arXiv:1509.09209v1 [math.LO] 30 Sep 2015

Inconsistency of Primitive Recursive Arithmetic

Edward Nelson

With an

Introduction by Sarah Jones Nelson

and an

Afterword by Sam Buss and Terence Tao

Introduction

In September of 2011 Edward Nelson announced that he had a proof of the inconsistency of Peano Arithmetic. He had devoted twenty-five years to constructing the proof. When Terence Tao and Daniel Tausk independently found an error, Ed withdrew his claim at once and cheerfully returned to work on it the next day. By March of 2013 – confident that he had corrected the error – he wrote a project proposal with "a crucial new insight: technically, bounds in the Hilbert-Ackermann consistency theorem depending only on rank and level, but not on the length of the proof." The project he proposed "challenges the entire current understanding and practice of mathematics....It will radically change the way mathematics is done. This will affect the philosophy of mathematics, how the nature of mathematics is conceived. It will also affect the sciences that use mathematics, especially physics....It addresses a very big question: does mathematics consist in the discovery of truths about some uncreated eternal reality (the traditional Platonic view), or is it a humble human endeavor to construct abstract patterns that will be sound, free of all contradiction, in the hope that some will be beautiful, uplifting the human spirit, and that some (not necessarily different ones) will be of practical use to improve the human lot?"

The following excerpts from Ed's proposal describe his vision of a new mathematics and the open question of the consistency of Peano Arithmetic.

"Peano Arithmetic is one of the simplest and most fundamental of mathematical theories. Its consistency, however, has not been proved by any means that all mathematicians accept. It implies that all primitive recursive functions are total, but they are directly defined only for numerals, and the argument that the values always reduce to numerals is circular. The proposal is to complete a proof that Peano Arithmetic is in fact inconsistent. The principal output will be a book entitled 'Elements'. The outcome will be a major change in the way mathematics is done, with philosophical and scientific consequences.

"The guiding spirit of this investigation is that mathematics is not some uncreated abstract reality that we can take for granted and explore, but that it is a human endeavor in which one should begin by looking at the very simplest concepts without taking them for granted.

"Numbers are constructed from 0 by successively taking successors; $\mathrm{S}\ldots\mathrm{S}0$ is called a numeral. Definitions of primitive recursive functions, such as addition, multiplication, exponentiation, superexponentiation, and so forth, are schemata for constructing numerals. They define a value for 0 and then a value for $\mathrm{S}x$ in terms of the value for x. But when numerals are substituted for the variables in such a schema it is not clear that it defines a numeral: the putative number of steps

needed to apply the definitions can only be expressed in terms of the expressions themselves. The argument is a vicious circle. Consequently, the consistency of Primitive Recursive Arithmetic, and *a fortiori* of Peano Arithmetic (P), is an open question.

"Here is a nontechnical description of how I propose to show that P is inconsistent. We start with a weaker theory Q and by relativization techniques extend it to a stronger theory Q^*. Proofs in Q^* reduce to proofs in Q. Q^* arithmetizes Q itself – that is, it expresses the syntax of Q by a term of Q^* that here I shall denote by @Q. Remarkably, Q^* proves that there is no open proof of a contradiction in @Q. ('Open' means that the proof has no quantifiers, i.e., symbols for 'there exists' and 'for all'.) All of this was done in my book 'Predicative Arithmetic' (Princeton University Press, 1986) and is being redone with complete proofs in the book 'Elements', a work in progress that is the subject of this proposal. The Hilbert-Ackermann consistency theorem implies that there is no proof of a contradiction, even with quantifiers, in @Q. This theorem can be only partially established in Q^*. The crucial new insight is that it can be proved provided there are bounds on features of the proof (called rank and level) but emphatically not depending on the length of the proof. These bounds on rank and level cannot be proved in Q^*, but for each specific proof, P proves that Q^* proves them! This opens the way to exploit the stunning proof without self-reference of Gödel's second incompleteness theorem by Kritchman and Raz (Notices of the American Mathematical Society, December 2011). The upshot is that P proves that Q is inconsistent. But, as is well known, P also proves that Q is consistent. Therefore Peano Arithmetic P is inconsistent."

Ed was the only living mathematician who could argue from purely syntactic reasoning without the traditional semantics established by Plato. John Conway suggested to me that this might explain why no one has fully understood Ed's deeply unique insights into the foundations of contemporary mathematics. He stood alone in the world, courageous as a formalist of a new ontology of integers: proof that completed infinities do not exist and that human minds invented numbers never discovered or revealed from platonic forms of any fundamental reality. I am hopeful that the mathematical community will boldly investigate "Elements" and the unshakeable foundations Ed sought to build.

Sarah Jones Nelson

September 10, 2015

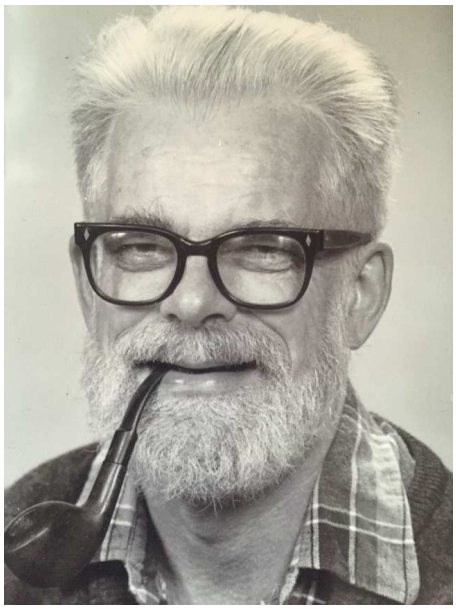

Photo courtesy Sarah Jones Nelson

Edward Nelson

Inconsistency of Primitive Recursive Arithmetic

Edward Nelson

1. Against finitism

Primitive Recursive Arithmetic (PRA) was invented by Skolem [Sk] in response to *Principia Mathematica* with the express purpose of avoiding quantification over infinite domains. His tools were primitive recursion and induction.

Familiar examples of primitive recursions are

$$\begin{aligned} x + 0 &= x \\ x + \mathrm{S}y &= \mathrm{S}(x + y) \\ x \cdot 0 &= 0 \\ x \cdot \mathrm{S}y &= x + (x \cdot y) \\ x \uparrow 0 &= \mathrm{S0} \\ x \uparrow \mathrm{S}y &= x \cdot (x \uparrow y) \\ x \Uparrow 0 &= \mathrm{S0} \\ x \Uparrow \mathrm{S}y &= x \uparrow (x \Uparrow y) \end{aligned}$$

A numeral is a term containing only S and 0, and a primitive recursive (PR) number is a variable-free term all of whose function symbols are PR. The finitary credo is that PR numbers reduce to numerals by applying the equations a sufficient number of times. If indeed that were so, the applications used could be counted by a numeral. But in general the number of applications needed can be expressed only in terms of PR numbers themselves—the argument is blatantly circular.

The objection being raised here is not some vague semantic "ultrafinitistic" assertion that some PR numbers are so big they don't really exist. Certainly the PR number $\mathrm{SS0} \Uparrow \mathrm{SSSSSS0}$ exists: here it is, in front of our eyes, consisting of eleven symbols. The problem is syntactical. Let A be a formula that holds for 0 and is such that whenever it holds for x it holds for $\mathrm{S}x$. Then A holds for any numeral n; this follows from the basis $\mathrm{A}_x(0)$ by modus ponens applied as many times as there are occurrences of S in n. But the postulation of induction, implying that A holds for every PR number, is an expression of the finitary credo.

PRA is a boldly speculative attempt to treat PR numbers as if they were equal to numerals. We shall see that it is inconsistent.

2. Outline

The next section describes the notational and terminological conventions used in this paper (including the present outline) and formulates PRA as a formal system. Section 4 explicitly defines a binary function symbol Eq such that $\vdash \mathrm{Eq}(x, y) = 0 \leftrightarrow x = y$ and §5 introduces bounded quantifiers. Section 6 introduces strings and their combinatorics, and §7 uses them to formulate arithmetization. Section 8 establishes a form of Chaitin's

theorem [Ch]. The heart of the paper is §9, which constructs a subsystem of PRA that proves the consistency of its own arithmetization. The final §10 exploits the method of the Kritchman-Raz proof www.ams.org/notices/201011/rtx101101454p.pdf, based on Chaitin's theorem and the surprise examination paradox, together with the self-consistency result of §9, to derive a contradiction in PRA.

Numbered and italicized steps occur throughout the paper to serve as a fuller outline.

3. The formal system PRA

#1. Formulate the axioms and rules of inference of PRA.

The *symbols* of PRA are *variables*, *function symbols*, =, ¬, and ∨. A "decorated letter" is a letter with zero or more digits as subscript and zero or more primes as superscript. We use decorated s to stand for symbols. Decorated italic letters are variables, and decorated x y z w stand for variables. An *expression* is a concatenation of symbols; decorated u v stand for expressions, f g h for function symbols. Each symbol s has an *index* (or arity), denoted by ιs, specifying how many arguments it takes. A symbol is 0-ary, unary, binary, and so forth, according as its index is 0, 1, 2, and so forth. A *constant* is a 0-ary function symbol; decorated e stands for constants. Variables are 0-ary, ¬ is unary, = and ∨ are binary. *Terms* are defined recursively as follows: x is a term; if $\mathrm{u}_1, \ldots, \mathrm{u}_{\iota \mathrm{f}}$ are terms then $\mathrm{f}\mathrm{u}_1 \ldots \mathrm{u}_{\iota \mathrm{f}}$ is a term. Decorated a b c d stand for terms. An *equation* is =ab. *Formulas* are defined recursively as follows: equations are formulas; if u and v are formulas, so are ¬u and ∨uv. (There are no quantifiers in PRA.) Decorated A B C D H stand for formulas. We frequently use infix notation for binary symbols; thus a = b abbreviates =ab and A∨B abbreviates ∨AB. The use of infix notation often requires groupers to avoid ambiguity; we use parentheses to group terms, and brackets and braces to group formulas. Some other useful abbreviations are A & B for ¬[¬A ∨ ¬B], A → B for ¬A ∨ B, and A ↔ B for [¬A ∨ B] & [A ∨ ¬B]. The symbol ¬ binds tightly, and ∨ and & bind more tightly than → and ↔. Apart from these precedence rules, infix symbols are associated from right to left. Function symbols are *nonlogical symbols*.

If ℓ is a decorated letter, $\vec{\ell}$ abbreviates $\ell_1 \ldots \ell_\mu$ for some μ called the *multiplicity* of $\vec{\ell}$ and denoted by $\mu\vec{\ell}$. The notation a ≠ b abbreviates ¬ a = b. Let $\mathrm{u}_{\vec{\mathrm{x}}}(\vec{\mathrm{a}})$, where $\mu\vec{\mathrm{x}} = \mu\vec{\mathrm{a}}$, be the expression, called an *instance* of u, obtained by replacing each occurrence of x_ν in u by a_ν, for all ν with $1 \le \nu \le \mu\vec{\mathrm{x}}$. Whenever we write $\mathrm{u}_{\vec{\mathrm{x}}}(\vec{\mathrm{a}})$ it is understood that $\mu\vec{\mathrm{x}} = \mu\vec{\mathrm{a}}$.

Sometimes parentheses and commas are inserted into terms to enhance readability. Although $\mathrm{A}_\mathrm{x}(\mathrm{x})$ and A are the same, the redundant notation $\mathrm{A}_\mathrm{x}(\mathrm{x})$ often increases readability.

A *truth valuation* on A is a function τ from the equations in A to $\{\mathsf{T}, \mathsf{F}\}$. We extend τ to all subformulas of A, keeping the notation τ, by letting $\tau(\neg\mathrm{B})$ be T if and only if $\tau(\mathrm{B})$ is F, and letting $\tau(\mathrm{B} \vee \mathrm{C})$ be T if and only if $\tau(\mathrm{B})$ is T or $\tau(\mathrm{C})$ is T. A *tautology* is a formula A such that $\tau(\mathrm{A})$ is T for all truth valuations τ on A; A is a *tautological consequence* of $\mathrm{A}_1, \ldots, \mathrm{A}_\nu$ in case $\mathrm{A}_1 \to \cdots \to \mathrm{A}_\nu \to \mathrm{A}$ is a tautology. Call A and B *tautologically equivalent* in case A ↔ B is a tautology. (Since → is associated from right to left, $\mathrm{A}_1 \to \cdots \to \mathrm{A}_\nu \to \mathrm{A}$ is tautologically equivalent to A_1 & ⋯ & $\mathrm{A}_\nu \to \mathrm{A}$.)

A *numeral* is a term containing no symbols other than S and 0.

Let $\vec{x}$, y, and z be distinct, let a contain no variables other than those in $\vec{x}$, and let b contain no variables other than those in $\vec{x}$, y, and z. Then f is *defined by primitive recursion from* a *and* b by

A1. $\mathrm{f}(\vec{x}, 0) = \mathrm{a}$

A2. $\mathrm{f}(\vec{x}, \mathrm{Sy}) = \mathrm{b}_\mathrm{z}\big(\mathrm{f}(\vec{x}, \mathrm{y})\big)$

A *construction* of f is a finite sequence $\mathrm{g}_1, \mathrm{g}_2, \ldots, \mathrm{g}_\nu$ where g_1 is 0, g_2 is S, f is in the sequence, and each g_μ for $3 \leq \mu \leq \nu$ is constructed by primitive recursion from terms containing no function symbols other than those strictly preceding it in the sequence. The PR *function symbols* are those that have a construction. A PR *term* is a term in which every function symbol is PR, and a *PR number* is a variable-free PR term.

PRA is formulated as a formal system as follows. Its nonlogical symbols are the PR function symbols. Its nonlogical axioms are the *construction axioms* A1 and A2 for definitions of PR function symbols, and the *successor axioms*

a3. $\neg\ \mathrm{S}x = 0$

a4. $\mathrm{S}x = \mathrm{S}y \quad \rightarrow \quad x = y$

The logical axioms are *reflexivity*

a5. $x = x$

symmetry

a6. $x = y \quad \rightarrow \quad y = x$

the *equality axioms*

A7. $\mathrm{x} = \mathrm{y} \quad \& \quad \mathrm{A}_\mathrm{x}(\mathrm{x}) \quad \rightarrow \quad \mathrm{A}_\mathrm{x}(\mathrm{y})$

and the *propositional axioms*

A8. $\mathrm{A} \vee \mathrm{A} \rightarrow \mathrm{A}$

A9. $\mathrm{A} \rightarrow \mathrm{A} \vee \mathrm{B}$

A10. $\mathrm{A} \vee \mathrm{B} \rightarrow \mathrm{B} \vee \mathrm{A}$

A11. $[\mathrm{B} \rightarrow \mathrm{C}] \rightarrow [\mathrm{A} \vee \mathrm{B} \rightarrow \mathrm{A} \vee \mathrm{C}]$

There are three rules of inference:

instance: from A infer an instance of A
modus ponens: from A and $\mathrm{A} \rightarrow \mathrm{B}$ infer B
induction: from $\mathrm{A}_\mathrm{x}(0)$ and $\mathrm{A}_\mathrm{x}(\mathrm{x}') \rightarrow \mathrm{A}_\mathrm{x}(\mathrm{Sx}')$ infer $\mathrm{A}_\mathrm{x}(\mathrm{x})$

As in any formal system, a *proof* is a finite sequence of formulas each of which is either an axiom or follows from strictly preceding formulas by a rule of inference, and it is a *proof of* A in case A is in the sequence. Decorated π stands for a finite sequence of formulas. The notation $\pi \vdash \mathrm{A}$ means that π is a proof in PRA of A, while $\vdash \mathrm{A}$ means that there is a proof π in PRA of A, in which case A is a *theorem* of PRA.

The Propositions in this paper are metamathematical in nature; they are statements about PRA whose proofs are finitary in the strict sense of being expressible in PRA.

PROPOSITION 1. *Certain familiar devices can be used to extend the notion of proof.*

(i) *Tautologies are theorems of* PRA.

(ii) *A tautological consequence of theorems of* PRA *is a theorem of* PRA.

(iii) *Previously proved theorems may be cited in proofs.*

(iv) *Deductions may be used in proofs, as follows. Introduce, in the course of a proof, an arbitrary formula* H*, the hypothesis, and follow it by* $\mathrm{B}_1, \ldots, \mathrm{B}_\nu$ *where each* B_μ *for* $1 \leq \mu \leq \nu$ *is a theorem or is a tautological consequence of strictly preceding formulas. Then discharge the hypothesis by writing* $\mathrm{H} \to \mathrm{B}_\nu$ *and never using* $\mathrm{H}, \mathrm{B}_1, \ldots, \mathrm{B}_\nu$ *again.*

(v) *Claims may be established, as follows. State a claim* A*, introduce the hypothesis* $\neg\mathrm{A}$*, and follow it by* $\mathrm{B}_1, \ldots, \mathrm{B}_\nu$ *where these are as in* (iii) *and furthermore a contradiction is obtained, meaning that for some preceding* B *is* $\neg\mathrm{B}_\nu$*. Then establish the claim by writing* A *and never using* $\neg\mathrm{A}, \mathrm{B}_1, \ldots, \mathrm{B}_\nu$ *again.*

Proof. For (i), refer to [HA]. Hilbert and Ackermann give a finitary proof that in the formal system whose only axioms are 8–11 and whose only rule of inference is modus ponens, the theorems are precisely the tautologies.

For (ii), suppose that $\vdash \mathrm{A}_1$, ..., $\vdash \mathrm{A}_\nu$ and that $\mathrm{A}_1 \to \cdots \to \mathrm{A}_\nu \to \mathrm{A}$ is a tautology, and hence a theorem by (i). Then we have $\vdash \mathrm{A}_2 \to \cdots \to \mathrm{A}_\nu \to \mathrm{A}$ by modus ponens. Proceeding in this way we obtain a proof of A in ν steps. In other words, tautological consequence is a derived rule of inference in PRA.

For (iii), just insert the proofs of the cited theorems.

Given a deduction as in (iv), replace $\mathrm{H}, \mathrm{B}_1, \ldots, \mathrm{B}_\nu$ by $\mathrm{H} \to \mathrm{H}, \mathrm{H} \to \mathrm{B}_1, \ldots, \mathrm{H} \to \mathrm{B}_\nu$. Then $\mathrm{H} \to \mathrm{H}$ is a theorem by (i). If B_μ is a theorem then $\mathrm{H} \to \mathrm{B}_\mu$ is a tautological consequence of it. If B_μ is a tautological consequence of strictly preceding formulas, then $\mathrm{H} \to \mathrm{B}_\mu$ is a tautological consequence of them with the B_λ, for $1 \leq \lambda < \mu$, among them replaced by $\mathrm{H} \to \mathrm{B}_\lambda$. In this way, by (ii), we have a proof of $\mathrm{H} \to \mathrm{B}_\nu$, proving (iv). (Notice that no instance of H is taken. This is sometimes expressed by saying that the variables in H are held constant.)

Given a claim as in (v), proceed as in (iv). Any formula, in particular A, is a tautological consequence of B_ν and $\neg\mathrm{B}_\nu$, so adjoin A to the deduction. Discharging the hypothesis $\neg\mathrm{A}$ we obtain $\neg\mathrm{A} \to \mathrm{A}$, of which A is a tautological consequence, proving (v). (A special case of this is an indirect proof, in which the theorem itself is the claim.) □

The only predicate symbol in PRA is $=$. Nevertheless, we can introduce other predicate symbols as abbreviations. Given A, let $\vec{\mathrm{x}}$ be its distinct variables in some order, set $\mathrm{p}(\vec{\mathrm{x}}) \leftrightarrow \mathrm{A}$, and let $\mathrm{p}(\vec{\mathrm{a}})$ abbreviate the instance $\mathrm{A}_{\vec{\mathrm{x}}}(\vec{\mathrm{a}})$. Use decorated p q to stand for predicate symbols other than $=$; they occur only in abbreviations. An *explicit definition* of f is $\mathrm{f}(\vec{\mathrm{x}}) = \mathrm{c}$ where no variable other than those in $\vec{\mathrm{x}}$ occurs in c. Then let $\mathrm{f}(\vec{\mathrm{a}})$ abbreviate $\mathrm{c}_{\vec{\mathrm{x}}}(\vec{\mathrm{a}})$. Explicitly defined function symbols occur only in abbreviations.

Some formulas are marked $\star$ or $\star\star$ for emphasis.

