

## Alexander A. Razborov 氏の業績

町 田 元

第3回 Nevanlinna 賞はステクロフ数学研究所(モスクワ)の A. A. Razborov 氏に授与された。Razborov 氏の主要な業績は計算量理論(computational complexity theory), さらに詳しくいえば, その中の下界の理論(lower bound theory)に関するものである。そこでまず計算量理論に対する簡単な紹介から始めることにする。

## 1. 計算量理論

計算量理論とは, 種々の関数(問題, 言語)に対しそれを計算する(解く, 受理する)ときに必要となる計算量を評価することを目指す理論である。計算量としては Turing 機械などの計算機械による計算時間や記憶領域の使用量をとる場合が標準的であるが, 一方, 関数を計算する論理回路の大きさや深さを計算量とする場合(Boolean complexity theory)や, 主に算術演算を用いて計算が進められる場合には算術演算の実行回数を計算量とする場合(algebraic complexity theory)などがある。これらは互に関連しあっているのだが, Razborov の仕事の主な部分が直接かかわるのは論理回路を対象とする計算量である。

計算量理論では, 例えば, 2つの関数  $f_1, f_2$  についてそれらを計算する際どちらが多く計算量を必要とするか, あるいは, 計算量によって定まる関数(問題)の2つのクラス  $C_1, C_2$  に対しそれらの間に包含関係が成り立つか, また, 成り立つ場合にはその包含関係は真の包含関係であるのか, などが主要な研究テーマとなる。それらの問いに答えるには, 関数  $f$  はある計算量では計算することができないこと, あるいは, クラス  $C$  に含まれない関数が存在することなどを示す必要が生じる。つまり何らかの意味で計算量の下界を示さなければならない。実は, この部分が計算量理論においてもっとも困難であり, また, もっとも魅力に富んだ部分なのである。この方面では, どんな関数に対しどの程度の下界を証明

したかという結果そのものよりも, どのような論法でその結果を得たかという, いわば, ‘証明の手法’の方が重視される傾向がある。下界を示すための証明の手法としてはこれまで対角線論法や数え上げ論法などいくつかの限られた手法しか知られていなかった。Razborov は ‘近似法(approximation method)’ という新しい強力な手法を開発した。また, 後に, 行列を用いる新しい方法も得た。

## 2. ブール関数の計算量

ブール関数の集合  $B$  が完全(complete)であれば, 例えば  $B = \{\text{AND, OR, NOT}\}$  であれば, 任意のブール関数  $f$  を  $B$  の要素から合成することができる。このとき, 合成の中に現われる  $B$  の要素の出現個数の最小値を  $f$  の計算量と定める。ただし, 合成のしかたとして2通りのものを考える。一つは(組合せ)論理回路としての合成であり, もう一つは通常論理式の形での合成である。(論理回路では, あるゲートからの出力を2つ以上のゲートへの入力として用いることが許されるが, 論理式ではそのようなことは許されない。つまり, 論理式の形の合成とは, (入力端子以外の)各ゲートの outdegree をすべて1に制限した形の論理回路に対応する合成である。) 前者による計算量を circuit (size) complexity とよんで  $C^B(f)$  と表わし, 一方, 後者によるそれを formula-size complexity とよび  $L^B(f)$  と表わす。

例えば積和標準形を考えれば, 完全な集合  $B$  と任意の  $n$  変数ブール関数  $f$  に対し  $C^B(f)$  も  $L^B(f)$  も  $O(n2^n)$  であることは明らかであるが, さらに強く Shannon(1942, 1949) や Lupanov(1958, 1962) によって次の結果が得られている。

‘ほとんどすべて’の  $n$  変数ブール関数  $f$  に対し

$$C^B(f) = \Theta\left(\frac{2^n}{n}\right), \quad L^B(f) = \Theta\left(\frac{2^n}{\log n}\right).$$

