数理解析研究所講究録
930巻 1995年 10-19

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$x,y,\ldots$でsecond ordervariablesを大文字$X,Y,\ldots$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. $\Sigma^1_0(BD)=\Pi^1_0(BD)$を一階のbounded quantifierしか持たないformulae全体とする.

$\varphi(X)$が$\Sigma^1_i(BD)$ならば, $\forall X<x\,\varphi(X)$は$\Pi^1_{i+1}(BD)$, $\varphi(X)$が$\Pi^1_i(BD)$ならば, $\exists X<x\,\varphi(X)$は$\Sigma^1_{i+1}(BD)$である.

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

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

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) $\forall x,y(x\leqq y\longleftrightarrow\exists z(z+x=y))$
(9) $\forall X(X\neq\phi\rightarrow\exists x\in X\forall y\in X(x\leqq y))$
(10) $\Sigma^1_i(BD)$-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_2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．$\#(X)=x\equiv\exists F(F$ is an one-to-one function from X onto $x)$

ただし，xは$\{0,1,2,\cdots,x-1\}$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$\Sigma^1_0(BD)$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$\forall v<y(v\in X\rightarrow\cdots\cdot)$，$\exists v<y(v\in X\wedge\cdots\cdot)$と書け，従って$\#(X)=x$は$\Sigma^1_1(BD)$である．

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

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

上記と同じ理由で，$PHP(y)$は$\Pi^1_1(BD)$で書けている．また，$Count(y)$は$\Sigma^1_2(BD)$である．

次の定理は容易に証明できる．

定理1．(1)　$Y_1\vdash\forall y\,Count(y)$

(2)　$Y_1\vdash\forall y\,PHP(y)$

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

また，Ajtai[1]より，

定理2．$Consis(Y_0+\neg\exists y\,PHP(y))$

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．$Y_0\vdash\forall y(Count(y)\longleftrightarrow\Phi(y))$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．$Consis(Y_0+\forall y\,PHP(y)+\exists y\neg Count(y))$

§ 1. Boolean valued model

Nを$\mathbb{N}$の可算elementary extension, $\delta \in N - \mathbb{N}$とする. x, i $\in$ Nに対して, 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. $\mathrm{bit}(x, i) = j \equiv (j = 0 \vee j = 1)$
$$\wedge \exists x_1, x_2 < x(x = x_1 + j\,2^i + x_2 2^{i+1} \wedge x_1 < 2^i)$$

定義. $M = \{x \in N \mid \forall n \in \mathbb{N}(\delta^n < 2^\delta)\}$
$$\mathbf{M} = \{X \subset M \mid \exists x \in N \forall i \in M(i \in X \longleftrightarrow \mathrm{bit}(x, i) = 1)\}$$

とすると, $\langle M, \mathbf{M}, +, \cdot, <, 0, 1\rangle$はすべての$n \in \mathbb{N}$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$\mathbf{M}_b$と書く. すなわち

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

$x \in M$, $X \in \mathbf{M}$に対して,

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

また, $X \in \mathbf{M}_b$に対して$u(X)$を$(X)_\alpha \neq \phi$となる最大の$\alpha \in N$とする.

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

(2) $\forall X \in \mathbf{M}_b(u(X) \in M)$

証明. Trivial.

我々の目的は, Mは変えずに**M**を**M**[G]拡大して$\langle M, \mathbf{M}[G]\rangle$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. $v_0, v_1, v_2, \cdots, v_{\alpha-1}, v_\alpha, \cdots (\alpha \in M)$を変数とし, $(M, \mathbf{M})$で生成されるBoolean circuitの全体を考える. すなわち,

定義. $\mathbf{B}_1 = \{X \in \mathbf{M}_b \mid \forall x((X)_x = \phi \vee \exists s, t \leqq x(s \neq t \wedge (X)_x = \{s, t\}))\}$

として, 各$X \in \mathbf{B}_1$に対して, Boolean circuit $\Phi(X, \alpha)$をαに関する帰納法で定義する.

$(X)_\alpha = \phi$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, $\Phi(X, \alpha) = \Phi(X, \beta) \vee \Phi(X, \gamma)$

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

$X, Y \in \mathbf{B}_1$に対して，$\neg X, X \vee Y \in \mathbf{B}_1$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$X \in \mathbf{B}_1$, $Z \in \mathbf{M}$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，$\forall Z \in \mathbf{M}(X(Z)=Y(Z))$の時$X=Y$とみなすことにより，$\mathbf{B}_1$はBool代数と考えることができる．