4. Equality

#2. Construct Eq *so that* $\vdash \mathrm{Eq}(x, y) = 0 \leftrightarrow x = y$.

Hilbert and Bernays construct such a function symbol in §7 of the first edition of [HB] (1939). Following a suggestion of Kreisel to establish the basic properties of $<$ without

using addition, Bernays omitted this explicit construction in the second edition (1968). We give the surprisingly long construction of Eq from the first edition. (Their unary δ is our P, their binary δ is our $-$, and their $\delta(a,b)+\delta(b,a)$ is our $\mathrm{Eq}(a,b)$.)

Primitive recursions are labeled with r, theorems with t, explicit definitions with e, and definitions of PR predicate symbols with d; if one of these letters is capitalized, it indicates a schema. If ξ labels a theorem A, and $\mathrm{x}_1, \ldots, \mathrm{x}_\nu$ are the first ν distinct variables of A in the order of first occurrence, then $\xi;\mathrm{a}_1;\ldots;\mathrm{a}_\nu$ is the theorem $\mathrm{A}_{\mathrm{x}_1,\ldots,\mathrm{x}_\nu}(\mathrm{a}_1,\ldots,\mathrm{a}_\nu)$.

r12. $x+0=x \quad \& \quad x+\mathrm{S}y=\mathrm{S}(x+y)$

t13*b*. $0+0=0+0$

Proof. H 5;0+0

t13*i*. $x+0=0+x \quad \rightarrow \quad \mathrm{S}x+0=0+\mathrm{S}x$

Proof. H:x 12;Sx 12;0;x 12;x

This is an indirect proof. The theorem being proved is a disjunction, $\neg\, x+0=0+x \vee \mathrm{S}x+0=0+\mathrm{S}x$, and H:$x$ is its negation $x+0=0+x \;\&\; \neg\, \mathrm{S}x+0=0+\mathrm{S}x$ (with $\neg\neg$ removed). The colon indicates that x is to be held fixed with this introduction of a hypothesis. The remaining formulas in the text proof together with some equality substitutions (instances of equality axioms A5) and implicit uses of symmetry a6, give a contradiction (marked *QEA* for quod est absurdum) by tautological consequence, completing the indirect proof of the theorem. If you are reading this online (it is posted at *not yet* www.math.princeton.edu/∼nelson/papers/Balrog.pdf), click on the blue *Proof* link. Otherwise, open a browser to www.math.princeton.edu/∼nelson/proof/ and click on 13i.pdf.

t13. $x+0=0+x$

When tξ immediately follows tξb and tξi, it is an inference by induction.

t14*b*. $x+\mathrm{S}0=\mathrm{S}x+0$

Proof. H:x 12;x;0 12;x 12;Sx

t14*i*. $x+\mathrm{S}y=\mathrm{S}x+y \quad \rightarrow \quad x+\mathrm{SS}y=\mathrm{S}x+\mathrm{S}y$

Proof. H:x:y 12;x;Sy 12;Sx;y

t14. $x+\mathrm{S}y=\mathrm{S}x+y$

t15*b*. $x+0=0 \quad \rightarrow \quad x=0 \quad \& \quad 0=0$

Proof. H:x 12;x

t15*i*. $[x+y=0 \quad \rightarrow \quad x=0 \quad \& \quad y=0] \quad \rightarrow \quad [x+\mathrm{S}y=0 \quad \rightarrow \quad x=0 \quad \& \quad \mathrm{S}y=0]$

Proof. H:x:y 12;x;y 3;x+y

t15. $x+y=0 \quad \rightarrow \quad x=0 \quad \& \quad y=0$

r16. $\mathrm{P}0=0 \quad \& \quad \mathrm{PS}x=x$

r17. $x-0=x \quad \& \quad x-\mathrm{S}y=\mathrm{P}(x-y)$

t18b. $\mathrm{S}x - \mathrm{S0} = x - 0$

Proof. H:x 17;Sx;0 17;Sx 16;x 17;x

t18i. $\mathrm{S}x - \mathrm{S}y = x - y \quad \rightarrow \quad \mathrm{S}x - \mathrm{SS}y = x - \mathrm{S}y$

Proof. H:x:y 17;Sx;Sy 17;x;y

t18. $\mathrm{S}x - \mathrm{S}y = x - y$

t19b. $0 - 0 = 0$

Proof. H 17;0

t19i. $x - x = 0 \quad \rightarrow \quad \mathrm{S}x - \mathrm{S}x = 0$

Proof. H:x 18;x;x

t19. $x - x = 0$

t20b. $\mathrm{S0} - 0 = \mathrm{S0}$

Proof. H 17;S0

t20i. $\mathrm{S}x - x = \mathrm{S0} \quad \rightarrow \quad \mathrm{SS}x - \mathrm{S}x = \mathrm{S0}$

Proof. H:x 18;Sx;x

t20. $\mathrm{S}x - x = \mathrm{S0}$

t21. $\mathrm{S}x - x \neq 0$

Proof. H:x 20;x 3;0

t22b. $0 \neq 0 \quad \rightarrow \quad 0 = \mathrm{SP0}$

Proof. H 5;0

t22i. $[x \neq 0 \quad \rightarrow \quad x = \mathrm{SP}x] \quad \rightarrow \quad [\mathrm{S}x \neq 0 \quad \rightarrow \quad \mathrm{S}x = \mathrm{SPS}x]$

Proof. H:x 16;x

t22. $x \neq 0 \quad \rightarrow \quad x = \mathrm{SP}x$

t23b. $y - 0 \neq 0 \quad \rightarrow \quad 0 + (y - 0) = y$

Proof. H:y 17;y 13;y 12;y

t23i. $[y - x \neq 0 \quad \rightarrow \quad x + (y - x) = y] \quad \rightarrow \quad [y - \mathrm{S}x \neq 0 \quad \rightarrow \quad \mathrm{S}x + (y - \mathrm{S}x) = y]$

Proof. H:y:x 17;y;x 16;$y{-}x$ 14;x;P($y{-}x$) 22;$y{-}x$

t23. $y - x \neq 0 \quad \rightarrow \quad x + (y - x) = y$

t24. $y - x = \mathrm{S0} \quad \rightarrow \quad \mathrm{S}x = y$

Proof. H:y:x 3;0 23;y;x 12;x;0

t25. $x \neq 0 \quad \& \quad \mathrm{P}x = 0 \quad \rightarrow \quad x = \mathrm{S0}$

Proof. H:x 22;x

t26. $y - x \neq 0 \quad \& \quad y - \mathrm{S}x = 0 \quad \rightarrow \quad y - x = \mathrm{S0}$

Proof. H:y:x 17;y;x 25;$y{-}x$

t27. $y - x \neq 0 \quad \rightarrow \quad \mathrm{S}x = y \quad \vee \quad y - \mathrm{S}x \neq 0$

Proof. H:y:x 26;y;x 24;y;x

t28b. $x - 0 \neq 0 \quad \rightarrow \quad \mathrm{S}x - 0 \neq 0$

Proof. H:x 17;Sx 3;x

t28i. $[x - y \neq 0 \quad \rightarrow \quad \mathrm{S}x - y \neq 0] \quad \rightarrow \quad [x - \mathrm{S}y \neq 0 \quad \rightarrow \quad \mathrm{S}x - \mathrm{S}y \neq 0]$

Proof. H:x:y 18;x;y 17;x;y 16

t28. $x - y \neq 0 \quad \rightarrow \quad \mathrm{S}x - y \neq 0$

t29b. $0 = y \quad \vee \quad y - 0 \neq 0 \quad \vee \quad 0 - y \neq 0$

Proof. H:y 17;y

t29i. $[x = y \quad \vee \quad y - x \neq 0 \quad \vee \quad x - y \neq 0] \quad \rightarrow \quad [\mathrm{S}x = y \quad \vee \quad y - \mathrm{S}x \neq 0 \quad \vee \quad \mathrm{S}x - y \neq 0]$

Proof. H:x:y 21;x 27;y;x 28;x;y

t29. $x = y \quad \vee \quad y - x \neq 0 \quad \vee \quad x - y \neq 0$

t30. $x - y = 0 \quad \& \quad y - x = 0 \quad \rightarrow \quad x = y$

Proof. H:x:y 29;x;y

e31. $\mathrm{Eq}(x, y) = (x - y) + (y - x)$

Here at last is the Hilbert-Bernays construction.

t32. $\mathrm{Eq}(x, y) = 0 \quad \leftrightarrow \quad x = y$ $\star\star$

Proof. H:x:y 31;x;y 15;x−y;y−x 30;x;y 19;x 12;0 ?Eq(x,y)≠0

The ? indicates the introduction of a claim.

#3. Using the case function symbol C *such that* $\mathrm{C}(x, y, z)$ *is* y *if* x *is* 0 *and is* z *otherwise, form the characteristic term* χA *so that* $\vdash \chi\mathrm{A} = 0 \leftrightarrow \mathrm{A}$. *Construct the formal system* χPRA, *equivalent to* PRA, *whose only symbols are variables and* PR *function symbols: the logical connectives and* $=$ *are eliminated. But continue working in* PRA.

r33. $\mathrm{C}(0, y, z) = y \quad \& \quad \mathrm{C}(\mathrm{S}x, y, z) = z$ $\star$

t34. $x \neq 0 \quad \rightarrow \quad \mathrm{C}(x, y, z) = z$

Proof. H:x:y:z 22;x 33;y;z;Px

t35. $\mathrm{C}(x, y, z) \neq z \quad \rightarrow \quad x = 0 \quad \& \quad \mathrm{C}(x, y, z) = y$

Proof. H:x:y:z 34;x;y;z 33;y;z

t36. $\mathrm{C}(x, 0, \mathrm{S}0) = 0 \quad \leftrightarrow \quad x = 0$

Proof. H:x 22;x 33;0;S0;Px 3;0 ?x≠0

t37. $\mathrm{C}(x, \mathrm{S}0, 0) = 0 \quad \leftrightarrow \quad x \neq 0$

Proof. H:x 22;x 33;S0;0;Px 3;0 ?x=0

t38. $\mathrm{C}(x, 0, \mathrm{S}0) = 0 \quad \vee \quad \mathrm{C}(x, 0, \mathrm{S}0) = \mathrm{S}0$

Proof. H:x 22;x 33;0;S0;Px

t39. $\mathrm{C}(x,\mathrm{S0},0)=0 \quad \vee \quad \mathrm{C}(x,\mathrm{S0},0)=\mathrm{S0}$

Proof. H:x 22;x 33;S0;0;Px

t40. $\mathrm{C}(x,0,0)=0$

Proof. H:x 22;x 33;0;0;Px

t41a. $\mathrm{C}\big(x,0,\mathrm{C}(y,0,\mathrm{S0})\big)=0 \quad \to \quad x=0 \quad \vee \quad y=0$

Proof. H:x:y 36;y 22;x 33;0;C(y,0,S0);Px

t41b. $x=0 \quad \vee \quad y=0 \quad \to \quad \mathrm{C}\big(x,0,\mathrm{C}(y,0,\mathrm{S0})\big)=0$

Proof. H:x:y 36;y 22;x 33;0;C(y,0,S0);Px

t41. $\mathrm{C}\big(x,0,\mathrm{C}(y,0,\mathrm{S0})\big)=0 \quad \leftrightarrow \quad x=0 \quad \vee \quad y=0$

Proof. Tautological consequence of 41a and 41b.

Think of 0 as true and S0 as false.

e42. $x \doteq y = \mathrm{C}\big(\mathrm{Eq}(x,y),0,\mathrm{S0}\big)$

e43. $\dot\neg x = \mathrm{C}(x,\mathrm{S0},0)$

e44. $x \mathbin{\dot\vee} y = \mathrm{C}\big(x,0,\mathrm{C}(y,0,\mathrm{S0})\big)$

t45. $x \doteq y = 0 \quad \vee \quad x \doteq y = \mathrm{S0}$

Proof. H:x:y 42;x;y 38;Eq(x,y)

t46. $\dot\neg x = 0 \quad \vee \quad \dot\neg x = \mathrm{S0}$

Proof. H:x 43;x 39;x

t47. $x \mathbin{\dot\vee} y = 0 \quad \vee \quad x \mathbin{\dot\vee} y = \mathrm{S0}$

Proof. H:x:y 44;x;y 38;y 40;x 38;x

e48. $x \mathbin{\dot\&} y = \dot\neg(\dot\neg x \mathbin{\dot\vee} \dot\neg y)$

e49. $x \mathbin{\dot\to} y = \dot\neg x \mathbin{\dot\vee} y$

e50. $x \mathbin{\dot\leftrightarrow} y = (\dot\neg x \mathbin{\dot\vee} y) \mathbin{\dot\&} (x \mathbin{\dot\vee} \dot\neg y)$

To each A associate a term χA, the *characteristic term of* A, recursively as follows.

(1) $\qquad \chi[\mathrm{a}=\mathrm{b}] \ \text{ is } \ \mathrm{a} \doteq \mathrm{b}$

(2) $\qquad \chi[\neg\mathrm{B}] \ \text{ is } \ \dot\neg\chi\mathrm{B}$

(3) $\qquad \chi[\mathrm{B}\vee\mathrm{C}] \ \text{ is } \ \chi\mathrm{B} \mathbin{\dot\vee} \chi\mathrm{C}$

That is, χA is obtained by replacing each $=$ by $\doteq$, each $\neg$ by $\dot\neg$, and each $\vee$ by $\dot\vee$. From this it follows that

(4) $\qquad [\chi\mathrm{A}]_{\vec{\mathrm{x}}}(\vec{\mathrm{a}}) \ \text{ is } \ \chi[\mathrm{A}_{\vec{\mathrm{x}}}(\vec{\mathrm{a}})]$

If ℓ is a decorated roman letter occurring in an expression schema v, then v, ℓ/u is the expression or expression schema obtained by replacing each occurrence of ℓ in v by u.

PROPOSITION 2. *The following are theorem schemata of* PRA.

T51. $\chi\mathrm{A} = 0 \quad \leftrightarrow \quad \mathrm{A}$

T52. $\chi\mathrm{A} = 0 \quad \vee \quad \chi\mathrm{A} = \mathrm{S}0$

Proof. We have $51, \mathrm{A}/\mathrm{a} = \mathrm{b}$ by (1) and 42;a;b and 36;Eq(a, b) and 32;a;b. If $51, \mathrm{A}/\mathrm{B}$ then $51, \mathrm{A}/\neg\mathrm{B}$ by (2) and 43;χB and 37;χB. If $51, \mathrm{A}/\mathrm{B}$ and $51, \mathrm{A}/\mathrm{C}$ then $51, \mathrm{A}/\mathrm{B} \vee \mathrm{C}$ by (3) and 47;χB;χC and 41;χB;χC. By metamathematical induction on the formation of formulas, each $\chi\mathrm{A} = 0 \leftrightarrow \mathrm{A}$ is a theorem of PRA.

We have $52, \mathrm{A}/\mathrm{a} = \mathrm{b}$ by (1) and 45;a;b; we have $52, \mathrm{A}/\neg\mathrm{B}$ by (2) and 46;χB; we have $52, \mathrm{A}/\mathrm{B} \vee \mathrm{C}$ by (3) and 47;χB;χC. By definition, every formula A is an equation, negation, or disjunction, so 52 holds. □

T53. $\chi\mathrm{A} = \mathrm{S}0 \quad \leftrightarrow \quad \neg\mathrm{A}$

Proof. Tautological consequence of 51 and 52 and 3;0.

T54. $[\mathrm{A} \leftrightarrow \mathrm{B}] \quad \leftrightarrow \quad \chi\mathrm{A} = \chi\mathrm{B}$

Proof. Tautological consequence of 51 and $51, \mathrm{A}/\mathrm{B}$ and 52 and $52, \mathrm{A}/\mathrm{B}$ and 3;0.

Now reformulate PRA as a formal system χPRA with a simpler data structure. The symbols of χPRA are the variables and the PR function symbols. Terms are as before. A χ-*equation* is a term of the form $\mathrm{a} \doteq \mathrm{b}$. The formulas of χPRA, called χ-*formulas*, are defined recursively as follows. A χ-equation is a χ-formula; if b and c are χ-formulas, so are $\dot{\neg}\mathrm{b}$ and $\mathrm{b} \mathbin{\dot\vee} \mathrm{c}$. Decorated $\alpha\ \beta\ \gamma\ \delta$ stand for χ-formulas. Note that χ is bijective from formulas of PRA onto formulas of χPRA; each α is $\chi\mathrm{A}$ for a unique A, $\chi^{-1}\alpha$.

Think of the χ-formula α as asserting that the term α is equal to 0. The axioms of χPRA are the characteristic terms of the axioms of PRA; the rules of inference of χPRA are formed from the rules of inference of PRA by replacing each premise and conclusion by its characteristic term.

Explicitly, the axioms and rules of inference of χPRA are as follows, where in Aχ1 and Aχ2, f is the function symbol defined by A1 and A2.

Aχ1. $\mathrm{f}(\vec{\mathrm{x}}, \mathrm{y}) \doteq \mathrm{a}$
Aχ2. $\mathrm{f}(\vec{\mathrm{x}}, \mathrm{Sy}) \doteq \mathrm{b}_{\mathrm{z}}\big(\mathrm{f}(\vec{\mathrm{x}}, \mathrm{y})\big)$
aχ3. $\dot{\neg}\ \mathrm{S}x \doteq 0$
aχ4. $\mathrm{S}x \doteq \mathrm{S}y \mathrel{\dot\to} x \doteq y$
aχ5. $x \doteq x$
aχ6. $x \doteq y \mathrel{\dot\to} y \doteq x$
Aχ7. $\mathrm{x} \doteq \mathrm{y} \ \mathbin{\dot\&}\ \alpha_{\mathrm{x}}(\mathrm{x}) \mathrel{\dot\to} \alpha_{\mathrm{x}}(\mathrm{y})$
Aχ8. $\alpha \mathbin{\dot\vee} \alpha \mathrel{\dot\to} \alpha$
Aχ9. $\alpha \mathrel{\dot\to} \alpha \mathbin{\dot\vee} \beta$
Aχ10. $\alpha \mathbin{\dot\vee} \beta \mathrel{\dot\to} \beta \mathbin{\dot\vee} \alpha$
Aχ11. $(\beta \mathrel{\dot\to} \gamma) \mathrel{\dot\to} (\alpha \mathbin{\dot\vee} \beta \mathrel{\dot\to} \alpha \mathbin{\dot\vee} \gamma)$

χ-*instance*: from α infer an instance of α
χ-*modus ponens*: from α and $\alpha \mathrel{\dot\to} \beta$ infer β
χ-*induction*: from $\alpha_{\mathrm{x}}(0)$ and $\alpha_{\mathrm{x}}(\mathrm{x}') \mathrel{\dot\to} \alpha_{\mathrm{x}}(\mathrm{Sx}')$ infer $\alpha_{\mathrm{x}}(\mathrm{x})$

A proof in χPRA is a *χ-proof*. Decorated σ stands for a finite sequence of χ-formulas, $\sigma \vdash^\chi \alpha$ asserts that σ is a χ-proof of α, and $\vdash^\chi \alpha$ asserts that α is a theorem of χPRA.

PROPOSITION 3. *The following are equivalent:* $\vdash \mathrm{A}$ *and* $\vdash \chi\mathrm{A} = 0$ *and* $\vdash^\chi \chi\mathrm{A}$.

Proof. The first two are equivalent by T51. Let $\pi \vdash \mathrm{A}$. Then $\chi \circ \pi \vdash^\chi \chi\mathrm{A}$—for if B in π is an axiom, so is χB, and if B is inferred by a rule of inference, then χB is inferred by the corresponding rule. Conversely, if $\sigma \vdash^\chi \chi\mathrm{A}$, let π consist of all B of the form $\chi^{-1}\beta = 0$ for β in σ. If β is an axiom, then $\chi^{-1}\beta$ is an axiom D of PRA, so B is $\chi\mathrm{D} = 0$, which is a theorem by T51, A/D. If β is inferred by a rule of inference, then B is inferred by the corresponding rule. Hence π is a proof with citation of theorems from the theorem schema T51, so $\vdash \mathrm{A}$. □

#4. Establish primitive recursion by cases, though it will not be used until much later.

The following Proposition expresses the familiar "if, else if, ..., else if, else" pattern for cases.

