Copyright © 1975 American Telephone and Telegraph Company
THE BELL SYSTEM TECHNICAL JOURNAL
Vol. 54, No. 3, March 1975
Printed in U.S.A.

Timing Recovery and Scramblers in Data Transmission

By R. D. GITLIN and J. F. HAYES

(Manuscript received August 28, 1974)

This paper considers several problems associated with envelope-derived timing recovery, equalization, and scrambling in synchronous data transmission. Particular attention is focused on the time intervals in which periodic data sequences are transmitted, such as during start-up or when an idle code is being transmitted. It is shown that the standard envelope-derived timing-recovery system may be significantly improved by zonal filtering of the received passband signal prior to forming the envelope. For phase-modulated systems, we discuss the limitations of the "precession" technique employed for the purpose of providing a periodic timing wave when there is an input of short period. The advantages of using a phase-locked loop to filter the envelope instead of a narrow-band filter are also described. A study of scrambler operation has provided an extension of previous results concerning the relationship between the input and output period. It is shown that the output period of several scramblers connected in tandem does not necessarily double with the addition of a stage, and that if a particular stage does not lock up then no succeeding stage can lock up.

I. INTRODUCTION

Recovery and tracking of the symbol rate, or timing frequency, is one of the most critical functions performed by a synchronous modem. Most modems are "self-timed" in that they derive their timing frequency and phase directly from the information-bearing signal, instead of using a separate subchannel to send synchronization information. A technique that is commonly used to acquire the symbol rate* (which is the receiver's basic sampling rate) is to filter the envelope of the modulated data signal. Our investigation will consider several problems related to this method of timing recovery which arise in high-speed modems incorporating both an adaptive equalizer and a scrambler.

* This technique is also used to provide the sampling epoch, or phase, within a symbol interval.

The envelope-derived timing recovery system is a well-studied topic.[1,2] However, as the degree of excess bandwidth decreases, the ease with which timing can be recovered using this approach rapidly diminishes. We focus our attention on periodic input sequences. These sequences are used to train (or adapt) the data receiver during start-up and during the idle period between blocks of random data. To provide a densely spaced line spectrum of uniform amplitude (which is necessary if the equalizer coefficients are to remain properly adjusted for random input data), high-speed modems use a scrambler to "randomize" the short periodic inputs commonly used during the idle period. We investigate the effect of the scrambler on both the line spectrum and the strength of the timing tone. It is observed that zonal filtering of the received data signal prior to taking the envelope can significantly improve the relative strength of the timing tone by suppressing the jitter component.

Using transform theory, a discussion is presented on the relationship between the scrambler input and output periods. We refine Savage's[3] well-known results for periodic inputs; these refinements are applied to the study of the tandem and parallel scrambler configurations.

Sections II to IV review the basic envelope-derived timing system and give expressions for the power in the timing and interfering tones. The role of the phase-locked loop in the timing recovery system is described in Section V. Section VI considers the effect of precessing* the data symbols on timing recovery. The necessary background material on self-synchronizing scramblers is presented in Section VII. The transform approach is used in Section VIII to determine the scrambler output period. In Section IX the performance of a cascaded scrambler configuration is contrasted with the conventional serial arrangement. The parallel scrambler configuration is discussed in Section X.

II. BASIC TIMING RECOVERY SYSTEM

In this section we describe the commonly used technique of acquiring the timing frequency and phase by processing the envelope of the received signal. The object is to extract a tone, located at the symbol rate, which is then used in the sampled-data receiver. Figure 1 shows a simplified receiver structure of an in-phase and quadrature (e.g., QAM) data-transmission system, where we have focused attention on the timing recovery and equalization functions of the receiver. For

* The advancing of the transmitted angle by a fixed phase (in a differential phase-modulated modem), independently of the input, is known as precession.

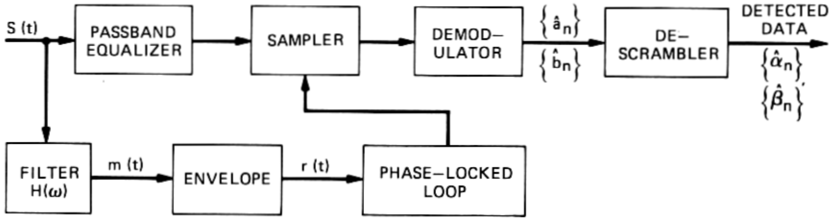

Fig. 1—Simplified QAM receiver.

our purposes it will be convenient to ignore both the additive noise and the quadrature component of channel distortion. Using the notation of Figs. 1 and 2, the received signal $s(t)$ is given by

$$s(t) = \sum_{n=-\infty}^{\infty} a_n g(t - nT) \cos \omega_c t - \sum_{n=-\infty}^{\infty} b_n g(t - nT) \sin \omega_c t, \quad (1)$$

where a_n and b_n are respectively the discrete-valued in-phase and quadrature data sequences obtained from the binary sequences α_n and β_n, $g(t)$ is the spectral-shaping pulse, ω_c is the carrier frequency, and $1/T$ is the symbol rate or timing frequency. The envelope of a filtered version of the received signal is tracked by a phase-locked loop tuned to the receiver's best *a priori* knowledge of the timing frequency. The output of a properly designed phase-locked loop will be a tone with frequency equal to the symbol rate and whose zero crossings may be used to derivc a sampling wave. Once the timing frequency is acquired, the estimated and unscrambled data sequences $\{\hat{\alpha}_n\}$ and $\{\hat{\beta}_n\}$ are available to the user. The decoder maps the sequence of multilevel two-tuples $(\hat{a}_n, \hat{b}_n)$ into a binary sequence which serves as the input to the inverse scrambler.

The data sequences $\{a_n\}$ and $\{b_n\}$ may be thought of as random (when user data are being sent) or as periodic (during start-up when the equalizer and timing parameters are being acquired, and during an

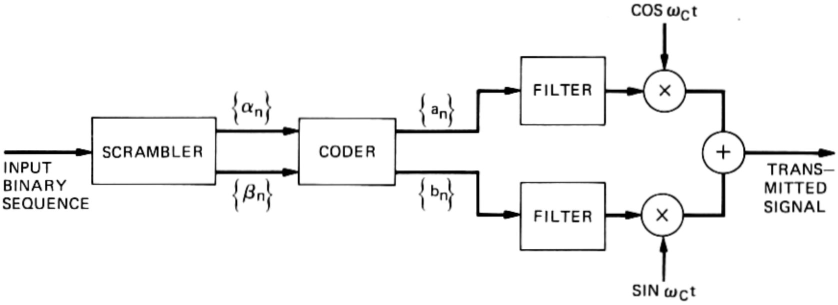

Fig. 2—Simplified QAM transmitter employing a scrambler.

idle period between random data transmissions). As we shall shortly see, the presence of a short periodic input can play havoc with the equalizer tap settings; hence, a scrambler is generally used at the transmitter to "randomize" these periodic sequences. As depicted in Fig. 2, the coder maps the binary stream of scrambled 0s and 1s into the channel pulse levels (e.g., 0 and 1 may be mapped into -1 and 1 respectively).* The effects of choosing a particular scrambler structure (e.g., serial vs parallel or serial vs cascade) on the timing recovery system will be treated in Sections VII and VIII.