定義．$\mathbf{B}_0=\{X \in \mathbf{B}_1 \mid X$; finitie depth$\}$

以下においては特にことわらない限り，$\mathbf{B}=\mathbf{B}_0$または$\mathbf{B}_1$とする．

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

$x, y, z \in M$, $X \in \mathbf{M}^{\mathbf{B}}$に対して，

定義．
$$
\begin{aligned}
&[\![x+y=z]\!]=1 &&\Leftrightarrow\quad x+y=z\\
&[\![x \cdot y=z]\!]=1 &&\Leftrightarrow\quad x \cdot y=z\\
&[\![x<y]\!]=1 &&\Leftrightarrow\quad x<y\\
&[\![x \in X]\!]=(X)_x &&\\
&[\![\varphi \vee \phi]\!]=[\![\varphi]\!] \vee [\![\phi]\!] &&\\
&[\![\neg\varphi]\!]=\neg[\![\varphi]\!] &&\\
&[\![\exists x<y\, \varphi(x)]\!]=\bigvee_{x<y}[\![\varphi(x)]\!] &&
\end{aligned}
$$

定理５．φがΣ^1_0(BD)-formulaならば，$[\![\varphi]\!] \in \mathbf{B}$．

$[\![\exists X<x\, \varphi(X)]\!]= \quad \vee\{[\![\varphi(X)]\!] \mid X \in \mathbf{M}^{\mathbf{B}},\ u(X)<x\}$と定義すると，一般には$[\![\exists X<x\, \varphi(X)]\!] \in \mathbf{B}_1$かどうかはわからない．

問題．φがΣ^1_0(BD)-formulaならば$[\![\exists X<x\, \varphi(X)]\!] \in \mathbf{B}_1$となるか？

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

$$\forall y((\check{X})_y=1_{\mathbf{B}} \quad \Leftrightarrow \quad y \in X)$$

ただし，$1_{\mathbf{B}}$はBの最大元とする．

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

定義．$\mathbf{D}$ is dense over $\mathbf{I}$ $\Leftrightarrow$ $\forall X \in \mathbf{B}-\mathbf{I}\ \exists Y \in \mathbf{D}-\mathbf{I}\ (Y \leqq X)$

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

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

$\Leftrightarrow \forall \mathbf{D} \in \mathfrak{M}$($\mathbf{D}$がdense over $\mathbf{I}$ならば，$(\mathbf{F} \cap (\mathbf{D}-\mathbf{I}) \neq \phi)$)

定義. $\mathbf{I}\subset\mathbf{B}$; M-complete

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

$$m(X)=(\{Y<\max(X)\mid X(Y)=1\}\text{ の個数})\leqq 2^{\max(X)}$$

（ただし個数はNの中で数える.）

$\mathbf{I}_0=\{X\in\mathbf{B}\mid m(X)\in M\}$とおくと，$\mathbf{I}$はM-complete.

$\mathbf{I}_0$は最小のM-complete idealになっている.

例. $\mu\in N-\mathbb{N}$,

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

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

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

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

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

$\mathbf{I}_1=\{X\in\mathbf{B}\mid m_1(X)\in M\}$とおくと，$\mathbf{I}_1$はM-complete.

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

(1)　$\forall X\in\mathbf{M}^{\mathbf{B}}\ \{Z\in\mathbf{B}\mid\exists y\in M(Z\leqq(X)_y)\}\in\mathfrak{M}$

(2)　$\bigvee_{y<x}(X)_y=1_{\mathbf{B}}$

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

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

$$\bigvee_{y<x}((X)_y\wedge W)=W\not\in\mathbf{I}$$

$\mathbf{I}$; M-completeだから，$(X)_y\wedge W\not\in\mathbf{I}$となる$y<x$が存在する. $(X)_y\wedge W\leqq(X)_y$だから，$(X)_y\wedge W\in\mathbf{D}-\mathbf{I}$. $(X)_y\wedge W\leqq W$だから$\mathbf{D}$はdense over $\mathbf{I}$になっている.

Gは$\mathfrak{M}$-genericだから，$Z\in G\cap D$となるZがある．Dの定義より$Z\leqq(X)_y$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$\mathfrak{M}$-generic above I．
(2) $\forall Y\in \mathbf{M}^{\mathbf{B}}\ \{Z\in \mathbf{B}\mid \exists y\in M(Z<(Y)_y)\}\in\mathfrak{M}$

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

定理6．$i_G(\check{X})=X$
証明．trivial
Cor．$\mathbf{M}\subset\mathbf{M}[G]$

$x_1,\cdots\in M$，$X_1,\cdots\in\mathbf{M}^{\mathbf{B}}$とする．
定理7．φをΣ^1_0(BD)-formula，IをM-completeなideal，ultra filter Gを$\mathfrak{M}$-generic above Iとすると，
$\langle M,\mathbf{M}[G]\rangle\models\varphi(x_1,\cdots,i_G(X_1),\cdots)\iff [\![\varphi(x_1,\cdots,X_1,\cdots)]\!]\in G$
証明．φが一階のformulaの時は，$[\![\varphi]\!]=0$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．

$$[\![x\in X]\!]\in G\iff (X)_x\in G\iff \langle M,\mathbf{M}[G]\rangle\models x\in i_G(X)$$

