ショートノート

擬似乱数生成法の考察 (II)†
——小型計算機用乗算型合同式法のパラメタ選択——

栗田 良春††

著者は，乗算型合同式法による擬似乱数生成式：
$X_{n+1}=a\cdot X_n \bmod m$
のパラメタ a, m の選択法，およびその方法によって選択された a, m の数値についてすでに本誌 (Vol. 17, No. 9) に報告した．この前報では，比較的長いレジスタを対象としたが，数年来の小型計算機の目覚しい普及に伴い，レジスタ長の短い場合 (8-, 12-, 16-, 20- および 24-ビット) のための選択されたパラメタ a, m の数値を提示して前報を補い実用に供する．この選択法は前報と殆んど同じであるが，そのあらましは，m としてレジスタに収まるなるべく大きい素数を選び，この m に対する a として $(X_p, X_{p+1}, \cdots X_{p+n-1})$, $p=0, 1, 2, \cdots$ を n 次元立方体 ($2\leqq n\leqq 5$) の中の点集合とした時に生じる超平面群の規則性が目立たないような m の原始根で系列相関係数がなるべく小さいものを実験的に探索するものである．

1. まえがき

著者は乗算型合同式法による擬似一様乱数生成式：

$$X_{n+1}=a\cdot X_n \bmod m \qquad (1)$$

のパラメタ a, m の選択法，およびその方法によって選択された a, m の数値についてすでに本誌に発表した[1]．(これを以下前報と呼ぶ)．そこでは比較的長いレジスタ (32, 36 および 48 ビット) をもつ計算機を対象としていた．その後，小型計算機の目覚しい普及に伴い，レジスタ長の短い場合の数値の問合せもいくつかあったので，前報を補う意味からも，この選択手続きによる 8, 12, 16, 20 および 24 ビットレジスタ用の a, m の選択された数値を報告する．

2. パラメタ選択法の要約

選択法はほぼ前報の通りであるので，ここではその骨子と前報からの変更点だけを述べる (詳しくは前報を参照して頂きたい)．生成式 (1) について，その性質，規則性およびプログラミングの容易さを考慮に入れて，パラメタ a, m の選択基準を次のようにとる．

i) レジスタ桁数の有効利用．生成列の周期をなるべく大きくすること．

† Consideration of Pseudo-random Number Generators (II) ——Choosing Suitable Parameters of Multiplicative Congruential Methods for Use with Short Registers—— by YOSHIHARU KURITA (2nd div., National Research Laboratory of Metrology (AIST)).

†† 工業技術院計量研究所第2部

表 1 選択された m の値，そのオイラー関数の値および m の原始根 a の選択範囲

Table 1 Some chosen prime numbers m for $X_{n+1}=a\,X_n \bmod m$, values of related Euler function $\varphi(m-1)$ and the interval in which multiplier a (primitive root of m) should be chosen.

	m	$\varphi(m-1)$	$(m/100,\ m-\sqrt{m})$
8	251(=2** 8−2**2−1)	100	(2, 236)
11	2 039(=2**11−2**3−1)	1 018	(20, 1 994)
12	4 093(=2**12−2 −1)	1 200	(40, 4 029)
15	32 257(=2**15−2**9+1)	9 216	(323, 32 077)
16	65 521(=2**16−2**4+1)	13 824	(655, 65 265)
19	524 287(=2**19 −1)	139 968	(5 243, 523 563)
23	8 388 593(=2**23−2**4+1)	4 194 288	(83 886, 8 385 670)

ii) 演算 mod のプログラミング上の問題．生成時間をなるべく小さくすること．

iii) n 次元立方体中の超平面の枚数 ν_n をできるだけ多くすること．

iv) 周期全体の系列相関係数の値 C をできるだけ小さくすること．

まず，m の値として上記の基準 i), ii) を考慮に入れて，**表1**，第2列に示すような素数を選ぶ．(なお表1の第1列はその行の呼び名であって，たとえば Case 11 と呼ぶときは，$m=2^{11}-2^3-1=2,039$ の場合を指すこととする)．この m の決定の後，適当な a を m の原始根(その個数を表1の第3列に示す)の中から選ぶことになるが，前報の場合よりも m が小さいこともあって次の方法によった：$a/m\ll 1$ であるような a は

