FIBONACCI NUMBERS AND DECIMATION OF BINARY SEQUENCES

Jovan Dj. Golić
Security Innovation, Telecom Italia
Via Reiss Romoli 274, 10148 Turin, Italy
(Submitted August 2004-Final Revision April 2005)

ABSTRACT

The problem of computing the number of sequences of various lengths that can be obtained by decimating a given binary sequence X^n of length n is considered. It is proven that this number is maximized iff X^n is an alternating sequence and that the maximum can be expressed in terms of the Fibonacci numbers. Some other upper bounds on this number are also determined, including another bound in terms of the Fibonacci numbers, depending on the run lengths in X^n.

1. INTRODUCTION

Irregular decimation of binary sequences is a well-known mathematical operation emerging in the analysis of codes for correcting synchronization errors, used in telecommunications, and stream ciphers based on clock-controlled shift registers, used in cryptography. For example, see [2] and [1], respectively.

Given a binary sequence $X = x_1, x_2, \ldots$, let $X_k^n = x_k, x_{k+1}, \ldots, x_n$ and $X^n = X_1^n$, and let X^0 be an empty set ϕ. A binary sequence of variable length is also denoted by X. The complement of X is denoted by $\overline{X} = \overline{x}_0, \overline{x}_1, \ldots$, where $\overline{x}_i = x_i \oplus 1$ and $\oplus$ stands for the modulo 2 addition. As usual, $X^m Y^n$ denotes the concatenation of X^m and Y^n, and c^n thus denotes a constant sequence $c, c, \ldots, c$.

Definition 1: Given an input binary sequence X^n and a decimation binary sequence C^n of the Hamming weight $w_H(C^n) = k$ (defined as the number of 1's in C^n), $0 \le k \le n$, the decimation of X^n according to C^n, denoted as $Z^k = DEC(X^n, C^n)$, is defined as the sequence of all the bits x_i, $1 \le i \le n$, such that $c_i = 1$, where the bits are taken in the same order as in X^n. The bits x_i such that $c_i = 0$ are thus discarded, and if $k = 0$, then $Z^0 = \phi$.

Let

$$D(X^n) = \{Z : (\exists C^n) DEC(X^n, C^n) = Z\} \tag{1}$$

and let $d_n(X^n) = |D(X^n)|$ denote the number of sequences of various lengths that can be obtained by decimating X^n. Let $\overline{d}_n$ be the maximum of $d_n(X^n)$ over all X^n. Clearly, $n+1 \le d_n(X^n) \le 2^n$ and $d_n(X^n) = d_n(\overline{X}^n)$.

Example 1: Given a sequence $X^4 = 0101$, we have $D(X^4) = \{\phi, 0, 1, 00, 01, 10, 11, 010, 011, 001, 101, 0101\}$ and hence $d_4(X^4) = 12$.

The problems dealt with in this paper are to find an algorithm for an efficient computation of $d_n(X^n)$ and to determine tight upper bounds on $d_n(X^n)$, for an arbitrary X^n. Interestingly, it turns out that the solutions are closely related to the Fibonacci numbers.

2. CONCATENATION UPPER BOUNDS

It is interesting that direct counting by computer simulations can be used to obtain upper bounds on $\overline{d}_n$, exponential in n, by using the following concatenation lemma for $d_n(X^n)$.

Lemma 1: For any $m, n \geq 1$,

$$d_{m+n}(X^m Y^n) \leq d_m(X^m) d_n(Y^n). \tag{2}$$

Proof: From the definition of the decimation operation, it follows that $Z \in D(X^m Y^n)$ iff there exist $Z_1 \in D(X^m)$ and $Z_2 \in D(Y^n)$ such that $Z = Z_1 Z_2$. Therefore, we have

$$|D(X^m Y^n)| \leq |D(X^m)| \cdot |D(Y^n)|. \quad \square \tag{3}$$

Theorem 1: For any $n \geq m \geq 1$,

$$\overline{d}_n \leq \eta_m (\overline{d}_m)^{n/m} \tag{4}$$

where

$$\eta_m = \max_{0 \leq l \leq m-1} \frac{\overline{d}_l}{(\overline{d}_m)^{l/m}}. \tag{5}$$

