Digital Inversive Pseudorandom Numbers

JÜRGEN EICHENAUER-HERRMANN
Technische Hochschule Darmstadt
and
HARALD NIEDERREITER
Austrian Academy of Sciences

A new algorithm, the *digital inversive method*, for generating uniform pseudorandom numbers is introduced. This algorithm starts from an inversive recursion in a large finite field and derives pseudorandom numbers from it by the digital method. If the underlying finite field has q elements, then the sequences of digital inversive pseudorandom numbers with maximum possible period length q can be characterized. Sequences of multiprecision pseudorandom numbers with very large period lengths are easily obtained by this new method. Digital inversive pseudorandom numbers satisfy statistical independence properties that are close to those of truly random numbers in the sense of asymptotic discrepancy. If q is a power of 2, then the digital inversive method can be implemented in a very fast manner.

Categories and Subject Descriptors: G.3 [**Mathematics of Computing**]: Probability and Statistics—*random number generation*

General Terms: Algorithms

Additional Key Words and Phrases: Digital pseudorandom numbers, discrepancy, inversive method, statistical independence

1. INTRODUCTION

Several nonlinear methods of generating uniform pseudorandom numbers in the interval $[0, 1]$ have been proposed in the literature. Reviews of the development of this area can be found in Eichenauer-Herrmann [1992; 1995] and Niederreiter [1992a; 1992b]. A particularly attractive nonlinear method is the (recursive) inversive congruential method with prime modulus. In this article a digital version of this inversive method, which offers several advantages over the former approach, is introduced and analyzed. First, a detailed description of this new method is given.

Let p be a prime, and put $q = p^k$ for some integer $k \geq 1$. Denote by F_q the finite field with q elements and by $F_q^* = F_q \setminus \{0\}$ the multiplicative group of nonzero elements of F_q. Identify the set $\mathbf{Z}_p = \{0, 1, \ldots, p-1\}$ of integers with

Authors' addresses: J. Eichenauer-Herrmann, Fachbereich Mathematik, Technische Hachschule, Schlossgartenstrasse 7, D-64289 Darmstadt, Germany; H. Niederreiter, Institute for Information Processing, Austrian Academy of Sciences, Sonnenfelsgasse 19, A-1010 Vienna, Austria; email:nied@qiinfo.oeaw.ac.at.

the finite field $F_p = \mathbf{Z}/p\mathbf{Z}$ with p elements. For $\gamma \in F_q^*$ let $\bar{\gamma} = \gamma^{-1} \in F_q^*$ be the multiplicative inverse of γ in F_q and define $\bar{0} = 0$. For an initial value $\gamma_0 \in F_q$ and *parameters* $\alpha \in F_q^*$ and $\beta \in F_q$ an *inversive sequence* $(\gamma_n)_{n \geq 0}$ of elements of F_q is defined by the recursion

$$\gamma_{n+1} = \alpha\bar{\gamma}_n + \beta, \quad n \geq 0. \tag{1}$$

Obviously, an inversive sequence $(\gamma_n)_{n \geq 0}$ is always purely periodic with period length less than or equal to q.

Let $\sigma, \tau \in F_{q^2}$ be the nonzero roots of the polynomial $x^2 - \beta x - \alpha \in F_q[x]$ associated with the inversive sequence $(\gamma_n)_{n \geq 0}$. Then Theorem 1 in Niederreiter [1994] implies that $(\gamma_n)_{n \geq 0}$ has the maximum possible period length $q = p^k$ if and only if the order of the quotient $\sigma\tau^{-1}$ in the multiplicative group $F_{q^2}^*$ is equal to $q + 1$. In this case the polynomial $x^2 - \beta x - \alpha \in F_q[x]$ is called an *inversive maximal period (IMP) polynomial* over F_q. It should be observed that any primitive quadratic polynomial over F_q is an IMP polynomial. A detailed study of IMP polynomials was carried out by Chou [1995]. As explained by Chou [1995] and Niederreiter [1994], the polynomial $x^2 - \beta x - \alpha \in F_q[x]$ is an IMP polynomial over F_q if and only if the roots of $x^2 + (\zeta^{-1} + 2)x + 1$ have order $q + 1$ in $F_{q^2}^*$, where $\alpha = \zeta\beta^2$.

