Taylor Models

Christoph Traut and Fabian Immler

June 16, 2019

Abstract

We present a formally verified implementation of multivariate Taylor models. Taylor models are a form of rigorous polynomial approximation, consisting of an approximation polynomial based on Taylor expansions, combined with a rigorous bound on the approximation error. Taylor models were introduced as a tool to mitigate the dependency problem of interval arithmetic. Our implementation automatically computes Taylor models for the class of elementary functions, expressed by composition of arithmetic operations and basic functions like exp, sin, or square root.

Contents

1 Topology for Floating Point Numbers **2**

2 Interval Type **3**
2.1 Membership 7
2.2 Quickcheck 14

3 Approximate Operations on Intervals of Floating Point Numbers **16**
3.1 Intervals with Floating Point Bounds 16
3.2 Intervals for standard functions 17

4 Horner Evaluation **27**

5 Splitting polynomials to reduce floating point precision **31**

6 Splitting polynomials by degree **32**

7 Multivariate Taylor Models **36**
7.1 Computing interval bounds on arithmetic expressions 36
7.2 Definition of Taylor models and notion of rangeity 36
7.3 Interval bounds for Taylor models 37
7.4 Computing taylor models for basic, univariate functions . . . 40

7.4.1 Derivations of floatarith expressions 41
7.4.2 Computing Taylor models for arbitrary univariate expressions 42
7.5 Operations on Taylor models 45
7.6 Computing Taylor models for multivariate expressions 53
7.7 Computing bounds for floatarith expressions 57

1 Topology for Floating Point Numbers

theory *Float-Topology*
imports
HOL−Analysis.Analysis
HOL−Library.Float
begin

This topology is totally disconnected and not complete, in which sense is it useful? Perhaps for convergence of intervals?

unbundle *float.lifting*

instantiation *float* :: *dist*
begin

lift-definition *dist-float* :: *float* ⇒ *float* ⇒ *real* **is** *dist* ⟨*proof*⟩

lemma *dist-float-eq-0-iff*: (*dist x y* = *0*) = (*x* = *y*) **for** *x y*::*float*
⟨*proof*⟩

lemma *dist-float-triangle2*: *dist x y* ≤ *dist x z* + *dist y z* **for** *x y z*::*float*
⟨*proof*⟩

instance ⟨*proof*⟩
end

instantiation *float* :: *uniformity*
begin

definition *uniformity-float* :: (*float* × *float*) *filter*
where *uniformity-float* = (*INF e*∈{*0*<..}. *principal* {(*x*, *y*). *dist x y* < *e*})

instance ⟨*proof*⟩
end

lemma *float-dense-in-real*:
fixes *x* :: *real*
assumes *x* < *y*
shows ∃ *r*∈*float*. *x* < *r* ∧ *r* < *y*
⟨*proof*⟩

lemma *real-of-float-dense*:
fixes x y :: *real*
assumes $x < y$
shows $\exists\, q$ :: *float*. $x <$ *real-of-float* $q \wedge$ *real-of-float* $q < y$
⟨*proof*⟩

instantiation *float* :: *linorder-topology*
begin

definition *open-float*::*float set* ⇒ *bool* **where**
open-float $S = (\forall\, x{\in}S.\ \exists\, e{>}0.\ \forall\, y.$ *dist* $y\ x < e \longrightarrow y \in S)$

instance
⟨*proof*⟩

end

instance *float* :: *metric-space*
⟨*proof*⟩

instance *float*::*topological-ab-group-add*
⟨*proof*⟩

lifting-update *float.lifting*
lifting-forget *float.lifting*

end

2 Interval Type

theory *Interval*
imports
HOL−Analysis.Analysis
HOL−Library.Set-Algebras
HOL−Library.Float
begin

A type of non-empty, closed intervals.

typedef (**overloaded**) $'a$ *interval* =
$\{(a{::}'a{::}$*preorder*$,\ b).\ a \leq b\}$
morphisms *bounds-of-interval Interval*
⟨*proof*⟩

setup-lifting *type-definition-interval*

lift-definition *lower*::($'a$::*preorder*) *interval* ⇒ $'a$ **is** *fst* ⟨*proof*⟩

lift-definition *upper*::($'a$::*preorder*) *interval* ⇒ $'a$ **is** *snd* ⟨*proof*⟩

lemma *interval-eq-iff*: $a = b \longleftrightarrow lower\ a = lower\ b \wedge upper\ a = upper\ b$
⟨*proof*⟩

lemma *interval-eqI*: $lower\ a = lower\ b \Longrightarrow upper\ a = upper\ b \Longrightarrow a = b$
⟨*proof*⟩

lemma *lower-le-upper*[*simp*]: $lower\ i \leq upper\ i$
⟨*proof*⟩

lift-definition *set-of* :: $'a$::*preorder interval* ⇒ $'a$ *set* **is** $\lambda x.\ \{fst\ x\ ..\ snd\ x\}$ ⟨*proof*⟩

lemma *set-of-eq*: $set\text{-}of\ x = \{lower\ x\ ..\ upper\ x\}$
⟨*proof*⟩

context notes [[*typedef-overloaded*]] **begin**

lift-definition(*code-dt*) *Interval*′::$'a$::*preorder* ⇒ $'a$::*preorder* ⇒ $'a$ *interval option*
is $\lambda a\ b.$ *if* $a \leq b$ *then Some* $(a,\ b)$ *else None*
⟨*proof*⟩

end

instantiation *interval* :: (*preorder*,*equal*) *equal*
begin

definition *equal-class.equal* $a\ b \equiv (lower\ a = lower\ b) \wedge (upper\ a = upper\ b)$

instance ⟨*proof*⟩
end

instantiation *interval* :: (*preorder*) *ord* **begin**

definition *less-eq-interval* :: $'a$ *interval* ⇒ $'a$ *interval* ⇒ *bool*
where $less\text{-}eq\text{-}interval\ a\ b \longleftrightarrow lower\ b \leq lower\ a \wedge upper\ a \leq upper\ b$

definition *less-interval* :: $'a$ *interval* ⇒ $'a$ *interval* ⇒ *bool*
where $less\text{-}interval\ x\ y = (x \leq y \wedge \neg\ y \leq x)$

instance ⟨*proof*⟩
end

instantiation *interval* :: (*lattice*) *semilattice-sup*
begin

lift-definition *sup-interval* :: $'a$ *interval* ⇒ $'a$ *interval* ⇒ $'a$ *interval*
is $\lambda(a,\ b)\ (c,\ d).\ (inf\ a\ c,\ sup\ b\ d)$
⟨*proof*⟩

lemma *lower-sup*[*simp*]: $lower\ (sup\ A\ B) = inf\ (lower\ A)\ (lower\ B)$

⟨*proof*⟩

lemma *upper-sup*[*simp*]: *upper* (*sup A B*) = *sup* (*upper A*) (*upper B*)
⟨*proof*⟩

instance ⟨*proof*⟩
end

lemma *set-of-interval-union*: *set-of A* ∪ *set-of B* ⊆ *set-of* (*sup A B*) **for** *A*::*'a*::*lattice interval*
⟨*proof*⟩

lemma *interval-union-commute*: *sup A B* = *sup B A* **for** *A*::*'a*::*lattice interval*
⟨*proof*⟩

lemma *interval-union-mono1*: *set-of a* ⊆ *set-of* (*sup a A*) **for** *A* :: *'a*::*lattice interval*
⟨*proof*⟩

lemma *interval-union-mono2*: *set-of A* ⊆ *set-of* (*sup a A*) **for** *A* :: *'a*::*lattice interval*
⟨*proof*⟩

lift-definition *interval-of* :: *'a*::*preorder* ⇒ *'a interval* **is** λ*x*. (*x*, *x*)
⟨*proof*⟩

lemma *lower-interval-of*[*simp*]: *lower* (*interval-of a*) = *a*
⟨*proof*⟩

lemma *upper-interval-of*[*simp*]: *upper* (*interval-of a*) = *a*
⟨*proof*⟩

definition *width* :: *'a*::{*preorder*,*minus*} *interval* ⇒ *'a*
where *width i* = *upper i* − *lower i*

instantiation *interval* :: (*ordered-ab-semigroup-add*) *ab-semigroup-add*
begin

lift-definition *plus-interval*::*'a interval* ⇒ *'a interval* ⇒ *'a interval*
is λ(*a*, *b*). λ(*c*, *d*). (*a* + *c*, *b* + *d*)
⟨*proof*⟩
lemma *lower-plus*[*simp*]: *lower* (*plus A B*) = *plus* (*lower A*) (*lower B*)
⟨*proof*⟩
lemma *upper-plus*[*simp*]: *upper* (*plus A B*) = *plus* (*upper A*) (*upper B*)
⟨*proof*⟩

instance ⟨*proof*⟩
end

instance *interval* :: ({*ordered-ab-semigroup-add*, *lattice*}) *ordered-ab-semigroup-add*
⟨*proof*⟩

instantiation *interval* :: ({*preorder*,*zero*}) *zero*
begin

lift-definition *zero-interval*::'*a interval* **is** (*0*, *0*) ⟨*proof*⟩
lemma *lower-zero*[*simp*]: *lower 0 = 0*
⟨*proof*⟩
lemma *upper-zero*[*simp*]: *upper 0 = 0*
⟨*proof*⟩
instance ⟨*proof*⟩
end

instance *interval* :: ({*ordered-comm-monoid-add*}) *comm-monoid-add*
⟨*proof*⟩

instance *interval* :: ({*ordered-comm-monoid-add*,*lattice*}) *ordered-comm-monoid-add*
⟨*proof*⟩

instantiation *interval* :: ({*ordered-ab-group-add*}) *uminus*
begin

lift-definition *uminus-interval*::'*a interval* ⇒ '*a interval* **is** λ(*a*, *b*). (−*b*, −*a*)
⟨*proof*⟩
lemma *lower-uminus*[*simp*]: *lower* (− *A*) = − *upper A*
⟨*proof*⟩
lemma *upper-uminus*[*simp*]: *upper* (− *A*) = − *lower A*
⟨*proof*⟩
instance ⟨*proof*⟩
end

instantiation *interval* :: ({*ordered-ab-group-add*}) *minus*
begin

definition *minus-interval*::'*a interval* ⇒ '*a interval* ⇒ '*a interval*
where *minus-interval a b* = *a* + − *b*
lemma *lower-minus*[*simp*]: *lower* (*minus A B*) = *minus* (*lower A*) (*upper B*)
⟨*proof*⟩
lemma *upper-minus*[*simp*]: *upper* (*minus A B*) = *minus* (*upper A*) (*lower B*)
⟨*proof*⟩

instance ⟨*proof*⟩
end

instantiation *interval* :: (*linordered-semiring*) *times*
begin

lift-definition *times-interval* :: *'a interval* ⇒ *'a interval* ⇒ *'a interval*
is λ(*a1*, *a2*). λ(*b1*, *b2*).
(*let x1* = *a1* ∗ *b1*; *x2* = *a1* ∗ *b2*; *x3* = *a2* ∗ *b1*; *x4* = *a2* ∗ *b2*
in (*min x1* (*min x2* (*min x3 x4*)), *max x1* (*max x2* (*max x3 x4*))))
⟨*proof*⟩

lemma *lower-times*:
lower (*times A B*) = *Min* {*lower A* ∗ *lower B*, *lower A* ∗ *upper B*, *upper A* ∗ *lower B*, *upper A* ∗ *upper B*}
⟨*proof*⟩

lemma *upper-times*:
upper (*times A B*) = *Max* {*lower A* ∗ *lower B*, *lower A* ∗ *upper B*, *upper A* ∗ *lower B*, *upper A* ∗ *upper B*}
⟨*proof*⟩

instance ⟨*proof*⟩
end

lemma *interval-eq-set-of-iff*: *X* = *Y* ⟷ *set-of X* = *set-of Y* **for** *X Y*::*'a*::*order interval*
⟨*proof*⟩

2.1 Membership

abbreviation (**in** *preorder*) *in-interval* ((-/ ∈$_i$ -) [*51*, *51*] *50*)
where *in-interval x X* ≡ *x* ∈ *set-of X*

lemma *in-interval-to-interval*[*intro*!]: *a* ∈$_i$ *interval-of a*
⟨*proof*⟩

lemma *plus-in-intervalI*:
fixes *x y* :: *'a* :: *ordered-ab-semigroup-add*
shows *x* ∈$_i$ *X* ⟹ *y* ∈$_i$ *Y* ⟹ *x* + *y* ∈$_i$ *X* + *Y*
⟨*proof*⟩

lemma *connected-set-of*[*intro*, *simp*]:
connected (*set-of X*) **for** *X*::*'a*::*linear-continuum-topology interval*
⟨*proof*⟩

lemma *ex-sum-in-interval-lemma*: ∃ *xa*∈{*la* .. *ua*}. ∃ *xb*∈{*lb* .. *ub*}. *x* = *xa* + *xb*
if *la* ≤ *ua lb* ≤ *ub la* + *lb* ≤ *x x* ≤ *ua* + *ub*
ua − *la* ≤ *ub* − *lb*
for *la b c d*::*'a*::*linordered-ab-group-add*
⟨*proof*⟩

lemma *ex-sum-in-interval*: ∃ *xa*≥*la*. *xa* ≤ *ua* ∧ (∃ *xb*≥*lb*. *xb* ≤ *ub* ∧ *x* = *xa* + *xb*)
if *a*: *la* ≤ *ua* **and** *b*: *lb* ≤ *ub* **and** *x*: *la* + *lb* ≤ *x x* ≤ *ua* + *ub*

for *la b c d*::*'a*::*linordered-ab-group-add*
⟨*proof*⟩

lemma *Icc-plus-Icc*:
fixes *a b c d*::*'a*::*linordered-ab-group-add*
assumes *a* ≤ *b c* ≤ *d*
shows {*a* .. *b*} + {*c* .. *d*} = {*a* + *c* .. *b* + *d*}
⟨*proof*⟩

lemma *set-of-plus*:
fixes *A* :: *'a*::*linordered-ab-group-add interval*
shows *set-of* (*A* + *B*) = *set-of A* + *set-of B*
⟨*proof*⟩

lemma *plus-in-intervalE*:
fixes *xy* :: *'a* :: *linordered-ab-group-add*
assumes *xy* ∈*i* *X* + *Y*
obtains *x y* **where** *xy* = *x* + *y x* ∈*i* *X y* ∈*i* *Y*
⟨*proof*⟩

lemma *set-of-uminus*: *set-of* (−*X*) = {− *x* | *x*. *x* ∈ *set-of X*}
for *X* :: *'a* :: *ordered-ab-group-add interval*
⟨*proof*⟩

lemma *uminus-in-intervalI*:
fixes *x* :: *'a* :: *ordered-ab-group-add*
shows *x* ∈*i* *X* ⟹ −*x* ∈*i* −*X*
⟨*proof*⟩

lemma *uminus-in-intervalD*:
fixes *x* :: *'a* :: *ordered-ab-group-add*
shows *x* ∈*i* − *X* ⟹ − *x* ∈*i* *X*
⟨*proof*⟩

lemma *minus-in-intervalI*:
fixes *x y* :: *'a* :: *ordered-ab-group-add*
shows *x* ∈*i* *X* ⟹ *y* ∈*i* *Y* ⟹ *x* − *y* ∈*i* *X* − *Y*
⟨*proof*⟩

lemma *set-of-minus*: *set-of* (*X* − *Y*) = {*x* − *y* | *x y* . *x* ∈ *set-of X* ∧ *y* ∈ *set-of Y*}
for *X Y* :: *'a* :: *linordered-ab-group-add interval*
⟨*proof*⟩

lemma *times-in-intervalI*:
fixes *x y*::*'a*::*linordered-ring*
assumes *x* ∈*i* *X y* ∈*i* *Y*
shows *x* ∗ *y* ∈*i* *X* ∗ *Y*
⟨*proof*⟩

lemma *times-in-intervalE*:
fixes *xy* :: *'a* :: {*linordered-semiring*, *real-normed-algebra*, *linear-continuum-topology*}
— TODO: linear continuum topology is pretty strong
assumes *xy* $\in_i$ *X* $*$ *Y*
obtains *x y* **where** *xy* = *x* $*$ *y x* $\in_i$ *X y* $\in_i$ *Y*
⟨*proof*⟩

lemma *set-of-times*: *set-of* (*X* $*$ *Y*) = {*x* $*$ *y* | *x y*. *x* ∈ *set-of X* ∧ *y* ∈ *set-of Y*}
for *X Y*::*'a* :: {*linordered-ring*, *real-normed-algebra*, *linear-continuum-topology*}
interval
⟨*proof*⟩

instance *interval* :: (*linordered-idom*) *cancel-semigroup-add*
⟨*proof*⟩

lemma *interval-mul-commute*: *A* $*$ *B* = *B* $*$ *A* **for** *A B*:: *'a*::*linordered-idom*
interval
⟨*proof*⟩

lemma *interval-times-zero-right*[*simp*]: *A* $*$ *0* = *0* **for** *A* :: *'a*::*linordered-ring*
interval
⟨*proof*⟩

lemma *interval-times-zero-left*[*simp*]:
0 $*$ *A* = *0* **for** *A* :: *'a*::*linordered-ring interval*
⟨*proof*⟩

instantiation *interval* :: ({*preorder*,*one*}) *one*
begin

lift-definition *one-interval*::*'a interval* **is** (*1*, *1*) ⟨*proof*⟩
lemma *lower-one*[*simp*]: *lower 1* = *1*
⟨*proof*⟩
lemma *upper-one*[*simp*]: *upper 1* = *1*
⟨*proof*⟩
instance ⟨*proof*⟩
end

instance *interval* :: ({*one*, *preorder*, *linordered-semiring*}) *power*
⟨*proof*⟩

lemma *set-of-one*[*simp*]: *set-of* (*1*::*'a*::{*one*, *order*} *interval*) = {*1*}
⟨*proof*⟩

instance *interval* ::
({*linordered-idom*,*linordered-ring*, *real-normed-algebra*, *linear-continuum-topology*})
monoid-mult
⟨*proof*⟩

lemma *one-times-ivl-left*[*simp*]: *1 * A = A* **for** *A* :: *'a*::*linordered-idom interval*
⟨*proof*⟩

lemma *one-times-ivl-right*[*simp*]: *A * 1 = A* **for** *A* :: *'a*::*linordered-idom interval*
⟨*proof*⟩

lemma *set-of-power-mono*: *a^n ∈ set-of (A^n)* **if** *a ∈ set-of A*
for *a* :: *'a*::*linordered-idom*
⟨*proof*⟩

