PROBABILITY OF FALSE POLYNOMIAL DIVISION SYNCHRONIZATION USING SHORTENED CYCLIC CODES

Anna Lynn Schauer
Mississippi State University*
(Now at Sandia National Laboratories,
Albuquerque, NM)

Frank M. Ingels
Mississippi State University

ABSTRACT

Shortened cyclic codes are not cyclic, but many cyclic shifts of various code words are still part of the shortened code set. This paper addresses the probability of false synchronization obtained through polynomial division of a serial shortened cyclic code stream in a "sliding" window correlator.

Key words: shortened cyclic codes, "sliding" window correlators, serial bit stream synchronization.

INTRODUCTION

Three basic operational modes have been considered for spacecraft uplink command communications. All of these modes have forty-eight bit command words.

The forty-eight bit command words include an eight bit spacecraft address, two fixed bits, thirty-one data bits and a seven bit parity check. Thus, each forty-eight bit command word would be comprised of forty-one bits plus a seven bit parity check. The seven bit parity check is formed by a polynomial division technique commonly referred to as Cyclic Rundancy Check, CRC, using the polynomial $g(x) = x^7 + x^6 + x2 + x^0$ derived from the CCSDS 201.0-B-1 Standard, paragraph 3.3.1.

This polynomial is a non-primitive generator polynomial for the 63,56 single error correcting (SEC), double error detecting (DED) Hamming code. It in turn is constructed from the generator polynomial for the 63,57 single error correcting code which is $p(x) = x^6 + x + 1$ by multiplication by $1 + x$ to produce the 63,56 cyclic code generator polynomial $g(x)$.

The command word is a shortened version of the 63,56 SEC, DED code. The shortening is accomplished in a virtual sense by assuming the first 15 bits of each word are zeroes. Thus, the forty-eight bit command words are actually a 48,41 SEC, DED code obtained by shortening the 63,56 SEC, DED cyclic code. (If no error correction is attempted, the code, which has minimum distance of four, can be used to detect up to

three errors.) Importantly, it must be realized that shortened cyclic codes are not themselves cyclic [1].

The command word acceptance technique would include an exact match for the eight bit spacecraft address code, an exact match of the two fixed bits, a command length of exactly 48 bits and an exact match of the error checking polynomial parity bits as rederived on the spacecraft by division of the first 41 bits by the generator polynomial g(x). It is the probability of false acceptance of the division process that this paper addresses.

Normally the cyclic shift of a code word will result in another valid code word. (A cyclic shift is easily envisioned by placing a code word in a shift register with the output line fed back to the input of the register. A shift of the register, thus, will cycle the output bit of the register to the input of the register. The MSB then becomes the LSB for each cyclic shift thereof.) However, for shortened versions of a cyclic code, this property does not hold for all code words in the shortened code set.

If a synchronization scheme incorporates the concept of division of a serial bit pattern in an X bit window by a generator polynomial and essentially interpreting a remainder of zero as a valid code word, then this amounts to a 'sliding window' correlator, i.e., as the serial bit stream 'slides' by the X bit window, the contents of the window are divided by g(x) on a bit-by-bit basis. False synchronization (false acceptance) occurs when the remainder term from the division is zero and segments of two adjacent words, *x* and *y*, are within the correlator window.

There are two mechanisms by which false synchronization may occur. First, a sync will occur if an apparent *i*th (or(n-i)th) cyclic shift of word *x* (or *y*) occurs, as a serial pattern is shifted through the window. Second, that portion of the bit stream within the correlator window may accidently "coincide" with a different valid code word other than a cyclic shifted version of the word under inspection. The probabilities of each of these occurrences have been derived separately [2]. In order to distinguish the two mechanisms by which false synchronization may occur, the subscripts "CS" (cyclic shift) and "CC" (coincidental correlation) are used. The two mechanisms represent mutually exclusive events, therefore the probability of false sync acquisition is the sum of two individual probabilities,

$$P(FSA) = P(FSA)_{CS} + P(FSA)_{CC}. \quad (1)$$

FALSE SYNCHRONIZATION DUE TO CYCLIC SHIFTS OF *X* AND *Y* (FULL-LENGTH CODES, *l* = 0), $P(FSA)_{CS}$ (*l* = SHORTENING PARAMETER)

After a valid word is located in the correlator window, a cyclic shift of *x* will occur on the first serial shift of the bit stream through the correlator window if the bit "shifted in" matches the bit "shifted out." Since bit values "1" and "0" are equally likely, the probability that a cyclic shift of *x* results on the first shift or the correlator window is

$$P(\text{False sync on shift no. } 1)_{CS} = 0.5.$$

False synchronization due to a cyclic shift of *x* occurs on the second shift if each of the two bits "shifted in" match each of the two bits "shifted out." Again, since code word bit values of "1" and "0" are equally likely, the probability that a cyclic shift of *x* occurs on the second shift of the correlator window is

$$P(\text{False sync on shift no. } 2)_{CS} = (\tfrac{1}{2})^2 = 0.25.$$

Once the correlator window contains more bits from word *y* than it does from word *x*, false synchronizations due to cyclic shifts are due to cyclic shifts of *y*. Thus, when full length codes are being considered, it is sufficient to calculate the first $\frac{n-1}{2}$ probabilities and use the property of symmetry to determine the remaining values.