$\varphi\equiv\neg\psi$，$\psi\wedge\chi$の時は明らか．
$\varphi\equiv\exists x<y\,\varphi(x)$の時．

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

Lemma 3．$\langle M,\mathbf{M}[G]\rangle\models$LNP
証明．任意の空でない$X\in\mathbf{M}[G]$をとると，$\mathbf{M}[G]$の定義より$i_G(\underline{X})=X$となる$\underline{X}\in\mathbf{M}^{\mathbf{B}}$が存在する．$Y\in\mathbf{M}^{\mathbf{B}}$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．

$$\bigvee_{x\leq z}(Y)_x=\bigvee_{x\leq z}(\underline{X})_x=[\![\exists x\leq z(x\in\underline{X})]\!]\geq[\![z\in\underline{X}]\!]\in G$$

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，

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

となり，定理7より，

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

Lemma 4．$\langle M,\mathbf{M}[G]\rangle\models\Sigma^1_0(\mathrm{BD})\text{-CA}$

Proof．$\varphi(x)$ を $\Sigma^1_0(\mathrm{BD})$-formulaとする．すべての $x\in M$ に対して $(Y)_x=[\![\varphi(x)]\!]$ となる $Y\in\mathbf{M}^B$ が存在する．このYに対して，

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

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

Lemma 3，4 より

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

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

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

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

定理9．$\Phi(X)$ を Σ^1_0-formulaとすると，

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

証明．⇒は明らか．⇐を証明する．

$\langle M,\mathbf{M}[G]\rangle\models\exists X\Phi(X)$ とすると，$\langle M,\mathbf{M}[G]\rangle\models\Phi(X)$ となる $X\in\mathbf{M}[G]$ が存在する．$\underline{X}\in\mathbf{M}^B$ を $i_G(\underline{X})=X$ とすると，定理7より，$[\![\Phi(\underline{X})]\!]\in G$．従って $[\![\Phi(\underline{X})]\!]=Z\neq0$．$Z\in\mathbf{B}$ だから，$Z<x$ となる $x\in M$ が存在する．

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

を満たす元$Y \in \mathbf{M}$をとり，

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

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

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

従って

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

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

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

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

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

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

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

証明．$\mathbf{M}[G] \models \mathrm{Count}(\delta)$と仮定する．$A_G=\bigcup\{A \mid \Phi(\langle A, B\rangle) \in \mathbf{G}\}$とおく．$\forall \alpha<\delta((Z)_\alpha=v_\alpha)$となる$Z \in \mathbf{M}^{\mathbf{B}}$をとると，

$$i_G(Z)=\{\alpha<\mu \mid v_\alpha \in \mathbf{G}\}=A_G$$

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

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

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

$$[\![\underline{F} \text{ is an one-to-one function from } Z \text{ onto } \gamma]\!] \in \mathbf{G}.$$

$\mathbf{I}$が$P \cap \mathbf{I}=\phi$を満たすidealのmaximalなものであり，$\mathbf{G}$は$\mathfrak{M}$-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

$$[\![\# Z=\gamma]\!]+W \geqq \Phi(\langle A, B\rangle) \in \mathbf{G}$$

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

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

$\gamma - \# A \leqq \dfrac{\mu - \#(A \cup B)}{2}$の時

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

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

だから, $\langle A \cup C, B \rangle \in P$になる. $\mathfrak{M}$-generic above $\mathbf{I}$を満たす$\mathbf{G}'$で$\langle A \cup C, B \rangle \in \mathbf{G}'$となるものを取ると, $\langle A, B \rangle > \langle A \cup C, B \rangle$だから

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

$W \in \mathbf{I}$だから,

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

$A \cup C \subset i_{\mathbf{G}'}(Z)$だから,

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

となり矛盾

$\gamma - \# A > \dfrac{\mu - \#(A \cup B)}{2}$の時は$\gamma - \# B \leqq \dfrac{\mu - \#(A \cup B)}{2}$だから, 同様にして矛盾が導かれる.

定理3の証明.

$\Phi(y)$を$\Sigma^1_1(BD) \cup \Pi^1_1(BD)$のboolean combinationで,

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

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

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

定理10より,

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

$\neg \Phi(y)$は$\Sigma^1_1(BD) \cup \Pi^1_1(BD)$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

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

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).