In the following, the finite field F_q is viewed as a k-dimensional vector space over $\mathbf{Z}_p$. Then for $n \geq 0$ let

$$\mathbf{c}_n = (c_n^{(1)}, \ldots, c_n^{(k)}) \in \mathbf{Z}_p^k$$

be the coordinate vector of $\gamma_n \in F_q$ relative to a given ordered basis of F_q over $\mathbf{Z}_p$. Now a sequence $(x_n)_{n \geq 0}$ of *digital inversive pseudorandom numbers* in the interval $[0, 1)$ is defined by

$$x_n = \sum_{j=1}^{k} c_n^{(j)} p^{-j}, \quad n \geq 0. \tag{2}$$

Obviously, the sequences $(x_n)_{n \geq 0}, (\mathbf{c}_n)_{n \geq 0}$, and $(\gamma_n)_{n \geq 0}$ have the same periodicity properties; in particular, the sequence $(x_n)_{n \geq 0}$ of digital inversive pseudorandom numbers is always purely periodic, and it has the maximum possible period length $q = p^k$ if and only if the polynomial $x^2 - \beta x - \alpha \in F_q[x]$ is an IMP polynomial over F_q.

A very important property that should be asked of pseudorandom numbers for stochastic simulations is the statistical independence of successive terms of the generated sequence. A reliable theoretical approach for assessing statistical independence properties is based on the notion of discrepancy of s-tuples of successive pseudorandom numbers. For N arbitrary points $\mathbf{t}_0, \mathbf{t}_1, \ldots, \mathbf{t}_{N-1} \in [0, 1)^s$ the *star discrepancy* is defined by

$$D_N^*(\mathbf{t}_0, \mathbf{t}_1, \ldots, \mathbf{t}_{N-1}) = \sup_J |E_N(J) - V(J)|,$$

where the supremum is extended over all subintervals J of $[0, 1)^s$ containing the origin; $E_N(J)$ is N^{-1} times the number of points among $\mathbf{t}_0, \mathbf{t}_1, \ldots, \mathbf{t}_{N-1}$ falling into J; and $V(J)$ denotes the s-dimensional volume of J.

In the following, for a sequence $(x_n)_{n \geq 0}$ of digital inversive pseudorandom numbers with period length $q = p^k$ the abbreviations

$$\mathbf{x}_n = (x_n, x_{n+1}, \ldots, x_{n+s-1}) \in [0,1)^s, \quad n \geq 0, \tag{3}$$

and

$$D_q^{*(s)} = D_q^*(\mathbf{x}_0, \mathbf{x}_1, \ldots, \mathbf{x}_{q-1})$$

are used. In Section 3 we establish upper and lower bounds for the star discrepancy $D_q^{*(s)}$. Their proofs are based on several auxiliary results that are collected in the second section. Section 4 contains a detailed discussion of computational aspects of the practical implementation of the digital inversive method. In the last section the features of the digital inversive method are summarized and discussed.

2. AUXILIARY RESULTS

Let $s \geq 2$, and denote by $C_{s \times k}(p)$ the set of all nonzero $s \times k$ matrices $H = (h_{ij})$ with integer entries h_{ij} satisfying $-p/2 < h_{ij} \leq p/2$ for $1 \leq i \leq s$ and $1 \leq j \leq k$. For $H \in C_{s \times k}(p)$ an *exponential sum* is defined by

$$S(H) = \sum_{n=0}^{q-1} e\left(\frac{1}{p} \sum_{i=1}^{s} \sum_{j=1}^{k} h_{ij} c_{n+i-1}^{(j)}\right),$$

where $e(u) = e^{2\pi\sqrt{-1}u}$ for real u. We collect some auxiliary results on these exponential sums. Lemma 2.1 was shown in the proof of Niederreiter [1994, Theorem 2], and Lemma 2.2 follows from the proof of Niederreiter [1994, Theorem 3]. As in Section 1 we put $q = p^k$.

LEMMA 2.1. *For all $H \in C_{s \times k}(p)$ we have*

$$|S(H)| \leq (s-1)(2q^{1/2} + 1).$$

LEMMA 2.2. *Let $H = (h_{ij}) \in C_{s \times k}(p)$ with $h_{11} = h_{21} = 1$ and all other entries equal to zero. Let $\zeta \in F_q^*$ be such that the roots of the polynomial $x^2 + (\zeta^{-1} + 2)x + 1 \in F_q[x]$ have order $q+1$ in $F_{q^2}^*$. Let $0 < t < 1$ and*

$$A_q(t) = \frac{1 - t^2 - 2(q-1)^{-1}}{4 - t^2 + 4q^{-1/2} + q^{-1}}.$$

Then there exist more than $A_q(t)(q-1)$ values of $\beta \in F_q^*$ such that with $\alpha = \zeta\beta^2$ in the underlying inversive sequence we have

$$|S(H)| \geq tq^{1/2}.$$

We remark that if α, β, and ζ are as in Lemma 2.2, then according to a characterization of IMP polynomials in Section 1 the inversive sequence (1) has the maximum possible period length q.

