ERROR DETECTION AND ERROR CORRECTION UNDER THE CONDITIONS OF QUARTERNARY DECISION LOGIC TECHNIQUES

A. BROTHMAN
Consultant
Sangamo Electric Co.
Transitel Division

C. YANIS, S. J. HALPERN and A. H. MILLER
Sangamo Electric Co.
Transitel Division

Summary The hardware and theory of a multi-threshold bit decision technique called Quarternary Decision Logic are described. Quartenary Bit Decision Logic results in two simultaneous decisions on each received bit of a binary digital transmission: (1) a binary status decision; and, (2) a reliability decision which reflects on the presence/absence of multilation in the bit. Both decisions are based on a Shannon Integration of the received information over the whole bit interval.

The ability to assess bit mutilation is then used to develop adjustable security-enforcing restraints on error correction and the receiving process itself. These restraints are developed by a Word Security Logic which keeps a “mutilation count” on each received word, The “mutilation count” per word results in a “Correction Permit/Inhibit” and a “Receiving Permit/Inhibit” output on each word. The “Correction Permit/ Inhibit” output bars error correction when the risk of a spurious correction is high. The “Receiving Permit/Inhibit” output blocks receiving when the risk of a direct evasion of security is high.

The improvement in bit decision security and the improvements in security against spurious correction and direct evasions of Error detection are evaluated quantitatively in comparison to conventional single-threshold techniques, These improvements enable secure operation with lower redundancy coding systems because of the information gain which Quarternary Decision Logic provides. The possible contributions of Quarternary Decision Logic to self-adaptive data transmission systems and to automatic line equalization are explored in the section entitled “Conclusions”.

Introduction The principal hazard to reliance on coding-based error correction is the lack of information on the extent of mutilation of a transmission. If the mutilation exceeds the code's radius of detection, the threat of a direct evasion of security is posed; and, if the mutilation exceeds the code's radius of non-spurious correction, the threat of a spurious correction is posed. [1] To minimize these hazards, codes of higher Hamming distance properties are frequently used. These, however impose the alternatives of a reduced information rate or a requirement for increased transmission speed. Realizing that the bounding relationship between code length (n_B) and the code's minimum distance property (n_d) is

$$n_d \leq \begin{cases} \frac{n_B}{2}, & \text{for } n_B \equiv 0 \bmod 4 \\ \frac{n_B-1}{2}, & \text{for } n_B \equiv 1 \bmod 4 \\ \frac{n_B-2}{2}, & \text{for } n_B \equiv 2 \bmod 4 \\ \frac{n_B+1}{2}, & \text{for } n_B \equiv 3 \bmod 4 \end{cases} \tag{1}$$

the cost in redundancy of improving (n_d) becomes apparent. [2] The further relationships between (n_d) and the code's radius of correction (r_c) and/or its radius of non-spurious correction (r_s) reinforce the magnitude of the penalty of greater intrinsic coding security. These relationships are:-

$$r_c \leq \frac{n_d - 1}{2} \tag{2}$$

and

$$r_s = n_d - r_c - 1 \tag{3}$$

To avoid the penalties of increased intrinsic coding security and yet to execute error detection and error correction under maximum security conditions involves a means of detecting transmission mutilation, Further such a goal requires that the "multilation count" per word or per block be fed back in the form of automatic receiving or correction restraints when excessive mutilation is encountered, A means of achieving a "mutilation count" and of generating rational security-enforcing restraints is offered in this paper. It is called a Quarternary Decision Logic device.

Causes of Mutilation The principal causes of bit mutilation are:-

a) the limitations on waveform fidelity imposed by bandpass limitations
b) relative amplitude distortion applied to information sidebands across the link's bandpass
c) differential angular retardation applied to information sidebands within the link's bandpass
d) "white noise" corruption of information sidebands and,
e) impulse, dropout, and burst noise corruption of information sidebands.

The major contribution to mutilation by Item (a) is to deprive a binary digital waveform of those spectral components which gives the source waveformits unambiguous character.[3] Because of this type of mutilation, the re-construction of the waveform at the receiving end of a transmission system is made dependent on decision thresholds, The mutilation contributed by Item (b) alters the power distribution in information sidebands, and thus further complicates the task of envelope recovery by altering both the front and back porches of inter-state binary transits. The differential delays which the link imposes on contemporaneously-generated information sidebands as per Item (c) deprives bit decisions in any one bit-interval of pertinent information, and then introduces the delayed information into decision intervals to which the sidebands are alien. Amplitude equalization and delay equalization networks when properly tailored can condition a link to minimize the effects of Items (b) and (c). The effects of Item (a) are beyond compensation except as bit-sampling and bit-decision methods at the receiving end are optimized.

The effects of the noise phenomena in Items (d) and (e), like the limitations imposed by Item (a), are unavoidable, but are less subject to compensation by optimized decision techniques because the corruption effects are stochastic. The influence of noise corruptions in Items (d) and (e) is to introduce alien spectral components, to deprive source components of their original power by cancellation effects, and to falsely strengthen source components by spurious construction. For all three basic types of binary receiving modems, the probability (p_w) of Nyquist Interval [4] error to “white noise” as the corrupting influence is:-

$$P_w = A \frac{E_N}{E_S} e^{-b\left(\frac{E_S}{E_N}\right)^2} \tag{4}$$

where

$$A = \begin{cases} \frac{1}{\sqrt{2\pi}}, & \text{for coherent FSK modems} \\ \frac{\sqrt{2}}{\pi^{3/2}}, & \text{for PSK modems} \\ \frac{2}{\sqrt{\pi}}, & \text{for AM modems} \end{cases} \tag{5}$$

and where

$$b = \begin{cases} 1/2, & \text{for coherent FSK modems} \\ \frac{\pi^2}{4}, & \text{for PSK modems} \\ 1/8, & \text{for AM modems} \end{cases} \tag{6}$$

In Eq. (4), E_N = the rms "white noise" voltage, and E_S = the rms signal voltage.

