Program Extraction (Part 3)

Kenji Miyamoto

3.10 – 8.10 Aurachhof, Fischbachau

Today's topics

- Soundness theorem
- Examples of program extraction.
  - on natural numbers
  - on real numbers
- We will see how the proof assistant Minlog works.

Soundness theorem

Theorem (Soundness)

Let M be a derivation of a formula A from assumptions $u_i : C_i$ $(i<k)$.

Then there is a derivation of

$$\begin{cases} et(M) \Vdash A & \text{if } A \text{ is c.r.} \\ A & \text{if } A \text{ is n.c.} \end{cases}$$

from assumptions $\begin{cases} z_{u_i} \Vdash C_i & \text{in case } C_i \text{ is c.r.} \\ C_i & \text{otherwise.} \end{cases}$

Proof. nd on the construction of derivation.

We first deal with logical rules, and then axioms.

Case $\mathcal{U}^A$.

If A is c.r. $\mathrm{et}(\mathcal{U}^A) = \mathbb{Z}_{\mathcal{U}}$. We prove $\mathbb{Z}_{\mathcal{U}} \not\cong A$.

$\mathcal{U}^{\mathbb{Z}_{\mathcal{U}} * A}$ is what we want.

If A is n.c.

$\mathcal{U}^A$ is what we want.

Case $(\lambda u^A M^B)^{A\to B}$. **If $A\to B$ is c.r.**

If A is c.r. $et((\lambda u^A M^B)^{A\to B}) = \lambda_{\vec{z}u}\, et(M)$.

we prove $\lambda_{\vec{z}u}\, et(M) \Vdash A\to B$. that is

$\forall w\,(w \Vdash A \to (\lambda_{\vec{z}u} et(M))\, w \Vdash B)$. hence by renaming,

$\forall_{\vec{z}u}(\vec{z}u \Vdash A \longrightarrow et(M) \Vdash B)$

By ind. hyp. there is a derivation of $et(M) \Vdash B$ from $\vec{z}u \Vdash A$.

If A is n.c. $et((\lambda u^A M^B)^{A\to B}) = et(M)$

we prove $et(M) \Vdash A\to B$, that is $A \to et(M) \Vdash B$.

By ind hyp. there is a derivation of $et(M) \Vdash B$ from A.

If $A\to B$ is n.c. easy by i.h. for B

Case $(\lambda u^A M^B)^{A \to^{nc} B}$.

If $A \to^{m} B$ is c.r.

If A is c.r. $et((\lambda u^A M^B)^{A \to^{nc} B}) = et(M)$

We prove $et(M) \Vdash A \to^{nc} B$, that is $\forall w (w \Vdash A \to et(M) \Vdash B)$.

By ind hyp. there is a derivation of $et(M) \Vdash B$ from $\Sigma u \Vdash A$.

If A is n.c. $et((\lambda u^A M^B)^{A \to^{nc} B}) = et(M)$

We prove $et(M) \Vdash A \to^{nc} B$ that is $A \to et(M) \Vdash B$

By ind. hyp. there is a derivation of $et(M) \Vdash B$ from A.

If $A \to^{nc} B$ is n.c. easy.

Case $(M^{A\to B} N^A)^B$. **If B is c.r.**

If A is c.r. $et((M^{A\to B} N^A)^B) = et(M)\,et(N)$

We prove $et(M)\,et(N) \Vdash B$. By ind. hyp.

(1. $et(M) \Vdash A \to B$, i.e. $\forall \omega\,(\omega \Vdash A \to et(M)\omega \Vdash B)$

2. $et(N) \Vdash A$.

Here we use $\forall^-$ and $\to^-$.

If A is n.c. $et((M^{A\to B} N^A)^B) = et(M)$

We prove $et(M) \Vdash B$ By ind hyp

(1. $et(M) \Vdash A \to B$ i.e. $A \to et(M) \Vdash B$

2. A

Here we use $\to^-$.

If B is n.c. 2 cases $\begin{cases} A \text{ c.r.} \\ A \text{ n.c} \end{cases}$ but easy.

