This is the Title PhL 3.26.05

I had some probability notes in Scrambler, but they ended up instead as an FT appendix. I did not want the same prob notes in two or three different places. FT already had to deal with statistical pulse trains.

A few Basics of Probability and Statistics Applied to GF(2)

tail of existing:

The probability of *events* A and B both being true is denoted by P(A∩B), or P(A,B). This is known as the joint second-order probability density function (pdf). A related concept is P(A|B) meaning the conditional probability that A is true given that B is true. Here are the relations:

$$P(A,B,C) = P(A\cap B\cap C) = P(A)P(B)P(C)\ . \qquad (2.5.7)$$

Case 1: Sequence values are 0 or 1

The "event" of interest is that $a_n = 1$. The sequence $\{a_n\}$ has some mean value which we denote by μ. The following shorthand notation is useful:

$$p(a_n) \equiv P(a_n=1) = \langle a_n\rangle = \mu$$

$$p(a_n, a_m) \equiv P(a_n= 1, a_m= 1)\quad . \qquad (2.5.8)$$

We can now express various mean values in terms of these pdf's:

$$\langle a_n\rangle = 1 \bullet P(a_n=1)\ + 0 \bullet P(a_n\neq 1)\ = P(a_n=1) = p(a_n)\ = \mu \qquad (2.5.9a)$$

$$\langle a_n^2\rangle = 1^2 \bullet P(a_n=1)\ + 0^2 \bullet P(a_n\neq 1)\ = P(a_n=1) = p(a_n) = \mu \qquad (2.5.9b)$$

$$\langle a_m a_n\rangle = 1^2 \bullet P(a_m=1,a_n=1) +3\ \text{ zero terms} = P(a_m=1,a_n=1) = p(a_m, a_n)\ . \qquad (2.5.9c)$$

If m≠n, it is possible that a_m and a_n could be statistically independent. In this case, one would have:

$$\langle a_m a_n\rangle = p(a_m, a_n) = p(a_m)\, p(a_n) = \langle a_m\rangle\langle a_n\rangle = \mu^2 \qquad \text{// uncorrelated} \qquad (2.5.10)$$

For m=n, it is impossible that a_m and a_n be statistically independent, and one has:

$$\langle a_n a_n\rangle = p(a_n, a_n) = \langle a_n^2\rangle = p(a_n) = \mu \neq p(a_n)\, p(a_n) \qquad \text{// correlated} \qquad (2.5.11)$$

In other words, the "diagonal" second-order statistical quantity $p(a_n, a_n)$ is really the first-order quantity $p(a_n)$.

We can now write down a few related statistical quantities (we are doing GF(2) symbols here):

The moments for N = 0,1,2,3...:

$$m_0 = \langle a_n^0 \rangle = \langle 1 \rangle = 1 \qquad N = 0$$

$$m_N \equiv \langle a_n^N \rangle = 1^N \bullet P(a_n=1) + 0^N \bullet P(a_n=1) = p(a_n) = \mu \qquad N = 1,2,3.. \qquad (2.5.12)$$

The central moments for N = 1,2,3..:

$$\mu_N = \langle (a_n - \langle a_n \rangle)^N \rangle = \langle (a_n - \mu)^N \rangle = \langle \Sigma_{j=0}^N \binom{N}{j} (a_n)^{N-j} [-\mu]^j \rangle$$

$$= \Sigma_{j=0}^N \binom{N}{j} (-1)^j \mu^j \langle (a_n)^{N-j} \rangle = \Sigma_{j=0}^{N-1} \binom{N}{j} (-1)^j \mu^{j+1} + (-1)^N \mu^N \qquad (2.5.13)$$

The N=1,2 central moments

$$\mu_1 = \langle (a_n - \langle a_n \rangle)^1 \rangle = \langle a_n \rangle - \langle a_n \rangle = \mu - \mu = 0$$

$$\mu_2 = \langle (a_n - \langle a_n \rangle)^2 \rangle = \langle (a_n - \mu)^2 \rangle = \langle a_n^2 \rangle - 2\mu \langle a_n \rangle + \mu^2 = \langle a_n^2 \rangle - \mu^2 = \mu - \mu^2 = \mu(1-\mu)$$

$$= \sigma^2 = (\text{standard deviation})^2 = \text{variance} \qquad (2.5.14)$$

Thus, in the special case of symbols in GF(2), all moment and central moments are determined by μ. For some different set of symbol values, this might not be the case.

In general, a full characterization of a statistical sequence requires specification of the probability density functions of all orders. However, much useful information is contained in the first two orders, and this information is sufficient for many applications.

Fact 1: The first and second order statistics are completely determined by the autocorrelation function.