Relative to impulse, dropout, and burst noise, the deviation of the probability (P_i) of Nyquist Interval error by this non-Gaussian noise begins with the definition of the transfer function of the information channel's bandpass filter. Let this property be matched to the two-sided average power spectrum $\overline{P}(\omega)$ of a binar di ital transmission where:-

$$\overline{P}(\omega) = \frac{E_s^2 t_b}{2}\left[\left(\frac{\sin\frac{\omega_c+\omega}{2}t_b}{\frac{\omega_c+\omega}{2}t_b}\right)^2+\left(\frac{\sin\frac{\omega_c-\omega}{2}t_b}{\frac{\omega_c-\omega}{2}t_b}\right)^2\right] \tag{7}$$

defines $\overline{P}(\omega)$. In Eq. (7), $\overline{P}(\omega)$ = the average sideband power at anangular displacement (ω) from (ω_c). ω_c = the angular carrier frequency, and t_b = the time-width of a singlet bit. For the spectrum in Eq. (7), a wellmatched bandpass filter would exhibit the transfer function defined by:-

$$H(\omega) = \beta\left[\frac{\sin\frac{\omega_c+\omega}{2}T}{\frac{\omega_c+\omega}{2}T}+\frac{\sin\frac{\omega_c-\omega}{2}T}{\frac{\omega_c-\omega}{2}T}\right]e^{-j\omega t} \tag{8}$$

where:-

β = the filter's gain factor
T = the sampling-time applied to the filter's output
t' = elapsed sampling-time

When a signal element of amplitude (A_N) and duration (t_N) is applied to a filter defined by Eq. (8), the signal voltage response ($e_s(t)$) is stated by:-

$$e_s(t) = \frac{\beta A_N t_N}{8\pi}\left\{\int_{-\infty}^{\infty}\left[\frac{\sin\frac{\omega_c+\omega}{2}T}{\frac{\omega_c+\omega}{2}T}\right]^2 e^{j\omega(t-c-t')}\,d\omega\right. \tag{9}$$

$$\left.+\int_{-\infty}^{\infty}\left[\frac{\sin\frac{\omega_c-\omega}{2}T}{\frac{\omega_c-\omega}{2}T}\right]^2 e^{j\omega(t-c-t')}\,d\omega\right\}$$

where:-

t = elapsed signal element time

and

c =time of transmission of the signal element

Setting t_N = T and at t-c = t', Eq. (9) is readily solved to yield

$$e_s(t) = \beta A_N \tag{10}$$

On the other hand, let there be an impulse, dropout, or burst input of amplitude (A_i) and duration (t_i) to the filter as per Eq. (8), and, if this event occurs at a time displacement (t") with respect to the signal element the noise response (e_i (t)) is stated by:-

$$e_i(t) = \frac{\beta}{2\pi} \int_{-\infty}^{\infty} A_i t_i e^{-j\omega t''} H(\omega) e^{j\omega(t-c)} d\omega \tag{11}$$

which, when combined with Eq. (8) in defining H(ω), yields

$$e_i(t) = \frac{\beta A_i t_i}{2\pi} \left\{ \int_{-\infty}^{\infty} \frac{\sin \frac{\omega_c+\omega}{2} T}{\frac{\omega_c+\omega}{2} T} e^{j\omega(t-c-t'-t'')} d\omega + \int_{-\infty}^{\infty} \frac{\sin \frac{\omega_c-\omega}{2} T}{\frac{\omega_c-\omega}{2} T} e^{j\omega(t-c-t'-t'')} d\omega \right\} \tag{12}$$

Again, setting t-c = t', Eq. (12) is readily solved to yield

$$e_i(t) = \frac{2\beta A_i t_i}{T} \cos \omega_c t'' \tag{13}$$

Towards the goal of evaluating the probability ($\overline{P}_i$) of an impulse/dropout/ burst caused error, the ratio of $\left(\frac{e_i(t)}{e_s(t)}\right)$ produces a useful vector, namely

$$\frac{e_i(t)}{e_s(t)} = \frac{2A_i t_i}{A_N t_N} \cos \omega_c t'' = \alpha \cos \theta \tag{14}$$

where (T) in Eq. (13) is set equal to (t_N) and

$$\frac{2A_i t_i}{A_N t_N} = \alpha$$

and

$$\omega_c t'' = \theta$$

Examining the vector ($|e_s(t) + e_i(t)|$) which would become the input to the Limiter-Discriminators-Demod cascade of a receiving modem in the event of "coincident"

signals and noise impulses , it is apparent that there are values of (αcos ϕ) at which spurious construction would occur, and values of (αcos ϕ)at which cancellation would be true. To evaluate (pi the bounds within which $|e_s(t) + e_i(t)|$) would and would not permit signal recovery in any given modem must be stated. We do this below for the case of FSK and PSK modems, for the reason that these two basic types of modems are the likeliest to be used in high security data transmission sets.