PROPOSITION 4. *Let* d *be* $\mathrm{C}\chi\mathrm{A}_1\mathrm{b}_1\mathrm{C}\chi\mathrm{A}_2\mathrm{b}_2 \ldots \mathrm{C}\chi\mathrm{A}_\nu\mathrm{b}_\nu\mathrm{c}_\nu$ *and for* $1 \le \mu \le \nu$ *let* B_μ *be* $\neg\mathrm{A}_1 \mathbin{\&} \cdots \mathbin{\&} \neg\mathrm{A}_\mu$. *Then*

$$\begin{aligned} \vdash\ & [\mathrm{A}_1 \to \mathrm{d} = \mathrm{b}_1] \quad \& \quad [\mathrm{B}_1 \mathbin{\&} \mathrm{A}_2 \to \mathrm{d} = \mathrm{b}_2] \quad \& \quad \cdots \quad \& \\ & [\mathrm{B}_{\nu-1} \mathbin{\&} \mathrm{A}_\nu \to \mathrm{d} = \mathrm{b}_\nu] \quad \& \quad [\mathrm{B}_\nu \to \mathrm{d} = \mathrm{c}_\nu] \end{aligned} \tag{5}$$

Proof. First let $\nu = 1$. Then d is $\mathrm{C}\chi\mathrm{A}_1\mathrm{b}_1\mathrm{c}_1$. We have $\chi\mathrm{A}_1 = 0 \leftrightarrow \mathrm{A}_1$ by T51, A/A_1, so $\mathrm{A}_1 \to \mathrm{d} = \mathrm{b}_1$ by 33;b_1;c_1. We have $\chi\mathrm{A}_1 = \mathrm{S0} \leftrightarrow \neg\mathrm{A}_1$ by T53, A/A_1, so $\neg\mathrm{A}_1 \to \mathrm{d} = \mathrm{c}_1$ by 33;b_1;c_1;0, proving the result for $\nu = 1$. Now assume as metamathematical induction hypothesis that the result holds for $\nu - 1$ and let c_1' be $\mathrm{C}\chi\mathrm{A}_2\mathrm{b}_2 \ldots \mathrm{C}\chi\mathrm{A}_\nu\mathrm{b}_\nu\mathrm{c}_\nu$. By the case $\nu = 1$, $\mathrm{A}_1 \to \mathrm{d} = \mathrm{b}_1$ and $\neg\mathrm{A}_1 \to \mathrm{d} = \mathrm{c}_1'$, so (5) holds by the induction hypothesis. □

If f is defined by the primitive recursion $\mathrm{f}(\vec{\mathrm{x}}, \mathrm{y}) = \mathrm{a} \mathbin{\&} \mathrm{f}(\vec{\mathrm{x}}, \mathrm{Sy}) = \mathrm{d}$ (where d is as in the Proposition) then we say that (5) holds by *primitive recursion by cases*.

5. Bounded quantifiers

#5. Given a formula A *and a variable* x*, construct the* PR *function symbol* μ_A *so that* $\mu_\mathrm{A}(\mathrm{x})$ *(with the other variables in* A *not indicated in the notation) finds the first* x′*, if any, such that* $\mathrm{A}_\mathrm{x}(\mathrm{x}')$ *holds.*

Introduce the PR predicate symbols $\le$ (*less than*) and $<$ (*strictly less than*).

d55. $x \le y \quad \leftrightarrow \quad x - y = 0$

d56. $x < y \quad \leftrightarrow \quad x \le y \quad \& \quad x \ne y$

t57. $x \le 0 \quad \to \quad x = 0$

Proof. H:x $\quad 55^{\to};x;0 \quad 17;x$

If dξ is $\mathrm{p}(\vec{\mathrm{x}}) \leftrightarrow \mathrm{D}$, then $\xi^{\to}$ is $\neg\mathrm{p}(\vec{\mathrm{x}}) \vee \mathrm{D}$ (which is $\mathrm{p}(\vec{\mathrm{x}}) \to \mathrm{D}$) and $\xi^{\leftarrow}$ is $\mathrm{p}(\vec{\mathrm{x}}) \vee \neg\mathrm{D}$ (which is tautologically equivalent to $\mathrm{D} \to \mathrm{p}(\vec{\mathrm{x}})$).

t58. $0 \leq x$

Proof. H:x 55$^{<-}$;0;x 23;0;x 15;x;0$-x$

t59. $\neg\, \mathrm{S}x \leq x$

Proof. H:x 55$^{->}$;Sx;x 21;x

t60. $x \leq x$

Proof. H:x 55$^{<-}$;x;x 19;x

t61. $x \leq y \quad \rightarrow \quad x < y \quad \vee \quad x = y$

Proof. H:x:y 56$^{<-}$;x;y

t62. $x < y \quad \vee \quad x = y \quad \rightarrow \quad x \leq y$

Proof. H:x:y 56$^{->}$;x;y 60;x

t63. $x \leq \mathrm{S}x$

Proof. H:x 17;x;x 19;x 16 55$^{<-}$;x;Sx

t64b. $\mathrm{P}0 \leq 0$

Proof. H 16 60;0

t64i. $\mathrm{P}x \leq x \quad \rightarrow \quad \mathrm{PS}x \leq \mathrm{S}x$

Proof. H:x 16;x 63;x

t64. $\mathrm{P}x \leq x$

t65. $x < y \quad \rightarrow \quad y - x \neq 0$

Proof. H:x:y 56$^{->}$;x;y 55$^{->}$;x;y 29;x;y

t66. $x < y \quad \rightarrow \quad y = x + (y - x)$

Proof. H:x:y 65;x;y 23;y;x

t67. $x = y \quad \rightarrow \quad y = x + (y - x)$

Proof. H:x:y 19;y 12;x

t68. $x \leq y \quad \rightarrow \quad y = x + (y - x)$

Proof. H:x:y 56$^{<-}$;x;y 67;x;y 66;x;y

t69b. $x - (y + 0) = (x - y) - 0$

Proof. H:x:y 12;y 17;$x$$-$$y$

t69i. $[x - (y + z) = (x - y) - z] \quad \rightarrow \quad [x - (y + \mathrm{S}z) = (x - y) - \mathrm{S}z]$

Proof. H:x:y:z 12;y;z 17;x;y+z 17;$x$$-$$y$;$z$

t69. $x - (y + z) = (x - y) - z$

t70b. $0 - 0 = 0$

Proof. H 19;0

t70i. $0 - x = 0 \quad \to \quad 0 - \mathrm{S}x = 0$

Proof. H:x 17;0;x 16

t70. $0 - x = 0$

t71. $x \leq x + y$

Proof. H:x:y 69;x;x;y 19;x 70;y 55$^{\leftarrow}$;x;x+y

t72b. $x + (y + 0) = (x + y) + 0$

Proof. H:x:y 12;y 12;x+y

t72i. $x + (y + z) = (x + y) + z \quad \to \quad x + (y + \mathrm{S}z) = (x + y) + \mathrm{S}z$

Proof. H:x:y:z 12;y;z 12;x;y+z 12;x+y;z 4;x+(y+z);(x+y)+z

t72. $x + (y + z) = (x + y) + z$

t73. $x \leq y \quad \& \quad y \leq z \quad \to \quad x \leq z$

Proof. H;x:y:z 68;x;y 68;y;z 72;x;y−x;z−y 71;x;(y−x)+(z−y)

t74. $x < y \quad \to \quad y - x \neq 0$

Proof. H:x:y 56$^{\rightarrow}$;x;y 68;x;y 12;x

t75. $y - x \neq 0 \quad \to \quad x < y$

Proof. H:y:x 23;y;x 71;x;y−x 56$^{\leftarrow}$;x;y 19;x

t76. $x \leq y \quad \& \quad y \leq x \quad \to \quad x = y$

Proof. H:x:y 55$^{\rightarrow}$;x;y 55$^{\rightarrow}$;y;x 30;x;y

t77. $x < y \quad \vee \quad x = y \quad \vee \quad y < x$

Proof. H:x:y 75;x;y 75;y;x 30;x;y

t78. $x < y \quad \to \quad \neg\, y \leq x$

Proof. H:x:y 56$^{\rightarrow}$;x;y 76;x;y

t79. $\neg\, y \leq x \quad \to \quad x < y$

Proof. H:y:x 77;x;y 56$^{\rightarrow}$;y;x 60;x

t80. $\neg\, [x < y \quad \& \quad y \leq x]$

Proof. H:x:y 78;x;y

t81. $\mathrm{S}x \leq y \quad \to \quad x < y$

Proof. H:x:y 56$^{\leftarrow}$;x;y 63;x 73;x;Sx;y 55$^{\rightarrow}$;Sx;x 21;x

Let $\vec{\mathrm{y}}$ be the distinct variables of A other than x in the order of first occurrence, and let $\mu_{\mathrm{A}}(\mathrm{a})$ abbreviate $\mu_{\mathrm{A}}(\vec{\mathrm{y}}, \mathrm{a})$. Define the PR function symbol μ_{A} by

R82. $\mu_{\mathrm{A}}(0) = \mathrm{C}(\chi[\mathrm{A_x}(0)], 0, \mathrm{S}0) \quad \&$
$\mu_{\mathrm{A}}(\mathrm{Sx}) = \mathrm{C}\big(\chi[\mu_{\mathrm{A}}(\mathrm{x}) \leq \mathrm{x}], \mu_{\mathrm{A}}(\mathrm{x}), \mathrm{C}(\chi[\mathrm{A_x}(\mathrm{Sx})], \mathrm{Sx}, \mathrm{SSx})\big)$ $\star$

Remark that if x_1 is any variable other than those in $\vec{\mathrm{y}}$ and A_1 is $\mathrm{A_x}(\mathrm{x}_1)$, then μ_{A_1} is the same as μ_{A}. We have $\mu_{\mathrm{A}}(\mathrm{x}) = \mathrm{Sx}$ until an x' (if any) is found such that $\mathrm{A_x}(\mathrm{x}')$ holds,

after which it remains x' forever, as we now demonstrate (with implicit uses of equality axioms and symmetry).

T83b. $\mu_A(0) \le 0 \quad \to \quad A_x\big(\mu_A(0)\big)$

Proof. Suppose not. Then

.1 $\mu_A(0) \le 0$

.2 $\neg A_x(\mu_A(0))$

By .1 and 57;$\mu_A(0)$,

.3 $\mu_A(0) = 0$

By .3 and 82,

.4 $C(\chi[A_x(0)], 0, S0) = 0$

By .4 and 36;$\chi[A_x(0)]$,

.5 $\chi[A_x(0)] = 0$

By .5 and 51, $A/A_x(0)$,

.6 $A_x(0)$

By .2 and .3,

.7 $\neg A_x(0)$

QEA by .6 and .7.

T83i. $\big[\mu_A(x) \le x \to A_x\big(\mu_A(x)\big)\big] \quad \to \quad \big[\mu_A(Sx) \le Sx \to A_x\big(\mu_A(Sx)\big)\big]$

Proof. Suppose not. Then

.1 $\mu_A(x) \le x \to A_x(\mu_A(x))$

.2 $\mu_A(Sx) \le Sx$

.3 $\neg A_x(\mu_A(Sx))$

Claim: $\neg\, \mu_A(x) \le x$. Suppose not. Then

.4 $\mu_A(x) \le x$

By .4 and 51, $A/\mu_A(x) \le x$,

.5 $\chi[\mu_A(x)] = 0$

By .4 and 82,

.6 $\mu_A(Sx) = C(0, \mu_A(x), C(\chi[A_x(Sx)], Sx, SSx))$

By .6 and 33;$\mu_A(x)$,

.7 $\mu_A(Sx) = \mu_A(x)$

By .1 and .4,

.8 $A_x(\mu_A(x))$

By .7 and .8,

.9 $A_x(\mu_A(Sx))$

The claim is proved by .3 and .9, and .4–.9 will not be used again.

.10 $\neg\, \mu_A(x) \le x$

By .10 and 53, $A/\mu_A(x) \le x$,

.11 $\chi[\mu_A(x) \le x] = S0$

By .11 and 82,

.12 $\mu_A(Sx) = C(S0, \mu_A(c), C(\chi[A_x(Sx)], Sx, SSx))$

By .12 and 33;$\mu_A(x)$;$C(\chi[A_x(Sx)], Sx, SSx)$;0,

.13 $\mu_A(Sx) = C(\chi[A_x(Sx)], Sx, SSx)$

By .2 and 59;Sx,

.14 $\mu_A(Sx) \ne SSx$

By .14 and 35;$\chi[\mathrm{A_x}(\mathrm{Sx})]$;Sx;SSx,
.15 $\chi[\mathrm{A_x}(\mathrm{Sx})] = 0$ & $\mathrm{C}(\chi[\mathrm{A_x}(\mathrm{Sx})], \mathrm{Sx}, \mathrm{SSx}) = \mathrm{Sx}$
By .15 and 51, A/$\mathrm{A_x}(\mathrm{Sx})$,
.16 $\mathrm{A_x}(\mathrm{Sx})$
By .13 and .15,
.17 $\mu_{\mathrm{A}}(\mathrm{Sx}) = \mathrm{Sx}$
By .16 and .17,
.18 $\mathrm{A_x}(\mu_{\mathrm{A}}(\mathrm{Sx}))$
QEA by .3 and .18.

T83. $\mu_{\mathrm{A}}(\mathrm{x}) \leq \mathrm{x} \quad \rightarrow \quad \mathrm{A_x}\big(\mu_{\mathrm{A}}(\mathrm{x})\big)$

T84*b*. $\mathrm{A_x}(0) \quad \rightarrow \quad \mu_{\mathrm{A}}(0) \leq 0$

Proof. Suppose not. Then
.1 $\mathrm{A_x}(0)$
.2 $\neg\, \mu_{\mathrm{A}}(0) \leq 0$
By .1 and 49, A/$\mathrm{A_x}(0)$,
.3 $\chi[\mathrm{A_x}(0) = 0] = 0$
By .3 and 82,
.4 $\mu_{\mathrm{A}}(0) = \mathrm{C}(0, \mathrm{S0}, \mathrm{SS0})$
By .4 and 40;0,
.5 $\mu_{\mathrm{A}}(0) = 0$
By .5 and 60;0,
.6 $\mu_{\mathrm{A}}(0) \leq 0$
QEA by .2 and .7.

T84*i*. $[\mathrm{A_x}(\mathrm{x}) \rightarrow \mu_{\mathrm{A}}(\mathrm{x}) \leq \mathrm{x}] \quad \rightarrow \quad [\mathrm{A_x}(\mathrm{Sx}) \rightarrow \mu_{\mathrm{A}}(\mathrm{Sx}) \leq \mathrm{Sx}]$

Proof. Suppose not. Then (the induction hypothesis is not needed in this proof)
.1 $\mathrm{A_x}(\mathrm{Sx})$
.2 $\neg\, \mu_{\mathrm{A}}(\mathrm{Sx}) \leq \mathrm{Sx}$
By .1 and 51, A/$\mathrm{A_x}(\mathrm{Sx})$,
.3 $\chi[\mathrm{A_x}(\mathrm{Sx})] = 0$
Claim: $\mu_{\mathrm{A}}(\mathrm{x}) \leq \mathrm{x}$. Suppose not. Then
.4 $\neg\, \mu_{\mathrm{A}}(\mathrm{x}) \leq \mathrm{x}$
By .4 and 53, A/$\mu_{\mathrm{x}}(\mathrm{x}) \leq \mathrm{x}$,
.5 $\chi[\mu_{\mathrm{A}}(\mathrm{x}) \leq \mathrm{x}] = \mathrm{S0}$
By .5 and 82,
.6 $\mu_{\mathrm{A}}(\mathrm{Sx}) = \mathrm{C}\big(\mathrm{S0}, \mu_{\mathrm{A}}(\mathrm{x}), \mathrm{C}(\chi[\mathrm{A_x}(\mathrm{Sx})], \mathrm{Sx}, \mathrm{SSx})\big)$
By .6 and 33;$\mu_{\mathrm{A}}(\mathrm{x})$;$\mathrm{C}(\chi[\mathrm{A_x}(\mathrm{Sx})], \mathrm{Sx}, \mathrm{SSx})$;0,
.7 $\mu_{\mathrm{A}}(\mathrm{Sx}) = \mathrm{C}\big(\chi[\mathrm{A_x}(\mathrm{Sx})], \mathrm{Sx}, \mathrm{SSx}\big)$
By .3 and .7,
.8 $\mu_{\mathrm{A}}(\mathrm{Sx}) = \mathrm{C}(0, \mathrm{Sx}, \mathrm{SSx})$
By .8 and 33;Sx;SSx,
.9 $\mu_{\mathrm{A}}(\mathrm{Sx}) = \mathrm{Sx}$
By .9 and 60;Sx,
.10 $\mu_{\mathrm{A}}(\mathrm{Sx}) \leq \mathrm{Sx}$
The claim is proved by .2 and .10, and .4–.10 will not be used again.

.11 $\mu_A(x) \leq x$

By .11 and 51, $A/\mu_A(x) \leq x$,

.12 $\chi[\mu_A(x) \leq x] = 0$

By .12 and 82,

.13 $\mu_A(Sx) = C(0, \mu_A(x), C(\chi[A_x(Sx)], Sx, SSx))$

By .13 and 33;$\mu_A(x)$;$C(\chi[A_x(Sx)], Sx, SSx)$,

.14 $\mu_A(Sx) = \mu_A(x)$

By .14 and .11,

.15 $\mu_A(Sx) \leq x$

By .15 and 63;x and 73;$\mu_A(x)$;x;Sx,

.16 $\mu_A(Sx) \leq Sx$

QEA by .2 and .16.

T84. $A_x(x) \quad \rightarrow \quad \mu_A(x) \leq x$

T85. $A_x(x) \quad \rightarrow \quad A_x(\mu_A(x)) \quad \& \quad \mu_A(x) \leq x$

Proof. By 84 and 83.

T86*b*. $\mu_A(x) \leq x \quad \rightarrow \quad \mu_A(x + 0) = \mu_A(x)$

Proof. By 12;x and 5;$\mu_A(x)$.

T86*i*. $[\mu_A(x) \leq x \rightarrow \mu_A(x + w) = \mu_A(x)] \quad \rightarrow \quad [\mu_A(x) \leq x \rightarrow \mu_A(x + Sw) = \mu_A(x)]$

Proof. Suppose not. Then

.1 $\mu_A(x) \leq x \rightarrow \mu_A(x + w) = \mu_A(x)$

.2 $\mu_A(x) \leq x$

.3 $\mu_A(x + Sw) \neq \mu_A(x)$

By .2 and .1,

.4 $\mu_A(x + w) = \mu_A(x)$

By 12;x;w,

.5 $x + Sw = S(x + w)$

By .4 and .2,

.6 $\mu_A(x + w) \leq x$

By .6 and 71;x;w and 73;$\mu_A(x + w)$;x;$x + w$,

.7 $\mu_A(x + w) \leq x + w$

By .7 and 51, $A/\mu_A(x + w) \leq x + w$,

.8 $\chi[\mu_A(x + w) \leq x + w] = 0$

By .8 and 82;$x + w$,

.9 $\mu_A(S(x + w)) = C(0, \mu_A(x + w), C(\chi[A_x(S(x + w))], S(x + w), SS(x + w)))$

By .9 and .5 and 33;$\mu_A(x + w)$;$C(\chi[A_x(S(x + w))], S(x + w), SS(x + w))$,

.10 $\mu_A(x + Sw) = \mu_A(x + w)$

By .10 and .4,

.11 $\mu_A(x + Sw) = \mu_A(x)$

QEA by .3 and .11.

T86. $\mu_A(x) \leq x \quad \rightarrow \quad \mu_A(x + w) = \mu_A(x)$

T87. $\mu_A(x) \leq x \quad \& \quad x \leq z \quad \rightarrow \quad \mu_A(z) = \mu_A(x)$

Proof. Suppose not. Then
.1 $\mu_{\mathrm{A}}(\mathrm{x}) \leq \mathrm{x}$
.2 $\mathrm{x} \leq \mathrm{z}$
.3 $\mu_{\mathrm{A}}(\mathrm{z}) \neq \mu_{\mathrm{A}}(\mathrm{x})$
By .2 and 68;x;z,
.4 $\mathrm{z} = \mathrm{x} + (\mathrm{z} - \mathrm{x})$
By .1 and .4 and 86;x;z − x,
.5 $\mu_{\mathrm{A}}(\mathrm{z}) = \mu_{\mathrm{A}}(\mathrm{x})$
QEA by .3 and .5.

