req.1 Regular Minimization is Representable in Q

inc:req:min:sec

Let's consider unbounded search. Suppose $g(x, z)$ is regular and representable in **Q**, say by the formula $\varphi_g(x, z, y)$. Let f be defined by $f(z) = \mu x\, [g(x, z) = 0]$. We would like to find a formula $\varphi_f(z, y)$ representing f. The value of $f(z)$ is that number x which (a) satisfies $g(x, z) = 0$ and (b) is the least such, i.e., for any $w < x$, $g(w, z) \neq 0$. So the following is a natural choice:

$$\varphi_f(z, y) \equiv \varphi_g(y, z, 0) \land \forall w\, (w < y \to \lnot \varphi_g(w, z, 0)).$$

In the general case, of course, we would have to replace z with $z_0, \ldots, z_k$.

The proof, again, will involve some lemmas about things **Q** is strong enough to prove.

inc:req:min:lem:succ

Lemma req.1. *For every variable x and every natural number n,*

$$\mathbf{Q} \vdash (x' + \overline{n}) = (x + \overline{n})'.$$

Proof. The proof is, as usual, by induction on n. In the base case, $n = 0$, we need to show that **Q** proves $(x' + 0) = (x + 0)'$. But we have:

inc:req:min:step1 inc:req:min:step2 inc:req:min:step3

$$\begin{aligned}
&\mathbf{Q} \vdash (x' + 0) = x' \quad \text{by axiom } Q_4 && (1)\\
&\mathbf{Q} \vdash (x + 0) = x \quad \text{by axiom } Q_4 && (2)\\
&\mathbf{Q} \vdash (x + 0)' = x' \quad \text{by eq. (2)} && (3)\\
&\mathbf{Q} \vdash (x' + 0) = (x + 0)' \quad \text{by eq. (1) and eq. (3)}
\end{aligned}$$

In the induction step, we can assume that we have shown that $\mathbf{Q} \vdash (x' + \overline{n}) = (x + \overline{n})'$. Since $\overline{n+1}$ is $\overline{n}'$, we need to show that **Q** proves $(x' + \overline{n}') = (x + \overline{n}')'$. We have:

inc:req:min:step5 inc:req:min:step6

$$\begin{aligned}
&\mathbf{Q} \vdash (x' + \overline{n}') = (x' + \overline{n})' \quad \text{by axiom } Q_5 && (4)\\
&\mathbf{Q} \vdash (x' + \overline{n}') = (x + \overline{n}')' \quad \text{inductive hypothesis} && (5)\\
&\mathbf{Q} \vdash (x' + \overline{n})' = (x + \overline{n}')' \quad \text{by eq. (4) and eq. (5).}
\end{aligned}$$

□

It is again worth mentioning that this is weaker than saying that **Q** proves $\forall x\, \forall y\, (x' + y) = (x + y)'$. Although this sentence is true in $\mathfrak{N}$, **Q** does not prove it.

inc:req:min:lem:less

Lemma req.2.

1. $\mathbf{Q} \vdash \forall x\, \lnot x < \mathsf{o}$.

2. *For every natural number n,*

$$\mathbf{Q} \vdash \forall x\, (x < \overline{n+1} \to (x = \mathsf{o} \lor \cdots \lor x = \overline{n})).$$

Proof. Let us do 1 and part of 2, informally (i.e., only giving hints as to how to construct the formal derivation).

For part 1, by the definition of $<$, we need to prove $\lnot\exists y\,(y' + x) = \mathsf{o}$ in $\mathbf{Q}$, which is equivalent (using the axioms and rules of first-order logic) to $\forall y\,(y' + x) \neq 0$. Here is the idea: suppose $(y' + x) = \mathsf{o}$. If $x = \mathsf{o}$, we have $(y' + \mathsf{o}) = \mathsf{o}$. But by axiom Q_4 of $\mathbf{Q}$, we have $(y' + \mathsf{o}) = y'$, and by axiom Q_2 we have $y' \neq \mathsf{o}$, a contradiction. So $\forall y\,(y' + x) \neq \mathsf{o}$. If $x \neq \mathsf{o}$, by axiom Q_3, there is a z such that $x = z'$. But then we have $(y' + z') = 0$. By axiom Q_5, we have $(y' + z)' = \mathsf{o}$, again contradicting axiom Q_2.

