Publ. RIMS, Kyoto Univ.
10 (1974), 77-89

On the Periods of Certain Pseudorandom Sequences

By

Masahiko SATO*

In [1], Rader et al. gave a fast method for generating pseudorandom sequences. Concerning these sequences, Moriyama et al. [2] made a research including the computational results by computers.

In this paper we shall study the periods of these sequences, and give an affirmative answer to the following conjecture presented in [2]:

"Let $k(n)$ be the maximum period of n-bit pseudorandom sequences generated by the Rader's method. Then $k(2n)=2k(n)$ for all n."

We shall also prove a number of algebraic properties of the periods, and give an efficient algorithm for computing $k(n)$.

We remark here that in this paper we are interested only in the algebraic properties of these sequences and not in the randomness of these sequences.

§1. Introduction

To make the present note self-contained, we begin with the definition of the pseudorandom sequences given by Rader et al.

An n-bit pseudorandom sequence $E=(E_i)_{i=0,1,\cdots}$ is defined inductively by:

$$(1)\qquad \begin{cases} E_0=e_0, \\ E_1=e_1, \\ E_{i+2}=D(E_{i+1}\oplus E_i) \qquad (i\geqq 0), \end{cases}$$

where e_0 and e_1 are given n-bit patterns, $\oplus$ denotes 'exclusive-or' of two n-bit patterns, and D is the operator rotating the argument cyclically 1 bit to the right. For instance, if $n=3$ and $e_0=011$, $e_1=001$, we have: $E_0=011$, $E_1=001$, $E_2=001$, $E_3=000$, $E_4=100$, ..., $E_{14}=001$, $E_{15}=011$,

Communicated by S. Takasu, September 18, 1973.
* Graduate School, Department of Mathematics, Kyoto University, Kyoto.

$E_{16}=001,\ldots$ We denote the j-th component of E_i by $E_i(j-1)$. Thus $E_i=E_i(0)\ldots E_i(n-1)$. In the original paper by Rader et al., D is replaced by T_p which performs the p-bit cyclic rotation. Let us call this sequence $(n;\,p)$-*sequence*. For the study of the period of the sequence, however, we have only to consider the case $p=1$. For, if $\mathrm{GCD}(p, n)=m\neq 1$, the sequence (E_i) can be reduced to m $(n/m;\,1)$-sequences (E_i^j) $(j=1,\ldots, m)$, where $E_i^j(l)=E_i(j+(l-1)n/m)$. The period k of the sequence (E_i) is therefore obtained by $k=\mathrm{LCM}(k_1,\ldots, k_m)$, where k_j is the period of (E_i^j). If $\mathrm{GCD}(p, n)=1$, (E_i) is isomorphic to the $(n;\,1)$ sequence (E_i'), where $E_i'(j)=E_i(p^j \bmod n)$.

Now, let us consider the following sequence $(F_i)_{i=0,1,\cdots}$ of elements in R, where R is a commutative ring with 1 and f_0, f_1, x are fixed elements in R.

$$\begin{cases} F_0=f_0\,, \\ F_1=f_1\,, \\ F_{i+2}=x(F_{i+1}+F_i) \qquad (i\geqq 0)\,. \end{cases} \tag{2}$$

Define the generating function $F\in R[[Y]]$ of (F_i) as follows:

$$F=\sum_{i=0}^{\infty} F_i Y^i. \tag{3}$$

From (2) and (3), by a simple computation, we obtain

$$\begin{aligned} F&=(f_0(1-xY)+f_1 Y)/(1-xY-xY^2) \\ &=(f_0+(f_1-f_0x)Y)\sum_{d=0}^{\infty} x^d Y^d(1+Y)^d\,. \end{aligned} \tag{4}$$

Hence,

$$F_i=f_0\sum_{\substack{d+j=i\\ j\leqq d}}\binom{d}{j}x^d+(f_1-f_0x)\sum_{\substack{d+j+1=i\\ j\leqq d}}\binom{d}{j}x^d \tag{5}$$

