ゲーデルの β 関数と，それによる記号の追加ついて

橋本航気

2022 年 2 月 20 日

概要

言語の追加，特に新しい関数記号の便利な導入方法について補足する．本稿 2 節の証明はすべて kaye [1] による．

目次

1 前提知識

Kaye [1] の 2 章，3.1 節，4 章（もしくは筆者の言語の追加 pdf[*1] ）を既に読んでいる読者を想定している．

2 ゲーデルの β 関数によるコード化

この節では 3.1 節で証明を保留していたゲーデルの補題を $I\Sigma_1$ で証明する．このゲーデルの補題が $I\Sigma_1$ で成立するという事実は深甚で，これによって形式的体系内部での有限列のコード化が可能になり，様々な関数を生み出せるようになる．

*1 https://nuhashikou.github.io/homepage/contents/genngonotuika.pdf

定義 2.1. 数論のための新しい関数や関係を以下のように定める．

$$\begin{aligned}
\left\lfloor \frac{x}{y} \right\rfloor &= z \leftrightarrow (y = 0 \land z = 0) \lor (y \neq 0 \land yz \leq x < y(z+1))) \\
\left(\frac{x}{y} \right) &= z \leftrightarrow (y = 0 \land z = 0) \lor (y \neq 0 \land \exists w \leq x(x = y \cdot w + z \land z < y)) \\
x|y &\leftrightarrow \exists z \leq y(xz = y \land x \neq 0) \\
x \equiv y \mod z &\leftrightarrow z \neq 0 \land \left(\frac{x}{z} \right) = \left(\frac{y}{z} \right) \\
\mathrm{prime}(x) &\leftrightarrow x \geq 2 \land \forall y, z(x|yz \to (x|y \lor x|z)) \\
\mathrm{ireed}(x) &\leftrightarrow x \geq 2 \land \forall y(y|x \to (y = 1 \lor y = x)) \\
(x, y) = 1 &\leftrightarrow x \geq 1 \land y \geq 1 \land \forall u(u|x \land u|y \to u = 1)
\end{aligned}$$

上から二つの関数は “x を y で割ったときの整数部”，“x を y で割った余り”，以降の関係は “x は y を割り切る”，“x と y は z を法として合同”，“x は素”，“x は既約”，“x と y は互いに素” を意図している．慣習に従い，$x \nmid y$ を $\neg(x|y)$ の意味で使う．

命題 2.2. $I\Delta_0 \vdash \forall x, y, \exists! z(y = 0 \land z = 0) \lor (y \neq 0 \land \exists w \leq x(x = y \cdot w + z \land z < y))$

証明. まず $\psi(x, y)$ を以下の Δ_0 論理式とする．

$$\exists! z \leq y[(y = 0 \land z = 0) \lor (y \neq 0 \land \exists w \leq x(x = y \cdot w + z \land z < y))]$$

y をパラメーターと見なし，x による帰納法で $\forall x \psi(x, y)$ 示す．$\psi(0, y)$ は自明．$x + 1$ の場合を考える．$y = 0$ なら自明なのでそうでないとする．

全域性: 帰納法の仮定より $x = y \cdot w + z$ を満たす $z < y, w \leq x$ が存在する． このとき $x+1 = yw+(z+1)$ となる．$z+1 < y$ なら自明であり，$z+1 = y$ でも $x+1 = y(w+1)+0$ なのでよい．

一意性: $x + 1 = yw + z = yw' + z'$ たる $w, w' \leq x + 1, z, z' < y$ が存在したとする．もし仮に $w < w'$ なら，$w + 1 \leq w'$ より，

$$x + 1 = yw + z < yw + y = y(w + 1) \leq yw' \leq yw' + z' = x + 1$$

となり矛盾する．$w' < w$ も同様なので，$w = w'$ であり，このとき明らかに $z = z'$ である．

□

系 2.3. (除法の原理) $I\Delta_0 \vdash \forall x, y \exists! r, s(y \neq 0 \to (x = ys + r \land r < y))$

系 2.4. $I\Delta_0 \vdash \forall x, y, \exists! z(y = 0 \land z = 0) \lor (y \neq 0 \land yz \leq x < y(z + 1)))$

証明. $y \neq 0, x$ を任意にとる．除法の原理より $x = yz + r \land r < y$ を満たす r, z が一意に存在する．このとき $yz \leq x < yz + y$ である．この z の一意性は明らか． □

次の命題は $I\Delta_0$ において $\mathrm{ireed}(x)$ と $(x, y) = 1$ は Δ_0 と見なせることを主張している．

命題 2.5. 次が成り立つ.

(a) $I\Delta_0 \vdash \forall x(\mathrm{ireed}(x) \leftrightarrow (x \geq 2 \wedge \forall y \leq x(y|x \to (y = 1 \vee y = x)))$

(b) $I\Delta_0 \vdash \forall x, y((x, y) = 1 \leftrightarrow x \geq 1 \wedge y \geq 1 \wedge \forall u \leq x + y(u|x \wedge u|y \to u = 1))$

証明. $\forall x, y(x > y \geq 1 \to \neg(x|y))$ より明らか. □

命題 2.6. 次が成り立つ.

(a) $I\Delta_0 \vdash \forall x, y, z(x|y \wedge y|z \to x|z)$

(b) $I\Delta_0 \vdash \forall w, y(w < y \to \left(\frac{w}{y}\right) = w)$

(c) $I\Delta_0 \vdash \forall y, r, s(y \neq 0 \to r + sy \equiv r \mod y)$

(d) $I\Delta_0 \vdash \forall x, w, r, s(w \geq 1 \wedge s = \left\lfloor \frac{x}{w} \right\rfloor \wedge r = \left(\frac{x}{w}\right) \to x = sw + r \wedge 0 \leq r < w)$

(e) $I\Delta_0 \vdash \forall x, p(p|x \wedge p|(x + 1) \to p = 1)$

証明. (a) は明らかなので (b) から示す. w, y を $w < y$ を満たすように任意にとると, $\left(\frac{w}{y}\right)$ の定義より

$$w = ya + \left(\frac{w}{y}\right)$$

となる $a \leq w$ が存在する. もし仮に $a \neq 0$ なら $a \geq 1$ なので

$$w = ya + \left(\frac{w}{y}\right) \geq y + \left(\frac{w}{y}\right) \geq y > w$$

となり矛盾が導かれる. よって $a = 0$.

次に (c) を示す. $y \neq 0, s \neq 0, r$ を任意にとる. $u = \left(\frac{r+sy}{y}\right)$ とおくと, 定義より

$$r + sy = wy + u \wedge u < y \tag{2.1}$$

となる $w \leq y$ が存在する. もし仮に $r < u$ なら $sy > wy$ なので $u = y(s - w) + r$ となり $\left(\frac{u}{y}\right) = r$ が導かれるが, (b) より $\left(\frac{u}{y}\right) = u$ となるので矛盾である. したがって $u \leq r$ であり, このとき $sy \leq wy$ なので $r = y(w - s) + u$ となり $\left(\frac{r}{y}\right) = u = \left(\frac{r+sy}{y}\right)$ が成り立つ.