III. SPECTRUM OF THE RECEIVED SIGNAL

We confine our attention to periodic inputs, beginning with a calculation of the Fourier transform of the received signal. Rewriting (1) in complex notation, we have

$$s(t) = \text{Re}\left\{ \sum_{n=-\infty}^{\infty} c_n g(t - nT) e^{j\omega_c t} \right\}, \tag{2}$$

where $c_n = a_n + jb_n$ and Re denotes the real part of a complex number. With a periodic data sequence, c_n, the signal $s(t)$ is periodic. This latter periodicity is best exhibited via the discrete Fourier transform[4] (DFT) of the periodic sequence. With the period of c_n denoted by N, the DFT of c_n is defined by

$$C(k\Omega) = \sum_{n=0}^{N-1} c_n e^{-jkn\Omega T} \qquad k = 0, 1, \cdots, N-1 \tag{3a}$$

and the inverse relation is

$$c_n = \frac{1}{N} \sum_{k=0}^{N-1} C(k\Omega) e^{jkn\Omega T} \qquad n = 0, 1, \cdots, N-1, \tag{3b}$$

where $\Omega = (1/N)(2\pi/T) = (1/N)\cdot$(symbol frequency). Hence, the DFT has N components uniformly spaced $1/NT$ Hz apart and the spectrum repeats every $2\pi/T$ Hz. Denoting the Fourier transform of $s(t)$ by $S(\omega)$ and convolution by $\circledast$, we have

$$S(\omega) = \tfrac{1}{2}\Big[\sum_n c_n e^{-j\omega nT} G(\omega)\Big] \circledast \delta(\omega - \omega_c), \qquad \omega > 0, \tag{4}$$

and using (3b) in (4) gives†

$$S(\omega) = \frac{1}{2} \sum_{k=0}^{N-1} C(k\Omega) \left[\sum_n G\left(k\Omega + \frac{2\pi n}{T}\right) \delta\left(\omega - \omega_c - k\Omega - \frac{2\pi n}{T}\right)\right]; \qquad \omega > 0. \tag{5}$$

Letting the timing frequency be denoted by $\omega_s = 2\pi/T = N\Omega$, it is

* In practice, the data would also be differentially and Gray encoded.

† We use the identity $\sum_n e^{-jn\omega T} = (2\pi/T) \sum_n \delta[\omega - (2\pi n/T)]$.

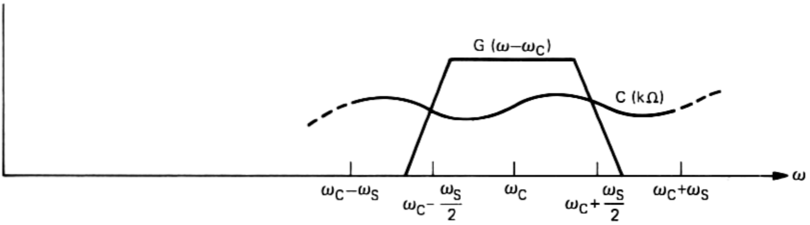

Fig. 3—The spectrum of the line signal for a periodic input is $S(w) = \text{Re}\ \{\sum_{k=0}^{N-1} C(k\Omega)[G(k\Omega)\delta(\omega-\omega_c-k\Omega)+G(k\Omega-\omega_s)\delta(\omega-\omega_c-k\Omega+\omega_s)]\}$ where the input period is NT seconds.

clear that $S(\omega)$ has discrete tones at $\omega_c + k\Omega + n\omega_s$. In practical data-transmission systems with pulses of less than 100-percent excess bandwidth, $G(k\Omega + 2\pi n/T)$ will be zero if $n \neq 0$ or -1, hence,

$$S(\omega) = \frac{\pi}{NT} \sum_{k=0}^{N-1} C(k\Omega)[G(k\Omega)\delta(\omega - \omega_c - k\Omega) \\ + G(k\Omega - \omega_s)\delta(\omega - \omega_c - k\Omega - \omega_s)]; \quad \omega > 0. \quad (6)$$

This spectrum is illustrated in Fig. 3, where it is seen that the envelope $C(k\Omega)$ modulates the baseband pulse shape, $G(\omega - \omega_c)$, in the range $\omega_c - \omega_s$ to $\omega_c + \omega_s$.

Since the signal $s(t)$ is used by the equalizer to adjust the tap weights, ideally the spectrum $C(k\Omega)$ should approximate that of random data, i.e., be constant. Of course, it is more critical that the equalizer be presented with a closely spaced line spectrum; for example, if the input period were two symbol intervals, it is clear that the equalizer can only compensate for distortion at two frequencies in the Nyquist band. Consequently, at the instant when the data return from the periodic to the random mode, the equalizer tap settings will be far from their optimum (for random data) values, and the distortion at the equalizer output could be much larger than the channel distortion. This situation generally causes the receiver to make so many errors that it is necessary to retrain the equalizer. As we shall see, the role of the scrambler is to lengthen the period of the transmitted sequence, thereby keeping the equalizer trained. Hence, for the rest of our discussion, we will assume that the scrambler is such that the periodic spectrum is (essentially) flat and densely spaced. Section VIII deals specifically with the factors that determine the period of the scrambler output.

IV. SPECTRUM OF THE ENVELOPE

The timing frequency is to be acquired from the envelope of the filtered line signal. Let the filtered line signal $m(t)$ be

$$m(t) = \sum_n a_n f(t - nT) \cos \omega_c t - \sum_n b_n f(t - nT) \sin \omega_c t, \quad (7)$$

where $f(t)$ is the (equivalent baseband) pulse shape after filtering at the receiver. The (squared) envelope of $m(t)$ is defined as

$$r(t) = [\sum_n a_n f(t - nT)]^2 + [\sum_n b_n f(t - nT)]^2. \tag{8}$$

As before, we introduce complex-signal notation by letting

$$d(t) = \sum_n c_n f(t - nT)$$

$$d^*(t) = \sum_n c_n^* f(t - nT), \tag{9}$$

so that we can write

$$r(t) = d(t) \cdot d^*(t), \tag{10}$$

where * stands for the complex conjugate. Thus, the Fourier transform of $r(t)$ is given by

$$R(\omega) = D(\omega) \circledast D_*(\omega) = [\sum_n c_n e^{-j\omega nT} F(\omega)] \circledast [\sum c_m^* e^{-j\omega mT} F(\omega)], \tag{11}$$

where $D_*(\omega)$ is the Fourier transform of $d^*(t)$, and $F(\omega)$ is the transform of $f(t)$. Using (3b), we have that

$$D(\omega) = \sum_n \left[\sum_{k=0}^{N-1} C(k\Omega) e^{-j(2\pi/N)kn} \right] e^{-j\omega nT} F(\omega)$$

$$= \sum_{k=0}^{N-1} C(k\Omega) F(\omega) \sum_n \delta(\omega - k\Omega - n\omega_s). \tag{12}$$

Substituting (12) into (11) and performing the convolution gives

$$R(\omega) = \sum_{k=0}^{N-1} \sum_{l=0}^{N-1} C(k\Omega) C^*(l\Omega) \sum_n \sum_m F(k\Omega + n\omega_s) F(m\omega_s - l\Omega)$$
$$\times \delta[\omega - (k - l)\Omega - (n + m)\omega_s]. \tag{13}$$

Evidently there are tones at $p\Omega + q\omega_s$ (where $p = k - l$ and $q = n + m$); the desired tone is at ω_s (i.e., $p = 0$, $q = 1$) and all other tones may be regarded as interferers. Again, practical bandlimiting of $F(\omega)$ and filtering of $R(\omega)$ will eliminate all terms where $q \neq 0$ or 1. The power in the desired tone is

$$R(\omega_s) = \sum_{k=0}^{N-1} |C(k\Omega)|^2 F(k\Omega) F(\omega_s - k\Omega), \tag{14}$$

while the power in an interfering tone (or sidelobe) is

$$R(\omega_s + p\Omega) = \sum_{k=0}^{N-1} C(k\Omega) C^*[(k - p)\Omega] F(k\Omega) F[(k - p)\Omega - \omega_s]$$
$$p = 1, 2, 3, \cdots. \tag{15}$$

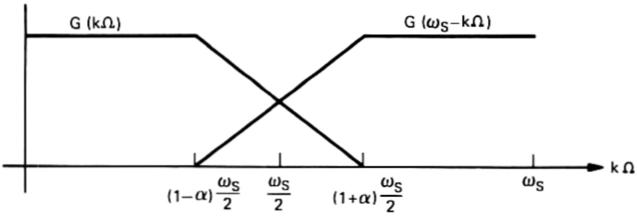

Fig. 4a—Strength of timing tone without loop filtering is $\sum_{k=0}^{N-1} |C(k\Omega)|^2 G(k\Omega)G(\omega_s - k\Omega)$.