To see the relation between (1) and (2) more clearly, the following fact should be mentioned. The operator D in (1) has the property that D^n is the identity operation. So if we put

(6) $$R=R_n=\boldsymbol{F}_2[X]/(X^n-1)$$

and $x=c(X)$, where c: $\boldsymbol{F}_2[X]\to\boldsymbol{F}_2[X]/(X^n-1)$ is the canonical mapping, *then we can identify* (2) *and* (1) *under the following correspondence*:

$$\left.\begin{matrix}\text{an element of } R \\ \sum_{i=0}^{n-1} a_iX^i \quad (a_i=0,1)\end{matrix}\right] \longleftrightarrow \left[\begin{matrix}\text{an } n\text{-bit pattern} \\ a_0a_1\dots a_{n-1} \quad (a_i=0,1)\end{matrix}\right.$$

$$\text{multiplication by } X \longleftrightarrow \text{operation of } D$$

$$+ \longleftrightarrow \oplus$$

So in the following we shall consider (2) instead of (1).

To decompose R_n into a direct sum, let

$$X^n-1=\prod_{i=1}^{h} P_i^{e_i}$$

be a factorization of X^n-1, where P_i's are distinct irreducible factors of X^n-1.

Since the derivative of X^n-1 is nX^{n-1}, $X^s-1=0$ has no repeated roots, i.e. $e_i=1$ for all i, when $n=s$ is odd. (In the following s always denotes an arbitrary *odd* number.) Hence we have the following isomorphism.

(7) $$R_s\cong\boldsymbol{F}_2[X]/(P_1)\oplus\cdots\oplus\boldsymbol{F}_2[X]/(P_h).$$

Now suppose n is even and $n=2^u s$. Then since $X^n-1=X^{s2^u}+1=(X^s+1)^{2^u}$, we have

$$X^n-1=P_1^{2^u}\dots P_h^{2^u}.$$

Thus, we have

(8) $$R_n\cong\boldsymbol{F}_2[X]/(P_1^{2^u})\oplus\cdots\oplus\boldsymbol{F}_2[X]/(P_h^{2^u}).$$

§2. Discussions in a Field

Now let P be any irreducible polynomial in $\boldsymbol{F}_2[X]$ with degree d. Let us consider the relation (2) in the field $K=\boldsymbol{F}_2[X]/(P)=GF(2^d)$, taking $x \in K$ as the image of $X \in \boldsymbol{F}_2[X]$ by the natural mapping from $\boldsymbol{F}_2[X]$ to K.

Then we can naturally define a linear map $S: K^2 \to K^2$ by:

$$S = \begin{pmatrix} 0 & 1 \\ x & x \end{pmatrix}. \tag{9}$$

That is, S is a function which maps $\begin{pmatrix} F_{i-1} \\ F_i \end{pmatrix}$ to $\begin{pmatrix} F_i \\ F_{i+1} \end{pmatrix}$. Hence,

$$S^i \begin{pmatrix} f_0 \\ f_1 \end{pmatrix} = \begin{pmatrix} F_i \\ F_{i+1} \end{pmatrix}. \tag{10}$$

Since $\det S = x \neq 0$, S is in $GL(2, K)$. So the group $G = <S> \subset GL(2, K)$ acts on K^2 from left in a natural way. For any $\boldsymbol{f} \in K^2$, we put $k_K(\boldsymbol{f}) = k(\boldsymbol{f}) = |G\boldsymbol{f}|$, namely the cardinality of the G-orbit containing $\boldsymbol{f}$. Clearly, $k(\boldsymbol{f})$ is the *period* of the sequence (2) for the initial value $\boldsymbol{f} = \begin{pmatrix} f_0 \\ f_1 \end{pmatrix}$.