lemma *set-of-add-cong*:
set-of (A + B) = set-of (A' + B')
if *set-of A = set-of A' set-of B = set-of B'*
for *A* :: *'a*::*linordered-ab-group-add interval*
⟨*proof*⟩

lemma *set-of-add-inc-left*:
set-of (A + B) ⊆ set-of (A' + B)
if *set-of A ⊆ set-of A'*
for *A* :: *'a*::*linordered-ab-group-add interval*
⟨*proof*⟩

lemma *set-of-add-inc-right*:
set-of (A + B) ⊆ set-of (A + B')
if *set-of B ⊆ set-of B'*
for *A* :: *'a*::*linordered-ab-group-add interval*
⟨*proof*⟩

lemma *set-of-add-inc*:
set-of (A + B) ⊆ set-of (A' + B')
if *set-of A ⊆ set-of A' set-of B ⊆ set-of B'*
for *A* :: *'a*::*linordered-ab-group-add interval*
⟨*proof*⟩

lemma *set-of-neg-inc*:
set-of (−A) ⊆ set-of (−A')
if *set-of A ⊆ set-of A'*
for *A* :: *'a*::*ordered-ab-group-add interval*
⟨*proof*⟩

lemma *set-of-sub-inc-left*:
set-of (A − B) ⊆ set-of (A' − B)
if *set-of A ⊆ set-of A'*
for *A* :: *'a*::*linordered-ab-group-add interval*
⟨*proof*⟩

lemma *set-of-sub-inc-right*:
set-of (A − B) ⊆ set-of (A − B')

if *set-of* $B \subseteq$ *set-of* B'
for A :: $'a$::*linordered-ab-group-add interval*
⟨*proof*⟩

lemma *set-of-sub-inc*:
set-of $(A - B) \subseteq$ *set-of* $(A' - B')$
if *set-of* $A \subseteq$ *set-of* A' *set-of* $B \subseteq$ *set-of* B'
for A :: $'a$::*linordered-idom interval*
⟨*proof*⟩

lemma *set-of-mul-inc-right*:
set-of $(A * B) \subseteq$ *set-of* $(A * B')$
if *set-of* $B \subseteq$ *set-of* B'
for A :: $'a$::*linordered-ring interval*
⟨*proof*⟩

lemma *set-of-distrib-left*:
set-of $(B * (A1 + A2)) \subseteq$ *set-of* $(B * A1 + B * A2)$
for $A1$ :: $'a$::*linordered-ring interval*
⟨*proof*⟩

lemma *set-of-distrib-right*:
set-of $((A1 + A2) * B) \subseteq$ *set-of* $(A1 * B + A2 * B)$
for $A1\ A2\ B$ :: $'a$::{*linordered-ring*, *real-normed-algebra*, *linear-continuum-topology*} *interval*
⟨*proof*⟩

lemma *set-of-mul-inc-left*:
set-of $(A * B) \subseteq$ *set-of* $(A' * B)$
if *set-of* $A \subseteq$ *set-of* A'
for A :: $'a$::{*linordered-ring*, *real-normed-algebra*, *linear-continuum-topology*} *interval*
⟨*proof*⟩

lemma *set-of-mul-inc*:
set-of $(A * B) \subseteq$ *set-of* $(A' * B')$
if *set-of* $A \subseteq$ *set-of* A' *set-of* $B \subseteq$ *set-of* B'
for A :: $'a$::{*linordered-ring*, *real-normed-algebra*, *linear-continuum-topology*} *interval*
⟨*proof*⟩

lemma *set-of-pow-inc*:
set-of $(A \hat{} n) \subseteq$ *set-of* $(A' \hat{} n)$
if *set-of* $A \subseteq$ *set-of* A'
for A :: $'a$::{*linordered-idom*, *real-normed-algebra*, *linear-continuum-topology*} *interval*
⟨*proof*⟩

lemma *set-of-distrib-right-left*:
set-of $((A1 + A2) * (B1 + B2)) \subseteq$ *set-of* $(A1 * B1 + A1 * B2 + A2 * B1 + A2 * B2)$

for *A1* :: *'a*::{*linordered-idom*, *real-normed-algebra*, *linear-continuum-topology*} *interval*
⟨*proof*⟩

lemma *mult-bounds-enclose-zero1*:
min (*la* ∗ *lb*) (*min* (*la* ∗ *ub*) (*min* (*lb* ∗ *ua*) (*ua* ∗ *ub*))) ≤ *0*
0 ≤ *max* (*la* ∗ *lb*) (*max* (*la* ∗ *ub*) (*max* (*lb* ∗ *ua*) (*ua* ∗ *ub*)))
if *la* ≤ *0* *0* ≤ *ua*
for *la lb ua ub*:: *'a*::*linordered-idom*
⟨*proof*⟩

lemma *mult-bounds-enclose-zero2*:
min (*la* ∗ *lb*) (*min* (*la* ∗ *ub*) (*min* (*lb* ∗ *ua*) (*ua* ∗ *ub*))) ≤ *0*
0 ≤ *max* (*la* ∗ *lb*) (*max* (*la* ∗ *ub*) (*max* (*lb* ∗ *ua*) (*ua* ∗ *ub*)))
if *lb* ≤ *0* *0* ≤ *ub*
for *la lb ua ub*:: *'a*::*linordered-idom*
⟨*proof*⟩

lemma *set-of-mul-contains-zero*:
0 ∈ *set-of* (*A* ∗ *B*)
if *0* ∈ *set-of A* ∨ *0* ∈ *set-of B*
for *A* :: *'a*::*linordered-idom interval*
⟨*proof*⟩

instance *interval* :: (*linordered-semiring*) *mult-zero*
⟨*proof*⟩

lift-definition *min-interval*::*'a*::*linorder interval* ⇒ *'a interval* ⇒ *'a interval* **is**
λ(*l1*, *u1*). λ(*l2*, *u2*). (*min l1 l2*, *min u1 u2*)
⟨*proof*⟩
lemma *lower-min-interval*[*simp*]: *lower* (*min-interval x y*) = *min* (*lower x*) (*lower y*)
⟨*proof*⟩
lemma *upper-min-interval*[*simp*]: *upper* (*min-interval x y*) = *min* (*upper x*) (*upper y*)
⟨*proof*⟩

lemma *min-intervalI*:
a ∈*i* *A* ⟹ *b* ∈*i* *B* ⟹ *min a b* ∈*i* *min-interval A B*
⟨*proof*⟩

lift-definition *max-interval*::*'a*::*linorder interval* ⇒ *'a interval* ⇒ *'a interval* **is**
λ(*l1*, *u1*). λ(*l2*, *u2*). (*max l1 l2*, *max u1 u2*)
⟨*proof*⟩
lemma *lower-max-interval*[*simp*]: *lower* (*max-interval x y*) = *max* (*lower x*) (*lower y*)
⟨*proof*⟩
lemma *upper-max-interval*[*simp*]: *upper* (*max-interval x y*) = *max* (*upper x*) (*upper y*)

⟨*proof*⟩

lemma *max-intervalI*:
a ∈$_i$ *A* ⟹ *b* ∈$_i$ *B* ⟹ *max a b* ∈$_i$ *max-interval A B*
⟨*proof*⟩

lift-definition *abs-interval*::'*a*::*linordered-idom interval* ⇒ '*a interval* **is**
(λ(*l*,*u*). (*if l* < *0* ∧ *0* < *u then 0 else min* |*l*| |*u*|, *max* |*l*| |*u*|))
⟨*proof*⟩

lemma *lower-abs-interval*[*simp*]:
lower (*abs-interval x*) = (*if lower x* < *0* ∧ *0* < *upper x then 0 else min* |*lower x*| |*upper x*|)
⟨*proof*⟩
lemma *upper-abs-interval*[*simp*]: *upper* (*abs-interval x*) = *max* |*lower x*| |*upper x*|
⟨*proof*⟩

lemma *in-abs-intervalI1*:
lx < *0* ⟹ *0* < *ux* ⟹ *0* ≤ *xa* ⟹ *xa* ≤ *max* (− *lx*) (*ux*) ⟹ *xa* ∈ *abs* ‘ {*lx*..*ux*}
for *xa*::'*a*::*linordered-idom*
⟨*proof*⟩

lemma *in-abs-intervalI2*:
min (|*lx*|) |*ux*| ≤ *xa* ⟹ *xa* ≤ *max* |*lx*| |*ux*| ⟹ *lx* ≤ *ux* ⟹ *0* ≤ *lx* ∨ *ux* ≤ *0* ⟹
xa ∈ *abs* ‘ {*lx*..*ux*}
for *xa*::'*a*::*linordered-idom*
⟨*proof*⟩

lemma *set-of-abs-interval*: *set-of* (*abs-interval x*) = *abs* ‘ *set-of x*
⟨*proof*⟩

fun *split-domain* :: ('*a*::*preorder interval* ⇒ '*a interval list*) ⇒ '*a interval list* ⇒ '*a interval list list*
where *split-domain split* [] = [[]]
| *split-domain split* (*I*#*Is*) = (
let S = *split I*;
D = *split-domain split Is*
in concat (*map* (λ*d*. *map* (λ*s*. *s* # *d*) *S*) *D*)
)

context notes [[*typedef-overloaded*]] **begin**
lift-definition(*code-dt*) *split-interval*::'*a*::*linorder interval* ⇒ '*a* ⇒ ('*a interval* × '*a interval*)
is λ(*l*, *u*) *x*. ((*min l x*, *max l x*), (*min u x*, *max u x*))
⟨*proof*⟩
end

lemma *split-domain-nonempty*:
assumes $\bigwedge I.$ *split* $I \neq []$
shows *split-domain split* $I \neq []$
⟨*proof*⟩

lemma *split-intervalD*: *split-interval* X $x = (A, B) \Longrightarrow$ *set-of* $X \subseteq$ *set-of* $A \cup$ *set-of* B
⟨*proof*⟩

definition *split-float-interval* $x =$ *split-interval* x $((lower\ x + upper\ x) * Float\ 1\ (-1))$

lemma *split-float-intervalD*: *split-float-interval* $X = (A, B) \Longrightarrow$ *set-of* $X \subseteq$ *set-of* $A \cup$ *set-of* B
⟨*proof*⟩

lemmas *float-round-down-le*[*intro*] = *order-trans*[*OF float-round-down*]
and *float-round-up-ge*[*intro*] = *order-trans*[*OF* - *float-round-up*]

instantiation *interval* :: ({*topological-space*, *preorder*}) *topological-space*
begin

definition *open-interval-def*[*code del*]: *open* $(X::'a\ interval\ set) =$
$(\forall x{\in}X.$
$\exists A\ B.$
open $A \wedge$
open $B \wedge$
$lower\ x \in A \wedge upper\ x \in B \wedge Interval\ `\ (A \times B) \subseteq X)$

instance
⟨*proof*⟩

end

definition *mid* :: *float interval* ⇒ *float*
where $mid\ i = (lower\ i + upper\ i) * Float\ 1\ (-1)$

lemma *mid-in-interval*: $mid\ i \in_i i$
⟨*proof*⟩

definition *centered* :: *float interval* ⇒ *float interval*
where $centered\ i = i - interval\text{-}of\ (mid\ i)$

2.2 Quickcheck

lift-definition $Ivl::'a \Rightarrow 'a::preorder \Rightarrow 'a\ interval$ **is** $\lambda a\ b.\ (min\ a\ b,\ b)$
⟨*proof*⟩

instantiation *interval* :: ({*exhaustive*,*preorder*}) *exhaustive*
begin

definition *exhaustive-interval*::('*a interval* ⇒ (*bool* × *term list*) *option*)
⇒ *natural* ⇒ (*bool* × *term list*) *option*
where
exhaustive-interval f d =
Quickcheck-Exhaustive.exhaustive (λ*x*. *Quickcheck-Exhaustive.exhaustive* (λ*y*. *f* (*Ivl x y*)) *d*) *d*

instance ⟨*proof*⟩

end

definition (**in** *term-syntax*) [*code-unfold*]:
valtermify-interval x y = *Code-Evaluation.valtermify* (*Ivl*::'*a*::{*preorder*,*typerep*}⇒-) {·} *x* {·} *y*

instantiation *interval* :: ({*full-exhaustive*,*preorder*,*typerep*}) *full-exhaustive*
begin

definition *full-exhaustive-interval*::
('*a interval* × (*unit* ⇒ *term*) ⇒ (*bool* × *term list*) *option*)
⇒ *natural* ⇒ (*bool* × *term list*) *option* **where**
full-exhaustive-interval f d =
Quickcheck-Exhaustive.full-exhaustive
(λ*x*. *Quickcheck-Exhaustive.full-exhaustive* (λ*y*. *f* (*valtermify-interval x y*)) *d*) *d*

instance ⟨*proof*⟩

end

instantiation *interval* :: ({*random*,*preorder*,*typerep*}) *random*
begin

definition *random-interval* ::
natural
⇒ *natural* × *natural*
⇒ ('*a interval* × (*unit* ⇒ *term*)) × *natural* × *natural* **where**
random-interval i =
scomp (*Quickcheck-Random.random i*)
(λ*man*. *scomp* (*Quickcheck-Random.random i*) (λ*exp*. *Pair* (*valtermify-interval man exp*)))

instance ⟨*proof*⟩

end

end

3 Approximate Operations on Intervals of Floating Point Numbers

theory *Interval-Approximation*
imports
HOL−Decision-Procs.Approximation-Bounds
Interval
begin

lifting-update *float.lifting* — TODO: in Float!
lifting-forget *float.lifting*

TODO: many of the lemmas should move to theories Float or Approximation (the latter should be based on type *interval*.

3.1 Intervals with Floating Point Bounds

lift-definition *round-interval* :: *nat* ⇒ *float interval* ⇒ *float interval*
is λ*p*. λ(*l*, *u*). (*float-round-down p l*, *float-round-up p u*)
⟨*proof*⟩

lemma *lower-round-ivl*[*simp*]: *lower* (*round-interval p x*) = *float-round-down p* (*lower x*)
⟨*proof*⟩
lemma *upper-round-ivl*[*simp*]: *upper* (*round-interval p x*) = *float-round-up p* (*upper x*)
⟨*proof*⟩

lemma *round-ivl-correct*: *set-of A* ⊆ *set-of* (*round-interval prec A*)
⟨*proof*⟩

lift-definition *truncate-ivl* :: *nat* ⇒ *real interval* ⇒ *real interval*
is λ*p*. λ(*l*, *u*). (*truncate-down p l*, *truncate-up p u*)
⟨*proof*⟩

lemma *lower-truncate-ivl*[*simp*]: *lower* (*truncate-ivl p x*) = *truncate-down p* (*lower x*)
⟨*proof*⟩
lemma *upper-truncate-ivl*[*simp*]: *upper* (*truncate-ivl p x*) = *truncate-up p* (*upper x*)
⟨*proof*⟩

lemma *truncate-ivl-correct*: *set-of A* ⊆ *set-of* (*truncate-ivl prec A*)
⟨*proof*⟩

lift-definition *real-interval*::*float interval* ⇒ *real interval*
is λ(*l*, *u*). (*real-of-float l*, *real-of-float u*)
⟨*proof*⟩

lemma *lower-real-interval*[*simp*]: *lower* (*real-interval x*) = *lower x*
⟨*proof*⟩
lemma *upper-real-interval*[*simp*]: *upper* (*real-interval x*) = *upper x*
⟨*proof*⟩

definition *set-of'* *x* = (*case x of None* ⇒ *UNIV* | *Some i* ⇒ *set-of* (*real-interval i*))

lemma *real-interval-min-interval*[*simp*]:
real-interval (*min-interval a b*) = *min-interval* (*real-interval a*) (*real-interval b*)
⟨*proof*⟩

lemma *real-interval-max-interval*[*simp*]:
real-interval (*max-interval a b*) = *max-interval* (*real-interval a*) (*real-interval b*)
⟨*proof*⟩

3.2 Intervals for standard functions

lift-definition *power-float-interval* :: *nat* ⇒ *nat* ⇒ *float interval* ⇒ *float interval*
is λ*p n* (*l*, *u*). *float-power-bnds p n l u*
⟨*proof*⟩

lemma *lower-power-float-interval*[*simp*]:
lower (*power-float-interval p n x*) = *fst* (*float-power-bnds p n* (*lower x*) (*upper x*))
⟨*proof*⟩
lemma *upper-power-float-interval*[*simp*]:
upper (*power-float-interval p n x*) = *snd* (*float-power-bnds p n* (*lower x*) (*upper x*))
⟨*proof*⟩

lemma *power-float-intervalI*: *x* ∈$_i$ *real-interval X* ⟹ *x* ^ *n* ∈$_i$ *real-interval* (*power-float-interval p n X*)
⟨*proof*⟩

lift-definition *mult-float-interval*::*nat* ⇒ *float interval* ⇒ *float interval* ⇒ *float interval*
is λ*prec*. λ(*a1*, *a2*). λ(*b1*, *b2*). *bnds-mult prec a1 a2 b1 b2*
⟨*proof*⟩

lemma *lower-mult-float-interval*[*simp*]:
lower (*mult-float-interval p x y*) = *fst* (*bnds-mult p* (*lower x*) (*upper x*) (*lower y*) (*upper y*))
⟨*proof*⟩
lemma *upper-mult-float-interval*[*simp*]:

upper (*mult-float-interval p x y*) = *snd* (*bnds-mult p* (*lower x*) (*upper x*) (*lower y*) (*upper y*))
⟨*proof*⟩

lemma *mult-float-interval*:
set-of (*real-interval A*) ∗ *set-of* (*real-interval B*) ⊆
set-of (*real-interval* (*mult-float-interval prec A B*))
⟨*proof*⟩

lemma *mult-float-intervalI*:
x ∗ *y* ∈$_i$ (*real-interval* (*mult-float-interval prec A B*))
if *x* ∈$_i$ *real-interval A y* ∈$_i$ *real-interval B*
⟨*proof*⟩

lift-definition *sqrt-float-interval*::*nat* ⇒ *float interval* ⇒ *float interval*
is λ*prec*. λ(*lx*, *ux*). (*lb-sqrt prec lx*, *ub-sqrt prec ux*)
⟨*proof*⟩

lemma *lower-float-interval*[*simp*]: *lower* (*sqrt-float-interval prec X*) = *lb-sqrt prec* (*lower X*)
⟨*proof*⟩

lemma *upper-float-interval*[*simp*]: *upper* (*sqrt-float-interval prec X*) = *ub-sqrt prec* (*upper X*)
⟨*proof*⟩

lemma *sqrt-float-interval*:
sqrt ‘ *set-of* (*real-interval X*) ⊆ *set-of* (*real-interval* (*sqrt-float-interval prec X*))
⟨*proof*⟩

lemma *sqrt-float-intervalI*:
sqrt x ∈$_i$ *real-interval* (*sqrt-float-interval p X*)
if *x* ∈ *set-of* (*real-interval X*)
⟨*proof*⟩

lemmas [*simp del*] = *lb-arctan.simps ub-arctan.simps*

lemma *lb-arctan*: *arctan* (*real-of-float x*) ≤ *y* ⟹ *real-of-float* (*lb-arctan prec x*) ≤ *y*
and *ub-arctan*: *y* ≤ *arctan x* ⟹ *y* ≤ *ub-arctan prec x*
for *x*::*float* **and** *y*::*real*
⟨*proof*⟩

lift-definition *arctan-float-interval* :: *nat* ⇒ *float interval* ⇒ *float interval*
is λ*prec*. λ(*lx*, *ux*). (*lb-arctan prec lx*, *ub-arctan prec ux*)
⟨*proof*⟩

lemma *lower-arctan-float-interval*[*simp*]: *lower* (*arctan-float-interval p x*) = *lb-arctan p* (*lower x*)

