How precious also are thy thoughts unto me, O God! how great is the sum of them! If I should count them, they are more in number than the sand; when I awake, I am still with thee.

(Psalm 139, 17–18)

Part A

Positive Results on Fragments of Arithmetic

Chapter I

Arithmetic as Number Theory, Set Theory and Logic

Introduction

We are going to investigate axiomatic theories formulated in the language L_0 of arithmetic. Such a theory T is *sound* if the standard model N is a model of T, i.e. all axioms of T are true in N. If T is sound then, trivially, each formula provable in T is true in N. We confine our attention to theories containing a rather weak finitely axiomatized theory Q (which will be defined in a moment) and shall study an infinite hierarchy of sound theories whose union is called *Peano arithmetic;* the theories from the hierarchy are called *fragments* of Peano arithmetic. In this chapter and the next, we shall elaborate *positive* results on these theories, i.e. we shall show that the expressive and deductive power of these fragments is rather big: our aim will be to show how some amount of arithmetization of metamathematics yields the possibility of speaking inside a fragment of arithmetic not only of numbers but also of finite sets and sequences and of definable infinite sets of numbers. This is the main result of Sect. 1. In Sect. 2 we shall study the structure of the hierarchy of fragments, i.e. show various equivalent axiomatizations and several inclusions among fragments. Section 3 is devoted to the development of some recursion theory in fragments, notably to a proof of the Low basis theorem, which can be viewed as a strong form of König's lemma. (The Low basis theorem will be crucial in proofs of combinatorial principles in fragments; this will be done in Chap. II.) Finally Sect. 4 further develops metamathematics in fragments; among other things, the Low arithmetized completeness theorem, i.e. a strong form of the completeness theorem, will be proved.

Let us close this introduction with two remarks: first, the reader will find here (in Part A) actual *proofs* of various theorems in fragments, not only proofs of provability of these theorems. (Model-theoretic methods of proving provability of a sentence in a fragment can be found in Chap. IV.) It is hoped that the reader will feel comfortable in these fragments and will gain good practice in proving theorems in them. If so, then he will agree that each fragment (as well as the whole of Peano arithmetic) captures a natural part of the truth about N.

Secondly, the *limitations* of the axiomatic approach in capturing the truth on natural numbers, i.e. the feature of *incompleteness*, will be studied in Part B.

1. Basic Developments; Partial Truth Definitions

(a) Properties of Addition and Multiplication, Divisibility and Primes

1.1 Definition. Q is the theory in the language L_0 with the following axioms:

(Q1) $$S(x) \neq \overline{0}$$
(Q2) $$S(x) = S(y) \rightarrow x = y$$
(Q3) $$x \neq \overline{0} \rightarrow (\exists y)(x = S(y))$$
(Q4) $$x + \overline{0} = x$$
(Q5) $$x + S(y) = S(x + y)$$
(Q6) $$x * \overline{0} = \overline{0}$$
(Q7) $$x * S(y) = (x * y) + x$$
(Q8) $$x \leq y \equiv (\exists z)(z + x = y)$$

Q is often called *Robinson arithmetic.* Note that thanks to our notational conventions, (Q7) may be written equally well as $x * S(y) = xy + x$ (omitting the parentheses and * on the right hand side); but since we are begining to develop axiomatic systems of arithmetic, we shall be slightly pedantic for some time. Later we shall again freely use our conventions. *Peano arithmetic* results from Q by adding the induction schema

$$\varphi(\overline{0})\,\&\,(\forall x)(\varphi(x) \rightarrow \varphi(S(x))). \rightarrow (\forall x)\varphi(x)\,.$$

This is indeed a *schema:* for each formula φ we have an induction axiom. Note that φ may contain free variables distinct from x as parameters. Peano arithmetic is denoted PA.

1.2 Lemma. In PA, the axiom (Q3) is redundant.

Proof. Let $\varphi(x)$ be $x = \overline{0} \vee (\exists y)(x = S(y))$ and proceed in PA: $\varphi(\overline{0})$ is obvious and $\varphi(S(x))$ too; thus we have $(\forall x)(\varphi(x) \rightarrow \varphi(S(x))$, and thus $(\forall x)\varphi(x)$. □

1.3. Particularly important fragments of PA result by restricting the induction schema to formulas φ from a prescribed class. This will be investigated in details in Sect. 2; here we make only a few particular choices. $I_{\mathrm{open}}, I\Sigma_0, I\Sigma_1$ will denote the theory Q plus the induction schema for φ open, Σ_0, Σ_1 respectively. (We shall also investigate a theory with an extended language.) Note that in Part A we shall develop mainly theories containing $I\Sigma_1$ (and contained in PA). This is because in $I\Sigma_1$ we can formalize a proof of the fact that total Δ_1 functions are closed under primitive recursion (a careful formulation is presented below). This is the most important feature of fragments containing $I\Sigma_1$ and makes them remarkably different from weaker systems. Note also at this time that Chap. V deals with $I\Sigma_0$ and related theories and elaborates their specific problems. I_{open} will play only a marginal role in this book.

1.4. Note that by (Q3), each non-zero number x has a predecessor, i.e. a y such that $S(y) = x$. Thus we may define, in Q, a total function P by the following definition:

$$y = P(x) \equiv .\, (x = \overline{0} \,\&\, y = \overline{0}) \vee (x \neq \overline{0} \,\&\, S(y) = x)\,.$$

We shall now prove several formulas in Q. Recall that for $m \in N$, $\overline{m}$ is the m-th numeral (cf. 0.28).

1.5 Lemma. The following formulas are provable in Q:

$$x + y = \overline{0} \rightarrow .\, x = \overline{0} \,\&\, y = \overline{0}\,, \tag{1}$$
$$x * y = \overline{0} \rightarrow .\, x = \overline{0} \vee y = \overline{0}\,, \tag{2}$$
$$x + \overline{1} = S(x)\,, \tag{3}$$
$$\overline{0} \leq x\,, \tag{4}$$
$$S(x) \leq \overline{n+1} \rightarrow x \leq \overline{n}\,, \tag{5}$$
$$S(x) + \overline{n} = x + \overline{n+1}\,, \tag{6}$$
$$\overline{n} \leq x \rightarrow .\, x = \overline{n} \vee \overline{n+1} \leq x\,. \tag{7}$$

Proof. Proceed in Q. We prove (1)–(4). Take (1). If $y \neq \overline{0}$ then $y = S(z)$ for some z, thus $x + y = S(x + z) \neq \overline{0}$. If $x \neq \overline{0} \,\&\, y = \overline{0}$ then $x + y = S(z)$ for some z. This proves (1). Ad (2): assume $x, y \neq \overline{0}, x = S(u), y = S(v)$. Then $x * y = S(u) * S(v) = (S(u) * v) + S(u) = S(S(u) + v) \neq \overline{0}$. (3) is trivial.

(4) is obvious by (Q4). (5): If $z + S(x) = \overline{n+1}$ then $S(z + x) = S(\overline{n})$, thus $z + x = \overline{n}$. Note that (5) is a schema; for each n we have a proof. Also (6) is a schema; we shall construct the desired proofs by induction. Observe that we shall use *no* induction *within* the proofs (since we have no induction in Q); we shall construct the $(n + 1)$-th proof from the n-th one. This will often be the case. For $n = 0$, Q proves $S(x) + \overline{0} = S(x) = x + \overline{1}$. Assuming

(6) we get $Q \vdash S(x) + \overline{n+1} = S(x) + S(\overline{n}) = S(S(x) + \overline{n})) = S(x + \overline{n+1}) = x + S(\overline{n+1}) = x + \overline{n+2}$.

(7) In Q, assume $\overline{n} \leq x \,\&\, x \neq \overline{n}$; then, for some $z \neq \overline{0}$, $\quad z + \overline{n} = x$. By (6), we get $x = P(z) + \overline{n+1}$, thus $\overline{n+1} \leq x$. □

1.6 Theorem. For each $n, m \in N$, Q proves the following:

$$\overline{m} + \overline{n} = \overline{m+n}\,, \tag{1}$$

$$\overline{m} * \overline{n} = \overline{m*n}\,, \tag{2}$$

$$\overline{m} \neq \overline{n} \text{ for } m \neq n\,, \tag{3}$$

$$x \leq \overline{n} \equiv .\, x = \overline{0} \vee x = \overline{1} \vee \ldots \vee x = \overline{n}\,, \tag{4}$$

$$x \leq \overline{n} \vee \overline{n} \leq x\,. \tag{5}$$

Proof. (1) We prove $Q \vdash \overline{m} + \overline{n} = \overline{m+n}$ by induction on n. For $n = 0$ we have to prove $Q \vdash \overline{m} + \overline{0} = \overline{m}$, which follows by (Q4). Assume we already have a proof of (1) and proceed in Q: $\overline{m} + \overline{n+1} = \overline{m} + S(\overline{n}) = S(\overline{m} + \overline{n}) = \overline{m+n+1}$. The proof of (2) is similar.

(3) Next we show that $m \neq n$ implies $Q \vdash \overline{m} \neq \overline{m}$. It suffices to assume $n < m$. For $m = 0$ the assumption is vacuous. Assume the assertion for m and let $n < m + 1$. Then either $n = 0$ and (Q1) gives $Q \vdash \overline{n} \neq \overline{m+1}$ or $n = n_0 + 1$ and we have $Q \vdash \overline{n_0} \neq \overline{m}$ by the inductive assumption; hence $Q \vdash \overline{n} \neq \overline{m+1}$ by (Q2).

(4) We construct proofs of the formulas in question by induction on n. For $n = 0$ see 1.5(1). Assume the assertion for n and consider $n + 1$. The implication $\leftarrow$ is clearly provable using (1); thus proceed in Q and assume $x \leq \overline{n+1}$. If $x = \overline{0}$ we are done; therefore assume $x \neq \overline{0}$. By 1.5(5) we get $P(x) \leq \overline{n}$, thus $P(x) = \overline{0} \vee \ldots \vee P(x) = \overline{n}$, which implies $x = \overline{1} \vee \ldots \vee x = \overline{n+1}$.

(5) $Q \vdash \overline{0} \leq x$ by 1.5(4). Assume $Q \vdash \overline{n} \leq x \vee x \leq \overline{n}$ and proceed in Q. If $x \leq \overline{n}$ then $x \leq \overline{n+1}$ using (4) and (1); if $\overline{n} \leq x$ then, by 1.5(7), either $\overline{n} = x$, thus $x \leq \overline{n+1}$, or $\overline{n+1} \leq x$. □

1.7 Remark. (1) $Q \vdash x + \overline{n} = \overline{k} \rightarrow x = \overline{k-n}$ (for $n \leq k$); this follows by iterated use of (Q2).

(2) Q proves

$$\vdash x + y = \overline{k} \rightarrow \bigvee_{i+j=k} x = \overline{i} \,\&\, y = \overline{j}$$

(by 1.6(4) using (1)).

1.8 Theorem. (Σ_1-completeness of Q.) Let $\varphi(x)$ be a Σ_0-formula with the only free variable x and let $N \models (\exists x)\varphi(x)$. Then $Q \vdash (\exists x)\varphi(x)$.

Proof. It is sufficient to show for each $\varphi(x_1, \ldots, x_n) \in \Sigma_0$ that $N \models \varphi(\overline{k_1}, \ldots, \overline{k_n})$ implies $Q \vdash \varphi(\overline{k_1}, \ldots, \overline{k_n})$. First show, using 1.6(1),(2), that for each term $t(x_1,\ldots,x_n)$ and each n-tuple $k_1,\ldots,k_n$ of elements of N,

$$Q \vdash t(\overline{k_1},\ldots,\overline{k_n}) = \overline{Val(t(\overline{k_1},\ldots,\overline{k_n})}$$

(thus, e.g. $Q \vdash (\overline{3}+\overline{5}) * \overline{8} = \overline{64}$). From this it follows, again using 1.6, that our assertion holds for φ atomic and negated atomic. (Observe that if $N \models \neg(\overline{k} \leq \overline{m})$ then $m < k$ and, by 1.6, $Q \vdash \overline{k} \leq \overline{m} \rightarrow (\overline{k} = \overline{0} \vee \ldots \vee \overline{k} = \overline{m})$, thus $Q \vdash \neg(\overline{k} \leq \overline{m})$.) The induction step for logical connectives is easy. Finally, assume φ to be $(\exists y \leq x_1)\psi(y,x_1,\ldots,x_n)$ and $N \models \varphi(\overline{k_1},\ldots,\overline{k_n})$; thus for some $k_0 \leq k_1$, $N \models \psi(\overline{k_0},\overline{k_1},\ldots,\overline{k_n})$ and, by the induction hypothesis, $Q \vdash \psi(\overline{k_0},\ldots,\overline{k_n})$. This gives $Q \vdash \varphi(\overline{k_1},\ldots,\overline{k_n})$. Similarly for $\neg\varphi$, i.e. for $(\forall y \leq x)\neg\psi(y,x_1,\ldots,x_n)$. □

1.9 Remark. Thus each theory containing Q is Σ_1-complete. (We shall show in Part B that no axiomatized consistent theory containing Q is Π_1-complete.)

1.10 Theorem. The following formulas are provable in I_{open}:

(1) $$x+y=y+x$$
(2) $$x+(y+z)=(x+y)+z$$
(3) $$x*y=y*x$$
(4) $$x*(y+z)=x*y+x*z$$
(5) $$x*(y*z)=(x*y)*z$$
(6) $$x+y=x+z \rightarrow x=y$$
(7) $$x \leq y \vee y \leq x$$
(8) $$x \leq y \,\&\, y \leq x \rightarrow x=y$$
(9) $$(x \leq y \,\&\, y \leq z) \rightarrow x \leq z$$
(10) $$x \leq y \equiv x+z \leq y+z$$
(11) $$z \neq \overline{0} \,\&\, x*z=y*z \rightarrow x=y$$
(12) $$z \neq \overline{0} \rightarrow (x \leq y \equiv x*z \leq y*z)$$

Proof. We shall now use the induction schema inside I_{open}. At the beginning we shall give detailed proofs; later we shall omit details. The important thing is always to be sure that we use an instance of the induction schema given by a formula belonging to the class for which it is assumed; in our case, an open formula of the langauge L_0.

(1) We first prove $(\forall x)(\overline{0}+x=x)$ in I_{open}. We use the induction axiom given by the open formula $\overline{0}+x=x$; denote it by $\varphi(x)$. First, $\varphi(\overline{0})$, i.e. $\overline{0}=\overline{0}$ follows by (Q3). To prove $(\forall x)(\varphi(x) \rightarrow \varphi(S(x))$, assume $\overline{0}+x=x$ and compute as follows: $\overline{0}+S(x) = S(\overline{0}+x) = S(x)$. Thus by the induction axiom we get $(\forall x)\varphi(x)$.

Second, we prove $(\forall y)(S(x) + y = S(x + y))$. Let $\varphi(y)$ be $S(x) + y = S(x + y)$. The proof of $\varphi(\overline{0})$ is easy. Assume $\varphi(y)$ and prove $\varphi(S(y))$ as follows: $S(x)+S(y) = S(S(x)+y) = S(S(x+y)) = S(x+S(y))$. Thus we get $(\forall y)(S(x)+y = S(x+y))$. Compare this proof with the proof of 1.5(6): There we constructed, by metamathematical induction, infinitely many proofs (for each n, we constructed a proof of $S(x) + \overline{n} = x + \overline{n+1}$ in Q); here we have a single proof in I_{open} of $(\forall y)(S(x) + y = S(x + y))$. Clearly the latter formula implies each instance of the former schema. Now let us prove, in I_{open}, $(\forall x)(x + y = y + x)$. Let $\varphi(x)$ be $x + y = y + x$; we shall apply induction for φ. We have proved $\overline{0} + y = y + \overline{0}$; assume $x + y = y + x$ and reason as follows:

$$S(x) + y = S(x + y) = S(y + x) = y + S(x)\,.$$

Thus we have proved $(\forall x)(\varphi(x) \to \varphi(S(x))$; by the induction axiom we get $(\forall x)\varphi(x)$.

(2) We prove $(x+y)+z = x+(y+z)$ by induction on z. First, $(x+y)+\overline{0} = x + (y + \overline{0}) = x + y$ is clear. Assume $(x + y) + z = x + (y + z)$ and consider $(x + y) + S(z)$. We get $(x + y) + S(z) = S((x + y) + z) = S(x + (y + z)) = x + S(y + z) = x + (y + (S(z))$. This completes the proof of (2). Note that from now on we may write sums like $x + y + z + u$ without parentheses.

(3) First prove $\overline{0}*x = \overline{0}$ by induction on x; then prove $S(x)*y = (x*y)+y$ by induction on y; finally, prove $x * y = y * x$ by induction on x. (Let us elaborate on the induction step for the second proof; assume $S(x) * y = (x * y) + y$. Then

$$\begin{aligned}
S(x) * S(y) &= S(x) * y + S(x) && \text{(axiom (Q7)} \\
&= (x * y) + y + S(x) && \text{(inductive assumption} \\
& && \quad\text{plus associativity)} \\
&= (x * y) + S(y + x) && \text{(axiom (Q5))} \\
&= (x * y) + S(x + y) && \text{(commutativity (1))} \\
&= x * y + x + S(y) && \text{(axiom (Q5))} \\
&= x * S(y) + S(y) && \text{(axiom (Q7)} \\
& && \quad\text{plus associativity).)}
\end{aligned}$$

(4) Prove $(x + y) * z = (x * z) + (y * z)$ by induction on z.

(5) Prove $(x * y) * z = x * (y * z)$ by induction on z. Thus products like $x * y * z * u$ (or $xyzu$) are meaningful.

(6) Prove $x + z = y + z \to x = y$ by induction on z. The induction step: assume $x+z = y+z \to x = y$ and $x+S(z) = y+S(z)$. Then $S(x+z) = S(y+z)$ by (Q5) and $x + z = y + z$ by (Q2); thus $x = y$.

(7) Prove $x \le y \lor y \le x$ by induction on x. (See the proof of 1.6(5).)

(8) Assume $x \le y \,\&\, y \le x$; thus $y = x+u$ and $x = y+v$. Then $x = x+u+v$ and $x = x + \overline{0}$; by (6), $u + v = \overline{0}$ and by 1.5(1), $u = v = \overline{0}$. Thus $x = y$.

(9) Easy using commutativity and associativity of addition.

(10) Use the same plus cancellation.

(11) We have to prove $z \neq \overline{0} \,\&\, x \neq y \,.\rightarrow x * z \neq y * z$. By (7), we may assume $x \leq y$. Thus we prove the following by induction on z:

$$x \leq y \,\&\, x \neq y \,\&\, z \neq \overline{0} \,.\rightarrow .\, x * z \leq y * z \,\&\, x * z \neq y * z \,.$$

Observe that this is an open formula of L_0; we may write it as follows:

$$(*) \qquad x < y \,\&\, z \neq \overline{0} \,.\rightarrow x * z < y * z$$

(see the next remark). Now $x < y$ means $y = x + u$ for some $u \neq \overline{0}$. Nothing need be proved for $z = \overline{0}$. Assume $(*)$ and consider $S(z)$. We may assume $z \neq \overline{0}$, hence $x * z < y * z$, which means $y * z = x * z + v$ for some $v \neq \overline{0}$. Thus

$$y * S(z) = y * z + y = x * z + x + u + v = x * S(z) + (u + v)$$

and clearly $u + v \neq \overline{0}$; we get $x * S(z) < y * S(z)$.

(12) The proof of $x \leq y \rightarrow x * z \leq y * z$ is easy. Recall $(*)$ in (11) above and observe that, by using (8), $\neg(x \leq y)$ is equivalent to $y < x$. Thus we get

$$z \neq \overline{0} \,.\rightarrow \neg(x \leq y) \rightarrow \neg(x * z \leq y * z)\,,$$

i.e.

$$z \neq \overline{0} \rightarrow (x \leq y \equiv x * z \leq y * z)\,. \qquad \square$$

1.11 Remark. (1) We have seen that I_{open} proves that $\leq$ is a linear order with $\overline{0}$ as the least element and that addition is monotone as well as multiplication by a non-zero element. As we previously did above, we define $x < y$ as $x < y \,\&\, x \neq y$ (the corresponding strict ordering); $x < y$ is equivalent to $(\exists u)(u \neq \overline{0} \,\&\, x + u = y)$. Furthermore, the ordering is discrete since for each x, $S(x)$ is the upper neighbour of x (and each non-zero element has a predecessor).

(2) I_{open} also proves $x * \overline{1} = x$ and, for each n, it proves

$$x * \overline{n} = \underbrace{(\dots((x + x) + \dots) + x}_{n \text{ times}}\,.$$

The easy proofs are left to the reader as an exercise.

1.13 Definition (I_{open}). (1) x *divides* y (notation: $x \mid y$) if $(\exists z)(xz = y)$. (Recall that this is shorthand for $(\exists z)(x * z = y)$.)

(2) x is *prime* ($Prime(x)$) if $x > \overline{1}$ and $(\forall u)(u \mid x \,.\rightarrow u = \overline{1} \vee u = x)$.

(3) $z = x - y$ if ($x \geq y$ and $x + z = y$) or ($x < y$ and $z = \overline{0}$).

1.14 Lemma (I_{open}). (1) $x \mid y$ iff $(\exists z \leq y)(xz = y)$
(2) $Prime(x)$ iff $x > \overline{1} \,\&\, (\forall u \leq x)(u \mid x \rightarrow .\, u = \overline{1} \vee u = x)$.

Proof. (1) Assume $x \mid y$. If $y = \overline{0}$ then for $z = \overline{0}$ we have $z \leq y \,\&\, xz = y$; so assume $y \neq \overline{0}$ and $xz = y$. Then $x \neq \overline{0}$, thus $x \geq \overline{1}$ and $z = z * \overline{1} \leq z * x = y$.
(2) Observe that for $x \geq \overline{1}$, $u \mid x$ implies $u \leq x$. □

1.15 Lemma (I_{open}).
(1) $\overline{1} \mid x$, $\quad x \mid x$, $\quad x \mid \overline{0}$, $\quad (x \mid y$ and $y \mid z) \rightarrow x \mid z$;
(2) $(x \mid y \,\&\, y \mid x) \rightarrow x = y$, $\quad x \mid y \rightarrow x \mid yz$;
(3) $(x \mid y \,\&\, x \mid z) \rightarrow x \mid (y + z)$;
(4) $y \neq \overline{0} \rightarrow (\exists! u \leq x)(\exists! v < y)(x = yu + v)$ (division with a remainder).

Proof. (1)–(3) are easy. We prove (4). Let $\varphi(u)$ be the formula $yu \leq x$. We have $\varphi(\overline{0})$ and for some u, e.g. for $u = x + 1$, we have $\neg\varphi(u)$ (since $y(x + 1) = yx + y \geq x + y > x$). By I_{open}, there is a u such that $yu \leq x$ and $y(u + 1) > x$. Since $\leq$ is a linear order and multiplication by a non-zero number is monotone, u is unique; furthermore $u \leq x$. Put $v = x - yu$; then $x = yu + v$ and $v < y$ (otherwise $v = y + v', yu + y = y(u + 1) \leq x$, a contradiction.) Clearly, v is uniquely determined. □

1.16 Lemma (I_{open}).
(1) If $x \geq y$ then $x - y = (x + z) - (y + z)$;
(2) if $x \geq y$ then $(x - y) + z = (x + z) - y$;
(3) $(x - y)z = xz - yz$;
(4) $z \mid x$ and $z \mid y$ implies $z \mid x - y$.

Proof. Exercise. □

1.17 Definition and Lemma (I_{open}). x is *even* if $2 \mid x$; x is *odd* if it is not even. For each x, either x or $x + 1$ is even.

Proof. 0 is even; assume $x \neq 0$. Consider the open formula $2u \leq x$ and denote it by $\varphi(u)$. Clearly, $\varphi(0)$ and for some u, $\neg\varphi(u)$ (e.g. for $u = x$). Thus there is an u such that $2u \leq x$ and $2(u+1) > x$. Then either $2u = x$ or $2u = x - 1$, and in the latter case $2(u + 1) = x + 1$. □

1.18 Theorem and Definition (pairing, I_{open}). For each x, y, there is a unique z such that $2z = (x + y)(x + y + 1) + 2x$; this z is denoted (x, y). For each z there is a unique pair x, y such that $z = (x, y)$.

Proof. Either $2 \mid (x + y)$ or $2 \mid (x + y + 1)$; thus $2 \mid ((x + y)(x + y + 1) + 2x)$. Therefore for some z, $2z = (x + y)(x + y + 1) + 2x$; clearly, this z is unique. Now take any z and using I_{open}, find an r such that $r(r + 1) \leq 2z$ and

$(r+1)(r+2) > 2z$. (Consider $\varphi(r) \equiv r(r+1) \leq 2z$.) Clearly, $2z - r(r+1)$ is even; let x be such that $2x = 2z - r(r+1)$. We have $x \leq r$ (otherwise we would have $2x > 2r$, $2r < 2z - r(r+1)$, $r^2 + 3r < 2z$ and $r^2 + 3r$ is even; thus $(r+1)(r+2) = r^2 + 3r + 2 \leq 2z$, a contradiction). Put $y = r - x$; then $x + y = r$, $2z = (x+y)(x+y+1) + 2x$, thus $z = (x, y)$. □

1.19 Definition. Let T be a theory containing I_{open}. A formula $\varphi(\mathbf{x})$ is said to be Σ_n (Π_n) *in* T if there is a Σ_n formula (Π_n formula) $\psi(\mathbf{x})$ such that $T \vdash \varphi(\mathbf{x}) \equiv \psi(\mathbf{x})$. Furthermore, $\varphi(\mathbf{x})$ is said to be Δ_n in T if it is both Σ_n in T and Π_n in T.

1.20 Examples. $x \mid y$, $Even(x)$, $Prime(x)$, $z = (x, y)$ are Σ_0 in I_{open}.

1.21 Theorem. Let $T \supseteq I_{\text{open}}$. For each natural number n and any formulas φ, ψ:
(1) if φ, ψ are $\Sigma_n(\Pi_n, \Delta_n)$ in T then so are $\varphi \,\&\, \psi$ and $\varphi \vee \psi$;
(2) if φ is Δ_n in T then so is $\neg\varphi$;
(3) if $n > 0$ and ψ is Σ_n in T then so is $(\exists x)\psi$;
(4) if $n > 0$ and ψ is Π_n in T then so is $(\forall x))\psi$.

Proof. Fully analogous to that of 0.34. (For each n and each choice of φ, ψ, a T-proof is constructed.) □

*

Now we turn to $I\Sigma_0$. Since $I\Sigma_0$ and related theories will be investigated in detail in Chap. V, we prove (or state) only some few basic facts.

1.22 Theorem. (1) $I\Sigma_0$ proves the *least number principle* for Σ_0 formulas: i.e. for each Σ_0 formula $I\Sigma_0$ proves

$$(\exists x))\varphi(x) \rightarrow (\exists x)(\varphi(x) \,\&\, (\forall y < x)\neg\varphi(y)).$$

(2) For each Σ_0 formula, $I\Sigma_0$ proves the following *order induction:*

$$(\forall x))((\forall y < x)\varphi(y) \rightarrow \varphi(x)) \rightarrow (\forall x)\varphi(x).$$

Proof. (1) Assume $(\exists x)(\varphi(x) \,\&\, (\forall x)(\varphi(x) \rightarrow (\exists y < x)\varphi(y))$ and apply induction to the formula $(\forall y < x)\neg\varphi(y)$ to obtain a contradiction. (2) Apply induction to the Σ_0 formula $(\forall y < x)\varphi(y)$. □

1.23 Definition ($I\Sigma_0$). If $x, y \neq 0$ then $gcd(x, y)$ is the maximal u such that $u \mid x$ and $u \mid y$; otherwise $gcd((x, y) = 0$ (greatest common divisor).

Note that $gcd(x, y)$ exists since it is the least $u \leq \min(x, y)$ such that $(\forall v \leq \min(x, y))(u + 1 \leq v \rightarrow \neg(v \mid x \,\&\, v \mid y))$.

1.24 Lemma ($I\Sigma_0$). $0 < y \le x \to (\exists u \le x)(\exists v \le x)(gcd(x,y) = xu - yv)$.

Proof. (0) Clearly we may assume $y < x$. Observe that if $0 < t < y$ and $t = xu - yv$ then there are $u < y$ and $v < x$ such that $t = xu - yv$. (To see this first show $u > y \equiv v > x$; thus if $u > y$ then we can replace u by $u - y$ and v by $v - x$. Apply $L\Sigma_0$.)

(1) Let z be the least number such that, for some $u, v < x$, $xu > yv \,\&\, z = xu - yv$. We show $z = gcd(x,y)$. First prove $z \mid x$. By 1.15(4), let $x = zs + t, t < z$. Clearly, $s \ne 0$ since $t < z < x$. If $t \ne 0$ then $t = x - zs = x - (xu - yv)s = x(1 + yq - u) - y(xq - v)$ where q is the least number such that $1 + yq > u$ and $xq > v$. Then clearly $1 + yq - u \le x$, $\quad xq - v \le x$ and we get a contradiction with the minimality of z. Thus $t = 0$ and $z \mid x$.

(2) The proof of $z \mid y$ is similar (note that $z \le y$ since $y = xy - y(x-1)$.

(3) Now if $w \mid x$ and $w \mid y$ then $w \mid z$ (by 1.13(4)); thus $w \le z$ and $z = gcd(x,y)$. This completes the proof. □

1.25 Lemma ($I\Sigma_0$). $gcd(x,y) = 1 \to (\forall z)(x \mid yz \to x \mid z)$.

Proof. Assume $gcd(x,y) = 1$ and $y \le x$. Then, for some $u, v \le x$, $1 = xu - yv$. Now if $x \mid yz$ then $x \mid xuz - yvz$, $x \mid (xu - yv)z$, $x \mid z$. □

1.26 Lemma ($I\Sigma_0$). (1) For each $x > 1$, there is a $y \le x$ such that $Prime(y)$ and $y \mid x$. (2) If $Prime(x)$ and $x \mid yz$ then $x \mid y$ or $x \mid z$.

Proof. (1) follows by the least number principle (1.22). (2) Assume that x does not divide y; since x is prime this means $gcd(x,y) = 1$. Thus $x \mid z$ by 1.25. □

1.27 Remark. The reader may move now to Chap. V where $I\Sigma_0$ is investigated in details. He will find there, among other things, a proof of the following theorem claiming that in $I\Sigma_0$ exponentiation is Σ_0 definable as a possibly partial function:

There is a Σ_0 formula $exp(z,x,y)$ such that $I\Sigma_0$ proves the following:

(1) $exp(z_1,x,y) \,\&\, exp(z_2,x,y). \to z_1 = z_2$,
(2) $exp(1,x,0)$,
(3) $exp(z,x,y) \to exp(zx,x,S(y))$,
(4) $exp(z,x,y) \,\&\, y' < y \to (\exists z')exp(z',x,y')$.

Many results of Chaps. I–IV are independent of this theorem; the reader may postpone reading its proof. In subsection (c) of the present section, we shall prove a weaker (and classical) result saying that there is a formula exp which is Δ_1 in $I\Sigma_1$ and such that $I\Sigma_1$ proves (1)–(4). This weaker result is basic for Chaps. I–IV.

(b) Coding Finite Sets and Sequences; the Theory $I\Sigma_0(exp)$

1.28. In this subsection we shall investigate a theory stronger than $I\Sigma_0$ and having a richer language: we extend the language by a new unary function symbol $\overline{2}^x$ for the x-th power of two. The extended language is denoted $L_0(exp)$. $\Sigma_0(exp)$ formulas result from atomic formulas of $L_0(exp)$ by iterated application of logical connectives and bounded quantifiers of the form $(\forall x \leq y)$, $(\exists x \leq y)$. The theory $I\Sigma_0(exp)$ has the following axioms:
(1) axioms of Q,
(2) two axioms for exponentiation, namely:

$$\overline{2}^{\overline{0}} = \overline{1}\,,$$
$$\overline{2}^{S(x)} = \overline{2}^x * \overline{2}\,,$$

(3) induction schema for all $\Sigma_0(exp)$ formulas.

1.29. We shall need another class of formulas called $\Sigma_0^{exp}(exp)$ formulas: they result from atomic $L_0(exp)$ formulas by iterated application of logical connectives and bounded quantifiers of the following form:

$$(\forall x \leq y), \quad (\exists x \leq y), \quad (\forall x \leq \overline{2}^y), \quad (\exists x \leq \overline{2}^y)\,.$$

1.30 Theorem ($I\Sigma_0(exp)$). (1) $x < 2^x$; (2) $x < y \rightarrow 2^x < 2^y$; (3) $2^x * 2^y = 2^{x+y}$.

Proof. (1) is easy. (2) Use induction on y. Nothing is to be proved for $y = \overline{0}$. Assume $x < y \rightarrow 2^x < 2^y$ and $x < y + 1$.

Case 1: $x < y$ is false; then necessarily $x = y$, $2^x = 2^y > y \geq \overline{0}$, thus $2^{y+1} = 2^y * 2 = 2^y + 2^y > 2^y = 2^x$.

Case 2: $x < y$ is true; then $2^x < 2^y < 2^y * 2 = 2^{y+1}$. Thus the induction step is proved. (3) Induction on y. □

1.30 Lemma. The schema of induction for $\Sigma_0^{exp}(exp)$ formulas is derivable in $I\Sigma_0(exp)$.

Proof. Clearly, it is enough to prove the least number principle for each $\Sigma_0^{exp}(exp)$ formula.We claim that for each such formula $\varphi(\mathbf{x})$ there is a $\Sigma_0(exp)$ formula $\varphi_0(\mathbf{x}, y)$ and a term $t(\mathbf{x})$ of $L_0(exp)$ such that $I\Sigma_0(exp)$ proves the following:

$$(*) \qquad (\forall y \geq t(\mathbf{x}))(\varphi(\mathbf{x}) \equiv \varphi_0(\mathbf{x}, y))$$

This is evident for φ atomic ($t(\mathbf{x}) = 0, \varphi_0(\mathbf{x}, y) = \varphi(\mathbf{x})$). If $(*)$ holds for φ, φ_0, t then it holds for $\neg\varphi, \neg\varphi_0, t$; if it holds for $\varphi_1, \varphi_{10}, t_1$ and $\varphi_2, \varphi_{20}, t_2$ then it holds for $\varphi_1 \,\&\, \varphi_2, \varphi_{10} \,\&\, \varphi_{20}, t_1 + t_2$. Assume that we have $\varphi(\mathbf{x}, u), \varphi_0(\mathbf{x}, u, y)$ and $t(\mathbf{x}, u)$ satisfying the analogue of $(*)$ and investigate $\psi(\mathbf{x})$ being $(\forall u \leq 2^x)\varphi(\mathbf{x}, u)$ (where $\mathbf{x} = x, \ldots$). Then $(*)$ holds for $\psi'_0(\mathbf{x})$ being $(\forall u \leq y)(u \leq 2^x \rightarrow \varphi_0(\mathbf{x}, u, y))$ and $t'(\mathbf{x})$ being $2^x + t(\mathbf{x}, 2^x)$. (Note that $I\Sigma_0(exp)$proves $u \leq 2^x \rightarrow t(\mathbf{x}, u) \leq t(\mathbf{x}, 2^x)$.) This proves our claim.