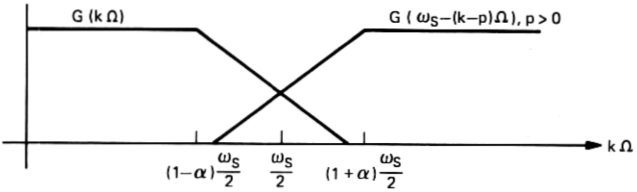

Fig. 4b—Strength of sidelobe interference at $\omega_s + p\Omega$ is $\sum_{k=0}^{N-1} C(k\Omega)C^*[(k - p)\Omega]G(k\Omega)G[(k - p)\Omega - \omega_s]$.

Conventionally, the signal $r(t)$ is fed to a phase-locked loop (PLL), which acts like a narrow-band filter in accepting tones in some region about ω_s (e.g., from $\omega_s - B\Omega$ to $\omega_s + B\Omega$, where $2B\Omega$ is the effective bandwidth of the loop) and produces an output that is dominated by a tone at ω_s. We first consider the above spectra in the absence of any timing loop filtering [i.e., $F(\omega) = G(\omega)$] as shown in Fig. 4. It is clear from (14) that the problem of timing-frequency recovery becomes more difficult as the amount of excess bandwidth (as measured by the parameter α) decreases—for zero excess bandwidth, this timing recovery technique clearly fails since the pulses $G(k\Omega)$ and $G(\omega_s - k\Omega)$ are disjoint. Figures 4a and 4b show how to compute the power of the tones at ω_s and at $\omega_s + p\Omega$ respectively. We note that, in general, $R(\omega_s + p\Omega) \neq R(\omega_s - p\Omega)$, and moreover, for the particular spectral shaping shown in the figure, it is clear that $R(\omega_s + p_1\Omega) > R(\omega_s + p_2\Omega)$ for $-B < p_2 < p_1 < B$; thus, half of the sidelobe tones are greater in magnitude than the desired tone. Thus, without any prefiltering in the timing loop, the desired tone is rather weak in comparison to the interfering tones. As we have already mentioned, this problem has a direct solution*: choose the loop filter $F(\omega - \omega_c)$ to be a narrow zonal filter around $\omega_c + (\omega_s/2)$ and $\omega_c = (\omega_s/2)$ as shown in Fig. 5. The resulting signal $m(t)$ has its energy concentrated at $\omega_c - (\omega_s/2)$ and $\omega_c + (\omega_s/2)$, and the relative strength of the timing tone is illustrated

* A filter in the timing loop has also been proposed by Franks and Bubrowski.[5]

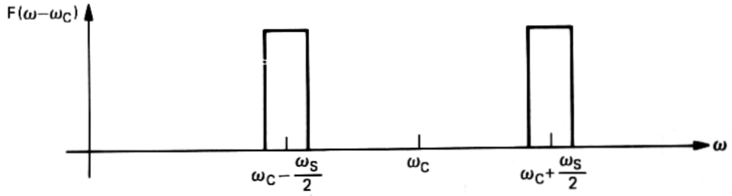

Fig. 5—Timing-loop filter shape which improves the tone-to-interference ratio.

in Figs. 6a, 6b, and 6c. The attenuation of the interferers is aided further by the fact that the magnitude of $\sum_{k=0}^{N-1} C_k C_{k-p}^*$ is a maximum for $p = 0$ (this follows from the Schwarz inequality). Clearly, by making $F(k\Omega) = \delta(k\Omega - \omega_s)$, we can make $R(\omega_s + p\Omega) = 0$ for all $p \neq 0$; however, *any narrow-zonal prefilter* of the type shown in Fig. 5 should significantly improve the relative strength of the timing tone. Since we merely require the filter to be narrow-band, any reasonable

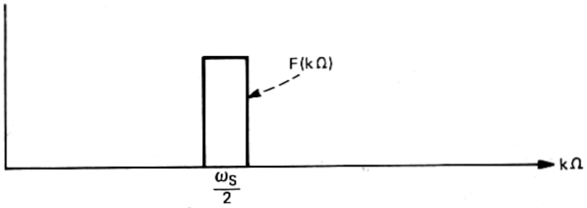

Fig. 6a—Strength of tone at $\omega_s \sim \sum_{k=0}^{N-1} |C(k\Omega)|^2 F(k\Omega) F(\omega_s - k\Omega)$.

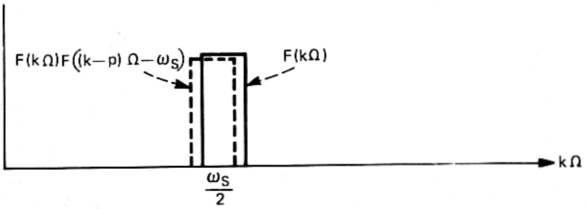

Fig. 6b—Strength of tone at $\omega_s + p\Omega \sim \sum_{k=0}^{N-1} C_k C_{k-p}^* F(k\Omega) F[(k-p)\Omega - \omega_s]$.

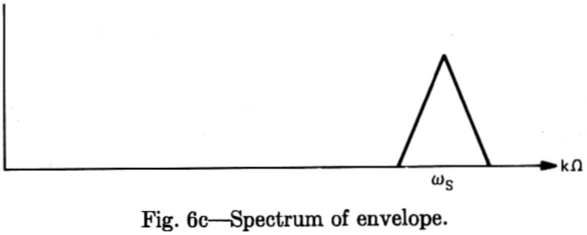

Fig. 6c—Spectrum of envelope.

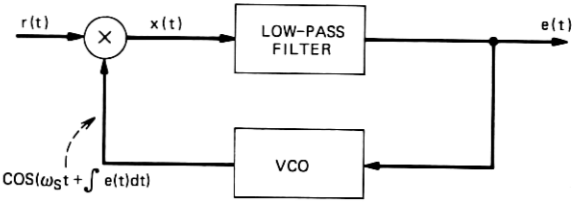

Fig. 7—First-order phase-locked loop.

choice wide enough to accommodate the uncertainty in ω_s would be adequate over a wide range of channel characteristics.

V. THE ROLE OF THE PHASE-LOCKED LOOP

As we have discussed, the signal $r(t)$ contains a desired tone as well as interfering tones. In this section, we wish to demonstrate that a phase-locked loop (PLL) can provide extremely narrow-band filtering even to the extent of extracting a single tone from a spectrum of adjacent interferers. Consider the standard first-order PLL[6] shown in Fig. 7. Let us assume that the input is the desired tone plus two interfering sidelobes, i.e.,

$$r(t) = A \sin \omega_s t + B \sin [(\omega_s + \Delta)t + \gamma] + B \sin [(\omega_s - \Delta)t - \gamma], \quad (16)$$

where Δ is the frequency displacement of the sidelobe from the desired tone and γ is the corresponding phase shift. Note that we have specialized the situation to the case where both interferers have the same amplitude and opposite phase angles (i.e., the distortion in the timing recovery system is symmetric about ω_s radians). We also assume that a perfectly tuned loop (i.e., the free-running frequency of the voltage-controlled oscillator (VCO) is ω_s) is employed.* From Fig. 7 the loop error signal is given by

$$e(t) = A \sin \left(\int e(t)dt + \alpha \right) + B \sin \left(\int e(t)dt + \alpha - \Delta t - \gamma \right) + B \sin \left(\int e(t)dt + \alpha + \Delta t + \gamma \right). \quad (17)$$

If we define $\phi(t)$ as the phase difference between VCO output phase and the PLL input phase corresponding to the desired tone, i.e.,

$$\phi(t) \triangleq \omega_s t - \left(\omega_s t + \int e(t)dt + \alpha \right), \quad (18)$$

* A perfectly tuned loop could arise by varying the free-running VCO frequency. As we show, via (22), when this condition is achieved the output will be a single tone. This observation suggests a feedback or error-sensing procedure for varying the nominal VCO frequency.

it is necessary that $\phi(t) \to 0$, as $t \to \infty$, since this implies successful tracking of the tone. Using (18) in (17) gives

$$e(t) = -[A + 2B\cos(\Delta t + \gamma)]\sin\phi(t), \tag{19}$$

and since from (18) $\dot{\phi}(t) = -e(t)$, the PLL is governed by the first-order differential equation

$$\frac{d\phi(t)}{dt} = -[A + 2B\cos(\Delta t + \gamma)]\sin\phi(t). \tag{20}$$

To solve (20), we first separate the variables and write

$$\frac{d\phi}{\sin\phi} = A + B\cos(\Delta t + \gamma)dt, \tag{21}$$

and, by direct integration, we obtain the solution

$$\phi(t) = 2\tan^{-1}\{e^{-At}\exp(2B/\Delta)[\sin(\Delta t + \gamma) - \sin\gamma]\}. \tag{22}$$

We then have $\phi(t) \to 0$ as $t \to \infty$, i.e., the loop locks on the desired tone for any strength of the interference tone. Clearly, the same would be true for a collection of interferers provided they met the assumed symmetry conditions on their amplitude and phase. This example illustrates the power of a PLL to capture a desired tone in the presence of considerable interference.

