Generating Binary Sequences for Stochastic Computing

P. Jeavons, D. A. Cohen, and J. Shawe-Taylor

Abstract—**This paper describes techniques for constructing statistically independent binary sequences with prescribed ratios of zeros and ones. The first construction is a general recursive construction, which forms the sequences from a class of "elementary" sequences. The second construction is a special construction which can be used when the ratio of ones to zeros is expressed in binary notation. The second construction is shown to be optimal in terms of the numbers of input sequences required to construct the desired sequence. The paper concludes with a discussion of how to generate independent "elementary" sequences using simple digital techniques.**

Index Terms—**Stochastic computing, pseudorandom sequences, neural networks.**

I. Introduction

In THIS paper we address the problem of generating statistically independent binary sequences with a prescribed ratio of ones to zeros. Sequences of this kind are necessary for the technique of stochastic computing [1] which offers the possibility of enormously simplified hardware implementations of a number of computing devices. In particular, stochastic computing is recognized as having significant potential for the efficient implementation of neural networks, particularly those involving mixed electro-optical designs [2]. Designs for neural networks using stochastic computing to simplify the hardware required for the synaptic calculations have recently been proposed [3]–[5].

We demonstrate below how the required sequences may be constructed from a class of "elementary" sequences, in which the possible ratios of ones to zeros is restricted to a small set of values. These sequences may be combined, using simple operations on the elements, in order to obtain more general sequences, with arbitrary ratios of ones to zeros, as described in the following sections.

When the required ratio is expressed exactly in binary notation, we show that there is a simple construction using the minimum possible number of "elementary" sequences. The "elementary" sequences in this case may be approximated by statistically independent pseudorandom sequences [10], which may be generated using linear feedback shift registers [11]. A typical way in which these devices may be used to generate appropriate sets of sequences is described in Section V.

The constructions we describe may be easily implemented in fully digital hardware, so they complement the fully digital neural network design described in [4]. Further details of the hardware implementation of the techniques described in this paper may be found in [13].

Previous approaches to the generation of binary sequences with prescribed ratios of ones to zeros have relied on processing the elements of one or more unbiased random binary sequences. A number of simple serial algorithms to do this are given in [6], although these algorithms are not immediately suitable for generating sequences at a very high uniform rate, as required for stochastic computing, since the time required to generate each output bit depends on the values of the input bits from a random sequence.

Random binary sequences with a specified probability of ones are also used for testing VLSI circuits, and there is a large literature on the generation of such test sequences using specialized hardware (see, for example, [7], [8]). An earlier hardware implementation of a suitable sequence generator is given in [1]. However, all of these proposed generation techniques either limit the possible probability values to a small number of fixed values, or require more complex circuitry than the approach described below.

Finally, we note that an alternative method for generating pseudorandom sequences has been described by Wolfram [9], who also mentions in passing that elements of such sequences may be combined to form a sequence with an arbitrary proportion of ones using elementary logic operations.

II. Definitions

Definition 2.1: A *binary sequence* is a sequence of ones (1's) and zeros (0's). The ith element of a binary sequence $\mathscr{A}$ will be denoted $\mathscr{A}[i]$. The sequence obtained from the binary sequence $\mathscr{A}$ by exchanging 1's and 0's will be denoted $\bar{\mathscr{A}}$.

Definition 2.2: The *probability* of a binary sequence $\mathscr{A}$ of length n, denoted $P(\mathscr{A})$, is defined to be the relative frequency of 1's:

$$P(\mathscr{A}) = \frac{\sum_{i=1}^{n} \mathscr{A}[i]}{n}.$$

Manuscript received Nov. 3, 1992; revised Aug. 4, 1993.

The authors are with The Department of Computer Science, Royal Holloway, University of London, London, England.

IEEE Log Number 9401787.

0018-9448/94$04.00 © 1994 IEEE

As an example, consider a pseudorandom sequence as generated by a maximum-period linear feedback shiftregister of length n [10]. Any subsequence of this sequence of length $2^n - 1$ contains 2^{n-1} 1's, and so has probability $2^{n-1}/(2^n - 1)$, or approximately $\frac{1}{2}$.