Case $(M^{A \to^{nc} B}\ N^A)^B$. If B is c.r.

$et((M^{A \to^{nc} B}\ N^A)^B) = et(M)$.

We prove $et(M) \Vdash B$. If A is c.r. By ind. hyp.

1. $et(M) \Vdash A \to^{nc} B$, i.e. $\forall \omega\,(\omega \Vdash A \to et(M) \Vdash B)$
2. $et(N) \Vdash A$.

If A is n.c. By ind hyp

1. $et(M) \Vdash A \to^{nc} B$ i.e. $A \to et(M) \Vdash B$
2. A

In any case, it is easy.

If B is n.c. similar to $\to^-$.

Case $(\lambda x\, M^A)^{\forall_x A}$. If $\forall_x A$ c.r.

$et((\lambda x\, M^A)^{\forall_x A}) = \lambda x\, et(M)$

we prove $\lambda x\, et(M) \Vdash \forall_x A$, i.e. $\forall x\,(et(M) \Vdash A)$.

By ind hyp. $et(M) \Vdash A$.

If $\forall_x A$ n.c. use i.h. for M^A. A n.c.

Case $(\lambda x\, M^A)^{\forall^{nc}_x A}$. If $\forall^{nc}_x A$ c.r.

$et((\lambda x M^A)^{\forall^{nc}_x A}) = et(M)$

we prove $et(M) \Vdash \forall^{nc}_x A$ i.e. $\forall x\,(et(M) \Vdash A)$

By ind hyp. $et(M) \Vdash A$.

If $\forall^{nc}_x A$ n.c. use i.h. for M^A where A is n.c.

Case $\left(M^{\forall x A(x)}\, t\right)^{A(t)}$. **If A is c.r.**

$et\left(\left(M^{\forall x A(x)}\, t\right)^{A(t)}\right) = et(M)\, t$.

We prove $et(M)\, t \Vdash A(t)$.

By ind hyp. there is a derivation of $et(M) \Vdash \forall x A(x)$,

that is, $\forall x \left(et(M)\, x \Vdash A(x)\right)$. Use $\forall$ with t.

If A is n.c.

Use i.h. for $M^{\forall x A(x)}$ when $\forall x A(x)$ is n.c.

Case $\left(M^{\forall^{nc}_x A(x)}\ t\right)^{A(t)}$.

If $A(x)$ is c.r.

$et\left(\left(M^{\forall^{nc}_x A(x)}\ t\right)^{A(t)}\right) = et(M)$

We prove $et(M) \Vdash A(t)$.

By ind hyp. there is a derivation of $et(M) \Vdash \forall^{nc}_x A(x)$

that is, $\forall x\,(et(M) \Vdash A(x))$. Use $\forall^-$ with t.

If $A(x)$ is n.c.

Use i.h. for $M^{\forall^{nc}_x A(x)}$ when $\forall^{nc}_x A(x)$ is n.c.

The logical rules managed. //

We consider a special case of $List := \mu_X\left(X\,Nil,\ \forall^{nc}_{x,xs}\left(Yx \to Xxs \to X(x:xs)\right)\right)$.

$List^+_0$, $List^+_1$ and $List^-$. with parameter Y c.r.

$List^+_0 : List_Y(Nil)$

$et(List^+_0) = Nil$. hence we prove $Nil \Vdash List_Y(Nil)$,

i.e, $List^{\Vdash}_{Y^*}(Nil, Nil)$. It is trivial due to $(List^{\Vdash})^+_0$.

$List^+_1 : \forall^{nc}_{x,xs}\left(Yx \to List_Y\, xs \to List_Y(x:xs)\right)$.

$et(List^+_1) = Cons^{\alpha \to L_\alpha \to L_\alpha}$

hence we prove $Cons \Vdash \forall^{nc}_{x,xs}\left(Yx \to List_Y\, xs \to List_Y(x:xs)\right)$

which is, $\forall_{x,xs,u,us}\left(Y^*ux \to List^*_{Y^*}(us,xs) \to List^*_{Y^*}(u:us, x:xs)\right)$.