(d) を示す. x, w, r, s をそれぞれ定理の前提を満たすようにとる. まず r の定義より $x = wz + r \wedge r < w$ を満たす z が存在する. 次に s の定義より $ws \leq x < ws + w$ なので, PA^- の公理より $x = ws + r'$ を満たす r' が存在する. もし仮に $r' \geq w$ なら

$$x = ws + r' \geq ws + w > x$$

となり矛盾する. よって $r' < w$ だと分かったので, 除法の原理より $r = r'$ かつ $s = z$ すなわち $x = ws + r$ が成り立つ.

最後に (e) を示す. $p|x \wedge p|(x + 1)$ の定義より, $p \neq 0$ であり,

$$pw_1 = x \wedge pw_2 = x + 1$$

を満たす w_1, w_2 が存在する．明らかに $w_1 < w_2$ であるので，$p(w_2 - w_1) = pw_2 - pw_1 = 1$ となる．よって $p = 1$ 以外あり得ない． □

それではベズーの補題を証明しよう．これは，任意の互いに素な x, y について，y を法とする x の積に関する逆元が存在することを意味する[*2]．

補題 2.7. (ベズーの補題) $I\Delta_0 \vdash \forall x, y((x, y) = 1 \to \exists z < y(zx \equiv 1 \mod y))$

証明． $M \models I\Delta_0$ とし，$x, y \in M$ を $M \models (x, y) = 1$ を満たすようにとる．まず x, y のいずれかが 1 なら自明なので考えなくてよい．いま，

$$M \models \exists w[(x, y) = 1 \land x > 1 \land y > 1 \to (w \geq 1 \land \exists z < y(zx \equiv w \mod y))] \tag{2.2}$$

が成り立つ．実際，$w = \left(\frac{x}{y}\right)$ とおくと $(x, y) = 1$ より $w \geq 1$ であり，$w < y$ なので命題 2.6(b) より $w = \left(\frac{w}{y}\right) = \left(\frac{x}{y}\right)$ が成り立つ．よって $z = 1$ で $zx \equiv w \mod y$ が成り立っている．したがって Δ_0 最小値原理より，(2.2) の四角括弧の中を満たす最小の w_0 が存在する．この w_0 に関してまず次が成り立つことを示そう．

$$M \models 1 \leq w_0 \leq \left(\frac{x}{y}\right) \leq \min(x, y) \land w_0 < y$$

$x \geq y$ のときは $\left(\frac{x}{y}\right) < y = \min(x, y)$ より明らか．$y > x$ のときも命題 2.6(b) から $\left(\frac{x}{y}\right) = x = \min(x, y) < y$ が成り立つ．$w_0 \leq \left(\frac{x}{y}\right)$ は $w = \left(\frac{x}{y}\right)$ が (2.2) を満たすので w_0 の最小性より成り立つ．

私たちの目標は $w_0 = 1$ を示すことである．そのためには，いま $(x, y) = 1$ なので $w_0 | x \land w_0 | y$ を示せば十分である．

まず $z_0 \in M$ を次を満たすようにとる．

$$M \models z_0 < y \land (z_0 x \equiv w_0 \mod y)$$

すると $\left(\frac{z_0 x}{y}\right) = \left(\frac{w_0}{y}\right)$ であり，$w_0 < y$ であったので命題 2.6(b) より $w_0 = \left(\frac{w_0}{y}\right)$，すなわち $w_0 = \left(\frac{z_0 x}{y}\right)$ 成り立つ．ここで $t = \lfloor \frac{z_0 x}{y} \rfloor$ とおくと，命題 2.6(d) より $z_0 x = ty + w_0$ が成り立つ．

Claim 1.$w_0 | x$

$s = \lfloor \frac{x}{w_0} \rfloor$，$r = \left(\frac{x}{w_0}\right)$ とおくと，命題 2.6(d) より $x = sw_0 + r$ と $0 \leq r < w_0$ が成り立つ．よって

$$r = x - sw_0 = x - s(z_0 x - ty) = x + sty - sz_0 x$$

[*2] ベズーの補題（またはベズーの等式）とはもともと任意の互いに素な整数 x, y について，$ax + by = 1$ となる整数 a, b が存在するという初等整数論における主張である．それを負の数という概念を表に出さずに書いたのが本主張である．

が成り立ち，Δ_0 論理式の最小値原理によって $0 \leq (1+uy-sz_0) < y$ を満たす u を取る[*3]と

$$\begin{aligned} r &\equiv r + uyx \mod y && (\because \text{命題 } 2.6(c)) \\ &\equiv x + sty - sz_0x + uyx \mod y \\ &\equiv sty + x(1+uy-sz_0) \mod y \\ &\equiv x(1+uy-sz_0) \mod y && (\because \text{命題 } 2.6(c)) \end{aligned}$$

が成り立つ．いま $r < w_0$ であり，w_0 は (2.2) を満たす最小元だったので $r = 0$ 以外はあり得ない．ゆえに $x = sw_0$ すなわち $w_0|x$ が成り立つ．

Claim 2.$w_0|y$

$c = \lfloor \frac{y}{w_0} \rfloor$，$d = \left(\frac{y}{w_0}\right)$ とおくと，命題 2.6(d) より $y = cw_0 + d$ と $0 \leq d < w_0$ が成り立つ．よって

$$d = y - cw_0 = y - c(z_0x - ty) = (1+ct)y - cz_0x$$

が成り立ち，$0 \leq (by - cz_0) < y$ を満たす b を取ると

$$\begin{aligned} d &\equiv d + byx \mod y && (\because \text{命題 } 2.6(c)) \\ &\equiv (1+ct)y - cz_0x + byx \mod y \\ &\equiv (by - cz_0)x \mod y && (\because \text{命題 } 2.6(c)) \end{aligned}$$

となり w_0 の最小性から $d = 0$ がいえるので $y = cw_0$ すなわち $w_0|y$ が成り立つ． □

このベズーの補題から，これまで保留してきた prime(x) も $I\Delta_0$ 上でなら Δ_0 と見なしうることが証明できる．

系 2.8. $I\Delta_0 \vdash \forall x(\mathrm{prime}(x) \leftrightarrow \mathrm{ireed}(x))$