Definition 2.3: Two binary sequences, $\mathcal{A}$ and $\mathcal{B}$, of the same length, are said to be *independent* if the probability of the sequence $\mathcal{A} \cdot \mathcal{B}$ obtained by elementwise multiplication is equal to the product of the probability of $\mathcal{A}$ and the probability of $\mathcal{B}$, that is

$$P(\mathcal{A} \cdot \mathcal{B}) = P(\mathcal{A}) P(\mathcal{B}).$$

In what follows, we shall assume that all the sequences we consider have the same length.

The definition of independence may be extended to the case of more than two sequences, as follows.

Definition 2.4: The binary sequences in a set, S, are said to be *independent* If the probability of any binary sequence formed by elementwise multiplication of any nonempty subset, R, of S is equal to the product of the probabilities of the sequences in R.

In the technique of stochastic computing, independent binary sequences are used to represent analog values in the interval $[0,1]$. Each value is represented by a binary sequence having probability equal to that value. Multiplication of analog values may then be carried out using simple elementwise multiplication on binary sequences, which can be implemented with a single AND gate.

Several simple consequences of the above definitions are listed in the following proposition.

Proposition 2.5: Let $\mathcal{A}$ and $\mathcal{B}$ be any binary sequences.

1) $P(\bar{\mathcal{A}}) = 1 - P(\mathcal{A})$.
2) If $\mathcal{A}$ and $\mathcal{B}$ are independent, then $\mathcal{A}$ and $\bar{\mathcal{B}}$ are independent.
3) If there is no index i such that $\mathcal{A}[i] = \mathcal{B}[i] = 1$, then we may form the binary sequence $\mathcal{A} + \mathcal{B}$ in which each element is the sum of the corresponding elements from $\mathcal{A}$ and $\mathcal{B}$ and

$$P(\mathcal{A} + \mathcal{B}) = P(\mathcal{A}) + P(\mathcal{B}).$$

We now define an integer-valued function of the probability of a sequence, which may be used to divide sequences into classes.

Definition 2.6: The *length* of a probability with respect to a specified base is the number of digits required after the point when the probability is expressed as a fraction in standard place notation with respect to that base.

When the base is obvious from the context then it will be omitted, and we will simply refer to the length of the probability. The length of the probability of binary sequence $\mathcal{A}$ with respect to base k will be denoted $\mu_k(\mathcal{A})$.

Note that a binary sequence with probability 0 consists entirely of zeros, and has length 0. Similarly, a binary sequence with probability 1 consists entirely of ones and has length 0.

Several simple properties of the length function are listed in the following proposition.

Proposition 2.7: Let $\mathcal{A}$ and $\mathcal{B}$ be any binary sequences, and let k be any number base.

1) $\mu_k(\bar{\mathcal{A}}) = \mu_k(\mathcal{A})$.
2) If $\mathcal{A}$ and $\mathcal{B}$ are independent, and neither sequence consists entirely of 0's, then

$$\mu_k(\mathcal{A} \cdot \mathcal{B}) = \mu_k(\mathcal{A}) + \mu_k(\mathcal{B}).$$

3) If there is no index i such that $\mathcal{A}[i] = \mathcal{B}[i] = 1$, then we may form the binary sequence $\mathcal{A} + \mathcal{B}$ in which each element is the sum of the corresponding elements from $\mathcal{A}$ and $\mathcal{B}$ and

$$\mu_k(A + B) \leq \max\{\mu_k(\mathcal{A}), \mu_k(\mathcal{B})\}.$$

Definition 2.8: An *elementary binary sequence* with respect to a specified base is one whose probability has length zero or one with respect to that base.

Again, when the base is obvious from the context we will simply refer to elementary sequences. Sequences with probability $\frac{1}{2}$ are elementary with respect to base 10, since the probability may be written in decimal notation as 0.5. They are also elementary with respect to base 2, since the probability may be written in binary notation as 0.1.

The bulk of this paper will be concerned with algorithms for constructing binary sequences whose probabilities are of arbitrary length from independent elementary binary sequences. We will restrict our attention to algorithms which use only a fixed function of a single element of each input sequence to compute each element of the output sequence. An algorithm that satisfies this restriction will be referred to as a *local* algorithm. This restriction allows us to quantify in a well-defined sense the number of elementary binary sequences required by an algorithm. It rules out, for example, algorithms that sample the odd elements of an input binary sequence and the even elements of the same input sequence, to obtain two separate elementary binary sequences which can then be combined in some way to construct an output sequence.