VI. EFFECT OF PRECESSION ON THE RECOVERY OF A TIMING TONE

In modems not employing adaptive equalization, the question arises as to whether or not a scrambler is needed to generate a timing tone during the idle period. Since there is no equalizer in the system, we are not concerned with having a densely spaced line spectrum but only that there be at least two spectral lines, spaced ω_s apart, in the passband signal. Using the framework we have developed in the preceding sections, we investigate the effect of "precessing" the data symbols. Let us consider the phase-modulated signal

$$s(t) = \sum_{n=-\infty}^{\infty} g(t - nT)\cos(\omega_c t + \theta_n), \tag{23}$$

whose idle code is $\theta_n = 0$ for all n. The spectrum of $s(t)$ is, by using (5) with $C(k\Omega) = \delta_{k0}$ and $N = 1$,

$$S(\omega) = \sum_{n=-\infty}^{\infty} G(n\omega_s)\delta(\omega - \omega_c - n\omega_s), \tag{24}$$

and for an excess bandwidth of less than 100 percent,

$$S(\omega) = G(0)\delta(\omega - \omega_c); \tag{25}$$

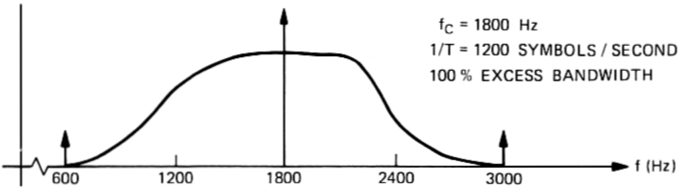

Fig. 8a—Spectrum without precession.

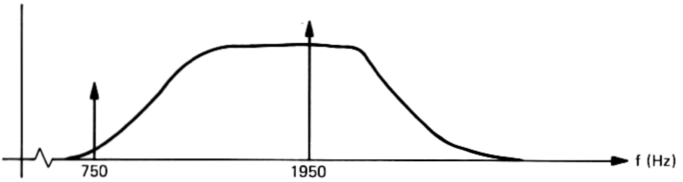

Fig. 8b—Spectrum with precession.

i.e., the spectrum consists of a single tone, which is obviously not sufficient to provide a timing tone. This situation is illustrated in Fig. 8a for a pulse $g(t)$ with 100-percent excess bandwidth and with $f_c = 1800$ Hz and $1/T = 1200$. To avoid the above situation, let $\theta_n = 2n\pi/M$, where $M/2$ is the number of points in the signal constellation and, thus, θ_n has period M. The advancing of the data symbol by $2\pi/M$ degrees, independently of any change in the input data, is known as *precession.*[*] Using the notation in Section I, we have

$$c_n = e^{j\theta_n} = e^{j(2n\pi/M)},$$

$$C(k\Omega) = \sum_{n=0}^{M-1} c_n e^{-jnk(2\pi/M)} = \sum_{n=0}^{M-1} e^{-j(2\pi/M)n(k-1)} = \delta_{k-1}, \tag{26}$$

which from (5) gives

$$S(\omega) = \sum_n G\left(n\omega_s + \frac{\omega_s}{M}\right) \delta\left(\omega - \omega_c - \frac{\omega_c}{M} - n\omega_s\right). \tag{27}$$

Thus, the effect of precession is to offset the tones by ω_s/M, producing the spectrum shown in Fig. 8b. Clearly, when squared, this signal provides a tone at $\omega_s = 1200$.

The situation is different, however, for the spectrum shown in Fig. 9a with $\theta_n = 0$. The spectrum with precession shifts the tone by 100 Hz, and clearly no pair of in-band tones is present. Thus, for spectra that

[*] Differential phase modulation with precession would generate a data sequence $\theta_n = \theta_{n-1} + \phi_n + 2n\pi/M$, where ϕ_n is one of $M/2$ equally spaced angles.

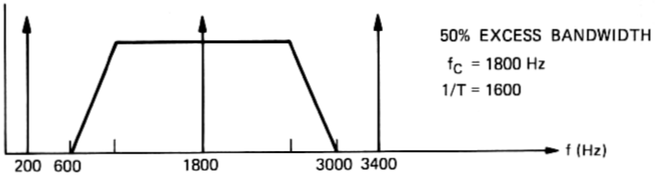

Fig. 9a—Signal spectrum without precession.

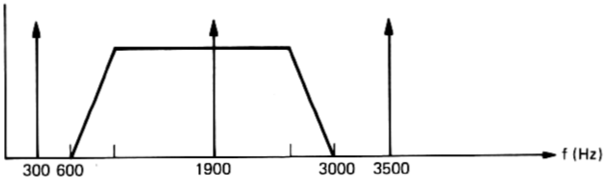

Fig. 9b—Signal spectrum with precession.

use small amounts of excess bandwidth, the tones necessary to provide timing would not be present with or without precession. Also, precession has little or no bearing on equalizer training since it simply shifts the spectrum and does not enrich it. For high-speed transmission in which the amount of excess bandwidth is small, spectral enrichment is provided by the scrambler and insures the proper operation of the equalizer and timing recovery system.

VII. SCRAMBLERS: BACKGROUND MATERIAL

We have shown in the preceding sections how the transmission of short repetitive patterns can play havoc with both the equalizer and timing recovery systems. As the name suggests, scramblers serve to "randomize" deterministic data sequences. The effect of this randomization on periodic sequences is to lengthen the period of the input sequence to the scrambler. Strictly speaking, the periodic output of the scrambler is not random. However, the scrambled data stream results in a line signal that has many more spectral components than the input data stream, and, thus, it looks more like the continuous spectrum that results when purely random data are encoded.

We confine our attention to the so-called self-synchronizing scrambler.[3] The generic forms for the self-synchronizing scrambler and the descrambler are shown in Figs. 10 and 11 and consist of, respectively, feedback and feedforward shift registers. Data symbols are fed into the scrambler every T seconds. These symbols are added (modulo p)*

* In practice, $p = 2$.

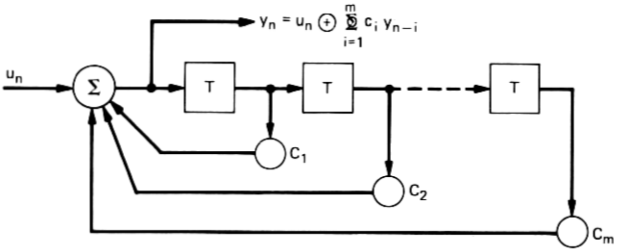

Fig. 10—Self-synchronizing scrambler.

