) *kind-eq* **by** *presburger*
    then have *isin*: $n \in ids\ g$
      by *simp*
    have *inputs*: $\{c,\ t,\ f\} = inputs\ g\ n$
      using *kind* **unfolding** *inputs.simps* **using** *inputs-of-ConditionalNode* **by** *simp*
    have $c \in ids\ g \wedge t \in ids\ g \wedge f \in ids\ g$
      using *closed* **unfolding** *wf-closed-def*
      using *isin inputs* **by** *blast*
    then have $c \notin new \wedge t \notin new \wedge f \notin new$
      using *new-def unchanged* **by** *blast*
    then show *?case* **using** *ConditionalNode* **apply** *simp*
      using *rep.ConditionalNode* **by** *presburger*
  next
    case (*AbsNode n x xe*)
    then have *kind*: *kind g n = AbsNode x*
      by *simp*
    then have *isin*: $n \in ids\ g$
      by *simp*
    have *inputs*: $\{x\} = inputs\ g\ n$
      using *kind* **unfolding** *inputs.simps* **by** *simp*
    have $x \in ids\ g$
      using *closed* **unfolding** *wf-closed-def*
      using *isin inputs* **by** *blast*
    then have $x \notin new$
      using *new-def unchanged* **by** *blast*
    then show *?case*
      using *AbsNode*
      using *rep.AbsNode* **by** *presburger*
  next
    case (*NotNode n x xe*)
    then have *kind*: *kind g n = NotNode x*
      by *simp*
    then have *isin*: $n \in ids\ g$
      by *simp*
    have *inputs*: $\{x\} = inputs\ g\ n$
      using *kind* **unfolding** *inputs.simps* **by** *simp*
    have $x \in ids\ g$
      using *closed* **unfolding** *wf-closed-def*
      using *isin inputs* **by** *blast*
    then have $x \notin new$
      using *new-def unchanged* **by** *blast*

then show *?case* **using** *NotNode*
  using *rep.NotNode* **by** *presburger*
next
  case (*NegateNode n x xe*)
  then have *kind*: *kind g n = NegateNode x*
    by *simp*
  then have *isin*: $n \in ids\ g$
    by *simp*
  have *inputs*: $\{x\} = inputs\ g\ n$
    using *kind* **unfolding** *inputs.simps* **by** *simp*
  have $x \in ids\ g$
    using *closed* **unfolding** *wf-closed-def*
    using *isin inputs* **by** *blast*
  then have $x \notin new$
    using *new-def unchanged* **by** *blast*
  then show *?case* **using** *NegateNode*
    using *rep.NegateNode* **by** *presburger*
next
  case (*LogicNegationNode n x xe*)
  then have *kind*: *kind g n = LogicNegationNode x*
    by *simp*
  then have *isin*: $n \in ids\ g$
    by *simp*
  have *inputs*: $\{x\} = inputs\ g\ n$
    using *kind* **unfolding** *inputs.simps* **by** *simp*
  have $x \in ids\ g$
    using *closed* **unfolding** *wf-closed-def*
    using *isin inputs* **by** *blast*
  then have $x \notin new$
    using *new-def unchanged* **by** *blast*
  then show *?case* **using** *LogicNegationNode*
    using *rep.LogicNegationNode* **by** *presburger*
next
  case (*AddNode n x y xe ye*)
  then have *kind*: *kind g n = AddNode x y*
    by *simp*
  then have *isin*: $n \in ids\ g$
    by *simp*
  have *inputs*: $\{x,\ y\} = inputs\ g\ n$
    using *kind* **unfolding** *inputs.simps* **by** *simp*
  have $x \in ids\ g \wedge y \in ids\ g$
    using *closed* **unfolding** *wf-closed-def*
    using *isin inputs* **by** *blast*
  then have $x \notin new \wedge y \notin new$
    using *new-def unchanged* **by** *blast*
  then show *?case* **using** *AddNode*
    using *rep.AddNode* **by** *presburger*
next
  case (*MulNode n x y xe ye*)

117

then have *kind*: *kind g n = MulNode x y*
  by *simp*
then have *isin*: *n ∈ ids g*
  by *simp*
have *inputs*: {*x*, *y*} = *inputs g n*
  using *kind* **unfolding** *inputs.simps* **by** *simp*
have *x ∈ ids g ∧ y ∈ ids g*
  using *closed* **unfolding** *wf-closed-def*
  using *isin inputs* **by** *blast*
then have *x ∉ new ∧ y ∉ new*
  using *new-def unchanged* **by** *blast*
then show *?case* **using** *MulNode*
  using *rep.MulNode* **by** *presburger*
next
  case (*SubNode n x y xe ye*)
  then have *kind*: *kind g n = SubNode x y*
    by *simp*
  then have *isin*: *n ∈ ids g*
    by *simp*
  have *inputs*: {*x*, *y*} = *inputs g n*
    using *kind* **unfolding** *inputs.simps* **by** *simp*
  have *x ∈ ids g ∧ y ∈ ids g*
    using *closed* **unfolding** *wf-closed-def*
    using *isin inputs* **by** *blast*
  then have *x ∉ new ∧ y ∉ new*
    using *new-def unchanged* **by** *blast*
  then show *?case* **using** *SubNode*
    using *rep.SubNode* **by** *presburger*
next
  case (*AndNode n x y xe ye*)
  then have *kind*: *kind g n = AndNode x y*
    by *simp*
  then have *isin*: *n ∈ ids g*
    by *simp*
  have *inputs*: {*x*, *y*} = *inputs g n*
    using *kind* **unfolding** *inputs.simps* **by** *simp*
  have *x ∈ ids g ∧ y ∈ ids g*
    using *closed* **unfolding** *wf-closed-def*
    using *isin inputs* **by** *blast*
  then have *x ∉ new ∧ y ∉ new*
    using *new-def unchanged* **by** *blast*
  then show *?case* **using** *AndNode*
    using *rep.AndNode* **by** *presburger*
next
  case (*OrNode n x y xe ye*)
  then have *kind*: *kind g n = OrNode x y*
    by *simp*
  then have *isin*: *n ∈ ids g*
    by *simp*

have *inputs*: $\{x, y\}$ = *inputs g n*
  using *kind* **unfolding** *inputs.simps* **by** *simp*
have $x \in ids\ g \wedge y \in ids\ g$
  using *closed* **unfolding** *wf-closed-def*
  using *isin inputs* **by** *blast*
then have $x \notin new \wedge y \notin new$
  using *new-def unchanged* **by** *blast*
then show *?case* **using** *OrNode*
  using *rep.OrNode* **by** *presburger*
next
  case (*XorNode n x y xe ye*)
  then have *kind*: *kind g n = XorNode x y*
    by *simp*
  then have *isin*: $n \in ids\ g$
    by *simp*
  have *inputs*: $\{x, y\}$ = *inputs g n*
    using *kind* **unfolding** *inputs.simps* **by** *simp*
  have $x \in ids\ g \wedge y \in ids\ g$
    using *closed* **unfolding** *wf-closed-def*
    using *isin inputs* **by** *blast*
  then have $x \notin new \wedge y \notin new$
    using *new-def unchanged* **by** *blast*
  then show *?case* **using** *XorNode*
    using *rep.XorNode* **by** *presburger*
next
  case (*ShortCircuitOrNode n x y xe ye*)
  then have *kind*: *kind g n = ShortCircuitOrNode x y*
    by *simp*
  then have *isin*: $n \in ids\ g$
    by *simp*
  have *inputs*: $\{x, y\}$ = *inputs g n*
    using *kind* **unfolding** *inputs.simps* **by** *simp*
  have $x \in ids\ g \wedge y \in ids\ g$
    using *closed* **unfolding** *wf-closed-def*
    using *isin inputs* **by** *blast*
  then have $x \notin new \wedge y \notin new$
    using *new-def unchanged* **by** *blast*
  then show *?case* **using** *ShortCircuitOrNode*
    using *rep.ShortCircuitOrNode* **by** *presburger*
next
  case (*LeftShiftNode n x y xe ye*)
  then have *kind*: *kind g n = LeftShiftNode x y*
    by *simp*
  then have *isin*: $n \in ids\ g$
    by *simp*
  have *inputs*: $\{x, y\}$ = *inputs g n*
    using *kind* **unfolding** *inputs.simps* **by** *simp*
  have $x \in ids\ g \wedge y \in ids\ g$
    using *closed* **unfolding** *wf-closed-def*

    using *isin inputs* **by** *blast*
  then have *x* ∉ *new* ∧ *y* ∉ *new*
    using *new-def unchanged* **by** *blast*
  then show *?case* **using** *LeftShiftNode*
    using *rep.LeftShiftNode* **by** *presburger*
next
  case (*RightShiftNode n x y xe ye*)
  then have *kind*: *kind g n = RightShiftNode x y*
    by *simp*
  then have *isin*: *n* ∈ *ids g*
    by *simp*
  have *inputs*: {*x*, *y*} = *inputs g n*
    using *kind* **unfolding** *inputs.simps* **by** *simp*
  have *x* ∈ *ids g* ∧ *y* ∈ *ids g*
    using *closed* **unfolding** *wf-closed-def*
    using *isin inputs* **by** *blast*
  then have *x* ∉ *new* ∧ *y* ∉ *new*
    using *new-def unchanged* **by** *blast*
  then show *?case* **using** *RightShiftNode*
    using *rep.RightShiftNode* **by** *presburger*
next
  case (*UnsignedRightShiftNode n x y xe ye*)
  then have *kind*: *kind g n = UnsignedRightShiftNode x y*
    by *simp*
  then have *isin*: *n* ∈ *ids g*
    by *simp*
  have *inputs*: {*x*, *y*} = *inputs g n*
    using *kind* **unfolding** *inputs.simps* **by** *simp*
  have *x* ∈ *ids g* ∧ *y* ∈ *ids g*
    using *closed* **unfolding** *wf-closed-def*
    using *isin inputs* **by** *blast*
  then have *x* ∉ *new* ∧ *y* ∉ *new*
    using *new-def unchanged* **by** *blast*
  then show *?case* **using** *UnsignedRightShiftNode*
    using *rep.UnsignedRightShiftNode* **by** *presburger*
next
  case (*IntegerBelowNode n x y xe ye*)
  then have *kind*: *kind g n = IntegerBelowNode x y*
    by *simp*
  then have *isin*: *n* ∈ *ids g*
    by *simp*
  have *inputs*: {*x*, *y*} = *inputs g n*
    using *kind* **unfolding** *inputs.simps* **by** *simp*
  have *x* ∈ *ids g* ∧ *y* ∈ *ids g*
    using *closed* **unfolding** *wf-closed-def*
    using *isin inputs* **by** *blast*
  then have *x* ∉ *new* ∧ *y* ∉ *new*
    using *new-def unchanged* **by** *blast*
  then show *?case* **using** *IntegerBelowNode*

using *rep.IntegerBelowNode* **by** *presburger*
next
  case (*IntegerEqualsNode n x y xe ye*)
  then have *kind*: *kind g n = IntegerEqualsNode x y*
    by *simp*
  then have *isin*: $n \in ids\ g$
    by *simp*
  have *inputs*: $\{x,\ y\} = inputs\ g\ n$
    using *kind* **unfolding** *inputs.simps* **by** *simp*
  have $x \in ids\ g \land y \in ids\ g$
    using *closed* **unfolding** *wf-closed-def*
    using *isin inputs* **by** *blast*
  then have $x \notin new \land y \notin new$
    using *new-def unchanged* **by** *blast*
  then show *?case* **using** *IntegerEqualsNode*
    using *rep.IntegerEqualsNode* **by** *presburger*
next
  case (*IntegerLessThanNode n x y xe ye*)
  then have *kind*: *kind g n = IntegerLessThanNode x y*
    by *simp*
  then have *isin*: $n \in ids\ g$
    by *simp*
  have *inputs*: $\{x,\ y\} = inputs\ g\ n$
    using *kind* **unfolding** *inputs.simps* **by** *simp*
  have $x \in ids\ g \land y \in ids\ g$
    using *closed* **unfolding** *wf-closed-def*
    using *isin inputs* **by** *blast*
  then have $x \notin new \land y \notin new$
    using *new-def unchanged* **by** *blast*
  then show *?case* **using** *IntegerLessThanNode*
    using *rep.IntegerLessThanNode* **by** *presburger*
next
  case (*NarrowNode n inputBits resultBits x xe*)
  then have *kind*: *kind g n = NarrowNode inputBits resultBits x*
    by *simp*
  then have *isin*: $n \in ids\ g$
    by *simp*
  have *inputs*: $\{x\} = inputs\ g\ n$
    using *kind* **unfolding** *inputs.simps* **by** *simp*
  have $x \in ids\ g$
    using *closed* **unfolding** *wf-closed-def*
    using *isin inputs* **by** *blast*
  then have $x \notin new$
    using *new-def unchanged* **by** *blast*
  then show *?case* **using** *NarrowNode*
    using *rep.NarrowNode* **by** *presburger*
next
  case (*SignExtendNode n inputBits resultBits x xe*)
  then have *kind*: *kind g n = SignExtendNode inputBits resultBits x*

121

     by *simp*
   then have *isin*: *n* ∈ *ids g*
     by *simp*
   have *inputs*: {*x*} = *inputs g n*
     using *kind* **unfolding** *inputs.simps* **by** *simp*
   have *x* ∈ *ids g*
     using *closed* **unfolding** *wf-closed-def*
     using *isin inputs* **by** *blast*
   then have *x* ∉ *new*
     using *new-def unchanged* **by** *blast*
   then show *?case* **using** *SignExtendNode*
     using *rep.SignExtendNode* **by** *presburger*
 next
   case (*ZeroExtendNode n inputBits resultBits x xe*)
   then have *kind*: *kind g n* = *ZeroExtendNode inputBits resultBits x*
     by *simp*
   then have *isin*: *n* ∈ *ids g*
     by *simp*
   have *inputs*: {*x*} = *inputs g n*
     using *kind* **unfolding** *inputs.simps* **by** *simp*
   have *x* ∈ *ids g*
     using *closed* **unfolding** *wf-closed-def*
     using *isin inputs* **by** *blast*
   then have *x* ∉ *new*
     using *new-def unchanged* **by** *blast*
   then show *?case* **using** *ZeroExtendNode*
     using *rep.ZeroExtendNode* **by** *presburger*
 next
   case (*LeafNode n s*)
   then show *?case*
     by (*metis no-encoding rep.LeafNode*)
 next
   case (*RefNode n n′ e*)
   then have *kind*: *kind g n* = *RefNode n′*
     by *simp*
   then have *isin*: *n* ∈ *ids g*
     by *simp*
   have *inputs*: {*n′*} = *inputs g n*
     using *kind* **unfolding** *inputs.simps* **by** *simp*
   have *n′* ∈ *ids g*
     using *closed* **unfolding** *wf-closed-def*
     using *isin inputs* **by** *blast*
   then have *n′* ∉ *new*
     using *new-def unchanged* **by** *blast*
   then show *?case*
     using *RefNode*
     using *rep.RefNode* **by** *presburger*
 qed
qed

lemma *not-in-no-rep*:
  $n \notin ids\ g \Longrightarrow \forall e.\ \neg(g \vdash n \simeq e)$
  using *eval-contains-id* **by** *blast*

lemma *unary-inputs*:
  assumes *kind g n = unary-node op x*
  shows *inputs g n = {x}*
  using *assms* **by** (*cases op*; *auto*)

lemma *unary-succ*:
  assumes *kind g n = unary-node op x*
  shows *succ g n = {}*
  using *assms* **by** (*cases op*; *auto*)

lemma *binary-inputs*:
  assumes *kind g n = bin-node op x y*
  shows *inputs g n = {x, y}*
  using *assms* **by** (*cases op*; *auto*)

lemma *binary-succ*:
  assumes *kind g n = bin-node op x y*
  shows *succ g n = {}*
  using *assms* **by** (*cases op*; *auto*)

lemma *unrep-contains*:
  assumes $g \oplus e \rightsquigarrow (g',\ n)$
  shows $n \in ids\ g'$
  using *assms*
  using *not-in-no-rep term-graph-reconstruction* **by** *blast*

lemma *unrep-preserves-contains*:
  assumes $n \in ids\ g$
  assumes $g \oplus e \rightsquigarrow (g',\ n')$
  shows $n \in ids\ g'$
  using *assms*
  by (*meson subsetD unrep-ids-subset*)

lemma *unrep-preserves-closure*:
  assumes *wf-closed g*
  assumes $g \oplus e \rightsquigarrow (g',\ n)$
  shows *wf-closed g'*
  using *assms(2,1)* **unfolding** *wf-closed-def*
  proof (*induction g e (g', n) arbitrary: g' n*)
    case (*ConstantNodeSame g c n*)
    then show *?case*
      by *blast*

next
  case (*ConstantNodeNew g c n g′*)
  then have *dom*: *ids g′ = ids g ∪ {n}*
    by (*meson IRNode.distinct(683) add-node-ids-subset ids-add-update*)
  have *k*: *kind g′ n = ConstantNode c*
    using *ConstantNodeNew add-node-lookup* **by** *simp*
  then have *inp*: *{} = inputs g′ n*
    unfolding *inputs.simps* **by** *simp*
  from *k* **have** *suc*: *{} = succ g′ n*
    unfolding *succ.simps* **by** *simp*
  have *inputs g′ n ⊆ ids g′ ∧ succ g′ n ⊆ ids g′ ∧ kind g′ n ≠ NoNode*
    using *inp suc k* **by** *simp*
  then show *?case*
  by (*smt* (*verit*) *ConstantNodeNew.hyps(3) ConstantNodeNew.prems Un-insert-right*
add-changed changeonly.elims(2) dom inputs.simps insert-iff singleton-iff subset-insertI
subset-trans succ.simps sup-bot-right)
  next
    case (*ParameterNodeSame g i s n*)
    then show *?case* **by** *blast*
  next
    case (*ParameterNodeNew g i s n g′*)
    then have *dom*: *ids g′ = ids g ∪ {n}*
      using *IRNode.distinct(2447) fresh-ids ids-add-update* **by** *presburger*
    have *k*: *kind g′ n = ParameterNode i*
      using *ParameterNodeNew add-node-lookup* **by** *simp*
    then have *inp*: *{} = inputs g′ n*
      unfolding *inputs.simps* **by** *simp*
    from *k* **have** *suc*: *{} = succ g′ n*
      unfolding *succ.simps* **by** *simp*
    have *inputs g′ n ⊆ ids g′ ∧ succ g′ n ⊆ ids g′ ∧ kind g′ n ≠ NoNode*
      using *k inp suc* **by** *simp*
    then show *?case*
    by (*smt* (*verit*) *ParameterNodeNew.hyps(3) ParameterNodeNew.prems Un-insert-right*
add-node-as-set dom inputs.elims insertE not-excluded-keep-type order-trans single-
tonD subset-insertI succ.elims sup-bot-right)
  next
    case (*ConditionalNodeSame g ce g2 c te g3 t fe g4 f s′ n*)
    then show *?case* **by** *blast*
  next
    case (*ConditionalNodeNew g ce g2 c te g3 t fe g4 f s′ n g′*)
    then have *dom*: *ids g′ = ids g4 ∪ {n}*
      by (*meson IRNode.distinct(591) add-node-ids-subset ids-add-update*)
    have *k*: *kind g′ n = ConditionalNode c t f*
      using *ConditionalNodeNew add-node-lookup* **by** *simp*
    then have *inp*: *{c, t, f} = inputs g′ n*
      unfolding *inputs.simps* **by** *simp*
    from *k* **have** *suc*: *{} = succ g′ n*
      unfolding *succ.simps* **by** *simp*
    have *inputs g′ n ⊆ ids g′ ∧ succ g′ n ⊆ ids g′ ∧ kind g′ n ≠ NoNode*

using *k inp suc unrep-contains unrep-preserves-contains*
   using *ConditionalNodeNew(1,3,5,10)*
     by (*smt* (*verit*) *IRNode.simps(643) Un-insert-right bot.extremum dom insert-absorb insert-subset subset-insertI sup-bot-right*)
   then show *?case* **using** *dom*
   by (*smt* (*z3*) *ConditionalNodeNew.hyps(10) ConditionalNodeNew.hyps(2) ConditionalNodeNew.hyps(4) ConditionalNodeNew.hyps(6) ConditionalNodeNew.prems Diff-eq-empty-iff Diff-iff Un-insert-right Un-upper1 add-node-def inputs.simps insertE replace-node-def replace-node-unchanged subset-trans succ.simps sup-bot-right*)
 next
   case (*UnaryNodeSame g xe g2 x s' op n*)
   then show *?case* **by** *blast*
 next
   case (*UnaryNodeNew g xe g2 x s' op n g'*)
   then have *dom*: *ids g' = ids g2 ∪ {n}*
     by (*metis add-node-ids-subset add-node-lookup ids-add-update ids-some unrep.UnaryNodeNew unrep-contains*)
   have *k*: *kind g' n = unary-node op x*
     using *UnaryNodeNew add-node-lookup*
     by (*metis fresh-ids ids-some*)
   then have *inp*: *{x} = inputs g' n*
     using *unary-inputs* **by** *simp*
   from *k* **have** *suc*: *{} = succ g' n*
     using *unary-succ* **by** *simp*
   have *inputs g' n ⊆ ids g' ∧ succ g' n ⊆ ids g' ∧ kind g' n ≠ NoNode*
     using *k inp suc unrep-contains unrep-preserves-contains*
     using *UnaryNodeNew(1,6)*
       by (*metis Un-upper1 dom empty-subsetI ids-some insert-not-empty insert-subsetI not-in-g-inputs subset-iff*)
   then show *?case*
   by (*smt* (*verit*) *Un-insert-right UnaryNodeNew.hyps(2) UnaryNodeNew.hyps(6) UnaryNodeNew.prems add-changed changeonly.elims(2) dom inputs.simps insert-iff singleton-iff subset-insertI subset-trans succ.simps sup-bot-right*)
 next
   case (*BinaryNodeSame g xe g2 x ye g3 y s' op n*)
   then show *?case* **by** *blast*
 next
   case (*BinaryNodeNew g xe g2 x ye g3 y s' op n g'*)
   then have *dom*: *ids g' = ids g3 ∪ {n}*
     by (*metis binary-inputs fresh-ids ids-add-update ids-some insert-not-empty not-in-g-inputs*)
   have *k*: *kind g' n = bin-node op x y*
     using *BinaryNodeNew add-node-lookup*
     by (*metis fresh-ids ids-some*)
   then have *inp*: *{x, y} = inputs g' n*
     using *binary-inputs* **by** *simp*
   from *k* **have** *suc*: *{} = succ g' n*
     using *binary-succ* **by** *simp*
   have *inputs g' n ⊆ ids g' ∧ succ g' n ⊆ ids g' ∧ kind g' n ≠ NoNode*

using *k inp suc unrep-contains unrep-preserves-contains*
using *BinaryNodeNew(1,3,6)*
    by (*metis Un-upper1 dom empty-subsetI ids-some insert-not-empty insert-subsetI not-in-g-inputs subset-iff*)
  then show *?case* **using** *dom BinaryNodeNew*
    by (*smt (verit, del-insts) Diff-eq-empty-iff Diff-iff Un-insert-right Un-upper1 add-node-def inputs.simps insertE replace-node-def replace-node-unchanged subset-trans succ.simps sup-bot-right*)
next
  case (*AllLeafNodes g n s*)
  then show *?case*
    by *blast*
qed

inductive-cases *ConstUnrepE*: $g \oplus (ConstantExpr\ x) \rightsquigarrow (g',\ n)$

definition *constant-value* **where**
  constant-value = (*IntVal32 0*)
definition *bad-graph* **where**
  bad-graph = *irgraph* [
    (*0, AbsNode 1, constantAsStamp constant-value*),
    (*1, RefNode 2, constantAsStamp constant-value*),
    (*2, ConstantNode constant-value, constantAsStamp constant-value*)
  ]

experiment begin
lemma
  assumes *maximal-sharing g*
  assumes *wf-closed g*
  assumes *kind g y = AbsNode y'*
  assumes *kind g y' = RefNode y''*
  assumes *kind g y'' = ConstantNode v*
  assumes *stamp g y'' = constantAsStamp v*
  assumes $g \oplus (UnaryExpr\ UnaryAbs\ (ConstantExpr\ v)) \rightsquigarrow (g',\ n)$ (**is** $g \oplus ?e \rightsquigarrow (g',\ n)$)
  shows $\neg(maximal\text{-}sharing\ g')$
  using *assms(3,2,1)*
proof −
  have $y'' \in ids\ g$
    using *assms(5)* **by** *simp*
  then have *List.member (sorted-list-of-set (ids g)) y''*
    by (*metis member-def unwrap-sorted*)
  then have *find* ($\lambda i.\ kind\ g\ i = ConstantNode\ v \wedge stamp\ g\ i = constantAsStamp$ *v*) (*sorted-list-of-set (ids g)*) = *Some y''*
    using *assms(5,6) find-Some-iff* **sorry**
  then have $g \oplus ConstantExpr\ v \rightsquigarrow (g,\ y'')$
    using *assms(5) ConstUnrepE* **sorry**
  then show *?thesis* **sorry**
qed

end

lemma *conditional-rep-kind*:
  assumes $g \vdash n \simeq ConditionalExpr\ ce\ te\ fe$
  assumes $g \vdash c \simeq ce$
  assumes $g \vdash t \simeq te$
  assumes $g \vdash f \simeq fe$
  assumes $\neg(\exists\, n'.\ kind\ g\ n = RefNode\ n')$
  shows *kind g n = ConditionalNode c t f*
  using *assms* **apply** (*induction n ConditionalExpr ce te fe rule*: *rep.induct*) **defer**
  apply *meson* **using** *repDet* **sorry**

lemma *unary-rep-kind*:
  assumes $g \vdash n \simeq UnaryExpr\ op\ xe$
  assumes $g \vdash x \simeq xe$
  assumes $\neg(\exists\, n'.\ kind\ g\ n = RefNode\ n')$
  shows *kind g n = unary-node op x*
  using *assms* **apply** (*cases op*) **using** *AbsNodeE* **sorry**

lemma *binary-rep-kind*:
  assumes $g \vdash n \simeq BinaryExpr\ op\ xe\ ye$
  assumes $g \vdash x \simeq xe$
  assumes $g \vdash y \simeq ye$
  assumes $\neg(\exists\, n'.\ kind\ g\ n = RefNode\ n')$
  shows *kind g n = bin-node op x y*
  using *assms* **sorry**

theorem *unrep-maximal-sharing*:
  assumes *maximal-sharing g*
  assumes *wf-closed g*
  assumes $g \oplus e \rightsquigarrow (g',\ n)$
  shows *maximal-sharing g′*
  using *assms(3,2,1)*
  proof (*induction g e* $(g',\ n)$ *arbitrary*: $g'\ n$)
    case (*ConstantNodeSame g c n*)
    then show *?case* **by** *blast*
  next
    case (*ConstantNodeNew g c n g′*)
    then have *kind g′ n = ConstantNode c*
      using *find-new-kind* **by** *blast*
    then have *repn*: $g' \vdash n \simeq ConstantExpr\ c$
      using *rep.ConstantNode* **by** *simp*
    from *ConstantNodeNew* **have** *real-node*: $\neg$(*is-RefNode* (*ConstantNode c*)) $\wedge$
ConstantNode $c \neq NoNode$
      by *simp*
    then have *dom*: *true-ids* $g' =$ *true-ids* $g \cup \{n\}$
      using *ConstantNodeNew.hyps(2) ConstantNodeNew.hyps(3) fresh-ids*
      by (*meson true-ids-add-update*)
    have *new*: $n \notin ids\ g$

using *fresh-ids*
using *ConstantNodeNew.hyps(2)* **by** *blast*
obtain *new* **where** *new = true-ids g′ − true-ids g*
by *simp*
then have *new-def*: *new = {n}*
by (*metis* (*no-types, lifting*) *DiffE Diff-cancel IRGraph.true-ids-def Un-insert-right dom insert-Diff-if new sup-bot-right*)
then have *unchanged*: (*new ⊴ as-set g′*) = *as-set g*
using *ConstantNodeNew(3) new add-node-as-set-eq*
by *presburger*
then have *kind-eq*: $\forall n'$. $n' \notin new \longrightarrow kind\ g\ n' = kind\ g'\ n'$
by (*metis ConstantNodeNew.hyps(3)* ‹*new = {n}*› *add-node-as-set dual-order.eq-iff not-excluded-keep-type not-in-g*)
from *unchanged* **have** *stamp-eq*: $\forall n' \in ids\ g$. $n' \notin new \longrightarrow stamp\ g\ n' = stamp\ g'\ n'$
using *not-excluded-keep-type new-def new*
by (*metis ConstantNodeNew.hyps(3) add-node-as-set*)
show *?case* **unfolding** *maximal-sharing* **apply** (*rule allI; rule allI; rule impI*)
using *ConstantNodeNew(5)* **unfolding** *maximal-sharing* **apply** *auto*
proof −
fix n_1 n_2 e
assume *1*: $\forall n_1$ n_2.
   $n_1 \in true\text{-}ids\ g \wedge n_2 \in true\text{-}ids\ g \longrightarrow$
   ($\exists e.\ (g \vdash n_1 \simeq e) \wedge (g \vdash n_2 \simeq e) \wedge stamp\ g\ n_1 = stamp\ g\ n_2) \longrightarrow n_1 = n_2$
assume $n_1 \in true\text{-}ids\ g'$
assume $n_2 \in true\text{-}ids\ g'$
show $g' \vdash n_1 \simeq e \Longrightarrow g' \vdash n_2 \simeq e \Longrightarrow stamp\ g'\ n_1 = stamp\ g'\ n_2 \Longrightarrow n_1 = n_2$

proof (*cases* $n_1 \in true\text{-}ids\ g$)
   case *n1*: *True*
   then show $g' \vdash n_1 \simeq e \Longrightarrow g' \vdash n_2 \simeq e \Longrightarrow stamp\ g'\ n_1 = stamp\ g'\ n_2 \Longrightarrow n_1 = n_2$
   proof (*cases* $n_2 \in true\text{-}ids\ g$)
      case *n2*: *True*
      assume *n1rep′*: $g' \vdash n_1 \simeq e$
      assume *n2rep′*: $g' \vdash n_2 \simeq e$
      assume *stmp*: $stamp\ g'\ n_1 = stamp\ g'\ n_2$
      have *n1rep*: $g \vdash n_1 \simeq e$
        using *n1rep′ kind-eq stamp-eq new-def add-preserves-rep*
          using *ConstantNodeNew.prems(1) IRGraph.true-ids-def n1 unchanged*
by *auto*
      have *n2rep*: $g \vdash n_2 \simeq e$
        using *n2rep′ kind-eq stamp-eq new-def add-preserves-rep*
          using *ConstantNodeNew.prems(1) IRGraph.true-ids-def n2 unchanged*
by *auto*
      have $stamp\ g\ n_1 = stamp\ g\ n_2$
        by (*metis ConstantNodeNew.hyps(3) stmp fresh-node-subset n1rep n2rep new subset-stamp*)
      then show *?thesis* **using** *1*

