

Bounded Second Order Arithmetic

名大多元数理研究科 安本雅洋 (Masahiro Yasumoto)

$L = \langle +, \cdot, <, 0, 1 \rangle$ を算術の言語, first order variablesを小文字 $x, y, \dots$ でsecond order variablesを大文字 $X, Y, \dots$ で表す. $\forall x \in X (x < t)$ の時, X は t でboundされていると呼び, $X < t$ と書く. $\forall x < t, \exists x < t$ を一階の bounded quantifiers, $\forall X < t, \exists X < t$ を二階の bounded quantifiersと呼ぶ. unbounded quantifierを持たないformulaをbounded formulaと呼ぶ.

bounded formulaeのhierarchyを次の様に定義する.

定義. $\Sigma_0^1(BD) = \Pi_0^1(BD)$ を一階のbounded quantifierしか持たないformulae全体とする.

$\varphi(X)$ が $\Sigma_1^1(BD)$ ならば, $\forall X < x \varphi(X)$ は $\Pi_{1+1}^1(BD)$, $\varphi(X)$ が $\Pi_1^1(BD)$ ならば, $\exists X < x \varphi(X)$ は $\Sigma_{1+1}^1(BD)$ である.

次にComprehension Axiomを定義する. 各formula $\varphi(x, y, Y)$ に対して,

定義. $CA(\varphi(x, y, Y)) \equiv \forall y \forall Y \exists X \forall x (x \in X \longleftrightarrow \varphi(x, y, Y))$

Γ をformulaの集合とする時, $\Gamma\text{-}CA = \{CA(\varphi) \mid \varphi \in \Gamma\}$ とする.

各自然数 i に対して公理系 Y_i を次の(1)~(10)で定義する.

- (1) $\forall x (x + 1 \neq 0)$
- (2) $\forall x, y (x + 1 = y + 1 \rightarrow x = y)$
- (3) $\forall x (x \neq 0 \rightarrow \exists y (x = y + 1))$
- (4) $\forall x (x + 0 = x)$
- (5) $\forall x, y ((x + y) + 1 = x + (y + 1))$
- (6) $\forall x (x \cdot 0 = 0)$
- (7) $\forall x, y (x(y + 1) = xy + x)$
- (8) $\forall x, y (x \leq y \longleftrightarrow \exists z (z + x = y))$
- (9) $\forall X (X \neq \emptyset \rightarrow \exists x \in X \forall y \in X (x \leq y))$
- (10) $\Sigma_1^1(BD)\text{-}CA$

上の公理系の(1)~(8)はRobinsonのQと呼ばれているもので, (9)は LNP(least

number principle)と書く. Y_0 のfirst order partは $I\Delta_0$ と同値になり, Y_1 のsecond order partはBussの S_1^1 と同じものとみなすことができる.

X をbounded(i. e. $X < y$)とすると, X の元の数が x 個であるということを考えることができる. これを $\#(X) = x$ と書く.

定義. $\#(X) = x \equiv \exists F (F \text{ is an one-to-one function from } X \text{ onto } x)$

ただし, x は $\{0, 1, 2, \dots, x-1\}$ と同一視するものとする. この定義の右辺のかっこの中は $\Sigma_1^1(BD)$ で書け, また $\exists F$ の F は $2y^2$ でおさえられている. 正確に書くところの右辺は

$$\exists F < 2y^2 (\forall v \in X \exists ! w < x (\langle v, w \rangle \in F) \wedge \forall w < x \exists ! v \in X (\langle v, w \rangle \in F))$$

となる. ただし $\langle v, w \rangle = \frac{1}{2}(v+w)(v+w+1) + v$ とする. X はbounded(i. e. $X < y$)だから $\forall v \in X, \exists v \in X$ はそれぞれ $\forall v < y (v \in X \rightarrow \dots)$, $\exists v < y (v \in X \wedge \dots)$ と書け, 従って $\#(X) = x$ は $\Sigma_1^1(BD)$ である.