証明. $x \in M \models I\Delta_0$ を固定しておく．

$(\mathrm{prime}(x) \to \mathrm{ireed}(x))$

まず仮定より $M \models x \geq 2 \wedge \forall y, z(x|yz \to (x|y \vee x|z))$ である．$y|x$ を満たす $y \in M$ を任意にとると，定義より $x = yz$ なる $z \in M$ が存在する．いま $x \geq 2$ なので $y, z > 0$ である．定義から $x|x$ なので $x|yz$ であり，prime(x) から $x|y \vee x|z$ が成り立つ．$x|y$ なら $x \leq y$ であるが，明らかに $y \leq x$ なので $y = x$．$x|z$ の場合も，$x \leq z$ かつ $z \leq x$ なので $z = x$ となり $y = 1$ が成り立つ．

$(\mathrm{ireed}(x) \to \mathrm{prime}(x))$

仮定より $M \models x \geq 2 \wedge \forall y(y|x \to (y = 1 \vee y = x))$ である．ここで，もし仮に $x|ab \wedge \neg(x|a) \wedge \neg(x|b)$ を満たす $a, b \in M$ が存在したとする．すると $(x, a) = 1$ が成り立つ．実際，$u|x$ かつ $u|a$ を満たす $u \in M$ を取ると，prime(x) より $u = 1 \vee u = x$ となる．もし $u = x$ なら $x|a$ となるの

[*3] 形式的な議論をすると，$\varphi(u, y, s, z_0) := 1 + uy \geq sz_0$ とし $\forall y, s, z_0(\exists u\varphi(u, y, s, z_0) \to \exists u(\varphi(u, y, s, z_0) \wedge \forall v < u \neg\varphi(v, y, s, z_0)))$ によって取れる最小の u が条件を満たす．実際，$u = 0$ なら $1 \geq sz_0$ なので $1 \geq 1 - sz_0 \geq 0$ から $y > 1 \geq 1 + uy - sz_0 \geq 0$ となり，そうでないなら $u \geq 1$ であり，$1 + uy \geq sz_0$ より $1 + uy - sz_0 \geq 0$ となり，また $u - 1(\geq 0)$ は $1 + (u-1)y < sz_0$ なので $1 + uy < y + sz_0$ すなわち $0 \leq 1 + uy - sz_0 < y$ が成り立つ．

で $u=1$ である．同様に $(x,b)=1$ も成り立つ．ここで補題 2.7 より

$$ra \equiv 1 \mod x, \qquad sb \equiv 1 \mod x$$

を満たす $r,s<x$ が存在する．したがって

$$ra = ux+1, \qquad sb = vx+1$$

を満たす u,v が存在し，いま $x|ab$ と仮定していたので $y \in M$ で $\models xy=ab$ を満たすものがある．よって

$$rsxy = rsab = (ux+1)(vx+1) = uvx^2+ux+vx+1$$

が成り立つので，$x \geq 2$ より命題 2.6(c) から

$$0 = \left(\frac{rsxy}{x}\right) = \left(\frac{uvx^2+ux+vx+1}{x}\right) = \left(\frac{1}{x}\right) = 1$$

が導かれて矛盾する． □

補題 2.9. $I\Delta_0 \vdash \forall x(x \geq 2 \to \exists p(\mathrm{prime}(p) \wedge p|x))$

証明. $x \in M \models I\Delta_0$ とする．まず次は明らかになり立つ．

$$M \models \exists v(x \geq 2 \to (v \geq 2 \wedge v|x)) \tag{2.3}$$

実際，$v=x$ とすればよい．よって最小値原理によって (2.3) を満たす最小の $v \in M$ が存在するので，それを p とおいたとき，この p が $\mathrm{prime}(p)$ を満たすことを示そう．自明な場合を除くために $x \geq 2$ としてよい．系 2.8 より $M \models \forall y(y|p \to (y=1 \vee y=p))$ を示せばよいので，まず $y|p$ となる $y \in M$ を任意にとり，$y \neq 1$ と仮定する．いま p の取り方から $p|x$ なので命題 2.6(a) より $y|x$ が成り立ち，y も (2.3) を満たすので，p の最小性から $p \leq y$ となる．したがって $y|p$ を思い出せば $y \leq p$ となり $y=p$ が成り立つ． □

補題 2.10. $I\Delta_0 \vdash \forall x,y[(x \geq 1 \wedge y \geq 1 \wedge \neg\exists z(\mathrm{prime}(z) \wedge z|x \wedge z|y)) \leftrightarrow (x,y)=1]$

証明. $x,y \in M \models I\Delta_0$ を固定しておく．まず $M \models (x,y)=1$ とすると，$M \models x \geq 1 \wedge y \geq y \wedge \forall u(u|x \wedge u|y \to u=1)$ だから $M \models z|x \wedge z|y$ を満たす z について $M \not\models \mathrm{prime}(z)$ は明らか．

逆に $M \models x \geq 1 \wedge y \geq 1 \wedge \neg\exists z(\mathrm{prime}(z) \wedge z|x \wedge z|y)$ と仮定する．$M \models u|x \wedge u|y$ を満たす u を任意にとり，$u \geq 2$ と仮定する．すると補題 2.9 よりある $p \in M$ によって $M \models \mathrm{prime}(p) \wedge p|u$ となる．するとこのとき $|$ の推移性から $M \models p|x \wedge p|y$ となるので仮定より $M \not\models \mathrm{prime}(p)$ が導かれて矛盾する．したがって $u<2$ となり，$u \neq 0$ より $u=1$ が分かる． □

次の補題は，

$$x+1, 2x+1, \dots, yx+1 \tag{2.4}$$

がすべて $z(\neq 0)$ と互いに素なら，z と互いに素な w で，(2.4) の全ての $xi+1$ で割り切れるものが存在するという事実が $I\Sigma_1$ で証明可能であることを意味する．$\mathbb{N}$ ならその総乗をとればよい．

補題 2.11.

$$I\Sigma_1 \vdash \forall x, y, z[\forall i < y((i+1)x+1, z) = 1 \land z \neq 0 \to \exists w((w, z) = 1 \land \forall i < y((i+1)x+1|w))]$$

証明. $x, y, z \in M \models I\Sigma_1$ を固定し，以下の $\Sigma_1(I\Sigma_1)$ 論理式を $\theta(k, x, y, z)$ とおく．

$$\forall i < y((i+1)x+1, z) = 1 \land z \neq 0 \to \exists w((w, z) = 1 \land \forall i < k((i+1)x+1|w)$$

$M \models \forall k \leq y\theta(k, x, y, z)$ を k による y までの高々帰納法で示せば十分．自明な場合を除くために

$$M \models \forall i < y((i+1)x+1, z) = 1 \land z \neq 0 \tag{2.5}$$

としておく．$k = 0$ なら $w = 1$ が条件を満たす．$k < y$ なる $k \in M$ で $w \in M \models (w, z) = 1 \land \forall i < k((i+1)x|w)$ とすると，$w' = w((k+1)x+1)$ が条件を満たすことを確認しよう．