Proof: Let $n = m\lfloor n/m \rfloor + l, 0 \leq l \leq m-1$. As a direct consequence of Lemma 1, we get

$$\overline{d}_n \leq \overline{d}_l (\overline{d}_m)^{\lfloor n/m \rfloor} \tag{6}$$

which further implies (4) and (5). $\square$

By using Theorem 1, non-trivial exponential upper bounds can be obtained from any $\overline{d}_m < 2^m$ found by direct counting. It follows that $\overline{d}_m = 2^m, m = 1, 2$, and that $\overline{d}_m < 2^m$ already for $m = 3$. For example, we obtain $\overline{d}_m = 7, 12, 20$ for $m = 3, 4, 5$, respectively. The corresponding upper bounds are approximately $1.094 \cdot 1.913^n$, $1.155 \cdot 1.862^n$, and $1.207 \cdot 1.821^n$, respectively.

The concatenation lemma directly implies a basic upper bound on $d_n(X^n)$ in terms of the run lengths in X^n. Recall that a run in a binary sequence X is a maximal-length subsequence of X consisting of equal consecutive bits. Any binary sequence X^n can uniquely be represented as a sequence of r runs, where $1 \leq r \leq n$. Let $l_1, l_2, \ldots, l_r$ be a generic notation for the positive integer sequence of run lengths in X^n, where $\sum_{i=1}^{r} l_i = n$. The only two sequences with the same sequence of run lenghts are X^n and $\overline{X}^n$. Then, by virtue of the fact that $d_k(c^k) = k+1$ for a constant sequence c^k, Lemma 1 implies that

$$d_n(X^n) \leq \prod_{i=1}^{r} (l_i + 1) \leq (1 + n/r)^r \leq \binom{n+r}{r}. \tag{7}$$

This bound also follows from the fact that $Z = DEC(X^n, C^n)$ depends only on how many bits from each of the runs in X^n are taken to form Z. Note that the rightmost bound in (7) is determined in [2]. However, the basic upper bound is not sharp enough for maximizing $d_n(X^n)$. Namely, for $r = n$, that is, for an alternating sequence X^n, the bound is equal to 2^n and is hence trivial.

3. RECURSIVE CHARACTERIZATION

In this section, we establish a recursive characterization of $d_n(X^n)$ with respect to the sequence length n. This characterization enables one to compute $d_n(X^n)$, for an arbitrary sequence X^n, in at most $2(n-1)$ steps. It is also used in the next section to prove that $d_n(X^n)$ is maximized iff X^n is an alternating sequence and to determine an explicit expression for the maximum $\overline{d}_n$ in terms of the Fibonacci numbers.

To this end, we first introduce the concept of minimal decimation sequences and then define an appropriate partition of the set $D(X^n)$. Note that the natural partition according to the Hamming weight of decimation sequences, that is, according to the length of output sequences obtained after the decimation does not turn out to be convenient.

Each $Z \in D(X^n)$ can be obtained as $DEC(X^n, C^n)$, where the decimation sequence C^n need not be unique. All C^n giving rise to the same Z are thus equivalent. They must have the same Hamming weight and can be represented by a unique decimation sequence $\tilde{C}^n$ which is called minimal and is defined as follows.

Definition 2: Every decimation sequence C^n of Hamming weight $w_H(C^n) = k \geq 1$ can uniquely be represented as an increasing sequence of positive integers $i_1, i_2, \ldots, i_k$ where i_j is the index of the j^{th} 1 in C^n. A decimation sequence $\tilde{C}^n = i_1, i_2, \ldots, i_k$ is called minimal if, for each $1 \leq j \leq k$, i_j is minimal on the set of all C^n such that $DEC(X^n, C^n) = DEC(X^n, \tilde{C}^n)$. Formally, the all-zero sequence $C^n = 0^n$ is considered to be minimal, for $Z = \phi$.