このように、ブール関数全体を相手にする、いわば、大域的な議論はすでに満足できる域に達していて決着がついているといえる。ところが、話を転じて、ある特定のブール関数  $f$ 、あるいは、特定のブール関数列  $\{f^{(n)}\}$  を対象としてその complexity を考えようとするとも様相は一変して現在のところまだほとんど何もわかっていない。とくに、 $C^B(f)$  や  $L^B(f)$  に対する(自明でない)下界を求める部分が難しく、正確な値でなくオーダーを求めるだけでよいのだが、それでも手段に窮している状態である。因みに、ある極めて‘人工的’な関数列  $\{f^{(n)}\}_{n=1}^{\infty}$  ( $f^{(n)}$  は  $n$  変数ブール関数)に対して

$$C^B(f^{(n)}) \geq 3n-3 \quad (2.1)$$

が証明されているが(Schnorr, N. Blum), これが現在特定の関数に対して証明されている  $C^B$  の下界値の最大のものである(ただし,  $B=2$  変数ブール関数全体).

一般の場合はこのように難しいので、何らかの制限をつけた場合を、つまり、下界が証明しやすいような場合を先に考えてみようとする試みが生じる。 $B$  として完全でない集合をとる場合や、回路の形に制約を設ける場合がその例である。

$B=\{\text{AND, OR}\}$  とすると  $B$  から合成されるブール関数は単調増大関数だけになる。AND ゲートと OR ゲートだけから構成される論理回路を単調論理回路と呼ぶ。任意の(定数関数以外の)単調増大関数  $f$  に対し単調論理回路だけを対象として上記の circuit complexity のような量を定める。

これを monotone (circuit) complexity とよび、 $C^+(f)$  と表わす。Razborov の代表的な仕事はこの monotone complexity に関するものである。 $C^+(f)$  に対してならばある程度大きな下界が証明できそうに思えるが、Razborov が登場するまで、その期待は裏切られ続けた。Tiekenheinrich による次の結果が Razborov 以前に証明された  $C^+$  に関する下界の最大のものである。 $T_k^n$  ( $1 \leq k \leq n$ ) を  $k$  を閾値とする  $n$  変数閾値関数とする。

$$T^{(n+1)}(x_1, \dots, x_{n+1}) = (T_2^n(x_1, \dots, x_n) \wedge x_{n+1}) \vee T_{n-1}^n(x_1, \dots, x_n)$$

とおくとき、(2.2)が成り立つ。

$$C^+(T^{(n+1)}) \geq 4n-8 \quad (2.2)$$

(2.1)と(2.2)の証明および類似の結果の証明ではいずれも論理回路の中のもっとも入力端子に近い部分にしか着目していない。回路の‘上っ面’しか眺めていないわけで、回路のもっと深いところを考慮に入れない限り

よい結果が得られそうにないのは自明の理である。一般の場合はその方法について皆目見当がつかず、依然闇に包まれたままだが、単調論理回路に対しては次節で見るように Razborov が初めて回路の内部を‘のぞき見る’ことに成功したのである。

なお、論理回路の形に制約を設ける例としては、回路の深さを一定の深さに限定する場合がよく考察される。このような制約のもとで考える計算量(ゲートの個数)を bounded-depth complexity とよぶ。これは PLA (programmable logic array) と関連して実用的な意味をもつ計算量である。

### 3. Razborov の代表的な結果とその意味

Razborov の最大の功績は、(1)近似法(approximation method)という新しい強力な証明手法を見出したこと、及び、(2)いくつかのブール関数列にその方法を適用してそれらの関数列の monotone complexity 又は bounded-depth complexity に関する多項式を超える (non-polynomial, superpolynomial) 下界を証明した事である。

本節では、多項式を超える下界が証明された関数列を具体的に紹介し、さらに、それらの結果のもつ意味について簡単に論じる。近似法については次節でその基本的な考え方を紹介する。

