Characterising Complexity Classes by Inductive Definitions in Bounded Arithmetic[⋆]

Naohi Eguchi[⋆⋆]

Institute of Computer Science, University of Innsbruck, Austria
naohi.eguchi@uibk.ac.at

Abstract. Famous descriptive characterisations of P and PSPACE are restated in terms of the Cook-Nguyen style second order bounded arithmetic. We introduce an axiom of inductive definitions over second order bounded arithmetic. We show that P can be captured by the axiom of inflationary inductive definitions whereas PSPACE can be captured by the axiom of non-inflationary inductive definitions.

1 Introduction

The notion of inductive definitions is widely accepted in logic and mathematics. Although inductive definitions usually deal with infinite sets, we can also discuss about finitary inductive definitions. Suppose a finite set S and an *operator* $\Phi : \mathcal{P}(S) \to \mathcal{P}(S)$, a mapping over the power set $\mathcal{P}(S)$ of S. For a natural m, define a subset P_Φ^m of S inductively by $P_\Phi^0 = \emptyset$ and $P_\Phi^{m+1} = \Phi(P_\Phi^m)$. If the operator Φ is *inflationary*, i.e., $X \subseteq \Phi(X)$ for any $X \subseteq S$, then there exists a natural $k \leq |S|$ such that $P_\Phi^{k+1} = P_\Phi^k$, where $|S|$ denotes the number of elements of S, and hence the operator Φ has a fixed point. On the side of finite model theory, a famous descriptive characterisation of the class of P of polytime predicates was given by N. Immerman [6] and M. Y. Vardi [11]. It is shown that the class P can be captured by the first order predicate logic with fixed point predicates of first order definable inflationary operators. In case that the operator Φ is not inflationary, it is not in general possible to find a fixed point of Φ. One can however find two naturals $k, l \leq 2^{|S|}$ such that $l \neq 0$ and $P_\Phi^{k+l} = P_\Phi^k$. Based on this observation, it is shown that the class PSPACE of polyspace predicates can be captured by the first order predicate logic with fixed point predicates of first order definable (non-inflationary) operators, cf. [4]. On the side of bounded arithmetic, it was shown by S. Buss that P can be captured by a first order system S_2^1 whereas PSPACE can be captured by a second order extension U_2^1 of S_2^1, cf. [2]. An alternative way to characterise P was invented by D. Zambella [12]. As well as Buss' characterisation by S_2^1, P can be captured by a certain form of comprehension axiom over a weak second order system

---

[⋆] The first version: June 7, 2013. Last revision: July 8, 2013.

[⋆⋆] The author had been supported by *Philosophical frontiers in Reverse Mathematics* sponsored by the John Templeton Foundation til March 2013 and has been supported by JSPS posdoctoral fellowships for young scientists since April 2013.

of bounded arithmetic. A modern formalisation of Zambella's idea including further discussions can be found in the book [3] by S. Cook and P. Nguyen. More recently, A. Skelley in [8] extended this idea to a third order formulation of bounded arithmetic, capturing PSPACE as well as Buss' characterisation by U^1_2. On the other side, as discussed by K. Tanaka [9,10] and others, cf. [7], inductive definitions over infinite sets of naturals can be axiomatised over second order arithmetic the most elegantly. All these motivate us to introduce an axiom of inductive definitions over second order bounded arithmetic. Let us recall that for each $i \geq 0$ the class Σ^{B}_i of formulas is defined in the same way as the class Σ^1_i of second order formulas, but only *bounded quantifiers* are taken into account. We show that over a suitable base system the class P can be captured by the axiom of inductive definitions under Σ^{B}_0-definable inflationary operators (Corollary 5.9) whereas PSPACE can be captured by the axiom of inductive definitions under Σ^{B}_0-definable (non-inflationary) operators (Corollary 7.12). There is likely no direct connection, but this work is also partially motivated by the axiom AID of Alogtime inductive definitions introduced by T. Arai in [1].

After the preliminary section, in Section 3 we introduce a system Σ^{B}_0-IID of inductive definitions under Σ^{B}_0-definable inflationary operators and a system Σ^{B}_0-ID of inductive definitions under Σ^{B}_0-definable (non-inflationary) operators. In Section 4 we show that every polytime function can be defined in Σ^{B}_0-IID. In Section 5 we show that conversely the system Σ^{B}_0-IID can only define polytime functions by reducing Σ^{B}_0-IID to Zambella's system V^1. In Section 6 we show that every polyspace function can be defined in Σ^{B}_0-ID. In Section 7 we show that conversely the system Σ^{B}_0-ID can only define polyspace functions by reducing Σ^{B}_0-ID to Skelley's system W^1_1.

2 Preliminaries

The two-sorted first order vocabulary $\mathcal{L}^2_A$ consists of 0, 1, $+$, $\cdot$, $|\ |$, $=_1$, $=_2$, $\leq$ and $\in$. At the risk of confusion, we also call $\mathcal{L}^2_A$ the second order vocabulary of bounded arithmetic. Note that $=_1$ and $=_2$ respectively denote the first order and the second order equality, and $t =_1 s$ or $U =_2 V$ will be simply written as $t = s$ or $U = V$. First order elements $x, y, z, \dots$ denote natural numbers whereas seconder order elements $X, Y, Z, \dots$ denote binary strings. The formula of the form $t \in X$ is abbreviated as $X(t)$. Under a standard interpretation, $|X|$ denotes the length of the string X, and $X(i)$ holds if and only if the ith bit of X is 1. Let $\mathcal{L}$ be a vocabulary such that $\mathcal{L}^2_A \subseteq \mathcal{L}$. We follow a convention that for an $\mathcal{L}$-term t, a string variable X and a formula φ, $(\exists X \leq t)\varphi$ stands for $\exists X(|X| \leq t \wedge \varphi)$ and $(\forall X \leq t)\varphi$ stands for $\forall X(|X| \leq t \to \varphi)$. Further $(\exists \boldsymbol{x} \leq \boldsymbol{t})\varphi$ stands for $(\exists x_1 \leq t_1) \cdots (\exists x_k \leq t_k)\varphi$ if $\boldsymbol{x} = x_1, \dots, x_k$ and $\boldsymbol{t} = t_1, \dots, t_k$. We follow similar conventions for $(\forall \boldsymbol{x} \leq \boldsymbol{t})\varphi$, $(\exists \boldsymbol{X} \leq \boldsymbol{t})\varphi$ and $(\forall \boldsymbol{X} \leq \boldsymbol{t})\varphi$. A quantifier of the form $(Qx \leq t)$ or $(QX \leq t)$ is called a *bounded quantifier*. Specific classes $\Sigma^{\mathrm{B}}_i(\mathcal{L})$ and $\Pi^{\mathrm{B}}_i(\mathcal{L})$ $(0 \leq i)$ are defined by the following clauses.

1. $\Sigma^{\mathrm{B}}_0(\mathcal{L}) = \Pi^{\mathrm{B}}_0(\mathcal{L})$ is the set of $\mathcal{L}$-formulas whose quantifiers are bounded number ones only.

2. $\Sigma^{\mathrm{B}}_{i+1}(\mathcal{L})$ ($\Pi^{\mathrm{B}}_{i+1}(\mathcal{L})$ resp.) is the set of formulas of the form $(\exists \boldsymbol{X} \leq \boldsymbol{t})\varphi(\boldsymbol{X})$ ($(\forall \boldsymbol{X} \leq \boldsymbol{t})\varphi(\boldsymbol{X})$ resp.), where φ is a $\Pi^{\mathrm{B}}_{i}(\mathcal{L})$-formula (a $\Sigma^{\mathrm{B}}_{i}(\mathcal{L})$-formula resp.) and $\boldsymbol{t}$ is a sequence of $\mathcal{L}$-terms not involving any variables from $\boldsymbol{X}$.

Finally the class $\Delta^{\mathrm{B}}_{i}(\mathcal{L})$ is defined in the most natural way for each $i \geq 0$. We simply write Σ^{B}_{i} (Π^{B}_{i} resp.) to denote $\Sigma^{\mathrm{B}}_{i}(\mathcal{L}^2_A)$ ($\Pi^{\mathrm{B}}_{i}(\mathcal{L}^2_A)$ resp.) if no confusion likely arises. Let us recall that for each $i \geq 0$ the system V^i is axiomatised over $\mathcal{L}^2_A$ by the defining axioms for numerical and string function symbols in $\mathcal{L}^2_A$ (B1–B12, L1, L2 and SE, see [3, p. 96]) and the axiom (Σ^{B}_{i}-COMP) of comprehension for Σ^{B}_{i} formulas:

$$\forall x(\exists Y \leq x)(\forall i < x)[Y(i) \leftrightarrow \varphi(i)], \qquad (\Sigma^{\mathrm{B}}_{i}\text{-COMP})$$

where $\varphi \in \Sigma^{\mathrm{B}}_{i}$. We will use the following fact frequently.

Proposition 2.1 (Zambella [12]). (Cf. [3, p. 98, Corollary V.1.8]) *The axiom* (Σ^{B}_{i}-IND) *of induction for* Σ^{B}_{i} *formulas holds in* V^i.

Let $\mathcal{L}^2_A \subseteq \mathcal{L}$. For a string function f, a class Φ of $\mathcal{L}$-formulas and a system T over $\mathcal{L}$, we say f is Φ-definable in T if there exists an $\mathcal{L}$-formula $\varphi(\boldsymbol{X}, Y) \in \Phi$ such that

- φ does not involve free variables other than $\boldsymbol{X}$ nor Y,
- the graph $f(\boldsymbol{X}) = Y$ of f is expressed by $\varphi(\boldsymbol{X}, Y)$ under a standard interpretation as mentioned at the beginning of this section, and
- the sentence $\forall \boldsymbol{X} \exists ! Y \varphi(\boldsymbol{X}, Y)$ is provable in T.

Note that every function over natural numbers can be regarded as a string one by representing naturals in their binary expansion.

Proposition 2.2 (Zambella [12]). (Cf. [3, p. 135, Theorem VI.2.2]) *A function is polytime computable if and only if it is* Σ^{B}_{1}*-definable in* V^1.

3 Axiom of Inductive Definitions

In this section we introduce an axiom of inductive definitions. We work over a conservative extension of V^0. For the sake of readers' convenience we recall from Cook-Nguyen [3] several string functions, all of which have Σ^{B}_{0}-definable bit-graphs. We suppose a standard numerical paring function $\langle x, y \rangle = (x+y)(x+y+1) + 2y$. Clearly the paring function is definable in $\mathcal{L}^2_A$.

(*String encoding* [3, p. 114 Definition V.4.26]) The xth component $Z^{[x]}$ of a string Z is defined by the axiom $Z^{[x]}(i) \leftrightarrow i < |Z| \wedge Z(\langle x, i \rangle)$.