LEMMA 2.3. *Let* $H = (h_{ij}) \in C_{s\times k}(p)$ *with* $h_{11} = h_{21} = 1$ *and all other entries equal to zero. Then*

$$|S(H)| = \left| \sum_{n=0}^{q-1} e\left(\frac{1}{p}(c_n^{(1)} + c_{n+1}^{(1)})\right)\right| \le 8(\pi + 1)qD_q^{*(s)}.$$

PROOF. We apply Niederreiter [1994, Lemma 3] with $M = p$, $N = q$, $d = s$, $\mathbf{y}_n = (c_n^{(1)}, c_{n+1}^{(1)}, \ldots, c_{n+s-1}^{(1)})$ – for $0 \le n \le q - 1$, and $\mathbf{h} = (1, 1, 0, \ldots, 0) \in \mathbf{Z}^s$. This yields

$$|S(H)| \le 8(\pi + 1)q \max_J |E_q(J) - V(J)|,$$

where the maximum is extended over all subintervals J of $[0, 1)^s$ of the form $J = \prod_{i=1}^s [0, b_i/p)$ with integers $0 < b_i \le p$ for $1 \le i \le s$, and where $E_q(J)$ is q^{-1} times the number of points among $\mathbf{t}_n = p^{-1}\mathbf{y}_n$, $0 \le n \le q - 1$, falling into J. In view of the definition of the pseudorandom numbers x_n in (2), it is clear that $\mathbf{t}_n \in J$ if and only if the point $\mathbf{x}_n$ in (3) satisfies $\mathbf{x}_n \in J$. Therefore

$$\max_J |E_q(J) - V(J)| \le D_q^{*(s)},$$

and the result of the lemma follows. □

3. DISCREPANCY BOUNDS

If the inversive sequence $(\gamma_n)_{n\ge 0}$ of elements of F_q has the maximum possible period length $q = q^k$, then $\gamma_0, \gamma_1, \ldots, \gamma_{q-1}$ run exactly through all elements of F_q. Consequently, the corresponding coordinate vectors $\mathbf{c}_0, \mathbf{c}_1, \ldots, \mathbf{c}_{q-1}$ run exactly through all elements of $\mathbf{Z}_p^k$. On account of (2), this implies that each rational number in $[0, 1)$ with fixed denominator p^k appears exactly once among the pseudorandom numbers $x_0, x_1, \ldots, x_{q-1}$. Therefore, the full period of the sequence $(x_n)_{n\ge 0}$ shows a perfect equidistribution in the interval $[0, 1)$.

In the following, we establish upper and lower discrepancy bounds for dimensions $s \ge 2$ in the case of the maximum possible period length q.

THEOREM 3.1. *Let* $(x_n)_{n\ge 0}$ *be a sequence of digital inversive pseudorandom numbers with period length* $q = p^k$. *Then for any* $s \ge 2$ *the star discrepancy* $D_q^{*(s)}$ *satisfies*

$$D_q^{*(s)} < (s - 1)(2q^{-1/2} + q^{-1})\left(\frac{2}{\pi}\log q + \frac{7}{5}k - \frac{k-1}{p}\right)^s \quad \text{for } p \ge 3$$

and

$$D_q^{*(s)} < (s - 1)(2q^{-1/2} + q^{-1})\left(\frac{k}{2} + 1\right)^s \quad \text{for } p = 2.$$

PROOF. By Niederreiter [1992b, Theorem 3.12] we obtain

$$D_q^{*(s)} \le 1 - (1 - q^{-1})^s + \frac{1}{q} \sum_{H \in C_{s\times k}(p)} W_p(H)|S(H)|,$$

where the weights $W_p(H)$ are as in the quoted theorem. Then an application of Lemma 2.1 yields

$$D_q^{*(s)} \le 1 - (1 - q^{-1})^s + (s - 1)(2q^{-1/2} + q^{-1}) \sum_{H \in C_{s\times k}(p)} W_p(H).$$