1985 年の論文 [3], [4] の中で次の (a), (b) に述べる結果が発表された。これらはこの分野の研究者達を驚愕させずにはおかない衝撃的な結果であった。

#### a) クリーク関数の monotone complexity

有限無向グラフ  $G$  に対し、 $G$  の部分グラフで頂点数  $s$  の完全グラフを  $s$ -クリーク (clique) とよぶ。グラフ  $G$  と正整数  $s$  が与えられたとき  $G$  が  $s$ -クリークをもつかどうかを判定する問題をクリーク問題という。

相異なる 2 頂点の対に対しそれらを結ぶ辺が存在するか否かによって 1 または 0 を対応させることにより、頂点数  $n$  の各グラフに  $\{0, 1\}^m$  の元が自然に対応する。ただし、 $m = {}_n C_2$  とおく。従って、頂点数  $n$  のグラフに対するクリーク問題は一つの  $m$  変数ブール関数として表わすことができる。この関数を  $\text{CLIQUE}_{m,s}$  と表わす。すなわち、

$$\text{CLIQUE}_{m,s}(x_{12}, x_{13}, \dots, x_{n-1,n}) = \bigvee_{I \subseteq \{1, 2, \dots, n\}} \bigwedge_{i < j \in I} x_{ij}$$

このクリーク関数の monotone complexity に関して

Razborov は次のような下界を証明した.

**定理 ([3]).**  $s = \left\lceil \frac{1}{4} \ln m \right\rceil$  とおくと、十分大きな  $m$  に対し

$$C^+(\text{CLIQUE}_{m,s}) = \Omega(m^{c \log m}), \quad c > 0 \quad (3.1)$$

なお、この結果は後に Alon と Boppana (1987) によって  $C^+(\text{CLIQUE}_{m,s}) = \exp(\Omega(n / \log n)^{1/3})$  にまで強められた.

この結果のもつ意味について簡単に述べる. この定理が強い関心をひいた理由は 2 つある. 1 つは前から述べているように、この結果が特定の関数に対する monotone complexity について (変数の個数に関する) 多項式を超える下界を証明した初めての結果だったことである. それ以前には  $4n$  程度の下界しか得られていなかったことを想起していただきたい.

関心をひいたもう一つの理由は、いわゆる

#### $P$ - $NP$ 問題

に関するものである. 決定性 Turing 機械で多項式時間で解くことのできる問題全体のクラスを  $P$  とよび、非決定性 Turing 機械で多項式時間で解くことのできる問題全体のクラスを  $NP$  とよぶ. 定義から直ちに

$$P \subseteq NP$$

が導かれるが、 $P$  と  $NP$  は一致するのか、それとも  $P$  は  $NP$  に真に含まれるのかを問う問題が  $P$ - $NP$  問題である. 1971 年の Cook の論文以後この問題の解決が計算量理論における最大の課題とされてきている. よく知られているように、任意の  $NP$  完全問題  $A$  に対し、 $A \in P$  と  $P \neq NP$  とは同値である. Razborov が考察したクリーク問題は代表的な  $NP$  完全問題の一つであるから、クリーク問題が  $P$  に属すかどうかかわれば  $P$ - $NP$  問題は解決されたことになる.

一方、決定性 Turing 機械の時間計算量とブール関数の circuit complexity の間には密接な関係があり、ある問題  $A$  に対応するブール関数列を  $\{f_A^{(n)}\}$  ( $f_A^{(n)}$  は  $n$  変数ブール関数) とおくと、 $A \in P$  であれば  $f_A^{(n)}$  の circuit complexity  $C(f_A^{(n)})$  は  $n$  に関する多項式程度であることを容易に示すことができる (いま、 $B$  は完全な集合であれば何でもよいので  $B$  を省略して  $C^B$  を  $C$  と書く). 従って、逆に、例えば  $C(\text{CLIQUE}_{m,s}) = \Omega(m^{c \log m})$  のような結果が証明できれば、同時に  $P \neq NP$  が証明できたことになるのである. Razborov の monotone complexity に関する結果の circuit complexity への拡張の可能性が注目を集めたのも蓋し当然のことである.