Formally, we define a local algorithm as follows.

Definition 2.9: There is a *local algorithm* that computes a binary sequence $\mathcal{A}$ from the sequences $\mathcal{A}_1, \mathcal{A}_2, \cdots, \mathcal{A}_m$ if and only if there exists a binary-valued function F of m binary variables such that, for all i,

$$\mathcal{A}[i] = F(\mathcal{A}_1[i], \mathcal{A}_2[i], \cdots, \mathcal{A}_m[i]).$$

Note that a local algorithm with no inputs must compute a constant function.

Local algorithms have the following desirable property.

Proposition 2.10: Let $\mathcal{A}_1, \mathcal{A}_2, \cdots, \mathcal{A}_m$ be independent binary sequences. If $\mathcal{B}$ is computed from $\mathcal{A}_1, \mathcal{A}_2, \cdots, \mathcal{A}_{m-1}$ by any local algorithm, then $\mathcal{B}$ is independent of $\mathcal{A}_m$.

Proof: The result is proved by induction. The result holds for $m = 1$, because in this case $\mathcal{B}$ must be the sequence consisting entirely of 1's or the sequence consisting entirely of 0's, and these are both independent of all other sequences.

Now assume that the result holds for all values of m less than r and consider the case when $m = r$. In this case we have a set of independent binary sequences, $\mathscr{A}_1,\mathscr{A}_2,\cdots,\mathscr{A}_r$, and we assume that $\mathscr{B}$ is computed from $\mathscr{A}_1,\mathscr{A}_2,\cdots,\mathscr{A}_{r-1}$ by a local algorithm.

By the definition of local algorithm there exists a function F such that

$$\mathscr{B}[i] = F(\mathscr{A}_1[i],\mathscr{A}_2[i],\cdots,\mathscr{A}_{r-1}[i]).$$

Define two sequences $\mathscr{B}_0$ and $\mathscr{B}_1$ as follows:

$$\mathscr{B}_0[i] = F(\mathscr{A}_1[i],\mathscr{A}_2[i],\cdots,\mathscr{A}_{r-2}[i],0),$$
$$\mathscr{B}_1[i] = F(\mathscr{A}_1[i],\mathscr{A}_2[i],\cdots,\mathscr{A}_{r-2}[i],1).$$

Now we have

$$\mathscr{B}[i] = \mathscr{A}_{r-1}[i]\cdot\mathscr{B}_1[i] + \overline{\mathscr{A}_{r-1}}[i]\cdot\mathscr{B}_0[i],$$

giving

$$\mathscr{B}[i]\cdot\mathscr{A}_r[i] = \mathscr{A}_{r-1}[i]\cdot\mathscr{B}_1[i]\cdot\mathscr{A}_r[i] + \overline{\mathscr{A}_{r-1}}[i]\cdot\mathscr{B}_0[i]\cdot\mathscr{A}_r[i].$$

Now consider the set of binary sequences $\mathscr{A}_1,\mathscr{A}_2,\cdots,\mathscr{A}_{r-2},\mathscr{A}_{r-1}\cdot\mathscr{A}_r$. This set is clearly independent, so by the induction hypothesis $\mathscr{B}_1$ is independent of $\mathscr{A}_{r-1}\cdot\mathscr{A}_r$. Similarly, the set of binary sequences $\mathscr{A}_1,\mathscr{A}_2,\cdots,\mathscr{A}_{r-2},\overline{\mathscr{A}_{r-1}}\cdot\mathscr{A}_r$ is independent and $\mathscr{B}_0$ is independent of $\overline{\mathscr{A}_{r-1}}\cdot\mathscr{A}_r$.

Therefore, using Proposition 2.5 we obtain

$$\begin{aligned} P(\mathscr{B}\cdot\mathscr{A}_r) &= P(\mathscr{A}_{r-1})\cdot P(\mathscr{B}_1)\cdot P(\mathscr{A}_r) \\ &\quad + P(\overline{\mathscr{A}_{r-1}})\cdot P(\mathscr{B}_0)\cdot P(\mathscr{A}_r) \\ &= P(\mathscr{B})P(\mathscr{A}_r). \end{aligned}$$

Hence $\mathscr{B}$ is independent of $\mathscr{A}_r$ and the result follows by induction. □

III. Constructing Binary Sequences

In this section we describe an algorithm for constructing binary sequences of any finite-length probability from elementary binary sequences. We first give an example for the case where the base is 10.