To complete the proof of 1.30, let $\varphi, \varphi_0 \in \Sigma_0^{exp}(exp)$ be as in the claim above. In $I\Sigma_0(exp)$, assume $\varphi(\mathbf{x})$ and put $y = t(\mathbf{x})$. Then we have $\varphi_0(\mathbf{x}, y)$; write it $\varphi_0(x_1, x_2, \ldots, y)$. By the least number principle for $I\Sigma_0(exp)$ formulas, let x'_1 be the least x_1 such that $\varphi_0(x_1, x_2, \ldots, y)$; this x'_1 is the least x_1 such that $\varphi(x_1, x_2, \ldots,)$. (Note that $t(x'_1, x_2, \ldots) \leq t(x_1, x_2, \ldots)$.)

1.31 Lemma and Definition ($I\Sigma_0(exp)$). For each x, y, there are unique $u \leq y$, $v \leq 1$, $w < 2^x$ such that

$$y = 2^{x+1} * u + 2^x * v + w\,.$$

The unique $v \leq 1$ such that $(\exists u \leq y)(\exists w < 2^x)(y = 2^{x+1} * u + 2^x * v + w)$ is called the x-th *bit* of y and denoted $bit(x, y)$. We further define

$$x \in y \equiv bit(x, y) = 1\,.$$

(Note that $x \in y$ is $\Sigma_0(exp)$ in $I\Sigma_0(exp)$.)

Proof. By 1.15(4) (division with remainder), there are $u \leq y$ and $q < 2^{x+1}$ such that $y = 2^{x+1} * u + q$; by the same theorem, there are $v \leq q$ and $w < 2^x$ such that $q = 2^x * v + w$. The numbers u, v, w are uniquely determined. Moreover, u must be less than 2 since otherwise we would have $q \geq 2^{x+1}$, a contradiction. □

1.32 Lemma ($I\Sigma_0(exp)$). (1) $x \in y \rightarrow x < y$. (2) $y = \overline{0} \rightarrow (\forall x)(x \notin y)$. (3) $y \neq \overline{0} \rightarrow y$ has a least and a largest element. (4) $y < 2^u \equiv (\forall x)(x \in y \rightarrow x < u)$.

Proof. (1) $bit(x, y) = 1$ implies $y \geq 2^x > x$. (2) follows from (1). Consider (3): If $y \neq \overline{0}$ then we first claim that there is a largest $x < y$ such that $2^x \leq y$; then it follows easily that $x \in y$ and x is the largest element of y. Having $(\exists x < y)(x \in y)$ we get a least element of y by the least number principle. Thus let us prove the claim. Let x be the least number such that $(\forall z < y)(2^z \leq y \rightarrow z \leq x)$. Then clearly $2^x \leq y$ and x is the largest such number. (4) The implication $\rightarrow$ is obvious. To prove the converse, assume $y \geq 2^u$ and let x be the largest such that $y \geq 2^x$. Then $y = 2^x + w$ for some $w < 2^x$, which implies $x \in y$; and obiously, $x \geq u$. □

1.33 Definition ($I\Sigma_0(exp)$). $x \subseteq y \equiv (\forall u < x)(u \in x \rightarrow u \in y)$
(Note that by 1.32, $x \subseteq y$ is equivalent to $(\forall u))(u \in x \rightarrow u \in y)$.)

1.34 Lemma ($I\Sigma_0(exp)$). (1) If $w < 2^z$ then for all x,

$$x \in 2^z + w \equiv . x \in w \vee x = z .$$

(2) For each u, y,

$$y < 2^u \equiv y \subseteq 2^u - 1 .$$

Proof. ($\leftarrow$) Clearly $z \in 2^z + w$ by definition. Assume $x \in w$, i.e. $w = 2^{x+1} * s + 2^x + t$, $t < 2^x$. Then $2^z + w = 2^z + 2^{x+1} * s + 2^x + t = 2^{x+1}(2^{z-x-1} + s) + 2^x + t$, i.e. $x \in 2^z + w$.

($\rightarrow$) Assume $x \in 2^z + w$; then $x \leq z$ (since $2^z + w \leq 2^{z+1}$). If $x = z$ then we are done; assume $x \leq z$. We have $2^z + w = 2^{x+1} * s + 2^x + t$.

Claim. $2^{x+1} * s \geq 2^z$. Otherwise $2^{x+1} * s < 2^z$ and since $2^z = 2^{x+1} * 2^{z-x-1}$, i.e. $2^{x+1} \mid 2^z$, we get $2^{x+1} * s \leq 2^z - 2^{x+1}$. But then $2^{x+1} * s + 2^x + t < 2^z$, a contradiction. The claim is proved.

Thus $s \geq 2^{z-x-1}$ and $s < 2^{z-x}$; this implies that in dividing s by 2^{z-x-1} we get $s = 2^{z-x-1} + q \quad (q < 2^{z-x-1})$,

$$\begin{aligned} 2^z + w &= 2^{x+1}(2^{z-x-1} + q) + 2^x + t = 2^z + 2^{x+1} * q + 2^x + t , \\ w &= 2^{x+1} * q + 2^x + t , \end{aligned}$$

and consequently $x \in w$. This completes the proof of (1).

(2) By 1.31, it suffices to show

(i) $$x < u \rightarrow bit(x, 2^u - 1) = 1 ,$$

(ii) $$x \geq u \rightarrow bit(x, 2^u - 1) = 0 .$$

But (ii) is obvious; let us prove

(*) $$(\forall u)(\forall x < u)(bit(x, 2^u - 1) = 1) .$$

(Show that the formula following $(\forall u)$ is $\Sigma^{exp}(exp)$ in $I\Sigma_0(exp)$.) Nothing need be proved for $u = 0$. Assume (*) and consider $u + 1$: $2^{u+1} - 1 = 2^u + (2^u - 1)$. Thus $bit(u, 2^{u+1} - 1) = 1$ and, by (*), for $x < u$, $bit(x, 2^u - 1) = 1$. But by (1), $bit(x, 2^u - 1) = bit(x, 2^{u+1} - 1)$. □

1.35 Definition ($I\Sigma_0(exp)$). For each x, y, put

$$\begin{aligned} \max(x) &= \text{the largest element of } x \text{ if } x \neq \overline{0}, \\ &= \overline{0} \text{ for } x = \overline{0} \text{ (cf. 1.34(3))} \\ (\leq x) &= 2^{x+1} - 1 \\ (< x) &= 2^x - 1 \\ seg(x) &= (\leq \max(x)) . \end{aligned}$$

Note that, by 1.34(2), $u \in (\leq x)$ iff $u \leq x$. We further make the following definition: y is a *restriction* of x to z (in symbols: $Restrict(y, x, z)$) if $y < 2^z$ and $(\forall u < z)(u \in x \equiv u \in y)$. Note that this notion is $\Sigma_0^{exp}(exp)$ in $I\Sigma_0(exp)$and that the latter theory proves the following: if $Restrict(y, x, z)$ and $z \geq 2^x$ then $(\forall u)(u \in x \equiv u \in y)$.

1.36 Theorem ($I\Sigma_0(exp)$-comprehension). For each $\Sigma_0^{exp}(exp)$-formula $\varphi(u,p)$, $I\Sigma_0(exp)$ proves

$$(\forall x)(\exists y < 2^x)(\forall u < x)(u \in y \equiv \varphi(u,p)).$$

Proof. We apply induction on x to the formula

$$(*) \qquad (\exists y < 2^x)(\forall u < x)(u \in y \equiv \varphi(u,p)).$$

The case $x = 0$ is trivial. Assume $(*)$ and let y be as in $(*)$. Consider $x + 1$. If $\varphi(x,p)$ holds, then put $y' = y + 2^x$; by the preceding,

$$(\forall u < x + 1)(u \in y' \equiv (u < x \,\&\, \varphi(u,p). \vee u = x) \equiv \varphi(u,p)).$$

If $\neg\varphi(x,p)$ holds, then put $y' = y$ and argue similarly. □

1.37 Theorem ($I\Sigma_0(exp)$). If $x \subseteq y$ then $x \leq y$.

Proof. Assume $x \subseteq y$ and let us prove the following by induction on z:

$$(*) \quad (\forall x' < 2^z)(\forall y' < 2^z)(Restrict(x', x, z) \,\&\, Restrict(y', y, z) \rightarrow x' \leq y').$$

The case $z = 0$ is trivial ($x' = y' = 0$). Assume $(*)$ and consider $z + 1$. Let $Restrict(x'', x, z + 1), Restrict(y'', y, z + 1)$. Put

$$x' = x'' - 2^z \text{ if } z \in x,$$
$$x' = x'' \text{ if } z \notin x$$

and similarly for y'. Then $Restrict(x', x, z), Restrict(y', y, z)$ and $x' \leq y'$. If $z \notin x$ then $x'' = x' \leq y' \leq y''$ by $(*)$. If $z \in x$ then $z \in y$ and $x'' = x' + 2^z \leq y' + 2^z = y''$ again by $(*)$. This completes the proof. □

1.38 Corollary ($I\Sigma_0(exp)$-extensionality). If $(\forall u)(u \in x \equiv u \in y)$ then $x = y$. (In particular, the restriction of x to z is uniquely determined.)

1.39 Theorem ($I\Sigma_0(exp)$). For any x, y, there exist uniquely determined numbers $x \cup y, x \cap y, x - y, x \times y, \bigcup x, \mathbf{P}(x)$ having the following properties:

(union)	$(\forall u)(u \in x \cup y \equiv . u \in x \vee u \in y)$
(intersection)	$(\forall u)(u \in x \cap y \equiv . u \in x \,\&\, u \in y)$
(set difference)	$(\forall u)(u \in x \setminus y \equiv . u \in x \,\&\, x \notin y)$
(Cartesian product)	$(\forall u)(u \in x \times y \equiv . (\exists u \in x)(\exists v \in y)(u = (v, w))$
(sum set)	$(\forall u)(u \in \bigcup x \equiv . (\exists v \in x)(u \in v))$
(power set)	$(\forall u)(u \in \mathbf{P}(x) \equiv . u \subseteq x)$

Proof. We always find a z such that the set in question is a $\Sigma_0^{exp}(exp)$-definable subset of $seg(z)$. Take the union and let $x \leq y$. Then $seg(x) \subseteq seg(y)$ and we put $z = y$; there is a w such that $(\forall u)(u \in w \equiv u \in seg(z) \,\&\, (u \in x \vee u \in y))$ (by comprehension). Thus u is $x \cup y$. Similarly for $x \cap y, x - y, \bigcup x$. For $x \times y$ observe that $u < x \,\&\, v < y$ implies $(u, v) < (x + y + 1) * (x + y + 1)$ (say); thus there is a w such that

$$(\forall z)(z \in w \equiv . z \in seg((x + y + 1)^2) \,\&\, (\exists u \in x)(\exists v \in y)(z = (u, v)).$$

Finally for the power set, observe that $u \subseteq x$ implies $u \leq x$; thus there is a w such that

$$(\forall u)(u \in w \equiv . u \in seg(x + 1) \,\&\, (\forall v \in u)(v \in x)). \qquad \square$$

Remark. Next we introduce some well-known notions concerning (finite) sets and show that their obvious properties are provable in $I\Sigma_0(exp)$. Note that in $I\Sigma_0(exp)$each number is a finite set (codes a finite set); thus instead of saying "a finite set" we just say "a number"; but we call the reader's attention to properties definable using the membership predicate (as defined above).

1.40 Definition ($I\Sigma_0(exp)$).
(1) x is a *relation* if x is a set of ordered pairs:

$$Rel(x) \equiv (\forall u \in x)(\exists v, w \in u)(u = (v, w))$$

(domain) $\quad v \in dom(x) \equiv (\exists u \in x)(\exists w \leq u)(u = (v, w))$

(range) $\quad w \in rng(x) \equiv (\exists u \in x)(\exists v \leq u)(u = (v, w))$

(show that $y = dom(x), y = rng(x)$ are $\Sigma_0^{exp}(exp)$ in $I\Sigma_0(exp)$.)

(2) y is a *linear order* on x if $Rel(y), dom(y) = rng(y) = x$ and y is reflexive, transitive and dichotomic on x, i.e.

$$(\forall \ldots)((u, v) \in y \,\&\, (v, w) \in y. \rightarrow (u, w) \in y),$$
$$(\forall u, v \in x)((u, v) \in y \vee (v, u) \in y),$$
$$(\forall u, v \in x)((u, v) \in y \,\&\, (v, u) \in y. \rightarrow u = v).$$

(3) y is a *mapping* of x into z if $Rel(y), dom(y) = x, rng(y) \subseteq z$ and

$$(\forall u \in x)(\forall v, w \in z)((u,v) \in y \,\&\, (u,w) \in y. \rightarrow v = w).$$

A mapping is an *injection* (or: is one-one) if

$$(\forall u_1, u_2 \in x)(\forall v \in z)((u_1,v) \in y \,\&\, (u_2,v) \in y \rightarrow u_1 = u_2);$$

y is a *bijection* of x onto z if, additionally, $rng(y) = z$.

(4) For each x, the *natural ordering* of x is the unique linear order y on x such that, for each $u, v \in x$, $(u,v) \in y \equiv u \leq v$. (Show the existence of y using comprehension.)

1.41 Theorem ($I\Sigma_0(exp)$). (1) (Cardinality.) For each x, there is a unique $y = card(x)$ such that there is a bijection of x to $(< y)$.

(2) (Pigeon-hole principle for finite sets.) If $card(x) < card(y)$ then there is no injection of y into x.

(3) If y is a linear order on $x \neq 0$ then x has a largest and a least element with respect to y.

Proof. One only checks that the usual proofs formalize in $I\Sigma_0(exp)$.

(1) The desired bijection f, if it exists, satisfies $f \leq 2^{(x+y+1)^2}$; thus we may prove the following by $\Sigma_0^{exp}(exp)$-induction on x:

$$(*) \qquad (\exists! y \leq x)(\exists f \leq 2^{(2x+1)^2})(f \text{ is a bijection of } x \text{ to } (< y)).$$

(Check that this is $\Sigma_0^{exp}(exp)$.)

For $x = 0$ we get $y = 0$; assume $(*)$ for each $x < z$ and investigate z. Let $u = \max(z)$ and $x = z - 2^u$; then $x < z$, $v \in x \equiv .v \in z \,\&\, v \neq u$ and there is a y satisfying $(*)$. Let f be the corresponding mapping; we extend f to a bijection g of z onto $(< y+1)$ by defining $g(v) = f(v)$ for $v \in x$, $g(u) = y$. The mapping (relation, set) exists thanks to $\Sigma_0^{exp}(exp)$-comprehension.

To prove both the uniqueness of cardinality and the pigeon-hole principle, we show the following by $\Sigma_0^{exp}(exp)$-induction:

$$\neg(\exists f \leq 2^{(2x+1)^2})(f \text{ is an injection of } (< x+1) \text{ into } (< x)).$$

This is clear for $x = 0$. Assume $(*)$ and let f be an injection of $(< x+2)$ into $(< x+1)$. We may also assume that $f(x+1) = x$ (if not we change f for the arguments $x+1$ and $f^{-1}(x)$ using comprehension). But then the restriction of f to $(< x+1)$ is an injection of $(< x+1)$ into $(< x)$, a contradiction. This completes the proof of the induction step.

Consequently, if there is a bijection of $(< x)$ onto $(< y)$ then $x = y$. Thus each finite set has its unique cardinality; and we get the pigeon-hole principle using composition of mappings. The fact that the composition of two mappings that are finite sets is a mapping (and a finite set) follows by comprehension.

(3) By induction on x; note that the universal quantifier $(\forall y)$ may be bounded by $2^{(2\max(x)+1)^2}$ so that $\Sigma_0^{exp}(exp)$-induction applies. Assume the assertion for all $z < x$ and consider z; let u be the maximal element of z with respect to the ordering $<$ and let $v \in x \equiv . v \in z \,\&\, v \neq u$. Then $x < z$ and if $y' = y \cap (x \times x)$ we see that y' is a linear order on x. By the induction assumption, x has a maximal element u' with respect to y'. Then either u or u' is maximal in z with respect to y. □

1.42 Definition ($I\Sigma_0(exp)$). Now we finally come to our definition of finite sequences; they are naturally defined as particular mappings.

$$Seq(z) \equiv (\exists x \leq z)(z \text{ is a mapping} \,\&\, dom(z) = (< x))\,;$$
$$Seq(z) \rightarrow . \, lh(z) = x \text{ iff } dom(z) = (< x)\,;$$
$$Seq(z) \,\&\, u < lh(z) . \rightarrow (z)_u = v \text{ iff } (u, v) \in z\,;$$
$$Seq(z) \,\&\, u \geq lh(z) . \rightarrow (z)_u = 0\,;$$
$$Seq(z) \rightarrow . \, w = z \frown \langle x \rangle \text{ iff } (\forall u < w)(u \in w \equiv . u \in z \vee u = (lh(z), x))\,;$$
$$\text{for } \neg Seq(z), \quad z \frown \langle x \rangle = 0\,;$$

$\emptyset$ is the empty sequence; $lh(\emptyset) = 0$;

$$\langle x \rangle = \emptyset \frown \langle x \rangle;\ \langle x_1, \ldots, x_n, x_{n+1} \rangle = \langle x_1, \ldots, x_n \rangle \frown \langle x_{n+1} \rangle$$
$$(n = 1, 2, \ldots)\,.$$

Note that all notions defined are $\Sigma_0^{exp}(exp)$ in $I\Sigma_0(exp)$.

1.43 Theorem. $I\Sigma_0(exp)$ proves the basic properties of sequences (as formulated in 0.41): For $Seq(s), Seq(s')$,

$$lh(s) \leq s \text{ and } (\forall u < lh(s))((s)_u < s)\,; \tag{1}$$
$$Seq(0) \,\&\, lh(0) = 0\,; \tag{2}$$
$$(\forall u < lh(s))((s)_u = (s \frown \langle z \rangle)_u \,\&\, (s \frown \langle z \rangle)_{lh(s)} = z \,\& \,\&\, lh(s \frown \langle z \rangle) = lh(s) + 1\,; \tag{3}$$
$$\text{if } lh(s) \leq lh(s') \text{ and } (\forall u < lh(s))((s)_u \leq (s')_u) \text{ then } s \leq s' \tag{4}$$
$$(\forall u)(\exists v > u) \neg Seq(v)\,. \tag{5}$$

(Consequently, if s, s' have the same length and the same corresponding elements then $s = s'$.)

Proof. (2) is trivial: 0 is the empty mapping. All monotonicities of (1) and (4) follow from the monotonicity of the ordered pair $(x, y \leq (x, y))$ and of membership ($x \in y \to x < y$). Indeed, if $s \neq 0, Seq(s)$ and $dom(s) = (< x)$, then $lh(s) = x$ and for some y, $(x-1, y) \in s$. Thus $x - 1 \leq (x-1, y) < s$ and hence $x < s$. If $(u, y) \in s$ then $y \leq (u, y) < s$. This proves (1)

We prove (4). First observe that for each sequence s and each $i < lh(s)$ we have the shortening of s to i (denoted by $s \downarrow i$ for a moment) which results from restricting the domain of s to $(< i)$. Existence follows by comprehension; and $s \downarrow lh(s)$ is s. Assume $lh(s) \leq lh(s')$ and $(\forall i < lh(s))((s)_i \leq (s')_i)$; let us prove $(\forall i < lh(s)((s \downarrow i) \leq (s' \downarrow i))$ by induction on i. Note that $s \downarrow (i+1) = (s \downarrow i) + 2^{(i,(s)_i)}$. We get $s \leq s' \downarrow lh(s)$; but $s' \downarrow lh(s) \leq s'$ is obvious since $s' \downarrow lh(s) \subseteq s'$.

Proofs of (3) and (5) are easy. □

Remark. Since $I\Sigma_0(exp)$ proves $(x, y) \leq (x + y + 1)^2$, it also proves the following: if $lh(s) = z$ and $(\forall i < z)((s)_i \leq x)$ then $s \leq 2^{(x+z+1)^2}$.

(c) Provably Recursive Functions; the Theory $I\Sigma_1$

We are going to investigate the theory $I\Sigma_1$ (Q plus induction for Σ_1 formulas). We have two main goals in this subsection: first, to show that exponentiation is definable in $I\Sigma_1$ in such a way that $I\Sigma_0(exp)$becomes a subtheory of $I\Sigma_1$; and, second, to show that the class of all Σ_1 definable functions (on N) whose totalness is provable in $I\Sigma_1$ is closed under primitive recursion and therefore each primitive recursive function is $I\Sigma_1$-provably recursive. The first goal is reached by developing, in some extent, an alternative weak (non-extensional) coding of finite sets in $I\Sigma_1$ based on divisibility. This coding could be fully developed, but we use it only to define exponentiation; then it may be forgotten and the coding based on exponentiation may be used instead. To reach the second goal, we prove more than stated: we show that for each Σ_1-definition of a total function in $I\Sigma_1$, we may construct another Σ_1-definition of a total function in $I\Sigma_1$ such that $I\Sigma_1$ proves that the latter function is the primitive recursive iteration of the former one. This will be frequently used throughout the book (and will be strengthened in the next subsection).

We start with some basic observations on $I\Sigma_1$. Trivially, $I\Sigma_1$ contains $I\Sigma_0$ and therefore proves the least number principle for Σ_0 formulas. (We postpone the proof of the fact that $I\Sigma_1$ proves the least number principle for Σ_1 formulas to Sect. 2.) Now we show that $I\Sigma_1$ proves *collection* for Σ_0 formulas.

1.44 Theorem. For each Σ_0 formula $\varphi(x, y)$ (possibly containing parameters distinct from u, v),

$$I\Sigma_1 \vdash (\forall x < u)(\exists y)\varphi(x, y) \to (\exists v)(\forall x < u)(\exists y < v)\varphi(x, y).$$

Proof. We proceed in $I\Sigma_1$. Assume $(\forall x < u)(\exists y)\varphi(x,y)$ and prove, by Σ_1 induction on w, the following:

$$(*) \qquad w \leq u \to (\exists v)(\forall x < w)(\exists y < v)\varphi(x,y).$$

Nothing is to be proved for $w = 0$; assuming $(*)$ for w and $w+1 \leq u$, let y_0 be such that $\varphi(w, y_0)$ and put $v' = \max(v, y')$. Then we get $(\forall x < w+1)(\exists y < v')\varphi(x,y)$. □

1.45 Corollary. (1) $I\Sigma_1$ proves collection for Σ_1 formulas. (2) Formulas Σ_1 in $I\Sigma_1$ are closed under bounded quantification. (3) Thus formulas Δ_1 in $I\Sigma_1$ are closed under bounded quantification. (4) $I\Sigma_1$ proves the following *order induction* for each Σ_1 formula $\varphi(x)$ (cf. 1.22):

$$(\forall x)((\forall y < x)\varphi(y) \to \varphi(x)) \to (\forall x)\varphi(x).$$

Proof. (1) by contraction of quantifiers. (2) Let $\varphi(\mathbf{x})$ be $(\exists y)\varphi_0(\mathbf{x}, y)$ where φ_0 is Σ_0 and $\mathbf{x}$ is $x_1, x_2, \ldots$. Then the formula $(\exists x_1 \leq x_2)\varphi(\mathbf{x})$ is Σ_1 in $I\Sigma_1$ (commute the existential quantifiers) and so is $(\forall x_1 \leq x_2)\varphi(\mathbf{x})$ since it is equivalent to $(\exists v)(\forall x_1 \leq x_2)(\exists y \leq v)\varphi_0(\mathbf{x}, y)$. (3) is immediate. (4) Apply induction to the formula $(Ay < x)\varphi(y)$ observing that the last formula is Σ_1 in $I\Sigma_1$ by (2). □

Now we shall exhibit an auxiliary coding of sequences.

1.46 Lemma and Definition ($I\Sigma_1$). For each x, there is a least y such that all positive $u \leq x$ divide y. We write $y = \mathit{hull}(x)$.

Proof. We prove $(\forall x)(\exists y)(\forall u \leq x)(0 < u \to u \mid y)$ by Σ_1 induction; the existence of a least such y follows by the least number principle for Σ_0 formulas.

For $x = 0$ the assertion is vacuous. Assume $(\forall u \leq x)(0 < u \to u \mid y)$ and take $y' = y * (x+1)$; then $(\forall u \leq x+1)(u > 0 \to u \mid y)$. □

1.47 Definition. $x \in_0 (y, z)$ iff $(1 + (1+x) * z) \mid y$.

1.48 Lemma (Comprehension). For each Σ_0 formula $\varphi(u)$ $I\Sigma_1$ proves the following:

$$(\forall x)(\exists y, z)(\forall u < x)(u \in_0 (y,z) \equiv \varphi(u)).$$

(φ may contain free variables distinct from u, y, z as parameters.)

Proof. We may assume $x > 1$. Let $z = \mathit{hull}(x)$. We claim that for $u < v < x$ the numbers $1 + (1+u)z, 1 + (1+v)z$ are relatively prime, i.e. their greatest common divisor is 1. (This claim is proved below.) Using this we show the following by Σ_1 induction on t:

$$(*)\qquad \begin{aligned}&(t \leq x \to (\exists y)(\forall u < x)[(u < t \,\&\, \varphi(u) \to u \in_0 (y,z))\,\&\\ &\qquad \&\,(u \geq t \vee \neg\varphi(u))) \to gcd(y, 1 + (1+u)z) = 1)]\,.\end{aligned}$$

For $t = 0$ take $y = 1$. Assume $(*)$ and consider $t+1$. Let y be as in $(*)$.

Case 1: $\neg\varphi(t)$. Then $(*)$ holds for t replaced by $t+1$ and for y as it stands.

Case 2: $\varphi(t)$. Put $y' = y * (1 + (1+t)) * z$. Then clearly $t \in_0 (y', z)$ and $u < t \,\&\, \varphi(u)$ implies $u \in_0 (y', z)$. If $u > t \vee \neg\varphi(u)$ then $gcd(y, 1+(1+u)z) = 1$ and $gcd(y, 1 + (1+t)z) = 1$. Moreover, by our claim, $gcd(1 + (1+u)z, 1 + (1+t)z) = 1$. Now if c divides both $1 + (1+u)z$ and $y' = y * (1 + (1+t)z)$ then, by 1.25, $c \mid y$ or $c \mid 1 + (1+t)z$; thus $c = 1$ and we are done. It remains to prove the claim. □

(Proof of the claim.) Assume $u < v < x$; then $0 < v - u < x$ and $v - u \mid z$. Write u_1, v_1 for $1+u, 1+v$ and let c be such that $c \mid 1+u_1 z$, $c \mid 1+v_1 z$. Then for some a, b we have $1+u_1 z = ac$, $1+v_1 z = bc$, $(1+u_1 z) \mid abc = a(1+v_1 z)$. Since trivially $(1+u_1 z) \mid a(1+u_1 z)$ we get (by subtracting) $(1+u_1 z) \mid a(v_1 z - u_1 z) = a(v-u)z$. Evidently, $gcd(1+u_1 z, z) = 1$; thus, by 1.25, $(1+u_1 z) \mid a(v-u) \mid az$. By the same reasoning, $(1 + u_1 z) \mid a$, which together with $1 + u_1 z = ac$ give $1 + u_1 z = a$ and $c = 1$. □

Remark. Note that the formula $u \in_0 (y, z)$ is Σ_0 in $I\Sigma_1$.

1.49 Definition ($I\Sigma_1$). (1) (y, z) *o-codes a sequence of length* x if for each $u < x$ there is a $v < y$ such that $(u, v) \in_0 (y, z)$. If this is the case then $(y, z)_u$ is the least $v < y$ such that $u, v) \in_0 (y, z)$.

(2) (y, z) is an *exponential sequence* of length x ($Exseq(y, z, x)$) if (y, z) o-codes a sequence of length x, $x \geq 1$, $(y, z)_0 = 1$ and, for each $u < x - 1$, $(y, z)_{u+1} = 2 * (y, z)_u$.

(3) $exp(x, v)$ if $(\exists y, z)(Exseq(y, z, x+1) \,\&\, (y, z)_x = v)$.

1.50 Theorem. (1) $I\Sigma_1 \vdash (\forall x)(\exists! v)(exp(x, v))$.

(2) The formula $exp(x, v)$ is Δ_1 in $I\Sigma_1$.

(3) If we define in $I\Sigma_1$ the function 2^x by $exp(x, v)$ then all axioms of $I\Sigma_0(exp)$ are provable in $I\Sigma_1$.

Proof. (1) First show in $I\Sigma_1$ that if $Exseq(y, z, x)$, $Exseq(y', z', x')$ and $x \leq x'$ then, for each $u < x'$, $(y, z)_u = (y', z')_u$ (uniqueness). This is proved by induction on u, the formula in question being Σ_0 in $I\Sigma_1$. Similarly we prove that $Exseq(y, z, x)$ and $u < x$ implies $u < (y, z)_u$; furthermore, $Exseq(y, z, x)$ and $u < v < x$ implies $(y, z)_u < (y, z)_v$.

Then prove the following by Σ_1 induction on x:

$$x \geq 1 \to (\exists y, z) Exseq(y, z, x)\,.$$

(Note that the formula $(\exists y, z)Exseq(y, z, x)$ is Σ_1 in $I\Sigma_1$ by contraction of quantifiers.) The assertion is evident for $x = 1$. Assume $x \geq 1$, $Exseq(y, z, x)$ and $(y, z)_{x-1} = q$; put $q' = (x, 2q)$. By 1.46, there are y', z' such that

$$(\forall u \leq q')(u \in_0 (y', z') \equiv . (u \in_0 (y, z) \,\&\, (\exists i < x)(\exists v < u)(u = (i, v)) \vee \\ \vee\, u = (x, 2q)) .$$

We get $Exseq(y', z', x + 1)$.

(2) Clearly, $exp(x, v)$ is Σ_1 as defined; but since we have (1), $\neg exp(x, v)$ is equivalent in $I\Sigma_1$ to $(\exists w)(x \neq v \,\&\, exp(x, w))$. Thus the result follows.

(3) We proceed in $I\Sigma_1$. Clearly, $2^0 = 1$. If $2^x = v$ and $2^{x+1} = w$ then we have $Exseq(y, z, x + 1)$, $Exseq(y', z', x + 2)$, $(y, z)_x = v$, $(y', z')_{x+1} = w$; but, by the claim in the proof of (1), $(y', z')_x = v$ and thus $w = 2v$. Thus the axioms for 2^x are provable. It remains to prove that induction for $\Sigma_0(exp)$ formulas is provable. But this follows from the fact that each $\Sigma_0(exp)$ formula is Δ_1 in $I\Sigma_1$. Let us prove this fact.

To prove that atomic $\Sigma_0(exp)$ formulas are Δ_1 it suffices to show that for each term t of $L_0(exp)$ and each variable x not occuring in t, the formula $t = x$ is Δ_1 in $I\Sigma_1$. This is clear for t atomic and the induction step for $S, +$ and $*$ is easy. (For example, $x = t + s$ is equivalent to $(\exists u, v \leq x)(u = t \,\&\, v = s \,\&\, x = u + v)$; if $u = t$ and $v = s$ are Δ_1 in $I\Sigma_1$ then so is $x = t + s$ by 1.45.) Consider $x = 2^t$ and let the formula $u = t$ be Δ_1. It is sufficient to remember that $x = 2^u$ is Δ_1 in $I\Sigma_1$ (see (2) above); $x = 2^t$ is equivalent to $(\exists u \leq x)(x = 2^u \,\&\, u = t)$.

For the rest of the proof it suffices to recall that formulas Δ_1 in $I\Sigma_1$ are closed under connectives and bounded quantifiers. □

*

1.51 Discussion and Definition. (1) Recall that we have Σ_n formulas and Π_n formulas; these are particular formulas of the language of arithmetic. Then we have Σ_n and Π_n sets of natural numbers; i.e. sets defined (in the standard model N by Σ_n formulas and Π_n formulas respectively). Δ_n sets are sets that are both Σ_n and Π_n (cf. Sect. 0). In 1.19 we defined a formula to be Σ_n (Π_n, Δ_n) in a theory T. Now we turn our attention to sets of natural numbers defined by such a formula. Instead of saying that a set X is defined by a formula that is Σ_n in T we say that X is T-provably Σ_n (similarly for Π_n, Δ_n). This generalizes to $X \subseteq N^k, k = 2, 3, \ldots$.

Clearly, if T is sound, i.e. N is a model of T and X is T-provably Σ_n (Δ_n etc.) then X is Σ_n (etc.). The converse need not be true, cf. Chap. IV, Sect. 3.

(2) A formula $\varphi(x, y)$ *defines a total function in* T if $T \vdash (\forall x)(\exists! y)\varphi(x, y)$. We may then extend T by defining a new function symbol F and the axiom $\varphi(x, F(x))$. We may againcall the resulting theory T but care is necessary when dealing with hierarchies of formulas, e.g. we distinguish Σ_0-formulas

and $\Sigma_0(exp)$-formulas. If the formula φ defining F in T is Σ_n in T then we say that F is Σ_n in T, etc.

Clearly, if $\varphi(x,y)$ defines a total function in T and T is sound then φ defines a total function in N. A function $f : N \to N$ is ***T-provably total*** if it has a definition $\varphi(x,y)$ which defines a total function in T. The function f is ***T-provably*** Σ_n (etc.) if it has a definition which is Σ_n in T. (This is a particular case of (1).) The function f is a ***T-provably total*** Σ_n ***function*** if it has a definition φ which is Σ_n in T and defines a total function in T. In particular we call f ***T-provably recursive*** if it is T-provably total Σ_1; since we shall often be interested in $I\Sigma_1$-provably recursive functions we shall call them just ***provably recursive.***

1.52 Lemma. Assume $T \supseteq I_{\text{open}}$. (1) If F is a function symbol Σ_1 in T then F is Δ_1 in T.

(2) If ψ is Δ_1 in T and F is a function symbol Δ_1 in T then the formula $(\exists x \le F(y))\psi$ is Δ_1 in T.

Proof. (1) If $\varphi(x,y)$ is as above then the formula $(\exists y' \neq y)\varphi(x,y')$ is Σ_1 in T and defines the complement of F; thus its negation is Π_1 and defines F.