#6. Introduce bounded quantifiers $\exists \mathrm{x} \leq \mathrm{b}\, \mathrm{A}$ *and* $\forall \mathrm{x} \leq \mathrm{b}\, \mathrm{A}$*, where* x *does not occur in* b*, as instances of* A*, using* μ_{A}*.*

If x does occur in b, let $\exists \mathrm{x} \leq \mathrm{b}\, \mathrm{A}$ abbreviate $\mathrm{A}_{\mathrm{x}}(\mu_{\mathrm{A}}(\mathrm{b}))$, and let $\forall \mathrm{x} \leq \mathrm{b}\, \mathrm{A}$ abbreviate $\mathrm{A}_{\mathrm{x}}(\mu_{\neg \mathrm{A}}(\mathrm{b}))$. Then $\forall \mathrm{x} \leq \mathrm{b}\, \mathrm{A}$ is tautologically equivalent to $\neg \exists \mathrm{x} \leq \mathrm{b}\, \neg \mathrm{A}$, since the latter is the double negation of the former. Call $\exists \mathrm{x} \leq \mathrm{b}$ and $\forall \mathrm{x} \leq \mathrm{b}$ *bounded quantifiers*; they occur only in abbreviations, and x does not occur in $\exists \mathrm{x} \leq \mathrm{b}\, \mathrm{A}$ or $\forall \mathrm{x} \leq \mathrm{b}\, \mathrm{A}$. Each is an instance of A.

T88. $\mathrm{x} \leq \mathrm{b} \quad \& \quad \mathrm{A}_{\mathrm{x}}(\mathrm{x}) \quad \rightarrow \quad \exists \mathrm{x} \leq \mathrm{b}\, \mathrm{A}$

Proof. Suppose not. Then
.1 $\mathrm{x} \leq \mathrm{b}$
.2 $\mathrm{A}_{\mathrm{x}}(\mathrm{x})$
.3 $\neg\, \mathrm{A}_{\mathrm{x}}(\mu_{\mathrm{A}}(\mathrm{b}))$
By .2 and 85,
.4 $\mathrm{A}_{\mathrm{x}}(\mu_{\mathrm{A}}(\mathrm{x})) \;\&\; \mu_{\mathrm{A}}(\mathrm{x}) \leq \mathrm{x}$
By .4 and .1 and 87;x;b,
.5 $\mu_{\mathrm{A}}(\mathrm{b}) = \mu_{\mathrm{A}}(\mathrm{x})$
By .5 and .4,
.6 $\mathrm{A}_{\mathrm{x}}(\mu_{\mathrm{A}}(\mathrm{b}))$
QEA by .3 and .6.

For the converse we have a specific number, $\mu_{\mathrm{A}}(\mathrm{b})$, that is less than b and satisfies A.

T89. $\exists \mathrm{x} \leq \mathrm{b}\, \mathrm{A} \quad \rightarrow \quad \mu_{\mathrm{A}}(\mathrm{b}) \leq \mathrm{b} \quad \& \quad \mathrm{A}_{\mathrm{x}}\big(\mu_{\mathrm{A}}(\mathrm{b})\big)$ ⋆

Proof. By 85;μ_{A}(b) (recalling that $\exists \mathrm{x} \leq \mathrm{b}\, \mathrm{A}$ is $\mathrm{A}_{\mathrm{x}}(\mu_{\mathrm{A}}(\mathrm{b}))$).

T90. $\forall \mathrm{x} \leq \mathrm{b}\, \mathrm{A} \quad \rightarrow \quad [\mathrm{x} \leq \mathrm{b} \quad \rightarrow \quad \mathrm{A}_{\mathrm{x}}(\mathrm{x})]$ ⋆

Proof. Tautologically equivalent to 88, A/¬A.

T91. $\exists \mathrm{x} \leq \mathrm{c}\, \mathrm{A} \quad \& \quad \mathrm{c} \leq \mathrm{b} \quad \rightarrow \quad \exists \mathrm{x} \leq \mathrm{b}\, \mathrm{A}$

Proof. Suppose not. Then
.1 $\mathrm{A}_{\mathrm{x}}(\mu_{\mathrm{A}}(\mathrm{c}))$
.2 $\mathrm{c} \leq \mathrm{b}$
.3 $\neg\, \mathrm{A}_{\mathrm{x}}(\mu_{\mathrm{A}}(\mathrm{b}))$
By 89, b/c,
.4 $\mu_{\mathrm{A}}(\mathrm{c}) \leq \mathrm{c} \;\&\; \mathrm{A}_{\mathrm{x}}(\mu_{\mathrm{A}}(\mathrm{b}))$
By 87;μ_{A}(c);c;b and .2,
.5 $\mu_{\mathrm{A}}(\mathrm{b}) = \mu_{\mathrm{A}}(\mathrm{c})$

QEA by .1 and .3 and .5.

T92. $\forall x{\leq}b\, A \quad \& \quad c \leq b \quad \rightarrow \quad \forall x{\leq}c\, A$

Proof. Tautologically equivalent to $91, A/\neg A$.

#7. Replace induction as a rule of inference by an axiom schema, and use this to construct formal systems PRA* *and* χPRA*, *equivalent to* PRA*, in which the only rule of inference is, respectively, modus ponens or* χ*-modus ponens, and such that variable-free theorems have variable-free proofs. But continue working in* PRA*;* χPRA* *will be arithmetized later.*

T93*b*. $A_x(0) \quad \& \quad \forall x'{\leq}Px[A_x(x') \rightarrow A_x(Sx')] \quad \rightarrow \quad A_x(0)$

Proof. Tautology.

T93*i*. $\{A_x(0) \quad \& \quad \forall x'{\leq}Px[A_x(x') \rightarrow A_x(Sx')] \quad \rightarrow \quad A_x(x)\} \quad \rightarrow$
$\{A_x(0) \quad \& \quad \forall x'{\leq}PSx[A_x(x') \rightarrow A_x(Sx')] \quad \rightarrow \quad A_x(Sx)\}$

Proof. Suppose not. Then
.1 $A_x(0)$ & $\forall x'{\leq}Px[A_x(x') \rightarrow A_x(Sx')] \rightarrow A_x(x)$
.2 $A_x(0)$
.3 $\forall x'{\leq}PSx[A_x(x) \rightarrow A_x(Sx')]$
.4 $\neg\, A_x(Sx)$
By .2 and .1,
.5 $\forall x'{\leq}Px[A_x(x') \rightarrow A_x(Sx')] \rightarrow A_x(x)$
By 16;x,
.6 $PSx = x$
By .6 and .3,
.7 $\forall x'{\leq}x[A_x(x') \rightarrow A_x(Sx')]$
By 60;x,
.8 $x \leq x$
By .8 and .7 and $90, x/x', b/x, A/A_x(x) \rightarrow A_x(Sx)$,
.9 $A_x(x) \rightarrow A_x(Sx)$
By 64;x,
.10 $Px \leq x$
By .10 and .7 and $90, x/x', b/Px, A/A_x(x) \rightarrow A_x(Sx)$,
.11 $\forall x'{\leq}Px[A_x(') \rightarrow A_x(Sx')]$
By .11 and .5,
.12 $A_x(x)$
By .12 and .9,
.13 $A_x(Sx)$
QEA by .4 and .13.

T93. $A_x(0) \quad \& \quad \forall x'{\leq}Px[A_x(x') \rightarrow A_x(Sx')] \quad \rightarrow \quad A_x(x)$ $\star\star$

Now simplify PRA even further, via formal theories PRA* and χPRA*. The symbols, terms, and formulas of PRA* are those of PRA; its axioms are all instances of axioms of PRA and of T93; its only rule of inference is modus ponens. The symbols, terms, and formulas of χPRA* are those of χPRA; its axioms are the characteristic terms of the axioms of PRA*; its only rule of inference is χ-modus ponens. Proofs and theorems of these two systems are indicated by $\vdash^*$ and $\vdash^{\chi *}$.

PROPOSITION 5. (i) $\vdash$ A *if and only if* $\vdash^*$ A.
(ii) *A variable-free theorem of* PRA* *has a variable-free proof.*
(iii) $\vdash^*$ A *if and only if* $\vdash^{\chi *}$ χA.
(vi) *A variable-free theorem of* χPRA* *has a variable-free proof.*

Proof. For (i), let $\pi \vdash$ A and let $B_x(x)$ be the first formula in π that is inferred by induction, from $B_x(0)$ and $B_x(x') \to B_x(Sx')$. Then we have proofs of these two premises without using induction. By an instance of the second premise we have $\forall x{\leq}Px[B_x(x') \to B_x(Sx')]$, so we have $B_x(0)$ & $\forall x{\leq}Px[B_x(x') \to B_x(Sx')]$ by tautological consequence. By $93, A/B$ we have $B_x(x)$. Proceeding in this way, by metamathematical induction on the number of inferences by induction in π, we have a proof π_1 of A from the axioms of PRA* without using induction. Now consider the first formula $C_{\vec{x}}(\vec{a})$ of π_1 that is inferred by instance, from C. Let π_2 the the part of π_1 strictly preceding $C_{\vec{x}}(\vec{a})$. Let D′ be $D_{\vec{x}}(\vec{a})$, and let π_2' consist of all D′ for D in π_2. Then $\pi_2\pi_2'C'$ is a proof from the axioms of PRA* of C′ (i.e., $C_{\vec{x}}(\vec{a})$) without using induction or instance, because if D is an axiom of PRA* so is D′ (since an instance of an instance is an instance), and if D is inferred from D_1 and $D_1 \to D$ by modus ponens, then D′ is inferred from D_1' and $D_1' \to D'$ by modus ponens (since $[D_1 \to D]'$ is $D_1' \to D'$). (Don't delete π_2, because later formulas in π_1 may be inferred by instance from a formula in it.) Proceeding in this way. by metamathematical induction on the number of inferences by instance in π_1, we obtain a proof of A in PRA*. The converse direction of (i) is trivial, since the axioms of PRA* are theorems of PRA and the rule of inference of PRA* is a rule of inference of PRA.

For (ii), let A be variable-free with $\pi \vdash^*$ A. Let D° be the formula obtained by replacing all variables in D by 0, and let π° consist of all D° for D in π. Then π° is a variable-free proof in PRA* of A, because if D is an axiom of PRA* so is D°; if D is inferred by modus ponens from D_1 and $D_1 \to D$, then D° is inferred by modus ponens from D_1° and $D_1^\circ \to D^\circ$; and A° is A.

For (iii), let $\pi \vdash^*$ A. Then $\chi \circ \pi \vdash^{\chi *}$ χA—for if B in π is an axiom, so is χB, and if B is inferred by modus ponens, then χB is inferred by χ-modus ponens. Conversely, if $\sigma \vdash^{\chi *}$ χA, let π consist of all B of the form $\chi^{-1}\beta = 0$ for β in σ. If β is an axiom, then $\chi^{-1}\beta$ is an axiom D of PRA*, which is a theorem of PRA, so B is $\chi D = 0$, which is a theorem of PRA by $T51, A/D$. If β is inferred by χ-modus ponens, then B is inferred by modus ponens. Hence π is a proof in PRA with citation of theorems, so $\vdash$ A. Consequently, $\vdash^*$ A by (i).

For (iv), let χA be a variable-free theorem of χ-PRA. By (iii), A is a variable-free theorem of PRA*, which by (ii) has a variable-free proof π in PRA*. As shown in the proof of (iii), $\chi \circ \pi \vdash^{\chi *}$ χA, and this proof is variable-free. □

#8. Construct the least number principle as a derived rule of inference.

If the recursion for μ_A finds an x′ such that $A_x(x')$ holds, then x′ is the least number for which $A_x(x')$ holds. This leads to the least number principle, a powerful form of induction.

T94. $A_x(x) \quad \to \quad [y < \mu_A(x) \quad \to \quad \neg A_x(y)]$

Proof. Suppose not. Then
.1 $A_x(x)$

.2 $y < \mu_A(x)$
.3 $A_x(y)$
By .3 and 85;y,
.4 $A_x(\mu_A(y))$
.5 $\mu_A(y) \leq y$
By .1 and 85;x,
.6 $A_x(\mu_A(x))$
.7 $\mu_A(x) \leq x$
By .2 and $56^{\rightarrow}$;y;$\mu_A(x)$,
.8 $y \leq \mu_A(x)$
By .8 and .7 and 73;$\mu_A(x)$;x,
.9 $y \leq x$
By .5 and .9 and 87;y;x,
.10 $\mu_A(x) = \mu_A(y)$
By .2 and .5 and .10,
.11 $y < \mu_A(y)$ & $\mu_A(y) \leq y$
QEA by .11 and 80;y;$\mu_A(y)$.

Let $\forall x{<}b\, A$ (where x does not occur in b) abbreviate $\forall x{\leq}b[x < b \rightarrow A]$. Then $\forall x{<}b\, A$ is an instance of $x < b \rightarrow A$. The following theorem schema follows from T94 by instance.

T95. $A_x(x) \quad \rightarrow \quad \forall y{<}\mu_A(x)[\neg A_x(y)]$

T96. $A_x(x) \quad \rightarrow \quad \mu_A(\mu_A(x)) = \mu_A(x)$

Proof. Suppose not. Then
.1 $A_x(x)$
.2 $\mu_A(\mu_A(x)) \neq \mu_A(x)$
By .1 and 85,
.3 $A_x(\mu_A(x))$
By .3 and 84;$\mu_A(x)$,
.4 $A_x(\mu_A(\mu_A(x)))$
.5 $\mu_A(\mu_A(x)) \leq \mu_A(x)$
By .2 and .5 and $56^{\leftarrow}$;$\mu_A(x)$;$\mu_A(\mu_A(x))$,
.6 $\mu_A(\mu_A(x)) < \mu_A(x)$
By .3 and .6 and 94;$\mu_A(x)$;$\mu_A(\mu_A(x))$,
.7 $\neg A_x(\mu_A(\mu_A(x)))$
QEA by .4 and .7.

PROPOSITION 6. *If* A *does not have a least counterexample, then* A *holds. That is, if* $\vdash \neg\{\neg A_x(z)$ & $\forall y{<}z[A_x(y)]\}$ *then* $\vdash A_x(x)$.

Proof. Suppose .0 $\vdash \neg\{\neg A_x(z)$ & $\forall y{<}z[A_x(y)]\}$. Then we prove $A_x(x)$ as follows. Suppose not. Then

.1 $\neg \mathrm{A}_{\mathrm{x}}(\mathrm{x})$
By .1 and 85, $\mathrm{A}/\neg\mathrm{A}$,
.2 $\neg \mathrm{A}(\mu_{\mathrm{A}}(\mathrm{x}))$
By .2 and 95, $\mathrm{A}/\neg\mathrm{A}, \mathrm{x}/\mu_{\mathrm{A}}(\mathrm{x})$,
.3 $\forall \mathrm{y}{<}\mu_{\neg\mathrm{A}}(\mu_{\neg\mathrm{A}}(\mathrm{x}))[\mathrm{A}_{\mathrm{x}}(\mathrm{y})]$
By .3 and .1 and 96, $\mathrm{A}/\neg\mathrm{A}$,
.4 $\forall \mathrm{y}{<}\mu_{\neg\mathrm{A}}(\mathrm{x})[\mathrm{A}_{\mathrm{x}}(\mathrm{y})]$
By .0;$\mu_{\neg\mathrm{A}}(\mathrm{x})$,
.5 $\neg\{\neg \mathrm{A}_{\mathrm{x}}(\mu_{\neg\mathrm{A}}(\mathrm{x})) \;\&\; \forall \mathrm{y}{<}\mu_{\neg\mathrm{A}}(\mathrm{x})[\mathrm{A}_{\mathrm{x}}(\mathrm{y})]\}$
By .5 and .2,
.6 $\neg\forall \mathrm{y}{<}\mu_{\neg\mathrm{A}}(\mathrm{x})[\mathrm{A}_{\mathrm{x}}(\mathrm{y})]$
QEA by .4 and .6. □

The derived rule of inference, from $\neg\{\neg \mathrm{A}_{\mathrm{x}}(\mathrm{z}) \;\&\; \forall \mathrm{y}{<}\mathrm{z}[\mathrm{A}_{\mathrm{x}}(\mathrm{y})]\}$ infer A, is the *least number principle*.

#9. Construct definition of function symbols with uniqueness condition and bounded existence condition.

PROPOSITION 7. *Let* A *contain no variables other than the distinct variables* $\vec{\mathrm{y}}$ *and* x. *The uniqueness condition* (UC) *is* $\mathrm{A}_{\mathrm{x}}(\mathrm{x}) \;\&\; \mathrm{A}_{\mathrm{x}}(\mathrm{x}') \to \mathrm{x} = \mathrm{x}'$, *where* x' *is distinct from the* $\vec{\mathrm{y}}$ *and* x. *The existence condition* (EC) *is* $\exists \mathrm{x}{\leq}\mathrm{b}\,\mathrm{A}$, *where* b *contains no variables other than those in* $\vec{\mathrm{y}}$. *If* UC *and* EC *are theorems, let* $\mathrm{f}(\vec{\mathrm{y}})$, *where* f *is a new function symbol, abbreviate* $\mu_{\mathrm{A}}(\mathrm{b})$. *Then* $\vdash \mathrm{f}(\vec{\mathrm{y}}) = \mathrm{x} \leftrightarrow \mathrm{A}$.

Proof. By definition, EC is $\mu_{\mathrm{A}}(\mathrm{b})$, and since it is a theorem, $\vdash \mathrm{A}_{\mathrm{x}}\big(\mu_{\mathrm{A}}(\mathrm{b})\big)$—i.e., $\vdash \mathrm{A}_{\mathrm{x}}\big(\mathrm{f}(\vec{\mathrm{y}})\big)$—by T89. Consequently, $\vdash \mathrm{f}(\vec{\mathrm{y}}) = \mathrm{x} \to \mathrm{A}$. The converse holds by UC. □

Such function symbols are *defined function symbols*; they occur only in abbreviations.

6. Strings

A string is a concatenation of bits. Identify the number x with the string consisting of the ones and zeros following the initial one in the binary representation of Sx. We implement this in PRA.

