Parallel Scrambling Techniques for Multibit-Interleaved Multiplexing Environments

Seok Chang Kim and Byeong Gi Lee

Department of Electronics Engineering, Seoul National University, Seoul, 151-742, Korea

ABSTRACT: In this paper, parallel scrambling technique is discussed which is applicable in the multibit-interleaved multiplexing environment. In support to the development of the technique, the concepts of SSRG (simple shift register generator), MSRG (modular shift register generator) and PSRG (parallel shift register generator) are introduced, and their properties are investigated in various aspects. It is shown in the paper that the resulting technique can be applied for parallel scrambling in the SDH-based lightwave transmission environment.

I. Introduction

In today’s lightwave transmission, the transmission rate extends from several hundred Mbps to a few Gbps. The transmission signal usually consists of integer multiple of some base-rate signals. The base rate refers to the rate at which the low-speed processing such as synchronization and frame formatting is performed. The base-rate signals are multiplexed through byte-interleaved multiplexing (BIM) to form the transmission-rate signal. The transmission-rate signal is scrambled and finally NRZ (non-return-to-zero) or RZ (return-to-zero) line-coded before transmission. The role of scrambling in this process is to provide a high data-transition density, to reduce inter-symbol interference, and to suppress static pattern-dependent jitter [1][2]. The most typical examples of such lightwave transmission can be found in the synchronous digital hierarchy (SDH) system which has been standardized by the CCITT [5]. In this system, the transmission rates of the signals STDM-1, STM-4 and STM-16 are respectively one, four and 16 times 155.520 Mbps.

Since scrambling at such a high transmission rate - so called serial scrambling - is not cost effective and is sometimes beyond the limit of existing technology, it is desirable to push down the serial scrambling to a base rate whenever it is possible. So the concept of parallel scrambling has been introduced to replace the serial scrambling in the bit-interleaved multiplexing environment [4]. Parallel scrambling refers to a set of scrambling performed at the base rate which collectively achieves, after bit-interleaved multiplexing, the effect of the serial scrambling at the transmission rate. That is, the bit-interleaved signal of the parallel-scrambled base-rate signals is identical to the serial-scrambled signal of the bit-interleaved base-rate signals. An example of parallel scrambling applied along with permuting to lightwave transmission can be found in [5].

Existing parallel scrambling technique for frame-synchronous scrambling relies on the property that parallel scrambler output sequence are decimations of the original serial scrambler output sequence [4]. It also relies on some fundamental properties of shift register generators (SRGs) described in [6] and [7]. However, those properties do not work for the byte-interleaved multiplexing environment, and therefore the parallel scrambling technique is not applicable to the SDH signals such as STM-4 and STM-16.

In this paper, we will develop a theory on parallel SRGs (PSRGs) that can extend the parallel scrambling technique to the multibit-interleaved multiplexing environment. In developing the theory we will introduce the concept of simple SRG (SSRG) and modular SRG (MSRG), and investigate their properties without proofs. The proofs can be found in [6] and [7]. We will consider PSRGs based on the MSRGs and examine how to achieve minimal realizations for the PSRGs as well as MSRGs. Finally, we will demonstrate the PSRG theory on parallel scrambling of the SDH signals STM-4 and STM-16.

II. Shift Register Generators

Shift register sequence generators can be classified into two categories: SSRG (Simple Shift Register Generator) and MSRG (Modular Shift Register Generator) [7]. An SSRG is determined by its characteristic polynomial

\[ C(x) = \sum_{i=0}^{L} c_i x^i, \quad (1a) \]

and an MSRG is determined by its generating polynomial

\[ G(x) = \sum_{i=0}^{L} g_i x^i, \quad (1b) \]

where \( L \) is the number of shift registers. In the expressions, the coefficients \( c_i \) and \( g_i \) are either 0 or 1 for \( i = 1, 2, \ldots, L-1 \), and are both 1 for \( i = 0 \) and \( L \). Note that summation and multiplications in this paper are all based on modulo-2 operations except for those in subscripts and superscripts.