In general, the probability of false synchronization due to cyclic shifts of *x* followed by *y* (full-length codes) is expressed as

$$\begin{aligned} &\text{For the first } \frac{n-1}{2} \text{ shifts: } P(\text{False sync on shift } i)_{CS} = (1/2)^i,\ i = 1 \text{ to } \frac{n-1}{2}\ ; \\ &\text{For the last } \frac{n-1}{2} \text{ shifts: } P(\text{False sync on shift } i)_{CS} = (1/2)^{n-i},\ i = \frac{n-1}{2} + 1 \text{ to } n-1. \end{aligned} \tag{2}$$

Once the individual shift probabilities $P(\text{False sync on shift i})_{CS}$ have been determined, the average probability of false sync, $P(FSA)_{CS}$, is calculated by

$$P(FSA)_{CS} = \frac{\sum_{i=1}^{n-l-1} P(\textit{False sync on shift } i)_{CS}}{n-l} \tag{3}$$

which yields an arithmetic average over *all* shifts.

Using Equation 3 and the symmetry of the probability P(False sync on shift i)$_{CS}$ from Equation 2, the probability of false sync acquisition for full-length codes is [2, pages 18-21]:

$$P(FSA)_{CS} = \frac{2 \times \left[\sum_{i=1}^{\frac{n-1}{2}} (1/2)^i \right]}{n} \quad (4)$$

FALSE SYNCHRONIZATION DUE TO CYCLIC SHIFTS OF *X* AND *Y*, (CODES SHORTENED BY *l* = 1), P(FSA)$_{CS}$

Once a full-length code is shortened, the cyclic relationship between all code words is lost. (There may still be many cyclic shift code words present but not all cyclic shifts will be present.) Recall that the full-length code word from which the shortened word (l = 1) is derived has a zero in the MSB position [1]:

$$\mathbf{x_0\ x_1 \ldots x_{n-3}\ x_{n-2}\ [0].}$$

The bracketed zero, [0], indicates the bit that is removed in order to shorten the code.

The full-length code words from which shortened words are derived will be used in the following discussion to demonstrate the conditions under which a cyclic shift of a valid (shortened) code word yields another valid code word.

Consider a full-length code word of the form $\mathbf{x_0\ x_1 \ldots x_{n-3}\ x_{n-2}\ 0}$. The first cyclic shift of this word has the form $\mathbf{0\ x_0\ x_1 \ldots x_{n-3}\ x_{n-2}}$. The original word, $\mathbf{x_0\ x_1 \ldots x_{n-3}\ x_{n-2}\ 0}$, may be shortened to form a word in a shortened code set. The new word of the full-length code formed by the first cyclic shift, $\mathbf{0\ x_0\ x_1 \ldots x_{n-3}\ x_{n-2}}$, may also be shortened if the last bit, $\mathbf{x_{n-2}}$, is a zero.

On the next cyclic shift, the word $\mathbf{x_{n-2}\ 0\ x_0\ x_1 \ldots x_{n-3}}$ is formed, and may be shortened if the last bit, x_{n-3}, is a zero. At each shift of a valid full-length code word, a valid code word in shortened set, l = 1, can be created if the last bit of the full-length word is a zero. Because the form of the original full-length code word is specified with a zero in the last bit position, cyclic shifts of the word must track the location of this zero as well. Thus, two bit positions may be monitored at each cyclic shift:

1) the last bit, and
2) the location of the zero (or zeroes, for $l > 1$).

As a bit stream comprised of shortened code words passes through a correlator window, successive "cyclic shifts" of a word *x* are defined as follows:

Original word in the correlator window: $\mathbf{x_0\ x_1\ x_2 \ldots x_{n-3}\ x_{n-2}}$

First shift.- $\mathbf{B_m\ x_0\ x_1 \ldots x_{n-4}\ x_{n-3}}$

Second shift: $\mathbf{b_n\ b_m\ x_0 \ldots x_{n-5}\ x_{n-4}}$

where $\mathbf{b_n}$ and $\mathbf{b_m}$ represent bits from the next word in the bit stream. At each shift *i*, a cyclic shift is said to occur and synchronization is flagged when

Rule 1) the n-*l* bits in the correlator window form the first n-*l* bits of the *i*th shift of the full-length word from which the original shortened code word is derived, and

Rule 2) the last *l* bits in the correlator window on shift i-*l* are zeroes.

These two stipulations relate to the two bit positions which may be monitored in cyclic shifts of full-length code words of the form $\mathbf{x_0\ x_1\ x_2 \ldots x_{n-l}\ 0_{n-l} \ldots 0_{n-1}}$.