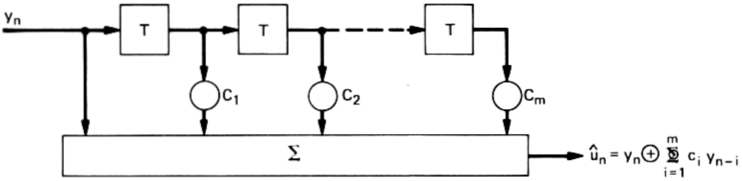

Fig. 11—Inverse scrambler.

to past outputs to produce the current output. The inputs to the delay elements shown in Fig. 10 are delayed by T seconds. The output of the scrambler is then encoded for transmission over the channel. After decoding at the receiver, the resulting sequence is put through a descrambler, shown in Fig. 11, where the original sequence is recovered. The inverse scrambler is self-synchronizing, and it will eventually cleanse itself of a transmission error once the error has propagated through the shift register. The number of errors in the descrambler output sequence is the number of channel errors multiplied by the number of nonzero tap weights in the shift register.

We shall study the input-output relationships of scramblers using d-transforms. Using this tool we are able, quite simply, to extend and clarify Savage's theorem[3] on scramblers with periodic inputs. Before getting into details on scrambler input-output relationships, a summary of some necessary background material on polynomials over Galois fields is in order.*

With p a prime number, we speak of a polynomial $Q(d)$ over $GF(p)$, where the coefficients of $Q(d)$ are modulo-p numbers. Multiplication, addition, and division of such polynomials are carried out in the usual fashion using modulo-p arithmetic on the coefficients. The *degree* of a polynomial $Q(d)$ is the highest power of d appearing in $Q(d)$. A polynomial of degree m is *irreducible* if it cannot be factored into poly-

* Much of the background material is taken from Ref. 7.

nomials of lower order. Two polynomials are relatively prime if they have no common factors. A crucial concept in our study of the scrambler is the *exponent* of a polynomial. The exponent of the polynomial $Q(d)$ is the minimum value of l such that $Q(d)$ divides $1 - d^l$, i.e., $(1 - d^l)/Q(d)$ is a polynomial of finite degree. For example, the exponent of the polynomial $1 + d^2 + d^3$ in $GF(2)$ is 7 since it divides $1 + d^7$, yielding $1 + d^2 + d^3 + d^4$, but it does not divide $1 + d^i$, $i < 7$. If the polynomials $P(d)$ and $Q(d)$ are relatively prime with exponents l_1 and l_2 respectively, it can be shown that the exponent of $P(d)Q(d)$ is the least common multiple (lcm) of l_1 and l_2. The exponent of $[Q(d)]^j$, where $Q(d)$ is over $GF(p)$, is $p^r l$, where l is the exponent of $Q(d)$ and r is such that $p^{r-1} < j \leqq p^r$. An irreducible polynomial of degree m is *primative* or of maximum exponent if its exponent is $p^m - 1$. Given a polynomial $Q(d)$ of order m, its reciprocal polynomial is $d^m Q(1/d)$, and it is known that reciprocal polynomials of irreducible polynomials are themselves irreducible, and that reciprocal polynomials of primative polynomials are themselves primative.

This theory of polynomials over a Galois field is applicable to the d-transforms[7] of the input and output sequences of a scrambler. Consider a time series $x_0, x_1, x_2, \cdots$, such that the x_i, $i = 0, 1, \cdots$ are elements from a Galois field, e.g., $01101 \cdots$. The d-transform of this series is defined as

$$X(d) \equiv \sum_{i=0}^{\infty} x_i d^i, \tag{28}$$

and inversion is accomplished by "reading" the coefficients of $X(d)$. The d-transform of a periodic sequence is of the form $R(d)/(1 - d^\lambda)$, where λ is the period of the sequence and $R(d)$ is a polynomial, of degree less than λ, in d over $GF(P)$. To illustrate, suppose we have a series of elements in $GF(3)$, 1021, 1021, $\cdots$. Using the relationship for a geometric progression we find that the d-transform of this series is $(1 + 2d^2 + d^3)/(1 - d^4)$. In general, it can be shown that the d-transform of a periodic time series is of the form $P(d)/Q(d)$, where $P(d)$ and $Q(d)$ are polynomials over a Galois field. If $P(d)$ and $Q(d)$ are relatively prime, the period of the time series represented by $P(d)/Q(d)$ is the exponent of $Q(d)$.

Linear sequential machines over $GF(p)$ are composed of modulo-p adders, multipliers, and delay elements connected according to a few elementary rules. As the name implies, such circuits are *linear* over modulo-p arithmetic. The laws of commutativity, associativity, and superposition apply. For example, the response of a circuit to the sum of two inputs is the sum of the responses to each input separately. The summations are carried out term-by-term modulo p on the input and output sequences.

The response of such circuits to inputs can be found using the classical techniques of linear system theory. The output consists of the sum of the *free response* and the *forced response*. The free response is due solely to initial conditions within the circuit with no input. If the circuit is in the quiescent state, i.e., it has zero initial conditions, there is no output without an input. The forced response is the output when an input is applied to a circuit in the quiescent state. As in the case of conventional linear circuits, the forced response can be found by convolving the impulse[*] response with the input sequence. Thus, if h_n, $n = 0, 1, \cdots$ is the impulse response of a circuit and u_n is its input at time nT, $n = 0, 1, \cdots$, then the output at time nT is

$$y_n = \sum_{k=0}^{n} h_k u_{n-k}, \tag{29}$$

where $\sum$ indicates summation modulo p. If we take the d-transform of both sides of (29), we find

$$Y(d) = U(d)H(d), \tag{30}$$

where $U(d)$ and $H(d)$ are the d-transforms of u_n and h_n respectively, and where $n = 0, 1, \cdots$.

VIII. SCRAMBLER INPUT-OUTPUT RELATIONSHIPS

Scramblers are linear sequential circuits and their input-output relationships can be found using linear system theory. In this section, we wish to demonstrate the utility of the d-transform approach in characterizing the nature of the output sequence for a given input sequence. Consider the m-stage scrambler shown in Fig. 10 with feedback coefficients $c_1, \cdots, c_m$. The output at time nT, y_n, is given by

$$\begin{aligned} y_n &= c_1 s_{1n} \oplus c_2 s_{2n} \oplus \cdots \oplus c_m s_{mn} \oplus u_n \\ s_{1n} &= y_{n-1} \\ s_{in} &= s_{i-1,n-1} \qquad i \geqq 2, \end{aligned} \tag{31}$$

where u_n is the input at time nT and s_{kl} is the output of the kth delay element at time l.[†] Now we find the impulse response. Let

$$u_n = \begin{cases} 1 & n = 0 \\ 0 & n > 0 \end{cases}$$

and

$$s_{i0} = 0, \forall i.$$

[*] By an impulse we, of course, mean a time series which is unity at the time origin and is zero elsewhere.

[†] The output may be rewritten as $y_n = \sum_{i=1}^{m} c_i y_{n-i} \oplus u_n$. At the descrambler we form $z_n = y_n \oplus \sum_{i=1}^{m} c_i y_{n-i}$, which recovers the input when there are no channel errors.

The output sequence can be written

$$y_n = \begin{cases} 1 & n = 0 \\ \sum_{i=1}^{n} c_i y_{n-1} & n \leqq m \\ \sum_{i=1}^{m} c_i y_{n-i} & n > m. \end{cases} \tag{32}$$

If we take d-transforms of both sides of (32) we find after some manipulation that the transform of the impulse response, i.e., the transfer function, is given by

$$H(d) \triangleq \sum_{k=0}^{\infty} y_k d^k = 1 \bigg/ \left(1 - \sum_{i=1}^{m} c_i d^i\right). \tag{33}$$

The d-transform of the forced response of the scrambler can be found from eqs. (30) and (33).