We denote by \( d_{j}^{(k)} \) and \( d_k \), for \( i = 0, 1, \ldots, L-1, k = 0, 1, \ldots \), the states of the \( i \)th shift register at time \( k \) of SSRG and MSRG respectively. Then the SSRG sequence \( \{ t_k, k = 0, 1, \ldots \} \) is identical to \( \{ d_{L-k}^{(L-k)}, k = 0, 1, \ldots \} \) and the MSRG sequence \( \{ s_k, k = 0, 1, \ldots \} \) is identical to \( \{ d_{L-k}^{(L-k)}, k = 0, 1, \ldots \} \). That is,

\[ t_k = d_{L-k}^{(L-k)}, \quad k = 0, 1, \ldots \quad (2a) \]

\[ s_k = d_{L-k}^{(L-k)}, \quad k = 0, 1, \ldots \quad (2b) \]

Fig. 1 shows configurations of the SSRG and the MSRG characterized by equations (1a) and (1b) respectively. In the figure, each rectangular block indicates a shift register, and the value \( d_{j}^{(k)} \) or \( d_k \) inside the block represents the \( k \)th state value of the shift register.

We define by \( D_k(s) \) and \( D_k(x) \) the \( k \)th state polynomials, which represent the shift register states at time \( k \) for SSRG and MSRG respectively. More specifically,

\[ D_k(s) = \sum_{i=0}^{L-1} d_{i}^{(k)} s^i, \quad (3a) \]
and
\[ D_k(x) = \sum_{i=0}^{L-1} d_i x_i^i. \]  

We call \( D_k(x) \) and \( D_k(x) \) the initial state polynomials of the SSRG and the MSRG sequences respectively. Then an SSRG sequence \( \{ s_k \} \) is completely determined by its characteristic polynomial \( C(x) \) and its initial state polynomial \( D_k(x) \); and an MSRG sequence \( \{ s_k \} \) is completely determined by its generating polynomial \( G(x) \) and its initial state polynomial \( D_k(x) \). Therefore, we can denote an SSRG sequence \( \{ s_k \} \) as \( S_{\text{SSRG}}(G(x), D_k(x)) \) and denote an MSRG sequence \( \{ s_k \} \) as \( S_{\text{MSRG}}(G(x), D_k(x)) \).

The following proposition shows that there exists one-to-one correspondence between the SSRG and MSRG configurations.

**Proposition 1 (Conversion Property).** The SSRG sequence \( S_{\text{SSRG}}(C(x), D_k(x)) \) is identical to the MSRG sequence \( S_{\text{MSRG}}(G(x), D_k(x)) \) if \( C(x) = x^L G(x^{-1}) \) and \( D_k(x) = G(x) D_k(x) \), where \( G(x) \) is the quotient polynomial of \( x^L D_k(x) \) divided by \( G(x) \).

By the proposition, once given one type of shift register sequence generator along with its initial states, we can always identify the other type together with the required initial states using the proposition. Therefore we will concentrate only on the MSRG type for discussions.

We define by an irreducible MSRG an MSRG whose generating polynomial is relatively prime to its accompanying initial state polynomial. Then, the following factoring property shows that an MSRG sequence generated by an MSRG can also be generated by its related irreducible MSRG.

**Proposition 2 (Factoring).** For a nonzero polynomial \( a(x) \), we have the relation \( S_{\text{MSRG}}(a(x), G(x), D_k(x)) = S_{\text{MSRG}}(G(x), D_k(x)) \).

The following uniqueness property shows that for an MSRG sequence, the irreducible MSRG generating the sequence is unique.

**Proposition 3 (Uniqueness).** Let \( G(x) \) and \( \hat{G}(x) \) be respectively, relatively prime to \( D_k(x) \) and \( \hat{D}(x) \). Then, \( S_{\text{MSRG}}(G(x), D_k(x)) = S_{\text{MSRG}}(\hat{G}(x), \hat{D}(x)) \), if, and only if, \( G(x) = \hat{G}(x) \) and \( D_k(x) = \hat{D}(x) \).

