JOURNAL ON

COMMUNICATIONS

VOLUME XLV. MARCH 1994

CODING IN COMMUNICATIONS

Business – Research – Education

JOURNAL ON COMMUNICATIONS

A PUBLICATION OF THE SCIENTIFIC SOCIETY FOR TELECOMMUNICATIONS, HUNGARY

Editorial office
Budapest II. Gábor Áron u. 65.
1525 Budapest, P.O.Box 15.
Hungary, H–1525
Phone: (361) 135-1097
(361) 201-7471
Fax: (361) 135-5560
(361) 201-7471

Subscription rates
Hungarian subscribers
1 year, 12 issues 5300 HUF, single copies 650 HUF
Hungarian individual subscribers
1 year, 12 issues 860 HUF, single copies 110 HUF
Foreign subscribers
12 issues 150 USD, 6 English issues 90 USD, single copies 24 USD
Transfer should be made to the Hungarian Foreign Trade Bank, Budapest, H–1821, A/C No. MKKB 203-21411

JOURNAL ON COMMUNICATIONS is published monthly, alternately in English and Hungarian by TYPOTEX Ltd. H–1015 Bp. Batthyány u. 14., phone: (361) 202-1365, fax: (361) 212-2211. Publisher: Zsuzsa Votisky. Type-setting by TYPOTEX Ltd. Printed by Dabasi Jegyzetnyomda, Dabas, Hungary HUISSN 0866-5583

EDITORIAL

It's a great pleasure for me to have this special issue on Coding in Communications. Being active in nonparametric statistics I am an outsider lover of coding. In the early 70's, when I started, coding techniques had some role only in military communications. However, in the 80's, based on the developments in microelectronics and because of the demands of multiple user communications, coding became an every-day practice implying new challenging research problems.

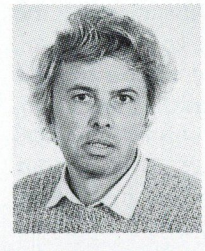
The papers by István Vajda and Anders Lundqvist are on such modern topics where algebraic codes are used not for error detection or correction, but for constructions of spreading signals or protocol sequences for code division multiple access channels. Here one has to design a code family which makes possible communication via a common channel not assuming a central intelligence. Each code from the family is assigned to a transmitter such that the disturbance of the others looks like an additive independent noise. Vajda made a survey on the various multiple access channel models, on the corresponding coding problems, bounds, and constructions. Lundqvist considered a specific case, made an efficient selection procedure in order to get codewords which have full cyclic order and are cyclically distinct.

The survey of Tamás Linder, Gábor Lugosi and Kenneth Zeger is on lossy universal source coding. In classical source coding (data compression) theory, on the one hand perfect reconstruction is required, on the other hand the probability distribution of the source is known. In many real life situations (speech, image, etc.) one allows some distortion, but the source distribution is unknown. Universality means that looking at a block of the source, the encoder is adapted to the actual source approaching the performance of codes designed according to the (unknown) probability distribution of the source.

The paper by Kálmán Elek and József Gaál suggests to revisit classical principles of communication engineers. Until the recent years, the main job of a communication engineer was to make an almost perfect channel for the given physical medium. It resulted in MODEM's, and the application of coding was very rare. Quite a few people questioned the conventional structure: coding → modulation → channel → demodulation → decoder. It turned out that there are essential reasons for changing this structure: either at the transmitter to make coded modulation, or at the receiver to combine the demodulation and decoding at some extent. This paper proves that it is really a good way to go, and it can be implemented using existing technology.

The paper by András Pataricza and Endre Selényi is on a recent interesting application of algebraic codes outside of communications: constructions of sequences for hardware testing. Although in testing and in communications the requirement on the sequences applied are very different, the structural properties of these codes, mainly Reed-Solomon codes, imply some of their applications in testing.

L. GYÖRFI



László Györfi received a degree in mathematics and physics in 1970 and the university doctor degree in 1974 from the Loránd Eötvös University, Budapest, Hungary, and the scientific degrees Candidate of Mathematical Sciences and Doctor of Mathematical Sciences from the Hungarian Academy of Sciences in 1978 and 1988, respectively. In the period from 1970 to 1975, he did research at the Telecommunication Research Institute within the field of stochastic approximation and pattern classification. In 1975, he joined the Research Group for Informatics and Electronics of the Hungarian Academy of Sciences. Since 1990 he has been the professor of mathematics at the Technical University of Budapest. His main interests are nonparametric estimation and multiple access communication. He served with Luc Devroye as a co-author of the book "Nonparametric Density Estimation: the L_1 View" (Wiley, 1985), and with Wolfgang Haerdle, Pascal Sarda, Philippe Vieu "Nonparametric Curve Estimation from Time Series" (Springer, 1989).

CODE CONSTRUCTIONS FOR CODE DIVISION MULTIPLE ACCESS CHANNELS

I. VAJDA

DEPARTMENT OF TELECOMMUNICATION
TECHNICAL UNIVERSITY OF BUDAPEST
H-1111 BUDAPEST, SZTOCZEK U. 2.

In the early 90's several significant civil applications showed up in the field of Code Division Multiple Access (CDMA) communications systems. One of the most important design points is the construction of CDMA code sets. This paper gives a brief overview on the basic approaches of code constructions together with presenting a few new results.

1. INTRODUCTION

Assume that there are T potential users in the communication system using the same channel. Simultaneously at most M users can be active out of T users, where M is typically much less than T. An active user can access the channel randomly in time, and typically there is no central time coordination in the system. Similarly there is no central coordination and access control in the available frequency domain. From these assumptions follows that the signals of active users can collide in the channel, which leads to the destruction of parts of messages. The effect of superposition of signals is described by channel models.

In order to minimize this unavoidable bad effects, some type of distributed control is established in such a system. One solution is to construct sets of signals for the T users where degradation is minimized in a random access enviroment. The signal sets are typically some mappings of codeword sets where the mapping is performed by some type of modulation. Fortunately the optimal selection can be made on codeword sets, because the signals inherit the optimality of codeword sets in these systems.

The task is to construct a set of codes $C = \{C_1, C_2, \ldots, C_T\}$, where C_i is the code of user i containing $|C_i|$ codewords. A codeword $c = (c_1, c_2, \ldots, c_L)$ is a sequence of length L and the elements of the codewords (characters) are from finite set F, shortly $c \in F^L$.

When designing the code usually we assume that the different users are time asynchronous at codeword level, but synchronous at character level. The reason for this assumption is the tractability of mathematical description. The results for case of character synchronism for typical systems can be generalized to character asynchronous channels. And also there are systems where a common character clock can be a practical assumption.

A multi-access code generally solves three-fold task:

- identification of active users (protecting the address information) (task i.),
- encoding data and its protection (data error or erasure correction at the receiver) (task ii.),
- synchronisation capability (reliable finding of the codeword time frames at the receiver) (task iii.).

A typical approach is when a so called protocol sequence (or signature sequence) is assigned to each user. Let the set of protocol sequences be denoted by C'

$$C' = \{c^{(1)}, c^{(2)}, \ldots, c^{(T)}\}, \; c^{(i)} \in F^L. \qquad (1)$$

In direct-sequential (DS) systems and in frequency-hopping (FH) systems these sequences are called signature sequences because each sequence is assigned to a user which identifies it. The term protocol sequence is mainly used in time hopping (TH) systems, where these are binary sequences and the ones of the sequences assign the time segments where a user may transmit a data packet. All these systems are called Code Division Multiple Access (CDMA) systems.

One design approach is when C' is contructed first in a way which solves tasks i.) and iii.). To get multi-access code an additional coding is superimposed on C' having data error protection capabilities. Here our main concern will be on underlying code C', but also show solutions on the secondary coding. There are methods where these two parts of code are constructed in one step in the same algebraic structure. In the sequel we describe the main code construction approaches for DS-, FH- and TH-CDMA systems.

2. DS-CDMA SYSTEMS

On Fig. 1. the block scheme of a DS-CDMA transmitter can be seen.

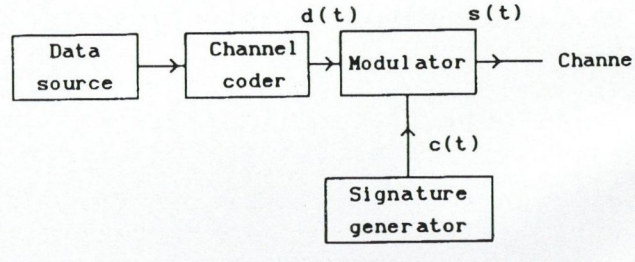


Fig. 1. The transmitter

The type of modulation is digital phase modulation, most often binary PSK. The output signal of the signature generator is a binary, $+1, -1$ valued c_n, $n = 0, 1, \ldots$ sequence

$$c(t) = c_n, \quad nT_c =\leq t < (n+1)T_c,$$

where T is the elementary time length (chip-time). The output of the channel encoder also a binary, $+1, -1$ valued d_m, $m = 0, 1 \ldots$ sequence

$$d(t) = d_m, \quad mT_s \leq t < (m+1)T_s,$$

where T_s is bit time and $T_s = LT_c$. The output of the modulator is

$$s(t) = \sqrt{2S}c(t) \cdot d(t) \cdot \sin(\omega_0 t + \phi), \qquad (2)$$

where ω_0 is the carrier frequency, S is the power constant and ϕ is the random phase of the carrier. Typically L equals to the period of the signature sequence denoted by c. Looking at product $c(t) \cdot d(t)$ as a coding method, data bit $d = +1$ is encoded into c and $d = -1$ is encoded into $-c$.

In Fig. 2. a star-like network topology can be seen.

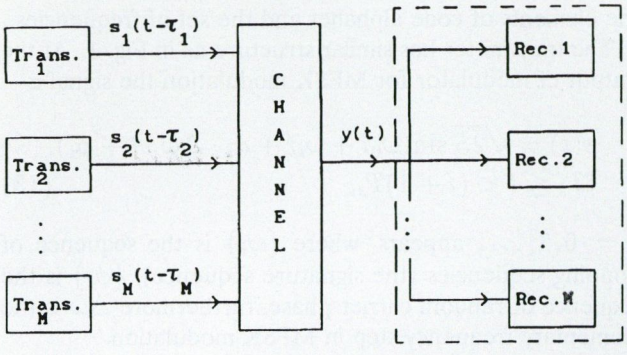


Fig. 2. The multi-access channel

The generators of code sequencies in the transmitter and the corresponding receiver have to run in time synchron. The most complex part of the corresponding receiver usually solves the code- and carrier-synchronization.

In many real systems the time frame detection is based on autocorrelation measurements between the incoming signal and its locally stored copy at the receiver. One usual method is the method of sliding correlation, when the local copy of the code sequence is shifted in phase step by step and at each step correlation is measured between the incoming code sequence and the shifted local copy. If the autocorrelation sidelobes are low enough then detection of in-phase step of shift can be made with acceptably small error probabilities in a multi-access, noisy enviroment. (Simon et.al. 1985).

At the output of an ideal distortion- and fading-free channel a sum of signals

$$y(t) = \sum_{i=1}^{M} \gamma_i s_i(t - \tau_i) + \nu(t) \qquad (3)$$

appears, where τ_i, $0 \leq \tau_i < T_w$ are the delay parameters and T_w is the time length of code sequence, furthermore γ_i, $0 < \gamma_i \leq 1$ are the attenuation parameters. In a jammer-free enviroment $\nu(t)$ is the additive receiver noise component. Having established code- and carrier-synchron, correlation type receiving is applied, i.e. the receiver calculates the integral

$$y' = \int_0^{T_b} y(t) \cdot [c(t) \cdot \cos(\omega_0 t + \phi)]dt\ . \qquad (4)$$

The result is a sum $y' = d + \nu$ of signal and noise components, from where $d' = \text{sign}(y')$ decision is made for data bit.

Adder channel models were assumed in Pursley (1977), Chung, Weldon (1979), Györfi, Vajda (1983) investigating DS-CDMA type multi-access communication channels. Considering adder channel (3) it is interesting to examine the bit error performance for randomly chosen $+1, -1$ valued code-sequences (Györfy, Vajda (1983)). Here citing only the simplest case of attenuation free and noiseless channel, $P(d \neq d')$ bit error probability can be bounded above by $\exp(-L/(2(M-1))$. This expression clearly shows the effect of code sequence length and number of active users on the performance. The examinations showed (Pursley et.al. (1982)) that for real codes this upper bound is practically applicable, even the more strict $\Phi(-\sqrt{L/(M-1)})$ approximation is useful. (Here Φ is the standard normal distribution function). So the information theoretic binary channel for the simple DS-CDMA can be modelled by a BSC channel with $p = \Phi(-\sqrt{L/(M-1)})$ crossover probabilities. This model can be used for initial selection of additional error correction codes.

Let's consider a code C'. The performance of a code is measured by auto- and crosscorrelation properties of its codewords. By these notations

$$\lambda_a = \max_{c \in C'} \max_{0<\tau<L} |\sum_{t=0}^{L-1} f(c_t, c_{t+\tau})| \qquad (5)$$

is the auto-correlation parameter and

$$\lambda_c = \max_{c \in C'_i, \bar{c} \in C'_j, i \neq j} \max_{0 \leq \tau < L} |\sum_{t=0}^{L-1} f(c_t, \bar{c}_{t+\tau}| \qquad (6)$$

is the cross-correlation parameter, where the addition in indices is taken modulo L. For $F = \{+1, -1\}$ and for

$$f(u, v) = u \cdot v, \qquad (7)$$

$u, v \in \{+1, -1\}$ we get conventional scalar-product correlation. Function f in (7) can be generalized to $f(u, v) = u \cdot v^*$, where F is a finite set of complex numbers and v^* is the complex conjugate of v.

The code C' is designed to minimize

$$\lambda_{max} = \max(\lambda_a, \lambda_c). \qquad (8)$$

Small value of λ_c is necessary in minimization of interferencies between signals of different active users and therefore necessary for maximization of identification capabilities at the receiver (task i.)).

The small value of λ_a is in connection with synchronization capabilities (task iii.)).

The requirement on minimal λ_{max} parameter partially comes from the requirement of simultaneous minimization of λ_a and λ_c and partially from technical reasons. Namely most of constructions is based on techniques of algebraic construction of linear cyclic codes where one parameter, the minimal Hamming-distance is optimized, which gives restrictions simultaneously on auto- and crosscorrelations between code words.

There exist a few useful bounds on λ_{max} under given T and N parameters for scalar-product-correlations (Welch (1974), Sidelnikov (1971)).

By the Welch's bound

$$(\lambda_{max}/L)^2 \geq (|C'| - 1)/(|C'| \cdot L - 1) \qquad (9)$$

which means that λ_{max} must be at least of the order $L^{1/2}$. Sarwate (1979) showed that one of parameters λ_a and λ_c can be small only at cost of large value of the other parameter. Namely

$$\lambda_c^2 + \left(\frac{L \cdot |C'| - 1}{L(|C'| - 1)}\right) \cdot \lambda_a^2 \geq L. \qquad (10)$$

From (10) it follows that

$$\lambda_{max} \geq L\sqrt{\frac{|C'| - 1}{L|C'| - 1}}, \qquad (11)$$

which is a form of Welch's bound. This bound applies also for complex valued sequences.

Sidelnikov-bound states that for any set of L or more binary sequences of period L

$$\lambda_{max} > (2L - 2)^{1/2}. \qquad (12)$$

For binary sequencies (12) gives asymptotically sharper lower bound than (11) for the case when $|C'| \geq L$.

The well known code constructions apply binary linear cyclic codes having large minimal Hamming distance, close to half of code length and select a subcode expurgating cyclic equivalents. The best known constructions are Gold- and Kasami-sets.

The $C'(T, L, \lambda_{max})$ set of so called Gold-sequences has parameters $C'(2^r + 1, 2^r - 1, 1 + 2^b)$, $b = \lfloor (r + 2)/2 \rfloor$, where $r \neq 0 \bmod 4$. This set is optimal with respect to the Sidelnikov-bound (Gold (1968)).

The $C'(T, L, \lambda_{max})$ set of so called small set of Kasami-sequences has parameters $C'(2^{r/2}, 2^r - 1, 1 + 2^{r/2})$, r is even. This set is optimal with respect to the Welch-bound (Gold (1968)).

While for FH- and TH-CDMA systems the design approach based solely on minimization of λ_{max} gives perfect solution, unfortunately for DS-CDMA systems minimization of λ_{max} gives only a partial solution for selecting good codes. We have no construction method for optimal DS-CDMA codes for the simple BPSK modulation mentioned above. The reason is that, because of code frame asynchronity, aperiodic correlations are calculated in the correlation receiver:

The sums in the right hand side of (5) and (6) are calculated for the entire codeword length and therefore called periodic correlation. Because the different users are (codeword) frame asynchronous therefore only parts of sequences coincide in the channel. Because multiaccess code C differs from protocol set C', at the receiver correlations are calculated between received codewords from C and local copies of elements from C' in a local time frame. Because of asynchronism leading and tailing portions of two codewords are in this time frame. If the two consecutive codewords carry different data bit then combinations of so called partial correlations can only be calculated and in a mixed way periodic and also partial correlations determine the performance. So criterion (8) may not correspond to any systems based on applying scalar-product correlations at the receiver. Although it can be argued that a signal set optimizing network performance has small value of λ_{max}, hence should find good signal sets among those with small λ_{max} (Sarwate, Pursley (1980), Massey, Uhran (1975), Pursley, Roefs (1979), Sarwate (1979), Vajda (1983/A)).

3. FH-CDMA SYSTEMS

There are many different coding-modulation methods for generation of frequency hopping signals. The essential part is the hopping (shifting) of the carrier frequency according to a non-binary code sequence. Having q frequencies available for transmission in the wideband channel, we construct an appropiate set of q-ary signature- (code-) sequencies, where there is a unique correspondence between the elements of code alphabet and the set of frequencies.

The transmitter has similar structure as in Fig. 1. At the output of modulator for MFSK modulation the signal is

$$s(t) = \sqrt{2S}\sin(\omega_0 t + \omega_i t + d_i \cdot \Delta\omega \cdot t + \phi_i),$$
$$iT_s \leq t < (i+1)T_s, \qquad (13)$$

$i = 0, 1, \ldots$, appears, where $\{\omega_i\}$ is the sequence of hopping sequencies (the signature sequence), $\{\phi_i\}$ is the sequence of random carrier phase, furthermore $\Delta\omega$ is the elementary frequency step in MFSK modulation.

The so called dwell-time T_h, the time duration of staying at a frequency before hopping can be longer or shorter than the symbol (typically data bit) time length. In the former case ($T_h \geq T_s$) we speak about Slow Frequency Hopping (SFH) and in the latter case ($T_h < T_s$) about Fast Frequency Hopping (FFH). In case SFH systems typically several source bits are transmitted on the same frequency (Simon et.al. (1985)).

Both FFH and SFH codes can be generated from appropriately chosen subsets of nonbinary cyclic codes. There are constructions based on Reed-Solomon codes (originally it has been described by Solomon (1973), but later discovered a few more times). Lempel, Greenberger (1974) gives the other basic construction based on nonbinary linear shiftregister sequences, which are really special nonbinary BCH codes. In this paper we give extensions on code constructions based on Reed-Solomon and also on BCH codes (Vajda (1992), Vajda (1993), Györfi, Vajda (1994)).

In the description of code performance the Hamming-correlation properties are used in FH and also in TH systems. Hamming-correlation is defined by the number of coincidences in the two sequences correlated. The code parameters λ_a and λ_c can be obtained from (5) and (6) by definition

$$f(u, v) = \begin{cases} 1, & \text{if } u = v \\ 0, & \text{otherwise} \end{cases}. \qquad (14)$$

The Hamming-correlation $\lambda_{i,j}(\tau)$ between codewords $c_i, c_j \in C$ at shift $\tau, \tau = 0, 1, \ldots, L-1$ is defined as the number of positions in which the correlated codewords coincide, i.e.

$$\lambda_{i,j}(\tau) = |\{u | 0 \leq u \leq L-1,\ c_{i,u} = c_{j,u+\tau}\}|, \qquad (15)$$

where addition of subscripts is carried out modulo L (Lempel-Greenberger (1974)). If the Hamming-correlation is h then the usual Hamming-distance is $L - h$.

3.1. FFH-CDMA systems

One type of FFH systems uses signal structure which can be described by a frequency-time matrix of dimensions $q \times L$, see Fig. 1.

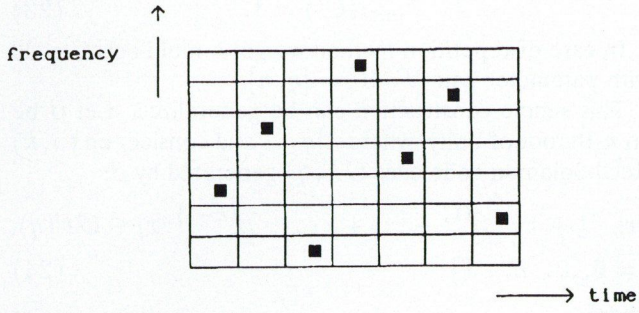


Fig. 3. The frequency-time matrix

The frequency-time matrix is a binary matrix of dimensions $q \times L$, where the rows correspond to q sub channels in the frequency range and the columns to L time slots on the time axis. This matrices have one element with value one in each column, resulting in L ones in matrices. Messages are mapped uniquely into such frequency-time matrices. This mapping can also be considered as a special block coding. After this encoding an on-off FSK type modulation is used to transmit the matrix, i.e. sine wave packets are transmitted in frequency-time cells (chips) corresponding to the one valued entries of the binary matrix. At the receiving end the chips are processed by energy detectors, making binary (0-1 valued) hard decisions. The channel noise can cause false detection, resulting in insertions or deletions of ones in chips.

The usual decision rule decides on the symbol (matrix) as the transmitted one, which has the most number of ones along the associated hopping pattern in the received binary matrix: i.e. the symbol decision results in symbol the assigned signal matrix to which has the maximal Hamming-correlation with the received binary matrix, where the Hamming-correlation measures the number of elements in which the two correlated matrices both have value one.

The channel model, when channel noise is neglected, is the OR-channel, which means that the elements of binary frequency-time matrices are superimposed by logical OR operation. The noisy OR-channel model is a cascade of a noiseless OR channel and a binary channel.

Performance of random coding for OR channels were examined in papers by Cohen et.al. (1971), Vajda et.al. (1980), Goodman et.al. (1980), Györfi, Kerekes (1981), Einarsson (1983), Einarsson, Vajda, Molnár (1987), Vajda (1991/A), Vajda (1991/B)).

First we introduce the concept using the simplest Reed-Solomon type construction. Let q be a prime power and β be an n-th root of unity, where $n|q-1$. Consider an $(n,2)$ Reed-Solomon code $\overline{C}$ over $GF(q)$ generated by β:

$$\overline{C} = \{x_0 \cdot \underline{1} + x_1 \cdot \underline{\beta}^{(1)} : x_1, x_0 \in GF(q)\}, \qquad (16)$$

where

$\underline{1} = (1,1,\ldots,1)$

$\underline{\beta}^{(1)} = (1,\beta^1,\ldots,\beta^{n-1})$.

Let's consider first the construction of an FFH-code (Simon et.al. (1985), Einarsson (1983), Healy (1985)). The task is to generate a set of q-ary codes, one code for each of the potential users. Let's partition $\overline{C}$ into a set $C_{FFH} = \{C_1, C_2, \ldots, C_T\}$, where the subset C_j is assigned to user j, $j = 1,2,\ldots,T$. Here C_j contains the following set of n-vectors over $GF(q)$:

$$C_j = \{a_j \cdot \underline{1} + m \cdot \underline{\beta}^{(1)} : m \in GF(q)\}\,. \qquad (17)$$

In (17) a_j is the address and m is the message of user j, where $m, a_j \in GF(q)$, $j = 1,2,\ldots,q$. Here we get $T = q$ and $|C_j| = q$, $j = 1,2,\ldots,q$. The Hamming-correlation between codewords of different users is at most 1 at any shift τ. The codewords inside a user's code (C_j) are not distinct cyclically. By shortening the code defined in (17) we can have codes also with length $L < n$ with the same correlation properties.

3.2. SFH-CDMA systems

In an SFH packet communication system, an active user sends a packet in each time slot on the selected frequency, where the selection is controlled by the frequency-hopping sequence (code sequence or signature sequence) (Pursley (1984), Pap (1991), Mohamed, Pap (1992) (1994)).