基準 iv）により避けるべきであるので，aの候補値となる原始根は $m/100$ 付近以上から採り，上限は基準 iii）から$m-\sqrt{m}$ までとする．こうしてきまる区間 $(m/100,\ m-\sqrt{m})$ に含まれる整数の集合を I_m, I_mに含まれる原始根の全体を $G(I_m)$，その要素数を $\#G(I_m)$ とすると，

$\#G(I_m)\simeq(m-\sqrt{m}-m/100)\cdot\varphi(m-1)/m$，ここに φ はオイラーの関数．

である．（表1，第3，4列参照．）

この $G(I_m)$ がaの候補値の全体であり，その各々について基準 iv）：n 次元立方体中の超平面の枚数の計算 $(n\leqslant 5)$ を行うことになるが，中型計算機で調べ上げることのできる候補値の個数は 10^4 個程度であるので Case 19, 23 についてはそれぞれ $G(I_m)$ から 10^4 個をランダムに抽出し，その他の Case については $G(I_m)$ すべてについて，前報で詳述した基準 iii）の篩による選択を行った．なお，この篩の目の粗さは ν_n（n次元超平面の枚数の上限）の 0.8 倍とした．

3. 数値結果

前節で述べた方法で選択されたパラメタaの値の個数は，各mの値について数個から数十個程度にわたるが，これを各mについて2個ずつ視察によって選び出した結果を**表2**に ν_n とCの値と共に掲げる．

4. 結　び

前報の統計的検定の項で述べたような，連の検定など，いくつかの検定では明らかな異常はここでも認め難いので，その詳細は省略する．さらには，この選択法によらずに任意に選び出した原始根をaとして生成した乱数と，ここで選択したパラメタによるそれとの通常の統計的検定による差の検出は難しい場合がありうる．ここで選択したパラメタの値の価値は，ここで用いた基準による“素姓”の保証，すなわち問題となりうる性質のうちのいくつかに対して解答が用意されているという意味で使いやすい点にある．なお，蛇足ながら，ここでは比較的小さいmを扱っているので，これらの数値を用いる場合には，実際に使用する長さが周期 $m-1$ を超えないように留意することが必要である．

表 2　選択されたパラメタ a, m の値およびその最小超平面数の値と系列相関係数の値

Table 1　Number of minimum hyper-planes ν_n (n-dim.) and serial correlation coefficient C of some chosen parameters a, m for $X_{n+1}=a\cdot X_n \bmod m$.

m	a	ν_2	ν_3	ν_4	ν_5	C
251	141	16	6	2	2	-7×10^{-3}
	213	15	5	3	3	4×10^{-3}
2,039	1,498	44	12	6	5	-1×10^{-3}
	1,691	41	11	6	4	1×10^{-3}
4,093	1,621	63	14	8	3	7×10^{-3}
	2,598	59	14	7	5	1×10^{-3}
32,257	1,161	168	30	13	6	3×10^{-5}
	24,622	173	29	14	6	1×10^{-5}
65,521	32,570	252	35	15	8	-2×10^{-3}
	47,871	254	37	16	3	-1×10^{-4}
524,287	304,016	738	86	20	13	-1×10^{-5}
	475,942	724	80	25	13	6×10^{-6}
8,388,593	4,532,816	2,841	184	52	23	1×10^{-7}
	5,762,412	2,961	208	56	20	2×10^{-6}

参考文献

1) 栗田良春：擬似乱数生成法の考察—乗算型合同式法のパラメタ選択と検定—，情報処理，Vol. 17, No. 9, pp. 828-834 (1976).

（昭和56年5月15日受付）
（昭和56年7月13日採録）