(*Encoding of bounded number sequences* [3, p. 115 Definition V.4.31]) The xth element $(Z)^x$ of the sequence encoded by Z is defined by the axiom

$$(Z)^x = y \leftrightarrow [y < |Z| \wedge Z(\langle x, y \rangle) \wedge (\forall z < y)\neg Z(\langle x, z \rangle)] \vee \\ [y = |Z| \wedge (\forall z < y)\neg Z(\langle x, z \rangle)].$$

(*String paring* [3, p. 243, Definition VIII.7.2]) The string function $\langle X, Y\rangle$ is defined by the axiom

$$\langle X_0, X_1\rangle(i) \leftrightarrow (\exists j \leq i)[(i = \langle 0, j\rangle \wedge X_0(j)) \vee (i = \langle 1, j\rangle \wedge X_1(j))].$$

Correspondingly, a pair of strings can be unpaired as $\langle Z_0, Z_1\rangle^{[i]} = Z_i$ $(i = 0, 1)$.

(*String constant, string successor, string addition* [3, p. 112, Example V.4.17]) The string constant $\emptyset$ is defined by the axiom $\emptyset(i) \leftrightarrow i < 0$. The string successor $S(X)$ is defined by the axiom

$$S(X)(i) \leftrightarrow i \leq |X| \wedge [X(i) \wedge (\exists j < i)\neg X(j)] \vee [\neg X(i) \wedge (\forall j < i)X(j)].$$

The string addition $X + Y$ is defined by the axiom

$$(X + Y)(i) \leftrightarrow (i < |X| + |Y| \wedge (X(i) \oplus Y(i) \oplus Carry(i, X, Y))),$$

where $\oplus$ denotes "exclusive or", i.e., $p \oplus q \equiv (p \wedge \neg q) \vee (\neg p \wedge q)$, and

$$Carry(i, X, Y) \leftrightarrow (\exists k < i)[X(k) \wedge Y(k) \wedge (\forall j < i)(k < j \rightarrow X(j) \vee Y(j)].$$

(*String ordering* [3, p. 219, Definition VIII.3.5]) The string relation $X < Y$ is defined by the axiom

$$\begin{aligned} X < Y \leftrightarrow {} & |X| \leq |Y| \wedge \\ & (\exists i \leq |Y|)[(\forall j \leq |Y|)(i < j \wedge X(j) \rightarrow Y(j)) \wedge Y(i) \wedge \neg X(i)]. \end{aligned}$$

We write $X \leq Y$ to denote $X = Y \vee X < Y$. It is known that if V^0 is augmented by adding a collection of Σ^{B}_0-defining axioms for string functions, then the resulting system is a conservative extension of V^0, cf. [3, p. 110, Corolalry V.4.14]. Hence we identify V^0 with the system resulting by augmenting V^0 by adding the Σ^{B}_0-defining axioms for those string functions and relations defined above.

Further we work over a slight extension of the vocabulary $\mathcal{L}^2_A$. For a formula $\varphi(i, X)$ let $P_\varphi(i, x, X)$ denote a fresh predicate symbol, where φ may contain free variables other than i and X. We write $\mathcal{L}^2_{\mathrm{ID}}$ to denote the vocabulary expanded by the new predicate P_φ for each φ. For a system T over a vocabulary $\mathcal{L}$ such that $\mathcal{L}^2_A \subseteq \mathcal{L}$ we write $T(\mathcal{L}^2_{\mathrm{ID}})$ to denote the conservative extension of T obtained by augmenting T with the expanded vocabulary $\mathcal{L}^2_{\mathrm{ID}}$. Now we introduce an *axiom of inductive definitions.*

Definition 3.1 (Axiom of Inductive Definitions). Let Φ be a class of formulas. Then the axiom schema (Φ-ID) of inductive definitions asserts that for any natural x there exist two strings U and V such that $|U|, |V| \leq x + 1$, $V \neq \emptyset$ fulfilling the following clauses, where $\varphi \in \Phi$.

1. $(\forall i < x)[P_\varphi(i, x, \emptyset) \leftrightarrow i < 0]$.
2. $(\forall X \leq x + 1)[X < U + V \rightarrow (\forall i < x)(P_\varphi(i, x, S(X)) \leftrightarrow \varphi(i, P^X_{\varphi,x}))]$, where $\varphi(i, P^X_{\varphi,x})$ denotes the result of replacing every occurrence of $Y(j)$ in $\varphi(i, Y)$ with $P_\varphi(j, x, X) \wedge j < x$.

3. $(\forall i < x)[P_\varphi(i, x, U + V) \leftrightarrow P_\varphi(i, x, U)]$.

We write (Φ-IID) for (Φ-ID) if additionally the formula $\varphi \in \Phi$ is *inflationary*, i.e., if $(\forall Y \leq x)(\forall i < x)[Y(i) \to \varphi(i, Y)]$ holds.

We write $P^X_{\varphi,x} = Y$ to denote $(\forall i < x)[P_\varphi(i, x, X) \leftrightarrow Y(i)]$. By definition, $P^X_{\varphi,x}$ denotes the string consisting of the first x bits of the string obtained by X-fold iteration of the operator defined by the formula φ (starting with the empty string).

Definition 3.2. Let Φ be a class of $\mathcal{L}^2_A$-formulas.

1. Φ-ID := $\mathrm{V}^0(\mathcal{L}^2_{\mathrm{ID}})$ + (Φ-ID).
2. Φ-IID := $\mathrm{V}^0(\mathcal{L}^2_{\mathrm{ID}})$ + (Φ-IID).

By definition the inclusion Φ-IID $\subseteq$ Φ-ID holds for any class Φ of $\mathcal{L}^2_A$-formulas. It is important to note that ($\Sigma^{\mathrm{B}}_i(\mathcal{L}^2_{\mathrm{ID}})$-COMP) is not allowed in $\mathrm{V}^i(\mathcal{L}^2_{\mathrm{ID}})$ for any $i \geq 0$, and hence $\forall x \forall X (\exists Y \leq x) P^X_{\varphi,x} = Y$ does not hold in $\mathrm{V}^0(\mathcal{L}^2_{\mathrm{ID}})$. The main theorem in this paper is stated as follows.

Theorem 3.3. *1. A function is polytime computable if and only if it is* Σ^{B}_1 $(\mathcal{L}^2_{\mathrm{ID}})$*-definable in* Σ^{B}_0-IID.
2. A function is polyspace computable if and only if it is $\Sigma^{\mathrm{B}}_1(\mathcal{L}^2_{\mathrm{ID}})$*-definable in* Σ^{B}_0-ID.

4 Defining P functions by inflationary inductive definitions

Theorem 4.1. *Every polytime function is* $\Sigma^{\mathrm{B}}_1(\mathcal{L}^2_{\mathrm{ID}})$*-definable in* Σ^{B}_0-IID.

Proof. Suppose that a function f is polytime computable. Assuming without loss of generality that f is a unary function such that $f(X)$ can be computed by a single-tape Turing machine M in a step bounded by a polynomial $p(|X|)$ in the binary length $|X|$ of an input X.

We can assume that each configuration of M on input X is encoded into a binary string whose length is exactly $q(|X|)$ for some polynomial q. The polynomial q can be found from information on the polynomial p since $|f(X)| \leq p(|X|)$ holds. Let the predicate Init_M denote the *initial* configuration of M and Next_M the *next* configuration of M. More precisely,

- $\mathsf{Init}_M(i, X)$ is true if and only if the ith bit of the binary string that encodes the initial configuration of M on input X is 1, and
- $\mathsf{Next}_M(i, X, Y)$ is true if and only if Y encodes a configuration of M on input X and the ith bit of the binary string that encodes the successor configuration of Y is 1. Note that $\mathsf{Next}_M(i, X, Y)$ never holds if Y does not encode a configuration of M, or if Y encodes the final configuration of M.

Careful readers will see that both Init and Next can be expressed by Σ_0^{B}-formulas. We define $\mathsf{MSP}(j, Y)$, the last j bits of a string Y, which is also known as the *most significant part* of Y, by

$$\mathsf{MSP}(j, Y)(i) \leftrightarrow i < j \wedge Y(|Y| \dot{-} j + i).$$

Let $\varphi(i, X, Y)$ denote the formula

$$i < |Y| + q(|X|) \wedge [Y(i) \vee \mathsf{Init}_M(i, X) \vee \mathsf{Next}_M(i \dot{-} |Y|, X, \mathsf{MSP}(q(|X|), Y))].$$

Clearly φ is a Σ_0^B-formula.

Now reason in Σ_0^{B}-IID. It is not difficult to see that $\varphi(i, X, Y)$ is inflationary with respect to Y. Hence, by the axiom (Σ_0^B-IID) of Σ_0^{B} inflationary inductive definitions, we can find two strings U and V such that $|U|, |V| \leq q(|X|) \cdot (p(|X|) + 1)$, $V \neq \emptyset$ and $P^{U+V}_{\varphi, q(|X|)\cdot(p(|X|)+1)} = P^{U}_{\varphi, q(|X|)\cdot(p(|X|)+1)}$. Hence the following $\Sigma_1^{\mathrm{B}}(\mathcal{L}^2_{\mathrm{ID}})$ formula $\psi_f(X, Y)$ holds.

$$\begin{aligned}(\exists U, V \leq q(|X|) \cdot (p(|X|) + 1))\ [V \neq \emptyset \wedge P^{U+V}_{\varphi, q(|X|)\cdot(p(|X|)+1)} = P^{U}_{\varphi, q(|X|)\cdot(p(|X|)+1)} \\ \wedge Y = \mathsf{Value}(\mathsf{MSP}(q(|X|), P^{U}_{\varphi, q(|X|)\cdot(p(|X|)+1)}))],\end{aligned}$$

where $\mathsf{Value}(Z)$ denotes the function Σ_0^{B}-definable in V^0 (depending on the underlying encoding) which extracts the value of the output from Z if Z encodes the final configuration of M. By the definition of φ, $\mathsf{MSP}(q(|X|), P^{U}_{\varphi, q(|X|)\cdot(p(|X|)+1)})$ encodes the final configuration of M, since in any terminating computation the same configuration does not occur more than once. Hence $\psi_f(X, Y)$ defines the graph $f(X) = Y$ of f. It is easy to see that $\forall X \exists Y \psi_f(X, Y)$ also holds. The uniqueness of Y such that $\psi_f(X, Y)$ can be shown accordingly, allowing us to conclude. $\square$

5 Reducing inflationary inductive definitions to V^1

In this section we show that every function $\Sigma_1^{\mathrm{B}}(\mathcal{L}^2_{\mathrm{ID}})$-definable in the system Σ_0^{B}-IID of Σ_0^{B} inflationary inductive definitions is polytime computable by reducing Σ_0^{B}-IID to the system V^1.

Notation. We write $x \dot{-} y$ to denote the *limited subtraction*: $x \dot{-} y = \max\{0, x - y\}$, and $\lfloor x \rfloor$ to denote the *devision* of x by 2: $\lfloor x \rfloor = \lfloor x/2 \rfloor$. We will write $x - y = z$ if $x \dot{-} y = z$ and $y \leq x$. We expand the notion of "Φ-definable in T" (presented on page 3) to those functions involving the numerical sort in addition to the string sort in an obvious way. Then it can be shown that both $x \dot{-} y$ and $\lfloor x \rfloor$ are Σ_0^{B}-definable in V^0, cf. [3, p. 60]. Further, though much harder to show, it can be also shown that a limited form of exponential, $Exp(x, y) = \min\{2^x, y\}$, is Σ_0^{B}-definable in V^0, cf. [3, p. 64].