We consider a system where if more than one user transmits on the same frequency and same time slot, then colliding packets destroy each other. Because an active user does not have to know the subset of active users (the active subset of sequences) and has even less knowledge about the timing of other active sequences therefore he does not know at which positions will his sequence be hit. If there is a feedback then collided packets can be retransmitted. If there is no feedback available, some type of forward error (erasure) correction have to be used. Typically Reed-Solomon codes can be applied, which codes have optimal erasure correction capabilities (Blahut (1983)). In this case the C' set of signature sequencies and the mentioned erasure correction code together constitute multi-access code C. There are two basic methods for correction of collided packets: the methods of

- repetition and
- erasure correction coding.

Repetition

In case of repetition method the same packet is repeated along the frequency pattern prescribed by the SFH protocol sequence. Different SFH sequences can coincide in at most $\lambda_c = z$ positions. Let parameter M define the largest integer for which

$$M = \lfloor L/z \rfloor\,. \qquad (18)$$

If the number of simultaneously active users is M (including the tagged user), then $L-(M-1)z$ packets can be transmitted error free by each active user. Because it can happen that more than two packets coincide, therefore the value of M is a lower bound on the maximum number of simultaneously active users and typically much more than $L-(M-1)z$ packets can be transmitted succesfully from each of the M active users during a code sequence. For example if for the events of coincidences random model could be used, namely

in a given slot each user sends packet with probability $1/M$ then during L chosen slots the expected number of successes is

$$L(1-1/M)^{M-1} \approx L/e. \tag{19}$$

Here $L/e >> L-(M-1)z$. The worst case and average behavior can be far from each other also for real constructions.

Erasure correction

To get multi-access code C solving the three-fold task mentioned in introduction we have to add a further coding to C'. Assume that a total population of T users occasionally has traffic to send over a common frequency hopping packet communications channel. The codewords constructed above are used as signature sequences. The time length of these sequences is termed furtherly as length of a frame. One packet is transmitted at each hop. The packets have some fixed length. Let's associate the packets to elements of a large field $GF(Q)$. For instance if the packets are binary and have length b, we take $Q \geq 2^b$.

Assume that there is no feedback and the receiver can detect the collision of packets in the channel (using CRC for example). A collision generates an erasure. This way considering packets as elements from a large alphabet we can use erasure correction coding to improve the throughput. This means that redundancy packets are appended to a series of data packets.

Assume that each of the active users wants to transmit at least m messages successfully in a frame, where the frame corresponds to the length of the SFH sequences. Because a packet is considered as an element of $GF(Q)$, a "super" message of m packects is a series of m elements from $GF(Q)$. A series of redundant packets is appended to this message. If we assume only erasures, the best way of generating redundant packets is by using Reed-Solomon code with $GF(Q)$ as code alphabet. Each user applies an $(L, m, L-m+1)$ shortened Reed-Solomon code over $GF(Q)$, where $Q > L$ and applies its erasure correcting capability. For the number of active users a following obvious lower bound is obtained

$$M \geq \left\lfloor \frac{L-m}{\lambda_{max}} \right\rfloor + 1. \tag{20}$$

Introducing also the sum rate R_{sum} by

$$R_{sum} = \frac{M \cdot m}{L}(no.\ of\ successfull\ packets/slot), \tag{21}$$

the following lower bound results

$$R_{sum} \geq \frac{(L-m)\cdot m}{\lambda_{max} \cdot L}.$$

This bound is maximized by $m = L/2$ resulting in

$$R_{sum} \geq \frac{L}{4 \cdot \lambda_{max}}. \tag{22}$$

This last bound emphasizes the role of parameter L/λ_{max}.

Construction 1.

The easiest possibility to generate protocol sequence for SFH is (16) as follows: choose code C' of size $T = q$, such that one codeword is selected from each C_j, defined by (16). For instance, let's choose the codewords corresponding to $x_1 = 1$. The selected codewords are named as protocol (signature) sequences. For code C' we get

$$\lambda_{max}(C') = 1. \tag{23}$$

In case of repetition method we get a multi-access code with parameter pair $[T, M] = [q, n]$.

This simple construction can be generalized. Let β be an n-th root of unity, where $n|q-1$ and consider an (n, k) Reed-Solomon code over $GF(q)$ generated by β:

$$\{x_0 \cdot \underline{1} + x_1 \cdot \underline{\beta}^{(1)} + \ldots + x_{k-1} \cdot \underline{\beta}^{(k-1)} : x_i \in GF(q), i = 0, \ldots, k-1\}, \tag{24}$$

where

$\beta^{(i)} = (1, \beta^i \ldots, \beta^{i(n-1)})$,

$i = 0, 1, \ldots, k-1$. Two subsets of this code will be interesting for us.

Let's fix $x_1 = 1$ and let D denote the subset of set in (24) containing those codewords for which $x_1 = 1$. This way the cyclic equivalents of codewords and the codewords with inner period are expurgated from the code D. From here it is obtained that well known fact that

$$\lambda_{max}(D) = k-1.$$

Using D as an SFH code with additional erasure correction we get

$$T = q^{k-1}$$
$$M \geq \left\lfloor \frac{n}{2(k-1)} \right\rfloor + 1. \tag{25}$$

Construction 2.

An other construction can be based on cyclic concatenation. This construction has been introduced in (Vajda (1992), Vajda (1993)) where it was shown that the number of potential users, T can largely be increased, while the resulted parameter M can be kept close to parameter M provided by the above construction. This improvement is done on account of an increase in length of sequences.

This construction is based on the cyclic concatenation of special subcodes of two Reed-Solomon codes. The inner code is a cyclic code of prime length, the codewords of which have no inner period. This coding method is illustrated in Fig. 4.

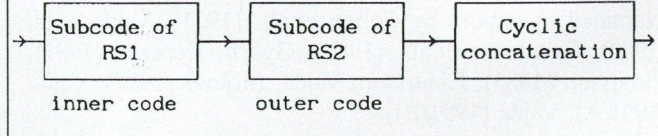


Fig. 4. The cascade coder

Let's consider an (n, k) code D defined above, where n is a prime number p and $p|q-1$. A subset is selected from D with size p^{r-1}. The inner code (RS2) is the set containing the elements of this subset and their cyclic shifts.

The outer code (RS1) is the subcode of an (N, K) Reed-Solomon code over $GF(p^r)$, generated by element δ according to rule (24), where $N|(p^r-1)$, furthermore

both x_0 and x_1 are kept fixed, namely $x_0 = 0$ and $x_1 = 1$.

The outer and inner codes are concatenated, where cyclic concatenation is applied (MacWilliams, Sloane (1977)).

Let N and n denote the code length of outer and inner code, resp.. Assume that $g.c.d.(N, n) = 1$. Using a one-to-one function h, the characters of the outer code are mapped into the codewords of the inner code. Considering the inner codewords as column vectors, we get a matrix B having n rows and N columns. The cyclic concatenation means that the i-th component of the resulted sequence c, $c \in C'$ is given by

$$c_i = B_{i \bmod n,\, i \bmod N}, \tag{26}$$

$i = 0, 1, \ldots, nN - 1$, where $B_{i,j}$ is the corresponding element of B.

In order to illustrate cyclic concatenation, let $n = 3$ and $N = 4$ and assume

$$B = \begin{array}{cccc} 0 & 1 & 2 & 3 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{array} \begin{array}{c} \\ 0 \\ 1 \\ 2 \end{array}$$

Applying rule (26) we get $c = (0,0,0,0,0,0,0,1,1,1,1,0,0)$.

Let c' be a cyclic shift of vector c. It is known (A, Györfi, Massey (1992)) that any cyclic shift of c in (26) uniquely corresponds to some cyclic shift of columns and rows of B. Let the matrix corresponding to c' be denoted by B'. For instance three times right cyclic shift of c in the above example, i.e.

$$c' = (1,0,0,0,0,0,0,0,0,0,1,1,1)$$

corresponds to matrix

$$B' = \begin{array}{cccc} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{array}$$

where B' is obtained from B by one step left shift of columns.

The Hamming-distance between c and c' is equal to the Hamming-distance between B and B'. The distance between B and B' is equal to the sum of distances between their corresponding columns. Futhermore the coloumns of B and also of B' are shifts of codewords of the inner code with well descibed distance properties. By this way it is easy to calculate the distance structure of code C'.

The inner code comes from Construction 1, where the length is restricted to be a prime number. The generalization is the use of an outer code with cyclic concatenation which preserves the property that the sequences must be cyclically different. If the rate of the outer code is low enough then the ratio $L/\lambda_{max}(L = nN)$ only slightly decreases. Comparing the code performance to Construction 1, it can be shown that the ratio of the number of potential users to sequence length (T/L) can be significantly increased, while the ratio of parameter λ_{max} to sequence length (λ_{max}/L) can be kept close to the same value of known construction.

(The detailed description of the construction as well as the evaluation is given in (Vajda (1993)).

Construction 3.

Let α be a primitive element of $GF(q^r)$, where q is a prime power. A primitive BCH code of length $n = q^r - 1$ is constructed based on field element α. The code D is defined by the parity-check polynomial $h(x)$:

$$h(x) = \prod_{j=0}^{s} M_j(x), \tag{27}$$

where $M_j(x)$ is the minimal polynomial of α^j over $GF(q)$ and $s < p$.

The minimum distance, d of code C can be bounded below by examining the set of roots of $h(x)$. The following lower bound can be obtained for the minimum distance of code D:

$$d \geq q^r - 1 - sq^{r-1}. \tag{28}$$

This way for the usual parameter triplet of D we get:

$$\begin{aligned} \text{length } (n) &= q^r - 1 \\ \text{size } (|C|) &= q^{sr+1} \\ \text{distance } (d) &\geq q^r - 1 - sq^{r-1}. \end{aligned} \tag{29}$$

Any cyclic code D can be generated by linear feedback shift register (LFSR) with characteristic polynomial $h(x)$. The structure of the code generator is shown on Fig. 5.

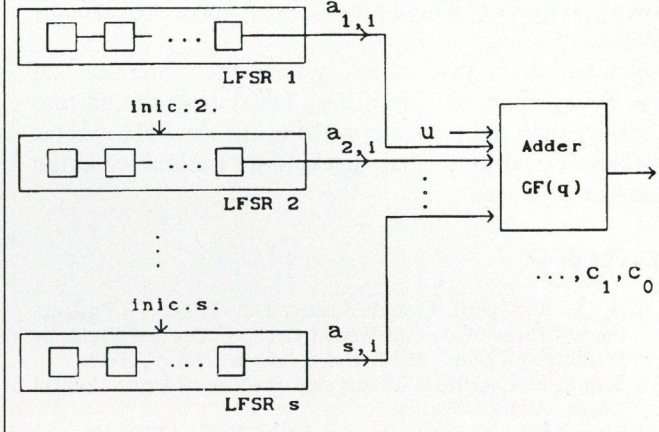


Fig. 5. The structure of the code generator

Taking the LFSR generation of the BCH code based on $h(x)$, where the initial load of component LFSR corresponding to polynomial $M_1(x)$ is kept to be a nonzero constant, we can get an C' code with parameters:

$$\begin{aligned} \text{length } (L) &= q^r - 1 \\ \text{size } (T) &= q^{(s-1)r+1} \\ \lambda_{max} &\leq sq^{r-1}. \end{aligned} \tag{30}$$

(The derivation of parameters (30) as well as the detailed description of the construction is given in (Györfi, Vajda (1994)).

It is interesting to compare ratios L/λ_{max} and T/L for this max BCH construction to the same ratios of the Lempel-Greenberger construction, which is a known SFH construction based on BCH codes over $GF(p)$ where p is

prime (Lempel, Greenberger (1974)). The parameters of the Lempel-Greenberger's LFSR code are

$$|\text{code abc}| = (q) = u^J$$
$$L = u^v - 1, \ (1 \geq J \geq v)$$
$$T = u^J$$
$$\lambda_{max} = u^{v-J},$$

where the value of T is limited above by q, i.e. by the number of frequencies. For this code obviously

$$T/L < 1,$$

furthermore

$$\lfloor L/\lambda_{max} \rfloor = q - 1. \tag{31}$$

For our code it can be seen that L/λ_{max} linearly decreases while T (and T/L) exponentially increases as parameter s increases. Namely

$$L/\lambda_{max} \geq \frac{q^r - 1}{sq^{r-1}} \approx \frac{q}{s}, \tag{32}$$

$$T/L = \frac{q^{(s-1)r+1}}{q^r - 1} \approx q^{(s-2)r}. \tag{33}$$

4. TH-CDMA

There are many different types of TH coding-modulation methods with common property that they transmit signals only in time slots associated to the ones of a binary protocol sequence. These protocol sequences are uniquely assigned to users.

Similarly as in case of FH-systems there are fast and slow TH systems. In case of fast TH systems the bit rate is smaller than the hop rate, while in the slow TH systems typically several source bits (packet) are transmitted in the time slot.

For fast TH systems (similarly as for FFH systems) a usual channel model is the OR channel or noisy OR channel. Performance of special random coding (random trellis coding) was examined in Cohen et.al. (1971) and Vajda et.al. (1980). In case of slow TH systems we assume that at those position where at least two ones of protocol sequences collide an erasure occurs. In cases of both slow and fast TH system we optimize the system in Hamming correlation (Lam, Sarwate (1986), Chung et.al. (1989), A, Györfi, Massey (1992), Györfi, Vajda (1994)).

Starting from SFH construction based on BCH code (point 3.2. above) binary protocol sequences can also be obtained with good performance properties Györfi, Vajda (1994). This construction has similarities to the SFH construction detailed in point 3.2.

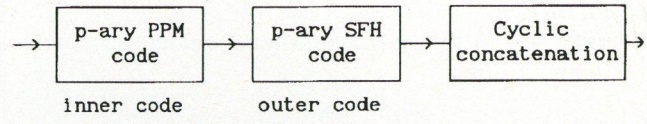


Fig. 6.

Namely here we chose q to be a prime number p. The mentioned p-ary SFH code is cyclically concatenated with a simple binary code. The simple code is called PPM (pulse-position-modulation) code consisting of all weight one sequences of length p.

For illustration if $p = 5$, then 0,1,2,3,4 elements of $GF(5)$ are encoded into PPM code words: (1,0,0,0,0), (0,1,0,0,0), (0,0,1,0,0), (0,0,0,1,0), (0,0,0,0,1).

Applying collision correction, similar to that detailed in 3.2., leads to binary protocol sequence sets with performance properties, better than those published in A, Györfi, Massey (1992).

REFERENCES

[1] N. Q., A., Györfi, L. and Massey, J. L. (1992): "Constructions of Binary Constant-Weight Cyclic Codes and Cyclically Permutable Codes", *IEEE Trans. Inform. Theory*, IT-37,

[2] Blahut, R. E.,(1983): Theory and Practice of Error Control Codes. Addison-Wesley.

[3] Chung, F. R. K., Salehi, J. A. and Wei, V. K. (1989): "Optical orthogonal codes: Design, Analysis and Applications", *IEEE Trans. Inform. Theory*, IT-35, 595-604.

[4] Chang, S. C. and Weldon, E. J. Jr., (1979): "Coding for T-user multiple access channels", *IEEE Trans. Inform. Theory*, IT-25, 684-691.

[5] Cohen, A. R., Heller, J. A. and Viterbi, A. J. (1971): "A new coding technique for high capacity mobile communication", *IEEE Trans. Commun. Tech.*, COM-15, 849-855.

[6] Einarsson, G. (1983): "Address assignment for a time-frequency-coded, spread-spectrum system", *Bell System Technical Journal*, Vol. 59, 3-9.

[7] Einarsson, G., Vajda, I. and Molnár, L. (1987): "Error probability of a code-division multiple access frequency hopping system", *Archiv für Electronic and Übertragungstechnik*, Hirzel Verlag Stuttgart, Vol. 41, 356-364.

[8] Einarsson, G., Molnár, L. and Vajda, I. (1985): "Error probability evaluation of a code-division multiple access frequency hopping system", *Technical Report TR-195*, TTT, University of Lund.

[9] Gold, R. (1968): "Maximal recursive sequences with 3-valued recursive cross-correlation functions", *IEEE Trans. Inform. Theory*, IT-14, 154-156.

[10] Goodman, D. J., Henry, P. S. and Prabhu, V. K. (1980): "Frequency-hopped multilevel FSK for mobile radio", *BSTJ*, Vol. 59, No. 7., 1257-1275.

[11] Györfi, L. and Kerekes, I. (1981): "A block code for noiseless asynchronous multiple access OR channels", *IEEE Trans.Inform. Theory*, IT-27, 788-791.

[12] Györfi, L. and Vajda, I. (1983): "Block coding and correlation decoder for M-user weighted adder channel", *Problems of Control and Inform. Theory*, Vol. 13, 405-417.

[13] Györfi, L. and Vajda, I. (1994): "Constructions of protocol sequences multi-access collision channels without feedback", *IEEE Trans. Inform. Theory*, Vol. 39, 1762-1765.

[14] Healy, T., (1985): "Coding and decoding for code division multiple user communication systems", *IEEE Trans. Communications*, COM-33, 310-316.

[15] IEEE Journal on Selected Areas in Communications, May 1990.

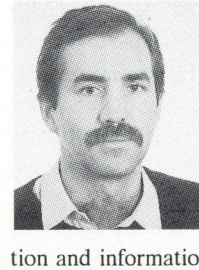
[16] IEEE Journal on Selected Areas in Communications, June 1990.

[17] Kasami, T. (1969): "Weight distribution of BCH codes", Combinatorial Mathematics and Its Applications, Chapel Hill, NC: Univ. of North Carolina Press.

[18] Lempel, A. and Greenberger, H. (1974): "Families of sequences with optimal Hamming-correlation properties", *IEEE Trans. Inform. Theory*, Vol. IT-20, 90-94.

[19] MacWilliams, F. J. and Sloane, N. J. A. (1977): The Theory of Error Correcting Codes. Amsterdam: North-Holland, 1977.

[20] Massey, J. L. and Uhran, J. J.,Jr. (1975): "Sub baud coding", Proc. 13th Annual Allerton Conf. on Circuit and System Theory, 539-547.
[21] Mohamed, K. A. and Pap, L. (1992): "Performance analysis of frequency-hopping unslottedpacket radio networks", Proceedings of ISSSTA-92, 115-118.
[22] Mohamed, K. A. and Pap, L. (1994): "Analysis of slotted frequency-hopped packet radio networks with random and deterministic hopping patterns", paper submitted to the IEEE ICC'94.
[23] Molnár, L. and Vajda, I. (1983): "Decoding error probability of the Einarsson-code for frequency-hopped multiple access channel", *Problems of Control and Inform. Theory*, Vol. 13, 109-120.
[24] Pap, L. (1991): "A szórt spektrumú kommunikáció néhány elméleti és gyakorlati problémája", Dissertation.
[25] Pursley, M. B. (1977): "Performance evaluation for phase-coded spread-spectrum multiple-access communications – Part I: System analysis", *IEEE Trans. Commun.*, COM-25, 795-799.
[26] Pursley, M. B. and Roefs, H. F. A. (1979): "Numerical Evaluation of Correlation Parameters for Optimal Phases of Binary Shift Register Sequences", *IEEE Trans. Commun.*, COM-27, 1597-1604.
[27] Pursley, M. B. (1984): "Frequency-hop transmission for satellite packet switching and terrestrial packet radio networks", Coordinated Science Laboratory Report, Report-144, July 1984.
[28] Pursley, M. B. and Stark, W. E. (1985): "Performance of Reed-Solomon Coded Frequency-Hop Spread-Spectrum Communications in Partial Band Interference", *IEEE Trans. Commun.*, COM-33, 767-774.
[29] Rowe, H. E. (1980): "Bound on the number of signals with restricted cross correlation", *IEEE Trans. Commun.*, COM-30.
[30] Sarwate, D. V. and Pursley, M. B. (1978): "Hopping patterns for frequency-hopped multiple-access communication", *IEEE Int. Conf. Commun.*, 7.4.1.-7.4.3.
[31] Sarwate, D. V. (1979): "Bounds on Crosscorrelation and Autocorrelation of Sequences", *IEEE Trans. Inform. Theory*, IT-25, 720-724.
[32] Sarwate D.V. and Pursley, M. B.(1980): "Cross-correlation Properties of Pseudorandom and Related Sequences", *Proceedings of the IEEE*, Vol. 68, 593-619.
[33] Sidelnikov, V. M. (1971): "On mutual correlation of sequences", *Soviet Math. Dokl.*, Vol. 12, 197-201.
[34] Simon, M. K., Omura, J. K., Scholtz, R. A. and Levitt, B. K. (1985): Spread Spectrum Systems. Vol. I-III., Computer Science Press.
[35] Solomon, G. (1973): "Optimal frequency hopping for multiple access", Proc. of the 1973, Symposium on Spread Spectrum Communications, Vol. 1, 33-35.
[36] Special Issue,(1977): Special Issue on Spread Spectrum Communications, *IEEE Trans. Commun.*, COM-25, August 1977.
[37] Special Issue, (1982): Special Issue on Spread Spectrum Communications, *IEEE Trans. Commun.*, COM-30, May 1982.
[38] Symp.Proc.,(1990): IEEE Symposium on Spread Spectrum Techniques and Applications, London 1990, Symposium Proceedings.
[39] Vajda, I., Kerekes, I., Györfi, L. and Gomez, H. (1980): "Remarks on a coding technique for asynchronous multiple access communication", *Problems of Control and Inform. Theory*, Vol. 9, 287-296.
[40] Vajda, I. (1983/A): "Kódosztásos többszörös hozzáférésű hírközlési csatornák kódválasztása", Dissertation.
[41] Vajda, I. (1983/B): "A coding rule for frequency-hopped multiple access channels", *Problems of Control and Inform. Theory*, Vol. 13, 331-335.
[42] Vajda, I. and Einarsson, G. (1987): "Code acquisition for a frequency hopping system", *IEEE Trans. Commun.*, COM-35, 566-568.
[43] Vajda, I. (1990/A): "AGC based on hard detected FFH signal matrices", *IEEE Electronics Letters*, Vol. 26, 218-219.
[44] Vajda, I. (1990/B): "On random code-hopping DS/SSMA systems", IEEE Symposium on Spread Spectrum Techniques and Applications, London 1990, Symposium Proceedings, 47-52
[45] Vajda, I. (1991/A): "Comments on Code-Division Multiple Access Techniques in Optical Fiber Networks", *IEEE Trans. Commun.*, COM-39.,196.
[46] Vajda, I. (1991/B): "Side information gained from signal matrices in spread spectrum systems", *Archiv für Electronic und Übertragungstechnik*, Hirzel Verlag Stuttgart, Vol. 45, 70-76.
[47] Vajda, I. and Nemetz, T. (1991/C): "Substitution of characters in q-ary m-sequences", in Lecture Notes in Computer Science 508, Springer-Verlag, 96-105.
[48] Vajda, I. (1992): "Code sequences for FH-CDMA channels", Proceedings of ISSSTA-92, 195-197.
[49] Vajda, I. (1993): "Code sequences for frequency-hopping multiple-access systems", submitted to the *IEEE Trans. Commun.*
[50] Viterbi, A. J. (1973): "A processing satellite transponder for multi access low rate mobile users", Digital Satellite Communications Conference, Montreal.
[51] Welch, L. R. (1974): "Lower bounds on the maximum cross correlation of signals", *IEEE Trans. Inform. Theory*, IT-20, 397-399.
[52] Zierler, N. (1959): "Linear recurring sequences", *J.SIAM.*, Vol. 7, No.1., 31-48.



István Vajda received the M.S. degree in electrical engineering from the Technical University of Budapest in 1976. He received the Ph.D. and the Candidate of Sciences degrees in 1978 and 1984, respectively. From 1976 to 1989 he was with the Research Group of Informatics and Electronics of H.A.S. Recently he is with the T.U. of Budapest as Associate Professor. His research interests are in communication and information theory, especially in Code Division Multiple Access Systems and Cryptography. Besides theoretical interests he took part in several development projects in these fields.