Claim1: $M \models (w', z) = 1$

補題 2.10 によって示す．もし仮に $M \models \mathrm{prime}(p) \land p|w' \land p|z$ となる $p \in M$ が存在すれば，特に $p|w((k+1)x+1)$ より $p|w$ または $p|((k+1)+1)$ である．$p|w$ とすると補題 2.10 から $(z, w) = 1$ に矛盾する．$p|((k+1)+1)$ としよう．いま $k < y$ なので，式 (2.5) より $M \models ((k+1)x+1, z) = 1$ であり，再び補題 2.5 から $p \not| z$ が導かれて矛盾する．以上からそのような p は存在せず，Claim1 の結論を得る．

Claim2: $M \models \forall i < k+1\ ((i+1)x+1|w)$

いま $M \models \forall i < k((i+1)x+1|w)$ であるので，$|$ の推移性と w' の定義から明らか． □

補題 2.12. $I\Sigma_1 \vdash \forall x, y\exists z[z > x \land \forall i, j < y(i \neq j \to (z(i+1)+1, z(j+1)+1) = 1)]$

証明. Claim: $I\Sigma_1 \models \forall x, y\exists z(z > x \land \forall i < y(i+1)|z)$

$x \in M \models I\Sigma_1$ を固定し，y に関する帰納法で示す．$y = 0$ なら $z = x+1$ でよく，$y \in M$ について

$$z_y \in M \models \forall i < y((i+1)|z_y)$$

なる z_y をとると，$z = z_y(y+1)(> x)$ によって $M \models \forall i < y+1((i+1)|z)$ が成り立つ．Claim の証明終わり．

$x, y \in M \models I\Sigma_1$ を任意にとって固定しておく．先の Claim によって $M \models z_y > x \land \forall i < y(i+1)|z_y$ を満たす z_y をとり，また $i < j < y$ なる $i, j \in M$ をとる．$\mathrm{prime}(p)$ なる p を任意にとったとき，

$$M \models \neg(p|(z(i+1)+1) \land p|(z(j+1)+1))$$

を示せば補題 2.10 より十分である．もし仮に $p|(z_y(i+1)+1)$ かつ $p|(z_y(j+1)+1)$ であったとすると，$p|(z_y(j+1)+1) - (z_y(i+1)+1)$ すなわち $p|z_y(j-i)$ が成り立ち，$\mathrm{prime}(p)$ の定義より $p|z_y$ または $p|(j-i)$ である．$p|(j-i)$ とすると，$j - i < y$ と z_y の取り方から $(j-i)|z_y$ であるので，結局 $p|z_y$ である．したがって $p|z_y(i+1)$ であるが，いま $p|(z_y(i+1)+1)$ でもあったので命題 2.6 より $p = 1$ が導かれて矛盾する． □

命題 2.13. 以下が成り立つ．

(1) $I\Delta_0 \vdash \forall x, y, a(x \equiv y \mod n \to a + x \equiv a + y \mod n)$
(2) $I\Delta_0 \vdash \forall x, y, a(x \equiv y \mod n \to ax \equiv ay \mod n)$

証明． 帰納法は使わず容易に示せる． □

補題 2.14. $I\Sigma_1 \vdash \forall a, m, x, y \exists a', m' \left[\forall i < y \left(\frac{a'}{m'(i+1)+1}\right) = \left(\frac{a}{m(i+1)+1}\right) \wedge \left(\frac{a'}{m'(y+1)+1}\right) = x\right]$

証明． $a, m, x, y \in M \models PA$ を任意にとって固定しておく．補題 2.12 より，

$$M \models m' > \max(x, m) \wedge \forall i, j \leq y(i \neq j \to (m'(i+1)+1, m'(j+1)+1) = 1) \tag{2.6}$$

を満たす $m' \in M$ がとれる．

<u>Claim:</u> $M \models \forall k \leq y \exists b \forall i < k \left(\frac{b}{m'(i+1)+1}\right) = \left(\frac{a}{m(i+1)+1}\right)$

k による y までの高々帰納法で示す $k = 0$ は示すべきことは何もない．$k < y$ について

$$b_k \in M \models \forall i < k \left(\frac{b_k}{m'(i+1)+1}\right) = \left(\frac{a}{m(i+1)+1}\right) \tag{2.7}$$

とする．ここで補題 2.11 における z を $m'(k+1)+1$ と見ると

$$w \in M \models (w, m'(k+1)+1) = 1 \wedge \forall i < k((m'(i+1)+1)|w) \tag{2.8}$$

を満たす w が取れる．補題 2.7 より

$$u \in M \models uw \equiv 1 \mod m'(k+1)+1 \tag{2.9}$$

で $u < m'(k+1)+1$ を満たす元 u が存在する．ここで $z = \left(\frac{a}{m(k+1)+1}\right)$ とおき，さらに $v = b_k m'(k+1) + z$ とおく．最後に $b' = b_k + uvw$ とおく．帰納法を完成させるために $M \models \forall i < k+1 \left(\frac{b'}{m'(i+1)+1}\right) = \left(\frac{a}{m(i+1)+1}\right)$ を示す．まず $i < k$ のときは式 (2.8) より $(m'(i+1)+1)|w$ であるから b' の定義より

$$\begin{aligned}
\left(\frac{b'}{m'(i+1)+1}\right) &= \left(\frac{b_k + uvw}{m'(i+1)+1}\right) \\
&= \left(\frac{b_k}{m'(i+1)+1}\right) \\
&= \left(\frac{a}{m(i+1)+1}\right) && (\because \text{帰納法の仮定})
\end{aligned}$$

であり，k の場合は

$$\begin{aligned}
uw &\equiv 1 && \mod m'(k+1)+1 && (\because \text{式 } (2.9)) \\
\Rightarrow uvw &\equiv v && \mod m'(k+1)+1 && (\because \text{命題 } 2.13) \\
\Rightarrow (b' =) b_k + uvw &\equiv b + v && \mod m'(k+1)+1 && (\because \text{命題 } 2.13) \\
&\equiv b_k + b_k m'(k+1) + z && \mod m'(k+1)+1 \\
&\equiv b_k(m'(k+1)+1) + z && \mod m'(k+1)+1 \\
&\equiv z && \mod m'(k+1)+1
\end{aligned}$$

より

$$\begin{aligned}\left(\frac{b'}{m'(k+1)+1}\right) &= \left(\frac{z}{m'(k+1)+1}\right) \\ &= z && (\because m' > \max(x,m) \geq m) \\ &= \left(\frac{a}{m(k+1)+1}\right)\end{aligned}$$

Claim の証明終わり．

示した Claim によって特に $k=y$ とすると

$$M \models \forall i < y \left(\frac{b}{m'(i+1)+1}\right) = \left(\frac{a}{m(i+1)+1}\right)$$