Definition 5.1. *A function* $\mathsf{val}(x, X)$*, which denotes the numerical value of the string consisting of the last* x *bits of a string* X*, is defined by*

$$\begin{aligned} \mathsf{val}(x, \emptyset) &= 0, \ \textit{or otherwise}, \\ \mathsf{val}(0, X) &= 0, \\ \mathsf{val}(x+1, X) &= \begin{cases} \mathsf{val}(x, X) & \textit{if } |X| \leq x, \\ 2 \cdot \mathsf{val}(x, X) & \textit{if } x < |X| \ \& \ \neg X((|X| \dot{-} 1) \dot{-} x), \\ 2 \cdot \mathsf{val}(x, X) + 1 & \textit{if } x < |X| \ \& \ X((|X| \dot{-} 1) \dot{-} x). \end{cases} \end{aligned}$$

Lemma 5.2. *The function* $(x, X) \mapsto \mathsf{val}(x, X)$ *is* Δ_1^{B}*-definable in* V^1 *if* $x \leq |y|$ *for some* y*. More precisely, the relation* $\mathsf{val}(x, X) = z$ *can be expressed by a* Δ_1^{B} *formula* $\psi_{\mathsf{val}}(x, y, z, X)$ *if* $x \leq |y|$*, and the sentence* $\forall y (\forall x \leq |y|) \forall X \exists! z \, \psi_{\mathsf{val}}(x, y, z, X)$ *is provable in* V^1*.*

Proof. Let $\psi(x, z, X, Y)$ denote the formula expressing that $z = 0$ if $|X| = 0$, or otherwise $(Y)^0 = 0$, $(Y)^x = z$, and for all $j < x$,

- $|X| \leq j \to (Y)^{j+1} = (Y)^j$,
- $j < |X| \wedge \neg X(|X| \dot{-} j \dot{-} 1) \to (Y)^{j+1} = 2(Y)^j$, and
- $j < |X| \wedge X(|X| \dot{-} j \dot{-} 1) \to (Y)^{j+1} = 2(Y)^j + 1$.

Define $\psi_{\mathsf{val}}(x, y, z, X, Y)$ to be $(\exists Y \leq \langle x, 2y{+}1 \rangle{+}1) \psi(x, z, X, Y)$. Clearly ψ_{val} is a Σ_1^{B} formula expressing the relation $\mathsf{val}(x, X) = z$ in case $x \leq |y|$. Note that $2^{|y|} \leq 2y{+}1$ for all y. Hence if $x \leq |y|$, then $\mathsf{val}(x, X) \leq 2^x \leq 2^{|y|} \leq 2y{+}1$. Reason in V^1. One can show that if $x \leq |y|$, then $(\exists z \leq 2y{+}1)(\exists Y \leq \langle x, 2y{+}1 \rangle{+}1) \psi(x, z, X, Y)$ holds by induction on x. Accordingly the uniqueness of those z and Y above can be also shown. From the uniqueness of z and Y, $\mathsf{val}(x, X) = z$ is equivalent to a Π_1^{B} formula $(\forall u \leq 2y + 1)(\exists Y \leq \langle x, 2y + 1 \rangle + 1)[\psi(x, y, u, X, Y) \to u = z]$. Hence ψ_{val} is a Δ_1^{B} formula. $\square$

Lemma 5.3. *Let* $\varphi(x, X)$ *be a* Σ_0^{B} *formula. Then the relation* $(x, X, Y) \mapsto P_{\varphi, x}^X = Y$ *can be expressed by a* Δ_1^{B} *formula* $\psi_{P_\varphi}(x, y, X, Y)$ *if* $|X| \leq |y|$*. More precisely, corresponding to Definition 3.1.1 and 3.1.2,* ψ_{P_φ} *enjoys the following.*

1. $\psi_{P_\varphi}(x, y, \emptyset, \emptyset)$.
2. $(\forall X \leq x + 1)(|X| \leq |y| \to \forall Y, Z[\psi_{P_\varphi}(x, y, X, Y) \wedge \psi_{P_\varphi}(x, y, S(X), Z) \to (\forall i < x)(Z(i) \leftrightarrow \varphi(i, Y))])$.

Further the sentence $\forall x, y (\forall X \leq |y|)(\exists! Y \leq x) \psi_{P_\varphi}(x, y, X, Y)$ *is provable in* V^1*.*

Proof. Let $\psi(x, X, Y, Z)$ denote a formula which expresses that

- $(\forall j \leq \mathsf{val}(|y|, X)) |(Z)^j| \leq x$,
- $Z^{[0]} = \emptyset$, $Z^{[\mathsf{val}(|y|, X)]} = Y$, and
- $(\forall j < \mathsf{val}(|y|, X))(\forall i < x)[Z^{[j+1]}(i) \leftrightarrow \varphi(i, Z^{[j]})]$.

Define $\psi_{P_\varphi}(x,y,X,Y)$ to be $(\exists Z \le \langle \mathsf{val}(|y|,X),x\rangle+1)\psi(x,X,Y,Z)$. Then, since φ is a Σ^{B}_0 formula, ψ_{P_φ} is a Σ^{B}_1 formula expressing the relation $P^X_{\varphi,x}=Y$ if $|X|\le|y|$. Reason in V^1. On can show $|X|\le|y| \to (\exists Y\le x)\psi_{P_\varphi}(x,y,X,Y,Z)$ by induction on $\mathsf{val}(|y|,X)$. The uniqueness of such strings Y and Z can be also shown. Hence, as in the previous proof, thanks to the uniqueness of Y and Z, ψ_{P_φ} is a Δ^{B}_1 formula. $\square$

Definition 5.4. *1. A string function* $\mathsf{Ones}(y)$*, which denotes the string consisting only of* 1 *of length* y*, is defined by the axiom* $\mathsf{Ones}(y)(i)\leftrightarrow i<y$*.*

2. The string predecessor $P(X)$ *is by the axiom*

$$P(X)(i)\leftrightarrow i<|X|\wedge[(X(i)\wedge(\exists j<i)X(j))\vee(\neg X(i)\wedge(\forall j<i)\neg X(j))].$$

Lemma 5.5. *1. In* V^0*, if* $0<|X|$*, then* $S(P(X))=X$ *holds.*

2. In V^1*, if* $x<|y|$*, then the following holds.*

$$\mathsf{val}(|y|,S(\mathsf{Ones}(x)))=\mathsf{val}(|y|,\mathsf{Ones}(x))+1. \tag{1}$$

3. In V^1*, if* $0<|X|\le|y|$*, then* $\mathsf{val}(|y|,P(X))+1=\mathsf{val}(|y|,X)$ *holds.*

Proof. 1. We reason in V^0. Suppose $0<|X|$. Then $X(i)$ holds for some $i<|X|$. Since the axiom (Σ^{B}_i-MIN) of minimisation for Σ^{B}_i formulas holds in V^i, cf. [3, p. 98, Corollary V.1.8], there exists an element $i_0<|X|$ such that $X(i_0)$ and $(\forall j<i_0)\neg X(j)$ hold. Define a string Y with use of (Σ^{B}_0-COMP) by

$$|Y|\le|X| \quad\text{and}\quad (\forall i<|X|)[Y(i)\leftrightarrow(i_0<i\wedge X(i))\vee i<i_0]. \tag{2}$$

We show (i) $S(Y)=X$ and (ii) $P(X)=Y$. It is not difficult to see $|S(Y)|=|X|$ and $|P(X)|=|Y|$. For (i) suppose $i<|S(X)|$ and $S(X)(i)$. If $Y(i)$ and $(\exists j<i)\neg Y(j)$ hold, then $i_0<i$ and $X(i)$ hold by the definition of Y. If $\neg Y(i)$ and $(\forall j<i)Y(j)$ hold, then $i=i_0$ holds. By the choice of i_0, $X(i_0)$ and $(\forall j< i_0)\neg X(j)$, and hence $X(i)$ holds. The converse inclusion can be shown in the same way. For (ii) suppose $i<|P(X)|$ and $P(X)(i)$. If $X(i)$ and $(\exists j<i)X(j)$ hold, then $X(i)$ and $i_0<i$ by the choice of i_0, and hence $Y(i)$. If $\neg X(i)$ and $(\forall j<i)\neg X(j)$ hold, then $i<i_0$, and hence $Y(i)$ holds. The converse inclusion can be shown in the same way.

2. By Lemma 5.2, both $\mathsf{val}(|y|,S(\mathsf{Ones}(x)))$ and $\mathsf{val}(|y|,\mathsf{Ones}(x))$ can be defined in V^1. We reason in V^1. Suppose $x\le|y|$. Then $|\mathsf{val}(x,\mathsf{Ones}(z))|+1\le|\mathsf{val}(x,S(\mathsf{Ones}(z)))|\le x+1\le|y|$. We show that (1) holds by induction on x. In case $x=0$, $\mathsf{Ones}(x)=\emptyset$, and hence $\mathsf{val}(|y|,S(\mathsf{Ones}(x)))=\mathsf{val}(|y|,S(\emptyset))=1=\mathsf{val}(|y|,\emptyset)+1$. For the induction step, assume by IH (Induction Hypothesis) that (1) holds. Then $\mathsf{val}(|y|,S(\mathsf{Ones}(x+1)))=2\cdot\mathsf{val}(|y|,S(\mathsf{Ones}(x)))=2\{\mathsf{val}(|y|,\mathsf{Ones}(x))+1\}=(2\cdot\mathsf{val}(|y|,\mathsf{Ones}(x))+1)+1=\mathsf{val}(|y|,\mathsf{Ones}(x+1))+1$.

3. We reason in V^1. Suppose $0<|X|\le|y|$. Choose an element $i_0<X$ as above and define a string Y in the same way as (2). Then $Y=P(X)$ as we showed above. By the choice of i_0, for any $j<|X|$, if $i_0<j$, then $X(j)\leftrightarrow Y(j)$ holds. Hence it suffices to show that $\mathsf{val}(|y|,\mathsf{Ones}(i_0))+1=\mathsf{val}(|y|,S(\mathsf{Ones}(i_0)))$ holds, but this follows from Lemma 5.5.2. $\square$

Theorem 5.6. *Let* $\varphi \in \Sigma^{\mathrm{B}}_0$*. In* V^1*, if* φ *is inflationary, then there exists a string* U *such that* $U \leq \mathsf{Ones}(|x|)$ *and the following holds.*

$$\forall Y, Z[\psi_{P_\varphi}(x, 2x, S(U), Y) \wedge \psi_{P_\varphi}(x, 2x, U, Z) \to (\forall i < x)(Y(i) \leftrightarrow Z(i))]. \quad (3)$$

Proof. Let us recall a numerical function $numones(x, X)$ which denotes the number of elements of X, or equivalently the number of 1 occurring in the string X, not exceeding x (See [3, p. 149]). It can be shown that $numones$ is Σ^{B}_1-definable in V^1 (See [3, p. 149]). As we observed in the proof of Lemma 5.2 or Lemma 5.3, $numones$ is even Δ^{B}_1-definable in V^1.