ON THE CONSTRUCTION OF CYCLICALLY PERMUTABLE CODES USING CYCLIC CODES OVER PRIME FIELDS

A. G. LUNDQVIST

LINKÖPING UNIVERSITY
DEPARTMENT OF ELECTRICAL ENGINEERING, DIVISION OF DATA TRANSMISSION
S-581 83 LINKÖPING, SWEDEN

We use an arbitrary linear cyclic $[n, k]$ code $\mathcal{C}$ over a prime field GF(p) (p odd prime) to construct binary constant-weight cyclically permutable codes of length N, weight w, and maximum cyclic correlation λ. By picking out exactly one representative from each cyclic equivalence class of size n in $\mathcal{C}$, we get a set of p-ary codewords suitable for use in asynchronous frequency-hopping systems. Using an orthogonal mapping, we map these codewords into a binary constant-weight ($N = np$, $w = n$) cyclically permutable code. This construction is better than or equally good as previously known constructions. An algorithm for selecting the representatives is described. The complexity of the algorithm is proportional to the maximum correlation of the resulting code. Finally we show how this construction works in the case when $\mathcal{C}$ is a BCH-code.

1. INTRODUCTION

The problem of reliable communication over an asynchronous communications channel can be solved in various ways. One traditional solution is to use a low-level communication protocol to ensure bit and frame synchronization, and to encode the data using a conventional error-correcting code. But, by instead using so called *comma-free codes* we may solve both these two problems, [7], [13]. The codes are self-synchronized, in the sense that the receiver can always detect the beginning of a codeword in a continuous bit-stream.

Recently, there has been a lot of activity in the area of coding for asynchronous code division multiple access (CDMA). One main problem has been the construction of spreading sequences (*e.g.* protocol sequences or signature sequences) suitable for use on a frame asynchronous OR-channel without feedback. It turns out that binary comma-free codes can be used to construct these codes, [1], [8]. In this paper we generalize the construction in [8].

Before going into a detailed description of the properties of these codes, we need to make some definitions.

We define the *cyclic order* of a codeword c, denoted by $|c|$, to be the smallest integer i greater than zero such that $\mathbf{S}^i(c) = c$, where $\mathbf{S}$ is the cyclic shift operator. A codeword is said to have *full cyclic order*, if the cyclic order of the codeword equals its length. Also, two codewords c and c' are said to be *cyclically distinct* if, for all integers i, $\mathbf{S}^i(c) \neq c'$.

The codewords in a comma-free code are all cyclically distinct.

We define the *minimum distance* of any code $\mathcal{C}$ as

$$d_{\min}(\mathcal{C}) \triangleq \min_{\substack{c,c' \in \mathcal{C} \\ c \neq c'}} d_H(c, c'),$$

where $d_H(\cdot)$ denotes the Hamming distance between the codewords. Further we define the *minimum cyclic distance* of any code $\mathcal{C}$ as

$$d_c(\mathcal{C}) \triangleq \min_{\substack{c,c' \in \mathcal{C} \\ i,j}} d_H(\mathbf{S}^i(c), \mathbf{S}^j(c')), \qquad (1)$$

where $c \neq c'$ or $i \not\equiv j \bmod N$. Note that if not all codewords have full cyclic order or if the codewords are not cyclically distinct then the minimum cyclic distance is zero.

1.1. Cyclically permutable codes

From now on, we will only consider one specific type of comma-free codes, the so called *cyclically permutable codes* (CP-codes). The CP-codes were introduced by Gilbert in [5]. They are also known as optical orthogonal codes (OOC's) in the literature on optical communications, [3], [4]. Throughout this paper we will use the name cyclically permutable, since these codes find applications outside the field of optical communication and, as we will soon show, they are not necessarily orthogonal.

An (N, w, λ) binary constant-weight cyclically permutable code (CW CP-code), $\mathcal{B}_{CP}$, of size M is a set of M binary vectors (codewords) $c = (c_0, c_1, \ldots, c_{N-1})$ of length N, weight w, and maximum correlation λ satisfying the following two properties:

1. The Autocorrelation Property:

$$\sum_{t=0}^{N-1} c_t c_{t \oplus \tau} \leq \lambda$$

for any $c \in \mathcal{B}_{CP}$ and any integer τ, $0 < \tau < N$.

2. The Cross-correlation Property:

$$\sum_{t=0}^{N-1} c_t c'_{t \oplus \tau} \leq \lambda$$

for any $c, c' \in \mathcal{B}_{CP}$, $c \neq c'$ and any integer τ, $0 \leq \tau < N$.

Note that $\oplus$ denotes addition modulo N. For a given weight w, length N, and maximum correlation λ we want the size of the CP-code to be as large as possible.

When $\mathcal{B}_{CP}$ is a constant-weight code, we have the following relationship between the correlation and the minimum cyclic distance:

$$d_c(\mathcal{B}_{CP}) = 2(w - \lambda).$$

From this follows that if $\lambda < w$ then all codewords in $\mathcal{B}_{CP}$ have full cyclic order and are also cyclically distinct.

The concept of CP-codes may also be extended to include non-binary codes, $\mathcal{C}_{CP}$. We demand that all codewords in $\mathcal{C}_{CP}$ have full cyclic order and that they are cyclically distinct.

1.2. Notation

As said before, $|c|$ denotes the cyclic order of a codeword c, but $|\cdot|$ will also be used to denote the multiplicative order of an element in a finite field and the size of a set. The context will convey the use. We let $m_\gamma(x)$ denote the minimal polynomial of $\gamma \in GF(p^r)$ over $GF(p)$. We know that

$$m_\gamma(x) = (x - \gamma)(x - \gamma^p) \cdots (x - \gamma^{p^{m-1}}),$$

where m is the smallest positive integer such that $\gamma^{p^m} = \gamma$. Parentheses $(\cdot)$ and angles $< \cdot >$ will be used to denote greatest common divisor (gcd) and least common multiple (lcm) respectively.

Definition 1 *Define $\mathcal{C}_\beta$ to be a linear cyclic code with parity-check polynomial $m_\beta(x)$.*

Definition 2 *Define $\mathcal{C}^* \triangleq \mathcal{C} \backslash \{0^n\}$ (where i^n is a constant vector $(i, i, \ldots, i)$ of length n) to be the set of all non-zero codewords in a code $\mathcal{C}$ of length n.*

Definition 3 *The direct sum of m equally long codes $\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_m$ is*

$$\sum_{i=1}^{m} \dot{\mathcal{C}}_i \triangleq \mathcal{C}_1 \dot{+} \mathcal{C}_2 \dot{+} \cdots \dot{+} \mathcal{C}_m \triangleq \{c_1 + c_2 + \cdots + c_m : c_i \in \mathcal{C}_i\}.$$

Definition 4 *The p-ary trace of an element $\gamma \in GF(p^r)$ is the sum*

$$Tr(\gamma) \triangleq \sum_{i=0}^{r-1} \gamma^{p^i}.$$

2. CONSTRUCTING THE CODES

In this section we will introduce a construction of binary CW CP-codes and non-binary CP-codes using an arbitrary p-ary (throughout this paper p will always be an odd prime) linear cyclic code, $\mathcal{C}$, of length n. We denote the set of codewords in $\mathcal{C}$ that have full cyclic order by $\mathcal{C}_{FCO}$. Since all codewords in $\mathcal{C}_{FCO}$ belong to a cyclic equivalence class of size n we can use one representative from each equivalence class to form a CP-code over GF(p), $\mathcal{C}_{CP}$. Finally, we will map the codewords in the p-ary code $\mathcal{C}_{CP}$ into a binary CP-code, $\mathcal{B}_{CP}$. We have the following relationship:

$$\mathcal{C} \supset \mathcal{C}_{FCO} \supset \mathcal{C}_{CP} \longleftrightarrow \mathcal{B}_{CP}.$$

2.1. Preliminaries

Let $\mathcal{C}$ denote a linear cyclic $[n, k]$ code over GF(p), where n and p are relatively prime. Let r be the multiplicative order of p modulo n, *i.e.* r is the smallest positive integer such that n divides $p^r - 1$. We may factor $g(x)$ and $h(x)$, the generator polynomial and the parity-check polynomial of $\mathcal{C}$, as

$$g(x) = \prod_{j=1}^{t} m_{\alpha_j}(x)$$

$$h(x) = \prod_{i=1}^{s} m_{\beta_i}(x)$$

and since n and p are relatively prime, so are all the polynomials m_{β_i} and $m_{\alpha_j}(x)$. We characterize the code $\mathcal{C}$ using one of the following sets:

$$A(\mathcal{C}) \triangleq \{\alpha_1, \alpha_2, \ldots, \alpha_t\},$$
$$B(\mathcal{C}) \triangleq \{\beta_1, \beta_2, \ldots, \beta_s\}.$$

2.2. Selecting Representatives

In order to construct the p-ary CP-code $\mathcal{C}_{CP}$ we need to select one representative from each cyclic equivalence class in $\mathcal{C}_{FCO}$. A trivial way of doing this is by considering one codeword at a time from $\mathcal{C}$. We first check if the codeword has full cyclic order, if it does we check to see if it is a cyclic shift of a previously accepted codeword. If not, we add this codeword to $\mathcal{C}_{CP}$ and repeat the process. Of course, this process is highly inefficient and in order to formulate a more efficient algorithm we need the following:

Lemma 1 *Let $\mathcal{C}$ be a linear cyclic code with $B(\mathcal{C}) = \{\beta_1, \beta_2, \ldots, \beta_s\}$. Then $\mathcal{C}^*$ may be partitioned in the following manner:*

$$\begin{aligned}\mathcal{C}^* &= \bigcup_{S \subseteq B(\mathcal{C})} \sum_{\beta \in S} \mathcal{C}^*_\beta \\ &= \mathcal{C}^*_{\beta_1} \cup \mathcal{C}^*_{\beta_2} \cup \ldots \cup \mathcal{C}^*_{\beta_s} \cup \\ &\quad (\mathcal{C}^*_{\beta_1} \dot{+} \mathcal{C}^*_{\beta_2}) \cup (\mathcal{C}^*_{\beta_1} \dot{+} \mathcal{C}^*_{\beta_3}) \cup \ldots \cup (\mathcal{C}^*_{\beta_{s-1}} \dot{+} \mathcal{C}^*_{\beta_s}) \cup \ldots \cup \\ &\quad (\mathcal{C}^*_{\beta_1} \dot{+} \mathcal{C}^*_{\beta_2} \dot{+} \cdots \dot{+} \mathcal{C}^*_{\beta_s}).\end{aligned}$$

Further, a partition $\mathcal{C}^*_{\beta_{i_1}} \dot{+} \mathcal{C}^*_{\beta_{i_2}} \dot{+} \cdots \dot{+} \mathcal{C}_{\beta_{j_m}}$ has the following properties:

1. *It is closed under the operation of cyclic shifts.*
2. *The codewords in it all have the same cyclic order, $< |\beta_{i_1}|, |\beta_{i_2}|, \ldots, |\beta_{i_m}| >$.*

Proof *Since the polynomials $m_{\beta_i}(x)$ are relatively prime, we may write the code $\mathcal{C}$ as a direct sum*

$$\mathcal{C} = \sum_{i=1}^{s} \mathcal{C}_{\beta_i} = \mathcal{C}_{\beta_1} \dot{+} \mathcal{C}_{\beta_2} \dot{+} \cdots \dot{+} \mathcal{C}_{\beta_s}$$

and we can uniquely write any codeword $c \in \mathcal{C}^*$ as $c = c_1 + c_2 + \cdots + c_s$, where $c_i \in \mathcal{C}_{\beta_i}$. Assuming that the codewords $c_{i_1}, c_{i_2}, \ldots, c_{i_m}$ are the nonzero codewords in this sum, then the set of indices $\{i_1, i_2, \ldots, i_m\}$ uniquely determines the partition that c belongs to. Property 1 follows directly from the additivity of the shift operator. In order to prove Property 2, we first need to show that

$$c \in \mathcal{C}^*_\beta \Rightarrow |c| = |\beta|.$$

We know from [6, p.63] that since $m_\beta(x)$ is irreducible, all nonzero codewords generated by $g(x) = (x^{|\beta|} -$

$1)/m_\beta(x)$ have order $|\beta|$. Since $|\beta|$ divides n, the length of the code, all nonzero codewords generated by $g'(x) = (x^n - 1)/m_\beta(x)$ also have order $|\beta|$. This follows from the fact that the codewords generated by $g'(x)$ are the codewords generated by $g(x)$ repeated $n/|\beta|$ times, which can be seen if we expand $g'(x)$ in the following manner:

$$g'(x) = \frac{x^n - 1}{m_\beta(x)} = (x^{n-|\beta|} + \cdots + x^{|\beta|} + 1)\frac{x^{|\beta|} - 1}{m_\beta(x)}$$
$$= (x^{n-|\beta|} + \cdots + x^{|\beta|} + 1)g(x).$$

Since the cyclic order of the sum of two codewords is the least common multiple of the cyclic order of the codewords, the second property directly follows.

All codewords in a partition $\mathcal{C}^*_{\beta_{i_1}} \dot{+} \mathcal{C}^*_{\beta_{i_2}} \dot{+} \cdots \dot{+} \mathcal{C}^*_{\beta_{i_m}}$ have the same cyclic order and all codewords in a cyclic equivalence class are contained in the same partition. This implies that we need only to consider the partitions where the codewords have full cyclic order and select representatives for the cyclic equivalence classes contained therein. The following theorem shows how to extract one representative from each cyclic equivalence class in a partition where the codewords have full cyclic order.

Theorem 1 *Let* $\mathcal{C} = \mathcal{C}^*_{\beta_1} \dot{+} \mathcal{C}^*_{\beta_2} \dot{+} \cdots \dot{+} \mathcal{C}^*_{\beta_m}$ *and assume* $\langle |\beta_1|, |\beta_2|, \ldots, |\beta_m| \rangle = n$ *and* $\deg m_{\beta_i}(x) = r$ *for all* i, $1 \le i \le m$. *Further, let* α *be a primitive element of GF*(p^r) *and let*

$$\gamma_i \triangleq (p^r - 1)\frac{\langle |\beta_1|, |\beta_2|, \ldots, |\beta_{i-1}| \rangle}{\langle |\beta_1|, |\beta_2|, \ldots, |\beta_i| \rangle}. \qquad (2)$$

Then a set of representatives for all $(p^r - 1)^m/n$ *cyclic equivalence classes of size* n *in* $\mathcal{C}$ *may be written as the direct sum*

$$\sum_{i=1}^{m} \mathcal{C}'_{\beta_i} = \mathcal{C}'_{\beta_1} \dot{+} \mathcal{C}'_{\beta_2} \dot{+} \cdots \dot{+} \mathcal{C}'_{\beta_m},$$

where

$$\mathcal{C}'_{\beta_i} \triangleq \{c(\alpha^{e_i}, \beta_i) \triangleq (\mathrm{Tr}(\alpha^{e_i}\beta_i^{-0}), \mathbf{Tr}(\alpha^{e_i}\beta_i^{-1}), \ldots,$$
$$\mathrm{Tr}(\alpha^{e_i}\beta_i^{-(n-1)})) : 0 \le e_i < \gamma_i\}.$$

The proof of this theorem can be found in Appendix A.

Now, using Lemma 1 and Theorem 1 we can construct $\mathcal{C}_{CP}$ using the following algorithm:

Algorithm 1:

Let $\mathcal{C}$ be a linear cyclic code of length n with $B(\mathcal{C}) = \{\beta_1, \beta_2, \ldots, \beta_s\}$.

1. Let $\mathcal{C}_{CP} \leftarrow \emptyset$.
2. Iteratively consider all subsets $S = \{\tilde{\beta}_1, \tilde{\beta}_2, \ldots, \tilde{\beta}_m\}$ of $B(\mathcal{C}) = \{\beta_1, \beta_2, \ldots, \beta_s\}$. If $\langle S \rangle = \langle |\tilde{\beta}_1|, |\tilde{\beta}_2|, \ldots, |\tilde{\beta}_m| \rangle = n$ then let

$$\mathcal{C}_{CP} \leftarrow \mathcal{C}_{CP} \cup \sum_{i=1}^{m} \mathcal{C}'_{\tilde{\beta}_i}.$$

The number of subsets that needs to be considered is 2^s, hence this algorithm is only efficient for small values of s.

The size of the resulting code is given by the following theorem:

Theorem 2 *If* $\deg m_\beta(x) = r$ *for all* $\beta \in B(\mathcal{C})$ *then*

$$M \triangleq |\mathcal{C}_{CP}| = \frac{1}{n} \sum_{\substack{S \subseteq B(\mathcal{C}) \\ \langle S \rangle = n}} (p^r - 1)^{|S|},$$

where $\langle S \rangle$ *denotes the least common multiple of the multiplicative orders of the elements in* S, *i.e. if* $S = \{\beta_1, \beta_2, \ldots, \beta_m\}$ *then* $\langle S \rangle = \langle |\beta_1|, |\beta_2|, \ldots, |\beta_m| \rangle$. *If there are at least* v *roots of multiplicative order* n *in* $B(\mathcal{C})$ *then*

$$M \ge \frac{p^k - p^{k-rv}}{n}.$$

The proof of this theorem can be found in Appendix A.

A direct consequence of Theorem 2 is that if all s roots in $B(\mathcal{C})$ have full multiplicative order then the size of $\mathcal{C}_{CP}$ equals

$$M = \frac{p^k - 1}{n}.$$

If we choose to consider $\mathcal{C}_{CP}$ as a p-ary CP-code then $d_c(\mathcal{C}_{CP}) \ge d_{\min}(\mathcal{C})$. This follows directly from the fact that $d_c(\mathcal{C}_{CP}) = d_{\min}(\mathcal{C}_{FCO})$ and that $\mathcal{C}_{FCO} \subset \mathcal{C}$, because then $d_c(\mathcal{C}_{CP}) = d_{\min}(\mathcal{C}_{FCO}) \ge d_{\min}(\mathcal{C})$.

kth-Order Near-Orthogonal Codes

Algorithm 1 may be interesting also from another point of view. The problem of selecting one representative from each cyclic equivalence class of size n in a Reed-Solomon code, has been treated in [11], [12], and [14] in connection with the construction of so called asynchronous kth-order near-orthogonal codes. These codes may be used as hopping patterns in time-asynchronous frequency-hopping spread-spectrum communication systems, by letting the symbols in a codeword correspond to frequency-time (FT) slots. The properties of these codes guarantee that any two codewords will not overlap in more that k FT slots.

If we let $\mathcal{C}$ be an $[n, k]$ RS-code with $B(\mathcal{C}) = \{\alpha^1, \alpha^2, \ldots, \alpha^k\}$ then $\mathcal{C}_{CP}$ will be an asynchronous kth-order near-orthogonal code. We also note that a subset of the CP-code generated by a code with $B(\mathcal{C}) = \{\alpha^0, \alpha^{-1}, \alpha^{-2}\}$ is used in a frequency-hopping scheme by Vajda and Einarsson [15]. They show that this code has some desirable synchronization properties.

The selection procedure presented in this paper is somewhat similar to the one in [12], although that procedure only deals with the case when $\mathcal{C}$ is a Reed-Solomon (RS) code of primitive length, $n = p - 1$. Another algorithm, also restricted to primitive RS-codes, is presented in [14] and gives the same result as our procedure if we, when we partition the code $\mathcal{C}$, only consider partitions $\mathcal{C}^*_{\beta_{i_1}} \dot{+} \mathcal{C}^*_{\beta_{i_2}} \dot{+} \cdots \dot{+} \mathcal{C}^*_{\beta_{i_m}}$ where $|\beta_i| = p - 1$ for some $i \in \{i_1, i_2, \ldots, i_m\}$. The size of the code will then be $M = (p^k - p^{k-v})/(p-1)$.

2.3. A Binary Cyclically Permutable Code

The codewords in the p-ary CP-code $\mathcal{C}_{CP}$ can also be used to construct a binary CW CP-code $\mathcal{B}_{CP}$. As in [1], we map each codeword $c = (c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}_{CP}$ into a binary matrix A of size $p \times n$ where column i in

A corresponds to symbol i in c. The mapping from the symbols in c to the columns of the matrix A is defined by

$$0 \mapsto (100\ldots0)^T$$
$$1 \mapsto (010\ldots0)^T$$
$$\vdots$$
$$p-1 \mapsto (000\ldots1)^T.$$

Consider the resulting $p \times n$ matrix is

$$A = \begin{pmatrix} a_{0,0} & a_{0,1} & \cdots & a_{0,n-1} \\ a_{1,0} & a_{1,1} & \cdots & a_{1,n-1} \\ \vdots & & & \vdots \\ a_{p-1,0} & a_{p-1,1} & \cdots & a_{p-1,n-1} \end{pmatrix}.$$

When n and p are relatively prime the Chinese remainder theorem [2, p.285] specifies a one-to-one correspondence between such matrices A and np-tuples $b = (b_0, b_1, \ldots, b_{np-1})$ in the manner that

$$b_i = a_{i \bmod p, i \bmod n}.$$

The code $\mathcal{B}_{CP}$ is defined to be the set of binary vectors corresponding to the p-ary codewords in $\mathcal{C}_{CP}$.

Definition 5 *Let $\mathcal{C}$ be a cyclic $[n,k]$ code such that $1 \notin B(\mathcal{C})$. Define $\mathcal{C}^+$ to be a linear cyclic $[n,k+1]$ code such that $B(\mathcal{C}^+) = B(\mathcal{C}) \cup \{1\}$.*

Theorem 3 *If $\mathcal{B}_{CP}$ is the set of binary codewords corresponding to $\mathcal{C}_{CP}$ then*

$$d_c(\mathcal{B}_{CP}) = \begin{cases} \geq 2d_{\min}(\mathcal{C}^+) & \text{if } 1 \notin B(\mathcal{C}) \\ 0 & \text{if } 1 \in B(\mathcal{C}) \end{cases}.$$

The proof of this theorem can be found in Appendix A.

Using the following lemma we may evaluate the bound in the case when $\mathcal{C}^+$ is a BCH-code.

Lemma 2 *Let $\mathcal{C}$ be a linear cyclic code such that $1 \notin B(\mathcal{C})$. Further, let α be an nth primitive root of unity in GF(p^r). If $B(\mathcal{C}^+) = \{\alpha^{j_0}, \alpha^{j_0+1}, \ldots, \alpha^{j_0+s}\}$ for some integer j_0 and $\deg m_\beta(x) = r$ for all $\beta \in B(\mathcal{C})$ then*

$$d_{\min}(\mathcal{C}^+) \geq n - sp^{r-1}.$$

Proof: From the definition of BCH-codes [2, p.166] it follows that if $A(\mathcal{C}^+)$ contains $d-1$ successive powers of α, then $d_{\min}(\mathcal{C}^+) \geq d$. Now, since

$$A(\mathcal{C}^+) \supseteq \{\alpha^{(j_0+s)p^{r-1}+1}, \ldots, \alpha^{n-1+j_0p^{r-1}}\}$$

contains $n - sp^{r-1} - 1$ successive powers of α, we have $d_{\min}(\mathcal{C}^+) \geq n - sp^{r-1}$.

The following lemma may be used to identify elements in GF(p^r) that have a minimal polynomial of degree r:

Lemma 3 *Let α be an nth primitive root of unity in GF(p^r). Then $\deg m_{\alpha^i}(x) = r$ if $0 < |i| \leq \lfloor n/p^{r-1} \rfloor$.*

Proof: Denote the set of logarithms of the roots of $m_{\alpha^i}(x)$ by A_i. We know that $A_i = \{ip^j \bmod n : 0 \leq j \leq r-1\}$. The size of A_i, or equivalently the degree of $m_{\alpha^i}(x)$, is equal to r if $|i|p^{r-1} \leq n$ and $i \neq 0$. Since $0 < |i| \leq \lfloor n/p^{r-1} \rfloor$ we have

$$|i|p^{r-1} \leq \left\lfloor \frac{n}{p^{r-1}} \right\rfloor p^{r-1} \leq n.$$

Construction 1

We are now ready to summarize. Let $\mathcal{C}$ be a linear cyclic $[n,k]$ code over GF(p) and let α be an nth primitive root of unity in GF(p^r). Let $B(\mathcal{C}^+) = \{\alpha^{j_0}, \alpha^{j_0+1}, \ldots, \alpha^{j_0+s}\}$ where $-\lfloor n/p^{r-1} \rfloor \leq j_0 \leq 0$ and $s + j_0 \leq \lfloor n/p^{r-1} \rfloor$. Then $\mathcal{B}_{CP}$ is an $(N = np, w = n, \lambda \leq sp^{r-1})$ binary CW CP-code of size

$$M = \frac{1}{n} \sum_{\substack{S \subseteq B(\mathcal{C}) \\ \langle S \rangle = n}} (p^r - 1)^{|S|}.$$

If $j_0 = -1$ then $B(\mathcal{C}^+) = \{\alpha^{-1}, \alpha^0, \ldots, \alpha^{s-1}\}$ and from Theorem 2 follows that $M \geq (p^k - p^{k-2r})/n$ since both α^{-1} and α^1 have multiplicative order n. If $\mathcal{C}$ is an RS-code ($r = 1, s = k$) then, under the same conditions as above, we will get a binary $(N = np, w = n, \lambda \leq k)$ CW CP-code of size $M \geq (p^k - p^{k-2})/n$.