⟨*proof*⟩
lemma *upper-arctan-float-interval*[*simp*]: *upper* (*arctan-float-interval p x*) = *ub-arctan p* (*upper x*)
⟨*proof*⟩

lemma *arctan-float-interval*:
arctan ‘ *set-of* (*real-interval x*) ⊆ *set-of* (*real-interval* (*arctan-float-interval p x*))
⟨*proof*⟩

lemma *arctan-float-intervalI*:
arctan x ∈$_i$ *real-interval* (*arctan-float-interval p X*)
if *x* ∈ *set-of* (*real-interval X*)
⟨*proof*⟩

lemma *bnds-cos-lower*: ⋀*x*. *real-of-float xl* ≤ *x* ⟹ *x* ≤ *real-of-float xu* ⟹ *cos x* ≤ *y* ⟹ *real-of-float* (*fst* (*bnds-cos prec xl xu*)) ≤ *y*
and *bnds-cos-upper*: ⋀*x*. *real-of-float xl* ≤ *x* ⟹ *x* ≤ *real-of-float xu* ⟹ *y* ≤ *cos x* ⟹ *y* ≤ *real-of-float* (*snd* (*bnds-cos prec xl xu*))
for *xl xu*::*float* **and** *y*::*real*
⟨*proof*⟩

lift-definition *cos-float-interval* :: *nat* ⇒ *float interval* ⇒ *float interval*
is λ*prec*. λ(*lx*, *ux*). *bnds-cos prec lx ux*
⟨*proof*⟩

lemma *lower-cos-float-interval*[*simp*]: *lower* (*cos-float-interval p x*) = *fst* (*bnds-cos p* (*lower x*) (*upper x*))
⟨*proof*⟩
lemma *upper-cos-float-interval*[*simp*]: *upper* (*cos-float-interval p x*) = *snd* (*bnds-cos p* (*lower x*) (*upper x*))
⟨*proof*⟩

lemma *cos-float-interval*:
cos ‘ *set-of* (*real-interval x*) ⊆ *set-of* (*real-interval* (*cos-float-interval p x*))
⟨*proof*⟩

lemma *cos-float-intervalI*:
cos x ∈$_i$ *real-interval* (*cos-float-interval p X*)
if *x* ∈ *set-of* (*real-interval X*)
⟨*proof*⟩

lemma *lb-exp*: *exp x* ≤ *y* ⟹ *lb-exp prec x* ≤ *y*
and *ub-exp*: *y* ≤ *exp x* ⟹ *y* ≤ *ub-exp prec x*
for *x*::*float* **and** *y*::*real* ⟨*proof*⟩

lift-definition *exp-float-interval* :: *nat* ⇒ *float interval* ⇒ *float interval*
is λ*prec*. λ(*lx*, *ux*). (*lb-exp prec lx*, *ub-exp prec ux*)
⟨*proof*⟩

lemma *lower-exp-float-interval*[*simp*]: *lower* (*exp-float-interval p x*) = *lb-exp p* (*lower x*)
⟨*proof*⟩
lemma *upper-exp-float-interval*[*simp*]: *upper* (*exp-float-interval p x*) = *ub-exp p* (*upper x*)
⟨*proof*⟩

lemma *exp-float-interval*:
exp ‘ *set-of* (*real-interval x*) ⊆ *set-of* (*real-interval* (*exp-float-interval p x*))
⟨*proof*⟩

lemma *exp-float-intervalI*:
exp x ∈$_i$ *real-interval* (*exp-float-interval p X*)
if *x* ∈ *set-of* (*real-interval X*)
⟨*proof*⟩

lemmas [*simp del*] = *lb-ln.simps ub-ln.simps*

lemma *lb-lnD*:
y ≤ *ln x* ∧ *0* < *real-of-float x* **if** *lb-ln prec x* = *Some y*
⟨*proof*⟩

lemma *ub-lnD*:
ln x ≤ *y*∧ *0* < *real-of-float x* **if** *ub-ln prec x* = *Some y*
⟨*proof*⟩

lift-definition(*code-dt*) *ln-float-interval* :: *nat* ⇒ *float interval* ⇒ *float interval option*
is λ*prec*. λ(*lx*, *ux*).
Option.bind (*lb-ln prec lx*) (λ*l*.
Option.bind (*ub-ln prec ux*) (λ*u*. *Some* (*l*, *u*)))
⟨*proof*⟩

lemma *ln-float-interval-eq-Some-conv*[*simp*]:
ln-float-interval p x = *Some y* ⟷
lb-ln p (*lower x*) = *Some* (*lower y*) ∧ *ub-ln p* (*upper x*) = *Some* (*upper y*)
⟨*proof*⟩

lemma *ln-float-interval*: *ln* ‘ *set-of* (*real-interval x*) ⊆ *set-of* (*real-interval y*)
if *ln-float-interval p x* = *Some y*
⟨*proof*⟩

lemma *ln-float-intervalI*:
ln x ∈ *set-of′* (*ln-float-interval p X*)
if *x* ∈$_i$ (*real-interval X*)
⟨*proof*⟩

lift-definition(*code-dt*) *powr-float-interval* :: *nat* ⇒ *float interval* ⇒ *float interval* ⇒ *float interval option*

is *λprec. λ(l1, u1). λ(l2, u2). bnds-powr prec l1 u1 l2 u2*
⟨*proof*⟩

lemma *powr-float-interval*:
{*x powr y* | *x y. x* ∈ *set-of* (*real-interval X*) ∧ *y* ∈ *set-of* (*real-interval Y*)}
⊆ *set-of* (*real-interval R*)
if *powr-float-interval prec X Y* = *Some R*
⟨*proof*⟩

lemma *powr-float-intervalI*:
x powr y ∈ *set-of'* (*powr-float-interval p X Y*)
if *x* ∈$_i$ *real-interval X y* ∈$_i$ *real-interval Y*
⟨*proof*⟩

lift-definition(*code-dt*) *inverse-float-interval*::*nat* ⇒ *float interval* ⇒ *float interval option* **is**
λprec (*l*, *u*). *if* (*0* < *l* ∨ *u* < *0*) *then Some* (*float-divl prec 1 u*, *float-divr prec 1 l*) *else None*
⟨*proof*⟩

lemma *inverse-float-interval-eq-Some-conv*[*simp*]:
defines *one* ≡ (*1*::*float*)
shows
inverse-float-interval p X = *Some R* ⟷
(*lower X* > *0* ∨ *upper X* < *0*) ∧
lower R = *float-divl p one* (*upper X*) ∧
upper R = *float-divr p one* (*lower X*)
⟨*proof*⟩

lemma *inverse-float-interval*:
inverse ‘ *set-of* (*real-interval X*) ⊆ *set-of* (*real-interval Y*)
if *inverse-float-interval p X* = *Some Y*
⟨*proof*⟩

lemma *inverse-float-intervalI*:
x ∈ *set-of* (*real-interval X*) ⟹ *inverse x* ∈ *set-of'* (*inverse-float-interval p X*)
⟨*proof*⟩

lift-definition *pi-float-interval*::*nat* ⇒ *float interval* **is** *λprec.* (*lb-pi prec*, *ub-pi prec*)
⟨*proof*⟩

lemma *lower-pi-float-interval*[*simp*]: *lower* (*pi-float-interval prec*) = *lb-pi prec*
⟨*proof*⟩
lemma *upper-pi-float-interval*[*simp*]: *upper* (*pi-float-interval prec*) = *ub-pi prec*
⟨*proof*⟩
lemma *pi-float-interval*: *pi* ∈ *set-of* (*real-interval* (*pi-float-interval prec*))
⟨*proof*⟩

lemma *real-interval-abs-interval*[*simp*]:
real-interval (*abs-interval x*) = *abs-interval* (*real-interval x*)
⟨*proof*⟩

lift-definition *floor-float-interval*::*float interval* ⇒ *float interval* **is**
λ(*l*, *u*). (*floor-fl l*, *floor-fl u*)
⟨*proof*⟩

lemma *lower-floor-float-interval*[*simp*]: *lower* (*floor-float-interval x*) = *floor-fl* (*lower x*)
⟨*proof*⟩
lemma *upper-floor-float-interval*[*simp*]: *upper* (*floor-float-interval x*) = *floor-fl* (*upper x*)
⟨*proof*⟩

lemma *floor-float-intervalI*: ⌊*x*⌋ ∈$_i$ *real-interval* (*floor-float-interval X*)
if *x* ∈$_i$ *real-interval X*
⟨*proof*⟩

lemma *in-intervalI*:
x ∈$_i$ *X* **if** *lower X* ≤ *x x* ≤ *upper X*
⟨*proof*⟩

abbreviation *in-real-interval* ((-/ ∈$_r$ -) [*51*, *51*] *50*) **where**
x ∈$_r$ *X* ≡ *x* ∈$_i$ *real-interval X*

lemma *in-real-intervalI*:
x ∈$_r$ *X* **if** *lower X* ≤ *x x* ≤ *upper X* **for** *x*::*real* **and** *X*::*float interval*
⟨*proof*⟩

lemma *lower-Interval*: *lower* (*Interval x*) = *fst x*
and *upper-Interval*: *upper* (*Interval x*) = *snd x*
if *fst x* ≤ *snd x*
⟨*proof*⟩

definition *all-in-i* :: 'a::*preorder list* ⇒ 'a *interval list* ⇒ *bool*
(**infix** (*all'-in*$_i$) *50*)
where *x all-in*$_i$ *I* = (*length x* = *length I* ∧ (∀ *i* < *length I*. *x* ! *i* ∈$_i$ *I* ! *i*))

definition *all-in* :: *real list* ⇒ *float interval list* ⇒ *bool*
(**infix** (*all'-in*) *50*)
where *x all-in I* = (*length x* = *length I* ∧ (∀ *i* < *length I*. *x* ! *i* ∈$_r$ *I* ! *i*))

definition *all-subset* :: 'a::*order interval list* ⇒ 'a *interval list* ⇒ *bool*
(**infix** (*all'-subset*) *50*)
where *I all-subset J* = (*length I* = *length J* ∧ (∀ *i* < *length I*. *set-of* (*I*!*i*) ⊆ *set-of* (*J*!*i*)))

lemmas [*simp*] = *all-in-def all-subset-def*

lemma *all-subsetD*:
assumes *I all-subset J*
assumes *x all-in I*
shows *x all-in J*
⟨*proof*⟩

lemma *plus-down-mono*: *plus-down p a b* ≤ *plus-down p c d* **if** *a* + *b* ≤ *c* + *d*
⟨*proof*⟩

lemma *plus-up-mono*: *plus-up p a b* ≤ *plus-up p c d* **if** *a* + *b* ≤ *c* + *d*
⟨*proof*⟩

lemma *round-interval-mono*: *set-of* (*round-interval prec X*) ⊆ *set-of* (*round-interval prec Y*)
if *set-of X* ⊆ *set-of Y*
⟨*proof*⟩

lemma *mult-mono-nonpos-nonneg*: *a* ∗ *b* ≤ *c* ∗ *d*
if *a* ≤ *c a* ≤ *0 0* ≤ *d d* ≤ *b* **for** *a b c d*::′*a*::*ordered-ring*
⟨*proof*⟩

lemma *mult-mono-nonneg-nonpos*: *b* ∗ *a* ≤ *d* ∗ *c*
if *a* ≤ *c c* ≤ *0 0* ≤ *d d* ≤ *b* **for** *a b c d*::′*a*::*ordered-ring*
⟨*proof*⟩

lemma *mult-mono-nonpos-nonpos*: *a* ∗ *b* ≤ *c* ∗ *d*
if *a* ≥ *c a* ≤ *0 b* ≥ *d d* ≤ *0* **for** *a b c d*::*real*
⟨*proof*⟩

lemma *mult-float-mono1*:
notes *mono-rules* = *plus-down-mono add-mono nprt-mono nprt-le-zero zero-le-pprt pprt-mono*
shows *a* ≤ *b* ⟹ *ab* ≤ *bb* ⟹
aa ≤ *a* ⟹
b ≤ *ba* ⟹
ac ≤ *ab* ⟹
bb ≤ *bc* ⟹
plus-down prec (*nprt aa* ∗ *pprt bc*)
(*plus-down prec* (*nprt ba* ∗ *nprt bc*)
(*plus-down prec* (*pprt aa* ∗ *pprt ac*)
(*pprt ba* ∗ *nprt ac*)))
≤ *plus-down prec* (*nprt a* ∗ *pprt bb*)
(*plus-down prec* (*nprt b* ∗ *nprt bb*)
(*plus-down prec* (*pprt a* ∗ *pprt ab*)
(*pprt b* ∗ *nprt ab*)))
⟨*proof*⟩

lemma *mult-float-mono2*:
notes *mono-rules* = *plus-up-mono add-mono nprt-mono nprt-le-zero zero-le-pprt pprt-mono*
shows $a \leq b \Longrightarrow$
$ab \leq bb \Longrightarrow$
$aa \leq a \Longrightarrow$
$b \leq ba \Longrightarrow$
$ac \leq ab \Longrightarrow$
$bb \leq bc \Longrightarrow$
plus-up prec (*pprt b* $*$ *pprt bb*)
(*plus-up prec* (*pprt a* $*$ *nprt bb*)
(*plus-up prec* (*nprt b* $*$ *pprt ab*)
(*nprt a* $*$ *nprt ab*)))
$\leq$ *plus-up prec* (*pprt ba* $*$ *pprt bc*)
(*plus-up prec* (*pprt aa* $*$ *nprt bc*)
(*plus-up prec* (*nprt ba* $*$ *pprt ac*)
(*nprt aa* $*$ *nprt ac*)))
⟨*proof*⟩

lemma *mult-float-interval-mono*: *set-of* (*mult-float-interval prec A B*) $\subseteq$ *set-of* (*mult-float-interval prec X Y*)
if *set-of A* $\subseteq$ *set-of X set-of B* $\subseteq$ *set-of Y*
⟨*proof*⟩

lemma *Ivl-simps*[*simp*]: *lower* (*Ivl a b*) = *min a b upper* (*Ivl a b*) = *b*
⟨*proof*⟩

lemmas [*simp del*] = *power-down.simps*(*2*) *power-up.simps*(*2*)
lemmas *power-down-simp* = *power-down.simps*(*2*)
lemmas *power-up-simp* = *power-up.simps*(*2*)

lemma *power-down-even-nonneg*: *even n* $\Longrightarrow$ *0* $\leq$ *power-down p x n*
⟨*proof*⟩

lemma *truncate-down-less-zero-iff*[*simp*]: *truncate-down p x* $<$ *0* $\longleftrightarrow$ *x* $<$ *0*
⟨*proof*⟩

lemma *truncate-down-nonneg-iff*[*simp*]: *truncate-down p x* $\geq$ *0* $\longleftrightarrow$ *x* $\geq$ *0*
⟨*proof*⟩

lemma *truncate-down-eq-zero-iff*[*simp*]: *truncate-down prec x* = *0* $\longleftrightarrow$ *x* = *0*
⟨*proof*⟩

lemma *power-down-eq-zero-iff*[*simp*]: *power-down prec b n* = *0* $\longleftrightarrow$ *b* = *0* $\wedge$ *n* $\neq$ *0*
⟨*proof*⟩

lemma *power-down-nonneg-iff*[*simp*]:

power-down prec b n $\geq$ *0* $\longleftrightarrow$ *even n* $\vee$ *b* $\geq$ *0*
⟨*proof*⟩

lemma *power-down-neg-iff* [*simp*]:
power-down prec b n < *0* $\longleftrightarrow$
b < *0* $\wedge$ *odd n*
⟨*proof*⟩

lemma *power-down-nonpos-iff* [*simp*]:
notes [*simp del*] = *power-down-neg-iff power-down-eq-zero-iff*
shows *power-down prec b n* $\leq$ *0* $\longleftrightarrow$ *b* < *0* $\wedge$ *odd n* $\vee$ *b* = *0* $\wedge$ *n* $\neq$ *0*
⟨*proof*⟩

lemma *power-down-mono*:
power-down prec a n $\leq$ *power-down prec b n*
if ((*0* $\leq$ *a* $\wedge$ *a* $\leq$ *b*)$\vee$(*odd n* $\wedge$ *a* $\leq$ *b*) $\vee$ (*even n* $\wedge$ *a* $\leq$ *0* $\wedge$ *b* $\leq$ *a*))
⟨*proof*⟩

lemma *truncate-up-nonneg*: *0* $\leq$ *truncate-up p x* **if** *0* $\leq$ *x*
⟨*proof*⟩

lemma *truncate-up-pos*: *0* < *truncate-up p x* **if** *0* < *x*
⟨*proof*⟩

lemma *truncate-up-less-zero-iff* [*simp*]: *truncate-up p x* < *0* $\longleftrightarrow$ *x* < *0*
⟨*proof*⟩

lemma *truncate-up-nonneg-iff* [*simp*]: *truncate-up p x* $\geq$ *0* $\longleftrightarrow$ *x* $\geq$ *0*
⟨*proof*⟩

lemma *power-up-even-nonneg*: *even n* $\Longrightarrow$ *0* $\leq$ *power-up p x n*
⟨*proof*⟩

lemma *truncate-up-eq-zero-iff* [*simp*]: *truncate-up prec x* = *0* $\longleftrightarrow$ *x* = *0*
⟨*proof*⟩

lemma *power-up-eq-zero-iff* [*simp*]: *power-up prec b n* = *0* $\longleftrightarrow$ *b* = *0* $\wedge$ *n* $\neq$ *0*
⟨*proof*⟩