Given $Z^k \in D(X^n)$, the corresponding minimal decimation sequence can recursively be constructed as follows: i_1 is the index of the first bit of X^n equal to z_1, and for each $2 \leq j \leq k$, i_j is the index of the first remaining bit x_i, $i_{j-1} < i \leq n$, equal to z_j. The constructed sequence is the unique minimal decimation sequence, because if we suppose that there exists a sequence C'^n such that $i'_j < i_j$ for at least one value of j, then we get a contradiction. Namely, from the construction, it then follows that $i'_{j'} < i_{j'}$ for every $1 \leq j' < j$, which is impossible for $j' = 1$.

Example 2: Given a sequence $X^4 = 0101$ from Example 1: for $Z = 0$, there are two equivalent decimation sequences 1000 and 0010, where 1000 is minimal; for $Z = 1$, there are two equivalent decimation sequences 0100 and 0001, where 0100 is minimal; for $Z = 01$, there are three equivalent decimation sequences 1100, 1001, and 0011, where 1100 is minimal; and for each of the remaining nine sequences Z, there is exactly one decimation sequence, which is then minimal.

Consequently, for a given X^n, there is an 1-1 correspondence between all possible Z from $D(X^n)$ and all minimal decimation sequences, so that $d_n(X^n)$ is equal to the number of minimal decimation sequences given X^n.

The basic properties of minimal decimation sequences are given by the following lemma, which directly follows from Definition 2.

Lemma 2: If C^n is minimal for X^n, then C^{n-1} is minimal for its prefix X^{n-1}. Furthermore, for any $0 < i < n$, $C^i 0^{n-i}$ is minimal for X^n iff C^i is minimal for its prefix X^i.

We are now ready to introduce a convenient partition of $D(X^n)$ that allows a recursive characterization of $d_n(X^n)$. Let for any $1 \leq i \leq n$, $\tilde{D}_i(X^n)$ denote the set of all the minimal decimation sequences $\tilde{C}^n$ such that i is the index of the last bit of $\tilde{C}^n$ equal to 1, whereas for $i = 0$, let $\tilde{D}_0(X^n) = \{0^n\}$. Let $\Delta_i(X^n) = |\tilde{D}_i(X^n)|$, $0 \leq i \leq n$. According to Lemma 2, we have $\Delta_i(X^n) = \Delta_i(X^i)$. It follows that $\Delta_0(X^0) = \Delta_1(X^1) = 1$, whereas $\Delta_2(00) = 1$ and

$\Delta_2(01) = 2$. Since $C^i = 1^i$ is always minimal, $\Delta_i(X^i) \geq 1$ is true. Consequently, $d_n(X^n)$ can be put into the form

$$d_n(X^n) = \sum_{i=0}^{n} \Delta_i(X^i) = d_{n-1}(X^{n-1}) + \Delta_n(X^n), \tag{8}$$

where formally $d_0(X^0) = 1$.

The desired recursive characterization of $\Delta_n(X^n)$ is established by the following two lemmas. Recall that $l_1, l_2, \ldots, l_r$ denotes the run-length structure of X^n. In particular, if $x_n \neq x_{n-1}$, then $l_r = 1$.

Lemma 3: If $x_n = x_{n-1}$, then

$$\Delta_n(X^n) = \Delta_{n-1}(X^{n-1}). \tag{9}$$

Proof: According to Lemma 2, if $\tilde{C}^n \in \tilde{D}_n(X^n)$, then its prefix $\tilde{C}^{n-1}$ is a minimal decimation sequence for X^{n-1}. If $x_n = x_{n-1}$, then it follows that $\tilde{c}_{n-1} = 1$, that is, $\tilde{C}^{n-1} \in \tilde{D}_{n-1}(X^{n-1})$. Namely, if $\tilde{c}_{n-1} = 0$, then it would be possible to swap the last two bits of $\tilde{C}^n$ without changing the output sequence, that is, $DEC(X^n, \tilde{C}^{n-2}01) = DEC(X^n, \tilde{C}^{n-2}10)$, which implies that $\tilde{C}^n$ would not be minimal for X^n. Consequently, $\Delta_n(X^n) \leq \Delta_{n-1}(X^{n-1})$.