#### b) 論理パーマネントの monotone complexity

$m \times m$  ブール行列  $X = (x_{ij})$  に対し次のようにして定められる  $n (= m^2)$  変数ブール関数  $PERM_m$  を  $X$  の論理パーマネント (logical permanent) という.

$$PERM_m(x_{11}, x_{12}, \dots, x_{mn}) = \sum_{\sigma \in S_m} \prod_{i=1}^m x_{i\sigma(i)}$$

論理パーマネントに対しても Razborov はやはり多項式を超える下界を証明した.

**定理 ([4]).** 任意の  $\epsilon > 0$  と十分大きな  $m$  に対し

$$C^+(PERM_m) = \Omega(m^{(\frac{1}{16}-\epsilon) \log m}) \quad (3.2)$$

この結果は次のような意味をもつ.  $2m$  個の頂点をもつ 2 部グラフ  $G = (V, E)$  を考える. ( $V = V_1 \cup V_2$ ,  $V_1 \cap V_2 = \phi$ ,  $|V_1| = |V_2| = m$ ,  $E \subseteq V_1 \times V_2$ ). 前項の場合と同様、 $V_1$  の頂点と  $V_2$  の頂点の対に対しそれらの間に辺があるか否かによって 1 又は 0 を対応させる事になると、頂点数  $2m$  の各 2 部グラフに  $\{0, 1\}^n$  の元が対応する. この対応のもとで論理パーマネント  $PERM_m$  は 2 部グラフの集合上の関数と考える事ができる.  $PERM_m$  の値が 1 であるのは対応するグラフが完全マッチング (perfect matching) をもつ場合である. 従って、上記の定理は、2 部グラフが完全マッチングを持つかどうかを判定する関数の monotone complexity が多項式を超える量である事を主張する定理であると解釈できる.

Pratt は 1975 年に circuit complexity と monotone complexity の差について考察し、行列の積の計算に伴う計算量について circuit complexity と monotone complexity の間に僅かながら差があることを示した (前者は  $O(n^{3-\epsilon})$ , 後者は  $\Omega(n^3)$ ). さらに、両者の差が多項式を超える場合があり得ることを予想した.

Hopcroft と Karp (1973) のアルゴリズムを用いると、2 部グラフが完全マッチングを持つかどうかを判定する問題の circuit complexity、即ち  $C(PERM_m)$  について  $C(PERM_m) = O(m^5)$  を示すことができる. この事と Razborov の定理をあわせると、 $PERM_m$  について circuit complexity と monotone complexity の間に多項式を超える差がある事がわかる. Pratt の予想は肯定的に解かれたのである.

なお、E. Tardos (1988) は circuit complexity と monotone complexity の間に指数関数の差がある例を示した.

#### c) 多数決関数の bounded-depth complexity

1981 年に Furst, Saxe と Sipser は次の結果を得た.

Parity 関数は、深さが定数でゲート数が多項式の回路では計算することができない。

これが、回路に強い制約があるとはいえ、多項式を超える計算量の下限を証明した最初の結果であった。

Razborov は 1987 年の論文 [6] において次の結果を証明した。深さが定数  $k$  で、使用するゲートは AND または  $\oplus$  (Exclusive-OR) が交互に繰り返す形の回路に関する circuit complexity を  $C_k^{(AND, \oplus)}$  と表わす (各ゲートの indegree には制限をつけない)。また、 $n$  変数の多数決関数を  $MAJ_n$  と表わす。

