Regular Minimization is Representable in $Q$

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:

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

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.

**Lemma req.1.** For every constant symbol $a$ and every natural number $n$,

$$Q \vdash (a^' + n) = (a + n)' .$$

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

1. $Q \vdash (a^' + 0) = a^'$ by axiom $Q_4$
2. $Q \vdash (a + 0) = a$ by axiom $Q_4$
3. $Q \vdash (a + 0)' = a'$ by eq. (2)
4. $Q \vdash (a^' + 0) = (a + 0)'$ by eq. (1) and eq. (3)

In the induction step, we can assume that we have shown that $Q \vdash (a^' + n) = (a + n)'$. Since $n+1$ is $n'$, we need to show that $Q$ proves $(a^' + n') = (a + n')'$. We have:

5. $Q \vdash (a^' + n') = (a + n')'$ by axiom $Q_5$
6. $Q \vdash (a + n')' = (a + n')'$ by eq. (4) and eq. (5).

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 $N$, $Q$ does not prove it.

**Lemma req.2.**

1. $Q \vdash \forall x \neg x < 0$.
2. For every natural number $n$,

$$Q \vdash \forall x (x < \overline{n + 1} \rightarrow (x = 0 \lor \cdots \lor x = n)).$$
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 $\neg \exists y (y' + a) = o$ in $Q$, which is equivalent (using the axioms and rules of first-order logic) to $\forall b (y' + a) \neq 0$. Here is the idea: suppose $(y' + b) = o$. If $a = o$, we have $(y' + o) = o$. But by axiom $Q_4$ of $Q$, we have $(b + o) = b'$, and by axiom $Q_2$ we have $b' \neq o$, a contradiction. So $\forall y (y' + a) \neq o$. If $a \neq o$, by axiom $Q_3$, there is a $c$ such that $a = c'$. But then we have $(b' + c') = 0$. By axiom $Q_5$, we have $(b' + c') = o$, 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 $a < 1 \rightarrow a = o$. Suppose $a < 1$. Then by the defining axiom for $<$, we have $\exists y (y' + a) = o'$.

Suppose $b$ has that property, i.e., we have $b' + a = o'$. We need to show $a = o$. By axiom $Q_3$, if $a \neq o$, we get $a = c'$ for some $z$. Then we have $(b' + c') = o'$. By axiom $Q_5$ of $Q$, we have $(b' + c') = o'$. By axiom $Q_1$, we have $(b' + c) = o$. But this means, by definition, $z < o$, contradicting part 1. \qed

Lemma req.3. For every $m \in \mathbb{N}$,

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

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

Now suppose we have

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

and we want to show

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

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

Now suppose $\overline{m} < b$, i.e., $\exists z (z' + \overline{m}) = b$. Suppose $c$ is such a $z$. By $Q_3$ and some logic, we have $c = o \lor \exists u c = u'$. If $c = o$, we have $(c + \overline{m}) = b$. Since $Q \vdash (o' + \overline{m}) = \overline{m + 1}$, we have $b = \overline{m + 1}$. Now suppose $\exists u c = u'$. Let $d$ be such a $u$. Then:

$$b = (c' + \overline{m}) \quad \text{by assumption}$$

$$(c' + \overline{m}) = (d'' + \overline{m}) \quad \text{from } c = d'$$

$$(d'' + \overline{m}) = (d' + \overline{m})' \quad \text{by Lemma req.1}$$

$$(d' + \overline{m})' = (d' + \overline{m})' \quad \text{by Lemma req.1}$$

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

Finally, assume \( b = \overline{m} \). Then, since \( Q \vdash (\alpha' + \overline{m}) = \overline{m + 1}, (\alpha' + b) = \overline{m + 1} \). From this we get \( \exists z (z' + b) = \overline{m + 1} \), or \( b < m + 1 \).

Hence, from each disjunct of the case for \( m \), we can obtain the case for \( m + 1 \).

\[ \square \]

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

\[ \varphi_f(z, y) \equiv \varphi_g(y, z, 0) \land \forall w (w < y \rightarrow \neg \varphi_g(w, z, 0)) \]

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

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

\[ Q \vdash \varphi_g(\overline{m}, \overline{n}, 0) \land \forall w (w < \overline{m} \rightarrow \neg \varphi_g(w, \overline{n}, 0)) \]

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

\[ Q \vdash \varphi_g(\overline{m}, \overline{n}, 0) \]

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

\[ Q \vdash \neg \varphi_g(\overline{k}, \overline{n}, 0) \]

We get that

\[ Q \vdash \forall w (w < \overline{m} \rightarrow \neg \varphi_g(w, \overline{n}, 0)) \] (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 \( Q \vdash \forall y (\varphi_f(y, y) \rightarrow y = \overline{n}) \). We again sketch the argument informally, leaving the formalization to the reader.

Suppose \( \varphi_f(\overline{n}, b) \). From this we get (a) \( \varphi_g(b, \overline{n}, 0) \) and (b) \( \forall w (w < b \rightarrow \neg \varphi_g(w, \overline{n}, 0)) \). By Lemma req.3, \( b < \overline{m} \lor \overline{m} < b \lor b = \overline{m} \). We’ll show that both \( b < \overline{m} \) and \( \overline{m} < b \) leads to a contradiction.

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

Now suppose \( b < \overline{m} \). Then since \( Q \vdash \forall w (w < \overline{m} \rightarrow \neg \varphi_g(w, \overline{n}, 0)) \) by eq. (6), we get \( \neg \varphi_g(b, \overline{n}, 0) \). This again contradicts (a).

\[ \square \]

**Photo Credits**

**Bibliography**