In the theoretical binary-level FSK receiving modem, signal recovery is possible as long as

$$|e_s(t) + e_i(t)| > |e_i(t)| \tag{15}$$

and, conversely, error will occur when

$$|e_s(t) + e_i(t)| \lessgtr |e_i(t)| \tag{16}$$

Solving Eq. (16) for the lower bound of (α) at which erroring becomes probable we note that b the use of E .(14), we obtain

$$|e_s(t) + (\alpha \cos \phi) e_s(t)| = |(\alpha \cos \phi) e_s(t)|$$

$$1 + 2\alpha \cos \phi + \alpha^2 \cos^2 \phi = \alpha^2 \cos^2 \phi$$

or (17)

$$\alpha = -\frac{1}{2 \cos \phi}$$

Eq. (I 7), we note, is the equation of a straight-line parallel to the j -axis in Fig. 1 and intersecting the real axis at (-1/2, 0). Fig, 1 tutors the conclusion that for a two-level FSK receivin modem

$$P_i = \frac{4\int_{x=1/2}^{\alpha} (\alpha^2 - x^2)^{1/2} dx}{\pi \alpha^2} = \frac{\left[\cos^{-1} \frac{1}{2\alpha}\right] \alpha^2 - \frac{1}{2}\left[\alpha^2 - \frac{1}{4}\right]^{1/2}}{\pi \alpha^2} \tag{18}$$

For the case of a two-level PSK modem, we note that signal recovery is possible as long as

$$|e_s(t)| > |e_i(t)| \tag{19}$$

and conversely that erroring will occur when at one limit

$$|e_s(t) + e_i(t)| = 0. \tag{20}$$

Similarly to the development of Eq. (17), we then obtain

$$1 + 2\alpha \cos\phi + \alpha^2 \cos^2\phi = 0$$

or (21)

$$\alpha = -\frac{1}{\cos\phi}.$$

Again we note that Eq. (21) is the equation of a straight-line parallel to the j-axis in Fig. 2 and intersecting the real axis at (-1, 0). Fig. 2 then urges that for a two-level PSK receiving modern

$$P_i = \frac{4\int_{x=1}^{\alpha} (\alpha^2 - x^2)^{1/2} dx}{\pi\alpha^2} = \frac{1}{\pi}\cos^{-1}\frac{1}{\alpha} - \frac{1}{\pi\alpha^2}(\alpha^2 - 1)^{1/2} \quad (22)$$

Eqs, 4, 5, 6, 12, 18, and 22 are useful in evaluating the Quarternary Decision Logic Method proposed by this paper.

Quarternary Decision Logic Hardware The block diagram of a Quarternary Decision Method Receiving Terminal is shown in Fig. 3. The method consists of:-

a) a full-time sampling of the “mark” and “space” discriminator outputs of a modem over very nearly the entire interval of each bit by a Quarternary Bit Sampling & Bit-Decision Logic
b) the outputting by the QDL Logic of two bit-decisions at the conclusion of each sampling operation:-
    i) a binary status bit-decision which is used to load the Word Receiver
    ii) a “gray’T’clear” fidelity decision which is used by a Word Security Logic to arrive at security decisions for the word receiving interval

and,

c) the outputting by the Word Security Logic of two decisions at the conclusion of eachword receiving cycle:-
    i) a Correction Inhibit/Permit decision to the Word Receiver
    and,
    ii a Receiving Inhibit/Permit decision to the Word Receiver.

Fig. 4 indicates the circuit and logic train by which Operations (a) and (b) are executed. Fig, 5 indicates the circuit and logic train by which Operation (c) is accomplished.

In Fig. 4, the circuit and logic train of the QDL Bit-Decision Logic, the “mark” and “space” outputs of a conventional two-level FSK or PSK receiving modem are inputted to the Q1 -Q2 differential amplifier. Assuming that the “mark” and “space” outputs rise positively from the same quiescent dc levels to the same peak output levels, the Q2-stage

collector output tends toward saturation for as long as the “mark”-output exceeds “space” output by a threshold set by R3’s adjustment. The output from Q2’s collector during such a time is subjected to amplitude limiting by the D1-D2-R5 configuration, and is then applied via the current-limiting resistor R8 to the base of Q3. Q3, which is biased into cutoff by the zener diode D3-resistor R9 string when Q2 is in cutoff, then becomes a current source for the charging of capacitor C1 for the entire period that Q2 is driven into or towards saturation. Accordingly, if the modem’s discriminators output a full-time output over the full bit-interval, the result is, in the best circumstances of a “1”-bit, the voltage ramp shown in Fig. 4's information-diagram. Conversely, if the modem’s output were an ideal “0”-bit, the result over a bit interval would be the “0”→“0” line of the information diagram. In the event of a pulse-per-Nyquist Interval output from the modem’s discriminators, an ideal “1”bit would be represented by the voltage staircase in the information-diagram, while the ideal “0”-bit would again be represented by the “0”→“0” line. And, finally, it follows that non-ideal bits are represented by a partial ascent along the indicated ramp or staircase, as the case may be.

In any case, the charge which is piled up on C1 over a bit-interval is submitted via the Q5-Q6 Darlington emitter follower configuration to three independent thresholded dc amplifier stages represented by the Q7, Q8, and Q9 members. With the Q7, Q8, and Q9 stages thresholded via their emitter bias conditions to impose the ramp or staircase thresholds shown in the information-diagram, the terminal state of the charge voltage on C1 results in a binary bit decision and a bit fidelity decision. These are

a) a "0" status decision if the charge voltage $E < E_B$
b) a "1" status decision if $E \geq E_B$
c) a supplementary "gray"-bit decision if $E_A \leq E \leq E_C$

and d) a supplementary "clear"-decision if $E < E_A$ or $E > E_C$

The results of the decision process are stored in the set-reset flip-flops 1 and 2 by outputs “A”, “B”, and “C” respectively from the Q7, Q8, and Q9 stages during the bit-sampling process. The decision-storing processes are self-evident from Fig. 4.

When, finally, the Receiving Synchronizer indicates the conclusion of a bit interval to the QDL Logic, the front-porch of the input pulse triggers the one -shot multivibrator chain 3 and 4, causing:-

I firstly, a test strobe from 3 by which the binary status and fidelity decisions are strobed from and-gates 5 and 6 to their destinations via signal “Y”

and,

II an ensuing reset strobe (“X”) by which C1 is discharged via the Q4 transistor stage and by which flops 2, and possibly 1 , are reset.

The time-constant of one-shot multivibrator 4 is minimized, and at worst is equal to the envelope rise-time of an incoming bit. In any event, the QDL is thus reset for its next duty cycle.

