SYNCHRONIZATION METHODS IN DIGITAL SYSTEMS

A Dissertation
submitted in partial fulfilment
of the requirements for the Degree
of
MASTER OF ENGINEERING
in
ELECTRONICS & COMMUNICATION ENGINEERING
(ADVANCED ELECTRONICS)

By

AKHILESH KUMAR AGRAWAL

DEPTT. OF ELECTRONICS & COMMUNICATION ENGINEERING
UNIVERSITY OF ROORKEE
ROORKEE
August, 1966

CERTIFICATE

Certified that the dissertation entitled "SYNCHRONISATION METHODS IN DIGITAL SYSTEMS" which is being submitted by Shri A. K. Agrawal in partial fulfilment for the award of the Degree of Master of Engineering in Advanced Electronics of the University of Roorkee is a record of the student's own work carried out by him under my supervision and guidance. The matter embodied in this dissertation has not been submitted for the award of any other Degree or Diploma.

This is further to certify that he has worked for a period of 7 months from 1.1.66 to 1.8.66 for preparing this dissertation for Master of Engineering at the University.

(N. N. BISWAS)
Professor
Electronics & Communication
Engineering Department
University of Roorkee
Roorkee

August 11, 1966.

ACKNOWLEDGEMENTS

I feel it my proud privilege to have worked under the noble and able guidance of Dr. N. K. Sharma, Professor, Deptt. of Electronics & Communication Engg., University of Roorkee, Roorkee, and fail to find words to express the deep sense of gratitude for suggesting the topic, constant encouragement and unending readiness in solving the intricate problems during the progress of the dissertation without which its completion would have been difficult. Once again I tender my sincere thanks to him.

I also wish to express my heart-felt thanks to Shri Harpreet Singh, Teacher-Trainee, for his valuable suggestions and unfailing help in many ways.

Agrawal

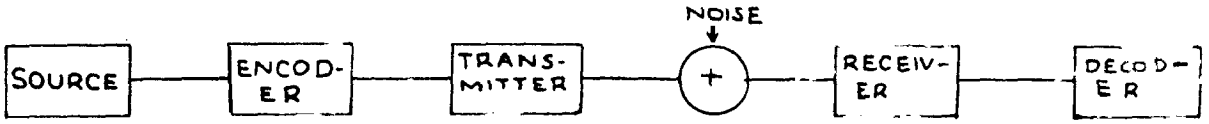
(A. K. AGRAWAL)

C O N T E N T S

*****

INTRODUCTION

1.1 In satellite and deep space communication, the source consists of the data from numerous experiments conducted during flight. The noise is primarily thermal in origin and is assumed to be stationary, white and gaussian.



CHANNEL MODEL

FIG.- 1-1

To transmit information over such a continuous, white, gaussian channel, two modes of operation are important. First, the transmission mode that the information must be conveyed with high reliability. Hence, successive blocks of data are encoded into sequences of binary digits (e.g., pulse or no pulse, represented by 1 or 0 respectively), called code words. The encoding is done to ensure reliability and to guard against symbol substitution caused by the noise. Second, the acquisition mode that the signal must be acquired at the receiver. The aspect of acquisition mode that is of concern here is to enable efficient decoding, which in turn necessitates a knowledge of the instants in time at which one code word ends and the succeeding word begins.

The problems presented by these two modes of operation have in general been handled separately i.e., codes have been found which are advantageous in the transmission mode in that their use insures a relatively low probability of error in the received data.

However, as observed, efficient decoding of these codes assumes the existence of the synchronizing information of the acquisition code, information which the codes themselves are ill equipped to provide. Sequences which are desirable as far as acquisition is concerned have also been determined.

1.2 There are various ways to achieve synchronization e.g., if synchronization is to be accomplished by continually sending a particular sequence and determining its phase at the receiver, the optimum sequence is that which has a minimum cross correlation with cyclic permutations of itself, viz., the pseudonoise (p-n) sequence. Such have found have autocorrelation functions which are small everywhere except at the inphase position. These sequences can be detected by (App.I) a matched filter at the receiver. The use of p-n sequences implies either a second channel to be used only for synchronization or if two way communication is available the same channel can at first transmit the Sync. sequence and then, upon notification from the receiver that Sync. has been obtained, begin transmitting data.

When the telemetry system consists of only one channel, a Sync. pattern can be inserted periodically or can be used to prefix each code word, thereby facilitating sync. without the use of an additional channel. For such applications the so called Barker (App. II) sequences whose aperiodic cross correlations are minimized are optimum. In the latter case the code must be such that the sync. pattern is not likely to occur in the data sequences, a condition not always easy to insure.

All of these methods, however decrease the capacity of the data channel by demanding some of the power that could presumably be used for data transmission. After sync. has been accomplished a simple counter is sufficient to retain it, and all additional sync. power is essentially wasted. While two way communication could limit this waste of power by switching off the sync. sequences as soon as the sync. has been obtained, the additional complexity needed for this ability may make it rather unattractive. Moreover, when these sequences are discontinued, there is no apparent way of monitoring the received signal to determine if sync. has been lost.

Hence a scheme using a p-n sequence as a sub-carrier to be phase modulated by the code word sequences. The received signal is then correlated (Appendix III) with a locally generated replica of the p-n sequence until correct sync. can be determined. By then multiplying (phase modulating) the received sequence by the p-n sequence, the latter is removed and all the transmitted power remains in the message. It is necessary that the product sequence retain the sync. properties of the p-n sequence, so the word symbol time is kept large compared to the p-n symbol time, or in other words several p-n symbols are necessary for each code symbol. Or the B.W. (Bandwidth) of the combined signal must be several times greater than that necessary to transmit the encoded data alone. This method, therefore, provides a means for obtaining sync. not at the cost of additional power, but rather of increased BW.

1.3 In the following pages, various methods of obtaining sync. are reviewed. In the last chapter various codes which are used for purposes of sync. operation are described, e.g., comma-free codes,

orthogonal and biorthogonal codes, etc. A new class of codes, called the self-synchronising codes, can be constructed from any of the former codes so that the max. absolute value of the correlation ρ between any code word and any sequence formed from the overlap of two code words is a minimum. Thus a large correlation is observed only in the sync. phase position. The obvious advantage of self-synchronising codes is that the amount and complexity of the equipment required is reduced. Also the additional power for sync. alarm is not needed. An algorithm for constructing these codes with the desired self sync. properties is presented and upper bounds on the value of ρ are thereby established.

oooooo

SYNCHRONIZATION IN PULSE MODULATION

2.1 Synchronization at the transmitting terminal :-

At the transmitting terminal it is essential that the marker and channel pulses occur in proper sequence at exactly the right times. Hence a master oscillator is used to control the overall operation, with a frequency so chosen that there is one cycle of oscillation for each pulse to be transmitted.

The control pulses might also be generated by a ring circuit driven by the master oscillator. The ring circuit constitutes a multistage device wherein each stage may be either in an "on" or an "off" condition with only one stage in the "on" condition at a time. For a 3 channel PAM system depicted in Fig. 2.1, the ring circuit could have 4 stages. At the output of each stage one pulse is produced every 4-cycles of the oscillating wave. Thus, in all 4-pulses are produced during each framing interval, which go to four paths at the output of the synchronizer. One path goes to the marker generator and the others to sampling circuits for the 3 channels.

2.2 Synchronization at the receiving terminal :-

There are two basic types of receiving synchronizers.

1. Start-stop synchronizer
2. Long time synchronizer.

2.21 Start stop synchronization[4]

This method is used in communication over high grade channels and involves transmitting some thing - usually a marker

pulse or marker space - in addition to the message bearing pulses to serve as a time mark within each frame interval, so that gates at the receiving terminal may be made to open and close at the proper times.

The following considerations limit the shape of the marker pulse.

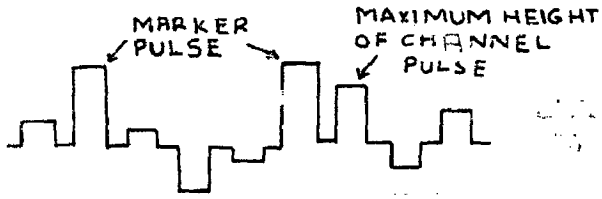
1. The marker pulse should be capable of being handled conveniently by the repeaters.

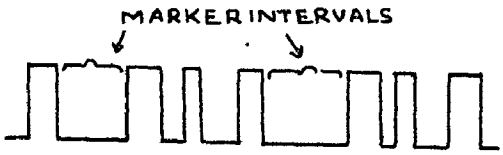
2. The marker pulse should not be of shorter duration than the channel pulses since this increases the BW.

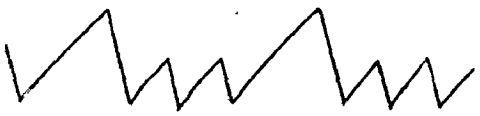
3. To simplify instrumentation it is advantageous to make the interval allotted to a marker pulse equal to that allotted to any other pulse.

In the Fig. 2.1 3 cases are shown for PAM, PDM, and PPM respectively. In all of the 3 cases the marker pulse (or space) can be separated easily by simple techniques. The marker pulses on separation are used to control the operation, of the sync. circuit at the receiving terminal e.g., in a 3 Ch. system there would be 3 RC circuits, all having different time constants.

During the time of occurrence of the marker, low impedance shunts are automatically connected across the capacitors to bring their voltages practically to ground potential, removed at the end, allowing the capacitors to charge through resistors connected to a


MARKER PULSE
MAXIMUM HEIGHT OF CHANNEL PULSE


MARKER INTERVALS



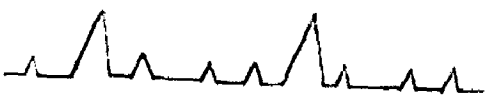
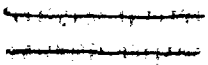


FIG. 2·1



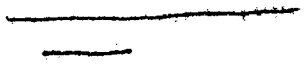


FIG. 2·2

positive d-c supply of relatively high voltage.

The time constant of the RC circuit is so chosen that the voltage across the capacitor reaches a preassigned value at the beginning of the gating interval of channel I. Each capacitor is connected to a circuit that generates a pulse as soon as the voltage across the capacitor reaches the above mentioned value. The circuits are so designed that the duration of each pulse is equal to the gating interval. The pulses generated are fed to the appropriate channel gates.

2.22 Long time synchronization

For a 3 channel PAM system with a frame rate of 8 KC/S the pulse rate is 32 KC/S. If such a pulse train is passed through a narrow band pass filter centered at 32 KC/S, the output of the filter will consist of a 32 KC/S sinusoidal component - shown in Fig. 2.2. This sinusoidal wave is used to control the timing operations in long time synchronization.

This component drives a 4-stage ring circuit. Successive stages of the ring circuit are switched to the "on" condition at the rate of one switching operation per cycle of the driving oscillation. The pulses from the 4-stages operate the respective gates for channels 1, 2, and 3 respectively.

Since there is nothing to distinguish one cycle from another, there is only one chance in 4 that the timing of the gates would be correct if nothing further were done. Hence to bring the

pulses from the ring circuit into proper time relationship with the channel pulses. First, an indicator is needed to determine whether or not the system is in sync. Second, during intervals when the system is not in sync, the time relationship between the ring circuit pulses and the incoming channel pulses must be changed automatically and progressively until the proper relationship is found. This action is termed hunting. The hunting circuit periodically causes the 4-stage ring to skip one step and thus establishes in succession the 4 possible relationships between the received pulses and those generated by the ring.

Indicator Operation :-

At the transmitting terminal the marker pulse is modulated by a 4-KC sinusoid (e.g. position modulated) in the same way that the channel pulses are modulated by the speech waves. Each voice input circuit is provided with a l-p filter which attenuates 4-KC, thereby insuring that the marker pulse is the only one that can ever be modulated at this rate.

When the system is in sync., each marker pulse passes through its gate and into the receiving channel equipment similar to that for the voice circuits. At the output of this particular channel equipment is a narrow b-p filter that freely passes 4-KC.

Under operating conditions, a 4-KC sinusoid appears at the output of the filter. When the system is out of sync., the filter output is substantially zero because channel pulses instead of marker pulses are passed by the marker gate. The 4-KC wave is rectified and

this rectified current controls a relay which turns on the "hunting" circuit whenever the system is out of sync. The circuit operates at a comparatively slow rate, say 10 times/sec. so that the relay will have time to function. On sync., the relay operates to turn off the hunting circuit.

To avoid the need of hunting, a low frequency equal to framing frequency or lower is obtained, by using a marker interval wider than the channel pulses, and by applying the received pulses to the input of a narrow b-p filter. The 8-KC component thus obtained is phased with respect to the pulses as indicated in the lower curve in fig. 2.2 and is caused to drive a pulse generator. This pulse generator produces pulses at the rate of 8,000 per sec. which operate gate generating circuits in a manner similar to that described for the R-C start stop system.

The low frequency used increases the timing errors, since a 1 degree error in 8-KC results in 4-degree error in 32-KC. It is used for small No. of channels since requirements for the b-p filter, phase correcting networks, and pulse-generating circuits are proportionately more stringent.

Sidebands appear around 8 or 32-KC when the pulses are position modulated. If the b-p filter does not cut sharply enough, a portion of these sidebands will pass through, and produce timing errors. To minimize this 1-f suppression networks are used in the channel transmitting equipment to prevent transmission of signal frequencies below a certain value.

2.3 Noise Considerations

1. Long time synchronization - The width of the band occupied by the interfering noise is equal to that of the sync. frequency filter which should and can be comparatively narrow. Or the channel noise is increased only a trivial amount by noise from the sync., circuit. In PPM, long time sync., has 3 db less noise than in the start stop system.