を満たす b が存在する．この b から Claim と同様の方法で条件を満たす a' を構成する．つまり，補題 2.11 より

$$w \in M \models (w, m'(y+1)+1) = 1 \wedge \forall i < y((m'(i+1)+1)|w) \tag{2.10}$$

によって w をとり，補題 2.7 から

$$u \in M \models uw \equiv 1 \mod m'(y+1)+1$$

で $u < m'(y+1)+1$ を満たす元 u をとり，$v = bm'(y+1)+x$ とおき最後に $a' = b+uvw$ とおく．このとき $i<y$ なる i については

$$\begin{aligned}\left(\frac{a'}{m'(i+1)+1}\right) &= \left(\frac{b+uvw}{m'(i+1)+1}\right) \\ &= \left(\frac{b}{m'(i+1)+1}\right) && (\because (m'(y+1)+1)|w) \\ &= \left(\frac{a}{m(i+1)+1}\right)\end{aligned}$$

であり，

$$\begin{aligned} uw &\equiv 1 && \mod m'(y+1)+1 \quad (\because \text{式 } (2)) \\ \Rightarrow (a'=)b+uvw &\equiv b+v && \mod m'(k+1)+1 \quad (\because \text{命題 } 2.13) \\ &\equiv b+bm'(y+1)+x && \mod m'(y+1)+1 \\ &\equiv b(m'(y+1)+1)+x && \mod m'(y+1)+1 \\ &\equiv x && \mod m'(y+1)+1 \end{aligned}$$

より

$$\begin{aligned}\left(\frac{a'}{m'(y+1)+1}\right) &= \left(\frac{x}{m'(y+1)+1}\right) \\ &= x && (\because m' > \max(x,m) \geq x)\end{aligned}$$

□

$\mathbb{N}$ 上において使用したペアリング関数は $I\Delta_0$ のもとでそれに期待する性質をすべて証明できる．

定義 2.15.
$$\langle x, y\rangle = z \leftrightarrow 2z = (x+y)(x+y+1) + 2y$$

命題 2.16. 次が成り立つ．

(a) $I\Delta_0 \vdash \forall y(2|y \vee 2|(y+1))$
(b) $I\Delta_0 \vdash \forall x, y \exists! z\, \langle x, y\rangle = z$
(c) $I\Delta_0 \vdash \forall x, y, z(\langle x, y\rangle = z \rightarrow x \leq z \wedge y \leq z)$
(d) $I\Delta_0 \vdash \forall z \exists x, y\, \langle x, y\rangle = z$
(e) $I\Delta_0 \vdash \forall x, y, x', y'(\langle x, y\rangle = \langle x', y'\rangle \rightarrow x = x' \wedge y = y')$

証明. (a) y に関する帰納法で示す[*4]．$y = 0$ なら $2|0$ より自明．帰納法の仮定理より $(2|y \vee 2|(y+1))$ であるので場合分けを行う．$2|(y+1)$ なら明らかなので，$2|y$ だとする．このとき $2z = y$ たる $z \leq y$ が存在し，$2(z+1) = y+2$ より $2|((y+1)+1)$.

(b) 唯一性は明らか．全域性に (a) を使う．

(c) (d) (e) $\mathbb{N}$ 上でペアリング関数の性質を示した際の議論を形式化すればよい． □

すこし脱線するが，このペアリング関数を用いることで Σ_n 論理式中の各ブロックにある量化は一つに書き換えられること，言い換えれば $I\Delta_0$（を含意するすべての理論）において，変数の数は本質的でないということを確認しておこう．

定義 2.17. 帰納的に以下で任意自然数個のペアリングを定義する $(k \geq 3)$.

$$\langle x_1, x_2, ..., x_k\rangle = z \leftrightarrow \exists y \leq z(\langle x_1, y\rangle = z \wedge \langle x_2, ..., x_k\rangle = y)$$

命題 2.18. 各 $k \geq 3$ についても以下が成り立つ．

(a) $I\Delta_0 \vdash \forall x_1, ..., x_k \exists! z\, \langle x_1, ..., x_k\rangle = z$
(b) $I\Delta_0 \vdash \forall x_1, ..., x_k, z(\langle x_1, ..., x_k\rangle = z \rightarrow x_1 \leq z \wedge \cdots \wedge x_k \leq z)$
(c) $I\Delta_0 \vdash \forall z \exists x_1, ..., x_k\, \langle x_1, ..., x_k\rangle = z$
(d) $I\Delta_0 \vdash \forall x_1, ..., x_k, x'_1, ..., x'_k(\langle x_1, ..., x_k\rangle = \langle x'_1, ..., x'_k\rangle \rightarrow x_1 = x'_1 \wedge \cdots \wedge x_k = x'_k)$

証明. k に関する帰納法で容易に確認できる． □

この命題から，$z = \langle x_1, ..., x_k\rangle$ は変数の数を明示せずに $z = \langle \overline{x}\rangle$ と書くことが許される．

命題 2.19. 任意の Σ_n 論理式 $\exists \overline{y}_1 \forall \overline{y}_2 \cdots Q\overline{y}_n \varphi(\overline{x}, \overline{y})$ (Q は n に応じて $\forall$ か $\exists$ のいずれかで,φ は Δ_0論理式) に対し，次を満たす Δ_0 論理式 ψ が存在する．

$$I\Delta_0 \vdash \forall \overline{x}(\exists \overline{y}_1 \forall \overline{y}_2 \cdots Q\overline{y}_n \varphi(\overline{x}, \overline{y}) \leftrightarrow \exists z_1 \forall z_2 \cdots Q z_n \psi(\overline{x}, \overline{z}))$$

[*4] このくらい帰納法など使わずとも示せそうだが，$\mathbb{Z}[X]^+ \models \neg(2|X) \wedge \neg(2|(X+1))$ なので本質的に帰納法が必要．

証明. ψ として

$$\exists \overline{y}_1 \leq z_1 \exists \overline{y}_2 \leq z_2 \cdots \exists \overline{y}_n \leq z_n \left(\varphi(\overline{x}, \overline{y}) \wedge \bigwedge_{i=1}^{n} z_i = \langle y_i \rangle \right)$$

が条件を満たす．これは明らかに Δ_0 であり，同値性もペアリングの性質から簡単に確認できる． □

定義 2.20 (ゲーデルの β 関数).

$$(x)_y = z \leftrightarrow \exists a, m \leq x \left[\langle a, m \rangle = x \wedge \left(\frac{a}{m(y+1)+1} \right) = z \right]$$