On the other hand, if $\tilde{C}^{n-1} \in \tilde{D}_{n-1}(X^{n-1})$, then the corresponding decimation sequence $\tilde{C}^{n-1}1$ is minimal for X^n, that is, $\tilde{C}^{n-1}1 \in \tilde{D}_n(X^n)$. Namely, if $\tilde{C}^{n-1}1$ is not minimal for X^n, then there exists another decimation sequence C^n such that $c_n = 0$ giving rise to the same output sequence, $DEC(X^n, \tilde{C}^{n-1}1)$. It follows that the same output sequence, $DEC(X^{n-1}, \tilde{C}^{n-1})$, could then be produced by using another decimation sequence obtained by taking the first $n-1$ bits of C^n and by substituting a 0 for the last bit of C^n equal to 1. As the last bit of this decimation sequence is equal to zero, this implies that $\tilde{C}^{n-1}$ would not be minimal for X^{n-1}. Therefore, $\Delta_n(X^n) \geq \Delta_{n-1}(X^{n-1})$. □

Lemma 4: If $x_n \neq x_{n-1}$ and $x_{n-1} = x_{n-2} = \cdots = x_{n-l_{r-1}} \neq x_{n-l_{r-1}-1}$, then

$$\Delta_n(X^n) = l_{r-1}\Delta_{n-1}(X^{n-1}) + \Delta_{n-l_{r-1}-1}(X^{n-l_{r-1}-1}). \tag{10}$$

Proof: According to Lemma 2, if $\tilde{C}^n \in \tilde{D}_n(X^n)$, then its prefix $\tilde{C}^{n-1}$ is a minimal decimation sequence for X^{n-1}. If $x_n \neq x_{n-1}$ and $x_{n-1} = x_{n-2} = \cdots = x_{n-l_{r-1}} \neq x_{n-l_{r-1}-1}$, then it follows that the index i of the last bit of $\tilde{C}^{n-1}$ equal to 1 satisfies $n-l_{r-1}-1 \leq i \leq n-1$, that is, $\tilde{C}^{n-1} \in \tilde{D}_i(X^{n-1})$ for such an i. Namely, if $i < n-l_{r-1}-1$, then it would be possible to swap the bits $\tilde{c}_n$ and $\tilde{c}_{n-l_{r-1}-1}$ without changing the output sequence, which implies that $\tilde{C}^n$ would not be minimal for X^n.

The converse is also true, that is, if $\tilde{C}^{n-1} \in \tilde{D}_i(X^{n-1})$ for any $n-l_{r-1}-1 \leq i \leq n-1$, then the corresponding decimation sequence $\tilde{C}^{n-1}1$ is minimal for X^n, that is, $\tilde{C}^{n-1}1 \in \tilde{D}_n(X^n)$. Namely, if $\tilde{C}^{n-1}1$ is not minimal for X^n, then there exists another decimation sequence C^n giving rise to the same output sequence, $DEC(X^n, \tilde{C}^{n-1}1)$, such that the index j of the last bit equal to 1 satisfies $j \leq n - l_{r-1} - 1$. It follows that the same output sequence, $DEC(X^{n-1}, \tilde{C}^{n-1})$, could then be produced by using another decimation sequence obtained by taking the first $n-1$ bits of C^n and by substituting a 0 for the last bit of C^n equal to 1. As

the index of the last bit of this decimation sequence equal to 1 is thus smaller than $n-l_{r-1}-1$, this implies that $\tilde{C}^{n-1}$ would not be minimal for X^{n-1}. Accordingly, we have

$$\Delta_n(X^n) = \sum_{i=n-l_{r-1}-1}^{n-1} \Delta_i(X^i), \tag{11}$$

which further, by virtue of Lemma 3, implies (10). □

The recursions (9) and (10) enable a very efficient computation of all $\Delta_i(X^i),\ 1 \le i \le n$, for an arbitrary X^n, in at most $n-1$ steps, where each step consists of one integer addition. In view of (8), the computation of $d_n(X^n)$ then requires at most $n-1$ further integer additions. Note that a brute force computation would require an exhaustive testing of all 2^n decimation sequences.