定理 ([6]). 任意の定数  $k$  に対し

$$C_k^{(AND, \oplus)}(MAJ_n) = \exp(\Omega(n^{1/(k+1)})) \quad (3.3)$$

証明は (a), (b) と同様に近似法を用いてなされる。この定理の重要性は、内容そのものよりも、近似法が {AND, OR} だけでなく {AND,  $\oplus$ } に対しても適用可能であることを示した点にあるといえよう。なお、{AND,  $\oplus$ } は完全ではないが、これに定数関数 1 を加えた集合 {AND,  $\oplus$ , 1} は完全な集合である。

4. 近似法

前節でとり上げた 3 つの結果 (3. 1), (3. 2), (3. 3) はいずれも近似法 (approximation method) とよばれる手法を用いて証明された。ここでは (3. 1), (3. 2) の場合、つまり monotone complexity の場合に則して近似法の入口の部分を紹介する。

$B_n = \{0, 1\}^n$  のべき集合  $\mathcal{L}_n = \mathfrak{P}(B_n)$  は演算  $\cap, \cup$  に関して束をなす。任意の  $n$  変数ブール関数  $f$  に対し、 $A(f) = f^{-1}(1)$  を対応させることにより  $f$  を  $\mathcal{L}_n$  の要素とみなす。ブール関数  $f, g$  に対する AND, OR の合成には  $A(f), A(g)$  に対する  $\cap, \cup$  の演算がそれぞれ対応する。従って、 $f$  の monotone complexity  $C^+(f)$  は、 $A(x_1), A(x_2), \dots, A(x_n)$  を出発点として  $A(f)$  を得るま

でに施される  $\cap$  と  $\cup$  の個数の最小値に一致する。ただし、これだけでは単なる言葉の言い換えにすぎない。 $\mathcal{L}_n$  全体を考えるのではなく  $\mathcal{L}_n$  の適当な部分束  $\mathfrak{M}$  を選び、 $\mathfrak{M}$  を対象にして上に類似したことを考えていくのが近似法の考え方のポイントである。

$\Omega_n$  の部分束で  $A(0), A(1), A(x_1), A(x_2), \dots, A(x_n)$  を含むものを regular lattice (または legitimate lattice) とよぶ。ブール関数  $f$  と regular lattice  $\mathfrak{M}$  の間の距離  $\rho(f, \mathfrak{M})$  を次のように定める。 $\rho(f, \mathfrak{M})$  は

$$M \subseteq A(f) \cup \bigcup_{i=1}^t \delta_-(M_i, N_i),$$

$$A(f) \subseteq M \cup \bigcup_{i=1}^t \delta_+(M_i, N_i)$$

をみたす  $M, M_i, N_i \in \mathfrak{M}$  が存在する様な  $t$  の最小値。ただし、 $\mathfrak{M}$  に於る join と meet をそれぞれ  $\sqcup, \sqcap$  とおき、

$$\delta_-(M_i, N_i) = (M_i \sqcup N_i) - (M_i \cap N_i),$$

$$\delta_+(M_i, N_i) = (M_i \cap N_i) - (M_i \sqcup N_i)$$

とおく。これは、実は、 $f$  を計算する monotone 回路において AND ゲート, OR ゲートを各々  $\sqcap, \sqcup$  で、また  $A(f)$  を  $M$  で置きかえる、つまり、'近似する' ことに対応する。従って、次の定理が成り立つ。

定理 ([3, 4]). 任意の  $n$  変数単調増大ブール関数  $f$  と任意の regular lattice  $\mathfrak{M} \subseteq \Omega_n$  に対し

$$C^+(f) \geq \rho(f, \mathfrak{M}).$$

この定理により  $C^+(f)$  の下限を求める問題が  $\rho(f, \mathfrak{M})$  の下限を求める問題に還元されたわけで、あとは  $\rho(f, \mathfrak{M})$  の値が大きくなるような regular lattice  $\mathfrak{M}$  をうまく選び、その  $\mathfrak{M}$  に対して  $\rho(f, \mathfrak{M})$  の評価を行えばよい。ただし、 $\rho(f, \mathfrak{M})$  の評価を行う部分は組合せ論的な大変こみいった議論が要求される。