次のうち (d) がコードの延長に関わる最も本質的な性質である．次節の便利な結果はほぼ全てこの (d) によるといってもよい．

補題 2.21. 次が成り立つ．

(a) $I\Delta_0 \vdash \forall x, y \exists! z\ (x)_y = z$
(b) $I\Delta_0 \vdash \forall x, y\ (x)_y \leq x$
(c) $I\Delta_0 \vdash \forall x, \exists y\ (y)_0 = x$
(d) $I\Sigma_1 \vdash \forall x, y, z \exists w\ (\forall i < y ((w)_i = (z)_i) \wedge (w)_y = x)$

証明. (a) $(x)_y = z$ において使われている関数の well-defined 性から明らか．
(b) 明らか．
(c) $y = \langle x, x \rangle$ を考えよ．
(d) 補題 2.14 から明らか． □

補題 2.22 (ゲーデルの補題). $M \models I\Sigma_1$，$n \in \mathbb{N}$ とする．このとき，$x_0, x_1, ..., x_{n-1} \in M$ について

$$M \models (u)_i = x_i$$

が各 $i (< n)$ で成り立つような $u \in M$ が存在する．

証明. 補題 2.21 によって n に関するメタ帰納法で簡単に示せる． □

列 $x_0, x_1, ..., x_{n-1}$ から u を得る操作をコード化とよび，u をその列のコードとよぶ．逆に u から $(u)_i$ を求める操作をデコードとよぶ．

3 形式的体系における関数の原始再帰的定義

$I\Sigma_1$ を含意する理論においては，補題 2.21 を利用することで原始再帰法によって関数を定義することが許される．またそれを応用し，長さと最大値が決まっている有限列をコードする際，そのコードの最小値の上界を与える関数を定義する．

定理 3.1. T を $T \vdash I\Sigma_n$ $(n \geq 1)$ を満たす $\mathscr{L}_A$ 理論とし，関数 f と g はそれぞれ $\mathscr{L}_A$ の Σ_n 論理式 $\varphi(\overline{x}, y)$，$\psi(\overline{x}, y, z, w)$ によって定義されているとする．[*5]いま論理式 $\theta(\overline{x}, y, z)$ を

$$\exists w[(w)_0 = f(\overline{x}) \land \forall i < y((w)_{i+1} = g(\overline{x}, i, (w)_i)) \land z = (w)_y]$$

とすると，このとき

$$T \vdash \forall \overline{x}, y \exists! z \theta(\overline{x}, y, z)$$

が成り立ち，新しい関数記号 h を用意して定義公理 $\forall \overline{x}, y(h(\overline{x}, y) = z \leftrightarrow \theta(\overline{x}, y, z))$ を T に追加することで保存的拡大理論を得る．拡大理論を再び T と書くことにして，この T の元で以下が成り立つ．

$$T \vdash \forall \overline{x}(h(\overline{x}, 0) = f(\overline{x}))$$
$$T \vdash \forall \overline{x}, y(h(\overline{x}, y+1) = g(\overline{x}, y, h(\overline{x}, y)))$$

証明. まず $T \vdash \forall \overline{x}, y \exists! z \theta(\overline{x}, y, z)$ を示す．$\forall \overline{x}, y \exists z \theta(\overline{x}, y, z)$ は y に関する帰納法と補題 2.21(d) から明らか．一意性は以下を示せば十分．

$$\begin{aligned} T \vdash \forall \overline{x}, y, w, w'[&(w)_0 = f(\overline{x}) \land \forall i < y((w)_{i+1} = g(\overline{x}, i, (w)_i)) \land \\ &(w')_0 = f(\overline{x}) \land \forall i < y((w')_{i+1} = g(\overline{x}, i, (w')_i)) \to (w)_y = (w')_y] \end{aligned}$$

任意に $\overline{x}, w, w'$ をとって固定し，y に関する帰納法で $(w)_y = (w')_y$ と仮定すれば

$$(w)_{y+1} = g(\overline{x}, y, (w)_y) = g(\overline{x}, y, (w')_y) = (w')_{y+1}$$

となるのでよい．残りの主張は明らか． □

この定理によって以降 $I\Sigma_n$ を含意する任意の理論 T において，$\Sigma_n(T)$ 論理式によって定義されている関数 f, g が与えられれば新しい関数 h を

$$\begin{cases} h(\overline{x}, 0) &= f(\overline{x}) \\ h(\overline{x}, y+1) &= g(\overline{x}, y, h(\overline{x}, y)) \end{cases}$$

によって定義し[*6]理論内部で扱えるようにすることもフォーマルな議論として考えて良い．この裏側では定理 3.1 を適用することで関数記号 h とその定義公理を言語や理論に追加し，その拡大を再び同じ記号で表すという一連の操作を行っているのだが，その都度定義公理を正確に書き，この定理に言及して言語と理論の拡大を考えていると断るのは文章の可読性を下げる．したがって以

[*5] より正確を期せば，

$$T \vdash \forall \overline{x} \exists! y \varphi(\overline{x}, y), \quad T \vdash \forall \overline{x}, y, z \exists! w \psi(\overline{x}, y, z, w)$$

であって，新しい関数記号 f, g を用意し，以下の定義公理によって定義による拡大理論をここでは再び T と表記している．

$$\forall \overline{x}, y(f(\overline{x}) = y \leftrightarrow \varphi(\overline{x}, y)), \quad \forall \overline{x}, y, z, w(g(\overline{x}, y, z) = w \leftrightarrow \psi(\overline{x}, y, z, w))$$

[*6] h は $\Sigma_n(T)$ 論理式で定義される

降原始再帰的に関数を定義する際には $h(\overline{x},0)$ と $h(\overline{x},y+1)$ だけを正確に書くことにする．また f,g が $I\Sigma_1$ を含意する理論 U で Σ_1 論理式によって定義されているなら原始再帰法によって h は $\Sigma_1(U)$ 論理式で定義されるので，h は U 上可証再帰的な関数になる．

系 3.2. PA は原始再帰法による関数の定義に閉じる．

以上からすべての原始再帰的関数が $I\Sigma_1$ を含む理論の内部で扱うことが可能になった．また可証再帰的関数を理論に追加しても論理式の階層を本質的に変えない[*7]ことを思い出せば，原子再帰法によって定義した関数を含むような帰納法公理も（適切に保存的な拡大を行った理論のもとで）ある程度自由に扱えることになった．

例 3.3. $I\Sigma_1$ において階乗や指数関数は以下でフォーマルに定義される．

$$\begin{cases} 0! &= 1 \\ (x+1)! &= (x+1)\cdot x! \end{cases} \qquad \begin{cases} 2^0 &= 1 \\ 2^{(x+1)} &= 2\cdot 2^x \end{cases}$$