lemma *power-up-nonneg-iff* [*simp*]:
power-up prec b n $\geq$ *0* $\longleftrightarrow$ *even n* $\vee$ *b* $\geq$ *0*
⟨*proof*⟩

lemma *power-up-neg-iff* [*simp*]:
power-up prec b n < *0* $\longleftrightarrow$ *b* < *0* $\wedge$ *odd n*
⟨*proof*⟩

lemma *power-up-nonpos-iff* [*simp*]:
notes [*simp del*] = *power-up-neg-iff power-up-eq-zero-iff*

shows *power-up prec b n* $\leq 0 \longleftrightarrow b < 0 \wedge odd\ n \vee b = 0 \wedge n \neq 0$
⟨*proof*⟩

lemma *power-up-mono*:
power-up prec a n $\leq$ *power-up prec b n*
if $((0 \leq a \wedge a \leq b) \vee (odd\ n \wedge a \leq b) \vee (even\ n \wedge a \leq 0 \wedge b \leq a))$
⟨*proof*⟩

lemma *set-of-subset-iff*: *set-of X* $\subseteq$ *set-of Y* $\longleftrightarrow$ *lower Y* $\leq$ *lower X* $\wedge$ *upper X* $\leq$ *upper Y*
for *X Y*::*'a*::*linorder interval*
⟨*proof*⟩

lemma *power-float-interval-mono*:
set-of (*power-float-interval prec n A*)
$\subseteq$ *set-of* (*power-float-interval prec n B*)
if *set-of A* $\subseteq$ *set-of B*
⟨*proof*⟩

lemma *bounds-of-interval-eq-lower-upper*:
bounds-of-interval ivl = (*lower ivl*, *upper ivl*) **if** *lower ivl* $\leq$ *upper ivl*
⟨*proof*⟩

lemma *real-interval-Ivl*: *real-interval* (*Ivl a b*) = *Ivl a b*
⟨*proof*⟩

lemma *set-of-mul-contains-real-zero*:
$0 \in_r (A * B)$ **if** $0 \in_r A \vee 0 \in_r B$
⟨*proof*⟩

fun *subdivide-interval* :: *nat* ⇒ *float interval* ⇒ *float interval list*
where *subdivide-interval 0 I* = [*I*]
| *subdivide-interval* (*Suc n*) *I* = (
let m = *mid I*
in (*subdivide-interval n* (*Ivl* (*lower I*) *m*)) @ (*subdivide-interval n* (*Ivl m* (*upper I*)))
)

lemma *subdivide-interval-length*:
shows *length* (*subdivide-interval n I*) = *2^n*
⟨*proof*⟩

lemma *lower-le-mid*: *lower x* $\leq$ *mid x real-of-float* (*lower x*) $\leq$ *mid x*
and *mid-le-upper*: *mid x* $\leq$ *upper x real-of-float* (*mid x*) $\leq$ *upper x*
⟨*proof*⟩

lemma *subdivide-interval-correct*:
list-ex ($\lambda i.\ x \in_r i$) (*subdivide-interval n I*) **if** $x \in_r I$ **for** *x*::*real*
⟨*proof*⟩

fun *interval-list-union* :: *'a::lattice interval list* ⇒ *'a interval*
where *interval-list-union* [] = *undefined*
| *interval-list-union* [*I*] = *I*
| *interval-list-union* (*I*#*Is*) = *sup I* (*interval-list-union Is*)

lemma *interval-list-union-correct*:
assumes *S* ≠ []
assumes *i* < *length S*
shows *set-of* (*S*!*i*) ⊆ *set-of* (*interval-list-union S*)
⟨*proof*⟩

lemma *split-domain-correct*:
fixes *x* :: *real list*
assumes *x all-in I*
assumes *split-correct*: ⋀*x a I*. *x* ∈$_r$ *I* ⟹ *list-ex* (λ*i*::*float interval*. *x* ∈$_r$ *i*) (*split I*)
shows *list-ex* (λ*s*. *x all-in s*) (*split-domain split I*)
⟨*proof*⟩

end

4 Horner Evaluation

theory *Horner-Eval*
imports *Interval*
begin

Function and lemmas for evaluating polynomials via the horner scheme. Because interval multiplication is not distributive, interval polynomials expressed as a sum of monomials are not equivalent to their respective horner form. The functions and lemmas in this theory can be used to express interval polynomials in horner form and prove facts about them.

fun *horner-eval'* **where**
horner-eval' f x v 0 = *v*
| *horner-eval' f x v* (*Suc i*) = *horner-eval' f x* (*f i* + *x* ∗ *v*) *i*

definition *horner-eval*
where *horner-eval f x n* = *horner-eval' f x 0 n*

lemma *horner-eval-cong*:
assumes ⋀*i*. *i* < *n* ⟹ *f i* = *g i*
assumes *x* = *y*
assumes *n* = *m*
shows *horner-eval f x n* = *horner-eval g y m*
⟨*proof*⟩

lemma *horner-eval-eq-setsum*:

fixes $x::'a::linordered\text{-}idom$
shows $horner\text{-}eval\ f\ x\ n = (\sum i{<}n.\ f\ i * x\hat{}i)$
⟨*proof*⟩

lemma *horner-eval-Suc*[*simp*]:
fixes $x::'a::linordered\text{-}idom$
shows $horner\text{-}eval\ f\ x\ (Suc\ n) = horner\text{-}eval\ f\ x\ n + (f\ n) * x\hat{}n$
⟨*proof*⟩

lemma *horner-eval-Suc'*[*simp*]:
fixes $x::'a::\{comm\text{-}monoid\text{-}add,\ times\}$
shows $horner\text{-}eval\ f\ x\ (Suc\ n) = f\ 0 + x * (horner\text{-}eval\ (\lambda i.\ f\ (Suc\ i))\ x\ n)$
⟨*proof*⟩

lemma *horner-eval-0*[*simp*]:
shows $horner\text{-}eval\ f\ x\ 0 = 0$
⟨*proof*⟩

lemma *horner-eval'-interval*:
fixes $x::'a::linordered\text{-}ring$
assumes $\bigwedge i.\ i < n \Longrightarrow f\ i \in set\text{-}of\ (g\ i)$
assumes $x \in_i I\ v \in_i V$
shows $horner\text{-}eval'\ f\ x\ v\ n \in_i horner\text{-}eval'\ g\ I\ V\ n$
⟨*proof*⟩

lemma *horner-eval-interval*:
fixes $x::'a::linordered\text{-}idom$
assumes $\bigwedge i.\ i < n \Longrightarrow f\ i \in set\text{-}of\ (g\ i)$
assumes $x \in set\text{-}of\ I$
shows $horner\text{-}eval\ f\ x\ n \in_i horner\text{-}eval\ g\ I\ n$
⟨*proof*⟩

end
theory *Polynomial-Expression-Additional*
imports *Interval-Approximation*
Polynomial-Expression
HOL−Decision-Procs.Approximation
begin

lemma *real-of-float-eq-zero-iff*[*simp*]: $real\text{-}of\text{-}float\ x = 0 \longleftrightarrow x = 0$
⟨*proof*⟩

Theory *Taylor-Models.Polynomial-Expression* contains a, more or less, 1:1 generalization of theory *Multivariate-Polynomial*. Any additions belong here.

declare [[*coercion-map map-poly*]]
declare [[*coercion interval-of*::*float*⇒*float interval*]]

Apply float interval arguments to a float poly.

value *Ipoly* [*Ivl* (*Float 4* (−*6*)) (*Float 10 6*)] (*poly.Add* (*poly.C* (*Float 3 5*)) (*poly.Bound 0*))

map-poly for homomorphisms

lemma *map-poly-homo-polyadd-eq-zero-iff*:
map-poly f (*p* +$_p$ *q*) = 0$_p$ ⟷ *p* +$_p$ *q* = 0$_p$
if [*symmetric*, *simp*]: ⋀*x y*. *f* (*x* + *y*) = *f x* + *f y* ⋀*x*. *f x* = *0* ⟷ *x* = *0*
⟨*proof*⟩

lemma *zero-iffD*: (⋀*x*. *f x* = *0* ⟷ *x* = *0*) ⟹ *f 0* = *0*
⟨*proof*⟩

lemma *map-poly-homo-polyadd*:
map-poly f (*p1* +$_p$ *p2*) = *map-poly f p1* +$_p$ *map-poly f p2*
if [*simp*]: ⋀*x y*. *f* (*x* + *y*) = *f x* + *f y* ⋀*x*. *f x* = *0* ⟷ *x* = *0*
⟨*proof*⟩

lemma *map-poly-homo-polyneg*:
map-poly f (~$_p$ *p1*) = ~$_p$ (*map-poly f p1*)
if [*simp*]: ⋀*x y*. *f* (− *x*) = − *f x*
⟨*proof*⟩

lemma *map-poly-homo-polysub*:
map-poly f (*p1* −$_p$ *p2*) = *map-poly f p1* −$_p$ *map-poly f p2*
if [*simp*]: ⋀*x y*. *f* (*x* + *y*) = *f x* + *f y* ⋀*x*. *f x* = *0* ⟷ *x* = *0* ⋀*x y*. *f* (− *x*) = − *f x*
⟨*proof*⟩

lemma *map-poly-homo-polymul*:
map-poly f (*p1* ∗$_p$ *p2*) = *map-poly f p1* ∗$_p$ *map-poly f p2*
if [*simp*]: ⋀*x y*. *f* (*x* + *y*) = *f x* + *f y* ⋀*x*. *f x* = *0* ⟷ *x* = *0* ⋀*x y*. *f* (*x* ∗ *y*) = *f x* ∗ *f y*
⟨*proof*⟩

lemma *map-poly-homo-polypow*:
map-poly f (*p1* ^$_p$ *n*) = *map-poly f p1* ^$_p$ *n*
if [*simp*]: ⋀*x y*. *f* (*x* + *y*) = *f x* + *f y* ⋀*x*. *f x* = *0* ⟷ *x* = *0* ⋀*x y*. *f* (*x* ∗ *y*) = *f x* ∗ *f y*
f 1 = *1*
⟨*proof*⟩

lemmas *map-poly-homo-polyarith* = *map-poly-homo-polyadd map-poly-homo-polyneg map-poly-homo-polysub map-poly-homo-polymul map-poly-homo-polypow*

Count the number of parameters of a polynomial.

fun *num-params* :: *'a poly* ⇒ *nat*
where *num-params* (*poly.C c*) = *0*
| *num-params* (*poly.Bound n*) = *Suc n*
| *num-params* (*poly.Add a b*) = *max* (*num-params a*) (*num-params b*)

| *num-params* (*poly.Sub a b*) = *max* (*num-params a*) (*num-params b*)
| *num-params* (*poly.Mul a b*) = *max* (*num-params a*) (*num-params b*)
| *num-params* (*poly.Neg a*) = *num-params a*
| *num-params* (*poly.Pw a n*) = *num-params a*
| *num-params* (*poly.CN a n b*) = *max* (*max* (*num-params a*) (*num-params b*)) (*Suc n*)

lemma *num-params-map-poly*[*simp*]:
shows *num-params* (*map-poly f p*) = *num-params p*
⟨*proof*⟩

lemma *num-params-polyadd*:
shows *num-params* (*p1* $+_p$ *p2*) ≤ *max* (*num-params p1*) (*num-params p2*)
⟨*proof*⟩

lemma *num-params-polyneg*:
shows *num-params* ($\sim_p$ *p*) = *num-params p*
⟨*proof*⟩

lemma *num-params-polymul*:
shows *num-params* (*p1* $*_p$ *p2*) ≤ *max* (*num-params p1*) (*num-params p2*)
⟨*proof*⟩

lemma *num-params-polypow*:
shows *num-params* (*p* $\hat{}_p$ *n*) ≤ *num-params p*
⟨*proof*⟩

lemma *num-params-polynate*:
shows *num-params* (*polynate p*) ≤ *num-params p*
⟨*proof*⟩

lemma *polynate-map-poly-real*[*simp*]:
fixes *p* :: *float poly*
shows *map-poly real-of-float* (*polynate p*) = *polynate* (*map-poly real-of-float p*)
⟨*proof*⟩

Evaluating a float poly is equivalent to evaluating the corresponding real poly with the float parameters converted to reals.

lemma *Ipoly-real-float-eqiv*:
fixes *p*::*float poly* **and** *xs*::*float list*
assumes *num-params p* ≤ *length xs*
shows *Ipoly xs* (*p*::*real poly*) = *Ipoly xs p*
⟨*proof*⟩

Evaluating an *'a poly* with *'a interval* arguments is monotone.

lemma *Ipoly-interval-args-mono*:
fixes *p*::*'a*::*linordered-idom poly*
and *x*::*'a list*
and *xs*::*'a interval list*

assumes *x all-in$_i$ xs*
assumes *num-params p* $\leq$ *length xs*
shows *Ipoly x p* $\in$ *set-of* (*Ipoly xs* (*map-poly interval-of p*))
⟨*proof*⟩

lemma *Ipoly-interval-args-inc-mono*:
fixes *p*::*'a*::{*real-normed-algebra*, *linear-continuum-topology*, *linordered-idom*} *poly*
and *I*::*'a interval list* **and** *J*::*'a interval list*
assumes *num-params p* $\leq$ *length I*
assumes *I all-subset J*
shows *set-of* (*Ipoly I* (*map-poly interval-of p*)) $\subseteq$ *set-of* (*Ipoly J* (*map-poly interval-of p*))
⟨*proof*⟩

5 Splitting polynomials to reduce floating point precision

TODO: Move this! Definitions regarding floating point numbers should not be in a theory about polynomials.

fun *float-prec* :: *float* ⇒ *int*
where *float-prec f* = (*let p*=*exponent f in if p* ≥ *0 then 0 else* −*p*)

fun *float-round* :: *nat* ⇒ *float* ⇒ *float*
where *float-round prec f* = (
let d = *float-down prec f*; *u* = *float-up prec f*
in if f − *d* < *u* − *f then d else u*)

Splits any polynomial p into two polynomials l, r, such that $\forall\, x{::}real.\ p(x) = l(x) + r(x)$ and all floating point coefficients in p are rounded to precision *prec*. Not all cases need to give good results. Polynomials normalized with polynate only contain *poly.C* and *poly.CN* constructors.

fun *split-by-prec* :: *nat* ⇒ *float poly* ⇒ *float poly* ∗ *float poly*
where *split-by-prec prec* (*poly.C f*) = (*let r* = *float-round prec f in* (*poly.C r*, *poly.C* (*f* − *r*)))
| *split-by-prec prec* (*poly.Bound n*) = (*poly.Bound n*, *poly.C 0*)
| *split-by-prec prec* (*poly.Add l r*) = (*let* (*ll*, *lr*) = *split-by-prec prec l*;
(*rl*, *rr*) = *split-by-prec prec r*
in (*poly.Add ll rl*, *poly.Add lr rr*))
| *split-by-prec prec* (*poly.Sub l r*) = (*let* (*ll*, *lr*) = *split-by-prec prec l*;
(*rl*, *rr*) = *split-by-prec prec r*
in (*poly.Sub ll rl*, *poly.Sub lr rr*))
| *split-by-prec prec* (*poly.Mul l r*) = (*let* (*ll*, *lr*) = *split-by-prec prec l*;
(*rl*, *rr*) = *split-by-prec prec r*
in (*poly.Mul ll rl*, *poly.Add* (*poly.Add* (*poly.Mul lr rl*) (*poly.Mul ll rr*)) (*poly.Mul lr rr*)))
| *split-by-prec prec* (*poly.Neg p*) = (*let* (*l*, *r*) = *split-by-prec prec p in* (*poly.Neg l*, *poly.Neg r*))

| *split-by-prec prec* (*poly.Pw p 0*) = (*poly.C 1*, *poly.C 0*)
| *split-by-prec prec* (*poly.Pw p* (*Suc n*)) = (*let* (*l*, *r*) = *split-by-prec prec p in* (*poly.Pw l n*, *poly.Sub* (*poly.Pw p* (*Suc n*)) (*poly.Pw l n*)))
| *split-by-prec prec* (*poly.CN c n p*) = (*let* (*cl*, *cr*) = *split-by-prec prec c*;
(*pl*, *pr*) = *split-by-prec prec p*
in (*poly.CN cl n pl*, *poly.CN cr n pr*))

TODO: Prove precision constraint on *l*.

lemma *split-by-prec-correct*:
fixes *args* :: *real list*
assumes (*l*, *r*) = *split-by-prec prec p*
shows *Ipoly args p* = *Ipoly args l* + *Ipoly args r* (**is** *?P1*)
and *num-params l* ≤ *num-params p* (**is** *?P2*)
and *num-params r* ≤ *num-params p* (**is** *?P3*)
⟨*proof*⟩

6 Splitting polynomials by degree

fun *maxdegree* :: ('*a*::*zero*) *poly* ⇒ *nat*
where *maxdegree* (*poly.C c*) = *0*
| *maxdegree* (*poly.Bound n*) = *1*
| *maxdegree* (*poly.Add l r*) = *max* (*maxdegree l*) (*maxdegree r*)
| *maxdegree* (*poly.Sub l r*) = *max* (*maxdegree l*) (*maxdegree r*)
| *maxdegree* (*poly.Mul l r*) = *maxdegree l* + *maxdegree r*
| *maxdegree* (*poly.Neg p*) = *maxdegree p*
| *maxdegree* (*poly.Pw p n*) = *n* ∗ *maxdegree p*
| *maxdegree* (*poly.CN c n p*) = *max* (*maxdegree c*) (*1* + *maxdegree p*)

fun *split-by-degree* :: *nat* ⇒ '*a*::*zero poly* ⇒ '*a poly* ∗ '*a poly*
where *split-by-degree n* (*poly.C c*) = (*poly.C c*, *poly.C 0*)
| *split-by-degree 0 p* = (*poly.C 0*, *p*)
| *split-by-degree* (*Suc n*) (*poly.CN c v p*) = (
let (*cl*, *cr*) = *split-by-degree* (*Suc n*) *c*;
(*pl*, *pr*) = *split-by-degree n p*
in (*poly.CN cl v pl*, *poly.CN cr v pr*))
— This function is only intended for use on polynomials in normal form. Hence most cases never get executed.
| *split-by-degree n p* = (*poly.C 0*, *p*)

lemma *split-by-degree-correct*:
fixes *x* :: *real list* **and** *p* :: *float poly*
assumes (*l*, *r*) = *split-by-degree ord p*
shows *maxdegree l* ≤ *ord* (**is** *?P1*)
and *Ipoly x p* = *Ipoly x l* + *Ipoly x r* (**is** *?P2*)
and *num-params l* ≤ *num-params p* (**is** *?P3*)
and *num-params r* ≤ *num-params p* (**is** *?P4*)
⟨*proof*⟩