       using *n1 n2*

       using *n1rep n2rep* **by** *blast*

    next

      case *n2*: *False*

      assume *n1rep'*: $g' \vdash n_1 \simeq e$

      assume *n2rep'*: $g' \vdash n_2 \simeq e$

      assume *stmp*: *stamp* $g'\ n_1 =$ *stamp* $g'\ n_2$

      have *n2-def*: $n_2 = n$

       using ‹$n_2 \in$ *true-ids* g'› *dom n2* **by** *auto*

      have *n1rep*: $g \vdash n_1 \simeq$ *ConstantExpr c*

         by (*metis* (*no-types, lifting*) *ConstantNodeNew.prems*(*1*) *DiffE IR-*
Graph.true-ids-def add-preserves-rep n1 n1rep' n2-def n2rep' repDet repn unchanged)

      then have *n1in*: $n_1 \in$ *ids g*

       using *no-encoding* **by** *metis*

      have *k*: *kind* $g\ n_1 =$ *ConstantNode c*

       using *TreeToGraphThms.true-ids-def n1 n1rep* **by** *force*

      have *s*: *stamp* $g\ n_1 =$ *constantAsStamp c*

      by (*metis ConstantNodeNew.hyps*(*3*) *real-node n2-def stmp find-new-stamp*
fresh-node-subset n1rep new subset-stamp)

      from *k s* **show** *?thesis*

       using *find-none ConstantNodeNew.hyps*(*1*) *n1in* **by** *blast*

    qed

   next

     case *n1*: *False*

     then show $g' \vdash n_1 \simeq e \Longrightarrow g' \vdash n_2 \simeq e \Longrightarrow$ *stamp* $g'\ n_1 =$ *stamp* $g'\ n_2$
$\Longrightarrow n_1 = n_2$

     proof (*cases* $n_2 \in$ *true-ids g*)

      case *n2*: *True*

      assume *n1rep'*: $g' \vdash n_1 \simeq e$

      assume *n2rep'*: $g' \vdash n_2 \simeq e$

      assume *stmp*: *stamp* $g'\ n_1 =$ *stamp* $g'\ n_2$

      have *n1-def*: $n_1 = n$

       using ‹$n_1 \in$ *true-ids* g'› *dom n1* **by** *auto*

      have *n2in*: $n_2 \in$ *ids g*

       using *IRGraph.true-ids-def n2* **by** *auto*

      have *k*: *kind* $g\ n_2 =$ *ConstantNode c*

      by (*metis* (*mono-tags, lifting*) *ConstantNodeE ConstantNodeNew.prems*(*1*)
DiffE IRGraph.true-ids-def add-preserves-rep mem-Collect-eq n1-def n1rep' n2 n2rep'
repDet repn unchanged)

      have *s*: *stamp* $g\ n_2 =$ *constantAsStamp c*

         by (*metis ConstantNodeNew.hyps*(*3*) *TreeToGraphThms.new-def*
add-node-lookup n1-def n2in real-node stamp-eq stmp unchanged)

      from *k s* **show** *?thesis*

       using *find-none ConstantNodeNew.hyps*(*1*) *n2in* **by** *blast*

     next

      case *n2*: *False*

      assume *n1rep'*: $g' \vdash n_1 \simeq e$

      assume *n2rep'*: $g' \vdash n_2 \simeq e$

      assume *stamp* $g'\ n_1 =$ *stamp* $g'\ n_2$

      have $n_1 = n \land n_2 = n$
        using ‹$n_1 \in$ *true-ids g'*› *dom n1*
        using ‹$n_2 \in$ *true-ids g'*› *n2* **by** *blast*
      then show *?thesis*
        by *simp*
     qed
    qed
   qed
 next
  case (*ParameterNodeSame g i s n*)
  then show *?case* **by** *blast*
 next
  case (*ParameterNodeNew g i s n g'*)
  then have *k*: *kind g' n = ParameterNode i*
   using *find-new-kind* **by** *blast*
  have *stamp g' n = s*
   using *ParameterNodeNew.hyps(3) find-new-stamp* **by** *blast*
  then have *repn*: $g' \vdash n \simeq ParameterExpr\ i\ s$
   using *rep.ParameterNode k* **by** *simp*
   from *ConstantNodeNew* **have** $\neg$(*is-RefNode* (*ParameterNode i*)) $\land$ *ParameterNode i $\neq$ NoNode*
   by *simp*
  then have *dom*: *true-ids g' = true-ids g* $\cup$ $\{n\}$
   using *ParameterNodeNew.hyps(2) ParameterNodeNew.hyps(3) fresh-ids*
   by (*meson true-ids-add-update*)
  have *new*: $n \notin ids\ g$
   using *fresh-ids*
   using *ParameterNodeNew.hyps(2)* **by** *blast*
  obtain *new* **where** *new = true-ids g'* $-$ *true-ids g*
   by *simp*
  then have *new-def*: *new* = $\{n\}$
  by (*metis* (*no-types, lifting*) *DiffE Diff-cancel IRGraph.true-ids-def Un-insert-right dom insert-Diff-if new sup-bot-right*)
  then have *unchanged*: (*new* $\trianglelefteq$ *as-set g'*) = *as-set g*
   using *ParameterNodeNew(3) new add-node-as-set-eq*
   by *presburger*
  then have *kind-eq*: $\forall n'\ .\ n' \notin new \longrightarrow kind\ g\ n' = kind\ g'\ n'$
  by (*metis ParameterNodeNew.hyps(3)* ‹*new* = $\{n\}$› *add-node-as-set dual-order.eq-iff not-excluded-keep-type not-in-g*)
   from *unchanged* **have** *stamp-eq*: $\forall n' \in ids\ g\ .\ n' \notin new \longrightarrow stamp\ g\ n' = stamp\ g'\ n'$
   using *not-excluded-keep-type new-def new*
   by (*metis ParameterNodeNew.hyps(3) add-node-as-set*)
  show *?case* **unfolding** *maximal-sharing* **apply** (*rule allI; rule allI; rule impI*)
   using *ParameterNodeNew(5)* **unfolding** *maximal-sharing* **apply** *auto*
   proof $-$
   fix $n_1\ n_2\ e$
   assume *1*: $\forall n_1\ n_2.$
     $n_1 \in true\text{-}ids\ g \land n_2 \in true\text{-}ids\ g \longrightarrow$

130

$(\exists\,e.\ (g \vdash n_1 \simeq e) \land (g \vdash n_2 \simeq e) \land stamp\ g\ n_1 = stamp\ g\ n_2) \longrightarrow n_1 = n_2$

assume $n_1 \in true\text{-}ids\ g'$

assume $n_2 \in true\text{-}ids\ g'$

show $g' \vdash n_1 \simeq e \implies g' \vdash n_2 \simeq e \implies stamp\ g'\ n_1 = stamp\ g'\ n_2 \implies n_1 = n_2$

 proof (*cases* $n_1 \in true\text{-}ids\ g$)

  case *n1*: *True*

  then show $g' \vdash n_1 \simeq e \implies g' \vdash n_2 \simeq e \implies stamp\ g'\ n_1 = stamp\ g'\ n_2 \implies n_1 = n_2$

  proof (*cases* $n_2 \in true\text{-}ids\ g$)

   case *n2*: *True*

   assume *n1rep'*: $g' \vdash n_1 \simeq e$

   assume *n2rep'*: $g' \vdash n_2 \simeq e$

   assume $stamp\ g'\ n_1 = stamp\ g'\ n_2$

   have *n1rep*: $g \vdash n_1 \simeq e$

    using *n1rep' kind-eq stamp-eq new-def add-preserves-rep*

    using *ParameterNodeNew.prems*(*1*) *IRGraph.true-ids-def n1 unchanged*

by *auto*

   have *n2rep*: $g \vdash n_2 \simeq e$

    using *n2rep' kind-eq stamp-eq new-def add-preserves-rep*

    using *ParameterNodeNew.prems*(*1*) *IRGraph.true-ids-def n2 unchanged*

by *auto*

   have $stamp\ g\ n_1 = stamp\ g\ n_2$

    by (*metis ParameterNodeNew.hyps*(*3*) ‹$stamp\ g'\ n_1 = stamp\ g'\ n_2$›

fresh-node-subset n1rep n2rep new subset-stamp)

   then show *?thesis* **using** *1*

    using *n1 n2*

    using *n1rep n2rep* **by** *blast*

  next

   case *n2*: *False*

   assume *n1rep'*: $g' \vdash n_1 \simeq e$

   assume *n2rep'*: $g' \vdash n_2 \simeq e$

   assume $stamp\ g'\ n_1 = stamp\ g'\ n_2$

   have $n_2 = n$

    using ‹$n_2 \in true\text{-}ids\ g'$› *dom n2* **by** *auto*

   then have *ne*: $n_2 \notin ids\ g$

    using *new n2* **by** *blast*

   have *n1rep*: $g \vdash n_1 \simeq e$

    using *n1rep' kind-eq stamp-eq new-def add-preserves-rep*

    using *ParameterNodeNew.prems*(*1*) *IRGraph.true-ids-def n1 unchanged*

by *auto*

   have *n2rep*: $g \vdash n_2 \simeq e$

    using *n2rep' kind-eq stamp-eq new-def add-preserves-rep*

    using *ParameterNodeNew.prems*(*1*) *IRGraph.true-ids-def unchanged*

     by (*metis* (*no-types, lifting*) *IRNode.disc*(*2703*) *ParameterNodeE*

ParameterNodeNew.hyps(*1*) *TreeToGraphThms.true-ids-def* ‹$n_2 = n$› *find-none*

mem-Collect-eq n1 n1rep' repDet repn)

   then show *?thesis*

    using *n2rep not-in-no-rep ne* **by** *blast*

      qed
     next
      case *n1*: *False*
      then show $g' \vdash n_1 \simeq e \implies g' \vdash n_2 \simeq e \implies stamp\ g'\ n_1 = stamp\ g'\ n_2$
$\implies n_1 = n_2$
        proof (*cases* $n_2 \in$ *true-ids g*)
         case *n2*: *True*
         assume *n1rep'*: $g' \vdash n_1 \simeq e$
         assume *n2rep'*: $g' \vdash n_2 \simeq e$
         assume *stamp* $g'\ n_1 =$ *stamp* $g'\ n_2$
         have $n_1 = n$
          using ‹$n_1 \in$ *true-ids g'*› *dom n1* **by** *auto*
         then have *ne*: $n_1 \notin$ *ids g*
          using *new n2* **by** *blast*
         have *n1rep*: $g \vdash n_1 \simeq e$
          using *n1rep' kind-eq stamp-eq new-def add-preserves-rep*
          using *ParameterNodeNew.prems*(*1*) *IRGraph.true-ids-def n1 unchanged*
            by (*metis* (*no-types, lifting*) *IRNode.disc*(*2703*) *ParameterNodeE*
ParameterNodeNew.hyps(*1*) *TreeToGraphThms.true-ids-def* ‹$n_1 = n$› *find-none*
mem-Collect-eq n2 n2rep' repDet repn)
        then show *?thesis*
         using *n1rep not-in-no-rep ne* **by** *blast*
       next
        case *n2*: *False*
        assume *n1rep'*: $g' \vdash n_1 \simeq e$
        assume *n2rep'*: $g' \vdash n_2 \simeq e$
        assume *stamp* $g'\ n_1 =$ *stamp* $g'\ n_2$
        have $n_1 = n \land n_2 = n$
         using ‹$n_1 \in$ *true-ids g'*› *dom n1*
         using ‹$n_2 \in$ *true-ids g'*› *n2* **by** *blast*
        then show *?thesis*
         by *simp*
       qed
      qed
    qed
   next
    case (*ConditionalNodeSame g ce g2 c te g3 t fe g4 f s' n*)
    then show *?case*
     using *unrep-preserves-closure* **by** *blast*
   next
    case (*ConditionalNodeNew g ce g2 c te g3 t fe g4 f s' n g'*)
    then have *k*: *kind* $g'\ n = ConditionalNode\ c\ t\ f$
     using *find-new-kind* **by** *blast*
    have *stamp* $g'\ n = s'$
     using *ConditionalNodeNew.hyps*(*10*) *IRNode.distinct*(*591*) *find-new-stamp* **by**
blast
    then have *repn*: $g' \vdash n \simeq ConditionalExpr\ ce\ te\ fe$
     using *rep.ConditionalNode k*
     by (*metis ConditionalNodeNew.hyps*(*1*) *ConditionalNodeNew.hyps*(*10*) *Condi-*

132

tionalNodeNew.hyps(*3*) *ConditionalNodeNew.hyps*(*5*) *ConditionalNodeNew.hyps*(*9*)
fresh-ids fresh-node-subset subset-implies-evals term-graph-reconstruction)
    from *ConstantNodeNew* **have** ¬(*is-RefNode* (*ConditionalNode c t f*)) ∧ *Con-*
ditionalNode c t f ≠ NoNode
      by *simp*
    then have *dom*: *true-ids g′ = true-ids g4 ∪ {n}*
      using *ConditionalNodeNew.hyps*(*10*) *ConditionalNodeNew.hyps*(*9*) *fresh-ids*
true-ids-add-update **by** *presburger*
    have *new*: *n ∉ ids g*
      using *fresh-ids*
      by (*meson ConditionalNodeNew.hyps*(*1*) *ConditionalNodeNew.hyps*(*3*) *Con-*
ditionalNodeNew.hyps(*5*) *ConditionalNodeNew.hyps*(*9*) *unrep-preserves-contains*)
    obtain *new* **where** *new = true-ids g′ − true-ids g4*
      by *simp*
    then have *new-def*: *new = {n}*
      using *dom*
      by (*metis ConditionalNodeNew.hyps*(*9*) *DiffD1 DiffI Diff-cancel Diff-insert*
Un-insert-right boolean-algebra.disj-zero-right fresh-ids insertCI insert-Diff true-ids)
    then have *unchanged*: (*new ⊴ as-set g′*) = *as-set g4*
      using *new add-node-as-set-eq*
      using *ConditionalNodeNew.hyps*(*10*) *ConditionalNodeNew.hyps*(*9*) *fresh-ids*
by *presburger*
    then have *kind-eq*: ∀ *n′* . *n′ ∉ new ⟶ kind g4 n′ = kind g′ n′*
    by (*metis ConditionalNodeNew.hyps*(*10*) *add-node-as-set equalityE local.new-def*
not-excluded-keep-type not-in-g)
    from *unchanged* **have** *stamp-eq*: ∀ *n′ ∈ ids g* . *n′ ∉ new ⟶ stamp g4 n′ =*
stamp g′ n′
      using *not-excluded-keep-type new-def new*
      by (*metis ConditionalNodeNew.hyps*(*1*) *ConditionalNodeNew.hyps*(*10*) *Condi-*
tionalNodeNew.hyps(*3*) *ConditionalNodeNew.hyps*(*5*) *add-node-as-set unrep-preserves-contains*)
    have *max-g4*: *maximal-sharing g4*
      using *ConditionalNodeNew.hyps*(*1*) *ConditionalNodeNew.hyps*(*2*) *Condition-*
alNodeNew.hyps(*3*) *ConditionalNodeNew.hyps*(*4*) *ConditionalNodeNew.hyps*(*6*) *Con-*
ditionalNodeNew.prems(*1*) *ConditionalNodeNew.prems*(*2*) *unrep-preserves-closure*
by *blast*
    show *?case* **unfolding** *maximal-sharing* **apply** (*rule allI*; *rule allI*; *rule impI*)
      using *max-g4* **unfolding** *maximal-sharing* **apply** *auto*
      proof −
      fix n_1 n_2 *e*
      assume *1*: ∀ n_1 n_2.
          n_1 ∈ *true-ids g4* ∧ n_2 ∈ *true-ids g4* ⟶
          (∃ *e*. (*g4 ⊢ n_1 ≃ e*) ∧ (*g4 ⊢ n_2 ≃ e*) ∧ *stamp g4 n_1 = stamp g4 n_2*) ⟶
n_1 = n_2
      assume n_1 ∈ *true-ids g′*
      assume n_2 ∈ *true-ids g′*
      show *g′ ⊢ n_1 ≃ e ⟹ g′ ⊢ n_2 ≃ e ⟹ stamp g′ n_1 = stamp g′ n_2 ⟹ n_1 =*
n_2
      proof (*cases n_1 ∈ true-ids g4*)
       case *n1*: *True*

133

then show $g' \vdash n_1 \simeq e \implies g' \vdash n_2 \simeq e \implies stamp\ g'\ n_1 = stamp\ g'\ n_2$
$\implies n_1 = n_2$
  proof (*cases $n_2 \in$ true-ids g4*)
    case *n2*: *True*
    assume *n1rep'*: $g' \vdash n_1 \simeq e$
    assume *n2rep'*: $g' \vdash n_2 \simeq e$
    assume *stamp $g'\ n_1 = stamp\ g'\ n_2$*
    have *n1rep*: $g4 \vdash n_1 \simeq e$
      using *n1rep' kind-eq stamp-eq new-def add-preserves-rep*
     using *ConditionalNodeNew.prems*(*1*) *IRGraph.true-ids-def n1 unchanged*
      by (*metis* (*mono-tags, lifting*) *ConditionalNodeNew.hyps*(*1*) *ConditionalNodeNew.hyps*(*3*) *ConditionalNodeNew.hyps*(*5*) *DiffE unrep-preserves-closure*)
    have *n2rep*: $g4 \vdash n_2 \simeq e$
      using *n2rep' kind-eq stamp-eq new-def add-preserves-rep*
     using *ConditionalNodeNew.prems*(*1*) *IRGraph.true-ids-def n2 unchanged*
      by (*metis* (*no-types, lifting*) *ConditionalNodeNew.hyps*(*1*) *ConditionalNodeNew.hyps*(*3*) *ConditionalNodeNew.hyps*(*5*) *DiffE unrep-preserves-closure*)
    have *stamp g4 $n_1 = stamp\ g4\ n_2$*
      by (*metis ConditionalNodeNew.hyps*(*10*) *ConditionalNodeNew.hyps*(*9*)
‹*stamp $g'\ n_1 = stamp\ g'\ n_2$*› *fresh-ids fresh-node-subset n1rep n2rep subset-stamp*)
    then show *?thesis* **using** *1*
      using *n1 n2*
      using *n1rep n2rep* **by** *blast*
  next
    case *n2*: *False*
    assume *n1rep'*: $g' \vdash n_1 \simeq e$
    assume *n2rep'*: $g' \vdash n_2 \simeq e$
    assume *stmp*: *stamp $g'\ n_1 = stamp\ g'\ n_2$*
    have *n2-def*: $n_2 = n$
      using ‹*$n_2 \in$ true-ids g'*› *dom n2* **by** *auto*
    have *n1rep*: $g4 \vdash n_1 \simeq ConditionalExpr\ ce\ te\ fe$
    by (*metis* (*no-types, lifting*) *ConditionalNodeNew.hyps*(*1*) *ConditionalNodeNew.hyps*(*3*) *ConditionalNodeNew.hyps*(*5*) *ConditionalNodeNew.prems*(*1*) *Diff-iff IRGraph.true-ids-def add-preserves-rep n1 n1rep' n2-def n2rep' repDet repn unchanged unrep-preserves-closure*)
    then have *n1in*: $n_1 \in ids\ g4$
      using *no-encoding* **by** *metis*

    have *rep*: $(g4 \vdash c \simeq ce) \wedge (g4 \vdash t \simeq te) \wedge (g4 \vdash f \simeq fe)$
      by (*meson ConditionalNodeNew.hyps*(*1*) *ConditionalNodeNew.hyps*(*3*) *ConditionalNodeNew.hyps*(*5*) *subset-implies-evals term-graph-reconstruction*)
    have *not-ref*: $\neg(\exists\, n'.\ kind\ g4\ n_1 = RefNode\ n')$
      using *TreeToGraphThms.true-ids-def n1* **by** *fastforce*
    then have *kind g4 $n_1 = ConditionalNode\ c\ t\ f$*
      using *conditional-rep-kind*
      using *local.rep n1rep* **by** *presburger*
    then show *?thesis*
      using *find-none ConditionalNodeNew.hyps*(*8*) *n1in*
      by (*metis ConditionalNodeNew.hyps*(*10*) *ConditionalNodeNew.hyps*(*9*)

‹*stamp g′ n = s′*› *fresh-ids fresh-node-subset n1rep n2-def stmp subset-stamp*)
    qed
  next
   case *n1*: *False*
   then show $g′ \vdash n_1 \simeq e \implies g′ \vdash n_2 \simeq e \implies stamp\ g′\ n_1 = stamp\ g′\ n_2 \implies n_1 = n_2$

    proof (*cases* $n_2 \in$ *true-ids g4*)
     case *n2*: *True*
     assume *n1rep′*: $g′ \vdash n_1 \simeq e$
     assume *n2rep′*: $g′ \vdash n_2 \simeq e$
     assume $stamp\ g′\ n_1 = stamp\ g′\ n_2$
     have *new-n1*: $n_1 = n$
      using ‹$n_1 \in$ *true-ids g*› *dom n1* **by** *auto*
     then have *ne*: $n_1 \notin ids\ g4$
      using *new n1*
      using *ConditionalNodeNew.hyps*(*9*) *fresh-ids* **by** *blast*
     have *unrep-cond*: $g4 \vdash n_2 \simeq ConditionalExpr\ ce\ te\ fe$
      using *n1rep′ kind-eq stamp-eq new-def add-preserves-rep*
      using *ConditionalNodeNew.prems*(*1*) *IRGraph.true-ids-def n2 unchanged*
      by (*metis* (*no-types, lifting*) *ConditionalNodeNew.hyps*(*1*) *ConditionalNodeNew.hyps*(*3*) *ConditionalNodeNew.hyps*(*5*) *DiffD1 n2rep′ new-n1 repDet repn unrep-preserves-closure*)
      have *rep*: $(g4 \vdash c \simeq ce) \land (g4 \vdash t \simeq te) \land (g4 \vdash f \simeq fe)$
       by (*meson ConditionalNodeNew.hyps*(*1*) *ConditionalNodeNew.hyps*(*3*) *ConditionalNodeNew.hyps*(*5*) *subset-implies-evals term-graph-reconstruction*)
      have *not-ref*: $\neg(\exists n′.\ kind\ g4\ n_2 = RefNode\ n′)$
       using *TreeToGraphThms.true-ids-def n2* **by** *fastforce*
      then have $kind\ g4\ n_2 = ConditionalNode\ c\ t\ f$
       using *conditional-rep-kind*
       using *local.rep unrep-cond* **by** *presburger*
      then show *?thesis* **using** *find-none ConditionalNodeNew.hyps*(*8*)
       by (*metis ConditionalNodeNew.hyps*(*10*) ‹*stamp g′ n = s′*› ‹*stamp g′ n_1 = stamp g′ n_2*› *encodes-contains fresh-node-subset ne new-n1 not-in-g subset-stamp unrep-cond*)
    next
     case *n2*: *False*
     assume *n1rep′*: $g′ \vdash n_1 \simeq e$
     assume *n2rep′*: $g′ \vdash n_2 \simeq e$
     assume $stamp\ g′\ n_1 = stamp\ g′\ n_2$
     have $n_1 = n \land n_2 = n$
      using ‹$n_1 \in$ *true-ids g*› *dom n1*
      using ‹$n_2 \in$ *true-ids g*› *n2*
      by *simp*
     then show *?thesis*
      by *simp*
    qed
   qed
  qed
 next

case (*UnaryNodeSame g xe g2 x s′ op n*)
  then show *?case* **by** *blast*
next
  case (*UnaryNodeNew g xe g2 x s′ op n g′*)
  then have *k*: *kind g′ n = unary-node op x*
    using *find-new-kind*
    by (*metis add-node-lookup fresh-ids ids-some*)
  have *stamp g′ n = s′*
    by (*metis UnaryNodeNew.hyps*(*6*) *empty-iff find-new-stamp ids-some insertI1*
k not-in-g-inputs unary-inputs)
  then have *repn*: $g′ \vdash n \simeq$ *UnaryExpr op xe*
    using *k*
  using *UnaryNodeNew.hyps*(*1*) *UnaryNodeNew.hyps*(*3*) *UnaryNodeNew.hyps*(*4*)
UnaryNodeNew.hyps(*5*) *UnaryNodeNew.hyps*(*6*) *term-graph-reconstruction unrep.UnaryNodeNew*
by *blast*
  from *ConstantNodeNew* **have** ¬(*is-RefNode* (*unary-node op x*)) ∧ *unary-node*
op x ≠ *NoNode*
    by (*cases op*; *auto*)
  then have *dom*: *true-ids g′ = true-ids g2* ∪ {*n*}
  using *UnaryNodeNew.hyps*(*5*) *UnaryNodeNew.hyps*(*6*) *fresh-ids true-ids-add-update*
by *presburger*
  have *new*: *n* ∉ *ids g*
    using *fresh-ids*
  by (*meson UnaryNodeNew.hyps*(*1*) *UnaryNodeNew.hyps*(*5*) *unrep-preserves-contains*)
  obtain *new* **where** *new = true-ids g′ − true-ids g2*
    by *simp*
  then have *new-def*: *new* = {*n*}
    using *dom*
    by (*metis Diff-cancel Diff-iff Un-insert-right UnaryNodeNew.hyps*(*5*) *fresh-ids*
insert-Diff-if sup-bot.right-neutral true-ids)
  then have *unchanged*: (*new* ⊴ *as-set g′*) = *as-set g2*
    using *new add-node-as-set-eq*
    using *UnaryNodeNew.hyps*(*5*) *UnaryNodeNew.hyps*(*6*) *fresh-ids* **by** *presburger*
  then have *kind-eq*: ∀ *n′* . *n′* ∉ *new* ⟶ *kind g2 n′ = kind g′ n′*
     by (*metis UnaryNodeNew.hyps*(*6*) *add-node-as-set equalityD1 local.new-def*
not-excluded-keep-type not-in-g)
   from *unchanged* **have** *stamp-eq*: ∀ *n′* ∈ *ids g* . *n′* ∉ *new* ⟶ *stamp g2 n′* =
stamp g′ n′
    using *not-excluded-keep-type new-def new*
     by (*metis UnaryNodeNew.hyps*(*1*) *UnaryNodeNew.hyps*(*6*) *add-node-as-set*
unrep-preserves-contains)
  have *max-g2*: *maximal-sharing g2*
    by (*simp add*: *UnaryNodeNew.hyps*(*2*) *UnaryNodeNew.prems*(*1*) *UnaryNode-*
New.prems(*2*))
  show *?case* **unfolding** *maximal-sharing* **apply** (*rule allI*; *rule allI*; *rule impI*)
    using *max-g2* **unfolding** *maximal-sharing* **apply** *auto*
    proof −
    fix n_1 n_2 *e*
    assume *1*: ∀ n_1 n_2.

$n_1 \in$ *true-ids g2* $\wedge$ $n_2 \in$ *true-ids g2* $\longrightarrow$

$(\exists\, e.\ (g2 \vdash n_1 \simeq e) \wedge (g2 \vdash n_2 \simeq e) \wedge$ *stamp g2* $n_1 =$ *stamp g2* $n_2) \longrightarrow$