With these guidelines in place, it is now possible to determine P(False sync on shift no. 1) when $l = 1$. On the first shift, the bit pattern in the correlator window is $\mathbf{b_m\ x_0\ x_1 \ldots x_{n-4}\ x_{n-3}}$. Synchronization will occur if the bit $\mathbf{b_m}$ is a zero (since the first cyclic shift of the full-length word from which the original shortened code word is derived is $\mathbf{0\ x_0\ x_1 \ldots x_{n-3}\ x_{n-2}}$) *and* bit $\mathbf{x_{n-2}}$ is a zero (since a full-length word must have a zero in the last location in order to be a valid shortened word when $l = 1$). Stated differently, synchronization will occur on the first shift if a zero is shifted in and a zero is shifted out. Thus, the corresponding probability of this event is

$$P(\text{False sync on shift no. 1})_{CS} = P(\text{Zero is shifted out}) \bullet P(\text{Zero is shifted in})$$

$$= (\tfrac{1}{2})\ (\tfrac{1}{2})$$

$$= 0.25.$$

Note that the events "zero is shifted out" and "zero is shifted in" are independent.

On the second shift through the correlator window, there are four combinations of "1"s and "0"s of bits to be shifted in: **00, 01, 10,** and **11**. By the definition of a cyclic shift, the bits which are "shifted in" are also "shifted out." However, since the word on which cyclic shifts are being performed is a full-length word of the form $\mathbf{x_0\ x_1\ x_2\ \ldots\ x_{n-3}\ x_{n-2}\ [0]}$, the bits which are shifted out are the last two bits, $\mathbf{x_{n-2}}$ and **0**. Of these combinations, **01** and **11** cannot yield synchronization due to cyclic shift since a "1" is in the **[0]** location. This preceding discussion provides an intuitive interpretation for Rule 1 (above).

In order to evaluate the remaining combinations **00** and **10**, Rule 2 must be considered. This is best illustrated by example. If **00** is shifted in on shift $i = 2$, the bit pattern in the window on each of the first two shifts is

$\mathbf{x_0\ x_1\ x_2\ \ldots\ x_{n-4}\ x_{n-3}\ x_{n-2}}$	*Original (shortened) word in correlator window*
$\mathbf{b_m = 0\ x_0\ x_1\ x_2\ \ldots\ x_{n-4}\ x_{n-3}}$	*First shift*
$\mathbf{b_n = 0\ b_m = 0\ x_0\ x_1\ x_2\ \ldots\ x_{n-4}}$	*Second shift.*

Recall that the full-length word from which this shortened word is derived has the form $\mathbf{x_0\ x_1\ x_2\ \ldots\ x_{n-4}\ x_{n-3}\ x_{n-2}\ x_{n-1}}$. If $\mathbf{b_n = 0\ b_m = 0}$ is cyclic shifted in, then $\mathbf{x_{n-2} = 0\ x_{n-1} = 0}$ must be shifted out. Therefore, for false synchronization to occur, the following three events must occur. First, $\mathbf{b_m}$ must be a zero (in accordance with Rule 1). Second, since $\mathbf{b_n = 0}$, $\mathbf{x_{n-2}}$ must also be a zero. Third, if a valid shortened word is to occur on shift $i = 2$, then the bit shifted out on $i = 1$ must be a zero (in accordance with Rule 2). Thus, $\mathbf{x_{n-3}}$ must be a zero.

Now consider the combination **10**. First, by Rule 1, if $\mathbf{b_n = 1\ b_m = 0}$ is cyclic shifted in, then bit $\mathbf{x_{n-2}}$ must be a one. Second, since $\mathbf{b_n = 1,\ x_{n-2}}$ must also be a one. Third, by Rule 2, $\mathbf{x_{n-3}}$ must be a zero.

The probability of false sync on the second shift is calculated as follows. First, only those combinations of bits shifted in which do not violate Rule 1 must be considered. For each combination that can yield false sync acquisition, the following independent probabilities must be considered:

1) The probability of shifting in bit pattern $\mathbf{b_n b_m}$ must be evaluated.

2) Since cyclic shifts are being considered, the bit $\mathbf{b_m}$ corresponds to the 0 that is removed when the full-length code is shortened, and bit $\mathbf{b_m}$ corresponds to the bit $\mathbf{x_{n-2}}$ which is shifted from the correlator window on shift $i = 1$. By definition of cyclic shifts, $\mathbf{x_{n-2} = b_n}$. The probability of this event must be considered.

3) Even though bit pattern $\mathbf{b_n b_m}$ may be shifted in on the first two shifts, and bit $\mathbf{x_{n-2} = b_n}$ may be shifted out on shift $i = 1$, there is still only a 50/50 chance that bit $\mathbf{x_{n-3}}$ is a 0, in accordance with Rule 2.