The Word Security Logic, shown in detail in Fig. 5, follows the main lines of organization of the QDL Bit Decision Logic. Here, "gray"-bit indications from the QDL Bit Decision Logic are driven into limit by the Q7 stage and are applied via capacitor C1 as a pulse input to the base of Q1. Q1, whose emitter-base circuit is normally biased into cutoff via the D1-R5-R6 and D3-R7 configurations, delivers a single-valued step-developing current pulse into capacitor C2 on each pulse output from the Q7 stages. Under this arrangement, the terminal voltage exhibited by the capacitor C2 at the conclusion of a word receiving cycle is a "mutilation count" by which thresholded dc amplifiers Q4 and Q5 are enabled to render their recieving, error detection, and error correction restraint outputs. Thus, if (V) is the terminal charge voltage on C2 and ($E\alpha$) and ($E\Delta$) are respectively the "mutilation count" voltage thresholds for 11correction inhibit" and "receiving inhibit":-

1) correction is permitted if $V < E_{\gamma}$
2) receiving subject to error detection but without the option of error correction is true if $E_{\gamma} < V < E_{\Delta}$

and

3) receiving is blocked totally if $V \geq E_{\Delta}$

The decisions as per (1), (2), and (3) are reached via the actions of thresholded amplifiers Q4 and Q5 on the set-reset flip-flops 1 and 2 in Fig. 5 during a word receiving cycle. After the Word Security Logic's security restraint outputs are used by the Word Receiver, the Word Receiver feeds back an End-of-Program (EOP) pulse by which:- capacitor C2 is discharged via the Q6 stage for its next duty cycle; and, the flip-flops 1 and 2 are reset for their next duty cycle.

Quantitative Benefits Of The QDL Method Receiving Terminal If the curves to which Eqs. (18) and (22) lead are broken into ranges of the α -parameter over which linear averaging of (P_i) is permissible, and if each such range $m \leq \alpha \leq n$ is assigned an anticipated number (n_{mn}) of impulses /dropouts /bursts per unit of time (τ) lying within the range, one is enabled to calculate a probability (P_{IM}) of Nyquist Interval mutilation by these noises from the equation

$$P_{IM} = \frac{1}{4\pi\omega_c \tau} \sum_{mn=\delta_1}^{mn=\delta_2} n_{mn} (\bar{P}_i)_{mn}$$

$(\bar{P}_i)_{mn}$ = the average value of (P_i) for the range $m \lessapprox \alpha \lessapprox n$

δ_1 = the range of (α) beginning with its lower error bound

δ_2 = the range of (α) which terminates with $P_i \approx 0.5$

(23)

Adding to (P_{IM}), the value of (P_w) in Eq. (4) which is appropriate for the dynamic ratio of E_S / E_N and for the modem, one arrives at

$$P_{IM} + P_w = P_M = 1 - q_M \tag{24}$$

where P_M = the probability of Nyquist Interval mutilation due to all noise causes, inclusive of "white noise", and q_M = the probability of a successful Nyquist Interval Transmission.

If then the threshold adjustment conditions in Fig. 4 are such that:-

a) the height of each "clear" zone is equivalent to (t) unmutilated Nyquist Intervals and

b) the height of the "gray"-zone is (h) unmutilated Nyquist Intervals, where h/2 = an integer

it will then follow that if h + t = s

$$P(1/1) = P(0/0) = \sum_{\mu=0}^{\mu=t-1} P_M^{\mu} q_M^{s-\mu} = P(A) \tag{25}$$

$$P(1/G_1) = P(0/G_0) = \sum_{\mu=t}^{\mu=s/2} P_M^{\mu} q_M^{s-\mu} = P(B) \tag{26}$$

$$P(1/G_0) = P(0/G_1) = \sum_{\mu=s/2+1}^{\mu=s-t} P_M^{\mu} q_M^{s-\mu} = P(C) \tag{27}$$

$$P(1/0) = P(0/1) = \sum_{\mu=s-t+1}^{\mu=s} P_M^{\mu} q_M^{s-\mu} = P(D) \tag{28}$$

where:

$P(1/1)$ = probability of a "1"-bit being received in clear -"1" status
$P(0/0)$ = probability of a "0"-bit being received in clear -"0" status
$P(1/G_1)$ = probability of a "1"-bit being received in gray -"1" status
$P(0/G_0)$ = probability of a "0"-bit being received in gray -"0" status
$P(1/G_0)$ = probability of a "1"-bit being received in gray -"0" status
$P(0/G_0)$ = probability of a "0"-bit being received in gray -"1" status
$P(1/0)$ = probability of a "1"-bit being received in clear-"0" status
$P(0/1)$ = probability of a "0"-bit being received in clear-"1" status
$P(A)$ = probability of a "clear"-bit
$P(B)$ = probability of a "gray-but-correct" bit
$P(C)$ = probability of a "gray-and-incorrect" bit
$P(D)$ = probability of an undetected bit error

Several conclusions are immediately possible from Eqs. (25) thru (28). These are:-

i) a descending order of probability of (A), (B), (C), and (D) events respectively according to

$$P(A) > P(B) >> P(C) >> P(D) \tag{29}$$

ii a sharp reduction under QDL methods of undetected bit errors as compared with conventional single-threshold bit decision methods.

We note in connection with Item (ii) that [P(1 /0)]c, the probability of binary bit inversion under conventional single-threshold methods, is indeed stated by:-

$$[P(1/0])_c = [P(0/1)]_c = P(C) + P(D) \tag{30}$$

and that if full benefit is taken of the information gain under QDL methods the probability of undetected bit errors may be restricted to P(D) itself.

Two important utilizations of the information gain under QDL Bit Decision methods are the security-enforcing restraints developed by the Word Security Logic in Fig. 5. The first of these is the increased protection against spurious corrections which is afforded by the “correction inhibit” output of the Word Security Logic. The second is the increased protection against direct evasion of error detection.

