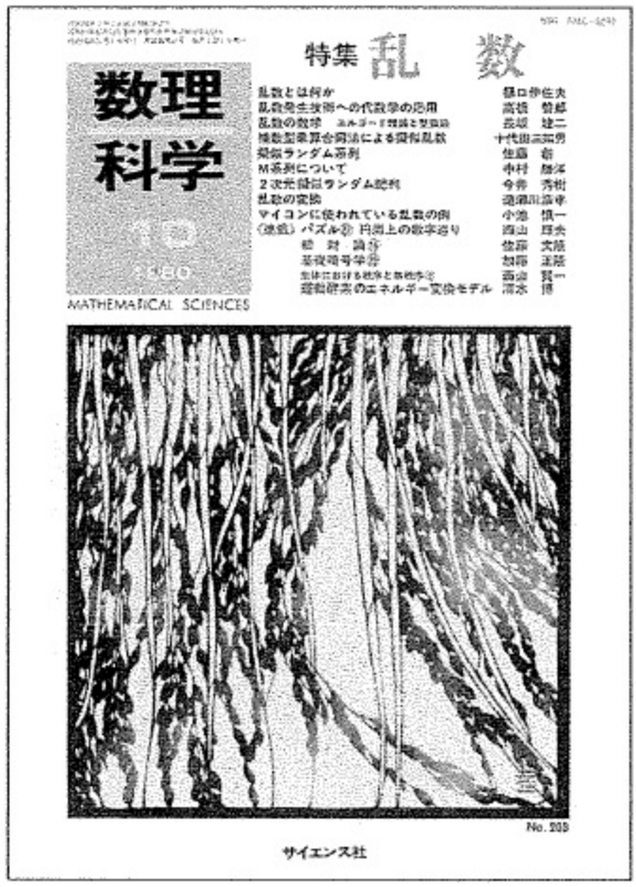
「数理科学」は語る

30年前から現代へのメッセージ

中村　勝洋

1980年10月号

「乱数」の特集の中で「M系列について」と題した記事を書いてからもう30年も経ってしまったのかと今更ながら驚いている．当時企業の中央研究所にいて，その十数年前から始まったデジタル情報通信技術の研究開発の真っ只中にいた．M系列は代表的な擬似乱数列として様々な場面で応用され，また多くの数学的構造と容易に結びつくことから，多くの数理科学者の興味あるいは研究の対象にもなっていた．この頃，現実の場面で求められる乱数列としては，乗数合同法による数列やM系列などの有限長（周期）系列が，所謂“擬似”乱数列として利用され，一応の用は足せていた．しかし，80年代を迎えた前後あたりから，即ち30年ぐらい前から，我が国でも欧米に倣って学会レベルでの開かれた暗号研究が始まるようになり，この分野特有の解読に耐え得る，より乱数性のきちんと定義された乱数列の生成が要求されるようになってきた．概念的には，特に計算量的観点から（擬似）乱数を，“一様分布から多項式時間では識別できない分布”に従って生成される数と定義したとき，擬似乱数の存在条件が一方向性関数の存在と同等であるといったことなどが導かれたりして，活発な研究の進展を見た[1]．



一方，様々な手法で現実的に構成した乱数列の乱数性の判定に関しては，NIST（米国標準技術局）が定めた乱数検定が最近はdefacto的に広く使われている．NIST乱数検定は，現在15個の検定法，計188個の検定項目からなるが，検定法として幾つかの誤りが指摘されている[2]．一部の検定法の理論的誤りは別として，30年前と違い，この間の目覚しいコンピュータの進展による計算能力の増大が統計的検定の計算誤差を浮き彫りにして発見させてくれた面もある．それは，被検定列があくまでも100万ビット長の“有限長”系列でありながら，理想分布として2項分布の代わりに正規分布，多項分布の代わりにχ^2分布，あるいは他の無限長系列を想定した理論分布を用いたことによる計算誤差や，理論分布のパラメータ値の近似誤差による計算誤差が，乱数列としての判定に影響を及ぼす点などの検討が十分でなかったためと考えられる．

また一方，最近のコンピュータの乱数生成ルーチンには，何らかの意味で物理的揺らぎを取り入れたルーチンも備えられ始めており，関連研究も進んでいる．

参考文献

1) O. Goldreich, “Modern Cryptology, Probabilistic Proofs and Pseudorandomness”, Springer-Verlag, 1999.
2) 奥富秀俊，中村勝洋，“NIST乱数検定を用いた合理的なランダム性の判定法に関する考察”，電子情報通信学会論文誌A，Vol.**J93-A**, No.1, pp.11–22, Jan. 2010.

（なかむら・かつひろ，千葉大学グランドフェロー）