For $p \ge 3$ the last sum can be bounded by the first part of Niederreiter [1992b, Lemma 3.13], and if we also observe that the weight of the zero matrix is equal to 1, then we get

$$\begin{aligned} D_q^{*(s)} &< \frac{s}{q} + (s - 1)(2q^{-1/2} + q^{-1})\left(\left(\frac{2}{\pi}\log q + \frac{7}{5}k - \frac{k-1}{p}\right)^s - 1\right) \\ &< (s - 1)(2q^{-1/2} + q^{-1})\left(\frac{2}{\pi}\log q + \frac{7}{5}k - \frac{k-1}{p}\right)^s. \end{aligned}$$

For $p = 2$ we obtain the desired bound for $D_q^{*(s)}$ by applying the second part of Niederreiter [1992b, Lemma 3.13]. □

THEOREM 3.2. *Let $\zeta \in F_q^*$ be such that the roots of the polynomial $x^2 + (\zeta^{-1} + 2)x + 1 \in F_q[x]$ have order $q + 1$ in $F_{q^2}^*$. Let $0 < t < 1$ and*

$$A_q(t) = \frac{1 - t^2 - 2(q - 1)^{-1}}{4 - t^2 + 4q^{-1/2} + q^{-1}}.$$

Then for any fixed ordered basis of F_q over $\mathbf{Z}_p$ there exist more than $A_q(t)(q - 1)$ values of $\beta \in F_q^*$ such that with $\alpha = \zeta\beta^2$ in the inversive sequence and all dimensions $s \ge 2$ the star discrepancy $D_q^{*(s)}$ for any corresponding sequence of digital inversive pseudorandom numbers with period length $q = p^k$ satisfies

$$D_q^{*(s)} \ge \frac{t}{8(\pi + 1)} q^{-1/2} \quad \text{for } p \ge 3$$

and

$$D_q^{*(s)} \ge \frac{t}{4} q^{-1/2} \quad \text{for } p = 2.$$

PROOF. If α, β, and ζ are as in the theorem, then any corresponding sequence of digital inversive pseudorandom numbers has periodlength q, by a characterization of IMP polynomials in Section 1. For $p \ge 3$ the desired result on $D_q^{*(s)}$ follows at once from Lemmas 2.2 and 2.3. Now let $p = 2$, and observe that for $a \in \{0, 1\}$ we have

$$\#\{0 \le n \le q - 1 : c_n^{(1)} = a\} = \frac{q}{2}.$$

Hence, there exists an integer d with

$$\#\{0 \le n \le q-1 : (c_n^{(1)}, c_{n+1}^{(1)}) = (a,b)\} = \begin{cases} \frac{q}{4} + d & \text{for} \quad (a,b) \in \{(0,0),(1,1)\}, \\ \frac{q}{4} - d & \text{for} \quad (a,b) \in \{(0,1),(1,0)\}, \end{cases}$$

which implies that

$$\left| \sum_{n=0}^{q-1} e\left((c_n^{(1)} + c_{n+1}^{(1)})/2\right) \right| = \left| 2\left(\frac{q}{4} + d\right) - 2\left(\frac{q}{4} - d\right) \right| = 4|d|.$$

Therefore

$$\begin{aligned} D_q^{*(s)} &\ge \left| E_q\left([0,1/2)^2 \times [0,1)^{s-2}\right) - \frac{1}{4} \right| \\ &= \left| \frac{1}{q} \#\{0 \le n \le q-1 : (c_n^{(1)}, c_{n+1}^{(1)}) = (0,0)\} - \frac{1}{4} \right| \\ &= \frac{1}{q}|d| = \frac{1}{4q} \left| \sum_{n=0}^{q-1} e\left((c_n^{(1)} + c_{n+1}^{(1)})/2\right) \right| \\ &= \frac{1}{4q}|S(H)|, \end{aligned}$$

where $H = (h_{ij}) \in C_{s \times k}(p)$ with $h_{11} = h_{21} = 1$ and all other entries equal to zero. Hence, the desired result follows from Lemma 2.2. □

We remark that since

$$\lim_{q \to \infty} A_q(t) = \frac{1 - t^2}{4 - t^2} > 0 \quad \text{for each } 0 < t < 1,$$

the lower bound for $D_q^{*(s)}$ in Theorem 3.2 holds for a positive asymptotic proportion of all elements $\beta \in F_q^*$.