Operations on lists.

lemma *length-map2*[*simp*]: *length* (*map2 f a b*) = *min* (*length a*) (*length b*)
⟨*proof*⟩

lemma *map2-nth*[*simp*]:
assumes *n* < *length a*
assumes *n* < *length b*
shows (*map2 f a b*)!*n* = *f* (*a*!*n*) (*b*!*n*)
⟨*proof*⟩

Translating a polynomial by a vector.

fun *poly-translate* :: *'a list* ⇒ *'a poly* ⇒ *'a poly*
where *poly-translate vs* (*poly.C c*) = *poly.C c*
| *poly-translate vs* (*poly.Bound n*) = *poly.Add* (*poly.Bound n*) (*poly.C* (*vs* ! *n*))
| *poly-translate vs* (*poly.Add l r*) = *poly.Add* (*poly-translate vs l*) (*poly-translate vs r*)
| *poly-translate vs* (*poly.Sub l r*) = *poly.Sub* (*poly-translate vs l*) (*poly-translate vs r*)
| *poly-translate vs* (*poly.Mul l r*) = *poly.Mul* (*poly-translate vs l*) (*poly-translate vs r*)
| *poly-translate vs* (*poly.Neg p*) = *poly.Neg* (*poly-translate vs p*)
| *poly-translate vs* (*poly.Pw p n*) = *poly.Pw* (*poly-translate vs p*) *n*
| *poly-translate vs* (*poly.CN c n p*) = *poly.Add* (*poly-translate vs c*) (*poly.Mul* (*poly.Add* (*poly.Bound n*) (*poly.C* (*vs* ! *n*))) (*poly-translate vs p*))

Translating a polynomial is equivalent to translating its argument.

lemma *poly-translate-correct*:
assumes *num-params p* ≤ *length x*
assumes *length x* = *length v*
shows *Ipoly x* (*poly-translate v p*) = *Ipoly* (*map2* (+) *x v*) *p*
⟨*proof*⟩

lemma *real-poly-translate*:
assumes *num-params p* ≤ *length v*
shows *Ipoly x* (*map-poly real-of-float* (*poly-translate v p*)) = *Ipoly x* (*poly-translate v* (*map-poly real-of-float p*))
⟨*proof*⟩

lemma *num-params-poly-translate*[*simp*]:
shows *num-params* (*poly-translate v p*) = *num-params p*
⟨*proof*⟩

end
theory *Taylor-Models-Misc*
imports
HOL−Library.Float
HOL−Library.Function-Algebras
HOL−Decision-Procs.Approximation
Affine-Arithmetic.Floatarith-Expression
begin

This theory contains anything that doesn't belong anywhere else.

lemma *of-nat-real-float-equiv*: $(\mathit{of\text{-}nat}\ n :: \mathit{real}) = (\mathit{of\text{-}nat}\ n :: \mathit{float})$
⟨*proof*⟩

lemma *fact-real-float-equiv*: $(\mathit{fact}\ n :: \mathit{float}) = (\mathit{fact}\ n :: \mathit{real})$
⟨*proof*⟩

lemma *Some-those-length*:
$\mathit{those}\ ys = \mathit{Some}\ xs \Longrightarrow \mathit{length}\ xs = \mathit{length}\ ys$
⟨*proof*⟩

lemma *those-eq-None-iff*: $\mathit{those}\ ys = \mathit{None} \longleftrightarrow \mathit{None} \in \mathit{set}\ ys$
⟨*proof*⟩

lemma *those-eq-Some-iff*: $\mathit{those}\ ys = (\mathit{Some}\ xs) \longleftrightarrow (ys = \mathit{map}\ \mathit{Some}\ xs)$
⟨*proof*⟩

lemma *Some-those-nth*:
assumes $\mathit{those}\ ys = \mathit{Some}\ xs$
assumes $i < \mathit{length}\ xs$
shows $\mathit{Some}\ (xs!i) = ys!i$
⟨*proof*⟩

lemma *fun-pow*: $f\hat{}n = (\lambda x.\ (f\ x)\ \hat{}n)$
⟨*proof*⟩

context includes *floatarith-notation* **begin**

Translate floatarith expressions by a vector of floats.

fun *fa-translate* :: *float list* ⇒ *floatarith* ⇒ *floatarith*
where $\mathit{fa\text{-}translate}\ v\ (\mathit{Add}\ a\ b) = \mathit{Add}\ (\mathit{fa\text{-}translate}\ v\ a)\ (\mathit{fa\text{-}translate}\ v\ b)$
| $\mathit{fa\text{-}translate}\ v\ (\mathit{Minus}\ a) = \mathit{Minus}\ (\mathit{fa\text{-}translate}\ v\ a)$
| $\mathit{fa\text{-}translate}\ v\ (\mathit{Mult}\ a\ b) = \mathit{Mult}\ (\mathit{fa\text{-}translate}\ v\ a)\ (\mathit{fa\text{-}translate}\ v\ b)$
| $\mathit{fa\text{-}translate}\ v\ (\mathit{Inverse}\ a) = \mathit{Inverse}\ (\mathit{fa\text{-}translate}\ v\ a)$
| $\mathit{fa\text{-}translate}\ v\ (\mathit{Cos}\ a) = \mathit{Cos}\ (\mathit{fa\text{-}translate}\ v\ a)$
| $\mathit{fa\text{-}translate}\ v\ (\mathit{Arctan}\ a) = \mathit{Arctan}\ (\mathit{fa\text{-}translate}\ v\ a)$
| $\mathit{fa\text{-}translate}\ v\ (\mathit{Min}\ a\ b) = \mathit{Min}\ (\mathit{fa\text{-}translate}\ v\ a)\ (\mathit{fa\text{-}translate}\ v\ b)$
| $\mathit{fa\text{-}translate}\ v\ (\mathit{Max}\ a\ b) = \mathit{Max}\ (\mathit{fa\text{-}translate}\ v\ a)\ (\mathit{fa\text{-}translate}\ v\ b)$
| $\mathit{fa\text{-}translate}\ v\ (\mathit{Abs}\ a) = \mathit{Abs}\ (\mathit{fa\text{-}translate}\ v\ a)$
| $\mathit{fa\text{-}translate}\ v\ (\mathit{Sqrt}\ a) = \mathit{Sqrt}\ (\mathit{fa\text{-}translate}\ v\ a)$
| $\mathit{fa\text{-}translate}\ v\ (\mathit{Exp}\ a) = \mathit{Exp}\ (\mathit{fa\text{-}translate}\ v\ a)$
| $\mathit{fa\text{-}translate}\ v\ (\mathit{Ln}\ a) = \mathit{Ln}\ (\mathit{fa\text{-}translate}\ v\ a)$
| $\mathit{fa\text{-}translate}\ v\ (\mathit{Var}\ n) = \mathit{Add}\ (\mathit{Var}\ n)\ (\mathit{Num}\ (v!n))$
| $\mathit{fa\text{-}translate}\ v\ (\mathit{Power}\ a\ n) = \mathit{Power}\ (\mathit{fa\text{-}translate}\ v\ a)\ n$
| $\mathit{fa\text{-}translate}\ v\ (\mathit{Powr}\ a\ b) = \mathit{Powr}\ (\mathit{fa\text{-}translate}\ v\ a)\ (\mathit{fa\text{-}translate}\ v\ b)$
| $\mathit{fa\text{-}translate}\ v\ (\mathit{Floor}\ x) = \mathit{Floor}\ (\mathit{fa\text{-}translate}\ v\ x)$
| $\mathit{fa\text{-}translate}\ v\ (\mathit{Num}\ c) = \mathit{Num}\ c$
| $\mathit{fa\text{-}translate}\ v\ \mathit{Pi} = \mathit{Pi}$

lemma *fa-translate-correct*:
assumes *max-Var-floatarith f* ≤ *length I*
assumes *length v* = *length I*
shows *interpret-floatarith* (*fa-translate v f*) *I* = *interpret-floatarith f* (*map2* (+) *I v*)
⟨*proof*⟩

primrec *vars-floatarith* **where**
vars-floatarith (*Add a b*) = (*vars-floatarith a*) ∪ (*vars-floatarith b*)
| *vars-floatarith* (*Mult a b*) = (*vars-floatarith a*) ∪ (*vars-floatarith b*)
| *vars-floatarith* (*Inverse a*) = *vars-floatarith a*
| *vars-floatarith* (*Minus a*) = *vars-floatarith a*
| *vars-floatarith* (*Num a*) = {}
| *vars-floatarith* (*Var i*) = {*i*}
| *vars-floatarith* (*Cos a*) = *vars-floatarith a*
| *vars-floatarith* (*Arctan a*) = *vars-floatarith a*
| *vars-floatarith* (*Abs a*) = *vars-floatarith a*
| *vars-floatarith* (*Max a b*) = (*vars-floatarith a*) ∪ (*vars-floatarith b*)
| *vars-floatarith* (*Min a b*) = (*vars-floatarith a*) ∪ (*vars-floatarith b*)
| *vars-floatarith* (*Pi*) = {}
| *vars-floatarith* (*Sqrt a*) = *vars-floatarith a*
| *vars-floatarith* (*Exp a*) = *vars-floatarith a*
| *vars-floatarith* (*Powr a b*) = (*vars-floatarith a*) ∪ (*vars-floatarith b*)
| *vars-floatarith* (*Ln a*) = *vars-floatarith a*
| *vars-floatarith* (*Power a n*) = *vars-floatarith a*
| *vars-floatarith* (*Floor a*) = *vars-floatarith a*

lemma *finite-vars-floatarith*[*simp*]: *finite* (*vars-floatarith x*)
⟨*proof*⟩

end

lemma *max-Var-floatarith-eq-Max-vars-floatarith*:
max-Var-floatarith fa = (*if vars-floatarith fa* = {} *then 0 else Suc* (*Max* (*vars-floatarith fa*)))
⟨*proof*⟩

end
theory *Taylor-Models*
imports *Interval-Approximation*
Horner-Eval
Polynomial-Expression-Additional
Taylor-Models-Misc
HOL−Decision-Procs.Approximation
HOL−Library.Function-Algebras
HOL−Library.Set-Algebras
Affine-Arithmetic.Straight-Line-Program
Affine-Arithmetic.Affine-Approximation
begin

TODO: get rid of float poly/float inteval and use real poly/real interval and data refinement?

7 Multivariate Taylor Models

7.1 Computing interval bounds on arithmetic expressions

This is a wrapper around the "approx" function. It computes range bounds on floatarith expressions.

fun *compute-bound-fa* :: *nat* ⇒ *floatarith* ⇒ *float interval list* ⇒ *float interval option*
  where *compute-bound-fa prec f I* =
  (*case approx prec f* (*map* (*Some o* (λ*x*. (*lower x*, *upper x*))) *I*) *of*
    Some (*a*, *b*) ⇒ (*if a* ≤ *b then Some* (*Ivl a b*) *else None*)
  | - ⇒ *None*)

lemma *compute-bound-fa-correct*:
  interpret-floatarith f i ∈$_r$ *ivl*
  if *compute-bound-fa prec f I* = *Some ivl*
    i all-in I
  for *i*::*real list*
⟨*proof*⟩

7.2 Definition of Taylor models and notion of rangeity

Taylor models are a pair of a polynomial and an absolute error bound.

datatype *taylor-model* = *TaylorModel* (*tm-poly*: *float poly*) (*tm-bound*: *float interval*)

Taylor model for a real valuation of variables

primrec *insertion* :: (*nat* ⇒ *'a*) ⇒ *'a poly* ⇒ *'a*::{*plus*,*zero*,*minus*,*uminus*,*times*,*one*,*power*}
where
  insertion bs (*C c*) = *c*
| *insertion bs* (*poly.Bound n*) = *bs n*
| *insertion bs* (*Neg a*) = − *insertion bs a*
| *insertion bs* (*poly.Add a b*) = *insertion bs a* + *insertion bs b*
| *insertion bs* (*Sub a b*) = *insertion bs a* − *insertion bs b*
| *insertion bs* (*Mul a b*) = *insertion bs a* ∗ *insertion bs b*
| *insertion bs* (*Pw t n*) = *insertion bs t* ^ *n*
| *insertion bs* (*CN c n p*) = *insertion bs c* + (*bs n*) ∗ *insertion bs p*

definition *range-tm* :: (*nat* ⇒ *real*) ⇒ *taylor-model* ⇒ *real interval* **where**
range-tm e tm = *interval-of* (*insertion e* (*tm-poly tm*)) + *real-interval* (*tm-bound tm*)

lemma *Ipoly-num-params-cong*: *Ipoly xs p* = *Ipoly ys p*
  if ⋀*i*. *i* < *num-params p* ⟹ *xs* ! *i* = *ys* ! *i*

⟨*proof*⟩

lemma *insertion-num-params-cong*: *insertion e p* = *insertion f p*
if ⋀*i*. *i* < *num-params p* ⟹ *e i* = *f i*
⟨*proof*⟩

lemma *insertion-eq-IpolyI*: *insertion xs p* = *Ipoly ys p*
if ⋀*i*. *i* < *num-params p* ⟹ *xs i* = *ys* ! *i*
⟨*proof*⟩

lemma *Ipoly-eq-insertionI*: *Ipoly ys p* = *insertion xs p*
if ⋀*i*. *i* < *num-params p* ⟹ *xs i* = *ys* ! *i*
⟨*proof*⟩

lemma *range-tmI*:
x ∈$_i$ *range-tm e tm*
if *x*: *x* ∈$_i$ *interval-of* (*insertion e* ((*tm-poly tm*))) + *real-interval* (*tm-bound tm*)
for *e*::*nat*⇒*real*
⟨*proof*⟩

lemma *range-tmD*:
x ∈$_i$ *interval-of* (*insertion e* (*tm-poly tm*)) + *real-interval* (*tm-bound tm*)
if *x* ∈$_i$ *range-tm e tm*
for *e*::*nat*⇒*real*
⟨*proof*⟩

7.3 Interval bounds for Taylor models

Bound a polynomial by simply approximating it with interval arguments.

fun *compute-bound-poly* :: *nat* ⇒ *float interval poly* ⇒ (*float interval list*) ⇒ (*float interval list*) ⇒ *float interval* **where**
compute-bound-poly prec (*poly.C f*) *I a* = *f*
| *compute-bound-poly prec* (*poly.Bound n*) *I a* = *round-interval prec* (*I* ! *n* − (*a* ! *n*))
| *compute-bound-poly prec* (*poly.Add p q*) *I a* =
round-interval prec (*compute-bound-poly prec p I a* + *compute-bound-poly prec q I a*)
| *compute-bound-poly prec* (*poly.Sub p q*) *I a* =
round-interval prec (*compute-bound-poly prec p I a* − *compute-bound-poly prec q I a*)
| *compute-bound-poly prec* (*poly.Mul p q*) *I a* =
mult-float-interval prec (*compute-bound-poly prec p I a*) (*compute-bound-poly prec q I a*)
| *compute-bound-poly prec* (*poly.Neg p*) *I a* = −*compute-bound-poly prec p I a*
| *compute-bound-poly prec* (*poly.Pw p n*) *I a* = *power-float-interval prec n* (*compute-bound-poly prec p I a*)
| *compute-bound-poly prec* (*poly.CN p n q*) *I a* =
round-interval prec (*compute-bound-poly prec p I a* +
mult-float-interval prec (*round-interval prec* (*I* ! *n* − (*a* ! *n*))) (*compute-bound-poly*

prec q I a))

Bounds on Taylor models are simply a bound on its polynomial, widened by the approximation error.

fun *compute-bound-tm* :: *nat* ⇒ *float interval list* ⇒ *float interval list* ⇒ *taylor-model* ⇒ *float interval*
  where *compute-bound-tm prec I a* (*TaylorModel p e*) = *compute-bound-poly prec p I a* + *e*

lemma *compute-bound-tm-def*:
  compute-bound-tm prec I a tm = *compute-bound-poly prec* (*tm-poly tm*) *I a* + (*tm-bound tm*)
  ⟨*proof*⟩

lemma *real-of-float-in-real-interval-of*[*intro*, *simp*]: *real-of-float x* ∈$_r$ *X* **if** *x* ∈$_i$ *X*
  ⟨*proof*⟩

lemma *in-set-of-round-interval*[*intro*, *simp*]:
  x ∈$_r$ *round-interval prec X* **if** *x* ∈$_r$ *X*
  ⟨*proof*⟩

lemma *in-set-real-minus-interval*[*intro*, *simp*]:
  x − *y* ∈$_r$ *X* − *Y* **if** *x* ∈$_r$ *X y* ∈$_r$ *Y*
  ⟨*proof*⟩

lemma *real-interval-plus*: *real-interval* (*a* + *b*) = *real-interval a* + *real-interval b*
  ⟨*proof*⟩

lemma *real-interval-uminus*: *real-interval* (− *b*) = − *real-interval b*
  ⟨*proof*⟩

lemma *real-interval-of*: *real-interval* (*interval-of b*) = *interval-of b*
  ⟨*proof*⟩

lemma *real-interval-minus*: *real-interval* (*a* − *b*) = *real-interval a* − *real-interval b*
  ⟨*proof*⟩

lemma *in-set-real-plus-interval*[*intro*, *simp*]:
  x + *y* ∈$_r$ *X* + *Y* **if** *x* ∈$_r$ *X y* ∈$_r$ *Y*
  ⟨*proof*⟩

lemma *in-set-neg-plus-interval*[*intro*, *simp*]:
  − *y* ∈$_r$ − *Y* **if** *y* ∈$_r$ *Y*
  ⟨*proof*⟩

lemma *real-interval-times*: *real-interval* (*a* ∗ *b*) = *real-interval a* ∗ *real-interval b*
  ⟨*proof*⟩

lemma *in-set-real-times-interval*[*intro*, *simp*]:
  $x * y \in_r X * Y$ **if** $x \in_r X$ $y \in_r Y$
  ⟨*proof*⟩

lemma *real-interval-one*: *real-interval 1 = 1*
  ⟨*proof*⟩

lemma *real-interval-zero*: *real-interval 0 = 0*
  ⟨*proof*⟩

lemma *real-interval-power*: *real-interval* $(a \hat{} b) =$ *real-interval* $a \hat{} b$
  ⟨*proof*⟩