(2) Let ψ' be $(\exists x \le F(y))\varphi$. Clearly, ψ' is Σ_1 (by contraction of quantifiers). But un T, ψ' is also equivalent to $(\forall z)(z = f(y) \to (\forall x \le z)\psi)$, which is Π_1 in T. □

1.53 Lemma. If $T \supseteq I_{\text{open}}$ then T-provably recursive functions are closed under composition.

Proof. By contraction of quantifiers. □

1.54 Theorem. If $T \supseteq I\Sigma_1$ then T-provably recursive functions are closed under primitive recursion. Thus each primitive recursive function is provably recursive.

For T containing $I\Sigma_1$ the converse is also true; thus provably recursive functions are exactly all primitive recursive functions. The converse inclusion will be proved in Chap. IV. The present theorem is an immediate consequence of the following lemma:

1.55. Let $T \supseteq I\Sigma_1$ and let $\varphi(\mathbf{x},y)$ and $\psi(\mathbf{x},u,v,y)$ be Σ_1 and define total functions in T, i.e. $T \vdash (\forall \mathbf{x})(\exists! y)\varphi(\mathbf{x},y)$ and $T \vdash (\forall \mathbf{x},u,v)(\exists! y)\psi(\mathbf{x},u,v,y)$. Then there is a Σ_1 formula $\chi(\mathbf{x},z,y)$ such that

$$T \vdash (\forall \mathbf{x}, z)(\exists! y)\chi(\mathbf{x},z,y)\,,$$
$$T \vdash (\forall \mathbf{x})(\forall y)(\chi(\mathbf{x},0,y) \equiv \varphi(\mathbf{x},y)\,,$$
$$T \vdash (\forall \mathbf{x},z,y,y_1)(\chi(\mathbf{x},z,y) \mathbin{\&} \chi(\mathbf{x},z+1,y_1). \to \psi(\mathbf{x},z,y,y_1))\,.$$

Thus if the functions defined by φ, ψ, χ are denoted by F, G, H respectively then $T \vdash F(\mathbf{x}, 0) = G(\mathbf{x})$ and $T \vdash F(\mathbf{x}, z+1) = H(\mathbf{x}, z, f(\mathbf{x}, z))$.

Proof. χ just describes the course of values (*Exseq* was a particular case):

$$\chi(\mathbf{x}, z, y) \equiv (\exists s)(Seq(s) \,\&\, lh(s) = z + 1 \,\&\, (s)_0 = G(\mathbf{x}) \,\&\, (s)_z = y \,\& \\ (\forall i < z)((s)_{i+1} = H(\mathbf{x}, i, (s)_i)).$$

Transcribing this with the help of φ, ψ is trivial but tiresome; clearly, χ is Σ_1 in T. $I\Sigma_1$ was used to prove $(\forall \mathbf{x}, z)(\exists y)\chi(\mathbf{x}, z, y)$; uniqueness is easy to prove and a pedantic elaboration of details of the proof of $F(\mathbf{x}, z+1) = H(\mathbf{x}, z, F(\mathbf{x}, z))$ is left to the reader.

1.56 Remark. The lemma says (in contradistinction to 1.54) that inside $I\Sigma_1$ we may define total Δ_1 functions from other Δ_1 functions by primitive recursion. Note that this generalizes easily to primitive recursion on the course of values, cf. 0.44.

*

We now describe some concrete consequences of the preceding lemma.

1.57 Lemma. In $I\Sigma_1$ we may define total Δ_1 functions Σ and Π (sum and product of a sequence) such that $I\Sigma_1$ proves the following:

$$\Sigma x = 0 \text{ if } x = 0 \text{ or } \neg Seq(x),$$
$$\Sigma(s \frown \langle x \rangle) = (\Sigma s) + x,$$
$$\Pi x = 1 \text{ if } x = 0 \text{ or } \neg Seq(x),$$
$$\Pi(s \frown \langle x \rangle) = (\Pi s) * x.$$

Proof. Left as an exercise. (Given s, prove by induction that for each $i \leq lh(s)$ there is a sequence s' of partial sums of length i such that $(s')_0 = (s)_0$ and, for $j < i - 1$, $(s')_{j+1} = (s')_j + (s)_{j+1}$. Put $\Sigma s = y$ if there is a sequence s' of partial sums of s of length $lh(s)$ such that $(s')_{lh((s)} = y$. Similarly for Π.) □

1.58 Theorem. (1) In $I\Sigma_1$ we may Δ_1 define general power and factorial functions; i.e. total functions x^y and $x!$ such that the formulas $z = x^y$ and $z = x!$ are Δ_1 in $I\Sigma_1$ and $I\Sigma_1$ proves the following:

$$x^0 = 1 \text{ and } x^{S(y)} = x^y * x,$$
$$0! = 1 \text{ and } (S(x))! = x! * S(x).$$

(2) $I\Sigma_1$ proves that there are infinitely many primes. In $I\Sigma_1$ we may define an increasing Δ_1 enumeration of all primes.

(3) $I\Sigma_1$ proves the prime factorization theorem.

Proof. (1) follows directly from 1.55. To prove (2) work in $I\Sigma_1$ and take any x; we show that there is a prime $p \geq x$. Let $z = hull(x)$, i.e. $(\forall u < x)(u \mid z)$ and take $z+1$. By 1.26, there is a $p \mid (z+1)$, but p is distinct from all $u < x$. (This is the classic Euclid's proof.) For each x, let $lp(x)$ be the least prime number greater than x; by what we have just proved, lp is a total Δ_1 function. Thus the function

$$p_0 = 2,$$
$$p_{x+1} = lp(p_x)$$

is Δ_1 and total – both provably in $I\Sigma_1$. This is the desired increasing enumeration of all primes.

(3) A sequence s is a *prime decomposition* if all members of s are primes and the sequence is non-decreasing, i.e. $(s)_i \leq (s)_{i+1}$ for all $i < lh(s) - 1$. We claim that for each $x > 0$ there is a unique prime decomposition s such that $\Pi s = x$. Existence is proved by induction: the prime decomposition of 1 is the empty sequence $\emptyset$. Let $x > 1$ and assume $(\forall y < x)(y > 0 \rightarrow$ y has a prime decomposition.). Let p be the largest prime dividing x (it exists by the least number principle for Σ_0 formulas) and take the y such that $x = p * y$ (divide x by p). Now $y < x$, so let s be a prime decomposition of y. Then $s \frown \langle p \rangle$ is a prime decomposition of x. □

1.59 Remark. (1) Prove the uniqueness of the prime decomposition of x as an exercise.

(2) Many theorems of elementary number theory formalize easily in $I\Sigma_1$ together with their proofs; for example, the proof of *Bertrand's postulate* (saying that for each $x > 0$ there is a prime number p such that $x \leq p \leq 2x$) as given in [Hardy-Wright] can be easily rewritten in $I\Sigma_1$.

(3) Moreover, in Theorems 1.56, 1.57 $I\Sigma_1$ may be replaced by $I\Sigma_0(exp)$ but proofs then cost some additional effort since we do *not* have 1.54–1.55 for $I\Sigma_0(exp)$. Instead we have the following: $I\Sigma_0(exp)$-provably total $\Sigma_0^{exp}(exp)$ functions are closed under bounded primitive recursion, i.e. if G, H, K are $I\Sigma_0(exp)$-provably total $\Sigma_0^{exp}(exp)$ functions, F results from G, H by primitive recursion and F is provably majorized by K then F is $I\Sigma_0(exp)$-provably total $\Sigma_0^{exp}(exp)$ function (and we have the corresponding lemma analogous to 1.55). The reader may elaborate details as an exercise.

(d) Arithmetization of Metamathematics: Partial Truth Definitions

Recall our investigations in 0.50–0.55 (beginning arithmetization of metamathematics): we showed there that various logical sets, functions, etc. are Δ_1 in N. As we promised there, we shall now strengthen these results and develop them further; we are going to show that logical notions (like formulas, terms etc.) are Δ_1 in $I\Sigma_1$ and that $I\Sigma_1$ proves their basic properties. We shall detail careful formulations; proofs consist more or less in checking that informal proofs presented in Sect. 0 can be read as proofs in $I\Sigma_1$. Our gain will be twofold: We shall see that some reasonable parts of logic formalize in $I\Sigma_1$ and secondly, we shall be able to expand expressive possibilities of $I\Sigma_1$ by introducing variables for Σ_n (Π_n, Δ_n) sets of numbers. This will be very useful.

1.60 Theorem. Let $T \supseteq I\Sigma_1$, let $At^\bullet, Op^\bullet, Ar^\bullet$ be formulas Δ_1 in T and assume that T proves $At^\bullet, Op^\bullet$ to be disjoint, $At^\bullet$ non-empty and $Ar^\bullet$ to define a total function, i.e.

$$\begin{aligned} &T \vdash (\forall x)(Op^\bullet(x) \to (\exists! y)Ar^\bullet(x,y)), \quad (\text{write } y = Ar^\bullet(x) \text{ for } Ar^\bullet(x,y)) \\ &T \vdash (\exists x)(At^\bullet(x)\,\&\,(\forall y)(At^\bullet(y) \to \neg(Seq^\bullet(y)\,\&\,Op^\bullet((y)_0)) \\ &\quad \text{cf. } (0.50)\,. \end{aligned}$$

Then there are formulas $Expr^\bullet, Appl^\bullet$ that are Δ_1 in T and such that T proves $(Expr^\bullet, Appl^\bullet)$ to be a free algebra of type $(Op^\bullet, Ar^\bullet)$ generated by $At^\bullet$, i.e.

$$\begin{aligned} &T \vdash At^\bullet(x) \to Expr^\bullet(\langle x\rangle)\,, \\ &T \vdash Appl^\bullet(o,s,y) \\ &\qquad \equiv (Op^\bullet(o), Seq^\bullet(s)\,\&\,lh(s) = Ar^\bullet(o), y = \langle o\rangle \frown Concseq(s))\,, \\ &T \vdash Appl^\bullet(o,s,y)\,\&\,(\forall i < lh(s))(Expr^\bullet(((s)_i)\,.\to Expr^\bullet(y)\,, \end{aligned}$$

and for each Σ_1 formula $\varphi(x)$ (possibly with parameters),

$$\begin{aligned} &T \vdash (\forall x)(At^\bullet(x) \to \varphi(x))\,\& \\ &\qquad \&\,((\forall o,s,y)(Appl^\bullet(o,s,y)\,\&\,(\forall i < lh(s))\varphi((s)_i)\,.\to \varphi(y)) \to \\ &\qquad \to (\forall x)(Expr^\bullet(x) \to \varphi(x))\,. \end{aligned}$$

Thus atomic expressions are expressions; applying an operation to a sequence of expressions of the appropriate length gives an expressions; each non-atomic expression uniquely determines its components; and Expr is the least Σ_1 set containing all atomic expressions and closed under application of operations.

Convention. We shall identify atomic expressions $\langle x\rangle$ with atoms x if there is no danger of misunderstanding. (This corresponds to the usual convention of omitting superfluous brackets.)

Proof. Define $Appl^\bullet(o,s) = \langle o\rangle \frown Concseq(s)$; we define w to be a derivation formalizing the definition in 0.51; define

$$Expr^\bullet(s) \equiv (\exists q)(q \text{ is a derivation and } s \text{ is its last element})\,.$$

The rest of the proof consists in checking the proof of 0.51. □

Now we could define a Δ_1 presentation of terms and formulas of an arbitrary language; instead, we restrict ourselves to the language of *arithmetic* leaving the general case to the reader as an exercise.

1.61 Theorem. In $I\Sigma_1$ we can define constants $S^\bullet$, $+^\bullet$, $*^\bullet$, $=^\bullet$, $\leq^\bullet$, $\overline{0}^\bullet$, $\neg^\bullet$, $\rightarrow^\bullet$, $\forall^\bullet$, Δ_1 predicates $Var^\bullet$, $Term^\bullet$, $Atform^\bullet$, $Form^\bullet$ and Δ_1 functions $Applterm^\bullet$, $Applform^\bullet$ such that basic properties of terms and formulas are provable. More precisely, $I\Sigma_1$ proves the following:

(1) $(Term^\bullet, Applterm^\bullet)$ is a free algebra over variables$^\bullet$ and the constant $\overline{0}^\bullet$ as atoms with the operations $S^\bullet$ (unary), $+^\bullet, *^\bullet$ (binary);

(2) An atomic formula$^\bullet$ consists of $=^\bullet$ or $\leq^\bullet$ together with two terms:

$$Atform^\bullet(x) \equiv (\exists s,t \leq x)(Term^\bullet(s)\,\&\,Term^\bullet(t) \\ \&\,.\,x = \langle =^\bullet, s, t\rangle \vee x = \langle \leq^\bullet, s, t\rangle)\,.$$

(3) $(Form^\bullet, Applform^\bullet)$ is a free algebra over atomic formulas$^\bullet$ as atoms with the following operations: $\neg^\bullet$ (unary), $\rightarrow^\bullet$ (binary), and each variable$^\bullet$.

(4) There are infinitely many variables$^\bullet$:

$$(\forall x)(\exists y \geq x)Var^\bullet(y))\,.$$

(5) Terms$^\bullet$ are disjoint from formulas$^\bullet$:

$$(\forall x)\neg(Term^\bullet(x)\,\&\,From^\bullet(x))\,.$$

In a still more transparent way this may be formulated as follows: Write

$$\begin{aligned}
x +^\bullet y &\text{ instead of } Applterm^\bullet(+^\bullet, \langle x,y\rangle)\,,\\
x *^\bullet y &\text{ instead of } Applterm^\bullet(*^\bullet, \langle x,y\rangle)\,,\\
S^\bullet(x) &\text{ instead of } Applterm^\bullet(S^\bullet, \langle x\rangle)\,,\\
t =^\bullet s &\text{ instead of } \langle =^\bullet, t, s\rangle\,,\\
t \leq^\bullet s &\text{ instead of } \langle \leq^\bullet, t, s\rangle\,,\\
\neg^\bullet(x) &\text{ instead of } Applform^\bullet(\neg^\bullet, \langle x\rangle)\,,\\
x \rightarrow^\bullet y &\text{ instead of } Applform^\bullet(\rightarrow^\bullet, \langle x,y\rangle)\,,\\
(\forall^\bullet u)x &\text{ instead of } Applform^\bullet(u, \langle x,y\rangle) \text{ where } Var^\bullet(u)
\end{aligned}$$

Then $I\Sigma_1$ proves the following:

* there are infinitely many variables$^\bullet$,
* each variable$^\bullet$ is a term$^\bullet$,
* if t, s are terms$^\bullet$ then $t +^\bullet s, t *^\bullet s, S^\bullet(t)$ are terms$^\bullet$,
* atomic formulas$^\bullet$ have the form $t =^\bullet s$ or $t \leq^\bullet s$ where t, s are terms$^\bullet$,
* if x, y are formulas$^\bullet$ and u is a variable$^\bullet$ then $x \to^\bullet y$, $\neg^\bullet x$, $(\forall^\bullet u)x$ are formulas$^\bullet$.

Furthermore, for each Σ_1 formula φ, $I\Sigma_1$ proves the following:
IF $\varphi(\overline{0}^\bullet)$, $(\forall x)(Var^\bullet(x) \to \varphi(x))$ and $(\forall t, s \text{ terms}^\bullet)(\varphi(t) \,\&\, \varphi(s) \to \varphi(S^\bullet(t)$, $\varphi(t +^\bullet s), \varphi(t *^\bullet s)$ THEN $(\forall x)(Term^\bullet(x) \to \varphi(x))$.
Similarly for formulas$^\bullet$.

Proof. Choose concrete natural numbers $n_1, \ldots, n_9$ such that $I\Sigma_1 \vdash \neg Seq(\overline{n_i})$ and put, in $I\Sigma_1$, $S^\bullet = \overline{n_1}, +^\bullet = \overline{n_2}, \ldots, \forall^\bullet = \overline{n_8}, v^\bullet = \overline{n_9}$ (auxiliary); define e.g. $Var^\bullet(x) \equiv (\exists y \leq x)(x = \langle v^\bullet, y\rangle)$. Then apply 1.60 twice: once for $\overline{0}^\bullet$ and variables$^\bullet$ as atoms and $S^\bullet, +^\bullet, *^\bullet$ as operations to get $Term^\bullet$ and then for atomic formulas$^\bullet$ as atoms ($Atform^\bullet$ as in (2))and $\neg^\bullet, \to^\bullet$ and variables$^\bullet$ as operations. □

1.62 Definition ($I\Sigma_1$). Define $vr^\bullet(y) = \langle v^\bullet, y\rangle$ (y-th variable), $nm^\bullet(\overline{0}) = \overline{0}^\bullet$, $nm^\bullet(x+1) = S^\bullet(nm^\bullet(x))$ (x-th numeral). Clearly, this defines total Δ_1 functions in $I\Sigma_1$. We often write $\dot{x}$ instead of $nm^\bullet(x)$.

1.63 Theorem. (Construction of a Δ_1 function by induction on terms.) Let G, H_1, H_2, H_3 be total Δ_1 functions in $I\Sigma_1$. Then there is a total Δ_1 function in $I\Sigma_1$ such that $I\Sigma_1$ proves the following:

$$\begin{aligned} F(x) &= G(x) \text{ if } Var^\bullet(x) \text{ or } x = \overline{0}^\bullet\,, \\ F(x +^\bullet y) &= H_1(x, y) \\ F(x *^\bullet y) &= H_2(x, y) \\ F(S^\bullet(x)) &= H_3(x) \text{ for } x, y \text{ terms}^\bullet\,, \\ F(x) &= \overline{0} \text{ for } \neg Term^\bullet(x). \end{aligned}$$

Proof. F may be constructed by recursion on the course of values (cf. 0.44 and 1.56). □

1.64 Remark. (1) In $I\Sigma_1$ we may define a total Δ_1 function assigning to each term$^\bullet$ u the finite set of its variables$^\bullet$:

$$\begin{aligned} \mathit{Var\_of}^\bullet(u) &= \{u\} \text{ if } Var^\bullet(u)\,, \\ \mathit{Var\_of}^\bullet(u) &= \emptyset \text{ if } u = \overline{0}^\bullet\,, \\ \mathit{Var\_of}(x +^\bullet y) &= (\mathit{Var\_of}^\bullet(x)) \cup \mathit{Var\_of}^\bullet(y))\,, \\ \mathit{Var\_of}^\bullet(x *^\bullet y) &= (\mathit{Var\_of}^\bullet(x)) \cup \mathit{Var\_of}^\bullet(y))\,, \\ \mathit{Var\_of}^\bullet(S^\bullet(x)) &= \mathit{Var\_of}^\bullet(x)\,. \end{aligned}$$

(2) A completely analogous theorem on the construction of a Δ_1 function by induction on formulas is now evident; for example, we may define the set of all its free variables$^\bullet$ of a formula$^\bullet$ as follows:

$$\begin{aligned}
\mathit{Freevar}^\bullet(u =^\bullet v) &= \mathit{Var_of}^\bullet(u) \cup \mathit{Var_of}^\bullet(v)\,,\\
\mathit{Freevar}^\bullet(u \leq^\bullet v) &= \text{ similarly}\,,\\
\mathit{Freevar}^\bullet(\neg^\bullet x) &= \mathit{Freevar}^\bullet(x)\,,\\
\mathit{Freevar}^\bullet(x \rightarrow^\bullet y) &= \mathit{Freevar}^\bullet(x) \cup \mathit{Freevar}^\bullet(y)\,,\\
\mathit{Freevar}^\bullet((\forall^\bullet w)x) &= \mathit{Freevar}^\bullet(x) \setminus \{w\}\,.
\end{aligned}$$

Furthermore, in $I\Sigma_1$ we may define total Δ_1 functions $\mathit{Subst}^\bullet$ (substitution), $\mathit{Val}^\bullet$ (evaluation of terms) such that $I\Sigma_1$ proves the following:

(3) (Substitution into terms.)

$$\begin{aligned}
\mathit{Subst}^\bullet(x, x, t) &= t \text{ if } Var^\bullet(x) \,\&\, Term^\bullet(t)\,,\\
\mathit{Subst}^\bullet(t_1 +^\bullet t_2, x, t) &= \mathit{Subst}^\bullet(t_1, x, t) +^\bullet \mathit{Subst}^\bullet(t_2, x, t)\,,
\end{aligned}$$

if t_1, t_2, t are terms$^\bullet$ and x is a variable$^\bullet$; similarly for $*^\bullet, S^\bullet$.

(4) (Substitution into formulas.)

$$\begin{aligned}
\mathit{Subst}^\bullet(t_1 =^\bullet t_2, x, t) &= (\mathit{Subst}^\bullet(t_1, x, t) =^\bullet \mathit{Subst}^\bullet(t_2, x, t))\,,\\
\mathit{Subst}^\bullet(\neg^\bullet z, x, t) &= \neg^\bullet \mathit{Subst}^\bullet(z, x, t)\,,\\
\mathit{Subst}^\bullet(z_1 \rightarrow^\bullet z_2, x, t) &= (\mathit{Subst}^\bullet(z_1, x) \rightarrow^\bullet \mathit{Subst}^\bullet(z_2, x, t))\,,\\
\mathit{Subst}^\bullet((\forall^\bullet u)z, x, t) &= (\forall^\bullet u)z \text{ if } u = x\,,\\
\mathit{Subst}^\bullet((\forall^\bullet u))z, x, t) &= (\forall^\bullet u)\mathit{Subst}^\bullet(z, x, t) \text{ if } u \neq x\,.
\end{aligned}$$

(5) (Value of a term.) If t is a term$^\bullet$ and z is an evaluation of its variables$^\bullet$, i.e. a finite mapping whose domain consists of some variables$^\bullet$, among them all variables$^\bullet$ of t then:

$$\begin{aligned}
\mathit{Val}^\bullet(t, z) &= z(t) \text{ if } t \text{ is a variable}^\bullet\,,\\
\mathit{Val}^\bullet(t_1 +^\bullet t_2, z) &= \mathit{Val}^\bullet(t_1, z) + \mathit{Val}^\bullet(t_2, z)
\end{aligned}$$

similarly for $*^\bullet, S^\bullet$ and $*, S$.

1.65 Remark. We have constructed a definition of sequences, terms, formulas, etc. that are Δ_1 in $I\Sigma_1$ and such that basic properties (in particular, closure properties) are provable in $I\Sigma_1$. Our definitions define the corresponding notions (sets, functions, etc.) in N; for example, φ is a formula iff $N \models Form^\bullet[\varphi]$ (this was discussed in Sect. 0). But since our definitions are Δ_1 in $I\Sigma_1$ we can use Σ_1-completeness of $I\Sigma_1$ (see 1.9) to get the following:

(i) For each $t \in N$,
t is a term iff $N \models Term^\bullet(\bar{t})$ iff $I\Sigma_1 \vdash Term^\bullet(\bar{t})$,

t is $t_1 + t_2$ iff $N \models \overline{t} = (\overline{t_1} +^\bullet \overline{t_2})$ iff $I\Sigma_1 \vdash \overline{t} = \overline{t_1} +^\bullet \overline{t_2}$, similarly for $S, *$.

(ii) For each $\varphi \in N$,
φ is a formula iff $N \models Form^\bullet(\overline{\varphi})$ iff $I\Sigma_1 \vdash Form^\bullet(\overline{\varphi})$,
φ is $t = s$ iff $N \models \overline{\varphi} = (\overline{t} =^\bullet \overline{s})$ iff $I\Sigma_1 \vdash \overline{\varphi} = (\overline{t} =^\bullet \overline{s})$,
φ is $\varphi_1 \to \varphi_2$ iff $N \models \overline{\varphi} = (\overline{\varphi_1} \to^\bullet \overline{\varphi_2})$ iff $I\Sigma_1 \vdash \overline{\varphi} = (\overline{\varphi_1} \to^\bullet \overline{\varphi_2})$,
similarly for $t \leq s$, $\neg$, $(\forall y)$.

(iii) If t, s are terms, φ is a formula and x is a variable then

$$I\Sigma_1 \vdash Subst^\bullet(\overline{t}, \overline{x}, \overline{s}) = \overline{Subst(t, x, s)}\,,$$
$$I\Sigma_1 \vdash Subst^\bullet(\overline{\varphi}, \overline{x}, \overline{s}) = \overline{Subst(\varphi, x, s)}\,.$$

1.66 Lemma. If $t(x_0, \ldots, x_n)$ is a term whose variables are among $x_0, \ldots, x_n$ then

$$I\Sigma_1 \vdash t(x_0, \ldots, x_n) = Val^\bullet(\overline{t}, z(x_0, \ldots, x_n))\,,$$

where $z(x_0, \ldots, x_n)$ is the finite mapping associating with each variable$^\bullet$ $\overline{x_i}$ the number x_i $(i = 0, \ldots, n)$.

Proof. Construct the corresponding $I\Sigma_1$-proofs by induction over subterms of t: if t is x_i then $I\Sigma_1 \vdash x_i = x_i$; if t is $t_1 + t_2$ and $I\Sigma_1 \vdash t_i = Val^\bullet(\overline{t_i}, z))(i = 1, 2)$ then $I\Sigma_1 \vdash t_1 + t_2 = Val^\bullet(\overline{t_1 + t_2}, z)$, etc. □

1.67 Remark. Note that this may also be expressed as follows: write $v(w/u)$ for $Subst^\bullet(v, u, w)$ and $v(w_1/u_1, \ldots, w_n/u_n)$ for iterated substitution. Then

$$I\Sigma_1 \vdash t(x_0, \ldots, x_n) = Val(\overline{t}(\dot{x}_0/\overline{x_0}, \ldots, \dot{x}_n/\overline{x_n}, \emptyset)\,.$$

In particular, for t without variables we get $I\Sigma_1 \vdash t = Val(\overline{t})$, e.g. $\overline{3} + \overline{7} = Val(\overline{3}^\bullet +^\bullet \overline{7}^\bullet) = \overline{10}$.

1.68 Lemma. There is a formula $\Sigma_0^\bullet(x)$ (saying: x is a $\Sigma_0^\bullet$-formula$^\bullet$) such that

(1) $\Sigma_0^\bullet(x)$ is a Δ_1 formula in $I\Sigma_1$ and

(2) $I\Sigma_1$ proves the following:

(i) Each atomic formula$^\bullet$ is $\Sigma_0^\bullet$,

(ii) $\Sigma_0^\bullet$ formulas$^\bullet$ are closed under connectives$^\bullet$ and [bounded quantifiers]$^\bullet$;

(3) Furthermore, for each Σ_1 formula $\varphi(x)$, $I\Sigma_1$ proves the following:

(iii) If each atomic formula$^\bullet$ satisfies φ and formulas$^\bullet$ satisfying φ are closed under connectives$^\bullet$ and [bounded quantifiers]$^\bullet$ then each $\Sigma_0^\bullet$ formula$^\bullet$ satisfies φ.

Proof. Formalization of bounded quantifiers is clear: $(\forall^\bullet u \leq^\bullet v)z$ is just $(\forall^\bullet u)(u \leq^\bullet v \to^\bullet z)$ The proof is completely analogous to the proof of 1.60 (Δ_1 definition of expressions). □

1.69 Lemma. There are formulas $\Sigma_y^\bullet(x), \Pi_y^\bullet(x)$ with two free variables (read: x is a $\Sigma_y^\bullet$ formula$^\bullet$, similarly for Π) such that (1) both $\Sigma_y^\bullet(x)$ and $\Pi_y^\bullet(x)$ are Δ_1 in $I\Sigma_1$, and (2) $I\Sigma_1$ proves the following:

(i) for $y = 0$, $\Sigma_0^\bullet(x) \equiv \Pi_y^\bullet(x)$;
(ii) $\Pi_{y+1}^\bullet(x)$ iff there is a variable$^\bullet$ $u \leq x$ and a $\Sigma_y^\bullet$ formula z such that $x = (\forall^\bullet u)z$;
(iii) similarly for $\Sigma_{y+1}^\bullet$.

Proof. Exercise. □

We are now ready for a definition of satisfaction for Σ_0 formulas.

1.70 Theorem. There is a formula $Sat_0(z, e)$ which is Δ_1 in $I\Sigma_1$ and such that $I\Sigma_1$ proves Tarski's satisfaction conditions (cf. 0.6) for Σ_0 formulas$^\bullet$, i.e. $I\Sigma_1$ proves the following:

(i) $Sat_0(z, e) \to z$ is a $\Sigma_0^\bullet$ formula$^\bullet$ and e is an evaluation$^\bullet$ for z,
(ii) if z is $\Sigma_0^\bullet$ and $z = (u =^\bullet v)$ then

$$Sat_0(z, e) \equiv Val^\bullet(u, e) = Val^\bullet(v, e)$$

and similarly for $z = (u \leq^\bullet v)$;
(iii) if z is $\Sigma_0^\bullet$ and $z = (\neg^\bullet u)$ then $Sat_0(z, e)$ iff $\neg Sat_0(u, e)$ and similarly for $z = (u \to^\bullet v))$;
(iv) if z is $\Sigma_0^\bullet$ and $z = ((\forall^\bullet w_1 \leq^\bullet w_2)u)$ then $Sat_0(z, e)$ iff for each e' evaluation of u coinciding with e on $Freevar^\bullet(z) \setminus \{w_1\}$ and such that $e'(w_1)$ is defined and $e'(w_1) \leq e'(w_2)$ we have $Sat_0(u, e')$.

The proof is in 1.71–1.73.

1.71 Definition ($I\Sigma_1$). (1) q is a *partial satisfaction* for $\Sigma_0^\bullet$ formulas$^\bullet$ $\leq p$ and their evaluations$^\bullet$ by numbers $\leq r$ (in symbols: $PSat_0(q, p, r)$) if q is a finite mapping whose domain consists of all pairs (z, e) where z is $\Sigma_0^\bullet$, $z \leq p$, e is an evaluation$^\bullet$ for z, $e \subseteq (\leq p) \times (\leq r)$, $range(q) \subseteq \{0, 1\}$ and Tarski's conditions hold for q whenever those things in question are defined, i.e. for each $(z, e) \in dom(q)$,

(ii) if $z = (u =^\bullet v)$ then $q(z, e) = \overline{1}$ iff $Val^\bullet(u, e) = Val^\bullet(v, e)$, similarly for $z = (u \leq^\bullet v)$;
(iii) if $z = (\neg^\bullet u)$ then $q(z, e) = \overline{1}$ iff $q(u, e) = \overline{0}$, similarly for $z = (u \to^\bullet v)$;
(iv) if $z = ((\forall^\bullet w_1 \leq^\bullet w_2)u)$ then $q(z, e) = \overline{1}$ iff for each $e' \subseteq (\leq p) \times (\leq q)$ as in (iv) above we have $q((u, e') = \overline{1}$.

(Note that e is assumed to be defined only for (some) variables$^\bullet$ y such that $y \leq p$ and evaluates them by numbers $\leq r$.)

(2) $Sat_0(z, e)$ iff there are q, p, r such that $PSat_0(q, p, r)$ and $q(z, e) = 1$.

1.72 Lemma. (1) $PSat_0$ is Δ_1 in $I\Sigma_1$.

(2) $I\Sigma_1$ proves that if q_1, q_2 are partial satisfactions for $\Sigma_0^\bullet$ then they coincide at the intersection of their domains.

(3) $I\Sigma_1$ proves that for each p, r, there is a q such that $PSat_0(q, p, r)$.

Proof. (1) Recall that Δ_1 includes $\Sigma_0^{exp}(exp)$ and also recall 1.52(2). For example, $dom(q)$ is characterized as follows:

$$\begin{aligned}&(\forall x \in dom(q))(\exists z, e \leq x)(x = (z, e)\,\&\, e \text{ is an evaluation}^\bullet\\ &\qquad\qquad \text{for } z \,\&\, z \leq p \,\&\, e \leq r)\,\&\\ &(\forall z, e \leq H(p, r))(e \text{ is an evaluation}^\bullet \text{ for } z\,\&\\ &\qquad\qquad \&\, z \leq p \,\&\, e \leq r. \rightarrow (z, e) \in dom(q))\end{aligned}$$

where $H(p, r)$ is a term majorizing all such (z, e); take e.g. $(p + r + 2)^2$. The rest is left as an exercise.

(2) In $I\Sigma_1$ we prove the formula

$$\begin{aligned}&PSat_0(q_1, p_1, r_1)\,\&\, PSat_0(q_2, p_2, r_2) \rightarrow\\ &\quad \rightarrow (\forall e < q_1)(\text{both } q_1(z, e) \text{ and } q_2(z, e) \text{ defined} \rightarrow q_1(z, e) = q_2(z, e))\end{aligned}$$

by induction on z (in the form 1.45(3)): if $q_1(z, e)$ and $q_2(z, e)$ are defined and z is atomic then the conclusion follows by the definition of $PSat_0$; if z is $\neg^\bullet u$ are $u \rightarrow^\bullet v$ then by the inductive assumption, $q_1(u, e)$ and $q_2(u, e)$ are defined and equal (and the same for v); thus $q_1(z, e) = q_2(z, e)$. If z is $(\forall^\bullet w_1 \leq^\bullet w_2)u$ and $q_i(z, e)$ is defined then $e(w_2)$ is defined and $e(w_2) \leq r$; thus if $e' \subseteq (\leq p) \times (\leq r)$ is a finite mapping coinciding with e on all free variables$^\bullet$ of u except possibly w_1, assigning to w_1 a value $\leq e(w_2)$ and undefined elsewhere then $q_i(u, e')$ is defined, and by the induction assumption, $q_1(u, e') = q_2(u, e')$. Thus $q_1(z, e) = q_2(z, e)$.

(3) We prove in $I\Sigma_1$ the formula

$$(*) \qquad\qquad (\exists q) PSat_0(q, p, r)$$

by induction on p, with r a parameter. Nothing has to be proved for $p = \overline{0}$; assume $(*)$, let $PSat_0((q, p, r)$ and take $u = p+1$. If u is neither a $\Sigma_0^\bullet$ formula nor a variable$^\bullet$ then we have $PSat_0(q, u, r)$; if u is a variable$^\bullet$ then we have to extend q to a q' such that q' is defined for all pairs (z, e) where z is a $\Sigma_0^\bullet$ formula$^\bullet$, $z \leq p$ and e is an evaluation for z, $e \subseteq (\leq u) \times (\leq r)$. Therefore e may be defined for u but the value is irrelevant for $q'(z, e)$ since u cannot occur in z. Thus put $q'(z, e) = q(z, e\downarrow)$ where $e\downarrow$ means the restriction of e to arguments different from u. Show using comprehension that q' exists; $PSat_0(q', u, r)$ is evident.