4. FAST IMPLEMENTATION OF THE DIGITAL INVERSIVE METHOD

The description of the digital inversive method in Section 1 shows that for the practical implementation of this method we need a convenient representation of the finite field F_q with $q = p^k$ elements and a good choice of an ordered basis of F_q over $\mathbf{Z}_p$ to facilitate the arithmetic in F_q. The coordinate vectors $\mathbf{c}_n$ in Section 1 will then be taken relative to this chosen ordered basis. The step from the $\mathbf{c}_n$ to the pseudorandom numbers x_n is accomplished in a straightforward manner according to (2).

Since all we are interested in are the coordinate vectors $\mathbf{c}_n$, it is advisable to represent the elements of F_q right away by their coordinate vectors relative to a fixed ordered basis of F_q over $\mathbf{Z}_p$. Thus, the problem of the representation of F_q is then reduced to that of the convenient choice of an ordered basis of F_q over $\mathbf{Z}_p$. Addition of field elements is the same as addition

of coordinate vectors, and field elements given in terms of coordinate vectors are multiplied with the help of a precomputed multiplication table for the basis elements (compare also with a discussion later in this section).

It will turn out in the following that it is advantageous to work with a special type of basis, namely, a *normal basis* of F_q over $\mathbf{Z}_p$, i.e., an ordered basis of F_q over $\mathbf{Z}_p$ of the form $\{\lambda, \lambda^p, \lambda^{p^2}, \ldots, \lambda^{p^{k-1}}\}$ with some $\lambda \in F_q$. By a fundamental result in the theory of finite fields, a normal basis of F_q over $\mathbf{Z}_p$ always exists (see Lidl and Niederreiter [1986, Theorem 2.35]).

The most expensive operation in the recursion (1) is the calculation of the multiplicative inverse $\bar{\gamma} = \gamma^{-1}$ of an element $\gamma \in F_q^*$. The conventional, but not necessarily most efficient, approach is to use the identity $\gamma^{-1} = \gamma^{q-2}$ for $\gamma \in F_q^*$ and then calculate γ^{q-2} by the standard square-and-multiply technique (e.g., see Lidl and Niederreiter [1986, p. 347]), which requires $O(\log q)$ multiplications in F_q.

A much faster algorithm for the calculation of γ^{-1} is available in the case where q is a power of 2, i.e., where $p = 2$, which also happens to be the case of greatest practical interest for the implementation of digital inversive pseudorandom numbers. This fast algorithm is due to Itoh and Tsujii [1988] and uses a normal basis $B = \{\lambda, \lambda^2, \lambda^4, \ldots, \lambda^{2^{k-1}}\}$ of F_q (with $q = 2^k$) over $\mathbf{Z}_2$. It is a crucial advantage of a normal basis that squaring elements of F_q is a cheap operation in such a basis: for any $\gamma \in F_q$, the coordinate vector of γ^2 relative to B is obtained by cyclically shifting the coordinate vector of γ relative to B by one position to the right. More generally, the coordinate vector of γ^{2^d}, $d \geq 1$, relative to B is obtained by cyclically shifting the coordinate vector of γ relative to B by d positions to the right. The calculation of $\gamma^{-1} = \gamma^{q-2}$ for $\gamma \in F_q^*$ proceeds now as follows. In view of the identity

$$\gamma^{q-2} = \left(\gamma^{2^{k-1}-1}\right)^2,$$

it suffices to describe how to compute powers of the form γ^{2^m-1}. the idea is to reduce the calculation of γ^{2^m-1} to that of $\gamma^{2^{\lfloor m/2 \rfloor}-1}$, where $\lfloor u \rfloor$ denotes as usual the greatest integer $\leq u$. This is achieved by the identities

$$\gamma^{2^m-1} = \left(\gamma^{2^{m/2}-1}\right)^{2^{m/2}} \gamma^{2^{m/2}-1} \qquad \text{for even } m,$$

$$\gamma^{2^m-1} = (\gamma 2^{(m-1)/2-1}) 2^{(m+1)/2} (\gamma 2^{(m-1)/2-1})^2 \gamma \qquad \text{for odd } m.$$

To compute γ^{2^m-1}, these identities are applied repeatedly. According to Itoh and Tsujii [1988], the resulting algorithm for calculating γ^{-1} for $\gamma \in F_q^*$ (with $q = 2^k$, $k \geq 2$) requires cyclic shifts by altogether $k - 1$ positions and $\lfloor \log_2(k-1) \rfloor + w(k-1) - 1$ multiplications in F_q, where $\log_2$ denotes the logarithm to the base 2, and $w(k-1)$ is the Hamming weight of $k - 1$, i.e., the number of 1's in the binary representation of $k - 1$. By using a trivial upper bound for $w(k-1)$, it is seen that at most $2\lfloor \log_2(k-1) \rfloor$ multiplications in F_q are needed. In terms of q this means that only $O(\log \log q)$ multiplications in F_q are required, as opposed to $O(\log q)$ multiplications in F_q by the square-and-multiply technique.

