松本眞さんの日本学術振興会賞受賞に際して

伏　見　正　則（南山大学数理情報学部）

広島大学大学院理学研究科教授の松本眞さんが「実用上ほぼ理想的な乱数発生法の開発」により第 4 回（平成 19 年度）日本学術振興会賞を受賞されました．まことにおめでたいことで，心よりお祝い申し上げます．日本学術振興会の web ページから授賞理由を引用すると次のようになっています．

「松本眞氏はメルセンヌ・ツイスター(MT)法と呼ばれる乱数発生法を共同研究者と開発した。これは、623 個の 32 ビット長データを、同じ組み合わせが出ないように 6002 桁もの大きな素数（メルセンヌ素数）を周期として入れ替えることにより、乱数を高速に発生させる方法であり、世界標準の乱数発生法として科学技術分野でのさまざまな研究に広く応用されている。乱数を利用して数値実験を行う技法の総称であるモンテカルロ法は、核物理学、流体力学、金融工学など多くの分野で大規模に用いられてきたが、90 年代初頭に乱数発生の偏りによるシミュレーション結果の狂いがいくつも報告され、高速・高品質の乱数発生法の開発が緊急の課題となった。同氏は、数学者として近代数学の成果に基づいた MT 法を開発し、その改良を重ね実用化した。応用面での貢献は極めて大きく、今後の更なる展開が期待される。」

世の中に広く普及しているソフトウェアの中には，未だに古典的な乱数発生法である線形合同法や，理論的な性質がよくわかっていない発生法を標準として採用しているものもあるが，MT 法は数年前に改訂された JIS 規格（JIS Z 9031:乱数発生及びランダム化の手順）に採用され，この規格を基にして ISO の規格を作る作業が現在進行中であるので，近い将来に真の世界標準となることが期待される．

松本さんは，第 4 回船井情報科学振興賞も受賞されていて，その業績の大変詳しく，かつ的確な紹介が二宮祥一さん（東京工業大学）によって数学通信第 10 巻第 2 号（2005 年 8 月）に掲載されているので，ここでは重複は避けて，やや別な観点から補足的な話をさせていただき，上記の授賞理由の最後にある“今後の更なる展開”を期待したいと思う．

コンピュータを使って“乱数らしきもの”(擬似乱数) を作ろうという試みを最初に行ったのは，計算機の発明者 J. von Neumann 自身であるといわれている．D. E. Knuth の有名な著書[2]には，「四則演算によって乱数を作り出そうと試みる者は、言うまでもなく神に背こうとしているのである。」という彼（von Neumann）の言葉が引用されてい

る．乱数の本質は“予測できないもの”であるのに，これを決定論的な方法で作ろうという行為に対する自戒の念をこめての言葉であろう．擬似乱数の生成法の研究は，このような原理的な矛盾の上に立って行われる，数学の中では大変に珍しい研究分野であるといえよう．そこで，実用的な生成法の研究と並んで，“乱数列とは何か？”という根本的な疑問に答えようとする研究も数多く行われて来た．[2]の中には，25 ページにわたって“What is a random sequence?”という表題のもとに乱数列の“種々の定義”が述べられている．また，同書の第 3 版では，さらに 7 ページほどの増補が行われている．たいていの数学の研究が，簡潔で明確な定義から出発するのときわめて対照的である．また，多くの定義があるにもかかわらず，実際に得られる数列が乱数列と見なせるかどうかの判定に役立つような定義もほとんどない. これが,“完璧な乱数生成法”ではなくて，“ほぼ理想的な乱数生成法”というやや苦しい表題にならざるを得ない理由である．

A. N. Kolmogorov も，晩年には乱数の定義に関する論文をいくつか発表している．この中では，最初（？）に発表された[3]が“比較的”実用に近いものである．これは，大ざっぱに言えば，有限長の整数列から種々の選出規則で部分列を抽出したときに，それらの各部分列における整数の度数分布がほぼ一様分布ならば，もとの整数列を乱数列と見なそうとするものである．そして Kolmogorov は，適用する部分列選出規則の個数があまり多くなければ，このような意味での乱数列が存在することを示した．そのような乱数列をどのようにして構成したらよいかは，もちろん示されていない．

部分列選出規則の中で，きわめて単純ではあるが，実用上大切なもののひとつは，“等間隔抽出（系統抽出)”である．これは，たとえば“3 番目ごとに抽出する”ことを意味する．一例を挙げれば，待ち行列のシミュレーションで，一人の客に対して 3 個の乱数を使い，到着時間間隔，サービスの種類，およびサービス時間を定めるものとしよう．この場合には，各目的のために使われるのは，元の数列から 3 番目ごとに抽出された部分数列であるから，この部分数列に現れる各数が互いに独立に一様分布に従っているとみなせることが望ましいことになる．MT 法についても，この観点からの解明が行われると，実用上大変に喜ばしい．

MT 法の基礎になっているのは, GF(2)上の原始多項式を特性多項式とする線形漸化式によって生成される 0-1 系列（1 ビットの系列）であり，電子工学の分野では M 系列あるいは PN 系列などと呼ばれ，古くからシフトレジスターを使って生成し，ノイズとして使われてきたものである．この系列については，度数分布，連，自己相関関数などがわかっていて，対象なベルヌーイ試行系列と類似の性質を持つことが知られている．MT 法は，この 1 ビットの系列を“複雑に組み合わせて”32 ビットの整数の数列を作り出すものと見ることができる．M 系列の持つ性質のうちで，度数分布に関するものは，623

次元の均等分布が保証されているという形で MT 法に継承されているが，MT 法によって生成される数列の連や自己相関関数については，現時点では解明されていない．特に並列計算やグリッドコンピューティングなどに使う場合には，この点の解明がされることが好ましい．

一般に周期を持つ擬似乱数列については，1 周期全体にわたる性質を理論的に解明するのに比べると，一部分の数列の性質を理論的に解明するのは，はるかに難しく，ほとんど見るべき研究成果が無いといってよい状態である．しかし，周期が長くなるほど，実際に使うのはごく一部分になるので，1 周期全体の性質だけでなく，部分についても理論的な性質がわかっていると，実務家にとっては大変ありがたいことは言うまでもない．実際には，たいていの場合理論的な性質が不明なので，統計的検定で補っているが，実際に使うすべての部分について統計的検定を行うのは著しく不便で，ほとんど不可能である．MT 法の周期は $2^{19937}-1$ で，実用上は無限大ともいえるほど長いので，実際に使う部分列の性質が理論的に解明されれば，実務家にとって大きな朗報となる．

以上，MT 法に対して実用上の立場からやや欲張った注文を出し過ぎたような形になってしまったが，現時点で MT 法がほぼ理想的な擬似乱数生成法であることは確かである．今後も松本さんが先頭に立って，さらに理論的な解明や改善が進められていくことを期待している．

参考文献

[1] 伏見正則（1989）：乱数（UP 応用数学選書 12）．東京大学出版会．

[2] Knuth, D. E. (1981): The Art of Computer Programming, Vol. 2: Seminumerical Algorithms, 2nd Ed. Addison-Wesley, Reading, Mass. [渋谷政昭（訳）（1981）：準数値算法/乱数，サイエンス社．]

[3] Kolmogorov, A. N. (1963): On tables of random numbers. Sankhya **A25**, 369-376.

[4] Matsumoto, M. and Nishimura, T. (1998): Mersenne Twister: A 623-dimensionally equi-distributed uniform pseudorandom number generator. ACM Transactions on Modeling and Computer Simulations **8**, 3-30.