In evaluating the first of these protections, let it be true of a data receiving terminal that it is performing error correction, that the (r_s) of its coding is such that $r_s \geq r_c$, and that its Word Security Logic is adjusted to impose “correction inhibit” when the “mutilation count” (n_g) per word (i. e. when the number of “gray”-bits per word) is such that $n_g \geq \lambda$ where $\lambda \leq r_c$. Under these conditions, the probability of a spurious correction, (P_{sc}), is given by:-

$$P_{SC} \approx \sum_{n_g=0}^{n_g=\lambda-1} \binom{n_B}{n_g}\binom{n_B-n_g}{r_S+1-n_g} P^{n_g}(C)\, P^{r_S+1-n_g}(D) \tag{31}$$

We note here that, in view of Eq. (29), the most significant term by far in the right-hand side of Eq. (31) is:-

$$\binom{n_B}{\lambda-1}\binom{n_B-\lambda+1}{r_S-\lambda} P^{\lambda-1}(C)\, P^{r_S-\lambda}(D)$$

whereby we could well reduce Eq. (31) to

$$P_{SC} \approx \binom{n_B}{\lambda-1}\binom{n_B-\lambda+1}{r_S-\lambda} P^{\lambda-1}(C)\, P^{r_S-\lambda}(D) \tag{32}$$

If then $[P_{sc}]_c$ denotes the probability of a spurious correction for the same coding system under conventional single -threshold bit decision conditions, $[P_{sc}]_c$ is given by:-

$$[P_{SC}]_c = \binom{n_B}{r_S+1} [P(C)+P(D)]^{r_S+1} \tag{33}$$

Towards the goal of determining the improvement, Eq. (33) is divided by Eq. (32), yielding

$$\frac{[P_{SC}]_c}{P_{SC}} = \frac{(\lambda-1)!\,(r_S-\lambda)!\,(n_B+1-r_S)!}{(r_S+1)!\,(n_B-1-r_S)!} \; \frac{[P(C)+P(D)]^{r_S+1}}{P^{\lambda-1}(C)\, P^{r_S-\lambda}(D)} \tag{34}$$

But, since the ratio of the factorials in Eq. (34) is very nearly equal to one, and since P(C) + P(D) ≈ P(C) by Eq. (29), Eq. (34) reduces to

$$\frac{[P_{SC}]_c}{P_{SC}} \approx \left(\frac{P(C)}{P(D)}\right)^{r_S-\lambda} \tag{35}$$

indicating a high order of improvement of security against spurious correction.

In the evaluation of the benefits of “receiving inhibit” by the Word Security Logic, let it be true that “receiving inhibit” is imposed when $n_g \geq \epsilon$, where $\epsilon \leq n_d$ the coding system’s minimum distance property. Then if (P_{DE}) is the probability of a direct evasion of the error detection process, (P_{DE}) is given b :-

$$P_{DE} \approx \frac{K}{\binom{n_B}{n_d}} \sum_{n_g=0}^{n_g=\epsilon-1} \binom{n_B}{n_g}\binom{n_B-n_g}{n_d-n_g} P^{n_g}(C)\, P^{n_d-n_g}(D) \tag{36}$$

where (K) denotes the number of ways in which (n_D) bit errors will yield a security-puncturing code set. By far, the most significant term in the right-hand side of Eq. (36) is

$$\frac{K}{\binom{n_B}{n_d}} \left\{ \binom{n_B}{\varepsilon-1} \binom{n_B-\varepsilon+1}{n_d-\varepsilon+1} P^{\varepsilon-1}(C) P^{n_d-\varepsilon+1}(D) \right\}$$

allowing Eq. (36) to be reduced to

$$P_{DE} \approx \frac{K n_d!}{(\varepsilon-1)!(n_d-\varepsilon+1)!} P^{\varepsilon-1}(C) P^{n_d-\varepsilon+1}(D) \tag{37}$$

Noting that if $[P_{DE}]_c$ denotes the probability of a "direct puncture" under single-threshold conditions, it is stated by

$$[P_{DE}]_C = K[P(C) + P(D)]^{n_d} \tag{38}$$

and that division of Eq. (38) by (37) leads to the improvement factor, we arrive at

$$\frac{[P_{DE}]_c}{P_{DE}} = \frac{(n_D-\varepsilon+1)!(\varepsilon-1)!}{n_d!} \left[\frac{P(C)}{P(D)}\right]^{n_d-\varepsilon+1} \tag{39}$$

The improvement is thus again a sharp one.

Conclusions Several extended uses of the "gray"/"clear" bit-reliability decision are of interest. These are:-

a) The direct use of "gray"-bit locations in a tutored correction process
b) the measurement of the time-incidence of "gray"-bits as a key to link perturbation, in particular as a measure of cluster noise" and extended "burst" conditions
c) the development of self-adaptive receiving end control measures during periods of high link perturbation

and

d) the use of "gray"-bits frequency in guiding automatic line conditioning,

The tutored correction use of "gray"-bits involves the test inversion of a "gray"-bit location in a received word if the received word fails to pass error detection. Tutored correction would preferably be subject to the "correction inhibit" and "receiving inhibit" outputs of the Word Security Logic. Such a correction process rests on Eqs. (25) thru (29), is based on the "gray"-bit being a [C]-event as per Eq. (27), and is furthermore based on the Bayes Law choice by which

$$\frac{P(C)}{P(C) + P(D)} \longrightarrow \text{unity.}$$

This use of “gray”-bits could add a correction capability to coding which does nothave intrinsic error correction capabilities,

Among the adaptabilities of “gray”-bits to self-adaptive receiving end optimization is the ability to automatically select alternative values of (λ) and (ϵ) in Eqs. (31) and (36) in response to “gray”-bits frequency measurements. Such an accommodation to link perturbation measurement would provide a self-adaptive security capability to data terminals.