定義. $\text{Count}(y) \equiv \forall X < y \exists ! x < y \#(X) = x$

定義. $\text{PHP}(y) \equiv \neg \exists x < y \exists F (F \text{ is an one-to-one function from } x \text{ to } x-1)$

上記と同じ理由で, $\text{PHP}(y)$ は $\Pi_1^1(BD)$ で書けている. また, $\text{Count}(y)$ は $\Sigma_1^1(BD)$ である.

次の定理は容易に証明できる.

定理 1. (1) $Y_1 \vdash \forall y \text{Count}(y)$

(2) $Y_1 \vdash \forall y \text{PHP}(y)$

(3) $Y_0 \vdash \forall y (\text{Count}(y) \rightarrow \text{PHP}(y))$

また, Ajtai[1]より,

定理 2. $\text{Consis}(Y_0 + \neg \exists y \text{PHP}(y))$

が知られている. この論文では, 定理 1 の(3)の逆のimplicationが成立しないことを示す.

定理 3. $Y_0 \vdash \forall y (\text{Count}(y) \leftrightarrow \Phi(y))$ を満たすformula $\Phi(y)$ は $\Sigma_1^1(BD) \cup \Pi_1^1(BD)$ のboolean combinationでは書けない.

定理 4. $\text{Consis}(Y_0 + \forall y \text{PHP}(y) + \exists y \neg \text{Count}(y))$

§ 1. Boolean valued model

N を N の可算 elementary extension, $\delta \in N - N$ とする. $x, i \in N$ に対して, $\text{bit}(x, i)$ を x を2進数で表した時の i 桁目の値とする. すなわち

定義. $\text{bit}(x, i) = j \equiv (j = 0 \vee j = 1) \wedge \exists x_1, x_2 < x (x = x_1 + j \cdot 2^i + x_2 \cdot 2^{i+1} \wedge x_1 < 2^i)$

定義. $M = \{x \in N \mid \forall n \in N (\delta^n < 2^x)\}$

$M = \{X \subset M \mid \exists x \in N \forall i \in M (i \in X \longleftrightarrow \text{bit}(x, i) = 1)\}$

とすると, $\langle M, M, +, \cdot, <, 0, 1 \rangle$ はすべての $n \in N$ に対して Y_n のmodelになっている. ただし一階の変数は M 上を, 二階の変数は M 上を走るものとする. M の元でboundedなものの集合を M_b と書く. すなわち

定義. $M_b = \{X \in M \mid \exists x \in M (X < x)\}$.

$x \in M, X \in M$ に対して,

定義. $(X)_x = \{y \in M \mid \langle x, y \rangle \in X\}$

また, $X \in M_b$ に対して $u(X)$ を $(X)_\alpha \neq \emptyset$ となる最大の $\alpha \in N$ とする.

Lemma 1. (1) $\forall X \in M \forall x \in M ((X)_x \in M)$

(2) $\forall X \in M_b (u(X) \in M)$

証明. Trivial.

我々の目的は, M は変えずに M を $M[G]$ 拡大して $\langle M, M[G] \rangle$ が必要な性質を持つようにすることである. その方法は集合論のBoolean valued extensionと基本的に同じであるが全く同じというわけにはいかない. 以下においては集合論の場合とのちがいを中心に説明する.

まずBoole代数 B を定義する. $v_0, v_1, v_2, \dots, v_{\alpha-1}, v_\alpha, \dots (\alpha \in M)$ を変数とし, (M, M) で生成されるBoolean circuitの全体を考える. すなわち,

定義. $B_1 = \{X \in M_b \mid \forall x ((X)_x = \emptyset \vee \exists s, t \leq x (s \neq t \wedge (X)_x = \{s, t\}))\}$

として, 各 $X \in B_1$ に対して, Boolean circuit $\Phi(X, \alpha)$ を α に関する帰納法で定義する.