In fact, one can first compute the run-length structure of X^n, with $n-1$ bit comparisons, and then, according to (10), recursively apply

$$\Delta_{L_i}(X^{L_i}) = l_{i-1}\Delta_{L_{i-1}}(X^{L_{i-1}}) + \Delta_{L_{i-2}}(X^{L_{i-2}}) \tag{12}$$

for $2 \le i \le r$, where $L_i = \sum_{j=1}^{i} l_j,\ 1 \le i \le r$, and $L_0 = 0$, starting from $\Delta_0(X^0) = \Delta_{l_1}(X^{l_1}) = 1$. Finally, according to (8), $d_n(X^n)$ is computed by

$$d_n(X^n) = 1 + \sum_{i=1}^{r} l_i \Delta_{L_i}(X^{L_i}). \tag{13}$$

The recursion (12) can be regarded as a linear recursion with variable coefficients and does not allow one to obtain an analytical expression for $d_n(X^n)$, for an arbitrary X^n.

4. OPTIMALITY OF ALTERNATING SEQUENCES AND FIBONACCI NUMBERS

If a sequence X^n is alternating, that is, if $x_i \ne x_{i-1}$ for each $2 \le i \le n$, then $r = n$ and $l_i = 1$, for each $1 \le i \le n$. The recursion (9) then never applies, whereas the recursion (10) (i.e., (12)) then becomes the well-known Fibonacci recursion

$$\Delta_n(X^n) = \Delta_{n-1}(X^{n-1}) + \Delta_{n-2}(X^{n-2}), \tag{14}$$

with the initial values $\Delta_0(X^0) = \Delta_1(X^1) = 1$. Its solution can directly be expressed in terms of the Fibonacci numbers as

$$\Delta_n(X^n) = F(n+1) = \frac{1}{\sqrt{5}}(\alpha^{n+1} - \beta^{n+1}), \tag{15}$$

where, as usual, $\alpha = (1+\sqrt{5})/2$ and $\beta = (1-\sqrt{5})/2$.

If we further apply (8), then we obtain an explicit expression for $d_n(X^n)$ for an alternating sequence X^n, in terms of the Fibonacci numbers.

Theorem 2: If X^n is an alternating sequence, then

$$d_n(X^n) = \sum_{i=0}^{n+1} F(i) = \frac{\sqrt{5}+2}{\sqrt{5}}\alpha^n + \frac{\sqrt{5}-2}{\sqrt{5}}\beta^n - 1. \tag{16}$$

For simplicity, if X^n is an alternating sequence, then denote $d_n(X^n)$ as $\tilde{d}_n$, whereas, according to (15), $\Delta_n(X^n) = F(n+1)$. The optimality of alternating sequences to be proved means that $\bar{d}_n = \tilde{d}_n$ or, equivalently, that $\tilde{d}_n$ is the tightest possible upper bound on $\Delta_n(X^n)$ that holds for every X^n. The main idea of the proof is to study the sequence of differences $\delta_n(X^n) = F(n+1) - \Delta_n(X^n)$ and to prove that this sequence is positive at the point where X^n starts to differ from an alternating sequence and nonnegative after that point. Initially, we have $\delta_1(X^1) = \delta_0(X^0) = 0$. This is achieved by induction, by using the following two lemmas.

Lemma 5: If $x_n = x_{n-1}$, then $\delta_n(X^n) > 0$ if $\delta_{n-1}(X^{n-1}) \geq 0$.