Let $\varphi \in \Sigma^{\mathrm{B}}_0$. Reason in V^1. Suppose that φ is inflationary, i.e., $(\forall Y \leq x)(\forall j < x)[Y(i) \to \varphi(i, Y)]$ holds. We show by contradiction the existence of a string U such that $U \leq \mathsf{Ones}(|x|)$ and the condition (3) holds. Since $|S(\mathsf{Ones}(|x|))| = |x| + 1 = |2x|$, by Lemma 5.3 $(\exists! Y \leq x) P^X_{\varphi,x} = Y$ holds for any $X \leq S(\mathsf{Ones}(|x|))$. Hence it suffices to find a string U such that $U \leq \mathsf{Ones}(|x|)$ and $P^{S(U)}_{\varphi,x} = P^U_{\varphi,x}$. Assume that such a string U does not exist. Then for any $X \leq \mathsf{Ones}(|x|)$ there exists $i < x$ such that $P^{S(X)}_{\varphi,x}(i)$ but $\neg P^X_{\varphi,x}(i)$. This means that $numones(x, P^X_{\varphi,x}) < numones(x, P^{S(X)}_{\varphi,x})$ holds for any $X \leq \mathsf{Ones}(|x|)$.

Claim. If $X \leq S(\mathsf{Ones}(|x|))$, then $\mathsf{val}(|x| + 1, X) \leq numones(x, P^X_{\varphi,x})$ holds.

We show the claim by induction on $\mathsf{val}(|x|+1, X)$. The base case that $\mathsf{val}(|x|+1, X) = 0$ is clear. For the induction step, consider the case $\mathsf{val}(|x| + 1, X) > 0$. In this case, $0 < |X|$, and hence by Lemma 5.5.3 $\mathsf{val}(|x| + 1, P(X)) + 1 = \mathsf{val}(|x|+1, X)$ holds. Hence by IH $\mathsf{val}(|x|+1, P(X)) \leq numones(x, P^{P(X)}_{\varphi,x})$ holds. By Lemma 5.5.1, $S(P(X)) = X$ holds. This together with IH yields $\mathsf{val}(|x| + 1, X) = \mathsf{val}(|x| + 1, P(X)) + 1 \leq numones(x, P^X_{\varphi,x})$ since $numones(x, P^{P(X)}_{\varphi,x}) < numones(x, P^{S(P(X))}_{\varphi,x}) = numones(x, P^X_{\varphi,x})$.

By the claim $\mathsf{val}(|x| + 1, S(\mathsf{Ones}(|x|))) \leq numones(x, P^{S(\mathsf{Ones}(|x|))}_{\varphi,x})$ holds. On the other hand $x < \mathsf{val}(|x| + 1, S(\mathsf{Ones}(|x|)))$ since $|x| < |x| + 1 = |S(\mathsf{Ones}(|x|))|$. Therefore $x < numones(x, P^{S(\mathsf{Ones}(|x|))}_{\varphi,x})$ holds, but this contradicts the definition of $numones$. □

Theorem 5.7. *Suppose* $1 \leq i$*. If* $\Sigma^{\mathrm{B}}_i(\mathcal{L}^2_{\mathrm{ID}})$ *formula* ψ *is provable in* Σ^{B}_0-IID*, then there exists a* Σ^{B}_i *formula* ψ' *provable in* V^1 *and provably equivalent to* ψ *in* $\mathrm{V}^1(\mathcal{L}^2_{\mathrm{ID}})$*.*

Proof. This theorem can be shown by an induction argument on the length a formal Σ^{B}_0-IID-proof resulting in ψ. We only discuss about the axiom (Σ^{B}_0-IID) of Σ^{B}_0 inflationary inductive definitions and kindly refer details to readers. One can see that any instance of (Σ^{B}_0-IID) is a Σ^{B}_2 formula (with a free variable x). Suppose a Σ^{B}_0 formula φ. We reason in V^1. Fix a natural x arbitrarily. Then, since $S(X) = X + S(\emptyset)$, Theorem 5.6 yields two strings U and V such that $|U|, |V| \leq |x|$, $V = \emptyset$, $|U + V| = |x| + 1 = |2x|$, and the following clauses hold corresponding to Definition 3.1.1–3.1.3.

1. $\psi_{P_\varphi}(x, 2x, \emptyset, \emptyset)$.
2. $(\forall X \leq x+1)(|X| \leq |x| \to \forall Y, Z[\psi_{P_\varphi}(x, 2x, X, Y) \wedge \psi_{P_\varphi}(x, 2x, S(X), Z) \to (\forall i < x)(Z(i) \leftrightarrow \varphi(i, Y))])$.
3. $\forall Y, Z[\psi_{P_\varphi}(x, 2x, U+V, Y) \wedge \psi_{P_\varphi}(x, 2x, U, Z) \to (\forall i < x)(Y(i) \leftrightarrow Z(i))]$.

One can check that in $\mathrm{V}^1(\mathcal{L}^2_{\mathrm{ID}})$ this statement is provably equivalent to the instance of (Σ^{B}_0-IID) in case φ. Further from Lemma 5.3 the unbounded universal quantifiers $\forall Y, Z$ in clause 2 and 3 can be replaced with the bounded one $(\forall Y, Z \leq x)$, hence the formula expressing the above statement is a Σ^{B}_2 formula as well as (Σ^{B}_0-IID). □

Note that Theorem 5.7 does not hold in case $i = 0$, since a $\Sigma^{\mathrm{B}}_0(\mathcal{L}^2_{\mathrm{ID}})$ formula of the form $P_\varphi(i, x, X)$ will be expressed only by a Σ^{B}_1 formula of the form $|x|+1 < |X| \vee x \leq i \vee (\exists Y \leq x)[\psi_{P_\varphi}(x, 2x, X, Y) \wedge Y(i)]$, or equivalently by a Π^{B}_1 formula of the form $|x|+1 < |X| \vee x \leq i \vee (\forall Y \leq x)[\psi_{P_\varphi}(x, 2x, X, Y) \to Y(i)]$.

Corollary 5.8. *Every function* $\Sigma^{\mathrm{B}}_1(\mathcal{L}^2_{\mathrm{ID}})$*-definable in* Σ^{B}_0-IID *is polytime computable.*

Proof. Suppose that a $\Sigma^{\mathrm{B}}_1(\mathcal{L}^2_{\mathrm{ID}})$ sentence ψ is provable in Σ^{B}_0-ID. Then by Theorem 5.7 we can find a Σ^{B}_1 sentence ψ' provable in V^1 and provably equivalent to ψ in $\mathrm{V}^1(\mathcal{L}^2_{\mathrm{ID}})$. In particular ψ and ψ' are equivalent under the underlying standard interpretation. Hence every function $\Sigma^{\mathrm{B}}_1(\mathcal{L}^2_{\mathrm{ID}})$-definable in Σ^{B}_0-IID is Σ^{B}_1-definable in V^1. Now employing Proposition 2.2 enables us to conclude. □

Corollary 5.9. *A predicate belongs to* P *if and only if it is* $\Delta^{\mathrm{B}}_1(\mathcal{L}^2_{\mathrm{ID}})$*-definable in* Σ^{B}_0-IID.

6 Defining PSPACE functions by non-inflationary inductive definitions

Theorem 6.1. *Every polyspace computable function is* $\Sigma^B_1(\mathcal{L}^2_{\mathrm{ID}})$*-definable in* Σ^B_0-ID.

Proof. The theorem can be shown in a similar manner as Theorem 4.1. Suppose that a function f is polyspace computable. As in the proof of Theorem 4.1 we can assume that f is a unary function such that $f(X)$ can be computed by a single-tape Turing machine M using a number of cells bounded by a polynomial $p(|X|)$ in $|X|$. Assuming a standard encoding of configurations of M into binary strings, the binary length of every configuration is exactly $q(|X|)$ for some polynomial q. Let Init_M denote the predicate defined on page 5. A new predicate $\mathsf{Next}'_M(i, X, Y)$ denotes the successor configuration of Y, but in contrast to Next_M, $\mathsf{Next}'_M(i, X, Y)$ does not change if Y encodes the final configuration. More precisely, if Y encodes the final configuration, then $(\forall i < q(|X|))(\mathsf{Next}'_M(i, X, Y) \leftrightarrow Y(i))$ holds. In contrast to the definition of φ on page 6, let $\varphi(i, X, Y)$ denote the formula

$$i < q(|X|) \wedge [\mathsf{Init}_M(i, X) \vee \mathsf{Next}'(i, X, Y)].$$

It is not difficult to convince ourselves that φ is a Σ_0^{B} formula. Hence, reasoning in Σ_0^{B}-ID, by the axiom ($\Sigma_0^{\mathcal{B}}$-ID) of Σ_0^{B} inductive definitions, we can find two strings U and V such that $|U|, |V| \leq q(|X|) + 1$, $V \neq \emptyset$ and $P^{U+V}_{\varphi,q(|X|)+1} = P^{U}_{\varphi,q(|X|)+1}$ hold. Hence the following $\Sigma_1^{\mathrm{B}}(\mathcal{L}^2_{\mathrm{ID}})$ formula $\psi_f(X, Y)$ holds.

$$\begin{aligned}(\exists U, V \leq q(|X|) + 1)\ [V \neq \emptyset \wedge P^{U+V}_{\varphi,q(|X|)+1} = P^{U}_{\varphi,q(|X|)+1} \wedge \\ Y = \mathsf{Value}(P^{U}_{\varphi,q(|X|)+1})],\end{aligned}$$

where $\mathsf{Value}(Z)$ denotes the extraction function Σ_0^{B}-definable in V^0 as in the proof of Theorem 4.1. As we observed, $P^{U}_{\varphi,q(|X|)+1}$ encodes the final configuration of M. Hence $\psi_f(X, Y)$ defines the graph $f(X) = Y$ of f. Now it is clear that $\forall X \exists Y \psi_f(X, Y)$ holds. The uniqueness of Y follows accordingly, allowing us to conclude. □

7 Reducing non-inflationary inductive definitions to $\mathbf{W}_1^1$

In this section we show that every function $\Sigma_1^{\mathrm{B}}(\mathcal{L}^2_{\mathrm{ID}})$-definable in the system Σ_0^{B}-ID of Σ_0^{B} inductive definitions is polyspace computable by reducing Σ_0^{B}-ID to a third order system W_1^1 of bounded arithmetic which was introduced by A. Skelley in [8]. The third order vocabulary $\mathcal{L}^3_A$ is defined augmenting the second order vocabulary $\mathcal{L}^2_A$ by the third order membership relation $\in_3$. As in the case of the second order membership, the formula of the form $Y \in_3 \mathcal{X}$ is abbreviated as $\mathcal{X}(Y)$. Third order elements $\mathcal{X}, \mathcal{Y}, \mathcal{Z}, \ldots$ would denote *hyper* strings, i.e., $\mathcal{X}(Y)$ holds if and only if the Yth bit of $\mathcal{X}$ is 1. Classes $\Sigma_i^{\mathcal{B}}$, $\Pi_i^{\mathcal{B}}$ and $\Delta_i^{\mathcal{B}}$ $(0 \leq i)$ are defined in the same manner as Σ_i^{B}, Π_i^{B} and Δ_i^{B} but third order quantifiers are taken into account instead of second order ones. For instance, $\Sigma_0^{\mathcal{B}} = \bigcup_{0 \leq i} \Sigma_i^{\mathrm{B}}(\mathcal{L}^3_A)$, and a $\Sigma_1^{\mathcal{B}}$ formula is of the form $\exists \mathcal{X} \psi(\mathcal{X})$, where no third order quantifier appears in ψ. For a class Φ of $\mathcal{L}^3_A$-formulas, the axiom of (Φ-3COMP) is defined by

$$\forall x \exists \mathcal{Z} (\forall Y \leq x)[\mathcal{Z}(Y) \leftrightarrow \varphi(Y)], \qquad (\Phi\text{-3COMP})$$

where $\varphi \in \Phi$. The system W_1^1 consists of the basic axioms of second order bounded arithmetic (B1–B12, L1, L2 and SE, [3, p. 96]), ($\Sigma_1^{\mathcal{B}}$-IND), ($\Sigma_0^{\mathcal{B}}$-COMP) and $\Sigma_0^{\mathcal{B}}$-3COMP.