2.4. Conclusion

If we compare our construction of binary CW CP-codes with other constructions also based on linear cyclic codes, we find that our construction is better or equally good.

In [1] an $[n,k]$ RS-code over GF(p) is used to construct an $(N = np, w = n, \lambda \leq k)$ CP-code, where the size of the resulting code is $M = p^{k-1}$. Given the same length, weight, and correlation our construction yields at least $M \geq (p^k - p^{k-2})/n$ codewords which is strictly greater than p^{k-1}. If we use non-primitive ($n \neq p-1$) RS-codes, our construction gives a factor of approximately $(p-1)/n$ more codewords.

A construction of a code with the same parameters as above is presented in [8]. This construction is based on an $[n,k]$ BCH-code over GF(p) and the size of the resulting code is $M = p^{k-r}$. Our construction yields $M \geq (p^k - p^{k-2r})/n$ codewords which is strictly greater. Again, if a non-primitive code length is used our construction gives a factor of approximately $(p^r - 1)/n$ more codewords.

In [9] and [10] we find constructions that in some cases coincide with ours when $j_0 = 0$. But by varying j_0 in our construction, which does not change the other parameters of the resulting code, it is in some cases possible to increase the size.

We have also presented an algorithm to select one representative from each cyclic equivalence class of size n in a linear cyclic code. This algorithm provides us with a systematic method of constructing our codes. The complexity of the algorithm is exponential in s, but since s is proportional to the correlation and a low correlation is desirable this is not prohibitive.

A. PROOFS

The following lemma is a reformulation of Theorem 6.5.1 in [16]. The proof can be found on p. 78 in [16].

Lemma 4 *Let β be an element in GF(p^r). If $\deg m_\beta(x) = r$ then the $[n,r]$ code $\mathcal{C}_\beta$ over GF(p) with parity-check polynomial $m_\beta(x)$ is given by*

$$\mathcal{C}_\beta = \{c(\xi,\beta) \triangleq (\mathrm{Tr}(\xi\beta^{-0}), \mathrm{Tr}(\xi\beta^{-1}), \ldots, \mathrm{Tr}(\xi\beta^{-(n-1)})) : \xi \in GF(p^r)\}\ .$$

Note that $c(\beta\xi,\beta)$ corresponds to a cyclic shift of $c(\xi,\beta)$.

Proof of Theorem 1: In order to simplify the notation we will first define the following:

$$b_i \triangleq |\beta_i|,$$
$$n_i \triangleq \langle |\beta_1|, |\beta_2|, \ldots, |\beta_i| \rangle .$$

First we prove that the number of codewords defined by $\gamma = (\gamma_1, \gamma_2, \ldots, \gamma_m)$ is indeed $(p^r-1)^m/n$. This follows directly from

$$\prod_{i=1}^{m} \gamma_i = \prod_{i=1}^{m} (p^r-1)\frac{\langle b_1, \ldots, b_{i-1}\rangle}{\langle b_1, \ldots, b_i\rangle} = \frac{(p^r-1)^m}{\langle b_1, \ldots, b_m\rangle} = \frac{(p^r-1)^m}{n}.$$

Next we proceed to show that all codewords are cyclically distinct. Consider the two codewords

$$c = \sum_{i=1}^{m} c(\alpha^{e_i}, \beta_i) \in \mathcal{C}_{CP}$$

and

$$c' = \sum_{i=1}^{m} c(\alpha^{e_i'}, \beta_i) \in \mathcal{C}_{CP},$$

where $0 \le e_i, e_i' < \gamma_i$. Assume that c' is a cyclic shift of c. Then as a consequence of Lemma 4.

$$\alpha^{e_i'} = \alpha^{e_i}\beta_i^s \quad 1 \le i \le m \tag{4}$$

for some integer s. We will prove that $c = c'$ by showing that (4) implies $e_i' = e_i$, $1 \le i \le m$. The proof will be of the following form:

1. Show that if $b_{i-1} \mid s$ for all i such that $0 \le i < j$ then $e_j' = e_j$.
2. Show that $e_j' = e_j$ implies $b_j \mid s$.

The first step, $b_0 \mid s$, is trivially true since we may define b_0 to equal one. The second implication follows directly from (4). Since $\alpha^{e_j'} = \alpha^{e_j}\beta_j^s$ and $e_j' = e_j$ we have $\beta_j^s = 1$ and $|\beta_j| = b_j \mid s$. Let f_i be an integer such that $\beta_i = \alpha^{f_i}$. We will now prove the first implication by rewriting (4) as

$$e_i' \equiv e_i + sf_i \bmod p^r - 1 \quad 1 \le i \le m$$

or, equivalently

$$e_i' - e_i \equiv sf_i \bmod p^r - 1 \tag{5}$$

for all $1 \le i \le m$. Because the left-hand side of (5) is bounded by $|e_i' - e_i| < \gamma_i$ and since $\gamma_i \mid (p^r-1)$ we may conclude that

$$e_i' - e_i \in (\gamma_i) \Leftrightarrow e_i' - e_i = 0, \tag{6}$$

where (γ_i) denotes the cyclic group generated by γ_i under the operation addition modulo p^r-1. Since $b_i \mid s$ for all i, $0 \le i < j$, we know that $\langle b_1, b_2, \ldots, b_{j-1}\rangle = n_{j-1} \mid s$. This implies that the set of values that the right-hand side of (5) can assume is $(f_j n_{j-1})$. We will show that this is a subset of (γ_j) by showing that $f_j n_{j-1}$ is a multiple of γ_j. By definition

$$\gamma_j = (p^r-1)\frac{n_{j-1}}{n_j}.$$

By multiplying both sides by f_j and rearranging terms, we arrive at

$$f_j n_{j-1} = \gamma_j \frac{f_j n_j}{p^r-1}. \tag{7}$$

Note that we may express the multiplicative order of a root as

$$b_i = \frac{p^r-1}{(p^r-1, f_i)}$$

which we may rewrite as

$$\frac{p^r-1}{b_j} = (p^r-1, f_j) \Rightarrow \frac{p^r-1}{b_j}\,\Big|\, f_j \Rightarrow (p^r-1)\frac{n_j}{b_j}\,\Big|\, f_j n_j.$$

Since $b_j \mid n_j \triangleq \langle b_1, b_2, \ldots, b_j\rangle$ we conclude that $(p^r-1) \mid f_j n_j$ and $f_j n_j/(p^r-1)$ is an integer. This, together with (7), shows that $f_j n_{j-1}$ is a multiple of γ_j and $(f_j n_{j-1}) \subseteq (\gamma_j)$. Finally, by (6) we conclude that $e_j' = e_j$. We have now proved that all codewords are cyclically distinct, and this concludes the proof.

Lemma 5 *Let $\mathcal{C}$ be a linear cyclic $[n,k]$ code over GF(p). Then*

$$|\mathcal{C}_{CP}| = \frac{1}{n}\sum_{\substack{S \subseteq B(\mathcal{C}) \\ \langle S\rangle = n}} \prod_{\beta\in S} (p^{\deg m_\beta(x)} - 1).$$

Proof: We know from Lemma 1 that all partitions with the property that the least common multiple of the multiplicative orders of the roots is equal to n, only contain codewords of full cyclic order. Hence,

$$|\mathcal{C}_{FCO}| = \Big|\bigcup_{\substack{S \subseteq B(\mathcal{C}) \\ \langle S\rangle = n}} \sum_{\beta\in S} \mathcal{C}_\beta^*\Big| = \sum_{\substack{S \subseteq B(\mathcal{C}) \\ \langle S\rangle = n}} \Big|\sum_{\beta\in S} \mathcal{C}_\beta^*\Big|$$
$$= \sum_{\substack{S \subseteq B(\mathcal{C}) \\ \langle S\rangle = n}} \prod_{\beta\in S} |\mathcal{C}_\beta^*| = \sum_{\substack{S \subseteq B(\mathcal{C}) \\ \langle S\rangle = n}} \prod_{\beta\in S} (p^{\deg m_\beta(x)} - 1).$$

In order to get $\mathcal{C}_{CP}$ we need to pick one codeword from each cyclic equivalence class in $\mathcal{C}_{FCO}$, hence the size of $|\mathcal{C}_{CP}|$ is

$$|\mathcal{C}_{CP}| = \frac{|\mathcal{C}_{FCO}|}{n} = \frac{1}{n}\sum_{\substack{S \subseteq B(\mathcal{C}) \\ \langle S\rangle = n}} \prod_{\beta\in S} (p^{\deg m_\beta(x)} - 1).$$

Proof of Theorem 2: Combining Lemma 5 with the fact that $\deg m_\beta(x) = r$ for all $\beta \in B(\mathcal{C})$ proves the first part of the theorem. The second part is proved by rewriting (3) by summing over the complement. Note that summing over all subsets gives us p^k, so

$$M = \frac{1}{n}\sum_{\langle S\rangle = n} (p^r-1)^{|S|} = \frac{1}{n}\left(p^k - \sum_{\langle S\rangle \ne n} (p^r-1)^{|S|}\right).$$

Now we assume that only those subsets containing at least one root of multiplicative order n have a least common multiple of n:

$$M \geq \frac{1}{n}\left(p^k - \sum_{i=0}^{s-v}\binom{s-v}{i}(p^r-1)^i\right) = \frac{p^k - p^{r(s-v)}}{n}$$
$$= \frac{p^k - p^{k-rv}}{n}.$$

Proof of Theorem 3: Consider the definition of minimum cyclic distance in (1). We now introduce some useful relations that are proved in [1, p. 941]. Let c be a codeword from $\mathcal{C}_{CP}$, A the corresponding binary matrix and b the binary vector. Further, let $\mathbf{R}$ denote the operator that shifts the columns of a matrix cyclically one step right-wards and let $\mathbf{D}$ denote the operator that shifts the rows cyclically one step down. Then:

$$\mathbf{S}^i(c) \longleftrightarrow \mathbf{R}^i(A)$$
$$c + i^n \longleftrightarrow \mathbf{D}^i(A)$$
$$\mathbf{S}(b) \longleftrightarrow \mathbf{DR}(A).$$

We can now conclude that each shift of b must correspond to some codeword c in $\mathcal{C}_{FCO}$ with some constant vector added to it:

$$d_c(\mathcal{B}_{CP}) = 2 \min_{\substack{c,c' \in \mathcal{C}_{FCO} \\ i,j \in GF(p)}} d_H(c + i^n, c' + j^n)$$
$$\geq 2 \min_{\substack{c,c' \in \mathcal{C} \\ i,j \in GF(p)}} d_H(c + i^n, c' + j^n)$$
$$= 2 \min_{\substack{c \in \mathcal{C} \setminus \{0^n\} \\ i \in GF(p)}} w_H(c + i^n).$$

The inequality follows from the fact that we minimize over $\mathcal{C}$ instead of $\mathcal{C}_{FCO} \subset \mathcal{C}$. First assume $1 \notin B(\mathcal{C})$. Adding the vectors $1^n, 2^n, \ldots, (p-1)^n$ to all codewords in the code $\mathcal{C}$ corresponds to adding a row consisting only of ones to the generator matrix and this is equivalent to adding 1 as a root to $B(\mathcal{C})$. In our case we do not add the constant vectors to all codewords, only to the non-zero ones. Noting that all constant vectors all have weight n and because we are minimizing over the weight these can be ignored. Hence,

$$\min_{\substack{c \in \mathcal{C} \setminus \{0^n\} \\ i \in GF(p)}} w_H(c + i^n) = \min_{\substack{c \in \mathcal{C}^+ \setminus \{i^n\} \\ i \in GF(p)}} w_H(c)$$
$$= \min_{c \in \mathcal{C}^+ \setminus \{0^n\}} w_H(c) = d_{\min}(\mathcal{C}^+).$$

Now assume that $1 \in B(\mathcal{C})$. This implies that $1^n \in \mathcal{C}$. If $c \in \mathcal{C}$ is a codeword of full cyclic order, then the same holds for $c + 1^n$. Since n and p are relatively prime, c and $c + 1^n$ must be cyclically distinct. Assume, without loss of generality, that c and $c + 1^n$ belong to $\mathcal{C}_{CP}$. Let A be the binary matrix corresponding to c and let b be the binary codeword corresponding to A. Then $c + 1^n$ corresponds to the matrix $\mathbf{D}(A)$. Since the vector $\mathbf{S}^i(b)$ corresponds to the matrix $\mathbf{R}^{i \bmod n}(\mathbf{D}^{i \bmod p}(A))$ we see that if the following two equations

$$0 = i \bmod n$$
$$1 = i \bmod p$$

has a simultaneous solution i then there are codewords in $\mathcal{C}_{CP}$ that are not cyclically distinct, hence $d_c(\mathcal{B}_{CP}) = 0$. Since n and p are relatively prime the Chinese remainder theorem guarantees that we indeed have a unique solution.

REFERENCES

[1] N. Q. A, L. Györfi, and J. L. Massey: Construction of binary constant-weight cyclic codes and cyclically permutable codes. *IEEE Trans. Inform. Theory*, IT-38(3):940–949, May 1992.

[2] R. E. Blahut: *Theory and Practice of Error Control Codes.* Addison-Wesley, 1983.

[3] F. R. K. Chung, J. A. Salehi, and V. K. Wei: Optical orthogonal codes: Design, analysis, and applications. *IEEE Trans. Inform. Theory*, IT-35(3):595–604, May 1989.

[4] H. Chung and P. V. Kumar: Optical orthogonal codes – New bounds and an optimal construction. *IEEE Trans. Inform. Theory*, IT-36(4):866–873, July 1990.

[5] E. N. Gilbert. Cyclically permutable error-correcting codes. *IEEE Trans. Inform. Theory*, IT-9:172–182, July 1963.

[6] A. Gill: *Linear Sequential Circuits.* McGraw-Hill, 1966.

[7] S. W. Golomb, B. Gordon, and L. R. Welch. Comma-free codes. *Canadian J. Math*, 10:202–209, 1958.

[8] L. Györfi and I. Vajda: Constructions of protocol sequences for multiple access collision channel without feedback. *IEEE Trans. Inform. Theory*, IT-39(5):1762–1765, September 1993.

[9] O. Moreno, Z. Zhang, P. V. Kumar, and V. A. Zinoviev: New constructions of optimal cyclically permutable constant weight codes. *IEEE Trans. Inform. Theory*, 1993.

[10] O. Moreno and V. A. Zinoviev: On cyclic constant weight codes. In *Sixth Joint Swedish-Russian International Workshop on Information Theory*, pages 413–417, August 1993.

[11] I. S. Reed: *k*th-Order near-orthogonal codes. *IEEE Trans. Inform. Theory*, IT-17(1):116–117, January 1971.

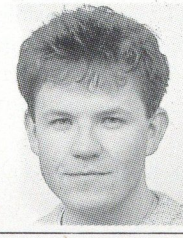
[12] I. S. Reed and C. T. Wolverton: The systematic selection of cyclically equivalent codes. *IEEE Trans. Inform. Theory*, IT-18(2):304–307, March 1972.

[13] J. A. Salehi: Code division multiple-access techiques in optical fiber networks—Part I: Fundamental principles. *IEEE Trans. Commun.*, COM-37(8):824–833, August 1989.

[14] H. Y. Song, I. S. Reed, and S. W. Golomb: On the nonperiodic cyclic equivalence classes of Reed-Solomon *IEEE Trans. Inform. Theory*, IT-39(4):1431–1434, July 1993.

[15] I. Vajda and G. Einarsson: Code acquisition for a frequency-hopping system. *IEEE Trans. Commun.*, COM-35(5):566–568, May 1987.

[16] J. H. van Lint: *Introduction to Coding Theory.* Springer-Verlag, 1982.



Anders G. Lundquist received his M.S. degree in Computer Science and Technology from Linköping University, Sweden, in 1991. Currently he is working towards a Ph.D. degree at the Department of Electrical Engineering, at the same university. His main interests are coding for multiple access and algebraic coding theory.

RECENT TRENDS IN LOSSY SOURCE CODING*

TAMÁS LINDER
DEPT. OF TELECOMMUNICATIONS
TECHNICAL UNIVERSITY OF BUDAPEST
1521 SZTOCZEK U. 2. BUDAPEST
HUNGARY

GÁBOR LUGOSI
DEPT. OF MATHEMATICS
FACULTY OF ELECT. ENGINEERING
TECHNICAL UNIVERSITY OF BUDAPEST
1521 SZTOCZEK U. 2. BUDAPEST
HUNGARY

KENNETH ZEGER
COORDINATED SCIENCE LABORATORY
DEPT. OF ELECT. AND COMP. ENGINEERING
UNIVERSITY OF ILLIONOIS
USA

A survey is given on some recent areas of interest in lossy source coding, that is, source coding relative to a fidelity criterion. In particular we discuss some recent results in rate-distortion theory, universal coding, and vector quantization techniques, and we indicate some current open problems.

1. INTRODUCTION

Lossy source coding (also called source coding with a fidelity criterion) is customarily considered a branch of information theory. The theory of lossy source coding was initiated by Claude Shannon, the founder of the principles of information theory [41]. In this paper we shall survey some aspects of lossy source coding which have developed into a separate field of study since Shannon's pioneering paper [42].

The survey will concentrate on theoretical issues rather than design and implementation problems. Our intention is to focus on some interesting recent results and open problems instead of giving an exhaustive survey of the existing theory and research trends. The topics we discuss here strongly reflect our own research interests. More comprehensive material on the practical side of lossy source coding can be found in e.g. [2], [13], and Kieffer [18].

It is assumed that the reader is familiar with the basic definitions and results of information theory, such as given in Cover and Thomas [9], Csiszár and Fritz [10] or Linder and Lugosi [24] (the last two books are in Hungarian).

Lossy source coding is concerned with the theoretical problems of signal compression: data is given by a mathematical model and is to be encoded into strings of binary digits so that both the encoding rate (the number of bits per data sample) and the distortion (a given measure of dissimilarity between the original signal and the signal reconstructed from its coded form) satisfy some prescribed constraints. The coding rate and the reconstruction quality are two conflicting measures of performance, and the main issue is to find an efficient tradeoff between these quantities. The abstract "data" can model different real-life signals such as speech, audio, still images, or video, and an efficient digital representation can serve several purposes such as transmission over a digital channel, storage on digital media, or easing the computational burden for data encryption. The methods to achieve the desired compression ratio with only a permissible degradation in the reproduction quality are rather different from the methods of lossless (also called noiseless) source coding, where one wants to reduce the data rate without introducing any distortion in the reproduction, as in the compression of data files for storage on computers. Nevertheless, there is much interaction between these two fields, and a familiarity with the basics of lossless coding is an important prerequisite for studying lossy coding.

The paper is organized as follows. In Section 2 we introduce the basic model of an information source, and the concept of source coding, and then state some fundamental results of rate-distortion theory. Section 3 addresses the problem of universal source coding, i.e., source coding with no prior knowledge of the statistical properties of the source to be encoded. In Section 4 we examine the theoretical aspects of multidimensional signal quantizers, and in Section 5 we shall give a brief review of high-resolution quantization theory, the only method available to date to obtain analytical expressions for vector quantizer performance.

2. RATE-DISTORTION THEORY

The term "rate-distortion theory" refers to the branch of information theory dealing with the rate-distortion tradeoff in source coding when the encoded blocklength gets large, i.e., when we effectively assume that the message to be encoded has infinite length. The mathematical model of an information source we use consists of a sequence $X_1, X_2, \ldots, X_n, \ldots$ of random variables taking values in a set $\mathcal{S}$ called the source alphabet. We assume a source is completely described by its finite dimensional probability distributions. In this paper we usually take $\mathcal{S} = \mathbb{R}$, the real line, or sometimes $\mathcal{S} = \mathbb{R}^k$, i.e. k-dimensional Euclidean space. For example, the X_i could be obtained by sampling from a "continuous time" signal $X(t)$: $X_i = X(iT)$ for some $T > 0$. Often, however, the signal to be encoded needs no time-discretization, as with compression of digital images.

A *source code of blocklength* n consists of an *encoder* g and a *decoder* φ. The encoder maps n-dimensional vectors into a finite set of all binary strings:

$$g : \mathbb{R}^n \to \{s_1, \ldots, s_N\} \subset \{0,1\}^*,$$

where $\{0,1\}^*$ denotes the set of finite length binary sequences. The decoder is a mapping

$$\varphi : \{s_1, \ldots, s_N\} \to \{y_1, \ldots, y_N\} \subset \mathbb{R}^n,$$

where the y_i are called the reproduction (or code) vectors. When the binary sequences $s_1, \ldots, s_N$ have the same length, we say that (g, φ) is a *fixed rate* code. We assume that given the set of codevectors $\{y_1, \ldots, y_N\}$ the encoder of a fixed rate code uses binary strings of the minimum possible length such that the mapping $\varphi(g(\cdot)) : \mathbb{R}^n \to \mathbb{R}^n$ is unchanged. The pair (g, φ) is called a *variable length* code when $\{s_1, \ldots, s_N\}$ is a binary prefix

* The research was supported in part by the National Science Foundation under Grant No. NCR-92-96231.

code i.e., when no s_i is a prefix of any s_j for $i \neq j$. In both cases, for any $k \geq 1$ there is one and only one way the binary sequence

$$g(X_1, \ldots, X_n) \ldots g(X_{(k-1)n+1}, \ldots, X_{kn}),$$

obtained by concatenating the binary strings g assigns to the vectors $(X_{(i-1)n+1}, \ldots, X_{in})$, $i = 1, \ldots, k$, can be decomposed into binary strings from the set $\{s_1, \ldots, s_N\}$. That is, the code is uniquely decodable. Thus, if the code (g, φ) is used k-times to encode the first kn samples of the source, and the resulting binary sequence is transmitted over an error free channel, then the reproduction vectors $y_i = \varphi(g(X_{(i-1)n+1}, \ldots, X_{in}))$, $i = 1, \ldots, k$ can be recovered without error. However, distortion is introduced by representing an n-dimensional vector (which possibly can take infinitely many values) by a finite set of vectors.

The *sample distortion* between two vectors $x^n = (x_1, \ldots, x_n)$ and $y^n = (y_1, \ldots, y_n)$ is measured by the squared error per sample

$$d_n(x^n, y^n) = \frac{1}{n} \sum_{i=1}^{n} (x_i - y_i)^2.$$

We use squared error here for the sake of simplicity — all the results in this section are valid with more general measures of distortion. The distortion of the code is given as the expected value of the sample distortion whenever $X^n = (X_1, \ldots, X_n)$ is encoded:

$$\Delta(g, \varphi) = \mathbf{E} d_n[X^n, \varphi(g(X^n))].$$

The above distortion is of course finite when $\mathbf{E}\|X^n\|^2 < \infty$, where $\|\cdot\|$ denotes Euclidean norm. The dependence of the distortion on the distribution of the source is suppressed in the notation. The rate $R(g)$ of a fixed rate code is defined as

$$R(g, \varphi) = \frac{1}{n} \log N,$$

i.e., the base 2 logarithm of the number of reproduction vectors normalized by the blocklength. Note that this is the number of encoding bits per source sample. The rate of a variable length code is the expected value of the normalized length of the encoded binary string:

$$R(g, \varphi) = \frac{1}{n} \mathbf{E} \left(\text{length}[g(X^n)] \right).$$

It is well known (see e.g. [10]) that the encoder always can be chosen (without changing the mapping $\varphi(g(\cdot))$) so that the average codelength of a variable length code is within $1/n$ bits of its lower bound $H(\varphi(g(X^n)))$, the entropy of the reproduction.

It is intuitively clear that both the rate and the distortion can not be arbitrarily small at the same time; if one of them is small then the other quantity will inevitably increase. In the remainder of this section we consider only fixed rate codes and present fundamental results on the distortion rate tradeoff. The main problem is the characterization of the minimum distortion that fixed rate codes can achieve while having rate that is less than or equal to a given rate R. For reasons of practicality, we assume the code rate is constant, but we note that analogous results hold when the distortion is fixed and the question is to find the minimum achievable rate.