$(X)_\alpha = \emptyset$ の時, $\Phi(X, \alpha) = v_\alpha$

$(X)_\alpha = \{\beta, \alpha\}, \beta < \alpha$ の時, $\Phi(X, \alpha) = \neg \Phi(X, \beta)$

$(X)_\alpha = \{\beta, \gamma\}, \beta < \gamma < \alpha$ の時, $\Phi(X, \alpha) = \Phi(X, \beta) \vee \Phi(X, \gamma)$

$\Phi(X) = \Phi(X, u(X))$

$X, Y \in B_1$ に対して, $\neg X, X \vee Y \in B_1$ をそれぞれ $\Phi(\neg X) = \neg \Phi(X)$,
 $\Phi(X \vee Y) = \Phi(X) \vee \Phi(Y)$ を満たすものとする. また $X \in B_1, Z \in M$ に対して,
 $X(Z)$ を変数 v_α に $\alpha \in Z$ の時は 1, $\alpha \notin Z$ の時は 0 を Boolean circuit $\Phi(X)$ の代
 入して得られる真理値とし, $\forall Z \in M (X(Z) = Y(Z))$ の時 $X = Y$ とみなすこと
 により, B_1 は Bool 代数と考えることができる.

定義. $B_0 = \{X \in B_1 \mid X \text{ ; finitie depth}\}$

以下においては特にことわらない限り, $B = B_0$ または B_1 とする.

定義. $M^B = \{X \in M \mid \forall x \in M ((X)_x \in B)\}$

$x, y, z \in M, X \in M^B$ に対して,

定義. $\llbracket x + y = z \rrbracket = 1 \Leftrightarrow x + y = z$
 $\llbracket x \cdot y = z \rrbracket = 1 \Leftrightarrow x \cdot y = z$
 $\llbracket x < y \rrbracket = 1 \Leftrightarrow x < y$
 $\llbracket x \in X \rrbracket = (X)_x$
 $\llbracket \varphi \vee \phi \rrbracket = \llbracket \varphi \rrbracket \vee \llbracket \phi \rrbracket$
 $\llbracket \neg \varphi \rrbracket = \neg \llbracket \varphi \rrbracket$
 $\llbracket \exists x < y \varphi(x) \rrbracket = \bigvee_{x < y} \llbracket \varphi(x) \rrbracket$

定理 5. φ が $\Sigma_0^1(BD)$ -formula ならば, $\llbracket \varphi \rrbracket \in B$.

$\llbracket \exists X < x \varphi(X) \rrbracket = \bigvee \{ \llbracket \varphi(X) \rrbracket \mid X \in M^B, u(X) < x \}$ と定義すると, 一
 般には $\llbracket \exists X < x \varphi(X) \rrbracket \in B_1$ かどうかはわからない.

問題. φ が $\Sigma_0^1(BD)$ -formula ならば $\llbracket \exists X < x \varphi(X) \rrbracket \in B_1$ となるか?

$X \in M$ に対して, $\check{X} \in M^B$ を次の条件を満たすものとする.

$$\forall y ((\check{X})_y = 1_B \Leftrightarrow y \in X)$$

ただし, 1_B は B の最大元とする.

$D \subset B, I \subset B$ を ideal とする.

定義. D is dense over $I \Leftrightarrow \forall X \in B - I \exists Y \in D - I (Y \leq X)$

$F \subset B, \mathcal{M} \subset \mathcal{P}(B)$ として,

定義. F is $\mathcal{M}$ -generic above I

$$\Leftrightarrow \forall D \in \mathcal{M} (D \text{ が dense over } I \text{ ならば, } (F \cap (D - I)) \neq \emptyset)$$

定義. $I \subset B$; M -complete

$$\Leftrightarrow \forall X \in M^B \forall Y \in M \forall x \in M (\forall y \in Y ((X)_y \in I) \rightarrow \bigvee_{\substack{y \in Y \\ y < x}} (X)_y \in I)$$

$$m(X) = (\{Y < \max(X) \mid X(Y) = 1\} \text{ の個数}) \leq 2^{\max(X)} \\ \text{(ただし個数は } N \text{ の中で数える.)}$$

$I_0 = \{X \in B \mid m(X) \in M\}$ とおくと, I は M -complete.