Again, it is trivial due to $(List^{\Vdash})^+_1$.

$$List^- : \forall^{nc}_{xs}\left(List_Y\, xs \to Y\, Nil \to \forall^{nc}_{x,xs}\left(Y\, x \to List_Y\, xs \to P\, xs \to P(x::xs)\right) \to P\, xs\right)$$

$$et(List^-) = \mathcal{R}^{\tau}_{\mathbb{L}\rho} \qquad (\text{let } \tau := \tau(P),\ \rho_i = \tau(Y))$$

So we prove $\mathcal{R}^{\tau}_{\mathbb{L}\rho}\ *$ ------, namely,

$$\forall_{xs,vs,w_0,w_1}\Big(List^*_{Y^*}(vs,xs) \to$$

$$P^*(w_0, Nil) \to$$

$$\forall_{x,xs,u,us,z}\Big(Y^*\, u\, x \to List^*_{Y^*}(us,xs) \to P^*(z,xs) \to P^*(w_1(u,us,z),\ x::xs)\Big) \to$$

$$P^*(R\ vs\ w_0\ w_1,\ xs)\Big).$$

Assume $xs, vs, w_0, w_1, \ldots$ and use $(List^*)^-$ with $Q\, i = \{vs,xs \mid P^*(R\, vs\, w_0 w_1, xs)\}$

$$(List^*)^- : List^*(vs,xs) \to Q(Nil,Nil) \to$$
$$\forall_{x,xs,u,us}\left(Y^*\, u\, x \to List^*_{Y^*}(us,xs) \to Q(us,xs) \to Q(u::us, x::xs)\right)$$
$$Q(vs,xs)$$

Then. It suffices to prove the premises of $(List^{\#})^-$.

1. $List^{\#}(vs, xs)$ is in the assumption.

2. $Q(Nil, Nil) = P^{\#}(R\ Nil\ w_0\ w_1, Nil)$

   $R\ Nil\ w_0\ w_1 \longmapsto w_0$ by comp. rule.

   $P^{\#}(w_0, Nil)$ is in the assumption.

3. $\forall_{x,xs,u,us}\left(Y^{\#}\,u\,x \to List^{\#}_{Y^{\#}}(us,xs) \to Q(us,xs) \to Q(u:us, x:xs)\right)$

   Assume $x, xs, u, us.\ Y^{\#}\,u\,x,\ List^{\#}_{Y^{\#}}(us,xs)$ and

   $Q(us,xs) \Leftrightarrow P^{\#}(R\ us\ w_0\ w_1, xs)$.

   Prove $Q(u:us, x:xs) \Leftrightarrow P^{\#}\left(w_1(u, us, (R\ us\ w_0\ w_1)), x:xs\right)$

   We use the assumption

   $\forall_{x,xs,u,us,z}\left(Y^{\#}\,u\,x \to List^{\#}_{Y^{\#}}(us,xs) \to P^{\#}(z,xs) \to P^{\#}(w_1(u,us,z), x:xs)\right)$

It suffices to show

$Y^* u x$, (✓ by asm.)

$\mathrm{List}^*_{Y^*}(uS, xS)$, (✓ by asm)

and $P^*(R\,uS\,w_0\,w_1, xS)$ (✓ by asm.)

for axioms C^A with n.c. A, there is nothing to do.

Example 7. even or odd

For any natural number n, n is either even or odd.

As a computational solution of this claim, we extract a program determining

for given n, n is even or odd,

from a proof of

$$\forall_n^{nc}(\mathrm{Tn} \to \mathrm{Even}\ n \vee \mathrm{Odd}\ n)$$

where Tn, Even, Odd defined on the next page ...

Def.

- $\mathrm{Even} := \mu_X\left(X\,0,\ \forall^{nc}_n\left(Xn \to X(S(Sn))\right)\right)$.

$\mathrm{Even}^+_0 : \mathrm{Even}\,0, \qquad \mathrm{Even}^+_1 : \forall^{nc}_n\left(\mathrm{Even}\,n \to \mathrm{Even}\,(S(Sn))\right)$

$\mathrm{Even}^- : \mathrm{Even}\,n \to P\,0 \to \forall^{nc}_n\left(\mathrm{Even}\,n \to Pn \to P(S(Sn)) \to Pn\right)$

- $\mathrm{Odd} := \{n \mid \mathrm{Even}(n+1)\}$

- T (total natural numbers).