lemma *in-set-real-power-interval*[*intro*, *simp*]:
  $x \hat{} n \in_r X \hat{} n$ **if** $x \in_r X$
  ⟨*proof*⟩

lemma *power-float-interval-real-interval*[*intro*, *simp*]:
  $x \hat{} n \in_r$ *power-float-interval prec n* X **if** $x \in_r X$
  ⟨*proof*⟩

lemma *in-set-mult-float-interval*[*intro*, *simp*]:
  $x * y \in_r$ *mult-float-interval prec* X Y **if** $x \in_r X$ $y \in_r Y$
  ⟨*proof*⟩

lemma *in-set-real-minus-swapI*: $e\ i \in_r I\ !\ i - a\ !\ i$
  if $x - e\ i \in_r a\ !\ i$ $x \in_r I\ !\ i$
  ⟨*proof*⟩

definition *develops-at-within*::$(nat \Rightarrow real) \Rightarrow$ *float interval list* $\Rightarrow$ *float interval list* $\Rightarrow$ *bool*
  where *develops-at-within e a I* $\longleftrightarrow$ $(a$ *all-subset I*$) \wedge (\forall i <$ *length I*. $e\ i \in_r I\ !\ i - a\ !\ i)$

lemma *develops-at-withinI*:
  assumes *all-in*: *a all-subset I*
  assumes *e*: $\bigwedge i.\ i <$ *length I* $\Longrightarrow e\ i \in_r I\ !\ i - a\ !\ i$
  shows *develops-at-within e a I*
  ⟨*proof*⟩

lemma *develops-at-withinD*:
  assumes *develops-at-within e a I*
  shows *a all-subset I*
    $\bigwedge i.\ i <$ *length I* $\Longrightarrow e\ i \in_r I\ !\ i - a\ !\ i$
  ⟨*proof*⟩

lemma *compute-bound-poly-correct*:
  fixes *p*::*float poly*
  assumes *num-params p* $\leq$ *length I*

assumes *dev*: *develops-at-within e a I*
shows *insertion e* (*p*::*real poly*) $\in_r$ *compute-bound-poly prec* (*map-poly interval-of p*) *I a*
⟨*proof*⟩

lemma *compute-bound-tm-correct*:
fixes *I* :: *float interval list* **and** *f* :: *real list* ⇒ *real*
assumes *n*: *num-params* (*tm-poly t*) ≤ *length I*
assumes *dev*: *develops-at-within e a I*
assumes *x0*: *x0* $\in_i$ *range-tm e t*
shows *x0* $\in_r$ *compute-bound-tm prec I a t*
⟨*proof*⟩

lemma *compute-bound-tm-correct-subset*:
fixes *I* :: *float interval list* **and** *f* :: *real list* ⇒ *real*
assumes *n*: *num-params* (*tm-poly t*) ≤ *length I*
assumes *dev*: *develops-at-within e a I*
shows *set-of* (*range-tm e t*) ⊆ *set-of* (*real-interval* (*compute-bound-tm prec I a t*))
⟨*proof*⟩

lemma *compute-bound-poly-mono*:
assumes *num-params p* ≤ *length I*
assumes *mem*: *I all-subset J a all-subset I*
shows *set-of* (*compute-bound-poly prec p I a*) ⊆ *set-of* (*compute-bound-poly prec p J a*)
⟨*proof*⟩

lemma *compute-bound-tm-mono*:
fixes *I* :: *float interval list* **and** *f* :: *real list* ⇒ *real*
assumes *num-params* (*tm-poly t*) ≤ *length I*
assumes *I all-subset J*
assumes *a all-subset I*
shows *set-of* (*compute-bound-tm prec I a t*) ⊆ *set-of* (*compute-bound-tm prec J a t*)
⟨*proof*⟩

7.4 Computing taylor models for basic, univariate functions

definition *tm-const* :: *float* ⇒ *taylor-model*
where *tm-const c* = *TaylorModel* (*poly.C c*) *0*

context includes *floatarith-notation* **begin**

definition *tm-pi* :: *nat* ⇒ *taylor-model*
where *tm-pi prec* = (
let pi-ivl = *the* (*compute-bound-fa prec Pi* [])
in TaylorModel (*poly.C* (*mid pi-ivl*)) (*centered pi-ivl*)
)

lemma *zero-real-interval*[*intro*,*simp*]: *0* $\in_r$ *0*
⟨*proof*⟩

lemma *range-TM-tm-const*[*simp*]: *range-tm e* (*tm-const c*) = *interval-of c*
⟨*proof*⟩

lemma *num-params-tm-const*[*simp*]: *num-params* (*tm-poly* (*tm-const c*)) = *0*
⟨*proof*⟩

lemma *num-params-tm-pi*[*simp*]: *num-params* (*tm-poly* (*tm-pi prec*)) = *0*
⟨*proof*⟩

lemma *range-tm-tm-pi*: *pi* $\in_i$ *range-tm e* (*tm-pi prec*)
⟨*proof*⟩

7.4.1 Derivations of floatarith expressions

Compute the nth derivative of a floatarith expression

fun *deriv* :: *nat* ⇒ *floatarith* ⇒ *nat* ⇒ *floatarith*
where *deriv v f 0* = *f*
| *deriv v f* (*Suc n*) = *DERIV-floatarith v* (*deriv v f n*)

lemma *isDERIV-DERIV-floatarith*:
assumes *isDERIV v f vs*
shows *isDERIV v* (*DERIV-floatarith v f*) *vs*
⟨*proof*⟩

lemma *isDERIV-is-analytic*:
isDERIV i (*Taylor-Models.deriv i f n*) *xs*
if *isDERIV i f xs*
⟨*proof*⟩

lemma *deriv-correct*:
assumes *isDERIV i f* (*xs*[*i*:=*t*]) *i* < *length xs*
shows ((λ*x*. *interpret-floatarith* (*deriv i f n*) (*xs*[*i*:=*x*])) *has-real-derivative interpret-floatarith* (*deriv i f* (*Suc n*)) (*xs*[*i*:=*t*]))
(*at t within S*)
⟨*proof*⟩

Faster derivation for univariate functions, producing smaller terms and thus less over-approximation.

TODO: Extend to Arctan, Log!

fun *deriv-rec* :: *floatarith* ⇒ *nat* ⇒ *floatarith*
where *deriv-rec* (*Exp* (*Var 0*)) - = *Exp* (*Var 0*)
| *deriv-rec* (*Cos* (*Var 0*)) *n* = (*case n mod 4*
of 0 ⇒ *Cos* (*Var 0*)
| *Suc 0* ⇒ *Minus* (*Sin* (*Var 0*))

| *Suc* (*Suc* 0) ⇒ *Minus* (*Cos* (*Var* 0))
| *Suc* (*Suc* (*Suc* 0)) ⇒ *Sin* (*Var* 0))
| *deriv-rec* (*Inverse* (*Var* 0)) *n* = (*if n* = 0 *then Inverse* (*Var* 0) *else Mult* (*Num* (*fact n* ∗ (*if n mod* 2 = 0 *then* 1 *else* −1))) (*Inverse* (*Power* (*Var* 0) (*Suc n*))))
| *deriv-rec f n* = *deriv* 0 *f n*

lemma *deriv-rec-correct*:
assumes *isDERIV* 0 *f* (*xs*[0:=*t*]) 0 < *length xs*
shows ((λ*x*. *interpret-floatarith* (*deriv-rec f n*) (*xs*[0:=*x*])) *has-real-derivative interpret-floatarith* (*deriv-rec f* (*Suc n*)) (*xs*[0:=*t*])) (*at t within S*)
⟨*proof*⟩

lemma *deriv-rec-0-idem*[*simp*]:
shows *deriv-rec f* 0 = *f*
⟨*proof*⟩

7.4.2 Computing Taylor models for arbitrary univariate expressions

fun *tmf-c* :: *nat* ⇒ *float interval list* ⇒ *floatarith* ⇒ *nat* ⇒ *float interval option*
where *tmf-c prec I f i* = *compute-bound-fa prec* (*Mult* (*deriv-rec f i*) (*Inverse* (*Num* (*fact i*)))) *I*
— The interval coefficients of the Taylor polynomial, i.e. the real coefficients approximated by a float interval.

fun *tmf-ivl-cs* :: *nat* ⇒ *nat* ⇒ *float interval list* ⇒ *float list* ⇒ *floatarith* ⇒ *float interval list option*
where *tmf-ivl-cs prec ord I a f* = *those* (*map* (*tmf-c prec a f*) [0..<*ord*] @ [*tmf-c prec I f ord*])
— Make a list of bounds on the n+1 coefficients, with the n+1-th coefficient bounding the remainder term of the Taylor-Lagrange formula.

fun *tmf-polys* :: *float interval list* ⇒ *float poly* × *float interval poly*
where *tmf-polys* [] = (*poly.C* 0, *poly.C* 0)
| *tmf-polys* (*c* # *cs*) = (
let (*pf*, *pi*) = *tmf-polys cs*
in (*poly.CN* (*poly.C* (*mid c*)) 0 *pf*, *poly.CN* (*poly.C* (*centered c*)) 0 *pi*)
)

fun *tm-floatarith* :: *nat* ⇒ *nat* ⇒ *float interval list* ⇒ *float list* ⇒ *floatarith* ⇒ *taylor-model option*
where *tm-floatarith prec ord I a f* = (
map-option (λ*cs*.
let (*pf*, *pi*) = *tmf-polys cs*;
- = *compute-bound-tm prec* (*List.map2* (−) *I a*);
e = *round-interval prec* (*Ipoly* (*List.map2* (−) *I a*) *pi*) — TODO: use *compute-bound-tm* here?!
in TaylorModel pf e
) (*tmf-ivl-cs prec ord I a f*)

) — Compute a Taylor model from an arbitrary, univariate floatarith expression, if possible. This is used to compute Taylor models for elemental functions like sin, cos, exp, etc.

term *compute-bound-poly*
lemma *tmf-c-correct*:
fixes *A*::*float interval list* **and** *I*::*float interval* **and** *f*::*floatarith* **and** *a*::*real list*
assumes *a all-in A*
assumes *tmf-c prec A f i = Some I*
shows *interpret-floatarith* (*deriv-rec f i*) *a* / *fact i* $\in_r$ *I*
⟨*proof*⟩

lemma *tmf-ivl-cs-length*:
assumes *tmf-ivl-cs prec n A a f = Some cs*
shows *length cs = n + 1*
⟨*proof*⟩

lemma *tmf-ivl-cs-correct*:
fixes *A*::*float interval list* **and** *f*::*floatarith*
assumes *a all-in I*
assumes *tmf-ivl-cs prec ord I a f = Some cs*
shows $\bigwedge i.\ i < ord \Longrightarrow$ *tmf-c prec* (*map interval-of a*) *f i = Some* (*cs*!*i*)
and *tmf-c prec I f ord = Some* (*cs*!*ord*)
and *length cs = Suc ord*
⟨*proof*⟩

lemma *Ipoly-fst-tmf-polys*:
Ipoly xs (*fst* (*tmf-polys z*)) = ($\sum i$<*length z*. *xs* ! *0* ^ *i* ∗ (*mid* (*z* ! *i*)))
for *xs*::*real list*
⟨*proof*⟩

lemma *insertion-fst-tmf-polys*:
insertion e (*fst* (*tmf-polys z*)) = ($\sum i$<*length z*. *e 0* ^ *i* ∗ (*mid* (*z* ! *i*)))
for *e*::*nat* ⇒ *real*
⟨*proof*⟩

lemma *Ipoly-snd-tmf-polys*:
set-of (*horner-eval* (*real-interval o centered o nth z*) *x* (*length z*)) ⊆ *set-of* (*Ipoly* [*x*] (*map-poly real-interval* (*snd* (*tmf-polys z*))))
⟨*proof*⟩

lemma *zero-interval*[*intro*,*simp*]: *0* $\in_i$ *0*
⟨*proof*⟩

lemma *sum-in-intervalI*: *sum f X* $\in_i$ *sum g X* **if** $\bigwedge x.\ x \in X \Longrightarrow f\ x \in_i g\ x$
for *f* :: - ⇒ *'a* :: *ordered-comm-monoid-add*
⟨*proof*⟩

lemma *set-of-sum-subset*: *set-of* (*sum f X*) ⊆ *set-of* (*sum g X*)

if $\bigwedge x.\ x \in X \Longrightarrow$ *set-of* $(f\ x) \subseteq$ *set-of* $(g\ x)$
for f :: *-⇒'a::linordered-ab-group-add interval*
⟨*proof*⟩

lemma *interval-of-plus*: *interval-of* $(a + b) =$ *interval-of* $a +$ *interval-of* b
⟨*proof*⟩

lemma *interval-of-uminus*: *interval-of* $(-\ a) = -$ *interval-of* a
⟨*proof*⟩

lemma *interval-of-zero*: *interval-of* $0 = 0$
⟨*proof*⟩

lemma *interval-of-sum*: *interval-of* $(sum\ f\ X) = sum\ (\lambda x.$ *interval-of* $(f\ x))\ X$
⟨*proof*⟩

lemma *interval-of-prod*: *interval-of* $(a * b) =$ *interval-of* $a *$ *interval-of* b
⟨*proof*⟩

lemma *in-set-of-interval-of*[*simp*]: $x \in_i$ (*interval-of* y) $\longleftrightarrow x = y$ **for** $x\ y$::'a::*order*
⟨*proof*⟩

lemma *real-interval-Ipoly*: *real-interval* (*Ipoly xs p*) = *Ipoly* (*map real-interval xs*) (*map-poly real-interval p*)
if *num-params p* ≤ *length xs*
⟨*proof*⟩

lemma *num-params-tmf-polys1*: *num-params* (*fst* (*tmf-polys z*)) ≤ *Suc 0*
⟨*proof*⟩

lemma *num-params-tmf-polys2*: *num-params* (*snd* (*tmf-polys z*)) ≤ *Suc 0*
⟨*proof*⟩

lemma *set-of-real-interval-subset*: *set-of* (*real-interval x*) ⊆ *set-of* (*real-interval y*)
if *set-of x* ⊆ *set-of y*
⟨*proof*⟩

theorem *tm-floatarith*:
assumes *t*: *tm-floatarith prec ord I xs f* = *Some t*
assumes *a*: *xs all-in I* **and** *x*: $x \in_r I\ !\ 0$
assumes *xs-ne*: $xs \neq []$
assumes *deriv*: $\bigwedge x.\ x \in_r I\ !\ 0 \Longrightarrow$ *isDERIV 0 f* $(xs[0 := x])$
assumes $\bigwedge i.\ 0 < i \Longrightarrow i <$ *length xs* $\Longrightarrow e\ i =$ *real-of-float* $(xs\ !\ i)$
assumes *diff-e*: $(x -$ *real-of-float* $(xs\ !\ 0)) = e\ 0$
shows *interpret-floatarith f* $(xs[0:=x]) \in_i$ *range-tm e t*
⟨*proof*⟩

7.5 Operations on Taylor models

fun *tm-norm-poly* :: *taylor-model* ⇒ *taylor-model*
where *tm-norm-poly* (*TaylorModel p e*) = *TaylorModel* (*polynate p*) *e*
— Normalizes the Taylor model by transforming its polynomial into horner form.

fun *tm-lower-order tm-lower-order-of-normed* :: *nat* ⇒ *nat* ⇒ *float interval list* ⇒ *float interval list* ⇒ *taylor-model* ⇒ *taylor-model*
where *tm-lower-order prec ord I a t* = *tm-lower-order-of-normed prec ord I a* (*tm-norm-poly t*)
| *tm-lower-order-of-normed prec ord I a* (*TaylorModel p e*) = (
let (*l*, *r*) = *split-by-degree ord p*
in TaylorModel l (*round-interval prec* (*e* + *compute-bound-poly prec r I a*))
)
— Reduces the degree of a Taylor model's polynomial to n and keeps it range by increasing the error bound.

fun *tm-round-floats tm-round-floats-of-normed* :: *nat* ⇒ *float interval list* ⇒ *float interval list* ⇒ *taylor-model* ⇒ *taylor-model*
where *tm-round-floats prec I a t* = *tm-round-floats-of-normed prec I a* (*tm-norm-poly t*)
| *tm-round-floats-of-normed prec I a* (*TaylorModel p e*) = (
let (*l*, *r*) = *split-by-prec prec p*
in TaylorModel l (*round-interval prec* (*e* + *compute-bound-poly prec r I a*))
)
— Rounding of Taylor models. Rounds both the coefficients of the polynomial and the floats in the error bound.

fun *tm-norm tm-norm′* :: *nat* ⇒ *nat* ⇒ *float interval list* ⇒ *float interval list* ⇒ *taylor-model* ⇒ *taylor-model*
where *tm-norm prec ord I a t* = *tm-norm′ prec ord I a* (*tm-norm-poly t*)
| *tm-norm′ prec ord I a t* = *tm-round-floats-of-normed prec I a* (*tm-lower-order-of-normed prec ord I a t*)
— Normalization of taylor models. Performs order lowering and rounding on tayor models, also converts the polynomial into horner form.

fun *tm-neg* :: *taylor-model* ⇒ *taylor-model*
where *tm-neg* (*TaylorModel p e*) = *TaylorModel* ($\sim_p$ *p*) (−*e*)

fun *tm-add* :: *taylor-model* ⇒ *taylor-model* ⇒ *taylor-model*
where *tm-add* (*TaylorModel p1 e1*) (*TaylorModel p2 e2*) = *TaylorModel* (*p1* $+_p$ *p2*) (*e1* + *e2*)

fun *tm-sub* :: *taylor-model* ⇒ *taylor-model* ⇒ *taylor-model*
where *tm-sub t1 t2* = *tm-add t1* (*tm-neg t2*)

fun *tm-mul* :: *nat* ⇒ *nat* ⇒ *float interval list* ⇒ *float interval list* ⇒ *taylor-model* ⇒ *taylor-model* ⇒ *taylor-model*
where *tm-mul prec ord I a* (*TaylorModel p1 e1*) (*TaylorModel p2 e2*) = (
let d1 = *compute-bound-poly prec p1 I a*;

```
        d2 = compute-bound-poly prec p2 I a;
        p = p1 *p p2;
        e = e1*d2 + d1*e2 + e1*e2
      in tm-norm' prec ord I a (TaylorModel p e)
  )
lemmas [simp del] = tm-norm'.simps

fun tm-pow :: nat ⇒ nat ⇒ float interval list ⇒ float interval list ⇒ taylor-model
⇒ nat ⇒ taylor-model
  where tm-pow prec ord I a t 0 = tm-const 1
  | tm-pow prec ord I a t (Suc n) = (
      if odd (Suc n)
      then tm-mul prec ord I a t (tm-pow prec ord I a t n)
      else let t' = tm-pow prec ord I a t ((Suc n) div 2)
           in tm-mul prec ord I a t' t'
    )
```