正確にはそれぞれ以下を定義公理としている．

$$x! = y \leftrightarrow \exists w[(w)_0 = 1 \land \forall i < x((w)_{i+1} = (i+1)(w)_i \land y = (w)_x]$$
$$2^x = y \leftrightarrow \exists w[(w)_0 = 1 \land \forall i < x((w)_{i+1} = 2(w)_i \land y = (w)_x]$$

原始再帰法の他に新しい関数を定義する方法を三つ導入する．一つ目は最小値原理による定義である．$\varphi(\overline{x},y)$ を $\mathscr{L}_A$ 論理式とし，理論 T は $\varphi(\overline{x},y)$ に関する最小値原理 $L_x\varphi$ を含意し，さらに $T\vdash\forall\overline{x}\exists y\varphi(\overline{x},y)$ が成り立つとする．このとき論理式 $\theta(\overline{x},y)$ を

$$\varphi(\overline{x},y)\land\forall y'<y\neg\varphi(\overline{x},y')$$

とすれば最小値原理によって明らかに $T\vdash\forall\overline{x}\exists!y\theta(\overline{x},y)$ であるから，$\forall\overline{x},y(h(\overline{x})=y\leftrightarrow\theta(\overline{x},y))$ によって関数 h が定義できる．この関数の定義の仕方を

$$h(\overline{x}) := \min\{\, y \mid \varphi(\overline{x},y) \,\} \tag{3.1}$$

と書くことにして，これもフォーマルな定義と考える．たとえば既知の関数になるが，$I\Delta_0$ では $\mathrm{suc}(x)=\min\{\, y \mid y>x \,\}$ によって後者関数が定義できる．

次は場合分けによる定義である．$\psi(\overline{x}),\varphi(\overline{x},y)$ を $T\vdash\forall\overline{x}(\psi(\overline{x})\to\exists!y\varphi(\overline{x},y))$ を満たす $\mathscr{L}_A$ 論理式とする．ここでさらに $f(\overline{x})$ を既に別の論理式で定義された関数とするとき，論理式 $\theta(\overline{x},y)$ を

$$(\psi(\overline{x})\to\varphi(\overline{x},y))\land(\neg\psi(\overline{x})\to y=f(\overline{x}))$$

とすれば $T\vdash\forall\overline{x}\exists!y\theta(\overline{x},y)$ であるから，$\forall\overline{x},y(h(\overline{x})=y\leftrightarrow\theta(\overline{x},y))$ によって関数 h が定義できる．この関数の定義の仕方を

$$h(\overline{x}) := \begin{cases} \varphi(\overline{x},y) & \text{if } \psi(\overline{x}) \\ f(\overline{x}) & \text{otherwise} \end{cases}$$

[*7] たとえば可証再帰的関数を含むΔ_0,Σ_3論理式はそれぞれ厳密な意味での $\mathscr{L}_A$の$\Delta_1(I\Sigma_1),\Sigma_3(I\Sigma_1)$ 論理式になる．

と書く[*8].

最後は有界最小化による関数の定義であり，これは一つ前の場合分けによる定義の応用である．$\varphi(\overline{x}, y)$ を $\mathscr{L}_A$ 論理式とし，理論 T は $\varphi(\overline{x}, y)$ に関する最小値原理 $L_y\varphi$ を含意しているとする．このとき $T \vdash \forall \overline{x}((\exists y \varphi(\overline{x}, y) \to \exists! y(\varphi(\overline{x}, y) \land \forall y' < y \neg \varphi(\overline{x}, y'))))$ であるから，

$$h(\overline{x}, z) := \begin{cases} \varphi(\overline{x}, y) \land \forall y' < y \neg \varphi(\overline{x}, y') & \text{if } \exists y \varphi(\overline{x}, y) \\ z + 1 & \text{otherwise} \end{cases}$$

に[*9]よって関数 h が定義できる．この関数の定義の仕方を

$$h(\overline{x}, z) := (\mu y \leq z)[\varphi(\overline{x}, y)]$$

と書くことする．

これまでに見てきたいくつかの補題およびその証明は原子再帰的関数を表に出すことでより簡明に記述できる．とくに重要なものは補題 2.14 であり，その証明をつぶさに観察することによって補題 2.21(d) における w の上界を与えることが次の目標である．

系 3.4. 以下が成り立つ．

(1)

$$\text{Béz}(x, y) := \begin{cases} \min\{\, z \mid z < y \land zx \equiv 1 \mod y \,\} & \text{if } (x, y) = 1 \\ 0 & \text{otherwise} \end{cases}$$

によって $I\Sigma_1$ 上可証再帰的な関数 Béz が定義可能である．

(2)

$$\begin{cases} \displaystyle\prod_{i=0}^{0-1} \{(i+1)x+1)\} & = 1 \\ \displaystyle\prod_{i=0}^{(y+1)-1} \{(i+1)x+1\} & = ((y+1)x+1) \displaystyle\prod_{i=0}^{y-1} \{(i+1)x+1\} \end{cases}$$

によって可証再帰的関数 $\prod_{i=0}^{y-1}\{(i+1)x+1\}$ を定義すると

$$\begin{aligned} I\Sigma_1 \vdash \forall x, y, z(\forall i < y((i+1)x+1, z) = 1 \land z \neq 0 \\ \to (\textstyle\prod_{i=0}^{y-1}\{(i+1)x+1\}, z) = 1 \land \forall i < y((i+1)x+1 | \textstyle\prod_{i=0}^{y-1}\{(i+1)x+1\})) \end{aligned}$$

が成り立つ．

(3) $I\Sigma_1 \vdash \forall x, y[y!(x+1) > x \land \forall i, j < y(i \neq j \to (y!(x+1)(i+1)+1, y!(x+1)(j+1)+1) = 1)]$

---

*8 ここでは場合の数が 2 であるような関数の導入を定義したが，より一般に場合の数は有限なら何通りでもよい．ここで一般的な形で定義しないのは，ただ以降で使わないことによる．

*9 場合分けによって関数を定義する際に，毎度この上段の論理式を書くのは不格好である．そのため記号の乱用だが場合分けによる定義においては $\varphi(\overline{x}, y) \land \forall y' < y \neg \varphi(\overline{x}, y')$ を指して $\min\{\, y \mid \varphi(\overline{x}, y) \,\}$ と書くことにする．この略記を用いるときは，理論が $\varphi(\overline{x}, y)$ に関する最小値原理を含意し，さらに場合分けにおける if の後ろに $\exists y \varphi(\overline{x}, y)$ ないしはそれを含意する論理式を配置すると約束しておく．

証明. それぞれ定理 2.7，補題 2.11，補題 2.12 から明らか． □

Béz については特に $I\Sigma_1 \vdash \forall x, y(\text{Béz}(x,y) \le y)$ に留意せよ．

補題 3.5.