Example 3.1: We make an example construction of a binary sequence $\mathscr{B}$ with probability of length 2 with respect to base 10, from three elementary binary sequences $\mathscr{A}_1,\mathscr{A}_2,\mathscr{A}_3$. Choose the elementary binary sequences $\mathscr{A}_1,\mathscr{A}_2,\mathscr{A}_3$ so that

$$P(\mathscr{A}_1) = 0.6, \qquad P(\mathscr{A}_2) = 0.2, \qquad P(\mathscr{A}_3) = 0.3.$$

Ensure that $\mathscr{A}_1$ and $\mathscr{A}_2$ are independent, and that $\mathscr{A}_1$ and $\mathscr{A}_3$ are independent.

We will now construct a sequence $\mathscr{B}$ with probability 0.26 from these three sequences. For each i, set the ith element of $\mathscr{B}$ as follows:

$$\mathscr{B}[i] = \overline{\mathscr{A}_1}[i]\cdot\mathscr{A}_2[i] + \mathscr{A}_1[i]\cdot\mathscr{A}_3[i].$$

Using Proposition 2.5 we have

$$P(\mathscr{B}) = (1 - P(\mathscr{A}_1))P(\mathscr{A}_2) + P(\mathscr{A}_1)P(\mathscr{A}_3).$$

Hence

$$P(\mathscr{B}) = (1 - 0.6)*0.2 + 0.6*0.3 = 0.26,$$

as required. The length of the probability of $\mathscr{B}$ with respect to base 10, $\mu_{10}(\mathscr{B})$, is 2.

This example illustrates the following general algorithm for constructing a binary sequence with a given probability from binary sequences with probabilities of shorter length.

Proposition 3.2: Let k be a suitable number base. It is possible to construct a binary sequence $\mathscr{B}$ having any desired probability value such that $\mu_k(\mathscr{B}) = n$ using three independent binary sequences, $\mathscr{A}_1$, $\mathscr{A}_2$, and $\mathscr{A}_3$ such that $\mu_k(\mathscr{A}_1) = n - 1$ and $\mathscr{A}_2$, $\mathscr{A}_3$ are elementary sequences with respect to base k.

Proof: Suppose that the desired probability is $P(\mathscr{B}) = 0\cdot d_1 d_2 \cdots d_n$ in standard place notation with respect to base k. Choose three sequences $\mathscr{A}_1,\mathscr{A}_2,\mathscr{A}_3$ such that

$$P(\mathscr{A}_1) = 0\cdot d_2 d_3 \cdots d_n,$$
$$P(\mathscr{A}_2) = 0\cdot d_1,$$
$$P(\mathscr{A}_3) = 0\cdot d_1 + 1/k,$$

and $\mathscr{A}_1$ is independent of both $\mathscr{A}_2$ and $\mathscr{A}_3$. [Note that $P(\mathscr{A}_2)$ may be equal to 0, and $P(\mathscr{A}_3)$ may be equal to 1.]

Calculate each element of $\mathscr{B}$ as follows:

$$\mathscr{B}[i] = \overline{\mathscr{A}_1}[i]\cdot\mathscr{A}_2[i] + \mathscr{A}_1[i]\cdot\mathscr{A}_3[i].$$

Using Proposition 2.5 the probability of $\mathscr{B}$ is

$$P(\mathscr{B}) = (1 - P(\mathscr{A}_1))P(\mathscr{A}_2) + P(\mathscr{A}_1)P(\mathscr{A}_3).$$

Hence

$$P(\mathscr{B}) = P(\mathscr{A}_2) + P(\mathscr{A}_1)/k = 0.d_1 d_2 \cdots d_n,$$

as required. □

This construction effectively allows us to add an extra digit to the probability of a sequence, by combining the sequence with two elementary sequences.