The free response of the scrambler can also be found from (31) when $u_n = 0$, for all n. We begin by assuming a particular initial state vector. Assume that the output of all of the delay elements but one are zero. Let the nonzero output be that of the ith delay element and denote this output by s_{i0}. It can be shown that y_n^i, the output of the scrambler due solely to state s_{i0}, is

$$y_n^i = \begin{cases} c_i s_{i0} & n = 0 \\ \sum_{j=1}^{n} c_j y_{n-j}^i + c_{i+n} s_{i0} & 0 < n \leqq m - i \\ \sum_{j=1}^{m} c_j y_{n-j}^i & n > m - i. \end{cases} \tag{34}$$

If we take the d-transform of both sides of eq. (34), we find that the d-transform of the response to initial condition s_{i0} is

$$Y^i(d) = \left(s_{i0} \sum_{k=0}^{m-i} c_{i+k} d^k\right) \bigg/ \left(1 - \sum_{j=1}^{m} c_j d^j\right). \tag{35}$$

Now, to find the response to any initial condition $s_{10}, s_{20}, \cdots, s_{m0}$, we sum over i. Thus, the d-transform of the free response is

$$Y_{\text{free}}(d) = S(d) \bigg/ \left(1 - \sum_{j=1}^{m} c_j d^j\right) = S(d) H(d), \tag{36}$$

where $S(d) \triangleq \sum_{i=1}^{m} s_{i0} \sum_{k=0}^{m-i} c_{i+k} d^k$.

A fact that is crucial to our analysis in the sequel is that the polynomial $S(d)$ spans the space of polynomials of degree $m - 1$ in $GF(p)$. By choosing the initial conditions s_{i0}, $i = 1, 2, \cdots, m$, $S(d)$ can be any polynomial of degree $m - 1$. To show this, suppose we have the polynomial $T(d) = t_0 + t_1 d + \cdots + t_{m-1}d^{m-1}$. Equating $T(d)$ and $S(d)$ term by term, we have m equations in m unknowns, $s_{10}, s_{20}, \cdots, s_{m0}$. The equations can be represented in the form

$$\begin{bmatrix} c_m & 0 & \cdots & 0 \\ c_{m-1} & c_m & \cdots & 0 \\ \vdots & \vdots & & \\ c_1 & c_2 & \cdots & c_m \end{bmatrix} \begin{bmatrix} s_{10} \\ s_{20} \\ \vdots \\ s_{m0} \end{bmatrix} = \begin{bmatrix} t_{m-1} \\ t_{m-2} \\ \vdots \\ t_0 \end{bmatrix}. \tag{37}$$

The $m \times m$ lower triangular matrix in (37) is nonsingular (since $c_m \neq 0$); therefore the m simultaneous equations have a unique solution.

From the foregoing, we see that the total response of a scrambler to an input, with transform $U(d)$, is

$$Y(d) = [U(d) + S(d)]/\Phi(d), \tag{38}$$

where $\Phi(d) \triangleq 1 - \sum_{i=1}^{m} c_i d^m$ is the transform of the feedback coefficients. The above equation completely describes the behavior of the scrambler to any input for any given initial state.

Now we consider the input-output relationships for the scrambler based on eq. (38). Throughout our discussion we shall assume that $\Phi(d)$ is a primitive polynomial implying that it has exponent $\phi = p^m - 1$, and thus can be written as $(1 - d^\phi)/\Phi'(d)$, where $\Phi'(d)$ is a finite degree (remainder) polynomial of degree $\phi - m$. Note that $\Phi'(d)$ is one "cycle" of the periodic polynomial $1/\Phi(d)$. Suppose that the input is zero, the transform of the output is simply $S(d)/\Phi(d)$. Since the degree of $S(d)$ is one less than that of $\Phi(d)$, $S(d)$ and $\Phi(d)$ are relatively prime,* and the output transform is $S(d)\Phi'(d)/(1 - d^\phi)$; hence, the output is periodic with period $= p^m - 1$. If the input is a sequence of finite duration j, then $U(d)$ is a polynomial of degree $j - 1$. If $j \leqq m$, then the above output transform is $U(d)\Phi'(d)/(1 - d^\phi)$, and since the degree of the numerator is less than ϕ, it is clear that the output is purely periodic with period ϕ. Note that there is no output transient. If $j \geqq m$, and if $U(d) + S(d)$ and $\Phi(d)$ are relatively prime, then it is easy to show that the output consists of a transient component $(j + 1 - m)$ long† and a periodic component with period ϕ. For any input $U(d)$ of finite duration, there are a unique set of initial conditions

* Since $\Phi(d)$ is a primative polynomial, $S(d)$ cannot be a factor of $\Phi(d)$; and since the degree of $S(d)$ is less than a $\Phi(d)$, $\Phi(d)$ cannot be a factor of $S(d)$. Thus, $S(d)$ and $\Phi(d)$ are relatively prime.

† This should be intuitively clear, since once $j - (m - 1)$ bits are accepted in the scrambler, the situation is one where the (remaining) input sequence is of a length less than m.

$S(d)$ such that

$$U(d) + S(d) = T(d)\Phi(d),$$

where $T(d)$ is some polynomial. In this situation the output has finite duration given by $T(d)$, i.e., the periodic component of the solution has been annihilated. To show this, we cite the following theorem.[8] Let $U(d)$ and Φ (d) be polynomials in $GF(p)$. Then there are unique polynomials $T(d)$ and $S(d)$ in $GF(p)$ such that $U(d) + S(d) = T(d)\Phi(d)$, where $S(d) \equiv 0$ or $S(d)$ is of lower degree then $U(d)$. Recall that by suitably choosing initial conditions, $S(d)$ can be any polynomial of degree $m - 1$ over $GF(P)$.

We turn to the important case of periodic inputs. The input sequence $U(d)$ can always be written in the form $U(d) = P(d)/Q(d)$, where $P(d)$ and $Q(d)$ are relatively prime. Let the exponent of $Q(d)$ be ℓ, i.e., the period of the input is ℓ. The d-transform of the output becomes

$$Y(d) = [S(d)Q(d) + P(d)]/\Phi(d)Q(d). \tag{39}$$

We consider first the case where $\Phi(d)$ and $Q(d)$ are relatively prime. If the numerator and denominator of eq. (39) are relatively prime, then, using the background material presented in Section VII, it is clear that the output is periodic with period N, where $N = \text{lcm}\ (l, p^m - 1)$. However, we will show that given $P(d)$ and $Q(d)$, there is a set of initial conditions for which

$$S(d)Q(d) + P(d) = T(d)\Phi(d), \tag{40a}$$

where $T(d)$ has degree $l - 1$. When (40) holds, the output period is l. Thus, assuming that all initial states are equiprobable, with probability p^{-m} the initial state will be such that the scrambler "locks up" and the output period equals the input period. (As we have previously mentioned, this is a very undesirable situation.) To support (40) we cite the following theorem.[8] There exist (unique) polynomials $T'(d)$ and $S'(d)$ such that

$$S'(d)Q(d) + T'(d)\Phi(d) = 1 \tag{40b}$$

only if $Q(d)$ and $\Phi(d)$ are nonzero relatively prime polynomials over $GF(p)$. Now multiply both sides of the above equation by $-P(d)$ and let $S(d) = - P(d)S'(d)$ and $T(d) = P(d)T'(d)$. Again we make use of the fact that $S(d)$ spans the space of polynomials of degree $m - 1$ to guarantee that for every $S'(d)$ there corresponds a $S(d)$. We now summarize the above.

Let the scrambler be defined by the primative polynomial $1 - \sum_{i=1}^{m} c_i d^i$, and also suppose that the transform of the input to the scrambler is $P(d)/Q(d)$, where $P(d)$ and $Q(d)$ are relatively prime. It is also assumed that $\Phi(d)$ and $Q(d)$ are relatively prime. For a particular set of initial conditions, the output period of the scrambler is the input period, l, where l is the exponent of $Q(d)$. For all other initial conditions the output period is the least common multiple of l and $p^m - 1$.