2. Start stop synchronization - Noise in start-stop sync., is more in PPM ~~XXX~~ It is because the edges of the received pulses do not rise in zero time but are somewhat sloping. This gives rise to "jitter in the marker and channel pulses.

xxxxx

SYNCHRONIZATION IN PCM

3.1 Information for synchronization[20]

Assume a PCM system (Fig. 3.1) with frame rate F, No. of channels (words per frame) n, and No. of bits M per word, including blank bits. Then the word rate is nF, and the bit rate is MnF. Let the airborne time-base oscillator have an instability of $\epsilon_t = \left|\frac{\Delta f}{f}\right|$ where f is the oscillator frequency and Δf the maximum possible change in the frequency. Assume the receiving time-base oscillator has an instability ϵ_r. Let us assume the worst case where the full instability of $\epsilon_t + \epsilon_r$ suddenly occurs, perhaps due to a sudden environmental change. Just before the sudden jump in frequency, let us assume the two oscillators have been in exact frequency and p sec synchronization, and that the maximum phase difference that can be tolerated at any time is 1/10 of the duration of a bit. Then the acquisition time t_a required for this phase difference of 1/10 MnF sec. to accumulate is

$$t_s = \frac{1}{10\,MnF(\epsilon_t + \epsilon_r)} \qquad \ldots (3.1)$$

This means that the sync. pulses must be sent at least at the rate

$$F_S = \frac{1}{t_s} = 10\,MnF(\epsilon_t + \epsilon_r) \qquad \ldots (3.2)$$

e.g. with MnF = 2.5×10^5 and $\epsilon_t + \epsilon_r = 10^{-5}$, this gives a sync. pulse rate of

$$F_p = 25 \text{ per sec.}$$

For shorter t_a, F_p must be increased

3.11 Information rate for the sync. maintenance mode

Think of the sync. pulse in terms of a PPM system with a very small full modulation capability consisting of a maximum time displacement of $\pm \frac{1}{10\ BnP}$ secs (a - priori uncertainty in pulse position). The error in pulse position due to random noise should be limited to some reasonable fraction of this, say $\pm \frac{1}{40\ BnP}$. Thus each pulse provides roughly two bits of information, so the information rate for the sync. maintenance mode is approximately

$$2D_o \text{ bits/sec.} \quad .... \quad (3.3)$$

3.12 Information rate for the acquisition mode :-

The maximum time displacement becomes $\pm \frac{t_s}{2} = \pm \frac{1}{20 M_n F(\epsilon_t + \epsilon_r)}$ (a priori uncertainty in pulse position), while the error in pulse position due to random noise remains at the former value of $\pm \frac{1}{40\ BnP}$. Thus each pulse now provides, roughly, $\log_2 \left(\frac{2}{\epsilon_t}\right)$ bits of information, and so the information rate for the acquisition mode is approximately

$$F_s \log_2 (2/\epsilon_t) \text{ bits/sec.} \quad .... (3.4)$$

or 450 bits/sec for the numerical example.

3.2 Effect of S/N ratio

At low S/N ratio the acquisition time will considerably exceed the t_o of (3.1) (due to the time required for the small information rate to accumulate enough information to determine acquisition phase). Also the position error in the individual sync. pulses can not be held to the value of $\pm \frac{1}{40\ BnP}$

previously used, and that the sync. pulses are not individually distinguishable from other received wave forms. Both of these conditions represent a decrease below the minimum sync-signal information rate which must be restored somehow. The only feasible way to do this in most systems is to sufficiently increase the sync. pulse rate. Then for the sync. maintenance mode of operation, the necessary information is recovered by a combination of gating to remove false pulses, and averaging to reduce random position errors.

3.3 Synchronization patterns

3.31 Bit synchronization

From (3.2) $P_0 = 1/t_0 = 10 \log (\epsilon_t + \epsilon_r)$

~~or P_0 is about 10 times the No. of bits/sec.~~

So the sync. at the bit rate can be obtained by correlation whenever 0-1 or 1-0 bit transitions occur with sufficient frequency ~~(10 x No. of bits/sec.)~~, at least once for each interval t_0, depending on the S/N ratio.

3.32 Word synchronization

A distinguishing pulse arrangement is sent every word or positive integer No. of words. Then y coders leave a blank bit space for sync. at the end of each word while they reset. This blank bit space amounts to 1/n of the entire information capacity of the PCM system (2 No bits/sec for sync. maintenance mode and No $\log_2 (2/\epsilon_t)$ bits/sec. for the acquisition mode), which is far more than need be devoted to sync.

In the numerical example :-

Information capacity of PCM system,

$I_{nP} = 2.5 \times 10^5$ bits/sec.

Information capacity of blank bit

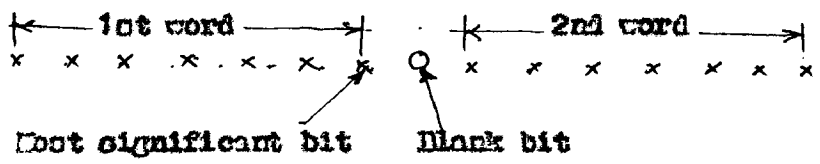
$n_P = 25000$ bits/sec (for $n = 10$)

and information rate required to maintain sync.

= 2Fs bits/secs. = 50 bits/sec. (from 3.3)

So the information capacity of the blank bit under low noise condition is - some 500 times the capacity needed. Of course in the presence of low S/N ratios, the information capacity of the blank bit is less than the above figure, but still much greater than needed.

3.321 Use of the blank space for synchronisation



If all the blank bits are made "0" the sync fails whenever all the n bits in a word are 0. Now if the channel signals are uncorrelated and symmetrically distrib uted about the half scale value, the probability of the most significant bit of all channels being below half scale is 2^{-n} $\left[= \frac{1}{2} \times \frac{1}{2} \times \ldots \times \frac{1}{2} \text{ (n places)}\right]$. Assuming there are (n-2) similar possibilities for the less significant bits (all with the same order of magnitude of probability),

the total probability of sync. failure (exclusive of misc) is approximately $(n-2+1) = (n-1)2^{-n}$ where we have neglected the very small intersection probabilities. A similar argument follows if we had chosen the blank bit to be 1.

Here, however, the assumption of uncorrelated channel information signals is dangerous ! It is not uncommon to see all channels of a telemeter connected in parallel for calibration purposes, and under this or similar conditions our word sync. scheme is certain to fail. (In the parallel connected case, failure does not occur only for the full scale level when all bits are 1).

The sync. difficulties due to highly correlated channel information signals can be removed by taking the following two steps. First,

Let the No. n of channels be odd.

This means that in successive frames the blank bit of a particular channel is alternately 0 and 1. Now it is not difficult to produce a false sync. pattern within a single frame, in some bit other than the blank bit, by static signals. If the signals are slowly varying or constant, the probability of producing at least one false set of n bits - which alternates from word to word during the frame is $1-2^{-n+1}$, which is very great.

[Probability of at least one out of n bits being 1

= 1 - Probability of the rest (n-1) - bits being 0

$= 1 - (1/2)^{n-1}$ $= 1 - 2^{-n+1}$]

If the No. of channels were even, this would cause failure of the sync., but with an odd No. of channels, the sync. does not fail because the false sync. pulse in a given channel does not alternate between 0 and 1 from frame to frame, while the true sync. pulse does. It is assumed that the recognition of the sync. pattern is averaged over several frames, as would be required in the presence of appreciable noise. With the above scheme, the only way a false sync. pattern could be produced would be by information signals highly correlated with the frame (sampling) rate, which is believed to be unlikely either in calibration or in actual use.

It is thought that the above scheme using a bit alternating from word to word in combination with an odd No. of channels may be a novel one.

3.33 Frame synchronization

Once word sync. is established it is still necessary to have frame sync. before the pulses can be steered to their correct destinations. The following schemes are used for frame sync.

3.331 Unique word scheme :-

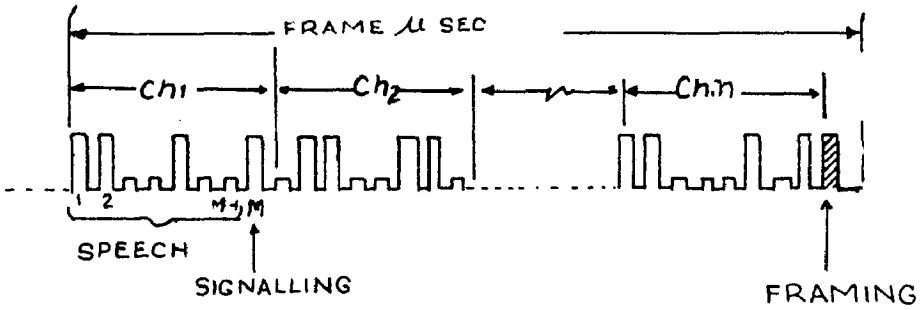
In this scheme a channel transmits a unique code which is forbidden to other channels at the beginning of each frame. The ultimate choice of code for simplicity and economy is a single digit. But since a pulse or space could exist for very long times in any position in the frame, this is not O.K. But on considering the coding procedure we find that an alternating pulse space pattern can not exist for long in any pulse position. Since an alternating pattern implies a 4-KC component in a signal and the input filters do not pass 4 KC.

In a typical PCM system with 24 channels, since each channel sample requires 8 time slots including the signalling, these 24 samples require a total of 192 time slots on the line. An additional or 193rd time slot is added to permit sync or framing the two ends of the system. The receiving circuit looks for the alternating pulse-space pattern at the same (193rd) position and gets locked to that position if it gets the same pattern for more than eight frames. Once locked if it gets some wrong pulses, it will wait and if many times it gets wrong pulses, it will unlock itself. Maximum possibility of hunting positions is 192.

Max. hunting time = 192 x time of one frame

= 192 x 1/8000 = 24 M-secs.

Framing time = 0.4 to 6 m-secs.



SYSTEM TIME ASSIGNMENT

FIG. 3-1

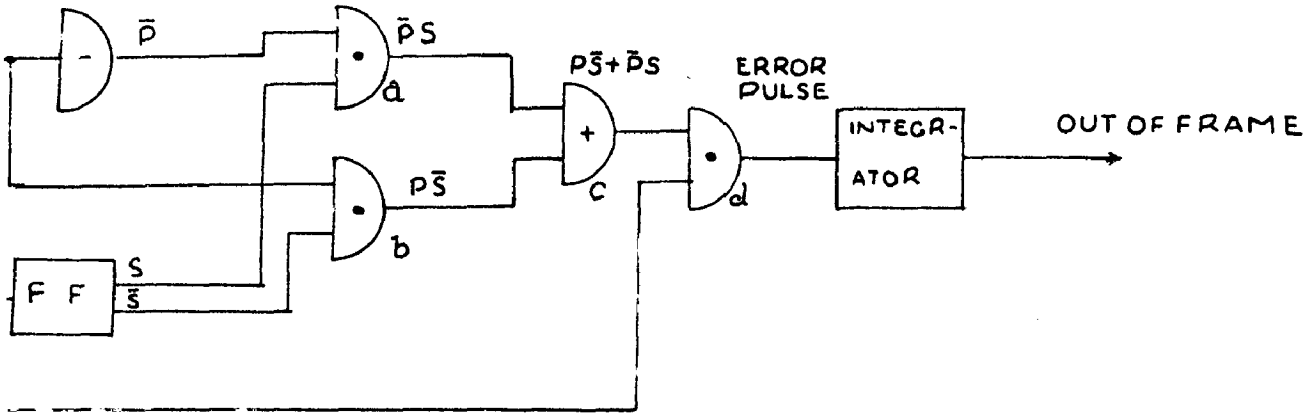


FIG. 3-2

According to the new technique it will look at two successive positions simultaneously.

In the block diagram of fig. 3.2 , P represents the incoming PCM signal, F the framing pulse from the receiving digit pulse generator. A pulse on the S' lead changes the state of the flip-flop when the system is in frame. The various possible combinations are summarised in the truth table below.

	P	S	a	b	c
Correct framing position →	0	0	0	0	0
	0	1	1	0	1
	1	0	0	1	1
→	1	1	0	0	0

At the incorrect framing position, an error pulse is generated which shifts the framing pulse F to look for the previous pulse.

Limitations :-

This scheme is very susceptible to random noise unless the word identification is averaged over a very large No. of frames, resulting in long acquisition time. This is quite satisfactory under low noise conditions, and if the No. n of channels is large, the fraction 1/n of the information capacity required is not large. This scheme can not work until word sync., is established, for in order to detect a unique word we must know the beginning and end of every word.

Illustrative example

If the random noise is such that the probability of error in any bit is 1/4 (this still gives useful yes-no information in any channel), the probability that the unique word will be received without error is $(3/4)^{n-1}$, or about 1/13 for the numerical example with n = 10. Thus the unique word is received correctly in the frame sync., channel on the average of once every 13 frames. If in one of the other n-1 channels the input is constant at a value which gives a word differing in only one bit from the unique frame sync. word, the probability of noise changing it into the unique word is $(3/4)^{n-2}$ 1/4 or 1/40 for the numerical example. Thus the average occurrence of the unique word in the frame sync., channel is three times greater than that possible in any other channel. The averaging to accomplish the frame identification must be many times the 13 frame average, and for the shortest acquisition time, all channels must be averaged simultaneously.

Precaution

If the channel information pulses contain a frequency which is not 4000 c/s but slightly less than 4 KC/S (e.g. 3800 C/S) this may also produce an alternating pattern. To counteract this, a complimentary code is sent on the line. Then the code pattern, for a frequency $\neq$ 4000 c/s, will go on changing at different sampling instants and the receiver will be able to detect the false alternating pattern.

3.332 Use of the excess information capacity in the word-sync. pulses :-

For example, in the alternating bit odd-word sync., scheme the second sync. bit in each frame can be reversed to give alternating groups 0-0-0 and 1-1-1 from frame to frame in the first three word sync. bits in each frame.

3.333 The blank bit of each word in a frame is made the same, with the sense of the blank bits reversing from frame to frame. Then averaged over several frames this scheme is immune to patterns of channel information words unless they are correlated with the frame rate.

3.34 Acquisition time is considerably different between

1. achieving word-sync. independently and then on this basis proceeding to frame sync.

Here a correlator must investigate at most N bit positions, and following this another correlator must investigate at most n channel channel positions, or a total of N + n positions.

2. achieving frame independently (to the accuracy of a bit space) and deriving word-sync. pulses by subdividing the frame sync. interval.

Here a correlator must investigate at most N positions.

Assu ption

Information signals in all channels are random (successive samples in the same channel independent., and independent. (This assumption is not usually true).

****

PREFIX SYNCHRONIZED ENCODINGS[13]

4.1 These are comma-free encodings of a special kind. A particular A-tuple (ALL) is selected and called a synchronizing prefix. Each code has the synchronizing prefix as its first A digits. The remaining L-A digits of the codes are so chosen, that, in an encoded message, no block of A consecutive digits can agree with the synchronizing prefix except blocks of A digits taken at the beginning of codes e.g., if the sync. prefix is taken to be 1010, then 1010101101100 is an allowed code but not 1010010101 10101001101, nor 10101101110. If blocks of L digits (including the prefix P) are used, the prefix P should be chosen to make large number G(L) of different blocks which satisfy the constraints. Lengthening the P decreases the number of "message digits (L-P)" which remains in the block but also relaxes the constraints. Thus for each L, there corresponds some optimum length of prefix. From the tables, the number G(L) is maximized by a prefix of the form 11...10. It is shown below that by suitable prefix sync. encodings the minimum bond of redundancy $(\log_2 N)/L$, can be approached.