Proposition 7.1 (Skelley [8]). *A function is polyspace computable if and only if it is $\Sigma_1^{\mathcal{B}}$-definable in W_1^1.*

Remark 7.2. In the original definition of W_1^1 presented in [8], the axiom (IND) of induction is allowed only for a class $\forall^2\Sigma_1^{\mathcal{B}}$ of formulas, which is slightly more restrictive than $\Sigma_1^{\mathcal{B}}$. However it can be shown that every $\Sigma_1^{\mathcal{B}}$ formula is provably equivalent to a $\forall^2\Sigma_1^{\mathcal{B}}$ formula in W_1^1 (See [8, Theorem 2 and Cororally 3]).

We show that even a stronger form of the axiom of Σ_0^{B} inductive definitions holds in W_1^1.

Definition 7.3 (Axiom of Relativised Inductive Definitions). We assume a new predicate symbol $P_\varphi(i,x,X,Y)$ instead of $P_\varphi(i,x,X)$ for each φ. Then a relativised form of the axiom of inductive definitions asserts that for any natural x and for any string Y such that $|Y| \leq x$ there exist two strings U and V such that $|U|, |V| \leq x+1$, $V \neq 0$ fulfilling the following clauses, where $\varphi \in \Phi$.

1. $(\forall i < x)[P_\varphi(i,x,\emptyset,Y) \leftrightarrow Y(i)]$.
2. $(\forall X \leq x+1)[X < U+V \to (\forall i < x)(P_\varphi(i,x,S(X),Y) \leftrightarrow \varphi(i, P^X_{\varphi,x}[Y]))]$, where $\varphi(i, P^X_{\varphi,x}[Y])$ denotes the result of replacing every occurrence of $X(j)$ in $\varphi(i,X)$ with $P_\varphi(j,x,X,Y) \wedge j < x$.
3. $(\forall i < x)(P_\varphi(i,x,U+V,Y) \leftrightarrow P_\varphi(i,x,U,Y))$.

As in the case of the predicate $P_\varphi(i,x,X)$, we write $P^X_{\varphi,x}[Y] = Z$ instead of $(\forall i < x)(P_\varphi(i,x,X,Y) \leftrightarrow Z(i))$. Apparently the axiom of relativised inductive definitions implies the original axiom of inductive definitions.

Definition 7.4. *1. The* complementary string Y^{C}_x *of a string Y of length x is defined by the axiom $Y^{\mathrm{C}}_x(i) \leftrightarrow i < x \wedge \neg Y(i)$.*
2. The string subtraction $X \mathbin{\dot{-}} Y$ *is defined by the axiom*

$$(X \mathbin{\dot{-}} Y)(i) \leftrightarrow (X \leq Y \wedge i < 0) \vee (Y < X \wedge i < |X| \wedge (X + S(Y^{\mathrm{C}}_{|X|}))(i)).$$

It can be shown that in V^0, if $|Y| \leq x$, then $Y + Y^{\mathrm{C}}_x = \mathsf{Ones}(x)$, and hence $Y + S(Y^{\mathrm{C}}_x) = S(\mathsf{Ones}(x))$ holds. Thus one can show that $|(X+Y) \mathbin{\dot{-}} Y| = |X|$ and, for any $i < |X|$, $[(X+Y) \mathbin{\dot{-}} Y](i) \leftrightarrow [X + S(\mathsf{Ones}(|X+Y|))](i) \leftrightarrow X(i)$, concluding $(X+Y) \mathbin{\dot{-}} Y = X$.

Lemma 7.5. *Let $\varphi(x,X)$ be a Σ^{B}_0 formula. Then the relation $(x,y,X,Y,Z) \mapsto P^X_{\varphi,x}[Y] = Z$ can be expressed by a $\Delta^{\mathcal{B}}_1$ formula $\psi_{P_\varphi}(x,X,Y,Z)$ if $|X|, |Y| \leq y$ in the same sense as in Lemma 5.3. Further the sentence $\forall x, y (\forall X \leq y)(\forall Y \leq x)(\exists! Z \leq x)\psi_{P_\varphi}(x,y,X,Y,Z)$ is provable in W^1_1.*

Notation. We define a string function $(\mathcal{Z})^X$, which denotes the Xth component of a hyper string $\mathcal{Z}$, by the axiom $(\mathcal{Z})^X = Y \leftrightarrow \mathcal{Z}(\langle X, Y \rangle)$. For a hyper string $\mathcal{Z}$ we write $\exists! \mathcal{Z} \leq x$ to refer to the uniqueness up to elements of length not exceeding x, i.e., $(\exists! \mathcal{Z} \leq x)\psi(\mathcal{Z})$ denotes $\exists \mathcal{Z} \psi(\mathcal{Z})$ and additionally,

$$\forall \mathcal{Z}_0, \mathcal{Z}_1 [\psi(\mathcal{Z}_0) \wedge \psi(\mathcal{Z}_1) \to (\forall Y \leq x)(\mathcal{Z}_0(Y) \leftrightarrow \mathcal{Z}_1(Y))]. \tag{4}$$

Proof. Let $\psi(x,y,X,Y,Z,\mathcal{Z})$ denote the $\Sigma^{\mathcal{B}}_0$ formula expressing

- $(\forall U \leq y)(U \leq X \to |(\mathcal{Z})^U| \leq x)$,
- $(\mathcal{Z})^\emptyset = Y$, $(\mathcal{Z})^X = Z$, and
- $(\forall U \leq y)(U < X \to (\forall i < x)[(\mathcal{Z})^{S(U)}(i) \leftrightarrow \varphi(i, (\mathcal{Z})^U)])$.

By the definition of ψ, the relation $P^X_{\varphi,x}[Y] = Z$ is expressed by the $\Sigma^{\mathcal{B}}_1$ formula $\exists \mathcal{Z} \psi(x,y,X,Y,Z,\mathcal{Z})$ if $|X| \leq y$. It suffices to show that $(\forall Y \leq x)(\exists! Z \leq x)(\exists! \mathcal{Z} \leq \langle |X|, x \rangle)\ \psi(x,X,Y,Z,\mathcal{Z})$ hols in W^1_1.

Reason in W^1_1. We only show the existence of such a string Z and a hyper string $\mathcal{Z}$. The uniqueness in the sense of (4) can be shown accordingly. We derive by induction on $|X|$ the $\Sigma^{\mathcal{B}}_1$ formula $(\forall Y \le x)(\exists Z \le x)\exists \mathcal{Z}\psi(x, X, Y, Z, \mathcal{Z})$. The argument is based on a standard "divide-and-conquer method". In the base case, $|X| = 0$, i.e., $X = \emptyset$, and hence the assertion is clear. The case that $|X| = 1$, i.e., $X = S(\emptyset)$, is also clear. Suppose that $|X| > 1$. Then we can find two strings X_0 and X_1 such that $|X_0| = |X_1| = |X| - 1$ and $X = X_0 + X_1$. Fix a string Y so that $|Y| \le x$. Then by IH we can find a string Z_0 and a hyper string $\mathcal{Z}_0$ such that $|Z_0| \le x$ and $\psi(x, X_0, Y, Z_0, \mathcal{Z}_0)$ hold. Since $|Z_0| \le x$, another application of IH yields Z_1 and $\mathcal{Z}_1$ such that $|Z_0| \le x$ and $\psi(x, X_1, Z_0, Z_1, \mathcal{Z}_1)$ hold. Define a hyper string $\mathcal{Z}$ with use of ($\Sigma^{\mathcal{B}}_0$-3COMP) by

$$(\forall U \le \langle |X|, x\rangle)[\mathcal{Z}(U) \leftrightarrow (U^{[0]} \le X_0 \wedge (\mathcal{Z}_0)^{U^{[0]}} = U^{[1]}) \vee \\ (X_0 < U^{[0]} \wedge (\mathcal{Z}_0)^{U^{[0]} \dot{-} X_0} = U^{[1]})]. \tag{5}$$

Intuitively $\mathcal{Z}$ denotes the concatenation $\mathcal{Z}_0 {}^\frown \mathcal{Z}_1$, the hyper string $\mathcal{Z}_0$ followed by $\mathcal{Z}_1$. Then by definition $\psi(x, X, Y, Z_1, \mathcal{Z})$ holds. Due to the uniqueness of the string Z and the hyper string $\mathcal{Z}$, the $\Sigma^{\mathcal{B}}_1$ formula $\exists \mathcal{Z}\psi(x, y, X, Y, Z, \mathcal{Z})$ is equivalent to the $\Pi^{\mathcal{B}}_1$ formula $(\forall V \le x)(\forall \mathcal{Z} \le \langle |X|, x\rangle)(\psi(x, X, Y, V, \mathcal{Z}) \to V = Z)$, and hence is also a $\Delta^{\mathcal{B}}_1$ formula. □

Lemma 7.6. *The following holds in* W^1_1.

$$\forall x, y(\forall X \le y)(\forall Y \le y)(\forall Z \le x)(|Y + X| \le y \to P^X_{\varphi,x}[P^Y_{\varphi,x}[Z]] = P^{Y+X}_{\varphi,x}[Z]).$$