As is well-known, $|G\boldsymbol{f}| = |G|/|G_{\boldsymbol{f}}|$, where $G_{\boldsymbol{f}}$ is the stabilizer of $\boldsymbol{f}$. We have therefore

$$k(\boldsymbol{f}) \mid |G| \qquad (\text{for all } \boldsymbol{f} \in K^2). \tag{11}$$

If we put $k = k(\boldsymbol{f})$, we have

$$S^k(\boldsymbol{f}) = \boldsymbol{f} \quad \text{and}$$

$$S^k(S\boldsymbol{f}) = S\boldsymbol{f}.$$

So, if $\{\boldsymbol{f}, S\boldsymbol{f}\}$ is a basis of K^2, we have $S^k = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. This, combined with (11), means $k(\boldsymbol{f}) = |G|$.

Thus, the initial value $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$ gives the maximum period, since $\begin{vmatrix} 0 & 1 \\ 1 & x \end{vmatrix} = 1 \neq 0$.

Remark. The above argument remains valid even if we take as P any non-constant polynomial in $\boldsymbol{F}_2[X]$ whose constant term is not 0, merely by replacing '$\neq 0$' by 'is invertible' in two places above.

Now, $\boldsymbol{f}$ and $S\boldsymbol{f}$ are linearly dependent iff $\boldsymbol{f}$ is an eigenvector of S. Since the eigenpolynomial of S is

$$E(t)=t^2+xt+x\,, \tag{12}$$

we have the following

Theorem 1. *If* $E(t)=0$ *has no roots in* K, *then every orbit other than* $\left\{\begin{pmatrix}0\\0\end{pmatrix}\right\}$ *has the same period* $k=|G|$.

Corollary 2. $|G|\,|\,2^{2d}-1$.

Let α, β be the roots of $E(t)=0$ in the algebraic closure $\bar{K}$ of K. Let $K'=K(\alpha, \beta)$. Since $\alpha+\beta=x\neq 0$, α and β are distinct. Since $\alpha\beta=x\neq 0$, α and β are not 0. Thus for some $U\in GL(2, K')$, we have

$$S=U\begin{pmatrix}\alpha & 0\\ 0 & \beta\end{pmatrix}U^{-1}. \tag{13}$$

If $K'\neq K$ then K' is an extension field of degree 2 over K. Hence $K'\cong GF(2^{2d})$. Since α and β are conjugate over K, we see $|\alpha|=|\beta|$, where $|\alpha|$, $|\beta|$ are the orders of α, β as elements of the multiplicative group of K'. And, since α is not in K, $|\alpha|$ can not divide $|K^*|$, where K^* is the multiplicative group of K. From (13) and the above arguments, the following theorem can be obtained.

Theorem 3. (i) *If* $E(t)=0$ *is unsolvable in* K, *then*

$$|G|=|\alpha|=|\beta|\,|\,2^{2d}-1, \quad \text{and}$$

$$|G|\nmid 2^d-1\,.$$

(ii) *If* $E(t)=0$ *is solvable in* K, *then*

$$|G|=\mathrm{LCM}(|\alpha|, |\beta|)|2^d-1, \quad \textit{and}$$

the period of $\boldsymbol{f}\neq 0$ *is*

$$k(\boldsymbol{f})=\begin{cases}|\alpha| & (\textit{if } S\boldsymbol{f}=\alpha\boldsymbol{f})\\ |\beta| & (\textit{if } S\boldsymbol{f}=\beta\boldsymbol{f})\\ |G| & (\textit{otherwise}).\end{cases}$$

Now, let us compute the general term of the sequence (F_i). As the transformation matrix U in (13), we may take

$$U=\begin{pmatrix} 1 & 1 \\ \alpha & \beta \end{pmatrix}, \tag{14}$$

$$U^{-1}=\frac{1}{\alpha+\beta}\begin{pmatrix} \beta & 1 \\ \alpha & 1 \end{pmatrix}.$$