Our description is the same as Savage's Theorem 1 with two differences—one superficial, the other crucial. Savage requires the polynomial $h(d) = d^m - \sum_{i=1}^m c_i d^{m-i}$ to be primative. However, $1 - \sum_{i=1}^m c_i d^i$ and $h(d)$ are reciprocal polynomials and, as we have seen, the reciprocals of primative polynomials are themselves primative with the same exponent. The second requirement is that $\Phi(d)$ and $Q(d)$ be relatively prime. This requirement, which is not part of Savage's theorem, is essential for a complete description of scrambler behavior.*

We will now show that the requirement that $\Phi(d)$ and $Q(d)$ be relatively prime is satisfied whenever the exponent of $Q(d)$ is not a multiple of $p^m - 1$. The proof is by contradiction. Suppose $\Phi(d)$ and $Q(d)$ are not relatively prime, then it is possible to write†

$$Q(d) = R(d)\Phi^j(d) \qquad j = 1, 2, \cdots, \tag{41}$$

where $R(d)$ is a polynomial, with exponent r, which is relatively prime to $\Phi(d)$. The exponent of $Q(d)$ is lcm $[r, p^k(p^{m-1})]$, where k is such that $p^{k-1} < j \leqq p^k$. Clearly, the exponent of $Q(d)$ is a multiple of $p^m - 1$, thus proving the desired result. Thus, when the input period is less than p^{m-1} (the practical case), then $\Phi(d)$ and $Q(d)$ are relatively prime. It is interesting to note that even if the input to the scrambler has an exponent which is a multiple of $p^m - 1$, it may be that $Q(d)$ and $\Phi(d)$ are still relatively prime. For example, $Q(d)$ can be the reciprocal polynomial to $\Phi(d)$.

Consider now the situation when $Q(d)$ and $\Phi(d)$ are not relatively prime. As above, we can then factor $Q(d)$ in the form $Q(d) = \Phi^j(d)R(d)$, $j \geqq 1$, where $R(d)$ is either 1 or a polynomial relatively prime to $\Phi(d)$. From (39) and (41) the d-transform of the output is

$$Y(d) = [S(d)\Phi^j(d)R(d) + P(d)]/\Phi^{j+1}(d)R(d). \tag{42}$$

Since by assumption $P(d)$ is relatively prime with $Q(d) = \Phi^j(d)R(d)$, the numerator and denominator of (42) are relatively prime. Since $\Phi^{j+1}(d)$ and $R(d)$ are relatively prime, the output period is then the least common multiple of $p^k(p^m - 1)$ and r, with k given by $p^{k-1} < j$

* In other words, Savage states that, apart from the special case when the output period equals the input period, the output period is the lcm(l, p^{m-1}). This is not strictly true since, as we shall show, if $\Phi(d)$ and $Q(d)$ are not relatively prime, the output period is not necessarily the lcm(l, p^{m-1}).

† Since $\Phi(d)$ is irreducible, we could not write $Q(d)$ as a factor of $\Phi(d)$.

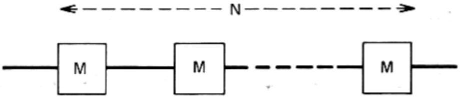

Fig. 12—Cascade of N M-bit scramblers.

$+ 1 \leqq p^k$. Note that this result holds independently of initial conditions.[*]

The above discussion provides a refinement of Savage's basic result[†] by indicating that the output period is contingent on whether or not $\Phi(d)$ and $Q(d)$ are relatively prime. It was shown that if the exponent of $Q(d)$ is not a multiple of $p^m - 1$, then $\Phi(d)$ and $Q(d)$ are relatively prime. However, when $Q(d)$ and $\Phi(d)$ are not relatively prime the output period must be determined from (42).

IX. CASCADED SCRAMBLERS

The cascade of identical scramblers provides an interesting example of when $Q(d)$ and $\Phi(d)$ are not relatively prime. Suppose, as in Fig. 12, we have n identical m-stage scramblers in tandem so that the output of the first is the input to the second and so on. Thus, assuming no lockup, the input to the second stage will have the same period as the free-running period of the second stage. With $S(d) = 0$ for all the scramblers, the output transform of the nth scrambler is

$$Y(d) = U(d)/\Phi^n(d), \tag{43}$$

where $U(d)$ is the transform of the input. Consider an example where $U(d) = 1/(1 + d) = 1/Q(d)$ with $p = 2$. Note that the exponent of $Q(d)$ is unity. The transform of the second output is $1/Q(d)\Phi^2(d)$, and we apply the results of the previous section to show that the output period is $2(2^m - 1)$, i.e., $k = 1$. Applying the above result to successive stages produces the data in Table I, which shows the period of the output as a function of n for a binary scrambler ($p = 2$). Table I points out that adding a stage in cascade does not always double the output period.

By considering each scrambler successively, we can comment on the output period of the cascade scrambler for arbitrary initial conditions and input, assuming $Q(d)$ and $\Phi(d)$ are relatively prime. Let the input to the first scrambler have exponent $l < p^m - 1$. From Section VIII

[*] If cancellation between the numerator and denominator in (42) were to occur, (40) would imply that $P = \Phi(1 + SR\Phi^{j-1})$. Now since (41) states that $Q = R\Phi^j$, it is clear that P and Q have the common factor Φ. This contradicts the assumption that P and Q are relatively prime. Thus, under the above conditions (i.e., Q and Φ are not relatively prime), the initial condition cannot force the output period to equal the input period.

[†] Results similar to ours were stated without proof in Ref. 9.

Table I

n	Output Period
1	$(2^m - 1)$
2	$2\ (2^m - 1)$
3	$4\ (2^m - 1)$
4	$4\ (2^m - 1)$
5	$8\ (2^m - 1)$
6	$8\ (2^m - 1)$
7	$8\ (2^m - 1)$
8	$8\ (2^m - 1)$
9	$16\ (2^m - 1)$

we know that the probability of the output having period l is p^{-m}. Otherwise, the output has period $\text{lcm}(l,\ p^m - 1)$. If the input to the second scrambler has period l we have the same situation as the first scrambler. However, if the output of the first scrambler has period $\text{lcm}\ (l,\ p^m - 1)$, the input polynomial to the second scrambler has denominator $Q(d)\Phi(d)$. By an argument analogous to that surrounding (42), it is clear that (40) cannot be satisfied, since $Q(d)\Phi(d)$ and $\Phi(d)$ are not relatively prime; thus, the scrambler cannot "lock up," and applying the results in Table I indicates that the output of the second scrambler has period $\text{lcm}[l,\ p(p^m - 1)]$. Thus, if a particular scrambler does not lock up, then no succeeding scrambler can lock up. The situation is summarized in Table II for four binary scramblers in tandem. We assume in Table II that all initial states are equiprobable.

We compare Table II to the serial scrambler in which all delay elements are combined into a scrambler that has $4m$ elements. With input period l, the output period is l with probability 2^{-4m} and $\text{lcm}(l,\ 2^{4m} - 1)$ with probability $1 - 2^{-4m}$. Both the cascade and serial scramblers lock up and have period l with the same probability (2^{-4m}); however, since

(*i*) the longest period of the cascade scrambler, $\text{lcm}[l,\ 4(2^m - 1)]$, is less than the largest period of the serial scrambler, $[\text{lcm}(l,\ 2^{4m} - 1)]$, and

Table II

Output Period	Probability
l	2^{-4m}
$\text{lcm}(l,\ 2^m - 1)$	$2^{-3m}(1 - 2^{-m})$
$\text{lcm}[l,\ 2(2^m - 1)]$	$2^{-2m}(1 - 2^{-m})$
$\text{lcm}[l,\ 4(2^m - 1)]$	$1 - 2^{-2m}$

(*ii*) the probability of the cascade scrambler attaining its largest period $(1 - 2^{-2m})$ is less than the probability of the serial scrambler attaining its largest period $(1 - 2^{-4m})$,

the superiority of the serial over the cascaded scrambler in terms of spectral density is clear.

X. PARALLEL SCRAMBLERS

Serial scramblers have the property that if a single bit error is made in demodulation, then M errors will appear in the unscrambled output sequence, where M is the number of nonzero coefficients in the scrambler primative polynomial. A parallel scrambler configuration has been proposed to ameliorate this error multiplication. In this section, we shall illustrate a spectral cancellation effect that can take place with parallel scrambling. For simplicity, we shall consider two parallel data streams. Suppose that the binary data, as in Fig. 13, are split into two data streams a_n' and b_n', where a_n is the scrambled[*] version of a_n', while $b_n = a_{n-m} \oplus b_n'$. The a_n and the b_n streams are then encoded for transmission over the channel. At the receiver, inverse operations recover the a_n' and the b_n' streams. A channel error in the a_n stream will cause M errors in the a_n' stream and one error[†] in the b_n' stream. A channel error in the b_n stream will cause a single error in the b_n' stream. Now suppose that a_n and b_n are Gray encoded so that a_n is the least significant bit. The result is that the probability of error in the a_n stream is much less than the probability of error in the b_n stream; thus, the average number of errors in the a_n' and the b_n' streams will be decreased compared with serial scrambling.