Proof. By the previous lemma the relation $P^X_{\varphi,x}[P^Y_{\varphi,x}[Z]] = P^{Y+X}_{\varphi,x}[Z]$ can be expressed by a $\Delta^{\mathcal{B}}_1$ formula if $|X|, |Y| \le y$. Reason in W^1_1. We show that

$$|X| \le y \to (\forall Y \le y)(\forall Z \le x)(|Y + X| \le y \to P^X_{\varphi,x}[P^Y_{\varphi,x}[Z]] = P^{Y+X}_{\varphi,x}[Z])$$

holds by induction on $|X|$. The base case that $|X| = 0$ or $|X| = 1$ is clear. Suppose $|X| > 0$. Then we can find two strings X_0 and X_1 such that $|X_0| = |X_1| = |X| - 1$ and $X_0 + X_1 = X$. Fix a string Z so that $|Z| \le x$. Since $|X_1| = |X_0| < |X| \le y$ and $|X_0 + X_1| = |X| \le y$, IH yields $P^{X_0}_{\varphi,x}[P^{X_1}_{\varphi,x}[Z]] = P^{X_0+X_1}_{\varphi,x}[Z]$. Hence

$$P^Y_{\varphi,x}[P^X_{\varphi,x}[Z]] = P^Y_{\varphi,x}[P^{X_0}_{\varphi,x}[P^{X_1}_{\varphi,x}[Z]]]. \tag{6}$$

On the other hand, since $|X_0| \le y$, $|Y + X_0| \le |Y + X| \le y$ and $|P^{X_1}_{\varphi,x}[Z]| \le x$, another application of IH yields

$$P^Y_{\varphi,x}[P^{X_0}_{\varphi,x}[P^{X_1}_{\varphi,x}[Z]]] = P^{Y+X_0}_{\varphi,x}[P^{X_1}_{\varphi,x}[Z]]. \tag{7}$$

Farther, since $|Y + X_0| \le y$ and $|X_1| \le |X| \le x$, the final application of IH yields

$$P^{Y+X_0}_{\varphi,x}[P^{X_1}_{\varphi,x}[Z]] = P^{Y+X_0+X_1}_{\varphi,x}[Z] = P^{Y+X}_{\varphi,x}[Z]. \tag{8}$$

Combining equation (6), (7) and (8) allows us to conclude. □

Definition 7.7. *A string function* $\mathsf{numones}^3[Y](X, \mathcal{X})$*, which counts the number of elements of* $\mathcal{X}$ *(starting with* Y*) such that* $\leq X$*, is defined by*

$$\mathsf{numones}^3[Y](\emptyset, \mathcal{X}) = Y,$$

$$\mathsf{numones}^3[Y](S(X), \mathcal{X}) = \begin{cases} S(\mathsf{numones}^3[Y](X, \mathcal{X})) & \textit{if } \mathcal{X}(X) \textit{ holds,} \\ \mathsf{numones}^3[Y](X, \mathcal{X}) & \textit{if } \neg\mathcal{X}(X) \textit{ holds.} \end{cases}$$

Lemma 7.8. *The function* $\mathsf{numones}^3$ *is* $\Delta_1^{\mathcal{B}}$*-definable in* W_1^1*.*

Proof. Let $\psi_{\mathsf{numones}^3}(X, Y, Z, \mathcal{X}, \mathcal{Y})$ denote the $\Sigma_0^{\mathcal{B}}$ formula expressing

- $Z \leq Y + X$,
- $(\mathcal{Y})^{\emptyset} = Y$,
- $(\mathcal{Y})^{X} = Z$,
- $(\forall U \leq |X|)[U < X \wedge \mathcal{X}(U) \rightarrow (\mathcal{Y})^{S(U)} = S((\mathcal{Y})^{U})]$, and
- $(\forall U \leq |X|)[U < X \wedge \neg\mathcal{X}(U) \rightarrow (\mathcal{Y})^{S(U)} = (\mathcal{Y})^{U}]$.

Then by definition the $\Sigma_1^{\mathcal{B}}$ formula $\exists\mathcal{Y}\psi_{\mathsf{numones}^3}(X, Y, Z, \mathcal{X}, \mathcal{Y})$ defines the graph $\mathsf{numones}^3[Y](X, \mathcal{X}) = Z$ of $\mathsf{numones}^3$. We show that if $|X| \leq x$, then

$$(\forall Y \leq x)[|Y + X| \leq x \rightarrow (\exists! Z \leq x)(\exists! \mathcal{Y} \leq \langle |X|, x\rangle)\psi_{\mathsf{numones}^3}(X, Y, Z, \mathcal{X}, \mathcal{Y})]$$

holds in W_1^1. Reason in W_1^1. Given x, we only show the existence of such a string Z and a hyper string $\mathcal{Y}$ by induction on $|X|$. The uniqueness can be shown in a similar manner. Fix x and Y so that $|Y| \leq x$ and $|Y + X| \leq x$. In case that $|X| = 0$, i.e., $X = \emptyset$, define $\mathcal{Y}$ by

$$(\forall U \leq \langle 0, x\rangle)[\mathcal{Y}(U) \leftrightarrow (U = \langle \emptyset, Y\rangle)].$$

Then $|Y| \leq x$, $Y \leq Y + \emptyset$ and $\psi_{\mathsf{numones}^3}(\emptyset, Y, Y, \mathcal{X}, \mathcal{Y})$ hold. In the case that $|X| = 1$, i.e., $X = S(\emptyset)$, define $\mathcal{Y}$ by

$$\begin{aligned}(\forall U \leq \langle 1, x\rangle)[\mathcal{Y}(U) \leftrightarrow U = \langle \emptyset, Z\rangle \vee {} & (\mathcal{X}(\emptyset) \wedge U = \langle S(\emptyset), S(Y)\rangle) \wedge \\ & (\neg\mathcal{X}(\emptyset) \wedge U = \langle S(\emptyset), Y\rangle)].\end{aligned}$$

Clearly $|(\mathcal{Y})^{S(\emptyset)}| \leq |S(Y)| = |Y + S(\emptyset)|$, $(\mathcal{Y})^{S(\emptyset)} \leq S(Y) = Y + S(\emptyset)$ and $\psi_{\mathsf{numones}^3}(S(\emptyset), (\mathcal{Y})^{S(\emptyset)}, Y, \mathcal{X}, \mathcal{Y})$ hold. For the induction step, suppose $|X| > 1$. Then there exist strings X_0 and X_1 such that $|X_0| = |X_1| = |X| - 1$ and $X_0 + X_1 = X$. By assumption $|Y + X_0| \leq |Y + X| \leq x$. Hence IH yields a string Z_0 and a hyper string $\mathcal{Y}_0$ such that $|Z_0| \leq x$ and $\psi_{\mathsf{numones}^3}(X_0, Y_0, Z_0, \mathcal{X}, \mathcal{Y}_0)$ hold. In particular $Z_0 \leq Y + X_0$ holds. This implies $|Z_0 + X_1| \leq |Y + X_0 + X_1| = |Y + X| \leq x$. Thus another application of IH yields Z_1 and $\mathcal{Y}_1$ such that $|Z_1| \leq x$ and $\psi_{\mathsf{numones}^3}(X_1, Z_0, Z_1, \mathcal{X}, \mathcal{Y}_1)$ hold. Define $\mathcal{Y}$ in the same way as (5) in the proof of Lemma 7.5, i.e., $\mathcal{Y} = \mathcal{Y}_0{}^\frown\mathcal{Y}_1$. It is not difficult to see that $\psi_{\mathsf{numones}^3}(X, Y, Z_1, \mathcal{X}, \mathcal{Y})$ holds. Thanks to the uniqueness of Z and $\mathcal{Y}$, one can see that $\exists\mathcal{Y}\psi_{\mathsf{numones}^3}(X, Y, Z, \mathcal{X}, \mathcal{Y})$ is a $\Delta_1^{\mathcal{B}}$ formula. $\square$

Lemma 7.9. *The axiom* ($\Sigma_1^{\mathcal{B}}$-3COMP) *of third order comprehension for* $\Sigma_1^{\mathcal{B}}$ *formulas holds in* W_1^1*.*

One will recall that the V^1 can be axiomatised by (Σ_0^{B}-COMP) and (Σ_1^{B}-IND) instead of (Σ_1^{B}-COMP), cf. [3, p. 149, Lemma VI.4.8]. Lemma 7.9 can be shown with the same idea as the proof of this fact. For the sake of completeness, we give a proof in the appendix.

Theorem 7.10. *The axiom* ($\Sigma_0^{\mathcal{B}}$-ID) *of* Σ_0^{B} *inductive definitions holds in* W_1^1 *in the same sense as in Theorem 5.6.*

Proof. Instead of showing that the axiom (Σ_0^{B}-ID) holds in W_1^1, we show that even the axiom of relativised Σ_0^{B} inductive definitions holds in W_1^1. Let $\varphi \in \Sigma_0^{\mathrm{B}}$. We reason in W_1^1. Fix x arbitrarily. Given X and Y, we define a hyper string $\mathcal{P}^X[Y]$ with use of ($\Sigma_1^{\mathcal{B}}$-3COMP) by

$$(\forall Z \leq x)[\mathcal{P}^X[Y](Z) \leftrightarrow (\exists U \leq |X|)[U < X \wedge P^U_{\varphi,x}[Y] = Z]].$$

Claim. For a string W, if $x < |W|$, then the following holds.

$$\begin{aligned}(\forall Y \leq x)\ [\mathsf{numones}^3(W, \mathcal{P}^X[Y]) \leq X \to \\ (\exists U, V \leq |X|)(U < V \leq X \wedge P^V_{\varphi,x}[Y] = P^U_{\varphi,x}[Y])].\end{aligned} \tag{9}$$

Assume the claim. Since $\mathsf{numones}^3(S(\mathsf{Ones}(x)), \mathcal{P}^{S(\mathsf{Ones}(x))}[Y]) \leq S(\mathsf{Ones}(x))$ by the definition of $\mathsf{numones}^3$ and $x < x + 1 = |S(\mathsf{Ones}(x))|$, (9) then implies the instance of (Σ_0^{B}-ID) in case of φ.

The rest of the proof is devoted to prove the claim. Let us observe that (9) is a $\Sigma_1^{\mathcal{B}}$ statement. We show the claim by induction on $|X|$. In the base case, $X = \emptyset$ and hence (9) trivially holds. The case that $X = S(\emptyset)$ is also trivial. For the induction step, suppose $|X| > 1$. Then there exist strings X_0 and X_1 such that $|X_0| = |X_1| = |X| - 1$ and $X_0 + X_1 = X$. Fix a string Y so that $|Y| \leq x$ and suppose $\mathsf{numones}^3(W, \mathcal{P}^X[Y]) \leq X$. By the definition of the hyper string $\mathcal{P}^X[Y]$ and Lemma 7.6, for any Z, if $|Z| \leq x$, then $\mathcal{P}^X[Y](Z) \leftrightarrow \mathcal{P}^{X_0}[Y](Z) \vee \mathcal{P}^{X_1}[P^{X_0}_{\varphi,x}[Y]](Z)$ holds, i.e., $\mathcal{P}^X[Y] = \mathcal{P}^{X_0}[Y] \cup \mathcal{P}^{X_1}[P^{X_0}_{\varphi,x}[Y]]$. On the other hand we can assume that $(\forall U < X_0)(\forall V < X_1) P^U_{\varphi,x}[Y] \neq P^V_{\varphi,x}[P^{X_0}_{\varphi,x}[Y]]$ holds, i.e., $\mathcal{P}^{X_0}[Y] \cap \mathcal{P}^{X_1}[P^{X_0}_{\varphi,x}[Y]] = \emptyset$. This yields

$$\begin{aligned}&\mathsf{numones}^3(W, \mathcal{P}^X[Y]) \\ &= \mathsf{numones}^3(W, \mathcal{P}^{X_0}[Y]) + \mathsf{numones}^3(W, \mathcal{P}^{X_1}[P^{X_0}_{\varphi,x}[Y]]).\end{aligned} \tag{10}$$

Case. $\mathsf{numones}^3(W, \mathcal{P}^{X_0}[Y]) \leq X_0$: In this case IH yields two strings U_0 and V_0 such that $|U_0|, |V_0| \leq |X_0|$, $U_0 < V_0 \leq X_0$ and $P^{V_0}_{\varphi,x}[Z] = P^{U_0}_{\varphi,x}[Z]$. Since $|X_0| \leq |X|$ and $\leq X_0 \leq X$, we can define U and V by $U = U_0$ and $V = V_0$.