In guiding automatic line conditioning circuitry, a threshold imposed on “gray”-bits frequency would provide an excellent gate-control measure as well as a feedback check on the circuitry’s self-adaptive accommodations, Thresholds on “gray”-bits frequency could also provide a basis for receiving end-to-transmission end feedback measures to control transmission speed andoptimize data security and data transmission rate.

NOTES

1. A code’s “radius of detection” is the maximum number of errored bits per word for which it provides infallible error detection. The ‘tradius of correction” of a code is the maximum number of errored bits per word for which it provides error correction. The Hamming “minimum distance” property of a code is the number of bit-positions in which the two most similar code-sets are distinguished. The “radius of non-spurious correction” is the maximum number of errored bits per word which can be tolerated before correction becomes spurious. For further data on these coding parameters, see:- Brothman, A., Brothman, E. H., Halpern, S. J., Horowitz, L. M., and Reiser, R. D. “The Use Of Binary Cyclic Codes In the Generation Of Two Other Classes Of Codes”, ITC/USA/65.

2. The relationships in Eq. (1) are for horizontal protection of information-sets rather than vertical protection, To achieve the indicated relationships between (nr,) and (n_B), the number of discrete messagesets which (n_d) affords can be as few as (n_B) itself. In the case of saturated binary codes consisting of (m) message bits (and therefore affording 2^m discrete message sets), the appended redundancy for a specified (n_d) is usually ($2n_d$-3) bits.

3. The principal degradation which a binary digital waveform suffers because of bandpass limitations is to rise-time and fall-time at binary transition points. Under ideal bandpass conditions (i.e. flat bandpass with respect to attenuation and zero differential sideband delay), the product of rise or fall-time and bandpass is a

constant. This degradation immediately compromises sampling for bit-decision purposes insofar as envelope excursion occurs at a delay from the theoretical bit-clocking, Sampling becomes especially difficult in the case of singlet “1”s and singlet “0”s.

4. A Nyquist Interval is by definition equal to one half-cycle of the information carrier. That a half -cycle of the carrier suffices for reliable information is however true only under noise-free conditions. The Nyquist Interval, despite this limitation, is a convenient digital unit, or “information quantum”, for carrier-conveyed data because equipment response lies within this time domain,

5. Brothman, E. H., Horowitz, L. M., and Reiser, R. D., “Factors Affecting The Speed And Security Of A Digital Data Transmission System”, Tranactions Paper 63-944, IEEE Summer General Meeting, June 1963.