If u is a $\Sigma_0^\bullet$ formula then we have to discuss several cases; but note that now u is not a variable$^\bullet$ so we have only to investigate only evaluations

$e \subseteq (\leq p) \times (\leq r)$. We need to extend q to a q' such that $q'(u,e)$ is defined for all e just mentioned.

(i) u is atomic, $u = (t =^\bullet s)$: define

$$\begin{aligned} q'(u,e) &= \bar{1} \text{ iff } Val^\bullet(t) = Val^\bullet(s)\,, \\ q'(u,e) &= \bar{0} \text{ otherwise}\,, \\ q'(z,e) &= q(z,e) \text{ if defined}\,. \end{aligned}$$

q' exists by comprehension.

(ii) u is $\neg^\bullet v$; since $v \leq p$, $q(v,e)$ is defined for all e in question. We put $q'(u,e) = \bar{1} - q(v,e)$, $q'(z,e) = q(z,e)$ if defined. Similarly for $u = (v \rightarrow^\bullet w)$.

(iii) u is $(\forall^\bullet w_1 \leq^\bullet w_2)v$. If $e \subseteq (\leq p) \times (\leq r)$ is an evaluation for u and $a = e(w_2)$ then extend q by defining $q'(u,e) = \bar{1}$ iff for all $e' \subseteq (\leq p) \times (\leq r)$ evaluations for v coinciding with e on $Freevar^\bullet(v) \setminus \{w_1\}$, defined also for w_1 and assigning to w_1 a value $e'(w_1) \leq a$ we have $q(v,e') = \bar{1}$; otherwise put $q'(u,e) = \bar{0}$. (Furthermore, $q'(z,e) = q(z,e)$ if defined.) Again q' exists by comprehension. This completes the proof. □

1.73 Lemma ($I\Sigma_1$). (1) Sat_0 is Δ_1 in $I\Sigma_1$. (2) $I\Sigma_1$ proves Tarski's satisfaction conditions for $\Sigma_0^\bullet$ formulas$^\bullet$ and Sat_0.

Proof. (1) As it stands, Sat_0 is clearly Σ_1. But by the preceding lemma, $I\Sigma_1$ proves (assuming that z is a formula$^\bullet$ and e is an evaluation$^\bullet$) $Sat_0(z,e)$ to be equivalent to

$$(\forall q,p,r)(PSat_0(q,p,r) \,\&\, q(z,e) \text{ defined } \rightarrow q(z,e) = 1)\,.$$

Thus Sat_0 is Π_1 in $I\Sigma_1$.

(2) The only thing to check is the condition for bounded quantifiers. Assume $z = (\forall^\bullet w_1 \leq^\bullet w_2)u$ and $Sat_0(z,e$; thus assume $PSat(p,q,r)$ and $q(z,e) = 1$. Then $z \leq p$ and for each $e' \subseteq (\leq p) \times (\leq r)$ such that e' coincides with e on $Freevar^\bullet(u) \setminus \{w_1\}$ and $e'(w_2) \leq e(w_1)$ we have $q(u,e') = 1$, i.e. $Sat_0(u,e')$. We have to get rid of the condition $e' \subseteq (\leq p) \times (\leq r)$. But if e' is as above except for the last condition then the restriction e'' of e to $Freevar^\bullet(u) \cup \{w_1\}$ does satisfy the condition $e'' \subseteq (\leq p) \times (\leq r)$ and for each q',p',r' such that $PSat(q',p',r')$ and both $q'(u,e')$ and $q'(u,e''))$ are defined, we have $q'(u,e') = q'(u,e'')$ (since ee', e'' coincide on relevant variables$^\bullet$). Thus we have $Sat_0(u,e'')$ and $Sat_0(u,e')$. We have proved the implication *to* in 1.70(iv); the converse implication is easy. This completes the proof of the lemma and of 1.70. □

1.74 Definition. For each $n > 0$ we define in $I\Sigma_1$ predicates $Sat_{\Sigma,n}$ and $Sat_{\Pi,n}$ as follows:

$$Sat_{\Sigma,0}(z,e) \equiv Sat_{\Pi,0}(z,e) \equiv Sat_0(z,e)\,;$$

given $Sat_{\Sigma,n}$ we define

$$\begin{aligned}Sat_{\Pi,n+1}(z,e) \equiv .\,[&z \text{ has the form } (\forall^\bullet x)u \text{ where } u \text{ is } \Sigma_n^\bullet\\ &e \text{ evaluates free variables}^\bullet \text{ of } z \text{ and for each}\\ &\text{evaluation } e' \text{ for } u \text{ coinciding with } e\\ &\text{on } \mathit{Freevar}^\bullet(u) \setminus \{x\} \text{ we have } Sat_{\Sigma,n}(u,e')]\,.\end{aligned}$$

Similarly for $Sat_{\Sigma,n+1}$ (from $Sat_{\Pi,n}$).

1.75 Theorem. (1) For each $n \leq 1$, $Sat_{\Sigma,n}$ is Σ_n in $I\Sigma_1$ and $Sat_{\Pi,n}$ is Π_n in $I\Sigma_1$.

(2) $I\Sigma_1$ proves Tarski's satisfaction conditions for $Sat_{\Sigma,n}$ and $\Sigma_n^\bullet$ formulas $^\bullet$ as well as for $Sat_{\Pi,n}$ and $\Pi_n^\bullet$ formulas$^\bullet$; i.e. it proves analogs of 1.70(i)–(iv) and, in addition,

(v) if $m \leq n$, z is $\Sigma_m^\bullet$ and $z = (\exists^\bullet x)u$ then $Sat_{\Sigma,n}(z,e)$ iff there is an evaluation$^\bullet$ e' of u coinciding with e on $\mathit{Freevar}^\bullet(z)$ and such that $Sat_{\Sigma,n}(u,e')$;

(v') if $m \leq n$, z is $\Pi_m^\bullet$ and $z = (\forall^\bullet x)u$ then $Sat_{\Sigma,n}(z,e)$ iff for all evaluations e' of u coinciding with e on $\mathit{Freevar}^\bullet(z)$ we have $Sat_{\Sigma,n}(u,e')$;

(v"), (v"') similarly for $Sat_{\Pi,n}$.

Proof. (1) is obvious from 1.70 by induction on n. Also (2) is easy to prove from the definitions. □

1.76 Corollary ("It's snowing"-It's Snowing-Lemma). If $\varphi(x_0,\ldots,x_n)$ is Σ_n then

$$I\Sigma_1 \vdash \varphi(x_0,\ldots,x_n) \equiv Sat_{\Sigma,n}(\overline{\varphi}(\dot{x}_0/\overline{x_0},\ldots,\dot{x}_n/\overline{x_n},\emptyset)\,.$$

This formalizes Tarski's example: the sentence "it's snowing" is true iff it's snowing. Recall that $\overline{\varphi}(\dot{x}_0/\overline{x_0},\ldots)$ is an abbreviation of

$$Subst^\bullet \ldots Subst^\bullet(Subst^\bullet(\overline{\varphi}, vr^\bullet(\overline{0}),\dot{x}_0), vr^\bullet(\overline{1}),\dot{x}_1),\ldots vr^\bullet(\overline{n}),\dot{x}_n)\,.$$

1.77 Remark. Observe that 1.70 is just a theorem in $I\Sigma_1$; to prove it we needed only a finite fragment of $I\Sigma_1$ (since each proof of a single theorem uses finitely many axioms). Similarly, for each fixed $n \leq 1$, Tarski's satisfaction conditions for $\Sigma_n^\bullet$ (or $\Pi_n^\bullet$) are expressed by finitely many sentences (or just one - take conjunction). Thus only a finite fragment of $I\Sigma_1$ is needed to prove them. This fact will be used in the next section to show finite axiomatizability of some fragments of arithmetic (including $I\Sigma_1$).

1.78 Definition. We shall close this long section by extending the expressive possibilities of theories containing $I\Sigma_1$ by introducing variables for some definable possibly infinite sets of numbers. Let n be a fixed natural number. We make in $I\Sigma_1$ the following definitions:

(1) c is a (code of a) $\Sigma_n^\bullet$ *set*$^\bullet$ iff c is a $\Sigma_n^\bullet$ formula$^\bullet$ and its only free variable$^\bullet$ is $vr^\bullet(0)$ (the 0-th variable$^\bullet$).
(2) $x \in_{\Sigma,n} c$ iff c is a $\Sigma_n^\bullet$ set$^\bullet$ and $Sat_{\Sigma,n}(c,[x])$ (where $[x]$ is the evaluation assigning x to $vr^\bullet(0)$).
(3) $\Pi_n^\bullet$ sets and $x \in_{\Pi,n} c$ are defined dually.

Note that the formula $x \in_{\Sigma,0} c$ is Δ_1 in $I\Sigma_1$ and, for $n \geq 1$, the formulas $x \in_{\Sigma,n} c$, $x \in_{\Pi,n} c$ are Σ_n and Π_n in $I\Sigma_1$ respectively. Given n we may introduce new variables in $I\Sigma_1$ ranging over $\Sigma_n^\bullet$ sets. If n is clear from the context we may use just $X, Y, \ldots$. The following lemma serves as an example of its usage.

1.79 Lemma ($I\Sigma_1$). For each $\Sigma_1^\bullet$ total function$^\bullet$ F there is a $\Sigma_1^\bullet$ total function$^\bullet$ G such that $G(0) = 0$ and, for each x,$G(x+1) = F(G(x))$.

Proof. Very similar to the proof of 1.54, with the only difference being that now we have *one* proof in $I\Sigma_1$ for all total $\Sigma_1^\bullet$ functions$^\bullet$, not a schema of theorems with infinitely many proofs. □

1.80 Remark. Note that if φ is a Σ_n formula whose only free variable is x_0 (the 0-th variable) then $I\Sigma_1$ proves that $\overline{\varphi}$ is a $\Sigma_n^\bullet$ set and that

$$x \in_{\Sigma,n} \overline{\varphi} \equiv Sat_{\Sigma,n}(\overline{\varphi},[x]) \equiv \varphi(x).$$

(cf. "it's snowing"-it's snowing Lemma 1.76).

1.81 Definitions Continued. Let $n \geq 0$ be fixed. In $I\Sigma_1$ we define a $\Delta_n^\bullet$ *set* to be a pair (c,d) where c is a $\Sigma_n^\bullet$ set, d is a $\Pi_n^\bullet$ set and $(\forall x)(x \in_{\Sigma,n} c \equiv x \in_{\Pi,n} d)$. Observe that the formula saying that x is a $\Delta_n^\bullet$ set is Π_{n+1} in $I\Sigma_1$. We may define $x \in_{\Delta,n} (c,d)$ in the obvious way; again, this formula is Π_{n+1} in $I\Sigma_1$. But observe that $I\Sigma_1$ proves the following:

$$\begin{aligned} &e = (c,d) \,\&\, \Delta_n^\bullet\text{-set}(e) \rightarrow \\ &\qquad\qquad (\forall x)(x \in_{\Delta,n} e \equiv x \in_{\Sigma,n} c \equiv x \in_{\Pi,n} d). \end{aligned}$$

Furthermore, $x \in_{\Sigma,n} c$ is Σ_n and $x \in_{\Pi,n} d$ is Π_n in $I\Sigma_1$.

1.82 Remark. Let us *summarize* what we have done in the present section. We first introduced Robinson's arithmetic Q and proved it to be Σ_1-complete. We further introduced I_{open} and proved in it some high-school laws for numbers: associativity and commutativity of addition and multiplication, distributivity, cancellation, monotonicity, etc. Furthermore, we exhibited the pairing function in I_{open}. Then we showed in $I\Sigma_0$ some properties of divisibility (and left thorough investigation of $I\Sigma_0$ to Chap. V). In $I\Sigma_0(exp)$ we developed a coding of finite sequences and finite sets and proved some basic facts about finite sets and their cardinalities. Then we turned to $I\Sigma_1$; we showed that $I\Sigma_1$-provably recursive functions are closed under primitive recursion and then we developed arithmetization of metamathematics in this theory. We defined terms$^\bullet$ and formulas$^\bullet$ and proved their basic properties. Our final development has been a definition of partial satisfactions; for each n we have the formulas $Sat_{\Sigma,n}$ and $Sat_{\Pi,n}$ with provable Tarski's properties. This enables us to introduce variables for $\Sigma_n^\bullet$ sets, etc. (for any fixed n). This basic apparatus will be used throughout Chaps. I–IV.

2. Fragments of First-Order Arithmetic

Recall that in Sect. 1 we already investigated some fragments of first-order arithmetic, notably $I\Sigma_0(exp)$ and $I\Sigma_1$. Now we are going to investigate systematically fragments obtained by postulating a number-theoretic principle as a scheme for all formulas of a certain class. In subsection (a) we shall deal with fragments based on induction, the least number principle and collection; in subsection (b) we shall study various other principles. Recall also that in Sect. 1 we exhibited satisfaction for Σ_n-formulas (Π_n-formulas) for any fixed n. In subsection (c) we shall use this device to show that most of our fragments are finitely axiomatizable; then we shall generalize and show that under some assumptions we can exhibit in $I\Sigma_1$ a reasonable satisfaction for the relativized arithmetical hierarchy; namely for formulas Σ_n in a set X. In subsection (d) we apply this to particular fragments; this will give us techniques very useful in the following section. Subsection (e) is an appendix presenting an alternative approach to fragments in the logic without function symbols. Results of this section will be used throughout the book.

(a) Induction and Collection

2.1. Here we shall investigate the following four axioms that we met already in Sect. 1:

$(I\varphi)$ $\qquad \varphi(0) \,\&\, (\forall x)(\varphi(x) \rightarrow \varphi(S(x))) \rightarrow (\forall x)\varphi(x)$

$(I'\varphi)$ $\qquad (\forall x)[(\forall y < x)\varphi(y)) \rightarrow \varphi(x)] \rightarrow (\forall x)\varphi(x)$

$(L\varphi)$ $\qquad (\exists x)\varphi(x) \rightarrow (\exists x)(\varphi(x) \,\&\, (\forall y < x)\neg\varphi(y))$

$(B\varphi)$ $\qquad (\forall u)[(\forall x \le u)(\exists y)\varphi(x,y)) \rightarrow (\exists v)(\forall x \le u)(\exists y \le v)\varphi(x,y)]$

They are called the *successor induction axiom* given by φ, the *order induction axiom* by φ, the *least number axiom* given by φ and the *collection axiom* given by φ respectively.

Both the axioms of induction and the least number principle appear to be sufficiently clear. Let us give a verbal formulation of collection: think of

$\varphi(x,y)$ as defining a multi-valued function Φ: $\varphi(x,y)$ says that y is a possible value of Φ for x. Call Φ *total* beneath u if each $x \leq u$ has at least one possible value. Call Φ cofinal on u if for each v there is an $x \leq u$ such that all possible Φ-values of x are bigger than v. B_φ says: if Φ is total beneath u then it is not cofinal on u.

2.2 Some Classes of Formulas. Recall Σ_n and Π_n formulas. If $\varphi(x_0 \ldots x_k)$ is any formula then an *instance* of φ is $\varphi(t_1, \ldots, t_k)$ where t_i are terms, t_i free for x_i in φ. $\Sigma_0(\varphi)$ is the smallest class of formulas that (1) contains all atomic formulas and all instances of φ and (2) is closed under connectives and bounded quantification. $\Sigma_n(\varphi)$ formulas are defined from $\Sigma_0(\varphi)$ formulas in the same manner as Σ_n was defined from Σ_0; thus a $\Sigma_n(\varphi)$ formula consists of a block of n alternating quantifiers, the first being $\exists$, followed by a $\Sigma_0(\varphi)$ formula. $\Sigma_m(\Sigma_n)$ is the union of all $\Sigma_m(\varphi)$, φ being Σ_n. Similarly for $\Pi_m(\Sigma_n)$ etc.

A formula ψ is $\Sigma_n(\varphi)$ *in a theory* T if there is a $\Sigma_n(\varphi)$ formula χ such that $T \vdash \psi \equiv \chi$. A formula ψ is $\Delta_n(\varphi)$ *in* T if it is both $\Sigma_n(\varphi)$ in T and $\Pi_n(\varphi)$ in T.

Observe that for each $\varphi(x_0 \ldots x_k)$ there is a formula $\psi(u)$ with exactly one free variable such that each $\Sigma_0(\varphi)$ formula is $\Sigma_0(\psi)$ in T and vice versa (we assume $T \supseteq I\Sigma_0(exp)$ for simplicity): take $\varphi(\mathrm{u})$ to be

$$(\exists x_0 \leq u) \ldots (\exists x_k \leq u)(u = \langle x_0, \ldots, x_k \rangle \,\&\, \varphi(x_0, \ldots x_k)).$$

2.3 Theories. Recall Q. For some technical reasons (see below) introduce also a theory Q' defined as Q plus the axiom $x < Sx$ (Note $I_{\mathrm{open}} \vdash x \leq Sx$.) We shall study the following theories:

$$\begin{aligned} I\Sigma_n &= Q \cup \{I\varphi \mid \varphi \in \Sigma_n\}, \\ I'\Sigma_n &= Q' \cup \{I'\varphi \mid \varphi \in \Sigma_n\}, \\ L\Sigma_n &= Q' \cup \{L\varphi \mid \varphi \in \Sigma_n\}. \end{aligned}$$

Similarly for $I\Gamma$, $I'\Gamma$, $L\Gamma$, where Γ is Π_n, $\Sigma_0(\Sigma_n)$ etc.
(Caution: $I\Delta_n$ has not any meaning yet, see below!) Further we define

$$B\Gamma = I\Sigma_0 \cup \{B\varphi \mid \varphi \in \Gamma\}$$

for Γ as above, i.e. we have $B\Sigma_n$, $B\Pi_n$ etc. Note that by definition $B\Gamma$ contains $I\Sigma_0$.

$I\Delta_n$ is Q together with the scheme

$$(\forall x)(\sigma(x) \equiv \pi(x)) \rightarrow I\sigma$$

for each pair $\sigma \in \Sigma_n$, $\pi \in \Pi_n$ (thus the axiom says: if σ and π are equivalent then induction holds for σ – and obviously also for Π). Similarly $L\Delta_n$.

In 2.4–2.5 and 2.7 we formulate the principal facts about these theories.

2.4 Theorem. For each n, the following nine theories are mutually equivalent:

$$\begin{array}{lll} I\Sigma_n, & I\Pi_n, & I\Sigma_0(\Sigma_n), \\ I'\Sigma_n, & I'\Pi_n, & I'\Sigma_0(\Sigma_n), \\ L\Sigma_n, & L\Pi_n, & L\Sigma_0(\Sigma_n). \end{array}$$

2.5 Theorem. For each n,

(1) $I\Sigma_{n+1} \Rightarrow B\Sigma_{n+1} \Rightarrow I\Sigma_n$;

(2) $B\Sigma_{n+1} \Leftrightarrow B\Pi_n \Leftrightarrow L\Delta_{n+1} \Rightarrow I\Delta_{n+1}$,

(3) For each Σ_n-formula φ, the formula $(\forall x \leq y)\varphi$ is Σ_n in $B\Sigma_n$.

(Here $\Rightarrow$ means "contains" (i.e. "proves all axioms of") and $\Leftrightarrow$ means "is equivalent to".)

Remark. It is unknown whether $I\Delta_n$ and $L\Delta_n$ are equivalent; all the other arrows will be shown to be strict in Chap. IV (the theories in question are not equivalent).

2.6 Definition. Let $\varphi(x_0, \dots, x_k)$ be a formula. Define in $I\Sigma_1$: q is a *z-piece* of φ if q is a finite mapping, $dom(q) = (< z)^{k+1}$, $range(q) \subseteq \{0, 1\}$ and

$$(\forall x_0 < z) \dots (\forall x_k < z)(q(\langle x_0, \dots x_k \rangle) = 1 \equiv \varphi(x_1 \dots x_k)) .$$

φ is *piecewise coded* in $T \supseteq I\Sigma_1$ if T proves $(\forall z)(\exists q)(q$ is a z-piece of $\varphi)$.

We often write "p.c." for "piecewise coded".

2.7 Theorem. For each $n \geq 1$,

(1) each $\Sigma_0(\Sigma_n)$ formula φ is p.c. in $I\Sigma_n$;

(2) if φ is Δ_{n+1} in $B\Sigma_{n+1}$ then φ is p.c. in $B\Sigma_{n+1}$.

In particular, each Σ_n formula is p.c. in $I\Sigma_n$. Note that by 2.5 (3), formulas Δ_{n+1} in $B\Sigma_{n+1}$ are closed under bounded quantifiers.

This completes our list of facts. In the sequel we shall present a series of lemmas that proves all the above theorems.

2.8 Lemma. (a) For each φ, $L\varphi \equiv I'\neg\varphi$ is provable in predicate logic (trivial). Thus $I'\Sigma_n \Leftrightarrow L\Pi_n$ and $I'\Pi_n \Leftrightarrow L\Sigma_n$.

(b) $I\Sigma_0 \Leftrightarrow L\Sigma_0 \Leftrightarrow I'\Sigma_0$.

Proof. The second equivalence is obvious from (a); for $I\Sigma_0 \Rightarrow L\Sigma_0$ see 1.22. We prove $L\Sigma_0 \rightarrow I\Sigma_0$. Assume $\varphi \in \Sigma_0$ and let us work in $L\Sigma_0$. Assume

$\varphi(0)$, $(\forall x)(\varphi(x) \to \varphi(S(x)))$ and $(\exists x)\neg\varphi(x)$. Then there is an x such that $\neg\varphi(x) \,\&\, (\forall y < x)\varphi(x)$. But $x \neq 0$ since $\varphi(0)$, thus $x = S(y)$ for some y; by Q', $y < x$, thus $\varphi(y)$ and therefore $\varphi(x)$ – a contradiction. □

2.9 Lemma. In $B\Sigma_n$, Σ_n-formulas as well as Π_n-formulas are closed under bounded quantification.

Proof. Evident for $n = 0$. Assume the lemma for n and consider $B\Sigma_{n+1}$ and a Σ_{n+1} formula $(\exists y)\varphi(x, y)$. Then

$$(*) \qquad B\Sigma_{n+1} \vdash (\forall x \leq u)(\exists y)\varphi(x, y) \equiv (\exists v)(\forall x \leq u)(\exists y \leq v)\varphi(x, y)$$

and the formula following $(\exists v)$ on the right hand side of $(*)$ is Π_n in $B\Sigma_n$ by the induction hypothesis. □

2.10 Lemma. $B\Sigma_{n+1} \Leftrightarrow B\Pi_n$.

Proof by contraction of quantifiers, cf. 1.45. □

2.11 Lemma. $I\Sigma_{n+1} \Rightarrow B\Sigma_{n+1}$.

Proof. For $n = 0$ see 1.44–1.45; proceed by induction on n. Assume the lemma for $n - 1$, let $\varphi \in \Pi_n$. In $I\Sigma_{n+1}$ assume $(\forall x \leq u)(\exists y)\varphi(x, y)$. Prove

$$(\forall v \leq u)(\exists t)(\forall x \leq v)(\exists y \leq t)\varphi(x, y)$$

by induction on v; note that, by $B\Sigma_n$, the formula $(\forall x \leq v)(\exists y \leq t)\varphi$ is Π_n in our theory (call it α) and consequently the formula $v \leq u \to (\exists t)\alpha$ is Σ_{n+1} in $I\Sigma_{n+1}$ so that induction can be used. □

2.12 Lemma. (1) $I\Sigma_n \Leftrightarrow I'\Sigma_n$ and similarly for Π_n and $\Sigma_0(\Sigma_n)$. Thus $I\Sigma_n \Leftrightarrow L\Pi_n$ and $I\Pi_n \Leftrightarrow L\Sigma_n$.

(2) $I\Sigma_n \Leftrightarrow I\Pi_n$.

Proof. (1) For $n = 0$ see above. Consider $n > 0$. First work in $I\Sigma_n$. Let $(\forall x)[(\forall y < x)\varphi(y) \to \varphi(x)]$; then we get $(\forall x)(\forall y < x)\varphi(y)$ by induction, observing that $(\forall y < x)\varphi(y)$ is Σ_n in $I\Sigma_n$.

Conversely, work in $I'\Sigma_n$; note that we have $I\Sigma_0$, thus basic properties of $<$, S are provable. Assume $\varphi(0)$ and $(\forall x)(\varphi(x) \to \varphi(S(x))$. We prove $(\forall x)[(\forall y < x)\varphi(y) \to \varphi(x)]$ by cases: If $x = 0$ we have $\varphi(x)$. If $x > 0$ then $x = S(z)$ for some z, thus $(\forall y < x)\varphi(y) \to \varphi(z) \to \varphi(S(z)) \to \varphi(x)$. By order induction we get $(\forall x)\varphi(x)$.

(2) Trivial for $n = 0$. Let $\varphi(x)$ be Π_n and work in $I\Sigma_n$; assume $\varphi(0)$, $(\forall x)(\varphi(x) \to \varphi(x + 1))$ and $\neg\varphi(a)$. Prove the following by induction on z, observing that the formula for which induction is used is Σ_n:

$$(\forall z)(z \leq a \to \neg\varphi(a - z)).$$

(cf. 1.13–1.16; in greater detail we could write $(\forall z)(z \leq a \rightarrow (\exists u \leq a)(z+u = a \,\&\, \neg\varphi(u))$. But then we get $\neg\varphi(a-a)$, thus $\neg\varphi(0)$, a contradiction). $\square$

2.13 Lemma. Let $n \geq 1$. (a) Each Σ_n formula is piecewise coded in $I\Sigma_n$. (b) Each $\Sigma_0(\Sigma_n)$ formula is piecewise coded in $I\Sigma_n$.

Proof. (a) $I\Sigma_n \vdash (\forall z)(\exists q)(q$ z-piece of $\varphi)$. Indeed, q is the least y such that y is a mapping of $(< z)^k$ into $\{0,1\}$ and

$$(\forall x_0 < z), \ldots, (\forall x_k < z)(\varphi(x_0 \ldots x_k) \rightarrow q(<x_0 \ldots x_k>) = 1);$$

q exists by $L\Pi_n$.

This proves (a).

(b) Let φ, $\psi \in \Sigma_n$; then $I\Sigma_n$ proves the following: If φ, ψ have a z-piece then $\varphi \,\&\, \psi$, $\neg\varphi$, $(\exists x \leq y)\varphi$ have a z-piece.

This follows easily by $\Sigma_0^{exp}(exp)$ – comprehension. Assertion (b) follows from the above by induction of the complexity on the $\Sigma_0(\Sigma_n)$ formula in question. $\square$

2.14 Lemma. $I\Sigma_n \Rightarrow I\Sigma_0(\Sigma_n)$.

Proof. Trivial for $n = 0$, thus let $n > 0$, let $\varphi \in \Sigma_0(\Sigma_n)$ and work in $I\Sigma_n$: we show $L\varphi$. Assume $\varphi(a)$ and let q be a z-piece of φ (with respect to the variable in question), $z > a$. (Use 2.13.) By $I\Sigma_1$, let i be the least number such that $(q)_i = 1$; then obviously $(q)_i$ is the least element x such that $\varphi(x)$. We have proved $L\Sigma_0(\Sigma_n)$; the proof of $I\Sigma_0(\Sigma_n)$ from $L\Sigma_0(\Sigma_n)$ is the same as the proof of 2.8 (b). $\square$

2.15 Lemma. $B\Sigma_{n+1} \Rightarrow I\Sigma_n$.

Proof. Trivial for $n = 0$; thus assume $n > 0$ and work in $B\Sigma_{n+1}$. Note that we may assume $I\Sigma_{n-1}$ (induction on n). Let $\varphi(x)$ be Σ_n, $\varphi(x) \equiv (\exists z)\psi(x,z)$. In $B\Sigma_{n+1}$ assume $\varphi(0)$, $(\forall x)(\varphi(x) \rightarrow \varphi(x+1))$. Let a be given; we prove $(\forall x \leq a)\varphi(x)$. We have the following:

$$\begin{gathered}
(\forall x)(\varphi(x) \rightarrow \varphi(x+1)) \rightarrow \\
(\forall x \leq a)[(\exists z)\psi(x,z) \rightarrow (\exists w)\psi(x+1,w)] \rightarrow \\
(\forall x \leq a)(\exists w)(\forall z)(\psi(x,z) \rightarrow \psi(x+1,w)) \rightarrow \\
(\exists v)(\forall x \leq a)(\exists w \leq v)(\forall z)(\psi(x,z) \rightarrow \psi(x+1,w)).
\end{gathered}$$

Fix such a v; we may also assume $(\exists w \leq v)\varphi(0,w)$. Then prove $(\forall x \leq a)(\exists w \leq v)\psi(x,w)$ by induction on x using $I\Sigma_{n-1}$. $\square$

2.16 Lemma. $B\Sigma_{n+1} \Rightarrow L\Delta_{n+1}$.

Proof. Work in $B\Sigma_{n+1}$. Assume $(\forall x)[(\exists y)\varphi(x,y) \equiv \neg(\exists z)\psi(x,z)]$, where φ, ψ are Π_n; furthermore, assume $(\exists y)\varphi(a,y)$. We have

$$(\forall x)(\exists y)(\varphi(x,y) \vee \psi(x,y)), \text{ hence for some } w\,,$$
$$(\forall x \leq a)(\exists y \leq w)(\varphi(x,y) \vee \psi(x,y))(\text{by } B\Sigma_{n+1}), \text{ thus}$$
$$(\forall x \leq a)((\exists y)\varphi(x,y) \to (\exists y \leq w)\varphi(x,y)).$$

Then we have $(\exists y \leq w)\varphi(a,y)$ and we may use $I\Sigma_n$ (preceding lemma), thus $L\Pi_n$ (2.11). Thus there is a least $a' \leq a$ such that $(\exists y \leq w)\varphi(a',y)$; but then a' is the least number such that $(\exists y)\varphi(a',y)$. This completes the proof. □

2.17 Lemma. $L\Delta_{n+1} \Rightarrow B\Sigma_{n+1}$.

Proof. By induction on n. Work in $L\Delta_{n+1}$, let $(\forall x \leq a)(\exists y)\theta(x,y)$, θ being Π_n. Put $\varphi(x) \equiv x \leq a \,\&\, (\exists v)[\theta(x,v) \,\&\, (\forall u < v)\neg\theta(x,u) \,\&\, (\forall z$ between $x,a)(\exists y \leq v)\theta(z,y)]$; thus $\varphi(x)$ means that the least witness for x majorizes the least witness for all z such that $x \leq z \leq a$. Observe that φ is Σ_{n+1}; for $n = 0$ this is evident, and for $n > 0$ it follows by $B\Sigma_n$. But $\varphi(x)$ is equivalent to the following formula $\psi(x)$: $\psi(x) \equiv x \leq a \,\&\, (\forall v)[\theta(x,v) \to (\forall z$ between $x,a)(\exists y \leq v)\theta(z,y)]$, thus: *each* witness for x majorizes the witnesses in question. Now $\psi(x)$ is Π_{n+1} (for analogous reasons) and therefore $L\Delta_{n+1}$ applies: let x_0 be the least element satisfying φ and $\theta(x_0,y_0)$.

Claim. $(\forall x \leq a)(\exists y \leq y_0)\theta(x,y)$. Indeed, the statement holds for x between x_0 and a by definition; if there is an $x < x_0$ such that $(\forall y \leq y_0)\neg\theta(x,y)$ then take the largest such x possible $-x$ is the least element such that

$$x < x_0 \,\&\, (\forall x' < x_0)(x < x' \to (\exists y < y_0)\theta(x,y))\,,$$

which is Δ_{n+1}. But then we have $\varphi(x') \,\&\, x' < x$ – a contradiction. □

2.18 Remark. (1) The proof of $L\Delta_{n+1} \Rightarrow I\Delta_{n+1}$ is easy and left to the reader (cf. 2.8).

(2) The reader may check that Theorem 2.4 follows from 2.8, 2.12 and 2.14; furthermore, Theorem 2.5 follows from 2.9, 2.10, 2.11, 2.15, 2.16, 2.17 and 2.18 (1). In addition, Theorem 2.7 (1) is proved in 2.13. Thus it remains to prove 2.7 (2); this is done in the following lemma.

2.19 Lemma. If $n \geq 1$ and φ is Δ_{n+1} in $B\Sigma_{n+1}$ then φ is piecewise coded in $B\Sigma_{n+1}$.

Proof. This is proved similarly to 2.13 (a): given z, the desired z-piece of $\varphi(x)$ is the least q such that q is a finite mapping, $dom(q) = (< z)^k$, $range(q) \subseteq \{0,1\}$ and $(\forall x_0 < z)\ldots(\forall x_k < z)(\varphi(x_0 \ldots x_k) \to q(\langle x_0 \ldots x_k\rangle) = 1)$. The condition in question is easily shown to be Δ_{n+1} in $B\Sigma_{n+1}$, thus $L\Delta_{n+1}$ applies. This completes the proofs of our theorems. □

(b) Further Principles and Facts About Fragments

2.20 Principles – *continued.* Let us introduce three new principles:
Strong collection $S\varphi$:

$$(\forall u)(\exists v)(\forall x \leq u)[(\exists y)\varphi(x,y) \rightarrow (\exists y \leq v)\varphi(x,y)]$$

Regularity $R\varphi$:

$$(Cx)(\exists y \leq u)\varphi(x,y) \rightarrow (\exists y \leq u)(Cx)\varphi(x,y)$$

where (Cx) is $(\forall w)(\exists x > w)$ – the quantifier "there are unboundedly many"

Pigeon hole principle $PHP(\varphi)$:

$$(\forall u)\neg[(\forall x \leq u)(\exists! y \leq u+1)\varphi(x,y) \,\&\, (\forall y \leq u+1)(\exists! x \leq u)\varphi(x,y)]$$

We offer the reader the following verbal reformulations: $S\varphi$ may be understood as saying that the partial multivalued function on $(< u)$ defined by φ is not cofinal on its domain. $R\varphi$ says that if unboundedly many x's have a value beneath u then there is a $y < u$ which is a value of unboundedly many x's. $PHP(\varphi)$ just says that φ cannot define a one-one mapping of $(< u)$ onto $(< u+1)$.

2.21 Principles – *completed.* We shall introduce three more principles, all asserting the existence of some sequences. Since we defined sequences in $I\Sigma_0(exp)$ we are obliged to relate these principles to theories containing $I\Sigma_0(exp)$; our choice will be $I\Sigma_1$.