Hence,

$$S^i=U\begin{pmatrix} \alpha^i & 0 \\ 0 & \beta^i \end{pmatrix}U^{-1} \tag{15}$$

$$=\frac{1}{\alpha+\beta}\begin{pmatrix} \alpha^i\beta+\alpha\beta^i & \alpha^i+\beta^i \\ \alpha^{i+1}\beta+\alpha\beta^{i+1} & \alpha^{i+1}+\beta^{i+1} \end{pmatrix}.$$

Hence, by (10) and (15),

$$F_i=\frac{1}{\alpha+\beta}(a\beta(\alpha^{i-1}+\beta^{i-1})f_0+(\alpha^i+\beta^i)f_1)\,. \tag{16}$$

§ 3. Proof of the Conjecture

Let us now return to the original problem and consider the case $n=s$. The relation (7) may be written as

$$R_s\cong K_1\oplus\cdots\oplus K_h\,.$$

Consider the sequence (2) in the ring R_s, and fix an initial value $\begin{pmatrix} f_0 \\ f_1 \end{pmatrix}\in R_s^2$. The above isomorphism is induced from the natural ring homomorphisms $\varphi_i\colon R_s\to K_i$. Hence the following relation clearly holds.

$$k_{R_s}\begin{pmatrix} f_0 \\ f_1 \end{pmatrix}=\mathrm{LCM}\left(k_{K_1}\begin{pmatrix} \varphi_1(f_0) \\ \varphi_1(f_1) \end{pmatrix},\dots,k_{K_h}\begin{pmatrix} \varphi_h(f_0) \\ \varphi_h(f_1) \end{pmatrix}\right). \tag{17}$$

Now, take any non-constant polynomial P in $\boldsymbol{F}_2[X]$ whose constant term is not 0, and consider the sequences (2) in two rings

$$Q_1=\boldsymbol{F}_2[X]/(P) \quad\text{and}\quad Q_2=\boldsymbol{F}_2[X]/(P^2)\,.$$

We examine the relation between the periods of two sequences in Q_1

and Q_2 for the initial values $\binom{0}{1} \in Q_1^2$ and $\binom{0}{1} \in Q_2^2$, respectively. To this end, we consider the sequence (2) in $\boldsymbol{F}_2[X]$ putting $f_0=0$ and $f_1=1$. Let $k=k_{Q_1}\binom{0}{1}$. Then for some $A_1, A_2, A_3, A_4 \in \boldsymbol{F}_2[X]$, we have

$$S^k=\begin{pmatrix} A_1P+1 & A_2P \\ A_3P & A_4P+1 \end{pmatrix}.$$

Hence,

$$S^{2k} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{P^2}. \tag{18}$$

Hence, by (11)

$$k_{Q_2}\begin{pmatrix} 0 \\ 1 \end{pmatrix} \Bigg| \, 2k.$$

On the other hand, if $l=k_{Q_2}\binom{0}{1}<k$ then, since $S^l \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{P^2}$, we have $S^l \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{P}$. This is a contradiction. Thus,

$$k_{Q_2}\begin{pmatrix} 0 \\ 1 \end{pmatrix}=k_{Q_1}\begin{pmatrix} 0 \\ 1 \end{pmatrix} \quad \text{or} \quad k_{Q_2}\begin{pmatrix} 0 \\ 1 \end{pmatrix}=2k_{Q_1}\begin{pmatrix} 0 \\ 1 \end{pmatrix}. \tag{19}$$

Now, let $k(n)$ be the maximum period of the n-bit random sequence (1). Then since the initial pattern $\binom{0}{1}$ gives the maximum period, we have

$$k(n)=k_{R_n}\begin{pmatrix} 0 \\ 1 \end{pmatrix}. \tag{20}$$

By (19), (20), and the fact that $(X^n+1)^2=X^{2n}+1$, we have

$$k(2n)=k(n) \quad \text{or} \quad k(2n)=2k(n). \tag{21}$$

We now prove that the case $k(2n)=k(n)$ never occurs.

