4.3. Some Existential Sentences.

In this section, we prove a crucial Lemma needed for section 4.4. We consider existential sentences of the following special form.

DEFINITION 4.3.1. Define $\lambda(k,n,m,R_1,\ldots,R_{n-1})$ =

$$(\exists \text{ infinite } B_1,\ldots,B_n \subseteq N^k)$$
$$(\forall i \in \{1,\ldots,n-1\})(\forall x_1,\ldots,x_m \in B_i)$$
$$(\exists y_1,\ldots,y_m \in B_{i+1})(R_i(x_1,\ldots,x_m,y_1,\ldots,y_m))$$

where $k,n,m \geq 1$, and $R_1,\ldots,R_{n-1} \subseteq N^{2km}$ are order invariant relations. Recall that order invariant sets of tuples are sets of tuples where membership depends only on the order type of a tuple.

Note the stratified structure of $\lambda(k,n,m,R_1,\ldots,R_{n-1})$. It asserts that there are n infinite sets such that for all elements of the first there are elements of the second with a property, and for all elements of the second there are elements of the third with a property, etcetera.

It is evident that even RCA_0 suffices to define truth for the sentences of the form $\lambda(k,n,m,R_1,\ldots,R_{n-1})$. For in RCA_0, we can

i. Appropriately code finite sequences of subsets of N^k as subsets of N.
ii. Appropriately code finite sequences of elements of N as elements of N.
iii. Appropriately treat order invariant sets of tuples from N.

This does not mean that we can form the set of all true sentences of the form $\lambda(k,n,m,R_1,\ldots,R_{n-1})$ in RCA_0 or even ACA'. However, we will show that this is in fact the case for ACA'. See Definition 1.4.1.

Specifically, we will present a primitive recursive criterion for the truth of sentences $\lambda(k,n,m,R_1,\ldots,R_{n-1})$, and prove that the criterion is correct, within the system ACA'.

We first put the sentences $\lambda(k,n,m,R_1,\ldots,R_{n-1})$ in substantially simpler form.

DEFINITION 4.3.2. Define $\lambda'(k,n,R_1,...,R_{n-1})$ =

$$(\exists \text{ infinite } B_1,...,B_n \subseteq N^k)$$
$$(\forall i \in \{1,...,n-1\})$$
$$(\forall x,y,z \in B_i)(\exists w \in B_{i+1})(R_i(x,y,z,w))$$

where $k,n \geq 1$, and $R_1,...,R_{n-1} \subseteq N^{4k}$ are order invariant relations.

LEMMA 4.3.1. There is a primitive recursive procedure for converting any sentence $\lambda(k,n,m,R_1,...,R_{n-1})$ to a sentence $\lambda'(k',n',S_1,...,S_{n'-1})$ with the same truth value. In fact, ACA' proves that any $\lambda(k,n,m,R_1,...,R_{n-1})$ has the same truth value as its conversion $\lambda'(k',n',S_1,...,S_{n'-1})$.

Proof: Start with

*) $(\exists \text{ infinite } B_1,...,B_n \subseteq N^k)(\forall i \in \{1,...,n-1\})$
$(\forall x_1,...,x_m \in B_i)(\exists y_1,...,y_m \in B_{i+1})(R_i(x_1,...,x_m,y_1,...,y_m))$.

Let $C,D \subseteq N^{km}$. We think of C,D as sets of m-tuples from N^k. We write $C\# \subseteq N^k$ for the set of all k-tuple components of elements of C.

We write $C \leq D$ if and only if $C,D \subseteq N^{km}$, and for all $(x_1,...,x_m),(y_1,...,y_m),(z_1,...,z_m) \in C$,

i. If $(x_1,...,x_m) = (y_1,...,y_m) = (z_1,...,z_m)$ then $(x_1,...,x_m) \in D$.
ii. If $(x_1,...,x_m),(y_1,...,y_m),(z_1,...,z_m)$ are distinct then $(x_2,...,x_m,x_1) \in D$.
iii. If $(x_1,...,x_m) \neq (y_1,...,y_m) = (z_1,...,z_m)$ then $(x_1,y_1,...,y_{m-1}) \in D$.
iv. If $(x_1,...,x_m) = (y_1,...,y_m) \neq (z_1,...,z_m)$ then $(x_1,y_1,...,y_{m-1}) \in D$.