$n_1 = n_2$

assume $n_1 \in$ *true-ids g$'$*

assume $n_2 \in$ *true-ids g$'$*

show $g' \vdash n_1 \simeq e \Longrightarrow g' \vdash n_2 \simeq e \Longrightarrow$ *stamp g$'$* $n_1 =$ *stamp g$'$* $n_2 \Longrightarrow n_1 = n_2$

proof (*cases* $n_1 \in$ *true-ids g2*)

  case *n1*: *True*

  then show $g' \vdash n_1 \simeq e \Longrightarrow g' \vdash n_2 \simeq e \Longrightarrow$ *stamp g$'$* $n_1 =$ *stamp g$'$* $n_2 \Longrightarrow n_1 = n_2$

  proof (*cases* $n_2 \in$ *true-ids g2*)

    case *n2*: *True*

    assume *n1rep$'$*: $g' \vdash n_1 \simeq e$

    assume *n2rep$'$*: $g' \vdash n_2 \simeq e$

    assume *stamp g$'$* $n_1 =$ *stamp g$'$* n_2

    have *n1rep*: $g2 \vdash n_1 \simeq e$

      using *n1rep$'$ kind-eq stamp-eq new-def add-preserves-rep*

      using *Diff-iff IRGraph.true-ids-def UnaryNodeNew.hyps*(*1*) *UnaryNode-New.prems*(*1*) *n1 unchanged unrep-preserves-closure* **by** *auto*

    have *n2rep*: $g2 \vdash n_2 \simeq e$

      using *n2rep$'$ kind-eq stamp-eq new-def add-preserves-rep*

        by (*metis* (*no-types, lifting*) *Diff-iff IRGraph.true-ids-def UnaryNode-New.hyps*(*1*) *UnaryNodeNew.prems*(*1*) *n2 unchanged unrep-preserves-closure*)

    have *stamp g2* $n_1 =$ *stamp g2* n_2

      by (*metis UnaryNodeNew.hyps*(*5*) *UnaryNodeNew.hyps*(*6*) ‹*stamp g$'$* $n_1 =$ *stamp g$'$* n_2› *fresh-ids fresh-node-subset n1rep n2rep subset-stamp*)

    then show *?thesis* **using** *1*

      using *n1 n2*

      using *n1rep n2rep* **by** *blast*

  next

    case *n2*: *False*

    assume *n1rep$'$*: $g' \vdash n_1 \simeq e$

    assume *n2rep$'$*: $g' \vdash n_2 \simeq e$

    assume *stamp g$'$* $n_1 =$ *stamp g$'$* n_2

    have *new-n2*: $n_2 = n$

      using ‹$n_2 \in$ *true-ids g$'$*› *dom n2* **by** *auto*

    then have *ne*: $n_2 \notin$ *ids g2*

      using *new n2*

      using *UnaryNodeNew.hyps*(*5*) *fresh-ids* **by** *blast*

    have *unrep-un*: $g2 \vdash n_1 \simeq$ *UnaryExpr op xe*

      using *n1rep$'$ kind-eq stamp-eq new-def add-preserves-rep*

        by (*metis* (*no-types, lifting*) *Diff-iff IRGraph.true-ids-def UnaryNode-New.hyps*(*1*) *UnaryNodeNew.prems*(*1*) *n1 n2rep$'$ new-n2 repDet repn unchanged unrep-preserves-closure*)

    have *rep*: $(g2 \vdash x \simeq xe)$

      using *UnaryNodeNew.hyps*(*1*) *term-graph-reconstruction* **by** *auto*

    have *not-ref*: $\neg(\exists\, n'.$ *kind g2* $n_1 =$ *RefNode* $n')$

      using *TreeToGraphThms.true-ids-def n1* **by** *force*

then have *kind g2 n_1 = unary-node op x*

using *unrep-un unary-rep-kind rep* **by** *simp*

then show *?thesis* **using** *find-none UnaryNodeNew.hyps(4)*

by (*metis UnaryNodeNew.hyps(6) ‹stamp g' n = s'› ‹stamp g' n_1 = stamp g' n_2› fresh-node-subset ne new-n2 no-encoding subset-stamp unrep-un*)

qed

next

case *n1: False*

then show $g' \vdash n_1 \simeq e \implies g' \vdash n_2 \simeq e \implies$ *stamp g' n_1 = stamp g' n_2* $\implies n_1 = n_2$

proof (*cases $n_2 \in$ true-ids g2*)

case *n2: True*

assume *n1rep': $g' \vdash n_1 \simeq e$*

assume *n2rep': $g' \vdash n_2 \simeq e$*

assume *stamp g' n_1 = stamp g' n_2*

have *new-n1: $n_1 = n$*

using *‹$n_1 \in$ true-ids g'› dom n1* **by** *auto*

then have *ne: $n_1 \notin$ ids g2*

using *new n1*

using *UnaryNodeNew.hyps(5) fresh-ids* **by** *blast*

have *unrep-un: $g2 \vdash n_2 \simeq$ UnaryExpr op xe*

using *n1rep' kind-eq stamp-eq new-def add-preserves-rep*

by (*metis (no-types, lifting) Diff-iff IRGraph.true-ids-def UnaryNodeNew.hyps(1) UnaryNodeNew.prems(1) n2 n2rep' new-n1 repDet repn unchanged unrep-preserves-closure*)

have *rep: ($g2 \vdash x \simeq xe$)*

using *UnaryNodeNew.hyps(1) term-graph-reconstruction* **by** *presburger*

have *not-ref: $\neg(\exists n'.$ kind g2 n_2 = RefNode $n')$*

using *TreeToGraphThms.true-ids-def n2* **by** *fastforce*

then have *kind g2 n_2 = unary-node op x*

using *unary-rep-kind*

using *local.rep unrep-un* **by** *presburger*

then show *?thesis* **using** *find-none UnaryNodeNew.hyps(4)*

by (*metis UnaryNodeNew.hyps(6) ‹stamp g' n = s'› ‹stamp g' n_1 = stamp g' n_2› fresh-node-subset ne new-n1 no-encoding subset-stamp unrep-un*)

next

case *n2: False*

assume *n1rep': $g' \vdash n_1 \simeq e$*

assume *n2rep': $g' \vdash n_2 \simeq e$*

assume *stamp g' n_1 = stamp g' n_2*

have $n_1 = n \wedge n_2 = n$

using *‹$n_1 \in$ true-ids g'› dom n1*

using *‹$n_2 \in$ true-ids g'› n2*

by *simp*

then show *?thesis*

by *simp*

qed

qed

138

qed
next
  case (*BinaryNodeSame g xe g2 x ye g3 y s' op n*)
  then show *?case*
    using *unrep-preserves-closure* **by** *blast*
next
  case (*BinaryNodeNew g xe g2 x ye g3 y s' op n g'*)
  then have *k*: *kind g' n = bin-node op x y*
    using *find-new-kind*
    by (*metis add-node-lookup fresh-ids ids-some*)
  have *stamp g' n = s'*
      by (*metis BinaryNodeNew.hyps*(*1*) *BinaryNodeNew.hyps*(*3*) *BinaryNode-New.hyps*(*5*) *BinaryNodeNew.hyps*(*6*) *BinaryNodeNew.hyps*(*7*) *BinaryNodeNew.hyps*(*8*) *find-new-stamp ids-some k unrep.BinaryNodeNew unrep-contains*)
  then have *repn*: *g' ⊢ n ≃ BinaryExpr op xe ye*
    using *k*
  using *BinaryNodeNew.hyps*(*1*) *BinaryNodeNew.hyps*(*3*) *BinaryNodeNew.hyps*(*5*) *BinaryNodeNew.hyps*(*6*) *BinaryNodeNew.hyps*(*7*) *BinaryNodeNew.hyps*(*8*) *term-graph-reconstruction unrep.BinaryNodeNew* **by** *blast*
  from *BinaryNodeNew* **have** ¬(*is-RefNode* (*bin-node op x y*)) ∧ *bin-node op x y ≠ NoNode*
    by (*cases op*; *auto*)
  then have *dom*: *true-ids g' = true-ids g3 ∪ {n}*
  using *BinaryNodeNew.hyps*(*7*) *BinaryNodeNew.hyps*(*8*) *fresh-ids true-ids-add-update*
by *presburger*
  have *new*: *n ∉ ids g*
    using *fresh-ids*
      by (*meson BinaryNodeNew.hyps*(*1*) *BinaryNodeNew.hyps*(*3*) *BinaryNode-New.hyps*(*7*) *unrep-preserves-contains*)
  obtain *new* **where** *new = true-ids g' − true-ids g3*
    by *simp*
  then have *new-def*: *new = {n}*
    using *dom*
   by (*metis BinaryNodeNew.hyps*(*7*) *Diff-cancel Diff-iff Un-insert-right fresh-ids insert-Diff-if sup-bot.right-neutral true-ids*)
  then have *unchanged*: (*new ⊴ as-set g'*) = *as-set g3*
    using *new add-node-as-set-eq*
  using *BinaryNodeNew.hyps*(*7*) *BinaryNodeNew.hyps*(*8*) *fresh-ids* **by** *presburger*
  then have *kind-eq*: ∀ *n'* . *n' ∉ new ⟶ kind g3 n' = kind g' n'*
    by (*metis BinaryNodeNew.hyps*(*8*) *add-node-as-set equalityD1 local.new-def not-excluded-keep-type not-in-g*)
   from *unchanged* **have** *stamp-eq*: ∀ *n' ∈ ids g* . *n' ∉ new ⟶ stamp g3 n' = stamp g' n'*
    using *not-excluded-keep-type new-def new*
      by (*metis BinaryNodeNew.hyps*(*1*) *BinaryNodeNew.hyps*(*3*) *BinaryNode-New.hyps*(*8*) *add-node-as-set unrep-preserves-contains*)
  have *max-g3*: *maximal-sharing g3*
  using *BinaryNodeNew.hyps*(*1*) *BinaryNodeNew.hyps*(*2*) *BinaryNodeNew.hyps*(*4*) *BinaryNodeNew.prems*(*1*) *BinaryNodeNew.prems*(*2*) *unrep-preserves-closure* **by** *blast*

139

show *?case* **unfolding** *maximal-sharing* **apply** (*rule allI*; *rule allI*; *rule impI*)
  using *max-g3* **unfolding** *maximal-sharing* **apply** *auto*
  proof −
  fix n_1 n_2 e
  assume *1*: $\forall\, n_1\ n_2.$
    $n_1 \in$ *true-ids g3* $\land$ $n_2 \in$ *true-ids g3* $\longrightarrow$
    $(\exists\, e.\ (g3 \vdash n_1 \simeq e) \land (g3 \vdash n_2 \simeq e) \land$ *stamp g3* $n_1 =$ *stamp g3* $n_2) \longrightarrow$
$n_1 = n_2$
  assume $n_1 \in$ *true-ids g′*
  assume $n_2 \in$ *true-ids g′*
  show $g′ \vdash n_1 \simeq e \Longrightarrow g′ \vdash n_2 \simeq e \Longrightarrow$ *stamp g′* $n_1 =$ *stamp g′* $n_2 \Longrightarrow n_1 =$
n_2

  proof (*cases* $n_1 \in$ *true-ids g3*)
    case *n1*: *True*
    then show $g′ \vdash n_1 \simeq e \Longrightarrow g′ \vdash n_2 \simeq e \Longrightarrow$ *stamp g′* $n_1 =$ *stamp g′* n_2
$\Longrightarrow n_1 = n_2$
    proof (*cases* $n_2 \in$ *true-ids g3*)
      case *n2*: *True*
      assume *n1rep′*: $g′ \vdash n_1 \simeq e$
      assume *n2rep′*: $g′ \vdash n_2 \simeq e$
      assume *stamp g′* $n_1 =$ *stamp g′* n_2
      have *n1rep*: $g3 \vdash n_1 \simeq e$
        using *n1rep′ kind-eq stamp-eq new-def add-preserves-rep*
          by (*metis* (*no-types, lifting*) *BinaryNodeNew.hyps*(*1*) *BinaryNode-*
New.hyps(*3*) *BinaryNodeNew.prems*(*1*) *Diff-iff IRGraph.true-ids-def n1 unchanged*
unrep-preserves-closure)
      have *n2rep*: $g3 \vdash n_2 \simeq e$
        using *n2rep′ kind-eq stamp-eq new-def add-preserves-rep*
        by (*metis BinaryNodeNew.hyps*(*1*) *BinaryNodeNew.hyps*(*3*) *BinaryNode-*
New.prems(*1*) *DiffE n2 true-ids unchanged unrep-preserves-closure*)
      have *stamp g3* $n_1 =$ *stamp g3* n_2
        by (*metis BinaryNodeNew.hyps*(*7*) *BinaryNodeNew.hyps*(*8*) ‹*stamp g′* n_1
$=$ *stamp g′* n_2› *fresh-ids fresh-node-subset n1rep n2rep subset-stamp*)
      then show *?thesis* **using** *1*
        using *n1 n2*
        using *n1rep n2rep* **by** *blast*
    next
      case *n2*: *False*
      assume *n1rep′*: $g′ \vdash n_1 \simeq e$
      assume *n2rep′*: $g′ \vdash n_2 \simeq e$
      assume *stamp g′* $n_1 =$ *stamp g′* n_2
      have *new-n2*: $n_2 = n$
        using ‹$n_2 \in$ *true-ids g′*› *dom n2* **by** *auto*
      then have *ne*: $n_2 \notin$ *ids g3*
        using *new n2*
        using *BinaryNodeNew.hyps*(*7*) *fresh-ids* **by** *presburger*
      have *unrep-bin*: $g3 \vdash n_1 \simeq$ *BinaryExpr op xe ye*
        using *n1rep′ kind-eq stamp-eq new-def add-preserves-rep*
      by (*metis BinaryNodeNew.hyps*(*1*) *BinaryNodeNew.hyps*(*3*) *BinaryNode-*

New.prems(*1*) *DiffE* ‹*new = true-ids g′ − true-ids g3*› *encodes-contains ids-some*
n1 n2rep′ new-n2 repDet repn unchanged unrep-preserves-closure)
        have *rep*: $(g3 \vdash x \simeq xe) \land (g3 \vdash y \simeq ye)$
     by (*meson BinaryNodeNew.hyps*(*1*) *BinaryNodeNew.hyps*(*3*) *term-graph-reconstruction*
unrep-contains unrep-unchanged)
        have *not-ref*: $\neg(\exists n'. \text{ kind } g3 \text{ } n_1 = \text{RefNode } n')$
      using *TreeToGraphThms.true-ids-def n1* **by** *force*
     then have *kind g3* n_1 = *bin-node op x y*
      using *unrep-bin binary-rep-kind rep* **by** *simp*
     then show *?thesis* **using** *find-none BinaryNodeNew.hyps*(*6*)
       by (*metis BinaryNodeNew.hyps*(*8*) ‹*stamp g′ n = s′*› ‹*stamp g′* n_1 =
stamp g′ n_2› *fresh-node-subset ne new-n2 no-encoding subset-stamp unrep-bin*)
    qed
   next
    case *n1: False*
    then show $g′ \vdash n_1 \simeq e \implies g′ \vdash n_2 \simeq e \implies \text{stamp } g′ \text{ } n_1 = \text{stamp } g′ \text{ } n_2$
$\implies n_1 = n_2$
    proof (*cases* $n_2 \in$ *true-ids g3*)
     case *n2: True*
     assume *n1rep′*: $g′ \vdash n_1 \simeq e$
     assume *n2rep′*: $g′ \vdash n_2 \simeq e$
     assume *stamp g′* n_1 = *stamp g′* n_2
     have *new-n1*: $n_1 = n$
      using ‹$n_1 \in$ *true-ids g′*› *dom n1* **by** *auto*
     then have *ne*: $n_1 \notin$ *ids g3*
      using *new n1*
      using *BinaryNodeNew.hyps*(*7*) *fresh-ids* **by** *blast*
     have *unrep-bin*: $g3 \vdash n_2 \simeq$ *BinaryExpr op xe ye*
      using *n1rep′ kind-eq stamp-eq new-def add-preserves-rep*
        by (*metis* (*mono-tags, lifting*) *BinaryNodeNew.hyps*(*1*) *BinaryN-*
odeNew.hyps(*3*) *BinaryNodeNew.prems*(*1*) *Diff-iff IRGraph.true-ids-def n2 n2rep′*
new-n1 repDet repn unchanged unrep-preserves-closure)
      have *rep*: $(g3 \vdash x \simeq xe) \land (g3 \vdash y \simeq ye)$
     using *BinaryNodeNew.hyps*(*1*) *BinaryNodeNew.hyps*(*3*) *term-graph-reconstruction*
unrep-contains unrep-unchanged **by** *blast*
      have *not-ref*: $\neg(\exists n'. \text{ kind } g3 \text{ } n_2 = \text{RefNode } n')$
      using *TreeToGraphThms.true-ids-def n2* **by** *fastforce*
     then have *kind g3* n_2 = *bin-node op x y*
      using *unrep-bin binary-rep-kind rep* **by** *simp*
     then show *?thesis* **using** *find-none BinaryNodeNew.hyps*(*6*)
       by (*metis BinaryNodeNew.hyps*(*8*) ‹*stamp g′ n = s′*› ‹*stamp g′* n_1 =
stamp g′ n_2› *fresh-node-subset ne new-n1 no-encoding subset-stamp unrep-bin*)
    next
     case *n2: False*
     assume *n1rep′*: $g′ \vdash n_1 \simeq e$
     assume *n2rep′*: $g′ \vdash n_2 \simeq e$
     assume *stamp g′* n_1 = *stamp g′* n_2
     have $n_1 = n \land n_2 = n$
      using ‹$n_1 \in$ *true-ids g′*› *dom n1*

using ‹n_2 ∈ *true-ids* g'› *n2*
              by *simp*
            then show *?thesis*
              by *simp*
        qed
      qed
    qed
  next
    case (*AllLeafNodes g n s*)
    then show *?case* **by** *blast*
  qed

end

8 Control-flow Semantics

theory *IRStepObj*
  imports
    TreeToGraph
begin

8.1 Object Heap

The heap model we introduce maps field references to object instances to runtime values. We use the H[f][p] heap representation. See $\backslash cite\{heap-reps-2011\}$.

We also introduce the DynamicHeap type which allocates new object references sequentially storing the next free object reference as 'Free'.

---

heapdef

type-synonym $('a, \,'b)$ *Heap* $= \,'a \Rightarrow \,'b \Rightarrow$ *Value*
type-synonym *Free* $=$ *nat*
type-synonym $('a, \,'b)$ *DynamicHeap* $= ('a, \,'b)$ *Heap* $\times$ *Free*

fun *h-load-field* :: $'a \Rightarrow \,'b \Rightarrow ('a, \,'b)$ *DynamicHeap* $\Rightarrow$ *Value* **where**
  h-load-field f r (h, n) $= h \, f \, r$

fun *h-store-field* :: $'a \Rightarrow \,'b \Rightarrow$ *Value* $\Rightarrow ('a, \,'b)$ *DynamicHeap* $\Rightarrow ('a, \,'b)$
DynamicHeap **where**
  h-store-field f r v (h, n) $= (h(f := ((h \, f)(r := v))), \, n)$

fun *h-new-inst* :: $('a, \,'b)$ *DynamicHeap* $\Rightarrow ('a, \,'b)$ *DynamicHeap* $\times$ *Value*
where
  h-new-inst (h, n) $= ((h,n+1), \, (ObjRef \, (Some \, n)))$

type-synonym *FieldRefHeap* $=$ (*string, objref*) *DynamicHeap*

---

definition new-heap :: $('a, \,'b)$ *DynamicHeap* **where**

new-heap = ((λf. λp. UndefVal), 0)

8.2   Intraprocedural Semantics

fun *find-index* :: *′a ⇒ ′a list ⇒ nat* **where**
  find-index - [] = 0 |
  find-index v (x # xs) = (if (x=v) then 0 else find-index v xs + 1)

fun *phi-list* :: *IRGraph ⇒ ID ⇒ ID list* **where**
  phi-list g n =
    (filter (λx.(is-PhiNode (kind g x)))
      (sorted-list-of-set (usages g n)))

fun *input-index* :: *IRGraph ⇒ ID ⇒ ID ⇒ nat* **where**
  input-index g n n′ = find-index n′ (inputs-of (kind g n))

fun *phi-inputs* :: *IRGraph ⇒ nat ⇒ ID list ⇒ ID list* **where**
  phi-inputs g i nodes = (map (λn. (inputs-of (kind g n))!(i + 1)) nodes)

fun *set-phis* :: *ID list ⇒ Value list ⇒ MapState ⇒ MapState* **where**
  set-phis [] [] m = m |
  set-phis (n # xs) (v # vs) m = (set-phis xs vs (m(n := v))) |
  set-phis [] (v # vs) m = m |
  set-phis (x # xs) [] m = m

Intraprocedural semantics are given as a small-step semantics.

Within the context of a graph, the configuration triple, (ID, MethodState, Heap), is related to the subsequent configuration.

inductive *step* :: *IRGraph ⇒ Params ⇒ (ID × MapState × FieldRefHeap) ⇒ (ID × MapState × FieldRefHeap) ⇒ bool*
  (-, - ⊢ - → - 55) **for** *g p* **where**

  SequentialNode:
  ⟦*is-sequential-node (kind g nid);*
    nid′ = (successors-of (kind g nid))!0⟧
    ⟹ g, p ⊢ (nid, m, h) → (nid′, m, h) |

  IfNode:
  ⟦*kind g nid = (IfNode cond tb fb);*
    g ⊢ cond ≃ condE;
    [m, p] ⊢ condE ↦ val;
    nid′ = (if val-to-bool val then tb else fb)⟧
    ⟹ g, p ⊢ (nid, m, h) → (nid′, m, h) |

  EndNodes:
  ⟦*is-AbstractEndNode (kind g nid);*
    merge = any-usage g nid;
    is-AbstractMergeNode (kind g merge);

$i = \textit{find-index nid (inputs-of (kind g merge))};$
$\textit{phis} = (\textit{phi-list g merge});$
$\textit{inps} = (\textit{phi-inputs g i phis});$
$g \vdash \textit{inps} \simeq_L \textit{inpsE};$
$[m,\, p] \vdash \textit{inpsE} \mapsto_L \textit{vs};$

$m' = \textit{set-phis phis vs m}]\!]$
$\implies g,\, p \vdash (\textit{nid},\, m,\, h) \rightarrow (\textit{merge},\, m',\, h) \mid$

NewInstanceNode:
$[\![\textit{kind g nid} = (\textit{NewInstanceNode nid f obj nid}');$
$\quad (h',\, \textit{ref}) = \textit{h-new-inst h};$
$\quad m' = m(\textit{nid} := \textit{ref})]\!]$
$\implies g,\, p \vdash (\textit{nid},\, m,\, h) \rightarrow (\textit{nid}',\, m',\, h') \mid$

LoadFieldNode:
$[\![\textit{kind g nid} = (\textit{LoadFieldNode nid f (Some obj) nid}');$
$\quad g \vdash \textit{obj} \simeq \textit{objE};$
$\quad [m,\, p] \vdash \textit{objE} \mapsto \textit{ObjRef ref};$
$\quad \textit{h-load-field f ref h} = v;$
$\quad m' = m(\textit{nid} := v)]\!]$
$\implies g,\, p \vdash (\textit{nid},\, m,\, h) \rightarrow (\textit{nid}',\, m',\, h) \mid$

SignedDivNode:
$[\![\textit{kind g nid} = (\textit{SignedDivNode nid x y zero sb nxt});$
$\quad g \vdash x \simeq \textit{xe};$
$\quad g \vdash y \simeq \textit{ye};$
$\quad [m,\, p] \vdash \textit{xe} \mapsto \textit{v1};$
$\quad [m,\, p] \vdash \textit{ye} \mapsto \textit{v2};$
$\quad v = (\textit{intval-div v1 v2});$
$\quad m' = m(\textit{nid} := v)]\!]$
$\implies g,\, p \vdash (\textit{nid},\, m,\, h) \rightarrow (\textit{nxt},\, m',\, h) \mid$

SignedRemNode:
$[\![\textit{kind g nid} = (\textit{SignedRemNode nid x y zero sb nxt});$
$\quad g \vdash x \simeq \textit{xe};$
$\quad g \vdash y \simeq \textit{ye};$
$\quad [m,\, p] \vdash \textit{xe} \mapsto \textit{v1};$
$\quad [m,\, p] \vdash \textit{ye} \mapsto \textit{v2};$
$\quad v = (\textit{intval-mod v1 v2});$
$\quad m' = m(\textit{nid} := v)]\!]$
$\implies g,\, p \vdash (\textit{nid},\, m,\, h) \rightarrow (\textit{nxt},\, m',\, h) \mid$

StaticLoadFieldNode:
$[\![\textit{kind g nid} = (\textit{LoadFieldNode nid f None nid}');$
$\quad \textit{h-load-field f None h} = v;$
$\quad m' = m(\textit{nid} := v)]\!]$
$\implies g,\, p \vdash (\textit{nid},\, m,\, h) \rightarrow (\textit{nid}',\, m',\, h) \mid$

StoreFieldNode:
  $\llbracket$*kind g nid* = (*StoreFieldNode nid f newval - (Some obj) nid'*);
    $g \vdash newval \simeq newvalE$;
    $g \vdash obj \simeq objE$;
    $[m, p] \vdash newvalE \mapsto val$;
    $[m, p] \vdash objE \mapsto ObjRef\ ref$;
    $h' = h\text{-store-field}\ f\ ref\ val\ h$;
    $m' = m(nid := val)\rrbracket$
  $\implies g, p \vdash (nid, m, h) \to (nid', m', h')$ |

StaticStoreFieldNode:
  $\llbracket$*kind g nid* = (*StoreFieldNode nid f newval - None nid'*);
    $g \vdash newval \simeq newvalE$;
    $[m, p] \vdash newvalE \mapsto val$;
    $h' = h\text{-store-field}\ f\ None\ val\ h$;
    $m' = m(nid := val)\rrbracket$
  $\implies g, p \vdash (nid, m, h) \to (nid', m', h')$

code-pred (*modes*: $i \Rightarrow i \Rightarrow i * i * i \Rightarrow o * o * o \Rightarrow bool$) *step* **.**

8.3   Interprocedural Semantics

type-synonym *Signature = string*
type-synonym *Program = Signature $\rightharpoonup$ IRGraph*

inductive *step-top :: Program $\Rightarrow$ (IRGraph $\times$ ID $\times$ MapState $\times$ Params) list $\times$ FieldRefHeap $\Rightarrow$ (IRGraph $\times$ ID $\times$ MapState $\times$ Params) list $\times$ FieldRefHeap $\Rightarrow$ bool*
  $(\text{-} \vdash \text{-} \longrightarrow \text{-} 55)$
  for *P* **where**

Lift:
$\llbracket g, p \vdash (nid, m, h) \to (nid', m', h')\rrbracket$
  $\implies P \vdash ((g,nid,m,p)\#stk, h) \longrightarrow ((g,nid',m',p)\#stk, h')$ |

InvokeNodeStep:
$\llbracket$*is-Invoke* (*kind g nid*);

  callTarget = ir-callTarget (*kind g nid*);
  kind g callTarget = (*MethodCallTargetNode targetMethod arguments*);
  Some targetGraph = P targetMethod;
  $m' = new\text{-}map\text{-}state$;
  $g \vdash arguments \simeq_L argsE$;
  $[m, p] \vdash argsE \mapsto_L p'\rrbracket$
  $\implies P \vdash ((g,nid,m,p)\#stk, h) \longrightarrow ((targetGraph,0,m',p')\#(g,nid,m,p)\#stk, h)$
|

145

ReturnNode:
⟦*kind g nid = (ReturnNode (Some expr) -);*
  $g \vdash expr \simeq e$;
  $[m, p] \vdash e \mapsto v$;

  $cm' = cm(cnid := v)$;
  $cnid' = (successors\text{-}of (kind \ cg \ cnid))!0$⟧
  $\implies P \vdash ((g,nid,m,p)\#(cg,cnid,cm,cp)\#stk, h) \longrightarrow ((cg,cnid',cm',cp)\#stk, h) \mid$

ReturnNodeVoid:
⟦*kind g nid = (ReturnNode None -);*
  $cm' = cm(cnid := (ObjRef (Some (2048))))$;

  $cnid' = (successors\text{-}of (kind \ cg \ cnid))!0$⟧
  $\implies P \vdash ((g,nid,m,p)\#(cg,cnid,cm,cp)\#stk, h) \longrightarrow ((cg,cnid',cm',cp)\#stk, h) \mid$

UnwindNode:
⟦*kind g nid = (UnwindNode exception);*

  $g \vdash exception \simeq exceptionE$;
  $[m, p] \vdash exceptionE \mapsto e$;

  kind cg cnid = (InvokeWithExceptionNode - - - - - - exEdge);

  $cm' = cm(cnid := e)$⟧
  $\implies P \vdash ((g,nid,m,p)\#(cg,cnid,cm,cp)\#stk, h) \longrightarrow ((cg,exEdge,cm',cp)\#stk, h)$

code-pred (*modes*: $i \Rightarrow i \Rightarrow o \Rightarrow bool$) *step-top* .

8.4   Big-step Execution

type-synonym *Trace* = $(IRGraph \times ID \times MapState \times Params)$ *list*

fun *has-return* :: *MapState* $\Rightarrow$ *bool* **where**
  has-return m = $(m \ 0 \neq UndefVal)$

inductive *exec* :: *Program*
    $\Rightarrow (IRGraph \times ID \times MapState \times Params)$ *list* $\times$ *FieldRefHeap*
    $\Rightarrow$ *Trace*
    $\Rightarrow (IRGraph \times ID \times MapState \times Params)$ *list* $\times$ *FieldRefHeap*
    $\Rightarrow$ *Trace*
    $\Rightarrow$ *bool*
  (- $\vdash$ - | - $\longrightarrow*$ - | -)
  for *P*
  where
  ⟦$P \vdash (((g,nid,m,p)\#xs),h) \longrightarrow (((g',nid',m',p')\#ys),h')$;
    $\neg(has\text{-}return \ m')$;

    $l' = (l \ @ \ [(g,nid,m,p)])$;

146

exec P (((g′,nid′,m′,p′)#ys),h′) l′ next-state l″⟧
 ⟹ *exec P (((g,nid,m,p)#xs),h) l next-state l″*

⟦$P \vdash$ *(((g,nid,m,p)#xs),h)* ⟶ *(((g′,nid′,m′,p′)#ys),h′)*;
 has-return m′;

 l′ = (l @ [(g,nid,m,p)])⟧
 ⟹ *exec P (((g,nid,m,p)#xs),h) l (((g′,nid′,m′,p′)#ys),h′) l′*
code-pred (*modes: i ⇒ i ⇒ i ⇒ o ⇒ o ⇒ bool as Exec) exec* **.**

inductive *exec-debug :: Program*
 ⇒ *(IRGraph × ID × MapState × Params) list × FieldRefHeap*
 ⇒ *nat*
 ⇒ *(IRGraph × ID × MapState × Params) list × FieldRefHeap*
 ⇒ *bool*
 (-⊢-⟶∗-∗ -)
 where
 ⟦*n > 0*;
  $p \vdash s$ ⟶ *s′*;
  exec-debug p s′ (n − 1) s″⟧
  ⟹ *exec-debug p s n s″* |

 ⟦*n = 0*⟧
  ⟹ *exec-debug p s n s*
code-pred (*modes: i ⇒ i ⇒ i ⇒ o ⇒ bool) exec-debug* **.**

8.4.1 Heap Testing

definition *p3:: Params* **where**
 p3 = [IntVal32 3]

values {*(prod.fst(prod.snd (prod.snd (hd (prod.fst res)))))) 0*
 | *res. (λx . Some eg2-sq)* ⊢ *([(eg2-sq,0,new-map-state,p3), (eg2-sq,0,new-map-state,p3)],*
new-heap) ⟶∗*2*∗ *res*}

definition *field-sq :: string* **where**
 field-sq = ″sq″

definition *eg3-sq :: IRGraph* **where**
 eg3-sq = irgraph [
  (0, StartNode None 4, VoidStamp),
  (1, ParameterNode 0, default-stamp),
  (3, MulNode 1 1, default-stamp),
  (4, StoreFieldNode 4 field-sq 3 None None 5, VoidStamp),
  (5, ReturnNode (Some 3) None, default-stamp)

   ]

values {*h-load-field field-sq None* (*prod.snd res*)
       | *res.* (*λx. Some eg3-sq*) ⊢ ([(*eg3-sq, 0, new-map-state, p3*), (*eg3-sq, 0, new-map-state, p3*)], *new-heap*) →∗*3*∗ *res*}

definition *eg4-sq* :: *IRGraph* **where**
  eg4-sq = irgraph [
   (*0, StartNode None 4, VoidStamp*),
   (*1, ParameterNode 0, default-stamp*),
   (*3, MulNode 1 1, default-stamp*),
   (*4, NewInstanceNode 4 ''obj-class'' None 5, ObjectStamp ''obj-class'' True True True*),
   (*5, StoreFieldNode 5 field-sq 3 None* (*Some 4*) *6, VoidStamp*),
   (*6, ReturnNode* (*Some 3*) *None, default-stamp*)
  ]

values {*h-load-field field-sq* (*Some 0*) (*prod.snd res*) | *res.*
       (*λx. Some eg4-sq*) ⊢ ([(*eg4-sq, 0, new-map-state, p3*), (*eg4-sq, 0, new-map-state, p3*)], *new-heap*) →∗*4*∗ *res*}

end

8.5   Control-flow Semantics Theorems

theory *IRStepThms*
  imports
   IRStepObj
   TreeToGraphThms
begin

We prove that within the same graph, a configuration triple will always transition to the same subsequent configuration. Therefore, our step semantics is deterministic.