Thus, the probability of false sync acquisition on shift $i = 2$ becomes

$$
\begin{aligned}
P(\text{False sync on shift no. 2})_{CS} &= \mathbf{P(00 \text{ shifted in}) \cdot P(x_{n-2} = 0) \cdot P(x_{n-3} = 0)} \\
&+ \mathbf{P(10 \text{ shifted in}) \cdot P(x_{n-2} = 1) \cdot P(x_{n-3} = 0)} \\
&= (\tfrac{1}{2})(\tfrac{1}{2}) \cdot (\tfrac{1}{2}) \cdot (\tfrac{1}{2}) + (\tfrac{1}{2})(\tfrac{1}{2}) \cdot (\tfrac{1}{2}) \cdot (\tfrac{1}{2}) \\
&= 0.125.
\end{aligned}
$$

Probability derivation for the third shift proceeds in a similar manner. There are 2^3 possible bit combinations shifted in and out. Of these, the combinations **001, 011, 101,** and **111** cannot result in false synchronization due to cyclic shifts of the original word *x* since a "1" is found in the deleted zero location of the full-length word from which the shortened word is derived. Each of the remaining combinations **000, 010, 100,** and **110** must be evaluated, and the same three independent probabilities must be considered on shift $i = 3$ as were considered on shift $i = 2$.

The probability of false sync on the third shift is

$$
\begin{aligned}
&P(\text{False sync on shift no. 2})_{CS} \\
&= \mathbf{P(000 \text{ shifted in}) \cdot P(x_{n-2} = 0\ x_{n-3} = 0) \cdot P(x_{n-4} = 0)} \\
&+ \mathbf{P(010 \text{ shifted in}) \cdot P(x_{n-2} = 0\ x_{n-3} = 1) \cdot P(x_{n-4} = 0)} \\
&+ \mathbf{P(100 \text{ shifted in}) \cdot P(x_{n-2} = 1\ x_{n-3} = 0) \cdot P(x_{n-4} = 0)} \\
&+ \mathbf{P(110 \text{ shifted in}) \cdot P(x_{n-2} = 1\ x_{n-3} = 1) \cdot P(x_{n-4} = 0)} \\
&= 4\,[(\tfrac{1}{2})\,(\tfrac{1}{2})\,(\tfrac{1}{2}) \cdot (\tfrac{1}{2})\,(\tfrac{1}{2}) \cdot (\tfrac{1}{2})] \\
&= 0.0625.
\end{aligned}
$$

If the bits within the correlator window are comprised evenly of portions from *x* and *y*, cyclic shifts of either word are equally possible. This special case, where cyclic shifts of *both x* and *y* may occur, is referred to as the *center probability*, CP. The probabilities P(False sync on shift $i)_{CS}$ are symmetric about the center probability.

In general, the probabilities of false sync due to cyclic shifts of code words shortened by $l = 1$ are as follows [2, pages 21-26 contain the full derivation]:

For the first int $\left(\frac{n-2}{2}\right)$ *shifts*:

$$P(\text{False sync on shift } i)_{CS} = 2^{i-1}(0.5)^{i+(i-1)+1}$$

$$= 2^{-(i+1)},\ i = l \text{ to int } \left(\frac{n-2}{2}\right);$$

For shift number int $\left(\frac{n-2}{2}\right) + 1$ (*Center Probability*):

$$P(\text{False sync on shift } i)_{CS} = 2^{i} \bullet (0.5)^{i+(i-1)+1}$$

$$= 2^{-i},\ i = \text{int}\left(\frac{n-2}{2}\right) + 1;$$

For the last int $\left(\frac{n-2}{2}\right)$ *shifts*:

$$P(\text{False sync on shift } i)_{CS} = 2^{n-i-2}(0.5)^{n-i-1+(n-i-2)+1}$$

$$= 2^{-n+i},\ i = \text{int}\left(\frac{n-2}{2}\right) + 2 \text{ to } n-2.^{*} \qquad (5)$$

*The operator *int* extracts the integer portion of the argument, i.e., *int*(4.7) = 4.

From Equation 5 (above) and Equation 3,

the probability of false sync acquisition may be written as

$$P(FSA)_{CS} = \frac{2\left[\sum_{i=1}^{\sigma} 2^{i-1}\,(0.25)^{i}\right] + 2^{\sigma+1}\,(0.25)^{\sigma+1}}{n-1} = \frac{2\left[\sum_{i=1}^{\sigma} 2^{-(i+1)}\right] + 2^{-i}}{n-1} \quad , \tag{6}$$

for the $l = 1$ shortened cyclic code using the symmetry property where σ = integer value of (n-2)/2.

FALSE SYNCHRONIZATION DUE TO CYCLIC SHIFTS OF *X* AND *Y*, (GENERAL CASE: CODES SHORTENED BY *l*), $(P(FSA)_{CS}$

Following the preceding discussion for codes shortened by $l = 1$, a general probability expression for codes shortened by l has been derived for each shift of the correlator window:

For the first l shifts:

$$P(\text{False sync on shift } i)_{CS} = (0.25)^{i},\ i = 1 \text{ to } l;$$

For the next $\text{int}\left(\frac{n-l-1}{2}\right) - l$ *shifts*:

$$P(\text{False sync on shift } i)_{CS} = 2^{-(i+l)},\ i = l+1 \text{ to } \text{int}\left(\frac{n-l-1}{2}\right);$$

IF $\left[\frac{n-l-1}{2} - \text{int}\left(\frac{n-l-1}{2}\right)\right] = 0.5$, THEN (*Center Probability*):

$$P(\text{False sync on shift } i)_{CS} = 2^{-(i+l-1)},\ i = \text{int}\left(\frac{n-l-1}{2}\right) + 1\ . \tag{7}$$

The property of symmetry is used to derive the remaining values for shift numbers greater than [(n-*l*-1)/2] + 1.