We claim that if C_1 has at least three elements and $C_1 \leq ... \leq C_{2m}$, then $C_1\#^m \subseteq C_{2m} \subseteq N^{km}$. To see this, let $C_1,...,C_{2m}$ be as given. By i), $C_1 \subseteq ... \subseteq C_{2m}$. By ii), $(x_1,...,x_m) \in C_1 \rightarrow (x_2,...,x_m,x_1) \in C_2$. We can continue for m steps, obtaining that for all $(x_1,...,x_m) \in C_1$, all m rotations of $(x_1,...,x_m)$ lie in C_m.

It follows that every $\alpha \in C_1\#^m$ is the sequence of first terms of some $\beta_1,...,\beta_m \in C_m$. (Here α is an m tuple from $C_1\#$ and $\beta_1,...,\beta_m$ are m tuples from C_m). By iii,iv, we can replace the first term of β_m by the first term of β_{m-1}, and shift the remaining terms of β_m to the right, removing the last term of β_m, with the resulting m tuple β' starting with the first term of β_{m-1} followed by the first term of β_m. Thus $\beta' \in C_{m+1}$. At the second stage, we can use β_{m-2} and β' to form $\beta'' \in C_{m+2}$. We continue this process until we finally use β_1, to arrive at $\alpha \in C_{2m}$.

We now claim that *) is equivalent to

**) $(\exists$ infinite $C_1,\ldots,C_{2nm} \subseteq N^{km})(C_1 \leq \ldots \leq C_{2m} \wedge C_{2m+1} \leq \ldots \leq C_{4m} \wedge \ldots \wedge C_{2nm-2m+1} \leq \ldots \leq C_{2nm} \wedge (\forall i \in \{1,\ldots,n-1\})$ $(\forall x \in C_{2im})(\exists y \in C_{2im+1})(R_i(x,y)))$.

To see this, let $B_1,\ldots,B_n$ witness *). Set

$$C_1 = \ldots = C_{2m} = B_1{}^m$$
$$\ldots$$
$$C_{2nm-2m+1} = \ldots = C_{2nm} = B_n{}^m.$$

Clearly

$$C_1 \leq \ldots \leq C_{2m}$$
$$\ldots$$
$$C_{2nm-2m+1} \leq \ldots \leq C_{2nm}.$$

Conversely, let $C_1,\ldots,C_{2nm}$ witness **). Since $C_1,\ldots,C_{2nm}$ are infinite, we see that $C_1\#^m \subseteq C_{2m} \wedge \ldots \wedge C_{2nm-2m+1}\#^m \subseteq C_{2nm}$. For all $1 \leq i \leq n$, set $B_i = C_{2(i-1)m+1}\#$. Then these B's witness *).

It is easy to see that **) is a sentence of the form $\lambda'(k',n',S_1,\ldots,S_{n'-1})$. The relations in **) between successive $C_1,\ldots,C_{2m}$, and between successive $C_{2m+1},\ldots,C_{4m}$, etcetera, are of the form $\forall\forall\forall\exists$ according to the definition of $\leq$. The relations in **) between C_{2m},C_{2m+1}, and between C_{4m},C_{4m+1}, etcetera, are of the form $\forall\exists$. QED

We now define sets $Y_1,\ldots,Y_n$ by

i. $Y_1 = N$.
ii. For $1 \leq i < n$, $Y_{i+1} = Y_i \times Y_i \times Y_i \times Y_i$.

LEMMA 4.3.2. A sentence $\lambda'(k,n,R_1,\ldots,R_{n-1})$ holds if and only if there exist functions $f_i:Y_i \to N^k$, $1 \leq i \leq n$, such that the following holds.
i. f_1 is one-one.
ii. For all $1 \leq i \leq n$ and $x,y,z \in Y_i$, $f_i(x,y,z,w)$ as a function of $w \in Y_i$, is one-one.

iii. For all $1 \leq i < n$ and $x,y,z \in Y_i$, $R_i(f_i(x),f_i(y),f_i(z),f_{i+1}(x,y,z,z))$.