8.5.1   Control-flow Step is Deterministic

theorem *stepDet*:
  (*g, p* ⊢ (*nid,m,h*) → *next*) ⟹
  (∀ *next'.* ((*g, p* ⊢ (*nid,m,h*) → *next'*) ⟶ *next = next'*))
proof (*induction rule*: *step.induct*)
  case (*SequentialNode nid next m h*)
  have *notif*: ¬(*is-IfNode* (*kind g nid*))
   using *SequentialNode.hyps*(*1*) *is-sequential-node.simps*
   by (*metis is-IfNode-def*)
  have *notend*: ¬(*is-AbstractEndNode* (*kind g nid*))
   using *SequentialNode.hyps*(*1*) *is-sequential-node.simps*

by (*metis is-AbstractEndNode.simps is-EndNode.elims*(*2*) *is-LoopEndNode-def*)
  have *notnew*: ¬(*is-NewInstanceNode* (*kind g nid*))
    using *SequentialNode.hyps*(*1*) *is-sequential-node.simps*
    by (*metis is-NewInstanceNode-def*)
  have *notload*: ¬(*is-LoadFieldNode* (*kind g nid*))
    using *SequentialNode.hyps*(*1*) *is-sequential-node.simps*
    by (*metis is-LoadFieldNode-def*)
  have *notstore*: ¬(*is-StoreFieldNode* (*kind g nid*))
    using *SequentialNode.hyps*(*1*) *is-sequential-node.simps*
    by (*metis is-StoreFieldNode-def*)
  have *notdivrem*: ¬(*is-IntegerDivRemNode* (*kind g nid*))
     using *SequentialNode.hyps*(*1*) *is-sequential-node.simps is-SignedDivNode-def*
is-SignedRemNode-def
    by (*metis is-IntegerDivRemNode.simps*)
  from *notif notend notnew notload notstore notdivrem*
  show *?case* **using** *SequentialNode step.cases*
  by (*smt* (*z3*) *IRNode.disc*(*1028*) *IRNode.disc*(*2270*) *IRNode.discI*(*31*) *Pair-inject*
is-sequential-node.simps(*18*) *is-sequential-node.simps*(*43*) *is-sequential-node.simps*(*44*))
next
  case (*IfNode nid cond tb fb m val next h*)
  then have *notseq*: ¬(*is-sequential-node* (*kind g nid*))
    using *is-sequential-node.simps is-AbstractMergeNode.simps*
    by (*simp add*: *IfNode.hyps*(*1*))
  have *notend*: ¬(*is-AbstractEndNode* (*kind g nid*))
    using *is-AbstractEndNode.simps*
    by (*simp add*: *IfNode.hyps*(*1*))
  have *notdivrem*: ¬(*is-IntegerDivRemNode* (*kind g nid*))
    using *is-AbstractEndNode.simps*
    by (*simp add*: *IfNode.hyps*(*1*))
  from *notseq notend notdivrem* **show** *?case* **using** *IfNode repDet evalDet IRN-
ode.distinct IRNode.inject*(*11*) *Pair-inject step.simps*
    by (*smt* (*z3*) *IRNode.distinct IRNode.inject*(*12*) *Pair-inject step.simps*)
next
  case (*EndNodes nid merge i phis inputs m vs m' h*)
  have *notseq*: ¬(*is-sequential-node* (*kind g nid*))
    using *EndNodes.hyps*(*1*) *is-AbstractEndNode.simps is-sequential-node.simps*
    by (*metis is-EndNode.elims*(*2*) *is-LoopEndNode-def*)
  have *notif*: ¬(*is-IfNode* (*kind g nid*))
    using *EndNodes.hyps*(*1*) *is-IfNode-def is-AbstractEndNode.elims*
    by (*metis IRNode.distinct-disc*(*1058*) *is-EndNode.simps*(*12*))
  have *notref*: ¬(*is-RefNode* (*kind g nid*))
    using *EndNodes.hyps*(*1*) *is-sequential-node.simps*
     using *IRNode.disc*(*1899*) *IRNode.distinct*(*1473*) *is-AbstractEndNode.simps*
is-EndNode.elims(*2*) *is-LoopEndNode-def is-RefNode-def*
    by *metis*
  have *notnew*: ¬(*is-NewInstanceNode* (*kind g nid*))
    using *EndNodes.hyps*(*1*) *is-AbstractEndNode.simps*
   using *IRNode.distinct-disc*(*1442*) *is-EndNode.simps*(*29*) *is-NewInstanceNode-def*
    by (*metis IRNode.distinct-disc*(*1901*) *is-EndNode.simps*(*32*))

149

have *notload*: ¬(*is-LoadFieldNode* (*kind g nid*))
  using *EndNodes.hyps*(*1*) *is-AbstractEndNode.simps*
  using *is-LoadFieldNode-def*
  by (*metis IRNode.distinct-disc*(*1706*) *is-EndNode.simps*(*21*))
have *notstore*: ¬(*is-StoreFieldNode* (*kind g nid*))
  using *EndNodes.hyps*(*1*) *is-AbstractEndNode.simps is-StoreFieldNode-def*
  by (*metis IRNode.distinct-disc*(*1926*) *is-EndNode.simps*(*44*))
have *notdivrem*: ¬(*is-IntegerDivRemNode* (*kind g nid*))
  using *EndNodes.hyps*(*1*) *is-AbstractEndNode.simps is-SignedDivNode-def is-SignedRemNode-def*
  using *IRNode.distinct-disc*(*1498*) *IRNode.distinct-disc*(*1500*) *is-IntegerDivRemNode.simps*
is-EndNode.simps(*36*) *is-EndNode.simps*(*37*)
    by *auto*
  from *notseq notif notref notnew notload notstore notdivrem*
  show *?case* **using** *EndNodes repAllDet evalAllDet*
  by (*smt* (*z3*) *is-IfNode-def is-LoadFieldNode-def is-NewInstanceNode-def is-RefNode-def*
is-StoreFieldNode-def is-SignedDivNode-def is-SignedRemNode-def Pair-inject is-IntegerDivRemNode.elims(*3*)
step.cases)
next
  case (*NewInstanceNode nid f obj nxt h′ ref h m′ m*)
  then have *notseq*: ¬(*is-sequential-node* (*kind g nid*))
    using *is-sequential-node.simps is-AbstractMergeNode.simps*
    by (*simp add*: *NewInstanceNode.hyps*(*1*))
  have *notend*: ¬(*is-AbstractEndNode* (*kind g nid*))
    using *is-AbstractMergeNode.simps*
    by (*simp add*: *NewInstanceNode.hyps*(*1*))
  have *notif*: ¬(*is-IfNode* (*kind g nid*))
    using *is-AbstractMergeNode.simps*
    by (*simp add*: *NewInstanceNode.hyps*(*1*))
  have *notref*: ¬(*is-RefNode* (*kind g nid*))
    using *is-AbstractMergeNode.simps*
    by (*simp add*: *NewInstanceNode.hyps*(*1*))
  have *notload*: ¬(*is-LoadFieldNode* (*kind g nid*))
    using *is-AbstractMergeNode.simps*
    by (*simp add*: *NewInstanceNode.hyps*(*1*))
  have *notstore*: ¬(*is-StoreFieldNode* (*kind g nid*))
    using *is-AbstractMergeNode.simps*
    by (*simp add*: *NewInstanceNode.hyps*(*1*))
  have *notdivrem*: ¬(*is-IntegerDivRemNode* (*kind g nid*))
    using *is-AbstractMergeNode.simps*
    by (*simp add*: *NewInstanceNode.hyps*(*1*))
  from *notseq notend notif notref notload notstore notdivrem*
  show *?case* **using** *NewInstanceNode step.cases*
    by (*smt* (*z3*) *IRNode.disc*(*1028*) *IRNode.disc*(*2270*) *IRNode.discI*(*11*) *IRNode.distinct*(*2311*) *IRNode.distinct*(*2313*) *IRNode.inject*(*31*) *Pair-inject*)
next
  case (*LoadFieldNode nid f obj nxt m ref h v m′*)
  then have *notseq*: ¬(*is-sequential-node* (*kind g nid*))
    using *is-sequential-node.simps is-AbstractMergeNode.simps*
    by (*simp add*: *LoadFieldNode.hyps*(*1*))

150

have *notend*: ¬(*is-AbstractEndNode* (*kind g nid*))
  using *is-AbstractEndNode.simps*
  by (*simp add*: *LoadFieldNode.hyps*(*1*))
have *notdivrem*: ¬(*is-IntegerDivRemNode* (*kind g nid*))
  using *is-AbstractEndNode.simps*
  by (*simp add*: *LoadFieldNode.hyps*(*1*))
from *notseq notend notdivrem*
show *?case* **using** *LoadFieldNode step.cases repDet evalDet*
  by (*smt* (*z3*) *IRNode.distinct*(*1051*) *IRNode.distinct*(*1721*) *IRNode.distinct*(*1739*)
IRNode.distinct(*1741*) *IRNode.distinct*(*1745*) *IRNode.inject*(*20*) *Pair-inject Value.inject*(*3*)
option.distinct(*1*) *option.inject*)
next
  case (*StaticLoadFieldNode nid f nxt h v m′ m*)
  then have *notseq*: ¬(*is-sequential-node* (*kind g nid*))
    using *is-sequential-node.simps is-AbstractMergeNode.simps*
    by (*simp add*: *StaticLoadFieldNode.hyps*(*1*))
  have *notend*: ¬(*is-AbstractEndNode* (*kind g nid*))
    using *is-AbstractEndNode.simps*
    by (*simp add*: *StaticLoadFieldNode.hyps*(*1*))
  have *notdivrem*: ¬(*is-IntegerDivRemNode* (*kind g nid*))
    by (*simp add*: *StaticLoadFieldNode.hyps*(*1*))
  from *notseq notend notdivrem*
  show *?case* **using** *StaticLoadFieldNode step.cases*
    by (*smt* (*z3*) *IRNode.distinct*(*1051*) *IRNode.distinct*(*1721*) *IRNode.distinct*(*1739*)
IRNode.distinct(*1741*) *IRNode.distinct*(*1745*) *IRNode.inject*(*20*) *Pair-inject option.distinct*(*1*))
next
  case (*StoreFieldNode nid f newval uu obj nxt m val ref h′ h m′*)
  then have *notseq*: ¬(*is-sequential-node* (*kind g nid*))
    using *is-sequential-node.simps is-AbstractMergeNode.simps*
    by (*simp add*: *StoreFieldNode.hyps*(*1*))
  have *notend*: ¬(*is-AbstractEndNode* (*kind g nid*))
    using *is-AbstractEndNode.simps*
    by (*simp add*: *StoreFieldNode.hyps*(*1*))
  have *notdivrem*: ¬(*is-IntegerDivRemNode* (*kind g nid*))
    by (*simp add*: *StoreFieldNode.hyps*(*1*))
  from *notseq notend notdivrem*
  show *?case* **using** *StoreFieldNode step.cases repDet evalDet*
    by (*smt* (*z3*) *IRNode.distinct*(*1097*) *IRNode.distinct*(*1745*) *IRNode.distinct*(*2317*)
IRNode.distinct(*2605*) *IRNode.distinct*(*2627*) *IRNode.inject*(*43*) *Pair-inject Value.inject*(*3*)
option.distinct(*1*) *option.inject*)
next
  case (*StaticStoreFieldNode nid f newval uv nxt m val h′ h m′*)
  then have *notseq*: ¬(*is-sequential-node* (*kind g nid*))
    using *is-sequential-node.simps is-AbstractMergeNode.simps*
    by (*simp add*: *StaticStoreFieldNode.hyps*(*1*))
  have *notend*: ¬(*is-AbstractEndNode* (*kind g nid*))
    using *is-AbstractEndNode.simps*
    by (*simp add*: *StaticStoreFieldNode.hyps*(*1*))
  have *notdivrem*: ¬(*is-IntegerDivRemNode* (*kind g nid*))

 by (*simp add*: *StaticStoreFieldNode.hyps*(*1*))
 from *notseq notend notdivrem*
 show *?case* **using** *StoreFieldNode step.cases repDet evalDet*
 by (*smt* (*z3*) *IRNode.distinct*(*1097*) *IRNode.distinct*(*1745*) *IRNode.distinct*(*2317*)
IRNode.distinct(*2605*) *IRNode.distinct*(*2627*) *IRNode.inject*(*43*) *Pair-inject Static-*
StoreFieldNode.hyps(*1*) *StaticStoreFieldNode.hyps*(*2*) *StaticStoreFieldNode.hyps*(*3*)
StaticStoreFieldNode.hyps(*4*) *StaticStoreFieldNode.hyps*(*5*) *option.distinct*(*1*))
next
 case (*SignedDivNode nid x y zero sb nxt m v1 v2 v m' h*)
 then have *notseq*: ¬(*is-sequential-node* (*kind g nid*))
  using *is-sequential-node.simps is-AbstractMergeNode.simps*
  by (*simp add*: *SignedDivNode.hyps*(*1*))
 have *notend*: ¬(*is-AbstractEndNode* (*kind g nid*))
  using *is-AbstractEndNode.simps*
  by (*simp add*: *SignedDivNode.hyps*(*1*))
 from *notseq notend*
 show *?case* **using** *SignedDivNode step.cases repDet evalDet*
 by (*smt* (*z3*) *IRNode.distinct*(*1091*) *IRNode.distinct*(*1739*) *IRNode.distinct*(*2311*)
IRNode.distinct(*2601*) *IRNode.distinct*(*2605*) *IRNode.inject*(*40*) *Pair-inject*)
next
 case (*SignedRemNode nid x y zero sb nxt m v1 v2 v m' h*)
 then have *notseq*: ¬(*is-sequential-node* (*kind g nid*))
  using *is-sequential-node.simps is-AbstractMergeNode.simps*
  by (*simp add*: *SignedRemNode.hyps*(*1*))
 have *notend*: ¬(*is-AbstractEndNode* (*kind g nid*))
  using *is-AbstractEndNode.simps*
  by (*simp add*: *SignedRemNode.hyps*(*1*))
 from *notseq notend*
 show *?case* **using** *SignedRemNode step.cases repDet evalDet*
 by (*smt* (*z3*) *IRNode.distinct*(*1093*) *IRNode.distinct*(*1741*) *IRNode.distinct*(*2313*)
IRNode.distinct(*2601*) *IRNode.distinct*(*2627*) *IRNode.inject*(*41*) *Pair-inject*)
qed

lemma *stepRefNode*:
 ⟦*kind g nid = RefNode nid'*⟧ ⟹ *g, p* ⊢ (*nid,m,h*) → (*nid',m,h*)
 using *SequentialNode*
 by (*metis IRNodes.successors-of-RefNode is-sequential-node.simps*(*7*) *nth-Cons-0*)

lemma *IfNodeStepCases*:
 assumes *kind g nid = IfNode cond tb fb*
 assumes *g* ⊢ *cond* ≃ *condE*
 assumes [*m, p*] ⊢ *condE* ↦ *v*
 assumes *g, p* ⊢ (*nid, m, h*) → (*nid', m, h*)
 shows *nid'* ∈ {*tb, fb*}
 using *step.IfNode repDet stepDet assms*
 by (*metis insert-iff old.prod.inject*)

lemma *IfNodeSeq*:
 shows *kind g nid = IfNode cond tb fb* ⟶ ¬(*is-sequential-node* (*kind g nid*))

unfolding *is-sequential-node.simps*
using *is-sequential-node.simps*(*18*) **by** *presburger*

lemma *IfNodeCond*:
  assumes *kind g nid = IfNode cond tb fb*
  assumes *g, p* ⊢ (*nid, m, h*) → (*nid′, m, h*)
  shows ∃ *condE v.* ((*g* ⊢ *cond* ≃ *condE*) ∧ ([*m, p*] ⊢ *condE* ↦ *v*))
  using *assms*(*2,1*) **by** (*induct* (*nid,m,h*) (*nid′,m,h*) *rule: step.induct; auto*)

lemma *step-in-ids*:
  assumes *g, p* ⊢ (*nid, m, h*) → (*nid′, m′, h′*)
  shows *nid* ∈ *ids g*
  using *assms* **apply** (*induct* (*nid, m, h*) (*nid′, m′, h′*) *rule: step.induct*)
  using *is-sequential-node.simps*(*45*) *not-in-g*
  apply *simp*
  apply (*metis is-sequential-node.simps*(*53*))
  using *ids-some*
  using *IRNode.distinct*(*1113*) **apply** *presburger*
  using *EndNodes*(*1*) *is-AbstractEndNode.simps is-EndNode.simps*(*45*) *ids-some*
  apply (*metis IRNode.disc*(*1218*) *is-EndNode.simps*(*52*))
  by *simp+*

end

9 Proof Infrastructure

9.1 Bisimulation

theory *Bisimulation*
imports
  Stuttering
begin

inductive *weak-bisimilar* :: *ID* ⇒ *IRGraph* ⇒ *IRGraph* ⇒ *bool*
  (- . - ∼ -) **for** *nid* **where**
  ⟦∀ *P′*. (*g m p h* ⊢ *nid* ⤳ *P′*) ⟶ (∃ *Q′* . (*g′ m p h* ⊢ *nid* ⤳ *Q′*) ∧ *P′* = *Q′*);
    ∀ *Q′*. (*g′ m p h* ⊢ *nid* ⤳ *Q′*) ⟶ (∃ *P′* . (*g m p h* ⊢ *nid* ⤳ *P′*) ∧ *P′* = *Q′*)⟧
  ⟹ *nid* . *g* ∼ *g′*

A strong bisimilution between no-op transitions

inductive *strong-noop-bisimilar* :: *ID* ⇒ *IRGraph* ⇒ *IRGraph* ⇒ *bool*
  (- | - ∼ -) **for** *nid* **where**
  ⟦∀ *P′*. (*g, p* ⊢ (*nid, m, h*) → *P′*) ⟶ (∃ *Q′* . (*g′, p* ⊢ (*nid, m, h*) → *Q′*) ∧ *P′* = *Q′*);
    ∀ *Q′*. (*g′, p* ⊢ (*nid, m, h*) → *Q′*) ⟶ (∃ *P′* . (*g, p* ⊢ (*nid, m, h*) → *P′*) ∧ *P′* = *Q′*)⟧
  ⟹ *nid* | *g* ∼ *g′*

lemma *lockstep-strong-bisimilulation*:
  assumes $g' = $ *replace-node nid node g*
  assumes $g, p \vdash (nid, m, h) \rightarrow (nid', m, h)$
  assumes $g', p \vdash (nid, m, h) \rightarrow (nid', m, h)$
  shows $nid \mid g \sim g'$
  using *assms(2) assms(3) stepDet strong-noop-bisimilar.simps* **by** *metis*

lemma *no-step-bisimulation*:
  assumes $\forall\, m\ p\ h\ nid'\ m'\ h'.\ \neg(g, p \vdash (nid, m, h) \rightarrow (nid', m', h'))$
  assumes $\forall\, m\ p\ h\ nid'\ m'\ h'.\ \neg(g', p \vdash (nid, m, h) \rightarrow (nid', m', h'))$
  shows $nid \mid g \sim g'$
  using *assms*
  by (*simp add: assms(1) assms(2) strong-noop-bisimilar.intros*)

end

9.2 Graph Rewriting

theory
  Rewrites
imports
  Stuttering
begin

fun *replace-usages* :: $ID \Rightarrow ID \Rightarrow IRGraph \Rightarrow IRGraph$ **where**
  replace-usages nid nid' g = replace-node nid (*RefNode nid', stamp g nid'*) *g*

lemma *replace-usages-effect*:
  assumes $g' = $ *replace-usages nid nid' g*
  shows *kind g' nid = RefNode nid'*
  using *assms replace-node-lookup replace-usages.simps*
  by (*metis IRNode.distinct(2755)*)

lemma *replace-usages-changeonly*:
  assumes $nid \in ids\ g$
  assumes $g' = $ *replace-usages nid nid' g*
  shows *changeonly* $\{nid\}$ *g g'*
  using *assms* **unfolding** *replace-usages.simps*
  by (*metis add-changed add-node-def replace-node-def*)

lemma *replace-usages-unchanged*:
  assumes $nid \in ids\ g$
  assumes $g' = $ *replace-usages nid nid' g*
  shows *unchanged* (*ids g* $-$ $\{nid\}$) *g g'*
  using *assms* **unfolding** *replace-usages.simps*
  using *assms(2) disjoint-change replace-usages-changeonly* **by** *presburger*

fun *nextNid* :: *IRGraph* $\Rightarrow$ *ID* **where**
　nextNid g = (*Max* (*ids g*)) + *1*

lemma *max-plus-one*:
　fixes *c* :: *ID set*
　shows ⟦*finite c*; *c* ≠ {}⟧ $\Longrightarrow$ (*Max c*) + *1* ∉ *c*
　by (*meson Max-gr-iff less-add-one less-irrefl*)

lemma *ids-finite*:
　finite (*ids g*)
　by *simp*

lemma *nextNidNotIn*:
　ids g ≠ {} $\longrightarrow$ *nextNid g* ∉ *ids g*
　unfolding *nextNid.simps*
　using *ids-finite max-plus-one* **by** *blast*

fun *constantCondition* :: *bool* $\Rightarrow$ *ID* $\Rightarrow$ *IRNode* $\Rightarrow$ *IRGraph* $\Rightarrow$ *IRGraph* **where**
　constantCondition val nid (*IfNode cond t f*) *g* =
　　replace-node nid (*IfNode* (*nextNid g*) *t f*, *stamp g nid*)
　　　(*add-node* (*nextNid g*) ((*ConstantNode* (*bool-to-val val*)), *constantAsStamp*
(*bool-to-val val*)) *g*) |
　constantCondition cond nid - *g* = *g*

lemma *constantConditionTrue*:
　assumes *kind g ifcond* = *IfNode cond t f*
　assumes *g′* = *constantCondition True ifcond* (*kind g ifcond*) *g*
　shows *g′*, *p* ⊢ (*ifcond*, *m*, *h*) → (*t*, *m*, *h*)
proof −
　have *ifn*: ⋀ *c t f*. *IfNode c t f* ≠ *NoNode*
　　by *simp*
　then have *if′*: *kind g′ ifcond* = *IfNode* (*nextNid g*) *t f*
　　using *assms*(*1*) *assms*(*2*) *constantCondition.simps*(*1*) *replace-node-lookup*
　　by *presburger*
　have *truedef*: *bool-to-val True* = (*IntVal32 1*)
　　by *auto*
　from *ifn* **have** *ifcond* ≠ (*nextNid g*)
　　by (*metis assms*(*1*) *emptyE ids-some nextNidNotIn*)
　moreover have ⋀ *c*. *ConstantNode c* ≠ *NoNode* **by** *simp*
　ultimately have *kind g′* (*nextNid g*) = *ConstantNode* (*bool-to-val True*)
　　using *add-changed add-node-def assms*(*1*) *assms*(*2*) *constantCondition.simps*(*1*)
not-in-g other-node-unchanged replace-node-def replace-node-lookup singletonD
　　by (*smt* (*z3*) *DiffI add-node-lookup replace-node-unchanged*)
　then have *c′*: *kind g′* (*nextNid g*) = *ConstantNode* (*IntVal32 1*)
　　using *truedef* **by** *simp*
　have *valid-value* (*IntVal32 1*) (*constantAsStamp* (*IntVal32 1*))
　　unfolding *constantAsStamp.simps valid-value.simps*
　　using *nat-numeral* **by** *blast*

155

then have $[g', m, p] \vdash nextNid\ g \mapsto IntVal32\ 1$
  using *ConstantExpr ConstantNode Value.distinct(1)* ‹*kind g' (nextNid g) = ConstantNode (bool-to-val True)*› *encodeeval-def truedef*
  by *metis*
  from *if' c'* **show** *?thesis* **using** *IfNode*
  by (*metis* (*no-types, opaque-lifting*) *val-to-bool.simps(1)* ‹$[g',m,p] \vdash nextNid\ g \mapsto IntVal32\ 1$› *encodeeval-def zero-neq-one*)
qed

lemma *constantConditionFalse*:
  assumes *kind g ifcond = IfNode cond t f*
  assumes *g' = constantCondition False ifcond (kind g ifcond) g*
  shows $g', p \vdash (ifcond, m, h) \rightarrow (f, m, h)$
proof −
  have *ifn*: $\bigwedge c\ t\ f.\ IfNode\ c\ t\ f \neq NoNode$
    by *simp*
  then have *if'*: *kind g' ifcond = IfNode (nextNid g) t f*
    by (*metis assms(1) assms(2) constantCondition.simps(1) replace-node-lookup*)
  have *falsedef*: *bool-to-val False = (IntVal32 0)*
    by *auto*
  from *ifn* **have** $ifcond \neq (nextNid\ g)$
    by (*metis assms(1) equals0D ids-some nextNidNotIn*)
  moreover have $\bigwedge c.\ ConstantNode\ c \neq NoNode$ **by** *simp*
  ultimately have *kind g' (nextNid g) = ConstantNode (bool-to-val False)*
     by (*smt* (*z3*) *add-changed add-node-def assms(1) assms(2) constantCondition.simps(1) not-in-g other-node-unchanged replace-node-def replace-node-lookup singletonD*)
  then have *c'*: *kind g' (nextNid g) = ConstantNode (IntVal32 0)*
    using *falsedef* **by** *simp*
  have *valid-value (IntVal32 0) (constantAsStamp (IntVal32 0))*
    unfolding *constantAsStamp.simps valid-value.simps*
    using *nat-numeral* **by** *blast*
  then have $[g', m, p] \vdash nextNid\ g \mapsto IntVal32\ 0$
    by (*metis ConstantExpr ConstantNode* ‹*kind g' (nextNid g) = ConstantNode (bool-to-val False)*› *encodeeval-def falsedef*)
  from *if' c'* **show** *?thesis* **using** *IfNode*
    by (*metis* (*no-types, opaque-lifting*) *val-to-bool.simps(1)* ‹$[g',m,p] \vdash nextNid\ g \mapsto IntVal32\ 0$› *encodeeval-def*)
qed

lemma *diff-forall*:
  assumes $\forall n \in ids\ g - \{nid\}.\ cond\ n$
  shows $\forall n.\ n \in ids\ g \wedge n \notin \{nid\} \longrightarrow cond\ n$
  by (*meson Diff-iff assms*)

lemma *replace-node-changeonly*:
  assumes *g' = replace-node nid node g*
  shows *changeonly* $\{nid\}\ g\ g'$
  using *assms replace-node-unchanged*

unfolding *changeonly.simps* **using** *diff-forall*
by (*metis add-changed add-node-def changeonly.simps replace-node-def*)

lemma *add-node-changeonly*:
  assumes $g' = add\text{-}node\ nid\ node\ g$
  shows *changeonly* $\{nid\}$ *g g'*
   by (*metis Rep-IRGraph-inverse add-node.rep-eq assms replace-node.rep-eq replace-node-changeonly*)

lemma *constantConditionNoEffect*:
  assumes $\neg(\textit{is-IfNode}\ (kind\ g\ nid))$
  shows $g = constantCondition\ b\ nid\ (kind\ g\ nid)\ g$
  using *assms* **apply** (*cases kind g nid*)
  using *constantCondition.simps*
  apply *presburger+*
  apply (*metis is-IfNode-def*)
  using *constantCondition.simps*
  by *presburger+*

lemma *constantConditionIfNode*:
  assumes *kind g nid = IfNode cond t f*
  shows *constantCondition val nid* (*kind g nid*) *g =*
    replace-node nid (*IfNode* (*nextNid g*) *t f, stamp g nid*)
      (*add-node* (*nextNid g*) ((*ConstantNode* (*bool-to-val val*)), *constantAsStamp*
(*bool-to-val val*)) *g*)
  using *constantCondition.simps*
  by (*simp add: assms*)

lemma *constantCondition-changeonly*:
  assumes $nid \in ids\ g$
  assumes $g' = constantCondition\ b\ nid\ (kind\ g\ nid)\ g$
  shows *changeonly* $\{nid\}$ *g g'*
proof (*cases is-IfNode* (*kind g nid*))
  case *True*
  have *nextNid g* $\notin$ *ids g*
    using *nextNidNotIn* **by** (*metis emptyE*)
  then show *?thesis* **using** *assms*
   using *replace-node-changeonly add-node-changeonly* **unfolding** *changeonly.simps*
    using *True constantCondition.simps(1) is-IfNode-def*
    by (*metis* (*no-types, lifting*) *insert-iff*)
next
  case *False*
  have $g = g'$
    using *constantConditionNoEffect*
    using *False assms(2)* **by** *blast*
  then show *?thesis* **by** *simp*
qed

lemma *constantConditionNoIf*:
  assumes ∀ *cond t f. kind g ifcond* ≠ *IfNode cond t f*
  assumes *g′* = *constantCondition val ifcond* (*kind g ifcond*) *g*
  shows ∃ *nid′* .(*g m p h* ⊢ *ifcond* ⤳ *nid′*) ⟷ (*g′ m p h* ⊢ *ifcond* ⤳ *nid′*)
proof −
  have *g′* = *g*
    using *assms*(*2*) *assms*(*1*)
    using *constantConditionNoEffect*
    by (*metis IRNode.collapse*(*11*))
  then show *?thesis* **by** *simp*
qed

lemma *constantConditionValid*:
  assumes *kind g ifcond* = *IfNode cond t f*
  assumes [*g, m, p*] ⊢ *cond* ↦ *v*
  assumes *const* = *val-to-bool v*
  assumes *g′* = *constantCondition const ifcond* (*kind g ifcond*) *g*
  shows ∃ *nid′* .(*g m p h* ⊢ *ifcond* ⤳ *nid′*) ⟷ (*g′ m p h* ⊢ *ifcond* ⤳ *nid′*)
proof (*cases const*)
  case *True*
  have *ifstep*: *g, p* ⊢ (*ifcond, m, h*) → (*t, m, h*)
    by (*meson IfNode True assms*(*1*) *assms*(*2*) *assms*(*3*) *encodeeval-def*)
  have *ifstep′*: *g′, p* ⊢ (*ifcond, m, h*) → (*t, m, h*)
    using *constantConditionTrue*
    using *True assms*(*1*) *assms*(*4*) **by** *presburger*
  from *ifstep ifstep′* **show** *?thesis*
    using *StutterStep* **by** *blast*
next
  case *False*
  have *ifstep*: *g, p* ⊢ (*ifcond, m, h*) → (*f, m, h*)
    by (*meson IfNode False assms*(*1*) *assms*(*2*) *assms*(*3*) *encodeeval-def*)
  have *ifstep′*: *g′, p* ⊢ (*ifcond, m, h*) → (*f, m, h*)
    using *constantConditionFalse*
    using *False assms*(*1*) *assms*(*4*) **by** *presburger*
  from *ifstep ifstep′* **show** *?thesis*
    using *StutterStep* **by** *blast*
qed

end

9.3 Stuttering

theory *Stuttering*
  imports
    Semantics.IRStepThms
begin

inductive *stutter*:: *IRGraph* ⇒ *MapState* ⇒ *Params* ⇒ *FieldRefHeap* ⇒ *ID* ⇒ *ID* ⇒ *bool* (- - - - ⊢ - ⤳ - *55*)

for *g m p h* **where**

StutterStep:
$[\![g,\ p \vdash (nid,m,h) \to (nid',m,h)]\!]$
$\implies g\ m\ p\ h \vdash nid \rightsquigarrow nid'\ |$