Evaluates a float polynomial, using a Taylor model as the parameter. This is used to compose Taylor models.

```
fun eval-poly-at-tm :: nat ⇒ nat ⇒ float interval list ⇒ float interval list ⇒ float
poly ⇒ taylor-model ⇒ taylor-model
  where eval-poly-at-tm prec ord I a (poly.C c) t = tm-const c
  | eval-poly-at-tm prec ord I a (poly.Bound n) t = t
  | eval-poly-at-tm prec ord I a (poly.Add p1 p2) t
      = tm-add (eval-poly-at-tm prec ord I a p1 t)
               (eval-poly-at-tm prec ord I a p2 t)
  | eval-poly-at-tm prec ord I a (poly.Sub p1 p2) t
      = tm-sub (eval-poly-at-tm prec ord I a p1 t)
               (eval-poly-at-tm prec ord I a p2 t)
  | eval-poly-at-tm prec ord I a (poly.Mul p1 p2) t
      = tm-mul prec ord I a (eval-poly-at-tm prec ord I a  p1 t)
                            (eval-poly-at-tm prec ord I a p2 t)
  | eval-poly-at-tm prec ord I a (poly.Neg p) t
      = tm-neg (eval-poly-at-tm prec ord I a p t)
  | eval-poly-at-tm prec ord I a (poly.Pw p n) t
      = tm-pow prec ord I a (eval-poly-at-tm prec ord I a p t) n
  | eval-poly-at-tm prec ord I a (poly.CN c n p) t = (
      let pt = eval-poly-at-tm prec ord I a p t;
          t-mul-pt = tm-mul prec ord I a t pt
      in tm-add (eval-poly-at-tm prec ord I a c t) t-mul-pt
    )

fun tm-inc-err :: float interval ⇒ taylor-model ⇒ taylor-model
  where tm-inc-err i (TaylorModel p e) = TaylorModel p (e + i)

fun tm-comp :: nat ⇒ nat ⇒ float interval list ⇒ float interval list ⇒ float ⇒
taylor-model ⇒ taylor-model ⇒ taylor-model
  where tm-comp prec ord I a ta (TaylorModel p e) t = (
      let t-sub-ta = tm-sub t (tm-const ta);
```

```
      pt = eval-poly-at-tm prec ord I a p t-sub-ta
    in tm-inc-err e pt
  )
```

tm-max, *tm-min* and *tm-abs* are implemented extremely naively, because I don't expect them to be very useful. But the implementation is fairly modular, i.e. *tm-*{*abs*,*min*,*max*} all can easily be swapped out, as long as the corresponding correctness lemmas *tm-*{*abs*,*min*,*max*}*-range* are updated as well.

fun *tm-abs* :: *nat* ⇒ *float interval list* ⇒ *float interval list* ⇒ *taylor-model* ⇒ *taylor-model*
  where *tm-abs prec I a t* = (
  let bound = *compute-bound-tm prec I a t*; *abs-bound*=*Ivl* (*0*::*float*) (*max* (*abs* (*lower bound*)) (*abs* (*upper bound*)))
  in TaylorModel (*poly.C* (*mid abs-bound*)) (*centered abs-bound*))

fun *tm-union* :: *nat* ⇒ *float interval list* ⇒ *float interval list* ⇒ *taylor-model* ⇒ *taylor-model* ⇒ *taylor-model*
  where *tm-union prec I a t1 t2* = (
  let b1 = *compute-bound-tm prec I a t1*; *b2* = *compute-bound-tm prec I a t2*;
    b-combined = *sup b1 b2*
  in TaylorModel (*poly.C* (*mid b-combined*)) (*centered b-combined*))

fun *tm-min* :: *nat* ⇒ *float interval list* ⇒ *float interval list* ⇒ *taylor-model* ⇒ *taylor-model* ⇒ *taylor-model*
  where *tm-min prec I a t1 t2* = *tm-union prec I a t1 t2*

fun *tm-max* :: *nat* ⇒ *float interval list* ⇒ *float interval list* ⇒ *taylor-model* ⇒ *taylor-model* ⇒ *taylor-model*
  where *tm-max prec I a t1 t2* = *tm-union prec I a t1 t2*

Rangeity of is preserved by our operations on Taylor models.

lemma *insertion-polyadd*[*simp*]: *insertion e* (*a* +$_p$ *b*) = *insertion e a* + *insertion e b*
  for *a b*::′*a*::*ring-1 poly*
  ⟨*proof*⟩

lemma *insertion-polyneg*[*simp*]: *insertion e* (~$_p$ *b*) = − *insertion e b*
  for *b*::′*a*::*ring-1 poly*
  ⟨*proof*⟩

lemma *insertion-polysub*[*simp*]: *insertion e* (*a* −$_p$ *b*) = *insertion e a* − *insertion e b*
  for *a b*::′*a*::*ring-1 poly*
  ⟨*proof*⟩

lemma *insertion-polymul*[*simp*]: *insertion e* (*a* ∗$_p$ *b*) = *insertion e a* ∗ *insertion e b*

for *a b*::*'a*::*comm-ring-1 poly*
⟨*proof*⟩

lemma *insertion-polypow*[*simp*]: *insertion e* (*a* ^$_p$ *b*) = *insertion e a* ^ *b*
for *a*::*'a*::*comm-ring-1 poly*
⟨*proof*⟩

lemma *insertion-polynate* [*simp*]:
insertion bs (*polynate p*) = (*insertion bs p* :: *'a*::*comm-ring-1*)
⟨*proof*⟩

lemma *tm-norm-poly-range*:
assumes *x* ∈$_i$ *range-tm e t*
shows *x* ∈$_i$ *range-tm e* (*tm-norm-poly t*)
⟨*proof*⟩

lemma *split-by-degree-correct-insertion*:
fixes *x* :: *nat* ⇒ *real* **and** *p* :: *float poly*
assumes *split-by-degree ord p* = (*l*, *r*)
shows *maxdegree l* ≤ *ord* (**is** *?P1*)
and *insertion x p* = *insertion x l* + *insertion x r* (**is** *?P2*)
and *num-params l* ≤ *num-params p* (**is** *?P3*)
and *num-params r* ≤ *num-params p* (**is** *?P4*)
⟨*proof*⟩

lemma *split-by-prec-correct-insertion*:
fixes *x* :: *nat* ⇒ *real* **and** *p* :: *float poly*
assumes *split-by-prec ord p* = (*l*, *r*)
shows *insertion x p* = *insertion x l* + *insertion x r* (**is** *?P1*)
and *num-params l* ≤ *num-params p* (**is** *?P2*)
and *num-params r* ≤ *num-params p* (**is** *?P3*)
⟨*proof*⟩

lemma *tm-lower-order-of-normed-range*:
assumes *x* ∈$_i$ *range-tm e t*
assumes *dev*: *develops-at-within e a I*
assumes *num-params* (*tm-poly t*) ≤ *length I*
shows *x* ∈$_i$ *range-tm e* (*tm-lower-order-of-normed prec ord I a t*)
⟨*proof*⟩

lemma *num-params-tm-norm-poly-le*: *num-params* (*tm-poly* (*tm-norm-poly t*)) ≤ *X*
if *num-params* (*tm-poly t*) ≤ *X*
⟨*proof*⟩

lemma *tm-lower-order-range*:
assumes *x* ∈$_i$ *range-tm e t*
assumes *dev*: *develops-at-within e a I*
assumes *num-params* (*tm-poly t*) ≤ *length I*

shows $x \in_i$ *range-tm e* (*tm-lower-order prec ord I a t*)
⟨*proof*⟩

lemma *tm-round-floats-of-normed-range*:
assumes $x \in_i$ *range-tm e t*
assumes *dev*: *develops-at-within e a I*
assumes *num-params* (*tm-poly t*) ≤ *length I*
shows $x \in_i$ *range-tm e* (*tm-round-floats-of-normed prec I a t*)
— TODO: this is a clone of ⟦*?x* $\in_i$ *range-tm ?e ?t*; *develops-at-within ?e ?a ?I*; *num-params* (*tm-poly ?t*) ≤ *length ?I*⟧ ⟹ *?x* $\in_i$ *range-tm ?e* (*tm-lower-order-of-normed ?prec ?ord ?I ?a ?t*) -¿ general sweeping method!
⟨*proof*⟩

lemma *num-params-split-by-degree-le*: *num-params* (*fst* (*split-by-degree ord x*)) ≤ *K*
num-params (*snd* (*split-by-degree ord x*)) ≤ *K*
if *num-params x* ≤ *K* **for** *x*::*float poly*
⟨*proof*⟩

lemma *num-params-split-by-prec-le*: *num-params* (*fst* (*split-by-prec ord x*)) ≤ *K*
num-params (*snd* (*split-by-prec ord x*)) ≤ *K*
if *num-params x* ≤ *K* **for** *x*::*float poly*
⟨*proof*⟩

lemma *num-params-tm-norm′-le*:
num-params (*tm-poly* (*tm-round-floats-of-normed prec I a t*)) ≤ *X*
if *num-params* (*tm-poly t*) ≤ *X*
⟨*proof*⟩

lemma *tm-round-floats-range*:
assumes $x \in_i$ *range-tm e t develops-at-within e a I num-params* (*tm-poly t*) ≤ *length I*
shows $x \in_i$ *range-tm e* (*tm-round-floats prec I a t*)
⟨*proof*⟩

lemma *num-params-tm-lower-order-of-normed-le*: *num-params* (*tm-poly* (*tm-lower-order-of-normed prec ord I a t*)) ≤ *X*
if *num-params* (*tm-poly t*) ≤ *X*
⟨*proof*⟩

lemma *tm-norm′-range*:
assumes $x \in_i$ *range-tm e t develops-at-within e a I num-params* (*tm-poly t*) ≤ *length I*
shows $x \in_i$ *range-tm e* (*tm-norm′ prec ord I a t*)
⟨*proof*⟩

lemma *num-params-tm-norm′*:
num-params (*tm-poly* (*tm-norm′ prec ord I a t*)) ≤ *X*

if *num-params* (*tm-poly t*) ≤ *X*
⟨*proof*⟩

lemma *tm-norm-range*:
assumes *x* ∈$_i$ *range-tm e t develops-at-within e a I num-params* (*tm-poly t*) ≤ *length I*
shows *x* ∈$_i$ *range-tm e* (*tm-norm prec ord I a t*)
⟨*proof*⟩
lemmas [*simp del*] = *tm-norm.simps*

lemma *tm-neg-range*:
assumes *x* ∈$_i$ *range-tm e t*
shows − *x* ∈$_i$ *range-tm e* (*tm-neg t*)
⟨*proof*⟩
lemmas [*simp del*] = *tm-neg.simps*

lemma *tm-bound-tm-add*[*simp*]: *tm-bound* (*tm-add t1 t2*) = *tm-bound t1* + *tm-bound t2*
⟨*proof*⟩

lemma *interval-of-add*: *interval-of* (*a* + *b*) = *interval-of a* + *interval-of b*
⟨*proof*⟩

lemma *tm-add-range*:
x + *y* ∈$_i$ *range-tm e* (*tm-add t1 t2*)
if *x* ∈$_i$ *range-tm e t1*
y ∈$_i$ *range-tm e t2*
⟨*proof*⟩
lemmas [*simp del*] = *tm-add.simps*

lemma *tm-sub-range*:
assumes *x* ∈$_i$ *range-tm e t1*
assumes *y* ∈$_i$ *range-tm e t2*
shows *x* − *y* ∈$_i$ *range-tm e* (*tm-sub t1 t2*)
⟨*proof*⟩
lemmas [*simp del*] = *tm-sub.simps*

lemma *set-of-intervalI*: *set-of* (*interval-of y*) ⊆ *set-of Y* **if** *y* ∈$_i$ *Y* **for** *y*::*'a*::*order*
⟨*proof*⟩

lemma *set-of-real-intervalI*: *set-of* (*interval-of y*) ⊆ *set-of* (*real-interval Y*) **if** *y* ∈$_r$ *Y*
⟨*proof*⟩

lemma *tm-mul-range*:
assumes *x* ∈$_i$ *range-tm e t1*
assumes *y* ∈$_i$ *range-tm e t2*
assumes *dev*: *develops-at-within e a I*

assumes *params*: *num-params* (*tm-poly t1*) ≤ *length I num-params* (*tm-poly t2*) ≤ *length I*
shows *x* ∗ *y* ∈$_i$ *range-tm e* (*tm-mul prec ord I a t1 t2*)
⟨*proof*⟩

lemma *num-params-tm-mul-le*:
num-params (*tm-poly* (*tm-mul prec ord I a t1 t2*)) ≤ *X*
if *num-params* (*tm-poly t1*) ≤ *X*
num-params (*tm-poly t2*) ≤ *X*
⟨*proof*⟩

lemmas [*simp del*] = *tm-pow.simps*— TODO: make a systematic decision

lemma
shows *tm-pow-range*: *num-params* (*tm-poly t*) ≤ *length I* ⟹
develops-at-within e a I ⟹
x ∈$_i$ *range-tm e t* ⟹
x ^ *n* ∈$_i$ *range-tm e* (*tm-pow prec ord I a t n*)
and *num-params-tm-pow-le*[*THEN order-trans*]:
num-params (*tm-poly* (*tm-pow prec ord I a t n*)) ≤ *num-params* (*tm-poly t*)
⟨*proof*⟩

lemma *num-params-tm-add-le*:
num-params (*tm-poly* (*tm-add t1 t2*)) ≤ *X*
if *num-params* (*tm-poly t1*) ≤ *X*
num-params (*tm-poly t2*) ≤ *X*
⟨*proof*⟩

lemma *num-params-tm-neg-eq*[*simp*]:
num-params (*tm-poly* (*tm-neg t1*)) = *num-params* (*tm-poly t1*)
⟨*proof*⟩

lemma *num-params-tm-sub-le*:
num-params (*tm-poly* (*tm-sub t1 t2*)) ≤ *X*
if *num-params* (*tm-poly t1*) ≤ *X*
num-params (*tm-poly t2*) ≤ *X*
⟨*proof*⟩

lemma *num-params-eval-poly-le*: *num-params* (*tm-poly* (*eval-poly-at-tm prec ord I a p t*)) ≤ *x*
if *num-params* (*tm-poly t*) ≤ *x num-params p* ≤ *max 1 x*
⟨*proof*⟩

lemma *eval-poly-at-tm-range*:
assumes *num-params p* ≤ *1*
assumes *tg-def*: *e′ 0* ∈$_i$ *range-tm e tg*
assumes *dev*: *develops-at-within e a I* **and** *params*: *num-params* (*tm-poly tg*) ≤ *length I*
shows *insertion e′ p* ∈$_i$ *range-tm e* (*eval-poly-at-tm prec ord I a p tg*)

⟨*proof*⟩

lemma *tm-inc-err-range*: $x \in_i$ *range-tm e* (*tm-inc-err i t*)
if $x \in_i$ *range-tm e t* + *real-interval i*
⟨*proof*⟩

lemma *num-params-tm-inc-err*: *num-params* (*tm-poly* (*tm-inc-err i t*)) $\leq X$
if *num-params* (*tm-poly t*) $\leq X$
⟨*proof*⟩

lemma *num-params-tm-comp-le*: *num-params* (*tm-poly* (*tm-comp prec ord I a ga tf tg*)) $\leq X$
if *num-params* (*tm-poly tf*) $\leq$ *max 1 X num-params* (*tm-poly tg*) $\leq X$
⟨*proof*⟩

lemma *tm-comp-range*:
assumes *tf-def*: $x \in_i$ *range-tm e' tf*
assumes *tg-def*: *e' 0* $\in_i$ *range-tm e* (*tm-sub tg* (*tm-const ga*))
assumes *params*: *num-params* (*tm-poly tf*) $\leq$ *1 num-params* (*tm-poly tg*) $\leq$ *length I*
assumes *dev*: *develops-at-within e a I*
shows $x \in_i$ *range-tm e* (*tm-comp prec ord I a ga tf tg*)
⟨*proof*⟩

lemma *mid-centered-collapse*:
interval-of (*real-of-float* (*mid abs-bound*)) + *real-interval* (*centered abs-bound*) = *real-interval abs-bound*
⟨*proof*⟩

lemmas [*simp del*] = *tm-abs.simps*
lemma *tm-abs-range*:
assumes *x*: $x \in_i$ *range-tm e t*
assumes *n*: *num-params* (*tm-poly t*) $\leq$ *length I* **and** *d*: *develops-at-within e a I*
shows *abs x* $\in_i$ *range-tm e* (*tm-abs prec I a t*)
⟨*proof*⟩

lemma *num-params-tm-abs-le*: *num-params* (*tm-poly* (*tm-abs prec I a t*)) $\leq X$ **if** *num-params* (*tm-poly t*) $\leq X$
⟨*proof*⟩

lemma *real-interval-sup*: *real-interval* (*sup a b*) = *sup* (*real-interval a*) (*real-interval b*)
⟨*proof*⟩

lemma *in-interval-supI1*: $x \in_i a \Longrightarrow x \in_i$ *sup a b*
and *in-interval-supI2*: $x \in_i b \Longrightarrow x \in_i$ *sup a b*
for *x*::*'a*::*lattice*
⟨*proof*⟩

lemma *tm-union-range-left*:
assumes $x \in_i$ *range-tm e t1*
num-params (*tm-poly t1*) $\leq$ *length I develops-at-within e a I*
shows $x \in_i$ *range-tm e* (*tm-union prec I a t1 t2*)
⟨*proof*⟩

lemma *tm-union-range-right*:
assumes $x \in_i$ *range-tm e t2*
num-params (*tm-poly t2*) $\leq$ *length I develops-at-within e a I*
shows $x \in_i$ *range-tm e* (*tm-union prec I a t1 t2*)
⟨*proof*⟩

lemma *num-params-tm-union-le*:
num-params (*tm-poly* (*tm-union prec I a t1 t2*)) $\leq X$
if *num-params* (*tm-poly t1*) $\leq X$ *num-params* (*tm-poly t2*) $\leq X$
⟨*proof*⟩

lemmas [*simp del*] = *tm-union.simps tm-min.simps tm-max.simps*

lemma *tm-min-range*:
assumes $x \in_i$ *range-tm e t1*
assumes $y \in_i$ *range-tm e t2*
num-params (*tm-poly t1*) $\leq$ *length I*
num-params (*tm-poly t2*) $\leq$ *length I*
develops-at-within e a I
shows *min x y* $\in_i$ *range-tm e* (*tm-min prec I a t1 t2*)
⟨*proof*⟩

lemma *tm-max-range*:
assumes $x \in_i$ *range-tm e t1*
assumes $y \in_i$ *range-tm e t2*
num-params (*tm-poly t1*) $\leq$ *length I*
num-params (*tm-poly t2*) $\leq$ *length I*
develops-at-within e a I
shows *max x y* $\in_i$ *range-tm e* (*tm-max prec I a t1 t2*)
⟨*proof*⟩