For part 2, use induction on n. Let us consider the base case, when $n = 0$. In that case, we need to show $x < \overline{1} \rightarrow x = \mathsf{o}$. Suppose $x < \overline{1}$. Then by the defining axiom for $<$, we have $\exists y\,(y' + x) = \mathsf{o}'$. Suppose y has that property; so we have $y' + x = \mathsf{o}'$.

We need to show $x = \mathsf{o}$. By axiom Q_3, if $x \neq \mathsf{o}$, we get $x = z'$ for some z. Then we have $(y' + z') = \mathsf{o}'$. By axiom Q_5 of $\mathbf{Q}$, we have $(y' + z)' = \mathsf{o}'$. By axiom Q_1, we have $(y' + z) = \mathsf{o}$. But this means, by definition, $z < \mathsf{o}$, contradicting part 1. □

Lemma req.3. *For every $m \in \mathbb{N}$,* inc:req:min:lem:trichotomy

$$\mathbf{Q} \vdash \forall y\,((y < \overline{m} \lor \overline{m} < y) \lor y = \overline{m}).$$

Proof. By induction on m. First, consider the case $m = 0$. $\mathbf{Q} \vdash \forall y\,(y \neq \mathsf{o} \rightarrow \exists z\, y = z')$ by Q_3. But if $y = z'$, then $(z' + \mathsf{o}) = (y + \mathsf{o})$ by the logic of $=$. By Q_4, $(y + \mathsf{o}) = y$, so we have $(z' + \mathsf{o}) = y$, and hence $\exists z\,(z' + \mathsf{o}) = y$. By the definition of $<$ in Q_8, $\mathsf{o} < y$. If $\mathsf{o} < y$, then also $\mathsf{o} < y \lor y < \mathsf{o}$. We obtain: $y \neq \mathsf{o} \rightarrow (\mathsf{o} < y \lor y < \mathsf{o})$, which is equivalent to $(\mathsf{o} < y \lor y < \mathsf{o}) \lor y = \mathsf{o}$.

Now suppose we have

$$\mathbf{Q} \vdash \forall y\,((y < \overline{m} \lor \overline{m} < y) \lor y = \overline{m})$$

and we want to show

$$\mathbf{Q} \vdash \forall y\,((y < \overline{m+1} \lor \overline{m+1} < y) \lor y = \overline{m+1})$$

The first disjunct $y < \overline{m}$ is equivalent (by Q_8) to $\exists z\,(z' + y) = \overline{m}$. If $(z' + y) = \overline{m}$, then also $(z' + y)' = \overline{m}'$. By Q_4, $(z' + y)' = (z'' + y)$. Hence, $(z'' + y) = \overline{m}'$. We get $\exists u\,(u' + y) = \overline{m+1}$ by existentially generalizing on z' and keeping in mind that $\overline{m}'$ is $\overline{m+1}$. Hence, if $y < \overline{m}$ then $y < \overline{m+1}$.

Now suppose $\overline{m} < y$, i.e., $\exists z\,(z' + \overline{m}) = y$. By Q_3 and some logic, we have $z = \mathsf{o} \lor \exists u\, z = u'$. If $z = \mathsf{o}$, we have $(\mathsf{o}' + \overline{m}) = y$. Since $\mathbf{Q} \vdash (\mathsf{o}' + \overline{m}) = \overline{m+1}$, we have $y = \overline{m+1}$. Now suppose $\exists u\, z = u'$. Then:

$$\begin{aligned}
y &= (z' + \overline{m}) && \text{by assumption}\\
(z' + \overline{m}) &= (u'' + \overline{m}) && \text{from } z = u'\\
(u'' + \overline{m}) &= (u' + \overline{m})' && \text{by Lemma req.1}\\
(u' + \overline{m})' &= (u' + \overline{m}') && \text{by } Q_5\text{, so}\\
y &= (u' + \overline{m+1})
\end{aligned}$$

By existential generalization, $\exists u\, (u' + \overline{m+1}) = y$, i.e., $\overline{m+1} < y$. So, if $\overline{m} < y$, then $\overline{m+1} < y \lor y = \overline{m+1}$.