Proof: From (9), it follows that

$$\delta_n(X^n) = \delta_{n-1}(X^{n-1)}) + (F(n+1) - F(n)). \tag{17}$$

The claim then follows since $F(n+1) > F(n)$, for any $n \geq 2$. □

Lemma 6: If $x_n \neq x_{n-1}$ and $x_{n-1} = x_{n-2} = \cdots = x_{n-l_{r-1}} \neq x_{n-l_{r-1}-1}$, then $\delta_n(X^n) \geq 0$ if $\delta_i(X^i) \geq 0$ for each $1 \leq i < n$.

Proof: From (10) and (9), it follows that

$$\begin{aligned} \delta_n(X^n) =& l_{r-1}\delta_{n-l_{r-1}}(X^{n-l_{r-1}}) + \delta_{n-l_{r-1}-1}(X^{n-l_{r-1}-1}) && (18)\\ &+ F(n+1) - l_{r-1}F(n-l_{r-1}+1) - F(n-l_{r-1}). && (19)\end{aligned}$$

The claim then follows since

$$\begin{aligned} F(n+1) &= F(l_{r-1}+1)F(n-l_{r-1}+1) + F(l_{r-1})F(n-l_{r-1}) && (20)\\ &\geq l_{r-1}F(n-l_{r-1}+1) + F(n-l_{r-1}) && (21)\end{aligned}$$

holds for any $n \geq l_{r-1}+1$, which itself is a consequence of the following properties of the Fibonacci numbers: $F(j+1) \geq 1$, $F(j+1) \geq j$, and $F(i+1) = F(j+1)F(i-j+1)+F(j)F(i-j)$, for any $i \geq j \geq 0$. □

Theorem 3: For an arbitrary sequence X^n,

$$d_n(X^n) \leq \tilde{d}_n \tag{22}$$

with equality iff X^n is an alternating sequence.

Proof: The proof is based on Lemmas 5 and 6 and

$$\tilde{d}_n - d_n(X^n) = \sum_{i=0}^{n} \delta_i(X^i), \tag{23}$$

which follows from (8).

If X^n is an alternating sequence, then (22) holds with equality. If X^n is not an alternating sequence, then let j be the minimal index such that $x_j = x_{j-1}$, where $2 \leq j \leq n$. It then follows that X^{j-1} is an alternating sequence, so that $d_i(X^i) = \tilde{d}_i$, $1 \leq i \leq j-1$. For $i = j$, Lemma 5 and (23) then imply that $d_j(X^j) < \tilde{d}_j$. For any $j < i \leq n$, Lemmas 6 and 5 together with (23) then imply that $d_i(X^i) < \tilde{d}_i$. □

Corollary 1:

$$\overline{d}_n = \tilde{d}_n < \frac{\sqrt{5}+2}{\sqrt{5}}\alpha^n < 1.89443 \cdot 1.6181^n. \tag{24}$$

5. ANOTHER BOUND IN TERMS OF FIBONACCI NUMBERS

In this section, we prove yet another upper bound on $d_n(X^n)$ in terms of the Fibonacci numbers. It depends on the run-length structure, $l_1, l_2, \ldots, l_r$, of X^n and, when maximized over X^n, yields another exponential upper bound on $d_n(X^n)$, which is larger than the tightest possible upper bound $\overline{d}_n$.

Theorem 4: For an arbitrary sequence X^n,

$$d_n(X^n) \le \sum_{i=0}^{r+1} F(i) \prod_{i=1}^{r} l_i \le \sum_{i=0}^{r+1} F(i) \left(\frac{n}{r}\right)^r \tag{25}$$

with equalities if X^n is an alternating sequence.

Proof: As $d_n(X^n)$ is equal to the number of minimal decimation sequences given X^n, the bound can be proven by analyzing the structure of minimal decimation sequences in terms of the run lengths in $X^n, l_1, l_2, \ldots, l_r$. Each minimal decimation sequence $\tilde{C}^n$ can be characterized by an r-bit sequence $b_1, \ldots, b_r$ such that $b_i = 1$ iff at least one bit from the i^{th} run of X^n is taken to the output, together with the numbers of bits taken to the output from each of the runs such that $b_i = 1$, where it is assumed that these bits have minimal indexes in each of these runs. The minimality of decimation sequences implies that there are no two consecutive 0's in $b_1, \ldots, b_r$, except possibly at the end, and that if $b_i = 0$, then the number of bits taken to the output from the $(i-1)^{\text{th}}$ run is maximal possible, l_{i-1}. So, $\tilde{C}^n$ is minimal iff it can be represented in this way.