I_0 は最小の M -complete ideal になっている.

例. $\mu \in N - N$,

$\Gamma_\mu = \{f \in N \mid f \text{ is a code of one-to-one function}$
with $\text{dom}(f) \subset \mu - 1, \text{ range}(f) \subset \mu\}$

$X \in B$ に対して, $\Gamma(\Phi(X)) \subset K$ を $\Phi(X)$ の complexity の induction で定義する.

$$\Gamma(\vee \alpha) = \begin{cases} \{f \in \Gamma_\mu \mid f(\langle \alpha \rangle_0) = \langle \alpha \rangle_1\} & \text{if } \alpha < \mu(\mu - 1) \\ \phi & \text{otherwise} \end{cases}$$

$$\Gamma(\neg \Phi(X)) = K - \Gamma(\Phi(X)), \quad \Gamma(\Phi(X) \vee \Psi(X)) = \Gamma(\Phi(X)) \vee \Gamma(\Psi(X))$$

$$m_1(X) = (\Gamma(\Phi(X)) \text{ の個数}) \quad (N \text{ の中で個数を数える.})$$

$I_1 = \{X \in B \mid m_1(X) \in M\}$ とおくと, I_1 は M -complete.

Lemma 2. I を M -complete ideal, $\mathcal{M} \subset \mathcal{P}(B)$, $X \in M^B$, $x \in M$ は次の条件を満たすとする.

$$(1) \quad \forall X \in M^B \{Z \in B \mid \exists y \in M (Z \leq (X)_y)\} \in \mathcal{M}$$

$$(2) \quad \bigvee_{y < x} (X)_y = 1_B$$

この時, ultra filter G が $\mathcal{M}$ -generic above I ならば, $(X)_y \in G$ となる $y < x$ が存在する.

証明. $D = \{Z \in B \mid \exists y < x (Z \leq (X)_y)\} \in \mathcal{M}$ とおく. まず D は dense over I になっていることを示す. $W \in B - I$ を任意にとると,

$$\bigvee_{y < x} ((X)_y \wedge W) = W \notin I$$

I ; M -complete だから, $(X)_y \wedge W \notin I$ となる $y < x$ が存在する. $(X)_y \wedge W \leq (X)_y$ だから, $(X)_y \wedge W \in D - I$. $(X)_y \wedge W \leq W$ だから D は dense over I になっている.

G は $\mathcal{M}$ -genericだから、 $Z \in G \cap D$ となる Z がある。 D の定義より $Z \leq (X)_y$ となる $y < x$ が存在し、この y に対して $(X)_y \in G$ となっている。

以下に於いては特にことわらない限り常に次の2条件を仮定しているとする。

- (1) G はnonprincipal ultra filterで $\mathcal{M}$ -generic above I .
- (2) $\forall Y \in M^B \{Z \in B \mid \exists y \in M(Z < (Y)_y)\} \in \mathcal{M}$

$X \in M^B$ に対して、 $i_G(X) = \{x \in M \mid (X)_x \in G\}$, $M[G] = \{i_G(X) \mid X \in M^B\}$ と定義し、 $\langle M, M[G], +, \cdot, <, 0, 1 \rangle$ をgeneric extensionと呼ぶ。

定理6. $i_G(\check{X}) = X$

証明. trivial

Cor. $M \subset M[G]$

$x_1, \dots \in M$, $X_1, \dots \in M^B$ とする。

定理7. φ を $\Sigma_1^1(BD)$ -formula, I を M -completeなideal, ultra filter G を $\mathcal{M}$ -generic above I とすると,

$$\langle M, M[G] \rangle \models \varphi(x_1, \dots, i_G(X_1), \dots) \Leftrightarrow \llbracket \varphi(x_1, \dots, X_1, \dots) \rrbracket \in G$$