Define $\hat{D}_n(R)$ as the minimum distortion which can be achieved using an n-length fixed rate source code of rate not exceeding $R > 0$, i.e.,

$$\hat{D}_n(R) = \inf_{R(g,\varphi) \leq R} \Delta(g, \varphi). \tag{1}$$

When $X_1, X_n, \ldots$ is a stationary sequence of random variables, it is not hard to see that

$$\lim_{n \to \infty} \hat{D}_n(R) = \inf_{n \geq 1} \hat{D}_n(R) \stackrel{\text{def}}{=} \hat{D}(R). \tag{2}$$

The function $\hat{D}(R)$ is a lower bound on the distortion of any fixed rate source code of rate at most R. The quantity $\hat{D}(R)$ is often called the *operational distortion-rate* function of the source with respect to fixed rate coding. Also, it follows from the first equality in (2) that for a given $\epsilon > 0$, if n is large enough there always exists a code (g_n, φ_n) with $R(g_n, \varphi_n) \leq R$ and $\Delta(g_n, \varphi_n) < \hat{D}(R) + \epsilon$. Define the n^{th} *order distortion-rate function* by

$$D_n(R) = \inf\{\mathbf{E} d_n(\bar{X}^n, \bar{Y}^n) : n^{-1} I(\bar{X}^n, \bar{Y}^n) \leq R\}$$

where the infimum is taken over all pairs of $(\bar{X}^n, \bar{Y}_n)$ such that $\bar{X}^n$ and X^n have the same distribution and the mutual information [10] between $\bar{X}^n$ and $\bar{Y}^n$ is at most R. By elementary properties of the mutual information we have

$$\hat{D}_n(R) \geq D_n(R)$$

for all n. The *source coding theorem* for ergodic sources states (see Berger [4]) that if $X_1, X_2, \ldots$ is stationary and ergodic, then

$$\hat{D}(R) = \lim_{n \to \infty} D_n(R) \stackrel{\text{def}}{=} D(R).$$

The quantity $D(R)$ is the *distortion-rate function of the source*. This theorem was first stated by Shannon [42] for finite alphabet memoryless sources, i.e., when $X_1, X_2, \ldots$ is sequence of independent and identically distributed random variables which can take only finitely many values. The reason why this result is of fundamental importance is that it gives a characterization of the otherwise intractable quantity $\hat{D}(R)$. On the other hand, several properties of $D(R)$ are known as a function of R (see e.g. Berger [4]).

If we relax the ergodic assumption and require only stationarity, we find that $\hat{D}(R) > D(R)$ can happen (see Gray and Davisson [15]). On the other hand, using variable length codes in the definition of $\hat{D}(R)$ instead of fixed rate codes, we have $\hat{D}(R) = D(R)$ for stationary nonergodic sources by a result of Leon-Garcia *et al.* [21]. We note here that several variations of the source coding theorem exist, proving similar results for more general source and reproduction alphabets, distortion measures, and source distributions (see [18] for more references).

The above discussion illustrates the advantage of using source codes of large blocklength. In general, however, block codes of length n introduce a delay of order n, since unless the code has special structure, the encoder has to wait until the last sample X_n arrives before producing the binary codeword for X^n. Also, the complexity of encoding

and decoding critically depend on the blocklength. Therefore, it is of great interest to estimate what improvement in distortion we can expect by increasing n. Unfortunately, an exact calculation of $\hat{D}_n(R)$, the distortion of the best code of length n and rate R seems intractable. Thus we have to settle for asymptotic results. Pilc [36] showed that for a finite alphabet memoryless source

$$\hat{D}_n(R) - D(R) \leq c\left(\frac{\log n}{n}\right),$$

where c is a constant depending on the source distribution and the rate. Wyner [45] proved the same asymptotics for memoryless Gaussian sources, and later obtained [46] that

$$\hat{D}_n(R) - D(R) \leq c\sqrt{\frac{\log n}{n}}, \qquad (3)$$

for any stationary Gaussian source whose spectral density satisfies some smoothness conditions. Linder *et al.* [26] showed that (3) holds when the source is memoryless and the X_i are bounded but otherwise have arbitrary distribution (i.e. this includes infinite alphabet sources). It is presently unknown whether Pilc's result is sharp, that is whether there exists a lower bound of the type $n^{-1}\log n$, or whether his upper bound can be generalized to memoryless sources with continuous distribution. We note that far more and stronger results are known for lossless coding (see e.g. Krichevsky and Trofimov [19]).

3. UNIVERSAL CODING

Results of rate-distortion theory guarantee the existence of source codes performing near the achievable optimum. These codes however strongly rely on the knowledge of the probability distribution of the source. In practice, the distribution is typically unkown, therefore there is a strong demand for coding methods that "learn" good codes from observing data emitted by the source.

The term "universal code" is used to denote a sequence of lossy codes of increasing blocklength such that they perform near-optimally on each source from a given collection of sources. Let $\mathcal{X}$ be a family of stationary real sources. For any source $\boldsymbol{X} = X_1, X_2, \ldots$ in $\mathcal{X}$ we define the operational distortion-rate function $\hat{D}(R, \boldsymbol{X})$ and the distortion-rate function $D(R, \boldsymbol{X})$ of $\boldsymbol{X}$ as in the previous section, only here we make explicit the dependence of these quantities on the particular source. A sequence of fixed rate codes (g_n, φ_n), $n = 1, 2, \ldots$ is said to be *weakly universal* at rate R if

$$R(g_n, \varphi_n) \leq R$$

and

$$\lim_{n\to\infty} \mathbf{E} d_n[X^n, \varphi(g(X^n))] = \hat{D}(R, \boldsymbol{X})$$

for all $\boldsymbol{X} \in \mathcal{X}$. In other words, (g_n, φ_n) performs optimally for all sources in $\mathcal{X}$ when $n \to \infty$. *Strong universality* means that in the above limit we have uniform convergence over $\mathcal{X}$. The practical significance of universal codes is clear: the same code can be used for different sources without much degradation in performance. Theoretically, the proof of existence and/or the construction of universal codes is often very challenging.

The existence of fixed rate weak universal codes for the class of stationary sources was first proved by Ziv [54] for general source and reproduction alphabets and distortion measures that include real sources and the mean-squared error criterion considered here. Neuhoff *et al.* [33] and Kieffer [16] provided various generalizations, the latter also dealing with universal variable-length lossy and lossless coding. Analyzing Ziv's scheme Linder *et al.* [26] proved that for any $R > 0$ there exists a sequence of fixed rate codes (g_n, φ_n) of rate R which are weakly universal for the family of real stationary sources with finite second moment, and for any memoryless source $\boldsymbol{X}$ with a bounded support

$$\mathbf{E} d_n[X^n, \varphi(g(X^n))] - \hat{D}(R, \boldsymbol{X}) \leq c\sqrt{\frac{\log\log n}{\log n}},$$

where c depends on the source and on R. In a related work [25] the same authors investigated fixed rate universal coding of memoryless sources. They showed that for the class of memoryless sources over a finite alphabet there exists a sequence of fixed rate codes (g_n, φ_n) of rate R such that

$$\mathbf{E} d_n[X^n, \varphi(g(X^n))] - \hat{D}(R, \boldsymbol{X}) \leq c\left(\frac{\log n}{n}\right), \qquad (4)$$

for some constant c. It was also shown that the code construction for proving the above result can be extended to yield a universal scheme for which

$$\mathbf{E} d_n[X^n, \varphi(g(X^n))] - \hat{D}(R, \boldsymbol{X}) \leq c\sqrt{\frac{\log n}{n}}$$

for any bounded *real valued* memoryless source. Furthermore, the above rate of convergence also holds with probability one:

$$d_n[X^n, \varphi(g(X^n))] - \hat{D}(R, \boldsymbol{X}) \leq$$
$$\leq O\left(\sqrt{\frac{\log n}{n}}\right), \text{ with probability one,}$$

where $f(n) = O(h(n))$ means that $|f(n)| \leq c|h(n)|$ for some $c > 0$, if n is large enough. Yu and Speed [48] obtained a result similar to (4); they demonstrated the existence of a sequence of variable length codes such that for all memoryless sources over a finite alphabet,

$$d_n[X^n, \varphi(g(X^n))] \leq D$$

and

$$R(g_n, \boldsymbol{X}) - R(D, \boldsymbol{X}) \leq c\frac{\log n}{n},$$

where $R(g_n, \boldsymbol{X})$ is the expected codelength (which depends on the source) and $R(D, \boldsymbol{X})$ is the rate-distortion function of $\boldsymbol{X}$, the inverse of $D(R, \boldsymbol{X})$.

It is of great theoretical as well as practical interest to find universal codes with reasonable complexity. The above results, even though proved by code construction, do not provide viable implementation. A currently "hot" research topic is to find a lossy counterpart of the lossless universal Lempel-Ziv codes [55]. This problem is still unsolved, although progress towards this goal was made for such a construction by Steinberg and Gutman [43]. A computationally efficient universal lossy coding algorithm which sequentially updates the set of codevectors was given by Zhang and Wei [53].

4. VECTOR QUANTIZATION

Source coding theorems guarantee the existence of lossy source codes whose performance approaches the distortion-rate bound as the blocklength n increases. While these results provide a beautiful theory, and indicate the best performance one can expect, their practical usefulness is limited by two facts. On the one hand, in practice, the complexity of the encoder and the decoder are limited by the computational resources available, so codes even with moderately large blocklengths cannot be realized. On the other hand, source coding theorems provide no guidance as to what optimal encoders look like. The theory of vector quantization is concerned with the design of encoders — i.e., vector quantizers — of fixed blocklength.

The basic problem may be formulated as follows. A k dimensional, N level vector quantizer Q is a function of the form $Q : \mathbb{R}^k \to \{y_1, \ldots, y_N\}$, where $y_1, \ldots, y_N \in \mathbb{R}^k$ are the *reproduction points* or *codevectors*. A quantizer is defined by its reproduction points, and *quantization regions* $B_i = \{z : Q(z) = y_i\}$, $i = 1, \ldots, N$. $Q(z)$ is interpreted as the quantized value of an input vector $z \in \mathbb{R}^k$. Note that a k-length fixed rate source code (g, φ) as defined in Section 2 determines a vector quantizer by $Q(z) = \varphi(g(z))$, and conversely, by encoding the output of a vector quantizer using fixed length binary sequences, we obtain a fixed rate source code. If $Z \in \mathbb{R}^k$ is a vector-valued random variable, the *average distortion* of Q (with respect to Z) is defined as

$$\Delta(Q) = \mathbf{E}\frac{1}{k}\|Z - Q(Z)\|^2,$$

which is finite provided that $\mathbf{E}\|Z\|^2 < \infty$. (We assume $\mathbf{E}\|Z\|^2 < \infty$ throughout.) We seek vector quantizers with small distortion. A quantizer Q^* is called *optimal*, if $\Delta(Q^*) \leq \Delta(Q)$ for any quantizer Q. Existence of optimal quantizers is always guaranteed, though they do not have to be unique (e.g. see Pollard [37] and Abaya and Wise [1]).

Some thought should convince the reader that any optimal quantizer satisfies the following properties.

a) NEAREST NEIGHBOR PROPERTY:

if $\|z - y_i\| < \|z - y_j\|$ for all j, then $Q^*(z) = y_i$

(ties may be broken arbitrarily).

b) CENTROID PROPERTY:

$$y_i = \mathbf{E}(Z|Z \in B_i), \quad i = 1, \ldots, N.$$

Property (a) says that input points should always be quantized to the nearest reproduction point. By the second property, the reproduction points should be placed at the centroids of the sets of points that are quantized to the same value. Apart from these properties, very little is known about optimal quantizers. Even for special distributions of Z, such as Gaussian or uniform distribution on the unit cube, no explicit formulas are available for the form of optimal quantizers. Using the above properties, various versions of an iterative method for designing quantizers have been introduced. This iterative method is varyingly known as the Lloyd-Max algorithm, Lloyd algorithm [28], Max algorithm [30], generalized Lloyd algorithm, or the Linde-Buzo-Gray algorithm [22]. The basic algorithm starts with an arbitrary quantizer, adjusts its regions B_i first to satisfy Property (a), then adjusts its reproduction points y_i to satisfy Property (b). Then these two steps are repeated for the re-adjusted quantizer. It is easy to see that the distortion of the quantizers obtained in successive stages of this algorithm cannot increase, therefore, it converges. Unfortunately, in general it does not converge to the distortion of an optimal quantizer, in other words, the algorithm may get stuck in local optima. In some lucky cases, however, the Lloyd-Max algorithm converges to an optimal quantizer; see Kieffer [17] and Trushkin [44] for sufficient conditions on the distribution of Z for global optimality.

A common serious problem for the designer of a vector quantizer is that the distribution of the source Z is unknown. The only information available is a *training sequence* $Z_1, \ldots, Z_m$ of vectors, where the Z_i's can often be modeled efficiently as independent, identically distributed random variables, with the same distribution as Z. Then the designer generally measures the *empirical distortion*

$$\Delta_m(Q) = \frac{1}{m}\sum_{i=1}^{m}\frac{1}{k}\|Z_i - Q(Z_i)\|^2$$

of a quantizer Q, and tries to find a quantizer minimizing $\Delta_m(Q)$. Denote such an *empirically optimal* quantizer by Q_m^*, that is,

$$Q_m^* = \arg\min_Q \Delta_m(Q).$$

The distortion of such an empirically chosen quantizer is

$$\Delta(Q_m^*) = \mathbf{E}\left(\frac{1}{k}\|Z - Q_m^*(Z)\|^2 | Z_1, \ldots, Z_m\right).$$

Note that $\Delta(Q_m^*)$ is a random variable, as it depends on the (random) training sequence. One expects that if the training sequence is long enough, then the distortion of an empirically optimal quantizer gets close to the distortion of a truly optimal quantizer. Indeed, Pollard [37], [39] proved that

$$\Delta(Q_m^*) - \Delta(Q^*) \to 0, \text{ with probability one}$$

is true for any distribution of Z with $\mathbf{E}\|Z\|^2 < \infty$. Under more restrictive conditions on the distribution, Pollard [38] also proved a central limit theorem, which indicates how fast the above difference can tend to zero. Along this line, Linder *et al.* [26] proved a large-deviation type probability inequality, which bounds the finite-sample behavior of the above difference. For example, the inequality in [26] implies that

$$\Delta(Q_m^*) - \Delta(Q^*) = O\left(\sqrt{\frac{\log m}{m}}\right) \text{ with probability one,}$$

which is true for any Z with a bounded support. Apparently, the exact rate of convergence is still an unknown and challenging problem.

While in principle, empirically optimal quantizers can be found, the computational complexity of such a general algorithm is often too large for practical realizations. Many

successful techniques have been proposed in the literature for designing quantizers from empirical data. We refer the reader to Makhoul *et al.* [29] Gersho and Gray [12] for good summaries of such algorithms. One of the most widely used of these techniques is the empirical version of the Lloyd-Max algorithm (also known as the Linde-Buzo-Gray algorithm, see [22]) which is simply the Lloyd-Max algorithm executed on the empirical distribution. This method produces good, but not necessarily empirically optimal quantizers from training sets. Sabin and Gray [40] demonstrated that if the size of the training sequence increases, this algorithm performs eventually as well as if the true distribution of the training data were known.

There have been some attempts to tackle the problem of having iterative descent algorithms get trapped in locally optimal solutions by introducing random perturbations or performing "soft competitions" in the iteration steps. Examples of these techniques are given in Yair *et al.* [47] Zeger *et al.* [52].

It is apparent that the encoding complexity of an unstructured vector quantizer (such as the typical output of the Lloyd-Max algorithm) becomes very quickly prohibitive when the vector dimension increases. There has been much research activity on finding good vector quantizers with structural constraints that ensure efficient implementation. Although there are several competing schemes such as trellis and tree structured quantizers, and lattice quantizers (see Gersho and Gray [12] and the references therein), so far none of these methods have been rigorously shown to achieve the rate-distortion limits. Among these schemes the theoretically best understood are lattice quantizers. As the next section will indicate, lattice quantizers can perform near the rate distortion limit and are conjectured to be optimal in a certain asymptotical sense.

5. HIGH-RATE QUANTIZATION THEORY

In all the previous sections we mainly dealt with $\hat{D}_n(R)$, the distortion of the best n-length fixed rate block code at rate R. We saw that rate-distortion theory characterizes the limit of this quantity as n gets large, and that the theory of vector quantizer design helps estimate the error made when the optimal source coder is designed from empirical data. However, the very important question of what the value of $\hat{D}_n(R)$ is for a given source, dimension, and distortion measure, remains unanswered. We now describe some results from the high rate theory of quantization which comes the closest to solving this problem. Also, in the framework of this theory it is often possible to deduce relevant properties of optimal quantizers and source coding schemes using some structural constraint.

5.1. Resolution-Constrained Quantization

Let us consider a k-dimensional vector quantizer with N-codevectors as in Section 4. The dimension k will be fixed throughout this section. Given the random vector X^k, we denote the mean-squared distortion of the best such quantizer by $D_r(N)$, i.e.:

$$D_r(N) = \min_Q \|X^k - Q(X^k)\|^2,$$

where the minimum is taken over Q's with N codevectors. As we mentioned before, there are no known methods for explicitly computing $D_r(N)$. As is turns out, however, for N large enough there exist good approximations to $D_r(N)$. For $k = 1$ Bennett [3] and Panter and Dite [35] derived a formula for sources with "nice" densities

$$D_r(N) \sim \frac{1}{12} c(f) N^{-2}, \tag{5}$$

where $c(f)$ is a constant depending only on the source density f, and $\sim$ means that the ratio of the two sides approaches 1 when $N \to \infty$. This asymptotic formula provides a good approximation to $D_r(N)$ for N large, and it has been observed (see e.g. Neuhoff [32]) that in many important cases (5) is quite accurate for $N \geq 8$. The first rigorous proof of (5) as well as its generalization to vector quantizers was given by Zador [49], [50]. He proved for any dimension k that for sources with sufficiently smooth densities

$$D_r(N) \sim \alpha_k c(f) N^{-2/k}, \tag{6}$$

where α_k is a constant depending only on the dimension k, and $c(f)$ is an easily computable function of the source density. Bucklew and Wise [5] proved that Zador's formula (6) holds for any source X^k having a density and satisfying $\mathbf{E}\|X^k\|^{2+\epsilon} < \infty$ for some $\epsilon > 0$. Cambanis and Gerr [6] investigated Bennett's "companding quantization", a scheme in which a memoryless mapping and its inverse is applied to the source and to the quantizer output, respectively, to implement scalar quantizers. They determined a simple sequence of N-level scalar quantizers which are asymptotically optimal in the sense that their distortion satisfies (5). The exact performance of companding quantizers under general conditions was investigated by Linder [23]. Na and Neuhoff [31] gave a multidimensional Bennett-type formula for certain sequences of quantizers. Recently, high-rate techniques have been applied to the performance analysis of quantizers with structural constraints by Neuhoff and Lee ([34] and [20]). Another application of the high-rate theory is an analysis of a universal quantization scheme by Zeger *et al.* [51].

5.2. Entropy-Constrained Quantization

The entropy $H(Q)$ of a quantizer with N codevectors is defined as

$$-\sum_{i=1}^{N} \mathbf{P}\{Q(X^k) = y_i\} \log \mathbf{P}\{Q(X^k) = y_i\}.$$

Let $D_e(H)$ be the minimum distortion over all k-dimensional quantizers with entropy less than or equal to H:

$$D_e(H) = \min_{Q: H(Q) \leq H} E\|X^k - Q(X^k)\|^2,$$

where the minimum is taken over all quantizers with a finite number of levels. As we mentioned before, for any Q there exists a variable length code (g, φ) such that $Q(x) = \varphi(g(x))$ for all $x \in \mathbb{R}^k$ and

$$R(g, \varphi) \leq \frac{1}{n} H(Q) + \frac{1}{n}. \tag{7}$$

Since $R(g, \varphi) \geq \frac{1}{n} H(Q)$ always holds when $Q(x) = \varphi(g(x))$, the inequality (7) shows that $D_e(H)$ is very

closely related to the distortion of optimal variable length source codes. On the other hand, $D_e(H)$ yields to high-rate analysis. Gish and Pierce [14] recognized that uniform scalar quantizers (i.e. quantizers with codepoints equally spaced along the real line) have good entropy constrained performance. Let Q_u be a uniform quantizer with entropy $H(Q_u)$ and distortion $\Delta(Q_u)$. Gish and Pierce proved that under some conditions on the source density, as $H(Q_u) \to \infty$

$$\Delta(Q_u) \sim \frac{1}{12} 2^{2h(f)} 2^{-2H(Q_u)}, \qquad (8)$$

where $h(f) = \int f(x) \log f(x) dx$ is the differential entropy of the source density. They also argued that uniform quantizers are asymptotically optimal in one dimension in the sense that $D_e(H(Q_u))/\Delta(Q_u) \to 1$ as $H(Q_u) \to \infty$. Zador [49], [50] showed that for $k \geq 1$ the optimal entropy constrained quantizers have the asymptotics

$$D_e(H) \sim \beta_k 2^{2h(f)/k} 2^{-2H/k},$$

where β_k is a constant that depends only on k. Based on a heuristic argument Gersho [11] conjectured that $\alpha_k = \beta_k$, and also that their value is the minimum normalized moment of inertia that a polytope capable of tessellating $\mathbb{R}^k$ can have. This conjecture is widely believed to be true, but no proof of it is known to date. Linder and Zeger [27] made precise and proved under general conditions Gersho's formula for the high-rate asymptotics of tessellating quantizers.

The multidimensional generalizations of uniform quantizers are lattice quantizers [8]. The code points of a k-dimensional lattice quantizer are the integral linear combinations of a given basis of $\mathbb{R}^k$. Lattice quantizers are popular because efficient algorithms are often known for their implementation (see e.g. Conway and Sloane [7]). Also, lattice quantizers based on "good" lattices have entropy-constrained performance near the optimum [11] and it may be conjectured that the rate distortion limit can be arbitrarily approached by lattice quantizers.

6. OPEN PROBLEMS

We mention a few open problems in the areas covered in this survey. In rate distortion theory the simple characterization of achievable rate and distortion levels for networks including several sources and receivers is unsolved. Also, efficient bounds are sought for the rate-distortion functions of non-Gaussian sources with memory. Computationally efficient universal codes and sharp redundancy bounds are hot research topics. The design of globally optimal quantizers at least for some often used vector source models is an open problem which has been unsuccessfully attacked in the past. An undecided question is whether tree-structured quantizers can achieve (at least in an asymptotic sense) the rate-distortion bound. A theory of high rate entropy constrained quantization as rigorous as the resolution-constrained theory is missing. A very interesting question is whether there exist lattice quantizers not using variable length encoding which have near optimum performance.

IRODALOM

[1] E. A. Abaya and G. L. Wise: Convergence of vector quantizers with applications to optimal quantization. *SIAM Journal on Applied Mathematics*, 44:183–189, 1984.

[2] H. Abut: *Vector Quantization* IEEE Press, New York, 1990.

[3] W. R. Bennett: Spectrum of quantized signals *Bell. Syst. Tech. J.*, 27:446–472, 1948.

[4] T. Berger: *Rate Distortion Theory* Prentice–Hall, Englewood Cliffs, New Jersey, 1971.

[5] J. A. Bucklew and G. L. Wise: Multidimensional asymptotic quantization theory with rth power distortion measures. *IEEE Trans. Inform. Theory*, IT-28:239–247, March 1982.

[6] S. Cambanis and N. L. Gerr: A simple class of asymptotically optimal quantizers *IEEE Trans. Inform. Theory*, IT-29:664–676, September 1983.

[7] J. H. Conway and N. J. A. Sloane: Fast quantizing and decoding algorithms for lattice quantizers and codes. *IEEE Trans. Inform. Theory*, IT-28:227–232, March 1982.

[8] J. H. Conway and N. J. A. Sloane: Voronoi regions of lattices, second moment of polytopes, and quantization. *IEEE Trans. Inform. Theory*, IT-28:211–226, March 1982.

[9] T. Cover and J. A. Thomas:. *Elements of Information Theory*. Wiley, New York, 1991.

[10] I. Csiszár and J. Fritz:. *Információelmélet*. Tankönyvkiadó, Budapest, 1986.

[11] E. Gersho: Asymptotically optimal block quantization. *IEEE Trans. Inform. Theory*, IT-25:373–380, July 1979.

[12] A Gersho and R. M. Gray: *Vector Quantization and Signal Compression*. Kluwer, Boston, 1992.

[13] A. Gersho, S. Wang, and K. Zeger: Vector quantization techniques in speech coding. In *Advances in Speech Signal Processing*, New York: Marcel Dekker, 1992.