Finally, assume $y = \overline{m}$. Then, since $\mathbf{Q} \vdash (\mathsf{o}' + \overline{m}) = \overline{m+1}$, $(\mathsf{o}' + y) = \overline{m+1}$. From this we get $\exists z\, (z' + y) = \overline{m+1}$, or $y < \overline{m+1}$.

Hence, from each disjunct of the case for m, we can obtain the case for $m + 1$. □

inc:req:min: prop:rep-minimization

Proposition req.4. *If $\varphi_g(x, z, y)$ represents $g(x, y)$ in* $\mathbf{Q}$*, then*

$$\varphi_f(z, y) \equiv \varphi_g(y, z, \mathsf{o}) \land \forall w\, (w < y \to \neg\varphi_g(w, z, \mathsf{o})).$$

represents $f(z) = \mu x\, [g(x, z) = 0]$.

Proof. First we show that if $f(n) = m$, then $\mathbf{Q} \vdash \varphi_f(\overline{n}, \overline{m})$, i.e.,

$$\mathbf{Q} \vdash \varphi_g(\overline{m}, \overline{n}, \mathsf{o}) \land \forall w\, (w < \overline{m} \to \neg\varphi_g(w, \overline{n}, \mathsf{o})).$$

Since $\varphi_g(x, z, y)$ represents $g(x, z)$ and $g(m, n) = 0$ if $f(n) = m$, we have

$$\mathbf{Q} \vdash \varphi_g(\overline{m}, \overline{n}, \mathsf{o}).$$

If $f(n) = m$, then for every $k < m$, $g(k, n) \neq 0$. So

$$\mathbf{Q} \vdash \neg\varphi_g(\overline{k}, \overline{n}, \mathsf{o}).$$

We get that

inc:req:min: rep-less

$$\mathbf{Q} \vdash \forall w\, (w < \overline{m} \to \neg\varphi_g(w, \overline{n}, \mathsf{o})). \tag{6}$$

by Lemma req.2 (by (1) in case $m = 0$ and by (2) otherwise).

Now let's show that if $f(n) = m$, then $\mathbf{Q} \vdash \forall y\, (\varphi_f(\overline{n}, y) \to y = \overline{m})$. We again sketch the argument informally, leaving the formalization to the reader.

Suppose $\varphi_f(\overline{n}, y)$. From this we get (a) $\varphi_g(y, \overline{n}, \mathsf{o})$ and (b) $\forall w\, (w < y \to \neg\varphi_g(w, \overline{n}, \mathsf{o}))$. By Lemma req.3, $(y < \overline{m} \lor \overline{m} < y) \lor y = \overline{m}$. We'll show that both $y < \overline{m}$ and $\overline{m} < y$ leads to a contradiction.

If $\overline{m} < y$, then $\neg\varphi_g(\overline{m}, \overline{n}, \mathsf{o})$ from (b). But $m = f(n)$, so $g(m, n) = 0$, and so $\mathbf{Q} \vdash \varphi_g(\overline{m}, \overline{n}, \mathsf{o})$ since φ_g represents g. So we have a contradiction.

Now suppose $y < \overline{m}$. Then since $\mathbf{Q} \vdash \forall w\, (w < \overline{m} \to \neg\varphi_g(w, \overline{n}, \mathsf{o}))$ by eq. (6), we get $\neg\varphi_g(y, \overline{n}, \mathsf{o})$. This again contradicts (a). □

Photo Credits

Bibliography