#10. Prove that every non-zero number Sx *can be written uniquely as* Qx+Rx *where* Qx *is a power of two and* Rx *is strictly less than* Qx.

t97*b*. $0 + 0 = 0$

Proof. H 12;0

t97*i*. $0 + x = x \quad \to \quad 0 + \mathrm{S}x = \mathrm{S}x$

Proof. H:x 12;0;x

t97. $0 + x = x$

t98*b*. $x + 0 = 0 + x$

Proof. H:x 12;x 97;x

t98*i*. $x + y = y + x \quad \to \quad x + \mathrm{S}y = \mathrm{S}y + x$

Proof. H:x:y 12;x;y 12;y;x 14;y;x

t98. $x + y = y + x$

Introduce *multiplication*. As usual, $\cdot$ binds more tightly than $+$.

r99. $x \cdot 0 = 0 \quad \& \quad x \cdot \mathrm{S}y = x + x \cdot y$

t100. $x \cdot 0 = 0 \quad \& \quad x \cdot \mathrm{S}y = x \cdot y + x$

Proof. H:x:y 99;x;y 98;x;$x \cdot y$

t101*b*. $x \cdot (y + 0) = x \cdot y + x \cdot 0$

Proof. H:x:y 12;y 100;x 12;$x \cdot y$

t101*i*. $x \cdot (y + z) = x \cdot y + x \cdot z \quad \to \quad x \cdot (y + \mathrm{S}z) = x \cdot y + x \cdot \mathrm{S}z$

Proof. H:x:y:z 12;y;z 100;x;z 100;x;$y+z$ 72;$x \cdot y$;$x \cdot z$;x

t101. $x \cdot (y + z) = x \cdot y + x \cdot z$

t102*b*. $x \cdot (y \cdot 0) = (x \cdot y) \cdot 0$

Proof. H:x:y 100;y 100;x 100;$x \cdot y$

t102*i*. $x \cdot (y \cdot z) = (x \cdot y) \cdot z \quad \to \quad x \cdot (y \cdot \mathrm{S}z) = (x \cdot y) \cdot \mathrm{S}z$

Proof. H:x:y:z 100;y;z 100;$x \cdot y$;z 101;x;$y \cdot z$;y

t102. $x \cdot (y \cdot z) = (x \cdot y) \cdot z$

t103*b*. $0 \cdot 0 = 0$

Proof. H 100;0

t103*i*. $0 \cdot x = 0 \quad \to \quad 0 \cdot \mathrm{S}x = 0$

Proof. H:x 100;0;x 12;0

t103. $0 \cdot x = 0$

t104*b*. $\mathrm{S}x \cdot 0 = x \cdot 0 + 0$

Proof. H:x 100;Sx 100;x 12;0

t104*i*. $\mathrm{S}x \cdot y = x \cdot y + y \quad \to \quad \mathrm{S}x \cdot \mathrm{S}y = x \cdot \mathrm{S}y + \mathrm{S}y$

Proof. H:x:y 100;x;y 100;Sx;y 72;$x \cdot y$;x;Sy 72;$x \cdot y$;y;Sx 14;y;x 98;Sy;x

t104. $\mathrm{S}x \cdot y = x \cdot y + y$

t105*b*. $x \cdot 0 = 0 \cdot x$

Proof. H:x 100;x 103;x

t105*i*. $x \cdot y = y \cdot x \quad \to \quad x \cdot \mathrm{S}y = \mathrm{S}y \cdot x$

Proof. H:x:y 100;x;y 104;y;x

t105. $x \cdot y = y \cdot x$

t106. $(x+y)\cdot z = x\cdot z + y\cdot z$

Proof. H:x:y:z 105;x+y;z 101;z;x;y 105;z;x 105;z;y

t107. $x \le y \quad\to\quad x\cdot z \le y\cdot z$

Proof. H:x:y:z 68;x;y 106;x;y−x;z 71;x·z;(y−x)·z

t108. $x < y \quad\to\quad x + (y-x) = y \quad \& \quad y - x \neq 0$

Proof. H:x:y 68;x;y 56$^{->}$;x;y 12;x

t109. $x < \mathrm{S}y \quad\to\quad x \le y$

Proof. H:x:y 108;x;Sy 22;Sy−x 12;x;P(Sy−x) 4;x+P(Sy−x);y 71;x;P(Sy−x)

t110. $x \le \mathrm{S}y \quad\to\quad x \le y \quad \vee \quad x = \mathrm{S}y$

Proof. H:x:y 61;x;Sy 109;x;y

t111. $\neg\,[x < y \quad \& \quad y < \mathrm{S}x]$

Proof. H:x:y 109;y;x 78;x;y

t112. $x \le y \quad\to\quad \mathrm{S}x \le \mathrm{S}y$

Proof. H:x:y 68;x;y 12;x;y−x 14;x;y−x 71;Sx;y−x

t113. $x < y \quad\to\quad \mathrm{S}x < \mathrm{S}y$

Proof. H:x:y 112;x;y 56$^{->}$;x;y 56$^{<-}$;Sx;Sy 4;x;y

t114. $x < y \quad\to\quad \mathrm{S}x \le y$

Proof. H:x:y 108;x;y 22;y−x 14;x;P(y−x) 71;Sx;P(y−x)

e115. $1 = \mathrm{S}0$

e116. $2 = \mathrm{SS}0$

t117. $1\cdot x = x$

Proof. H:x 115 104;0;x 97;x 103;x

t118. $2\cdot x = x + x$

Proof. H:x 116 115 104;1;x 117;x

t119b. $y + 0 = z + 0 \quad\to\quad y = z$

Proof. H:y:z 12;y 12;z

t119i. $[y + x = z + x \to y = z] \quad\to\quad [y + \mathrm{S}x = z + \mathrm{S}x \to y = z]$

Proof. H:y:x:z 12;y;x 12;z;x 4;y+x;z+x

t119. $y + x = z + x \quad\to\quad y = z$

t120. $x + y = x + z \quad\to\quad y = z$

Proof. H:x:y:z 98;x;y 98;x;z 119;y;x;z

t121. $y \neq 0 \quad\to\quad x < x + y$

Proof. H:y:x 71;x;y 56$^{<-}$;x;x+y 120;x;0;y 12;x

t122. $x \le y \quad \& \quad y < z \quad \to \quad x < z$

Proof. H:x:y:z $56^{\to}$;y;z 73;x;y;z $56^{\leftarrow}$;x;z 80;y;x

t123. $x < y \quad \to \quad y \neq 0$

Proof. H:x:y $56^{\to}$;x;y 57;x

t124. $x < y \quad \to \quad \mathrm{S}x < 2 \cdot y$

Proof. H:x:y 118;y 114;x;y 123;x;y 121;y;y 122;Sx;y;y+y

t125. $x < \mathrm{S}x$

Proof. H:x 59;x 79;Sx;x

Introduce *exponentiation*.

r126. $x \uparrow 0 = 1 \quad \& \quad x \uparrow \mathrm{S}y = x \cdot (x \uparrow y)$

t127b. $0 < 2 \uparrow 0$

Proof. H 116 115 126;2 125;0

t127i. $x < 2 \uparrow x \quad \to \quad \mathrm{S}x < 2 \uparrow \mathrm{S}x$

Proof. H:x 126;2;x 124;x;2↑x

t127. $x < 2 \uparrow x$

t128. $x \le 2 \uparrow x$

Proof. H:x 127;x $56^{\to}$;x;2↑x

d129. q is a power of two $\quad \leftrightarrow \quad \exists x{\le}q[2 \uparrow x = q]$ ⋆

Although "is a power of two" contains English words, it is a formal predicate symbol, written in suffix notation. The negation of "q is a power of two" is "¬ q is a power of two", whereas "q is not a power of two" is not even an expression.

t130. 1 is a power of two

Proof. H 115 $129^{\leftarrow}$;1;0 128;0 126;2

Here is the explanation of the notation $129^{\leftarrow}$;1;0 in the proof. The formula $129^{\leftarrow}$ is

$$q \text{ is a power of two} \quad \vee \quad \neg\exists x{\le}q[2 \uparrow x = q]$$

which is tautologically equivalent to

$$q \text{ is a power of two} \quad \vee \quad \forall x{\le}q[2 \uparrow x \neq q]$$

Then $129^{\leftarrow}$;1 is tautologically equivalent to

$$1 \text{ is a power of two} \quad \vee \quad \forall x{\le}1[2 \uparrow x \neq 1]$$

This is a variable-free formula and the ;0 in $129^{\leftarrow}$;1;0 is an implicit use of T90. That is, $129^{\leftarrow}$;1;0 is

$$1 \text{ is a power of two} \quad \vee \quad [0 \le 1 \quad \to \quad 2 \uparrow 0 \neq 1]$$

In general, $\forall \mathrm{x}{\le}\mathrm{b}\,\mathrm{A}$ obeys the expected rule: we can substitute any term c, indicated by ;c, and obtain $\mathrm{c} \le \mathrm{b} \to \mathrm{A}_{\mathrm{x}}(\mathrm{c})$.

t131. $2 \uparrow x$ is a power of two

Proof. H:x 116 129$^{\leftarrow}$;2$\uparrow x$;x 128;x 5;2$\uparrow x$

t132. $x \cdot y = 0 \quad \rightarrow \quad x = 0 \quad \vee \quad y = 0$

Proof. H:x:y 22;y 99;x;Py 15;x;x·Py

t133b. $2 \uparrow 0 \neq 0$

Proof. H 116 115 126;2 3;1

t133i. $2 \uparrow x \neq 0 \quad \rightarrow \quad 2 \uparrow \mathrm{S}x \neq 0$

Proof. H:x 116 115 126;2;x 132;2;2$\uparrow x$ 3;1

t133. $2 \uparrow x \neq 0$

t134. $\neg\, 0$ is a power of two

Proof. H 129$^{\rightarrow}$;0:x 133;x

Here is the explanation of the notation 129$^{\rightarrow}$;0:x in the proof. The formula 129$^{\rightarrow}$ is

$\neg\, q$ is a power of two $\quad \vee \quad \exists x{\leq}q[2 \uparrow x = q]$

so 129$^{\rightarrow}$;0 is

$\neg\, 0$ is a power of two $\quad \vee \quad \exists x{\leq}0[2 \uparrow x = 0]$

Let x abbreviate $\mu_{[\mathrm{SS}0\uparrow x=0]}(0)$ and implicitly use T89. Then 129$^{\rightarrow}$;0:x is

$\neg\, 0$ is a power of two $\quad \vee \quad [x{\leq}0 \quad \& \quad 2 \uparrow x = 0]$

In general, $\exists$x$\leq$b A obeys the expected rule: we can choose any y not previously used in the proof, hold it fixed, indicated by :y, and obtain y $\leq$ b & $\mathrm{A_x(y)}$.

t135. q is a power of two $\quad \rightarrow \quad 2 \cdot q$ is a power of two

Proof. H:q 129$^{\rightarrow}$;q:x 129$^{\leftarrow}$;2·q;Sx 126;2;x 128;Sx

t136b. $x \uparrow (y + 0) = (x \uparrow y) \cdot (x \uparrow 0)$

Proof. H:x:y 12;y 126;x 117;$x\uparrow y$ 105;$x\uparrow y$;1

t136i. $x \uparrow (y + z) = (x \uparrow y) \cdot (x \uparrow z) \quad \rightarrow \quad x \uparrow (y + \mathrm{S}z) = (x \uparrow y) \cdot (x \uparrow \mathrm{S}z)$

Proof. H:x:y:z 12;y;z 126;x;y+z 126;x;z 102;x;$x\uparrow y$;$x\uparrow z$ 102;$x\uparrow y$;x;$x\uparrow z$ 105;x;$x\uparrow y$

t136. $x \uparrow (y + z) = (x \uparrow y) \cdot (x \uparrow z)$

t137. $x \neq 0 \quad \rightarrow \quad x < 2 \cdot x$

Proof. H:x 22;x 125;Px 124;Px;x

t138. $0 \leq x$

Proof. H:x 97;x 71;0;x

t139. $x \neq 0 \quad \rightarrow \quad 1 \leq x$

Proof. H:x 116 115 22;x 138;Px 112;0;Px

t140. $x \neq 0 \quad \rightarrow \quad 2 \leq 2 \uparrow x$

Proof. H:x 116 115 127;x 114;x;$2 \uparrow x$ 139;x 112;1;x 73;2;Sx;$2 \uparrow x$

t141a. $x \cdot z = y \cdot z \quad \& \quad x < y \quad \& \quad z \neq 0 \quad \rightarrow \quad x = y$

Proof. H:x:z:y 108;x;y 106;x;$y-x$;z 132;$y-x$;z 12;$x \cdot z$ 120;$x \cdot z$;0;$(y-x) \cdot z$

t141. $x \cdot z = y \cdot z \quad \& \quad z \neq 0 \quad \rightarrow \quad x = y$

Proof. H;x;z;y 141a;x;z;y 141a;y;z;x 77;x;y

t142. $x \leq y \quad \rightarrow \quad z \cdot x \leq z \cdot y$

Proof. H:x:y:z 107;x;y;z 105;z;x 105;z;y

t143. $x \neq 0 \quad \rightarrow \quad x < x \cdot 2$

Proof. H:x 137;x 105;x;2

t144. $x < y \quad \& \quad y \leq z \quad \rightarrow \quad x < z$

Proof. H:x:y:z 56$^{\rightarrow}$;x;y 73;x;y;z 56$^{\leftarrow}$;x;z 80;x;y

t145. $x < y \quad \rightarrow \quad 2 \uparrow x < 2 \uparrow y$

Proof. H:x:y 108;x;y 136;2;x;$y-x$ 140;$y-x$ 142;2;$2 \uparrow (y-x)$;$2 \uparrow x$ 133;x 143;$2 \uparrow x$ 144;$2 \uparrow x$;$(2 \uparrow x) \cdot 2$;$2 \uparrow y$

t146. $x \leq y \quad \rightarrow \quad 2 \uparrow x \leq 2 \uparrow y$

Proof. H:x:y 61;x;y 145;x;y 56$^{\rightarrow}$;$2 \uparrow x$;$2 \uparrow y$ 60;$2 \uparrow x$

t147. $2 \uparrow x < 2 \uparrow y \quad \rightarrow \quad x < y$

Proof. H:x:y 77;x;y 56$^{\rightarrow}$;$2 \uparrow x$;$2 \uparrow y$ 145;y;x 80;$2 \uparrow x$;$2 \uparrow y$ 56$^{\rightarrow}$;$2 \uparrow y$;$2 \uparrow x$

t148a. $2 \uparrow x = 2 \uparrow y \quad \rightarrow \quad \neg \, x < y$

Proof. H:x:y 145;x;y 56$^{\rightarrow}$;$2 \uparrow x$;$2 \uparrow y$

t148. $2 \uparrow x = 2 \uparrow y \quad \rightarrow \quad x = y$

Proof. H:x:y 148a;x;y 148a;y;x 77;x;y

t149. $\neg$ [q is a power of two $\quad \& \quad$ q' is a power of two $\quad \& \quad q < q' \quad \& \quad q' < 2 \cdot q$]

Proof. H:q:q' 135;q 129$^{\rightarrow}$;q:x 129$^{\rightarrow}$;q':y 129$^{\rightarrow}$;$2 \cdot q$:z 126;2;x 147;x;y 147;y;z 148;Sx;z 111;x;y

d150. $\mathrm{p}_{150}(q, x) \quad \leftrightarrow \quad q$ is a power of two $\quad \& \quad q \leq \mathrm{S}x \quad \& \quad \mathrm{S}x < 2 \cdot q$

t151a. $\mathrm{p}_{150}(q, x) \quad \& \quad \mathrm{p}_{150}(q', x) \quad \rightarrow \quad \neg \, q < q'$

Proof. H:q:x:q' 150$^{\rightarrow}$;q;x 150$^{\rightarrow}$;q';x 149;q;q' 122;q';Sx;$2 \cdot q$ 56$^{\rightarrow}$;q;q'

t151. $\mathrm{p}_{150}(q,x) \quad \& \quad \mathrm{p}_{150}(q',x) \quad \to \quad q = q'$

Proof. H:q:x:q' 151a;q;x;q' 151a;q';x;q 77;q;q'

t152. $\mathrm{p}_{150}(q,x) \quad \& \quad \mathrm{SS}x < 2\cdot q \quad \to \quad \mathrm{p}_{150}(q,\mathrm{S}x)$

Proof. H:q:x 150$^{\to}$;q;x 150$^{\leftarrow}$;q;Sx 63;Sx 73;q;Sx;SSx

t153. $\mathrm{p}_{150}(q,x) \quad \& \quad \neg\, \mathrm{SS}x < 2\cdot q \quad \to \quad \mathrm{p}_{150}(2\cdot q,\mathrm{S}x)$

Proof. H:q:x 150$^{\to}$;q;x 150$^{\leftarrow}$;$2\cdot q$;Sx 135;q 124;Sx;$2\cdot q$ 114;Sx;$2\cdot q$ 56$^{\leftarrow}$;SSx;$2\cdot q$ 60;SSx

t154. $x \le y \quad \to \quad x \le \mathrm{S}y$

Proof. H:x:y 63;y 73;x;y;Sy

t155. $\mathrm{p}_{150}(q,x) \quad \to \quad \exists q_1{\le}\mathrm{SS}x[\mathrm{p}_{150}(q_1,\mathrm{S}x)]$

Proof. H:q:x^A ^{A};q ^{A};$2\cdot q$ 152;q;x 153;q;x 150$^{\to}$;q;x 150$^{\to}$;$2\cdot q$;Sx 154;q;Sx

The formula H:q:x is tautologically equivalent to $\mathrm{p}_{150}(q,x)\ \&\ \forall q_1{\le}\mathrm{SS}x[\neg\mathrm{p}_{150}(q_1,\mathrm{S}x)]$. The superscript ^{A} labels the remnant $\forall q_1{\le}\mathrm{SS}x[\neg\mathrm{p}_{150}(q_1,\mathrm{S}x)]$ for later substitution of values for q_1.

t156b. $\exists q{\le}1[\mathrm{p}_{150}(q,0)]$

Proof. H;1 116 115 150$^{\leftarrow}$;1;0 130 60;1 3;0 137;1

t156i. $\exists q{\le}\mathrm{S}x[\mathrm{p}_{150}(q,x)] \quad \to \quad \exists q_1{\le}\mathrm{SS}x[\mathrm{p}_{150}(q_1,\mathrm{S}x)]$

Proof. H:x:q^A 155;q;x:q_1 ^{A};q_1

Note that $\exists q{\le}\mathrm{S}x[\mathrm{p}_{150}(q,x)]$ is $\mu_{\mathrm{A}}(\mathrm{S}x)$ where A is $\mathrm{p}_{150}(q,x)$, and $\exists q_1{\le}\mathrm{SS}x[\mathrm{p}_{150}(q_1,\mathrm{S}x)]$ is $\mu_{\mathrm{A}_1}(\mathrm{S}x)$ where A_1 is $\mathrm{A}_q(q_1)$. By the remark after R82 they are the same formula, so induction applies.

t156. $\exists q{\le}\mathrm{S}x[\mathrm{p}_{150}(q,x)]$

d157. $\mathrm{Q}x = q \quad \leftrightarrow \quad \mathrm{p}_{150}(q,x)$

By 151 (UC) and 156 (EC) (and Proposition 7).

t158. $\mathrm{Q}x$ is a power of two $\quad \& \quad \mathrm{Q}x \le \mathrm{S}x \quad \& \quad \mathrm{S}x < 2\cdot\mathrm{Q}x$ ⋆

Proof. H:x 157$^{\to}$;x;Qx 150$^{\to}$;Qx;x 5;Qx

Qx expresses $\lfloor \log_2(x+1) \rfloor$, the largest power of two less than $x+1$.

t159. q is a power of two $\quad \& \quad q \le \mathrm{S}x \quad \& \quad \mathrm{S}x < 2\cdot q \quad \to \quad q = \mathrm{Q}x$ ⋆

Proof. H:q:x 150$^{\leftarrow}$;q;x 157$^{\leftarrow}$;x;q

e160. $\mathrm{R}x = \mathrm{S}x - \mathrm{Q}x$

t161. $\mathrm{S}x = \mathrm{Q}x + \mathrm{R}x$

Proof. H:x 158;x 160;x 68;Qx;Sx

t162. $x < y \quad \to \quad \exists w{\le}y[x + w = y \quad \& \quad w \ne 0]$

Proof. H:x:y;$y{-}x$ 108;x;y 98;x;$y{-}x$ 71;$y{-}x$;x

t163. $x + y = z \quad \& \quad y \neq 0 \quad \to \quad x < z$

Proof. H:x:y:z $56^{<-}$;x;z 71;x;y 12;x 120;x;y;0

t164. $x + y < x + z \quad \to \quad y < z$

Proof. H:x:y:z 162;x+y;x+z:w 72;x;y;w 120;x;y+w;z 163;y;w;z

t165. $\mathrm{R}x < \mathrm{Q}x$

Proof. H:x 161;x 158;x 118;Qx 164;Qx;Rx;Qx

t166. $\mathrm{S}x = \mathrm{Q}x + \mathrm{R}x \quad \& \quad \mathrm{Q}x$ is a power of two $\quad \& \quad \mathrm{R}x < \mathrm{Q}x$ $\star$

Proof. H:x 161;x 158;x 165;x

t167. $x \leq y \quad \to \quad \exists w{\leq}y[x + w = y]$

Proof. H:x:y;$y-x$ 68;x;y 98;x;$y-x$ 71;$y-x$;x

t168. $x + y \leq x + z \quad \to \quad y \leq z$

Proof. H:x:y:z 167;x+y;x+z:w 72;x;y;w 120;x;y+w;z 71;y;w

t169. $x + y \leq x + z \quad \to \quad y \leq z$

Proof. H:x:y:z 167;x+y;x+z:w 72;x;y;w 120;x;y+w;z 71;y;w

t170. $x < y \quad \to \quad x + z < y + z$

Proof. H:x:y:z 79;y+z;x+z 98;y;z 98;x;z 168;z;y;x 80;x;y

t171. $\mathrm{S}x = q + r \quad \& \quad q$ is a power of two $\quad \& \quad r < q \quad \to \quad q = \mathrm{Q}x \quad \& \quad r = \mathrm{R}x$ $\star$

Proof. H:x:q:r 71;q;r 118;q 98;q;r 170;r;q;q 159;q;x 120;Qx;r;Rx 161;x

#11. Introduce concatenation of strings and prove a few of its properties.

e172. $x \oplus y = \mathrm{P}(\mathrm{S}x \cdot \mathrm{Q}y + \mathrm{R}y)$ $\star$

Why is $\oplus$ called concatenation? As an example, consider the string 101 (i.e., the number x such that Sx in binary is 1101) and the string 01 (i.e., the number y such that Sy in binary is 101). In binary, Qy is 100, Ry is 1, and S$x \cdot$ Qy + Ry is 110101, so $x \oplus y$ is the string 10101 (i.e., the number whose successor in binary is 110101).