The first principle is called the *finite axiom of choice* ($FAC(\varphi)$) and claims that if a multivalued function is total beneath u then there is a sequence s which selects for each $x < u$ one of the values of x (i.e. $(s)_x$ is the selected value).

$$\begin{aligned}(\forall x \leq u)(\exists y)\varphi(x,y) \rightarrow (\exists s)(&Seq(s) \,\&\, lh(s) = u+1\\ &\&\, (\forall x \leq u)\varphi(x,(s)_x)\,.\end{aligned}$$

The last two principles concern approximations of functions. Let us begin with informal formulations; we shall show how to obtain the corresponding formulas. Say that φ defines a partial function if $(\forall x,y,z)(\varphi(x,y) \,\&\, \varphi(x,z) \rightarrow y = z)$ (abbreviate this $PFUN(\varphi)$); say that φ defines a total function if $(\forall x)(\exists! y)\varphi(x,y)$ (abbreviate this $TFUN(\varphi)$). Write $y = F(x)$ for $\varphi(x,y)$ for a moment. Call a finite sequence s an *approximation* of F if for each i such that $i+1 < lh(s)$ and each $x \leq (s)_i$, $y = F(x)$ implies $y \leq (s)_{i+1}$. The principle of approximation for a *total* function says that if φ defines a total function then this function has arbitrarily long approximations; similarly for *partial* functions. Write $Approx_\varphi(s)$ for

$$Seq(s) \,\&\, (\forall i)(\forall x)(i+1 < lh(s) \,\&\, x \leq (s)_i \,\&\, \varphi(x,y). \rightarrow y \leq (s)_{i+1})\,.$$

The principles are as follows:

$$(P_\varphi) \quad PFUN(\varphi) \to (\forall z)(\exists s)Approx_\varphi(s) \,\&\, lh(s) = z),$$
$$(T_\varphi) \quad TFUN(\varphi) \to (\forall z)(\exists s)Approx_\varphi(s) \,\&\, lh(s) = z).$$

Note that both (P_φ) and (T_φ) are meaningful in $I\Sigma_1$ (even in $I\Sigma_0(exp)$; *Seq* is used). This completes our list of principles; obviously, for each φ all the above principles are true in N.

2.22 Theories. (1) Theories based on S, R and PHP are assumed to contain $I\Sigma_0$:

$$S\Gamma = I\Sigma_0 \cup \{S\varphi \mid \varphi \in \Gamma\},$$
$$R\Gamma = I\Sigma_0 \cup \{R\varphi \mid \varphi \in \Gamma\},$$
$$PHP(\Gamma) = I\Sigma_0 \cup \{PHP(\varphi) \mid \varphi \in \Gamma\}.$$

Here Γ stands for Σ_n, Π_n and possibly $\Sigma_0(\Sigma_n)$.

(2) Theories based on FAC, T, P are assumed to contain $I\Sigma_1$:

$$FAC(\Gamma) = I\Sigma_1 \cup \{FAC(\varphi) \mid \varphi \in \Gamma\}$$
$$T(\Gamma) = I\Sigma_1 \cup \{T\varphi \mid \varphi \in \Gamma\}$$
$$P(\Gamma) = I\Sigma_1 \cup \{P\varphi \mid \varphi \in \Gamma\}.$$

Thus we may use the notion of finite sequences. Note that in Chap. V a theory of finite sequences in $I\Sigma_0$ will be elaborated; having this we could discuss also the principles FAC, T, P over $I\Sigma_0$. But we shall not investigate this now. Our results are contained in the following three theorems:

2.23 Theorem. For each natural n:
(1) $S\Sigma_{n+1} \Leftrightarrow S\Pi_n \Leftrightarrow I\Sigma_{n+1}$
(2) $PHP(\Sigma_0(\Sigma_n)) \Leftrightarrow I\Sigma_{n+1}$
(3) for $n \geq 1$, $PHP(\Sigma_{n+1}) \Leftrightarrow B\Sigma_{n+1}$; furthermore, $PHP(\Sigma_1) \Rightarrow B\Sigma_1$.
(4) $R\Sigma_{n+1} \Leftrightarrow R\Pi_n \Leftrightarrow B\Pi_{n+1} \Leftrightarrow B\Sigma_{n+2}$.

2.24 Theorem.
(1) For $n \geq 1$, $B\Sigma_{n+1} \Leftrightarrow FAC(\Sigma_{n+1})$; and $I\Sigma_1 \Leftrightarrow FAC(\Sigma_1)$.
(2) For $n \geq 1$, $T\Sigma_{n+1} \Rightarrow P\Sigma_{n+1} \Rightarrow T\Sigma_n$.
(3) For $n \geq 0$, $I\Sigma_{n+1} \Leftrightarrow T\Sigma_{n+1} \Leftrightarrow T\Pi_n$, and $P\Sigma_{n+1} \Leftrightarrow P\Pi_n$.

2.25 Theorem. Each $\Sigma_0(\Sigma_n)$ formula is Δ_{n+1} in $I\Sigma_n$.

2.26 Remark. The structure of our fragments is visualized in Fig. 1. We shall show in Chap. IV that all inclusions are strict and that theories incomparable in the figure are incomparable as theories, i.e. neither includes the other.

$$
\begin{tikzcd}
 & {} \arrow[dr] & \vdots & {} \arrow[dl] & \\
 & & I\Sigma_3 \arrow[dl] \arrow[dr] & & \\
 & P\Sigma_2 \arrow[dr] & & B\Sigma_3 \arrow[dl] & \\
 & & I\Sigma_2 \arrow[dl] \arrow[dr] & & \\
P\Sigma_0 \arrow[r, phantom, "\equiv"] & P\Sigma_1 \arrow[dr] & & B\Sigma_2 \arrow[dl] & \\
 & & I\Sigma_1 \arrow[d] & & \\
 & & B\Sigma_1 \arrow[rr, phantom, "\equiv"] \arrow[d] & & B\Sigma_0 \\
 & & I\Sigma_0 & &
\end{tikzcd}
$$

Fig. 1.

The subsequent series of lemmas proves our three theorems.

Overview. 2.23 (1) proved in 2.27–2.29, (2–3) in 2.30–2.33, (4) in 2.36–2.44 and uses 2.24 (1); 2.24 (1) proved in 2.35, (2–3) in 2.45–2.48 and uses 2.37; 2.25 is proved in 2.49–2.50 and uses 2.23 (1).

2.27 Lemma. $I\Sigma_{n+1} \Rightarrow S\Pi_n$.

Proof. Let φ be Π_n and work in $I\Sigma_{n+1}$. Let u be given; let q be the $(u+1)$-piece of $(\exists y)\varphi(x,y)$ (cf. 2.13). We prove $(\exists v)(\forall x \leq a)((q)_x = 1 \rightarrow (\exists y \leq v)\varphi(x,y))$. This is achieved easily by proving the following sentence by induction on z:

$$(*) \qquad z \leq u \rightarrow (\exists v)(\forall x \leq z)((q)_x = 1 \rightarrow (\exists y \leq v)\varphi(x,y)).$$

This is clear for $z = 0$. Let v satisfy $(*)$ w.r.t. z and let $z+1 \leq u$; if $\neg(\exists y)\varphi(z+1,y)$ then v satisfies $(*)$ for $u+1$; if $\varphi(z+1,y)$, then $(*)$ holds for $z+1$ and $\max(v,y)$ instead of z,v. This completes the proof. $\square$

2.28 Lemma. $S\Pi_n \Rightarrow S\Sigma_{n+1}$.

Proof. Contracting quantifiers (cf. 2.10). □

2.29 Lemma. $S\Pi_n \Rightarrow I\Sigma_{n+1}$.

Proof. By induction on n. Recall that $S\Pi_n$ contains $I\Sigma_0$. Let φ be Π_n. Work in $S\Pi_n$; assume $(\exists y)\varphi(0,y)$ and $(\forall x)((\exists y)\varphi(x,y) \rightarrow (\exists y)\varphi(x+1,y)$. Take any u and use $S\Pi_n$ to get a v such that $(\forall x \leq u)((\exists y)\varphi(x,y) \rightarrow (\exists y \leq v)\varphi(x,y))$. Then use $I\Sigma_n$ to prove $(\forall x \leq u)(\exists y \leq v)\varphi(x,y)$. □

2.30 Lemma. $I\Sigma_{n+1} \Leftrightarrow PHP(\Sigma_0(\Sigma_{n+1}))$.

Proof. ($\Rightarrow$) follows by Lemma 2.13 (b): if φ defines a mapping of $u+1$ into u then its $(u+1)$-piece is a finite set function and using comprehension we obtain the mapping in question as a finite set. But $I\Sigma_1$ proves the pigeon hole principle for finite sets, see 1.41.

Conversely, assume $PHP(\Sigma_0(\Sigma_{n+1}))$ and let φ be a Σ_{n+1}-formula violating $I\Sigma_{n+1}$: let a be such that

$$\varphi(0) \,\&\, (\forall x)(\varphi(x) \rightarrow \varphi(x+1) \,\&\, \neg\varphi(a).$$

Define, for $x \leq a$, $f(x) = x - 1$ if $\neg\varphi(x)$ and $f(x) = x$ otherwise. Then f is $\Sigma_0(\Sigma_{n+1})$-definable and violates $PHP(\Sigma_0(\Sigma_{n+1}))$. □

2.31 Lemma. $PHP(\Sigma_{n+1}) \Rightarrow B\Sigma_{n+1}$.

Proof. We shall construct the proofs by induction on n; this allows us to assume $B\Sigma_n$ if $n > 0$. Let n be given and work in $PHP(\Sigma_{n+1})$.

(1) First prove $I\Sigma_n$. This is immediate if $n = 0$ (since $PHP(\Sigma_{n+1})$ extends $I\Sigma_0$). If $n > 0$ imitate the proof of 2.30 ($\Leftarrow$), φ being now Σ_n; by $B\Sigma_n$, the function f is now Σ_{n+1} definable and $PHP(\Sigma_{n+1})$ gives the result.

(2) Now assume that $B\varphi$ is violated for a $\varphi \in \Pi_n$; we want to deduce a contradiction, which will complete the proof. Put $\varphi'(x,y) \equiv (\exists z \leq y)\varphi(x,z) \,\&\, y = (x,z)$; then $B\varphi'$ fails and $x_1 < x_2 \leq u \,\&\, \varphi(x_1, y_2)$ implies $y_1 = y_2$. Thus $(\forall x \leq u)(\exists y)\varphi'(x,y)$ but $(\forall v)(\exists x \leq v)(\forall y \leq v)\neg\varphi'(x,y)$. By $I\Sigma_n$, for each $x \leq u$ there is a least y such that $\varphi'(x,y)$; denote it by $m(x)$. Clearly, m is one-one on $(\leq u)$. For $x, x' \leq u$ put $x' = F(x)$ if $m(x) < m(x')$ and $\neg(\exists x'' < u)(m(x) < m(x'') < m(x'))$.

(3) We show that F is Σ_{n+1}. Indeed, since m is $\Sigma_0(\Sigma_n)$ and we have $I\Sigma_n$, m is piecewise coded; thus for each z, $\{\langle x,y\rangle \mid x \leq u \,\&\, y \leq z \,\&\, y = m(x)\}$ is a finite set. (Say that the set codes m on $(\leq u) \times (\leq z)$.) Thus $x' = F(x)$ is equivalent to $(\exists q)(q$ codes m on $(\leq u) \times (\leq z) \,\&\, (\exists y, y' \leq z)[q(x) = y \,\&\, q(x') = y' \,\&\, \neg(\exists x' \leq u)(\exists y'' \leq z)(q(x'') = y'' \,\&\, y < y'' < y')]$.

The formula "q codes m on $(\leq u) \times z$" is Δ_{n+1}, the second conjunct is Δ_1; thus the whole is Σ_{n+1}.

(4) F is total on $(\leq u)$ and there is an $x_0 \leq u$ such that F maps $(\leq u)$ onto $(\leq u) - \{x_0\}$. Indeed, there is the least y such that $(\exists x \leq u)\varphi'(x, y)$ (by $I\Sigma_n$; the formula is Π_n in $I\Sigma_n$). If $\varphi(x_0, y)$ then $y = m(x_0)$ and $y \notin \mathit{range}(F)$. For each $x' \leq u$ different from x_0 there is an $x \leq u$ such that $x' = F(x)$: to see this assume $x' \neq x_0$, $y = m(x')$ and let q code m on $(\leq u) \times (\leq y)$. The desired x is easily obtained from q using $I\Sigma_1$.

(5) F is one-one: trivial from the definition. Thus F maps $(\leq u)$ one-one onto $(\leq u) - \{x_0\}$ and F is Σ_{n+1}. Changing F inessentially we may assume $x_0 = u$, thus $\mathit{range}(F) = (\leq u - 1)$ and we have a contradiction with $PHP(\Sigma_{n+1})$. □

2.32 Lemma. $(B\Sigma_{n+1} + PHP(\Sigma_n)) \Rightarrow PHP(\Sigma_{n+1})$.

Proof. If $\theta(x, y) \equiv (\exists z)\psi(x, y, z)$ is Σ_{n+1} and defines in $B\Sigma_{n+1}$ a 1-1-mapping of $(\leq a)$ to $(\leq a - 1)$ then find a t such that the formula $(\exists z < t)\psi(x, y, z)$ (which is Π_n in $B\Sigma_{n+1}$) defines the same mapping. □

2.33 Lemma. For $n \geq 1$, $B\Sigma_{n+1} \Rightarrow PHP(\Sigma_{n+1})$

Proof. In the theory in question, we have $I\Sigma_n$, which implies $PHP(\Pi_n)$ by 2.30, and 2.32 gives the result. □

2.34 Remark. Note that 2.23 (1)–(3) has been proved. Before we prove 2.23 (4) let us discuss FAC.

2.35 Lemma. $I\Sigma_1 + B\Pi_m \Leftrightarrow FAC(\Pi_m)$.

Remark. If $m = 0$ then $I\Sigma_1 + B\Pi_m$ is $I\Sigma_1$; if $m > 0$ it is $B\Sigma_m$.

Proof. ($\Rightarrow$) In $I\Sigma_1 + B\Pi_m$ assume $(\forall x \leq u)(\exists y)\varphi(x, y)$, $\varphi \in \Pi_m$; thus for some v we have $(\forall x \leq u)(\exists y \leq v)\varphi(x, y)$. Prove the following formula by induction on z:

$$(\forall z \leq u)(\exists s \leq 2^{(u+v+1)^2})(lh(s) = x + 1 \,\&\, (\forall i \leq x)\varphi(i, (s)_i))$$

(cf. the remark in 1.43). Observe that the formula in question is Δ_1 for $m = 0$ and is Δ_m for $m > 0$; thus the corresponding induction axiom is at our disposal.

$\Leftarrow$ is evident. □

Remark. Observe that $FAC(\Pi_m) \Rightarrow FAC(\Sigma_{m+1})$ (cf. 2.10); thus 1.24 (1) is proved.

2.36 Definition. Given a formula φ, the following formula (that can be denoted $MFUNS(\varphi)$) says that φ defines a monotone function on an initial segment:

$$(\forall x, y_1, y_2)(\varphi(x, y_1) \,\&\, \varphi(x_1, y_2) \to y_1 = y_2)$$
$$(\forall x_1, y_1, x_2, y_2)(x_1 < x_2 \,\&\, \varphi(x_1, y_1) \,\&\, \varphi(x_2, y_2) \to y_1 < y_2)$$
$$(\forall x_1, x_2, y_2)(x_1 < x_2 \,\&\, \varphi(x_2, y_2) \to (\exists y_1)\varphi(x_1, y_1)).$$

2.37 Lemma. For each formula $\theta(x, y) \in \Pi_m$ there is a $\psi_o \in \Pi_m$ such that $(I\Sigma_1 + B\Pi_m)$ proves the following:

(a) $(\forall x < a)(\exists y)\theta \equiv (\forall x < a)(\exists y)\psi_0$.

(b) ψ_0 defines an increasing function on an initial segment. (Note once more that if $m = 0$ then the theory in question is $I\Sigma_1$; if $m > 0$ then it is $B\Pi_m$.)

Proof. For $m = 0$, ψ_0 says: y is the function associating with each $x_0 \leq x$ the least y_0 such that $\theta(x_0, y_0)$. For $m > 0$ let $\theta(x_0, y_0)$ be $(\forall z)\lambda(x_0, y_0, z)$.

We make the following definitions. A *superwitness* for x is a pair (y, s) where $\theta(x, y)$ (i.e. y witnesses $(\exists y)\varphi(x, y)$ and s is a sequence of length y such that for each $z < y$, $(s)_z$ is the smallest u such that $\neg\lambda(x, z, u)$ (this sequence witnesses for each $z < y$ that $\neg\theta(x, z)$ holds; altogether, (y, s) witnesses that y is the least element satisfying $\theta(x, y)$). Write $SW(x, (y, s))$ for "y is the superwitness for x" and observe $SW(x, (y, s)) \in \Pi_m$. Now define $SSW(x, q)$ (q is a super-superwitness for x) if q is a sequence of length $x + 1$ such that for each $z \leq x$, $(q)_z$ is the superwitness for z. Observe that $B\Pi_m$ proves the following

(1) $SW(x, t) \,\&\, SW(x, t') \to t = t'$;
(2) $SSW(x, t) \,\&\, SSW(x, t') \to t = t'$;
(3) $x < x' \,\&\, SSW(x', t') \to (SSW(x, t) \equiv t$ is the restriction of t' to $(\leq x))$;
(4) $(\forall x \leq a)(\exists y)\theta(x, y) \equiv (\exists t)SSW(a, t)$.

To prove (4), observe that $\Leftarrow$ is trivial; let us prove $\Rightarrow$. Assume $(\forall x \leq a)(\exists y)\theta(x, y)$; then $(\forall x \leq a)(\exists w)SW(x, w)$, since (i) by $L\Pi_m$, there exists the least y such that $\theta(x, y)$, (ii) again by $L\Pi_m$, for each $z < y$ exists the least u such that $\neg\lambda(x, z, u)$ and by $FAC(\Pi_m)$, there is a sequence s associating with each $z < y$ this least u. Applying $FAC(\Pi_m)$ to $(\forall x \leq a)(\exists w)SW(x, w)$ we gain directly the sequence which is the desired super-superwitness. The lemma now follows easily. □

2.38 Definition $(I\Sigma_1)$. If $\psi_0(x, y)$ defines an increasing function F on an initial segment then call a sequence s a *code of the primitive recursive iteration of* F if $(s)_0 = 0$ and for each x such that $x + 1 < lh(s)$ we have $(s)_{x+1} = F((s)_x)$. (In symbols: $CPRI_{\psi_0}(s)$.)

2.39 Lemma. Let ψ_0 be Π_m; $(I\Sigma_1 + B\Pi_m)$ proves the following: If ψ_0 defines an increasing function F on an initial segment then

(a) $(\forall x < a)(\exists y)\psi_0 \rightarrow (\exists t > a)\, CPRI_{\psi_0}(t)$

(b) Let $K(a)$ be the constant sequence of length a whose each member is a. Then

$$(\exists t > K(a))\, CPRI_{\psi_0}(t) \rightarrow (\forall x < a)(\exists y)\psi_0 \, .$$

Proof. (a) Note that $CPRI_{\psi_0}(t)$ is Π_m and we have $L\Pi_m(L\Pi_1$ for $m = 0.)$ Let s be the maximal code of the primitive recursive iteration of F such that $s \leq a$; let $u = lh(s) - 1$ and $v = (s)_u$. Clearly, $v < a$ and if w is such that $\psi_0(v, w)$ then let t be the concatenation of a with the element w, i.e. $t = s \frown \langle w \rangle$. Then $t > s$, thus $t > a$.

(b) Assume $\neg(\forall x < a)(\exists y)\psi_0$. Then evidently each primitive recursive iteration t of F is less than $K(a)$. □

2.40 Lemma. Let ψ_0 be Π_m; $(I\Sigma_1 + B\Pi_m)$ proves the following: if ψ_0 defines an increasing function on an initial segment then

$$(\forall x)(\exists y)\psi_0 \equiv (Ct)\, CPRI_{\psi_0}(t) \, .$$

Immediate from the preceding.

2.41 Lemma. For each $\theta(x, y) \in \Pi_m$ there is a $\psi(t) \in \Pi_m$ such that $(I\Sigma_1 + B\Pi_m) \vdash (\forall x)(\exists y)\theta \equiv (Ct)\psi$.

Immediate from the preceding.

2.42 Lemma. $B\Sigma_{m+2} \Rightarrow R\Sigma_{m+1}$

Proof. Assume $\neg(\exists y < a)(Cx)\theta(\theta \in \Sigma_{m+1})$. Using $B\Pi_{m+1}$ show $(\exists t)(\forall y < a)(\forall x > t)\neg\theta$, i.e. $\neg(Cx)(\exists y < a)\theta$. □

2.43 Lemma. $R\Pi_0 \Rightarrow I\Sigma_1$.

Proof. Recall that by definition, $R\Pi_0$ contains $I\Sigma_0$. In $R\Pi_0$, assume $(\exists z)\varphi(a, z)$ where $\varphi \in \Sigma_0$. Trivially,

$$(\forall x \leq a)(\exists w)(\forall u > w)[(\exists z < u)\varphi(x, z) \equiv (\exists z < u + 1)\varphi(x, z)] \, .$$

Applying $R\Pi_0$ we get

$$\neg(Cu)(\exists x < a)[(\exists z < u + 1)\varphi(x, z) \,\&\, \neg(\exists z < u)\varphi(x, z)]$$

thus

$$(\exists t)(\forall u \geq t)(\forall x < z)[(\exists z < u)\varphi(x, z) \equiv (\exists z < u + 1)\psi(x, z)] \, .$$

Hence

$$(\forall x \leq a)[(\exists z)\varphi(x,z) \equiv (\exists z < t)\psi(x,z)].$$

Thus $I\Sigma_0$ gives the desired minimum. □

2.44 Lemma. $R\Pi_m \Rightarrow B\Pi_{m+1}$

Proof by induction on m; thus we may assume $B\Pi_m$. (For $m = 0$ this follows from 2.43.) Let $\theta(x,y,z)$ be Σ_m and consider $(\forall z)\theta(x,y,z)$. Work in $(R\Pi_m + B\Pi_m)$; assume

$$(\forall x < a)(\exists y)(\forall z)\theta(x,y,z).$$

By 2.37, let $\psi_0(x,y,z) \in \Pi_m$ be such that ψ_0 defines an increasing function on an initial segment and

$$(\forall q)(\forall y < q)(\exists z)\neg\theta(x,y,z) \equiv (\forall y < q)(\exists z)\psi_0(x,y,z). \qquad (*)$$

Then we have the following:

$(\forall x < a)(\exists y)(\forall z)\theta(x,y,z) \rightarrow$ by (*))
$(\forall x < a)\neg(\forall y)(\exists z)\psi_0(x,y,z) \rightarrow$ (by 2.40)
$(\forall x < a)\neg(Ct)CPRI_{\psi_0}(x,t) \rightarrow$ (by $R\Pi_m$)
$\neg(Ct)(\exists x < a)CPRI_{\psi_0}(x,t) \rightarrow$ (definition of C)
$(\exists q)(\forall t > q)(\forall x < a)\neg CPRI_{\psi_0}(x,t) \rightarrow$ (logic)
$(\exists q)(\forall x < a)(\forall t > q)\neg CPRI_{\psi_0}(x,t) \rightarrow$ (cf. 2.39)
$(\exists q)(\forall x < a)(\exists y < q)(\forall z)\neg\psi_0(x,y,z) \rightarrow$ (by (*))
$(\exists q)(\forall x < a)(\exists y < q)(\forall z)\theta(x,y,z)$.

This completes the proof of $B\Pi_{m+1}$. □

Remark. Note that the proof of 2.23 (4) is complete. We turn to 2.24 (2)–(3).

2.45 Lemma. $I\Sigma_{n+1} \Rightarrow T\Sigma_{n+1}$

Proof. Let φ be Σ_{n+1} and work in $I\Sigma_{n+1} + TFUN(\varphi)$, i.e. assume that φ defines a total function F. Then φ is Δ_{n+1} in our theory. Define

$$G(x) = (\min y > x)(\forall u \leq x)(F(u) \leq y).$$

G is total, monotone and Δ_{n+1}; show by the usual technique that its primitive recursive iteration $H(0) = 0$, $H(x+1) = G(H(x))$ is total and Δ_{n+1}. Moreover, H is piecewise coded; from this it is easy to conclude that for each x, the restriction of H to $(\leq x)$ is a finite set h; but h is an approximation of F of length $x+1$. □

2.46 Lemma. $T\Sigma_{n+1} \Rightarrow I\Sigma_{n+1}$.

Proof. Trivial for $n = 0$ by our definition of $T\Sigma_1$; thus assume $n > 0$ and work in $T\Sigma_{n+1} + I\Sigma_n$. First prove $B\Pi_n$. Let ψ be Π_n and assume $(\forall x \leq u)(\exists y)\psi(x, y)$. Define $F(x) = (\min y)\psi(x, y)$ for $x \leq u$, $F(x) = 0$ otherwise; F is Δ_{n+1} in our theory. Let s be an approximation of F, $lh(s) > u + 1$. Then $(s)_u \geq u$, thus $(\forall x \leq u)(\exists y \leq (s)_{u+1})\varphi(x, y)$. $B\Pi_n$ follows.

To prove $I\Sigma_{n+1}$ take $\varphi \in \Sigma_{n+1}$, $\varphi(x) \equiv (\exists y)\chi(x, y)$ and assume $\varphi(0)$ and $(\forall x)(\varphi(x) \rightarrow \varphi(x + 1))$. For each x, let $G(x) = y$ if y is a sequence of length $(x + 1)$ and for each $i \leq x$, $(y)_i$ is the least z such that $\chi(x, z)$. G is a function (possibly partial) and is Δ_{n+1} in our theory. If G is bounded, i.e. $y = G(x)$ implies $y \leq w$, then we get $(\forall x)(\exists y \leq w)(y = G(x))$ by $I\Delta_{n+1}$, which is at our disposal (thanks to $B\Sigma_{n+1}$); thus assume G unbounded. Thus $(\forall v)(\exists x, y)(y = G(x) \,\&\, (x, y) > v)$. Define $H(v)$ to be the least pair (x, y) such that $y = G(x)$; then H is Δ_{n+1} in our theory and H is total. Let s be an approximation of H of length $z + 1$; then s is a sequence of increasing pairs (x, y) such that $y = G(x)$. Thus if $(x, y) = (s)_z$ then $x \geq z$, $y = G(x)$ and therefore y gives witnesses for each $i \leq x$; thus $(\forall i \leq x)(\exists y)\chi(i, y)$ and $\varphi(x)$ follows. □

2.47 Lemma. $T(\Pi_n) \Leftrightarrow T(\Sigma_{n+1})$ and $P(\Pi_n) \Leftrightarrow P(\Sigma_{n+1})$.

Proof. Assume $T(\Pi_n)$; note that we may also assume $I\Sigma_n$ (for $n = 0$ by definition, for $n > 0$ as the induction hypothesis on n). Let $(\exists z)\theta(x, y, z)$ be Σ_{n+1} and assume that this formua defines a total function F. Define $G(x) = (y, q)$ as: q is a superwitness (for $n = 0$: a witness) of $y = F(x)$ (cf. 2.37), i.e., for some z, s, $q = (z, s)$, we have $\theta(x, y, z)$ and s is a sequence witnessing minimality of z. Then $G(x)$ is Π_n, total and majorizes F; each approximation of G is an approximation of F. Thus $T(\Pi_n)$ gives $T(\Sigma_{n+1})$.

Now assume $P(\Pi_n)$; then $T(\Pi_n)$, thus $T(\Sigma_{n+1})$. Let F be Σ_{n+1} and partial; as above show that there is a Π_n function G with the same domain majorizing F. Each approximation of G is an approximation of F. □

2.48 Lemma. For $n \geq 1$, $I\Sigma_{n+1} \Rightarrow P\Sigma_n \Rightarrow I\Sigma_n$.

Proof. By 2.47, $P(\Sigma_n) \Leftrightarrow P(\Pi_{n-1})$; so assume $T\Sigma_{n+1}$ and let φ be Π_{n-1} and define a partial function G. Then the trivial totalization of G ($H(x) = G(x)$ if defined, $= 0$ otherwise) is Δ_{n+1}, and thus has approximations of arbitrary length; each of them is an approximation of G.

The second statement is trivial since $P\Sigma_n \Rightarrow T\Sigma_n$. This completes the proof of 2.24 (2)–(3). □

Our last task in this subsection is to prove Theorem 2.25. This is dome in the following two lemmas.

2.49 Lemma. For each $\Sigma_0(\varphi)$-formula Ψ there is a formula Ψ' of the form

$$(*) \qquad (Q_1 y_1 \leq z_1)\dots(Q_k y_k \leq z_k)\Psi_0(x_1,\dots,y_1,\dots,z_1,\dots)$$

where $Q_1,\dots,Q_k$ are quantifiers, Ψ_0 is a boolean combination of instances of φ and atomic formulas, the sets of variables $\{x_1,\dots\}$, $\{y_1,\dots\}$, $\{z_1,\dots\}$ are pairwise disjoint and the equivalence $\Psi \equiv \Psi'$ is provable in I_{open}. (We call $(*)$ the *bounded prenex normal form* of Ψ.)

Proof. First show that Ψ is equivalent to a formula Ψ_1 consisting of a block of bounded quantifiers followed by a boolean combination of instances of φ and atomic formulas. To this end check that analogues of the following hold for bounded quantifiers: renaming of bound variables, de Morgan rules and factoring out a quantifier Q from the antecedent (succedent) of an implication whose succedent (antecedent) does not contain free occurence of the variable bound by Q. *Caution:* it is important that bounded quantifiers use non-strict inequalities; i.e. if u is not free in χ then

$$(\exists u \leq v)(\chi \to \varphi) \equiv (\chi \to (\exists u \leq v)\varphi) \quad \text{is provable in } I_{\mathrm{open}} \text{ but}$$
$$(\exists u < v)(\chi \to \varphi) \equiv (\chi \to (\exists u < v)\varphi) \quad \text{is not}$$

(think of $v = 0$; we need $(\forall v)(\exists u)(u \leq v)$ to be provable).

Ψ_1 has a *clash of variables* if there are variables x, y, z such that Ψ_1 has the form

$$\dots(Q_1 z \leq y)\dots(Q_2 x \leq z)\dots\Psi_0\,,$$

i.e. z is both the bound in one quantifier and the quantified variable in a quantifier further out. It remains to show that Ψ_1 can be made clash-free. To this end let Ψ_2 be a subformula of Ψ_1 having a clash and such that each proper subformula of Ψ_2 is clash-free. Thus Ψ_2 is

$$(*) \qquad (Q y_1 \leq z_1)\dots(\forall y_i \leq y_1)\dots\Psi$$

and similarly for $\exists$ instead of $\forall$. But $(*)$ is equivalent in I_{open} to

$$(Q y_1 \leq z)\dots(\forall y_i \leq z)\dots(y_i \leq y_1 \to \Psi_0)$$

and similarly for $\exists$.

Iterated use of this procedure gives the result. □

2.50 Lemma. If $\varphi \in \Sigma_n$ and Ψ is $\Sigma_0(\varphi)$ then Ψ is Δ_{n+1} in $I\Sigma_n$.

Proof. Trivial for $n = 0$; thus assume $n > 0$. Assume ψ has the form guaranteed by 2.49 and apply propositional calculus to Ψ_0; then we get an equivalent formula Ψ'' of the form

$$(Q\mathbf{y} \leq \mathbf{z})(\bigwedge(\sigma_i \vee \pi_i))$$

where σ_i are Σ_n and π_i are Π_n. Write σ_i as $(\exists y)\sigma_{0i}(\mathbf{x}, y)$.

Using $S\Sigma_n$, bound all $(\exists y)$'s:

$$(\exists q)(\forall x, \ldots \leq \max(\mathbf{z})) \wedge (\sigma_i \rightarrow (\exists y < q)\sigma_{0i}(\mathbf{x}, y)) .$$

Then Ψ'' is equivalent in I_{open} to

$$(\exists q)(Q_1, x_1 \leq z_1) \ldots (Q_k x_k \leq z_k)(\wedge(\exists y \leq q)\sigma_{0i} \vee \pi_i) ,$$

the conjunction is Π_n in $I\Sigma_n$ and the whole last formula is Σ_{n+1} in $I\Sigma_n$. But this suffices since $\neg\Psi$ is also $\Sigma_0(\Sigma_n)$ and therefore Σ_{n+1} in $I\Sigma_n$. This completes the proof of the lemma (and of 2.25). □

(c) Finite Axiomatizability; Partial Truth Definitions for Relativized Arithmetical Formulas

The aim of the present subsection is two-fold: first, to show that for $n > 0$, $I\Sigma_n$, $B\Sigma_{n+1}$ and $P\Sigma_n$ are finitely axiomatizable; we show this using partial truth definitions elaborated in Sect. 1 (d). Second, we shall extend our possibility of dealing with infinite sets inside fragments of arithmetic by showing that, under some conditions, we may speak in $I\Sigma_1$ of sets Σ_n-defined *from a given set* (and quantify over such sets). This will give us very useful meansof expression.

2.51 Discussion. Let us survey our sets and membership in arithmetic. First, we defined in $I\Sigma_0(exp)$ the memebership predicate $\in$ with respect to which numbers behave like hereditarily finite sets; in particular, $I\Sigma_0(exp)$ proves comprehension for $\Sigma_0^{exp}(exp)$ formulas. Furthermore, given any formula $\varphi(x)$ with just one variable, we may introduce a constant (A, say) for the set of all numbers satisfying φ together with an *ad hoc* membership predicate $\in$ such that $x \in A$ just means $\varphi(x)$. Analogously for formulas with more variables – we may introduce a constant for the *relation* defined by φ. In particular, assuming that $\varphi(x, y)$ defines a total function (which we denoted $TFUN(\varphi)$) we may write $y = F(x)$ for $(x, y) \in F$, which in turn just means $\varphi(x, y)$. More generally, our φ may contain free variables distinct from those displayed; they act as parameters. In this case we may consider the parameters to be just *codes* for the corresponding classes; if φ is $\varphi(x, par)$ then $x \in X_{par}$ (or even $x \in par$) means simply $\varphi(x, par)$. A particular case of this is given by partial truth definitions: if $Sat(z, e)$ is a formula which is a partial satisfaction for Γ-formulas (e.g. Σ_n-formulas) then we may take Γ-formulas with exactly one free variable for codes of Γ-sets as we did in Sect. 1 (d). In this last case we have double profit: *first*, we may quantify over Γ-sets and *second,* we have "it's snowing"-it's snowing lemma saying, roughly, for each Γ-formula $\varphi(x)$ that: the Γ-set coded by φ consists exactly of all numbers x satisfying $\varphi(x)$.