Proof: Let $\lambda'(k,n,R_1,...,R_{n-1})$ be given. Suppose $\lambda'(k,n,R_1,...,R_{n-1})$ is true. Let $B_1,...,B_n \subseteq N^k$ be infinite, where for all $1 \leq i < n$, $(\forall x,y,z \in B_i)(\exists w \in B_{i+1})(R_i(x,y,z))$.

We now define $f_1,...,f_n$ inductively as follows. Let $f_1:N \to B_1$ be a bijection. Suppose surjective $f_i:Y_i \to B_i$ has been defined, $1 \leq i < n$. To define $f_{i+1}:Y_{i+1} \to B_{i+1}$, let $x,y,z \in Y_i$. Since $f_i(x),f_i(y),f_i(z) \in B_i$, set $f_{i+1}(x,y,z,z) \in B_{i+1}$ to be such that $R_i(f_i(x),f_i(y),f_i(z),f_{i+1}(x,y,z,z))$. Define $f_{i+1}(x,y,z,w)$, $w \in Y_i$, $w \neq z$, so that $f_{i+1}(x,y,z,w)$ is a bijection from Y_{i+1} onto B_{i+1} as a function of w.

Conversely, let $f_i:Y_i \to N^k$, $1 \leq i \leq n$, be such that i)-iii) above hold. For all $1 \leq i \leq n$, let $B_i = \mathrm{rng}(f_i)$. Then each B_i is infinite. Let $1 \leq i < n$ and $u,v,w \in B_i$. Let $u = f_i(x)$, $v = f_i(y)$, $w = f_i(z)$, where $x,y,z \in Y_i$. Then $R_i(u,v,w,f_{i+1}(x,y,z,z))$. Since $f_{i+1}(x,y,z,z) \in B_{i+1}$, we are done. QED

We can use Lemma 4.3.2 to convert $\lambda'(k,n,R_1,...,R_{n-1})$ into a sentence of a rather simple form.

DEFINITION 4.3.3. Define $\mu(p,q,\varphi)$ =

$$(\exists f:N^p \to N)(\forall x_1,...,x_q \in N)(\varphi)$$

where φ is a propositional combination of atomic formulas of the forms $x_i < x_j$, $f(y_1,...,y_p) < f(z_1,...,z_p)$, where $x_i,x_j,y_1,...,y_p,z_1,...,z_p$ are among the (distinct) variables $x_1,...,x_q$.

LEMMA 4.3.3. There is a primitive recursive procedure for converting any sentence $\lambda'(k,n,S_1,...,S_{n-1})$ to a sentence $\mu(p,q,\varphi)$, with the same truth value. In fact, ACA′ proves that any $\lambda'(k,n,S_1,...,S_{n-1})$ has the same truth value as its conversion $\mu(p,q,\varphi)$.

Proof: We use Lemma 4.3.2. We can obviously identify each Y_i with $N^{4\wedge(i-1)}$. Then the condition in Lemma 4.3.2 takes the following form: there exists a definite finite number of functions from various Cartesian powers of N into N^k such that a universally quantified statement (quantifiers in N) holds whose matrix is a propositional combination of numerical comparisons, either between integer variables, or designated coordinates of values (which lie in N^k) of the functions at tuples of variables. This is clear by examining clauses i) - iii) in Lemma 4.3.2, and noting that the S_i are order invariant.

The use of N^k as a range here can be eliminated in favor of using more functions from various Cartesian powers of N into N. Thus we obtain an equivalent of the following form: there exists a definite finite number of functions from various Cartesian powers of N into N such that a universally quantified statement holds whose matrix is a propositional combination of numerical comparisons, either between integer variables, or values of the functions at tuples of variables.

By adding dummy variables, we can assume that all of the functions have the same arity. Thus we have

$$*)\quad (\exists f_1,\ldots,f_r:N^p \rightarrow N)(\forall x_1,\ldots,x_q \in N)(\varphi)$$

where φ is a propositional combination of atomic formulas of the forms $x_i < x_j$, $f_a(y_1,\ldots,y_p) < f_b(z_1,\ldots,z_p)$, where $x_i,x_j,y_1,\ldots,y_p,z_1,\ldots,z_p$ are among the (distinct) variables $x_1,\ldots,x_q$. It remains to reduce this to quantification over a single function.