As in the previous case for $l = 1$, Equation 3 can be used to determine the average value for $P(FSA)_{CS}$. A computer algorithm was written for ease in performing the calculations for $P(FSA)_{CS}$.

FALSE SYNC ACQUISITION DUE TO COINCIDENTAL CORRELATION, $P(FSA)_{CC}$

Coincidental correlation occurs when a valid code word is formed from segments of two adjacent words on shift *i*, but this windowed code word is not the i^{th} cyclic shift of word *x*, or the $(n\text{-}l\text{-}i)^{th}$ shift of word *y*. In order to derive an expression for $P(FSA)_{CC}$, a shift-by-shift analysis of word *x* as it passes through the correlator window was performed.

Analogous to cyclic shifts, the average coincidental correlation false synchronization, $P(FSA)_{CC}$, is:

$$P(FSA)_{CC} = \frac{\sum_{i=1}^{n-l-1} P(\textit{False sync on shift } i)_{CC}}{n - l} \quad . \tag{8}$$

Performing a shift-by-shift analysis of a non-shortened word *x* as it passes through the correlator window reveals that individual shift probabilities are calculated from

$P(\text{False sync on shift } i)_{CC} =$
$P(\text{Valid code word}) \bullet P(\text{At least } d_{min}, \text{ differences or "errors" occur on shift } i).$ (9)

The probability term P(Valid code word) was derived for full-length and shortened codes. The probability term P(At least d_{min} "errors" occur on shift *i*) derivation is somewhat involved and refers to the possibility that a new different valid code word is accidently formed after *i* shifts. A conservative approximation for P(At least d_{min} "errors" occur on shift *i*) is presented for shortened codes, and an exact expression is given for full-length codes. The results of both terms are applied to the final expressions for $P(\text{False sync on shift } i)_{CC}$, and a computer algorithm for computing upper and lower bounds for $P(FSA)_{CC}$ was written.

Because the derivation of $P(FSA)_{CC}$ is somewhat involved, an outline of the procedure is given in Figure 1.

Derivation of P(FSA), A Bottom-up Approach

Step 1: Derivation of P(Valid code word)

Step 2: Derivation of P(At least d_{min} "errors" occur on shift i)

a) Compute $N_{\epsilon}(i; d_{min}, n, k)$

b) Compute probabilities associated with each bit pattern containing d_{min} or more "errors"

i) *For* $l = 0$, an exact expression for P(At least d_{min} errors occur on shift i) may be derived

ii) *For* $l > 0$, upper and lower bounds for P(At least d_{min} errors occur on shift i) may be derived

Step 3: Derivation of P(False sync on shift i)$_{CC}$

Step 4: Computation of P(FSA)$_{CC}$

Figure 1. Outline of $P(FSA)_{CC}$ Derivation

On the first shift of a full-length code word x through the correlator window, the bit pattern in the window will appear as a cyclic shift of *x*, or a shifted version of *x* in "error" by one bit in the first location*:

(First shift)

$\mathbf{X_{n-1}\ X_0\ X_1\ X_2 \cdots X_{n-3}\ X_{n-2}}$ (No "errors")

$\epsilon\ \mathbf{X_0\ X_1\ X_2 \cdots X_{n-3}\ X_{n-2}}$ ("Error" in first bit location)*

If a cyclic shift has not occurred, then assuming for the moment that the minimum distance of the code is $d_{min} = 3$, division of the word $\epsilon\ \mathbf{X_0\ X_1\ X_2 \cdots X_{n-3}\ X_{n-2}}$ by the generator polynomial g(X) will result in a non-zero remainder, and false synchronization due to coincidental correlation cannot occur.

On the second shift of the bit stream through the correlator window, the bits within the window will appear to be one of the following four cases:

(Second shift)

$\mathbf{X_{n-2}\ X_{n-1}\ X_0\ X_1\ X_2 \cdots X_{n-3}}$ (No "errors")

$\epsilon\ \mathbf{X_{n-1}\ X_0\ X_1\ X_2 \cdots X_{n-3}}$ ("Error" in first bit location)

$\mathbf{X_{n-2}\ \epsilon\ X_0\ X_1\ X_2 \cdots X_{n-3}}$ ("Error" in second bit location)

$\epsilon\ \epsilon\ \mathbf{X_0\ X_1\ X_2 \cdots X_{n-3}}$ ("Errors" in first bit locations)

*The word "error" as used here is unrelated to the channel bit error rate.

The first of the four cases represents the probability of false synchronization due to a cyclic shift of the word *x*, equal to 0.25. This coincides exactly with the probability of false sync on shift $i = 2$ found in the previous section. However, since $d_{min} = 3$, there are not enough accumulated "errors" (possible differences) to cause false synchronization due to coincidental correlation.