証明. φ が一階のformulaの時は、 $\llbracket \varphi \rrbracket = 0$ または1であるから明らか。

φ がatomicの時、一階のformulaでないのは $x \in X$ の形の時のみ。

$$\llbracket x \in X \rrbracket \in G \Leftrightarrow (X)_x \in G \Leftrightarrow \langle M, M[G] \rangle \models x \in i_G(X)$$

$\varphi \equiv \neg \psi$, $\psi \wedge \chi$ の時は明らか。

$\varphi \equiv \exists x < y \varphi(x)$ の時。

$$\begin{aligned} \llbracket \exists x < y \varphi(x) \rrbracket \in G &\Leftrightarrow \bigvee_{x < y} \llbracket \varphi(x) \rrbracket \in G \\ &\Leftrightarrow \exists x < y (\llbracket \varphi(x) \rrbracket \in G) \quad (\text{Lemma 2}) \\ &\Leftrightarrow \langle M, M[G] \rangle \models \exists x < y \varphi(x) \end{aligned}$$

Lemma 3. $\langle M, M[G] \rangle \models LNP$

証明. 任意の空でない $X \in M[G]$ をとると、 $M[G]$ の定義より $i_G(X) = X$ となる $\underline{X} \in M^B$ が存在する。 $Y \in M^B$ を次の条件を満たすようにさだめる。

$$\forall x \in M((Y)_x = (\underline{X})_x - \bigvee_{y < x} (\underline{X})_y)$$

X は空でないから $z \in X$ がある.

$$\bigvee_{x \leq z} (Y)_x = \bigvee_{x \leq z} (\underline{X})_x = \llbracket \exists x \leq z (x \in \underline{X}) \rrbracket \geq \llbracket z \in \underline{X} \rrbracket \in G$$

Lemma 2 より, $(Y)_x \in G$ となる $x \leq z$ が存在する. この x に対して,

$$\begin{aligned} \llbracket x \in \underline{X} \wedge \forall y \in \underline{X} (x \leq y) \rrbracket &\geq (\underline{X})_x \wedge \bigwedge_{y \leq z} ((\underline{X})_y \rightarrow \llbracket x \leq y \rrbracket) \\ &= (\underline{X})_x \wedge \bigwedge_{y < x} \neg (\underline{X})_y = (Y)_x \in G \end{aligned}$$

となり, 定理 7 より,

$$\langle M, M[G] \rangle \models x \in X \wedge \forall y \in X (x \leq y)$$

Lemma 4. $\langle M, M[G] \rangle \models \Sigma_0^1(\text{BD})\text{-CA}$

Proof. $\varphi(x)$ を $\Sigma_0^1(\text{BD})$ -formula とする. すべての $x \in M$ に対して $(Y)_x =$

$\llbracket \varphi(x) \rrbracket$ となる $Y \in M^B$ が存在する. この Y に対して,

$$\begin{aligned} x \in i_G(Y) &\Leftrightarrow (Y)_x = \llbracket \varphi(x) \rrbracket \in G \\ &\Leftrightarrow \langle M, M[G] \rangle \models \varphi(x) \end{aligned}$$

従って, $\{x \in M \mid \langle M, M[G] \rangle \models \varphi(x)\} = i_G(X) \in M[G]$.

Lemma 3, 4 より

定理 8. I を M -complete なイデアル, G を nonprincipal ultra filter で $\mathcal{M}$ -generic above I とする. もしすべての $Y \in M^B$ に対して

$$\{Z \in B \mid \exists y \in M (Z < (Y)_y)\} \in \mathcal{M}$$

ならば, $\langle M, M[G] \rangle \models Y_0$ になる.

問題. 上の定理 8 と同じ仮定のもとで, $\langle M, M[G] \rangle \models Y_1$?

定理 9. $\Phi(X)$ を Σ_0^1 -formula とすると,

$$\langle M, M \rangle \models \exists X \Phi(X) \Leftrightarrow \langle M, M[G] \rangle \models \exists X \Phi(X)$$

証明. $\Rightarrow$ は明らか. $\Leftarrow$ を証明する.