String arithmetic is analogous to number arithmetic, with one zero, ϵ, but with two successors: $x \mapsto x \oplus \underline{0}$ and $x \mapsto x \oplus \underline{1}$. Concatenation is the string analogue of addition. We have founded string arithmetic on number arithmetic, but we need to develop it to the point that it becomes independent of this foundation.

t173. $x \neq 0 \quad \& \quad y < z \quad \to \quad y < x \cdot z$

Proof. H:x:y:z 22;x 104;Px;z 98;Px·z;z 71;z;Px·z 144;y;z;x·z

t174. $x < y \quad \to \quad z + x < z + y$

Proof. H:x:y:z 98;z;x 98;z;y 170;x;y;z

t175. $r < q \quad \& \quad r' < q' \quad \to \quad r \cdot q' + r' < q \cdot q'$

Proof. H:r:q:r':q' 162;r;q:w 162;r';q':w' 101;r;r';w' 106;r;w;r'+w' 173;w;r';q' 174;r';w·q';r·r'+r·w'

t176. $\mathrm{R}x \cdot \mathrm{Q}y + \mathrm{R}y < \mathrm{Q}x \cdot \mathrm{Q}y$

Proof. H:x:y 166;x 166;y 175;Rx;Qx;Ry;Qy

t177. q_1 is a power of two & q_2 is a power of two $\rightarrow$ $q_1 \cdot q_2$ is a power of two

Proof. H:q_1:q_2 129$^{\rightarrow}$;q_1:x_1 129$^{\rightarrow}$;q_2:x_2 136;2;x_1;x_2 131;x_1+x_2

t178. $\mathrm{Q}x \neq 0$

Proof. H:x 158;x 134

t179. $\mathrm{S}(x \oplus y) = \mathrm{S}x \cdot \mathrm{Q}y + \mathrm{R}y$

Proof. H;x;y 172;x;y 22;Sx·Qy+Ry 15;Sx·Qy;Ry 3;x 178;y 132;Sx;Qy

t180. $\mathrm{Q}(x \oplus y) = \mathrm{Q}x \cdot \mathrm{Q}y$ & $\mathrm{R}(x \oplus y) = \mathrm{R}x \cdot \mathrm{Q}y + \mathrm{R}y$

Proof. H:x:y 179;x;y 166;x 166;y 106;Qx;Rx;Qy 72;Qx·Qy;Rx·Qy;Ry 177;Qx;Qy 176;x;y 171;x⊕y;Qx·Qy;Rx·Qy+Ry

t181. $\mathrm{Q}\big(x \oplus (y \oplus z)\big) = \mathrm{Q}\big((x \oplus y) \oplus z\big)$

Proof. H:x:y:z 180;y;z 180;x;y 180;x;y⊕z 180;x⊕y;z 102;Qx;Qy;Qz

t182. $\mathrm{R}\big(x \oplus (y \oplus z)\big) = \mathrm{R}\big((x \oplus y) \oplus z\big)$

Proof. H:x:y:z 180;y;z 180;x;y 180;x;y⊕z 180;x⊕y;z 102;Rx;Qy;Qz 106;Rx·Qy;Ry;Qz 72;Rx·Qy·Qz;Ry·Qz;Rz

t183. $x \oplus (y \oplus z) = (x \oplus y) \oplus z$ ⋆

Proof. H:x:y:z 181;x;y;z 182;x;y;z 166;x⊕(y⊕z) 166;(x⊕y)⊕z 4;(x⊕y)⊕z;x⊕(y⊕z)

t184. $x_1 \leq y_1$ & $x_2 \leq y_2$ $\rightarrow$ $x_1 + x_2 \leq y_1 + y_2$

Proof. H:x_1:y_1:x_2:y_2 167;x_1;y_1:w_1 167;x_2;y_2:w_2 72;x_1;w_1;x_2+w_2 72;w_1;x_2;w_2 98;w_1;x_2 72;x_2;w_1;w_2 72;x_1;x_2;w_1+w_2 71;x_1+x_2;w_1+w_2

With our identification of strings with numbers, 0 is the empty string, 1 is the zero bit, and 2 is the one bit. For greater readability, introduce new notation for these objects emphasizing their role as strings.

e185. $\epsilon = 0$ ⋆

e186. $\underline{0} = 1$ ⋆

e187. $\underline{1} = 2$ ⋆

t188. $\underline{0} \neq \epsilon$ & $\underline{1} \neq \epsilon$ & $\underline{0} \neq \underline{1}$ ⋆

Proof. H 116 115 185 186 187 3;0 3;1 4;0;1

t189. $\mathrm{Q}\epsilon = 1$ & $\mathrm{R}\epsilon = 0$

Proof. H 116 115 185 12;1 125;0 130 171;0;1;0

t190. 2 is a power of two

Proof. H 116 115 131;1 126;2;0 117;2 105;2;1

t191. $\mathrm{Q}\underline{0} = 2$ & $\mathrm{R}\underline{0} = 0$

Proof. H 116 115 186 12;2 190 125;0 125;1 56$^{\rightarrow}$;0;1 122;0;1;2 171;1;2;0

t192. $\underline{\mathrm{Q}1} = 2 \quad \& \quad \underline{\mathrm{R}1} = 1$

Proof. H 116 115 187 12;2;0 190 125;1 171;2;2;1

t193. $\mathrm{Q}x = \mathrm{Q}y \quad \& \quad \mathrm{R}x = \mathrm{R}y \quad \to \quad x = y$

Proof. H:x:y 166;x 166;y 4;x;y

t194. $\epsilon \oplus x = x$ ⋆

Proof. H:x 193;$\epsilon\oplus x$;x 189 180;ϵ;x 117;Qx 103;Qx 97;Rx

t195. $x \cdot 1 = x$

Proof. H:x 117;x 105;x;1

t196. $x \oplus \epsilon = x$ ⋆

Proof. H:x 193;$x\oplus\epsilon$;x 189 180;x;ϵ 195;Qx 195;Rx 12;Rx

t197. $y \oplus x = z \oplus x \quad \to \quad y = z$ ⋆

Proof. H:y:x:z 180;y;x 180;z;x 178;x 141;Qy;Qx;Qz 119;Ry·Qx;Rx;Rz·Qx 141;Ry;Qx;Rz 193;y;z

t198. $x \cdot y = x \cdot z \quad \& \quad x \neq 0 \quad \to \quad y = z$

Proof. H:x:y:z 105;x;y 105;x;z 141;y;x;z

t199. $x \oplus y = x \oplus z \quad \to \quad y = z$ ⋆

Proof. H:x:y:z 180;x;y 180;x;z 178;x 198;Qx;Qy;Qz 120;Rx·Qy;Ry;Rz 193;y;z

t200. $x \leq 1 \quad \to \quad x = 0 \quad \vee \quad x = 1$

Proof. H:x 116 115 167;x;1:w 22;w 12;x;Pw 4;x+Pw;0 15;x;Pw

t201. $x \neq 0 \quad \to \quad y \leq x \cdot y$

Proof. H:x:y 22;x 104;Px;y 98;P$x\cdot y$;y 71;y;P$x\cdot y$

t202. $x \cdot y = 1 \quad \to \quad x = 1 \quad \& \quad y = 1$

Proof. H:x:y 116 115 103;y 105;x;y 103;x 201;x;y 201;y;x 200;x 200;y 3;0

t203. $\mathrm{Q}x = 1 \quad \to \quad x = \epsilon$

Proof. H:x 116 115 185 12;1 166;x 200;Rx 56$^{\to}$;Rx;1 4;x;0

t204. $x \oplus y = \epsilon \quad \to \quad x = \epsilon \quad \& \quad y = \epsilon$ ⋆

Proof. H:x:y 180;x;y 189 202;Qx;Qy 203;x 203;y

r205. $\mathrm{Parity}\,0 = 0 \quad \& \quad \mathrm{Parity}\,\mathrm{S}x = \mathrm{C}(\mathrm{Parity}\,x, 1, 0)$

Parity $x = 0$ expresses that x is even, and Parity $x = \mathrm{S}0$ that x is odd.

t206. $\mathrm{Parity}\,x = 0 \quad \to \quad \mathrm{Parity}\,\mathrm{S}x = 1$

Proof. H:x 205;x 33;1;0;0

t207. $\mathrm{Parity}\,x = 1 \quad \to \quad \mathrm{Parity}\,\mathrm{S}x = 0$

Proof. H:x 116 115 205;x 33;1;0;0

t208. $\text{Parity}\,0 = 0 \quad \& \quad \text{Parity}\,1 = 1 \quad \& \quad \text{Parity}\,2 = 0 \quad \& \quad \text{Parity}\,\epsilon = 0 \quad \& \quad \text{Parity}\,\underline{0} = 1 \quad \& \quad \text{Parity}\,\underline{1} = 0$

Proof. H 116 115 205;0 205;1 185 186 187 33;1;0;0

t209. $\text{Parity}\,x = 0 \quad \vee \quad \text{Parity}\,x = 1$

Proof. H:x 116 115 205;x 205;Px 22;x 39;Parity Px

t210b. $\text{Parity}\,x = 0 \quad \rightarrow \quad \text{Parity}(x + 0) = \text{Parity}\,0$

Proof. H:x 208 12;x

t210i. $[\text{Parity}\,x = 0 \quad \rightarrow \quad \text{Parity}(x + y) = \text{Parity}\,y] \quad \rightarrow \quad [\text{Parity}\,x = 0 \quad \rightarrow \quad \text{Parity}(x + \text{S}y) = \text{Parity S}y]$

Proof. H:x:y 12;x;y 205;x+y 205;y

t210. $\text{Parity}\,x = 0 \quad \rightarrow \quad \text{Parity}(x + y) = \text{Parity}\,y$

t211b. $\text{Parity}\,x = 0 \quad \rightarrow \quad \text{Parity}(x \cdot 0) = 0$

Proof. H:x 100;x 205

t211i. $[\text{Parity}\,x = 0 \quad \rightarrow \quad \text{Parity}(x \cdot y) = 0] \quad \rightarrow \quad [\text{Parity}\,x = 0 \quad \rightarrow \quad \text{Parity}(x \cdot \text{S}y) = 0]$

Proof. H:x:y 99;x;y 210;x;x·y

t211. $\text{Parity}\,x = 0 \quad \rightarrow \quad \text{Parity}(x \cdot y) = 0$

t212. $\text{Parity}(x \cdot 2 + y) = \text{Parity}\,y$

Proof. *H*:x:y 208 105;x;2 211;2;x 210;2·x;y

t213. $\text{Parity}(x \cdot 2) = 0$

Proof. H:x 212;x;0 208 12;x·2

t214. $\text{Parity}(x \cdot 2 + 1) = 1$

Proof. H:x 212;x;1 208

t215. $\text{Parity R}(x \oplus \underline{0}) = 0$

Proof. H:x 180;x;$\underline{0}$ 191 212;Rx;0 205

t216. $\text{Parity R}(x \oplus \underline{1}) = 1$

Proof. H:x 180;x;$\underline{1}$ 192 212;Rx;1 208

t217. $x \oplus \underline{0} \neq y \oplus \underline{1}$ ⋆

Proof. H:x:y 116 115 215;x 216;y 3;0

#12. Construct the unary PR *function symbol* Chop *that deletes the last bit, if any, of a string.*

r218. $\text{Half}\,0 = 0 \quad \& \quad \text{Half S}x = \text{C}(\text{Parity}\,x, \text{Half}\,x, \text{S Half}\,x)$

Half x expresses $\lfloor x/2 \rfloor$. It deletes the rightmost binary bit of x (if x is not 0 or 1).

t219. $\text{Parity}\,x = 0 \quad \rightarrow \quad \text{Half S}x = \text{Half}\,x$

Proof. H:x 218;x 33;Half x;S Half$x$

t220. $\mathrm{Parity}\, x = 1 \quad \to \quad \mathrm{Half}\, \mathrm{S}x = \mathrm{S}\, \mathrm{Half}\, x$

Proof. H:x 116 115 218;x 33;Half x;S Half$x$;0

t221. $\mathrm{Half}\, 0 = 0 \quad \& \quad \mathrm{Half}\, 1 = 0 \quad \& \quad \mathrm{Half}\, 2 = 1 \quad \& \quad \mathrm{Half}\, \mathrm{S}2 = 1$

Proof. H 116 115 218;0 218;1 218;2 208 219;x 33;0;1;0 33;0;2;1 33;1;2;0

d222. $\mathrm{p}_{222}(x) \quad \leftrightarrow \quad [\mathrm{Parity}\, x = 0 \quad \to \quad x = 2 \cdot \mathrm{Half}\, x] \quad \& \quad [\mathrm{Parity}\, x = 1 \quad \to \quad x = 2 \cdot \mathrm{Half}\, x + 1]$

t223b. $\mathrm{p}_{222}(0)$

Proof. H 116 115 222$^{<-}$;0 205 221 99;2 3;0

t223i. $\mathrm{p}_{222}(x) \quad \to \quad \mathrm{p}_{222}(\mathrm{S}x)$

Proof. H:x 116 115 222$^{->}$;x 222$^{<-}$;Sx ?Parity x=1 209;x 3;0 12;2·Half x;0 206;x 207;x 219;x 220;x 12;2·Half x;1 100;2;Half x

t223. $\mathrm{p}_{222}(x)$

t224. $\mathrm{Parity}\, x = 0 \quad \to \quad x = 2 \cdot \mathrm{Half}\, x$

Proof. H:x 223;x 222$^{->}$;x

t225. $\mathrm{Parity}\, x = 1 \quad \to \quad x = 2 \cdot \mathrm{Half}\, x + 1$

Proof. H:x 223;x 222$^{->}$;x

t226. $x \leq 2 \cdot \mathrm{Half}\, x + 1$

Proof. H:x 224;x 225;x 71;2·Half x;1 209;x 60;x

t227. $\mathrm{Half}\, x = 0 \quad \to \quad x = 0 \quad \vee \quad x = 1$

Proof. H:x 226;x 100;2 97;1 200;x

t228. $x \neq \epsilon \quad \to \quad \mathrm{Half}\, \mathrm{Q}x + \mathrm{Half}\, \mathrm{R}x \neq 0$

Proof. H:x 15;Half Qx;Half Rx 227;Qx 178;x 203;x

e229. $\mathrm{Chop}\, x = \mathrm{P}(\mathrm{Half}\, \mathrm{Q}x + \mathrm{Half}\, \mathrm{R}x)$

Chop x deletes the rightmost bit, if any, of the string x. It is the string analogue of P.

t230. $\mathrm{Chop}\, \epsilon = \epsilon$ ⋆

Proof. H 229;ϵ 189 185 221 12;0 16

t231. $x \neq \epsilon \quad \to \quad \mathrm{S}\, \mathrm{Chop}\, x = \mathrm{Half}\, \mathrm{Q}x + \mathrm{Half}\, \mathrm{R}x$

Proof. H:x 229;x 228;x 22;Half Qx+Half Rx

t232. $2 \cdot \mathrm{Half}\, x \leq x$

Proof. H:x 224;x 225;x 60;x 71;2·Half x;1 209;x

t233. $\mathrm{Parity}\, q = 0 \quad \& \quad r < q \quad \to \quad \mathrm{Half}\, r < \mathrm{Half}\, q$

Proof. H:q:r 79;Half q;Half r 224;q 118;Half q 184;Half q;Half r;Half q;Half r 232;r 118;Half r 73;q;Half r+Half r;r 80;r;q

t234. $\mathrm{Parity}(2\uparrow \mathrm{S}x) = 0$

Proof. H:x 126;2;x 208 211;2;2↑x

t235. $\mathrm{Half}(2\uparrow \mathrm{S}x) = 2\uparrow x$

Proof. H:x 116 115 234;x 224;2↑Sx 126;2;x 3;1 198;2;Half(2↑Sx);2↑x

t236. q is a power of two & $q \neq 1$ → Parity $q = 0$

Proof. H:q 129$^{\rightarrow}$;q:x 126;2;x 22;x 134 234;Px

t237. $x \neq 0$ → Half$(2\uparrow x)$ is a power of two

Proof. H;x 116 115 22;x 235;Px 131;Px

t238. $x \neq \epsilon$ → Half Qx is a power of two

Proof. H:x 158;x 116 115 129$^{\rightarrow}$;Qx:y 126;2 203;x 237;y

t239. $x \neq \epsilon$ → Q Chop x = Half Qx & R Chop x = Half Rx

Proof. H:x 171;Chop x;Half Qx;Half Rx 231;x 238;x 236;Qx 166;x 203;x 233;Q x;Rx

t240. Chop $\underline{0} = \epsilon$ & Chop $\underline{1} = \epsilon$ ⋆

Proof. H 239;$\underline{0}$ 239;$\underline{1}$ 188 191 192 221 203;Chop $\underline{0}$ 203;Chop $\underline{1}$

t241b. Half$(0 \cdot 2) = 0$ & Half$(0 \cdot 2 + 1) = 0$

Proof. H 103;2 97;1 221

t241i. Half$(x{\cdot}2{+}1) = x$ & Half$(x{\cdot}2) = x$ → Half$(\mathrm{S}x{\cdot}2{+}1) = \mathrm{S}x$ & Half$(\mathrm{S}x{\cdot}2) = \mathrm{S}x$

Proof. H:x 116 115 104;x;2 12;$x{\cdot}2$;1 212;x;1 208 220;$x{\cdot}2{+}1$ 12;$x{\cdot}2{+}2$;0 12;S$(x{\cdot}2{+}2)$ 212;x;2 219;$x{\cdot}2{+}2$

t241. Half$(x \cdot 2 + 1) = x$ & Half$(x \cdot 2) = x$

t242. $x \oplus \underline{0} \neq \epsilon$ & $x \oplus \underline{1} \neq \epsilon$

Proof. H:x 204;x;$\underline{0}$ 204;x;$\underline{1}$ 188

t243. Chop$(x \oplus \underline{0}) = x$ ⋆

Proof. H:x 242;x 239;$x{\oplus}\underline{0}$ 180;x;$\underline{0}$ 191 241;Qx 241;Rx 12;R$x{\cdot}2$ 193;x;Chop$(x{\oplus}\underline{0})$

t244. Chop$(x \oplus \underline{1}) = x$ ⋆

Proof. H:x 242;x 239;$x{\oplus}\underline{1}$ 180;x;$\underline{1}$ 192 241;Qx 241;Rx 12;R$x{\cdot}2$ 193;x;Chop$(x{\oplus}\underline{1})$

t245. $x \neq \epsilon$ → Q(Chop $x \oplus \underline{0}$) = Qx & Q(Chop $x \oplus \underline{1}$) = Qx

Proof. H:x 180;Chop x;$\underline{0}$ 180;Chop x;$\underline{1}$ 191 192 158;x 203;x 236;Qx 224;Qx 239;x 105;2;Q Chop x

t246. Parity x = Parity y & Half x = Half y → $x = y$

Proof. H:x:y 224;x 224;y 225;x 225;y 221;x 209;x ?Parity x=0

t247. $x \neq \epsilon$ → R(Chop$x \oplus \underline{0}$) = Half R $x \cdot 2$

Proof. H:x 180;Chop x;$\underline{0}$ 191 12;R Chop $x{\cdot}2$ 239;x

t248. $x \neq \epsilon$ & Parity R$x = 0$ → R(Chop $x \oplus \underline{0}$) = Rx

Proof. H:x 247;x 241;Half Rx 213;Half Rx 246;R(Chop $x{\oplus}\underline{0}$);Rx

t249. $x \neq \epsilon \quad \to \quad \mathrm{R}(\mathrm{Chop}x \oplus \underline{1}) = \mathrm{Half}\,\mathrm{R}x \cdot 2 + 1$

Proof. H:x 180;Chop x;$\underline{1}$ 192 239;x

t250. $x \neq \epsilon \quad \& \quad \mathrm{Parity}\,\mathrm{R}x = 1 \quad \to \quad \mathrm{R}(\mathrm{Chop}\,x \oplus \underline{1}) = \mathrm{R}x$

Proof. H:x 249;x 241;Half Rx 214;Half Rx 246;R(Chop $x\oplus\underline{1}$);Rx

t251. $x \neq \epsilon \quad \& \quad \mathrm{Parity}\,\mathrm{R}x = 0 \quad \to \quad x = \mathrm{Chop}\,x \oplus \underline{0}$

Proof. H:x 245;x 248;x 193;x;Chop $x\oplus\underline{0}$

t252. $x \neq \epsilon \quad \& \quad \mathrm{Parity}\,\mathrm{R}x = 1 \quad \to \quad x = \mathrm{Chop}\,x \oplus \underline{1}$

Proof. H:x 245;x 250;x 193;x;Chop $x\oplus\underline{1}$

t253. $x \neq \epsilon \quad \to \quad x = \mathrm{Chop}\,x \oplus \underline{0} \quad \vee \quad x = \mathrm{Chop}\,x \oplus \underline{1}$ $\star\star$

Proof. H:x 251;x 252;x 209;Rx

t254. $y \neq \epsilon \quad \to \quad \mathrm{Chop}(x \oplus y) = x \oplus \mathrm{Chop}\,y$ $\star$

Proof. H:y:x 253;y 183;x;Chop y;$\underline{0}$ 183;x;Chop y;$\underline{1}$ 243;$x\oplus$Chop y 244;$x\oplus$Chop y

#13. Establish string recursion and string induction.