$T := \mu_X\left(X\,0,\ \forall^{nc}_n\left(Xn \to X(Sn)\right)\right)$.

$T^+_0 : T\,0, \qquad T^+_1 : \forall^{nc}_n\left(Tn \to T(Sn)\right)$.

$T^- : Tn \to P\,0 \to \forall^{nc}_n\left(Pn \to Tn \to T(Sn)\right) \to Pn$

Example 2. Approximate Split Property

For given real numbers x, z, we cannot determine either $x \leq z$ or $z \leq x$.

However, for reals x, y, z, assuming $x < y$, we can determine $x \leq z$ or $z \leq y$.

We call this property of reals the approximate split property.

Real numbers

A real number x is defined to be a pair $\langle (a_n)_n^{\mathbb{N}\to\mathbb{Q}}, M^{\mathbb{Z}\to\mathbb{N}} \rangle$ satisfying

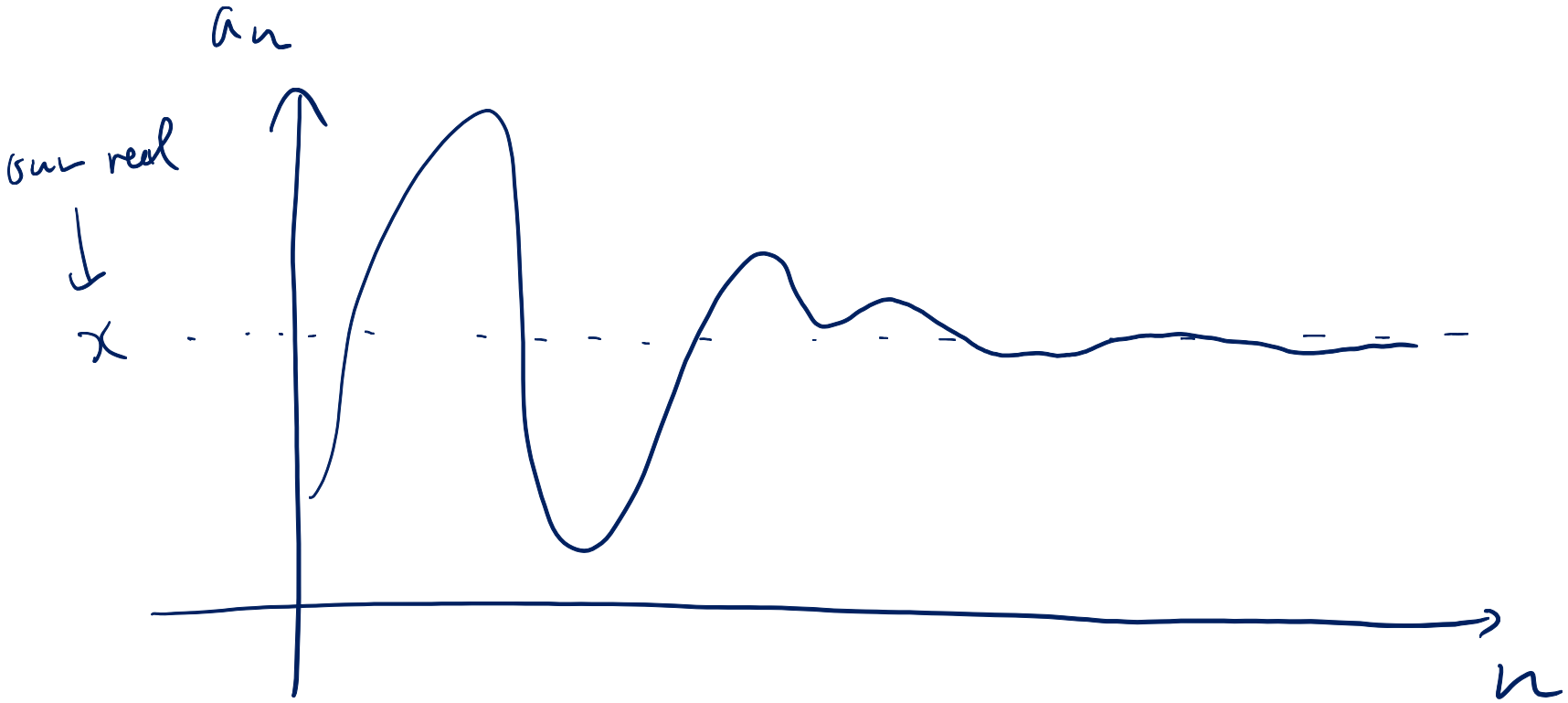
$$\forall_k^{\mathbb{Z}} \forall_{n,m}^{\mathbb{N}} \geq M_k \left(|a_n - a_m| \leq 2^{-k} \right)$$