The idea is to introduce a single function variable $f:N^{p+r} \rightarrow N$ which does the work of $f_1,\ldots,f_r$ in a sufficiently explicit way. We say that f is special if and only if for all distinct $c,d \in N$, $f(y_1,\ldots,y_p,c,\ldots,c,d,\ldots,d)$ depends only on $y_1,\ldots,y_p$ and the number of c's displayed (which is from 1 to r), and not what integers c,d are (as long as $c \neq d$).

It is now clear that *) is equivalent to

$$**)\quad (\exists f:N^{p+r} \rightarrow N)(\forall u,v \in N)(\forall x_1,\ldots,x_p \in N)$$
$$(f \text{ is special} \wedge (u \neq v \rightarrow \varphi'))$$

where φ' is obtained from φ by replacing each $f_i(y_1,\ldots,y_p)$ in *) by $f(y_1,\ldots,y_p,u,\ldots,u,v,\ldots,v)$, where the number of u's displayed is i. QED

We now prove a combinatorial lemma.

DEFINITION 4.3.4. Let $f:N^p \to N$ and $A \subseteq N$. We say that A is an SOI for f if and only if the truth value of any statement

$$f(x_1,\ldots,x_p) < f(y_1,\ldots,y_p)$$

where $x_1,\ldots,x_p,y_1,\ldots,y_p \in A$, depends only on the order type of the 2p-tuple $(x_1,\ldots,x_p,y_1,\ldots,y_p)$.

DEFINITION 4.3.5. We say that A is a strong SOI for f if and only if A is an SOI for f such that the following holds. Let $x_1,\ldots,x_p,y_1,\ldots,y_p \in A$. Suppose $(x_1,\ldots,x_p)$ and $(y_1,\ldots,y_p)$ have the same order type. Suppose also that for all $1 \leq i \leq p$, $x_i = y_i \vee y_i > \max(x_1,\ldots,x_p)$. Then $f(x_1,\ldots,x_p) \leq f(y_1,\ldots,y_p)$;

DEFINITION 4.3.6. We say that A is a special SOI for f if and only if A is a strong SOI for f such that the following holds. Let $x1,\ldots,xp,y1,\ldots,yp \in A$. Suppose $(x_1,\ldots,x_p)$ and $(y_1,\ldots,y_p)$ have the same order type. Suppose also that for all $1 \leq i \leq p$, $x_i = y_i \vee y_i > \max(x_1,\ldots,x_p)$. If $f(x_1,\ldots,x_p) < f(y_1,\ldots,y_p)$ then $f(y_1,\ldots,y_p)$ is greater than all $f(z_1,\ldots,z_p)$, with $|z_1,\ldots,z_p| \leq |x_1,\ldots,x_p|$.

The above definitions makes perfectly good sense for functions $f:A^p \to N$ where A is finite. In this finite context, we will be particularly interested in the case $A = [0,q]$.

LEMMA 4.3.4. The following is provable in ACA'. For all $p \geq 1$, every $f:N^p \to N$ has an infinite special SOI $A \subseteq N$. In fact, every infinite SOI for $f:N^p \to N$ is a special SOI for f.

Proof: Let $f:N^p \to N$. By the infinite Ramsey theorem for 2p-tuples, let $A \subseteq N$ be an infinite SOI for f. We now show that A is a special SOI for f.

Let $x_1,\ldots,x_p,y_1,\ldots,y_p \in A$. Suppose $x = (x_1,\ldots,x_p)$ and $y = (y_1,\ldots,y_p)$ have the same order type, and for all $1 \leq i \leq p$, $x_i = y_i \vee y_i > \max(x_1,\ldots,x_p)$.