Case. $X_0 < \mathsf{numones}^3(W, \mathcal{P}^{X_0}[Y])$: In this case, $\mathsf{numones}^3(W, \mathcal{P}^{X_1}[P^{X_0}[Y]])$ $\leq X_1$ by the equality (10). Since $|P^{X_0}[Y]| \leq x$ by definition, another application of IH yields two strings U_1 and V_1 such that $|U_1|, |V_1| \leq |X_1|$, $U_1 < V_1 \leq X_1$ and $P^{V_1}_{\varphi,x}[P^{X_0}_{\varphi,x}[Y]] = P^{U_1}_{\varphi,x}[P^{X_0}_{\varphi,x}[Y]]$ hold. Define strings U and V by $U = X_0 + U_1$ and $V = X_0 + V_1$. Since $P^V_{\varphi,x}[Y] = P^{V_1}_{\varphi,x}[P^{X_0}_{\varphi,x}[Y]]$ and $P^U_{\varphi,x}[Y] = P^{U_1}_{\varphi,x}[P^{X_0}_{\varphi,x}[Y]]$ by Lemma 7.6, now it is easy to check that the assertion (9) holds. □

Corollary 7.11. *Every function* $\Sigma^{\mathrm{B}}_1(\mathcal{L}^2_{\mathrm{ID}})$*-definable in* Σ^{B}_0-ID *is polyspace computable.*

Proof. Suppose that a $\Sigma^{\mathrm{B}}_1(\mathcal{L}^2_{\mathrm{ID}})$ formula ψ is provable in Σ^{B}_0-ID. Then, as in the proof of Theorem 5.7, from Lemma 7.5 and Theorem 7.10 one can find a $\Sigma^{\mathcal{B}}_1$ formula ψ' provable in W^1_1 and provably equivalent to ψ in $\mathrm{W}^1_1(\mathcal{L}^2_{\mathrm{ID}})$. In particular ψ and ψ' are equivalent under the underlying interpretation. Hence every string function $\Sigma^{\mathrm{B}}_1(\mathcal{L}^2_{\mathrm{ID}})$-definable in Σ^{B}_0-ID is $\Sigma^{\mathcal{B}}_1$-definable in W^1_1. Thus employing Proposition 7.1 enables us to conclude. ☐

Corollary 7.12. *A predicate belongs to* PSPACE *if and only if it is* $\Delta^{\mathrm{B}}_1(\mathcal{L}^2_{\mathrm{ID}})$*-definable in* Σ^{B}_0-ID.

8 Conclusion

In this paper we introduced a novel axiom of finitary inductive definitions over the Cook-Nguyen style second order bounded arithmetic. We showed that over a conservative extension $\mathrm{V}^0(\mathcal{L}^2_{\mathrm{ID}})$ of V^0 by fixed point predicates, P can be captured by the axiom of inductive definitions under Σ^{B}_0-definable inflationary operators whereas PSPACE can be captured by the axiom of inductive definitions under (non-inflationary) Σ^{B}_0-definable operators. It seems also possible for each $i \geq 0$ to capture the ith level of the polynomial hierarchy by the axiom of inductive definitions under Σ^{B}_i-definable inflationary operator, e.g., a predicate belongs to NP if and only if it is $\Delta^{\mathrm{B}}_2(\mathcal{L}^2_{\mathrm{ID}})$-definable in Σ^{B}_1-IID. As shown by Y. Gurevich and S. Shelah in [5], over finite structures the fixed point of a first order definable inflationary operator can be reduced the least fixed point of a first order definable monotone operator. In accordance with this fact, it is natural to ask whether the axiom Σ^{B}_0-IID of inflationary inductive definitions for Σ^{B}_0-definable operators can be reduced a suitable axiom of monotone inductive definitions for Σ^{B}_0-definable operators. One would define a third order version of *Pigeon Hole Principle* $\mathrm{PHP}^3(x, \mathcal{X})$ as

$$\begin{aligned}&(\forall Y \leq x)(\exists Z \leq x+1)\mathcal{X}(\langle Y, Z\rangle) \to \\ &(\exists U \leq x)(\exists V \leq x)(\exists Z \leq x+1)[U < V \wedge \mathcal{X}(\langle U, Z\rangle) \wedge \mathcal{X}(\langle V, Z\rangle)].\end{aligned}$$

Modifying the proof of Theorem 7.10, one could show that $\forall x \forall \mathcal{X} \mathrm{PHP}^3(x, \mathcal{X})$ holds in Σ^{B}_0-ID. We have shown that (Σ^{B}_1-COMP) implies (Σ^{B}_0-IID) over $\mathrm{V}^0(\mathcal{L}^2_{\mathrm{ID}})$ (from Theorem 5.6) and ($\Sigma^{\mathcal{B}}_1$-3COMP) implies (Σ^{B}_0-ID) over a third order conservative extension of $\mathrm{V}^0(\mathcal{L}^2_{\mathrm{ID}})$ (from Theorem 7.10). In terms of *bounded reverse mathematics* it may be of interest to ask whether, conversely, (Σ^{B}_0-IID) also implies (Σ^{B}_1-COMP), or whether (Σ^{B}_0-ID) implies ($\Sigma^{\mathcal{B}}_1$-3COMP), over a suitable weak base system.

Acknowledgment

The author acknowledges valuable discussions with Toshiyasu Arai during the author's visit at Chiba University. He pointed out that the numerical function

val and the string one $P^X_{\varphi,x}$ $(|X| \leq |y|)$ are not only Σ^{B}_1-definable but even Δ^{B}_1-definable in V^1 (Lemma 5.2 and 5.3) and $P^X_{\varphi,x}$ and $\mathsf{numones}^3$ are even $\Delta^{\mathcal{B}}_1$-definable in W^1_1 as well (Lemma 7.5 and 7.8). This observation made later arguments easier.

References

1. T. Arai. A Bounded Arithmetic AID for Frege Systems. *Annals of Pure Applied Logic*, 103(1-3):155–199, 2000.
2. S. Buss. *Bounded Arithmetic.* Bibliopolis, Napoli, 1986.
3. S. Cook and P. Nguyen. *Logical Foundations of Complexity.* Cambridge University Press, 2010.
4. H.-D. Ebbinghaus and J. Flum. *Finite Model Theory. Second edition.* Perspectives in Mathematical Logic. Springer, 1999.
5. Y. Gurevich and S. Shelah. Fixed-point Extensions of First-order Logic. *Annals of Pure and Applied Logic*, 32(3):265–280, 1986.
6. N. Immerman. Relational Queries Computable in Polynomial Time (Extended Abstract). In *Proceedings of the 14th Annual ACM Symposium on Theory of Computing*, pages 147–152, 1982.
7. W. Pohlers. Subsystems of Set Theory and Second Order Number Theory. In S. R. Buss, editor, *Handbook of Proof Theory*, pages 210–335. North Holland, Amsterdam, 1998.
8. A. Skelley. A Third-order Bounded Arithmetic Theory for PSPACE. In *Proceedings of Computer Science Logic 2004, the 18th International Workshop of the EACSL, Lecture Notes in Computer Science*, volume 3210, pages 340–354. Springer, Berlin, 2004.
9. K. Tanaka. The Galvin-Prikry Theorem and Set Existence Axioms. *Annals of Pure Applied Logic*, 42(1):81–104, 1989.
10. K. Tanaka. Weak Axioms of Determinacy and Subsystems of Analysis II (Σ^0_2 Games). *Annals of Pure Applied Logic*, 52(1-2):181–193, 1991.
11. M. Y. Vardi. The Complexity of Relational Query Languages (Extended Abstract). In *Proceedings of the 14th Annual ACM Symposium on Theory of Computing*, pages 137–146, 1982.
12. D. Zambella. Notes on Polynomially Bounded Arithmetic. *Journal of Symbolic Logic*, 61(3):942–966, 1996.

A Proving ($\Sigma^{\mathcal{B}}_1$-3COMP) in W^1_1

In the appendix we show Lemma 7.9 which states that the axiom ($\Sigma^{\mathcal{B}}_1$-3COMP) of third order comprehension for $\Sigma^{\mathcal{B}}_1$ formulas (presented on page 11) holds in W^1_1.

Lemma A.1. *In W^1_1 for any number x, string X and hyper string $\mathcal{Z}$, if $|X| \leq x$ and $\emptyset < \mathsf{numones}^3(X, \mathcal{Z})$, then the following holds.*

$$(\exists Y \leq x)(Y < X \wedge S(\mathsf{numones}^3(Y, \mathcal{Z})) = \mathsf{numones}^3(X, \mathcal{Z})).$$

Proof. Reason in W^1_1. Fix x and $\mathcal{Z}$. We show the following stronger assertion holds by induction on $|X| \leq x$.

$$(\forall U \leq x)\ |U+X| \leq x \wedge \mathsf{numones}^3(U,\mathcal{Z}) < \mathsf{numones}^3(U+X,\mathcal{Z}) \to \\ (\exists Y \leq x)(Y < X \wedge S(\mathsf{numones}^3(U+Y,\mathcal{Z})) = \mathsf{numones}^3(U+X,\mathcal{Z})).$$

If $|X| = 0$, i.e., $X = \emptyset$, then $\mathsf{numones}^3(U,\mathcal{Z}) = \mathsf{numones}^3(U+X,\mathcal{Z})$, and hence the assertion trivially holds. In the case $|X| = 1$, i.e., $X = S(\emptyset)$, if $\mathsf{numones}^3(U,\mathcal{Z}) < \mathsf{numones}^3(U+S(\emptyset),\mathcal{Z})$, then the assertion is witnessed by $Y = \emptyset$. For the induction step, suppose $|X| > 1$. Then there exist two strings X_0 and X_1 such that $|X_0| = |X_1| = |X|-1$ and $X_0+X_1 = X$. Fix a string U so that $|U| \leq x$ and suppose that $|U+X| \leq x$ and $\mathsf{numones}^3(U,\mathcal{Z}) < \mathsf{numones}^3(U+X,\mathcal{Z})$ hold. Then $|U+X_0| \leq x$.