— $(a_n)_n$ is a sequence of rationals.

— M is so-called Cauchy modulus.

Basic idea of Cauchy sequences is to feed a natural number large enough, so that we get a rational which is a good approximation of the real.

Cauchy modulus



Assume we know how good our approximation should be.

(i.e. we have k in our mind)

We have to know how large n should be

→ For a given k, M answers the question!

Addition and inversion

Let x, y be reals s.t. $x = \langle (a_n)_n, M \rangle$, $y = \langle (b_n)_n, N \rangle$.

$$x + y := \left\langle \lambda n (a_n + b_n),\ \lambda k \left(\max\left(M(k+1), N(k+1) \right) \right) \right\rangle.$$

$$-x := \langle \lambda n (-a_n),\ M \rangle$$

Obviously, $x - y$ is defined to be $x + (-y)$.

$\mathbb{R}^{0+}$ and $\leq$

Real $x = \langle (a_n)_n, M \rangle$.

$$x \in \mathbb{R}^{0+} \iff \forall_k \exists_p \forall_{n \geq p} \left(-2^{-k} \leq a_n \right).$$

We say "x is a non-negative real" for $x \in \mathbb{R}^{0+}$.

We define $x \leq y$ to be $y - x \in \mathbb{R}^{0+}$.

$\mathbb{R}^+$ and $<_k$

Assume x, y are reals.

$x = \langle (a_n)_n, M \rangle \qquad y = \langle (b_n)_n, N \rangle.$

$x \in_k \mathbb{R}^+ \iff \forall k^{\mathbb{Z}} \left(2^{-k} \leq a_{M(k+7)} \right).$

We say "x is k-positive" for $x \in_k \mathbb{R}^+$.

We define $x <_k y := y - x \in_k \mathbb{R}^+$.

We can omit k and write $x < y$ if k is obvious.

Approximate Splitting Property

for given reals x, y, z and an integer k,

assuming $x <_k y$, then $z \leq y$ or $x \leq z$.

