Bounded Arithmetic と初等整数論

——ガウスの整数論の証明論的研究の提唱——

河合文教研　倉田令二朗

1　多項式階層

1.1. $P=NP$(?) 等問題

DTM, $NDTM$ をそれぞれ決定性ないしは非決定性チューリング機械を意味するものとし, Σ を入力アルファベット, Σ^* を Σ 上の有限列の全体とする. $x\in\Sigma^*$ に対し, $|x|$ は x の長さとする.

$P=\{L\subseteq\Sigma^*|$ ある $M(DTM)$ と, 多項式 (自然数係数) $P(n)$ があって

$x\in L\Longleftrightarrow x$ は $P(|x|)$ 時間内に M によって受容される$\}$

$PTC=\{f:\Sigma^*\to\Sigma^*|$ ある $M(DTM)$ と $P(n)$ があって, 任意の $x\in\Sigma^*$ に対し $f(x)$ が $P(|x|)$ 時間以内に計算可能$\}$

$NP=\{L\subseteq\Sigma^*|$ ある $M(NDTM)$ と $P(n)$ があって

$x\in L\Longleftrightarrow x$ は $P(|x|)$ 時間内に M によって受容される$\}$

三大問題 $P=NP$?　$NP=co-NP$?　$NP\cap co-NP=P$?

これらは未解決問題である.

ここに $co-NP=\{\Sigma^*-L|L\in NP\}$

1.2. 主な成果

(1)　NP−完全集合の存在 (Cook 1971)

$\tilde{L}\subseteq\Sigma^*$ が NP−完全集合とはまず(i) $\tilde{L}\in NP$

(ii)　任意の $L\in NP$ に対し, $f\in PTC$ があって, $x\in L\Longleftrightarrow f(x)\in\tilde{L}$

ゆえに $\tilde{L}\in P\Longleftrightarrow P=NP$, $\tilde{L}\in co-NP\Longleftrightarrow NP=co-NP$ となる.

例として命題論理式の充足可能性問題がある.

(2)　NP−完全でない集合

$P\neq NP$ なら, P でも NP−完全でもない NP集合が存在する.

$NP\neq co-NP$ なら, $co-NP$ でも NP−完全でもない NP 集合が存在する

(Ladner 1975 Schöning 1982)

相対化 $A\subseteq\Sigma^*$ に対し "$x\in A$" か否かを1ステップで判定する装置をもったオラクル(神託)つき DTM または $NDTM$, M^A が考えられ, P^A, NP^A, $co-NP^A$ が定義されるが

(3)　ある集合に対しては $P^A=NP^A$, ある集合 A' に対しては $P^{A'}\neq NP^{A'}$ となる

(Backer, Gill, Solovay 1975)

(4)　$P_r\{x\in A\}=\frac{1}{2}$ となるあるランダムオラクルに対して $P_r\{P^A\neq NP^A\}=1$

(Bennett, Gill 1981)

(5) 多項式階層 (Meyer, Stockmeyer 1976) への拡張

$$\Sigma_i^p, \Pi_i^p, \Delta_i^p, \square_i^p \quad (i=1, 2, \cdots\cdots)$$

$$\Delta_1^p = P,\ \Sigma_1^p = NP,\ \Pi_1^p = co-NP,\ \square_1^p = PTC$$

問題の一般化

$$\Sigma_i^p = \Sigma_{i+1}^p(?),\ \Delta_i^p = \Sigma_i^p(?),\ \Sigma_i^p = \Pi_i^p(?),\ \Pi_i^p \cap \Sigma_i^p = \Delta_i^p(?)$$

2 Bounded Arithmetic (Buss1985)

2.1. 言語と公理

(1) 言語 0, S (次のもの), $+$, $\cdot$, $|x|$, $\left\lfloor \frac{1}{2}x \right\rfloor$, $x\#y(=2^{|x|\cdot|y|})$, $\leq$.

(2) $BASIC$ (1)の記号に関する自明の公理

制限論理式の自然な階層 Σ_i^b, $\Pi_i^b(i=0, 1, 2, \cdots\cdots)$ が定義され, これに対して Σ_i^b, Π_i^b は Σ_i^p, Π_i^p と一致する.

(3) 帰納法の公理

$$IND \quad A(0) \wedge \forall x(A(x) \supset A(Sx)) \supset \forall x A(x)$$

$$PIND \quad A(0) \wedge \forall x\left(A\left(\left\lfloor \frac{1}{2}x \right\rfloor\right) \supset A(x)\right) \supset \forall x A(x)$$

$$LIND \quad A(0) \wedge \forall x(A(x) \supset A(Sx)) \supset \forall x A(x|)$$

(4) S_2^i, T_2^i, S_2T_2

$$S_2^i = BASIC + \Sigma_i^b - PIND (= BASIC + \Sigma_i^b - LIND)\ i=0, 1, 2, \cdots\cdots$$

$$T_2^i = BASIC + \Sigma_i^b - IND \quad i=0, 1, 2, \cdots\cdots$$

$$S_2^{-1} = BASIC \quad S_2 = \bigcup_i S_2^i \quad T_2 = \bigcup_i T_2^i$$

2.2. わかっていること

(1) $S_2^i \subseteq T_2^i \subseteq S_2^{i+1}$. $=$ か $\subsetneq$ か不明

(2) $T_2^i = S_2^{i+1} \Longrightarrow \Sigma_{i+2}^b = \Pi_{i+2}^b$

(3) $f \in \square_i^p \Longleftrightarrow f$ is Σ_i^b-definable in S_2^i(項 t と Σ_i^b-論理式 A があって

$$S_2^i \vdash (\forall \vec{x})(\exists y \leq t(\vec{x}))A(\vec{x}, y),\ (\forall \vec{x})(\exists ! y)A(\vec{x}, y)$$

$$f(\vec{x}) = y \Longleftrightarrow N \models A(\vec{x}, y)$$

(4) $NP = co-NP \Longleftrightarrow$ ある Consistent, Bound, Finite extensin R of S_2^1 があってすべての $A \in \Pi_1^p$ に対して

$$R \vdash A(\vec{a}) \supset [\exists y P_r f_R(y, \ulcorner A(I_{\vec{a}}) \urcorner)]$$