Now, for a periodic binary sequence, we consider how to determine the smallest-sized MSRG generating the sequence. We call such an MSRG the minimal MSRG for the sequence. That is, the minimal MSRG for a given sequence is the one whose generating polynomial is of the lowest order among all the MSRGs generating the sequence. Then, by Propositions 2 and 3, we can easily show that the minimal MSRG for a periodic sequence is the irreducible MSRG generating the sequence. The following proposition describes how to obtain the minimal MSRG for a given sequence, or the irreducible MSRG generating the sequence.

**Proposition 4 (Minimal Realization).** Given a periodic sequence \( \{ s_k \} \) of period \( P \), let \( d(x) \) be the greatest common divisor of the polynomials \( x^P + 1 \) and \( \sum_{i=0}^{P-1-i} d_i x_i^i \). Then, the minimal MSRG for the sequence \( \{ s_k \} \) is the irreducible MSRG having the generating polynomial \( x^P + 1 \) and the initial state polynomial \( \sum_{i=0}^{P-1-i} d_i u_i \).

III. Parallel Shift Register Generators

In this section, we consider parallel-form realizations of sequence generators. We first define parallel shift register generators, and then discuss some properties of the MSRG sequences in relation to parallel shift register generators. Finally, we consider their realizations.

We define by a PSRG (Parallel Shift Register Generator) a shift register generator which generates multiple sequences — so called parallel sequences. For a given sequence \( \{ s_k \} \), if a PSRG generates \( N \) parallel sequences \( \gamma_i, i = 0, 1, \ldots, N-1 \), meeting the relations

\[
T_0 = \{ s_0, s_1, \ldots, s_{2^M-1}\}, T_1 = \{ s_{M}, s_{M+1}, \ldots, s_{2^M-1}\}, T_2 = \{ s_{2M}, s_{2M+1}, \ldots, s_{2^M-1}\}, \ldots \]

\[
T_{N-1} = \{ s_{(N-1)M}, s_{(N-1)M+1}, \ldots, s_{2^M-1}\}, \]

then we call this PSRG an \( (M, N) \) PSRG for the sequence \( \{ s_k \} \). In other words, an \( (M, N) \) PSRG for a sequence generates \( N \) parallel sequences such that the \( M \)-bit interleaved sequence, which is obtained by interleaving them by \( M \) sequence elements (or \( M \) bits), is identical to the original sequence. Fig.2 describes an \((M, N)\) PSRG for a sequence \( \{ s_k \} \).

We define the \( i \)-th \( n \)-decimated sequence \( U_{ij}, i = 0, 1, \ldots, n-1 \), of a sequence \( \{ s_k \} \) to be \( U_{ij} = \{ s_{j+im}, i = 0, 1, \ldots, n-1 \} \). Then, the sequence \( \{ s_k \} \) becomes the interleaved (that is, 1-bit interleaved) sequence of the \( n \)-decimated sequences \( U_{ij} \), \( i = 0, 1, \ldots, n-1 \). We obtain the following two properties in relation to decimation and interleaving.

**Proposition 5 (Decimation).** Let \( U_{ij}, i = 0, 1, \ldots, n-1 \), be the \( i \)-th \( n \)-decimated sequence of a sequence \( S_{\text{MSRG}}(G(x), \sum_{j=0}^{L-1} d_j x_j^j) \), where \( L \)

\[
is the degree of \( G(x) \). Then, \( U_{ij} = S_{\text{MSRG}}(G(x), \sum_{j=0}^{(n-i)j} d_j x_j^j) \).

**Proposition 6 (Interleaving).** Let \( T \) be the interleaved sequence of \( n \) sequences \( S_{\text{MSRG}}(G(x), D_k(x)) \), \( i = 0, 1, \ldots, n-1 \). Then, \( T = S_{\text{MSRG}}(G(x), \sum_{j=0}^{n-1-j} D_k(x^j)) \).

We can generate \((M, N)\) PSRG sequences by applying the two properties. That is, the \((M, N)\) PSRG sequences \( T_j \) in (4) can be obtained by \( MN \)-decimating the sequence \( \{ s_k \} \) and then interleaving each adjacent \( M \)-th \( MN \)-decimated sequences.