Note that, given any further sequence $\mathscr{A}_4$, such that $\mathscr{A}_1$, $\mathscr{A}_2$, $\mathscr{A}_3$, and $\mathscr{A}_4$ are independent, we know from Proposition 2.10 that $\mathscr{A}_4$ will be independent of the binary sequence $\mathscr{B}$ constructed by this algorithm. Hence, using this construction repeatedly, we can construct binary sequences with probabilities of arbitrary finite length from a set of independent elementary sequences.

Corollary 3.3: Let k be a suitable number base. It is possible to construct a binary sequence $\mathscr{B}$ having any desired probability value such that $\mu_k(\mathscr{B}) = n$ using at most $2n - 1$ independent elementary binary sequences with respect to base k.

Proof: Use Proposition 3.2 repeatedly. □

This result gives an upper bound for the number of elementary sequences required to construct a sequence with a probability of a given length. We can also obtain a lower bound for the number of independent elementary binary sequences required by any local construction algorithm. This lower bound is obtained as a consequence of the following proposition.

Proposition 3.4: If $\mathscr{B}$ is computed from a set of independent binary sequences $\mathscr{A}_1, \mathscr{A}_2, \cdots, \mathscr{A}_m$ by any local algorithm, then for any number base k,

$$\mu_k(\mathscr{B}) \leq \sum_{i=1}^{m} \mu_k(\mathscr{A}_i).$$

Proof: This result is proved by induction. The result holds for $m = 0$, because in this case $\mathscr{B}$ must be the sequence consisting entirely of 1's or the sequence consisting entirely of 0's, and these both have length 0.

Now assume that the result holds for all values of m less than r and consider the case when $m = r$. In this case we assume that $\mathscr{B}$ is computed from $\mathscr{A}_1, \mathscr{A}_2, \cdots, \mathscr{A}_r$ by a local algorithm. By the definition of local algorithm there exists a function F such that

$$\mathscr{B}[i] = F(\mathscr{A}_1[i], \mathscr{A}_2[i], \cdots, \mathscr{A}_r[i]).$$

Define two sequences $\mathscr{B}_0$ and $\mathscr{B}_1$ as follows:

$$\mathscr{B}_0[i] = F(\mathscr{A}_1[i], \mathscr{A}_2[i], \cdots, \mathscr{A}_{r-1}[i], 0),$$
$$\mathscr{B}_1[i] = F(\mathscr{A}_1[i], \mathscr{A}_2[i], \cdots, \mathscr{A}_{r-1}[i], 1).$$

Now we have

$$\mathscr{B}[i] = \mathscr{A}_r[i] \cdot \mathscr{B}_1[i] + \overline{\mathscr{A}_r}[i] \cdot \mathscr{B}_0[i].$$

Using Proposition 2.7 we obtain

$$\begin{aligned} \mu_k(\mathscr{B}) &\leq \max\{\mu_k(\mathscr{A}_r \cdot \mathscr{B}_1), \mu_k(\overline{\mathscr{A}_r} \cdot \mathscr{B}_0)\} \\ &= \max\{\mu_k(\mathscr{A}_r) + \mu_k(\mathscr{B}_1), \mu_k(\mathscr{A}_r) + \mu_k(\mathscr{B}_0)\} \\ &= \mu_k(\mathscr{A}_r) + \max\{\mu_k(\mathscr{B}_1), \mu_k(\mathscr{B}_0)\}. \end{aligned}$$

By the induction hypothesis,

$$\mu_k(\mathscr{B}_0) \leq \sum_{i=1}^{r-1} \mu_k(\mathscr{A}_i),$$
$$\mu_k(\mathscr{B}_1) \leq \sum_{i=1}^{r-1} \mu_k(\mathscr{A}_i).$$

So we have

$$\mu_k(\mathscr{B}) \leq \sum_{i=1}^{r} \mu_k(\mathscr{A}_i),$$

and the result follows by induction. □

The following is then a direct corollary.

Corollary 3.5: If $\mathscr{B}$ is computed from a set of m independent elementary binary sequences with respect to base k and $\mu_k(\mathscr{B}) = n$, then $m \geq n$.