Transitive:
$[\![g,\ p \vdash (nid,m,h) \to (nid'',m,h);$
$\quad g\ m\ p\ h \vdash nid'' \rightsquigarrow nid']\!]$
$\implies g\ m\ p\ h \vdash nid \rightsquigarrow nid'$

lemma *stuttering-successor*:
  assumes $(g,\ p \vdash (nid,\ m,\ h) \to (nid',\ m,\ h))$
  shows $\{P'.\ (g\ m\ p\ h \vdash nid \rightsquigarrow P')\} = \{nid'\} \cup \{nid''.\ (g\ m\ p\ h \vdash nid' \rightsquigarrow nid'')\}$
proof $-$
  have *nextin*: $nid' \in \{P'.\ (g\ m\ p\ h \vdash nid \rightsquigarrow P')\}$
    using *assms StutterStep* **by** *blast*
  have *nextsubset*: $\{nid''.\ (g\ m\ p\ h \vdash nid' \rightsquigarrow nid'')\} \subseteq \{P'.\ (g\ m\ p\ h \vdash nid \rightsquigarrow P')\}$
    by (*metis Collect-mono assms stutter.Transitive*)
  have $\forall n \in \{P'.\ (g\ m\ p\ h \vdash nid \rightsquigarrow P')\}\ .\ n = nid' \vee n \in \{nid''.\ (g\ m\ p\ h \vdash nid'$
$\rightsquigarrow nid'')\}$
    using *stepDet*
    by (*metis (no-types, lifting) Pair-inject assms mem-Collect-eq stutter.simps*)
  then show *?thesis*
    using *insert-absorb mk-disjoint-insert nextin nextsubset* **by** *auto*
qed

end

9.4   Evaluation Stamp Theorems

theory *StampEvalThms*
  imports *Semantics.IRTreeEvalThms*
begin

9.4.1   Support Lemmas for Stamps and Upper/Lower Bounds

lemma *size32*: *size v = 32* **for** *v :: 32 word*
  using *size-word.rep-eq*
  using *One-nat-def add.right-neutral add-Suc-right len-of-numeral-defs(2) len-of-numeral-defs(3)*
mult.right-neutral mult-Suc-right numeral-2-eq-2 numeral-Bit0
  by (*smt (verit, del-insts) mult.commute*)

lemma *size64*: *size v = 64* **for** *v :: 64 word*
  using *size-word.rep-eq*
  using *One-nat-def add.right-neutral add-Suc-right len-of-numeral-defs(2) len-of-numeral-defs(3)*
mult.right-neutral mult-Suc-right numeral-2-eq-2 numeral-Bit0
  by (*smt (verit, del-insts) mult.commute*)

declare $[[\textit{show-types=true}]]$

lemma *signed-int-bottom32*: $-(((2{::}int) \verb|^| 31)) \leq sint\ (v{::}int32)$
  using *sint-range-size size32*
  by (*smt* (*verit, ccfv-SIG*) *One-nat-def Suc-pred add-Suc add-Suc-right eval-nat-numeral*(*3*) *nat.inject numeral-2-eq-2 numeral-Bit0 numeral-Bit1 zero-less-numeral*)

lemma *signed-int-top32*: $(2 \verb|^| 31) - 1 \geq sint\ (v{::}int32)$
  using *sint-range-size size32*
  by (*smt* (*verit, ccfv-SIG*) *One-nat-def Suc-pred add-Suc add-Suc-right eval-nat-numeral*(*3*) *nat.inject numeral-2-eq-2 numeral-Bit0 numeral-Bit1 zero-less-numeral*)

lemma *lower-bounds-equiv32*: $-(((2{::}int) \verb|^| 31)) = (2{::}int) \verb|^| 32\ div\ 2 * - 1$
  by *fastforce*

lemma *upper-bounds-equiv32*: $(2{::}int) \verb|^| 31 = (2{::}int) \verb|^| 32\ div\ 2$
  by *simp*

lemma *bit-bounds-min32*: $((fst\ (bit\text{-}bounds\ 32))) \leq (sint\ (v{::}int32))$
  unfolding *bit-bounds.simps fst-def* **using** *signed-int-bottom32 lower-bounds-equiv32*
  by *auto*

lemma *bit-bounds-max32*: $((snd\ (bit\text{-}bounds\ 32))) \geq (sint\ (v{::}int32))$
  unfolding *bit-bounds.simps fst-def* **using** *signed-int-top32 upper-bounds-equiv32*
  by *auto*

lemma *signed-int-bottom64*: $-(((2{::}int) \verb|^| 63)) \leq sint\ (v{::}int64)$
  using *sint-range-size size64*
  by (*smt* (*verit, ccfv-SIG*) *One-nat-def Suc-pred add-Suc add-Suc-right eval-nat-numeral*(*3*) *nat.inject numeral-2-eq-2 numeral-Bit0 numeral-Bit1 zero-less-numeral*)

lemma *signed-int-top64*: $(2 \verb|^| 63) - 1 \geq sint\ (v{::}int64)$
  using *sint-range-size size64*
  by (*smt* (*verit, ccfv-SIG*) *One-nat-def Suc-pred add-Suc add-Suc-right eval-nat-numeral*(*3*) *nat.inject numeral-2-eq-2 numeral-Bit0 numeral-Bit1 zero-less-numeral*)

lemma *lower-bounds-equiv64*: $-(((2{::}int) \verb|^| 63)) = (2{::}int) \verb|^| 64\ div\ 2 * - 1$
  by *fastforce*

lemma *upper-bounds-equiv64*: $(2{::}int) \verb|^| 63 = (2{::}int) \verb|^| 64\ div\ 2$
  by *simp*

lemma *bit-bounds-min64*: $((fst\ (bit\text{-}bounds\ 64))) \leq (sint\ (v{::}int64))$
  unfolding *bit-bounds.simps fst-def* **using** *signed-int-bottom64 lower-bounds-equiv64*
  by *auto*

lemma *bit-bounds-max64*: $((snd\ (bit\text{-}bounds\ 64))) \geq (sint\ (v{::}int64))$
  unfolding *bit-bounds.simps fst-def* **using** *signed-int-top64 upper-bounds-equiv64*
  by *auto*

lemma *unrestricted-32bit-always-valid* [*simp*]:
  valid-value (*IntVal32 v*) (*unrestricted-stamp* (*IntegerStamp 32 lo hi*))
  using *valid-value.simps*(*1*) *bit-bounds-min32 bit-bounds-max32*
  using *unrestricted-stamp.simps*(*2*) **by** *presburger*

lemma *unrestricted-64bit-always-valid* [*simp*]:
  valid-value (*IntVal64 v*) (*unrestricted-stamp* (*IntegerStamp 64 lo hi*))
  using *valid-value.simps*(*2*) *bit-bounds-min64 bit-bounds-max64*
  using *unrestricted-stamp.simps*(*2*) **by** *presburger*

lemma *unary-undef*: *val = UndefVal* $\implies$ *unary-eval op val = UndefVal*
  by (*cases op*; *auto*)

lemma *unary-obj*: *val = ObjRef x* $\implies$ *unary-eval op val = UndefVal*
  by (*cases op*; *auto*)

lemma *lower-bounds-equiv*:
  assumes $N > 0$
  shows $-(((2::int) \,\hat{}\, (N{-}1))) = (2::int) \,\hat{}\, N \ div\ 2 * -\ 1$
  by (*simp add*: *assms int-power-div-base*)

lemma *upper-bounds-equiv*:
  assumes $N > 0$
  shows $(2::int) \,\hat{}\, (N{-}1) = (2::int) \,\hat{}\, N \ div\ 2$
  by (*simp add*: *assms int-power-div-base*)

Next we show that casting a word to a wider word preserves any upper/lower bounds.

lemma *scast-max-bound*:
  assumes *sint* ($v :: {}'a :: len\ word$) $< M$
  assumes $LENGTH({}'a) < LENGTH({}'b)$
  shows *sint* (($scast\ v$) :: ${}'b :: len\ word$) $< M$
  unfolding *Word.scast-eq Word.sint-sbintrunc$'$*
  using *Bit-Operations.signed-take-bit-int-eq-self-iff*
 by (*smt* (*verit, best*) *One-nat-def assms*(*1*) *assms*(*2*) *decr-length-less-iff linorder-not-le*
power-strict-increasing-iff signed-take-bit-int-less-self-iff sint-greater-eq)

lemma *scast-min-bound*:
  assumes $M \leq sint$ ($v :: {}'a :: len\ word$)
  assumes $LENGTH({}'a) < LENGTH({}'b)$
  shows $M \leq sint$ (($scast\ v$) :: ${}'b :: len\ word$)
  unfolding *Word.scast-eq Word.sint-sbintrunc$'$*
  using *Bit-Operations.signed-take-bit-int-eq-self-iff*
  by (*smt* (*verit*) *One-nat-def Suc-pred assms*(*1*) *assms*(*2*) *len-gt-0 less-Suc-eq order-less-le order-less-le-trans power-le-imp-le-exp signed-take-bit-int-greater-eq-self-iff*

sint-lt)

lemma *scast-bigger-max-bound*:
  assumes (*result* :: *'b* :: *len word*) = *scast* (*v* :: *'a* :: *len word*)
  shows *sint result* < *2* $\widehat{\ }$ *LENGTH*(*'a*) *div 2*
  using *sint-lt upper-bounds-equiv scast-max-bound*
 by (*smt* (*verit, best*) *assms*(*1*) *len-gt-0 signed-scast-eq signed-take-bit-int-greater-self-iff*
sint-ge sint-less upper-bounds-equiv)

lemma *scast-bigger-min-bound*:
  assumes (*result* :: *'b* :: *len word*) = *scast* (*v* :: *'a* :: *len word*)
  shows − (*2* $\widehat{\ }$ *LENGTH*(*'a*) *div 2*) ≤ *sint result*
  using *sint-ge lower-bounds-equiv scast-min-bound*
  by (*smt* (*verit*) *assms len-gt-0 nat-less-le not-less scast-max-bound*)

lemma *scast-bigger-bit-bounds*:
  assumes (*result* :: *'b* :: *len word*) = *scast* (*v* :: *'a* :: *len word*)
 shows *fst* (*bit-bounds* (*LENGTH*(*'a*))) ≤ *sint result* ∧ *sint result* ≤ *snd* (*bit-bounds*
(*LENGTH*(*'a*)))
  using *assms scast-bigger-min-bound scast-bigger-max-bound*
  by *auto*

lemma *unrestricted-stamp32-always-valid* [*simp*]:
  assumes *fst* (*bit-bounds bits*) ≤ *sint ival* ∧ *sint ival* ≤ *snd* (*bit-bounds bits*)
  assumes *bits* = *32* ∨ *bits* = *16* ∨ *bits* = *8* ∨ *bits* = *1*
  assumes *result* = *IntVal32 ival*
  shows *valid-value result* (*unrestricted-stamp* (*IntegerStamp bits lo hi*))
  using *assms valid-value.simps*(*1*) *unrestricted-stamp.simps*(*2*) **by** *presburger*

lemma *larger-stamp32-always-valid* [*simp*]:
  assumes *valid-value result* (*unrestricted-stamp* (*IntegerStamp inBits lo hi*))
  assumes *result* = *IntVal32 ival*
  assumes *outBits* = *32* ∨ *outBits* = *16* ∨ *outBits* = *8* ∨ *outBits* = *1*
  assumes *inBits* ≤ *outBits*
  shows *valid-value result* (*unrestricted-stamp* (*IntegerStamp outBits lo hi*))
 using *assms.simps* **by** (*smt* (*z3*) *bit-bounds.simps diff-le-mono linorder-not-less lower-bounds-equiv*
not-numeral-le-zero numerals(*1*) *power-increasing-iff prod.sel*(*1*) *prod.sel*(*2*) *unre-*
stricted-stamp.simps(*2*) *valid-value.simps*(*1*))

Possibly helpful lemmas about $signed_{t}ake_{b}it$, to help with UnaryNarrow.
Note: we could use signed to convert between bit-widths, instead of signed_take_bit.
But this has to be done separately for each bit-width type.

value *sint*(*signed-take-bit 7* (*128* :: *int8*))

ML-val ‹@{*thm signed-take-bit-decr-length-iff*}›
declare [[*show-types=true*]]
ML-val ‹@{*thm signed-take-bit-int-less-exp*}›

lemma *signed-take-bit-int-less-exp-word*:
  assumes $n < LENGTH('a)$
  shows $sint(signed\text{-}take\text{-}bit\ n\ (k :: 'a :: len\ word)) < (2::int)\ \widehat{}\ n$
  apply *transfer*
  by (*smt* (*verit, best*) *not-take-bit-negative signed-take-bit-eq-take-bit-shift*
    signed-take-bit-int-less-exp take-bit-int-greater-self-iff)

lemma *signed-take-bit-int-greater-eq-minus-exp-word*:
  assumes $n < LENGTH('a)$
  shows $- (2\ \widehat{}\ n) \leq sint(signed\text{-}take\text{-}bit\ n\ (k :: 'a :: len\ word))$
  apply *transfer*
  by (*smt* (*verit, best*) *signed-take-bit-int-greater-eq-minus-exp*
    signed-take-bit-int-greater-eq-self-iff signed-take-bit-int-less-exp)

Some important lemmas showing that sign_extend_helper produces integer
results whose range is determined by the inBits parameter.

lemma *sign-extend-helper-output-range64*:
  assumes $result = sign\text{-}extend\text{-}helper\ inBits\ outBits\ val$
  assumes $result = IntVal64\ ival$
  shows $outBits = 64 \wedge -(2\ \widehat{}\ (inBits - 1)) \leq sint\ ival \wedge sint\ ival \leq 2\ \widehat{}\ (inBits - 1)$

proof −
  have $ival$: $ival = (scast\ (signed\text{-}take\text{-}bit\ (inBits - 1)\ val))$
    using *assms sign-extend-helper.simps*
    by (*smt* (*verit, ccfv-SIG*) *Value.distinct*(*3*) *Value.inject*(*2*) *Value.simps*(*14*))
  then have lo: $-(2\ \widehat{}\ (inBits - 1)) \leq sint\ (signed\text{-}take\text{-}bit\ (inBits - 1)\ val)$
    using *signed-take-bit-int-greater-eq-minus-exp-word*
     by (*smt* (*verit, best*) *diff-le-self not-less power-increasing-iff sint-below-size wsst-TYs*(*3*))
  then have $lo2$: $-(2\ \widehat{}\ (inBits - 1)) \leq sint\ (scast\ (signed\text{-}take\text{-}bit\ (inBits - 1)\ val))$
      by (*smt* (*verit, best*) *diff-less len-gt-0 less-Suc-eq power-strict-increasing-iff signed-scast-eq signed-take-bit-int-greater-eq-self-iff signed-take-bit-int-less-exp-word sint-range-size wsst-TYs*(*3*))
  have hi: $sint\ (signed\text{-}take\text{-}bit\ (inBits - 1)\ val) < 2\ \widehat{}\ (inBits - 1)$
    using *signed-take-bit-int-less-exp-word*
   by (*metis diff-le-mono less-imp-diff-less linorder-not-le one-le-numeral power-increasing sint-above-size wsst-TYs*(*3*))
  then have $hi2$: $sint\ (scast\ (signed\text{-}take\text{-}bit\ (inBits - 1)\ val)) < 2\ \widehat{}\ (inBits - 1)$
    by (*smt* (*verit*) *One-nat-def lo signed-scast-eq signed-take-bit-int-less-eq-self-iff sint-lt*)
  show *?thesis*
    unfolding *bit-bounds.simps fst-def ival*
    using *assms lo2 hi2 order-le-less*
    by (*smt* (*verit, best*) *Value.simps*(*14*) *Value.simps*(*8*) *sign-extend-helper.simps*)
qed

lemma *sign-extend-helper-output-range32*:

assumes *result = sign-extend-helper inBits outBits val*
assumes *result = IntVal32 ival*
shows *outBits ≤ 32 ∧ −(2 ^ (inBits − 1)) ≤ sint ival ∧ sint ival ≤ 2 ^ (inBits − 1)*

proof −
  have *ival*: *ival = (signed-take-bit (inBits − 1) val)*
    using *assms sign-extend-helper.simps*
     by (*smt (verit, ccfv-SIG) Value.distinct(1) Value.inject(1) Value.simps(14) scast-id*)
  have *def*: *result ≠ UndefVal*
    using *assms*
    by *blast*
  then have *ok*: *0 < inBits ∧ inBits ≤ 32 ∧*
     inBits ≤ outBits ∧
     outBits ∈ valid-int-widths ∧
     inBits ∈ valid-int-widths
    using *assms sign-extend-helper-ok* **by** *blast*
  then have *lo*: *−(2 ^ (inBits − 1)) ≤ sint (signed-take-bit (inBits − 1) val)*
    using *signed-take-bit-int-greater-eq-minus-exp-word*
     by (*smt (verit, best) diff-le-self not-less power-increasing-iff sint-below-size wsst-TYs(3)*)
  have *hi*: *sint (signed-take-bit (inBits − 1) val) < 2 ^ (inBits − 1)*
    using *signed-take-bit-int-less-exp-word*
   by (*metis diff-le-mono less-imp-diff-less linorder-not-le one-le-numeral power-increasing sint-above-size wsst-TYs(3)*)
  show *?thesis*
    unfolding *bit-bounds.simps fst-def ival*
    using *assms ival ok lo hi order-le-less*
    by *force*
qed

9.4.2 Support Lemmas for integer input/output size of unary and binary operators

These help us to deduce integer sizes through expressions. Not used yet.

lemma *unary-abs-io32*:
  assumes *result = unary-eval UnaryAbs val*
  assumes *result = IntVal32 r32*
  shows *∃ v32. val = IntVal32 v32*
  by (*smt (verit, best) Value.distinct(9) Value.simps(6) assms(1) assms(2) int-val-abs.elims unary-eval.simps(1)*)

lemma *unary-abs-io64*:
  assumes *result = unary-eval UnaryAbs val*
  assumes *result = IntVal64 r64*
  shows *∃ v64. val = IntVal64 v64*
  by (*metis Value.collapse(2) Value.collapse(3) Value.collapse(4) Value.disc(3) Value.exhaust-disc Value.simps(8) assms(1) assms(2) intval-abs.simps(1) intval-abs.simps(5)*)

is-IntVal32-def unary-eval.simps(1) unary-obj unary-undef)

lemma *unary-neg-io32*:
  assumes *result = unary-eval UnaryNeg val*
  assumes *result = IntVal32 r32*
  shows $\exists$ *v32. val = IntVal32 v32*
  by (*metis Value.disc(7) Value.distinct(1) assms(1) assms(2) intval-negate.elims*
is-IntVal64-def unary-eval.simps(2))

lemma *unary-neg-io64*:
  assumes *result = unary-eval UnaryNeg val*
  assumes *result = IntVal64 r64*
  shows $\exists$ *v64. val = IntVal64 v64*
  by (*metis Value.disc(3) Value.simps(8) assms(1) assms(2) intval-negate.elims*
is-IntVal32-def unary-eval.simps(2))

9.4.3 Validity of UnaryAbs

A set of lemmas for each evaltree step. Questions: 1. do we need separate 32/64 lemmas? Yes, I think so, because almost every operator behaves differently on each width. And it makes the matching more direct, does not need is_IntVal_def etc. 2. is this top-down approach (assume the result node evaluation) best? Maybe. It seems to be the shortest/simplest trigger?

lemma *unary-abs-result64*:
  assumes $[m,p] \vdash$ (*UnaryExpr UnaryAbs e*) $\mapsto$ *IntVal64 v*
  obtains *ve* **where** ($[m, p] \vdash e \mapsto$ *IntVal64 ve*) $\wedge$
      $v = $ (*if ve $<s$ 0 then $-ve$ else ve*)
proof $-$
  obtain *ve* **where** $[m,p] \vdash e \mapsto$ *IntVal64 ve*
    by (*smt (verit, best) assms UnaryExprE Value.distinct evalDet intval-abs.elims*
unary-eval.simps(1))
  then show *?thesis*
     by (*metis UnaryExprE Value.sel(2) assms evalDet intval-abs.simps(2) that*
unary-eval.simps(1))
qed

lemma *unary-abs-result32*:
  assumes *1*:$[m,p] \vdash$ (*UnaryExpr UnaryAbs e*) $\mapsto$ *IntVal32 v*
  shows $\exists$ *ve.* ($[m, p] \vdash e \mapsto$ *IntVal32 ve*) $\wedge$
      $v = $ (*if ve $<s$ 0 then $-ve$ else ve*)
proof $-$
  obtain *ve* **where** $[m,p] \vdash e \mapsto$ *IntVal32 ve*
     by (*smt (verit, best) 1 UnaryExprE Value.distinct evalDet intval-abs.elims*
unary-eval.simps(1))
  then show *?thesis*
  by (*metis UnaryExprE Value.inject(1) assms evalDet intval-abs.simps(1) unary-eval.simps(1)*)
qed

lemma *unary-abs-implies-valid-value*:
  assumes *1*:$[m,p] \vdash expr \mapsto val$
  assumes *2*:*result = unary-eval UnaryAbs val*
  assumes *3*:*result $\neq$ UndefVal*
  assumes *4*:*valid-value val (stamp-expr expr)*
  shows *valid-value result (stamp-expr (UnaryExpr UnaryAbs expr))*
proof −
  have *5*:$[m,p] \vdash (UnaryExpr\ UnaryAbs\ expr) \mapsto result$
    using *assms* **by** *blast*
  then have *6*: *is-IntegerStamp (stamp-expr expr)*
    using *assms valid-value.elims(2)* **by** *fastforce*
  then consider *v32* **where** *result = IntVal32 v32* | *v64* **where** *result = IntVal64 v64*
  by *(metis 2 4 Stamp.collapse(1) intval-abs.simps(1) intval-abs.simps(2) unary-eval.simps(1) valid32or64)*
  then show *?thesis*
  proof *cases*
    case *1*
    then obtain *ve* **where** *ve*: $([m, p] \vdash expr \mapsto IntVal32\ ve) \wedge$
        result = (if ve <s 0 then IntVal32 (−ve) else IntVal32 ve)
      using *5 unary-abs-result32* **by** *metis*
    then have *32*: *val = IntVal32 ve*
      using *assms(1) evalDet* **by** *presburger*

    then obtain *b lo hi* **where** *se*: *stamp-expr expr = IntegerStamp b lo hi*
      using *6 is-IntegerStamp-def* **by** *auto*
    then have $((b=32 \vee b=16 \vee b=8 \vee b=1) \wedge (lo \leq sint\ ve) \wedge (sint\ ve \leq hi))$
      using *4 32 se* **by** *simp*
      then have *stamp-expr (UnaryExpr UnaryAbs expr) = unrestricted-stamp (IntegerStamp 32 lo hi)*
      using *se* **by** *fastforce*
    then show *?thesis*
      using *1 unrestricted-32bit-always-valid* **by** *presburger*
  next
    case *2*
    then obtain *ve* **where** *ve*: $([m, p] \vdash expr \mapsto IntVal64\ ve) \wedge$
        result = (if ve <s 0 then IntVal64 (−ve) else IntVal64 ve)
      using *5 unary-abs-result64* **by** *metis*
    then have *64*: *val = IntVal64 ve*
      using *assms(1) evalDet* **by** *presburger*

    then obtain *b lo hi* **where** *se*: *stamp-expr expr = IntegerStamp b lo hi*
      using *6 is-IntegerStamp-def* **by** *auto*
    then have *range64*: $b=64 \wedge (lo \leq sint\ ve) \wedge (sint\ ve \leq hi)$
      using *4 64 se* **by** *simp*
      then have *stamp-expr (UnaryExpr UnaryAbs expr) = unrestricted-stamp (IntegerStamp b lo hi)*

using *se* **by** *simp*
  then show *?thesis*
    by (*metis 2 range64 unrestricted-64bit-always-valid*)
  qed
qed

9.4.4 Validity of UnaryNeg

lemma *unary-neg-implies-valid-value*:
  assumes *1*:$[m,p] \vdash expr \mapsto val$
  assumes *2*:*result = unary-eval UnaryNeg val*
  assumes *3*:*result $\neq$ UndefVal*
  assumes *4*:*valid-value val* (*stamp-expr expr*)
  shows *valid-value result* (*stamp-expr* (*UnaryExpr UnaryNeg expr*))
proof −
  have *6*: *result = intval-negate val*
    using *assms* **by** *auto*
  then have *7*: *is-IntegerStamp* (*stamp-expr expr*)
    using *assms valid-value.elims*(*2*) **by** *fastforce*
  then obtain *b lo hi* **where** *se*: *stamp-expr expr = IntegerStamp b lo hi*
    using *7 assms valid-value.elims*(*2*) *is-IntegerStamp-def* **by** *auto*
  then have *stamp-expr* (*UnaryExpr UnaryNeg expr*) *= unrestricted-stamp* (*IntegerStamp*
(*if b=64 then 64 else 32*) *lo hi*)
    using *assms* **by** *auto*
  then show *?thesis*
    using *assms 6 se*
  by (*smt* (*verit, best*) *intval-negate.simps*(*1*) *intval-negate.simps*(*2*) *unrestricted-32bit-always-valid*
unrestricted-64bit-always-valid valid32or64 valid-int64 valid-value.simps(*2*))
qed

9.4.5 Validity of UnaryNot

lemma *unary-not-implies-valid-value*:
  assumes *1*:$[m,p] \vdash expr \mapsto val$
  assumes *2*:*result = unary-eval UnaryNot val*
  assumes *3*:*result $\neq$ UndefVal*
  assumes *4*:*valid-value val* (*stamp-expr expr*)
  shows *valid-value result* (*stamp-expr* (*UnaryExpr UnaryNot expr*))
proof −
  have *6*: *result = intval-not val*
    using *assms* **by** *auto*
  then have *7*: *is-IntegerStamp* (*stamp-expr expr*)
    using *assms valid-value.elims*(*2*) **by** *fastforce*
  then obtain *b lo hi* **where** *se*: *stamp-expr expr = IntegerStamp b lo hi*
    using *7 assms valid-value.elims*(*2*) *is-IntegerStamp-def* **by** *auto*
  then have *stamp-expr* (*UnaryExpr UnaryNot expr*) *= unrestricted-stamp* (*IntegerStamp*
(*if b=64 then 64 else 32*) *lo hi*)
    using *assms* **by** *auto*
  then show *?thesis*
    using *assms 6 se*

by (*smt* (*verit, best*) *intval-not.simps*(*1*) *intval-not.simps*(*2*) *unrestricted-32bit-always-valid*
unrestricted-64bit-always-valid valid32or64 valid-int64 valid-value.simps(*2*))
qed

9.4.6 Validity of UnaryLogicNegation

lemma *unary-logic-negation-implies-valid-value*:
  assumes *1*:[*m,p*] ⊢ *expr* ↦ *val*
  assumes *2*:*result = unary-eval UnaryLogicNegation val*
  assumes *3*:*result ≠ UndefVal*
  assumes *4*:*valid-value val* (*stamp-expr expr*)
  shows *valid-value result* (*stamp-expr* (*UnaryExpr UnaryLogicNegation expr*))
proof −
  have *6*: *result = intval-logic-negation val*
    using *assms* **by** *auto*
  then have *7*: *is-IntegerStamp* (*stamp-expr expr*)
    using *assms valid-value.elims*(*2*) **by** *fastforce*
  then obtain *b lo hi* **where** *se*: *stamp-expr expr = IntegerStamp b lo hi*
    using *7 assms valid-value.elims*(*2*) *is-IntegerStamp-def* **by** *auto*
 then have *stamp-expr* (*UnaryExpr UnaryLogicNegation expr*) = *unrestricted-stamp*
(*IntegerStamp* (*if b=64 then 64 else 32*) *lo hi*)
    using *assms* **by** *auto*
  then show *?thesis*
    using *assms 6 se*
  by (*smt* (*verit, best*) *intval-logic-negation.simps*(*1*) *intval-logic-negation.simps*(*2*)
unrestricted-32bit-always-valid unrestricted-64bit-always-valid valid32or64 valid-int64
valid-value.simps(*2*))
qed

9.4.7 Validity of UnaryNarrow

Possibly helpful lemmas about mod - mostly not used now.

lemma *uint-distr-mod*:
  fixes *n :: nat*
  assumes $n < LENGTH('a)$
  shows *uint* ((*uval* :: *'a* :: *len word*) *mod* $2\hat{}n$) = *uint uval mod* $2\hat{}n$
  by (*metis take-bit-eq-mod unsigned-take-bit-eq*)

lemma *sint-mod-not-sign-bit*:
  fixes *n :: nat*
  assumes $n < LENGTH('a)$
  shows ¬ *bit* ((*uval* :: *'a* :: *len word*) *mod* $2\hat{}n$) *LENGTH*(*'a*)
  by *simp*

lemma *sint-mod-upper-bound*:
  fixes *n :: nat*
  assumes $n < LENGTH('a)$
  shows *sint* ((*uval* :: *'a* :: *len word*) *mod* $2\hat{}n$) < $2\hat{}n$
  by (*metis assms*(*1*) *signed-take-bit-eq take-bit-eq-mod take-bit-int-less-exp*)

168

lemma *sint-mod-lower-bound*:
  fixes n :: *nat*
  assumes $n < LENGTH('a)$
  shows $0 \leq$ *sint* $((uval :: 'a :: len\ word)\ mod\ 2\string^n)$
  unfolding *sint-uint*
  by (*metis assms signed-take-bit-eq sint-uint take-bit-eq-mod take-bit-nonnegative*)

lemma *sint-mod-range*:
  fixes n :: *nat*
  assumes $n < LENGTH('a)$
  assumes *smaller* $= ((val :: 'a :: len\ word)\ mod\ 2\string^n)$
  shows $0 \leq$ *sint smaller* $\wedge$ *sint smaller* $< 2\string^n$
  using *assms sint-mod-upper-bound sint-mod-lower-bound*
  using *le-less* **by** *blast*

lemma *sint-mod-eq-uint*:
  fixes n :: *nat*
  assumes $n < LENGTH('a)$
  shows *sint* $((uval :: 'a :: len\ word)\ mod\ 2\string^n) =$ *uint* $(uval\ mod\ 2\string^n)$
  unfolding *sint-uint*
 by (*metis Suc-pred assms le-less len-gt-0 signed-take-bit-eq sint-uint take-bit-eq-mod*
       take-bit-signed-take-bit unsigned-take-bit-eq)

lemma *unary-narrow-helper32*:
  assumes $[m,p] \vdash expr \mapsto IntVal32\ i32$
  assumes *stamp-expr expr* $= IntegerStamp\ b\ lo\ hi$
  assumes $r32 = signed\text{-}take\text{-}bit\ (outBits - 1)\ i32$
  assumes *result* $= IntVal32\ r32$
  assumes $outBits{=}32 \vee outBits{=}16 \vee outBits{=}8 \vee outBits{=}1$
  assumes *stamp-expr* (*UnaryExpr* (*UnaryNarrow inBits outBits*) *expr*)
      $=$ *unrestricted-stamp* (*IntegerStamp outBits lo hi*)
  shows *valid-value result* (*stamp-expr* (*UnaryExpr* (*UnaryNarrow inBits outBits*)
expr))
proof $-$
  have *hi*: *sint* $r32 < 2\string^(outBits{-}1)$
    using *assms signed-take-bit-int-less-exp-word*
    by (*metis diff-le-mono less-imp-diff-less linorder-not-le one-le-numeral*
        power-increasing sint-above-size word-size)
  then have *lo*: $- (2\string^(outBits{-}1)) \leq$ *sint* $r32$
    using *assms signed-take-bit-int-greater-eq-minus-exp-word*
    by (*smt* (*verit, best*) *diff-le-self less-le-trans power-less-imp-less-exp sint-ge*)
  then show *?thesis*
    using *assms lo hi* **apply** *simp*
    by (*metis int-power-div-base lessI zero-less-numeral*)
qed

lemma *unary-narrow-helper64*:
  assumes $[m,p] \vdash expr \mapsto IntVal64\ i64$
  assumes *stamp-expr expr* = *IntegerStamp b lo hi*
  assumes $r32 = signed\text{-}take\text{-}bit\ (outBits - 1)\ (scast\ i64)$
  assumes *result* = *IntVal32 r32*
  assumes *outBits=32* ∨ *outBits=16* ∨ *outBits=8* ∨ *outBits=1*
  assumes *stamp-expr* (*UnaryExpr* (*UnaryNarrow inBits outBits*) *expr*)
        = *unrestricted-stamp* (*IntegerStamp outBits lo hi*)
  shows *valid-value result* (*stamp-expr* (*UnaryExpr* (*UnaryNarrow inBits outBits*)
expr))
proof −
  have *hi*: *sint r32* $< 2\widehat{}\ (outBits-1)$
    using *assms signed-take-bit-int-less-exp-word*
    by (*metis diff-le-mono less-imp-diff-less linorder-not-le one-le-numeral*
        power-increasing sint-above-size word-size)
  then have *lo*: $- (2\widehat{}\ (outBits-1)) \leq sint\ r32$
    using *assms signed-take-bit-int-greater-eq-minus-exp-word*
    by (*smt* (*verit, best*) *diff-le-self less-le-trans power-less-imp-less-exp sint-ge*)
  then show *?thesis*
    using *assms lo hi* **apply** *simp*
    by (*metis int-power-div-base lessI zero-less-numeral*)
qed

lemma *unary-narrow-implies-valid-value*:
  assumes $[m,p] \vdash expr \mapsto val$
  assumes *result* = *unary-eval* (*UnaryNarrow inBits outBits*) *val*
  assumes *result* ≠ *UndefVal*
  assumes *valid-value val* (*stamp-expr expr*)
  shows *valid-value result* (*stamp-expr* (*UnaryExpr* (*UnaryNarrow inBits outBits*)
expr))
proof −

  have *i*: *is-IntegerStamp* (*stamp-expr expr*)
    using *assms valid-value.elims*(*2*) **by** *fastforce*
  then obtain *b lo hi* **where** *se*:*stamp-expr expr* = *IntegerStamp b lo hi*
    by (*auto simp add*: *assms valid-value.elims*(*2*) *is-IntegerStamp-def*)
  then have *u*: *stamp-expr* (*UnaryExpr* (*UnaryNarrow inBits outBits*) *expr*)
        = *unrestricted-stamp* (*IntegerStamp outBits lo hi*)
    by *simp*

  have *r*: *result* = *intval-narrow inBits outBits val*
    by (*simp add*: *assms*(*2*))
  then have *ok*: *0* < *outBits* ∧ *outBits* ≤ *inBits* ∧
      outBits ∈ *valid-int-widths* ∧ *inBits* ∈ *valid-int-widths*
    using *assms intval-narrow-ok* **by** *simp*
  then consider *i32* **where** *val* = *IntVal32 i32* | *i64* **where** *val* = *IntVal64 i64*
    using *assms* **by** (*metis se valid32or64*)
  then show *?thesis*

proof *cases*
  case *1*
  then have *r1*: *result = narrow-helper inBits outBits i32*
    using *assms r* **by** (*metis intval-narrow.simps(1)*)
  then have *r2*: *result = (IntVal32 (signed-take-bit (outBits − 1) i32))*
    using *assms* **by** (*metis narrow-helper.simps*)
  then obtain *r32* **where**
    r32: *result = IntVal32 r32 ∧ r32 = signed-take-bit (outBits − 1) i32*
    by *simp*
  then have *outBits=32 ∨ outBits=16 ∨ outBits=8 ∨ outBits=1*
    using *ok 1 assms* **by** *force*
  then show *?thesis*
    using *ok 1 assms u r32 se unary-narrow-helper32* **by** *force*
next
  case *2*
  then have *in64*: *inBits = 64*
    using *assms ok intval-narrow.simps(2) r* **by** *presburger*
  then show *?thesis*
    proof (*cases outBits = 64*)
      case *True*
      then show *?thesis*
       using *2 in64 r u intval-narrow.simps(2) unrestricted-64bit-always-valid* **by**
presburger
    next
      case *False*

      then have *out32*: *outBits=32 ∨ outBits=16 ∨ outBits=8 ∨ outBits=1*
       using *ok assms* **by** *force*
      then have *r1*: *result = narrow-helper inBits outBits (scast i64)*
       using *assms 2 False in64 r ok narrow-takes-64* **by** *simp*
     then have *r2*: *result = (IntVal32 (signed-take-bit (outBits − 1) (scast i64)))*
       using *assms* **by** (*metis narrow-helper.simps*)
      then obtain *r32* **where**
        r32: *result = IntVal32 r32 ∧ r32 = signed-take-bit (outBits − 1) (scast
i64)*
        by *simp*
      then show *?thesis*
       using *assms 2 r32 out32 u se unary-narrow-helper64* **by** *blast*
    qed
  qed
qed