For example, we consider the \((8, 4)\) PSRGS for the MSRG sequence \( S_{\text{MSRG}}(x^{16} + x^8 + x^6 + x^1 + 1) \) shown in Fig.3a. Note that by the conversion property it is equivalent to the SSRG sequence \( S_{\text{SSRG}}(x^{16} + x^8 + x^6 + x^1 + 1) \) shown in Fig.3b. The SRG shown in Fig.3b is the one employed for scrambling in the SDH systems. Using the factoring and the decimation properties, we can easily find that the minimal MSRG expressions for the 32-decimated sequences \( V_{ij}, i = 0, 1, \ldots, 31 \), are

\[
V_0 = S_{\text{MSRG}}(x^8 + x + 1) \quad V_1 = S_{\text{MSRG}}(x^8 + x^2 + 1) \quad V_2 = S_{\text{MSRG}}(x^8 + x^3 + 1) \quad V_3 = S_{\text{MSRG}}(x^8 + x^5 + 1)
\]

and so on. We now apply the interleaving property with \( n = 8 \). Then, we finally obtain the following four \((8, 4)\) PSRG sequences:

\[
T_0 = S_{\text{MSRG}}(x^{16} + x^8 + x^6 + x^1 + 1) \quad T_1 = S_{\text{MSRG}}(x^{16} + x^8 + x^6 + x^1 + 1) \quad T_2 = S_{\text{MSRG}}(x^{16} + x^8 + x^6 + x^1 + 1) \quad T_3 = S_{\text{MSRG}}(x^{16} + x^8 + x^6 + x^1 + 1)
\]
\[ T_1 = S_{MSRG}(x) = x^8 + x^3 + x + 1, \]
\[ T_2 = S_{MSRG}(x) = x^8 + x^3 + x + 1, \]
\[ T_3 = S_{MSRG}(x) = x^8 + x^3 + x + 1. \]

We now consider how to realize PSRGs. We specifically consider \((M, N)\) PSRGs for the sequences whose generating polynomials are irreducible and whose periods are relatively prime to \(M\), which is true in most practical cases. We denote by \(S_{MSRG}(G(x), D_i(x))\) and \(S_{MSRG}(G(x), E_i(x))\) the minimal MSRG expressions for the \(i\)th \((M, N)\)-th sequence \(V_0\) and the \(i\)th parallel sequence \(T_0\) respectively.

We introduce the sequences \(W_i\) and \(\tilde{W}_i\), \(i = 0, 1, \ldots, M-1\), defined by
\[ W_i = S_{MSRG}(\tilde{G}(x), D_i(x)), \]
\[ \tilde{W}_i = \sum_{j=0}^{M-1} a_{M-1-i-j} W_j, \]
where \(D_i(x)\) are the \(i\)th state polynomial of the minimal MSRG for the \(i\)th parallel sequence \(T_0\) with \(\tilde{G}(x) = \sum_{j=0}^{M-1} a_j x^j\). The following four propositions show how the PSRGs can be realized based on the minimal SSRS or the minimal MSRG for the \(i\)th parallel sequence \(T_0\).

**Proposition 7A (Parallel Sequence Decomposition).** Let \(a_i, i = 0, 1, \ldots, N-1\), \(j = 0, 1, \ldots, L-1\), be such that \(R[\tilde{G}(x), x^{N+i}] = \sum_{j=0}^{M-1} a_j x^j\), where \(w\) is the smallest integer that satisfies \(w N = 1 \mod m\) (the period of the given sequence) and \(R[\tilde{G}(x), x^{N+i}]\) is the remainder polynomial of \(x^{N+i}\) divided by \(\tilde{G}(x)\). Then,
\[ T_i = \sum_{j=0}^{M-1} a_j \tilde{W}_{j+i}, i = 0, 1, \ldots, M-1. \]

**Proposition 7B (Parallel Sequence Decomposition).** Let \(b_i, i = 0, 1, \ldots, N-1\), \(j = 0, 1, \ldots, L-1\), be such that \(Q[\tilde{G}(x), x^{N+i}] = \sum_{j=0}^{M-1} b_j x^j\). Then,
\[ T_i = \sum_{j=0}^{M-1} b_j \tilde{W}_{j+i}, i = 0, 1, \ldots, M-1. \]

**Proposition 8A (SSRS-based Realization).** For the minimal SSRS for the \(i\)th parallel sequence \(T_0\), \(W_i = \{ d_{M-1-i-j} \}, i = 0, 1, \ldots, M-L-1\).