Letting N_r denote the number of all r-bit sequences $b_1, \ldots, b_r$ that can contain consecutive 0's only at the end, we thus obtain

$$d_n(X^n) \le N_r \prod_{i=1}^{r} l_i. \tag{26}$$

If X^n is an alternating sequence, that is, if $r = n$, then $\tilde{C}^n$ is minimal iff there are no consecutive 0's in $b_1, \ldots, b_r$, except possibly at the end. Consequently, (26) then holds with equality and reduces to $d_n(X^n) = N_n$.

The number N_r can be expressed as $\sum_{j=0}^{r} M_j$, where M_j is the number of all r-bit sequences under consideration with the additional property that j is the index of the last bit equal to 1 (where $j = 0$ means that there are no 1's at all). It follows that $M_0 = M_1 = 1$. Letting $\mathcal{M}_j$ denote the set of all j-bit sequences with the j^{th} bit equal to 1 and without consecutive 0's, we have $M_j = |\mathcal{M}_j|, j \ge 1$. If $b_1, \ldots, b_j \in \mathcal{M}_j, j \ge 2$, then b_{j-1} can be equal to 1 or 0. In the former case, we get $b_1, \ldots, b_{j-1} \in \mathcal{M}_{j-1}$ and in the latter case, provided that $j \ge 3$, we get $b_1, \ldots, b_{j-2} \in \mathcal{M}_{j-2}$. Accordingly, we have

$$M_j = M_{j-1} + M_{j-2}, \quad j \ge 2. \tag{27}$$

Therefore, $M_j = F(j+1)$ are the Fibonacci numbers, so that $N_r = \sum_{j=0}^{r+1} F(j)$. The left-hand inequality in (25) thus follows from (26), whereas the right-hand inequality in (25) is a consequence of $(\prod_{i=1}^{r} l_i)^{1/r} \le (\sum_{i=1}^{r} l_i)/r = n/r$. □

Corollary 2:

$$\overline{d}_n < \frac{\sqrt{5}+2}{\sqrt{5}} \left(e^{\alpha/e}\right)^n < 1.89443 \cdot 1.81347^n. \tag{28}$$

Proof: In view of Theorem 2 and Corollary 1, (25) implies that

$$d_n(X^n) < \frac{\sqrt{5}+2}{\sqrt{5}} \alpha^r \left(\frac{n}{r}\right)^r = \frac{\sqrt{5}+2}{\sqrt{5}} \left(e^{g(r/n)}\right)^n \tag{29}$$

where $g(\gamma) = \gamma \ln \alpha - \gamma \ln \gamma$, and $\gamma = r/n$. Accordingly, we have

$$\overline{d}_n < \frac{\sqrt{5}+2}{\sqrt{5}} \left(e^{g_{\max}}\right)^n \tag{30}$$

where $g_{\max}$ is the maximum of $g(\gamma)$ on (0,1]. It is easy to prove that g'' is negative, so that g is concave and has a unique maximum reached for $\gamma = \alpha/e$. Consequently, we get (28). □

ACKNOWLEDGMENT

The author is grateful to an anonymous referee for helpful comments.

REFERENCES

[1] J. Dj. Golić and L. O'Connor. "Embedding and Probabilistic Correlation Attacks on Clock-controlled Shift Registers." *Advances in Cryptology - EUROCRYPT '94, Lecture Notes in Computer Science*, Vol. 950, 230-243, 1995.

[2] V. I. Levenshtein. "Binary Codes for the Correction of Deletions, Insertions, and Substitutions of Symbols." *Doklady Akad. Nauk SSSR* **163** (1965): 845-848.

AMS Classification Numbers: 11B50, 11B39, 94B50

✠ ✠ ✠