[14] H. Gish and J. N. Pierce: Asymptotically efficient quantizing. *IEEE Trans. Inform. Theory*, IT-14:676–683, September 1968.

[15] R. M. Gray and L. D. Davisson: Source coding theorems without the ergodic assumption. *IEEE Trans. Inform. Theory*, IT-20:502–516, 1974.

[16] J. C. Kieffer: A unified approach to week universal source coding. *IEEE Trans. Inform. Theory*, IT-24:674–682, November 1978.

[17] J. C. Kieffer: Exponential rate of convergence for Lloyd's method I. *IEEE Trans. Inform. Theory*, IT-28:205–210, March 1982.

[18] J. C. Kieffer: Survey of the theory of source coding with a fidelity criterion. *IEEE Trans. Inform. Theory*, IT-39:1473–1491, Sep. 1993.

[19] R. E. Krichevsky and V. K. Trofimov: The performance of universal encoding. *IEEE Trans. Inform. Theory*, IT-27:199–207, March 1981.

[20] D. H. Lee and D. L. Neuhoff: An asymptotic analysis of two-stage vector quantization. IEEE Int. Symp. Inform. Theory, p. 316, Budapest, June, 1991.

[21] A. Leon-Garcia, L. D. Davisson, and D. L. Neuhoff: New results on coding of stationary nonergodic sources. *IEEE Trans. Inform. Theory*, IT-25:137–144, Jan. 1979.

[22] Y. Linde, A. Buzo, and R. M. Gray: An algorithm for vector quantizer design. *IEEE Transactions on Communications*, COM-28:84–95, January 1980.

[23] T. Linder: On asymptotically optimal companding quantization. *Problems of Control and Information Theory*, vol. 20(6), 1991.

[24] T. Linder and G. Lugosi: *Bevezetés az Információelméletbe*. Tankönyvkiadó, Budapest, 1991.

[25] T. Linder, G. Lugosi, and K. Zeger: Fixed rate universal lossy source coding and rate of convergence for memoryless sources. submitted to *IEEE Trans. Inform. Theory*, 1993.

[26] T. Linder, G. Lugosi, and K. Zeger: Rates of convergence in the source coding theorem, in empirical quantizer design,

and in universal lossy source coding. *IEEE Trans. Inform. Theory* (to appear), 1993.

[27] T. Linder and K. Zeger: Asymptotic entropy constrained performance of tessellating and universal randomized lattice quantization. *IEEE Trans. Inform. Theory*, March 1994.

[28] S. P. Lloyd: Least squares quantization in PCM. *IEEE Trans. Inform. Theory*, IT-28:129–137, March 1982. Originally a 1957 Bell Labs memorandum.

[29] J. Makhoul, S. Roucos, and H. Gish: Vector quantization in speech coding. *Proc. IEEE*, 73(11):1551–1588, November 1985.

[30] J. Max: Quantizing for minimum distortion. *IEEE Trans. Inform. Theory*, IT-6:7–12, March 1960.

[31] S. Na and D. L. Neuhoff: Bennett's integral for vector quantizers. to appear in *IEEE Trans. Inform. Theory*, 1994.

[32] D. L. Neuhoff: The other asymptotic theory of lossy source coding. Joint IEEE/DIMACS Conference on Vector Quantization, 1992.

[33] D. L. Neuhoff, R. M. Gray, and L. D. Davisson: Fixed rate universal block source coding with a fidelity criterion. *IEEE Trans. Inform. Theory*, IT-21:511–523, September 1975.

[34] D. L. Neuhoff and D. H. Lee: On the performance of tree-structured vector quantization. In *Proceedings of ICASSP91*, pages 2277–2280, Toronto, 1991.

[35] P. F. Panter and W. Dite: Quantization distortion is pulse-count modulation with nonuniform spacing of levels. *Proc IRE*, 39:44–48, 1951.

[36] R. Pilc: The transmission distortion of a source as a function of the encoding block length. *Bell System Technical Journal*, 47:827–885, 1968.

[37] D. Pollard: Strong consistency of k-means clustering. *Annals of Statistics*, 9, no. 1:135–140, 1981.

[38] D. Pollard: A central limit theorem for k-means clustering. *Annals of Probability*, vol. 10, no. 4:919–926, 1982.

[39] D. Pollard: Quantization and the method of k-means. *IEEE Trans. Inform. Theory*, IT-28:199–205, March 1982.

[40] M. J. Sabin and R. M. Gray: Global convergence and empirical consistency of the generalized Lloyd algorithm. *IEEE Trans. Inform. Theory*, IT-32:148–155, March 1986.

[41] C. E. Shannon: A mathematical theory of communication. *Bell Syst. Tech. J.*, vol. 27:379–423, 1948.

[42] C. E. Shannon: Coding theorems for a discrete source with a fidelity criterion. *IRE Nat. Conv. Rec.*, part 4:138–143, 1959.

[43] Y. Steinberg and M. Gutman: An algorithm for source coding subject to a fidelity criterion based on string matching. *IEEE Trans. Inform. Theory*, IT-39:877–887, May 1993.

[44] A. V. Trushkin: Sufficient conditions for uniqueness of a locally optimal quantizer for a class of convex error weighting function. *IEEE Trans. Inform. Theory*, IT-28:187–198, March 1982.

[45] A. D. Wyner: Communication of analog data from a Gaussian source over a noisy channel. *Bell System Technical Journal*, pages 801–812, May-June 1968.

[46] A. D. Wyner: On the transmission of correlated Gaussian data over a noisy channel with finite encoding block length. *Information and Control*, 20:193–215, 1972.

[47] E. Yair, K. Zeger, and A. Gersho: Competitive learning and soft competition for vector quantizer design. *IEEE Trans. Signal Processing*, vol. 40:294–309, February 1992.

[48] B. Yu and T. P. Speed: A rate of convergence result for a universal D-semifaithful code. *IEEE Trans. Inform. Theory*, IT-39:813–821, May 1993.

[49] P. Zador: *Development and evaluation of procedures for quantizing multivariate distributions*. PhD thesis, Stanford Univ., 1964: Univ. Microfilm no. 64-9855.

[50] P. Zador: Asymptotic quantization error of continuous signals and the quantization dimension. *IEEE Trans. Inform. Theory*, IT-28:139–149, March 1982.

[51] K. Zeger, A. Bist, and T. Linder: Universal source coding with codebook transmission. *IEEE Trans. Communications*, February 1994.

[52] K. Zeger and A. Gersho: Globally optimal vector quantizer design by stochastic relaxation. *IEEE Trans. Signal Processing*, vol. 40:310–322, February 1992.

[53] Z. Zhang and V. K. Wei: An online universal lossy data compression algorithm via continuous codebook refinement. Preprint, 1993.

[54] J. Ziv: Coding of sources with unknown statistics- Part II: Distortion relative to a fidelity criterion. *IEEE Trans. Inform. Theory*, IT-18:389–394, May 1972.

[55] J. Ziv and A. Lempel: A universal algorithm for sequential data compression. *IEEE Trans. Inform. Theory*, IT-33:337–343, 1977.

Tamás Linder was born in Budapest, Hungary in 1964. He received the M.S. degree in electrical engineering from the Technical University of Budapest in 1988, and the Ph.D degree from the Hungarian Academy of Sciences in EE in 1992. He was a post-doctoral fellow at the University of Hawaii in 1993, and a Visiting Fulbright Scholar at the Coordinated Science Laboratory, University of Illinois at Urbana-Champaign in 1993. He is currently an Associate Researcher at the Research Group for Informatics and Electronics of the Hungarian Academy of Sciences. His research interests include information theory, vector quantization, rate-distortion theory, and statistical pattern recognition.

Gábor Lugosi was born in Budapest, Hungary, in 1964. He graduated from the Technical University of Budapest with a degree in electrical engineering in 1987, and received the Ph.D. degree from the Hungarian Academy of Sciences in 1991. He has been an Associate Professor in the Department of Mathematics and Computer Science at the Faculty of Electrical Engineering, Technical University of Budapest. Between 1990 and 1993 he spent some time as a visiting researcher at the Technical University of Vienna, the Catholic University of Leuven, the University of Manitoba, Winnipeg, Concordia University, Montreal, and the University of Illinois at Urbana-Champaign. His research interests include pattern recognition, nonparametric statistics, and source coding.

Kenneth Zeger received both the S.B. and S.M. degrees in EECS from MIT in 1984, and both the M.A. degree in mathematics and the Ph.D. in EE at the University of California, Santa Barbara, in 1989 and 1990 respectively. Dr. Zeger was an Assistant Professor of Electrical Engineering at the University of Hawaii from June 1990 to June 1992 and since July 1992 has been an Assistant Professor of Electrical Engineering at the University of Illinois at Urbana-Champaign. His present research interests include information theory, source and channel coding, speech and image compression, and computational complexity theory. He was Co-Chairman of the 1990 IEEE Communication Theory Workshop, received an NSF Research Initiation Award in 1990, and an NSF Presidential Young Investigator Award in 1991.

IMPLEMENTATION OF TRELLIS CODED MODEMS

K. ELEK and J. GAÁL

TECHNICAL UNIVERSITY OF BUDAPEST
DEPARTMENT OF TELECOMMUNICATIONS
H-1111 BUDAPEST, STOCZEK U. 2.

Digital signal processing implementation of high speed (up to 14400 bit/s) CCITT modems are presented in this paper. In these modems trellis coding is combined with multistate QAM modulation (up to 128 states). Algorithm and implementation of trellis encoder and that of the Viterbi decoder are detailed. Measurements are presented in order to prove the effectiveness of the implemented trellis coding technique.

1. INTRODUCTION

Modem is an electronic device that incorporates both a modulator and a demodulator into a single piece of signal conversion equipment. Interfacing directly to the communication channel, modems establish communication links between various computer systems and terminal equipment. The International Telegraph and Telephone Consultative Committee (CCITT), which determines protocols and standards for telephone and telegraph equipment, has authored a number of recommendations describing modem operation [1]. In most cases the communications channel is the general switched telephone network (GSTN) or a two- or four-wire leased circuit. When radio channel is used it can be handled as a four-wire communication link. Originally, these channels were assigned for voiceband transmission so they are bandlimited from 300 Hz to 3400 Hz.

The CCITT V.32.bis recommendation [2] specifies the symbol rate of 2400 bauds per second. To achieve data transmission rates of 7200, 9600, 12000 and 14400 bits per second, three, four, five or six bits must be transmitted in one symbol interval. By adding a single bit to a binary symbol with k bits, the number of waveforms to be produced by the modulator produce is increased from 2^k to 2^{k+1}. To achieve the same value of the probability of error, an increase in alphabet size within the same bandwith requires a 3 dB increase in the signal to noise ratio (SNR) .

Traditionally, a modem was implemented using analog discrete components. Today, digital circuits centered around one or two high perfomance digital signal processors (DSPs) can meet the demands of modem algorithms without the difficulties associated with analog circuitry. A digital modem implementation offers programmability, realizability of sophisticated algorithms, temperature insensivity, ease of design and often reduced cost when compared with analog implementations.

In this paper we are going to present our results on developing and implementation of modems. A general purpose digital signal processig board was developed in our laboratory [4]. The complete modem was implemented on this PC-DSP board which is in PC/AT plug-in board containing two Texas Instr. TMS320C25 signal processors, program- and data-memories and A/D, D/A converters.

A modem in wide sense is rather complex system. In Sec. 2 the framework of codings and signal processing procedures included in a modem are overviewed. In spite of decisive importance of signal processing algorithms like filtering, adaptive equalizing, symbol timing recovery, carrier reconstruction, etc., this paper is essentially devoted on problems of coding-decoding methods applied in medium- and high speed modems (7200,. . .14400 bit/s data rates).

The trellis encoder is introduced in Sec. 3. The Viterbi algorithm, as a delayed decision method and its implementation are detailed in Sec. 4 and 5. To give illustration and experimentally prove of the increased efficiency of those more sophisticated coding techniques, measurements have been carried out. The results are presented in Sec. 6.

2. PROCEDURES OF DATA TRANSMISSION

The block diagram of the data transmission over (analog) telephone channel is shown in Fig. 1. The transmitter converts the input data stream into the analog signal appropriate for the bandlimited, analog telephone channel (CCITT G712). The transmitter and the receiver have inverse structure regarding their functions.

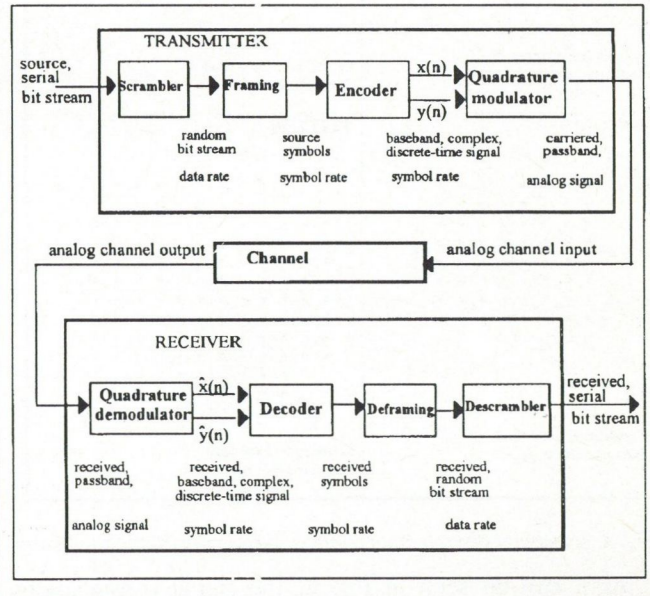


Fig. 1. Data transmission over analog channel

Self-syncronizing **scrambler/descrambler** is used in the system. Its duty is to "randomize" the input bit stream, because the appropriate operation of the modulator-demodulator needs message independent statistically well balanced signal sequences.

The data rates (measured in bit/s) are the same for the input, scrambled, received, and descrambled bit streams.

Typical values are 7200, 9600, 12000, 14400 bps. The high speed CCITT modems use constant symbol rate of 2400 Baud (=2400 symbol/s). (It is determined by the 300-3400 Hz telephone bandwith.) **Framing/deframing** is used to convert the different data rates (bit/sec) to the constant 2400 Baud symbol rate. The scrambled bit stream to be transmitted is framed into source symbols of 3, 4, 5, 6 consecutive data bits in case of 7200, 9600, 12000, 14400 bps data rates, respectively. The symbol alphabets at the input of the encoder have 8, 16, 32, 64 elements (source codewords) according to the data rate. Deframing means parallel/serial conversion of the bits of the decoded codewords, and so, from the 2400 Baud symbol rate the proper data rate is reconstructed..

The **encoder** maps the incoming source symbol sequence into the complex discrete-time signal sequence. The sets of possible complex signal elements for different data rates are shown in Fig. 2. This representation of modem signals are called the signal constellation diagrams. As we see, the signal elements differ not only in phase but also in amplitudes. Sometimes the x, y coordinates of the complex signals are called quadrature components of the signals and this type of modulations is called quadrature amplitude modulation (QAM). The **decoder** carries out two dimensional quantization of the received discrete-time complex signal (decision) and maps the decided signal sequence into the received sequence of codewords.

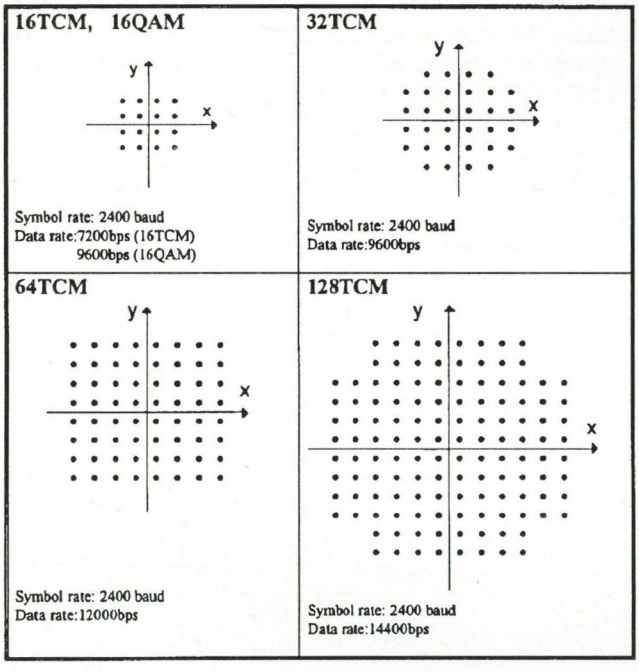


Fig. 2. Baseband discrete-time complex signal constellation diagrams

As it can be seen in Fig. 2, the signal constellations always have invariancy of rotation of $\pi/2$. In the receiver the demodulator can't reconstruct the absolute phase of the baseband complex signal, therefore there is always a constant but unknown phase shift between the encoder output and the decoder input complex signals. This phase shift uncertainty is integer multiple of $\pi/2$. For this reason, the information carried by the quarter of signal plain always have to be differentially encoded .

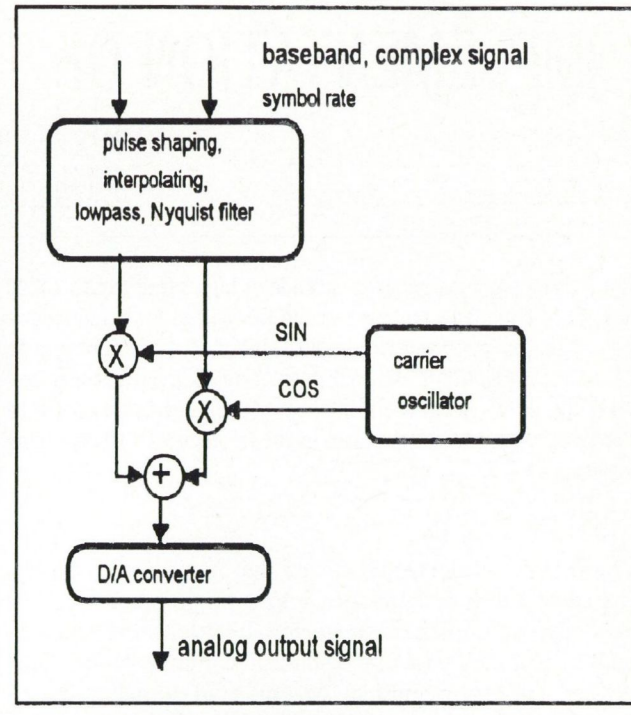


Fig. 3. Quadrature modulator

There are two types of signal element coding: nonredundant (QAM) coding and redundant, trellis coding (TCM). In the case of nonredundant QAM coding the number of the source symbol alphabet and the number of the possible signal elements are equal and there is memoryless one-to-one mapping of the differentially coded symbols into the complex signal elements. It follows, that in the decoder memoryless quantization is applied to make hard decision based on the received signal and the corresponding codeword is promtly determined .

In the case of trellis coding the number of possible signal elements is double of the number of source symbol elements. A convolutional encoder (sequentional machine) adds redundant bit to the former differentially coded bits and the sequence of these codewords are mapped into the enlarged signal space. As a delayed decision techniques, the Viterbi algorithm is used for decoding the codewords in the receiver.

Quadrature modulator is used to map the 2400 Baud complex signal into the carrier analog signal suitable to transmit over the bandlimited (300-3400 Hz) telephone channel. Block diagram of the modulator is shown in Fig. 3.

In the receiver the quadrature demodulator reconstructs the received baseband complex signal with the frequency of the symbol rate. To realize this demodulator, rather complex digital signal processing algorithms have to be implemented (filterings, AGC, interpolation, adaptive equalizing, phase locked loop techniques for symbol-timing and carrier recovery, detections of tracking states, etc.). Without discussing the details the block diagram of the implemented demodulator is given in Fig. 4.

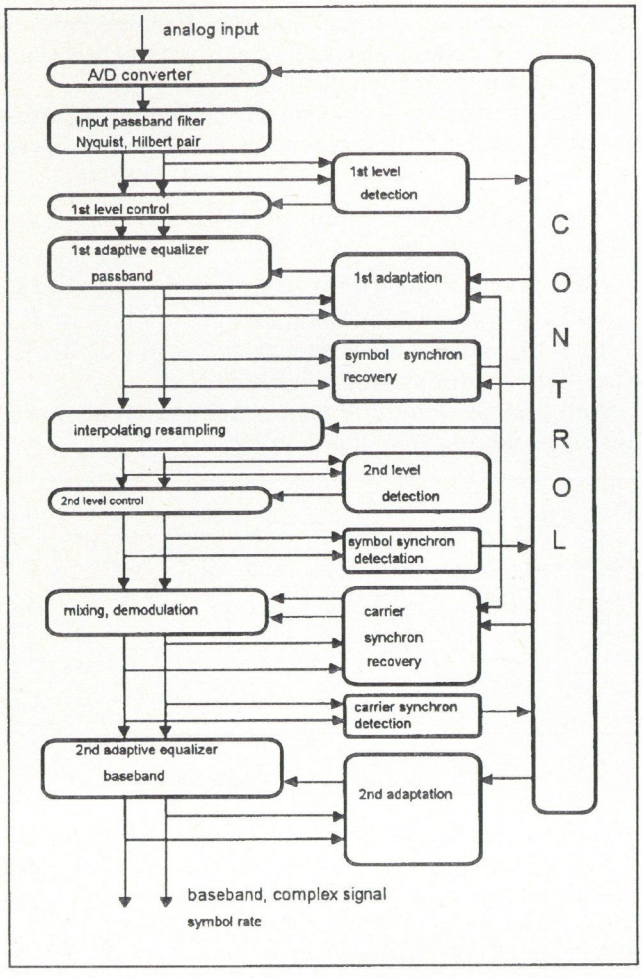


Fig. 4. Quadrature demodulator

3. TRELLIS ENCODER

As we mentioned former, the trellis encoder includes a serial/parallel converter, a differential encoder, a convolutional encoder and a signal mapping block. (Fig. 5)

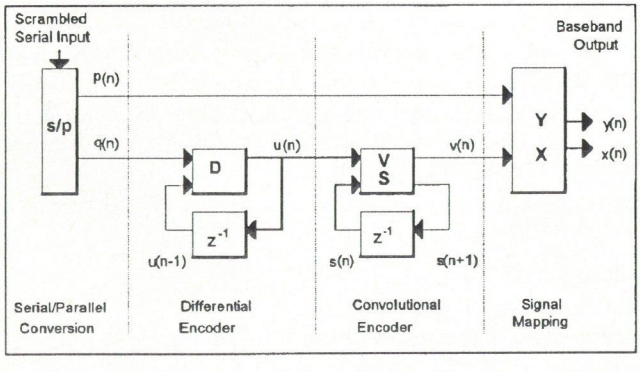


Fig. 5. Block diagram of framing and the trellis encoder

As the results of the S/P conversions the source symbols appear with 2400 Baud rate. These 3, 4, 5 or 6 bits codewords correspond to 7200, 9600, 12000 and 14400 bit/s data rates. These codewords are divided into 2 bits q part and into 1, 2, 3 or 4 bits p part. First two bits in time belong to q and the rest are in p:

$$q(n) \in Q, \quad Q = \{0,1,2,3\}$$

$p(n) \in P$,	16TCM:	$P = \{0,1\}$,	7200 bps
	32TCM:	$P = \{0,1,2,3\}$,	9600 bps
	64TCM:	$P = \{0,1,2,3,4,5,6,7\}$,	12000 bps
	128TCM:	$P = \{0,1,\ldots,15\}$,	14400 bps.

The two-bit word q has to be coded differentially because an integer multiple of $\pi/2$ phase uncertainty is always present in the receiver carrier recovery. Differential encoder is determined formally by the function **D**:

$$u(n) = \mathbf{D}(q(n)u(n-1)), \; u(0) = 0$$
$$u(n) \in U, \;\; U = \{0,1,2,3\}.$$

The CCITT-defined numerical details of function D is given in the Appendix.

The differentially encoded $u(n)$ is the input of the convolutional encoder which is a finite state sequentional machine described as follows:
The state transition function:

$$s(n+1) = \mathbf{S}(s(n), u(n))$$
$$s(n) \in S \;\; S = \{0,1,2,3,4,5,6,7\}.$$

The output function:

$$v(n) = \mathbf{V}(s(n), u(n))$$
$$v(n) \in V \;\; V = \{0,1,2,3,4,5,6,7\}.$$

The functions **S** and **V** are also given in the Appendix. Let us note that the redundancy introduced by the trellis encoder is included in $v(n)$, e.g. in the output of the convolutional encoder.