It is on the third shift of the bit stream through the correlator window that at least one case accumulates at least d_{min} "errors:"

(Third shift)

$\mathbf{x_{n-3}\ x_{n-2}\ x_{n-1}\ x_0\ x_1\ x_2 \ldots x_{n-4}}$	$\mathbf{x_{n-3} \in x_{n-1}\ x_0\ x_1\ x_2 \ldots x_{n-4}}$
$\mathbf{x_{n-3}\ x_{n-2} \in x_0\ x_1\ x_2 \ldots x_{n-4}}$	$\mathbf{x_{n-3} \in \in x_0\ x_1\ x_2 \ldots x_{n-4}}$
$\mathbf{\in x_{n-2}\ x_{n-1}\ x_0\ x_1\ x_2 \ldots x_{n-4}}$	$\mathbf{\in \in x_{n-1}\ x_0\ x_1\ x_2 \ldots x_{n-4}}$
$\mathbf{\in x_{n-2} \in x_0\ x_1\ x_2 \ldots x_{n-4}}$ ("Errors" in 1st and 3rd bit locations)	$\mathbf{\in \in \in x_0\ x_1\ x_2 \ldots x_{n-4}}$• ("Errors" in first three bit locations)

Again note that the first of the eight cases listed above will generate false synchronization due to a cyclic shift of the word *x*, corresponding to the 0.125 P(False sync on shift no. 1) found from Equation 2 in the previous section. The last case, where the word in the correlator window appears to be the third cyclic shift of Word *x* corrupted by "errors" in the first bit locations, may result in false synchronization. The probability that at least d_{min} "errors" occur on shift *i* must be "weighted" by the probability that a random set of n-l bits forms a valid code word, where $l = 0$ for full-length codes. For full-length codes, all patterns have equal probability, whereas for shortened codes the pattern probabilities differ.

DERIVING P(VALID CODE WORD)

In any full-length (n, k) code, the total number of possible combinations of n bits is 2^n, and the number of valid code words in the set is equal to 2^k. Therefore, the probability that any random set of n bits is a valid code word is

$$P(\textit{Valid code word}) = \frac{2^k}{2^n} = 2^{(k-n)} = \frac{1}{2^{(n-k)}} \quad . \tag{10a}$$

In a shortened (*n-1, k-1*) code, the same equation is derived:

$$P(Valid\ code\ word) = \frac{2^{k-1}}{2^{n-1}} = 2^{(k-n)} = \frac{1}{2^{(n-k)}} \quad . \tag{10b}$$

This expression may be substituted directly into equation 9.

DERIVING P(AT LEAST d_{min} "ERRORS" OCCUR ON SHIFT *i*)

At each of the first $int\left(\frac{n-l-1}{2}\right)$ shifts of word x through the correlator window, the pattern of bits in the correlator window at shift *i* will appear to be one of the following:

- the i^{th} cyclic shift of word *x*, or
- the i^{th} cyclic shift of word *x* corrupted by "errors" in one or more of the first *i* bit positions.

When at least d_{min} or more "errors" have accumulated in the i^{th} cyclic shift of word *x*, it is possible for the bit pattern to match a valid code word in the code set. For all shifts *i* such that $d_{min} \le i \le n\text{-}d_{min}\text{-}l$, there will be at least one possible pattern containing at least d_{min} "errors." Associated with each pattern containing at least d_{min} "errors" is a probability of occurrence; by summing the probabilities for each possible pattern containing at least d_{min} "errors" at each shift *i*, a value for P(At least d_{min} "errors" occur on shift *i*) can be derived. Thus, the probability P(At least d_{min} "errors" occur on shift *i*) is obtained in a two-step process:

1) The number, N_ϵ (i; d_{min}, n, k), of possible patterns with at least d_{min} "errors" must be computed for each shift *i*; and

2) For each shift *i*, the probabilities associated with all possible bit patterns with at least d_{min} "errors" must be summed together to obtain P(At least d_{min} "errors" occur on shift *i*).

We note that as *i* increases, virtually all the patterns have d_{min} or more "errors."

In general, the number of possible bit patterns with at least d_{min} "errors" in shift number i can be expressed as follows:

No. of ways in which d_{min} *or more "errors" can occur on shift* $i = N_\epsilon (i; d_{min}, n, k)$

$$= 0, \quad i < d_{min}$$

$$= \sum_{m=d_{min}}^{i} \binom{i}{m}, \quad d_{min} \le i \le \text{int}\left(\frac{n-1-l}{2}\right)$$

$$\textbf{IF} \quad \left(\frac{n-1-l}{2}\right) - \text{int}\left(\frac{n-1-l}{2}\right) = 0.5, \quad \textbf{THEN}$$

$$= \sum_{m=d_{min}}^{i} \binom{i}{m}, \quad i = \text{int}\left(\frac{n-1-l}{2}\right) + 1$$

$$= \sum_{m=i}^{n-d_{min}-l} \binom{n-m}{d_{min}}, \quad n-l-\text{int}\left(\frac{n-1-l}{2}\right) \le i \le n-d_{min}-l$$

$$= 0, \quad i > n-d_{min}-l \ . \tag{11}$$

Thus, the upper bound for the probability at least d_{min} "errors" occur on shift i is 1.0. A lower bound for shortened codes has been derived by assuming that each of N_ϵ (i; d_{min}, n, k) patterns have a minimum probability of occurrence. Thus, the general lower bound expression is (l = shortening parameter):

$$\begin{aligned} P(\text{At least } d_{min} \text{ "errors" occur on shift } i)_{LB} &= N_\epsilon (i; d_{min}, n, k)\,(0.25)^l && i = 1 \text{ to } l \\ &= N_\epsilon (i; d_{min}, n, k)\,(.25)^l\,(0.5)^{i-l} && i = l+1 \text{ to CP} \end{aligned} \tag{12}$$

Again, symmetry may be used to determine the values for the remaining shifts.