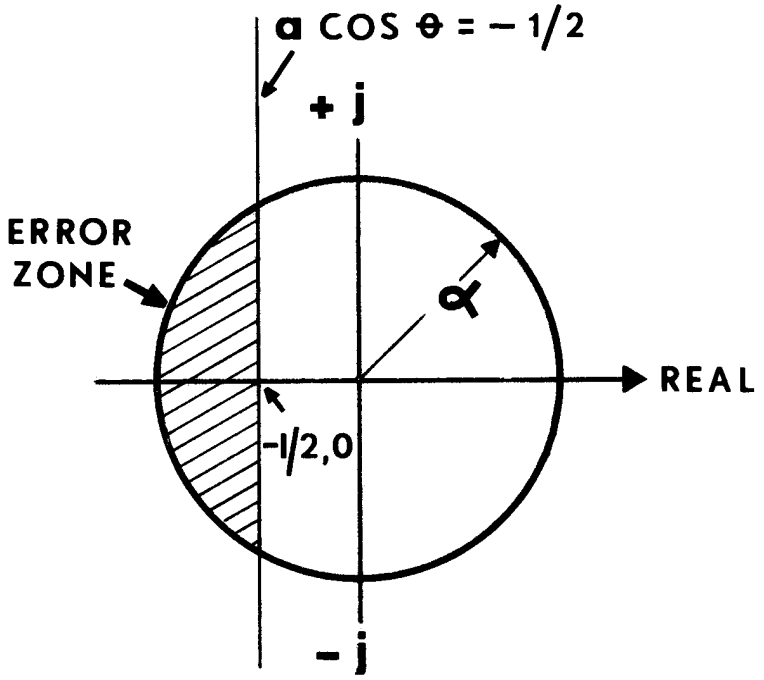

FIG. I - SIGNAL-PLUS-IMPULSE SPACE DIAGRAM FOR FREQUENCY SHIFT CARRIER TECHNIQUES

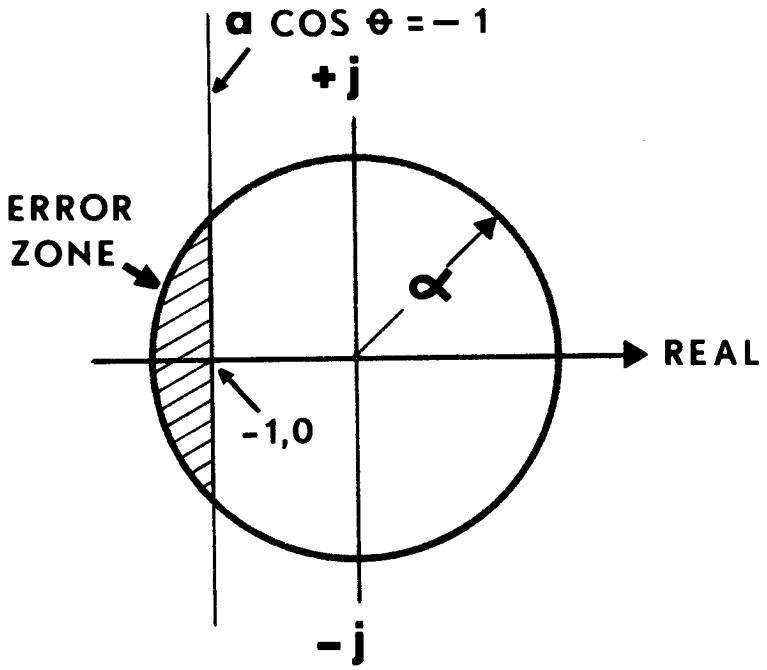

FIG. 2 - SIGNAL-PLUS-IMPULSE SPACE DIAGRAM FOR PHASE-SHIFT TECHNIQUES