There are some possible versions of graphical representation of the state transition function. The most popular of them is shown in Fig. 6. This is called trellis diagram. The possible paths are shown in the figure supposing the starting state $s(0)$ to be 0. In this directed graph, the nodes represent the possible states of the convolutional encoder in time instant n. Specific input and output symbols belong to all branches according to the state transition- and output functions. Four branches originate from each nodes and four branches lead into each nodes from the previous states according to the four possible input symbols $u(n) \in U$, $U = \{0,1,2,3\}$. Let us note that knowing the state $s(n)$ and the output v leading to this state, the previous state $s(n-1)$, and corresponding input u can be determined by the trellis diagram (trace back of path on trellis). We emphasize, that the convolutional encoder is the same in all cases of different data rates.

Here we mention that two inverse functions can be derived:

$$s(n) = \mathbf{S}^{-1}(s(n+1), u(n)).$$

The inverse state transition function $\mathbf{S}^{-1}$ gives information about the previous state $s(n-1)$ assuming that the current state $s(n)$ and one possible input u of the convolutional encoder is

$$s(n-1) = \mathbf{S}^{-1}(s(n)u).$$

Having obtained the function $\mathbf{S}^{-1}$ we can write

$$v(n) = \mathbf{V}(s(n)u(n)) = \mathbf{V}(\mathbf{S}^{-1}(s(n+1), u(n)), u(n) =$$
$$= \mathbf{V}^{-1}(s(n+1), u(n)).$$

In other words, the function $\mathbf{V}^{-1}$ gives the previous output of the convolutional encoder $v(n-1)$ assuming the current state is $s(n)$ and one possible input is u:

$$v(n-1) = \mathbf{V}^{-1}(s(n)u).$$

These derived functions are used in the Viterbi algorithm as a part of decoding procedure in the receiver. (See the next section.)

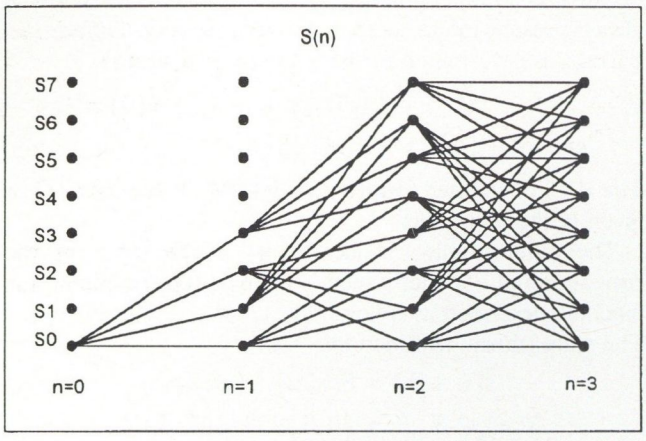


Fig. 6. Trellis diagram of encoder state sequence

The outputs of the former blocks $v(n)$ and $p(n)$ are the inputs of the following signal mapping functions:

$$x(n) = \mathbf{X}(v(n), p(n)),$$
$$y(n) = \mathbf{Y}(v(n), p(n)).$$

The output of the signal mapping functions can be interpreted as complex baseband signal with the symbol rate 2400 Baud (see Fig. 2.). For the 9600 bit/s 32TCM-case see the numerical values in the Appendix.

4. THE VITERBI ALGORITHM

The optimum (maximum likelihood) decoding for convolutional code can be either Viterbi algorithm or sequential decoding. Both are of low computational complexity. Each sequence of source symbols corresponds to a path in the trellis. The maximum likelihood decoder selects the path the probability of which is maximum for the actually received sequence. Let the cost of a path be the negative logarithm of its probability for the actually received sequence, then the maximum likelihood decoding is the search for the path of minimum cost. If the channel is an additive white Gaussian noise channel then this cost is proportional to the Euclidean distance of source sequence (corresponding to the path) and the received sequence. In the sequel we consider this cost.

The Viterbi algorithm is a minimum-cost search technique specifically suited for a trellis. It is an example of a dynamic programming technique which was originally developed for error control codes. A good general development for this application may be found in Forney [3].

The key idea of Viterbi algorithm is the following. The minimum cost path from time 0 to time n must be an extension of one of the minimum cost paths to a node at time $n-1$. Thus in order to find the best possible path of length L, we compute the best path to each state for each time unit by finding the best extension from the previous states into the current state and we perform this procedure for each time unit up until time L.

Before the formal description of the Viterbi algorithm we introduce the min operation as a two-output operation:.

$$\min_{x \in X}\{a(x), x\} \Rightarrow \{a_m, x_m\},$$

where

x is a variable in finite set X, $x \in X = \{x_1, x_2 \ldots x_M\}$,
$a(x)$ is a real valued function over X: $a(x)$: $X \Rightarrow R$
a_m is the **value** of the minimum: $a_m \leq a(x), x \in X$
x_m is the **address** of the minimum: $a(x_m) = a_m$.

With this notation the Viterbi algorithm can be wieved as a signal flow diagram shown in Fig. 7.

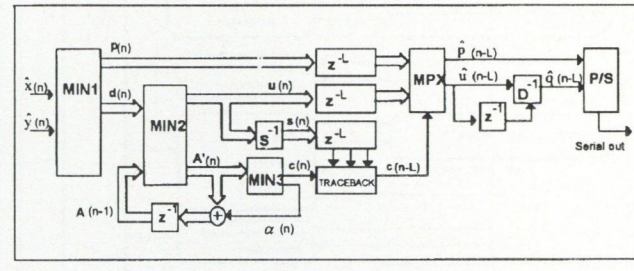


Fig. 7. Block diagram of Viterbi decoder

The inputs of the Viterbi decoder are the outputs of the quadrature demodulator $\hat{x}(n)$, $\hat{y}(n)$. The first block yields conditional minimums over the subsets of the total signal space:

$$\textbf{MIN1}: \min_{p \in P}\{t(\hat{x}(n), \hat{y}(n), v, p), p\} \Rightarrow \{d_v(n), p_v(n)\}, \forall v \in V,$$

where $t(x, y, v, p) = \sqrt{(x - \mathbf{X}(v,p))^2 + (y - \mathbf{Y}(v,p))^2}$.

Function $t(x, y, v, p)$ represents the Eucledian distance between the received (x, y) point and the $(\mathbf{X}(v,p), \mathbf{Y}(v,p))$ point which is the ideal signal point determined by possible v and p parameters. Values d_v are the minimum distances for all groups indexed by supposed v parameters and $p_v - s$ are the p values minimizing t, supposing v (conditional decisions). Let **p** and **d** denote the vector of the p_v and of the d_v values $\forall v \in V$ respectively. The time sequence of $\mathbf{p}(n)$ vectors are stored in L step deeply.

The conditional minimum distance values in vector $\mathbf{d}(n)$ are used to calculate the conditional accumulated distance values vector $\mathbf{A}'(n)$:

$$\textbf{MIN2}: \min_{u \in U}\{\mathbf{A}_k(n-1) + d_m(n)), u\} \Rightarrow \{A'_s(n), u_s(n)\}, \forall s \in S,$$

where $k = \mathbf{S}^{-1}(s, u)$, $m = \mathbf{V}^{-1}(s, u)$
and $A_s(n) = A'_s(n) - \alpha(n)$,
where $\alpha(n)$ is the result of the third minimum search:

$$\textbf{MIN3}: \quad \min_{s \in S}\{A'_s(n), s\} \Rightarrow \{\alpha(n), c(n)\}.$$

The values in the vector **d** refer to the **v** parameters (all supposed outputs in the convolutional encoder). The values in the $\mathbf{A}'$ vector refer to the possible s parameters (all supposed encoder states). The $A_s(n)$ component of $\mathbf{A}(n)$ vector is the conditional accumulated distance in the n-th time instant assuming the encoder state is s.

The distinction between $A_s(n)$ and $A'_s(n)$ is introduced to avoid overflow in the accumulation. $A's(n), \forall s \in$

S are the direct results of the conditional accumulated distances, however, it is enough to store their relative distance $A_s(n)$ from their minimum $\alpha(n)$.

The operation **MIN2** yields not only conditional accumulated distances $A's(n)$ (supposing the actual state is s) but it also has an other output vector $\mathbf{u}(n)$. The element $u_s(n)$ means the input to the convolutional encoder in time instant n supposing the state is s and $u_s(n)$ results the minimum conditional accumulated distance $A'_s(n)$. $u_s(n)$ minimizes the conditional accumulated distance (the condition is that encoder state is s in the time instant n).

If we suppose that the encoder would be in state r in the n-th time instant and knowing that under this asumption $u_r(n)$ is the encoder input — which minimizes the conditional accumulated distance $A'_r(n)$ — we could determine the encoder state in time instant $n-1$ using the inverse state-transition function $\mathbf{S}^{-1}$:

$$s_r(n) = \mathbf{S}^{-1}(r, u_r(n)), \quad \forall r \in S.$$

$s_r(n)$ is the previous encoder state which is the most probable state in sense that this minimizes the conditional accumulated distance supposing the actual state being r. All these conditional previous states are stored and delayed in order to make L-step delayed unconditional decision on the encoder state in the time instant $(n-L)$. The algorithm leading to this delayed decision is called TRACEBACK. The array of the stored **s** vectors ($\mathbf{s}(n)$, $\mathbf{s}(n-1), \ldots \mathbf{s}(n-L+1)$) contains all the best conditional paths belonging to all supposed actual states. Making decision according to **MIN3**, we obtain the state c(n) which minimizes the conditional accumulated distances and $c(n)$ is therefore the best starting point to find the survival path. The traceback algorithm is as follows:

$$\begin{aligned} c(n-1) &= s_{c(n)}(n) \\ c(n-2) &= s_{c(n-1)}(n-1) \\ &\ldots \\ c(n-L) &= s_{c(n-L+1)(n-L+1)}. \end{aligned}$$

Having obtained the delayed decision on the encoder state $s_c(n-L)$, we can select (MPX) the encoder input in the time instant $(n-L)$:

$$\hat{u}(n-L) = u_{c(n-L)}(n-L),$$

and the encoder output is:

$$\hat{v}(n-L) = \mathbf{V}(c(n-L), \hat{u}(n-L)),$$

so the selected (MPX) p value is:

$$\hat{p}(n-L) = p_{\hat{v}(n-L)}(n-L).$$

According to the differential coding of q in the encoder, in the decoder the $\mathbf{D}^{-1}$ inverse function has to be used to get the reconstructed q:

$$\hat{q}(n-L) = \mathbf{D}^{-1}(\hat{u}(n-L), \hat{u}(n-L-1)).$$

Making parallel-to-serial conversion on the two bits of $\hat{q}$ and 1, 2, 3 or 4 bits of $\hat{p}$ words, we get the received data stream with the data rate 7200, 9600, 12000 or 14400 bit/s, respectively.

5. IMPLEMENTATION OF THE ALGORITHM

As we have mentioned in the introduction, the CCITT V32bis modem has been implemented on the PC-DSP digital signal processing board plugged in an IBM PC/AT. Two Texas Instr. TMS320C25 signal processors, A/D and D/A converters and 2x32kword program-, 2x32kword local- and 32kword common (global) data memories have been placed on the board. The instruction execution time of the processors is 100 nsec (clock frequency is 40 MHz). It means that max. 8333 instructions can be executed in one symbol time interval providing the symbol rate is 2400 Baud.

The architecture of the implemented receiver is shown in Fig. 8. Further on we shall focus only on the Viterbi decoder implementation.

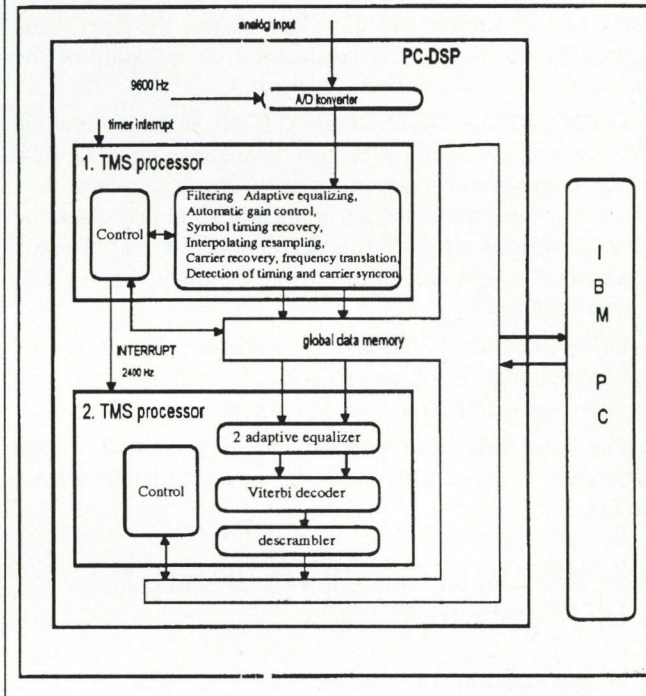


Fig. 8. Implementation of the receiver on PC-DSP board

The program of the Viterbi decoder consists of seven procedures.

INITIALIZATION: At each starts of the repeated execution of the Viterbi algorithm, initial values of some pointers and state variables have to be set (2μsec).

MINIMUM DISTANCE: This part of the algorithm determines eight conditional minimum distances (see vector **d** in previous section). To avoid time-consuming calculations, the implementation uses large look-up tables. The two-dimensional signal plane is divided into 32×32 cells and the input (x, y) complex signal is two-dimensionaly quantized on the base of that grid. Proper scaling of the signal ensures that 5 most significant bits of x and y can address the tables containing the precalculated conditional minimum distances belonging to the given cell. This method needs an 8×1024-word memory. The same technique is used to determine the conditional p parts of the received codewords ($\approx .4\mu$sec).

ACCUMULATED DISTANCE: This procedure is the most time-consuming part of the Viterbi decoder. Double-

nested cycle is used to determine the conditional temporary accumulated distances for all assumed states and for all possible encoder outputs (v) and the minimums are selected and stored. Those u values which belong to the minimum conditional accumulated distances are also stored. Using inverse state transition table ($\mathbf{S}^{-1}$ function), the previous states are determined and stored (140.8μsec).

ACC. DIST. UPDATE: Minimum of the temporary accummulated distance is determined by exhaustive searching. This minimum is subtracted from all temporary values. The address of the determined minima is the starting value of the trace-back pointer (11.8μsec).

TRACE.BACK: This procedure searches the survival path $L = 15$ step back. It is done on the base of the stored previous states. This data field of 8×16 elements is a chained-list structure containing pointers. The starting value of the pointer was discussed above, the final value is the address of the delayed decision on the state of the encoder 16 symbols before (23.6μsec).

CODEWORD DETERMINATION: Having obtained the decided encoder state, this addresses the data field which contains the delayed encoder input values $u(n-15)$. Convolutional encoder input and state addresses the encoder output table (**V** function), and this output value addresses the data field of the stored conditional $p(n-15)$ values (2.4μsec).

DIFFERENTIAL DECODER: This function is carried out by reading a look-up table ($\mathbf{D}^{-1}$ function) addressed by $u(n-15)$ and $u(n-16)$ (2.4μsec).

The total execution time of the implemented Viterbi algorithm is 186.2μsec. It is 45 percent of one symbol period.

6. COMPARING MEASUREMENTS OF TRELLIS ENCODER PERFORMANCE

In this section we would like to demonstrate how much more efficient the trellis coding system is than the memoryless QAM coding system. It may seem to be an obvious question to compare the 16QAM memoryless and 32TCM trellis coding because both use the same symbol rate (2400 Baud) and the same data rate (9600 bps) (see Fig. 2).

The typically used measure of modem performances is the BER (bit error ratio) versus SNR characteristics where SNR expresses the ratio of the average signal power and of the noise power added to the analog signal in the channel. BER is the result of comparison of the modulator input bit stream and of the demodulator output bit stream.

This overall measure of quality also depends on scrambling, coding, and the performance of the implemented modems. We note that the performance of a modem highly depends on the implemented signal processing algorithms, e.g. filtering, adaptive equalizing, timing and carrier recovery, etc. In our case we only want to measure the effect of changing the coding algorithm without its consequences on the modem performance. (If we change the coding, the signalling will be also changed, and a real demodulator could exhibit different performance in different signalling systems). If we only want to measure the performance of the encoder-decoder pair, we need ideal modulator, channel, and demodulator. Because of its practical difficulties, the measurement is made in the baseband, i. e. complex (two-dimensional) noise is added to the complex output signal of the encoder, and this complex noisy signal is directly fed to the input of the decoder. The block diagram of the measuring system implemented on the PC-DSP signal processing board is shown in Fig. 9.

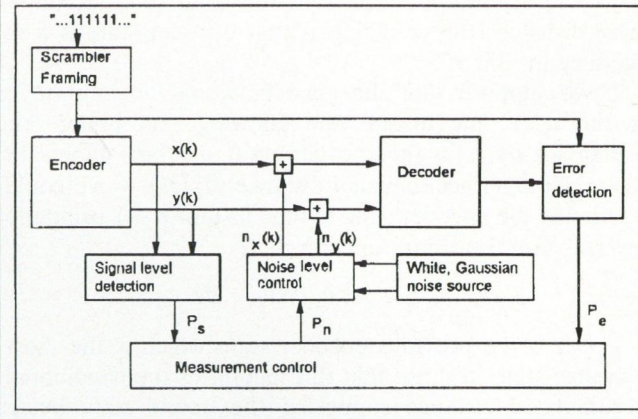


Fig. 9. Block diagram of baseband measurement of the error probability versus SNR

In our case SNR (signal to noise ratio) is defined as

$$SNR = 10\log_{10}(P_s/P_n) = 10\log_1 0\frac{\text{ave}[x^2(k)+y^2(k)]}{\text{ave}[n_x^2(k)+n_y^2(k)]},$$

where ave means averaging.

The probability of error (probability of false decision) P_e is estimated by relative frequency of received false symbols. The measured results are shown in Fig. 10.

To give perceptible insight what SNR values indicate, there are some illustrations of noisy signals in Fig. 11. The cases of the 14 dB and 20 dB SNR levels can be compared for 16QAM and 32TCM signals.

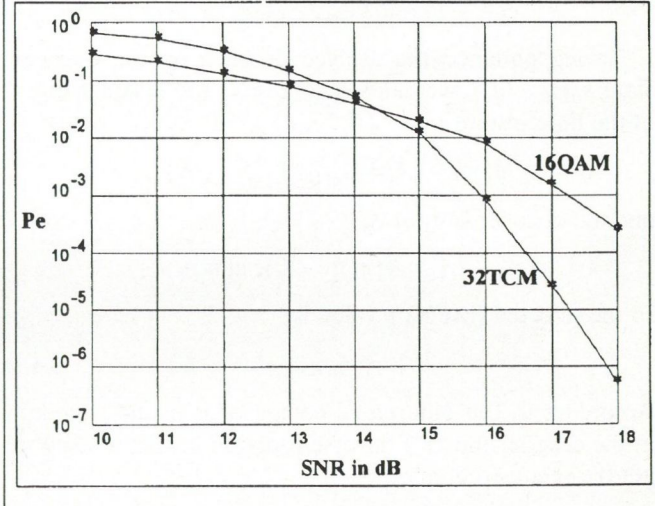


Fig. 10. Probability of error (Pe) versus signal to noise ratio (SNR) in case of 16QAM and 32TCM coding techniques

Comparing the performances of the 16QAM and the 32TCM coding methods we can see the crossover at about SNR=14dB (Fig. 10). At higher SNR values the

redundant trellis coding (32TCM) is more efficient, i.e. the probability of false decision is less than that of the 16QAM in spite of less distances between the signal states. Under extra noisy conditions (SNR is less then 14 dB), almost all the conditional decisions are already failed, and therefore it is not possible to make the advantage of the delayed decisions based on the conditional cumulated distortions. On this account the nonredundant 16QAM (having less number of possible signal states and thus greater distances of states) results a bit less probability of false decision. We have to emphasize that in all practically important cases ($P_e < 10^{-2}$) the trellis coding is more efficient than the memoryless QAM decisions.

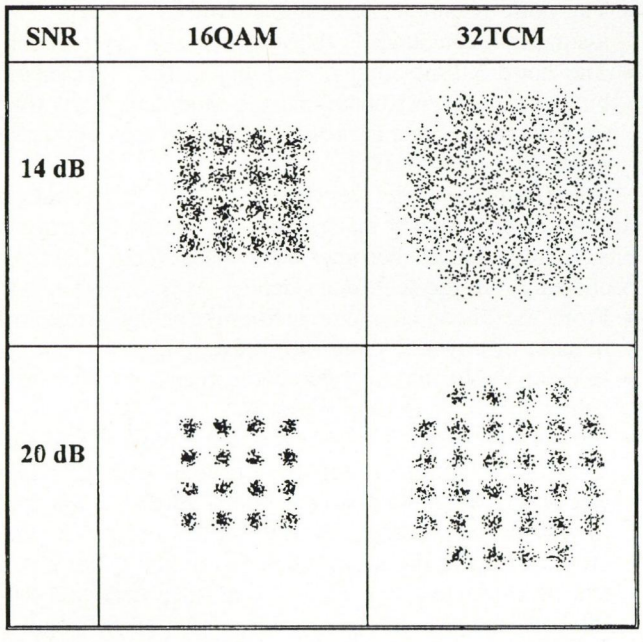


Fig. 11. Noisy signal constellations

APPENDIX

Tables of the differential encoder, decoder.

u(n) = D(q(n),u(n-1))		u(n-1)			
		0	1	2	3
q(n)	0	0	1	2	3
	1	1	0	3	2
	2	2	3	1	0
	3	3	2	0	1

q(n) = D^{-1}(u(n),u(n-1))		u(n-1)			
		0	1	2	3
u(n)	0	0	1	3	2
	1	1	0	2	3
	2	2	3	0	1
	3	3	2	1	0

Tables of the convolutional encoder.

s(n+1) = S(s(n),u(n))		u(n)			
		0	1	2	3
s(n)	0	0	3	2	1
	1	4	5	7	6
	2	1	2	3	0
	3	7	6	4	5
	4	2	1	0	3
	5	6	7	5	4
	6	3	0	1	2
	7	5	4	6	7

v(n)= V(s(n),u(n))		u(n)			
		0	1	2	3
s(n)	0	0	1	2	3
	1	4	5	6	7
	2	0	1	2	3
	3	4	5	6	7
	4	0	1	2	3
	5	4	5	6	7
	6	0	1	2	3
	7	4	5	6	7

Tables of signal mapping in case of 32TCM.

x(n)= X(v(n),p(n))		p(n)			
		0	1	2	3
v(n)	0	-4	0	0	4
	1	4	0	0	-4
	2	-2	-2	2	2
	3	2	2	-2	-2
	4	-3	1	-3	1
	5	3	-1	3	-1
	6	1	-3	1	1
	7	-1	3	-1	-1

y(n)= Y(v(n),p(n))		p(n)			
		0	1	2	3
v(n)	0	1	-3	1	1
	1	-1	3	-1	-1
	2	3	-1	3	-1
	3	-3	1	-3	1
	4	-2	-2	2	2
	5	2	2	-2	-2
	6	4	0	0	-4
	7	-4	0	0	4

Tables of derived inverse functions used in the decoder.

s(n-1) = S^{-1}(s(n),u)		u			
		0	1	2	3
s(n)	0	0	3	2	1
	1	4	5	7	6
	2	1	2	3	0
	3	7	6	4	5
	4	2	1	0	3
	5	6	7	5	4
	6	3	0	1	2
	7	5	4	6	7

v(n-1) = V^{-1}(s(n),u)		u			
		0	1	2	3
s(n)	0	0	1	2	3
	1	4	5	6	7
	2	0	1	2	3
	3	4	5	6	7
	4	0	1	2	3
	5	4	5	6	7
	6	0	1	2	3
	7	4	5	6	7

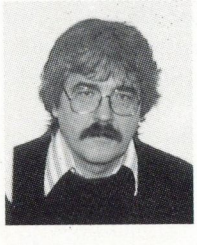
REFERENCES

[1] CCITT Data Communication Over the Telephone Network Series V Recommendations, BLUE BOOK Volume VIII-Fascicle VIII.1 Melbourne, 1988.

[2] CCITT Recommendation V.32 bis Geneva, 1991.

[3] Forney, G. D.,Jr.: The Viterbi algorithm. *Proc. IEEE*, 61:268-278, March, 1973.