近似法が circuit complexity に対しても適用できれば  $P$ - $NP$  問題の解決に向けて道が拓かれることになるが、現在のところその可能性については不明というしかない。Razborov は論文 [12] において単純な拡張では  $\rho(f, \mathfrak{M}) = O(n^2)$  になってしまうこと、つまり、大きな下限を得ることは期待できないことを示した。しかし一方では、補助変数を用いる形式化を行えば  $C(f)$  に十分近い下限を証明することも可能であることを主張している。

また、かりに近似法を一般の場合に拡張することが困難であるとしても、monotone complexity を考えるだけで  $P$ - $NP$  問題を解決してしまう可能性もある。それには slice 関数とよばれる関数を考えればよい。 $n$  変数ブール関数  $f$  は、 $\sum_{i=1}^n x_i < k$  のとき常に  $f(x_1, \dots, x_n) = 0$  であり、また  $\sum_{i=1}^n x_i > k$  のとき常に  $f(x_1, \dots, x_n) = 1$  であるとき  $k$ -slice 関数とよばれる。Berkowitz (1982) は、任意の slice 関数に対しその circuit complexity と monotone complexity の差は高々多項式程度であることを示した。従って、slice 関数  $f$  の monotone com-

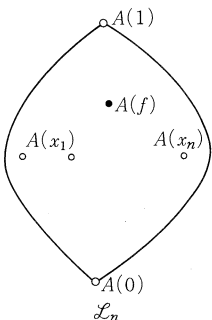


図 1

plexity に対する多項式を超える下界は, そのまま  $f$  の circuit complexity に対する多項式を超える下界へと移行する.  $NP$  完全問題に対応する slice 関数も存在するので, monotone complexity を考察するだけで  $P-NP$  問題を解決する可能性もあることになる.

## 5. 行列法

Razborov は計算量の下界を求める手法として, 近似法のほかに行列法(matrix method)とよばれる手法を導入した. これは Khrapchenko などの仕事に影響を受けたもので, formula-size complexity に関する下界を得るためのものである.

例えば次のような定理が得られている.

**定理** ([10]). 任意の  $n$  変数 ブール関数  $f$  に対し  $U \subseteq f^{-1}(0)$ ,  $V \subseteq f^{-1}(1)$  を任意に定める.  $A$  を (任意の体  $k$  上の)  $|U| \times |V|$  行列とする. このとき

$$L(f) \geq \text{rank}(A) / \max_{R \subseteq \mathcal{R}(U, V)} \text{rank}(A_R)$$

が成り立つ.

ここで, 詳しくは述べないが,  $\mathcal{R}(U, V)$  は  $U \times V$  のある種の部分集合のクラスであり,  $A_R$  は  $A$  の中から  $R$  に対応する成分だけを抜き出して得られる  $A$  の部分行列である.

Razborov は 'MINIMUM COVER' の問題  $MC_n$  にこの方法を適用して

$$L^+(MC_n) \geq n^{\Omega(\log n)}$$

という結果を得た.

この方法の能力等について論文 [16] の中で論じている. 一般の場合への拡張については, 成分が必ずしもすべて指定されていない partial matrix のようなものを用いないとあまり強い結果は得られないようである.

## 6. その他

以上述べたほかに, Razborov は論文 [18] で 'Switching-and-rectifiers' 回路を対象として多数決関数などの対称関数に対する non-linear の下界を証明した.

また, 論文 [13] では, 組みひも群(braid group)において braid が極小であるかどうかを問う問題は co- $NP$  完全であることを示した. これは,  $P=NP$  でない限り, 極小性を判定する速いアルゴリズムは存在しないことを意味する.

最後に, 最近, Wigderson らが communication

complexity という概念を媒介にして単調論理回路の depth complexity に関する linear の下界を得たことを付記しておく. これは formula-size complexity に焼き直すとは指数関数の下界になる.

