Program Extraction from Large Proof Developments

Luís Cruz-Filipe

Bas Spitters

Disclaimer

For reasons beyond the authors' control, none of the programs which will be discussed were executable. Therefore, all statements of type

$$\text{program A is} \left\{ \begin{array}{c} \text{more} \\ \text{as} \\ \text{less} \end{array} \right\} \text{efficient} \left\{ \begin{array}{c} \text{than} \\ \text{as} \\ \text{than} \end{array} \right\} \text{program B}$$

should be taken with the proverbial grain of salt.

Connectives

$$
\begin{array}{rcl}
\neg & : & s \to \mathsf{Prop} \\
\to & : & s_1 \to s_2 \to s_2 \\
\vee & : & s_1 \to s_2 \to \mathsf{Set} \\
\underline{\vee} & : & \mathsf{Prop} \to \mathsf{Prop} \to \mathsf{Prop} \\
\wedge & : & s_1 \to s_2 \to \begin{cases} \mathsf{Prop} & s_1 = s_2 = \mathsf{Prop} \\ \mathsf{Set} & s_1 = \mathsf{Set} \text{ or } s_2 = \mathsf{Set} \end{cases} \\
\forall & : & \Pi(A : t_\forall).(A \to s) \to s \\
\exists & : & \Pi(A : t_\exists).(A \to s) \to \mathsf{Prop} \\
\underline{\exists} & : & \Pi(A : t_\exists).(A \to \mathsf{Prop}) \to \mathsf{Prop}
\end{array}
$$

where $\{s, s_1, s_2\}$ denote either Set or Prop, $t_\forall$ is a type of propositions or a datatype, and $t_\exists$ is a generic datatype

$$
\dfrac{(x+y)_m - (x+y)_n =^{*}_{\beta\delta} (x_m + y_m) - (x_n + y_n) \qquad \dfrac{\dfrac{\dfrac{\dfrac{}{|(x_m - x_n)| \leqslant \frac{\varepsilon}{2}} \qquad \dfrac{}{|(y_m - y_n)| \leqslant \frac{\varepsilon}{2}}}{|(x_m - x_n) + (y_m - y_n)| \leqslant \frac{\varepsilon}{2} + \frac{\varepsilon}{2}}\ \leqslant + \leqslant\text{-}|\cdot| \qquad \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon}{|(x_m - x_n) + (y_m - y_n)| \leqslant \varepsilon}\ \leqslant\text{-wd} \qquad (x_m - x_n) + (y_m - y_n) = (x_m + y_m) - (x_n + y_n)}{|(x_m + y_m) - (x_n + y_n)| \leqslant \varepsilon}\ \leqslant\text{-wd}}{|(x+y)_m - (x+y)_n| \leqslant \varepsilon}\ \text{conv}
$$

$$
\dfrac{|(x+y)_m - (x+y)_n| \leq \frac{\varepsilon}{2} \qquad \frac{\varepsilon}{2} < \varepsilon}{|(x+y)_m - (x+y)_n| < \varepsilon}\ \leq\text{-}<\text{-trans}
$$

$<$-$<$-tr	$a < b \to b < c \to a < c$
$<$-$\leq$-tr	$a < b \to b \leq c \to a < c$
$\leq$-$<$-tr	$a \leq b \to b < c \to a < c$
$< + <$-tr	$a < a' \to b < b' \to a + b < a' + b'$
$< + \leq$-tr	$a < a' \to b \leq b' \to a + b < a' + b'$
$\leq + <$-tr	$a \leq a' \to b < b' \to a + b < a' + b'$
$\leq$-$\leq$-tr	$a \leq b \to b \leq c \to a \leq c$
$\leq + \leq$-tr	$a \leq a' \to b \leq b' \to a + b \leq a' + b'$
$<$-$\leq$	$a < b \to a \leq b$

Kneser Lemma

Lemma: For every $n \geq 2$ there exists a real number $q \in]0, 1[$ such that for every polynomial with leading coefficient 1

$$f(x) = x^n + b_{n-1}x^{n-1} + \ldots + b_1 x + b_0$$

one has

$$\forall_{c>|b_0|} \exists_{z\in\mathbb{C}} \left[|z| < c^{\frac{1}{n}} \wedge |f(z)| < qc \right]$$

Proof: Let $r = |z|$, $a_i = |b_i|$ and $q = 1 - 3^{-2n^2-n}$; there exist a_0, η, ε and k such that the following chain of inequalities holds:

$$
\begin{aligned}
\left|\sum_{i=0}^{n} b_i z^i\right| &\leqslant \left|b_0 + b_k z^k\right| + \sum_{i\neq 0,k} a_i r^i \\
&\leqslant \left(a_0 - a_k r^k + \eta\right) + \left(\left(1 - 3^{-n}\right) a_k r^k + 3^n \varepsilon\right) \\
&= a_0 - 3^{-n} a_k r^k + 3^n \varepsilon + \eta \\
&\leqslant a_0 - 3^{-n}\left(3^{-2n^2} a_0 - 2\varepsilon\right) + 3^n \varepsilon + \eta \\
&= \left(1 - 3^{-2n^2-n}\right) a_0 + 3^n \varepsilon + 3^{-n} 2\varepsilon + \eta \\
&\leqslant \left(1 - 3^{-2n^2-n}\right) a_0 + 3^n \varepsilon + \varepsilon + \eta \\
&= q a_0 + 3^n \varepsilon + \varepsilon + \eta \\
&< qc
\end{aligned}
$$

$$\frac{|f(z)| \leq qa_0 + 3^n\varepsilon + \varepsilon + \eta \quad qa_0 + 3^n\varepsilon + \varepsilon + \eta < qc}{|f(z)| < qc} \leq\text{-}<\text{-tr}$$

Change	Reals (Mb)	fta (Mb)	Total (Mb)	Δ(%)
Original	7.5	7.5	15	
New Cauchy seq.	1.5	6.5	8	47
New Kneser proof	1.5	5.0	6.5	19
New Division	1.4	2.0	3.4	48
Various	1.4	1.6	3.0	12

Description	Size (kb)	% of total
"Relevant" code	110	6.5
Unfolding of $\mathbb{C}$	1050	62.5
Unfolding of polynomials ($R[x]$)	330	19.5
Coercions	190	11.5
Total	1680	100