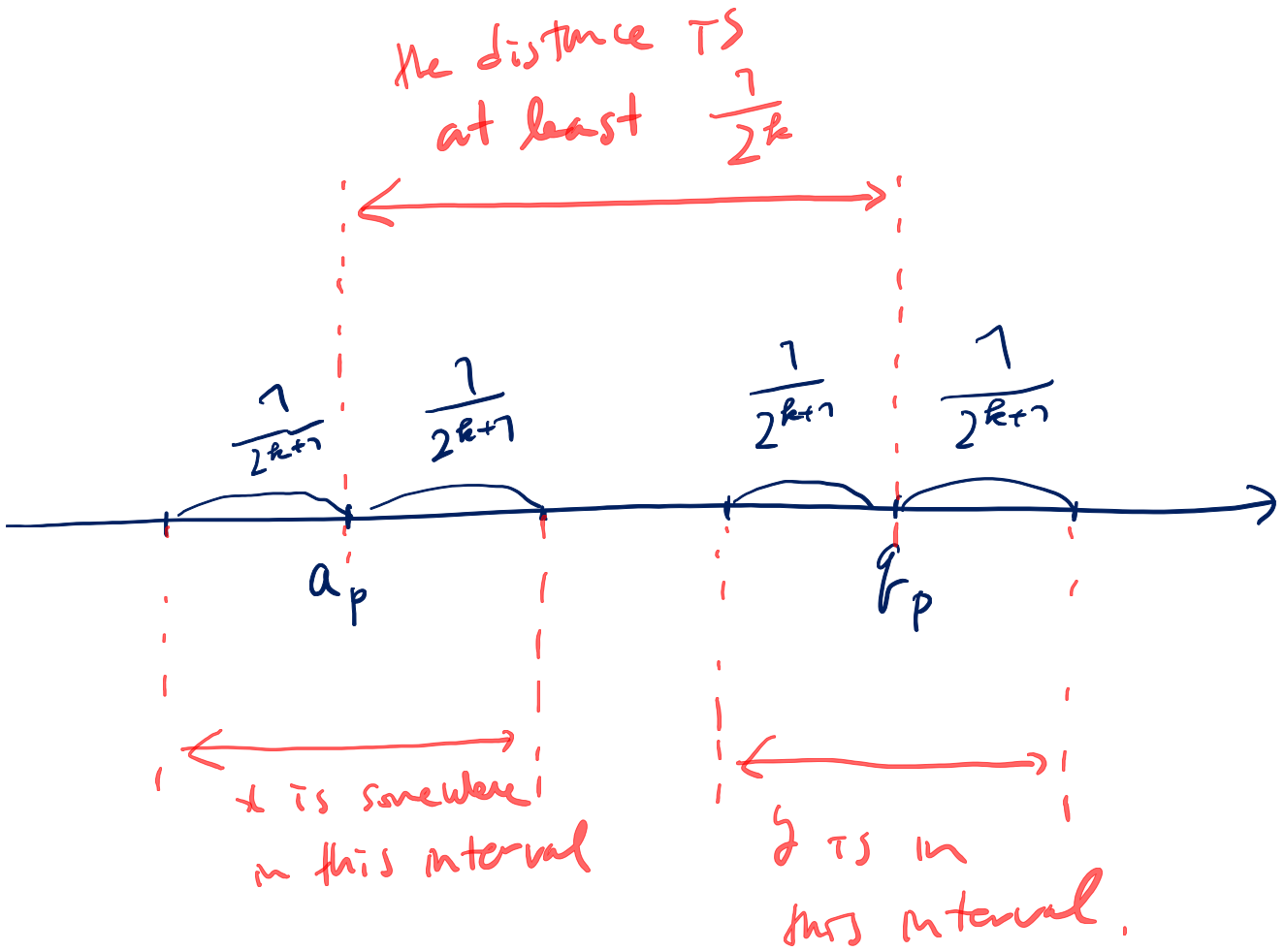
Proof

Let $x = \langle (a_n)_n, M \rangle$ $y = \langle (b_n)_n, N \rangle$

and $z = \langle (c_n)_n, L \rangle$.

and $y - x \in_k \mathbb{R}^+$.

Let $p := \max(M(k+2), N(k+2))$



By approximating $\mathbb{Z}$, the problem is reduced to be rational arithmetic.

Let q be $\max(p, L(k+2))$.

We make a case distinction, either $c_q \le \frac{a_p+b_p}{2}$ or not.

Case $c_q \le \frac{a_p+b_p}{2}$

We prove $x \le y$. It suffices to prove $\forall n \ge q \ (c_n \le b_n)$

$$c_n \le c_q + \frac{1}{2^k}$$

$$\le \frac{a_p+b_p}{2} + \frac{b_p-a_p}{4} = \frac{a_p}{4} + \frac{3}{4} b_p$$

$$= b_p - \frac{b_p-a_p}{4} \le b_p - \frac{1}{2^{k+2}} \le b_n .$$

Case $c_q \not\le \frac{a_p+b_p}{2}$. We prove $x \le z$ in a similar way.

Minlog

- Minlog is an implementation of our theory of PE.
- We saw a formal proof of the two examples in Minlog.
  - Proof of the claims,
  - Extracting programs
  - Generating the soundness (or correctness) proofs.