Case. $\mathsf{numones}^3(U,\mathcal{Z}) = \mathsf{numones}^3(U+X_0,\mathcal{Z})$: By IH there exists a string $Y < X_1 < X$ such that $|Y| \leq x$ and $S(\mathsf{numones}^3(U+Y,\mathcal{Z})) = \mathsf{numones}^3(U+X_1,\mathcal{Z}) = \mathsf{numones}^3(U+X_0+X_1,\mathcal{Z}) = \mathsf{numones}^3(U+X,\mathcal{Z})$.

Case. $\mathsf{numones}^3(U,\mathcal{Z}) < \mathsf{numones}^3(U+X_0,\mathcal{Z})$: In this case by IH there exists a string $Y_0 < X_0$ such that $|Y_0| \leq x$ and $S(\mathsf{numones}^3(U+Y_0,\mathcal{Z})) = \mathsf{numones}^3(U+X_0,\mathcal{Z})$ holds. If $\mathsf{numones}^3(U+X_0,\mathcal{Z}) = \mathsf{numones}^3(U+X,\mathcal{Z})$, then the witnessing string Y can be defined to be Y_0. Consider the case $\mathsf{numones}^3(U+X_0,\mathcal{Z}) < \mathsf{numones}^3(U+X,\mathcal{Z})$. Then another application of IH yields a string $Y_1 < X_1$ such that $|Y_1| \leq x$ and $S(\mathsf{numones}^3((U+X_0)+Y_1,\mathcal{Z})) = \mathsf{numones}^3((U+X_0)+X_1,\mathcal{Z})$ hold. Define a string Y by X_0+Y_1. Then $|Y| \leq |X| \leq x$, $Y = X_0+Y_1 < X_0+X_1 = X$ and $S(\mathsf{numones}^3(U+Y,\mathcal{Z})) = \mathsf{numones}^3(U+X,\mathcal{Z})$ hold. □

Lemma A.2. *In W^1_1, for any number x, strings X, Z and hyper string $\mathcal{Z}$, if $|X| \leq x$ and $\emptyset < Z \leq \mathsf{numones}^3(X,\mathcal{Z})$, then the following holds.*

$$(\exists Y \leq x)(Y < X \wedge \mathsf{numones}^3(Y,\mathcal{Z}) + Z = \mathsf{numones}^3(X,\mathcal{Z})).$$

Proof. Reason in W^1_1. Fix x and $\mathcal{Z}$. We show the following stronger assertion holds by induction on $|Z|$.

$$(\forall X \leq x)(\forall U \leq x) \\ \{|U+Z| \leq x \wedge \emptyset < Z \leq \mathsf{numones}^3(X,\mathcal{Z}) \to \\ (\exists Y \leq x)(Y < X \wedge \mathsf{numones}^3(Y,\mathcal{Z}) + U + Z = \mathsf{numones}^3(X,\mathcal{Z}) + U)\}.$$

If $|Z| = 0$, i.e., $Z = \emptyset$, then the assertion trivially holds. In the case $|Z| = 1$, i.e., $Z = S(\emptyset)$, since $\mathsf{numones}^3(Y,\mathcal{Z}) + U + S(\emptyset) = S(\mathsf{numones}^3(Y,\mathcal{Z})) + U$, the assertion follows from Lemma A.1. For the induction step, suppose $|Z| > 1$. Then, as in the previous proof, there exist strings Z_0 and Z_1 such that $|Z_0| = |Z_1| = |Z|-1$ and $Z_0+Z_1 = Z$. Fix two strings X and U so that $|X|, |U| \leq x$ and $|U+Z| \leq x$ and suppose that $\emptyset < Z \leq \mathsf{numones}^3(X,\mathcal{Z})$. Then, since $|U+Z_0| \leq |U+Z| \leq x$ and $\emptyset < Z_0 < Z \leq \mathsf{numones}^3(X,\mathcal{Z})$, IH yields a string $Y_0 < X$ such that $|Y_0| \leq x$ and $\mathsf{numones}^3(Y_0,\mathcal{Z}) + U + Z_0 = \mathsf{numones}^3(X,\mathcal{Z}) + U$ hold. Since $|Y_0| \leq |X| \leq x$ and $|U+Z_0| \leq |U+Z| \leq x$, another application of IH yields a string $Y_1 < Y_0 < X$ such that $|Y_1| \leq x$ and $\mathsf{numones}^3(Y_0,\mathcal{Z}) + (U+Z_0) + Z_1 = \mathsf{numones}^3(Y_1,\mathcal{Z}) + U + Z_0 = \mathsf{numones}^3(X,\mathcal{Z}) + U$ holds. Thus the witnessing string Y can be defined to be Y_0. □

Notation. In contrast to the empty string $\emptyset$, we write $\emptyset^3$ to denote the *empty hyper string* defined by the axiom $\emptyset^3(X) \leftrightarrow |X| < 0$.

Proof (of Lemma 7.9). Suppose a $\Sigma_1^{\mathcal{B}}$ formula $\varphi(Z)$. We have to show the existence of a hyper string $\mathcal{Y}$ such that $(\forall Z \leq x)(\mathcal{Y}(Z) \leftrightarrow \varphi(Z))$ holds. Let $\psi(x, U, X, \mathcal{Y})$ denote the following formula.

$$(\forall Z \leq x)(\mathcal{Y}(Z) \to \varphi(Z)) \wedge X = U + \mathsf{numones}^3(S(\mathsf{Ones}(x)), \mathcal{Y}).$$

By Lemma 7.8, ψ is a $\Sigma_1^{\mathcal{B}}$ formula, and hence so is $\exists \mathcal{Y} \psi(x, U, X, \mathcal{Y})$. Reason in W_1^1. The argument splits into two (main) cases.

Case. $(\exists X \leq x+1)[X < S(\mathsf{Ones}(x)) \wedge \exists \mathcal{Y} \psi(x, \emptyset, X, \mathcal{Y}) \wedge (\forall Y \leq x+1)(Y \leq S(\mathsf{Ones}(x)) \wedge X < Y \to \neg \exists \mathcal{Y} \psi(x, \emptyset, Y, \mathcal{Y}))]$: Suppose that a string X_0 witnesses this case. Let $\psi(x, \emptyset, X_0, \mathcal{Y})$. Then clearly $(\forall Z \leq x)(\mathcal{Y}(Z) \to \varphi(Z))$ holds. We show the converse inclusion by contradiction. Assume that there exists a string Z_0 such that $|Z_0| \leq x$, $\varphi(Z_0)$ but $\neg \mathcal{Y}(Z_0)$. Define a hyper string $\mathcal{Y}'$ by

$$(\forall Z \leq x)[\mathcal{Y}'(Z) \leftrightarrow (Z = Z_0 \vee \mathcal{Y}(Z))].$$

Then $(\forall Z \leq x)(\mathcal{Y}'(Z) \to \varphi(Z))$ by definition, and also $\mathsf{numones}^3(S(\mathsf{Ones}(x)), \mathcal{Y}) = X_0 < S(X_0) = \mathsf{numones}^3(S(\mathsf{Ones}(x)), \mathcal{Y}') \leq S(\mathsf{Ones}(x))$. But this contradicts the assumption of this case.

Case. The previous case fails: Namely, $(\forall X \leq x+1)[X < S(\mathsf{Ones}(x)) \wedge \exists \mathcal{Y} \psi(x, \emptyset, X, \mathcal{Y}) \to (\exists Y \leq x+1)(Y \leq S(\mathsf{Ones}(x)) \wedge X < Y \wedge \exists \mathcal{Y} \psi(x, \emptyset, Y, \mathcal{Y}))]$ holds. We derive the following $\Sigma_1^{\mathcal{B}}$ formula by induction on $|X|$.

$$\begin{aligned}(\forall U \leq x+1)[&U + X \leq S(\mathsf{Ones}(x)) \to \\ &(\exists Y \leq x+1)(\exists \mathcal{Y} \psi(x, U, Y, \mathcal{Y}) \wedge U + X \leq Y \leq S(\mathsf{Ones}(x)))].\end{aligned} \tag{11}$$

Assume the formula (11) holds. Let $U = \emptyset$ and $X = S(\mathsf{Ones}(x))$. Then by (11) we can find a string Y and a hyper string $\mathcal{Y}$ such that $|Y| \leq x+1$ and $\mathsf{numones}^3(S(\mathsf{Ones}(x)), \mathcal{Y}) = Y = S(\mathsf{Ones}(x))$. This means that $(\forall Z \leq x)\mathcal{Y}(Z)$ holds, and hence in particular $(\forall Z \leq x)[\varphi(Z) \to \mathcal{Y}(Z)]$ holds.

In the base case, if $|X| = 0$, i.e., $X = \emptyset$, then $\psi(x, U, U, \emptyset^3)$ holds. This implies $\psi(x, \emptyset, \emptyset, \emptyset^3)$. Hence by the assumption of this case, we can find a string Y and a hyper string $\mathcal{Y}$ such that $|Y| \leq x+1$, $Y \leq S(\mathsf{Ones}(x))$, $\emptyset < Y$ and $\psi(x, \emptyset, Y, \mathcal{Y})$. These imply the case $|X| = 1$, i.e., $\psi(x, U, U+Y, \mathcal{Y})$ and $U + S(\emptyset) \leq U + Y$. For the induction step, suppose $|X| > 1$. Then there exist two strings X_0 and X_1 such that $|X_0| = |X_1| = |X| - 1$ and $X_0 + X_1 = X$. Fix a string U so that $|U + X| \leq x+1$. Then by IH we can find a string Y_0 and a hyper string $\mathcal{Y}_0$ such that $|Y_0| \leq x+1$, $\psi(x, U, Y_0, \mathcal{Y}_0)$ and $U + X_0 \leq Y_0$.

Subcase. $U + X_0 = Y_0$: In this subcase, another application of IH yields a string Y_1 and a hyper string $\mathcal{Y}_1$ such that $|Y_1| \leq x+1$, $\psi(x, Y_0, Y_1, \mathcal{Y}_1)$ and $Y_0 + X_1 \leq Y_1$. Since $U + X = U + X = Y_0 + X_1 \leq Y_1$, it can be observed that $\psi(x, U, Y_1, \mathcal{Y}_0 {}^\frown \mathcal{Y}_1)$ holds.

Subcase. $U + X_0 < Y_0$: In this subcase we can assume that $Y_0 < U + X$ holds. Hence by Lemma A.2, we can find a string $V < S(\mathsf{Ones}(x))$ such that $\mathsf{numones}^3(V, \mathcal{Y}_0) = U + X_0$ holds. Define a hyper string $\mathcal{Y}_0 \restriction V$ by

$$(\forall Z \leq x)[(\mathcal{Y}_0 \restriction V)(Z) \leftrightarrow Z < V \wedge \mathcal{Y}_0(Z)].$$

Then $\mathsf{numones}^3(S(\mathsf{Ones}(x)), \mathcal{Y}_0 \restriction V) = U + X_0$ holds by definition. Now we can proceed in the same way as the previous subcase but we define the witnessing hyper string $\mathcal{Y}$ by $\mathcal{Y} = (\mathcal{Y}_0 \restriction V)^\frown \mathcal{Y}_1$. This completes the proof of Lemma 7.9. $\square$