For full-length codes, it is possible to calculate exactly the probability of at least d_{min} "errors" occur on shift i. These probabilities for full-length codes are:

$$\begin{aligned} P(\text{At least } d_{min} \text{ "errors" occur on shift } i) &= N_\epsilon (i; d_{min}, n, k)\,(0.5)^{-i} && i = 1 \text{ to } \frac{n-1}{2} \\ &= N_\epsilon (i; d_{min}, n, k)\,(0.5)^{n-i} && i = \frac{n}{2} \text{ to } n \end{aligned} \tag{13}$$

COMPUTING P(FALSE SYNC ON SHIFT i)$_{CC}$

Expressions for P(Valid code word) and P(At least d_{min} errors occur on shift i) have been derived in the previous section. In summary, the probability of coincidental correlation on shift i is computed as the product of two probabilities, P(False Acceptance) and P(At least d_{min} errors occur on shift), and is equal to (l = shortening parameter):

$$\begin{aligned}
&\text{P(False sync on shift } i)_{CC(l=0)} \\
&\quad = \text{P(At least } d_{min} \text{ "errors" occur on shift } i) \bullet \text{P(False Acceptance)} \\
&\quad = N_\epsilon(i; d_{min}, n, k) \bullet \frac{1}{2^i} \bullet \frac{1}{2^{(n-k)}} \\
&\quad = N_\epsilon(i; d_{min}, n, k) \bullet \frac{1}{2^{(n-k+i)}} \; ;
\end{aligned} \tag{14a}$$

For $l > 0$:

$$\begin{aligned}
&\text{P(False sync on shift } i)_{CC,UB} \\
&\quad = \text{P(At least } d_{min} \text{ "errors" occur on shift } i) \bullet \text{P(False Acceptance)} \\
&\quad = 1.0 \bullet \frac{1}{2^{n-k}}
\end{aligned}$$

$$\begin{aligned}
&\text{P(False sync on shift } i)_{CC,LB} \\
&\quad = \text{P(False Acceptance)} \bullet \text{P(At least } d_{min} \text{ "errors" occur on shift } i) \\
&\quad = \left(\frac{1}{2^{n-k}}\right) \bullet (0.25)^l \bullet N_\epsilon(i; d_{\min}, n, k), \quad i \le l \\
&\quad = \left(\frac{1}{2^{n-k}}\right) \bullet \left(\frac{1}{2^i - l}\right) \bullet (0.25)^l \bullet N_\epsilon(i; d_{\min}, n, k), \quad i > l.
\end{aligned} \tag{14b}$$

and P(FSA)$_{CC}$ is the average value of P(False sync on shift i)$_{CC}$:

$$P(FSA)_{CC} = \frac{\sum_{i=1}^{n-l-1} P(\text{False sync on shift } i)_{CC}}{n - l} \; . \tag{15}$$

A computer algorithm was developed for computing exact values for this expression when $l = 0$, and upper and lower bounds when $l > 0$. Comparisons of exact values and the upper and lower bound approximations are given in Table 1 for two codes. The (14,10) code has been shortened from the (15,11) code, and the (30,25) code has been shortened from the (31,26) code. A simulated serial bit stream was used to calculate actual probabilities of false synchronization on shift i for various codes. Assuming all valid code

words are equally possible, shortened code words selected at random were simulated. The results in Table 2 were compiled using twenty sets of 1000 serially transmitted code words and averaging the results.

CONCLUSIONS

For full-length codes, where the probability of false sync acquisition may be calculated exactly, the theoretical and simulated results are virtually identical. The predicted value tends to be conservative, and this result may be predicted by examining the expression for $P(FSA)_{CC}$. The probability of $P(FSA)_{CC}$ is developed using the probability of false sync acquisition on any shift *i*. The P(False sync on shift *i*) is found to be the product of two probabilities, P(Valid code word) and P(At least d_{min} "errors" occur on shift *i*). The probability P(Valid code word) is an approximation to the more conservative (smaller) probability, P(Valid code word given the position of the accumulated "errors"). For example, no code word from the (7,4) code differs from any other word in the code set in three (and only three) consecutive locations. Thus, the third shift through the correlator window of a code word *x* from the (7,4) code set will not yield a coincidental match. Therefore, false synchronizations from this code set are a function of cyclic shifts only. The predicted value for P(FSA), however, will account for some coincidental correlation. The percent error in each is small: less than 4% of the predicted value in each of the three cases (1.17% for the (15,11) code; 1.35% for the (31,26) code; and 3.5% for the (63,57) code).

