擬似乱数に対するランダムウォーク検定 (4)
—反転M系列の統計検定について—

高嶋 恵三 （大阪教育大学）

1 反転多項式と反転M系列

\[ f(x) \] を Galois 体 \( GF(2) \) 上の多項式とする。

\[
f(x) = \sum_{k=0}^{p} c_k x^k, \quad c_0 = c_p = 1, \quad c_k \in GF(2).
\]

更に, \( f(x) \) が原始多項式であるとは:

\[
2^p - 1 = \min \{ n > 0 : f(x) \text{ divides } x^n + 1 \}
\]

が成り立つことである. 式 (1) の \( f(x) \) に対して, その反転多項式 (reciprocal polynomial) \( f^*(x) \) を以下で定義する:

\[
f^*(x) = \sum_{k=0}^{p} c_k x^{p-k} = x^p f\left(\frac{1}{x}\right) \quad (\text{cf.} \ [4]).
\]

\( f(x) \) が原始多項式であれば, その反転多項式 \( f^*(x) \) も原始多項式である. このように, \( f(x) \) と \( f^*(x) \) とは幾つかの代数的な性質を共有することが知られている (cf. [4]).

式 (1) の原始多項式 \( f(x) \) に基づくM系列擬似乱数 \( a_n, n \geq 0, a_n \in GF(2) \) を

\[
a_n = \sum_{k=1}^{p} c_k a_{n-k} \quad (\text{mod} \ 2), \quad n \geq p,
\]

で定義する. ここで, 初期値 \( a_0, \ldots, a_{p-1} \) はすべて \( 0 \), \( (a_j = 0 \text{ for all } j = 0, \ldots, p-1) \) を除いて, 任意に与えられる. この \( f(x) \) を \( a_n \) の feedback polynomial と呼ぶことにする (cf. Jungnickel [3]).

M系列 \( a_n \) (3) に対して, その反転M系列 (reciprocal m-sequence), \( a_n^*, n \geq 0 \) を以下で定義する:

\[
a_n^* = \sum_{k=1}^{p} c_p a_{n-k}^* \quad (\text{mod} \ 2), \quad n \geq p,
\]

ここで \( a_j^* \) の初期値は \( a_j \) の場合と同様に任意に与えられるものとする. \( a_n^* \) は \( a_n \) を逆向きにみた系列, と見なすことができる. また, \( a_n^* \) の feedback polynomial は \( f^*(x) \) である:

\( f(x), \ \deg f = p, \) を feedback polynomial に持つあるM系列擬似乱数 \( \{a_n : 0 \leq n \leq 2^p - 1\} \) を考える. 逆向きにみた系列 \( \{a_n' : 0 \leq n \leq 2^p - 1\} \) を

\[
a_n' = a_{2^{p-2} - n}, \text{ for } 0 \leq n \leq 2^p - 1,
\]

で定義すると \( \{a_n' : 0 \leq n \leq 2^p - 1\} \) は式 (4) を満たす, 即ち, \( \{a_n : 0 \leq n < 2^p - 1\} \) の反転M系列になっている.

- 75 -
注意 一般に、M系列表に対して “特性多項式 (characteristic polynomial)” という用語が用いられる (cf. [1], [4]). しかしながら、この用語はいささか混乱がある。式 (3) で定まるM系列表 a_n に対して、例えば [1] では f(x) を characteristic polynomial と呼ぶのに対して、[4] では、f*(x) をcharacteristic polynomial と呼んでいる。そこで、本報告では characteristic polynomial の代わりに feedback polynomial という用語を用いることにする。

2 ランダムウォークによる統計的検定

以下のような原始5項式に基づくM系列表似乱数とその反転M系列表似乱数に対して以下のようなランダムウォークによる検定を試みた:

<table>
<thead>
<tr>
<th>番号</th>
<th>多項式</th>
</tr>
</thead>
<tbody>
<tr>
<td>P5</td>
<td>x^{61} + x^5 + x^2 + x + 1</td>
</tr>
<tr>
<td>P7</td>
<td>x^{61} + x^7 + x^4 + x + 1</td>
</tr>
<tr>
<td>P8</td>
<td>x^{61} + x^8 + x^7 + x^2 + 1</td>
</tr>
<tr>
<td>P10</td>
<td>x^{61} + x^{10} + x^6 + x^5 + 1</td>
</tr>
<tr>
<td>P47</td>
<td>x^{61} + x^{47} + x^{20} + x^3 + 1</td>
</tr>
<tr>
<td>P53</td>
<td>x^{61} + x^{53} + x^{23} + x^3 + 1</td>
</tr>
</tbody>
</table>

これらの5項式 P5, P7, P8, P10, P47, P53, とそれらの反転5項式 R5, R7, R8, R10, R47, R53, は次数が245以下の3項式および4項式を倍数に持たないことを数式処理ソフト Mathematica を用いて確かめた。これは、これらの原始5項式を feedback polynomial に持つM系列表似乱数の長さ245以下のHamming weights は同じ3次、4次の moments を持つ、ことを意味する(cf. [2], [5])。

