数理解析研究所講究録
406巻 1980年 1-12

数学者にとっての数式処理

理化学研究所　佐々木建昭

1. はじめに

数学者にとって、数式処理とは二つの顔をもつと考えられる。一つは有力な計算助手としての顔であり、もう一つはその発展のために数学者の助けを求めている顔である。本稿では、数式処理システムないしそれに類似のシステムを使って行われた数学的研究のいくつかを述べ、数式処理システムの有用性を示すとともに、数式処理アルゴリズムのいくつかをとりあげて、アルゴリズム開発が数学者にとっても興味ある研究対象であることを強調したい。

2. 道具としての数式処理

数式処理システムないし類似のシステムが数学研究に利用された例は数多くあろうが、最も成功を収めた代表例は群論であろう。

群論では、計算の大部分が整数演算と集合演算なので、多項式および有理式演算を得意とする数式処理システムを使用するよりも、群論専用にシステムを作成して使用していることが多い。しかしながら、任意精度整数演算とかガーベッジコレクションなどの機能は、群論用システムと言えども不可欠である。さらに、最近の群論用システムをみると、多項式および有理式演算も含むようになっており〔→文献7, 66頁〕, 標準的数式処理システムに近づいているといえる。計算機を群論研究に利用することは古くからなされていたらしく、1960年代の初期にもいくつか論文がみえる。そのころの研究のサーベイについては文献1をみられたい。群論における種々の量を計算機で効率的に計算する方法の研究も非常に盛んで、計算機による記号・代数計算の国際会議には、毎回多数の群論関係の論文が寄せられている〔→文献5, 6, 7, 8〕。

筆者は群論には素人なので、群論用アルゴリズムの解説は手に余る。そこで、計算機を利用して得られた結果のうち、目についたものを2例あげておこう。現在、計算機を利用した群論研究がどのレベルにまで達したか、想像できよう。

Smis は1971年にすでに、位数448,345,497,600の鈴木群や位数5,859,000,000の群 $G_2(5)$ などを計算機で研究している〔→文献5, 23頁〕。また、表1はいくつかの群に対する計算

COMPUTATION OF A CHAIN OF STABILISERS OF

$\underline{G} = \underline{G}^{(1)} \geqq \underline{G}^{(2)} \geqq \ldots \geqq \underline{G}^{(K+1)} = 1$

BY BEING GIVEN A SET OF GENERATORS FOR $\underline{G}$

GROUP	DEGREE	ORDER	TIME(SEC)
SL(2,9)	2	720	0.35
SL(2,31)	2	29,760	1.51
$U_3(3)$	3	6,048	1.78
$SP_4(2)$	4	720	1.45
$SP_4(3)$	4	51,840	7.59
$SP_4(5)$	4	9,360,000	37.79
SZ(8)	4	29,120	3.81
SZ(32)	4	32,537,600	85.40
$U_5(2)$	5	13,685,760	28.77
$U_3(3)$xSL(2,9)	5	4,354,560	9.58
J_2	6	604,800	132.96
$SP_6(2)$	6	1,451,520	22.11
$SP_6(3)$	6	9,170,703,360	154.04
$SP_8(2)$	8	47,377,612,800	308.72
$SP_{10}(2)$	10	24,815,256,521,932,800	3513.59

表1

機処理の結果である。この計算はCDC Cyber 72を用いて、1976年にButlerにより行なわれた〔→文献7, 167頁〕。群論関係の文献をさらにいくつか文末に挙げておいたので、興味ある読者は参照されたい〔→文献2, 3, 4〕

次の応用例として、数式処理システムMACSYMA（本講究録，金田の報告参照）を利用して計算した，Whittaker定数Wの上下限の計算を述べよう〔一方文献9，121頁〕。この定数の定義はさておいて，これまでの最良の上下限は1947年にMacintyreによって得られたもので，

$$0.7259 < W < 0.7378$$

であった。このためW = 2/e ≈ 0.735759であることの予測をする人もいた。Wの効率的な計算法は1944年にLevinsonにより与えられた。$G_0(z)=1$として，次の漸化式

$$G_n(z; z_1, \cdots, z_n) = z^n/n! - \sum_{k=0}^{n-1} z^{n-k}_{k+1} G_k(z; z_1, \cdots, z_k)/(n-k)!$$

で定義される多変数多項式をGončarov多項式と呼ぶ。

$$L_n = \max\{|G_n(0; z_1, \cdots, z_n)| : |z_1| = \cdots = |z_n| = 1\},$$
$$M_n = \max\{|G_n(z_0; z_1, \cdots, z_n)| : |z_0| = \cdots = |z_n| = 1\}$$