Proof: Assume that the autocorrelation sequence r_k is known. Then,

first order:

$$p(a_n) = \langle a_n \rangle = \langle a_n^2 \rangle = r_0 \qquad // \ (2.5.9a), (2.5.9b), (2.54)$$

second order:

$$p(a_n, a_n) = \langle a_n^2 \rangle = p(a_n) = r_0 \qquad // (2.5.9b), (2.54)$$

$$p(a_m, a_n) = \langle a_m a_n \rangle = r_{m-n} \qquad m \neq n \qquad // (2.5.4)$$

Corollary 1: Third and higher order statistics are not determined by the autocorrelation sequence. One needs more information to get these higher statistics.

Example: Consider the third-order density:

$$p(a_n, a_{n+k}, a_{n+k'}) = \langle a_n a_{n+k} a_{n+k'} \rangle$$

One could relate this to some kind of fancier 2-variable autocorrelation sequence defined this way,

$$r_{k,k'} \equiv (1/P) \sum_{n=1}^{P} a_n \, a_{n+k} \, a_{n+k'}$$

Fact 2: For a *statistically independent sequence*, all higher order statistics are determined by the first order statistics: ($p(a_m)$ is independent of m)

$$\langle a_m a_n \rangle = p(a_m, a_n) = p(a_m)\, p(a_n) = [p(a_m)]^2 = \mu^2 \qquad m \neq n$$

$$\langle a_m a_n a_k \rangle = p(a_m, a_n, a_k) = p(a_m)\, p(a_n)\, p(a_k) = [p(a_m)]^3 = \mu^3 \qquad m \neq n \neq k$$

etc.

Proof: This follows from the definition of "statistical independence" given above (= uncorrelated).
ok to here
Definition: A *white* sequence over GF(2) is one which is uncorrelated and has $p(a_n) = \mu = 1/2$.

For such a sequence, we have:

$$\langle a_n \rangle = p(a_n) = \mu = 1/2 = r_0$$

$$\langle a_m a_n \rangle = p(a_m, a_n) = p(a_m)\, p(a_n) = \mu^2 = (1/2)^2 = 1/4 = r_{m-n} \qquad m \neq n$$

$$\langle a_m a_n a_k \rangle = p(a_m, a_n, a_k) = p(a_m)\, p(a_n)\, p(a_k) = \mu^3 = (1/2)^3 = 1/8 \qquad m \neq n \neq k$$

etc. (2.5.15)

From (2.5.15) here is a plot of the autocorrelation sequence for a white sequence a_n defined over GF(2):

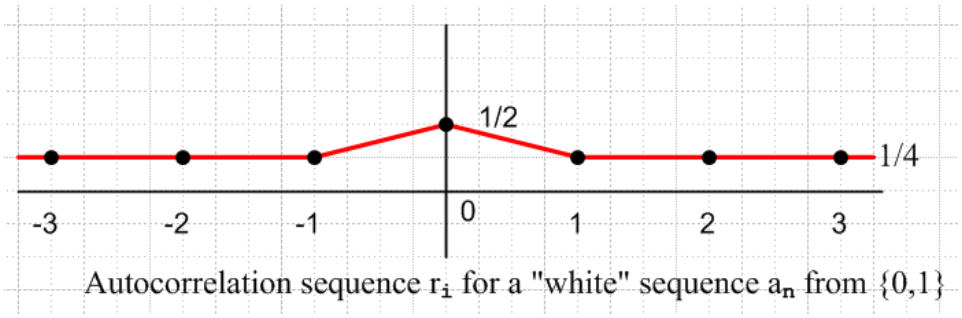


Figure 2.5.1: Autocorrelation function of a white sequence over GF(2) = {0,1}.

This fits the general template shown in Fig *** above where $\alpha = \mu^2 = 1/4$ and $\beta = \sigma^2+\mu^2 = \mu = 1/2$

Case 2: Sequence values are -1 or 1

It is sometimes convenient to think of the elements of the sequence a_n as belonging to the set {-1, +1} instead of to the official GF(2) set { 0,1 }. In this case, various statements made above must be modified. For example,

$P(a_n = 1) = p(a_n) \equiv p$

$P(a_n \neq 1) = P(a_n = -1) = 1 - p(a_n) = 1-p$

$$\langle a_n \rangle = 1 \bullet p(a_n) + (-1) \bullet [\, 1 - p(a_n)] = P(a_n=1) = [\, 2\, p(a_n) - 1\,] = (2p-1) = \mu \qquad (2.5.9a)'$$

$$\langle a_n^2 \rangle = 1^2 \bullet p(a_n) + (-1)^2 \bullet [\, 1 - p(a_n)] = 1 \qquad (2.5.9b)'$$

$$\langle a_m a_n \rangle = 1^2 \bullet P(a_m=1, a_n=1) + 1 \bullet (-1)\, P(a_m=1, a_n=-1) + (-1) \bullet 1 \bullet P(a_m=-1, a_n=1) + (-1)^2\, P(a_m=1, a_n=-1) \qquad (2.5.9c)'$$

If $m \neq n$, it is possible that a_m and a_n could be statistically independent. In this case, one would have:

$$\langle a_m a_n \rangle = p(a_m, a_n) = p(a_m)\, p(a_n) = \langle a_m \rangle \langle a_n \rangle = (2p-1)^2 = \mu^2 \qquad \text{// uncorrelated} \quad . \qquad (2.5.10)'$$