## Razborov 氏の業績

- [1] Разборов А. А., О системах уравнений в свободной группе (On systems of equations in a free group), Изв. АН СССР, сер. матем., 1984, т. 48, МА, с. 779-832.
- [2] Разборов А. А., Об уравнениях в свободной группе, общие решения которых не представимы в виде суперпозиции конечного числа параметрических функций (On equations in a free group, whose general solution cannot be represented as a superposition of a finite number of parametric functions) — Тезисы 9 всесоюзного симпозиума по теории групп. — М., 1984, с. 54.
- [3] Разборов А. А., Нижние оценки монотонной сложности некоторых булевых функций (Lower bounds for the monotone complexity of some Boolean functions) — ДАН СССР, 1985, т. 281, МА, с. 798-801. (Engl. transl. in : Sov. Math. Dokl. 31, 354-357.)
- [4] Разборов А. А., Нижние оценки монотонной сложности логического перманента (Lower bounds on monotone complexity of the logical permanent) — Матем. зам., 1985, т. 37, вып. 6, с. 887-900. (Engl. transl. in : Mathem. Notes of the Academy of Sci. of the USSR 37, 485-493.)
- [5] Алян С. И., Разборов А. А., Периодические группы и алгебры Ли (Periodic groups and Lie algebras) — Успехи. матем. наук, 1987, т. 42, вып. 2, с. 3-68.
- [6] Разборов А. А., Нижние оценки размера схем ограниченной глубины в полном базисе, содержащем функцию логического сложения (Lower bounds for the size of bounded-depth circuits over a complete basis containing the logical sum) — Матем. зам., 1987, т. 41, вып. 4, с. 598-607. (Engl. transl. in : Mathem. Notes of the Academy of Sci. of the USSR 41 : 4, 333-338).
- [7] Разборов А. А., Нижние оценки монотонной сложности булевых функций (Lower bounds for the monotone complexity of Boolean functions), in : "Proceedings of the International Congress of Mathematicians", Berkeley, California, USA, 1986, vol. 2, p. 1478-1487.
- [8] Разборов А. А., О системах уравнений в свободной группе (On systems of equations in a free group) — кандидатская диссертация, М., 1987.
- [9] Разборов А. А., Формулы ограниченной глубины в базисе  $\{\&, \oplus\}$  и некоторые комбинаторные задачи (Bounded-depth formulas over the basis  $\{\&, \oplus\}$  and some combinatorial problems) — в сб. "Вопросы кибернетики. Сложность вычислений и прикладная математическая логика", М. : 1988, с. 149-166.
- [10] Razborov A. A., Applications of Matrix

- Methods to the Theory of Lower Bounds in Computational Complexity, to appear in *Combinatorica*.
- [11] Adjan S. I., Razborov A. A., Repin N. N., Upper and lower bounds for nilpotency classes of Lie algebras with Engel conditions, in: "Group Theory, Proceedings of the Singapore Group Theory Conference held at the National University of Singapore, June 8-19, 1987", Walter de Gruyter, 1989, pp. 57-75.
- [12] Razborov A. A., On the method of approximations, Proc. of 21st ACM STOC, 1989, pp. 167-176.
- [13] Paterson M. S., Razborov A. A., The set of minimal braids is co-NP-complete, Research report 130 of the Warwick Univ., 1988. Submitted to *Journal of Algorithms*.
- [14] Разборов А. А., Об устойчивых матрицах (On rigid matrices), 1989—представлено в сборник "Вопросы чистой и прикладной математики".
- [15] Razborov A. A., On the Distributional Complexity of Disjointness, to appear in "Proceedings of the ICALP-90".
- [16] Razborov A. A., On submodular complexity measures, preprint, 1989.
- [17] Razborov A. A., The Gap between the Chromatic Number of a Graph and the Rank of its Adjacency Matrix is Superlinear, 1989. Submitted to 'Combinatorial and Algebraic Structures' in the memory of Z. Frolík.
- [18] Разборов А. А., Нижние оценки сложности реализации симметрических булевых функций контактно—вентильными схемами (Lower bounds for the size of switching-and-rectifiers networks realizing symmetric Boolean functions), 1989—представлено в 'Математические заметки'.