4.2 STATE DIAGRAMS

Let N be $(\underbrace{p_1, p_2, \ldots, p_A}_{P}, x_1, x_2, \ldots, x_n)$

Then the allowed choices of $x_1, x_2, \ldots, x_n$, are those for which no A consecutive digits taken from the $(n+A-2)$-tuple

$$(p_2, p_3, \ldots, p_A, x_1, x_2, \ldots, x_n, p_1, p_2, \ldots, p_{A-1})$$

agree with the A-tuple P.

Imagine a conceptual machine which will scan an incoming message digit and ring a bell whenever the given prefix P appears. Such a machine with only $A + 1$ states $S_0, S_1, \ldots, S_A$ may be described as follows:

Let Π denote the A-tuple formed by the most recent message digits. If $\Pi = P$, the machine is to be in state $S0$ and the bell must ring.

The machine is to be in state Sk $(K \geq 1)$ if both of the the following conditions hold hold.

1. The last $A-K$ digits of Π are the first $A-K$ digits of P.
2. The condition (1) does not hold for any value $K' \neq K$

where $0 \leq K' < K$.

Thus the state S_K implies that at least K more digits must arrive before the bell can ring.

State	Π
S0	0101 = P
S1	x 010
S2	xx01 but not 0101
S3	either xx00 or x110
S4	xx11

Table 4.1

In the table (4.1), x's represent digits which may be either 0 or 1; e.g., 02 corresponds to 0001, 1001, and 1101.

4.3 State Diagrams of machines

For three choices of P, the states S_0, S_1, S_2,.... are represented by nodes labeled 0, 1, 2,.... Given a state S, a path which begins at S and follows arrows of the state diagram may be associated with the sequence of binary digits which is encountered on the arrows of the state diagram may be associated with the sequence of binary digits which is encountered on the arrows e.g., in Fig. 41 with P = 0101 the path which starts at 3 and visits the states 2,4,4,3,3,2,1,0,4 in that order is associated with the binary sequence 11001011. This association provides a graphical way of stating the constraints which have been placed on the digits of an allowed code.

End State

Let a state S($S \neq S_0$) be called an 'end state' if the path $p_1, p_2, \cdots, p_{A-1}$ starting at S, never visits S_0. Then the path $x_1, \cdots x_n$ starting at S_0 must never return to S_0 (and must end at an end state). Such a return would indicate an appearance of the A-tuple P in the block of digits.

$$p_2, p_3, \cdots, p_A, x_1, x_2, \cdots, x_n, p_1, p_2, \cdots, p_{A-1}$$

In Fig. 1 the end states appear as double circles.

4.31 To verify that the states $S_0, S_1, \ldots$ as defined describe a valid machine

Let two input sequences are ending in an A-tuple Π, the other ending in an A-tuple Π', both put the machine in state S_k

To show that the two sequences ending in Md and M'd correspond to the same new state (d is a digit).

Proof: Suppose

$$2 \leq K \leq A-1$$

To correspond to S_K, the last A-K digits of both M Δ M' must be $p_1, p_2, \ldots, p_{A-K}$. If $d = p_{A-(K-1)}$, then S_{K-1} is the new state following both M Δ M'.

If d is not $p_{A-(K-1)}$ then the new blocks for Md & M'd are S_K and $S_{K'}$ where both $K \leq K$ and $K \leq K'$ (as shown below).

[$Md = x_1, x_2, \ldots, x_K, p_1, p_2, \ldots, p_{A-K}, d.$

$M'd = y_1, y_2, \ldots, y_K, p_1, p_2, \ldots, p_{A-K}, d.$

① If $d \neq p_{A-(K-1)}$ and also $d \neq p_1$

then Md and M'd are both in state S_A.

② If $d = p_1$ then

Md and M'd are both in state S_{A-1}.]

However the sequence of K digits which will lead from Md to the A-tuple P will also lead from M'd to P; thus $K' \leq K$. Similarly $K \leq K'$ then $K = K'$ which was to be proved.

The cases $K=1$ and $K=A$ may be handled by a similar argument.

4.4 No. of Codes

The No. $G(n)$, of the codes which satisfy the requirements of section 4.2 depends not only on n but also on the A-tuple prefix P. Two different prefixes P, P' will be called equivalent if P' can be

obtained by applying a complementation, or a reversal or both (called symmetry transformations) to P.

Complementation - It replaces each digit pi of P by 1-pi.

Reversal - It rewrites the digits of p in reverse order (pi is replaced by pA + 1 - i).

Applied to P = 01101, complementation and reversal produce 10010 and 10110 - respectively.

Since equivalent prefix es have the same $G(n)$, it suffices to compute $G(n)$ for one prefix from each equivalent class. The No. of equivalent classes of A-tuples is found to be

$$\frac{1}{4}\left\{2^A + 2^{[(A+2)/2]}\right\}$$

where the straight brackets [ ] denote "integer part". For A = 2, 3, 4 every A-tuple is equivalent to one of the following: 11, 10, 111, 110, 101, 1111, 0111, 1101, 0110, 0011, 1011, 0101.

4.5 To compute $G(n)$ for a particular choice of an A-tuple prefix P

0.5) Theorem 1:

For $N \geq A$, $G(n)$ is the coefficient of z^{n-A} in the power series of the generating function -

$$f(z) = \frac{(1-2z)(v_1 z + \cdots + v_{A-1} z^{A-1}) + v_A z^A}{(1-2z)(1+T_1 z + \cdots + T_{A-1} z^{A-1}) + z^A} \quad \ldots(4.1)$$

For $N > 2A$ $G(n)$ satisfies a recurrence

$$G(n) + d_1 G(n-1) + \cdots + d_A G(n-A) = 0 \quad \ldots\ldots (4.2)$$

where

$$d_k = \begin{cases} T_k - 2T_{k-1}, & k = 1, 2, \ldots, A-1. \\ 1 - 2T_{A-1}, & k = A. \end{cases}$$

[And

T_n = No. of binary n-tuples which describe paths in the state diagram starting at S_0 and ending at S_0.

V_n = No. of binary n-tuples describing paths from S_0 to one of the end states. The convention $T_0 = 1$ and $V_0 = 0$ will be adopted.

For example, taking P = 1101,

$T_0 = 1$, $T_1 = 0$, $T_2 = 0$ $T_3 = 1$, $T_4 = 1$,

$V_0 = 0$, $V_1 = 2$, $V_2 = 3$, $V_3 = 6$, $V_4 = 13$

In general, when $n \geq A$, T_n counts all n-tuples for which the last A-digits form the prefix P; then,

$$T_n = z^{n-A}, \qquad n \geq A$$

{ T_n is of the form $\underbrace{x\,x\,x\,\cdots\,x\,x}_{n-A \text{ places}}, p_1, p_2, \cdots, p_A$ }

Likewise $V_n = V_A\, z^{n-A}, \quad n \geq A$]

When $T_1, \ldots, T_{A-1}$; $V_1, \ldots, V_A$ have been found, $G(N)$ may be computed with the aid of theorem 1.

e.g. taking P = 1101, the theorem states that $G(N) = 2G(N-1) - G(N-3) + G(N-4)$,

and $$f(z) = \frac{(1-2z)(z + 3z^2 + 6z^3)}{(1-2z)(1+z^3) + z^4}$$

$$= \frac{2z - z^2 + z^4}{1 - 2z + z^3 - z^4}$$

4.511 Corollary

1. Let $F(n) = G(A + n)$ the theorem gives a formula for a generating function.

$$f(z) = \sum_{n=0}^{\infty} F(n)\, z^n.$$

2. $G(n)$ might also have been computed by expanding $f(z)$ in a power series to get the coefficient of z^{n-A}.

4.52 Theorem 2

Of all A- digit prefixes, P, the one which makes $G(n)$ grow most rapidly for large n is $P = 11\ldots1$. Slowest growth of $G(n)$ for large n is obtained with any one of the $A-1$ prefixes $11\ldots10$, $11\ldots100$, $\ldots$, $10\ldots0$. However for all $N > A+1$ the No. of codes $G(n)$ obtained with the A-digit prefix $11\ldots1$, is never as great as the No. obtained with the $(A+1)$ - digit prefix $11\ldots10$.

[Although when A is fixed, the choice $P = 11\ldots1$ produces the most rapid growth of $F(n)$ for large n, this choice is never the best one when n is fixed and A can be varied. e.g., every n-tuple which is allowed for the prefix $11\ldots1$ (A ones) is also allowed for the prefix $11\ldots$ (A ones and 1 zero). The converse is not true; e. g., when $A = 3$ and $n = 10$, the 10-tuple 111010 111 is allowed for the prefix 1110 but not for 111. Then $11\ldots10$ is always a better prefix than $11\ldots1$.]

Some numerical results appear in Tables 4.2 and 4.3. If A is fixed the best prefix P (i.e., the one with the largest $G(n)$) has a curious dependence on n. At $A = 3$, $P = 110$ is best until $n = 14$; $P = 101$ is best for $n = 15, \ldots, 19$. And $P = 111$ is best thereafter. For any fixed A, the prefix $11\ldots1$ is ultimately the best.

The best choice of A and the correspondingly maximum $G(n)$ are given in table 4.3. This table also lists the No. N' which for all P, is an upper bound on $G(n)$.

Table 4.2

G(Π) for different profiles

N	11	10	111	110	101	1111	1110 & 1110	1010	1101 & 1001
3	1	2							
4	1	3	1	2	1				
5	2	4	1	4	2	1	2	2	2
6	3	5	2	7	4	1	4	3	3
7	5	6	4	12	7	2	8	4	6
8	8	7	7	20	12	4	15	9	11
9	13	8	13	33	21	8	28	16	21
10	21	9	24	54	37	15	52	32	39
11	34	10	44	88	65	29	95	60	73
12	55	11	81	143	114	56	177	115	136
13	89	12	149	232	200	109	326	210	254
14	144	13	274	376	351	208	600	405	474
15	233	14	504	609	616	401	1104	764	885
16	377	15	927	986	1081	773	2091	1440	1652
17	610	16	1705	1595	1897	1490	3756	2710	3024
18			3136	2583	3329	2872	6872	5103	5757
19			5768	4180	5842	5535	12640	9612	10747
20			10609	6764	10252	10671	23249	18101	20062
21						20569	42762	34086	37451
22						39640	78652	64152	69912

Table 4.3

G(n) For P = 11 ... 10

n	A	G(n)	$(n^{-1} 2^n)$	n	A	G(n)	$(n^{-1} 2^n) \times 10^{-6}$
3	2	2	2	19	4	12,540	0.027,6
4	2	3	4	20	4	23,249	0.052,4
5	2 or 3	4	6	21	4	42,762	0.105
6	3	7	10	22	5	82,392	0.190
7	3	12	18	23	5	158,816	0.365
8	3	20	32	24	5	306,128	0.70
9	3	33	56	25	5	590,081	1.34
10	3	54	102	26	5	1,137,418	2.58
11	4	96	186	27	5	2,192,444	4.96
12	4	177	341	28	5	4,226,[illegible]72	9.6
13	4	326	630	29	5	8,146,016	18.5
14	4	600	1170	30	5	15,701,951	35.8
15	4	1,104	2180	31	5	30,266,484	69.5
16	4	2,031	4096	32	5	58,340,524	134
17	4	3,736	7710	33	5	112,454,976	258
18	4	6,872	14563	34	5	216,763,936	505
				35	5	417,825,921	981

4.6 Redundancy Estimates

Let the sync. prefix be 11...1 (A digits) and let $N = A^2+1$. Instead of using all N-tuples which satisfy the constraints of section 4.2 the even stronger constraints

$$X_1 = X_{A+1} = X_{2A+1} = \cdots = X_{N-A} = 0$$

are imposed. Thus, the typical N-tuple has the appearance (for A = 4)

$$1\ 1\ 1\ 1\ 0\ X\ X\ X\ 0\ X\ X\ X\ 0\ X\ X\ X\ 0 .$$

where the X's represent digits which are unrestricted. Since 2A of the A^2+1 digits are fixed, the redundancy is $2A/A^2 + 1$, which equals $\frac{2(N-1)^{1/2}}{N}$. This is of the same order of magnitude as that for the comma free encoding ($= \frac{2^N}{N}$). In table 4.3 the best values of G(N) fall short of $\frac{2^N}{N}$ by factors of the order of 1/2. A possible advantage of this encoding is that the unrestricted digits (X's) may be taken directly from a given binary message without further encoding.

PSEUDORANDOM PULSE SYSTEMS FOR SYNCHRONIZATION

5.1 The security of a pulse type communication system can be improved by the incorporation of an element of randomness in the time of transmission, which is not random, but is determined by an extremely complex programme. By duplicating the programme in the remote equipment, the receiver can anticipate the time of arrival of the local transmissions.

The pseudorandom pulse system[23] (PRP system) has two modes of operation. One is designated uncoded operation and is characterized by a constant intermessage period. The system can be operated in either mode, and a fail-safe feature is provided to return the system to the periodic mode if the local and remote units become unsynchronized while in the pseudorandom mode.

In the coded mode the time of transmission and reception is caused to jitter by the outputs of two synchronized pseudorandom pulse generators - one in the remote unit and one in the local unit. The pseudorandom pulse generator is an eight stage magnetic core re-entrant shift register (Appendix IV iii) which produces a long sequence of one and zero outputs at a rate determined by a shift pulse input. The output sequence of the shift register has a very complicated time structure, but is purely causal in nature. The output sequence is operated upon by a computer to add additional scrambling and produce a pseudorandom No. between zero & 63 - which is used in binary form, with a new No. from zero to 63 being generated each maximal repetition period (10,000 μsec). The duration of each intermessage period is determined by the magnitude of the No. produced by the computer.

In the operation of the PRP system, two types of synchronization must be maintained; the clock frequency generators must be synchronized to ensure proper internal time, & the pseudorandom pulse generators must be in step for the receiver to correctly anticipate the transmission. The system is started in the uncoded mode; and after clock sync. is achieved, the system is caused to operate in the coded mode by command from the local transmiter. If the code generators should not remain in step, or if reception is interrupted for a preset period, the receiver automatically drops out of coded operation and returns to uncoded operation. Coded operation may again be initiated by command from the local transmitter when communication is restored in the uncoded mode. The 2nd coded start may be either with the same code as the first start or a different predetermined code.