**Proposition 8B (MSRG-based Realization).** For the minimal MSRG for the \(i\)th parallel sequence \(T_0\), \(\tilde{W}_i = \{ d_{M-1-i-j} \}, i = 0, 1, \ldots, M-L-1\).

Propositions 7A and 7B imply that each parallel sequence \(T_i, i = 0, 1, \ldots, N-1\), can be decomposed into a sum of the \(L\) sequences \(W_{M-1} = 0, 1, \ldots, L-1\), or the \(L\) sequences \(W_{M-1} = 0, 1, \ldots, L-1\). Proposotions 8A and 8B show how to obtain the sequences \(W_i\) and \(\tilde{W}_i\). Proposition 8A means that the sequence \(W_j\) is identical to the shift register output sequence \(\{ d_{M-1-i-j} \}\) of the minimal SSRS for the \(i\)th parallel sequence \(T_0\); and Proposition 8B means that the sequence \(\tilde{W}_i\) is identical to the shift register output sequence \(\{ d_{M-1-i-j} \}\) of the minimal MSRG for the \(i\)th parallel sequence \(T_0\).

Therefore, these four propositions enable us to realize PSRGs based on the minimal SSRS or the minimal MSRG for the \(i\)th parallel sequence \(T_0\).

For example, we consider the PSRGs generating the parallel sequences in \(3\), or equivalently, the \((8, 4)\) PSRGs for the MSRG sequence \(S_{MSRG}(x, 7, 2, 8, 8, 8, 8, 8, 8)\), whose period 127 is relatively prime to \(8\times 4\) and the generating polynomial \(x^8 + x + 1\) is irreducible. First, by Proposition 7A with \(m = 4\), we have the following decomposed expressions of the parallel sequences:
\[ T_0 = W_0, \]
\[ T_1 = W_0 + W_4 + W_8, \]
\[ T_2 = W_0 + W_4, \]
\[ T_3 = W_0 + W_4 + W_8. \]

Then by Proposition 8A, we can identify each \(W_i\) to be the shift register output sequence \(\{ d_{M-1-i-j} \}\) of the minimal SSRS, which can be obtained by \((5a)\) and Proposition 7B and Proposition 8B the realization is as shown in Fig. 4a. For an MSRG-based realization of the PSRG, we obtain, by \((5a)\) and Propositions 7B and 8B, the realization in Fig. 4b in a similar manner.

**IV. Applications to Parallel Scrambling for SDH Systems**

In this section, we consider parallel scramblers applicable to the SDH transmission systems employing the properties of PSRGs we have discussed so far.

In the SDH system, \(N\) of AUO (administrative unit group) signals are byte-interleaved in the unit of eight bits to form a STM-N payload, and SOH (section overhead) data are added to it to complete an STM-N signal. The frame format for this is shown in Fig. 5. The STM-N signal is scrambled, and then transmitted. The first 9N bytes of the frame (the shaded bytes in Fig. 5) are excluded from the scrambling. In the receiver, the reverse operation of the transmitter is processed. The overall processing is depicted in Fig. 6. The scrambler and descrambler are supposed to have the characteristic polynomial \(x^2 + x + 1\) and to be reset to the state \(11111111\) at the beginning of each frame. This corresponds to the SSRS with \(C(x) = x^2 + x + 1\) and \(D(x) = x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1\), which is shown in Fig. 3b. Since the first 9N bytes of the STM-N signal is excluded from the scrambling process, the scrambler and descrambler SSRSs resume the initial state \(D(x)\) at the \((9N+1)\)th byte of every frame.