It remains to discuss the efficient implementation of multiplications in F_q, where we now return to the general case $q = p^k$ with an arbitrary prime p. We choose again a normal basis $B = \{\lambda, \lambda^p, \lambda^{p^2}, \ldots, \lambda^{p^{k-1}}\}$ of F_q over $\mathbf{Z}_p$, and the elements of F_q are represented by their coordinate vectors relative to B. If $\gamma, \delta \in F_q$ have the coordinate vectors $(c^{(1)}, \ldots, c^{(k)}) \in \mathbf{Z}_p^k$ and $(d^{(1)}, \ldots, d^{(k)}) \in \mathbf{Z}_p^k$, respectively, so that

$$\gamma = \sum_{j=1}^{k} c^{(j)} \lambda^{p^{j-1}}, \quad \delta = \sum_{j=1}^{k} d^{(j)} \lambda^{p^{j-1}},$$

then

$$\gamma\delta = \sum_{i,j=1}^{k} c^{(i)} d^{(j)} \lambda^{p^{i-1}} \lambda^{p^{j-1}}.$$

Thus, to obtain the coordinate vector of $\gamma\delta$ relative to B, it suffices to know the coordinate vectors of $\lambda^{p^{i-1}} \lambda^{p^{j-1}}$, $1 \le i, j \le k$, relative to B. These are given by the multiplication table

$$\lambda^{p^{i-1}} \lambda^{p^{j-1}} = \sum_{h=1}^{k} a(h,i,j) \lambda^{p^{h-1}} \quad \text{for } 1 \le i, j \le k,$$

where all $a(h,i,j) \in \mathbf{Z}_p$. The multiplicative arithmetic in F_q is thus completely described by the coefficients $a(h,i,j)$. It is clear that multiplication in F_q by this procedure becomes faster if many of the coefficients $a(h,i,j)$ are zero. A relevant concept here is that of the *complexity* $C(B)$ of the normal basis B, which is defined as the number of ordered pairs (h,j) with $1 \le h, j \le k$ for which $a(h,1,j) \ne 0$. We always have $2k - 1 \le C(B) \le k^2$, where the lower bound is shown in Menezes et al. [1993, Theorem 5.1], and the upper bound is trivial. The number of ordered triples (h,i,j) with $1 \le h, i, j \le k$ for which $a(h,i,j) \ne 0$ is equal to $C(B)k$ (compare with Menezes et al. [1993, pp. 94–95]).

Multiplication in F_q by the procedure above becomes particularly efficient if we choose an *optimal normal basis* B of F_q (with $q = p^k$) over $\mathbf{Z}_p$, i.e., a normal basis B of F_q over $\mathbf{Z}_p$ with complexity $C(B) = 2k - 1$. Optimal normal bases do not exist for all values of p and k, but a complete classification of all optimal normal bases is known (see Menezes et al. [1993, Chapter 5]). For $p = 2$, a table of all values of $k \le 2000$ for which there exists an optimal normal basis of F_{2^k} over $\mathbf{Z}_2$ is available in Menezes et al. [1993, Table 5.1, p. 100]. For pseudorandom number generation, the following values of k extracted from this table may be of interest (these values of k are reasonably close to powers of 2):

$$k = 30, 33, 35, 36, 58, 60, 65, 66, 119, 130, 131, 251, 254, 508, 509.$$

Example 4.1. Choose $p = 2$ and $k = 3$, so that $q = 2^{33}$. According to Menezes et al. [1993, Theorem 5.3] and the fact that 2 is a primitive element of $\mathbf{Z}_{67}$, an optimal normal basis B of F_q over $\mathbf{Z}_2$ is generated by $\lambda = \eta + \eta^{-1}$, where η is a primitive 67th root of unity over $\mathbf{Z}_2$. Relative to this normal

basis B, the algorithm of Itoh and Tsujii for computing γ^{-1} for $\gamma \in F_q^*$ requires $\lfloor \log_2(k-1) \rfloor + w(k-1) - 1 = 5$ multiplications in F_q and cyclic shifts by altogether 32 positions. To calculate the multiplication table for B, it is convenient to rearrange the elements of B in the form

$$B = \{\psi^j + \eta^{-j} : j = 1, 2, \ldots, 33\}.$$

Then

$$(\eta^i + \eta^{-i})(\eta^j + \eta^{-j}) = (\eta^{i+j} + \eta^{-(i+j)}) + (\eta^{i-j} + \eta^{-(i-j)}) \quad \text{for } 1 \le i, j \le 33,$$

which is thus equal to an element of B if $i = j$ and equal to a sum of two distinct elements of B if $i \neq j$.