Now we wish to examine the effect of "slaving" the b_n stream to the a_n stream. For our purposes it will be sufficient to code the scrambled output sequences into 1 and -1, i.e., the transmitted data sequence is given by[‡] (recall the notation of Section III)

$$\begin{aligned} c_n &= (2a_n - 1) + j(2b_n - 1) \\ &= 2a_n - 1 + j[2(a_{n-m} \oplus b_n') - 1]. \end{aligned} \tag{44}$$

As we have shown in Sections III and IV, *both* the line and envelope spectra critically depend on the discrete Fourier transform (DFT) of the c_n sequence, $C(k\Omega)$. Unfortunately, it is not possible to express

[*] At the inverse scrambler, a_n' is recovered as in the standard configuration, while b_n' is estimated as $b_n + a_{n-m}$.

[†] Since the estimated b_n' is formed as the "mod 2" sum of b_n and a_{n-m}, a single channel error will only affect the b_n' output once; however, the a_n' output will see the propagation of this error through the shift register.

[‡] The function $(2a_n - 1)$ maps "0" into "-1" and "1" into "1" and thus serves as a mapping from the scrambler output sequence to the transmitted (line) sequence.

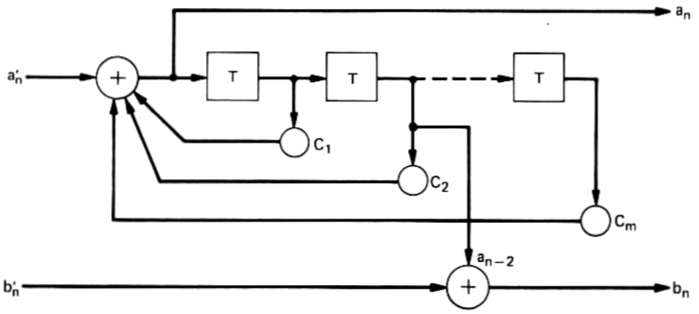

Fig. 13—Parallel scrambler configuration.

$C(k\Omega)$ directly in terms of the scrambler primative polynomial, which is a most difficult problem since, in the space of *real*-valued sequences, the DFT is a linear operation and the scrambler output is a nonlinear function of the input [of course, the scrambler input and output are linearly related in $GF(p)$]. However, in the present situation we are able to proceed since we are only interested in illustrating the possibility of spectral cancelling due to the parallel structure. We first indicate two simple relations between mod 2 operations and the corresponding real variable operations: with $a, b \in GF(2)$,

$$a \oplus b = (a - b)^2 \tag{45a}$$

$$a^2 = a. \tag{45b}$$

Using (45) we write (44) as

$$\begin{aligned} c_n &= (2a_n - 1) + j[2(a_{n-m} - 2b'_n a_{n-m} + b_n) - 1] \\ &= 2(a_n + ja_{n-m}) + 2jb'_n - 4jb'_n a_{n-m} - (1 + j). \end{aligned} \tag{46a}$$

Let us consider the effect of the first term on the spectrum of c_n. Now with L and $C(k\Omega)$ denoting respectively the period of a_n (and b_n) and the DFT of $a_n + ja_{n-m}$, we have*

$$\begin{aligned} C(k\Omega) &= [1 + je^{-j(2\pi/L)mk}]A(k\Omega) \\ &= 1 + e^{j[(\pi/2)-(2\pi/L)mk]}A(k\Omega). \end{aligned} \tag{46b}$$

Suppose that the scrambler produces a flat output spectrum (i.e., it would be a satisfactory scrambler if used solely in the serial mode), it is clear that $C(k\Omega)$ will have periodically spaced nulls. Since the energy in the timing tone is given by

$$R(\omega_s) = \sum_{k=0}^{N-1} |C(k\Omega)|^2 F(k\Omega) F(\omega_s - k\Omega), \tag{14}$$

* For the purposes of our discussion, we, in effect, assume that $b_n = 0$, i.e., $c_n = a_n + ja_{n-m}$.

any amplitude tapering provided by $|C(k\Omega)|^2$ could impair the timing recovery system. From (46) we have

$$\begin{aligned}|C(k\Omega)|^2 &= [1+\sin(2\pi/L)mk]^2+[\cos\,(2\pi/L)mk]^2\\ &= 2[1+\sin\,(2\pi/L)mk],\end{aligned}\tag{47}$$

where $k = 1, 2, \cdots, L$, and $m = 1, 2, \cdots, M$ with M being the number of stages in the scrambler. The strength of the tone, described by (14), will be particularly attenuated when $|C(k\Omega)|$ has a null at $k = L/2$, which corresponds to a frequency of $\omega_s/2$. It is easy to see that for some values of "m," the attenuation of the tone can be quite severe near $\omega_s/2$ (i.e., $k = L/2$).

In practice, the remedy is to change the value of m so that the null occurs as far away from $\omega_s/2$ as is possible. Of course, this cannot be done prior to transmission since the exact value of ω_s is unknown.

In this section, we have described a possible pitfall associated with the use of a parallel scrambler configuration. In practice, whether or not there is severe attenuation of the timing tone depends on the details of the pulse shaping and the operation of the phase-locked loop.

XI. CONCLUSIONS

We have examined several problems occurring in data-transmission systems that employ envelope-derived timing recovery, adaptive equalization, and self-synchronizing scramblers. Several conclusions have been reached regarding both the individual and joint action of these subsystems.

(*i*) The performance of the envelope-derived timing recovery system can be significantly improved by narrow-zonal prefiltering of the received signal prior to extracting the envelope.

(*ii*) The technique of "precessing" the data symbols in a phase-modulated modem is sufficient to provide a timing tone in a large excess-bandwidth system, but does not provide a tone in a small excess-bandwidth system.

(*iii*) A complete description was given of the output period of a cascaded scrambler as a function of the number of stages. Of interest are the facts that the output period does not necessarily double with the addition of a stage, and that if a particular scrambler stage does not lock up, then no succeeding stage can lock up.

(*iv*) It was demonstrated that the parallel scrambler configuration can, via spectral cancellation, cause the strength of the timing tone to be attenuated.

XII. ACKNOWLEDGMENT

The authors would like to thank T. M. Dennis for apprising them of the interaction between the parallel scrambler configuration and the timing-recovery system.

REFERENCES

1. W. R. Bennett, "Statistics of Regenerative Digital Transmission," B.S.T.J., *37*, No. 6 (November 1958), pp. 1501–1542.
2. Y. Takasaki, "Timing Extraction in Baseband Pulse Transmission," IEEE Trans. Commun., *COM-20*, No. 5 (October 1972), pp. 877–884.
3. J. E. Savage, "Some Simple Self-Synchronizing Digital Data Scramblers," B.S.T.J., *46*, No. 2 (February 1967), pp. 449–487.
4. B. Gold and C. M. Rader, *Digital Processing of Signals*, New York: McGraw-Hill, 1969.
5. L. E. Franks and J. P. Bubrowski, "Statistical Properties of Timing Jitter in a PAM Timing Recovery Scheme," IEEE Trans. Commun., *COM-22*, No. 7 (July 1974), pp. 913–920.
6. A. J. Viterbi, *Principles of Coherent Communication*, New York: McGraw-Hill, 1966.
7. A. Gill, *Linear Sequential Circuits*, New York: McGraw-Hill, 1967.
8. H. Pollard, *Theory of Algebraic Numbers*, New York: John Wiley, 1950.
9. K. Nakamura and Y. Iwaderl, "Data Scramblers for Multilevel Pulse Sequences," NEC Research and Development, No. 26 (July 1972), pp. 53–63.