$$
\begin{aligned}
&I\Sigma_1 \vdash \forall x, y, z \exists w < U_p(x,y,z)\ (\forall i < y((w)_i = (z)_i) \land (w)_y = x)\\
&I\Sigma_1 \vdash \forall x, x', y, z(x \le x' \to U_p(x,y,z) \le U_p(x',y,z))\\
&I\Sigma_1 \vdash \forall x, y, y', z(y \le y' \to U_p(x,y,z) \le U_p(x,y',z))\\
&I\Sigma_1 \vdash \forall x, y, z, z'(z \le z' \to U_p(x,y,z) \le U_p(x,y,z'))
\end{aligned}
$$

を満たす $I\Sigma_1$ 上可証再帰的な関数 $U_p(w,x,y)$ が存在する．

証明. 基本的には補題 2.14 を証明をなぞってゆけばよい．補題 2.14 証明中の Claim は y 以下の k についてある条件を満たす b が存在するという主張であるが，この b は帰納的に構成されている．よって b は以下の（k に関する）原始再帰的関数の出力と見なすことができる．

$$
\begin{aligned}
F(x,y,a,m,0) &= 0\\
F(x,y,a,m,k+1) &= F(x,y,a,m,k) + \{\text{Béz}(\textstyle\prod_{i=0}^{k-1}\{(i+1)m'\}, m')\\
&\quad \times (F(x,y,a,m,k)m'(k+1) + \left(\frac{a}{m(k+1)+1}\right))\\
&\quad \times \textstyle\prod_{i=0}^{k-1}\{(i+1)m'+1\}\}
\end{aligned}
$$

ただしここで m'は $(y+1)!\max(x,m)$ の略記である．

[*10]つまり，Claim を書き換えることによって以下が成り立つ．

$$
I\Sigma_1 \vdash \forall k \le y \forall i < k \left(\frac{F(x,y,a,m,k)}{m'(i+1)+1}\right) = \left(\frac{a}{m(i+1)+1}\right)
$$

次に $b = F(x,y,a,m,y)$ とおけば，補題 2.14 証明中の a' は以下のように取れる．

$$
a' = b + \{\text{Béz}(\textstyle\prod_{i=0}^{y-1}\{(i+1)m'\}, m') \times (bm'(y+1)+x) \times \prod_{i=0}^{y-1}\{(i+1)m'+1\}\}
$$

ただしここで m'は $(y+1)!\max(x,m)$ の略記である．

この a' を上から押さえる便利な関数を考えたい．そのために F をすべてのパラメーターで上から押さえる補助関数 G を次の様に定める．F と G の違いは $\left(\frac{a}{m(k+1)+1}\right)$ を $m(k+1)+1$ に，$\text{Béz}(\prod_{i=0}^{k-1}\{(i+1)m'\}, m')$ を m' で置き換えただけである．

$$
\begin{aligned}
G(x,y,m,0) &= 0\\
G(x,y,m,k+1) &= G(x,y,m,k) +\\
&\quad \{m' \times (G(x,y,m,k)m'(k+1) + m(k+1)+1) \times \textstyle\prod_{i=0}^{k-1}\{(i+1)m'+1\}\}
\end{aligned}
$$

[*10] ここで $F(x,y,a,m,0)$ の値はなんでもよい．

明らかに G は x, y, m, k に単調増加し，$F(x, y, a, m, y) \leq G(x, y, m, k)$ である．ここで $H(x, y, m)$ を

$$H(x, y, m) = G(x, y, m, y) + m' \times (G(x, y, m, y)m'(y+1) + x) \times \prod_{i=0}^{y-1}\{(i+1)m' + 1\}$$

とおけば，$a' \leq H(x, y, m)$ であって H は x, y, m に単調増加する．以上から

$$U_p(x, y, z) = w \leftrightarrow \langle H(x, y, z), (y+1)! \max(x, z)\rangle = w$$

とおけば[*11] U_p もまた x, y, z に単調増加し，

$$\langle a', m'\rangle \leq \langle H(x, y, m), m'\rangle \leq \langle H(x, y, \langle a, m\rangle), (y+1)! \max(x, \langle a, m\rangle)\rangle$$

であるから

$$I\Sigma_1 \vdash \forall x, y, z \exists w < U_p(x, y, z)\ (\forall i < z((w)_i = (y)_i) \wedge (w)_z = x)$$

が成り立つ．この U_p が $I\Sigma_1$ 上可証再帰的であることは明らか． □

コードすべき列 $x_0, x_1, ...$ の長さと最大値が初めから分かっている場合にはコードそれ自体を上から押さえる関数が U_p を使って構成できる．

系 3.6. 次を満たす $I\Sigma_1$ 上可証再帰的な関数 $F(u, y)$ が存在する．

$$\begin{aligned}
&I\Sigma_1 \vdash \forall c, u, y[\forall i < y((c)_i \leq u) \rightarrow \exists c' \leq F(u, y)(\forall i < y((c')_i = (c)_i))] \\
&I\Sigma_1 \vdash \forall u, u', y(u \leq u' \rightarrow F(u, y) \leq F(u', y)) \\
&I\Sigma_1 \vdash \forall u, y, y'(y \leq y' \rightarrow F(u, y) \leq F(u, y'))
\end{aligned}$$

証明.

$$\begin{aligned}
F(u, 0) &= 0 \\
F(u, y+1) &= U_p(u, y, F(u, y))
\end{aligned}$$

が条件を満たすことを示そう．ここで U_p とは先の補題で定義した $I\Sigma_1$ 上の可証再帰的関数である．F が可証再帰的関数であることは明らか．c, u を固定し，y に関する帰納法で示す．$y = 0$ なら示すべきことはなにもない．$\forall i < y+1((c)_i \leq u)$ とすると，帰納法の仮定から $c' \leq F(u, y) \wedge \forall i < y((c)_i = (c')_i)$ を満たす c' が存在する．したがって補題 3.5 から

$$c'' \leq U_p((c)_y, y, c') \wedge \forall i < y((c'')_i = (c')_i) \wedge (c'')_y = (c)_y$$

を満たす c'' が取れる．するとこのとき

$$c'' \leq U_p((c)_y, y, c') \leq U_p(u, y, F(u, y)) = F(u, y+1)$$

が成り立つ．F の単調増加性は U_p のそれから従う．

□

[*11] $U_p(x, y, z) = w$ は $\exists a, m \leq z[z = \langle a, m\rangle \wedge \langle H(x, y, m), (y+1)! \max(x, m)\rangle = w]$ とおいた方がよいと思われるかも知れないが，$\langle a, m\rangle \leq z$ であるので $U_p(x, y, z)$ が z に関して単調に増加するためにはこの方が確実である．

参考文献

[1] Richard Kaye, “Models of Peano Arithmetic” ,（Oxford logic guides, 15）（Oxford science publications）Clarendon Press , Oxford University Press,1991.