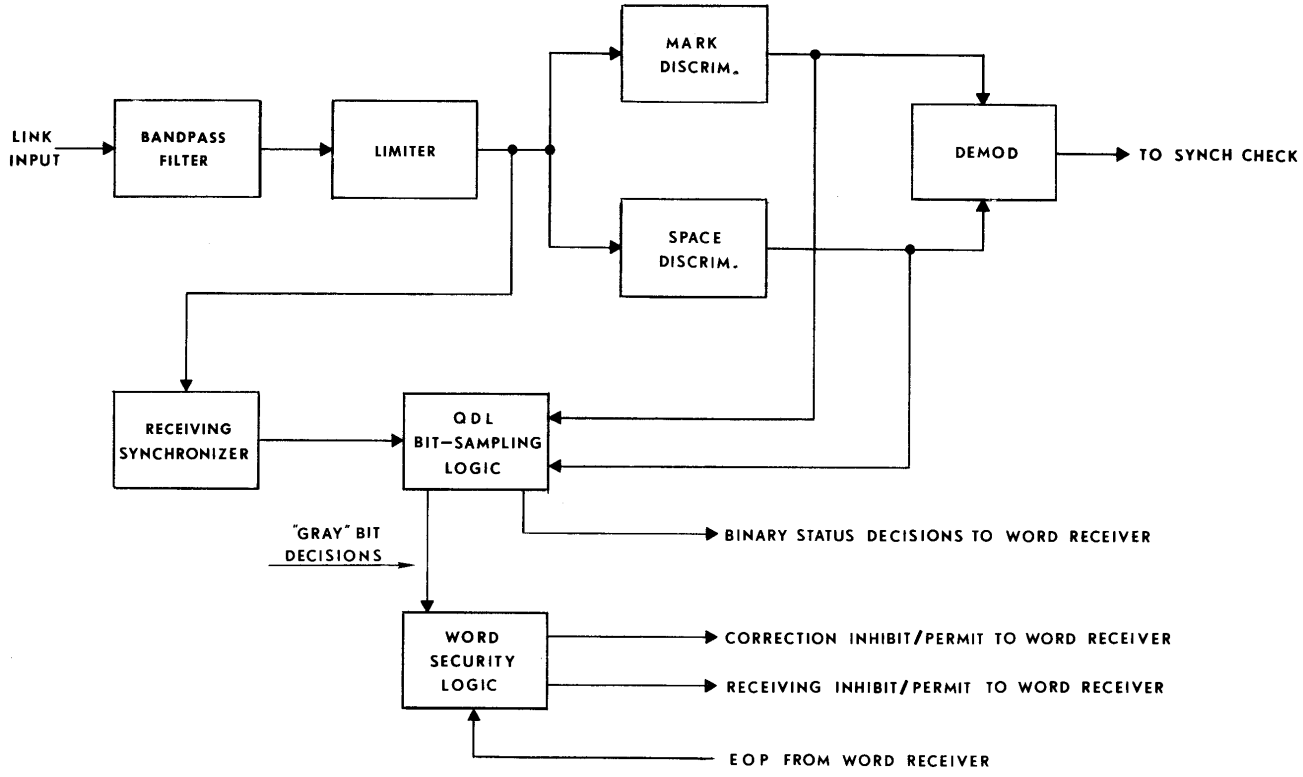

FIG. 3 - QUARTERNARY DECISION METHOD RECEIVING TERMINAL

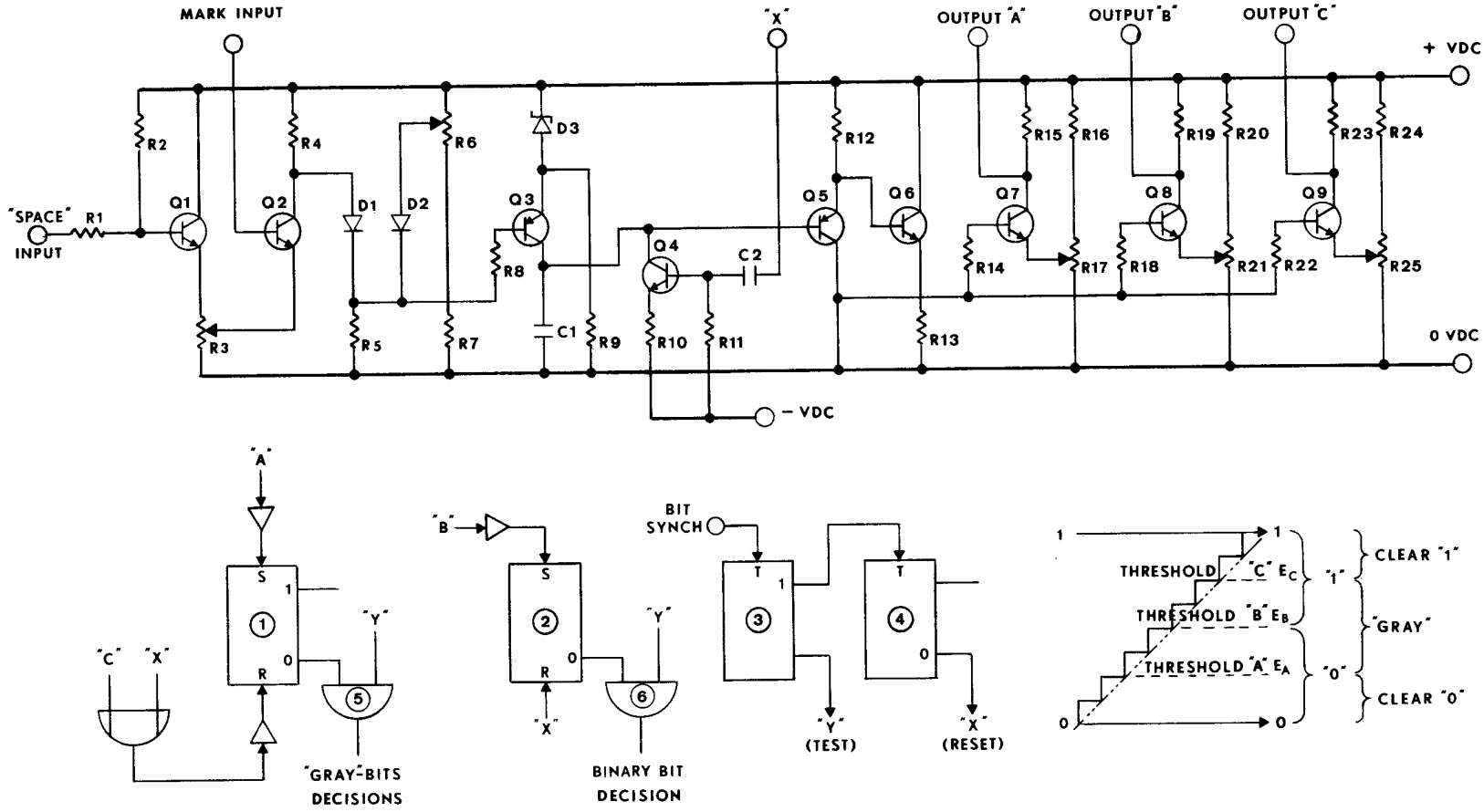

FIG. 4 - BIT-SAMPLING AND BIT-DECISION LOGIC

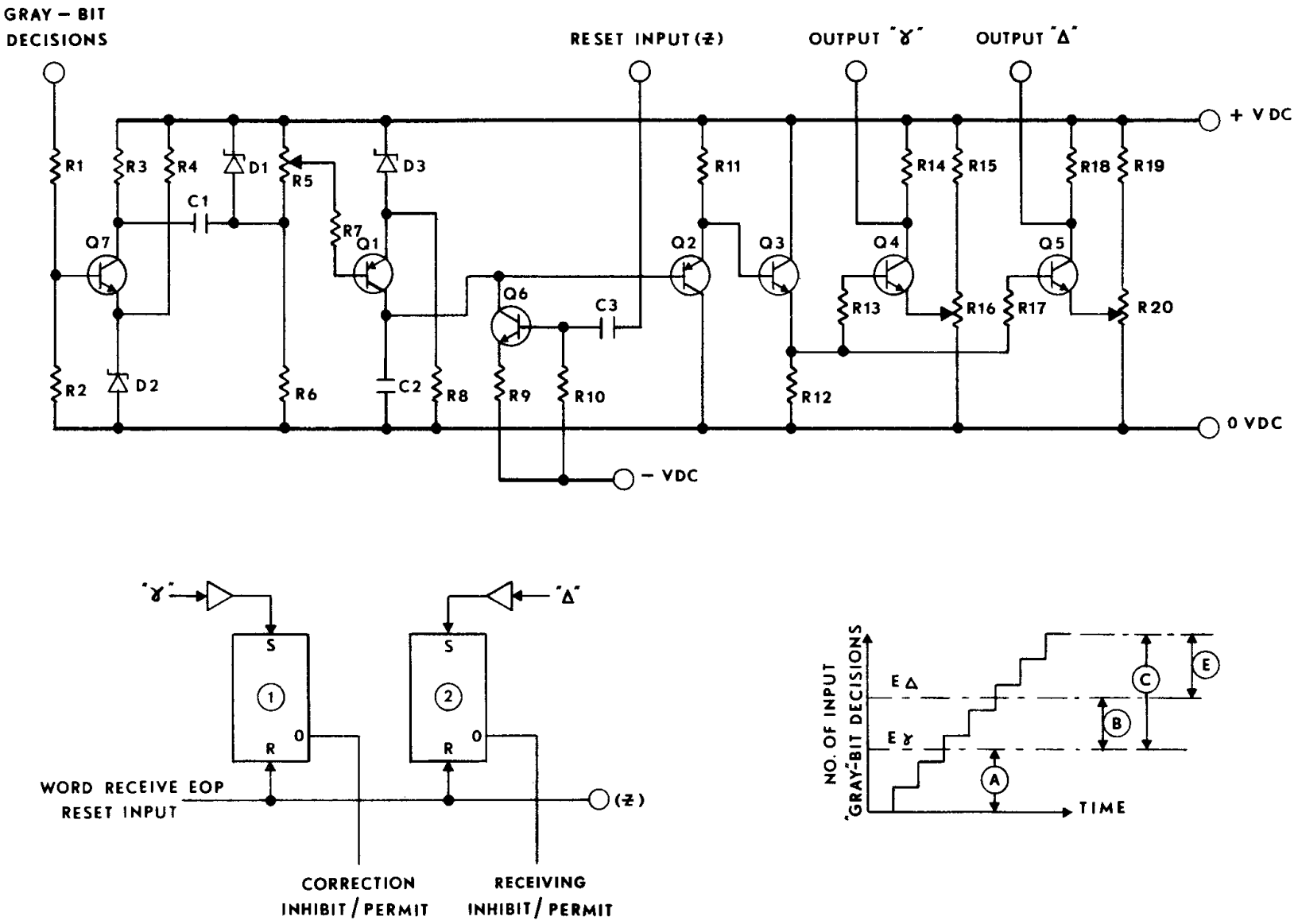

FIG. 5 - WORD SECURITY LOGIC