と定義する。L_nの値がわかれば，Wは

$$W = \left\{\lim_{n\to\infty} L_n^{1/n}\right\}^{-1}$$

で与えられることがわかっている。nの値が小さいとき，L_n

の定義式より，Gončarov 多項式を直接偏微分して Ln の値を計算できる。n が大きくなるとこの方法では計算が大変になる。そこで，Mn と Ln の間に成立する次の不等式

$$M_n \leqslant \max_{0 \leqslant \alpha \leqslant \pi/2} 2\left\{\sum_{r=1}^{n} \frac{\sin(r\alpha)}{r!} L_{n-r}\right\},$$

$$L_n \leqslant \frac{1}{n}\left\{\sum_{r=1}^{n} L_{r-1} M_{n-r}\right\}$$

を交互に利用して，Ln の値を近似していく。この方法により，Varga と Wang は，1977年に $W > 0.736$ を得た。彼らは同様に上限として $W < 0.737756$ を得ている。したがって，少なくとも $W \neq 2/e$ の予測が間違いであることが示された。

上述の計算では，必要な機能は多項式演算と偏微分，および簡単な方程式系の解法ルーチンであり，不定積分などの高級な機能を必要としていない。このような計算は，数式処理システムの応用例の大部分を占めるものである。しかしながら，単純な計算といえどもバカにならず，アルゴリズムが悪いと計算できるものも計算できなくなる。

筆者らも最近，高次方程式の判別式を計算機で計算したが〔→文献13〕，そこでも効率的なアルゴリズムが不可欠であった。同じ計算は数年前に津田塾の渡辺により試みられたが，変数を一つずつ消去するオーソドックスな方法では，6次方程式

までしか計算できなかった。今回、我々は互換次のシルベスタ行列式を低次に環元する公式（のちに、その公式に類似のものとして、ベズーの公式があることを知った）をみつけ、それによって7次まで計算することができた。表2にその結果を示す。次数が増加すると、数式が予想しないほど膨大になることがよくわかる。

CALCULATION OF DISCRIMINANTS OF EQUATIONS

DEGREE	# OF TERMS	TIME (SEC)
2	2	0.079
3	5	0.107
4	16	0.182
5	59	0.414
6	246	1.565
7	1103	9.91
8	5247	78.5
9	26059	1932.

本講究録の戸田・小野および三井の計算も、数学研究への数学研究への典型的な応用例といえる。特に戸田・小野の計算では、多変数多項式の因数分解の機能が利用されており、しか

もそれが大きな威力を発揮していて興味深い。ほんの最近までは、この種の因数分解はMACSYMAとSCRATCHPAD上でしか実行できなかったが、いまではREDUCE上でも可能になった〔→本講究録，金田の報告参照〕。

3. アルゴリズム開発からみた数式処理

1979年夏に行なわれた記号・代数計算国際会議に，代数学の大家が一人出席していた。彼はクロージング・セッションで特に発言を求め，"自分を含めて数学者の大部分は，問題をいかに解くかには興味をもっても，その効率がどうであるかをほとんど考慮しなかった。しかし，この会議に出席してみて，計算の効率化が重要であり，かつ興味あるものであることを強く認識した。今後もこの種の会議には是非出席したいと思う。"と語り，その場でACMのSIGSAM（Special Interest Group on Symbolic Algebraic Manipulation）の会員になった。ある問題に対する数学的解法が知られていても，それが実用的でないことは非常に多い。実用的な解法を探求することは，それだけでも数学の興味ある対象であることを，このエピソードは如実に物語っている。

たとえば多項式のGCDは，原理的にユークリッドの互除法で計算できることはわかっている。しかし，この方法を多

変数多項式に適用すると，たちまち式が指数関数的に増大してしまう。この式の爆発的膨張を何とか押えようとする努力によって，部分終結式なる概念が導入され，ユークリッドの互除法は驚くほど改善されたのである。より詳しくは，Collins がMSSの会誌に書いた解説〔→ 文献14〕，あるいは拙著〔→ 文献15〕を参照頂きたい。

アルゴリズム開発に対する数学者の代表的貢献例として，ヘンゼルの補題を利用した因数分解法をみよう。Pを正の奇数素数とし，$G_1(x)$ と $H_1(x)$ が mod p で互いに素で，かつ

$$f(x) \equiv G_1(x)\, H_1(x) \pmod{p}$$

を満たすとき，任意の正整数 n に対して

$$F(x) \equiv G_n(x)\, H_n(x) \pmod{p^n},$$
$$G(x) \equiv G_1(x),\ H_n(x) \equiv H_1(x) \pmod{p}$$

を満足する G_n と H_n が存在し，F, G_i, H_i, $i=1,\cdots,n-1$, から有理演算だけで構成できる。これが今世紀初頭にヘンゼルが発見した補題である。

多項式（多変数でもよい）の因数分解法として，1960年代以前に知られていた方法は有名なクロネッカーのアルゴリズムである。このアルゴリズムは，1変数多項式の場合ですら，