IV. A Special Construction for Base 2

In this section we show that a binary sequence of length n with respect to base 2 may be constructed using only n independent elementary binary sequences with respect to base 2. In the light of Corollary 3.5 this is an optimal construction. This construction also has the advantage that the only nonconstant elementary sequences with respect to base 2 have probability $\frac{1}{2}$. This means that good approximations to independent elementary sequences may be easily obtained using linear feedback shift registers, as will be described in Section V.

Proposition 4.1: Any binary sequence $\mathscr{B}$ such that $\mu_2(\mathscr{B}) = n$ may be constructed using n independent elementary binary sequences with respect to base 2.

Proof: The construction for each successive digit in the expression for $P(\mathscr{B})$ is the same as that used in the proof of Proposition 3.2, but when the base is 2 there are only 2 possible cases.

1) $P(\mathscr{A}_2) = 0$, $P(\mathscr{A}_3) = \frac{1}{2}$.
2) $P(\mathscr{A}_2) = \frac{1}{2}$, $P(\mathscr{A}_3) = 1$.

In the first case the construction simplifies to

$$\mathscr{B}[i] = \mathscr{A}_1[i] \cdot \mathscr{A}_3[i],$$

and in the second case it simplifies to

$$\mathscr{B}[i] = \overline{\mathscr{A}_1}[i] \cdot \mathscr{A}_2[i] + \mathscr{A}_1[i].$$

In either case there is only one additional elementary sequence required for each digit, so only n independent elementary sequences are required in total. □

Note that the two cases mentioned in this construction consist of taking either the conjunction or the disjunction of two binary sequences. Hence the construction of any binary sequence with probability of length n with respect to base 2 can be performed using only $n - 1$ binary logical connectives. Since we have shown in Corollary 3.5 that n input sequences are required, this is clearly the minimum possible number of binary connectives. One consequence of this is that the construction may be implemented using very simple logic circuitry [13].

It is possible to apply the construction described above to form sequences whose desired probability is not expressed in binary notation: the probability is simply converted to binary notation. Note, however, that this conversion increases the length of the probability, in general.

V. Constructing Elementary Sequences

The results in the previous sections have reduced the problem of constructing independent binary sequences with arbitrary probability to the problem of constructing independent *elementary* sequences. In this section we will explain a simple general method for generating n elementary binary sequences with respect to base 2.

The method uses the well-established technology of linear feedback shift registers [10]–[12]. A linear feedback shift register of degree n generates a sequence, $\mathscr{A}$, of arbitrary length, as follows:

$$\mathscr{A}[1], \mathscr{A}[2], \cdots, \mathscr{A}[n] \text{ are arbitrary binary values}$$

$$\forall p \geq 0, \qquad \mathscr{A}[n+1+p] = \sum_{i=1}^{n} a_i \mathscr{A}[i+p]$$

(where the a_i are fixed binary values and the addition is performed modulo 2). Sequences generated by linear feedback shift registers can be shown to have the following properties.

Proposition 5.1 [12]: If $\mathscr{A}$ is a sequence generated by a linear feedback shift register of degree n, then

1) $\mathscr{A}$ is periodic.
2) the period of $\mathscr{A}$ is $\leq 2^n - 1$.
3) if $\mathscr{A}$ has period $2^n - 1$, then every nonzero binary sequence of length n occurs exactly once as a subsequence of $\mathscr{A}$ for each cycle.

A sequence of period $2^n - 1$ generated by a linear feedback shift register of degree n is often referred to as a "pseudorandom" sequence. The main result of this section can now be proved.

Proposition 5.2: Let $\mathscr{A}$ be a pseudorandom sequence generated by a linear feedback shift register of degree n and let $\mathscr{A}_1,\cdots,\mathscr{A}_n$ be n subsequences of $\mathscr{A}$ of length $2^n - 1$ beginning at n consecutive positions in $\mathscr{A}$. Then the n sequences $\mathscr{B}_1, \mathscr{B}_2,\cdots, \mathscr{B}_n$ formed by appending a zero to each of these sequences are all independent with probability $\frac{1}{2}$.