For shortened codes, where the actual probability of false sync acquisition lies between theoretical upper and lower bounds, the results again compare well; the simulated results lie between the theoretical bound for all but the (12,8) and (58,52) codes. For these codes, the error can be explained by examining the shift-by-shift probabilities of false sync acquisition, where the bulk of the error can be traced to the second and second-from-last shift probabilities. Whereas the predicted probability of false sync acquisition on these shifts is approximately 0.0625, the simulated value is approximately twice that, or 0.125. Simulations of (13,9) and (59,53) codes (where the code has been shortened by a lesser amount), and (11,7) and (57,51) codes (where the code has been shortened by a greater amount) yield simulated values which again lie between the predicted bounds. By examining the generator polynomial and the shortened code words, this discrepancy can be explained.

Table 1. Comparison of Exact and Upper and Lower Bound Values for P(False sync on AM i)$_{CC}$

Shift No.	(14,10) Code Exact Value	(14,10) Code Upper Bound	(14,10) Code Lower Bound	(30,25) Code Exact Value	(30,25) Code Upper Bound	(30,25) Code Lower Bound
1	0.0	0.0	0.0	0.0	0.0	0.0
2	0.0	0.0	0.0	0.0	0.0	0.0
3	0.011719	0.0625	0.003906	0.005859	0.031250	0.001953
4	0.025391	0.0625	0.009765	0.012695	0.031250	0.004883
5	0.037109	0.0625	0.015625	0.018555	0.031250	0.007813
6	0.045898	0.0625	0.020509	0.022949	0.031250	0.010254
7	0.052002	0.0625	0.024170	0.026001	0.031250	0.012085
8	0.045898	0.0625	0.020509	0.028015	0.031250	0.013367
9	0.037109	0.0625	0.015625	0.029297	0.031250	0.014221
10	0.025391	0.0625	0.009765	0.030090	0.031250	0.014771
11	0.011719	0.0625	0.003906	0.030571	0.031250	0.015114
12	0.0	0.0	0.0	0.030857	0.031250	0.015324
13	0.0	0.0	0.0	0.031025	0.031250	0.015450
14	0.0	0.0	0.0	0.031122	0.031250	0.015524
15	0.0	0.0	0.0	0.031178	0.031250	0.015567
16	0.0	0.0	0.0	0.031122	0.031250	0.015524
17	0.0	0.0	0.0	0.031025	0.031250	0.015450
18	0.0	0.0	0.0	0.030857	0.031250	0.015324
19	0.0	0.0	0.0	0.030571	0.031250	0.015114
20	0.0	0.0	0.0	0.030090	0.031250	0.014771
21	0.0	0.0	0.0	0.029297	0.031250	0.014221
22	0.0	0.0	0.0	0.028015	0.031250	0.013367
23	0.0	0.0	0.0	0.026001	0.031250	0.012085
24	0.0	0.0	0.0	0.022949	0.031250	0.010254
25	0.0	0.0	0.0	0.018555	0.031250	0.007813
26	0.0	0.0	0.0	0.012695	0.031250	0.004883
27	0.0	0.0	0.0	0.005859	0.031250	0.001953
28	0.0	0.0	0.0	0.0	0.0	0.0
29	0.0	0.0	0.0	0.0	0.0	0.0

Table 2. Average Probability of False Sync Acquisition Over All Possible Shifts

Full-Length Codes	Simulated Value	Predicted Value	
(15,11) Code	0.150233	0.152018	
(31,26) Code	0.083545	0.084684	
(63,57) Code	0.043075	0.046384	
Shortened Codes	**Upper Bound**	**Simulated Value**	**Lower Bound**
(10,6) Code	0.097751	0.091046	0.067039
(12,8) Code	0.093422	0.096597	0.006026
(21,16) Code	0.055536	0.054200	0.031959
(26,21) Code	0.050927	0.048117	0.026302
(28,23) Code	0.050219	0.048978	0.026925
(53,47) Code	0.026729	0.026109	0.012627
(58,52) Code	0.025806	0.029025	0.011918
(60,54) Code	0.025777	0.024082	0.013049
OMV (48,41) Code	0.020562	0.020252	0.013897

Each of these two code sets has a generator polynomial of the form $g(X) = 1 + X + X^{(n-k)}$. When the code sets are shortened by n-k + 1, the percentage of (shortened) code words which form a shifted version of the generator polynomial is approximately doubled. This may be shown empirically by successively shortening the full-length code sets and monitoring the location of cyclic shifts of the generator polynomial.

It should be noted that these results do not include any bit errors which might be incurred during transmission.

REFERENCES

1. Linn, Shu and Daniel J. Costello, *Error Control Coding Fundamentals and Applications* Prentiss-Hall, Inc., New Jersey, 1983.

2. Schauer, Anna L., *Analysis of a Proposed Orbital Maneuvering Vehicle (OMV) Synchronization Method*, Master's Thesis, Mississippi State University, May 1991.