2.52 Theorem. For $n > 0$, each of the theories $I\Sigma_n$, $B\Sigma_{n+1}$, $P\Sigma_n$ is finitely axiomatizable.

Proof (sketch). Let n be given. We show that $I\Sigma_n$ is finitely axiomatizable. Observe that the assertion "$Sat_{\Sigma,n}$ satisfies Tarski truth conditions for Σ_n-formulas" is a conjunction of finitely many conditions (one for atomic formulas, one for each connective, two for the bounded quantifiers and two for unbounded ones, say). Thus it is a single formula provable in $I\Sigma_1$; let I_n be the finite subtheory of $I\Sigma_1$ making this formula meaningful and provable. In I_n we can express the single sentence saying

$$(*) \quad \begin{array}{l}(\forall X \;\; \Sigma_n^\bullet\text{-set}^\bullet) \\ \left[(0 \in_{\Sigma,n} X \,\&\, (\forall x)(x \in_{\Sigma,n} X \to S(x) \in_{\Sigma,n} X)) \to (\forall x)(x \in_{\Sigma,n} X)\right]\end{array}$$

(each $\Sigma_n^\bullet$-set satisfies induction). Observe that this is in fact one particular instance of Σ_n-induction (since $\in_{\Sigma,n}$ is Σ_n, thus $(*)$ is provable in $I\Sigma_n$; on the other hand, each instance of Σ_n-induction follows from $I_n + (*)$. Indeed, take a Σ_n-formula $\sigma(x,y)$ (y being a parameter); then $\overline{\varphi}' = Subst^\bullet(\overline{\varphi}, \overline{y}, \dot{y})$ is a $\Sigma_n^\bullet$-set – a formula$^\bullet$ with one free variable. Adding possibly one new axiom we may prove $Sat_n(\overline{\varphi}, \{(\overline{x}, \dot{x}), (\overline{y}, \dot{y})\}) \equiv Sat_n^\bullet(\overline{\varphi}', \{(\overline{x}, \dot{x})\}) \equiv \varphi(x,y)$. Now the class X coded by $\overline{\varphi}'$ is inductive by $(*)$; this gives I_φ. □

2.53 Definition ($I\Sigma_1$). A set X is *piecewise coded* (p.c.), if for each u there is a sequence s of zeros and ones of length u such that $(\forall i < u)((s)_i = 1 \equiv i \in X)$.

Remark. This is in fact a *scheme* of definitions, depending on the chosen notion of a set and membership (cf. 2.51). Recall also Def. 2.6 (a formula is piecewise coded in a theory $T \supseteq I\Sigma_1$). Evidently, the relation is as follows: $\varphi(x_0, \ldots, x_n)$ is p.c. in T iff T proves that the set of all n-tuples $\langle x_0, \ldots, x_n\rangle$ such that $\varphi(x_0, \ldots, x_n)$ is p.c.

2.54 Definition. (1) Let X be a new variable and let new atomic formulas be the old ones plus $t \in X$ where t is any term. $\Sigma_0(X)$ formulas result from new atomic formulas using connectives and bounded quantifiers.

(2) Copy the definition in $I\Sigma_1$, i.e., define $\Sigma_0^\bullet(X^\bullet)$ formulas in the obvious way. Clearly, φ is a $\Sigma_0(X)$-formula iff $I\Sigma_1 \vdash [\overline{\varphi}$ is a $\Sigma_0^\bullet(X^\bullet)$-formula$]$.

(3) Analogously for $\Sigma_n(X)$, $\Pi_n(X)$, $\Sigma_n^\bullet(X^\bullet)$, $\Pi_n^\bullet(X^\bullet)$.

2.55 Main Theorem. (Satisfaction for $\Sigma_0^\bullet(X^\bullet)$-formulas.) There is a formula $Sat_{0,X}(z,c)$ such that $I\Sigma_1$ proves the following:

If X is p.c. then $Sat_{0,X}$ obeys Tarski truth conditions for $\Sigma_0^\bullet(X^\bullet)$ formulas with $X^\bullet$ interpreted as X. Furthermore, under this interpretation each $\Sigma_0^\bullet(X^\bullet)$ set is p.c. and hence satisfies the least number principle. Under the assumption "X is p.c.", Sat_0 is $\Delta_1(X)$ in $I\Sigma_1$.

2.56 Remark. Clearly, this is again a scheme dependent on which notion of sets and membership is used. We can summarize the theorem by saying that in I_1 we can define satisfaction for sets Σ_0 definable from a set X *provided* X is p.c. Thus for a p.c. set X, we have coding for $\Sigma_0(X)$ sets; they are all p.c. and hence satisfy the least number principle. The enigmatic formulation saying that Sat_0 is $\Delta_1(X)$ under the assumption of X being p.c. means, pedantically, the following: we have a $\Sigma_1(X)$ formula Sat_0 and a $\Pi_1(X)$ formula Sat' and $I\Sigma_1 \vdash [X \text{ p.c.} \rightarrow Sat_{0,X} \equiv Sat'_{0,X}]$.

2.57 Corollary (Satisfaction for $\Sigma_k^\bullet(X^\bullet)$ formulas and $\Pi_k^\bullet(X^\bullet)$ formulas.) For each $k > 0$, there is a $\Sigma_k(X)$-formula $Sat_{\Sigma,k,X}(z, e)$ such that $I\Sigma_1$ proves the following:

If X is p.c. then $Sat_{\Sigma,k,X}$ obeys Tarski truth conditions for $\Sigma_k^\bullet(X^\bullet)$-formulas, $X^\bullet$ being interpreted as X.

Similarly for $\Pi_k(X)$.

(Obviously, $Sat_{\Sigma,k,X}$ is constructed from $Sat_{0,X}$ – or more precisely, from the two forms of $Sat_{0,X}$, exactly as $Sat_{\Sigma,k}$ was constructed from Sat_0.)

Caution. Nothing is claimed on $\Sigma_k^\bullet(X^\bullet)$-sets being p.c.!

2.58 Corollary ("It's snowing"-it's snowing lemma). If $\varphi(x_0, \ldots, x_k)$ is $\Sigma_n(X)$ then $I\Sigma_1$ proves the following:

If X is p.c. then $[\varphi(x_0, \ldots, x_k) \equiv Sat_{\Sigma,n,X}(\overline{\varphi}(\dot{x}_0(\overline{x}_0, \ldots), \emptyset]$.

The rest of the subsection elaborates the proof of 2.55 and contains some additional technical devices.

2.58 Definition ($I\Sigma_1$). q is a *partial satisfaction* for $\Sigma_0^\bullet(X^\bullet)$-formulas$^\bullet$ $\leq p$, their evaluations by numbers $\leq r$ and partial interpretation of X by a string s of zeros and ones (in symbols: $PSat'_0(q, p, v, s)$ if q is a finite mapping whose domain consists of all pairs (z, e) where z is $\Sigma_0^\bullet(X^\bullet)$, $z \leq p$, e is an evaluation for z, $e \subseteq (\leq p) \times (\leq v)$, $range(q) \subseteq \{0, 1\}$, $lh(s) > r^p$ and Tarski conditions hold for q whenever defined, i.e. we have the same conditions as in 1.71 and, in addition, (v) if z is $t \in X^\bullet$ where t is a term$^\bullet$ then $q(z, e) = 1$ iff $(s)_{Val(t,e)} = 1$.

Remark. (1) Note that general power x^y is definable in $I\Sigma_1$ by the usual inductive conditions, see 1.58.

(2) Prove in $I\Sigma_1$ that if t is a term$^\bullet$, $t \leq p$ and e its evaluation$^\bullet$ by numbers $\leq r$ then $Val(t, e) \leq r^p$; this follows from the fact that under our assumption on e, $Val(t, e) \leq r^{lh(t)}$, which is proved easily by induction on $lh(t)$. Thus the condition $lh(s) \geq r^p$ guarantees that $(s)_{Val(t,e)}$ is defined.

2.59 Lemma. (1) $PSat_0^\bullet$ is Δ_1 in $I\Sigma_1$.

(2) $I\Sigma_1$ proves the following: If $PSat_0^\bullet(q,p,r,s)$, $PSat_0^\bullet(q',p',r',s')$ and s coincides with s' on the intersection of their domains then then q coincides with q' on the intersection of their domains.

(3) Furthermore, $I\Sigma_1$ proves: for each p, r, s such that s is a string of zeros and ones and $lh(s) \geq r^p$ there is a q such that $PSat_0^\bullet(q,p,r,s)$.

Proof is fully analogous to the proof of 1.72. To get (3) prove the following by induction on p (r and s being parameters):

$$lh(s) \geq r^p \rightarrow (\exists q) PSat^\bullet(q,p,r,s)\,. \qquad \square$$

2.60 Definition ($I\Sigma_1$). Let X be p.c. Define $Sat_{0,X}(z,e)$ iff there are q,p,r,s, such that s is a piece of X, $PSat_0^\bullet(q,p,r,s)$ and $q(q(z,e)=1$.

Note that $Sat_{0,X}(z,e)$ implies that z is a $\Sigma_0^\bullet(X^\bullet)$-formula and e is its evaluation$^\bullet$.

2.61 *Proof of the Main Theorem 2.55.* We prove that the formula $Sat_{0,X}(z,e)$ has the properties stated. Work in $I\Sigma_1$. First observe that for $z \in \Sigma_0^\bullet(X^\bullet)$, e its evaluation$^\bullet$, and assuming X to be p.c. (so that we have arbitrarily long pieces of X) Lemma 2.59 implies the following:

$$(*) \qquad \begin{gathered} \neg Sat_{0,X}(z,e) \text{ iff there are } q,p,r,s \text{ such that } s \\ \text{is a piece of } X,\ PSat_0^\bullet(q,p,r,s) \text{ and } q(\neg^\bullet z, e) = 1\,. \end{gathered}$$

This shows that $Sat_{0,X}$ obeys Tarski condition for negation. Looking from outside $I\Sigma_1$ observe that the definition of $Sat_{0,X}$ is $\Sigma_1(X)$ in $I\Sigma_1$ and $(*)$ gives a $\Pi_1(X)$ definition of $Sat_{0,x}$ under the assumption that X is p.c. The proof of other Tarski conditions is similar and is left to the reader.

Work again in $I\Sigma_1$ and assume X p.c. Then we may speak on $\Sigma_0^\bullet(X^\bullet)$ sets, $X^\bullet$ being interpreted as X (briefly, speak on $\Sigma_0^\bullet(X)$ sets). It remains to be shown that each $\Sigma_0^\bullet(X)$ set is p.c. But this is now trivial: if $z \in \Sigma_0^\bullet(X^\bullet)$ is a formula$^\bullet$ with exactly one free variable$^\bullet$ and w is arbitrary, then the w-piece of z is easily obtained from any q such that $PSat_0^\bullet(q,p,r,s)$, where $p > z$, $r > w$ and s is a satisfactorily long piece of X. This completes the proof. $\square$

We close this subsection with a lemma on $\Sigma_1^\bullet(X)$ formulas which will be useful later. Recall that having proved 2.55 we also have $Sat_{\Sigma,n,X}$ and $Sat_{\Pi,n,X}$ (cf. 2.57).

2.62 Lemma. There is a formula $WSat_{\Sigma,1}$ which is Δ_1 in $I\Sigma_1$ and such that $I\Sigma_1$ proves the following: for each X p.c., each $z \in \Sigma_1^\bullet(X^\bullet)$ with exactly one free variable and each x, the following are equivalent:

(i) $Sat_{\Sigma,1,X}(z,[x])$ (where $[x]$ is the evaluation of the free variable of z by x);
(ii) $(\exists s$ piece of $X)\, WSat_{\Sigma,1}(z,x,s)$;
(iii) $(\exists w)(\forall s$ piece of X longer than $w)\, WSat_{\Sigma,1}(z,x,s)$. Furthermore $I\Sigma_1$ proves $WSat_{\Sigma,1}(z,x,s) \,\&\, s \subseteq s' \rightarrow WSat_{\Sigma,1}(z,x,s')$ (monotonicity). $WSat_{\Sigma,1}(z,x,s)$ is read: s *witnesses the satisfaction* of z by x.

Proof. $WSat_{\Sigma,1}(z,x,s)$ says: there are $u, z_1 \leq z$ such that $z = (\exists^\bullet u)z_1$, $z_1 \in \Sigma_0^\bullet(X^\bullet)$ and there is a $y \leq s$ such that for *some* q,p,r we have: $PSat_0^\bullet(q,p,r,s)$ and $q(z_1,[x,y]) = 1$ (with the obvious meaning of $[x,y]$).

Clearly, this is equivalent to saying that there are $u, z_1 \leq z$ as above and a $y \leq s$ such that for *all* q,p,r such that $PSat_0^\bullet(q,p,r,s)$ and $q(z_1,x,y)$ is defined, we have $q(z_1,x,y) = 1$. The rest is evident. □

(d) Relativized Hierarchy in Fragments

Here we shall investigate sets p.c. in $I\Sigma_n$ and in $B\Sigma_{n+1}$ ($n \geq 1$). In particular, we show that $B\Sigma_{n+1}$ proves all Σ_{n+1} sets to be p.c.; we introduce *low* Δ_{n+1} sets in $B\Sigma_{n+1}$ (in 2.69) and prove their basic properties (2.71). The concept of a low Δ_{n+1} set plays a very prominent role in the next section in connection with the analysis of provable forms of König's lemma. Finally we exhibit a class of sets called $\Sigma_0^{exp}(\Sigma_n)$ sets meaningful in $I\Sigma_n$ (2.73); we show that $I\Sigma_n$ proves each $\Sigma_0^{exp}(\Sigma_n)$ class to be p.c. and Δ_{n+1}. This will be useful for generalizing results on König's lemma proved in $B\Sigma_{n+1}$ to results in $I\Sigma_n$.

2.63 Lemma. (1) $I\Sigma_n$ proves each $\Sigma_n^\bullet$ set to be p.c. (2) $I\Sigma_n$ proves that $\Delta_n^\bullet$ total functions are closed under primitive recursion. (3) $B\Sigma_{n+1}$ proves each $\Delta_{n+1}^\bullet$ set to be p.c.

Proof. Imitate the proof of 2.13 (a) (but now working *inside* $I\Sigma_1$: we just prove one theorem with a universal quantifier over all $\Sigma_n^\bullet$ sets): Let X be a $\Sigma_n^\bullet$ set and let z be given: the z-piece of X is the least sequence s of length $z+1$ such that $(\forall i \leq z)(i \in X \rightarrow (s)_i = 1)$. (Alternatively, you could derive our assertion directly from 2.13 (a) using the fact that the formula $Sat_{\Sigma,1}$ is Σ_1 and therefore piecewise coded in $I\Sigma_1$.)

(2) Routine.

(3) Imitate the proof of 2.19 inside $B\Sigma_{n+1}$. □

2.64 Definition ($I\Sigma_1$). (1) A set X is *unbounded* if $(\forall x)(\exists y > x)(y \in X)$, i.e. $(Cx)(x \in X)$.

(2) A set X has the *order-type of the universe* (o.t.u.) if for each x there is a sequence s of length x enumerating increasingly the first x elements s, i.e.

$$Seq(s) \,\&\, lh(s) = x \,\&\, (\forall i < x)((s)_i \in X) \,\&\, (\forall i < j < x)((s)_i < (s)_j) \,\&\, (\forall i < x)(\forall y < (s)_i)(y \in X \rightarrow (\exists j < i)(y = (s)_j)\,.$$

2.65 Lemma. For $n \geq 1$, $I\Sigma_n$ proves that each $\Delta_n^\bullet$ unbounded set has o.t.u.

Proof. If X is $\Delta_n^\bullet$ unbounded then the function $F(x) = (\text{least } y)(y \in X \,\&\, y > x)$ is $\Delta_n^\bullet$ total; thus the function G defined by primitive recursion to be

$$G(0) = \min X$$
$$G(x+1) = F(G(x))$$

is $\Delta_n^\bullet$, total and G is the increasing enumeration of *all* elements of X. G is p.c.; thus for each x, the restriction of G to $(\leq x)$ is a set – the desired sequence s. □

2.66 Corollary (of 2.63). (1) In $I\Sigma_n$, we have satisfaction for $\Sigma_0^\bullet(\Sigma_n^\bullet)$ formulas and therefore may quantify over $\Sigma_0^\bullet(\Sigma_n^\bullet)$ sets. $I\Sigma_n$ proves that each $\Sigma_0^\bullet(\Sigma_n^\bullet)$ set is p.c.

(2) In $B\Sigma_{n+1}$, we have satisfaction for $\Sigma_0^\bullet(\Delta_{n+1}^\bullet)$ and therefore may quantify over $\Sigma_0^\bullet(\Delta_{n+1}^\bullet)$ sets. $B\Sigma_{n+1}$ proves that each $\Sigma_0^\bullet(\Delta_{n+1}^\bullet)$ set is p.c.

Remark. Compare (1) with 2.7 (1) or 2.13 (b): there we had a schema, here a single statement. A schema analogous to our present (2) is possible but cumbersome.

2.67 Theorem. ($I\Sigma_1 + B\Sigma_m, m \geq 1$). (1) Each $\Sigma_0^\bullet(\Delta_m^\bullet)$ set is a $\Delta_m^\bullet$ set; thus $\Sigma_0^\bullet(\Delta_m^\bullet)$ sets coincide with $\Delta_m^\bullet$ sets.

(2) $\Sigma_1^\bullet(\Delta_m^\bullet)$ sets coincide with $\Sigma_m^\bullet$ sets.

Proof. A quick way to prove this is to find (actual) formulas $\sigma(x, par) \in \Sigma_m$ and $\pi(x, par) \in \Pi_m$ and to show in $I\Sigma_1 + B\Sigma_m$ that if X is $\Sigma_0^\bullet(\Delta_m^\bullet)$ then for some par, $x \in X$ is equivalent both to $\sigma(x, par)$ and to $\pi(x, par)$. The result follows by the "it's snowing"-it's snowing lemma. Thus assume X to be $\Sigma_0^\bullet(Y)$ where Y is $\Delta_m^\bullet$; let z be the $\Sigma_0^\bullet(X')$-formula defining X from Y and let $u \in \Sigma_m^\bullet$, $v \in \Pi_m^\bullet$, both defining Y. Observe that the formula "s is a piece of Y" can be written both as $\sigma_1(s, u, v)$, $\sigma_1 \in \Sigma_m$ in $B\Sigma_m$ and $\pi_1(s, u, v)$, $\pi_1 \in \Pi_m$ in $B\Sigma_m$, e.g. σ_1 is

$$(\forall i < lh(s))((s)_i = 1 \rightarrow Sat_{\Sigma,m}((u, [i]) \,\&\, (s)_i = 0 \rightarrow \neg Sat_{\Pi,m}(v, i)) .$$

Now

$$x \in X \equiv (\exists q, p, r, s)(s \text{ piece of } Y \,\&\, PSat(q, p, r, s) \,\&\, q(z, [x]) = 1)$$

and

$$x \notin X \equiv (\exists q, p, r, s)(s \text{ piece of } Y \,\&\, PSat(q, p, r, s) \,\&\, q(z, [x]) = 0) .$$

This completes the proof of (1).

(2) is easy: by (1), a $\Sigma_1^\bullet(\Delta_m^\bullet)$ set can be defined by a formula of the form $(\exists^\bullet u)z$, where z is $\Delta_m^\bullet$; in the usual manner $(\exists^\bullet u)z$ may be replaced by a $\Sigma_1^\bullet$-formula (contraction of quantifiers). □

2.68 Corollary. For $n, m \geq 1$, $B\Sigma_{n+m}$ proves that each $\Sigma_{n+1}^\bullet(\Delta_m^\bullet)$ set satisfies the least number principle and is p.c.

2.69 Definition ($B\Sigma_{n+1}$, $n \geq 1$). A set X is *low* $\Delta_{n+1}^\bullet$ if it is $\Delta_{n+1}^\bullet$ and each $\Sigma_1^\bullet((X)$ set is also $\Delta_{n+1}^\bullet$.

Remark. This notion comes from recursion theory. Note that sets Δ_2 definable in $\mathbf{N}$ are exactly all sets recursive in K (the Σ_1-complete set), i.e. sets X such that $dg(X) \leq 0'$ (dg is the Turing degree). A Δ_2 set X is low if $(dg((X))' = 0'$, i.e. the jump of the degree of X is as small as possible. A reader not familiar with the notions involved may disregard this remark.

2.70 Remark. The definition of a low $\Delta_{n+1}^\bullet$ set is meaningful in $B\Sigma_{n+1}$ ($n \geq 1$) since this theory has satisfaction for $\Sigma_1^\bullet(\Delta_{n+1}^\bullet)$ formulas. Obviously, in $B\Sigma_{n+1}$ we may quantify over low $\Delta_{n+1}^\bullet$ sets: they are just some particular $\Delta_{n+1}^\bullet$ sets. Let us generalize: we may speak on low $\Delta_k^\bullet(X)$ sets if we know that $\Delta_k^\bullet(X)$ sets are p.c.

2.71 Theorem. The following equalities are expressible and provable in $B\Sigma_1 (m \geq 2)$:

$$\begin{aligned} low\, \Delta_m^\bullet &= low\, \Delta_2^\bullet(low\, \Delta_m^\bullet) = low\, \Delta_2^\bullet(\Delta_{m-1}^\bullet) \\ &= \Delta_1^\bullet(low\, \Delta_m^\bullet),\ \Sigma_2^\bullet(low\, \Delta_m^\bullet) = \Sigma_m^\bullet \end{aligned}$$

Proof. Work in $B\Sigma_m$. We know that low $\Delta_m^\bullet$ sets are p.c. (since $\Delta_m^\bullet$ sets are); therefore each set $\Sigma_0^\bullet$-defined from a low $\Delta_m^\bullet$ set X is p.c., thus also $\Delta_k^\bullet(X)$ makes sense. Moreover, if X is low $\Delta_m^\bullet$ and Y is $\Delta_2^\bullet(X)$ then Y is $\Delta_m^\bullet$ (since it is $\Sigma_1^\bullet$ in a $\Pi_1^\bullet(X)$ set, i.e. $\Sigma_1^\bullet$ in a $\Delta_m^\bullet$-set, i.e. $\Sigma_m^\bullet$, and similarly, Y is $\Pi_m^\bullet$) and thus Y is p.c. We have proved $\Delta_2^\bullet(low\, \Delta_m^\bullet) \subseteq \Delta_m^\bullet$. But then $low\, \Delta_2^\bullet(low\, \Delta_m^\bullet) \subseteq low\, \Delta_m^\bullet$. This completes the proof. □

*

In the rest of this subsection we discuss $I\Sigma_n$ instead of $B\Sigma_{n+1}$.

2.72 Theorem ($I\Sigma_n$, $n \geq 1$). Each $\Sigma_0^\bullet(\Sigma_n^\bullet)$ set is a $\Delta_{n+1}^\bullet$ set.

Proof. Similar to 2.67, we find formulas $\sigma(x, c, z)$ and $\pi(x, c, z)$ Σ_{n+1} and Π_{n+1} in $I\Sigma_n$ such that $I\Sigma_n$ proves the following:

If X_c is $\Sigma_n^\bullet$-defined by $c \in \Sigma_n^\bullet$ and Y_z is $\Sigma_n^\bullet(X^\bullet)$-defined by z from X_c then $(\forall x)(x \in Y \equiv \sigma(x, c, z) \equiv \pi(x, c, z))$.

By the "it's snowing"-it's snowing lemma we get that Y_z is a $\Delta_{n+1}^\bullet$ set. Details follow.

Now, $I\Sigma_n$ proves

$$(*) \qquad \begin{aligned} x \in Y_z \equiv &(\exists)(s \text{ is a piece of } X_c \,\&\, (\exists q, u, v)(PSat(q, u, s) \\ &\quad \& \, q(z, [x]) = 1) \\ \equiv &(\forall s)(s \text{ is a piece of } X_c \to (\forall q, u, v)(PSat((q, u, s) \\ &\quad \& \, q(z[x]) \text{ defined} \to q(z[x]) = 1)\,. \end{aligned}$$

Here "s is a piece of X" is $\Sigma_0(Sat_{\Sigma,n})$, therefore $\Sigma_0(\Sigma_n)$ in $I\Sigma_n$; by 2.25, it is Δ_{n+1} in $I\Sigma_n$. Hence the formula $(\exists s)(\ldots)$ in $(*)$ is Σ_{n+1} in $I\Sigma_n$ and so $(\forall s)(\ldots)$ is Π_{n+1} in $I\Sigma_n$. This completes the proof. □

2.73 Definition (cf. 2.54). (1) Let X be a new variable and add $t \in X$ (t a term) to the atomic formulas. $\Sigma_0^{exp}(X)$ formulas result from new atomic formulas using connectives and bounded quantifiers of the form $(\forall x \leq y)$, $(\forall x \leq 2^y)$ and similarly for $\exists$.

(2) In $I\Sigma_1$ define $\Sigma_0^{exp}(X^\bullet)$ formulas copying the definition.

2.74 Theorem (cf. 2.55). There is a formula $Sat_{0,X}^{exp}(z, e)$ such that $I\Sigma_1$ proves the following:

If X is p.c., then $Sat_{0,X}^{exp}$ obeys Tarski truth conditions for $\Sigma_0^{exp}(X^\bullet)$ formulas with $X^\bullet$ interpreted as X, and each $\Sigma_0^{exp}(X)$ set is p.c. and thus satisfies the least number principle. Under the assumption "X is p.c." $Sat_{0,X}^{exp}$ is $\Delta_1(X)$ in $I\Sigma_1$.

Proof. We shall define $PSat_0^{exp}(q, p, r, s)$ (partial satisfaction) analogously to 2.58, but we must be sure that if q is defined for a formula $(\forall u < 2^v)\varphi(u, \ldots)$ and an e evaluating v by some x then q will be defined for the evaluation e' extending e and evaluating u by any number $\leq 2^x$. To achieve this make the following definitions:

$qd(z)$ is the quantifier depth of a formula: $qd(z) = 0$ for open formulas, $qd(z_1 \,\&\, z_2) = \max(qd(q_1), qd(z_2))$, $qd(\neg z) = qd(z)$, $qd((\forall u \leq 2^v)z) = qd(z) + 1$.

2_y^x is the iterated power of $2 : 2_0^x = x$, $2_{y+1}^x = 2^{2_y^x}$.

Then require in the definition of $PSat_0^{exp}$ that $q(z, e)$ be defined whenever $z \leq u$ and $2_{qd(z)}^{\max(e)} \leq v$; the rest is the same as in 2.58, in particular, $v^u \leq lh(s)$ is assumed. Given this, it is easy to prove the following:

- $PSat_0^{exp}$ is Δ_1 in $I\Sigma_1$,
- if $PSat_0^{exp}(q_i, u_i, v_i, s_i)$ $(i = 1, 2)$ and s_1 coincides with s_2 where defined then q_1 coincides with q_2 where defined;

– for each u, v and each string s such that $lh(s) > v^u$, there is a q such that $PSat_0^{exp}(q, u, v, s)$.

Then $Sat_{0,X}^{exp}(z, e)$ is defined as

$$(\exists q, u, v, s) \quad (s \text{ is a piece of } X,\ PSat_0^{exp}(q, u, v, s) \text{ and } q(z, e) = 1)\,;$$

assuming X p.c., $Sat_{0,X}^{exp}(z, e)$ is equivalent to $(\forall q, u, v, s)$ (s is a piece of X and $PSat_0^{exp}(q, u, v, s)$ and $q(z, e)$ defined $\rightarrow q(z, e) = 1$). □

2.75 Corollary. We may introduce $Sat_{\Sigma,n,X}^{exp}$ in the obvious way and for each n prove in $I\Sigma_1$ the following: if X is p.c. then $Sat_{\Sigma,n,X}^{exp}$ and $Sat_{\Pi,n,X}^{exp}$ obey the respective Tarski truth condition.

Consequently, we have the corresponding "it's snowing"-it's snowing lemma.

2.76 Theorem. $I\Sigma_n$ proves that each $\Sigma_0^{exp}(\Sigma_n)$ set is p.c. and is Δ_{n+1}.

The proof of the fact that each Σ_0^{exp} set is p.c. is routine and uses the finite partial satisfactions. To prove that each $\Sigma_0^{exp}(\Sigma_n)$ set is Δ_{n+1}, first show that each (actual) $\Sigma_0^{exp}(\Sigma_n)$ formula is Δ_{n+1} in $I\Sigma_n$ (generalizing 2.49–2.50) and then imitate the proof of 2.72.

2.77 Definition. (1) In the above exponentiation may be replaced by any total Δ_1 function H; moreover, in $I\Sigma_n$ we may define X to be a $\Sigma_0^*(\Sigma_n)$ set if for some total Δ_1 function H and some Σ_n set Y, X is $\Sigma_0^H(X)$. We have satisfaction for $\Sigma_0^*(\Sigma_n)$ sets obeying Tarski truth conditions.

(2) We may define low $\Sigma_0^{exp}(\Sigma_n)$ sets (or *low* $\Sigma_0^*(\Sigma_n)$ sets) in $I\Sigma_n$: a set X is *low* $\Sigma_0^H(\Sigma_n)$ if it is $\Sigma_0^H(\Sigma_n)$ and each $\Sigma_1(X)$ set is $\Sigma_0^H(\Sigma_n)$. This is useful for generalizations of the low basis theorem in the next section.

(3) From here on out we shall write LL_n instead of low $\Sigma_0^*(\Sigma_n)$ (*n-very low sets*).

2.78 Lemma. For $n \geq 1$, $I\Sigma_n$ proves $I\Sigma_1(LL_n)$ and $B\Sigma_1(LL_n)$, i.e. induction and collection for $\Sigma_1(LL_n)$ sets.

Proof. This follows from the obvious modification of 2.76 (for $\Sigma_0^*(\Sigma_n)$ sets rather than $\Sigma_0^{exp}(\Sigma_n)$ sets) and the fact that each $\Sigma_1(LL_n)$ set is a $\Sigma_0^*(\Sigma_n)$ set: we get induction. Collection follows from induction in the usual way. □

Caution. In saying "X is $\Sigma_1(LL_n)$" we mean that for some LL_n set Y, X is $\Sigma_1(Y)$.

2.79 Theorem. For $n \geq 1$, $I\Sigma_n$ proves $\Delta_1(LL_n) = LL_n$, i.e. if Z is LL_n and $Y \in \Delta_1(Z)$ then Y is LL_n.

Proof. Let Y, Z be as above and let $X \in \Sigma_1(Y)$. Then, for appropriate $\Sigma_1(Z)$-formulas$^\bullet$ φ, ψ, we have

$$Y = \{y \mid (\exists s \text{ piece of } Z)\, WSat_{\Sigma,1}(\varphi, y, s)\},$$
$$-Y = \{y \mid (\exists s \text{ piece of } Z)\, WSat_{\Sigma,1}(\psi, y, s)\}.$$

(For *WSat* see 2.62.) Using $B\Sigma_1(LL_n)$ we get a common bound:

$$(\forall y < a)(\exists s \text{ piece of } Z)(\, WSat_{\Sigma,1}(\varphi, y, s) \vee WSat_{\Sigma,1}(\psi, y, s)).$$

Thus, for some Δ_1 formula δ,

$$t \text{ is a piece of } Y \equiv (\exists s \text{ piece of } Z)\delta(t, s).$$

Now $X \in \Sigma_1(Y)$; i.e. for some $\rho \in \Sigma_1(Y)$,

$$X = \{x \mid (\exists t \text{ piece of } Y)\, WSat(\rho, x, t)\} =$$
$$= \{x \mid (\exists s \text{ piece of } Z)(\exists t)(\delta(t, s) \,\&\, WSat_{\Sigma,1}(\rho, x, t))\}.$$

This shows that $X \in \Sigma_1(Z)$. Thus $\Sigma_1(Y) \subseteq \Sigma_1(Z) \subseteq \Sigma_0^*(\Sigma_n)$ and consequently $Y \in LL_n$. We have shown $\Delta_1(LL_n) \subseteq LL_n$. □

2.80 Corollary. $(I\Sigma_n)$. If $Z \in LL_n$ then $\Delta_1(\Delta_1(Z)) = \Delta_1(Z)$.

(e) Axiomatic Systems of Arithmetic with No Function Symbols

There are various situations in which it is useful to work with fragments of arithmetic formalized in a language having no function symbols. We shall encounter such situations repeatedly in this book. In the present subsection we prepare the necessary formalism.

2.81 Definition. L' is the language with a constant 0 (zero), binary predicates $=$, $\leq$, S (equality, less-than, successor), ternary predicates A, M (addition, multiplication). Bounded quantifiers are defined in the obvious way; formulas of L' with all quantifiers bounded are called *bounded' formulas* or Σ_0'-formulas. Σ_n' and Π_n' formulas result from Σ_0'-formulas in the obvious way.

2.82 Remark. We describe a rather weak axiom system called BA'. The main idea is that S, A, M may describe partial functions and that there may be a largest element (top). The functions defined by S, A, M have to satisfy the usual inductive conditions whenever the values in question are defined.

Since we do not want to spend much time polishing the axiom system we shall make no optimization (minimalization) of the number of axioms.

2.83 Definition. BA' is the theory in L' having the following axioms:

(1) Axioms saying that $\leq$ is a discrete linear order with the least element 0.
(2) $S(x,y)$ iff y is the upper neighbour of x w.r.t. $\leq$.

Further axioms say that A and M define binary operations, possibly partial.

(3) Induction properties of A and M:
$A(x,0,z) \equiv z = x$
$S(y,y') \,\&\, S(z,z') \to (A(x,y,z) \equiv A(x,y',z'))$
$M(x,0,z) \equiv z = 0$
$S(y,y') \,\&\, A(z,x,z'). \to .(M(x,y,z) \equiv M(x,y',z')$
(4) Commutativity and associativity of A and M, distributivity, monotonicity of addition, monotonicity of multiplication by a positive number, the relation of $\leq$ to addition: $x \leq y \equiv (\exists u \leq y)A(x,u,y)$.

Caution: equalities are understood to be saying "if one side is defined then the second is too and both sides are equal", e.g.

$$A(x,y,z) \equiv A(y,x,z)\,,$$
$$(\exists u)(A(x,y,u) \,\&\, A(u,z,w)) \equiv (\exists v)(A(y,z,v) \,\&\, A(x,v,w))$$

(associativity); monotonicity for A reads

$$(A(x,z,u) \,\&\, A(y,z,v)) \to (x \leq y \equiv u \leq v)\,.$$

(5) Schema of induction for Σ_0'-formulas:

$$(\varphi(0) \,\&\, (\forall x,y)(\varphi(x) \,\&\, S(x,y) \to \varphi(y))) \to (\forall x)\varphi(x)$$

2.84 Remark. (1) The reader may try to get rid of (parts of) (4) by proving some of these axioms from the remaining ones in analogy to the corresponding proofs in I_{open}.