5.2 System Parameters

1. Nominal PRP = 100 cps.
2. Max. intermessage period deviation = 20% of nominal
3. Assumed message length 20 - 25 μsec
4. Message position quantization interval 30 μsec.
5. Pseudorandom period greater than 5 minutes

The quantization interval is defined as the spacing in time between two adjacent possible message positions.

Example

The 20% max. duration from the periodic position in the 10,000 μsec nominal intermessage time is 2000 μsec and hence the No. of possible positions separated by 30 μsec is 2000/30 = 66.6

For ease of implementation, these parameters were adjusted to 64 possible message positions with a quantization interval of 30 μsec resulting in a max. message duration of 19.2 ms x (number) (as shown in the above figure 5.3.

The message position used for any particular transmission is determined by the output sequence of the pseudorandom pulse generator; the uncoded messages are always located in the first of the 64 possible position.

The choice of the ms duration from the periodic position depends on two factors.

1. The time necessary within the circuitry associated with the randomization to prepare for the next transmission.

2. The time required for the receiver to process a message and prepare for the next one.

At 100 cps PRF, the duration limit is ≃ 75 ms and will be reduced as the nominal PRF is increased, since a specific amount of time is required to perform gating, shifting and counting operations.

5.3 In the described equipment the 'multiple' pulse message typical of a pulse code communication system is replaced by a much simpler message structure. In uncoded operation the message consists of a single pulse of 1 μsec duration. During coded operation the message consists of two pulses of 1 μsec duration spaced 4 μsec apart in time. The double pulse informs the coding controller in the receiver that the transmissions are coded. This simplification is

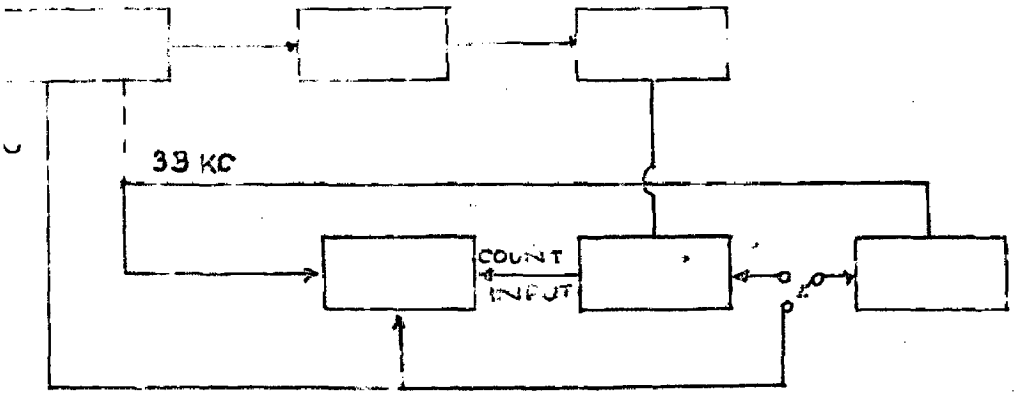


FIG- 5-1

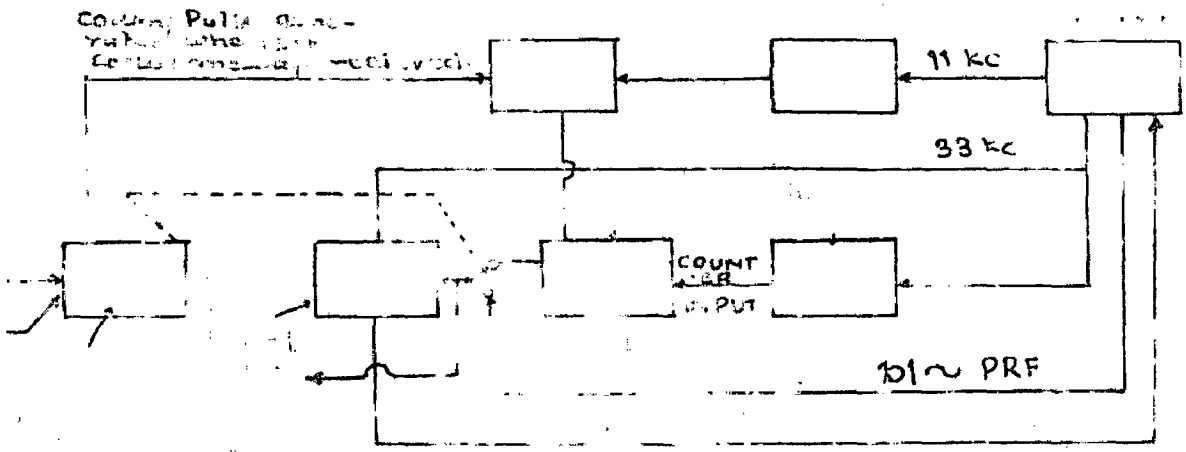
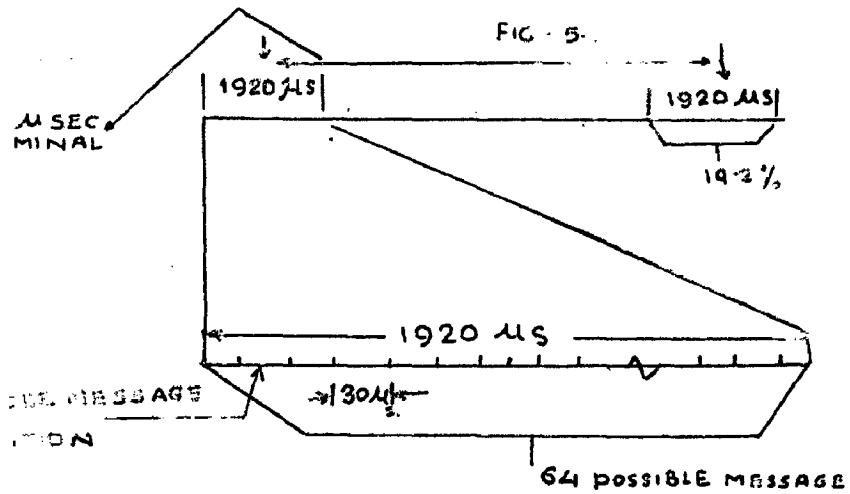


FIG - 5-



PRP SYSTEM MESSAGE ST MELVE

FIG-5-3

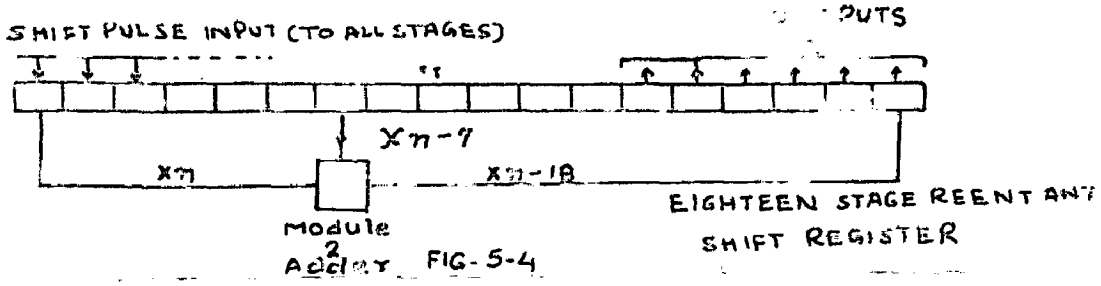


FIG-5-4

irrevalent to the operation of the system.

Transmitter Operation (Fig. 5-1)

1. Coded Mode Operation

The timing of the transmitter unit is controlled by a 100 K-C shift pulses across a clock oscillator and the frequency divider chain. A burst of seven 11 K-C shift pulses causes a series of seven one and zero pulses to be generated by the code generator. The first six of these pulses are used to represent a No. from zero to 63 in binary notation (the seventh pulse is discarded to provide additional security against code breaking). This No. is then read into the preset counter and stored there. (Until the time of the 101-cps pulse). The counter is a specific type which supplies an output when a predetermined predetermined No. of counts has been received; in this case the preset No. is 63 (zero is considered a No.) The 101 cps pulse causes 3 -KC pulses to be gated into the counter where they are counted. Thus the length of time between the 101 cps pulse and the preset counter output pulse is determined by the difference between 63 and the No. read into the counter from the code generator. This time delay is different for each message and is determined by the output of the code generator; if the output sequence represents a large No. the delay is short and if the code generator output is a small number the delay will be correspondingly long.

The output from the counter triggers a gate generator which selects the next 33-KC pulse in a coincidence circuit to trigger the output pulse generator. In effect, the delay mechanism merely determines which one of the clock controlled 33-KC pulses will be used

to trigger the output. In coded operation the selected trigger pulse is also delayed 4 μsec by a delay line and caused to retrigger the output pulse generator giving rise to a double output pulse.

2. Uncoded mode operation

Here the 1.1 - cycle signal is used to trigger a gate generator which selects the following 33-50 pulse in a coincedence circuit to trigger the output pulse generator.

Receiver Operation (Fig. 5-2)

Here two new blocks are added, (1) Pulse selector is replaced by the block marked coding controller and there is one additional block designated time descriminator.

1. Uncoded mode

Here the transmitter and receiver clock sources are in synchronism (in phase) and the arrival of the transmitted pulse will coincide with the internally generated 33-KC pulse gated from the frequency divider. The time descriminator checks the time coincidence of these two pulses and generates an error voltage of appropriate sign if they are not exactly coincident. The error signal is applied to the receiver clock source (a voltage controlled oscillator) forming a closed-loop system which maintains pulse coincidence. When the clock sources are in sync., the 101-cycle output from the frequency divider initiates the receiver enable gate.

2. Coded mode

The coded message structure, consisting of two 1 μsec pulses spaced 4-μsec apart, is sensed by the coding controller which causes the

receiver unit to be switched into coded operation. The switching operation is completed by the time of arrival of the next message and the transmitter and receiver code generators are running in sync. and the jittered output is used to trigger the receiver enable gate. Coded operation will be maintained until a predetermined number of messages fail to be received. The present system requires the loss of 25 messages before reversion to uncoded operation; this is a fail-safe feature should the code generators become unsynchronised.

Pseudorandom pulse generation

The exact time of transmission should be unpredictable to all except the intended receiver. PPG is a device which is capable of storing the timing information in digital form. If the receiver is to have a narrow enable gate to protect it from spurious signals, jamming, noise, information about the exact times of transmission is stored before hand in the PPG.

PPG is a shift register which reads out the stored information in serial form when interrogated by serial shift pulses. The output of the last stage of the shift register is combined with the output of an intermediate stage using appropriate logic and the result is caused to reenter the first stage of the register. This technique permits the generation of a repetitive sequence of pulses of No. 2^n-1 where n is the No. of stages in the shift register. As long as the sequence is not repeated the output cannot in general be predicted and therefore has a random quality. There are 3

important factors which determine the exact time structure of the output sequence.

1. The initial condition - (original sequence set into the shift register.)
2. The type of logic used to combine the outputs.
3. The position of the tap on the shift register; i.e., which of the intermediate stages is used not every tap on the shift register will provide a usable sequence.

If two pseudorandom pulse generators are set up with the above mentioned factors identical and if they are caused to shift in synchronism, their outputs will be identical at all times.

For a non-repetitive sequence of 5 min. duration with a choice of 64($=2^6$) possible position for each message, a 180,000 digit sequence is required.

$$(5\ \text{min.})\left(60\ \frac{\text{sec}}{\text{min.}}\right)\left(100\ \frac{\text{messages}}{\text{sec}}\right)\left(6\ \frac{\text{bits}}{\text{message}}\right) = 180,000\ \text{bits}$$

The 18 stage recentrant shift register, comprising of 18 magnetic core bistable memory units, with Modulo - 2 logic will generate a sequence of 262, 143 bits without repetition. The last 6 stages provide the six binary digits necessary to define a No. from zero to 63. Magnetic core type shift registers will operate at shift rate upto a few hundred KC/S. The logic circuit is a difference

amplifier which performs Modulo-2 addition according to the rules:

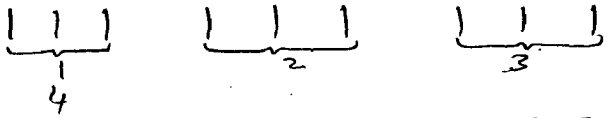
$0 + 0 = 1$ $\qquad$ $1 + 0 = 1$

$0 + 1 = 1$ $\qquad$ $1 + 1 = 0$

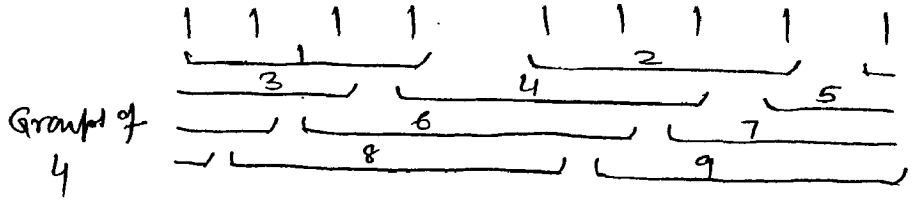
5.5 Additional Scrambling Techniques

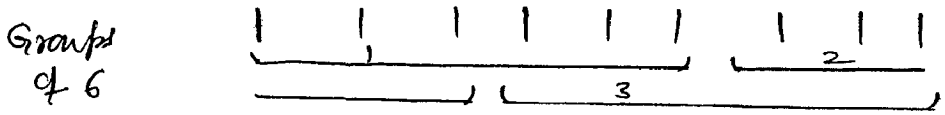
The above shift register is susceptible to certain techniques of code breaking so that to provide high security against code-breaking additional scrambling is applied to the output of the pseudorandom pulse generator. The output sequence is taken in groups of 6 pulses, which are operated upon by the counter to produce a single offset (converted to a binary No. and subtracted from 63). In addition, one or more pulses are periodically dropped from the generated sequence. With the 18 stage shift register, one can afford to throw many pulses, as a Max. of only 180,000 is necessary for 5 min. of nonrepeated transmission. The present form of equipment is designed to shift a new pulse sequence from the pseudorandom pulse generator for every message transmission. Six of the pulses are read into the counter and the seventh is discarded. Thus there is no one-to-one correspondence between the output of the pseudorandom generator and the message structure. The repetition period of jittered message structure is 6.2 minutes.

Consider a sequence of 9 pulses (the output sequence will always be an odd No.)



If we form groups of 3, there are only 3 possible different groups because group 4 is same as group one.





In the 2nd case the min. No. of groups equals the sequence length itself i.e. 9. In the 3rd case it is 3, because of the factor 3 being common to the sequence length and the No. of pulses per group.