次数の増加とともに指数関数的に増加する手間を必要とする。一方，素数Pを法とするGF(P)上では，いくつかの興味深い因数分解法が知られていたが，特に1967年にBerlekampが，小さなPに対して非常に効率的な方法を考案した。翌々年，Zassenhausは，Berlekampの方法で得られるmod pでの因子G_iとH_iを用いて，ヘンゼルの補題により mod p^kでの因子を計算し，係数を調節して整数上での因数分解を計算する方法を発表した。Zassenhausの方法にヒントを得て，MusserとWangはそれぞれ独立に，ヘンゼルの補題を多変数多項式に拡張し，Zassenhausの因数分解法が多変数多項式にまで拡張できることを示した。この方法は非常に効率がよく，変数の数が4～5，次数が6～8，項数50～80程度の多項式でも数秒以内に因数分解する。因数分解についてさらに知りたい読者は，文献16を参照されたい。

現代代数学の系統的手ほどきを受けていない我々計算機屋からみると，GF(P)上での種々の代数的性質やヘンゼルの補題などが思いつける数学者とは，アルゴリズム開発において実にすばらしい存在にみえる。数学者がアルゴリズム開発に重要な貢献をした別の例は，Rischによる初等関数の不定積分アルゴリズムであり〔→文献17〕，また，微分方程式などの数式処理に多くの数学者が興味をもっている〔→文献18，7〕。

さらに、数学者の助けを必要としている広大な分野に、特殊関数の数式処理がある。我が国においても、数式処理システムがかなり普及し、また計算速度を飛躍的に向上させるシステムも近い将来に出現する予定であり、アルゴリズム研究においても一昔ほどの不便さをかこつことはなくなった。さらに、数式処理アルゴリズム研究グループも結成されており、国内外の最新の情報を交換するとともに、研究面で協力し合っている。このグループに、数式処理アルゴリズムに興味をもつ数学者を、1人でも2人でも迎えることを強く希望している。

参考文献

1. J.J. Cannon, "Computers and Group Theory," C.ACM vol. 12 (1969), pp. 3-12.
2. Computational Problems in Abstract Algebra (Proc. Conf. Oxford, 1967), edited by John Leech, Pergamon, Oxford, 1970.
3. Computers in Algebra and Number Theory (Proc. Symp. in Applied Math., New York, 1970), edited by

Garrett Birkoff and Marshall Hall Jr., SIAM-AMS Proc. vol. 4, AMS, 1971.

4. Proc. 2nd Intnl. Conf. on the Theory of Groups (Canberra, 1973), edited by M. F. Newman, Lecture Notes in Math. #372, Springer, Berlin, 1974.

5. Proc. ACM Symp. on Symbolic and Algebraic Manipulation (Los Angels, 1971), edited by S. R. Petrick, ACM SIGSAM, 1971.

6. Proc. European Symp. on Symbolic and Algebraic Manipulation (Stockholm, 1974), ACM SIGSAM Bulletin #31, 1974.

7. Proc. ACM Symp. on Symbolic and Algebraic Computation (New York, 1976), edited by R. D. Jenks, ACM SIGSAM, 1976.

8. Proc. Intnl. Symp. on Symbolic and Algebraic Manipulation (Marseille, 1979), edited by E. Ng, Lecture Notes in Computer Science #72, Springer-Verlag, Berlin-Heidelberg-New York, 1979.

9. Proc. 1979 MACSYMA Users Conf. (Washington, DC, 1979), edited by V. E. Lewis, MIT Laboratory for Computer Science, Cambridge, Mass., 1979.

10. 金田康正，"日本で使用できる数式処理システム，" 本講究録。

11. 戸田英雄・小野令美，" MACSYMAの活用例，" 本講究録。

12. 三井斌友，" 2階導関数を使う Runge-Kutta 型公式の探索，" 本講究録。

13. T. Sasaki, Y. Kanada & Watanabe, "Calculation of Discriminants of High Degree Equations," Tokyo J. Math. (to appear).

14. J. E. Collins, "Computer Algebra of Polynomials and Rational Functions," Amer. Math. Monthly, Vol. 80 (1973), pp. 725 - 755.

15. 佐々木建昭・渡辺隼郎著，数式処理，情報処理学会叢書，（1981年4月頃出版予定）。

16. 佐々木建昭，"数式処理－アルゴリズムの進展，" bit（共立出版）Vol. 12 (1980), pp. 568 - 576.

17. R. H. Risch, "The Problem of Integration in Finite Terms," Trans. AMS vol. 139 (1969), pp. 167 - 189; ———, "The Solution of the Problem of Integration in Finite Terms," Bull. AMS vol. 76 (1970), pp. 605 - 608.

18. 渡辺隼郎著，常微分方程式の数式処理，教育出版，東京，1974年。