(まちはじめ・一橋大学)

## プレ/ポスト コンGRES報告

### Algebraic Geometry and Analytic Geometry, Tokyo 1990

(8月13日～8月17日於都立大)

1. 開催までの経緯. ICM-90 開催を機に、わが国が指導的立場にある代数幾何・解析幾何においても大規模な国際集会をやるという雰囲気が、1989年初頭から徐々に高まってきました。開催地をどこにするかをめぐって少々難航しましたが、同年夏頃までには、Algebraic Geometry and Analytic Geometry なる集会を1990年8月中旬に都立大学で行うことが決定しました。主催責任者には笹倉頌夫氏が就き、私も実務面でお手伝いさせていただくことになりました。数論幾何・双有理幾何・双正則幾何・解析幾何・ケーラー幾何をカバーする大規模な集会であるため、まずプログラム委員として加藤和也・森重文・斎藤恭司・諏訪立雄・桂利行・笹倉・宮岡の7名を選び、招待参加者の選定にあたることとしました。開催に要する資金はかなりの額になると予想されましたが、用途が必ずしも立っていない段階で準備作業に入りました。

1989年秋、第百生命保険が会場と宿舎とを提供してくれるかもしれないとの耳よりな知らせが渡辺公夫氏を通じてもたらされた時から集会開催は果然具体化して参りました。同氏に第百生命との交渉を進めていただく一方、Preliminary announcement を公表するや内外より思わぬ反響があり、開催への期待の大きさを感じないわけにはいきませんでした。実際に出席希望についてアンケートを集めて見ると、希望者の数は当方の予想をはる

かに越え、最終的には海外からの参加者だけで100名以上に達しました。

2. 集会の概要. 'Algebraic Geometry and Analytic Geometry, Tokyo 1990' は、都立大学教養部(午前中の総合講演)および第百生命野沢研修センター(午後の分科会講演)を会場に、8月13-17日の5日間にわたって開催されました。参加者総数は300余名。一時間の総合講演は各分野のバランスを考慮して B. Mazur, C. Soulé, V. Varchenko, C. Simpson, S. Bloch, A. Beilinson, J. Kollár, R. Lazarsfeld, P. Kronheimer, Y.-T. Siu 各氏にお願いしました。午後は45分講演で、水曜日(15日)を除く毎日、4つの分科会(数論幾何・代数幾何・解析幾何 I・解析幾何 II)で各4コマを行いました。分科会のプログラム編成は、各々、加藤和也・森重文・諏訪立雄・藤木明各氏に一任しました。紙数の関係上、講演者の名前だけを挙げておきます。

数論幾何: J. Coates, P. Schneider, 斎藤毅, L. Breen, J. P. Murre, G. Laumon, F. Bogomolov, 塩田徹治, P. Berthelot, V. Mehta, M. Harris, 斎藤秀司, Yu. Zarhin, V. Murty, 藤原一宏, W. L. Baily.

代数幾何: U. Persson, J. Kollár, R. V. Gurjar, N. Shepherd-Barron, E. Viehweg, L. Ein, A. Holme, V. A. Iskovskih, 中山昇, V. V. Shokurov, V. V. Nikulin, 向井茂, M. Reid, Th. Peternell, Z. Ran, F. Catanese.

解析幾何 I: Lê Dũng Tráng, 渡辺公夫, H. Flenner, V. Srinivas, J. H. M. Steenbrink, X. Gomez-Mont, A. Durfee, O. Riemenschneider, M. Falk, 石井志保子, P. Slodowy, J. Damon, C. T. C. Wall, D. Siersma, G.