Hence, when the sequence length is not evenly divisible by the No. of pulses per group, then the No. of unrepeated messages will be greater. If the sequence length is evenly divisible (as in case 1) the No. of unrepeated transmission is determined by the quotient

Applying above reasoning, drawing 8 pulses from the PRP generator for each transmission and discarding two would result in a jittered message period of 43.6 minutes. On the other hand, a 15 stage shift register will provide a 5.4 min. run using the output in groups of six.

The output sequence from the shift register (Fig.54) is an iterative Boolean sequence satisfying a linear (Modulo - 2) recursion equation of two terms. This may be expressed in general as

$$x_n = x_{n-a} + x_{n-b} \qquad (\text{mod. } 2)$$

or for the configuration of fig. 5-4 :

$$x_n = x_{n-7} + x_{n-18} \quad (mod\ 2)$$

x_n can be 0 or 1 and represents the output of the logic circuit.

Delay and add property

A sequence y_n obtained from the x_n sequence by adding to x_n a delayed version of itself, such that $y_n = x_n + x_{n-r}$ satisfies the original recursion equation. Thus y_n is identical with x_n although shifted in time. This delay-and-add property of sequences generated by linear logic offers to a hacker the opportunity of breaking the code. So additional sophistication is added by using the sequence in groups and periodically dropping pulses from the sequence instead of combining more variables in the logic circuit.

To make the system more secure the binary adder of the logic circuit is replaced by a binary multiplier operating according to the rules. $1 \times 1 = 1$ $\quad 0 \times 1 = 0$

$1 \times 0 = 0$ $\quad 0 \times 0 = 0$

This makes the pseudorandom generation 'nonlinear'

The other properties desirable for coding are (alongwith security) (1) random appearance (2) the max. or near max. length (max. length $2^n - 1$ terms where n is the No. of shift register stages) and (3) An autocorrelation fun suggestive of random noise. The main problem is that of testing the resulting sequence to make certain that it possesses the above mentioned desirable properties.

5.6 Applications

1. Radar - Here the sync. problem is simpler since the transmitter and receiver are at the same location and two separate pseudorandom generators are not strictly required. Receiver enable gate information can be obtained directly from the transmitter code generator and delayed appropriately for range tracking.

An advantage in addition to security consideration is the elimination of range ambiguity and blind spots which are inherent in a constant PRF system.

Another advantage is its retrofit potential. If the receiver cannot process the read. message at pseudorandom times, the message may be stored upon reception and processed periodically. This essentially delays the message one nominal period which is of little consequence in most communication systems.

*****

SYNCHRONIZATION IN DELTA-MODULATION

6.1 A method to shorten the time required for the frame operation in the t.d.m. delta modulation[21] system is described. Employing successive "1"s as the sync. pattern, the system detects the sync. channel out of the delta modulated information pulses which occur at the rate of one half in average.

Principle of operation

First, the pulses in one frame period after the start of hunting are stored in the memory device, and in the second frame, the stored pulses are read out, taken the logical product on the time division basis with the incoming pulses which belong to the second frame, and the resultant pulses are stored in the memory device. The stored pulses are then read out in the 3rd frame, and the resultant pulses are stored in the memory device. Thus the same operation is performed successively until only one pulse in one frame is identified to exist in the memory device. With this arrangement the speech pulses which by nature do not always appear in every frame are erased out of the memory during the successive operation and the sync. pulse which appears in every frame is finally extracted. This method makes it possible to take correlation of each channel in parallel on the time-division basis so that the time required for sync. becomes shorter than that in existing systems.

Fig. 6.1 shows a block diagram of the system. The sync. pulse extractor, which contains a memory device with the capacity of one frame, extracts the synchronous pulse from the information pulses taking the correlation of each frame after the start of hunting the

The sync. detector observes the state of the memory device of the sync. pulse extractor, if only one pulse recirculates in the memory device confirms that the sync. is established. Means are provided to maintain it even if succeeding sync. pulse happens to disappear due to transmission disturbances.

Lost sync.

During the extraction process, the recirculating pulse in the memory device is lost because of the error of the sync. pulse. The lost sync. detector observes whether no pulse is recirculating in the memory device.

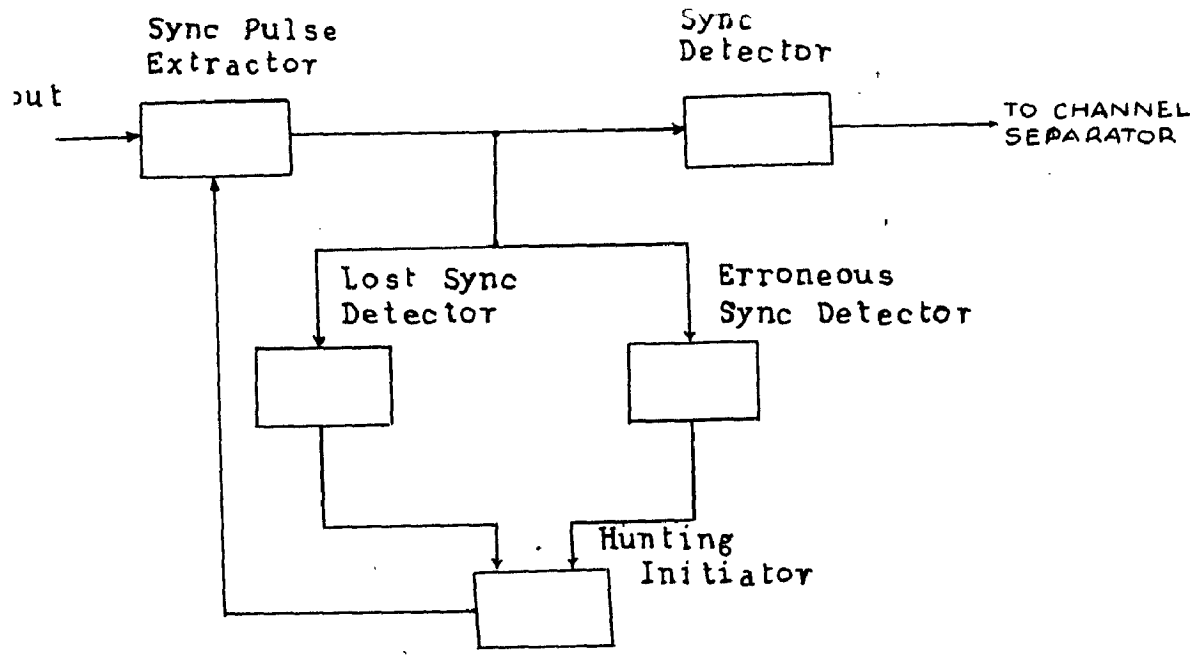
Erroneous sync.

In this case one of the information channels is mistaken as the sync. channel. The erroneous sync. detector utilizes the fact that the probability that "0" occurs in the sync. channel is sufficiently small as compared with the probability that "0" occurs in the information channels, which is one-half in delta modulation.

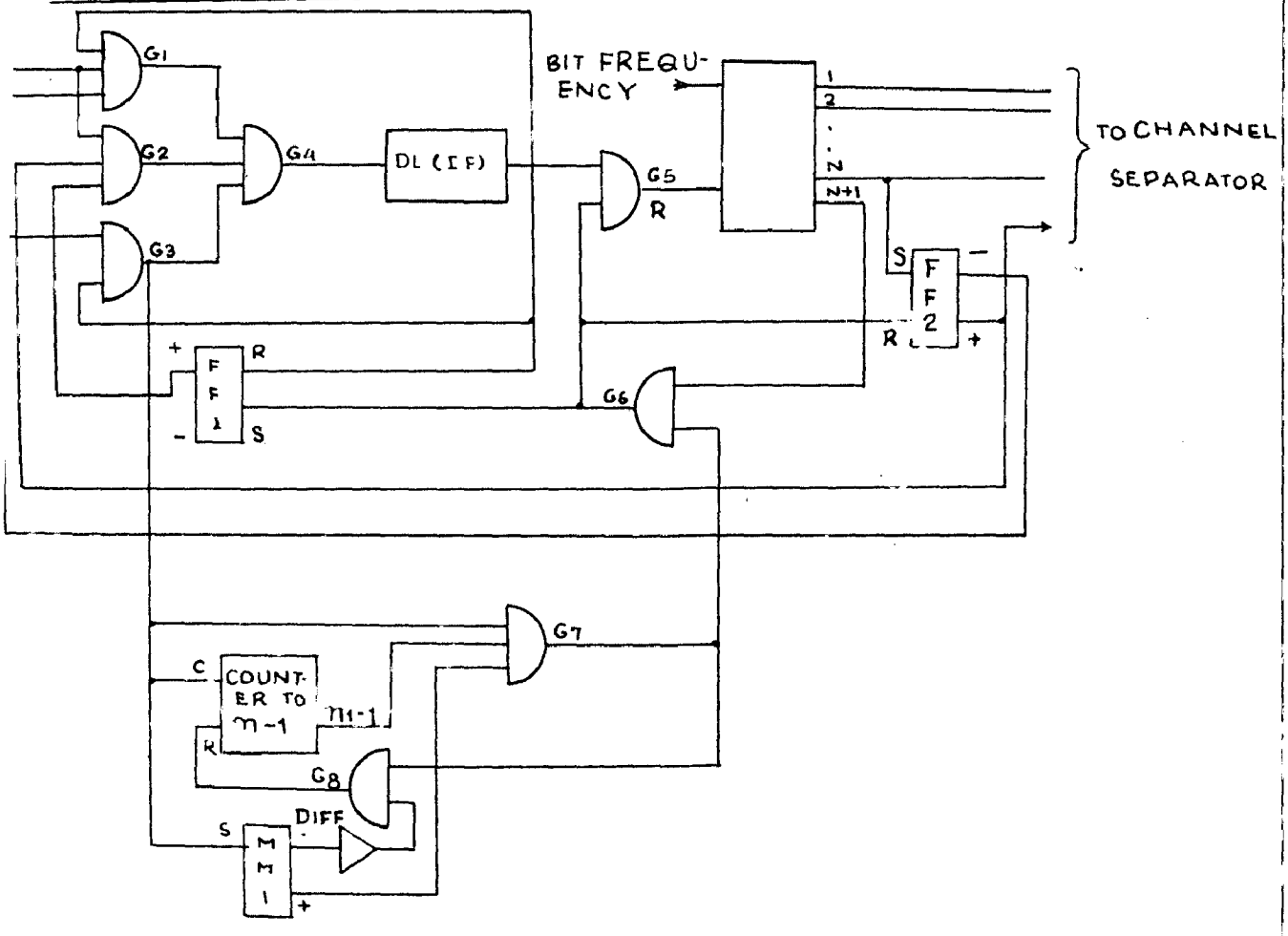
When the lost sync or the erroneous sync. is detected, hunting is started again by the hunting initiator which initiates the operation of the sync. pulse extractor.

6.2 System Description (Fig. 6.2)

DL is a magnetostrictive delay line with the capacity of one frame. When hunting is required, FF1 is set FF2 and the "counter to N + 1" are reset. G2 is opened by the set output of FF1 for only one frame after the start of hunting and DL stores the information during the period. FF1 is reset by the 1st appearing output pulse of DL after the start of hunting and as the result G2 is closed. Thus the information in one frame is stored in DL and is recirculating. The



-1 A BLOCK DIAGRAM OF THE FRAME SEPARATION SYSTEM



A BASIC CONFIGURATION OF THE FRAME SEPARATION SYSTEM

FIG 6·2

logical products of each channel after the start of hunting are successively taken at G1 so that the channels in which "1" successes are written exclusively into DL. The "counter to N+1" (where N is the No. of channels in one frame) counts the clock pulse occuring in every channel and is reset when the output pulse of DL appears, which also resets FF1. Thus, the first appeared output N of the "counter to N+1" shows the state of sync. and sets FF2 which indicates the establishment of sync. After the establishment of sync., the "counter to N + 1" is reset by the sync. pulse recirculating in DL. The set output of FF2 and the output of the "counter to N + 1" are utilized for channel separation.

Once FF2 is set, G3 is opened and as a result, the sync. pulse recirculates through G3 and is held, even if the sync. pulse does not arrive at G1 in case the sync. pulse accidently becomes "0". Therefore sync. pulse can always recirculate in DL, through G1 when it arrives correctly, or through G3 when it happens to be lost by error. This is to stabilize the sync. within a certain extent against the case that the sync. pulse becomes "0" by error after the sync. has been established.

Lost synchronization detection

The sync. detector also works as a lost sync. detector utilizing the fact that the confirmation of the sync. and the detection of the lost sync. do not occur at the same time. In the system of Fig. 6.2, the lost sync. is indicated by the output N + 1 of the "counter to N + 1". The presence of the output N + 1 indicates that no pulse recirculates in DL, since the "counter to N + 1" should be reset in N counts or less, if at least one pulse is recirculating in DL.

The output N + 1 resets the "counter to N + 1" and sets FF1. Although FF2 is set by the output N of the "counter to N + 1", it is reset one bit later by the output N + 1 of the counter to N + 1". And thus the hunting is initiated again.

Erroneous Synchronization Detection

The output of G3 appears when an error ("0") occurs in the channel suspected to be the sync. channel, and triggers MM which generates the output pulse with the width of n2 frames. Thus the No. of errors of the suspected sync. pulse in n2 frames is counted by the "counter to n1 - 1". If n1 errors are detected in n2 successive frames from the first error pulse, a pulse appears at the output of G7 and indicates the erroneous sync. The "counter to n1 - 1" is reset and FF2 which is provided to indicate the establishment of sync. is also reset and the hunting is started again. However, if the errors of the sync. pulse are less than n1, it is assumed that sync. pulse is accidently lost and the frame separation is correct. Therefore, the "counter to n1 -1" is reset by the trailing edge of the output of MM to prevent the accumulation of the counts of errors.

As for the memory device, where one frame consists of a large No. of bits, a magnetostrictive delay line might be more economical than a shift shift register. But a shift register might be convenient for the confirmation of the sync. or the detection of the lost sync., since the content of the memory can be continuously read in parallel. This is also useful, when the sync. pulse is consisted of several bits, to detect the pattern at the input of the memory device.