The SSRSs we employ for the scrambler and descrambler of the SDH system operate at the speed of the STM-N signal rate, which is 155.520 Mbps for \(N = 1\), 622.080 Mbps for \(N = 4\), and 2.48832 Mbps for \(N = 16\). If we employ PSRGs instead of SSRSs for the cases \(N = 4\) or 16, then the operating speed could drop from the STM-N rate to the STM-1 rate. This implies that the 622.080 Mbps or 2.48832 Mbps rate scrambling operation could be done at the 155.520 Mbps rate, which accompanies a considerable amount of cost saving. We call the PSRG-based implementation of scrambling the parallel scrambling. Especially, we call the parallel scrambling for use in the multibit-interleaved multiplexing environment the multibit-interleaved parallel scrambling. As opposed to this, the original SSRS-based scrambling is called the serial scrambling.

The SDH system, when employing the parallel scrambling, is rearranged as shown in Fig. 7. We observe from the figure that parallel scrambling is now performed prior to byte-interleaved multiplexer (or BIM). The SOH insertion process should be modified accordingly. For the parallel scrambling we adopt an \((8, N)\) PSRG since byte-interleaving is an 8-bit based operation. Note that what we should achieve in employing the parallel scrambling is to keep the transmission signal unchanged.
In the case of STM-4 signals, we need an (8,4) PSRG for parallel scrambling. This is already considered in the previous section. Therefore the four parallel sequences \( T_0 \) through \( T_3 \) for use in Fig. 7 are those either in Fig. 4a or in Fig. 4b. In the case of STM-16 signals, we can derive the (8,16) PSRG configurations shown in Fig. 8 in a similar manner for use in parallel scrambling.

V. Conclusion

In this paper, we have developed a theory on parallel shift register generators that makes the parallel scrambling technique applicable to multibit-interleaved multiplexing environments. The multibit-interleaved parallel scrambling thus obtained is a generalization of the existing parallel scrambling. In developing the theory, the concepts of SSRG, MMSRG and PSRG played the main role, so we investigated several properties of them.

In order to consider the \( M \)-bit interleaved multiplexing environment we introduced the concept of \((M, N)\) PSRG, with \( N \) indicating the number of parallel sequences. We found that in the case when the original generating polynomials are irreducible, which is true in most practical cases, an \((M, N)\) PSRG can be realized based on the minimal MSRG or SSRG for the 0th parallel sequence. The resulting \((M, N)\) PSRG enables multibit-interleaved parallel scrambling, which is a generalization of the existing (single bit-interleaved) parallel scrambling. Note that the existing parallel scrambling technique is a special example using (1, N) PSRGs.

We finally demonstrated how the developed theory could be applied for scrambling in the SDH systems, in which byte-interleaved multiplexing is employed. Setting \( M = 8 \) to reflect the byte-interleaving, and setting \( N = 4 \) to reflect that the STM-4 consists of four base-rate signals, we could obtain an (8,4) PSRG which generates four parallel sequences for use in the corresponding parallel scrambler and descrambler. We repeated the demonstration setting \( N = 16 \) for the STM-16 to obtain an (8,16) PSRG implementation.

The demonstrated (8,4) PSRGs and (8,16) PSRGs can be directly used for parallel scrambling of the STM-4 and STM-16 signals in the practical SDH-based waveform transmission systems. In both cases the scrambling can now be performed at the base rate, i.e., 155.520 Mbps instead of the transmission rates 622.080 Mbps and 2.488320 Gbps. This implies a significant amount of cost reduction since MOS technology could be still usable for implementation of the parallel scrambling.

REFERENCES


Fig. 1. Shift register sequence generators. (a) SSRG, (b) MMSRG.

Fig. 3. The SRGs employed in the SDH systems. (a) MMSRG configuration, (b) SSRG configuration.
Fig. 4. An example of (8,4) PSRGs for the sequence generated in Fig. 3. 
(a) SSRG configuration, (b) MSRG configuration.

Fig. 5. Frame format for the STM-N signal.

Fig. 6. Block diagram of the SDH systems employing byte-parallel scrambler. (a) Transmitter, (b) receiver.
(a) Transmitter, (b) receiver.

Fig. 7. Block diagram of the SDH systems.

Fig. 8. An example of (8,16) PSRGs for the sequence generated in Fig. 3. 
(a) SSRG configuration, (b) MSRG configuration.