9.4.8 Validity of UnarySignExtend

lemma *valid-sign-extend32-or-less*:
  assumes (*result :: int32*) = *scast* (*v :: 'a :: len word*)
  assumes $LENGTH('a) = 32 ∨ LENGTH('a) = 16 ∨ LENGTH('a) = 8 ∨$
$LENGTH('a) = 1$
  shows *valid-value* (*IntVal32 result*) (*IntegerStamp LENGTH('a)*

$(fst\ (bit\text{-}bounds\ (LENGTH('a))))$
$(snd\ (bit\text{-}bounds\ (LENGTH('a)))))$
unfolding *valid-value.simps*
using *scast-bigger-bit-bounds assms* **by** *blast*

lemma *valid-sign-extend64*:
  assumes $(result :: int64) = scast\ (v :: 'a :: len\ word)$
  shows *valid-value* $(IntVal64\ result)$ $(IntegerStamp\ 64$
               $(fst\ (bit\text{-}bounds\ (LENGTH('a))))$
               $(snd\ (bit\text{-}bounds\ (LENGTH('a))))))$
  unfolding *valid-value.simps*
  using *scast-bigger-bit-bounds*
  using *assms(1) len-gt-0* **by** *blast*

lemma *unary-sign-extend-implies-valid-value*:
  assumes $[m,p] \vdash expr \mapsto val$
  assumes $result = unary\text{-}eval\ (UnarySignExtend\ inBits\ outBits)\ val$
  assumes $result \neq UndefVal$
  assumes *valid-value val (stamp-expr expr)*
  shows *valid-value result (stamp-expr (UnaryExpr (UnarySignExtend inBits out-Bits) expr))*
proof −

  have *i*: *is-IntegerStamp (stamp-expr expr)*
    using *assms valid-value.elims(2)* **by** *fastforce*
  then obtain *b lo hi* **where** *se*:*stamp-expr expr = IntegerStamp b lo hi*
    by (*auto simp add*: *assms valid-value.elims(2) is-IntegerStamp-def*)
  then have *u*: *stamp-expr (UnaryExpr (UnarySignExtend inBits outBits) expr)*
        = *unrestricted-stamp (IntegerStamp outBits lo hi)*
    by *simp*
  then show *?thesis*
  proof (*cases is-IntVal64 val*)
    case *True*
    then show *?thesis*
      using *assms u unrestricted-64bit-always-valid*
      using *is-IntVal64-def* **by** *fastforce*
  next
    case *False*
    then obtain *i32* **where** *i32*: *result = sign-extend-helper inBits outBits i32*
      using *assms intval-sign-extend.simps*
      by (*metis is-IntVal64-def se unary-eval.simps(6) valid32or64*)
    then have *ok*: $0 < inBits \wedge inBits \leq 32 \wedge inBits \leq outBits \wedge$
      $outBits \in valid\text{-}int\text{-}widths \wedge inBits \in valid\text{-}int\text{-}widths$
      using *assms sign-extend-helper-ok* **by** *blast*
    then show *?thesis*
    proof (*cases outBits = 64*)
      case *True*

then obtain *r64* **where** *result = IntVal64 r64*
          by (*metis assms(3) i32 sign-extend-helper.simps*)
        then show *?thesis*
          using *True u unrestricted-64bit-always-valid* **by** *presburger*
    next
      case *False*
      then obtain *r32* **where** *r32*: *result = IntVal32 r32*
        using *ok i32* **by** *force*
     then have *lohi*: $-(2\ \hat{}\ (inBits - 1)) \leq sint\ r32 \wedge sint\ r32 < 2\ \hat{}\ (inBits - 1)$
        using *sign-extend-helper-output-range32*
        by (*smt* (*verit, ccfv-threshold*) *False Value.inject(1) assms(3) diff-le-self i32*
linorder-not-le power-less-imp-less-exp sign-extend-helper.simps signed-take-bit-int-less-exp-word
sint-lt)
      then have *bnds*: $fst\ (bit\text{-}bounds\ inBits) \leq sint\ r32 \wedge sint\ r32 \leq snd\ (bit\text{-}bounds$
inBits)
        unfolding *bit-bounds.simps fst-def*
        using *ok lower-bounds-equiv upper-bounds-equiv* **by** *simp*
       then have *v*: *valid-value result* (*unrestricted-stamp* (*IntegerStamp inBits lo*
hi))
        using *ok r32* **by** *force*
      then have *outBits=1 $\vee$ outBits=8 $\vee$ outBits=16 $\vee$ outBits=32*
        using *ok False* **by** *fastforce*
      then show *?thesis*
        unfolding *u* **using** *ok v r32 larger-stamp32-always-valid* **by** *presburger*
    qed
  qed
qed

9.4.9 Validity of all Unary Operators

lemma *unary-eval-implies-valid-value*:
  assumes $[m,p] \vdash expr \mapsto val$
  assumes *result = unary-eval op val*
  assumes *result $\neq$ UndefVal*
  assumes *valid-value val* (*stamp-expr expr*)
  shows *valid-value result* (*stamp-expr* (*UnaryExpr op expr*))
proof (*cases op*)
  case *UnaryAbs*
  then show *?thesis* **using** *assms unary-abs-implies-valid-value* **by** *presburger*
next
  case *UnaryNeg*
  then show *?thesis* **using** *assms unary-neg-implies-valid-value* **by** *presburger*
next
  case *UnaryNot*
  then show *?thesis* **using** *assms unary-not-implies-valid-value* **by** *presburger*
next
  case *UnaryLogicNegation*
  then show *?thesis* **using** *assms unary-logic-negation-implies-valid-value* **by** *pres-*
burger

next
  case (*UnaryNarrow x51 x52*)
  then show *?thesis* **using** *assms unary-narrow-implies-valid-value* **by** *presburger*
next
  case (*UnarySignExtend x61 x62*)
  then show *?thesis* **using** *assms unary-sign-extend-implies-valid-value* **by** *pres-burger*
next
  case (*UnaryZeroExtend x71 x72*)
  then show *?thesis* **sorry**
qed

9.4.10 Support Lemmas for Binary Operators

lemma *binary-undef*: *v1 = UndefVal ∨ v2 = UndefVal ⟹ bin-eval op v1 v2 = UndefVal*
  by (*cases op*; *auto*)

lemma *binary-obj*: *v1 = ObjRef x ∨ v2 = ObjRef y ⟹ bin-eval op v1 v2 = UndefVal*
  by (*cases op*; *auto*)

lemma *binary-eval-implies-valid-value*:
  assumes *[m,p] ⊢ expr1 ↦ val1*
  assumes *[m,p] ⊢ expr2 ↦ val2*
  assumes *result = bin-eval op val1 val2*
  assumes *result ≠ UndefVal*
  assumes *valid-value val1 (stamp-expr expr1)*
  assumes *valid-value val2 (stamp-expr expr2)*
  shows *valid-value result (stamp-expr (BinaryExpr op expr1 expr2))*
proof −
  have *is-IntVal*: ∃ *x y. result = IntVal32 x ∨ result = IntVal64 y*
    using *assms(1,2,3,4)* **apply** (*cases op*; *auto*; *cases val1*; *auto*; *cases val2*; *auto*)
    by (*meson Values.bool-to-val.elims*)+
  then have *expr1-intstamp*: *is-IntegerStamp (stamp-expr expr1)*
   using *assms(1,3,4,5)* **apply** (*cases (stamp-expr expr1)*; *auto simp*: *valid-VoidStamp binary-undef*)
    using *valid-ObjStamp binary-obj* **apply** (*metis assms(4)*)
    using *valid-ObjStamp binary-obj* **by** (*metis assms(4)*)
  from *is-IntVal* **have** *expr2-intstamp*: *is-IntegerStamp (stamp-expr expr2)*
   using *assms(2,3,4,6)* **apply** (*cases (stamp-expr expr2)*; *auto simp*: *valid-VoidStamp binary-undef*)
    using *valid-ObjStamp binary-obj* **apply** (*metis assms(4)*)
    using *valid-ObjStamp binary-obj* **by** (*metis assms(4)*)
  from *expr1-intstamp* **obtain** *b1 lo1 hi1* **where** *stamp-expr1-def*: *stamp-expr expr1*

174

$= (IntegerStamp\ b1\ lo1\ hi1)$
    using *is-IntegerStamp-def* **by** *auto*
   from *expr2-intstamp* **obtain** *b2 lo2 hi2* **where** *stamp-expr2-def*: *stamp-expr*
$expr2 = (IntegerStamp\ b2\ lo2\ hi2)$
    using *is-IntegerStamp-def* **by** *auto*

  have $b1 = b2$
   using *assms(3,4,5,6) stamp-expr1-def stamp-expr2-def*
   sorry
  then have *stamp-def*: *stamp-expr* (*BinaryExpr op expr1 expr2*) =
    (*if op* $\notin$ *fixed-32* $\land$ *b1=64*
       then unrestricted-stamp (*IntegerStamp 64 lo1 hi1*)
       else unrestricted-stamp (*IntegerStamp 32 lo1 hi1*))
   using *stamp-expr.simps(2) stamp-binary.simps(1)*
   using *stamp-expr1-def stamp-expr2-def* **by** *presburger*
  show *?thesis*
   proof (*cases op* $\notin$ *fixed-32* $\land$ *b1=64*)
    case *True*
    then obtain x **where** *bit64*: *result = IntVal64 x*
     using *stamp-expr1-def assms* **by** (*cases op*; *cases val1*; *cases val2*; *simp*)
    then show *?thesis*
     by (*metis True stamp-def unrestricted-64bit-always-valid*)
   next
    case *False*
    then obtain x **where** *bit32*: *result = IntVal32 x*
     using *assms stamp-expr1-def* **apply** (*cases op*; *cases val1*; *cases val2*; *auto*)
     by (*meson Values.bool-to-val.elims*)+
    then show *?thesis*
     using *False stamp-def unrestricted-32bit-always-valid* **by** *presburger*
   qed
  qed

9.4.11   Validity of Stamp Meet and Join Operators

lemma *stamp-meet-is-valid*:
  assumes *valid-value val stamp1* $\lor$ *valid-value val stamp2*
  assumes *meet stamp1 stamp2* $\neq$ *IllegalStamp*
  shows *valid-value val* (*meet stamp1 stamp2*)
  using *assms*
proof (*cases stamp1*)
  case *VoidStamp*
   then show *?thesis*
    by (*metis Stamp.exhaust assms(1) assms(2) meet.simps(1) meet.simps(37)*
meet.simps(44) meet.simps(51) meet.simps(58) meet.simps(65) meet.simps(66) meet.simps(67))
  next
  case (*IntegerStamp b lo hi*)

obtain *b2 lo2 hi2* **where** *stamp2-def*: *stamp2 = IntegerStamp b2 lo2 hi2*
  by (*metis IntegerStamp assms*(*2*) *meet.simps*(*45*) *meet.simps*(*52*) *meet.simps*(*59*)
meet.simps(*6*) *meet.simps*(*65*) *meet.simps*(*66*) *meet.simps*(*67*) *unrestricted-stamp.cases*)
  then have *b = b2* **using** *meet.simps*(*2*) *assms*(*2*)
    by (*metis IntegerStamp*)
  then have *meet-def*: *meet stamp1 stamp2 = (IntegerStamp b (min lo lo2) (max hi hi2))*
    by (*simp add*: *IntegerStamp stamp2-def*)
  then show *?thesis* **proof** (*cases b = 64*)
    case *True*
    then obtain *x* **where** *val-def*: *val = IntVal64 x*
      using *IntegerStamp assms*(*1*) *valid64*
      using ‹*b = b2*› *stamp2-def* **by** *blast*
    have *min*: *sint x ≥ min lo lo2*
      using *val-def*
      using *IntegerStamp assms*(*1*)
      using *stamp2-def* **by** *force*
    have *max*: *sint x ≤ max hi hi2*
      using *val-def*
      using *IntegerStamp assms*(*1*)
      using *stamp2-def* **by** *force*
    from *min max* **show** *?thesis*
      by (*simp add*: *True meet-def val-def*)
  next
    case *False*
    then have *bit32*: *b = 32 ∨ b = 16 ∨ b = 8 ∨ b = 1*
      using *assms*(*1*) *IntegerStamp valid-value.simps valid32or64-both*
      by (*metis* ‹*b = b2*› *stamp2-def*)
    then obtain *x* **where** *val-def*: *val = IntVal32 x*
      using *IntegerStamp assms*(*1*) *valid32 valid-int16 valid-int8 valid-int1*
      using ‹*b = b2*› *stamp2-def* **by** *blast*
    have *min*: *sint x ≥ min lo lo2*
      using *val-def*
      using *IntegerStamp assms*(*1*)
      using *stamp2-def* **by** *force*
    have *max*: *sint x ≤ max hi hi2*
      using *val-def*
      using *IntegerStamp assms*(*1*)
      using *stamp2-def* **by** *force*
    from *min max* **show** *?thesis*
      using *bit32 meet-def val-def valid-value.simps*(*1*) **by** *presburger*
  qed
next
  case (*KlassPointerStamp x31 x32*)
  then show *?thesis* **using** *assms valid-value.elims*(*2*)
    by *fastforce*
next
  case (*MethodCountersPointerStamp x41 x42*)
  then show *?thesis* **using** *assms valid-value.elims*(*2*)

by *fastforce*
next
  case (*MethodPointersStamp x51 x52*)
  then show *?thesis* **using** *assms valid-value.elims(2)*
    by *fastforce*
next
  case (*ObjectStamp x61 x62 x63 x64*)
  then show *?thesis* **using** *assms*
    using *meet.simps(34)* **by** *blast*
next
  case (*RawPointerStamp x71 x72*)
  then show *?thesis* **using** *assms*
    using *meet.simps(35)* **by** *blast*
next
  case *IllegalStamp*
  then show *?thesis* **using** *assms*
    using *meet.simps(36)* **by** *blast*
qed

lemma *conditional-eval-implies-valid-value*:
  assumes $[m,p] \vdash cond \mapsto condv$
  assumes *expr* = (*if val-to-bool condv then expr1 else expr2*)
  assumes $[m,p] \vdash expr \mapsto val$
  assumes $val \neq UndefVal$
  assumes *valid-value condv* (*stamp-expr cond*)
  assumes *valid-value val* (*stamp-expr expr*)
  assumes *compatible* (*stamp-expr expr1*) (*stamp-expr expr2*)
  shows *valid-value val* (*stamp-expr* (*ConditionalExpr cond expr1 expr2*))
proof −
  have *meet* (*stamp-expr expr1*) (*stamp-expr expr2*) $\neq$ *IllegalStamp*
    using *assms*
  by (*metis Stamp.distinct(13) Stamp.distinct(25) compatible.elims(2) meet.simps(1)*
meet.simps(2))
  then show *?thesis* **using** *stamp-meet-is-valid* **using** *stamp-expr.simps(6)*
    using *assms(2) assms(6)* **by** *presburger*
qed

9.4.12 Validity of Whole Expression Tree Evaluation

experiment begin
lemma *stamp-implies-valid-value*:
  assumes $[m,p] \vdash expr \mapsto val$
  shows *valid-value val* (*stamp-expr expr*)
  using *assms* **proof** (*induction expr val*)
  case (*UnaryExpr expr val result op*)
    then show *?case* **using** *unary-eval-implies-valid-value* **by** *simp*
  next
    case (*BinaryExpr expr1 val1 expr2 val2 result op*)

then show *?case* **using** *binary-eval-implies-valid-value* **by** *simp*
next
  case (*ConditionalExpr cond condv expr expr1 expr2 val*)
  then show *?case* **using** *conditional-eval-implies-valid-value* **sorry**
next
  case (*ParameterExpr x1 x2*)
  then show *?case* **by** *auto*
next
  case (*LeafExpr x1 x2*)
  then show *?case* **by** *auto*
next
  case (*ConstantExpr x*)
  then show *?case* **by** *auto*
qed

lemma *value-range*:
  assumes $[m, p] \vdash e \mapsto v$
  shows $v \in \{val\ .\ valid\text{-}value\ val\ (stamp\text{-}expr\ e)\}$
  using *assms* **sorry**
end

lemma *upper-bound-32*:
  assumes *val* = *IntVal32 v*
  assumes $\exists\ l\ h.\ s = (IntegerStamp\ 32\ l\ h)$
  shows $valid\text{-}value\ val\ s \implies sint\ v \leq (stpi\text{-}upper\ s)$
  using *assms* **by** *force*

lemma *upper-bound-64*:
  assumes *val* = *IntVal64 v*
  assumes $\exists\ l\ h.\ s = (IntegerStamp\ 64\ l\ h)$
  shows $valid\text{-}value\ val\ s \implies sint\ v \leq (stpi\text{-}upper\ s)$
  using *assms* **by** *force*

lemma *lower-bound-32*:
  assumes *val* = *IntVal32 v*
  assumes $\exists\ l\ h.\ s = (IntegerStamp\ 32\ l\ h)$
  shows $valid\text{-}value\ val\ s \implies sint\ v \geq (stpi\text{-}lower\ s)$
  using *assms* **by** *force*

lemma *lower-bound-64*:
  assumes *val* = *IntVal64 v*
  assumes $\exists\ l\ h.\ s = (IntegerStamp\ 64\ l\ h)$
  shows $valid\text{-}value\ val\ s \implies sint\ v \geq (stpi\text{-}lower\ s)$
  using *assms*
  by *force*

lemma *stamp-under-semantics*:
  assumes *stamp-under* (*stamp-expr x*) (*stamp-expr y*)

assumes $[m, p] \vdash (BinaryExpr\ BinIntegerLessThan\ x\ y) \mapsto v$

assumes *xvalid*: $(\forall\ m\ p\ v.\ ([m,\ p] \vdash x \mapsto v) \longrightarrow valid\text{-}value\ v\ (stamp\text{-}expr\ x))$

assumes *yvalid*: $(\forall\ m\ p\ v.\ ([m,\ p] \vdash y \mapsto v) \longrightarrow valid\text{-}value\ v\ (stamp\text{-}expr\ y))$

shows *val-to-bool v*

proof −

  obtain *xval* **where** *xval-def*: $[m,\ p] \vdash x \mapsto xval$

    using *assms*(2) **by** *blast*

  obtain *yval* **where** *yval-def*: $[m,\ p] \vdash y \mapsto yval$

    using *assms*(2) **by** *blast*

  have *is-IntVal32 xval* $\lor$ *is-IntVal64 xval*

    by (*metis BinaryExprE Value.collapse*(3) *Value.collapse*(4) *Value.exhaust-disc assms*(2) *binary-obj evalDet evaltree-not-undef valid-value.simps*(19) *xval-def xvalid*)

  have *is-IntVal32 yval* $\lor$ *is-IntVal64 yval*

    by (*metis BinaryExprE Value.collapse*(3) *Value.collapse*(4) *Value.exhaust-disc assms*(2) *binary-obj evalDet evaltree-not-undef valid-value.simps*(19) *yval-def yvalid*)

  have *is-IntVal32 xval = is-IntVal32 yval*

    using *BinaryExprE Value.collapse*(2) ‹*is-IntVal32 xval* $\lor$ *is-IntVal64 xval*› ‹*is-IntVal32 yval* $\lor$ *is-IntVal64 yval*› *assms*(2) *bin-eval.simps*(11) *evalDet intval-less-than.simps*(12) *intval-less-than.simps*(5) *is-IntVal32-def xval-def yval-def*

    by (*smt* (*verit, ccfv-SIG*) *bin-eval.simps*(12))

  have *is-IntVal64 xval = is-IntVal64 yval*

    using ‹*is-IntVal32 xval = is-IntVal32 yval*› ‹*is-IntVal32 xval* $\lor$ *is-IntVal64 xval*› ‹*is-IntVal32 yval* $\lor$ *is-IntVal64 yval*› **by** *blast*

  have (*intval-less-than xval yval*) $\neq$ *UndefVal*

    using *assms*(2)

    by (*metis bin-eval.simps*(12) *evalDet unfold-binary xval-def yval-def*)

  have *is-IntVal32 xval* $\Longrightarrow$ $((\exists\ lo\ hi.\ stamp\text{-}expr\ x = IntegerStamp\ 32\ lo\ hi) \land (\exists\ lo\ hi.\ stamp\text{-}expr\ y = IntegerStamp\ 32\ lo\ hi))$

    sorry

  have *is-IntVal64 xval* $\Longrightarrow$ $((\exists\ lo\ hi.\ stamp\text{-}expr\ x = IntegerStamp\ 64\ lo\ hi) \land (\exists\ lo\ hi.\ stamp\text{-}expr\ y = IntegerStamp\ 64\ lo\ hi))$

    sorry

  have *xvalid*: *valid-value xval* (*stamp-expr x*)

    using *xvalid xval-def* **by** *auto*

  have *yvalid*: *valid-value yval* (*stamp-expr y*)

    using *yvalid yval-def* **by** *auto*

  { assume *c*: *is-IntVal32 xval*

  obtain *xxval* **where** *x32*: *xval = IntVal32 xxval*

    using *c is-IntVal32-def* **by** *blast*

  obtain *yyval* **where** *y32*: *yval = IntVal32 yyval*

    using ‹*is-IntVal32 xval = is-IntVal32 yval*› *c is-IntVal32-def* **by** *auto*

  have *xs*: $\exists\ lo\ hi.\ stamp\text{-}expr\ x = IntegerStamp\ 32\ lo\ hi$

    by (*simp add*: ‹*is-IntVal32 xval* $\Longrightarrow$ $(\exists\ lo\ hi.\ stamp\text{-}expr\ x = IntegerStamp\ 32\ lo\ hi) \land (\exists\ lo\ hi.\ stamp\text{-}expr\ y = IntegerStamp\ 32\ lo\ hi)$› *c*)

  have *ys*: $\exists\ lo\ hi.\ stamp\text{-}expr\ y = IntegerStamp\ 32\ lo\ hi$

    using ‹*is-IntVal32 xval* $\Longrightarrow$ $(\exists\ lo\ hi.\ stamp\text{-}expr\ x = IntegerStamp\ 32\ lo\ hi) \land (\exists\ lo\ hi.\ stamp\text{-}expr\ y = IntegerStamp\ 32\ lo\ hi)$› *c* **by** *blast*

have *sint xxval* ≤ *stpi-upper* (*stamp-expr x*)
    using *upper-bound-32 x32 xs xvalid* **by** *presburger*
  have *stpi-lower* (*stamp-expr y*) ≤ *sint yyval*
    using *lower-bound-32 y32 ys yvalid* **by** *presburger*
  have *stpi-upper* (*stamp-expr x*) < *stpi-lower* (*stamp-expr y*)
    using *assms*(*1*) **unfolding** *stamp-under.simps*
    by *auto*
  then have *xxval* <s *yyval*
    using *assms*(*1*) **unfolding** *stamp-under.simps*
    using ‹*sint xxval* ⊑ *stpi-upper* (*stamp-expr x*)› ‹*stpi-lower* (*stamp-expr y*) ⊑
sint yyval› *word-sless-alt* **by** *fastforce*
  then have (*intval-less-than xval yval*) = *IntVal32 1*
    by (*simp add: x32 y32*)
}
note *case32* = *this*
{ assume *c*: *is-IntVal64 xval*
  obtain *xxval* **where** *x64*: *xval* = *IntVal64 xxval*
    using *c is-IntVal64-def* **by** *blast*
  obtain *yyval* **where** *y64*: *yval* = *IntVal64 yyval*
    using ‹*is-IntVal64 xval* = *is-IntVal64 yval*› *c is-IntVal64-def* **by** *auto*
  have *xs*: ∃ *lo hi. stamp-expr x* = *IntegerStamp 64 lo hi*
    by (*simp add*: ‹*is-IntVal64 xval* ⟹ (∃ *lo hi. stamp-expr x* = *IntegerStamp 64
lo hi*) ∧ (∃ *lo hi. stamp-expr y* = *IntegerStamp 64 lo hi*)› *c*)
  have *ys*: ∃ *lo hi. stamp-expr y* = *IntegerStamp 64 lo hi*
    using ‹*is-IntVal64 xval* ⟹ (∃ *lo hi. stamp-expr x* = *IntegerStamp 64 lo hi*)
∧ (∃ *lo hi. stamp-expr y* = *IntegerStamp 64 lo hi*)› *c* **by** *blast*
  have *sint xxval* ≤ *stpi-upper* (*stamp-expr x*)
    using *upper-bound-64 x64 xs xvalid* **by** *presburger*
  have *stpi-lower* (*stamp-expr y*) ≤ *sint yyval*
    using *lower-bound-64 y64 ys yvalid* **by** *presburger*
  have *stpi-upper* (*stamp-expr x*) < *stpi-lower* (*stamp-expr y*)
    using *assms*(*1*) **unfolding** *stamp-under.simps*
    by *auto*
  then have *xxval* <s *yyval*
    using *assms*(*1*) **unfolding** *stamp-under.simps*
    using ‹*sint xxval* ⊑ *stpi-upper* (*stamp-expr x*)› ‹*stpi-lower* (*stamp-expr y*) ⊑
sint yyval› *word-sless-alt* **by** *fastforce*
  then have (*intval-less-than xval yval*) = *IntVal32 1*
    by (*simp add: x64 y64*)
}
note *case64* = *this*
have (*intval-less-than xval yval*) = *IntVal32 1*
  using ‹*is-IntVal32 xval* ∨ *is-IntVal64 xval*› *case32 case64* **by** *fastforce*
then show *?thesis*
  by (*metis EvalTreeE*(*5*) *assms*(*2*) *bin-eval.simps*(*12*) *evalDet val-to-bool.simps*(*1*)
xval-def yval-def zero-neq-one)
qed

lemma *stamp-under-semantics-inversed*:

assumes *stamp-under* (*stamp-expr y*) (*stamp-expr x*)
assumes [*m, p*] ⊢ (*BinaryExpr BinIntegerLessThan x y*) ↦ *v*
assumes *xvalid*: (∀ *m p v*. ([*m, p*] ⊢ *x* ↦ *v*) ⟶ *valid-value v* (*stamp-expr x*))
assumes *yvalid*: (∀ *m p v*. ([*m, p*] ⊢ *y* ↦ *v*) ⟶ *valid-value v* (*stamp-expr y*))
shows ¬(*val-to-bool v*)
proof −
 obtain *xval* **where** *xval-def*: [*m, p*] ⊢ *x* ↦ *xval*
  using *assms*(*2*) **by** *blast*
 obtain *yval* **where** *yval-def*: [*m, p*] ⊢ *y* ↦ *yval*
  using *assms*(*2*) **by** *blast*
 have *is-IntVal32 xval* ∨ *is-IntVal64 xval*
 by (*metis BinaryExprE Value.discI*(*1*) *Value.discI*(*2*) *assms*(*2*) *bin-eval.simps*(*12*)
binary-obj
    constantAsStamp.elims evalDet evaltree-not-undef intval-less-than.simps(*9*)
xval-def)
 have *is-IntVal32 yval* ∨ *is-IntVal64 yval*
 by (*metis BinaryExprE Value.discI*(*1*) *Value.discI*(*2*) *assms*(*2*) *bin-eval.simps*(*12*)
binary-obj
    constantAsStamp.elims evalDet evaltree-not-undef intval-less-than.simps(*16*)
yval-def)
 have *is-IntVal32 xval* = *is-IntVal32 yval*
  by (*metis BinaryExprE Value.collapse*(*2*) ‹*is-IntVal32 xval* ∨ *is-IntVal64 xval*›
‹*is-IntVal32 yval* ∨ *is-IntVal64 yval*› *assms*(*2*) *bin-eval.simps*(*12*) *evalDet int-
val-less-than.simps*(*12*) *intval-less-than.simps*(*5*) *is-IntVal32-def xval-def yval-def*)
 have *is-IntVal64 xval* = *is-IntVal64 yval*
  using ‹*is-IntVal32 xval* = *is-IntVal32 yval*› ‹*is-IntVal32 xval* ∨ *is-IntVal64 xval*›
‹*is-IntVal32 yval* ∨ *is-IntVal64 yval*› **by** *blast*
 have (*intval-less-than xval yval*) ≠ *UndefVal*
  using *assms*(*2*)
  by (*metis BinaryExprE bin-eval.simps*(*12*) *evalDet xval-def yval-def*)
 have *is-IntVal32 xval* ⟹ ((∃ *lo hi*. *stamp-expr x* = *IntegerStamp 32 lo hi*) ∧
(∃ *lo hi*. *stamp-expr y* = *IntegerStamp 32 lo hi*))