6.3 Improvement of sync. recovery ~~channel~~ by pattern alteration (Fig. 6.4)

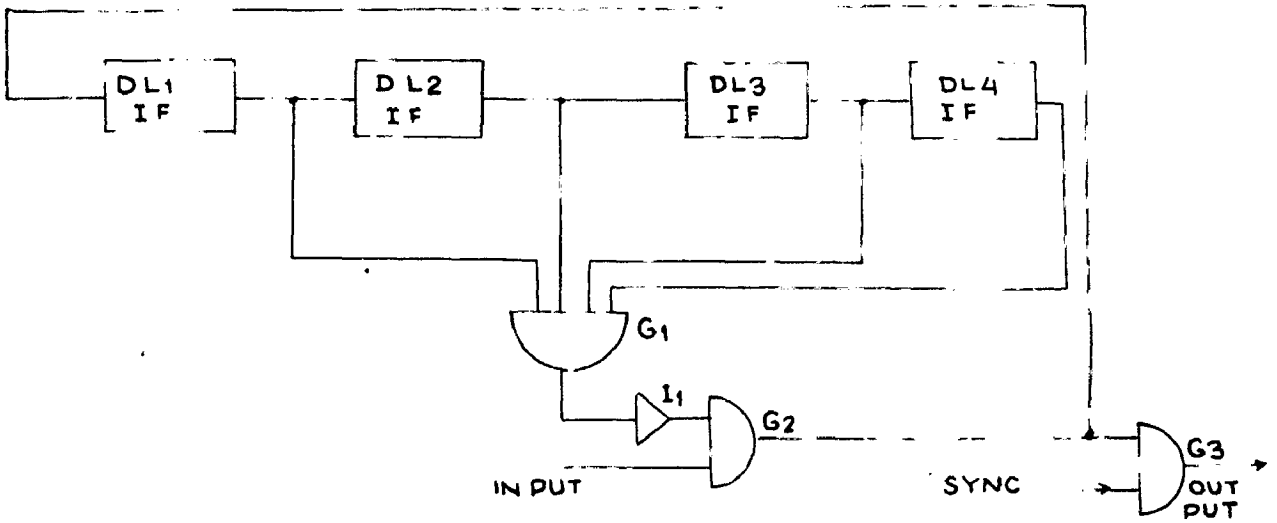
In the system mentioned above, the time required for sync.

depends on how long "1" succeeds in the channels except sync. channel. This is due to the statistical properties of the signal.

Since the pattern which disturbs the establishment of sync. is 11...1, if this pattern is altered to the pattern 11...10 at the transmitting one such an arrangement (Fig. 6.3) will shorten the time required for sync. with some decrease in S/N ratio.

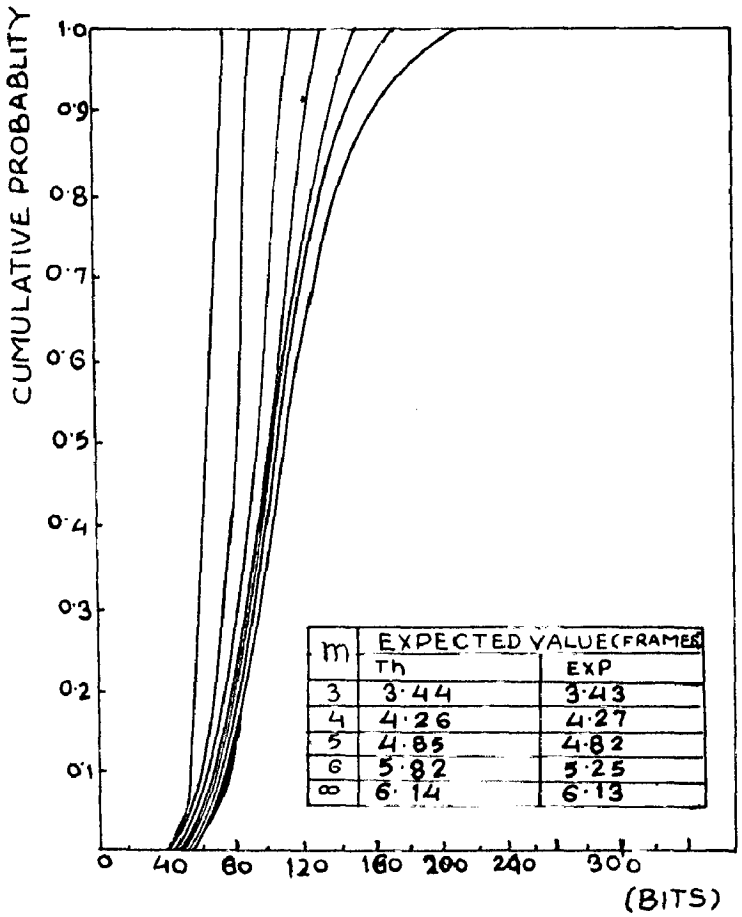
An arrangement for pattern alteration

In the arrangement when m "1" succeeds 4 times in a channel, "1" appears at the end of each delay line and as a result a pulse appears at gate G1. The pulse is inverted by the inverter I, the fifth "1" is inhibited at gate G2. The information pulses thus altered are mixed with the sync. pulse at the gate G3. Generally we need (n-1) delay lines to alter the pattern $\underbrace{11\ldots1}_{m}$ to $\underbrace{11\ldots10}_{m-1}$ but the arrangement ensures the sync. to be established within (n + 1) frames, in the case that the sync. pulse has no error. The lost sync. or the erroneous sync. can also be detected earlier.



AN ARRANGEMENT FOR PATTERN ALTERATION

FIG. 6-3



IMPROVEMENT OF SYNC. RECOVERY CH. BY PATTERN-ALTERATION.

FIG. 6-4

SYNCHRONIZABLE CODES

7.1 Need for Coding

Assume the data to be transmitted are stored on an endless paper or magnetic tape. If the tape is driven past the reading head at a constant velocity, the output of the receiver (a tape reader) would correspond to that of a fixed or constant data rate channel. If the words on the tape were equal in length, there would be no requirement for sync. except for an accurate clock. Furthermore, if the tape were driven with a variable velocity, but in a deterministically controlled manner, in principle a new variable rate clock could be designed that could automatically insert divisions or commas between the words emanating from the tape reader. However, if the velocity of the tape were a random process there would no longer exist a way to predict with certainty the position of a comma.

For the randomly variable rate channel, sync. can be achieved only by encoding, and consequently only by a reduction in channel capacity. For such a channel, the sync. error is as much an error as additive noise. For a channel corresponding to a tape driven with constant velocity, but stopped at random times for random intervals, comma-free encoding would seem to be necessary in order to establish the comma with certainty.

7.2 Comma-free codes (18, 20)

The encoding is a list of n-tuples so chosen that any overlap formed from one code word followed by another differs in at least one symbol from any word in the code dictionary. If the receiver starts to decode when it is out of synchronism, then it

always looks after an N-tuple (code) which is not one of the codes in the list. After at most N - 1 digit times, and at most N-1 false starts, the receiver finds the correct synchronism.

Example N = 5 ; a list of six 5-tuples:

01000	01110
01100	01011
01010	01111

This encoding has a redundancy

$$= 1 - \log_2 6/5 = 0.48$$

Delbrück, Golomb, Gordon & Welch found the upper bound on the No. of codes which a comma-free encoding may contain, which on simplification is given by

$$G(N) \leq \frac{2^N}{N} \qquad \ldots(7.1)$$

From (7.1) a redundancy at least as great as $\log_2 N/N$ is necessary for a comma-free encoding using N-tuples.

7.21 Index of comma freedom :

The codes where any overlap disagrees in at least p positions from any code word, are said to have an index of comma freedom p. It has been shown that p increases at least proportionately with the No. of code words. As an example, a dictionary containing 256 words has been obtained with p = 34. Because of the rather low correlation between any overlap and code word of these codes, sync. can be obtained quite rapidly even at the threshold signal-to-noise conditions. Also it was found that over a continuous channel it would be necessary to use a sequence of approximately 16 symbols as a prefix to each word to

achieve sync. with the 256-word dictionary as rapidly as is possible by making the dictionary comma-free.

The comma-free sync. method necessitates increased complexity at the receiver. Each sync. position must be observed simultaneously in order to obtain sync. in the minimum time. But there are situations in which additional receiver complexity is a small price to pay for more rapid sync., particularly when it can be achieved without expending any extra power and without increasing the complexity of the transmitter.

7.31 Orthogonal codes(42)

These codes are good for transmission mode of operation. Here the cross-correlation, ρ_{ij} between the ith and the jth word is identically zero. For Gaussian channel the optimum codes are those in which $\rho_{ij} = -\frac{1}{n-1}$. However for large values of N this is essentially the orthogonal situation. For these codes the probability of an error has been shown to decrease exponentially with $n = \log_2 N$.

Bandwidth occupancy

If a set of 2^n code words is to be orthogonal, each word must contain 2^n symbols; i.e., there are 2^n subintervals during which the word may be at either the +1 or -1 level. Each symbol is of duration $\frac{nT}{2^n}$ secs.

If a particular channel phase radiates a sinusoidal carrier $\sin \omega t$, it is possible to have other sinusoidal carriers at

$$\omega + \frac{2\pi v}{nT/2^n}, \qquad (v = \pm 1, \pm 2, \ldots)$$

without interfering with the given signal, provided v is a multiple of $\pi \Big/ \left(\frac{nT}{2^n}\right)$, because over any given sub-interval $nT/2^n$,

$$\int_0^{\frac{nT}{2^n}} \sin \omega t \sin\left[\left(\omega + \frac{2\pi v}{nT/2^n}\right)t + \phi\right] dt = 0 \qquad (v = \pm 1, \pm 2, \ldots)$$

Thus the effective BW occupied by the channel is $\frac{2^n}{nT}$ c/s and hence becomes infinite asymptotically with n.

Another characteristic of the orthogonal code sets is that the noise components of the correlator outputs are mutually independent.

7.32 Construction of binary orthogonal codes

Two code words are orthogonal if the No. of symmetrical positions in which they are similar equals the No. in which they are dissimilar or $\sum_{i=1}^{k} x_i y_i = 0$

A single bit of information may be sent by selecting from a set of two orthogonal code words of two symbols each

0 0

0 1

Two bits might be sent by using the code word set

0 0 0 0

0 1 0 1

0 0 1 1

0 1 1 0

It should be noted that this set can be constructed by extending the set for one bit both horizontally and vertically. The lower right hand square is filled by the complements of these words.

To prove that the construction yields an orthogonal code set at each step, assume that such a construction exists for K bits. Then for K + 1 bits, extending the 2^K words vertically yields a set of 2^{K+1} words which are all orthogonal, except that each word in

extending the words horizontally, the upper half of the extensions is the compliment of the lower half. Thus each pair of words in the set has as many similar symbols as it has dissimilar ones. Hence, the set is orthogonal.

7.4 Biorthogonal codes (or Reed Muller Codes)

The codes are so named because the correlation between any two code words is either zero or minus one, i.e., the No. of positions in which corresponding symbols of two code words of N symbols are different is either N/2 or N. (These codes are known to exist for all $N = 2^{\nu}$, for all $\nu \geq 4$ and to contain $2N$ words).

They can be generated by taking a set of orthogonal codes and adding to it the compliments of each word. A biorthogonal code for 5 bits may be constructed from the preceding orthogonal code for 2 bits.

0 0 0 0	1 1 1 1
0 1 0 1	1 0 1 0
0 0 1 1	1 1 0 0
0 1 1 0	1 0 0 1

One advantage over corresponding orthogonal set is that it requires one-half as many symbols per code word. Thus, the BW required to transmit the same No. of bits/sec. is cut in half. Also, the average Pij among all the codes in a set of 2^n words is $-1/n_{2-1}$; there are in all $(2^n-1)\,2^{n-1}$ pairs. The pij's are -1 for 2^{n-1} pairs, and zero for all the rest.

Thus the average correlation is $\dfrac{(-1)\,2^{n-1}}{(2^n-1)\,2^{n-1}} = -\dfrac{1}{2^n-1}$

Sets of biorthogonal codes have equal No. of zeros and ones.

likely, this occurs that the modulating signal will have zero mean; hence all the power in the carrier will be modulated.

7.5 Self synchronising codes (57, 58)

To make the codes self synchronising, one way is to select a dictionary from the comma free dictionary, with desired error correcting properties. At low S/N ratios p is desired to be low and also that the codes be made more redundant to achieve the desired error correction. Or the comma-free dictionary can be selected from a dictionary which possesses the necessary error correcting capabilities. Since the error correcting properties of a binary code are unaffected by a cyclic interchange of the ith symbol or by a permutation of the ith and jth symbols of every code word, the code can be made comma-free by just performing either operation or some combination of such operations. But several conditions may be imposed upon the self sync. code:

1. The expected or maximum time necessary to obtain sync. must be small.

2. The error probability in the sync. operation must not be increased with a resulting decrease in the information rate due to the addition of self sync. properties.

3. No redundancy should be introduced, for purposes of sync.

These limitations seem to indicate that self-sync. is not practicable. Since each correctly detected word conveys exactly $n = \log_2 N$ bits of information, and since (according to 3) no redundancy is to be added to facilitate the sync. process, these n bits must correspond

to a bits of data information. Thus there are no surplus bits available to carry the sync. information. But on close inspection we find that the asynchronous error probability is greater and that consequently, the information rate is less than that possible with the same channel at the same S/N ratio after sync has been obtained. This difference between the sync. and async information rate represents a rate at which it is theoretically possible to send sync. information without violating any of the basic principles of information theory. A way to utilise some of this sync. capacity for orthogonal codes is described below.

7.51 A subclass of orthogonal codes is that consisting of a sequence of pulses of duration T/N and constant +ve or -ve amplitude. For N = 4 such a code dictionary may be represented as follows :-

1 1 1 1

1 1-1-1

1-1-11

That such codes exist for all values of N = is apparent by observing that, if A is an N x N = 2^n matrix whose rows represent the words of an orthogonal code, then B has the same properties but with N = 2^{n+1}

where B = $\begin{matrix} A & A \\ A & -A \end{matrix}$ (7.3)

And where -A is obtained by replacing the 1's of A by -1's and the -1's by 1's.

These codes are referred to as binary codes for obvious reasons. If the ith word of A consists of the symbols $\{\xi_\mu^i\}$, substituting $x_\mu^i = \frac{1}{2}(1-\xi_\mu^i)$ for ξ_μ^i yields a matrix A' consisting of ones and zeros, the conventional binary symbols. The correlation

$$\rho_{ij} = \frac{1}{N}\sum_{\mu=1}^{N} \xi_\mu^i \xi_\mu^j = \frac{1}{N}\sum_{\mu=1}^{N}(1-2x_\mu^i)(1-2x_\mu^j)$$

$$= \frac{A_{ij} - D_{ij}}{N} = \frac{N-2D_{ij}}{N}$$

Where A_{ij} is the No. of times the corresponding symbols of the ith and jth words are in agreement, and D_{ij} is for disagreements.