PROPOSITION 8. *Let* $\vec{\mathrm{x}}$, y, *and* z *be distinct, let* a *contain no variables other than those in* $\vec{\mathrm{x}}$, *and let* b *and* c *contain no variables other than those in* $\vec{\mathrm{x}}$, y, *and* z. *Define* f *by primitive recursion by cases:*

$$\begin{aligned}(6)\qquad &\mathrm{f}(\vec{\mathrm{x}}, 0) = \mathrm{a} \quad \& \quad \mathrm{f}(\vec{\mathrm{x}}, \mathrm{Sy}) = \\ &\mathrm{C}\big(\chi[\mathrm{Sy} = \mathrm{Chop}\,\mathrm{Sy} \oplus \underline{0}], \mathrm{b_z}(\mathrm{Chop}\,\mathrm{Sy}), \mathrm{C}(\chi[\mathrm{Sy} = \mathrm{Chop}\,\mathrm{Sy} \oplus \underline{1}], \mathrm{c_z}(\mathrm{Chop}\,\mathrm{Sy}), 0)\big)\end{aligned}$$

Then

$$(7)\qquad \mathrm{f}(\vec{\mathrm{x}}, \epsilon) = \mathrm{a} \quad \& \quad \mathrm{f}(\vec{\mathrm{x}}, \mathrm{w} \oplus \underline{0}) = \mathrm{b_z}(\mathrm{w}) \quad \& \quad \mathrm{f}(\vec{\mathrm{x}}, \mathrm{w} \oplus \underline{1}) = \mathrm{c_z}(\mathrm{w})$$

Proof. We have $\mathrm{f}(\vec{\mathrm{x}}, \epsilon) = \mathrm{a}$ by 185. By Proposition 4 of §4,

$$(8)\qquad \mathrm{Sy} = \mathrm{Chop}\,\mathrm{Sy} \oplus \underline{0} \quad \to \quad \mathrm{f}(\vec{\mathrm{x}}, \mathrm{Sy}) = \mathrm{b_z}(\mathrm{Chop}\,\mathrm{Sy})$$
$$(9)\qquad \neg[\mathrm{Sy} = \mathrm{Chop}\,\mathrm{Sy} \oplus \underline{0}] \quad \& \quad [\mathrm{Sy} = \mathrm{Chop}\,\mathrm{Sy} \oplus \underline{1}] \quad \to \quad \mathrm{f}(\vec{\mathrm{x}}, \mathrm{Sy}) = \mathrm{c_z}(\mathrm{Chop}\,\mathrm{Sy})$$
$$(10)\qquad \neg[\mathrm{Sy} = \mathrm{Chop}\,\mathrm{Sy} \oplus \underline{0}] \quad \& \quad \neg[\mathrm{Sy} = \mathrm{Chop}\,\mathrm{Sy} \oplus \underline{1}] \quad \to \quad \mathrm{f}(\vec{\mathrm{x}}, \mathrm{Sy}) = 0$$

By 217;Chop Sy;Chop Sy and (9),

$$(11)\qquad \mathrm{Sy} = \mathrm{Chop}\,\mathrm{Sy} \oplus \underline{1} \quad \to \quad \mathrm{f}(\vec{\mathrm{x}}, \mathrm{Sy}) = \mathrm{c_z}(\mathrm{Chop}\,\mathrm{Sy})$$

Note that (10), the "else" clause, is irrelevant, since its hypothesis cannot hold, by 253;Sy together with 3;y and 185. Now consider (8);P(w $\oplus\,\underline{0}$):

$$\mathrm{SP}(\mathrm{w} \oplus \underline{0}) = \mathrm{Chop}\,\mathrm{SP}(\mathrm{w} \oplus \underline{0}) \oplus \underline{0} \quad \to \quad \mathrm{f}(\vec{\mathrm{x}}, \mathrm{SP}(\mathrm{w} \oplus \underline{0})) = \mathrm{b_z}(\mathrm{Chop}\,\mathrm{SP}(\mathrm{w} \oplus \underline{0}))$$

We have $\mathrm{w} \oplus \underline{0} \neq 0$ (by 185 and 204;w;$\underline{0}$ and 188), so $\mathrm{SP}(\mathrm{w} \oplus \underline{0}) = \mathrm{w} \oplus \underline{0}$ by 22;w$\oplus\underline{0}$. Also, $\mathrm{Chop}(\mathrm{w} \oplus \underline{0}) = \mathrm{w}$ by 243;w. Therefore

$$\mathrm{w} \oplus \underline{0} = \mathrm{w} \oplus \underline{0} \quad \to \quad \mathrm{f}(\vec{\mathrm{x}}, \mathrm{w} \oplus \underline{0}) = \mathrm{b}_{\mathrm{z}}(\mathrm{w})$$

and so $\mathrm{f}(\vec{\mathrm{x}}, \mathrm{w} \oplus \underline{0}) = \mathrm{b}_{\mathrm{z}}(\mathrm{w})$. The derivation of $\mathrm{f}(\vec{\mathrm{x}}, \mathrm{w} \oplus \underline{1}) = \mathrm{c}_{\mathrm{z}}(\mathrm{w})$ from (11);$\mathrm{SP}(\mathrm{w} \oplus \underline{1})$ is entirely similar. Hence (7). □

A *string recursion* is a primitive recursion of the form (6), but string recursions will be introduced simply by (7).

t255. $x < x \oplus \underline{0}$

Proof. H:x 172;x;$\underline{0}$ 191 12;Sx·2 105;Sx;2 118;Sx 12;Sx;x 16;Sx+x 71;Sx;x 125;x 144;x;Sx;Sx+x

t256. $x + 1 = \mathrm{S}x$

Proof. H:x 115 12;x;0

t257. $x < x \oplus \underline{1}$

Proof. H:x 172;x;$\underline{1}$ 192 256;Sx·2 16;Sx·2 105;Sx;2 118;Sx 125;x 71;Sx;Sx 144;x;Sx;Sx+Sx

t258. $x \neq \epsilon \quad \to \quad \mathrm{Chop}\, x < x$

Proof. H:x 253;x 255;Chop x 257;Chop x

PROPOSITION 9. *If* $\vdash \mathrm{A}_{\mathrm{x}}(\epsilon)$ *and* $\vdash \mathrm{A}_{\mathrm{x}}(\mathrm{x}') \to \mathrm{A}_{\mathrm{x}}(\mathrm{x}' \oplus \underline{0})$ *and* $\vdash \mathrm{A}_{\mathrm{x}}(\mathrm{x}') \to \mathrm{A}_{\mathrm{x}}(\mathrm{x}' \oplus \underline{1})$, *then* $\vdash \mathrm{A}_{\mathrm{x}}(\mathrm{x})$.

Proof. Suppose that

(12) $$\mathrm{A}_{\mathrm{x}}(\epsilon)$$

(13) $$\mathrm{A}_{\mathrm{x}}(\mathrm{x}') \quad \to \quad \mathrm{A}_{\mathrm{x}}(\mathrm{x}' \oplus \underline{0})$$

(14) $$\mathrm{A}_{\mathrm{x}}(\mathrm{x}') \quad \to \quad \mathrm{A}_{\mathrm{x}}(\mathrm{x}' \oplus \underline{1})$$

and use the least number principle (Proposition 6 of §5). Suppose that there is a least counterexample z to A:

(15) $$\neg \mathrm{A}_{\mathrm{x}}(\mathrm{z}) \quad \& \quad \forall \mathrm{y}{<}\mathrm{z}[\mathrm{A}_{\mathrm{x}}(\mathrm{y})]$$

We have $\mathrm{z} \neq \epsilon$ by (12). Then, by 253;z,

(16) $$\mathrm{z} = \mathrm{Chop}\, \mathrm{z} \oplus \underline{0} \quad \vee \quad \mathrm{z} = \mathrm{Chop}\, \mathrm{z} \oplus \underline{1}$$

By (15);z;Chop z and 258;z,

$$\mathrm{A}_{\mathrm{x}}(\mathrm{Chop}\, \mathrm{z})$$

The first alternative of (16) does not hold, by (13);Chop z, and the second does not hold, by (14);Chop z. Hence $\mathrm{A}_{\mathrm{x}}(\mathrm{x})$ by the least number principle. □

The derived rule of inference, from $\mathrm{A}_{\mathrm{x}}(\epsilon)$ and $\mathrm{A}_{\mathrm{x}}(\mathrm{x}') \to \mathrm{A}_{\mathrm{x}}(\mathrm{x}' \oplus \underline{0})$ and $\mathrm{A}_{\mathrm{x}}(\mathrm{x}') \to \mathrm{A}_{\mathrm{x}}(\mathrm{x}' \oplus \underline{1})$ infer $\mathrm{A}_{\mathrm{x}}(\mathrm{x})$, is *string induction.*

#14. Construct Length *by string recursion, and introduce* $\preceq$ *(shorter than) and* $\prec$ *(strictly shorter than). Prove* $x \preceq y \to x \leq 2 \cdot \mathrm{Q}x$ *and* $x \prec y \to x < y$. *The first will enable bounded quantifiers with bounding symbol* $\preceq$ *rather than* $\leq$, *and the second will enable the use of the least number principle for strings ("the shortest string principle"). Express the i'th bit of a string.*

r259. $\mathrm{Length}\,\epsilon = 0 \quad \& \quad \mathrm{Length}(x \oplus \underline{0}) = \mathrm{S}\,\mathrm{Length}\,x \quad \& \quad \mathrm{Length}(x \oplus \underline{1}) = \mathrm{S}\,\mathrm{Length}\,x \;\star$

t260b. $\mathrm{Length}(x \oplus \epsilon) = \mathrm{Length}\,x + \mathrm{Length}\,\epsilon$

Proof. H:x 196;x 259 12;$\mathrm{Length}\,x$

t260ij. $\mathrm{Length}(x \oplus y) = \mathrm{Length}\,x + \mathrm{Length}\,y \quad \to \quad \mathrm{Length}\big(x \oplus (y \oplus \underline{0})\big) = \mathrm{Length}\,x + \mathrm{Length}(y \oplus \underline{0}) \quad \& \quad \mathrm{Length}\big(x \oplus (y \oplus \underline{1})\big) = \mathrm{Length}\,x + \mathrm{Length}(y \oplus \underline{1})$

Proof. H:x:y 259;y 183;x;y;$\underline{0}$ 183;x;y;$\underline{1}$ 259;$x\oplus y$ 12;$\mathrm{Length}\,x$;$\mathrm{Length}\,y$

t260. $\mathrm{Length}(x \oplus y) = \mathrm{Length}\,x + \mathrm{Length}\,y$

When tξ immediately follows tξb, tξi, and tξj, it is an inference by string induction. Sometimes, as here, the two string induction steps are combined into a single formula tξij.

t261b. $\mathrm{Q}\epsilon = 2 \uparrow (\mathrm{Length}\,\epsilon)$

Proof. H 259 126;2 189

t261ij. $\mathrm{Q}x = 2{\uparrow}\mathrm{Length}\,x \quad \to \quad \mathrm{Q}(x{\oplus}\underline{0}) = 2{\uparrow}\mathrm{Length}(x{\oplus}\underline{0}) \quad \& \quad \mathrm{Q}(x{\oplus}\underline{1}) = 2{\uparrow}\mathrm{Length}(x{\oplus}\underline{1})$

Proof. H:x 259;x 126;2;$\mathrm{Length}\,x$ 180;x;$\underline{0}$ 180;x;$\underline{1}$ 191 192 105;$\mathrm{Q}x$;2

t261. $\mathrm{Q}x = 2 \uparrow \mathrm{Length}\,x$

t262. $x \leq \mathrm{S}y \quad \to \quad x \leq y \quad \vee \quad x = \mathrm{S}y$

Proof. H:x:y 68;x;Sy 22;S$y{-}x$ 12;x;P(S$y{-}x$) 4;y;x+P(S$y{-}x$) 71;x;P(S$y{-}x$)

t263b. $x \leq 0 \quad \to \quad 2 \uparrow x \leq 2 \uparrow 0$

Proof. H:x 57;x 60;2↑0

t263i. $[x \leq y \quad \to \quad 2 \uparrow x \leq 2 \uparrow y] \quad \to \quad [x \leq \mathrm{S}y \quad \to \quad 2 \uparrow x \leq 2 \uparrow \mathrm{S}y]$

Proof. H:x:y 262;x;y 60;2↑x 126;2;y 118;2↑y 71;2↑y;2↑y 73;2↑x;2↑y;2·(2↑y)

t263. $x \leq y \quad \to \quad 2 \uparrow x \leq 2 \uparrow y$

d264. $x \preceq y \quad \leftrightarrow \quad \mathrm{Length}\,x \leq \mathrm{Length}\,y$

d265. $x \prec y \quad \leftrightarrow \quad \mathrm{Length}\,x < \mathrm{Length}\,y$

t266. $x \leq y \quad \to \quad 2 \cdot x \leq 2 \cdot y$

Proof. H:x:y 118;x 118;y 184;x;y;x;y

t267. $x \preceq y \quad \to \quad x \leq 2 \cdot \mathrm{Q}y$ $\star$

Proof. H:x:y 264$^{\to}$;x;y 263;$\mathrm{Length}\,x$;$\mathrm{Length}\,y$ 261;x 261;y 158;x 63;x 56$^{\to}$;Sx;2·Qx 73;x;Sx;2·Qx 266;Qx;Qy 73;x;2·Qx;2·Qy

Let s be a binary predicate symbol, written in infix notation. If for some term d containing no variable other than y we have $\vdash x\ \mathrm{s}\ y \to x \leq \mathrm{d}$, then we call s a *bounding symbol* with *bound* d. Thus $\preceq$ is a bounding symbol with bound $2 \cdot \mathrm{Q}y$ by t267. For a bounding symbol s with bound d let $\exists \mathrm{x}\,\mathrm{s}\,\mathrm{b}\,\mathrm{A}$ abbreviate $\exists \mathrm{x} {\leq} \mathrm{d}_y(\mathrm{b})[\mathrm{x}\ \mathrm{s}\ \mathrm{b}\ \&\ \mathrm{A}]$ and $\forall \mathrm{x}\,\mathrm{s}\,\mathrm{b}\,\mathrm{A}$ abbreviate $\forall \mathrm{x} {\leq} \mathrm{d}_y(\mathrm{b})[\mathrm{x}\ \mathrm{s}\ \mathrm{b} \to \mathrm{A}]$. (The bound d is not unique, but we choose one, and it is implicit in the notations $\exists \mathrm{x}\,\mathrm{s}\,\mathrm{b}\,\mathrm{A}$ and $\forall \mathrm{x}\,\mathrm{s}\,\mathrm{b}\,\mathrm{A}$.) We have already used these abbreviations for the bounding symbol $<$ (with bound y).

t268. $\mathrm{SR}x < \mathrm{Q}x \quad \to \quad \mathrm{QS}x = \mathrm{Q}x$

Proof. H:x 166;x 12;Qx;Rx 171;Sx;Qx;SRx

t269. q is a power of two $\quad \to \quad 0 < q$

Proof. H:q 134 58;q 56$^{\leftarrow}$;0;q

t270. $\mathrm{SR}x = \mathrm{Q}x \quad \to \quad \mathrm{QS}x = 2 \cdot \mathrm{Q}x$

Proof. H:x 166;x 190 177;2;Qx 12;Qx;Rx 118;Qx 269;2·Qx 12;2·Qx 171;Sx;2·Qx;0

t271. $\mathrm{Q}x \leq \mathrm{QS}x$

Proof. H:x 60;Qx 268;x 166;x 270;x 118;Qx 71;Qx;Qx 114;Rx;Qx 56$^{\leftarrow}$;SRx;Qx

t272b. $x \leq 0 \quad \to \quad \mathrm{Q}x \leq \mathrm{Q}0$

Proof. H:x 57;x 60;Q0

t272i. $[x \leq y \quad \to \quad \mathrm{Q}x \leq \mathrm{Q}y] \quad \to \quad [x \leq \mathrm{S}y \quad \to \quad \mathrm{Q}x \leq \mathrm{QS}y]$

Proof. H:x:y 110;x;y 60;QSy 271;y 73;Qx;Qy;QSy

t272. $x \leq y \quad \to \quad \mathrm{Q}x \leq \mathrm{Q}y$

t273. $x \prec y \quad \to \quad x < y$ $\star$

Since Length $x <$ Length y, we have $\mathrm{Q}x < \mathrm{Q}y$ by t261 and t145. If $\neg\ x < y$, then $y \leq x$, so $\mathrm{Q}y \leq \mathrm{Q}x$ by t272, a contradiction. It is essential to have the strict bound y itself on $\prec$ to apply the least number principle to strings.