Suppose $x \neq y$. We claim that x,y are the first two terms of an infinite sequence of elements of N^p, written $x,y,w_1,w_2,\ldots$, such that the order types of (x,y), (y,w_1), (w_1,w_2), ..., are the same. To see this, let $x_1' < \ldots < x_i'$ and $y_1' < \ldots < y_j'$ be the strictly increasing enumeration of the terms of $(x_1,...,x_p)$ and $(y_1,...,y_p)$, respectively. Since $(x_1,...,x_p)$ and $(y_1,...,y_p)$ have the same order type, i = j. It is also clear that for the least k such that $x_k' \neq y_k'$, we have $y_k' > x_i'$. Now choose w_1 of the same order type as x,y so that its strictly increasing enumeration starts with the same $x_1' < ... < x_{k-1}'$ and continues higher than y_i'. Then obviously (x,y) and (y,w_1) have the same order type. Continue in this way indefinitely.

Now suppose f(x) > f(y). Then $x \neq y$ and we can use the $x,y,w_1,w_2,...$ constructed in the previous paragraph. Since A is an SOI for f, if f(x) > f(y) then $f(x) > f(y) > f(w_1) > f(w_2) ...$, which is impossible. Hence $f(x) \leq f(y)$.

Finally, suppose f(x) < f(y), and let $z \in [0,\max(x)]^p$. Since $x \neq y$, we can use the $x,y,w_1,w_2,...$ constructed previously. Note that the pairs $(y,z),(w_1,z),(w_2,z)$, ... all have the same order type. Suppose $f(y) \leq f(z)$. Since A is an SOI for f, we see that each $f(w_i) \leq f(z)$. Also since A is an SOI for f and f(x) < f(y), we have that each $f(w_i) < f(w_{i+1})$, and therefore the $f(w_i)$ are unbounded. This is a contradiction. QED

LEMMA 4.3.5. The following is provable in ACA'. Let $q \geq 3p \geq 1$, and $f:[0,q]^p \to N$. Assume [0,q] is a special SOI for f. There exists $g:N^p \to N$ such that N is a special SOI for g, where for all $x,y \in [0,q]^p$, $f(x) \leq f(y) \leftrightarrow g(x) \leq g(y)$.

Proof: Let p,q,f be as given. We now put a relation $\leq^*$ on N^p as follows. Let $x,y \in N^p$. Then $x \leq^* y$ if and only if there exists $\alpha,\beta \in [0,q]^p$ such that

i. (x,y) and (α,β) have the same order type.
ii. $f(\alpha) \leq f(\beta)$.

Since [0,q] is an SOI for f, we have that $x \leq y^*$ if and only if

for all $\alpha,\beta \in [0,q]^p$, if (x,y) and (α,β) have the same order type then $f(\alpha) \leq f(\beta)$.

Since $q \geq 2p$, every element of N^{2p} is of the same order type as an element of $[0,q]^{2p}$. Hence $\leq^*$ is reflexive and connected.

To see that $\leq^*$ is transitive, let $x \leq^* y \wedge y \leq^* z$. Let $a_1 < \ldots < a_r$ be an enumeration of the combined coordinates of x,y,z. Clearly $1 \leq r \leq 3p \leq q$. Let (x,y,z) have the same order type as $(\alpha,\beta,\gamma) \in [0,q]^{3p}$. Then $f(\alpha) \leq f(\beta)$ and $f(\beta) \leq f(\gamma)$. Hence $f(\alpha) \leq f(\gamma)$ and $(x,z),(\alpha,\gamma)$ have the same order type. Therefore $x \leq^* z$.

It is standard to define the equivalence relation of $\leq^*$ by $x =^* y \leftrightarrow (x \leq^* y \wedge y \leq^* x)$. This is obviously equivalent to the existence of $\alpha,\beta \in [0,q]^p$ such that $(x,y),(\alpha,\beta)$ have the same order type and $f(\alpha) = f(\beta)$. This is also equivalent to: for all $\alpha,\beta \in [0,q]^p$, if (x,y) and (α,β) have the same order type then $f(\alpha) = f(\beta)$.

We now show that the order type of $\leq^*$, modulo its equivalence relation $=^*$, is finite or ω.