[ ] は $\exists y P_r f_R(y, \ulcorner A(I_{\vec{x}}) \urcorner)$ —— $I_{\vec{x}}$ は $\vec{x}$ に対応する項——の形式化

(5) S_2 の弱さ

(a) S_2 で 2^x が定義されない. $S_2 \nvdash \forall x \exists y(x = |y|)$

(b) S_2 の中で命題論理のカット消去定理が証明できない

(c) $S_2 \nvdash Con(S_2^{-1})$

すなわち S_2 は多項式階層の証明論的定式化には十分であるが，証明論の古典的常識が大はばに崩れるのである．

2．3．モダンを越える地平

(1) ポストモダン現象としての $P=NP$ 等問題

以上見たように $P=PN$ 等，問題は，モダンのただ中(コンピュータサイエンス)から生じ，かつ差異化——計算可能性一般ではなく，多項式時間内計算可能という tractability にもとづく差異化——をキーワードとする点でポストモダン現象の典型である．

(2) 古典的基礎論との関係

さまざまないかがわしさをもったポストモダンの中で，21 世紀につながる未来展望的ポストモダンを選びわける判定基準は古典に関する新しい知見の開示だといえる．現在，問題へのアプローチの仕方として

1．計算論的（チューリング的）方法

2．証明論的（Bdd Arith 的）方法

3．モデル論的（non standard 的）方法

の 3 つが考えられる．

モデル論的方法の例（Attile Máté の場合）

TA（Truth Arithmetic）の nonstandard model M, N と，non standard number n に対し，N が M の partial extension w, r, to n であるということが定義され，

PA の制限論理 $A(x)$ があってある $m \leq 2^n$ に対し，$A(m)$ は M で真だが N では偽となるならば $NP \neq co-NP$ である．

2．2．(5)で示されたように $P=NP$ 等問題は，とくにその証明論的アプローチにおいて古典的証明論の常識が大きく崩れるという形で，古典との新しい関係が根本的に問われている．おそらく $P=NP$ 問題の解決には 30 年代以降に確立された基礎論の古典を越える何かが要請されているのだ．

だがもう一つのより古典的な古典ととの関係がある．

3 Bdd Arith と初等整数論

3．1．一つの制限論理式が問題

差異を明らかにする問題は何か一つの制限論理式（Budd formula）を見出す問題となる．2．2．(4)の見地からいえば次のような制限論理式 $A(a)$ があれば $NP \neq coNP$ となる．

どんな Consistent, Bounded Finite extension R of S_2^1 をとってきても無限個の n に対して $A(n)$ は真，$R \vdash A(I_n)$ の証明のゲーデル数が 2^n を越える．

Attila Ma'te' の場合も同じである．

3．2．作ることと捜すこと

(1) 竹内外史代の最近の結果

S_2, T_2は2階のBuddArith U_2^i, V_2^iに拡張される．制限論理式$A(a)$に対して$\{x|A(x)\}$を許すものである．U_2^iは$PIND$を，V_2^iはINDをもつ．

竹内氏はFermatの小定理$a^{p-1}\equiv 1(mod, p)$(ここにpは素数，$a<p$)とWilsonの定理$(p-1)!\equiv -1(mod\ p)$はいずれもS_2では証明されないがU_2では証明できることを示し，さらに原始根の存在はV_2では証明できるがU_2ではできない．平方剰余相互法則はV_2でもいえないだろうと予想した．

(2) 制限論理式を見出すということは，捜すことと作ることが考えられるが自然数論においてはキーポイントとなる論理式や関数はたいていその目的のために人工的に作り出されて来た（Gödelの不完全性定理の核になる文，Kleeneの階層定理で扱われる命題，Paris Harringtonの命題等）この点は集合論に対して基礎論の果した役割と対照的である．ここでは現場的意味をもつ命題，連続仮説，Suslin仮説等の独立性等が解明されて来た．Bdd Arithが十分発達した結果，現場的意味をもつ初等整数論の命題の証明論的差異性が問題にされるようになってきたわけである．

3．3．初等的数論の命題の証明論的性格

初等整数論の諸定理がどの体系では証明でき，どの体系ではだめであるかの検討が問題になる．この場合S_2, V_2等の大そう弱い体系が問題になるのであるから集合論にもとずく現代的証明はあまり役に立たない．やはりガウスのDAでなければならない．

DAには更に利点がある．それはガウスが直観主義者，アルゴリズム主義者であったことで，ガウスは実験と表作りのためにアルゴリズムを必要としたのであった．たとえば$\forall x\exists y A(x, y)$の形の定理が問題にされるとき，ガウスはかならず$x$に対して$y$を計算するアルゴリズムを要求した．

このことは命題の型（どの$\sum_i^0$に入るか）とS_2等内における証明法を見やすくする．

DAのすべての命題について，それが真であるというだけでなく，どの階層に入るか，どこで証明されるのか，S_2^iかT_2^iかU_2^iかV_2^iかPAか$(ACA)_0$かを問題にしようというのである．