Theorem 4. $k(2n)=2k(n)$.

Proof. If $n=s$ then by (17),

$$k(s)=\mathrm{LCM}\left(k_{K_1}\begin{pmatrix}0\\1\end{pmatrix},\dots,k_{K_h}\begin{pmatrix}0\\1\end{pmatrix}\right). \tag{22}$$

Then by Theorem 3 we see that $k_i=k_{K_i}\begin{pmatrix}0\\1\end{pmatrix}$ is odd for all $1\leqq i\leqq h$. Hence $k(s)$ is odd. If $n=2^m s$ $(m\geqq 0)$, then by (19) and (22),

$$\begin{aligned} k(n)&=\mathrm{LCM}(2^{m_1}k_1,\dots,2^{m_h}k_h) \qquad (0\leqq m_i\leqq m)\\ &=2^{\max\{m_1,\dots,m_h\}}k(s). \end{aligned} \tag{23}$$

Hence, *if* we can prove that

$$m=\max\{m_1,\dots,m_h\} \tag{24}$$

then we have

$$k(2^m s)=2^m k(s) \qquad (m\geqq 0). \tag{25}$$

This yields immediately Theorem 4.

Now, since $X+1$ is an irreducible factor of X^s+1, we may assume $K_1=\boldsymbol{F}_2[X]/(X+1)$. So, to prove (24), we have only to show that $m_1=m$. Comparing (24), with (23), we see that $m_1=m$ iff $k_{R_{2^m}}\begin{pmatrix}0\\1\end{pmatrix}=2^m k_{R_1}\begin{pmatrix}0\\1\end{pmatrix}$. Hence we have only to prove

$$\begin{aligned} k(2^m)&=2^m k(1)\\ &=2^m 3. \end{aligned} \tag{26}$$

Thus (25) is reduced to its special case (26).

Now, to show (26), let us consider the sequence (2) in the field $\overline{\boldsymbol{F}_2(X)}$, where $\overline{\boldsymbol{F}_2(X)}$ is the algebraic closure of the field $\boldsymbol{F}_2(X)$ which is the quotient field of $\boldsymbol{F}_2[X]$. If we set $f_0=0$ and $f_1=1$, then by (16),

$$F_i=(\alpha^i+\beta^i)/(\alpha+\beta), \tag{27}$$

where α and β are the two roots of $E(t)=t^2+Xt+X=0$ in $\overline{\boldsymbol{F}_2(X)}$. Since $\alpha+\beta=X$, we have

(28) $$F_{2^m}=(\alpha^{2^m}+\beta^{2^m})/(\alpha+\beta)=(\alpha+\beta)^{2^m}/(\alpha+\beta)=X^{2^m-1}.$$

Now, (26) trivially holds for $m=0$. For $m\geqq 1$, we prove $k(2^m)=2^m 3$ assuming $k(2^{m-1})=2^{m-1}3$. Let us suppose that $k(2^m)\neq 2^m 3$. Then, by (21),

$$k(2^m)=k(2^{m-1})=2^{m-1}3.$$

Hence by (28),

$$\begin{aligned} X^{2^{m+1}-1} &= F_{2^{m+1}} \\ &= F_{2^{m-1}+2^{m-1}3} \\ &\equiv F_{2^{m-1}} \qquad (\text{mod } X^{2^m}+1) \\ &\equiv X^{2^{m-1}-1} \qquad (\text{mod } X^{2^m}+1). \end{aligned}$$

On the other hand,

$$\begin{aligned} X^{2^{m+1}-1} &= X^{2^m}X^{2^m-1} \\ &\equiv X^{2^m-1} \qquad (\text{mod } X^{2^m}+1). \end{aligned}$$

This is a contradiction. Theorem 4 is now proved.