$\langle M, M[G] \rangle \models \exists X \Phi(X)$ とすると, $\langle M, M[G] \rangle \models \Phi(X)$ となる $X \in M[G]$ が存在する. $\underline{X} \in M^B$ を $i_G(\underline{X}) = X$ とすると, 定理 7 より, $\llbracket \Phi(\underline{X}) \rrbracket \in G$. 従って $\llbracket \Phi(\underline{X}) \rrbracket = Z \neq 0$. $Z \in B$ だから, $Z < x$ となる $x \in M$ が存在する.

$$\bigwedge_{a \in Y} a \wedge \bigwedge_{\substack{a \notin Y \\ a < x}} \neg a \leq Z$$

を満たす元 $Y \in \mathbf{M}$ をとり,

$$F = \{W \in \mathbf{B} \mid W \geq \bigwedge_{\alpha \in Y} v_\alpha \wedge \bigwedge_{\substack{\alpha \notin Y \\ \alpha < z}} \neg v_\alpha \text{ for some } z \in M\}$$

とおくと, F は ultra filter で $\mathcal{M}$ -generic above $\{0\}$. $F \in \mathbf{M}$ だから $\mathbf{M} = \mathbf{M}[F]$ で $i_c(\underline{X}) = Y \in \mathbf{M}$ になる. 再び定理 7 より, $Z \in F$ だから,

$$\langle \mathbf{M}, \mathbf{M} \rangle = \langle \mathbf{M}, \mathbf{M}[F] \rangle \models \Phi(Y)$$

従って

$$\langle \mathbf{M}, \mathbf{M} \rangle \models \exists X \Phi(X).$$

Cor. Φ を $\Sigma^1_1(\text{BD}) \cup \Pi^1_1(\text{BD})$ -formulae の boolean combination とすると,

$$\langle \mathbf{M}, \mathbf{M} \rangle \models \Phi \Leftrightarrow \langle \mathbf{M}, \mathbf{M}[G] \rangle \models \Phi$$

§ 2. この section では $\mathbf{B} = \mathbf{B}_0$ とする.

$$P = \{ \langle A, B \rangle \mid A, B < \delta, A, B \in \mathbf{M}, A \cap B = \emptyset, \\ \#(A \cup B) < \delta - \delta^\varepsilon \text{ for some standard } \varepsilon > 0 \}$$

とおき, 各 $\langle A, B \rangle \in P$ に対して $\Phi(\langle A, B \rangle) = \bigwedge_{\alpha \in A} v_\alpha \wedge \bigwedge_{\alpha \in B} \neg v_\alpha \in \mathbf{B}$ と定義する.

$\mathbf{I}$ を $\mathbf{I} \cap \Phi(P) = \emptyset$ を満たす $\mathbf{B}_0$ の maximal ideal とすると, Håstad の switching Lemma ([2]) より, $\mathbf{I}$ は $\mathbf{M}$ -complete になる. G を ultra filter で $\mathcal{M}$ -generic over $\mathbf{I}$ とする.

定理 10. $\langle \mathbf{M}, \mathbf{M}[G] \rangle \models \neg \text{Count}(\delta)$

証明. $\mathbf{M}[G] \models \text{Count}(\delta)$ と仮定する. $A_c = \bigcup \{A \mid \Phi(\langle A, B \rangle) \in G\}$ とおく.

