

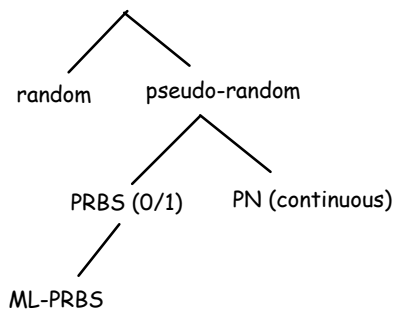
PN Sequences and Scramblers

Random and Pseudo-Random Signals

A random signal is one whose value cannot be predicted. An example is the thermal noise generated by a resistor or transistor. Some statistics of the noise such as the power and spectrum may be known, but we can't predict the future voltage of the waveform.

It is sometimes useful to generate waveforms that have the same statistics as a truly random signal but whose values *are* predictable. These types of signals are called “pseudo-random” signals. If the pseudo-random signal is noise-like it's called a pseudo-noise (PN) signal, and if it's two-valued (0,1) it's called a pseudo-random bit sequence (PRBS).

So we have the following taxonomy of random signals:



PN and PRBS signals have many important applications in communications systems. In this chapter we will study the properties of a type of PRBS called a maximal-length (ML) sequence, learn how to generate these sequences and look at one of their applications – “scrambling.” Other applications include spread-spectrum systems and the generation of test signals.

Properties of a ML PRBS

ML PRBS sequences, sometimes called m-sequences, have a number of useful properties including:

- a long period: the sequence is called maximum-length because the sequence has a period of (i.e. repeats after) $2^m - 1$ bits where m is the number of bits of state in the generator. This is one less

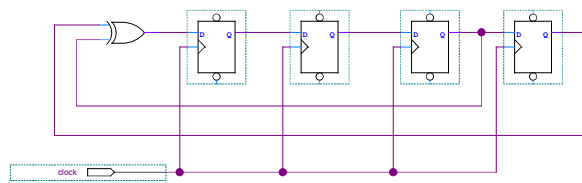
than the maximum number of states of an m -bit counter.

- approximately equal number of 1's and 0's: there are 2^{m-1} ones and $2^{m-1} - 1$ zeros.
- distribution of run lengths: one-half of the runs¹ have length 1, one-quarter have length 2, etc. (except that there is one run of length m ones and one of length $m-1$ zeros)
- the generator runs through every possible set of states except all-zero,
- adding any (circular) shift of the sequence to itself is also an m-sequence

Exercise 1: How many bits are there in an m-sequence for $m = 6$? How many are 1's? How many are 0's?

Generating a ML PRBS

A ML PRBS can be implemented using a shift register whose input is the modulo-2 sum of other taps.



Exercise 2: If the initial value of each flip-flop is 1, what are the values of the next 4 bits output by the right-most flip-flop?

This is known as a linear-feedback shift register (LFSR) generator. There are published tables showing the LFSR tap connections that result in a ML PRBS generator.

If the contents of the shift register ever become all zero then all future values will be zero. This is why the generator has only $2^m - 1$ states – the state corresponding to all zeros is not allowed.

Exercise 3: How many flip-flops would be required to generate a ML PRBS of period 8191? How many ones would the sequence have? What is the longest sequence of 0's?

¹A run is a sequence of bits with the same value.

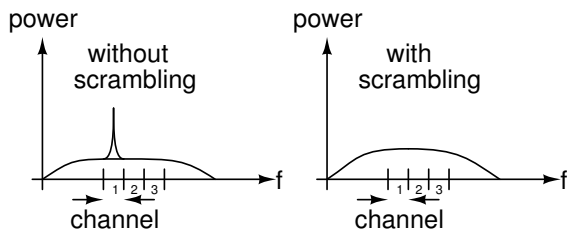
Scrambling

Much real-world data contains repetitive (periodic) components. Examples include padding sequences transmitted when there is no data to be sent, digitized waveforms with periodic components (e.g. scan lines, or video frames), or repeated values (e.g. zeros) in a file being transmitted.

Two possible problems are introduced by these patterns in the data.

The most serious problem is that periodic components of a signal generate narrow-band (discrete) spectral components that have larger than average power. These discrete frequency components can cause interference (called “electro-magnetic interference”, EMI) to wireless devices using the frequency that these components fall on.