§4. Other Properties of $k(n)$

Besides that $k(2n)=2k(n)$, $k(n)$ has many properties. In this § we prove some of them. Theorem 4 established in the last § plays an important rôle. Using these properties we give an algorithm for calculating $k(n)$ which is more efficient than the straightforward algorithm.

Theorem 5. *If $m|n$ then $k(m)|k(n)$.*

Proof. First suppose m and n are both odd. Then if P is an irreducible polynomial dividing X^m+1, P divides X^n+1. Hence by (22), we see $k(m)|k(n)$. Now consider the general case. Suppose $m=2^{u_1}s_1$ and $n=2^{u_2}s_2$, where s_1, s_2 are odd. Then, $k(m)=2^{u_1}k(s_1)$ and $k(n)=2^{u_2}k(s_2)$ by Theorem 4. If $m|n$, then $u_1\leqq u_2$ and $s_1|s_2$. Hence $k(m)|$

$k(n)$, since $k(s_1)|k(s_2)$.

Corollary 6. $3|k(n)$.

Proof. $1|n$ and $k(1)=3$.

Theorem 7. $n|k(n)$.

Proof. First suppose $n=s$. Let ζ be a primitive s-th root of 1. Then $L_s=\boldsymbol{F}_2(\zeta)$ is the splitting field of $X^s+1=0$. Let $d(s)=[L_s: \boldsymbol{F}_2]$. Let $P\in\boldsymbol{F}_2[X]$ be the minimal polynomial of ζ. Then $P=(X-\zeta)(X-\zeta^2)\cdots(X-\zeta^{2^{d(s)-1}})$. Hence $d(s)$ is the least positive integer such that $s|2^{d(s)}-1$. Since $\zeta, \zeta^2,\dots, \zeta^{2^{d(s)-1}}$ are the roots of $X^s+1=0, P|X^s+1$. Thus P is an irreducible factor of X^s+1. Consider the sequence (2) in the field L_s, where we set $x=\zeta$. From (22), we have

$$k_{L_s}\begin{pmatrix}0\\1\end{pmatrix}\Big| k(s)\,. \tag{29}$$

Let $k=k_{L_s}\begin{pmatrix}0\\1\end{pmatrix}$. From (13) we see that

$$\alpha^k=\beta^k=1\,,$$

where α, β are the roots of $t^2+\zeta t+\zeta=0$. Hence $\zeta^k=(\alpha\beta)^k=1$. Hence

$$s|k\,. \tag{30}$$

By (29) and (30), we have $s|k(s)$. The case when n is even can be proved by using Theorem 4.

Theorem 8. $k(s)\,|\,2^{2d(s)}-1$

Proof. Since L_s is the splitting field of $X^s+1=0$, we may consider that each $K_i=\boldsymbol{F}_2[X]/(P_i)$ is a subfield of L_s. Hence by (11) and Theorem 3, we have $k_{K_i}\begin{pmatrix}0\\1\end{pmatrix}\Big|2^{2d(s)}-1$. Hence, by (22), we have $k(s)|2^{2d(s)}-1$.

Theorem 3 and the above proof show that if $E_i(t)=t^2+\zeta^i t+\zeta^i=0$

is solvable in L_s for all $1 \leqq i \leqq s$, then $k(s)|2^{d(s)}-1$. But the following theorem tells that this case does not occur. Before proving the theorem, we give an example.

Let $s=7$. Then $d(s)=3$. The factorization of X^7+1 is $(X+1)(X^3+X+1)(X^3+X^2+1)$. Let ζ be a root of $X^3+X^2+1=0$. Then since $(\zeta^2)^2+\zeta(\zeta^2)+\zeta=\zeta(\zeta^3+\zeta^2+1)=0$, $E_i(t)=0$ is solvable in L_s for $i=1, 2, 4$. But, for other i's, $E_i(t)=0$ is unsolvable in L_s.