Example 4.2. Choose $p = 2$ and $k = 66$, so that $q = 2^{66}$. According to Menezes et al. [1993, Theorem 5.2] and the fact that 2 is a primitive element of $\mathbf{Z}_{67}$, an optimal normal basis B of F_q over $\mathbf{Z}_2$ is generated by a primitive 67th root of unity η over $\mathbf{Z}_2$. Relative to this normal basis B, the algorithm of Itoh and Tsujii for computing γ^{-1} for $\gamma \in F_q^*$ requires $\lfloor \log_2(k-1) \rfloor + w(k-1) - 1 = 7$ multiplications in F_q and cyclic shifts by altogether 65 positions. To calculate the multiplication table for B, it is convenient to rearrange the elements of B in the form

$$B = \{\eta^j : j = 1, 2, \ldots, 66\}.$$

Then $\eta^i \eta^j = \eta^{i+j}$ for $1 \le i, j \le 66$, which is equal to an element of B if $i + j \not\equiv 0 \bmod 67$, whereas

$$\eta^i \eta^j = 1 = \sum_{h=1}^{66} \eta^h \quad \text{if } i + j \equiv 0 \bmod 67.$$

For values of p and k for which an optimal normal basis of F_q (with $q = p^k$) over $\mathbf{Z}_p$ does not exist, it may still be possible to find a normal basis B of F_q over $\mathbf{Z}_p$ with a relatively low complexity $C(B)$. We refer to Jungnickel [1993, Section 3.3] and Menezes et al. [1993, Section 5.2] for various constructions of low-complexity normal bases.

Another computational issue that arises in the practical implementation of the digital inversive method is the calculation of IMP polynomials. As we have seen in Section 1, an IMP polynomial $x^2 - \beta x - \alpha$ over F_q (with $q = p^k$) is needed to obtain parameters $\alpha, \beta \in F_q$ in the recursion (1) that yield the maximum possible period length q. We have also noted in Section 1 that any primitive quadratic polynomial over F_q is an IMP polynomial. Primitive quadratic polynomials over large finite fields F_q are not available in standard tables,but there are far-reaching tables of primitive polynomials of large degrees over the finite prime fields $\mathbf{Z}_p$; see Hansen and Mullen [1992] for $p \le 97$ and the more extensive table of Živković [1994] for the important special case $p = 2$. We can therefore proceed as follows to get a primitive quadratic polynomial over F_q. Choose a primitive polynomial over $\mathbf{Z}_p$ of degree $2k$; this polynomial defines the extension field F_{q^2} of $\mathbf{Z}_p$ and has a

primitive element σ of F_{q^2} as a root. Then the minimal polynomial of σ over F_q, which is given by

$$(x - \sigma)(x - \sigma^q) = x^2 - (\sigma + \sigma^q)x + \sigma^{q+1},$$

is a primitive quadratic polynomial over F_q. Thus we can take $\alpha = -\sigma^{q+1}$ and $\beta = \sigma + \sigma^q$ in (1). Note that even for very large q the element σ^q can be calculated easily by repeatedly computing pth powers, which is very simple in characteristic p.

Example 4.3. For the situation in Example 4.1, namely, $p = 2$ and $k = 33$, a primitive polynomial over $\mathbf{Z}_p$ of degree $2k$ is given by $x^{66} + x^9 + x^8 + x^6 + 1$, and for the situation in Example 4.2, namely, $p = 2$ and $k = 66$, it is given by $x^{132} + x^{29} + 1$, in both cases according to the table in Hansen and Mullen [1992].

5. DISCUSSION AND CONCLUSIONS

The digital inversive method for pseudorandom number generation has several attractive properties. First of all, there exists a handy criterion for the maximum possible period length $q = p^k$, namely, that $x^2 - \beta x - \alpha$ is an IMP polynomial over F_q. The property that $x^2 - \beta x - \alpha$ is a primitive polynomial over F_q provides a sufficient condition for the maximum period length q.