$\forall \alpha < \delta ((Z)_\alpha = v_\alpha)$ となる $Z \in \mathbf{M}^B$ をとると,

$$i_c(Z) = \{ \alpha < \mu \mid v_\alpha \in G \} = A_c$$

$\langle \mathbf{M}, \mathbf{M}[G] \rangle \models \# A_c = \gamma$ とすると, ある $F \in \mathbf{M}[G]$ が存在して,

$$\langle \mathbf{M}, \mathbf{M}[G] \rangle \models F \text{ is an one-to-one function from } A_c \text{ onto } \gamma.$$

$\underline{F} \in \mathbf{M}^B$ を $i_c(\underline{F}) = F$ となる元とすると定理 7 より,

$$\llbracket \underline{F} \text{ is an one-to-one function from } Z \text{ onto } \gamma \rrbracket \in G.$$

$\mathbf{I}$ が $P \cap \mathbf{I} = \emptyset$ を満たす ideal の maximal なものであり, G は $\mathcal{M}$ -generic above $\mathbf{I}$ であることより, ある $\langle A, B \rangle \in P$ と $W \in \mathbf{I}$ が存在して

$$\llbracket \# Z = \gamma \rrbracket + W \geq \Phi(\langle A, B \rangle) \in G$$

A_c の定義より, $A \subset A_c$, $B \subset \mu - A_c$, $\#(A \cup B) < \mu - \mu^\varepsilon$, $\# A < \gamma$,

$$\#B < \mu - \gamma, \quad \gamma - \#A < \mu^\varepsilon.$$

$$\gamma - \#A \leq \frac{\mu - \#(A \cup B)}{2} \text{の時}$$

$C \subset \mu - A \cup B$, $\#C = \gamma - \#A + 1$ を満たす C をとると

$$\begin{aligned} \#(A \cup C \cup B) &< \mu - \mu^\varepsilon + \gamma - \#A + 1 \\ &\leq \mu - \mu^\varepsilon + \frac{\mu - \#(A \cup B)}{2} + 1 \leq \mu - \frac{\mu^\varepsilon}{2} + 1 \\ &< \mu - \mu^{\varepsilon/2} \end{aligned}$$

だから, $\langle A \cup C, B \rangle \in P$ になる. $\mathcal{M}$ -generic above I を満たす G' で

$\langle A \cup C, B \rangle \in G'$ となるものを取ると, $\langle A, B \rangle > \langle A \cup C, B \rangle$ だから

$$[\#Z = \gamma] + W \geq \Phi(\langle A, B \rangle) > \Phi(\langle A \cup C, B \rangle) \in G'$$

$W \in I$ だから,

$$\mathbf{M}[G'] \models \#ig(Z) = \gamma$$

$A \cup C \subset ig(Z)$ だから,

$$\mathbf{M}[G'] \models \#ig(Z) \geq \#(A \cup C) = \gamma + 1$$

となり矛盾

$$\gamma - \#A > \frac{\mu - \#(A \cup B)}{2} \text{の時は } \gamma - \#B \leq \frac{\mu - \#(A \cup B)}{2} \text{だから, 同様}$$

にして矛盾が導かれる.

定理3の証明.

$\Phi(y)$ を $\Sigma^+(BD) \cup \Pi^+(BD)$ のboolean combinationで,

$$Y_0 \vdash \forall y (\text{Count}(y) \longleftrightarrow \Phi(y))$$

を満たすものとする. $\langle M, \mathbf{M}[G] \rangle \models Y_0$ だから, すべての $y \in M$ に対して,

$$\langle M, \mathbf{M}[G] \rangle \models \text{Count}(y) \longleftrightarrow \Phi(y)$$

定理10より,

$$\langle M, \mathbf{M}[G] \rangle \models \neg \Phi(\delta)$$

$\neg \Phi(y)$ は $\Sigma^+(BD) \cup \Pi^+(BD)$ のboolean combinationで書けるから, 定理9のCor.

より

$$\langle M, \mathbf{M} \rangle \models \neg \Phi(\delta)$$

$\langle M, \mathbf{M} \rangle \models Y_0$ より

$$\langle M, \mathbf{M} \rangle \models \neg \text{Count}(\delta)$$

となり. 矛盾.

References

- [1] Ajtai, M. The complexity of Pigeonhole principle, Proc. IEEE 29th Annual Symp. on Foundation of Computer Science, 346-355 (1988)
- [2] Håstad, J. Computation limits of small depth circuits, ACM Doctoral Dissertation Award 1986, MIT Press (1987).