Proof: Consider the product of any k of the n sequences, $\mathscr{B}_{j_1}\cdot\mathscr{B}_{j_2}\cdots\mathscr{B}_{j_k}$. For any i in the range 1 to $2^n - 1$ we have

$$\mathscr{B}_{j_1}[i]\cdot\mathscr{B}_{j_2}[i]\cdots\mathscr{B}_{j_k}[i] = \mathscr{A}[m+j_1+i]\cdot\mathscr{A}[m+j_2+i]\cdots\mathscr{A}[m+j_k+i]$$

for some $m \geq 0$. Using Proposition 5.1, we know that the expression on the right-hand side will take the value 1 exactly 2^{n-k} times as i varies from 1 to $2^n - 1$. When $i = 2^n$ then $\mathscr{B}_{j_1}.\mathscr{B}_{j_2}\cdots\mathscr{B}_{j_k} = 0$ by construction. Hence

$$P(\mathscr{B}_{j_1}\cdot\mathscr{B}_{j_2}\cdots\mathscr{B}_{j_k}) = 2^{n-k}/2^n = 1/2^k.$$

Taking k equal to 1, we have shown that the probability of each of the sequences $\mathscr{B}_j$ is $\frac{1}{2}$. Since the value of k is arbitrary we have also demonstrated the independence of the set $\mathscr{B}_1, \mathscr{B}_2,\cdots, \mathscr{B}_n$. □

Corollary 5.3: The vectors $\mathscr{A}_1,\cdots,\mathscr{A}_n$ have probability $2^{n-1}/(2^n - 1)$, and the product of any k of these sequences has probability $2^{n-k}/(2^n - 1)$.

Hence, when the value of n is large the sequences $\mathscr{A}_1, \mathscr{A}_2,\cdots,\mathscr{A}_n$ may be used without modification to provide a very good approximation to independent elementary sequences.

VI. Conclusion

This paper has described a method for generating binary sequences with arbitrary ratios of 1's to 0's using simple digital techniques. We are currently implementing these techniques in a hardware device which will be used to supply inputs to a stochastic neural network chip [13]. The extreme simplicity of the circuitry required to implement techniques we have described allows many parallel sequence generators to be incorporated on a single chip.

References

[1] B. R. Gaines, "Stochastic computing systems," *Adv. Inf. Syst. Sci.*, vol. 2, pp. 37–172, 1969.

[2] R. A. Leaver, and P. Mars, "Stochastic computing and reinforcement neural networks," presented at the IEE Conf. Artificial Neural Networks, 1989, pp. 163–169.

[3] J. S. Shawe-Taylor, P. G. Jeavons, and M. Van Daalen, "Probabilistic bit stream neural chip: Theory," *Connect. Sci.*, vol. 3, pp. 317–328, 1991.

[4] M. Van Daalen, P. G. Jeavons, and J. S. Shawe-Taylor, "Probabilistic bit stream neural chip: Implementation," in *Proc. Int. Workshop on VLSI for AI and Neural Networks*, (Oxford), 1990.

[5] M. S. Tomlinson, Jr., D. J. Walker, and M. A. Sivilotti, "A digital neural network architecture for VLSI," *International Joint Conference on Neural Networks* (San Diego, CA), II, 1990, pp. 545–550.

[6] D. E. Knuth, and A. C. Yao, "The complexity of nonuniform random number generation," in *Algorithms and Complexity*, J. T. Traub, Ed. New York: Academic Press, 1976, pp. 357–428.

[7] J. A. Waicukauski, E. Lindbloom, E. Eichelberger, and O. P. Forlenza, "A method for generating weighted random test patterns," *IBM J. Res. Dev.*, vol. 33, pp. 149–161, 1989.

[8] A. P. Ströle and H-J. Wunderlich, "TESTCHIP: A chip for weighted random pattern generation, evaluation and test control," *IEEE J. Solid-State Circuits*, vol. 26, pp. 1056–63, 1991.

[9] S. Wolfram, "Random sequence generation by cellular automata," *Adv. Appl. Math.*, vol. 7, pp. 123–169, 1986.

[10] G. H. de Visme, *Binary Sequences*. London: English University Press, 1971.

[11] P. H. R. Scholefield, "Shift register generating m-sequences," *Electron. Tech.*, Oct. 1960.

[12] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. North-Holland, 1983.

[13] M. Van Daalen, P. Jeavons, and J. Shawe-Taylor, "Device for generating binary sequences for stochastic computing," *Electron. Lett.*, vol. 29, pp. 80–81, 1993.