Any digital inversive sequence with maximum period length shows nice statistical independence properties in the sense of asymptotic discrepancy. Theorem 3.1 implies that $D_q^{*(s)} = O(q^{-1/2}(\log q)^s)$, where the implied constant is absolute. Theorem 3.2 shows that this upper bound is in general best possible up to the logarithmic factor, since there exist digital inversive sequences with a star discrepancy $D_q^{*(s)}$ of an order of magnitude at least $q^{-1/2}$. It is in this range of magnitudes where one also finds the discrepancy of q independent and uniformly distributed random points from $[0, 1)^s$, which is almost always of an order of magnitude $q^{-1/2}(\log \log q)^{1/2}$ according to the law of the iterated logarithm for discrepancies (see Kiefer [1961]). Digital inversive pseudorandom numbers have the usual merit of inversive pseudorandom numbers, namely, that once the maximum possible period length is achieved, then they satisfy the upper discrepancy bounds irrespective of the specific choice of the parameters α and β in the recursion (1).

The most convenient practical implementation of the digital inversive method arises if we choose $p = 2$ and a sufficiently large integer k such that an acceptable maximum period length $q = 2^k$ is attained. This choice has the additional advantage that it allows a fast implementation of the necessary arithmetic. As we have shown in Section 4, one step of the recursion (1) requires then only $O(\log \log q)$ multiplications in F_q, one addition in F_q, and some cyclic shifts of coordinate vectors. This should be contrasted with the cost of one step in the (recursive) inversive congruential method with prime modulus, which in the present setup corresponds to the choice where p is a large prime and $k = 1$. In the latter method, the number of required multiplications in F_p in one step of the recursion is $O(\log p)$. Consequently, for

comparable maximum period lengths the digital inversive method with $p = 2$ allows a significantly faster generation of the pseudorandom numbers than the inversive congruential method with prime modulus. On the other hand, the theoretical results on the statistical independence properties for these two types of generators are quite similar (compare with Niederreiter [1992b, Chapter 8] for the properties of inversive congruential pseudorandom numbers with prime modulus).

ACKNOWLEDGMENT

The authors gratefully acknowledge the insightful and constructive comments of the referees and of the associate editor.

REFERENCES

CHOU, W.-S. 1995. On inversive maximal period polynomials over finite fields. *Appl. Algebra Eng. Commun. Comput.* Forthcoming.

EICHENAUER-HERRMANN, J. 1995. Pseudorandom number generation by nonlinear methods. *Int. Stat. Rev.* Forthcoming.

EICHENAUER-HERRMANN, J. 1992. Inversive congruential pseudorandom numbers: A tutorial. *Int. Stat. Rev. 60*, 167–176.

HANSEN, T. AND MULLEN, G.L. 1992. Primitive polynomials over finite fields. *Math. Comput. 59*, 639–643, S47–S50.

ITOH, T. AND TSUJII, S. 1988. A fast algorithm for computing multiplicative inverses in $GF(2^m)$ using normal bases. *Inf. Comput. 78*, 171–177.

JUNGNICKEL, D. 1993. *Finite Fields: Structure and Arithmetics*. Bibliographisches Institut, Mannheim, Germany.

KIEFER, J. 1961. On large deviations of the empiric d.f. of vector chance variables and a law of the iterated logarithm. *Pac. J. Math. 11*, 649–660.

LIDL, R. AND NIEDERREITER, H. 1986. *Introduction to Finite Fields and Their Applications*. Cambridge University Press, Cambridge, U.K..

MENEZES, A.J., BLAKE, I.F., GAO, X.H., MULLIN, R.C., VANSTONE, S.A., AND YAGHOOBIAN, T. 1993. *Applications of Finite Fields*. Kluwer, Boston, Mass.

NIEDERREITER, H. 1994. Pseudorandom vector generation by the inversive method. *ACM Trans. Modeling Comput. Simul. 4*, 2 (Apr.), 191–212.

NIEDERREITER, H. 1992a. Nonlinear methods for pseudorandom number and vector generation. In *Simulation and Optimization*, G. Pflug and U. Dieter, Eds. Lecture Notes in Economics and Mathematical Systems, vol. 374. Springer, Berlin, 145–153.

NIEDERREITER, H. 1992b. *Random Number Generation and Quasi-Monte Carlo Methods*. SIAM, Philadelphia, Pa.

ŽIVKOVIĆ, M. 1994. A table of primitive binary polynomials. *Math. Comput. 62*, 385–386 (with microfiche supplement).

Received January; accepted June 1994