For any given value of $L = 2^n$ there are, in general, many different orthogonal codes. Different members of this class are then evaluated according to their sync. properties on the criterion, that the cross-correlation between any out of phase sequence received and any of the possible in-phase sequences is uniformly small.

Since no constraint is to be placed on the sequence of the words transmitted, the words may be transmitted in such a way that the maximum ρ_{ij} occurs with high regularity. Consequently, it is the maximum value of this ρ_{ij} that is to be minimized. Thus if $|\rho|_{max}$ is the maximum absolute value of the correlation between a code word and a sequence formed from the overlap of two code words, it is desired that

$$|\rho|_{max} = \left|\frac{N-2D}{N}\right|_{max} \text{ be a min., and hence that}$$

$$\min(D_{max}, N-D_{max}) = \rho_N \text{ be a max.}$$

7.52 Orthogonal self-synchronizing codes

Consider now a binary encoding represented by a matrix A, the rows of which form the code words. It will be observed that the correlation between any two rows is unaltered by any arbitrary permutation or complimentation of the columns of A. But if

$a = \alpha_1, \alpha_2, \ldots, \alpha_N$; $b = \beta_1, \beta_2, \ldots, \beta_N$ and $c = \gamma_1, \gamma_2, \ldots, \gamma_N$.

are three code words of A, it is evident that the correlation between

$\alpha_1, \alpha_2, \ldots, \alpha_N$; $\beta_K, \beta_{K+1}, \ldots, \beta_N$ and $\gamma_1, \gamma_2, \ldots, \gamma_{K-1}$ b,

in general, varies when the pth and qth elements of these rows are interchanged. Thus there is a large class of elementary operations on A which leave it invariant as far a c i to operation in the two emission mode is concerned but which may result in quite different codes from the sync. point of view. In the special case of orthogonal codes there is another such operation which should be noted. Since the correlation between any two code words is zero in this case, the dictionary resulting when any or all of the code words are complemented remains orthogonal. This operation, however, evidently could alter the above mentioned asynchronous correlation.

Suppose two orthogonal codes A and B, containing M and N words, respectively, are known to exist and to have the property that corresponding biorthogonal code AV(-A) is such that $M > o$ and BV(-B) such that $N > 0$. Then consider the construction $C = (A \times B) \cup [-(A \times B)]$ where x is the kronecker product defined as follows :-

$$A \times B = (a_{ij}) \times (b_{km}) = \begin{bmatrix} a_{11}B & a_{12}B & \cdots & a_{1M}B \\ \vdots & & & \vdots \\ a_{M1}B & a_{M2}B & \cdots & a_{MM}B \end{bmatrix} \quad \cdots (7.4)$$

A is an MM matrix and B is an NN matrix. Here Aij and Bkm are either +1 or - 1. Let α_j denote the jth row of A and β_k represent the kth row of B. Then A x B

Consider any two arbitrary rows of (7.4), viz. $a_{i1}\beta_k, a_{i2}\beta_k, \ldots a_{iM}\beta_k$ ($a_{j1}\beta_m, a_{j2}\beta_m, \ldots a_{jm}\beta_m$

of matrix $\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1M} \\ \vdots & & & \vdots \\ a_{M1} & a_{M2} & \cdots & a_{MM} \end{bmatrix} \begin{bmatrix} \beta_1 \\ \vdots \\ \beta_N \end{bmatrix}$

Then if $k \neq m$ these two rows are certainly orthogonal due to the orthogonality of the rows of B.

e.g. (7.4) can also be written as

$$A \times B = \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_M \end{bmatrix} \begin{bmatrix} b_{11}, & b_{12}, & \cdots, & b_{1N} \\ \vdots & & & \\ b_{N1}, & b_{N2}, & \cdots & b_{NN} \end{bmatrix} \quad \ldots (7.5)$$

any two rows of (7.5) are

$$\alpha_i b_{k1}, \ \alpha_i b_{k2}, \ \text{---}, \ \alpha_i b_{kN}$$

$$\alpha_j b_{m1}, \ \alpha_j b_{m2}, \ \text{---}, \ \alpha_j b_{mN}$$

which are also orthogonal if $i \neq j$, due to the orthogonality of the rows of A. But an inspection of (7.4) and (7.5) quickly reveals, there are no two distinct rows of A&B for which both $i = j$ and $n = k$. Hence all rows of A x B are mutually orthogonal.

The construction C, (A x B) U(-A x B)) is then a biorthogonal code in which the following represents a typical word:

$$\gamma_k = \pm \beta_i \ , \pm \beta_i \ , \ \ldots \ , \pm \beta_i \quad (N \text{ terms})$$

For all binary orthogonal dictionaries containing $N = 2^n$ words note that $2^{n-4} \times 2^4 = 2^n$ and that, since codes exist with a value for $n = 4, 5, 6, 7$ (No such codes exist for values of $n < 4$), they can be obtained for all larger n by recurrence. Also no smaller dictionary of less than $2^8 = 256$ words can be formed by this method.

Example

The codes are of the form

C = CII BII

Where B_{2N} is generated from BII in the manner which described earlier (7.3), and the product indicates that each column of BII is multiplied by the corresponding component of N-tuple CII. The matrix B4 is that orthogonal code given earlier (7.2). Thus it remains only to list the N-tuples CII used to obtain the indicated values of PN.

Ex.1 N = 16, p16 = 2

C_{16} = 1 1 −1 1 1 1 −1 −1 −1 −1 1 −1 1 −1 −1 −1 .

Ex. 2 N = 32, p32 = 6

C_{32} = −1 1 1 1 −1 −1 1 −1 −1 −1 1 −1 1 −1 1 1 1 1 −1 1 1 −1 1 −1 −1 −1 1 1 1 1
−1 −1 −1 −1 .

N	pN
16	2
32	6
64	14
128	34

Table 7.1

Table (7.1) summarizes the construction of codes for the 4 values of n and the values of pN attained by them. Note that, for N = 128, $|\rho|_{max} \leq 15/32$

Thus the difference between the in-phase and max. out-of-phase correlations is approximately one-half the value obtainable with a pseudo-noise sequence. However, as soon as sync. is obtained, these

codes are able to transmit information without any change in the communication system, a statement which certainly does not apply to the p-n sequences.

CONCLUSION

Coding of information into sets of sequences characterised by low cross-correlation coefficients has the effect of reducing the error probabilities at the cost of expanding the bandwidth for a fixed rate of transmission. If the time allotted per bit is T secs. and the No. of bits per code word is n, the transmission rate is $\frac{1}{T}$ bits/sec or $= \frac{1}{nT}$ words/sec and the effective bandwidth is $\frac{2^n}{nT}$ c/s for orthogonal codes and $\frac{2^{n-1}}{nT}$ c/s. for biorthogonal codes.

If five bits of information are to be sent with a word error probability of 10^{-3}, the use of a bi-orthogonal code word will reduce the required

$$\frac{\text{received signal energy/bit}}{\text{noise power/bandwidth}}$$ ratio by 5 db.

under that required for similar performance with bit-by-bit detection. If 10 bits are to be sent with the same word error probability, biorthogonal encoding reduces the ratio required without encoding by 5 db. orthogonal codes are very nearly as effective as bi-orthogonal codes for $n > 5$ but require twice as much bandwidth.

Much work remains to be done in the investigation of codes with self synchronising properties. The results obtained with bi-orthogonal codes tend to indicate, however, that this may be quite a practical method for achieving self synchronisation.

APPENDIX I

MATCHED FILTER

Definition

Let s(t) be any physical waveform and its Fourier transform (or spectrum) be $S(j2\pi f) = \int_{-\infty}^{\infty} s(t)\, e^{-j2\pi ft}\, dt$ (A-1)

Then a filter which is matched to s(t) is, by definition, one with impulse response $h(t) = K s(\Delta - t)$ (A-2)

where K & T are arbitrary constants.

Transfer function of the matched filter

$$H(j2\pi f) = \int_{-\infty}^{\infty} h(t)\, e^{-j2\pi ft}\, dt$$

$$= K \int_{-\infty}^{\infty} s(\Delta - t)\, e^{-j2\pi ft}\, dt$$

$$= K e^{-j2\pi f\Delta} \int_{-\infty}^{\infty} s(t')\, e^{j2\pi ft'}\, dt'$$

which from (A-1) becomes

$$= K S(-j2\pi f)\, e^{-j2\pi f\Delta} = K S^*(j2\pi f)\, e^{-j2\pi f\Delta} \quad \cdots (A-3)$$

i.e., except for a possible amplitude and delay factor of the form $Ke^{-j2\pi f\Delta}$, the transfer function of a matched filter is the complex conjugate of the spectrum of the signal to which it is matched. For this reason a matched filter is often called a conjugate filter.

APPENDIX II

BARKER SEQUENCES (OR CODES)

These are sequences of numbers x_i having each $x_i = \pm 1$ and possessing the auto correlation function

$$\sum_{i=1}^{n-k} x_i x_{i+k} = C_k = \begin{cases} 0, \pm 1 & \text{for } k = 1, 2, \ldots, N-1 \\ N & \text{for } k = 0. \end{cases}$$

The only known solutions are sequences of length N = 1, 2, 3, 4, 5, 7, 11, 13.

For N even: we must have

$$C_k + C_{N-k} = \sum_{i=1}^{N} x_i x_{i+k} = 0 \qquad (k \geq 1)$$

Then, since $\sum_{i=1}^{N} x_i^2 = N$ we have

$$\sum_{k=0}^{N-1} \sum_{i=1}^{N} x_i x_{i+k} = N$$

$$\sum_{k=0}^{N-1} \sum_{i=1}^{N} x_i x_{i+k} = \sum_{i=1}^{N} x_i \sum_{j=1}^{N} x_j = N$$

$$\text{or } \sum_{i=1}^{N} x_i = \pm\sqrt{N}$$

Since $\sum_{i=1}^{N} x_i$ is an integer we must have N a perfect square (except N = 2), or the Barker codes of even length must be a perfect square.

It has been verified that there is no Barker code of length 16. This leaves N = 36, 64, 64 as the only possibilities for $N < 100$, which is about the limiting length for practical usefulness.

APPENDIX III

CORRELATION DETECTION

Basic communication system model

If the noise is stationary, white and gaussian, the probability computer consists of 2^n correlators (Fig. A-1.) which multiply the incoming signal by each of the 2^n stored or locally generated replicas of the possible transmitted words, integrate over the transmission interval, and are sampled at the end of this time. The output of the kth correlator, which corresponds to the kth word x_k, is

$$\int_0^{nT} x_k(t)\, y(t)\, dt \quad , \text{ where } \quad y(t) = x_m(t) + N(t)$$

$x_m(t)$ is the received signal, and N(t) is the channel noise (Fig. A-2). If the 2^n words were a priori all equally likely to be transmitted with equal energy, i.e., $P(x_i) = P(x_j)$ and

$$\int_0^{nT} x_i^2(t)\, dt \quad = \int_0^{nT} x_j^2(t)\, dt \quad \text{for all } i \text{ and } j, \text{ then}$$

the conditional probability that was sent, given that y was received, is proportional to the exponential of the output of the kth correlator.

$$P(x_k/y) \simeq \exp \int_0^{nT} x_k(t)\, y(t)\, dt \qquad \ldots\ (A\text{-}4)$$

The decision device then examines all the correlator outputs and selects the waveform $X_k(t)$ corresponding to the maximum correlator output. This is known as maximum likelihood detection and can be shown to minimize the probability of error when all the signals are sig equally likely and contain equal energies.