3 検定結果について

表 (1), (2), (3), (4) に検定結果の一部を示す。これらの検定結果から原始5項式 P5, P7, P8, P10 に基づくM系列表似乱数とそれらの反転5項式 R5, R7, R8, R10 に基づくM系列表似乱数の間には maximum test, sojouran time test に関して、統計的に明らかな差異が認められる。一方、Mathematica の計算結果から予想されるように Hamming weight test に関しては、M系列とその反転M系列との間に統計的差異は認められない。

M系列表似乱数の理論は Galois 体 GF(2) およびその拡大体 GF(2^n) の理論事実するのものであることを考慮すると、上記の統計的検定結果は原始5項式とその反転5項式の間に代数的差異があること示している。しかしながら、原始多項式とその反転多項式に関するどの様な代数的性質において差異があるのか、という問題は未解決である。


参考文献

### Table 1: P5 and R5, 100 samples

<table>
<thead>
<tr>
<th>Test type</th>
<th>Path length</th>
<th>N (×1000)</th>
<th>P5 $K_{30}^{-}$</th>
<th>R5 $K_{30}^{-}$</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>95%~99%</td>
<td>99%~</td>
</tr>
<tr>
<td>HW</td>
<td>160</td>
<td>100</td>
<td>14</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>240</td>
<td>100</td>
<td>9</td>
<td>3</td>
</tr>
<tr>
<td>MX</td>
<td>160</td>
<td>100</td>
<td>25</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td>240</td>
<td>100</td>
<td>14</td>
<td>6</td>
</tr>
<tr>
<td>SJ</td>
<td>160</td>
<td>100</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>240</td>
<td>100</td>
<td>6</td>
<td>1</td>
</tr>
<tr>
<td>FP $\tau = 12$</td>
<td>160</td>
<td>100</td>
<td>8</td>
<td>1</td>
</tr>
<tr>
<td>$\tau = 20$</td>
<td>160</td>
<td>100</td>
<td>6</td>
<td>2</td>
</tr>
</tbody>
</table>


### Table 2: P7 and R7, 100 samples

<table>
<thead>
<tr>
<th>Test type</th>
<th>Path length</th>
<th>$N$ (×1000)</th>
<th>P7 $K_{30}$</th>
<th>R7 $K_{30}$</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>95%~99%</td>
<td>99%~</td>
</tr>
<tr>
<td>HW</td>
<td>160</td>
<td>100</td>
<td>15</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td>240</td>
<td>100</td>
<td>12</td>
<td>2</td>
</tr>
<tr>
<td>MX</td>
<td>160</td>
<td>100</td>
<td>10</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>240</td>
<td>100</td>
<td>7</td>
<td>1</td>
</tr>
<tr>
<td>SJ</td>
<td>160</td>
<td>100</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>240</td>
<td>100</td>
<td>9</td>
<td>0</td>
</tr>
<tr>
<td>FP$_r = 12$</td>
<td>160</td>
<td>100</td>
<td>7</td>
<td>1</td>
</tr>
<tr>
<td>r = 20</td>
<td>240</td>
<td>100</td>
<td>5</td>
<td>2</td>
</tr>
</tbody>
</table>

### Table 3: P8 and R8, 100 samples

<table>
<thead>
<tr>
<th>Test type</th>
<th>Path length</th>
<th>$N$ (×1000)</th>
<th>P8 $K_{30}$</th>
<th>R8 $K_{30}$</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>95%~99%</td>
<td>99%~</td>
</tr>
<tr>
<td>HW</td>
<td>160</td>
<td>100</td>
<td>20</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>240</td>
<td>100</td>
<td>10</td>
<td>2</td>
</tr>
<tr>
<td>MX</td>
<td>160</td>
<td>100</td>
<td>10</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>240</td>
<td>100</td>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td>SJ</td>
<td>160</td>
<td>100</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>240</td>
<td>100</td>
<td>6</td>
<td>1</td>
</tr>
<tr>
<td>FP$_r = 12$</td>
<td>160</td>
<td>100</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>r = 20</td>
<td>240</td>
<td>100</td>
<td>4</td>
<td>0</td>
</tr>
</tbody>
</table>

### Table 4: P10 and R10, 100 samples

<table>
<thead>
<tr>
<th>Test type</th>
<th>Path length</th>
<th>$N$ (×1000)</th>
<th>P10 $K_{30}$</th>
<th>R10 $K_{30}$</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>95%~99%</td>
<td>99%~</td>
</tr>
<tr>
<td>HW</td>
<td>160</td>
<td>100</td>
<td>12</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>240</td>
<td>100</td>
<td>11</td>
<td>5</td>
</tr>
<tr>
<td>MX</td>
<td>160</td>
<td>100</td>
<td>20</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td>240</td>
<td>100</td>
<td>16</td>
<td>5</td>
</tr>
<tr>
<td>SJ</td>
<td>160</td>
<td>100</td>
<td>7</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>240</td>
<td>100</td>
<td>7</td>
<td>1</td>
</tr>
<tr>
<td>FP$_r = 12$</td>
<td>160</td>
<td>100</td>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>r = 20</td>
<td>240</td>
<td>100</td>
<td>7</td>
<td>3</td>
</tr>
</tbody>
</table>