7.6 Computing Taylor models for multivariate expressions

Compute Taylor models for expressions of the form "f (g x)", where f is an elementary function like exp or cos, by composing Taylor models for f and g. For our correctness proof, we need to make it explicit that the range of g on I is inside the domain of f, by introducing the *f-exists-on* predicate.

fun *compute-tm-by-comp* :: *nat* ⇒ *nat* ⇒ *float interval list* ⇒ *float interval list* ⇒ *floatarith* ⇒ *taylor-model option* ⇒ (*float interval* ⇒ *bool*) ⇒ *taylor-model option*
where *compute-tm-by-comp prec ord I a f g f-exists-on* = (
case g
of Some tg ⇒ (

```
        let gI = compute-bound-tm prec I a tg;
            ga = mid (compute-bound-tm prec a a tg)
        in if f-exists-on gI
            then map-option (λtf. tm-comp prec ord I a ga tf tg ) (tm-floatarith
prec ord [gI] [ga] f)
           else None)
      | - ⇒ None
    )
```

Compute Taylor models with numerical precision *prec* of degree *ord*, with Taylor models in the environment *env* whose variables are jointly interpreted with domain I and expanded around point a. from floatarith expressions on a rectangular domain.

```
fun approx-tm :: nat ⇒ nat ⇒ float interval list ⇒ float interval list ⇒ floatarith
⇒ taylor-model list ⇒
    taylor-model option
  where approx-tm - - I - (Num c) env = Some (tm-const c)
  | approx-tm - - I a (Var n) env = (if n < length env then Some (env ! n) else
None)
  | approx-tm prec ord I a (Add l r) env = (
        case (approx-tm prec ord I a l env, approx-tm prec ord I a r env)
        of (Some t1, Some t2) ⇒ Some (tm-add t1 t2)
         | - ⇒ None)
  | approx-tm prec ord I a (Minus f) env
        = map-option tm-neg (approx-tm prec ord I a f env)
  | approx-tm prec ord I a (Mult l r) env = (
        case (approx-tm prec ord I a l env, approx-tm prec ord I a r env)
        of (Some t1, Some t2) ⇒ Some (tm-mul prec ord I a t1 t2)
         | - ⇒ None)
  | approx-tm prec ord I a (Power f k) env
        = map-option (λt. tm-pow prec ord I a t k)
                     (approx-tm prec ord I a f env)
  | approx-tm prec ord I a (Inverse f) env
        = compute-tm-by-comp prec ord I a (Inverse (Var 0)) (approx-tm prec ord
I a f env) (λx. 0 < lower x ∨ upper x < 0)
  | approx-tm prec ord I a (Cos f) env
        = compute-tm-by-comp prec ord I a (Cos (Var 0)) (approx-tm prec ord I a
f env) (λx. True)
  | approx-tm prec ord I a (Arctan f) env
        = compute-tm-by-comp prec ord I a (Arctan (Var 0)) (approx-tm prec ord
I a f env) (λx. True)
  | approx-tm prec ord I a (Exp f) env
        = compute-tm-by-comp prec ord I a (Exp (Var 0)) (approx-tm prec ord I a
f env) (λx. True)
  | approx-tm prec ord I a (Ln f) env
        = compute-tm-by-comp prec ord I a (Ln (Var 0)) (approx-tm prec ord I a f
env) (λx. 0 < lower x)
  | approx-tm prec ord I a (Sqrt f) env
        = compute-tm-by-comp prec ord I a (Sqrt (Var 0)) (approx-tm prec ord I a
```

f env) (λ*x*. *0* < *lower x*)
| *approx-tm prec ord I a Pi env* = *Some* (*tm-pi prec*)
| *approx-tm prec ord I a* (*Abs f*) *env*
= *map-option* (*tm-abs prec I a*) (*approx-tm prec ord I a f env*)
| *approx-tm prec ord I a* (*Min l r*) *env* = (
case (*approx-tm prec ord I a l env*, *approx-tm prec ord I a r env*)
of (*Some t1*, *Some t2*) ⇒ *Some* (*tm-min prec I a t1 t2*)
| - ⇒ *None*)
| *approx-tm prec ord I a* (*Max l r*) *env* = (
case (*approx-tm prec ord I a l env*, *approx-tm prec ord I a r env*)
of (*Some t1*, *Some t2*) ⇒ *Some* (*tm-max prec I a t1 t2*)
| - ⇒ *None*)
| *approx-tm prec ord I a* (*Powr l r*) *env* = *None* — TODO
| *approx-tm prec ord I a* (*Floor l*) *env* = *None* — TODO

lemma *mid-in-real-interval*: *mid i* ∈*r i*
⟨*proof*⟩

lemma *set-of-real-interval-mono*:*set-of* (*real-interval x*) ⊆ *set-of* (*real-interval y*)
if *set-of x* ⊆ *set-of y*
⟨*proof*⟩

lemmas [*simp del*] = *compute-bound-poly.simps tm-floatarith.simps*

lemmas [*simp del*] = *tmf-ivl-cs.simps compute-bound-tm.simps tmf-polys.simps*

lemma *tm-floatarith-eq-Some-num-params*:
tm-floatarith prec ord a b f = *Some tf* ⟹ *num-params* (*tm-poly tf*) ≤ *1*
⟨*proof*⟩

lemma *compute-tm-by-comp-range*:
assumes *max-Var-floatarith f* ≤ *1*
assumes *a*: *a all-subset I*
assumes *tx-range*: *x* ∈*i range-tm e tg*
assumes *t-def*: *compute-tm-by-comp prec ord I a f* (*Some tg*) *c* = *Some t*
assumes *f-deriv*:
⋀*x*. *x* ∈*r compute-bound-tm prec I a tg* ⟹ *c* (*compute-bound-tm prec I a tg*)
⟹ *isDERIV 0 f* [*x*]
assumes *params*: *num-params* (*tm-poly tg*) ≤ *length I*
and *dev*: *develops-at-within e a I*
shows *interpret-floatarith f* [*x*] ∈*i range-tm e t*
⟨*proof*⟩

lemmas [*simp del*] = *compute-tm-by-comp.simps*

lemma *compute-tm-by-comp-num-params-le*:
assumes *compute-tm-by-comp prec ord I a f* (*Some t0*) *i* = *Some t*

assumes $1 \leq X$ *num-params* (*tm-poly t0*) $\leq X$
shows *num-params* (*tm-poly t*) $\leq X$
⟨*proof*⟩

lemma *compute-tm-by-comp-eq-Some-iff*: *compute-tm-by-comp prec ord I a f t0 i* = *Some t* ⟷
(∃ *z x2*. *t0* = *Some x2* ∧
tm-floatarith prec ord [*compute-bound-tm prec I a x2*]
[*mid* (*compute-bound-tm prec a a x2*)] *f* =
Some z
∧ *tm-comp prec ord I a*
(*mid* (*compute-bound-tm prec a a x2*)) *z x2* = *t*
∧ *i* (*compute-bound-tm prec I a x2*))
⟨*proof*⟩

lemma *num-params-approx-tm*:
assumes *approx-tm prec ord I a f env* = *Some t*
assumes ⋀*tm*. *tm* ∈ *set env* ⟹ *num-params* (*tm-poly tm*) ≤ *length I*
shows *num-params* (*tm-poly t*) ≤ *length I*
⟨*proof*⟩

lemma *in-interval-realI*: *a* ∈$_i$ *I* **if** *a* ∈$_r$ *I* ⟨*proof*⟩

lemma *all-subset-all-inI*: *map interval-of a all-subset I* **if** *a all-in I*
⟨*proof*⟩

lemma *compute-tm-by-comp-None*: *compute-tm-by-comp p ord I a x None k* = *None*
⟨*proof*⟩

lemma *approx-tm-num-Vars-None*:
assumes *max-Var-floatarith f* > *length env*
shows *approx-tm p ord I a f env* = *None*
⟨*proof*⟩

lemma *approx-tm-num-Vars*:
assumes *approx-tm prec ord I a f env* = *Some t*
shows *max-Var-floatarith f* ≤ *length env*
⟨*proof*⟩

definition *range-tms e xs* = *map* (*range-tm e*) *xs*

lemma *approx-tm-range*:
assumes *a*: *a all-subset I*
assumes *t-def*: *approx-tm prec ord I a f env* = *Some t*
assumes *allin*: *xs all-in*$_i$ *range-tms e env*
assumes *devs*: *develops-at-within e a I*
assumes *env*: ⋀*tm*. *tm* ∈ *set env* ⟹ *num-params* (*tm-poly tm*) ≤ *length I*
shows *interpret-floatarith f xs* ∈$_i$ *range-tm e t*

⟨*proof*⟩

Evaluate expression with Taylor models in environment.

7.7 Computing bounds for floatarith expressions

TODO: compare parametrization of input vs. uncertainty for input...

definition *tm-of-ivl-par n ivl* = *TaylorModel* (*CN* (*C* ((*upper ivl* + *lower ivl*)∗*Float* 1 (−1))) *n*
(*C* ((*upper ivl* − *lower ivl*)∗*Float* 1 (−1)))) *0*
— track uncertainty in parameter *n*, which is to be interpreted over standardized domain [−*1*, *1*].

value *tm-of-ivl-par 3* (*Ivl* (−*1*) *1*)

definition *tms-of-ivls ivls* = *map* (λ(*i*, *ivl*). *tm-of-ivl-par i ivl*) (*zip* [*0*..<*length ivls*] *ivls*)

value *tms-of-ivls* [*Ivl 1 2*, *Ivl 4 5*]

primrec *approx-slp'*::*nat* ⇒ *nat* ⇒ *float interval list* ⇒ *float interval list* ⇒ *slp* ⇒
taylor-model list ⇒ *taylor-model list option*
where
approx-slp' p ord I a [] *xs* = *Some xs*
| *approx-slp' p ord I a* (*ea* # *eas*) *xs* =
do {
r ← *approx-tm p ord I a ea xs*;
approx-slp' p ord I a eas (*r*#*xs*)
}

lemma *mem-range-tms-Cons-iff* [*simp*]: *x*#*xs all-in*$_i$ *range-tms e* (*X*#*XS*) ⟷ *x* ∈$_i$ *range-tm e X* ∧ *xs all-in*$_i$ *range-tms e XS*
⟨*proof*⟩

lemma *approx-slp'-range*:
assumes *i*: *i all-subset I*
assumes *dev*: *develops-at-within e i I*
assumes *vs*: *vs all-in*$_i$ *range-tms e VS* (⋀*tm*. *tm* ∈ *set VS* ⟹ *num-params* (*tm-poly tm*) ≤ *length I*)
assumes *appr*: *approx-slp' p ord I i ra VS* = *Some X*
shows *interpret-slp ra vs all-in*$_i$ *range-tms e X*
⟨*proof*⟩

definition *approx-slp*::*nat* ⇒ *nat* ⇒ *nat* ⇒ *slp* ⇒ *taylor-model list* ⇒ *taylor-model list option*
where
approx-slp p ord d slp tms =
map-option (*take d*)

(*approx-slp'* *p* *ord* (*replicate* (*length* *tms*) (*Ivl* (−*1*) *1*)) (*replicate* (*length* *tms*) *0*) *slp* *tms*)

lemma *length-range-tms*[*simp*]: *length* (*range-tms* *e* *VS*) = *length* *VS*
⟨*proof*⟩

lemma *set-of-Ivl*: *set-of* (*Ivl* *a* *b*) = {*a* .. *b*} **if** *a* ≤ *b*
⟨*proof*⟩

lemma *set-of-zero*[*simp*]: *set-of* *0* = {*0*::'*a*::*ordered-comm-monoid-add*}
⟨*proof*⟩

theorem *approx-slp-range-tms*:
assumes *approx-slp* *p* *ord* *d* *slp* *VS* = *Some* *X*
assumes *slp-def*: *slp* = *slp-of-fas* *fas*
assumes *d-def*: *d* = *length* *fas*
assumes *e*: *e* ∈ *UNIV* → {−*1* .. *1*}
assumes *vs*: *vs* *all-in*$_i$ *range-tms* *e* *VS*
assumes *lens*: ⋀*tm*. *tm* ∈ *set* *VS* ⟹ *num-params* (*tm-poly* *tm*) ≤ *length* *vs*
shows *interpret-floatariths* *fas* *vs* *all-in*$_i$ *range-tms* *e* *X*
⟨*proof*⟩

end

end
theory *Experiments*
imports *Taylor-Models*
Affine-Arithmetic.Affine-Arithmetic
begin

instantiation *interval*::({*show*, *preorder*}) *show* **begin**

lift-definition *shows-prec-interval*::
nat ⇒ '*a* *interval* ⇒ *char* *list* ⇒ *char* *list*
is λ*p* *ivl* *s*. (*shows-string* ''*Interval*'' *o* *shows* *ivl*) *s* ⟨*proof*⟩

lift-definition *shows-list-interval*::
'*a* *interval* *list* ⇒ *char* *list* ⇒ *char* *list*
is λ*ivls* *s*. *shows-list* *ivls* *s* ⟨*proof*⟩

instance
⟨*proof*⟩

end

definition *split-largest-interval* :: *float* *interval* *list* ⇒ *float* *interval* *list* × *float* *interval* *list* **where**
split-largest-interval *xs* = (*case* *sort-key* (*uminus* *o* *snd*) (*zip* [*0*..<*length* *xs*] (*map*

(λx. upper x − lower x) xs)) of Nil ⇒ ([], [])
| (i, -)#- ⇒ let x = xs! i in (xs[i:=Ivl (lower x) ((upper x + lower x)∗Float 1 (−1))],
xs[i:=Ivl ((upper x + lower x)∗Float 1 (−1)) (upper x)]))

definition *Inf-tm p params tm* =
lower (*compute-bound-tm p* (*replicate params* (*Ivl* (−1) (1))) (*replicate params* (*Ivl 0 0*)) *tm*)

primrec *prove-pos*::*bool* ⇒ *nat* ⇒ *nat* ⇒ *nat* ⇒
(*nat* ⇒ *nat* ⇒ *taylor-model list* ⇒ *taylor-model option*) ⇒ *float interval list list* ⇒ *bool* **where**
prove-pos prnt 0 p ord F X = (*let* - = *if prnt then print* (*STR* ''# *depth limit exceeded*↩'') *else* () *in False*)
| *prove-pos prnt* (*Suc i*) *p ord F XXS* =
(*case XXS of* [] ⇒ *True* | (*X*#*XS*) ⇒
let
params = *length X*;
R = *F p ord* (*tms-of-ivls X*);
- = *if prnt then print* (*String.implode* ((*shows* ''# '' *o shows* (*map* (λ*ivl*. (*lower ivl*, *upper ivl*)) *X*)) ''↩'')) *else* ()
in
if R ≠ *None* ∧ 0 < *Inf-tm p params* (*the R*)
then let - = *if prnt then print* (*STR* ''# *Success*↩'') *else* () *in prove-pos prnt i p ord F XS*
else let - = *if prnt then print* (*String.implode* ((*shows* ''# *Split* ('' *o shows* ((*map-option* (*Inf-tm p params*)) *R*) *o shows* '')'') ''↩'')) *else* () *in case split-largest-interval X of* (*a*, *b*) ⇒
prove-pos prnt i p ord F (*a*#*b*#*XS*))

hide-const (**open**) *prove-pos-slp*

definition *prove-pos-slp prnt prec ord fa i xs* = (*let slp* = *slp-of-fas* [*fa*] *in prove-pos prnt i prec ord* (λ*p ord xs*.
case approx-slp prec ord 1 slp xs of None ⇒ *None* | *Some* [*x*] ⇒ *Some x* | *Some* - ⇒ *None*) *xs*)

experiment begin

unbundle *floatarith-notation*

abbreviation *schwefel* ≡
(*5.8806* / *10* ^ *10*) + (*Var 0* − (*Var 1*) ^$_e$ *2*) ^$_e$ *2* + (*Var 1* − *1*) ^$_e$ *2* + (*Var 0* − (*Var 2*) ^$_e$ *2*) ^$_e$ *2* + (*Var 2* − *1*) ^$_e$ *2*

lemma *prove-pos-slp True 30 0 schwefel 100000* [*replicate 3* (*Ivl* (−*10*) *10*)]
⟨*proof*⟩

abbreviation *delta6* ≡ (*Var 0* ∗ *Var 3* ∗ (−*Var 0* + *Var 1* + *Var 2* − *Var 3* +

Var 4 + Var 5) +
*Var 1 * Var 4 * (Var 0 − Var 1 + Var 2 + Var 3 − Var 4 + Var 5) +*
*Var 2 * Var 5 * (Var 0 + Var 1 − Var 2 + Var 3 + Var 4 − Var 5)*
*− Var 1 * Var 2 * Var 3*
*− Var 0 * Var 2 * Var 4*
*− Var 0 * Var 1 * Var 5*
*− Var 3 * Var 4 * Var 5)*

lemma *prove-pos-slp True 30 3 delta6 10000 [replicate 6 (Ivl 4 (Float 104045 (−14)))]*
⟨*proof*⟩

abbreviation *caprasse ≡ (3.1801 + − Var 0 * (Var 2) ^e 3 + 4 * Var 1 * (Var 2) ^e 2 * Var 3 +*
*4 * Var 0 * Var 2 * (Var 3) ^e 2 + 2 * Var 1 * (Var 3) ^e 3 + 4 * Var 0 * Var 2 + 4 * (Var 2) ^e 2 − 10 * Var 1 * Var 3 +*
*−10 * (Var 3) ^e 2 + 2)*

lemma *prove-pos-slp True 30 2 caprasse 10000 [replicate 4 (Ivl (−Float 1 (−1)) (Float 1 (−1)))]*
⟨*proof*⟩

abbreviation *magnetism ≡*
*0.25001 + (Var 0) ^e 2 + 2 * (Var 1) ^e 2 + 2 * (Var 2) ^e 2 + 2 * (Var 3) ^e 2 + 2 * (Var 4) ^e 2 + 2 * (Var 5) ^e 2 +*
*2 * (Var 6) ^e 2 − Var 0*

end

end