  sorry
 have *is-IntVal64 xval* ⟹ ((∃ *lo hi*. *stamp-expr x* = *IntegerStamp 64 lo hi*) ∧
(∃ *lo hi*. *stamp-expr y* = *IntegerStamp 64 lo hi*))

  sorry
 have *xvalid*: *valid-value xval* (*stamp-expr x*)
  using *xvalid xval-def* **by** *auto*
 have *yvalid*: *valid-value yval* (*stamp-expr y*)
  using *yvalid yval-def* **by** *auto*
 { assume *c*: *is-IntVal32 xval*
  obtain *xxval* **where** *x32*: *xval* = *IntVal32 xxval*
   using *c is-IntVal32-def* **by** *blast*
  obtain *yyval* **where** *y32*: *yval* = *IntVal32 yyval*
   using ‹*is-IntVal32 xval* = *is-IntVal32 yval*› *c is-IntVal32-def* **by** *auto*
  have *xs*: ∃ *lo hi*. *stamp-expr x* = *IntegerStamp 32 lo hi*
   by (*simp add*: ‹*is-IntVal32 xval* ⟹ (∃ *lo hi*. *stamp-expr x* = *IntegerStamp 32*

lo hi) ∧ (∃ *lo hi. stamp-expr y = IntegerStamp 32 lo hi*)› *c*)

  have *ys*: ∃ *lo hi. stamp-expr y = IntegerStamp 32 lo hi*

    using ‹*is-IntVal32 xval* ⟹ (∃ *lo hi. stamp-expr x = IntegerStamp 32 lo hi*)
∧ (∃ *lo hi. stamp-expr y = IntegerStamp 32 lo hi*)› *c* **by** *blast*

  have *sint yyval* ≤ *stpi-upper* (*stamp-expr y*)

    using *y32 ys yvalid* **by** *force*

  have *stpi-lower* (*stamp-expr x*) ≤ *sint xxval*

    using *x32 xs xvalid* **by** *force*

  have *stpi-upper* (*stamp-expr y*) < *stpi-lower* (*stamp-expr x*)

    using *assms*(*1*) **unfolding** *stamp-under.simps*

    by *auto*

  then have *yyval* <*s xxval*

    using *assms*(*1*) **unfolding** *stamp-under.simps*

    using ‹*sint yyval* ⊑ *stpi-upper* (*stamp-expr y*)› ‹*stpi-lower* (*stamp-expr x*) ⊑
sint xxval› *word-sless-alt* **by** *fastforce*

  then have (*intval-less-than xval yval*) = *IntVal32 0*

    using *signed.less-not-sym x32 y32* **by** *fastforce*

  }

  note *case32* = *this*

  { assume *c*: *is-IntVal64 xval*

  obtain *xxval* **where** *x64*: *xval* = *IntVal64 xxval*

    using *c is-IntVal64-def* **by** *blast*

  obtain *yyval* **where** *y64*: *yval* = *IntVal64 yyval*

    using ‹*is-IntVal64 xval* = *is-IntVal64 yval*› *c is-IntVal64-def* **by** *auto*

  have *xs*: ∃ *lo hi. stamp-expr x = IntegerStamp 64 lo hi*

    by (*simp add*: ‹*is-IntVal64 xval* ⟹ (∃ *lo hi. stamp-expr x = IntegerStamp 64
lo hi*) ∧ (∃ *lo hi. stamp-expr y = IntegerStamp 64 lo hi*)› *c*)

  have *ys*: ∃ *lo hi. stamp-expr y = IntegerStamp 64 lo hi*

    using ‹*is-IntVal64 xval* ⟹ (∃ *lo hi. stamp-expr x = IntegerStamp 64 lo hi*)
∧ (∃ *lo hi. stamp-expr y = IntegerStamp 64 lo hi*)› *c* **by** *blast*

  have *sint yyval* ≤ *stpi-upper* (*stamp-expr y*)

    using *y64 ys yvalid* **by** *force*

  have *stpi-lower* (*stamp-expr x*) ≤ *sint xxval*

    using *x64 xs xvalid* **by** *force*

  have *stpi-upper* (*stamp-expr y*) < *stpi-lower* (*stamp-expr x*)

    using *assms*(*1*) **unfolding** *stamp-under.simps*

    by *auto*

  then have *yyval* <*s xxval*

    using *assms*(*1*) **unfolding** *stamp-under.simps*

    using ‹*sint yyval* ⊑ *stpi-upper* (*stamp-expr y*)› ‹*stpi-lower* (*stamp-expr x*) ⊑
sint xxval› *word-sless-alt* **by** *fastforce*

  then have (*intval-less-than xval yval*) = *IntVal32 0*

    using *signed.less-imp-triv x64 y64* **by** *fastforce*

  }

  note *case64* = *this*

  have (*intval-less-than xval yval*) = *IntVal32 0*

    using ‹*is-IntVal32 xval* ∨ *is-IntVal64 xval*› *case32 case64* **by** *fastforce*

  then show *?thesis*

    by (*metis BinaryExprE assms*(*2*) *bin-eval.simps*(*12*) *evalDet val-to-bool.simps*(*1*)

182

xval-def yval-def)
qed

end

10 Optization DSLs

theory *Markup*
  imports *Semantics.IRTreeEval Snippets.Snipping*
begin

datatype *$'a$ Rewrite =*
  Transform $'a$ $'a$ (- ⟼ - 10) |
  Conditional $'a$ $'a$ bool (- ⟼ - when - 70) |
  Sequential $'a$ Rewrite $'a$ Rewrite |
  Transitive $'a$ Rewrite

datatype *$'a$ ExtraNotation =*
  ConditionalNotation $'a$ $'a$ $'a$ (- ? - : -) |
  EqualsNotation $'a$ $'a$ (- eq -) |
  ConstantNotation $'a$ (const - 120) |
  TrueNotation (true) |
  FalseNotation (false) |
  ExclusiveOr $'a$ $'a$ (- ⊕ -) |
  LogicNegationNotation $'a$ (!-) |
  ShortCircuitOr $'a$ $'a$ (- || -)

definition *word* :: *($'a$::len) word ⇒ $'a$ word* **where**
  word x = x

ML-file ‹*markup.ML*›

ML ‹
structure IRExprTranslator : DSL-TRANSLATION =
struct
fun markup DSL-Tokens.Add = @{term BinaryExpr} $ @{term BinAdd}
  | markup DSL-Tokens.Sub = @{term BinaryExpr} $ @{term BinSub}
  | markup DSL-Tokens.Mul = @{term BinaryExpr} $ @{term BinMul}
  | markup DSL-Tokens.And = @{term BinaryExpr} $ @{term BinAnd}
  | markup DSL-Tokens.Or = @{term BinaryExpr} $ @{term BinOr}
  | markup DSL-Tokens.Xor = @{term BinaryExpr} $ @{term BinXor}
  | markup DSL-Tokens.ShortCircuitOr = @{term BinaryExpr} $ @{term Bin-
ShortCircuitOr}
  | markup DSL-Tokens.Abs = @{term UnaryExpr} $ @{term UnaryAbs}
  | markup DSL-Tokens.Less = @{term BinaryExpr} $ @{term BinIntegerLessThan}
  | markup DSL-Tokens.Equals = @{term BinaryExpr} $ @{term BinIntegerEquals}
  | markup DSL-Tokens.Not = @{term UnaryExpr} $ @{term UnaryNot}
  | markup DSL-Tokens.Negate = @{term UnaryExpr} $ @{term UnaryNeg}
  | markup DSL-Tokens.LogicNegate = @{term UnaryExpr} $ @{term UnaryLog-

183

icNegation}
  | *markup DSL-Tokens.LeftShift = @{term BinaryExpr} $ @{term BinLeftShift}*
 | *markup DSL-Tokens.RightShift = @{term BinaryExpr} $ @{term BinRightShift}*
 | *markup DSL-Tokens.UnsignedRightShift = @{term BinaryExpr} $ @{term Bin-*
URightShift}
  | *markup DSL-Tokens.Conditional = @{term ConditionalExpr}*
  | *markup DSL-Tokens.Constant = @{term ConstantExpr}*
  | *markup DSL-Tokens.TrueConstant = @{term ConstantExpr (IntVal32 1)}*
  | *markup DSL-Tokens.FalseConstant = @{term ConstantExpr (IntVal32 0)}*
end

structure IntValTranslator : DSL-TRANSLATION =
struct
fun markup DSL-Tokens.Add = @{term intval-add}
  | *markup DSL-Tokens.Sub = @{term intval-sub}*
  | *markup DSL-Tokens.Mul = @{term intval-mul}*
  | *markup DSL-Tokens.And = @{term intval-and}*
  | *markup DSL-Tokens.Or = @{term intval-or}*
  | *markup DSL-Tokens.ShortCircuitOr = @{term intval-short-circuit-or}*
  | *markup DSL-Tokens.Xor = @{term intval-xor}*
  | *markup DSL-Tokens.Abs = @{term intval-abs}*
  | *markup DSL-Tokens.Less = @{term intval-less-than}*
  | *markup DSL-Tokens.Equals = @{term intval-equals}*
  | *markup DSL-Tokens.Not = @{term intval-not}*
  | *markup DSL-Tokens.Negate = @{term intval-negate}*
  | *markup DSL-Tokens.LogicNegate = @{term intval-logic-negation}*
  | *markup DSL-Tokens.LeftShift = @{term intval-left-shift}*
  | *markup DSL-Tokens.RightShift = @{term intval-right-shift}*
  | *markup DSL-Tokens.UnsignedRightShift = @{term intval-uright-shift}*
  | *markup DSL-Tokens.Conditional = @{term intval-conditional}*
  | *markup DSL-Tokens.Constant = @{term IntVal32}*
  | *markup DSL-Tokens.TrueConstant = @{term IntVal32 1}*
  | *markup DSL-Tokens.FalseConstant = @{term IntVal32 0}*
end

structure WordTranslator : DSL-TRANSLATION =
struct
fun markup DSL-Tokens.Add = @{term plus}
  | *markup DSL-Tokens.Sub = @{term minus}*
  | *markup DSL-Tokens.Mul = @{term times}*
 | *markup DSL-Tokens.And = @{term Bit-Operations.semiring-bit-operations-class.and}*
  | *markup DSL-Tokens.Or = @{term or}*
  | *markup DSL-Tokens.Xor = @{term xor}*
  | *markup DSL-Tokens.Abs = @{term abs}*
  | *markup DSL-Tokens.Less = @{term less}*
  | *markup DSL-Tokens.Equals = @{term HOL.eq}*
  | *markup DSL-Tokens.Not = @{term not}*
  | *markup DSL-Tokens.Negate = @{term uminus}*
  | *markup DSL-Tokens.LogicNegate = @{term logic-negate}*

```
    | markup DSL-Tokens.LeftShift = @{term shiftl}
    | markup DSL-Tokens.RightShift = @{term signed-shiftr}
    | markup DSL-Tokens.UnsignedRightShift = @{term shiftr}
    | markup DSL-Tokens.Constant = @{term word}
    | markup DSL-Tokens.TrueConstant = @{term 1}
    | markup DSL-Tokens.FalseConstant = @{term 0}
end

structure IRExprMarkup = DSL-Markup(IRExprTranslator);
structure IntValMarkup = DSL-Markup(IntValTranslator);
structure WordMarkup = DSL-Markup(WordTranslator);
›
```

---

ir expression translation

syntax *-expandExpr :: term ⇒ term* (*exp*[-])
parse-translation ‹ [(@{*syntax-const -expandExpr*} , *IRExprMarkup.markup-expr* [])] ›

---

value expression translation

syntax *-expandIntVal :: term ⇒ term* (*val*[-])
parse-translation ‹ [(@{*syntax-const -expandIntVal*} , *IntValMarkup.markup-expr* [])] ›

---

word expression translation

syntax *-expandWord :: term ⇒ term* (*bin*[-])
parse-translation ‹ [(@{*syntax-const -expandWord*} , *WordMarkup.markup-expr* [])] ›

---

ir expression example

value $exp[(e_1 < e_2) \ ? \ e_1 : e_2]$

ConditionalExpr (*BinaryExpr BinIntegerLessThan* e_1 e_2) e_1 e_2

---

value expression example

value $val[(e_1 < e_2) \ ? \ e_1 : e_2]$

intval-conditional (*intval-less-than* e_1 e_2) e_1 e_2

---

value $exp[((e_1 - e_2) + (const \ (IntVal32 \ 0)) + e_2) \longmapsto e_1 \ when \ True]$
value $val[((e_1 - e_2) + (const \ 0) + e_2) \longmapsto e_1 \ when \ True]$

value $bin[-x]$
value $val[-x]$
value $exp[-x]$

value $bin[!x]$
value $val[!x]$
value $exp[!x]$

value $bin[\neg x]$
value $val[\neg x]$
value $exp[\neg x]$

value $bin[\sim x]$
value $val[\sim x]$
value $exp[\sim x]$

value $\sim x$

end
theory *Phase*
  imports *Main*
begin

ML-file *map.ML*
ML-file *phase.ML*

end

10.1   Canonicalization DSL

theory *Canonicalization*
  imports
    Markup
    Phase
    HOL−Eisbach.Eisbach
  keywords
    phase :: *thy-decl* **and**
    terminating :: *quasi-command* **and**
    print-phases :: *diag* **and**
    optimization :: *thy-goal-defn*
begin

ML ‹

```
datatype 'a Rewrite =
  Transform of 'a * 'a |
  Conditional of 'a * 'a * term |
  Sequential of 'a Rewrite * 'a Rewrite |
  Transitive of 'a Rewrite

type rewrite = {name: string, rewrite: term Rewrite}

structure RewriteRule : Rule =
struct
type T = rewrite;

fun pretty-rewrite ctxt (Transform (from, to)) =
      Pretty.block [
        Syntax.pretty-term ctxt from,
        Pretty.str  ↦ ,
        Syntax.pretty-term ctxt to
      ]
  | pretty-rewrite ctxt (Conditional (from, to, cond)) =
      Pretty.block [
        Syntax.pretty-term ctxt from,
        Pretty.str  ↦ ,
        Syntax.pretty-term ctxt to,
        Pretty.str  when ,
        Syntax.pretty-term ctxt cond
      ]
  | pretty-rewrite - - = Pretty.str not implemented

fun pretty ctxt t =
  Pretty.block [
    Pretty.str ((#name t) ⌢: ),
    pretty-rewrite ctxt (#rewrite t)
  ]
end

structure RewritePhase = DSL-Phase(RewriteRule);

val - =
  Outer-Syntax.command command-keyword‹phase› enter an optimization phase
    (Parse.binding −−| Parse.$$$ terminating −− Parse.const −−| Parse.begin
      >> (Toplevel.begin-main-target true o RewritePhase.setup));

fun print-phases ctxt =
  let
    val thy = Proof-Context.theory-of ctxt;
    fun print phase = RewritePhase.pretty phase ctxt
  in
    map print (RewritePhase.phases thy)
  end
```

fun print-optimizations thy =
  print-phases thy |> Pretty.writeln-chunks

val - =
  Outer-Syntax.command **command-keyword**‹*print-phases*›
    print debug information for optimizations
    (*Scan.succeed*
      (*Toplevel.keep* (*print-optimizations o Toplevel.context-of*)));
›

ML-file *rewrites.ML*

fun *rewrite-preservation* :: *IRExpr Rewrite* ⇒ *bool* **where**
  rewrite-preservation (*Transform x y*) = (*y* ≤ *x*) |
  rewrite-preservation (*Conditional x y cond*) = (*cond* ⟶ (*y* ≤ *x*)) |
  rewrite-preservation (*Sequential x y*) = (*rewrite-preservation x* ∧ *rewrite-preservation*
y) |
  rewrite-preservation (*Transitive x*) = *rewrite-preservation x*

fun *rewrite-termination* :: *IRExpr Rewrite* ⇒ (*IRExpr* ⇒ *nat*) ⇒ *bool* **where**
  rewrite-termination (*Transform x y*) *trm* = (*trm x* > *trm y*) |
  rewrite-termination (*Conditional x y cond*) *trm* = (*cond* ⟶ (*trm x* > *trm y*)) |
  rewrite-termination (*Sequential x y*) *trm* = (*rewrite-termination x trm* ∧ *rewrite-termination*
y trm) |
  rewrite-termination (*Transitive x*) *trm* = *rewrite-termination x trm*

fun *intval* :: *Value Rewrite* ⇒ *bool* **where**
  intval (*Transform x y*) = (*x* ≠ *UndefVal* ∧ *y* ≠ *UndefVal* ⟶ *x* = *y*) |
  intval (*Conditional x y cond*) = (*cond* ⟶ (*x* = *y*)) |
  intval (*Sequential x y*) = (*intval x* ∧ *intval y*) |
  intval (*Transitive x*) = *intval x*

fun *size* :: *IRExpr* ⇒ *nat* **where**
  size (*UnaryExpr op e*) = (*size e*) + *1* |
  size (*BinaryExpr BinAdd x y*) = (*size x*) + ((*size y*) * *2*) |
  size (*BinaryExpr op x y*) = (*size x*) + (*size y*) |
  size (*ConditionalExpr cond t f*) = (*size cond*) + (*size t*) + (*size f*) + *2* |
  size (*ConstantExpr c*) = *1* |
  size (*ParameterExpr ind s*) = *2* |
  size (*LeafExpr nid s*) = *2* |
  size (*ConstantVar c*) = *2* |
  size (*VariableExpr x s*) = *2*

method *unfold-optimization* =
  (*unfold rewrite-preservation.simps, unfold rewrite-termination.simps,*
    unfold intval.simps,
    rule conjE, simp, simp del: *le-expr-def, force?*)
  | (*unfold rewrite-preservation.simps, unfold rewrite-termination.simps,*

rule conjE, simp, simp del: le-expr-def, force?)

method *unfold-size =*
  (unfold size.simps, simp del: le-expr-def)?
  | (unfold size.simps)?

print-methods

ML ‹
structure System : RewriteSystem =
struct
val preservation = @{const rewrite-preservation};
val termination = @{const rewrite-termination};
val intval = @{const intval};
end

structure DSL = DSL-Rewrites(System);

val - =
  Outer-Syntax.local-theory-to-proof **command-keyword**‹*optimization*›
    define an optimization and open proof obligation
    (Parse-Spec.thm-name : −− Parse.term
      >> DSL.rewrite-cmd);
›

end

11   Canonicalization Phase

theory *Common*
  imports
    OptimizationDSL.Canonicalization
    Semantics.IRTreeEvalThms
begin

lemma *size-pos[simp]: 0 < size y*
  apply (*induction y; auto?*)
  subgoal premises *prems* **for** *op a b*
    using *prems* **by** (*induction op; auto*)
  done

lemma *size-non-add: op ≠ BinAdd ⟹ size (BinaryExpr op a b) = size a + size b*
  by (*induction op; auto*)

lemma *size-non-const*:
  ¬ *is-ConstantExpr y* ⟹ *1 < size y*
  using *size-pos* **apply** (*induction y; auto*)
  subgoal premises *prems* **for** *op a b*
    apply (*cases op = BinAdd*)
    using *size-non-add size-pos* **apply** *auto*
    by (*simp add: Suc-lessI one-is-add*)+
  done

definition *well-formed-equal* :: *Value* ⇒ *Value* ⇒ *bool*
  (**infix** ≈ *50*) **where**
  well-formed-equal v₁ v₂ = (*v₁* ≠ *UndefVal* ⟶ *v₁* = *v₂*)

lemma *well-formed-equal-defn* [*simp*]:
  well-formed-equal v₁ v₂ = (*v₁* ≠ *UndefVal* ⟶ *v₁* = *v₂*)
  unfolding *well-formed-equal-def* **by** *simp*

end

11.1   Conditional Expression

theory *ConditionalPhase*
  imports
    Common
begin

phase *Conditional*
  terminating *size*
begin

lemma *negates*: *is-IntVal32 e* ∨ *is-IntVal64 e* ⟹ *val-to-bool* (*val*[*e*]) ≡ ¬(*val-to-bool*
(*val*[*!e*]))
  using *intval-logic-negation.simps* **unfolding** *logic-negate-def*
 by (*smt* (*verit, best*) *Value.collapse*(*1*) *is-IntVal64-def val-to-bool.simps*(*1*) *val-to-bool.simps*(*2*)
zero-neq-one)

lemma *negation-condition-intval*:
  assumes *e* ≠ *UndefVal* ∧ ¬(*is-ObjRef e*) ∧ ¬(*is-ObjStr e*)
  shows *val*[(*!e*) *? x* : *y*] = *val*[*e ? y* : *x*]
  using *assms* **by** (*cases e; auto simp: negates logic-negate-def*)

optimization *negate-condition*: ((*!e*) *? x* : *y*) ⟼ (*e ? y* : *x*)
    apply *simp* **using** *negation-condition-intval*
  by (*smt* (*verit, ccfv-SIG*) *ConditionalExpr ConditionalExprE Value.collapse*(*3*)
Value.collapse(*4*) *Value.exhaust-disc evaltree-not-undef intval-logic-negation.simps*(*4*)
intval-logic-negation.simps(*5*) *negates unary-eval.simps*(*4*) *unfold-unary*)

optimization *const-true*: (*true ? x* : *y*) ⟼ *x* .

optimization *const-false*: (*false ? x : y*) $\longmapsto$ *y* **.**

optimization *equal-branches*: (*e ? x : x*) $\longmapsto$ *x* **.**

definition *wff-stamps* :: *bool* **where**
  wff-stamps = ($\forall$ *m p expr val* . ([*m,p*] $\vdash$ *expr* $\mapsto$ *val*) $\longrightarrow$ *valid-value val* (*stamp-expr expr*))

definition *wf-stamp* :: *IRExpr* $\Rightarrow$ *bool* **where**
  wf-stamp e = ($\forall$ *m p v*. ([*m, p*] $\vdash$ *e* $\mapsto$ *v*) $\longrightarrow$ *valid-value v* (*stamp-expr e*))

optimization *b[intval]*: ((*x eq y*) *? x : y*) $\longmapsto$ *y*
 sorry

lemma *val-optimise-integer-test*:
  assumes *is-IntVal32 x*
  shows *intval-conditional* (*intval-equals val*[(*x & (IntVal32 1)*)] (*IntVal32 0*))
        (*IntVal32 0*) (*IntVal32 1*) =
        val[*x & IntVal32 1*]
   apply *simp-all*
   apply *auto*
  using *bool-to-val.elims intval-equals.elims val-to-bool.simps(1) val-to-bool.simps(3)*
   sorry

optimization *val-conditional-eliminate-known-less*: ((*x < y*) *? x : y*) $\longmapsto$ *x*
                          when (*stamp-under* (*stamp-expr x*) (*stamp-expr y*)
                             $\wedge$ *wf-stamp x* $\wedge$ *wf-stamp y*)
      apply *auto*
    using *stamp-under.simps wf-stamp-def val-to-bool.simps*
    sorry

optimization *opt-conditional-eq-is-RHS*: ((*BinaryExpr BinIntegerEquals x y*) *? x
: y*) $\longmapsto$ *y*
   apply *simp-all* **apply** *auto* **using** *b*
   apply (*metis* (*mono-tags, lifting*) *Canonicalization.intval.simps(1) evalDet
        intval-conditional.simps intval-equals.simps(10)*)
   done

optimization *opt-normalize-x*: *((x eq const (IntVal32 0)) ?*
(const (IntVal32 0)) : (const (IntVal32 1))) ⟼ x
when (x = ConstantExpr (IntVal32 0) | (x = ConstantExpr
(IntVal32 1)))
   done

optimization *opt-normalize-x2*: *((x eq (const (IntVal32 1))) ?*
(const (IntVal32 1)) : (const (IntVal32 0))) ⟼ x
when (x = ConstantExpr (IntVal32 0) | (x = ConstantExpr
(IntVal32 1)))
   done

optimization *opt-flip-x*: *((x eq (const (IntVal32 0))) ?*
(const (IntVal32 1)) : (const (IntVal32 0))) ⟼
x ⊕ (const (IntVal32 1))
when (x = ConstantExpr (IntVal32 0) | (x = ConstantExpr
(IntVal32 1)))
   done

optimization *opt-flip-x2*: *((x eq (const (IntVal32 1))) ?*
(const (IntVal32 0)) : (const (IntVal32 1))) ⟼
x ⊕ (const (IntVal32 1))
when (x = ConstantExpr (IntVal32 0) | (x = ConstantExpr
(IntVal32 1)))
   done

optimization *opt-optimise-integer-test*:
(((x & (const (IntVal32 1))) eq (const (IntVal32 0))) ?
(const (IntVal32 0)) : (const (IntVal32 1))) ⟼
x & (const (IntVal32 1))
when (stamp-expr x = default-stamp)
   apply *simp-all*
   apply *auto*
 using *val-optimise-integer-test* **sorry**

optimization *opt-optimise-integer-test-2*:
(((x & (const (IntVal32 1))) eq (const (IntVal32 0))) ?
(const (IntVal32 0)) : (const (IntVal32 1))) ⟼
x
when (x = ConstantExpr (IntVal32 0) | (x = ConstantExpr (IntVal32
1)))
   done

optimization *opt-conditional-eliminate-known-less*: $((x < y) \ ? \ x : y) \longmapsto x$
$$\text{when } (((\textit{stamp-under } (\textit{stamp-expr } x) \ (\textit{stamp-expr } y)) \ | $$
$$((\textit{stpi-upper } (\textit{stamp-expr } x)) = (\textit{stpi-lower } (\textit{stamp-expr }$$
$y))))$
$$\wedge \ \textit{wf-stamp } x \wedge \textit{wf-stamp } y)$$
  unfolding *le-expr-def* **apply** *auto*
 using *stamp-under.simps wf-stamp-def val-conditional-eliminate-known-less*
 sorry

end

end

12   Conditional Elimination Phase

theory *ConditionalElimination*
 imports
  Proofs.Rewrites
  Proofs.Bisimulation
begin

12.1   Individual Elimination Rules

We introduce a TriState as in the Graal compiler to represent when static analysis can tell us information about the value of a boolean expression. Unknown = No information can be inferred KnownTrue/KnownFalse = We can infer the expression will always be true or false.

datatype *TriState = Unknown | KnownTrue | KnownFalse*

The implies relation corresponds to the LogicNode.implies method from the compiler which attempts to infer when one logic nodes value can be inferred from a known logic node.

inductive *implies* :: *IRGraph* $\Rightarrow$ *IRNode* $\Rightarrow$ *IRNode* $\Rightarrow$ *TriState* $\Rightarrow$ *bool*
 $(\text{-} \vdash \text{-} \ \& \ \text{-} \hookrightarrow \text{-})$ **for** *g* **where**
 eq-imp-less:
 $g \vdash (\textit{IntegerEqualsNode } x \ y) \ \& \ (\textit{IntegerLessThanNode } x \ y) \hookrightarrow \textit{KnownFalse} \ |$
 eq-imp-less-rev:
 $g \vdash (\textit{IntegerEqualsNode } x \ y) \ \& \ (\textit{IntegerLessThanNode } y \ x) \hookrightarrow \textit{KnownFalse} \ |$
 less-imp-rev-less:
 $g \vdash (\textit{IntegerLessThanNode } x \ y) \ \& \ (\textit{IntegerLessThanNode } y \ x) \hookrightarrow \textit{KnownFalse} \ |$
 less-imp-not-eq:

$g \vdash (IntegerLessThanNode\ x\ y)\ \&\ (IntegerEqualsNode\ x\ y) \hookrightarrow KnownFalse\ |$
less-imp-not-eq-rev:
$g \vdash (IntegerLessThanNode\ x\ y)\ \&\ (IntegerEqualsNode\ y\ x) \hookrightarrow KnownFalse\ |$

x-imp-x:
$g \vdash x\ \&\ x \hookrightarrow KnownTrue\ |$

negate-false:
$[\![g \vdash x\ \&\ (kind\ g\ y) \hookrightarrow KnownTrue]\!] \implies g \vdash x\ \&\ (LogicNegationNode\ y) \hookrightarrow$
$KnownFalse\ |$
negate-true:
$[\![g \vdash x\ \&\ (kind\ g\ y) \hookrightarrow KnownFalse]\!] \implies g \vdash x\ \&\ (LogicNegationNode\ y) \hookrightarrow$
$KnownTrue$

Total relation over partial implies relation

inductive *condition-implies* :: $IRGraph \Rightarrow IRNode \Rightarrow IRNode \Rightarrow TriState \Rightarrow bool$
$(\text{-} \vdash \text{-}\ \&\ \text{-} \rightharpoonup \text{-})$ **for** g **where**
$[\![\neg(g \vdash a\ \&\ b \hookrightarrow imp)]\!] \implies (g \vdash a\ \&\ b \rightharpoonup Unknown)\ |$
$[\![(g \vdash a\ \&\ b \hookrightarrow imp)]\!] \implies (g \vdash a\ \&\ b \rightharpoonup imp)$

inductive *implies-tree* :: $IRExpr \Rightarrow IRExpr \Rightarrow bool \Rightarrow bool$
$(\text{-}\ \&\ \text{-} \hookrightarrow \text{-})$ **where**
eq-imp-less:
$(BinaryExpr\ BinIntegerEquals\ x\ y)\ \&\ (BinaryExpr\ BinIntegerLessThan\ x\ y) \hookrightarrow$
$False\ |$
eq-imp-less-rev:
$(BinaryExpr\ BinIntegerEquals\ x\ y)\ \&\ (BinaryExpr\ BinIntegerLessThan\ y\ x) \hookrightarrow$
$False\ |$
less-imp-rev-less:
$(BinaryExpr\ BinIntegerLessThan\ x\ y)\ \&\ (BinaryExpr\ BinIntegerLessThan\ y\ x)$
$\hookrightarrow False\ |$
less-imp-not-eq:
$(BinaryExpr\ BinIntegerLessThan\ x\ y)\ \&\ (BinaryExpr\ BinIntegerEquals\ x\ y) \hookrightarrow$
$False\ |$
less-imp-not-eq-rev:
$(BinaryExpr\ BinIntegerLessThan\ x\ y)\ \&\ (BinaryExpr\ BinIntegerEquals\ y\ x) \hookrightarrow$
$False\ |$

x-imp-x:
$x\ \&\ x \hookrightarrow True\ |$

negate-false:
$[\![x\ \&\ y \hookrightarrow True]\!] \implies x\ \&\ (UnaryExpr\ UnaryLogicNegation\ y) \hookrightarrow False\ |$
negate-true:
$[\![x\ \&\ y \hookrightarrow False]\!] \implies x\ \&\ (UnaryExpr\ UnaryLogicNegation\ y) \hookrightarrow True$

Proofs that the implies relation is correct with respect to the existing eval-

uation semantics.