We first verify that $\leq^*$ is well founded. Suppose $x_1 >^* x_2 >^* \ldots$. Apply Ramsey's theorem to the comparison of the b-th coordinate of x_i with the b-th coordinate of x_j, $b = 1,\ldots,p$. Then we obtain an infinite subsequence $y_1 >^* y_2 >^* \ldots$ such that for all $1 \leq b \leq p$, either the b-th coordinates of the y's are constant, or strictly increasing. We can then pass to an infinite subsequence $z_1 >^* z_2 >^* \ldots$ such that for all $i < j$, the p-tuples z_i,z_j satisfy the hypotheses in the definition of strong SOI. Let (z_1,z_2) and (α,β) have the same order type, where $\alpha,\beta \in [0,q]^p$. Then α,β satisfy the hypotheses in the definition of strong SOI. Therefore $f(\alpha) \leq^* f(\beta)$, and hence $z_1 \leq^* z_2$. This is a contradiction.

We now verify that $\leq^*$ has no limit points. Suppose $y_1 <^* y_2 \ldots <^* x$. As before, pass to an infinite subsequence $z_1 <^* z_2 \ldots <^* x$, such that for all $i < j$ the p-tuples z_i,z_j satisfy the hypotheses in the definition of strong SOI. Choose $z_i <^* z_{i+1}$ such that $\max(z_i) > \max(x)$. Let $\alpha,\beta,\gamma \in [0,q]^p$, where (α,β,γ) and (x,z_i,z_{i+1}) have the same order type. Then β,γ satisfy the hypotheses in the definition of special SOI. Also $f(\beta) < f(\gamma)$ and $|\alpha| < |\beta|$. Since $[0,q]$ is a special SOI for f, $f(\gamma) > f(\alpha)$. Hence $z_{i+1} >^* x$. This is a contradiction.

So we have now shown that the order type of $\leq^*$ is finite or ω. Note that $\leq^*$ is order invariant. Hence $=^*$, $<^*$ are also order invariant.

We define $g:N^p \to N$ by: $g(x)$ is the position of x in the ordering $\leq^*$, counting from 0. Obviously N is an SOI for g, since $<^*$ is order invariant. Hence by Lemma 4.3.4, N is a special SOI for g.

For the final claim of Lemma 4.3.5, let $x,y \in [0,q]^p$. Suppose $f(x) \leq f(y)$. Then $x \leq^* y$, and hence $g(x) \leq g(y)$. Suppose $g(x) \leq g(y)$. Then $x \leq^* y$. Let (x,y) and (α,β) have the same order type, $\alpha,\beta \in [0,q]^p$, where $f(\alpha) \leq f(\beta)$. Then $f(x) \leq f(y)$. QED

LEMMA 4.3.6. The following is provable in ACA'. Let $q \geq 3p \geq 1$, and $f:[0,q]^p \to N$. Assume $[0,q]$ is a special SOI for f. Let $g:N^p \to N$ be such that N is a special SOI for g, where for all $x,y \in [0,q]^p$, $f(x) \leq f(y) \leftrightarrow g(x) \leq g(y)$. Then $\mu(p,q,\varphi)$ holds with f, where the universal quantifiers are restricted to $[0,q]$, if and only if $\mu(p,q,\varphi)$ holds with g.

Proof: Let p,q,f,g, and $\mu(p,q,\varphi)$ be as given. Assume $\mu(p,q,\varphi)$ holds with f, where the universal quantifiers are restricted to $[0,q]$.

Suppose $\mu(p,q,\varphi)$ fails with g. Let $x_1,\ldots,x_q \in N$ be a counterexample to $\mu(p,q,\varphi)$ with g.

We claim that we can push this counterexample down to lie within $[0,q]$, by merely choosing $x_1',\ldots,x_q' \in [0,q]$ such that $(x_1',\ldots,x_q')$ and $(x_1,\ldots,x_q)$ have the same order type. The reason is that φ is a propositional combination of formulas of the forms

$$y < z$$
$$f(y_1,\ldots,y_q) < f(z_1,\ldots,z_q)$$

where $y,z,y_1,\ldots,y_q,z_1,\ldots,z_q$ are among the variables $x_1,\ldots,x_q$. Using the fact that N is a special SOI for g, the above inequalities have the same truth values as the inequalities

$$y' < z'$$
$$f(y_1',\ldots,y_q') < f(z_1',\ldots,z_q').$$

By hypothesis, we can now replace f by g in φ with $x_1',\ldots,x_q' \in [0,q]$, obtaining $\neg\mu(p,q,\varphi)$ with g.