Proof. H:x:y 265$^{\rightarrow}$;x;y 145;Length x;Length y 261;x 261;y 272;y;x 80;Qx;Qy 79;y;x

t274. $\epsilon \preceq x \quad \& \quad x \preceq x$

Proof. H:x 264$^{\leftarrow}$;ϵ;x 264$^{\leftarrow}$;x;x 259 58;Length x 60;Length x

t275. $x \preceq y \quad \& \quad y \preceq z \quad \to \quad x \preceq z$

Proof. H:x:y:z 264$^{\rightarrow}$;x;y 264$^{\rightarrow}$;y;z 73;Length x;Length y;Length z 264$^{\leftarrow}$;x;z

t276. $x \oplus y \preceq y \oplus x$

Proof. H:x:y 260;x;y 260;y;x 98;Length x;Length y 60;Length x+Length y 264$^{\leftarrow}$;$x\oplus y$;$y\oplus x$

t277. $x \preceq x \oplus y \quad \& \quad y \preceq x \oplus y$

Proof. H:x:y 264$^{\leftarrow}$;x;$x\oplus y$ 264$^{\leftarrow}$;y;$x\oplus y$ 260;x;y 71;Length x;Length y 98;Length x;Length y 71;Length y;Length x

t278. $\mathrm{Length}\,\underline{0} = 1 \quad \& \quad \mathrm{Length}\,\underline{1} = 1$

Proof. H 259;ϵ 194;$\underline{0}$ 194;$\underline{1}$ 115

t000b. $x_1 \oplus \epsilon = x_2 \oplus \epsilon \quad \to \quad x_1 = x_2$sam000b. H:$x_1$:$x_2$ 196;x_1 196;x_2

t000i. $[x_1 \oplus y = x_2 \oplus y \quad \to \quad x_1 = x_2] \quad \to \quad [x_1 \oplus y \oplus \underline{0} = x_2 \oplus y \oplus \underline{0} \quad \to \quad x_1 = x_2]$

Proof. H:x_1:y:x_2 183;x_1;y;$\underline{0}$ 183;x_2;y;$\underline{0}$ 243;$x_1\oplus y$ 243;$x_2\oplus y$

t000j. $[x_1 \oplus y = x_2 \oplus y \quad \to \quad x_1 = x_2] \quad \to \quad [x_1 \oplus y \oplus \underline{1} = x_2 \oplus y \oplus \underline{1} \quad \to \quad x_1 = x_2]$

Proof. H:x_1:y:x_2 183;x_1;y;$\underline{1}$ 183;x_2;y;$\underline{1}$ 244;$x_1\oplus y$ 244;$x_2\oplus y$

t000. $x_1 \oplus y = x_2 \oplus y \quad \rightarrow \quad x_1 = x_2$

t001. $\text{Length}\, x = 0 \quad \rightarrow \quad x = \epsilon$

Proof. H:x 253;x 260;Chop x;$\underline{0}$ 260;Chop x;$\underline{1}$ 278 15;Length Chop x;1 115 3;0

d288. x ends with $c \quad \leftrightarrow \quad \exists a \preceq x[x = a \oplus c]$

t289. $a \oplus c$ ends with c

Proof. H:a:c 277;a;c 288$^{\leftarrow}$;$a\oplus c$;c;a 5;$a\oplus c$

d290. x begins with $a \quad \leftrightarrow \quad \exists c \preceq x[x = a \oplus c]$

t291. $a \oplus c$ begins with a

Proof. H:a:c 277;a;c 290$^{\leftarrow}$;$a\oplus c$;a;c 5;$a\oplus c$

t292. x begins with $a \quad \rightarrow \quad x \oplus y$ begins with a

Proof. H:x:a:y 290$^{\rightarrow}$;x;a:c 183;a;c;y 291;a;$c\oplus y$

t293. y ends with $c \quad \rightarrow \quad x \oplus y$ ends with c

Proof. H:y:c:x 288$^{\rightarrow}$;y;c:a 183;x;a;c 289;$x\oplus a$;c

t294. x ends with $x \quad \& \quad x$ ends with $\epsilon \quad \& \quad x$ begins with $x \quad \& \quad x$ begins with ϵ

Proof. H:x 194;x 196;x 289;ϵ;x 289;x;ϵ 291;ϵ;x 291;x;ϵ

t002. ϵ begins with $x \quad \vee \quad \epsilon$ ends with $x \quad \rightarrow \quad x = \epsilon$

Proof. H:x 290$^{\rightarrow}$;ϵ;x:c 288$^{\rightarrow}$;ϵ;x:a 204;x;c 204;a;x

t005. $x_1 + y_1 = x_2 + y_2 \quad \& \quad x_1 \leq x_2 \quad \rightarrow \quad y_2 \leq y_1$

Proof. H:x_1:y_1:x_2:y_2 68;x_1;x_2 72;x_1;$x_2 - x_1$;y_2 120;x_1;y_1;$(x_2 - x_1) + y_2$ 98;$x_2 - x_1$;y_2 71;y_2;$x_2 - x_1$

t006. $a_1 \oplus c_1 = a_2 \oplus c_2 \quad \& \quad a_1 \preceq a_2 \quad \rightarrow \quad c_2 \preceq c_1$

Proof. H:a_1:c_1:a_2:c_2 264$^{\rightarrow}$;a_1;a_2 264$^{\leftarrow}$;c_2;c_1 260;a_1;c_1 260;a_2;c_2 005;Length a_1;Length c_1; Length a_2;Length c_2

t008. $x \preceq \epsilon \quad \rightarrow \quad x = \epsilon$

Proof. H:x 264$^{\rightarrow}$;x;ϵ 57;Length x 001;x 259

t007. $a_1 \oplus c_1 = a_2 \oplus c_2 \quad \& \quad a_1 \preceq a_2 \quad \& \quad c_2 \neq \epsilon \quad \rightarrow \quad c_1 \neq \epsilon$

Proof. H:a_1:c_1:a_2:c_2 006;a_1;c_1;a_2;c_2 008;c_2

t003*b*. ϵ begins with $a_1 \quad \& \quad \epsilon$ begins with $a_2 \quad \& \quad a_1 \preceq a_2 \quad \rightarrow \quad a_2$ begins with a_1

Proof. H:a_1:a_2 002;a_1 002;a_2 294;ϵ

t003*i*. [x begins with $a_1 \quad \& \quad x$ begins with $a_2 \quad \& \quad a_1 \preceq a_2 \quad \rightarrow \quad a_2$ begins with a_1] $\rightarrow$ [$x \oplus \underline{0}$ begins with $a_1 \quad \& \quad x \oplus \underline{0}$ begins with $a_2 \quad \& \quad a_1 \preceq a_2 \quad \rightarrow \quad a_2$ begins with a_1]

Proof. Suppose not. Then
.1 x begins with a_1 & x begins with a_2 & $a_1 \preceq a_2 \rightarrow a_2$ begins with a_1
.2 $x \oplus \underline{0}$ begins with a_1
.3 $x \oplus \underline{0}$ begins with a_2
.4 $a_1 \preceq a_2$

.5 $\neg$ a_2 begins with a_1
By .3 and 290$^{\rightarrow}$;$x \oplus \underline{0}$;a_2:c_2,
.6 $x \oplus \underline{0} = a_2 \oplus c_2$
By 196;a_2,
.7 $a_2 \oplus \epsilon = a_2$
Claim: $c_2 \neq \epsilon$. Suppose not. Then
.8 $c_2 = \epsilon$
By .6 and .7,
.9 $x \oplus \underline{0} = a_2$
The claim is proved by .2 and .5 and .9, and .8–.9 will not be used again.
.10 $c_2 \neq \epsilon$
By 254;a_2;c_2 and .10,
.11 $\mathrm{Chop}(a_2 \oplus c_2) = a_2 \oplus \mathrm{Chop}\, c_2$
By 243;x,
.12 $\mathrm{Chop}(x \oplus \underline{0}) = x$
By .6 and .12 and .11,
.13 $x = a_2 \oplus \mathrm{Chop}\, c_2$
By 291;a_2;Chop c_2 and .13,
.14 x begins with a_2
By .2 and 290$^{\rightarrow}$;$x \oplus \underline{0}$;a_1:c_1,
.15 $x \oplus \underline{0} = a_1 \oplus c_1$
By 196;a_1,
.16 $a_1 \oplus \epsilon = \epsilon$
By 007;a_1;c_1;a_2;c_2 and .6 and .15 and .4 and .10,
.17 $c_1 \neq \epsilon$
By 254;a_1;c_1 and .17,
.18 $\mathrm{Chop}(a_1 \oplus c_1) = a_1 \oplus \mathrm{Chop}\, c_1$
By 291;a_1;Chopc_1 an .18 and .12 and .15,
.19 x begins with a_1
QEA by .1 and .19 and .14 and .4 and .5.

t003j. [x begins with a_1 & x begins with a_2 & $a_1 \preceq a_2$ $\rightarrow$ a_2 begins with a_1] $\rightarrow$ [$x \oplus \underline{1}$ begins with a_1 & $x \oplus \underline{1}$ begins with a_2 & $a_1 \preceq a_2$ $\rightarrow$ a_2 begins with a_1]

The proof is entirely similar: replace each $\underline{0}$ by $\underline{1}$ and 243 by 244.

t003. x begins with a_1 & x begins with a_2 & $a_1 \preceq a_2$ $\rightarrow$ a_2 begins with a_1

t010. x begins with y & y begins with x $\rightarrow$ $x = y$

Proof. H:x:y 290$^{\rightarrow}$;x;y:c 290$^{\rightarrow}$;y;x:d 183;x;d;c 196;x 199;x;ϵ;$d \oplus c$ 204;d;c

t011. x ends with y & y ends with x $\rightarrow$ $x = y$

Proof. H:x:y 288$^{\rightarrow}$;x;y:c 288$^{\rightarrow}$;y;x:d 194;x 183;c;d;x 197;ϵ;x;$c \oplus d$ 204;c;d

d012. last-bit(x, b) $\leftrightarrow$ [$x = \mathrm{Chop}x \oplus \underline{0}$ & $b = \underline{0}$] $\vee$ [$x = \mathrm{Chop}x \oplus \underline{1}$ & $b = \underline{1}$] $\vee$ [$x = \epsilon$ & $b = \epsilon$]

t013. last-bit(x, b_1) & last-bit(x, b_2) $\rightarrow$ $b_1 = b_2$

Proof. H:x:b_1:b_2 012$^{\rightarrow}$;x;b_1 012$^{\rightarrow}$;x;b_2 253;x ?$x \neq \epsilon$

Afterword on two works by Ed Nelson

Sam Buss and Terence Tao

Two of Ed Nelson's unfinished papers, *Elements* (dated March 12, 2013) and *Inconsistency of Primitive Recursive Arithmetic* (undated, also known as the *Balrog* paper) have the goal of proving the inconsistency of number theory. As Nelson writes in *Elements*, "The aim of this work is to show that contemporary mathematics, including Peano arithmetic, is inconsistent ...".

Neither of these papers have been circulated before in their current forms. An earlier version of *Elements* was circulated in 2011, but was found to have problems in its treatment of proofs generated by Chaitin machines. The new 2013 version uses a similar approach, but gives a much more detailed explanation of the planned proof, and it handles Chaitin machines differently so as to address the earlier problems.

Nelson's remarkable program to establish the inconsistency of Peano arithmetic was intertwined with his development of Internal Set Theory [4] and especially Predicative Arithmetic [5]. Predicative Arithmetic is a constructive fragment of arithmetic, and Nelson's development of Predicative Arithmetic was inspired in part by Yessenin-Volpin's ultra-intuitionistic set theory [6]. The mathematical content of Predicate Arithmetic is closely tied to theories of bounded arithmetic such as $\mathrm{I}\Delta_0$, $\mathrm{I}\Delta_0 + \Omega_1$, S^i_2 and T^i_2. Indeed, Nelson [5] independently discovered some of the important tools for bounded arithmetic, including the technique of speeding up induction on cuts and the local interpretability of predicative arithmetic and bounded arithmetic in Robinson's theory Q. Nelson's Predicative Arithmetic was also influential for the definition by one of us (Buss) of the theories S^i_2 and T^i_2 of bounded arithmetic, including notably the use of Nelson's smash function.

The *Elements* manuscript gives a detailed, high-level outline of Nelson's plan for a proof of the inconsistency of Peano arithmetic (and primitive recursive arithmetic). One of the principal tools is a novel use of a recent proof by Kritchman and Raz [3] of Godel's second incompleteness theorem based on the "surprise examination". Nelson also uses Kolmogorov complexity and techniques from cut-elimination. The detailed plan of the inconsistency proof is outlined as Steps 1-17 in section 9 near the end of *Elements*. The plan first discusses a system S^* which is a predicative theory including bounded induction and which is strong enough to express concepts about metamathetical concepts, Chaitin machine computation, and Kolmogorov complexity. Step 7 introduces a finitary theory $\mathcal{F}$; the details of the system $\mathcal{F}$ are not fully specified, but it needs to be able to formalize cut-elimination or normalization. Thus it seems that $\mathcal{F}$ can be taken to be, for instance, $\mathrm{I}\Delta_0 + \mathrm{superexp}$ or $\mathrm{I}\Sigma_1$. The heart of the argument is reached in Step 16. Unfortunately, the argument becomes very uncertain here. Nelson argues that S^* disproves a sequence of statements:

first $A_{\kappa,0}$, then $A_{\kappa,1}$, etc., up through $A_{\kappa,I}$. The base case that S^* disproves $A_{\kappa,0}$ is fine, but the later stages are unclear. It seems that the disproof of $A_{\kappa,\delta}$ requires an assumption that S^* is consistent. The reason for this is that the Chaitin machine cannot be given the value of δ as an input since the Kolmogorov complexity of δ may not be sufficiently below that of κ. The only alternative to explicitly specifying δ that we can think of, is for the Chaitin machine to first search for the S^* proof that "$\neg A_{\kappa,\delta+1}$" and then also wait until δ many strings are found to have Chaitin complexity less than κ. This however assumes that S^* is consistent. Of course, S^* does not prove its own consistency. Perhaps Nelson had a different argument in mind, but this is our best attempt to flesh out his arguments. At any rate, Nelson was apparently aware of the potential problem here, since he earlier discusses the need for a system to prove the "consistency of its own arithmetization".

In the spirit of a quote by Carl Sagan, "Extraordinary claims require extraordinary evidence", Nelson planned to fulfill his inconsistency proof by exhibiting a fully formal, computer-verified derivation of a contradiction. That is, he planned not to prove that there is a proof of contradiction, but to actually exhibit an explicit proof of a contradiction. The first steps of this are carried out at the end of *Elements*, and it is even further pursued in *Balrog*. The *Balrog* manuscript is still incomplete, as only six sections are complete, and at least ten sections were planned. The *Balrog* manuscript is in essence a formalization of the "bootstrapping" of predicative arithmetic in the spirit of [5]. A remarkable feature of *Balrog* is that proofs of theorems are indicated in a terse fashion that permits a Perl program, called *qea*, to automatically verify the proofs. For instance, Theorems *13b.* and *13i.* of *Balrog*, and their proofs, are typeset with the TeX code

```
\" \t//13b.  0 + 0 = 0 + 0 \"

\sam13b.
\"\p/13b.
/\'H' \
/5 ; 0 + 0 \
\"

\" \t/13i.  x + 0 = 0 + x \imp \'S' x + 0 = 0 + \'S' x \"

\sam13i.
\"\p/13i.
/\'H' : x \
/12 ; \'S' x \
/12 ; 0 ; x \
/12 ; x \
\"
```

These indicate that *13b.* is proved by substituting 0+0 for x in axiom *a5.*, and that *13i.* is proved by using definition *r12.* three times, first substituting Sx

for x, then 0 and x for x and y, and finally x for x. After these substitutions, the desired conclusions follow propositionally from equality axioms. The *qea* system then automatically generated an expanded proof; the expanded proof was produced as a TeX file, and automatically converted to PDF. An example is shown in an appendix to the *Balrog* manuscript posted to the *arXiv*.

We of course believe that Peano arithmetic is consistent; thus we do not expect that Nelson's project can be completed according to his plans. Nonetheless, there is much new in his papers that is of potential mathematical, philosophical and computational interest. For this reason, they are being posted to the *arXiv*. Two aspects of these papers seem particularly useful. The first aspect is the novel use of the "surprise examination" and Kolmogorov complexity; there is some possibility that similar techniques might lead to new separation results for fragments of arithmetic. The second aspect is Nelson's automatic proof-checking via TeX and *qea*. This is highly interesting and provides a novel method of integrating human-readable proofs with computer verification of proofs.

The reader interested in further discussion of Nelson's Predicative Arithmetic can consult the mostly-survey article [1]. The volume [2] contains papers about many other aspects of Nelson's wide-ranging research. Other works by Nelson are available at `math.princeton.edu/~nelson`, including a number of philosophical works.

[1] S. R. Buss, *Nelson's work on logic and foundations and other reflections on foundations of mathematics*, in Diffusion, Quantum Theory, and Radically Elementary Mathematics, Princeton University Press, 2006, pp. 183–208. Edited by W. Faris.

[2] W. G. Faris, ed., *Diffusion, Quantum Theory, and Radically Elementary Mathematics*, Mathematical Notes, #47, Princeton University Press, 2006.

[3] S. Kritchman and R. Raz, *The surprise examination and the second incompleteness theorem*, Notices of the American Mathematical Society, 57 (2010), pp. 1454–1458.

[4] E. Nelson, *Internal set theory: A new approach to nonstandard analysis*, Bulletin of the American Mathematical Society, 83 (1977), pp. 1165–1198.

[5] E. Nelson, *Predicative Arithmetic*, Princeton University Press, 1986.

[6] A. S. Yessenin-Volpin, *The ultra-intuitionistic criticism and the antitraditional program for foundations of mathematics*, in Intuitionism and Proof Theory, A. Kino, J. Myhill, and R. E. Vesley, eds., North-Holland, 1970, pp. 1–45.

Sam Buss

Terence Tao

August 31, 2015

Appendix

Example: Expanded proof of Balrog 13i

Nelson's *qea* proof system consists of a Perl script which reads the TeX source code, and checks the proof correctness and generates an expanded version of the proof. The *Balrog* and *Elements* documents contained active hyperlinks, in a blue font, to these expanded proofs.

As an example, the expanded version of the proof of *13i.* in *Balrog* as generated by *qea* is shown below.

Proof of Theorem 13i

The theorem to be proved is

$x + 0 = 0 + x \quad \rightarrow \quad \mathrm{S}x + 0 = 0 + \mathrm{S}x$

Suppose the theorem does not hold. Then, with the variables held fixed,

(H) $\quad [[(x + 0) = (0 + x)] \quad \& \quad [\neg\, ((\mathrm{S}x) + 0) = (0 + (\mathrm{S}x))]]$

Special cases of the hypothesis and previous results:

0: $\quad 0 + x = x + 0 \qquad$ from $\quad$ H:x

1: $\quad \neg\, (\mathrm{S}x) + 0 = 0 + (\mathrm{S}x) \qquad$ from $\quad$ H:x

2: $\quad (\mathrm{S}x) + 0 = \mathrm{S}x \qquad$ from $\quad$ 12;Sx

3: $\quad \mathrm{S}(0 + x) = 0 + (\mathrm{S}x) \qquad$ from $\quad$ 12;0;x

4: $\quad x + 0 = x \qquad$ from $\quad$ 12;x

Equality substitutions:

5: $\quad \neg\, 0 + x = x + 0 \quad \vee \quad \neg\, \mathrm{S}(0 + x) = 0 + (\mathrm{S}x) \quad \vee \quad \mathrm{S}(x + 0) = 0 + (\mathrm{S}x)$

6: $\quad \neg\, (\mathrm{S}x) + 0 = \mathrm{S}x \quad \vee \quad (\mathrm{S}x) + 0 = 0 + (\mathrm{S}x) \quad \vee \quad \neg\, \mathrm{S}x = 0 + (\mathrm{S}x)$

7: $\quad \neg\, x + 0 = x \quad \vee \quad \neg\, \mathrm{S}(x + 0) = 0 + (\mathrm{S}x) \quad \vee \quad \mathrm{S}(x) = 0 + (\mathrm{S}x)$

Inferences:

8: $\neg\, \mathrm{S}(0+x) = 0 + (\mathrm{S}x) \quad \vee \quad \mathrm{S}(x+0) = 0 + (\mathrm{S}x)$ by

0: $0 + x = x + 0$

5: $\neg\, 0 + x = x + 0 \quad \vee \quad \neg\, \mathrm{S}(0+x) = 0 + (\mathrm{S}x) \quad \vee \quad \mathrm{S}(x+0) = 0 + (\mathrm{S}x)$

9: $\neg\, (\mathrm{S}x) + 0 = \mathrm{S}x \quad \vee \quad \neg\, 0 + (\mathrm{S}x) = \mathrm{S}x$ by

1: $\neg\, (\mathrm{S}x) + 0 = 0 + (\mathrm{S}x)$

6: $\neg\, (\mathrm{S}x) + 0 = \mathrm{S}x \quad \vee \quad (\mathrm{S}x) + 0 = 0 + (\mathrm{S}x) \quad \vee \quad \neg\, 0 + (\mathrm{S}x) = \mathrm{S}x$

10: $\neg\, 0 + (\mathrm{S}x) = \mathrm{S}x$ by

2: $(\mathrm{S}x) + 0 = \mathrm{S}x$

9: $\neg\, (\mathrm{S}x) + 0 = \mathrm{S}x \quad \vee \quad \neg\, 0 + (\mathrm{S}x) = \mathrm{S}x$

11: $\mathrm{S}(x+0) = 0 + (\mathrm{S}x)$ by

3: $\mathrm{S}(0+x) = 0 + (\mathrm{S}x)$

8: $\neg\, \mathrm{S}(0+x) = 0 + (\mathrm{S}x) \quad \vee \quad \mathrm{S}(x+0) = 0 + (\mathrm{S}x)$

12: $\neg\, \mathrm{S}(x+0) = 0 + (\mathrm{S}x) \quad \vee \quad 0 + (\mathrm{S}x) = \mathrm{S}x$ by

4: $x + 0 = x$

7: $\neg\, x + 0 = x \quad \vee \quad \neg\, \mathrm{S}(x+0) = 0 + (\mathrm{S}x) \quad \vee \quad 0 + (\mathrm{S}x) = \mathrm{S}x$

13: $\neg\, \mathrm{S}(x+0) = 0 + (\mathrm{S}x)$ by

10: $\neg\, 0 + (\mathrm{S}x) = \mathrm{S}x$

12: $\neg\, \mathrm{S}(x+0) = 0 + (\mathrm{S}x) \quad \vee \quad 0 + (\mathrm{S}x) = \mathrm{S}x$

14: QEA by

11: $\mathrm{S}(x+0) = 0 + (\mathrm{S}x)$

13: $\neg\, \mathrm{S}(x+0) = 0 + (\mathrm{S}x)$