The diagram below shows an example. The periodic component results in a discrete spectral component that would cause interference to a user of channel 1. Scrambling distributes that power and reduces the peak power spectral density of the interference. Although the other channels see more interference power, they are all (hopefully) still usable.



Prior to being marketed, all electronic devices must be tested to ensure such interference is below government regulatory limits. A device that fails such tests cannot be sold.

Another possible issue is that long sequences of certain values in random data may result in a signal that may not have enough transitions to allow for clock recovery.

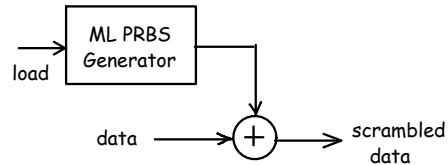
To solve these problems most data communication standards specify a “scrambling” algorithm that must be used at the transmitter to remove periodicities and long constant sequences in the data. The receiver reverses this process to recover the original data. Two common types of scramblers are described below.

However, it is important to understand that a scrambling is *not* encryption and does not provide secrecy.

Exercise 4: Why not?

Frame-Synchronous Scramblers

The simplest type of scrambler consists of a ML PRBS generator whose output is exclusive-OR’ed with the data. These types of scramblers are called “additive” scramblers because the PN sequence is added, modulo-2, to the data (i.e. it is exclusive-or’ed with the data).



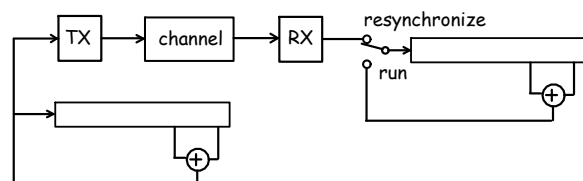
Since the scrambling sequence needs to be the same at the transmitter and receiver, this type of scrambler is only practical for systems that have a frame structure that can be used to synchronize the sequences. The state of the ML PRBS generator can be set to a specific value at the start of each frame. This value can be either a fixed value for every frame or it can be an arbitrary (typically pseudo-random) value transmitted in the frame’s preamble or header.

This type of scrambler is typically used on communication systems where each frame must be processed independently of others (e.g. WiFi).

PRBS Test Sequences

We can test a communication system by transmitting a PRBS sequence over the channel and comparing the received sequence to a locally-generated copy. Since the hardware to generate a very long ML-PRBS is very simple, it is practical to use long sequences for testing.

One problem that arises is how to synchronize the transmitter and a remote receiver. This can be done by loading the receiver PRBS generator’s shift register with any m consecutive received bits. As long as there were no errors in these m bits then from that point on the transmit and receive generators will generate the same sequences:



If the receiver ever becomes un-synchronized with the transmitter the error rate will become very high.

When this is detected at the receiver the local PRBS generator can resynchronize as above.

Exercise 5: In the diagram above, what two signals would the receiver compare to detect errors?

Walsh-Hadamard Sequences

A Hadamard matrix is a square matrix with entries of ± 1 whose rows are mutually orthogonal. This makes the rows useful as spreading codes and they are used in WCDMA downlink (forward) channels to multiplex various synchronization, control and data streams (called “channels”) onto the same carriers.

An easy way to construct Hadamard matrix of order $n = 2^k$ is by replicating a Hadamard matrix of 2^{k-1} in the following structure:

$$\begin{bmatrix} H & H \\ H & -H \end{bmatrix}$$

starting with $H_1 = [1]$.

Exercise 6: Derive H_2 and H_4 . Show that the first two rows and last two columns of each matrix are orthogonal.

This construction technique includes a replicated version of the lower-rate code in each higher-rate code. This allows the creation of a family of spreading codes with different lengths that are orthogonal when transmitted at different rates. In WCDMA this is called OVVSF (Orthogonal Variable Spreading Factor) codes. For example, a high-rate stream could use the spreading code H_1 (no spreading) while a lower-rate stream could use one of the codes from H_4 . These two streams would be orthogonal and could be separated at the receiver.

Exercise 7: Show this.

Although the spreading sequences obtained from Hadamard matrices are orthogonal to each other, they do not have the minimum-autocorrelation properties of m-sequences. Thus these are useful for multiplexing but not for time synchronization or for situations where the spreading codes might be offset in time (e.g. for separating different users on the uplink).

Hadamard matrices have other useful applications. For example, the rows of a Hadamard matrix can also be used as the codewords of an error-correcting code and the Walsh transform uses the rows of a Hadamard matrix as the orthogonal basis functions for the Walsh transform.