PSEUDO-RANDOM NOISE CODES

A PN code used for DS-spreading exists of NDS units called chips; these chips can have two values: -1/1 (polar) or 0/1. As we combine every data symbol with a complete PN code, the DS processing gain is equal to the code-length. To be usable for direct-sequence spreading, a PN code must meet the following constraints:

The sequences must be building from 2-leveled numbers.

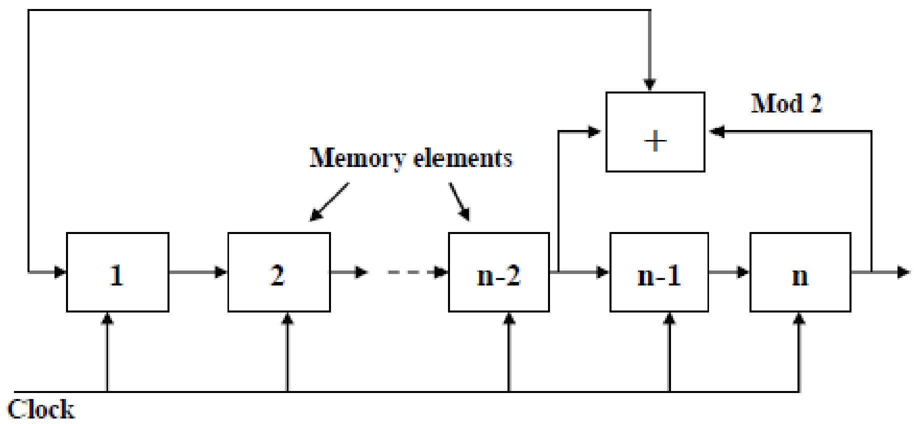
- The codes must have a sharp (1-chip wide) autocorrelation peak to enable code synchronization.
- The codes must have a low cross-correlation value, the lower this cross-correlation, the more users we can allow in the system. This holds for both full-code correlation and partial-code correlation. The latter because in most situations there will not be a full-period correlation of two codes, it is more likely that codes will only correlate partially (due to random-access nature).

This last requirement stands for good spectral density properties (equally spreading the energy over the whole frequency-band). Codes that can be found in practical DS-systems are: Walsh-Hadamard codes, M-sequences, Gold codes and Kasami-codes. These code sets can be roughly divided into two classes: orthogonal codes and non-orthogonal codes. Walsh sequences fall in the first category, while the other group contains the so-called shift-register sequences. We first spell out some desired properties we want the spreading sequences to possess:

1. Sequence elements should behave like iid random variables, i.e., the sequence should be pseudorandom.
2. It should be easy to distinguish a spreading signal from a time-shifted version of it.
3. It should be easy to distinguish a spreading signal from other spreading signals, including time shifted versions of them, in the set.
4. It should be easy for the transmitter and the intended receiver to generate the spreading sequence.
5. It should be difficult for any unintended receiver to acquire and regenerate the spreading sequence.

We would like the spreading sequences to approximate random sequences so that we are actually spreading the spectrum of the data signal. This explains the first desired property. The second property is used for sequence acquisition and multipath. The third property is obviously needed for CDMA systems. The fourth property indicates the practical consideration in sequence design. A sequence is of no use no matter how well it behaves if an excessive amount of hardware is needed to generate it. The fifth property is important when transmission security is our main concern. Due to the restriction imposed by the fourth property above, spreading sequences are usually generated by feedback shift registers in practice since shift registers are easy to build. The spreading sequences generated by feedback shift registers are periodic and they are usually pseudo-random. We will not consider the fifth property on transmission security in this brief treatment. The second and third properties are our major concerns here, i.e., we focus on the distinguish ability of spreading signals.

m-sequence:



Maximal length pseudo random sequence generator

Several spreading codes are popular for use in practical spread spectrum systems. Some of these are Maximal Sequence (m-sequence) length codes, Gold codes, Kasami codes and Barker codes. In this section will be briefly discussed about the m-sequences. These are longest codes that can be generated by a shift register of a specific length, say, L. An L-stage shift register and a few EX-OR gates can be used to generate an m-sequence of length 2^L -1. Figure shows an m-sequence generator using n memory elements, such as flip-flops. If we keep on clocking such a sequence generator, the sequence will repeat, but after 2^L -1 bits. The number of 1-s in the complete sequence and the number of 0-s will differ by one. That is, if L = 8, there will be 128 one-s and 127 zero-s in one complete cycle of the sequence. Further, the auto-correlation of an m-sequence is -1 except for relative shifts of (0 ± 1) chips. This behavior of the auto correlation function is somewhat similar to that of thermal noise as the auto correlation shows the degree of correspondence between the code and its phase-shifted version. Hence, the m-sequences are also known as, pseudo-noise or PN sequences.

Gold sequence:

Another interesting property of an m-sequence is that, the sequence, when added (modulo-2) with a cyclically shifted version of itself, results in another shifted version of the original sequence. For moderate and large values of L, multiple sequences exist, which are of the same length. The cross correlation of all these codes are studied. All these properties of a PN sequence are useful in the design of a spread spectrum system. Sometimes, to indicate the occurrence of specific patterns of sequences, we define 'run' as a series of ones and zero-s, grouped consecutively. For example, consider a sequence 1011010. We say, the sequence of has three runs of single '0', two runs of single '1' and one run of two ones. In a maximum length sequence of length and 2^L -1, there are exactly 2^L-(p+2) runs of length 'p' for both of ones and zeros except that there is only one run containing L one-s and one containing (L-1) zero-s. There is no run of zero-s of length L or ones of length (L-1). That is, the number of runs of each length is a decreasing power of two as the run length increases.

If the period of an m-sequence is N chips, $N = (2^n - 1)$, where 'n' is the number of stages in the code generator. The autocorrelation function of an m-sequence is periodic in nature and it assumes only two values, viz. 1 and (-1/N) when the shift parameter (τ) is an integral multiple of chip duration.

Several properties of PN sequences are used in the design of DS systems. Some features of maximal length pseudo random periodic sequences (m-sequence or PN sequence) are noted below:

Over one period of the sequence, the number of '+1' differs from the number of '-1' by exactly one. Also the number of positive runs equals the number of negative runs. Half of the runs of bits in every period of the same sign (i.e. +1 or -1) are of length 1, one fourth of the runs of bits are of length 2, one eighth of the runs of bits are of length 3 and so on. The autocorrelation of a periodic sequence is two-valued.