Theorem 9. If $d<2d(s)$ then $k(s)\nmid 2^d-1$

Proof. Consider the sequence (2) in the field $\overline{F_2(X)}$, setting $f_0=0$, $f_1=1$. Then by (27), since $\alpha+\beta=X$,

(31) $$F_{2i}=(\alpha^{2i}+\beta^{2i})/(\alpha+\beta)=XF_i^2 .$$

Let

(32) $$G_m=F_{2^m-1} .$$

Then by (31), $F_{2^{m+1}-2}=XG_m^2$. By (28), $F_{2^{m+1}}=X^{2^{m+1}-1}$. Since $X^{2^{m+1}-1}=F_{2^{m+1}}=X(F_{2^{m+1}-1}+F_{2^{m+1}-2})=X(G_{m+1}+XG_m^2)$, we have

(33) $$G_{m+1}=X^{2^{m+1}-2}+XG_m^2 .$$

Using (33) we can prove by induction that

(34) $$G_m=\sum_{j=0}^{m-1} X^{2^m-2^j-1} .$$

If $k(s)|2^d-1$ then we have $G_d\equiv 0 \pmod{X^s+1}$. Hence, if we write G_d in the form of (34), there must be some $0<j<d$ such that

$$X^{2^d-2^j-1}\equiv X^{2^d+2^0-1} \qquad (\text{mod } X^s+1) .$$

Hence

$$2^d-2^j-1\equiv 2^d-2 \qquad (\text{mod } s) .$$

Or

$$2^j\equiv 1 \qquad (\text{mod } s) .$$

Since $d(s)$ is the least positive integer such that $s|2^{d(s)}-1$, we have $j \geqq d(s)$. Hence G_d contains the term $X^{2^d-2^{d(s)-1}-1}$. This term must be canceled by some term of the form $X^{2^d-2^j-1}$, where $d(s)-1<j<d$. Hence

$$2^d-2^{d(s)-1}-1 \equiv 2^d-2^j-1 \pmod{s}.$$

Or

$$2^{d(s)-1} \equiv 2^j \pmod{s}.$$

Or

$$1 \equiv 2^{j+1} \pmod{s}.$$

Since $j+1>d(s)$, we must have $j+1 \geqq 2d(s)$. This contradicts with the fact that $2d(s)>d>j$.

Putting Theorems 8 and 9 together, we have the following

Corollary 10. $d(k(s))=2d(s)$.

Let us now consider the sequence (2) in $\overline{F_2(X)}$, setting $f_0=0$, $f_1=1$. By (2) and (27), we have

$$\text{(35)} \qquad \begin{cases} F_{2i}=XF_i^2 \\ F_{2i+1}=F_{i+1}^2+XF_i^2. \end{cases}$$

Clearly these equations also hold in R_n (for the initial values $f_0=0$, $f_1=1$). Then, for any given m, by the iterative use of (35), we can easily calculate the value of F_m (in R_n). Now, since the candidates m for the period $k(n)$ can be confined to a reasonable number by using Theorems 5–9, we can compute $k(n)$ pretty easily. Indeed, sometimes we can determine the period without any computations:

Theorem 11. If f is a Fermat prime then $k(f-2)=(f-2)f$.

Proof. Let $f=2^e+1$. Then $d(f-2)=d(2^e-1)=e$. By Theorem 7, $f-2|k(f-2)$. By Theorem 8, $k(f-2)|(f-2)f$. By Theorem 9, $k(f-2)\nmid f-2$. Therefore, since f is a prime, $k(f-2)=(f-2)f$.

References

[1] Rader, C. M., Rabiner, L. R. and Schafer, R. W., A fast method of generating digital random numbers, *Bell System Tech. J.*, **148** (1970), 2203–2310.

[2] Moriyama, S. and Kitamura, S., On a fast method of generating random numbers (in Japanese), *Joho-shori*, **14** (1973), 15–22.