For m=n, it is impossible that a_m and a_n be statistically independent, and one has:

$$\langle a_n a_n \rangle = p(a_n, a_n) = \langle a_n^2 \rangle = 1 \neq p(a_n)\, p(a_n) = p^2 \quad . \qquad (2.5.11)'$$

<u>The moments for N = 0,1,2,3...:</u>

$$m_0 = \langle a_n^0 \rangle = \langle 1 \rangle = 1 \qquad N = 0$$

$$m_N = \langle a_n^N \rangle = 1^N \bullet p(a_n) + (-1)^N \bullet [\, 1 - p(a_n)] = p + (-1)^N (1-p) \qquad N = 1,2,3.. \qquad (2.5.12)'$$

$$= \begin{cases} 1 & N \text{ even} \\ (2p-1) & N \text{ odd} \end{cases}$$

<u>The central moments for N = 1,2,3..:</u>

$$\mu_N = \langle (a_n - \langle a_n \rangle)^N \rangle = \langle (a_n - p)^N \rangle = \langle \Sigma_{j=0}^N \binom{N}{j} (a_n)^{N-j} [-p]^j \rangle$$

$$= \Sigma_{j=0}^N \binom{N}{j} (-1)^j p^j \langle (a_n)^{N-j} \rangle = \Sigma_{j=0}^N \binom{N}{j} (-1)^j p^j\, m_{N-j} \qquad (2.5.13)'$$

<u>The N=1,2 central moments:</u>

$$\mu_1 = \langle (a_n - \langle a_n \rangle)^1 \rangle = \langle a_n \rangle - \langle a_n \rangle = 0$$

$$\mu_2 = \langle (a_n - \langle a_n \rangle)^2 \rangle = \langle a_n^2 \rangle - 2\langle a_n \rangle^2 + \langle a_n \rangle^2 = \langle a_n^2 \rangle - \langle a_n \rangle^2 = 1 - (2p-1)^2 = 4p(1-p) = 1-\mu^2$$

$$= \sigma^2 = (\text{standard deviation})^2 = \text{variance} \qquad (2.5.14)'$$

Fact 1': The first and second order statistics are completely determined by the autocorrelation function.

Proof: Assume that the autocorrelation function r_k is known. Then,

first order:

$p(a_n) = \langle a_n \rangle = \langle a_n^2 \rangle = r_0$ // (2.5.9a), (2.5.9b), (2.54)

second order:

$p(a_n, a_n) = \langle a_n^2 \rangle = p(a_n) = r_0$ // (2.5.9b), (2.54)

$p(a_m, a_n) = \langle a_m a_n \rangle = r_{m-n}$ $m \neq n$ // (2.5.4)

For a *white sequence*, we have p = 1/2 so

$\langle a_n \rangle = (2p-1) = 0 = \mu$

$\langle a_n^2 \rangle = 1 = r_0$ // (2.5.4)

$\langle a_m a_n \rangle = p(a_m, a_n) = p(a_m)\, p(a_n) = \langle a_n \rangle \langle a_n \rangle = 0 = r_{m-n}$ $m \neq n$ // (2.5.4)

$\langle a_m a_n a_k \rangle = p(a_m, a_n, a_k) = p(a_m)\, p(a_n)\, p(a_k) = 0$ $m \neq n \neq k$

etc. (2.5.15)'

From (2.5.15)' here is a plot of the autocorrelation sequence for a white sequence a_n defined over {-1, +1} where we set p = 1/2 in the above equations:

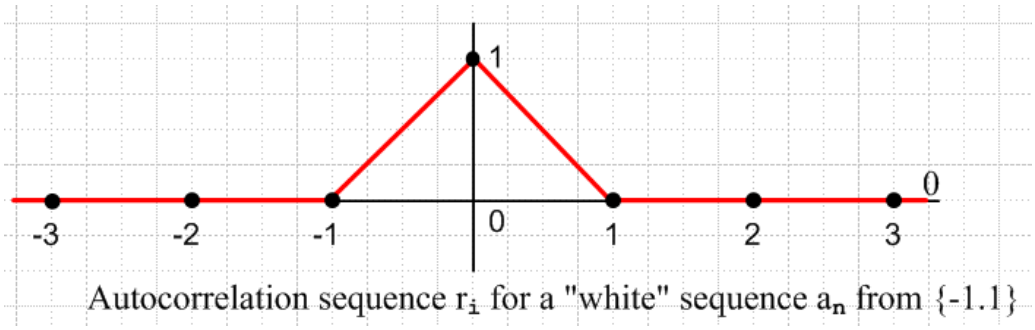


Figure 2.5.2: Autocorrelation function of a white sequence over {-1,+1}.

This fits the general template shown in Fig *** above where now $\alpha = \mu^2 = 0$ and $\beta = \sigma^2 + \mu^2 = 1$.