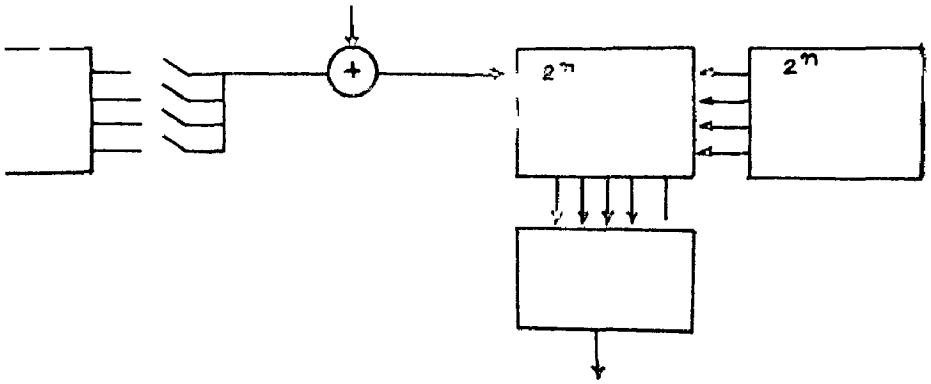


FIG A-1

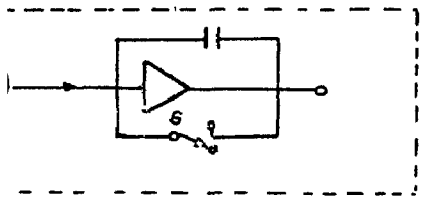


FIG A-2

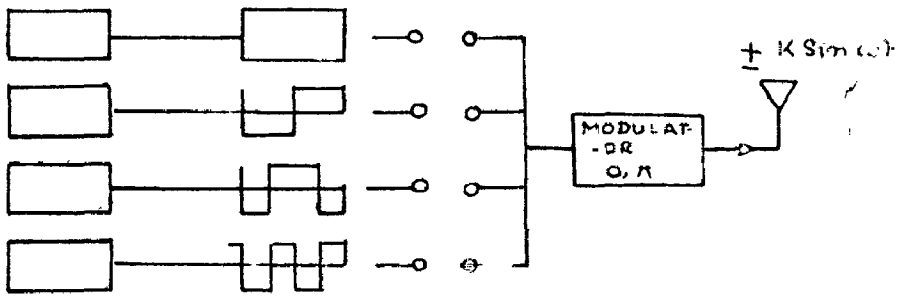


FIG - A-3

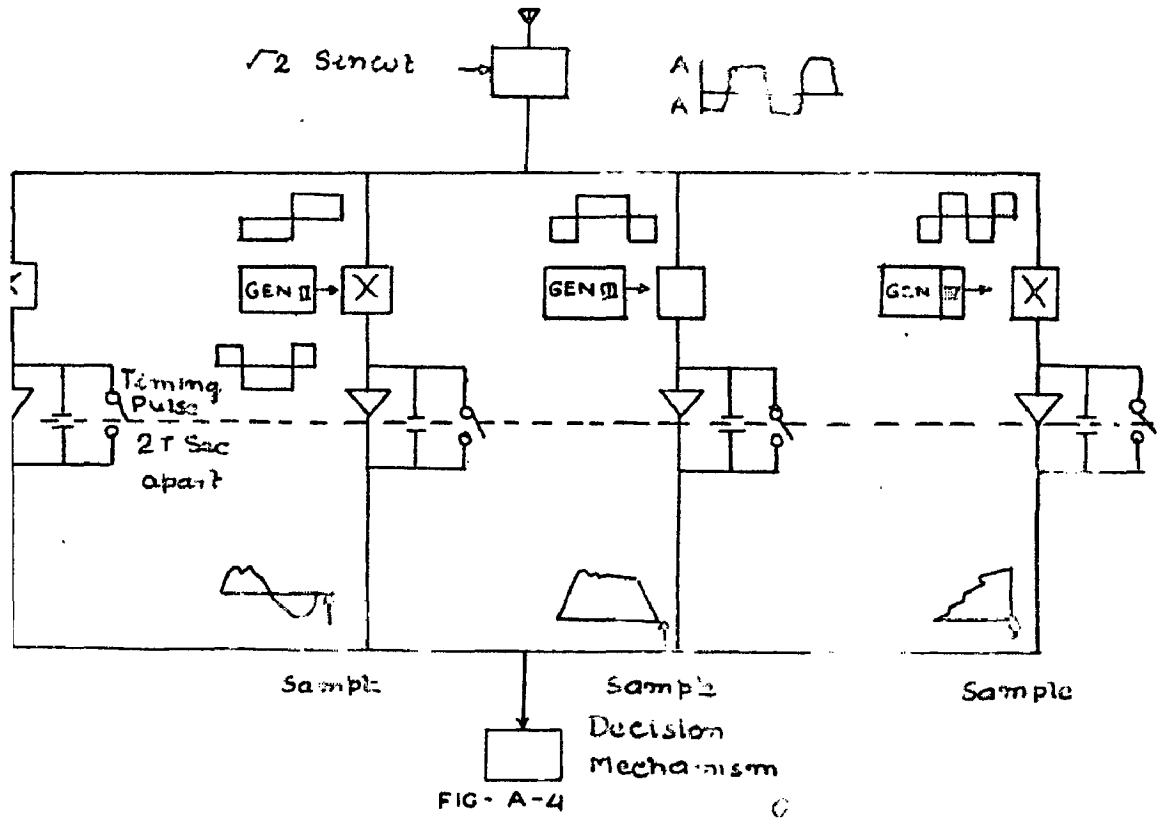


FIG - A-4

In order to achieve low probability of error, the cross-correlation coefficients among all pairs of words should be made as low as possible.

$$\rho = \frac{\int_0^{\lambda T} x_i(t)\, x_j(t)\, dt}{\left[\int_0^{\lambda T} x_i^2(t)\, dt \int_0^{\lambda T} x_j^2(t)\, dt\right]^{1/2}} \qquad \cdots (A-5)$$

The least possible value of ρ is -1. However, this is only when No. of the words in the set is two ($n = 1$) or ($2^n = 2$). In this case, if $x_1(t) = -x_2(t)$, $\rho = -1$ and the words are said to be antipodal. If all ρ's are zero the set of words is then said to be orthogonal.

Blocks of two bits of information are transmitted by selecting one of a set of 4 binary code words. This set is orthogonal since the words switch between $+1$ and -1, and it is easily verified that

$$\int_0^{2T} x_i(t)\, x_j(t)\, dt = 0 \qquad \text{for } i \neq j$$

Phase modulation of Kilocycles by π radians when the carrier is at -1 level is equivalent to amplitude modulation of the carrier by $+1$'s and -1's.

At the receiver, the noisy signal is demodulated and fed to 4 correlators. Only the I-f- components of these inputs is shown in (Fig. A-4). Actually the component contained at a frequency of 2cycles/sec. is eliminated by the integrator provided T is a multiple where n is the No. of bits/ word.

Because the code words are orthogonal, the outputs of all correlators, except the one corresponding to the word sent, are zero in the absence of noise. If this were not the case, the noise free output of the ith correlator would be proportional to

$\int_0^{2T} x_i(t)\, x_j(t)\, dt$ when the jth word was sent.

It should be noted that multiplication of the additive noise by the locally generate words (arbitrarily by + 1 and -1) does not alter its white gaussian statistics since it does not alter the 1st order distribution, nor does it render them correlated.

In general, if n bits are transmitted as one word, the integration time is nT. The integrate and discharge filter is assumed to produce an attenuation of 1/nT. Thus the signal will produce an output at time nT of e(nT) = A provided that nT is a multiple of $\pi/2$.

APPENDIX IV

Shift Register Codes

Shift registers with linear modulation feed back logic produce codes which have two level autocorrelation functions. If the register has length n and the code is of maximal length, 2^n-1, the lower level will be $-\frac{1}{2^n-1}$ (Fig.). Thus a set of 2^{n-1} codes with uniform negative pij can be constructed by taking all shifted replicas of one maximal length shift register sequences, e.g., a set of seven code words can be generated by taking all possible shifts of the sequence from a 3 stage shift register with linear logic. The eighth code word in this fig. is the 0 vector (0000000). The pij among all possible pairs is

1 1 0 1 0 0 1
1 1 1 0 1 0 0
0 1 1 1 0 1 0
0 0 1 1 1 0 1 ... (A-6)
1 0 0 1 1 1 0
0 1 0 0 1 1 1
1 0 1 0 0 1 1

Shift registers can be used to generate orthogonal and biorthogonal codes quite simply, e.g., if a zero is added to every word of the set of Fig.(A6)- and to the 0 vector, a set of eight orthogonal code words is obtained. By taking the complemented out ut of the shift register, the complementary orthogonal code set is also obtained.

Orthog. code set

0 1 1 0 1 0 0 1

0 1 1 1 0 1 0 0

0 0 1 1 1 0 1 0

0 0 0 1 1 1 0 1

0 1 0 0 1 1 1 0

0 0 1 0 0 1 1 1

0 1 0 1 0 0 1 1

0 0 0 0 0 0 0 0

This example can be generalised to any No. of bits. Note that this is not the same set as that in ref. 7·4.

To demonstrate how elegantly shift register codes can be used, consider the case in which the sequence 1001 is to be transmitted by a bi-orthogonal code sequence. The 1st digit is transmitted immediately, while the digits 001 are loaded from right to left into the register of (fig. 5·4), which is made to circulate, and the complemented output digits of the shift register, are transmitted. Thus the whole transmitted sequence is 11100010, one of the words in the above set. If the 1st digit had been a zero, the uncomplemented output digits of the shift register would have been transmitted. Hence, each possible combination of four binary digits would generate a different word in the set.

oooooo

BIBLIOGRAPHY

1. Balakrishnan, A. V. "A contribution to the sphere-packing problem of communication theory", J. Math. Anal. Appl; Dec., 1961.

2. Barker, R. H. "Group Synchronizing of binary digital systems", in "Communication Theory", W. Jackson, Ed., Academic Press, Inc., New York, N.Y. pp. 273-287; 1953.

3. Birdsall T. G. and Ristenbatt, M.P. "Introduction to binary shift Register Generated Sequences", University of Michigan Research Institute, Ann Arbor., Tech. Dept. No. 90; Oct., '58.

4. Black, H.S. "Modulation Theory", D. Van Nostrand Company, Inc., Princeton, New Jersey, Feb., 1960.

5. Davis, C. G. "An Experimental PCM system for short-haul Trunks", The BSTJ 1, June. 1962.

6. Davis T. L. and Doherty T.H. "Widely separated clocks with μ-Sec. Sync. & Independent Distribution system", IRE Trans. on space Electronics and Telemetry, Vol. 8 -6, Sept.-Dec., 1960 pp 138-46.

7. Dutka J. and Neverhoff A.A. "Synchronization of pulse Trains" N.C.A. Rev., Vol. 12, pp 410 419; Sept.19

8. Eastman, W.L. and "On Synchronizable and Self-synchronizable

IRE Trans Inform. Theory (IT),
Vol. IT-1?, No. 4, 351-6 (Oct. 1954).

9. J. O. Edson — United States Patent 2, 457,906, Jan., 4, 1949 (for Mobile Trans. systems).

10. Fano, R.M. — "Communication in the ~~reduce~~ presence of additive noise (gaus ian)" in "Communication Theory", W. Jackson, Ed., Academic Press, Inc., New York, N.Y. pp 169-182; 1953.

11. Fano R. M. — "Transmission of Information", M.I.T. Press, Cambridge, Mass., and John Wiley & Sons, Inc., New York, N.Y., pp 148-157, 1961

12. Fine N.J. — "Classes of periodic sequences", Illinois J. Math., Vol. 2, pp 285-302; June 1958.

13. Gilbert E.N. — "Sync. of Binary Messages" IRE Trans. on Information Theory pp 470-7, Sept., 1960.

14. Gilbert E.N. and Moore E.F. — "Variable length Binary encodings", BSTJ, Vol. 38, pp 933-67; July, 1959.

15. Gouldrup, S.V. — "Sequences with Randomness properties" GlennL. Martin Co. Baltimore, Md. Terminal Progress report. Under contract Ref. No. 63948; June 1955.

16. Golomb S.W. Davey J.R., Reed I.S., Vantreese E. . Stiffler J.J., "Synchronization IEEE Trans. on comm. systems, Vol. CS-11 No. 4, pp481-91, Dec. 1963.

17. Golomb, S.W. & Gordon, B. "Codes with Bounded sync. delay", Information & Control (USA), Vol. 8, No. 4, 355-72 (Aug., 1965).

18. Golomb S.W., Gordon B., and Welch L.R. "Comma free codes" Canadian J. Math., Vol. 10, No. 2 pp 202-9; 1958 .

19. Golomb S.W. & Welch L.R. "Non linear shift register sequences", Jet propulsion labs. Pasadena Calif Tech No. 20-149; Oct., 1957.

20. Golomb S.W., Welch L.R. and Delbruck M' "Construction and properties of Comma free codes" Biol. Med. Danskee Vid Selsk. Vol. 23, No. 9 pp 1-34; 1958.

21. Inose, H., Takasi, H and Aoki, Y. A method of frame separation in the time division multiplexed delta Modulation system. IEEE Trans. on communication system, Vol. CS-11 No. 4 Dec., 1963.

22. Jennings V.A. and Miller C.C. A linear autocorrelator for synchronization of binary coded messages. IEEE Trans. on common and electronics, pp 151-8, May 1963.

23. Lerner R.M. "A matched filter detection system for doppler shifted signals" IRE Trans. on Inf. Th. Vol. IT-3 pp 373 June 1960

24. Richard C. Mackey "A synchronized pulse communication system with pseudorandom interpulse period", IRE Trans. on "Communications systems vol. C.S. 10 pp 109-113, March 1962.

25. Manley, "Synchronization for the PCM Receiver" Bell Labs. Rec. Vol. 27, pp 65 66 Feb., 1949.

26. Middleton, D. and Van Meter, D. Detection and extraction of signals in noise from the point of view of statistical detection theory. Journal Soc. Ind. and Appl. Maths. Vol. 3, Pt. I. pp 192-253, Dec. 1955 Vol. 4, pt. 2, pp 86-119, June 1956.

27. Nakamaru Y. & Kaneko H. "Synchronization system for digital transmission" J. Inst. Elec. Communication Engrs. (Japan), Vol. 43, pp. 1388-1396 Dec., 1960.

28. Quelon P. Notes on sync. for burst error correcting codes, J. Inst. Elect. Commun. Engrs. Japan, Vol. 47, No. 6 pp. 925-32, June 1964.

29. Rauch, Lawrence, L. "Considerations on synchronization for PCM Telemetry" IEE Trans. on Space Electrons. & Telemetry Vol. Set - pp 95-98; Sep. Dec. 1960.

30. Reed. I.S. A class of multiple erro. correcting codes and the decoding scheme, IEE Trans. on Inf. th., Vol. I^{4}-4 pp 38-49, Sep. 1954.

31. Reed. R.S. and Pett rburg, L.W. Comm. with orth. polyphase signals over a noisy channel with Doppler Freq. shift, IEEE Trans. Com. Technol. (USA), Vol. Com-12, No. 4, pp 116-18 (Dec. 1964).

32. Rhodes, Donald R. "On some practical aspects of the ideal group sync. process", IEE Trans. on "Communication System" Vol. CS-10, pp 222-9, June 1963.

33. Riordan John. "An Introduction to Combinatorial Analysis", John. Wiley and Sons, Inc. New York, N.Y. 1958.

34. Sago, G.E. Serial Sync. of Pseudonoise systems, IEEE Trans. Commun. Technol (USA), Vol. COM-12, No. 4, 123-7, Dec. 1964

35. Schreiber, F. Lukas, E and Zocker, P. — An error correcting data transmission system with block by block sync. operation over telephone channels, IEEE Internat. Convention Record (USA) Vol. 12, Pt. 5, pp 72-82, 1964.

36. Seaver — "PCM Synchronization" Proc. Natl. Telemetry Conf. Santa Monca Calif, Instrumentation Society of America" New York, N.Y. pp 251-8 1960

37. Stiffler, J. — "Self Synchronizing Binary Telemetry Codes", Ph.D. dissertation, Deptt. of Elec. Engrg., Calif, Inst. Tech. Pasadena, pp 117-121 1962.

38. Stiffler, J.J. — "Synchronization Methods for Block Codes", IRE Trans. on I.T. 1962 International Symposium on Inf. Theory, 525-34, Sept. 1962.

39. Stiffler J.J. — "Synchronization of Telemetry Codes". IEEE Trans. on "Space Electronics & Telemetry" Vol. SET-8, pp 112-117 June 1962.

40. Turin, G.L. — "An introduction to matched filters" IRE Trans. on Information Theory, Vol. IT-6 pp. 311-329; June 1960

41. Vanhorn, J.T. "A theoretical sync. system for use with noisy digital signals". IRE Trans. comm. System (USA), Vol. CST-12, No. 3, 82-90 (Sept. 1964)

42. Viterbi, A.J. "On coded phase coherent communications" IRE Trans. on space electronics and telemetry, Vol. SET-7 pp 3-17; March '61.

43. Woodward, "Probability & Information Theory with Applications to Radar" Mc. Graw-Hill Book Co., Inc., New York, N.Y. pp 62-90 1955.

44. Woodward & Davis I.... "Information theory & Inverse Probability in telecommunications" Proc. IEE Vol. 99, pt. 3, pp 37-45; 1952.

45. Zierler N. "Several Binary Sequence Generators", MIT Lincoln Lab., Lexington, Mass. Tech. Report No. 95, Sep. 12, 1955.

oooo