(2) Show that BA' proves the least number principle in the usual way.

(3) Prove the following in BA':

$$(A(x,y,z) \,\&\, y_0 \leq y) \to (\exists z_0 \leq z)A(x,y_0,z_0)$$
$$A(x,y,z) \to (x \leq z \,\&\, y \leq z)$$
$$(M(x,y,z) \,\&\, y_0 \leq y) \to (\exists z_0 \leq z)M(x,y_0,z_0)$$
$$(M(x,y,z) \,\&\, z \neq 0) \to (x \leq z \,\&\, y \leq z)$$

(or just accept these formulas as further axioms).

2.85 Definition. (a) $I\Sigma'_0$ results from BA' by adding the axiom "S, A, M define total functions" ($(\forall x)(\exists y)S(x,y)$ etc.). It follows that there is no top element ($(\forall x)(\exists y)(x < y)$). $I\Sigma'_n$ results from $I\Sigma'_0$ by allowing any Σ'_n-formula φ in the induction schema; similarly $I\Pi'_n$.

(b) TA' is arithmetic with a top – the extension of BA' by the axiom "there is a top element" ($(\exists x)(\forall y)(y \leq x)$).

2.86 Lemma. TA' proves induction for each L'-formula.

Proof. This is evident: each quantifier can be bounded by the top. □

2.87 Remark. Clearly, in $I\Sigma_0$ we may define S, A, M in the obvious way ($S(x,y) \equiv y = S(x)$, $A(x,y,z) \equiv z = x + y$, etc.); then we obviously get $I\Sigma_0 \vdash I\Sigma'_0$ and similarly $I\Sigma_n \vdash I\Sigma'_n$. On the other hand, in $I\Sigma'_0$ we have axioms stating that S, A, M define total functions, thus we may introduce the operations S, $+$, $*$. To prove $I\Sigma'_0 \vdash I\Sigma_0$, etc., we need the following.

2.88 Lemma. For each bounded formula $\varphi(\mathbf{x})$ there is a bounded$'$ formula $\varphi'(\mathbf{x}, y)$ (with one new free variable) and a constant k such that $I\Sigma'_0$ (enriched by the function symbols S, $+$, $*$) proves

$$\bigwedge_i y > x_i^{\overline{k}} \rightarrow \varphi(\mathbf{x}) \equiv \varphi'(\mathbf{x}, y).$$

Proof. The only problem is with atomic formulas and this leads us to terms. For each term t and new variables y, z let $z =_y t$ be defined as the following example shows:

$$z =_y (x_1 + x_2) * x_3 \text{ is}$$
$$(\exists w_1 \leq y)(\exists w_2 \leq y)(A(x_1, x_2, w_1 \,\&\, M(w_1, x_3, w_2) \,\&\, w_2 = z);$$

then $z =_y t$ is bounded$'$ and if k is the term t understood to be a natural number then

$$I\Sigma'_0 \vdash y \geq (\max \mathbf{x})^{\overline{k}} \rightarrow (z = t \equiv z =_y t).$$

(Observe that if t consists of n symbols then $k \geq n$; and if $\mathbf{x}$ is the tuple of variables in t then $I\Sigma' \vdash t \leq (\max \mathbf{x})^n$.)

Let $t_1 = t_2$ be atomic and let k be this formula interpreted as a number. Then

$$I\Sigma'_0 \vdash (\max \mathbf{x})^k \leq y \rightarrow (t_1 = t_2 \equiv (\exists z \leq y)(z =_y t_1 \,\&\, z =_y t_2))$$

and similarly for $t_1 \leq t_2$. This shows the constructions of φ' for φ atomic. The induction step is easy. □

2.89 Theorem. For each n, $I\Sigma'_n \vdash I\Sigma_n$.

Proof. By the preceding, for any Σ'_0-formula φ and the corresponding φ', we have

$$I\Sigma'_0 \vdash \varphi(\mathbf{x}) \equiv (\forall y)(\bigwedge_i x_i^k < y \to \varphi(\mathbf{x}) = \varphi'(\mathbf{x}, y))$$
$$\equiv (\exists y)(\bigwedge_i x_i^k < y \,\&\, \varphi(\mathbf{x}) \equiv \varphi'(\mathbf{x}, y))\,.$$

In $I\Sigma'_0$, assume $\varphi(x, \ldots)$; we find a least x such that $\varphi(x, \ldots)$; this will show $L\Sigma_0$ and thus $I\Sigma_0$. Let $x, \ldots$ be given and take a y such that $(x^k < y \,\&\, \ldots)$; then we get $\varphi'(x, \ldots, y)$. By $L\Sigma'_0$ (provable in $I\Sigma'_0$) we get a least x such that $\varphi'(x, \ldots, y)$; by the above equivalence, this is the least x such that $\varphi(x, \ldots)$.
For $I\Sigma'_n$ ($n > 0$) reason similarly; by the above equivalence (and by contraction of quantifiers), each Σ_n-formula is Σ'_n in $I\Sigma'_n$. □

2.90 Corollary. Since all of the reasoning above is formalizable in $I\Sigma_1$ we get

$$I\Sigma_1 \vdash Con^\bullet(I\Sigma_n^\bullet) \equiv Con^\bullet(I\Sigma_n'^\bullet)$$

for each n.

3. Fragments and Recursion Theory

Introduction. In this section we shall first prove in $I\Sigma_1$ two advanced theorems concerning the arithmetical hierarchy: the *limit theorem* for Δ_2 functions (subsection (a)) and the *low basis theorem,* which is an effective version of König's lemma (subsection (b)). The classical König's lemma says that an infinite (countable) finitely branching tree has an infinite branch; in arithmetic, we have to assume something about the arithmetical complexity of the tree and the conclusion is the existence of an infinite branch of a certain complexity. (See below for details.) Both the limit theorem and the low basis theorem are heavily used in Chap. 2. In subsection (c) we elucidate the status of the theorem saying that each infinite Σ_1 set contains an infinite Δ_1 subset. Finally, in subsection (d) we formulate Matiyasevič's theorem in $I\Sigma_1$.

(a) Limit Theorem

3.1 Definition ($I\Sigma_1$). Let F be a total function; c is the *limit* of F (notation: $c = \lim_s F(s)$) if $(\exists t)(\forall s \geq t)(F(s) = c)$. Similarly for $G(x) = \lim_s F(x, s)$, etc.

3.2 Uniform Limit Theorem for Functions. $I\Sigma_1$ proves the following: there is a total Δ_1 function F of three arguments such that for each total Δ_2 function G of one argument we have

$$(\forall x)(G(x) = \lim_s(F(e, x, s)),$$

where e is a code of G (i.e. a code of the Δ_2 relation $y = G(x)$).

3.3 Corollary ($I\Sigma_1$). (1) For each Δ_2 total function G of one argument there is a Δ_1 total function F of two arguments such that $(\forall x)(G(x) = \lim_s F(x, s))$.

(2) In particular, for each Δ_2 set X there is a total binary Δ_1 function F such that for each x,

$$x \in X \equiv \lim_s F(x, s) = 1 \text{ and } x \notin X = \lim_s F(x, s) = 0\,.$$

3.4 *Proof – Part 1.* We first deal with Δ_2 sets. We proceed in $I\Sigma_1$. Let X be Δ_2 and let

$$x \in X \equiv (\exists u)(\forall v)\varphi(x, u, v, e)$$
$$x \in X \equiv (\forall u)(\exists v)\psi(x, u, v, e)$$

where $\varphi(x, u, v, e) \equiv Sat_0(e_0, [x, u, v])$, $\psi(x, u, v, e) \equiv Sat_0(e_1, [x, u, v])$ and $e = (e_0, e_1)$; e naturally codes X and φ, ψ are Δ_1. Define (omitting the argument e throughout)

$$F(x, s) = 1 \equiv (\exists u \le s)[(\forall v \le s)\varphi(x, u, v) \,\&\, (\forall u' < u)(\exists v \le s)\psi(x, u', v)]\,,$$
$$F(x, s) = 0 \text{ otherwise}.$$

Clearly, F is Δ_1 and total.

We prove

$$(1) \qquad x \in X \to \lim_s F(x, s) = 1$$

$$(2) \qquad x \notin X \to \lim_s F(x, s) = 0\,.$$

Assume $x \in X$ and let u_0 be any number such that $(\forall v)\varphi(x, u_0, v)$; by $B\Sigma_1$, there is an $s_0 \ge u_0$ such that $(\forall u' < u_0)(\exists v < s_0)\psi(x, u_0, v)$. Then for each $s \ge s_0$ we have $F(x, s) = 1$.

Now let $x \notin X$, thus $(\exists u)(\forall v)\neg\psi(x, u, v)$ and $(\forall u)(\exists v)\neg\varphi(x, u, v)$. Let u_0 be such that $(\forall v)\neg\psi(x, u_0, v)$ and let $s_0 \ge u_0$ be such that $(\forall u \le u_0)(\exists v \le s_0)\neg\varphi(x, u, v)$. Now let u be arbitrary; we show that for each $s \ge s_0$, u does not witness the formula defining $F(x, s)$ to be equal to 1. If $u \le u_0$ then we get

$(\exists v \leq s)\neg\varphi(x,u,v)$; and if $u_0 < u$ then we get $(\exists u' < u)(\forall v < u)\neg\varphi(x,u',v)$ (namely $u' = u_0$). Thus (1) & (2) have been proved. □

Proof – Part 2. Now let K be a unary total Δ_2 function; by 3.4 there is a total Δ_1 function G such that

$$y = K(x) \equiv \lim_s G(x,y,s) = 1 \tag{3}$$

$$y \neq K(x) \equiv \lim_s G(x,y,s) = 0\,. \tag{4}$$

Let $V(s,y,x) = \min\{r \leq s \mid r \geq y \,\&\, (\forall t)(r \leq t \leq s \rightarrow G(x,y,t) = 1\}$.

$$V(s,y,x) = s+1 \text{ if the above is undefined.}$$

Note that the interval $(V(s,y,x),s)$ is the longest interval ending with s on which $G(x,y,-)$ is constantly equal to 1.

Put $F(x,s) = y$ if

$$[(\forall y' \leq s)(V(s,y',x) \geq V(s,y,x) \text{ and } (\forall y' < y)(V(s,y',x) > V(s,y,x))]\,.$$

Thus $F(x,s) = y$ means that y is the smallest possible number among $y' \leq s$ having the maximal possible interval $(\ldots,s)$ (subinterval of (y',s)) on which $G(x,y,-)$ constantly equals to 1. We claim $K(x) = \lim_s F(x,s)$. Let $K(x) = y_0$ and let $s_0 \geq y_0$ be such that $s \geq s_0$ implies $G(x,y_0,s) = 1$. Furthermore, using $B\Sigma_1$ assume $s_1 \geq s_0$ to be large enough to satisfy

$$(*) \qquad (\forall y' \leq s_0)(y' = y \rightarrow (\exists s < s_1)(s > s_0 \,\&\, G(x,y,s) = 0))\,.$$

Then for $s > s_1$ we have $F(x,s) = y_0$: $V(s,y_0,x) \leq s_0$ but for all other $y' \leq s$ we have $V(s,y',x) > s_0$ by $(*)$ and for $y' > s_0$ since $V(s,y',x) \geq y'$. This completes the proof. □

3.6 Remark. The proofs 3.4–3.5 are due to Švejdar; observe that they prove the limit theorem as a schema in $B\Sigma_1$ ($I\Sigma_1$ is not necessary).

(b) Low Basis Theorem

3.7 Definition ($I\Sigma_1$). A *tree* is a set T of finite sequences containing with each sequence all its initial segments:

$$\mathit{Tree}(T) \equiv (\forall s \in T)(\mathit{Seq}(s)) \,\&\, (\forall s,t)(\mathit{Seq}(s) \,\&\, s \subseteq t \,\&\, t \in T \rightarrow s \in T)\,.$$

T is *finitely branching* if for each $s \in T$ the set of all upper neighbours t of s (i.e. $s \subseteq t \in T$ and $lh(t) = lh(s)+1$) is bounded. T is Δ_1*-estimated* if there is a Δ_1 function F such that $(\forall x)(\forall s \in T)(lh(s) = x \rightarrow s \leq F(x))$. (Evidently, a Δ_1-estimated tree is finitely branching.) A subtree $B \subseteq T$ is a *branch* of T if B is linearly ordered by the relation "being an initial segment of" (i.e. by inclusion).

3.8 Low Basis Theorem ($I\Sigma_1$). Each unbounded Δ_1 tree which is Δ_1 estimated has a low $\Sigma_0^*(\Sigma_1)$ unbounded branch.

3.9 Remark. (1) The theorem will be proved in this subsection; for the notion of low $\Sigma_0^*(\Sigma_1)$ sets (or LL_1 sets) see 2.77–78. In particular, recall that $I\Sigma_1$ proves induction and the least number principle for $\Sigma_0^*(\Sigma_1)$ sets, so that the notion of LL_1 sets makes sense.

(2) Recall 2.65: if T is Δ_1 and unbounded then it is o.t.u. (of the order type of the universe). Moreover, if Z is an LL_1 unbounded branch through a Δ_1 tree then Z is also o.t.u. – cf. 2.78: we have $I\Sigma_1(Z)$ and may relativize 2.65.

(3) Thus if $T \in \Delta_1$ is a Δ_1-estimated unbounded tree and B is an LL_1 unbounded branch through T then B determines a total function

$$Z(x) = y \equiv (\exists s \leq F(x+1))(s \in B \,\&\, (s)_x = y)$$

(where F is an estimator for T). Clearly, Z is $\Delta_1(B)$ and hence LL_1 by 2.79. Call Z a *branch function.* Conversely, an LL_1 branch function determines an LL_1 branch.

3.10 Corollary. Let $k \geq 1$. (1) $I\Sigma_k$ proves that each $T \in LL_k$ which is an unbounded LL_k-estimated tree has an LL_k unbounded branch. (In particular, each Δ_k, Δ_k-estimated unbounded tree has an LL_k unbounded branch.)

(2) $I\Sigma_{k+1}$ proves that each $T \in LL_k$ which is an unbounded finitely branching tree has an LL_{k+1} unbounded branch.

(3) $B\Sigma_2$ proves that each $T \in \Delta_1$ which is an unbounded Δ_1-estimated tree has a low Δ_2 unbounded branch.

(4) $B\Sigma_{k+1}$ proves that each $T \in$ *low* Δ_{k+1} which is an unbounded *low* Δ_{k+1}-estimated tree has a *low* Δ_{k+1} unbounded branch.

(5) $B\Sigma_{k+2}$ proves that each $T \in$ *low* Δ_{k+1} which is an unbounded finitely branching tree has a *low* Δ_{k+2} unbounded branch.

3.11 Remark. (1) follows by relativization since $I\Sigma_k$ proves $I\Sigma_1(LL_k)$ and, furthermore, $I\Sigma_k$ proves *low* $\Sigma_0^*(\Sigma_1(LL_k)) \subseteq LL_k$. (Easy; first prove $\Sigma_0^*(\Sigma_1(LL_k)) \subseteq \Sigma_0^*(\Sigma_k)$.)

(2) follows from (1) for $k+1$: observe in $I\Sigma_{k+1}$ that a LL_k finitely branching tree is $\Pi_1(T)$-estimated, thus Δ_{k+1}-estimated and LL_{k+1}-estimated.

(3) follows from 3.8: In $B\Sigma_2$ we know that each LL_1 set is low Δ_2. Having (3) we get (4) and (5) analogously to (1) and (2).

3.12 Lemma ($I\Sigma_1$). Let T be a Δ_1, unbounded, Δ_1-estimated tree; then there is an $s \in T$ of length 1 such that $T_s = \{t \supseteq s \mid t \in T\}$ is unbounded.

Proof. First observe that a Δ_1-estimated Δ_1 tree is unbounded iff for each x, there is a $t \in T$ of length x (thus being unbounded is Π_1 for such a tree). Without loss of generality we may assume that the elements of T of length 1 are $(0), (1), \ldots (a-1)$; assume that all $T_{\{i\}}$, $i < a$, are bounded, i.e.

$$(\forall i < a)(\exists h)(\forall s < F(h))(lh(s) = h \rightarrow s \notin T_{\{i\}})$$

(where F is a Δ_1 estimator of the tree). By $B\Sigma_1$,

$$(\exists h)(\forall i < a)(\forall s < F(h))(lh(s) = h \rightarrow s \notin T_{\{i\}}),$$

thus T has no elements of length h and therefore is unbounded. $\square$

3.13 Remark. We are now going to prove the low basis theorem. Recall the Δ_1 formula *WSat* such that $I\Sigma_1$ proves, for each X p.c., each $\Sigma_1^\bullet(X^\bullet)$ formula z with just one variable, and each number x,

$$Sat_{\Sigma,1,X}(z, [x]) \equiv (\exists s \text{ piece of } X)\, WSat_{\Sigma,1}(z, x, s);$$

$WSat(z, x, s)$ reads "s witnesses the satisfaction of z by x" (see 2.62 for more details; we shall omit the superscripts $\Sigma, 1$). If X is a *function* (i.e. a particular binary relation) such that for each u, the restriction $X \restriction u$ exists as a finite sequence (which implies that X is p.c.) it is convenient to change slightly the notion of witnessing by replacing "piece of" with "restriction of"; thus for the new Δ_1 predicate (which we still call *WSat*) we have in $I\Sigma_1$:

If X is a function as above, $z \in \Sigma_1^\bullet(X^\bullet)$ (one free variable) and x is arbitrary, then the following are equivalent:

$$Sat_{\Sigma,1,x}(z, [x]),$$
$$(\exists x)(\exists s = X \restriction x)\, WSat(z, x, s),$$
$$(\exists x)(\forall y \geq x)(\forall s = X \restriction y)\, WSat(z, x, s).$$

In this subsection we shall use this modification of *WSat*.

3.14. We start the proof of 3.8. We work in $I\Sigma_1$; the proof is an inspection of a usual recursion-theoretic proof. Let T be a Δ_1 unbounded tree, let F be a Δ_1 estimator for T. For technical reasons assume that F also estimates the full dyadic tree, i.e. for each sequence s of zeros and ones of length e, we have $s < F(e)$. The construction proceeds in steps. In step e, we define two strings s_e and c_e of length e; s_e will be a piece of the desired branch Z, and c_e information about a truncation of T enforced by previous steps. We use a Δ_1 enumeration (φ_e, a_e) of all pairs consisting of a $\Sigma_1^\bullet(X^\bullet)$-formula with one free variable and of a number. In step e we decide whether φ_e will be satisfied by a_e and Z, or not. For each e, let (e) be the finite set of all sequences less than $F(e)$ $(s \in (e) \equiv Seq(s) \,\&\, s \leq F(e))$. Clearly, $\Sigma_0^*(\Sigma_1)$ sets are closed under the quantification of the form $(\exists s \in (e))$, $(\forall s \in string(e))$. Two sequences s, t are called compatible if $s \subseteq t$ or $t \subseteq s$.

For $s, c \in (e)$ let $T(e,s,c) = \{t \in T \mid (t \text{ compatible with } s) \,\&\, (\forall i < e)((c)_i = 1 \rightarrow \neg WSat(\varphi_i, a_i, t))\}$. Obviously, $T(e,s,c)$ is Δ_1, and so is $T'(e,s,c)$ where $T'(e,s,c) = \{t \mid t \in T(e,s,c) \,\&\, \neg WSat(\varphi_e, a_e, t)\}$. Finally, let $cond(e,c,s',c')$ be the following condition (saying how to extend (s,c) to (s',c')):

$(s,c \in (e)) \,\&\, (s',c' \in (e+1)) \,\&\, (s \subseteq s' \,\&\, c \subseteq c') \,\&\, (\mathit{Case}\ 1 \vee \mathit{Case}\ 2)$, where

Case 1. $T'(e,s,c)$ is unbounded, $c' = c \frown \langle 1 \rangle$ (concatenation), and $s' = s \frown \langle i \rangle$, where $i < F(e+1)$ is minimal such that $T'(e,s,c)$ is unbounded over $s \frown \langle i \rangle$ (and $s' = \emptyset$, say, if such an i does not exist);

Case 2. $T'(e,s,c)$ is bounded, $c' = c \frown \langle 0 \rangle$ and $s' = s \frown \langle i \rangle$ where $i < F(e+1)$ is minimal such that $T(e,s,c)$ is unbounded over $s \frown \langle i \rangle$, $s' = \emptyset$ if such an i does not exist. (When we say that a tree T'' is unbounded over t_0, we mean that $\{t \in T'' \mid t \supseteq t_0\}$ is unbounded).

Observe that cond is $\Sigma_0^*(\Sigma_1)$ (since, as we know, "T is unbounded" is Π_1, see above).

3.15 Fact. (1) If $T(e,s,c)$ is unbounded then $(\exists s',c')cond(e,s,c,s',c')$.

(2) If $T(e,s,c)$ is unbounded and $cond(e,s,c,s',c')$, then $T(e+1,s',c')$ is unbounded (and contains s').

3.16. Define

$$Path(e,s,c) \equiv s,c \in (e) \,\&\, (\forall i < e) cond(i, s \restriction i, c \restriction i, s \restriction (i+1), c \restriction (i+1))$$

(where $s \restriction i$ is the initial segment of s of length i, etc.). Observe that $Path$ is $\Sigma_0^*(\Sigma_1)$.

3.17 Fact. If T is as above, then

$$(\forall e)[(\exists! s,c) Path(e,s,c) \,\&\, (\forall s,c)(Path(e,s,c) \rightarrow T(e,s,c) \text{ is unbounded})].$$

(This can be proved by induction, since $[\ldots]$ is $\Sigma_0^*(\Sigma_1)$. The induction step follows by 3.15.)

3.18. Define $Z(x) = y \equiv (\exists s,c \in (x+1))(Path(x+1,s,c) \,\&\, (s)_x = y)$. Clearly, Z is a $\Sigma_0^*(\Sigma_1)$ total function; it is a branch through T.

3.19 Lemma. $Sat_{\Sigma,1,Z}(\varphi_e, [a_e])$ iff for the unique s,c satisfying $Path(e,s,c)$ we have Case 2, i.e. $T'(e,s,c)$ is bounded.

Proof. Note that, by 2.22, $Sat_{\Sigma,1,Z}(\varphi_e, a_e)$ is equivalent to the existence of a piece t of Z such that $WSat(\varphi_e, a_e, t)$. Assume Case 2, i.e. $T'(e,s,c)$ is bounded, and let t be a piece of Z longer than a bound for $T'(e,s,c)$. Then $t \in T(e,s,c)$ and $WSat(\varphi_e, a_e, t)$; thus $Sat_{\Sigma,1,Z}(\varphi_e, a_e)$. Now assume Case 1. Then we can prove for each $i > e$

$$(\forall s', c' \in (i))(Path(i, s', c') \rightarrow \neg WSat(\varphi_e, a_e, s'))$$

by induction on i (since the formula in question is $\Sigma_0^*(\Sigma_1)$). Thus there is no piece t of Z such that $WSat(\varphi_e, a_e, t)$. $\square$

3.20. Consequently, Z is low $\Sigma_0^*(\Sigma_1)$; we have

$$Sat_{\Sigma,1,Z}(\varphi_e, a_e) \equiv (\exists s, c \in (e+1) \mid (Path(e,s,c) \,\&\, (c)_e = 0),$$

or, in still more detail, given φ, a, let $e = e(\varphi, a)$ iff $(\varphi, a) = (\varphi_e, a_e)$; then

$$\begin{gathered} Sat_{\Sigma,1,Z}(\varphi, a) \equiv \\ \equiv (\exists s, c \in (e(\varphi,a)+1))Path(e(\varphi,a), s, c) \,\&\, (c)_{e(\varphi,a)} = 0). \end{gathered}$$

This completes the proof of the Low basis theorem.

3.21 Remark. An inspection of the proof gives the following in $I\Sigma_1$: if T is a dyadic unbounded Δ_1 tree (i.e. elements of T are sequences or zeros and ones) then T has a low $\Sigma_0^{exp}(\Sigma_1)$ unbounded tree.

(c) Infinite Δ_1 Subsets

In this subsection we pay attention to the fact that in $B\Sigma_m$ ($m \geq 2$) we have two notions of infinity for Σ_m sets: being unbounded and being o.t.u. (cf. again 2.64–65). We show that $I\Sigma_m$ proves that a Σ_m set is unbounded iff it is o.t.u. ($m \geq 1$); and obviously, $I\Sigma_1$ proves that if a Σ_m set is o.t.u. then it is unbounded. But in general, $B\Sigma_m$ does not prove that each unbounded Σ_m set is o.t.u., thus our notions differ, even for Σ_m sets ($m \geq 2$) The well-known recursion-theoretic fact that an infinite Σ_m set has an infinite Δ_m subset has two formalizations in $B\Sigma_m$ – for our two notions of finiteness. We shall show that both formalizations are provable. (For $m = 1$ we have to add something to make quantification over Σ_1 sets possible – let us just add $I\Sigma_1$).

3.22 Theorem. (a) $I\Sigma_1$ proves that each unbounded Σ_1 set has an unbounded Δ_1 subset.

(b) For $n \geq 1$, $I\Sigma_n$ proves that each unbounded Σ_{n+1} set has an unbounded Δ_{n+1} subset.

Proof. For $n \geq 0$ work in $I\Sigma_{\max(1,n)}$ and let $x \in X \equiv (\exists y)\psi(x,y)$ where ψ is Π_n (for $n = 0$, ψ is Δ_1). For each u, let $F(u)$ be the $v \geq u$ such that $(\exists y)\psi(v,y)$ with the smallest possible witness, i.e.

$$F(u) = v \equiv (\exists w)(\psi(w_0),(w)_1) \mathbin{\&} (w)_0 = v \geq u \mathbin{\&} \\ \mathbin{\&} \neg(\exists w' < w)(\psi((w')_0,(w')_1) \mathbin{\&} (w')_0 \geq u).$$

Then F is a total Σ_{n+1} function (due to $L\Pi_n$ or $L\Delta_1$), hence a Δ_{n+1} function, and for $Y = \mathit{range}(F)$ we have $v \in Y \equiv F(v) = v$ ($\Leftarrow$ is trivial; conversely, if $F(u) = v$ then $F(v) = v$ by the definition of F) and Y is clearly unbounded. Thus Y is a Δ_{n+1} unbounded subset of X. $\square$

3.23 Theorem. For $n \geq 1$, $I\Sigma_n$ proves that each unbounded Σ_n set is o.t.u.

Proof. For Δ_n sets see 2.65. Let X be Σ_n unbounded; recall that X is p.c. By 3.22 and 2.65, let $Y \subseteq X$ be Δ_n and o.t.u. and let s be the sequence of the first x elements of Y. Let a be the maximal element of s and let q be the piece of X up to $a+1$. Working with q as a finite set and using $I\Sigma_1$ let t be the increasing enumeration of numbers i such that $q(i) = 1$, i.e. $i \in X \mathbin{\&} i \leq a$. Clearly, each element of the sequence s occurs in t, thus $lh(t) \geq x$. Thus X is o.t.u. $\square$

3.24 Theorem. For $n \geq 1$, $I\Sigma_1 \cup B\Sigma_n$ proves that each Σ_n set which is o.t.u. contains a Δ_n o.t.u. subset.

Proof (a modification of a proof of J. Paris).

Let $x \in A \equiv (\exists y)\theta(x,y)$ where θ is Π_{n-1} (for $n = 0$: θ is Δ_1). Let

$$(u,v) \in R \equiv \theta(u,v) \mathbin{\&} (\forall w < v)\neg\theta(u,w),$$

thus R is Δ_n (selector for θ). Consider R as a set of ordered pairs and let $F(a) = b$ if b is the increasing enumeration of the first a elements of R. F is Δ_n; we show that it is total.

If a is given and c is the sequence coding the first a elements of A then, by $B\Pi_{n-1}$, there is a d such that $(\forall i < a)(\exists y < d)\theta((c)_i,y)$. Thus if e enumerates all elements of R less than $(\max(c),d)$ then e must have at least a members. Thus F is total.

Let $x \in B \equiv (\exists t < x)(\exists v < F(2t+1))\theta(x,v)$. Then B is Δ_n and $B \subseteq A$. Let a be given; $F(2a+1)$ is a sequence enumerating the $(2a+1)$ first elements (u,v) of R. For at most $(a+1)$ of them we have $u \leq (a+1)$ (since R is a function); i.e. for at least a of them we have $u > a$ and $v < F(2a+1)$ and hence $(u,v) \in B$. Thus if s enumerates increasingly all elements of B less than $F(2a+1)$ then $lh(s) \geq a$. $\square$

(d) Matiyasevič's Theorem in $I\Sigma_1$

Recall Matiyasevič(-Robinson-Davis-Putnam)'s theorem 0.48: it says that Σ_1 subsets (or subrelations) of N coincide with $\exists$ subsets (subrelations), i.e. with subsets defined by purely existential formulas. (Each $\exists$ formula is trivially a Σ_1 formula; thus one inclusion is trivial.) In this short subsection we carefully formulate Matiyasevič's theorem in $I\Sigma_1$. Needless to say, the fact that this important theorem is provable in $I\Sigma_1$ (and even in a weaker theory, see below) is very interesting. But since we shall use this fact only once (in Chap. IV) and since even a proof of the non-formalized Matiyasevič's theorem is rather lengthy but its formalization in $I\Sigma_1$ is more or less immediate, we shall only comment on the proof and shall refer to the literature.

3.25 Theorem. For each Σ_1 formula $\varphi(x_1,\ldots,x_n)$ there is a $\exists$ formula $\psi(x_1,\ldots,x_n)$ with the same free variables such that $I\Sigma_1 \vdash \varphi \equiv \psi$.

Remark on the proof. Clearly, the theorem is proved by induction on the complexity of φ; the case of open formulas is obvious and so is the inductive step for $\exists$, &, $\vee$. (For Σ_0 formulas φ one has to prove that both φ and $\neg\varphi$ are equivalent to some $\exists$ formulas.) The only non-trivial, but extremely peculiar, case is that of a bounded universal quantifier – this is the heart of the proof of Matiyasevič's theorem. But realizing this, one can just read an accessible proof (for example [Davis 73], to which we referred also for the proof of 0.84) and check that everything formalizes.

Alternatively, one can consult [Dimitracopoulos 80] where a proof of Matiyasevič's theorem is elaborated even in $I\Sigma_0(exp)$. Detailed instructions for the formalization are also contained in [Gaifman-Dimitracopoulos 82].

Since we have the satisfaction $Sat_{\Sigma,1}$ which is itself a Σ_1 formula, we get the following

3.27 Corollary ($I\Sigma_1$). Each $\Sigma_1^\bullet$ set is an $\exists^\bullet$ set, i.e. for each $\Sigma_1^\bullet$ formula z there is an $\exists^\bullet$ formula w (both with just one free variable) such that z and w are equivalent:

$$(\forall x)(Sat_{\Sigma,1}(z,[x]) \equiv Sat_{\Sigma,1}(w,[x])\,.$$

(Let $\rho(z,x)$ be an $\exists$ formula such that $I\Sigma_1 \vdash Sat_{\Sigma,1}(z,x) \equiv \rho(z,x)$; in $I\Sigma_1$, given z, let w be $Subst^\bullet(\overline{\rho},\overline{z},\dot{z})$, i.e. substitute the numeral$^\bullet$ $\dot{z}$ for the variable$^\bullet$ $\overline{z}$ in the formula$^\bullet$ $\overline{\rho}$.)

4. Elements of Logic in Fragments

We have already developed some elements of logic in $I\Sigma_1$: in Sect. 1(d) we introduced formulas of arithmetic, $\Sigma_y^\bullet$ formulas, etc., and given k, we defined in $I\Sigma_1$ satisfaction of $\Sigma_k^\bullet$ formulas in the universe of all numbers. Moreover, in Sect. 2 we investigated partial satisfaction for the relativized hierarchy; satisfaction also concerned the universe of all numbers. We shall now extend this in several respects: first, we allow an arbitrary language, not just the language of arithmetic. Second, we shall discuss, inside $I\Sigma_1$, the notion of provability; among other things, we shall be interested in the fact that in $I\Sigma_1$ we have Herbrand's theorem. Third, we shall formalize in $I\Sigma_1$ some facts from general model theory; among other things we prove a version of Gödel's completeness theorem (called the Low arithmetized completeness theorem). Finally we apply these techniques and facts to the language of arithmetic; among other things we show that for each k, $I\Sigma_{k+1}$ proves the consistency of $I\Sigma_k$. A natural continuation is then to formalize, inside $I\Sigma_1$, some facts on non-standard models of arithmetic; but this presupposes that a (informal) model theory of fragments has been elaborated. Thus we shall continueour present investigation of logic inside fragments dealing with models of fragments constructed in fragments in Chap. IV.

In subsections (a), (b) we show how to prove some facts stated in Sect. 0 (0.3–0.21). Note that some model-theoretical proofs do not formalize (or at least their formalization is not known) so that we shall have to use alternative, more elementary proofs.

Note also that a reader hurrying to study Gödel's incompleteness theorems and related topics presented in Chap. III should read subsection (a) of the present section; then he may switch to Chap. III.

(a) Arithmetizing Provability

4.1. We shall work in $I\Sigma_1$ but everything relativizes to $I\Sigma_1(\Gamma)$ where Γ is as in Sect. 3. Recall that in $I\Sigma_1$, total Δ_1 functions are closed under primitive recursion (cf. 1.54). Recall also the theorem on the free algebra of expressions. We now apply this theorem for the chosen construction of terms and formulas of arbitrary Δ_1 language.

4.2 Definition. ($I\Sigma_1$). A Δ_1 *language* L consists of mutually disjoint Δ_1 sets Pred$^\bullet$, Fct$^\bullet$, Const$^\bullet$ of predicates, functions and constants respectively and a Σ_1 function ar$^\bullet$ associating with each predicate and function symbol its arity (positive number). We further assume that Pred$^\bullet$, Fct$^\bullet$ and Const$^\bullet$ are disjoint from an infinite Δ_1 set of variables$^\bullet$ and from logical connectives$^\bullet$ and quantifiers$^\bullet$.

The reader can supply without difficulties definitions of the Δ_1 set Term$^\bullet$ of terms and the Δ_1 set Form$^\bullet$ of formulas in complete analogy to 1.61 and can prove in $I\Sigma_1$ the properties of formulas and terms analogous to those in 1.61.

Furthermore, we define the Δ_1 set LogAx$^\bullet$ of logical axioms and two Δ_1 relations-rules of inference, copying the definition in 0.10.