experiment begin
lemma *logic-negate-type*:
  assumes *[m, p] ⊢ UnaryExpr UnaryLogicNegation x ↦ v*
  assumes *v ≠ UndefVal*
  shows *∃ v2. [m, p] ⊢ x ↦ IntVal32 v2*
proof −
  obtain *ve* **where** *ve: [m, p] ⊢ x ↦ ve*
    using *assms(1)* **by** *blast*
  then have *[m, p] ⊢ UnaryExpr UnaryLogicNegation x ↦ unary-eval UnaryLogicNegation ve*
    by (*metis UnaryExprE assms(1) evalDet*)
  then show *?thesis* **using** *assms unary-eval.elims evalDet ve IRUnaryOp.distinct*
    sorry
qed

lemma *logic-negation-relation-tree*:
  assumes *[m, p] ⊢ y ↦ val*
  assumes *[m, p] ⊢ UnaryExpr UnaryLogicNegation y ↦ invval*
  assumes *invval ≠ UndefVal*
  shows *val-to-bool val ⟷ ¬(val-to-bool invval)*
proof −
  obtain *v* **where** *invval = unary-eval UnaryLogicNegation v*
    using *assms(2)* **by** *blast*
  then have *[m, p] ⊢ y ↦ v* **using** *UnaryExprE assms(1,2)* **sorry**
  then show *?thesis* **sorry**
  qed

lemma *logic-negation-relation*:
  assumes *[g, m, p] ⊢ y ↦ val*
  assumes *kind g neg = LogicNegationNode y*
  assumes *[g, m, p] ⊢ neg ↦ invval*
  assumes *invval ≠ UndefVal*
  shows *val-to-bool val ⟷ ¬(val-to-bool invval)*
proof −
  obtain *yencode* **where** *g ⊢ y ≃ yencode*
    using *assms(1) encodeeval-def* **by** *auto*
  then have *g ⊢ neg ≃ UnaryExpr UnaryLogicNegation yencode*
    using *rep.intros(7) assms(2)* **by** *simp*
  then have *[m, p] ⊢ UnaryExpr UnaryLogicNegation yencode ↦ invval*
    using *assms(3) encodeeval-def*
    by (*metis repDet*)
  obtain *v1* **where** *[g, m, p] ⊢ y ↦ IntVal32 v1*
    using *assms(1,2,3,4)* **using** *logic-negate-type* **sorry**
  have *invval = bool-to-val (¬(val-to-bool val))*
    using *assms(1,2,3) evalDet unary-eval.simps(4)*
      by (*smt* (*verit, ccfv-threshold*) *UnaryExprE* ‹*[g,m,p] ⊢ y ↦ IntVal32 v1*›
‹*[m,p] ⊢ UnaryExpr UnaryLogicNegation yencode ↦ invval*› ‹*g ⊢ y ≃ yencode*›

bool-to-val.simps(1) bool-to-val.simps(2) encodeeval-def graphDet intval-logic-negation.simps(1)
logic-negate-def val-to-bool.simps(1))
  have *val-to-bool invval* $\longleftrightarrow$ $\neg$(*val-to-bool val*)
    using ‹*invval = bool-to-val* ($\neg$ *val-to-bool val*)› **by** *force*
  then show *?thesis*
    by *simp*
qed
end

lemma *implies-valid*:
  assumes x & $y \hookrightarrow imp$
  assumes $[m, p] \vdash x \mapsto v1$
  assumes $[m, p] \vdash y \mapsto v2$
  assumes $v1 \neq UndefVal \wedge v2 \neq UndefVal$
  shows ($imp \longrightarrow$ (*val-to-bool v1* $\longrightarrow$ *val-to-bool v2*)) $\wedge$
       ($\neg imp \longrightarrow$ (*val-to-bool v1* $\longrightarrow \neg$(*val-to-bool v2*)))
   (**is** (*?TP* $\longrightarrow$ *?TC*) $\wedge$ (*?FP* $\longrightarrow$ *?FC*))
  apply (*intro conjI; rule impI*)
proof −
  assume *KnownTrue*: *?TP*
  show *?TC*
 using *assms(1) KnownTrue assms(2−)* **proof** (*induct x y imp rule: implies-tree.induct*)
   case (*eq-imp-less x y*)
   then show *?case* **by** *simp*
  next
   case (*eq-imp-less-rev x y*)
   then show *?case* **by** *simp*
  next
   case (*less-imp-rev-less x y*)
   then show *?case* **by** *simp*
  next
   case (*less-imp-not-eq x y*)
   then show *?case* **by** *simp*
  next
   case (*less-imp-not-eq-rev x y*)
   then show *?case* **by** *simp*
  next
   case (*x-imp-x*)
   then show *?case*
    by (*metis evalDet*)
  next
   case (*negate-false x1*)
   then show *?case* **using** *evalDet*
    using *assms(2,3)* **by** *blast*
  next
   case (*negate-true y*)
   then show *?case*
    sorry
  qed

next
  assume *KnownFalse*: *?FP*
 show *?FC* **using** *assms KnownFalse* **proof** (*induct x y imp rule*: *implies-tree.induct*)
   case (*eq-imp-less x y*)
   obtain *xval* **where** *xval*: $[m, p] \vdash x \mapsto xval$
    using *eq-imp-less*(*1*) *eq-imp-less.prems*(*3*)
    by *blast*
   then obtain *yval* **where** *yval*: $[m, p] \vdash y \mapsto yval$
    using *eq-imp-less.prems*(*3*)
    using *eq-imp-less.prems*(*2*) **by** *blast*
   have *eqeval*: $[m, p] \vdash$ (*BinaryExpr BinIntegerEquals x y*) $\mapsto$ *intval-equals xval yval*
    using *xval yval evaltree.BinaryExpr*
    by (*metis BinaryExprE bin-eval.simps*(*11*) *eq-imp-less.prems*(*1*) *evalDet*)
   have *lesseval*: $[m, p] \vdash$ (*BinaryExpr BinIntegerLessThan x y*) $\mapsto$ *intval-less-than xval yval*
    using *xval yval evaltree.BinaryExpr*
    by (*metis BinaryExprE bin-eval.simps*(*12*) *eq-imp-less.prems*(*2*) *evalDet*)
   have *val-to-bool* (*intval-equals xval yval*) $\longrightarrow \neg$(*val-to-bool* (*intval-less-than xval yval*))
    using *assms*(*4*) **apply** (*cases xval*; *cases yval*; *auto*)
     apply (*metis* (*full-types*) *val-to-bool.simps*(*1*) *Values.bool-to-val.simps*(*2*) *signed.less-irrefl*)
   by (*metis* (*mono-tags*) *val-to-bool.simps*(*1*) *Values.bool-to-val.elims signed.order.strict-implies-not-eq*)
   then show *?case*
    using *eqeval lesseval*
    by (*metis eq-imp-less.prems*(*1*) *eq-imp-less.prems*(*2*) *evalDet*)
  next
   case (*eq-imp-less-rev x y*)
   obtain *xval* **where** *xval*: $[m, p] \vdash x \mapsto xval$
    using *eq-imp-less-rev.prems*(*3*)
    using *eq-imp-less-rev.prems*(*2*) **by** *blast*
   obtain *yval* **where** *yval*: $[m, p] \vdash y \mapsto yval$
    using *eq-imp-less-rev.prems*(*3*)
    using *eq-imp-less-rev.prems*(*2*) **by** *blast*
   have *eqeval*: $[m, p] \vdash$ (*BinaryExpr BinIntegerEquals x y*) $\mapsto$ *intval-equals xval yval*
    using *xval yval evaltree.BinaryExpr*
    by (*metis BinaryExprE bin-eval.simps*(*11*) *eq-imp-less-rev.prems*(*1*) *evalDet*)
   have *lesseval*: $[m, p] \vdash$ (*BinaryExpr BinIntegerLessThan y x*) $\mapsto$ *intval-less-than yval xval*
    using *xval yval evaltree.BinaryExpr*
    by (*metis BinaryExprE bin-eval.simps*(*12*) *eq-imp-less-rev.prems*(*2*) *evalDet*)
   have *val-to-bool* (*intval-equals xval yval*) $\longrightarrow \neg$(*val-to-bool* (*intval-less-than yval xval*))
    using *assms*(*4*) **apply** (*cases xval*; *cases yval*; *auto*)
     apply (*metis* (*full-types*) *val-to-bool.simps*(*1*) *Values.bool-to-val.simps*(*2*) *signed.less-irrefl*)
   by (*metis* (*full-types*) *val-to-bool.simps*(*1*) *Values.bool-to-val.elims signed.order.strict-implies-not-eq*)

    then show *?case*
      using *eqeval lesseval*
      by (*metis eq-imp-less-rev.prems*(*1*) *eq-imp-less-rev.prems*(*2*) *evalDet*)
  next
    case (*less-imp-rev-less x y*)
    obtain *xval* **where** *xval*: [*m*, *p*] ⊢ *x* ↦ *xval*
      using *less-imp-rev-less.prems*(*3*)
      using *less-imp-rev-less.prems*(*2*) **by** *blast*
    obtain *yval* **where** *yval*: [*m*, *p*] ⊢ *y* ↦ *yval*
      using *less-imp-rev-less.prems*(*3*)
      using *less-imp-rev-less.prems*(*2*) **by** *blast*
   have *lesseval*: [*m*, *p*] ⊢ (*BinaryExpr BinIntegerLessThan x y*) ↦ *intval-less-than xval yval*
      using *xval yval evaltree.BinaryExpr*
     by (*metis BinaryExprE bin-eval.simps*(*12*) *evalDet less-imp-rev-less.prems*(*1*))
      have *revlesseval*: [*m*, *p*] ⊢ (*BinaryExpr BinIntegerLessThan y x*) ↦ *intval-less-than yval xval*
      using *xval yval evaltree.BinaryExpr*
     by (*metis BinaryExprE bin-eval.simps*(*12*) *evalDet less-imp-rev-less.prems*(*2*))
   have *val-to-bool* (*intval-less-than xval yval*) ⟶ ¬(*val-to-bool* (*intval-less-than yval xval*))
      using *assms*(*4*) **apply** (*cases xval*; *cases yval*; *auto*)
    apply (*metis val-to-bool.simps*(*1*) *Values.bool-to-val.elims signed.not-less-iff-gr-or-eq*)
     by (*metis val-to-bool.simps*(*1*) *Values.bool-to-val.elims signed.less-asym′*)
    then show *?case*
     by (*metis evalDet less-imp-rev-less.prems*(*1*) *less-imp-rev-less.prems*(*2*) *lesseval revlesseval*)
  next
    case (*less-imp-not-eq x y*)
    obtain *xval* **where** *xval*: [*m*, *p*] ⊢ *x* ↦ *xval*
      using *less-imp-not-eq.prems*(*3*)
      using *less-imp-not-eq.prems*(*1*) **by** *blast*
    obtain *yval* **where** *yval*: [*m*, *p*] ⊢ *y* ↦ *yval*
      using *less-imp-not-eq.prems*(*3*)
      using *less-imp-not-eq.prems*(*1*) **by** *blast*
   have *eqeval*: [*m*, *p*] ⊢ (*BinaryExpr BinIntegerEquals x y*) ↦ *intval-equals xval yval*
      using *xval yval evaltree.BinaryExpr*
     by (*metis BinaryExprE bin-eval.simps*(*11*) *evalDet less-imp-not-eq.prems*(*2*))
   have *lesseval*: [*m*, *p*] ⊢ (*BinaryExpr BinIntegerLessThan x y*) ↦ *intval-less-than xval yval*
      using *xval yval evaltree.BinaryExpr*
     by (*metis BinaryExprE bin-eval.simps*(*12*) *evalDet less-imp-not-eq.prems*(*1*))
   have *val-to-bool* (*intval-less-than xval yval*) ⟶ ¬(*val-to-bool* (*intval-equals xval yval*))
      using *assms*(*4*) **apply** (*cases xval*; *cases yval*; *auto*)
     apply (*metis* (*full-types*) *bool-to-val.simps*(*2*) *signed.less-imp-not-eq val-to-bool.simps*(*1*))
     by (*metis* (*full-types*) *bool-to-val.simps*(*2*) *signed.less-imp-not-eq2 val-to-bool.simps*(*1*))
    then show *?case*

      by (*metis eqeval evalDet less-imp-not-eq.prems*(*1*) *less-imp-not-eq.prems*(*2*)
lesseval)
  next
    case (*less-imp-not-eq-rev x y*)
    obtain *xval* **where** *xval*: [*m, p*] ⊢ *x* ↦ *xval*
      using *less-imp-not-eq-rev.prems*(*3*)
      using *less-imp-not-eq-rev.prems*(*1*) **by** *blast*
    obtain *yval* **where** *yval*: [*m, p*] ⊢ *y* ↦ *yval*
      using *less-imp-not-eq-rev.prems*(*3*)
      using *less-imp-not-eq-rev.prems*(*1*) **by** *blast*
    have *eqeval*: [*m, p*] ⊢ (*BinaryExpr BinIntegerEquals y x*) ↦ *intval-equals yval
xval*
      using *xval yval evaltree.BinaryExpr*
    by (*metis BinaryExprE bin-eval.simps*(*11*) *evalDet less-imp-not-eq-rev.prems*(*2*))
    have *lesseval*: [*m, p*] ⊢ (*BinaryExpr BinIntegerLessThan x y*) ↦ *intval-less-than
xval yval*
      using *xval yval evaltree.BinaryExpr*
    by (*metis BinaryExprE bin-eval.simps*(*12*) *evalDet less-imp-not-eq-rev.prems*(*1*))
    have *val-to-bool* (*intval-less-than xval yval*) ⟶ ¬(*val-to-bool* (*intval-equals yval
xval*))
      using *assms*(*4*) **apply** (*cases xval*; *cases yval*; *auto*)
    apply (*metis* (*full-types*) *bool-to-val.simps*(*2*) *signed.less-imp-not-eq2 val-to-bool.simps*(*1*))
    by (*metis* (*full-types, opaque-lifting*) *val-to-bool.simps*(*1*) *Values.bool-to-val.elims
signed.dual-order.strict-implies-not-eq*)
    then show *?case*
    by (*metis eqeval evalDet less-imp-not-eq-rev.prems*(*1*) *less-imp-not-eq-rev.prems*(*2*)
lesseval)
  next
    case (*x-imp-x x1*)
    then show *?case* **by** *simp*
  next
    case (*negate-false x y*)
    then show *?case* **sorry**
  next
    case (*negate-true x1*)
    then show *?case* **by** *simp*
  qed
qed

lemma *implies-true-valid*:
  assumes *x & y* ↪ *imp*
  assumes *imp*
  assumes [*m, p*] ⊢ *x* ↦ *v1*
  assumes [*m, p*] ⊢ *y* ↦ *v2*
  assumes *v1* ≠ *UndefVal* ∧ *v2* ≠ *UndefVal*
  shows *val-to-bool v1* ⟶ *val-to-bool v2*
  using *assms implies-valid*
  by *blast*

lemma *implies-false-valid*:
  assumes *x & y ↪ imp*
  assumes *¬imp*
  assumes *[m, p] ⊢ x ↦ v1*
  assumes *[m, p] ⊢ y ↦ v2*
  assumes *v1 ≠ UndefVal ∧ v2 ≠ UndefVal*
  shows *val-to-bool v1 ⟶ ¬(val-to-bool v2)*
  using *assms implies-valid* **by** *blast*

The following relation corresponds to the UnaryOpLogicNode.tryFold and BinaryOpLogicNode.tryFold methods and their associated concrete implementations.

The relation determines if a logic operation can be shown true or false through the stamp typing information.

inductive *tryFold :: IRNode ⇒ (ID ⇒ Stamp) ⇒ bool ⇒ bool*
  where
  ⟦*alwaysDistinct (stamps x) (stamps y)*⟧
    ⟹ *tryFold (IntegerEqualsNode x y) stamps False* |
  ⟦*neverDistinct (stamps x) (stamps y)*⟧
    ⟹ *tryFold (IntegerEqualsNode x y) stamps True* |
  ⟦*is-IntegerStamp (stamps x);*
   is-IntegerStamp (stamps y);
   stpi-upper (stamps x) < stpi-lower (stamps y)⟧
    ⟹ *tryFold (IntegerLessThanNode x y) stamps True* |
  ⟦*is-IntegerStamp (stamps x);*
   is-IntegerStamp (stamps y);
   stpi-lower (stamps x) ≥ stpi-upper (stamps y)⟧
    ⟹ *tryFold (IntegerLessThanNode x y) stamps False*

Proofs that show that when the stamp lookup function is well-formed, the tryFold relation correctly predicts the output value with respect to our evaluation semantics.

lemma
  assumes *kind g nid = IntegerEqualsNode x y*
  assumes *[g, m, p] ⊢ nid ↦ v*
  assumes *v ≠ UndefVal*
  assumes *([g, m, p] ⊢ x ↦ xval) ∧ ([g, m, p] ⊢ y ↦ yval)*
  shows *val-to-bool (intval-equals xval yval) ⟷ v = IntVal32 1*
proof −
  have *v = intval-equals xval yval*
    using *assms(1, 2, 3, 4) BinaryExprE IntegerEqualsNode bin-eval.simps(7)*
    by *(smt (verit) bin-eval.simps(11) encodeeval-def evalDet repDet)*
  then show *?thesis* **using** *intval-equals.simps val-to-bool.simps* **sorry**
qed

lemma *tryFoldIntegerEqualsAlwaysDistinct*:
  assumes *wf-stamp g stamps*
  assumes *kind g nid = (IntegerEqualsNode x y)*

   assumes $[g, m, p] \vdash nid \mapsto v$
   assumes *alwaysDistinct* (*stamps x*) (*stamps y*)
   shows $v = IntVal32\ 0$
proof $-$
  have $\forall\ val.\ \neg(valid\text{-}value\ val\ (join\ (stamps\ x)\ (stamps\ y)))$
   using *assms(1,4)* **unfolding** *alwaysDistinct.simps*
  by (*metis is-stamp-empty.elims(2) le-less-trans not-less valid32or64 valid-value.simps(1)*
valid-value.simps(2))
  have $\neg(\exists\ val\ .\ ([g, m, p] \vdash x \mapsto val) \wedge ([g, m, p] \vdash y \mapsto val))$
    using *assms(1,4)* **unfolding** *alwaysDistinct.simps wf-stamp.simps encodee-*
val-def **sorry**
  then show *?thesis* **sorry**
qed

lemma *tryFoldIntegerEqualsNeverDistinct*:
  assumes *wf-stamp g stamps*
  assumes *kind g nid* = (*IntegerEqualsNode x y*)
  assumes $[g, m, p] \vdash nid \mapsto v$
  assumes *neverDistinct* (*stamps x*) (*stamps y*)
  shows $v = IntVal32\ 1$
  using *assms IntegerEqualsNodeE* **sorry**

lemma *tryFoldIntegerLessThanTrue*:
  assumes *wf-stamp g stamps*
  assumes *kind g nid* = (*IntegerLessThanNode x y*)
  assumes $[g, m, p] \vdash nid \mapsto v$
  assumes *stpi-upper* (*stamps x*) $<$ *stpi-lower* (*stamps y*)
  shows $v = IntVal32\ 1$
proof $-$
  have *stamp-type*: *is-IntegerStamp* (*stamps x*)
   using *assms*
   sorry
  obtain *xval* **where** *xval*: $[g, m, p] \vdash x \mapsto xval$
   using *assms(2,3)* **sorry**
  obtain *yval* **where** *yval*: $[g, m, p] \vdash y \mapsto yval$
   using *assms(2,3)* **sorry**
  have *is-IntegerStamp* (*stamps x*) $\wedge$ *is-IntegerStamp* (*stamps y*)
   using *assms(4)*
   sorry
  then have *val-to-bool* (*intval-less-than xval yval*)
   sorry
  then show *?thesis*
   sorry
qed

lemma *tryFoldIntegerLessThanFalse*:
  assumes *wf-stamp g stamps*
  assumes *kind g nid* = (*IntegerLessThanNode x y*)
  assumes $[g, m, p] \vdash nid \mapsto v$

    assumes *stpi-lower* (*stamps x*) ≥ *stpi-upper* (*stamps y*)

    shows *v* = *IntVal32 0*

    proof −

    have *stamp-type*: *is-IntegerStamp* (*stamps x*)

      using *assms*

      sorry

    obtain *xval* **where** *xval*: [*g*, *m*, *p*] ⊢ *x* ↦ *xval*

      using *assms(2,3)* **sorry**

    obtain *yval* **where** *yval*: [*g*, *m*, *p*] ⊢ *y* ↦ *yval*

      using *assms(2,3)* **sorry**

    have *is-IntegerStamp* (*stamps x*) ∧ *is-IntegerStamp* (*stamps y*)

      using *assms(4)*

      sorry

    then have ¬(*val-to-bool* (*intval-less-than xval yval*))

      sorry

    then show *?thesis*

      sorry

qed

theorem *tryFoldProofTrue*:

  assumes *wf-stamp g stamps*

  assumes *tryFold* (*kind g nid*) *stamps True*

  assumes [*g*, *m*, *p*] ⊢ *nid* ↦ *v*

  shows *val-to-bool v*

  using *assms(2)* **proof** (*induction kind g nid stamps True rule*: *tryFold.induct*)

case (*1 stamps x y*)

  then show *?case* **using** *tryFoldIntegerEqualsAlwaysDistinct assms* **sorry**

next

  case (*2 stamps x y*)

  then show *?case* **using** *tryFoldIntegerEqualsAlwaysDistinct assms* **sorry**

next

  case (*3 stamps x y*)

  then show *?case* **using** *tryFoldIntegerLessThanTrue assms* **sorry**

next

case (*4 stamps x y*)

  then show *?case* **using** *tryFoldIntegerLessThanFalse assms* **sorry**

qed

theorem *tryFoldProofFalse*:

  assumes *wf-stamp g stamps*

  assumes *tryFold* (*kind g nid*) *stamps False*

  assumes [*g*, *m*, *p*] ⊢ *nid* ↦ *v*

  shows ¬(*val-to-bool v*)

using *assms(2)* **proof** (*induction kind g nid stamps False rule*: *tryFold.induct*)

case (*1 stamps x y*)

  then show *?case* **using** *tryFoldIntegerEqualsAlwaysDistinct assms* **sorry**

next

case (*2 stamps x y*)

  then show *?case* **using** *tryFoldIntegerEqualsNeverDistinct assms* **sorry**

next
  case (*3 stamps x y*)
  then show *?case* **using** *tryFoldIntegerLessThanTrue assms* **sorry**
next
  case (*4 stamps x y*)
  then show *?case* **using** *tryFoldIntegerLessThanFalse assms* **sorry**

qed

inductive-cases *StepE*:
  g, p ⊢ (nid,m,h) → (nid′,m′,h)

Perform conditional elimination rewrites on the graph for a particular node.

In order to determine conditional eliminations appropriately the rule needs two data structures produced by static analysis. The first parameter is the set of IRNodes that we know result in a true value when evaluated. The second parameter is a mapping from node identifiers to the flow-sensitive stamp.

The relation transforms the third parameter to the fifth parameter for a node identifier which represents the fourth parameter.

inductive *ConditionalEliminationStep* ::
  IRExpr set ⇒ (ID ⇒ Stamp) ⇒ IRGraph ⇒ ID ⇒ IRGraph ⇒ bool **where**
  impliesTrue:
  ⟦*kind g ifcond = (IfNode cid t f);*
    g ⊢ cid ≃ cond;
    ∃ ce ∈ conds . (ce & cond ↪ True);
    g′ = constantCondition True ifcond (kind g ifcond) g
    ⟧ ⟹ *ConditionalEliminationStep conds stamps g ifcond g′* |

  impliesFalse:
  ⟦*kind g ifcond = (IfNode cid t f);*
    g ⊢ cid ≃ cond;
    ∃ ce ∈ conds . (ce & cond ↪ False);
    g′ = constantCondition False ifcond (kind g ifcond) g
    ⟧ ⟹ *ConditionalEliminationStep conds stamps g ifcond g′* |

  tryFoldTrue:
  ⟦*kind g ifcond = (IfNode cid t f);*
    cond = kind g cid;
    tryFold (kind g cid) stamps True;
    g′ = constantCondition True ifcond (kind g ifcond) g
    ⟧ ⟹ *ConditionalEliminationStep conds stamps g ifcond g′* |

  tryFoldFalse:
  ⟦*kind g ifcond = (IfNode cid t f);*
    cond = kind g cid;

203

tryFold (*kind g cid*) *stamps False*;
g′ = constantCondition False ifcond (*kind g ifcond*) *g*
⟧ ⟹ *ConditionalEliminationStep conds stamps g ifcond g′*

code-pred (*modes: i ⟹ i ⟹ i ⟹ i ⟹ o ⟹ bool*) *ConditionalEliminationStep* .

thm *ConditionalEliminationStep.equation*

12.2   Control-flow Graph Traversal

type-synonym *Seen = ID set*
type-synonym *Condition = IRNode*
type-synonym *Conditions = Condition list*
type-synonym *StampFlow = (ID ⟹ Stamp) list*

nextEdge helps determine which node to traverse next by returning the first successor edge that isn't in the set of already visited nodes. If there is not an appropriate successor, None is returned instead.

fun *nextEdge :: Seen ⟹ ID ⟹ IRGraph ⟹ ID option* **where**
  nextEdge seen nid g =
    (*let nids = (filter (λnid′. nid′ ∉ seen) (successors-of (kind g nid))) in*
    (*if length nids > 0 then Some (hd nids) else None*))

pred determines which node, if any, acts as the predecessor of another.

Merge nodes represent a special case where-in the predecessor exists as an input edge of the merge node, to simplify the traversal we treat only the first input end node as the predecessor, ignoring that multiple nodes may act as a successor.

For all other nodes, the predecessor is the first element of the predecessors set. Note that in a well-formed graph there should only be one element in the predecessor set.

fun *pred :: IRGraph ⟹ ID ⟹ ID option* **where**
  pred g nid = (case kind g nid of
    (*MergeNode ends - -*) ⟹ *Some (hd ends)* |
    - ⟹
      (*if IRGraph.predecessors g nid = {}*
        then None else
        Some (hd (sorted-list-of-set (IRGraph.predecessors g nid)))
)
)

When the basic block of an if statement is entered, we know that the condition of the preceding if statement must be true. As in the GraalVM compiler, we introduce the registerNewCondition funciton which roughly corresponds to the ConditionalEliminationPhase.registerNewCondition. This method updates the flow-sensitive stamp information based on the condition which we know must be true.

fun *clip-upper* :: *Stamp* ⇒ *int* ⇒ *Stamp* **where**
  clip-upper (*IntegerStamp b l h*) *c* = (*IntegerStamp b l c*) |
  clip-upper s c = *s*
fun *clip-lower* :: *Stamp* ⇒ *int* ⇒ *Stamp* **where**
  clip-lower (*IntegerStamp b l h*) *c* = (*IntegerStamp b c h*) |
  clip-lower s c = *s*

fun *registerNewCondition* :: *IRGraph* ⇒ *Condition* ⇒ (*ID* ⇒ *Stamp*) ⇒ (*ID* ⇒ *Stamp*) **where**

  registerNewCondition g (*IntegerEqualsNode x y*) *stamps* =
    (*stamps*(*x* := *join* (*stamps x*) (*stamps y*)))(*y* := *join* (*stamps x*) (*stamps y*)) |

  registerNewCondition g (*IntegerLessThanNode x y*) *stamps* =
    (*stamps*
      (*x* := *clip-upper* (*stamps x*) (*stpi-lower* (*stamps y*))))
      (*y* := *clip-lower* (*stamps y*) (*stpi-upper* (*stamps x*))) |
  registerNewCondition g - stamps = *stamps*

fun *hdOr* :: *'a list* ⇒ *'a* ⇒ *'a* **where**
  hdOr (*x # xs*) *de* = *x* |
  hdOr [] *de* = *de*

The Step relation is a small-step traversal of the graph which handles transitions between individual nodes of the graph.

It relates a pairs of tuple of the current node, the set of seen nodes, the always true stack of IfNode conditions, and the flow-sensitive stamp information.

inductive *Step*
  :: *IRGraph* ⇒ (*ID* × *Seen* × *Conditions* × *StampFlow*) ⇒ (*ID* × *Seen* × *Conditions* × *StampFlow*) *option* ⇒ *bool*
  for *g* **where**
  — Hit a BeginNode with an IfNode predecessor which represents the start of a basic block for the IfNode. 1. nid' will be the successor of the begin node. 2. Find the first and only predecessor. 3. Extract condition from the preceding IfNode. 4. Negate condition if the begin node is second branch (we've taken the else branch of the condition) 5. Add the condition or the negated condition to stack 6. Perform any stamp updates based on the condition using the registerNewCondition function and place them on the top of the stack of stamp information
  [[*kind g nid* = *BeginNode nid'*;

  nid ∉ *seen*;
  seen' = {*nid*} ∪ *seen*;

  Some ifcond = *pred g nid*;
  kind g ifcond = *IfNode cond t f*;

  i = *find-index nid* (*successors-of* (*kind g ifcond*));
  c = (*if i = 0 then kind g cond else LogicNegationNode cond*);
  conds' = *c # conds*;

$flow' = registerNewCondition \ g \ c \ (hdOr \ flow \ (stamp \ g))\rrbracket$
$\implies Step \ g \ (nid, \ seen, \ conds, \ flow) \ (Some \ (nid', \ seen', \ conds', \ flow' \ \# \ flow)) \ |$

— Hit an EndNode 1. nid' will be the usage of EndNode 2. pop the conditions and stamp stack
$\llbracket kind \ g \ nid = EndNode;$

$nid \notin seen;$
$seen' = \{nid\} \cup seen;$

$nid' = any\text{-}usage \ g \ nid;$

$conds' = tl \ conds;$
$flow' = tl \ flow\rrbracket$
$\implies Step \ g \ (nid, \ seen, \ conds, \ flow) \ (Some \ (nid', \ seen', \ conds', \ flow')) \ |$

— We can find a successor edge that is not in seen, go there
$\llbracket \neg(is\text{-}EndNode \ (kind \ g \ nid));$
$\neg(is\text{-}BeginNode \ (kind \ g \ nid));$

$nid \notin seen;$
$seen' = \{nid\} \cup seen;$

$Some \ nid' = nextEdge \ seen' \ nid \ g\rrbracket$
$\implies Step \ g \ (nid, \ seen, \ conds, \ flow) \ (Some \ (nid', \ seen', \ conds, \ flow)) \ |$

— We can cannot find a successor edge that is not in seen, give back None
$\llbracket \neg(is\text{-}EndNode \ (kind \ g \ nid));$
$\neg(is\text{-}BeginNode \ (kind \ g \ nid));$

$nid \notin seen;$
$seen' = \{nid\} \cup seen;$

$None = nextEdge \ seen' \ nid \ g\rrbracket$
$\implies Step \ g \ (nid, \ seen, \ conds, \ flow) \ None \ |$

— We've already seen this node, give back None
$\llbracket nid \in seen\rrbracket \implies Step \ g \ (nid, \ seen, \ conds, \ flow) \ None$

code-pred (*modes*: $i \Rightarrow i \Rightarrow o \Rightarrow bool$) *Step* **.**

The ConditionalEliminationPhase relation is responsible for combining the individual traversal steps from the Step relation and the optimizations from the ConditionalEliminationStep relation to perform a transformation of the whole graph.

end

206