Conversely, suppose $\mu(p,q,\varphi)$ fails with f. Let $x_1,\ldots,x_q \in [0,q]$ be a counterexample to $\mu(p,q,\varphi)$ with f. Then by the same argument, $x_1,\ldots,x_q$ is a counterexample to $\mu(p,q,\varphi)$ with g.

It is worth noting that this argument would fail if we allowed inequalities of the form $u < f(v_1,\ldots,v_q)$ in φ. Thus the restriction on φ is important. QED

LEMMA 4.3.7. The following is provable in ACA'. A sentence $\mu(p,q,\varphi)$, $q \geq 3p$, holds if and only if there exists $f:[0,q]^p \to [0,(q+1)^p]$ such that $[0,q]$ is a special SOI for f, and φ holds for f (with universal quantifiers ranging over $[0,q]$).

Proof: Let $\mu(p,q,\varphi)$ be given, $q \geq 3p$. Let $f:[0,q]^p \to [0,(q+1)^p]$, where $[0,q]$ is a special SOI for f, and $\mu(p,q,\varphi)$ holds with f, with universal quantifiers restricted to $[0,q]$. Let g be as given by Lemma 4.3.5. By Lemma 4.3.6, $\mu(p,q,\varphi)$ holds with g. In particular, $\mu(p,q,\varphi)$ holds.

Conversely, let $\mu(p,q,\varphi)$ hold with $g:N^p \to N$. By Lemma 4.3.4, let $A \subseteq N$ be a special SOI for g of cardinality q+1. Then $\mu(p,q,\varphi)$ holds for g with universal quantifiers restricted to A. Note that $g|A^p$ is isomorphic to a unique $f:[0,q]^p \to N$ by the unique increasing bijection h from A onto $[0,q]$. (Here the isomorphism h acts only on the domains, and so only provides the transfer of statements of the form $f(x_1,\ldots,x_p)\ \tau\ f(y_1,\ldots,y_p)$ to $g(h(x_1),\ldots,h(x_p))\ \tau\ g(h(y_1),\ldots,h(y_p))$, where $\tau \in \{\leq,<,=\}$). Hence $\mu(p,q,\varphi)$ holds with f.

Now A is a special SOI for $g|A^p$. We now show that $[0,q]$ is a special SOI for f. By the isomorphism h from $g|A^p$ onto f, clearly $[0,q]$ is a strong SOI for f. Now let $(x_1,\ldots,x_p)$ and $(y_1,\ldots,y_p)$ from $[0,q]^p$ have the same order type. Suppose also that for all $1 \leq i \leq p$, $x_i = y_i \vee y_i > \max(x_1,\ldots,x_p)$. Suppose

$$1)\ f(x_1,\ldots,x_p) < f(y_1,\ldots,y_p)$$
$$|z_1,\ldots,z_p| \leq |x_1,\ldots,x_p|.$$

We must show that $f(y_1,\ldots,y_p) > f(z_1,\ldots,z_p)$. Since $|z_1,\ldots,z_p| \leq q$, we can take h^{-1} throughout 1), and then apply that A is a special SOI for $g|A^p$.

Note that we can obviously arrange that $\mathrm{rng}(f) \subseteq [0,(q+1)^p]$ by counting. QED

THEOREM 4.3.8. There is a presentation of a primitive recursive function h such that the following holds. ACA′ proves that $\lambda(k,n,m,R_1,...,R_{n-1})$ is true if and only if $h(k,n,m,R_1,...,R_{n-1}) = 1$.

Proof: Start with $\lambda(k,n,m,R_1,...,R_{n-1})$. Pass to $\lambda'(k',n',S_1,...,S_{n'-1})$ by Lemma 4.3.1. Pass to $\mu(p,q,\varphi)$, $q \geq 3p$, by Lemma 4.3.3. Now apply Lemma 4.3.7. QED