4.3 Definition ($I\Sigma_1$). A *theory* is given by a Δ_1 language L and a set T (not necessarily Δ_1) of formulas of L called ***special axioms***, including equality axioms$^\bullet$ (defined in the obvious way, cf. 0.11). We call T a theory if L is clear from the context. A finite sequence s of L-formulas is a *T-proof$^\bullet$* if for each $i < lh(s)$, $(s)_i$ is a logical or special axiom$^\bullet$ or follows from some previous members of s by a rule of inference. Note that if T is p.c. then the set $Proof^\bullet_T$ of all T-proofs is in $\Delta_1(T)$; in particular, if T is Δ_1 then $Proof^\bullet_T$ is Δ_1. We write $Proof^\bullet_T(s,x)$ if s is a T-proof$^\bullet$ and its last member is x. $\mathrm{Pr}^\bullet_T(x)$ (or $T \vdash^\bullet x$) means that x is T-provable, i.e. $(\exists s)Proof^\bullet_T(s,x)$.

4.4 Lemma ($I\Sigma_1$-compactness). If $T \vdash^\bullet x$ then there is a finite subset $t \subseteq T$ such that $t \vdash^\bullet x$.

Proof. (We do not assume $T \in \Delta_1$.) Let $Proof^\bullet_T(s,x)$ and let t be the set of elements $(s)_i$ of the sequence s such that $(s)_i$ is not a logical axiom and does not follow from previous numbers. Since s is a T-proof, $t \subseteq T$; and $Proof^\bullet_t(s,x)$. □

4.5 Definition ($I\Sigma_1$). A theory T is *Δ_1-decidable* or simply *decidable* if the set of all T-provable formulas is Δ_1.

4.6 Fact ($I\Sigma_1$). If T is Δ_1 then $Proof^\bullet_T$ is Δ_1 and $\{x \mid T \vdash^\bullet x\}$ is Σ_1. (Evident)

4.7 Definition ($I\Sigma_1$). T is *consistent* (in symbols: $\mathrm{Con}^\bullet_T$) if there is no closed formula$^\bullet$ x such that $T \vdash^\bullet x$ and $T \vdash^\bullet \neg^\bullet x$.

4.8 Remark. A switch to Chap. III is possible now.

4.9 Theorem ($I\Sigma_1$). Let T be a theory and let $T \vdash^\bullet (\exists^\bullet u)\varphi(u)$.

Let c be a constant$^\bullet$ not in the language of T, let T' be $T + \varphi(c)$ ($\varphi(c)$ is shorthand for $Subst^\bullet(\varphi, u, c)$). Then T' is a conservative extension of T. If T is decidable then T' is also decidable.

Proof. Copy the usual proof: given a T'-proof, replace each of its members $\alpha(c)$ by $\varphi(x) \to \alpha(x)$ where x is a new variable. Show by Σ_1-induction that each $\varphi(x) \to \alpha(x)$ is T-provable. Thus we get: $T' \vdash^\bullet \alpha(c)$ iff $T \vdash^\bullet \varphi(x) \to$

$\alpha(x)$ (thus T' is decidable if T is); in particular, if α is a T-formula we get $T' \vdash^\bullet (\exists^\bullet x)\varphi(x) \to \alpha$ iff $T \vdash^\bullet \alpha$. □

4.10 Theorem ($I\Sigma_1$). Each theory T has a conservative Henkin extension T', i.e. for each T'-formula $\varphi(u)$ with just one free variable there is a constant c such that $T' \vdash^\bullet (\exists^\bullet u)\varphi(u) \to^\bullet \varphi(c)$.

If $T \in \Delta_1$ then $T' \in \Delta_1$ and if T is decidable then so is T'.

Proof. This seems to be a trivial consequence of the preceding theorem but there are two difficulties: (1) *First* one has to construct a language L' extending the language of L and a Δ_1 function C associating with each L'-formula φ having just one free variable a constant $C(\varphi)$ (also denoted c_φ) not occuring in φ. (If necessary, we replace L by an isomorphic copy so that we have infinitely many non-members of L). This is easily achieved by generalizing the notion of an expression: take variables and constants of L as atoms and generate simultaneously terms, formulas and constants of L'. (Define a *derivation* of a term, formula or constant in the obvious way and prove all necessary facts). So assume we have L' and C. Extend T by adding all axioms $\varphi(u) \to^\bullet \varphi(c_\varphi)$: the result is T'. It remains to be proved that T' extends T conservatively. By 4.4 it suffices to show that for each finite $t_1 \subseteq T$ and for each finite set t_2 of the added axioms, $t_1 \cup t_2$ extends t_1 conservatively. We cannot prove this by induction on t_2 since "extends conservatively" is Π_2 and we work in $I\Sigma_1$. This is the *second* obstacle. But assume that p is a $(t_1 \cup t_2)$-proof of a T-formula φ and prove $t_1 \vdash^\bullet \varphi$.

Let t_2' be the least subset of t_2 such that $t_1 \cup t_2' \vdash^\bullet \varphi$ (we use $L\Sigma_1$); if t' is non-empty, 4.9 gives a smaller t'' such that $t_1 \cup t'' \vdash^\bullet \varphi$. Thus t' is empty and $t_1 \vdash^\bullet \varphi$. Moreover, iterated use of 4.9 gives a Δ_1 function D associating with each T'-sentence z a T-sentence $D(z)$ such that $T' \vdash^\bullet z$ iff $T \vdash D(z)$; thus if T is decidable then so is T'. □

We have presented a rather detailed proof to show for a relatively simple example some difficulties that we may ecounter when formalizing metamathematical proofs in fragments, as well as ways to overcome them. Similar tricks will be used rather frequently in the succeeding chapters.

4.11 Theorem ($I\Sigma_1$). Let L be a language (and assume that its complement is infinite; otherwise take an isomorphic copy).

(1) There is a Δ_1 function PNF associating to each L-formula φ its prenex normal form $\varphi = PNF(\varphi)$ such that ψ is an L-formula, consists of a block of quantifiers followed by an open formula, has the same free variables as φ and the equivalence $(\varphi \equiv \psi)$ is provable in the empty theory with the language L (pure predicate calculus).

(2) There is a language L' extending L by new function symbols and a Δ_1 function F associating with each L'-formula φ and each variable y a function

symbol $F(\varphi, y)$ from L'-L (denoted also by $F_{\varphi,y}$) not occurring in φ, whose arity equals the number of free variables of φ distinct from y.

(3) There is a Δ_1 function Sk associating with each L-formula Φ in prenex normal form its Skolem normal form satisfying conditions copied from 0.15 (where F_i^Φ is $F((Q_{i+1}x_{i+1})\dots(Q_k x_k)\varphi, x_k))$ in the notation of 0.15, i.e Φ is $(Q_1 x_1)\dots(Q_k x_k)\varphi(\mathbf{x}, \mathbf{y})$, Q_i are quantifiers, $t_i = x_i$ if $Q_i = \forall$, $t_i = F_i^\Phi(\leftarrow t_{i-1})$ if Q_i is $\exists$ and $Sk(\Phi)$ is $\varphi(t_1, \dots, t_k, \mathbf{y})$.

(4) There is a Δ_1 function He associating with each L-formula Φ in prenex normal form its Herbrand normal form, i.e. $He(\Phi)$ is logically equivalent to the existential closure of $\neg Sk(\neg\varphi)$.

Proof. Checking that everything formalizes in $I\Sigma_1$ is trivial except perhaps for (2): but this is achieved in the same way as the construction of Henkin constants in 4.10. □

4.12 Remark. Observe that we have not claimed anything about deductive properties of Skolem and Herbrand normal forms. We shall finally obtain all expected results but now we come to the place where no direct formalization of easy model theoretic proofs is known (at least to the authors, see the problem in 4.28). Thus we have to use a more elementary and tedious approach. We rely on the book by Shoenfield.

4.13 Hilbert-Ackermann's Theorem ($I\Sigma_1$). Let T be an open theory (all axioms open). If T is inconsistent then there is a disjunction D of instances of negations of axioms of T such that D is a propositional tautology.

Remark. An instance of a formula $\varphi(x_1 \dots x_n)$ is any formula $\varphi(t_1, \dots, t_n)$ where $t_1, \dots t_i$ are terms, t_i free for x_i in φ. An open formula is a propositional tautology if each evaluation of its atoms by zeros and ones produces the value 1 using the truth tables of connectives.

Checking the fact that Shoenfield's proof formalizes in $I\Sigma_1$ is tedious but straightforward and we shall omit it. Note that we assume the equality axioms to be particular axioms of T so that our tautologies are just Shoenfield's quasi-tautologies.

4.14 Corollary ($I\Sigma_1$). A closed existential formula is provable (in predicate calculus) iff there is a disjunction of instances of its open part which is a propositional tautology.

4.15 Herbrand's Theorem ($I\Sigma_1$). A formula φ is provable in predicate calculus iff its Herbrand normal form is provable in predicate calculus iff there is a disjunction of closed instances of the open part of $He(\varphi)$ that is a propositional tautology.

Remark. Here again we refer to the proof in Shoenfield's book; the reader may check without difficulty that this proof formalizes in $I\Sigma_1$. See 0.21 and

III.3.30. Note again that Herbrand's theorem is also analyzed in Chap. V where it is shown that it is provable a theory weaker than $I\Sigma_1$.

4.16 Theorem ($I\Sigma_1$). If T is a theory in L, $T \vdash (\forall x)(\exists y)\varphi(x,y)$ and F is a new function symbol then $T \cup \{(\forall x)\varphi(x, F(x))\}$ extends T conservatively.

Proof. As in [Shoenfield]. Take F to be $F_{\varphi,y}$ and observe that it suffices to show that whenever $(\forall x)\varphi(F(x)) \rightarrow \alpha$ is provable in predicate calculus (where α is a L-formula) then $(\forall x)(\exists y)\varphi(x,y) \rightarrow \alpha$ is also provable. To see this it is enough to observe that both formulas have the same Herbrand normal form. $\square$

4.17 Definition ($I\Sigma_1$). $Sk(T) = \{Sk(\varphi)) \mid \varphi \in T\}$.

4.18 Corollary ($I\Sigma_1$). $Sk(T)$ is a conservative extension of T.

Proof. Routine, use 4.16 (similarly to the proof of 4.10, i.e. using $L\Sigma_1$). $\square$

4.19 Corollary ($I\Sigma_1$). T is consistent iff each finite set of closed instances of $Sk(T)$ is propositionally satisfiable.

Proof. T is consistent iff each finite $t \subseteq T$ is consistent. Such a $t = \{\varphi_0, \ldots, \varphi_v)$ is consistent iff $\{Sk(\varphi_0), \ldots, Sk(\varphi_v)\}$ is consistent (by 4.18); this is equivalent to the propositional satisfiability of each finite set of closed instances of $Sk(\varphi_0), \ldots Sk(\varphi_v)$ by Hilbert-Ackermann. $\square$

4.20 Theorem ($I\Sigma_1$). Each theory T has a conservative open extension T' in which each formula is equivalent to an open formula. If T is Δ_1 then T' is also Δ_1.

Proof. Like 0.17, using 4.11 (2) (construction of the language). $\square$

(b) Arithmetizing Model Theory

Here we shall define models for a language and prove some theorems on the relation between consistency and existence of a model. The notion of a partial satisfaction plays a prominent role.

4.21 Definition ($I\Sigma_1$). Let L be a language. A *model* for L consists of a non-empty set M and a system $S = ((R_P)_{P \in Pred}, (f_F)_{F \in Fct}, (m_c)_{c \in \mathrm{const}})$ such that for each $P \in Pred$, $R_P \subseteq M^x$ where x is the arity of P, f_F: $M^x \rightarrow M$ where x is the arity of F and m_c is an element of M. As usual, we write M instead of (M, S).

Remark. This sounds very familiar but the reader should keep in mind two things:

(1) In fact this is a scheme of definitions depending on the range of the variable M. We may speak on Δ_1 models, Σ_{17} models, etc; working in $B\Sigma_2$, we may speak on low Δ_2 models etc.

(2) S is a system of sets indexed by elements of a set; this is easily expressed by requiring that S be a set of ordered pairs and, for example, if $P \in \mathit{Pred}$, then $R_P = \{x \mid (x, P) \in S\}$: saying that R_P is a z-ary relation we mean that R_P consists of sequences s of elements of M such that $lh(s) = z$. A mapping $f : M^x \to M$ is understood to be a particular $(x+1)$-ary relation on M.

(*Definition* continued). Let M be a model for a language L. Define an *evaluation of variables of a term* by copying Def. 0.4 in $I\Sigma_1$ (and generalizing 1.64): e is an evaluation of variables of G in M if e is a finite mapping associating to some variables (among them all variables of t) elements of M. A function Val is an *evaluation of terms in M* if it satisfies the conditions of 0.4 (copied in $I\Sigma_1$), i.e. $\mathit{Val}(u, e) = e(u)$ if u is a variable, $\mathit{Val}(u, e) = u_M$ if u is a constant, $\mathit{Val}(F(t_1 \dots t_x), e) = f_F(\mathit{Val}(t_1, e), \dots, \mathit{Val}(t_x, e))$.

4.22 Lemma ($I\Sigma_1$). If M is Δ_1 then there is a unique Δ_1 evaluation of terms in M.

Proof. Routine. (Note that we assume M to be Δ_1.) □

4.23 Definition ($I\Sigma_1$). Let M be a model for L and let Val be a valuation of terms. Let Λ be a set of L-formulas closed under the taking of subformulas and substituting terms. A relation Sat is a *partial satisfaction* for Λ in M if it satisfies Tarski's conditions w.r.t. M and Λ (copy 0.4). Sat is a *full* satisfaction for M if it is a satisfaction for all L-formulas in M. (M, Sat) is a *full model* if M is a model and Sat is a full satisfaction in M.

Under the notation of 4.23, a Λ-formula is *true* in (M, Sat) if for each evaluation e of variables of z, $(z, e) \in \mathit{Sat}$. If T is a theory and each axiom of T is a Λ-formula then M is a *model* of T if each axiom of T is true in (M, Sat).

4.24 Theorem ($I\Sigma_1$). If M is a model for L and M is Δ_1 then there is a unique $S \in \Delta_1$ which is a satisfaction for open formulas in M.

Proof. Routine (imitate 1.71–1.74; you have to relate everything to M but you do not have to deal with quantifiers). □

4.25 Theorem ($I\Sigma_1$). If T is a decidable theory (i.e. the set of all provable formulas is Δ_1) then T has a full Δ_1 model.

Proof. Just imitate the usual proof of the completeness theorem: first extend T conservatively to a Henkin theory $T' \in \Delta$ (recall that T' is decidable) and then extend T' to a complete decidable theory T'' having the same language as T'. To this end, use a Δ_1 increasing enumeration Z of closed T'-formulas (write z_i for $Z(i)$ and define $H(i) = z_i$ if $Con^\bullet(T' \cup \{H(0), \ldots, H(i-1), z_i\})$, $H(i) = \neg z_i$ otherwise; put $T'' = range(H)$, i.e. $z_i \in T''$ iff $T'' \vdash z_i$ iff $H(i) = z_i$. Thus T'' is decidable. For each closed term t let $E(t)$ be the least closed term t' such that $T'' \vdash t =^\bullet t'$; let $M = range(E)$. Observe that M is Δ_1 ($t \in M$ iff $T'' \vdash E(t) =^\bullet t$); for $t_1, \ldots, t_x \in M$ put $(t_1 \ldots t_x) \in R_P$ iff $T'' \vdash^\bullet P(t_1 \ldots t_x)$ and put $f_F(t_1 \ldots t_x) = E(F(t_1 \ldots t_x))$. If z is a formula and $u_0 \ldots u_x$ are its free variables then put

$$Sat(z, [t_0 \ldots t_x]) \equiv T' \vdash^\bullet Subst^\bullet(z, (u_0 \ldots u_x), (t_1 \ldots t_x)))$$

(x-fold substitution). Then show by induction on formulas that Tarski's truth conditions are obeyed, observing that they are $\Sigma_0(\Sigma_1)$ (condition for $\forall$!); thus $I\Sigma_1$ is sufficient. □

4.26 Theorem ($I\Sigma_1$). If M is a Δ_1 model and $T = Tr_{\text{open}}(M)$ is the set of all open formulas true in M then $Con^\bullet(T)$.

Proof. By Hilbert-Ackermann's theorem, if T is inconsistent then there is a disjunction δ of instances of negations of axioms of T that is a propositional tautology. Let Sat be the satisfaction for open formulas in M; prove by Δ_1-induction that δ is true in M. (For each evaluation of variables of δ compute the corresponding evaluation of atoms of δ by zeros and ones; 1 means that the atom is satisfied). Show that for each open formula built from these atoms we get: φ is satisfied by our evaluation in M iff our propositional evaluation gives φ the value 1.)

On the other hand, each instance of our axiom is true in M, and the same holds for any conjunction of such instances (again Σ_1 induction suffices). Thus $\neg\delta$ is true in M and also δ; this is a contradiction. Thus T is consistent. □

4.27 Low Arithmetized Completeness Theorem.

(1) ($I\Sigma_1$) If $T \in \Delta_1$ is a theory then T is consistent iff it has a full *low* $\Sigma_0^*(\Sigma_1)$ model.

(2) ($B\Sigma_2$) If $T \in \Delta_1$ is a theory then T is consistent iff it has a full *low* Δ_2 model.

Proof. Let $T \in \Delta_1$; we may assume T to be Henkin. Define a dyadic tree $Tree(T)$ as follows: first take a Δ_1 enumeration of all sentences of L; denote it by $(z_0, z_1, \ldots)$. Put $(0)z = \neg^\bullet z$ and $(1)z = z$. For each string s, let $s \in Tree(T)$ iff there is no $p \leq s$ such that p is a T-proof of a contradiction from $\{((s)_i)z_i \mid i < lh(s)\}$.

Thus s is in the tree iff there is no short proof of a contradiction from the first $lh(s)$ sentences negated or asserted according to s. We show by Σ_1-induction that the tree is unbounded, namely we show that for each x there is an s such that $Con(\{((s)_i)z_i \mid i < x\})$. (The induction step is evident.) Thus the Low Basis Theorem gives an infinite branch $B = (\varepsilon_0, \varepsilon_1, \dots)$.

The branch is LL_1 (i.e. $\Sigma_0^*(\Sigma_1)$). Use the Δ_1 enumeration of all closed formulas above: we define $\hat{T} = \{z_n \mid \varepsilon_n = 1\}$. Clearly, $\hat{T}$ is $\Delta_1(B)$ and hence LL_1. $\hat{T}$ defines the canonical structure as follows: $M = \{c \text{ constant} \mid (\forall c' < c, c' \text{ constant})((c \neq^\bullet c') \in \hat{T})\}$ (representatives of classes of provably equal constants) – note that M is $\Delta_1(\hat{T})$ and hence LL_1. Predicates and function symbols are interpreted as follows:

$$(c_0, \dots c_x) \in R_P \text{ iff } P(c_0, \dots c_x) \in \hat{T}\,;$$
$$d = f_F(c_0, \dots, c_x) \text{ iff } (d =^\bullet F(c_0, \dots, c_x)) \in \hat{T}\,.$$

Clearly the structure M is LL_1; one defines $Sat_M(z, e)$ iff $Subst^\bullet(z, e) \in \hat{T}$ (we substitute the constants assigned by e for the free variables of z). Clearly, Sat_M is LL_1 and one verifies easily Tarski truth conditions for connectives and quantifiers. Thus (M, Sat_M) is a full LL_1 model, and for each (closed) axiom z of T, $Sat_M(z, \emptyset)$; thus (M, Sat_M) is a model of T.

Conversely, assume that (M, Sat) is a full LL_1 model of T. Let $z_0, \dots z_x$ be a T-proof; show as usual by induction that each member of this sequence is true in (M, Sat). The induction step is routine; and the statement is $(\forall e$ evaluation of $z_i)(Sat(z_i, e))$, thus $\Pi_1(Sat)$, *a fortiori*, $\Sigma_0^*(\Sigma_1)$ and the result follows by $I\Sigma_0^*(\Sigma_1)$. (Alternatively, we can prove that for each i, the universal closure $(\forall^\bullet \dots)z_i$ of z_i is satisfied by $\emptyset$, which is $\Delta_1(Sat)$.) □

4.28 Problem. Can we formalize the trivial model-theoretic proof of 0.14? This seems to be a peculiar task; starting from a LL_1 model you can interpret a Skolem function by an LL_1 mapping as in 0.14; but does the expanded structure have an LL_1 full satisfaction?

(c) Applications to Arithmetic

In subsections (a), (b) we arithmetized some parts of logic of axiomatized theories; in (a) we dealt with elements of proof theory and in (b) with elements of model theory. This logic has been developed in $I\Sigma_1$. In this subsection we apply this framework to particular arithmetized theories, namely to fragments of arithmetic themselves. We shall introduce Δ_1 theories $I\Sigma_k^\bullet$, $B\Sigma_k^\bullet$, $PA^\bullet$ etc. and derive some of their properties in $I\Sigma_1$. We show that, for each k, $I\Sigma_{k+1} \vdash Con^\bullet(I\Sigma_k^\bullet)$ (theorem 4.34). Formalization of parts of the model theory of fragments presupposes satisfactory knowledge of the non-formalized (actual) model theory of fragments, which will be studied in Chap. IV. Thus we postpone our discussion of important parts of arithmetized metamathematics of fragments until that chapter. Note that by using formalized model theory we shall be able to strengthen the above result and prove that, for each k, $I\Sigma_{k+1} \vdash Con^\bullet(B\Sigma^\bullet_{k+1})$ (Theorem IV.4.8). And Gödel's second incompleteness theorem (III.2.21) gives the unprovability of $Con(I\Sigma^\bullet_{k+1})$ in $I\Sigma_{k+1}$.

4.29 Definition ($I\Sigma_1$). Define in the obvious way Δ_1 functions assigning to each formula z of the language of arithmetic and to each variable$^\bullet$ u the corresponding scheme$^\bullet$ $I^\bullet z$ and collection scheme$^\bullet$ $B^\bullet z$; define the finite set $Q^\bullet$ of axioms$^\bullet$ of Robinson's arithmetic as $\{\overline{Q}_0, \ldots, \overline{Q}_8\}$, where Q_i are axioms of Q. Define $I\Sigma^\bullet_x$ to be the set $Q^\bullet \cup \{I^\bullet z \mid z \in \Sigma^\bullet_x\}$ and similarly for $B\Sigma^\bullet_x$, $PA^\bullet$, etc.

4.30 Remark. For each k, the set $I\Sigma^\bullet_k$ is provably Δ_1 and obviously defines $I\Sigma_k$ in N; evidently, the formula $(z \in I\Sigma^\bullet_k)$ binumerates $I\Sigma_k$ in $I\Sigma_1$, i.e. for each formula α, α is an axiom of $I\Sigma_k$ iff $I\Sigma_1 \vdash \alpha \in I\Sigma^\bullet_k$, and α is not an axiom of $I\Sigma_k$ iff $I\Sigma_1 \vdash \alpha \notin I\Sigma^\bullet_k$.

Binumerations of (actual) axiom systems will be studied closely in Chap. III; here we have for each of our systems just one particular binumeration, whose definition in $I\Sigma_1$ only copies the actual definition we gave in Sect. 1 or 2.

4.31 Remark. We have a particular model for the language of arithmetic, namely the *universe* (the Δ_1 set V of all numbers) endowed with the Δ_1 relation Ord' defined by $x \leq y$, the Δ_1 functions *succ* ($succ(x) = S(x)$), *add* ($add(x, y) = x + y$) and *mult* ($mult(x, y) = x * y$) and the element 0. We can also speak of the *standard model* but the reader should keep in mind that everything is said and meant *inside* of $I\Sigma_1$. Recall satisfactions $Sat_{\Sigma,k}$ and $Sat_{\Pi,k}$: they are partial satisfactions for the universe in the sense of 4.22.

4.32 Theorem ($I\Sigma_1$-formalized Σ_1-completeness). $Q^\bullet$ proves each true $\Sigma^\bullet_1$-sentence$^\bullet$, i.e. if $z \in \Sigma^\bullet_1$ is closed and $Sat_{\Sigma,1}(z, \emptyset)$ then $Q^\bullet \vdash^\bullet z$.

Proof. Copy the proof of 1.8; it suffices to prove the assertion for $z \in \Sigma_0$. Since $Q^\bullet \vdash^\bullet z$ is a Σ_1-formula the proof by induction formalizes as it stands. □

4.33 Theorem. For each $k \geq 1$, $I\Sigma_k$ proves the consistency of the set of all true $\Pi^\bullet_{k+1}$ sentences, i.e. if $Tr(\Pi^\bullet_{k+1})$ is the Π_{k+1}-set of all true $\Pi^\bullet_{k+1}$-sentences then $I\Sigma_k \vdash Con^\bullet(Tr(\Pi^\bullet_{k+1}))$. (More pedantically, $Tr(\Pi^\bullet_{k+1})$ is a formula with the only free variable x saying "x is a closed formula$^\bullet$ and $Sat^\bullet_{\Pi,k+1}(x, \emptyset)$".)

Proof. The idea of the proof is rather simple: in $I\Sigma_k$, take a finite set π of true $\Pi^\bullet_{k+1}$ formulas and expand the standard model to a Δ_k model of $Sk(\pi)$. Since $Sk(\pi)$ is open, we get $Con^\bullet(Sk(\pi))$ by relativizing 4.26 to $I\Sigma_1(\Delta_1) = I\Sigma_1$. And we get $Con^\bullet(\pi)$ since $Sk(\pi)$ proves π.

We shall elaborate on this. Let π be our finite set of true $\Pi^\bullet_{k+1}$-formulas and let Φ be one of them. We may assume that the axioms of linear order appear among them; then we may assume without loss of generality that each Φ has its bounded part in bounded prenex form, i.e. Φ consists of a block of unbounded alternating quantifiers (the first being $\forall$) followed by a block of bounded quantifiers followed by an open formula.

Follow the definition of the Skolem normal form in 4.11. Our Φ may be presented as follows:

$$(\forall^\bullet u_1)(\exists^\bullet u_2)\dots(Q_{k+1}u_{k+1})(Q_{k+2}u_{k+2} \leq^\bullet v_{k+2})\dots(Q_r u_r \leq^\bullet v_r)\varphi(\mathbf{u},\mathbf{v})$$

where each v_i is some u_j, $j < i$.

For $i = 0,\dots p$, let $\Phi^{(i)}$ be the result of deleting the i leftmost quantifiers (binding $u_1,\dots,u_i$) in Φ. Recall the terms $t_1,\dots t_p$ in 4.11: if Q_j is $\exists^\bullet$ then t_j is $F^\Phi_j(\leftarrow t_{j-1})$ and if Q_j is a $\forall^\bullet$ then t_j is u_j. We define

$$f^\Phi_1(x_1) = (\text{least } x_2)Sat_{\pi,k-1}(\Phi^{(2)}, [x_1, x_2])\,;$$

note that $\Phi^{(2)}$ is just $(Q_3u_3\dots)\varphi(u)$, which is Σ_{k-1}; thus f^Φ_1 is total since Φ is true and by $L\Sigma_{k-1}$. Furthermore, f^Φ_1 is Δ_k. For all other i such that Q_{i+1} is $\exists^\bullet$ we define

(a) for $i \leq k$:

$f^\Phi_i(\leftarrow x_i) = (\text{least } x_{i+1})Sat_{\Pi,k-1}(\Phi^{(i+1)}, [x_1,\dots x_{i+1}])$ if there is such an x_{i+1}, and $= 0$ otherwise.

(b) for $i > k$:

$f^\Phi_i(\leftarrow x_i) = (\text{least } x_{i+1} \leq x_j)Sat_0^{(\Phi(i+1)}[x_1\dots x_{i+1}])$ if there is such an x_{i+1}, $= 0$ otherwise (here v_{i+1} is u_j).

Observe that $i \geq 3$ so that f^Φ_i is certainly Δ_k. We consider the Δ_k extension of the standard model by all the (finitely many) f^Φ_i as interpretations of F^Φ_i. Recall that we have a Δ_k valuation Val^* of terms and a Δ_k satisfaction Sat^* for open formulas of the extended language (relativized 4.24). □

Claim. Let $[\mathbf{x}]$ be an evaluation of variables$^\bullet$ $u_1,\dots u_q$ by numbers $x_1,\dots,x_q$ such that for each $i = 1,\dots k$ we have $x_i = Val^*(t_i, [\mathbf{x}])$;
then $Sat_0(\varphi(u_1\dots u_k), [\mathbf{x}])$.

Prove the claim by showing the following by induction on $j = 0,\dots q$: $Sat_{\Pi,k-1}(\Phi^{(j)}, [\mathbf{x}])$. We have induction enough at our disposal; and the induction step just uses the definition of F^Φ_i.

Note that the evaluation $[\mathbf{x}]$ satisfying the condition of the claim is fully determined by its members x_i such that Q_i is $\forall^\bullet$; let $[\mathbf{x}]'$ be the corresponding subevaluation. The claim gives evidently the following: for each evaluation $[\mathbf{x}]'$, $Sat^*(\varphi(t_1,\dots t_q), [\mathbf{x}]')$. (This is because we get $Val^*(t_i,[x]') = Val^*(t_i,[\mathbf{x}]') = x_i$; recall that φ is open).

Consequently, we have shown that for each Φ in π and each evaluation e of free variables of $Sk(\pi)$, e satisfies $Sk(\pi)$ in Sat^*, hence $Sk(\pi)$ is consistent and π is also consistent. (Once again: consistency of $Sk(\pi)$ uses Hilbert-Ackermann, see 4.26; consistency of π follows since π is provable from $Sk(\pi)$ in logic.)

4.34 Corollary. (1) For each k, $I\Sigma_{k+1} \vdash Con(I\Sigma_k^\bullet)$. (This is because $I\Sigma_k^\bullet$ is $\Pi_{k+2}^\bullet$-axiomatized.)

(2) Moreover, $I\Sigma_{k+1}$ proves the following: if z is a true $\Sigma_{k+3}^\bullet$-sentence (i.e. $Sat_{\Sigma,k+3}(z,\emptyset)$) then $Con^\bullet(I\Sigma_k \cup \{z\})$. (This is because a true $\Sigma_{k+3}^\bullet$ sentence z is implied by a true $\Pi_{k+2}^\bullet$-sentence in which the leftmost existential quantifier of z is replaced by a witness.)

(3) (Reflection). For each Σ_{k+3} formula φ, $I\Sigma_{k+1} \vdash \varphi \to Con^\bullet(\varphi)$. (Thus for *each* φ, $PA \vdash \varphi \to Con(\varphi)$.)

4.35 Remark. (1) This cannot be improved on by allowing φ to be also Π_{k+3} since $I\Sigma_{k+1}$ is itself axiomatized by a single Π_{k+3} sentence and we would have $I\Sigma_{k+3} \vdash Con^\bullet(I\Sigma_{k+3})$ which contradicts Gödel's second incompleteness theorem.

(2) Note that in Chap. IV we prove $I\Sigma_{k+1} \vdash Con^\bullet(B\Sigma_{k+1}^\bullet)$; this will use the formalized model theory of fragments.

(3) In the rest of this section, we prove a theorem which is a modification of 4.33 (or at least its proof is a modification of the proof of 4.33). It is a sufficient condition for consistency using Δ_1 models. We shall use it in Chap. II in connection with Paris-Harrington principle.

4.36 Definition. ($I\Sigma_1$). The skolemization of a formula Φ in the language of arithmetic with respect to unbounded quantifiers is defined similarly to the full skolemization, but bounded quantifiers are left untouched. Thus: let Φ be $(Q_1x_1)\dots(Q_k,x_k)\varphi(\mathbf{x},y)$ where φ is $\Sigma_0^\bullet$ and Q_i is $\forall^\bullet$ or $\exists^\bullet$. Let

$$t_i = x_i \text{ if } Q_i \text{ is } \forall^\bullet,$$
$$t_i = F_i^\Phi(\leftarrow t_{i-1}) \text{ if } Q_i \text{ is } \exists^\bullet.$$

Then $Sk_0(\Phi)$ is $\varphi(t_1\dots t_k)$. A closed instance of $Sk_0(\Phi)$ is any formula $\varphi(s_1,\dots s_u,\mathbf{u})$ where $\mathbf{s},\mathbf{u}$, are tuples of closed terms in the extended language, and if Q_i is $\exists^\bullet$ then s_i is $F_i^\Phi(\leftarrow s_{i-1},\mathbf{u})$. For each set T of formulas, $Sk_0(T) = \{Sk_0(\Phi) \mid \Phi \in T\}$.

4.37 Theorem ($I\Sigma_1$). Let T be a Δ_1 theory in the language of arithmetic. Assume that for each finite set S_0 of closed instances of $Sk_0(T)$ there is a Δ_1 expansion of the standard model to a model of S_0. Then $Con(T)$.

Proof. First two remarks. (1) Recall 4.13 implying that if each finite set of closed instances of $Sk(T)$ (full skolemization) is true in a Δ_1 expansion of the standard model then $Con(T)$ (since truth of an open-closed formula in a Δ_1 model gives trivially propositional satisfaction).

(2) We know that a Δ_1 structure has a Δ_1 satisfaction for open formulas; observe that if we Δ_1 expand the standard model by adding interpretation of (finitely many) functions then the satisfaction Sat_0 immediately extends to a Δ_1 satisfaction for formulas resulting from $\Sigma_o^{\bullet}$ formulas by substituting $L^{\bullet}$-terms for their variables ($Sk_0(\Phi)$ has such a form): define for $[\mathbf{x}] = [x_1 \dots x_k]$

$$Sat_0(\varphi(t_1, \dots t_k), [x_1 \dots x_k]) \text{ iff}$$
$$Sat_0(\varphi(u_1 \dots u_k), [Val(t_1[\mathbf{x}]), \dots Val(t_k, [\mathbf{x}])]).$$

Trivially, Tarski conditions are satisfied. Saying that a Δ_1 structure expanding the standard model is a model of S_0 means that each element of S_0 is true in the extension of Sat_0 just described.

The proof of 4.37 may now follow the same pattern as that of 4.33 with the only difference being that the Skolem functions for unbounded quantifiers need not be constructed since they are given (as Δ_1 functions) in advance:

Take a finite set S of closed instances of $Sk(T)$ and find a finite set S_0 of closed instances of $Sk_0(T)$ such that S is a set of instances of $Sk(S_0)$. Let M be a Δ_1 expansion of the standard model in which S_0 is true. Now define Δ_1 interpretations of Skolem functions of $Sk(S_0)$ (we deal with bounded quantifiers now – cf. 4.33 for $i > k$) and get a Δ_1 expansion M' of M in which S is true. □

4.38 Remark. The same holds for the case where T is formulated in the language with predicates for the successor, addition and multiplication, cf. Sect. 2 (e).