[4] Koller I., Elek K., Gaál J.: PC-DSP: TMS320C25 alapú multiprocesszoros jelfeldolgozó kártya, Híradástechnika, XLIV.évf. 3-4. szám. 1993 márc.-ápr. 55-57 old.



Kálmán Elek was born in Budapest, in 1947. He received the Electrical Engineer and Dr. Univ. degrees from the Technical University of Budapest in 1971 and 1982 respectively. Since graduation he is a lecturer at the Department of Communication Electronics, giving lectures on Technical Acoustics, Programming, Control Systems, Digital Signal Processing, etc. In the 70's he continued research on the field of electromechanical filters, especially crystal and surface acoustic filters. Since 1983 his iterest turned into the field of digital signal processing applied in audio systems. Ih the latest years he took part of several research and developing projects such as digital signal processing in inertial navigation, adaptive differential PCM coding, signal processing implementation of data modems.

József Gaál was born in Budapest, in 1952. He received the Electrical Engineer and Dr. Univ. degrees from the Technical University of Budapest in 1976 and 1979 respectively. Since graduation he is a lecturer at the Department of Communication Electronics. Until 1984 his field of research was the Monte Carlo methods applied in the theory of network tolerances. He is the author of the monograph "Statistical Analysis and Synthesis of Electronic Circuits by Monte Carlo Methods" published by Akadémiai Kiadó Budapest in 1987. Since 1984 his research interest are in the field of digital signal processing. He took parts in several development and research projects such as digital signal processing in PCM codec, digital signal processing in inertial navigation, adaptive differential PCM coding, signal processing implementation of data modems.

ERROR-DETECTING CODES IN HARDWARE TESTING*

A. PATARICZA and E. SELÉNYI

TECHNICAL UNIVERSITY OF BUDAPEST
DEPARTMENT OF MEASURING INSTRUMENTS
AND MEASUREMENT TECHNOLOGY
MŰEGYETEM RKP. 9, H-1111 BUDAPEST

The ever-increasing complexity of the digital circuits results in more and more crucial problems in testing, both in the generation of test vectors and in the evaluation of the test responses. The most promising approach for VLSI-based circuits and systems is the application of the error correcting codes, widely used in telecommunication application. However in the article it is shown, that differences in the fault models and in the technical requirements prohibit the simple adaptation of the solutions in the telecommunication for the testing problems and new code designs are required. The first illustrative example, the error protection of semiconductor memories shows, that information redundancy resulting in hardware overhead can be partially substituted by time redundancy. The difference between telecommunication and testing application is illustrated in the next example, where it is shown that Reed-Solomon codes widely used in telecommunication have only poor characteristics as multiple-input signature analyzers. The basic ideas in the use of codes for test generation are presented by some novel results in pseudo-exhaustive test generation.

1. INTRODUCTION

The growing complexity of the digital circuits exposes in an increasing way methods for the assurance of the required reliability. As this complexity growth supersedes the manufacturing technology-related increase in the quality, the only solution is the use of thorough testing not only during manufacturing, but during the operation of the device as well. The basic problem can be formulated in a question of the following form: "How can we check, that a long, occasionally very long stream of data gained during the normal operation or during some kind of testing is correct?"

In applications requiring an extremely high reliability of operation, like in the nuclear industry, military and some biomedical electronics applications the only solution is some form of replication of the functional unit, like triplicated modular redundancy or the application of a duplicated processor kernel in master-checker mode [1]. However, in the majority of the applications with a moderate requirement for reliability this huge redundancy is still intolerable. A natural way to overcome this problem is the use of error-detecting and occasionally error-correcting codes resulting in a moderate hardware overhead.

Despite the formal analogy between the error control problems in the traditional field of telecommunication and hardware testing in using information redundancy for checking the correctness of the data, there are essential differences both from the theoretical and practical points of view between these fields of application.

As example the most widely used error models in the telecommunication originate the corruption of data in the transfer through a noisy channel. In the case of the well-known symmetric channel hypothesis the main consequences for the interrelationship between data and error are the following properties:

- The noise is independent of the data transmitted. This assumption concludes in the symmetric channel model.
- The noise is time-limited, resulting in the independent bit error model, assumed, that the time limit is less than the bit transfer time in the channel, or in the burst error model, if it exceeds that.

The resulting model consists a simple, homogenous-fault-to error mapping mechanism. The number or faulty bits or burst length becomes to a measure of the error probability. On the technical side:

- From the bit or character error probability a maximal number of errors to cope with is established.
- Additionally to the error detection, their correction to a limited extent is a primary goal.
- In telecommunication applications the most simple way to assure a high error detection probability is to subdivide the message data stream into segments and attach to each segment check symbols. In this process moderate increases in the information redundancy, like check bits or characters are tolerable, as they decrease only the code speed and the selection of the block length is within limits at the designer's choice.

However, in the case of hardware testing the fault-to-error mapping mechanism is rather complex, even when using simplifying assumptions in the fault model. The most widely used fault model assumes the presence of single or multiple so-called stuck-at faults. Their effect is that at the fault site a constant logic value is present independently of the correct value. This model is asymmetric, as in the case of a match between the correct value and this constant, no error is observable at the fault site, and the fault is manifested only as an error if they are of an opposite value. This model results in the so-called unidirectional error model well-describing the effects of a stuck-at fault at an output of the circuit. However even a single bit transient or permanent fault inside of the circuit, e.g. at the root point of multiple paths to the outputs or inside a feedback loop can cause errors at numerous circuit nodes and outputs during multiple time phases.

On the other side the assumption of the equiprobability of all error patterns is equivalent with independency of the value sequences in the fault-free and faulty case contradicting such observations, like an automaton with a cyclic operation saves this basic property even for many faults causing errors at the outputs.

Accordingly, in contrast to the telecommunication applications

*This work was supported by Grants OTKA T-760, T3394.

- in typical hardware testing tasks no homogenous, simple error models can be used,
- the limitation on the fault effects can not result in the general case in a simplified error model neither the sense of time nor in space distribution,
- there is no strict correlation between the number of faulty characters in an error pattern and its probability to occur,
- the number of characters in a pattern to check is determined overwhelmingly by external design factors, like the device under test, the test procedure developed for it.

From the practical side:

- the allowed amount of information redundancy is low, as in the majority of the applications it results in a significant hardware overhead,
- the processing speed must be at least as high as the normal operation of the circuit, in order to detect dynamic faults, appearing only at a sufficiently frequencies,
- in the majority of applications no error correction is required.

As result instead of a pure analytical methodology either all faults are simulated or benchmark-like error pattern sets are used for the estimation of the fault coverage when using an error control coding (ECC) technique for fault detection.

Additionally to the problems in test response evaluation the generation of the test input sequences becomes more and more crucial, especially in built-in test application. Both the number of the potential faults in a fault model and the length and complexity of the test sequence to detect them make the traditional approaches inapplicable. The exhaustive testing checking the reaction of the circuit under test to all possible input combinations is irrealistic due to the huge number of test vectors to be applied and some simple method is required assuring a tolerable overhead in testing time.

In the following sections we present some characteristic examples for the illustration of the main problems and error control codes based solutions for the hardware testing problems.

2. INFORMATION VS. TIME REDUNDANCY

The protection of semiconductor RAM memories is a very typical and traditional field of application of the error correcting codes in hardware devices, clearly illustrating the basic problems and main concepts in the most simple form. Its speciality is, that in this case also an error correction is typically required [3].

Memory chips can fail due to different failure modes:

- Permanent or hard errors originate in manufacturing problems or aging. This defects can affect:
  - A single cell or word, e.g. the overwhelming majority of defects in DRAM chips result from single-bit capacitor oxide failure. The "hard" (repeatable) failure rate of DRAM chips in the field is by about 200 FIT. (200 failures per 10^9 device-hours).
  - A group of adjacent cells (e.g. by a parasitic capacitive coupling between them).
  - Row(s) or column(s) in the cell matrix (due to errors in the row or column address decoders).
  - All cells on a data line (due to a defective read/write amplifier or data wire).
- Soft errors originate in particles radiation on power supply noises and result mostly in single or multiple cell errors, occurring according to the experiences by one order of magnitude more often than hard ones.

Permanent faults are typically detected in the power-on phase, when thorough functional tests can be executed, as the memory contains no valuable data. In the case of an error, degradation can be performed. In mission-time critical applications however both of the hard and soft faults must be masked in some form. When coping with soft errors the only way for their detection and eventually for their correction is the use of the hardware redundancy in the form of some error correcting code.

In a safety-relevant application the fault model consists both of hard and soft bit and word errors. At first, in the following we will present the main effects and concepts in handling soft errors following in a slightly simplified form the ideas presented in [2] .

Let's assume, that we want to build up a memory of a capacity of M words each of a length N. The occurrence of soft errors (Fig. 1) is usually modelled as a Poisson process of a soft bit error arrival rate λ. We assume, that the whole memory area is used and neglect the effect of fault masking due to overwriting of potentially faulty, but still unused data by new values. The probability of a single cell remaining fault-free during a period T is $P_0(T) = e^{-\lambda T}$ and the reliability of the chip, i.e. the probability that each bit in each word of it remains fault-free is $R_{unprotected}(T) = [P_0(T)]^{N \times M} = e^{-\lambda NMT}$. It is obvious, that a growth in the memory size drastically reduces the reliability. As the memory is unprotected, it will fail at the first fault and the mean time between failure (MTBF) will be as low, as $MTTF = 1/(\lambda NMT)$. Moreover, the mean time T' of a fault-free memory service period of a reliability of 99% ($R_{unprotected}(T') = 0.99$) is only by about one hundredth of the MTBF. In the case of a medium massively parallel multiprocessor configuration consisting of 100 processors with a memory capacity in each node of 32 MBytes this time period is as low as approximately 130 seconds, even if we assume a soft error rate 1 in 10^8 hours/bit.

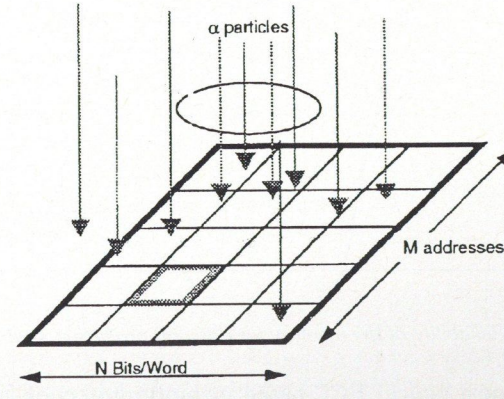


Fig. 1. Soft errors in a memory

If each word in the memory has a error correcting code by adding of K check bits, than the probability that a word of the length $(N + K)$ remains fault-free or correctable after a time period T increases to $P_{word,ECC}(T) = \sum_{i=0}^{d} P_{word,i}(T)$, where $P_{word,i}(T)$ denotes the probability of a word being hit i-fold during T, assumed, that bit errors in a word occur independently and repeated hits into a cell do not repair its content. The reliability of the memory, i.e. the probability, that no word in it consists of an uncorrectable error is $R_{ECC}(T) = [P_{word}(T)]^M$. As shown in Fig. 2 the use of ECC assures a higher initial reliability, but due to the redundancy introduced by the check bits the long-term reliability of the memory decreases. Moreover, as the possibility of tolerating more errors in a word would require more and more redundancy in the form of ECC check bits another way must be selected.

As error detection and correction occur only when the corresponding data is read and if a data word is not used for a longer period it can become uncorrectable due to the cumulative effect of multiple faults. An increase in the error detecting and correcting capabilities of the encoding would require more check symbols, i.e. it would result in an additional hardware overhead.

An alternative solution is based on the idea of the reduction of the mission time of the ECC based protection. In the case of memory scrubbing each word in the memory is periodically read out with a relatively low time period T_s and correctable errors are immediately removed. In this way information and hardware redundancy is substituted by time redundancy. The reliability in this case will be $R_{scrubbing}(T) = [R_{ECC}(T_s)]^{T/T_s}$, as the required total error-free service time T will be subdivided into T/T_s time slots each of the length T_s. The three approaches can be well-characterized by comparing their reliability, as shown in Fig. 2.

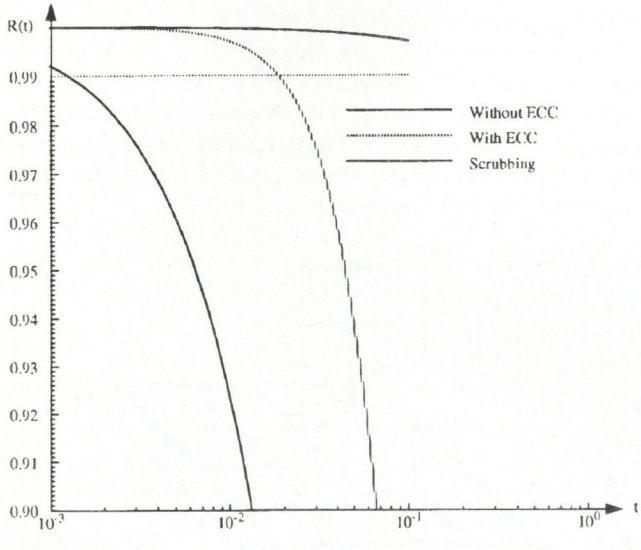


Fig. 2. Reliability of the memory for different protection strategies

The most typical ECC-based memory protection methods used in the practice are in an increasing fault-tolerance capability as follows [3]:

- Single bit error detecting (SED) with a parity bit.
- Single bit error correcting, double bit error detecting (SEC-DED) codes with the use of a modified Hamming code.
- Single byte error correcting (SbEC) codes (Hamming, Burton, Fujiwara, Hong-Patel codes).
- Single byte error correcting, double byte error detecting (SbEC-DbED) codes, like Reed-Solomon [4], [5], Kaneda-Fujiwara codes.

Another idea in reducing the information redundancy is based on the explicit utilization of the permanent nature of the hard faults. The main idea is as follows: let's assume, that a memory word, protected by a SEC-DED code consists a hard stuck-at and a soft error. As there are two bits in error, the syndrome decoding logic signalizes an uncorrectable error. However when writing back the binary complement of this faulty data, the bit value in the hard fault position will coincide with the stuck-at constant, and in the read data only the soft error will be active. After correcting this, the hard error reduces to an erasure error.

3. ERROR DETECTING CODES IN COMPACT TESTING

In the traditional scheme for hardware testing the output of the device under test (DUT) as response to some test input sequence is compared with the output sequence from a known faultfree reference device, or its model. However for the high-speed testing of complex devices, especially in the case of self-test neither the physical reference unit nor the model based approach can be applied, as the first one is equivalent with the duplication, and the second one can not fulfil the speed requirements. A possibility is the storage of the reference output sequences, but for long sequences the huge amount of storage area makes it impractical. [6] .

The idea of compact testing dates back to 1975 [7] . It is based on the observation, that when the output sequences of the DUT and of the reference device are treated as data parts of a systematic code their match can be evaluated by generating and comparing the check part of this code.

For checking the following information compression methods are used:

- Ones-count compression using the binary Hamming-weight of the data stream as check information;
- Transition-count, i.e. the total number of rising and falling edges in the stream, corresponding to the Hamming weight of the derivate of the stream;
- Accumulator compression testing, using the Hamming-weight and its time integral as reference;
- Signature analysis, using binary linear compression techniques; (a circuit is said to be linear over GF(2), if it consists only of storage elements and XOR type gates);

This last category is the most widely used one as general-purpose test compressor, as it can be proven, that only it provides a maximal error detection, if at the phase of compression method selection the reference sequences are unknown. In the case of equiprobable errors, the probability of an undetected error, in other terminology of a fault escape equals approximately 2^{-n}, where n is the signature bit count. In this way a proper detection probability is assured in the majority of

the applications using 16 check bits with an approximate fault escape probability of 1.5×10^{-5}. Moreover, the same circuits, which compress the test response, can easily reconfigurated to an exhaustive pattern generator supporting fully the self-test of a combinational circuit. In the built-in self-test of integrated circuits and boards this idea is realized in different forms, like in the following typical examples:

- Built-in evaluation and self-test (BEST [8]) using separate pseudorandom test generator and linear compactor;
- LSSD on-chip self-test (LOCST [9]), combining the concepts of level-sensitive scan design, single-bit pseudorandom pattern generation and single-bit linear compression;
- Built-in logic block observer (BILBO [10]) using registers for multiple-output pseudo-random test generation and multiple-input linear compression by implementing their function in a controllable mode;
- CEBS [11], combining pseudorandom test generation and linear compaction for the chip level, and boundary scan for the board level testing.

If the circuit has only a single output to be checked, than the use of error detecting polynomial codes, referred as single-input signature analysis is the most widely used solution, due to the high fault coverage and the simplicity of the checking circuit, depicted in Fig. 3.

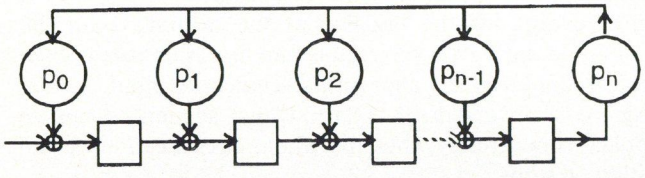


Fig. 3. Polynomial division circuit

Despite the formal analogy of this testing problem with the traditional field of application, the essential fault models in the background are rather different. The first difference is, that the length of the data part is not previously fixed or limitable during the code design phase. The analyzer must be capable of processing a serial bit pattern of an arbitrary length, which can reach several millions of bits.

A typical benchmark set consists of the following error patterns expressing some characteristic types of correlation due to the hardware faults between the error bits [15]:

- Errors with a few of error bits (1,2,3).
- Burst type error, where the positions in error are located in a limited interval.
- Cyclic and repeated errors, where the same error subsequence is repeated in time.

The basic phenomenon in selecting the first two groups is not the independency of the bits in error, as in a symmetric channel model, but the often performed minimization of the test input sequence in order to shorten the time needed to test. In an ideal minimal test set only a single test is contained for each fault. The burst model is typical, if the test input sequence is composed as concatenation of the subtests of the individual and independent functional units. In the practice primitive polynomial based checks are used, for which a maximal detection of the error patterns enlisted above is granted.

For the check of multiple output circuits many pure heuristic signature analyzers structures were evaluated. In the remaining, more systematic approaches the main idea in information compression is essentially analogous with the single-line signature analysis: the sequence of binary m-tuples of length L appearing on the outputs of the DUT as test response is compressed by generating the check symbols of a multi-bit symbol based error detecting code.

An interesting idea appears in [12] , where the use of a Read-Solomon (RS) code checker was proposed as multiple-input signature analyzer registers (MISR). We assume, that the reader is familiar with the basics of the RS codes, otherwise please refer [4] or [5].

In RS encoding the symbols (binary m-tuples) are interpreted as elements of the Galois-field $GF(2^m)$. In the most common case the RS code can be generated by a polynomial having subsequent elements from $GF(2^m)$ as roots, i.e. the generator polynomial is of the form $p(x) = (x - \alpha^j) \cdot (x - \alpha^{j+1} \cdot \ldots \cdot (x - \alpha^{j+k})$ for an arbitrary integer j (Here α is a primitive element of $GF(2^m)$.) By mapping the input data symbols into the corresponding $GF(2^m)$ elements, the input symbol stream can be interpreted as a polynomial over $GF(2^m)$ with the highest degree term corresponding to the first character in time. As check symbols the remainder from the division of the input and generator polynomials will be used. The polynomial division circuit is similar to that shown in Fig. 3, however with storage elements, constant multipliers and adders performing operations over $GF(2^m)$.

RS codes are maximum distance separable (MDS). For a code consisting no more binary m-tuples as symbols, than $2^m - 1$, RS encoding ensures the detection of as many random symbol errors, as checking characters are applied. This means a maximal utilization of the redundancy in the form of the checking characters. Due to this feature this codes are favorite candidates for a wide field of applications extending from telecommunication to consumer electronics.

An RS code is improper solution as MISR, despite its excellent error detection characteristics in telecommunication type applications. The typical benchmark pattern set of the multiple-input signature analysis consists of the following time and/or space limited patterns [17]

- Single in phase (SIP), with a corresponding error polynomial $c(x) = a_j x^i$. Here the value of the error symbol is described by the first, and its position in time by the second term.
- Same error pattern (SEP), where the same error symbol is repeated in time, with an error polynomial $e(x) = \alpha^j r(x)$. Here the binary polynomial describes the repetition in time of the error character of value α^j.
- Single in line (SIL) as a special case of SEP with errors at a single output of the DUT. The error polynomial is of an identical form, as for SEP, however here $0 \leq j \leq m$, because the single bit errors to be repeated correspond to the first m states in the state transition graph of the polynomial $g(x)$ generating $GF(2^m)$.

As all repetition polynomials are binary ones, and the error pattern is obviously undetectable, if his polynomial is a

multiple of the generator one, the error detection features of the RS encoder depend on the minimal degree non-zero binary polynomial $G(x)$, for which $G(x)|p(x)$. From the mathematical side this problem is essentially identical with the estimation of the generator polynomial of a Bose-Chaudhuri-Hocquenghem (BCH) code with the solution $G(x) = \text{l.c.m}(m_j(x), m_{j+1}(x), \ldots, m_{j+k-1}(x))$, where $m_i(x)$ denotes the minimal degree binary polynomial, for which $m_i(\alpha^i) = 0$.

E.g. in the $j = 1$, $m = 4$, $k = 4$ case (four check characters of a width of four bits) over $GF(2^4)$ generated by $(x^4 + x + 1)$, the minimal binary polynomial of the RS checker becomes to $G(x) = \text{l.c.m}(m_1(x)m_2(x), m_3(x), m_4(x)) = (x^4 + x + 1) \cdot (x^4+x^3+x^2+x+1)$ i.e. the degree $G(x)$ of is only 8, and the fault escape probability is as high, as $2^{-8} = 1/256$! A traditional MISR design having the same number of signature bits would assure an approximate fault escape probability of the value $2^{-n} = 2^{-16} = 1/65536$. For practical sense that means, that applying RS codes e.g. in CPU testing, there is a non-negligible probability to leave a bit manipulation fault resulting in error patterns of the SIL type undetected.

As summary of the error detection features of the RS encoders in MISR applications, we can state, that they are usually far away from the theoretical upper limits. It should be pointed out, that this drawbacks are direct consequences of the different fault models in hardware testing as for telecommunication applications. A main conclusion from the example above is, that even the well-proven solutions need a careful rechecking while transplanting them from a field of application to another one.

4. PSEUDOEXHAUSTIVE TESTING

Traditional test techniques require the estimation of the input test sets with the associated output responses based on a fault model of the device under test, so, that the faults contained by the model could be detected (or perhaps diagnosed). These test sets are then programmed into an automatic tester, which applies them to the unit under test and checks the responses. There are a number of difficulties with this approach [19].

- An explicit fault model is required. In LSI and VLSI circuits the classical assumption that only single stuck-at-faults have to be considered may no longer valid. The use of more complex models substantially increases the difficulty of pattern generation.
- Pattern generation is required. Automatic test pattern generation is expensive (because it is a NP-complete problem) and does not provide sufficiently high fault coverage. Manual methods are restricted in complexity and they considerably increase the production cycle time.
- An expensive tester is needed.

Much effort has been made all over the world to avoid these problems. To refine the classical method new and more effective test generating algorithms have been developed, more productive testers have been designed, etc. Besides these advances two new approaches have been worked out recently.

- Design for testability resulting structural restrictions for the circuit designer, but simplifying testing. Typical examples of this method are the above mentioned LSSD, BILBO etc.
- The other approach named pseudoexhaustive testing has been worked out by E.J.McCluskey et al. in order to eliminate redundant test vectors in the pseudorandom approach [20].

The traditional exhaustive test of a combinational circuit includes every combination of the input variables. Thus except for those bridging-faults that transform the circuit into an asynchronous sequential one, the unit is completely tested without any specific fault model. The disadvantage of this method is that for n inputs 2^n test vectors are required. In practice only ROM-based circuits need this kind of testing; gate structured circuits can be exhaustively tested by a considerably shorter sequence of test patterns. This simplification can be achieved by partitioning the circuit into subcircuits which are then separately tested exhaustively.

Fig. 4 shows a circuit, where F1, F2 and F3 are arbitrarily realized logical functions. The circuit has six inputs, so its exhaustive test would contain 64 test vectors. However in this case the number of test vectors can be reduced, as each output depends on only 4 of the inputs. Thus, except for the bridging of the outputs, both the F1-F2 and the F1-F3 subcircuits can be tested using 16-16 vectors only. By an appropriate choice of input vectors (e.g. $a \neq e$ and $b \neq f$) these two sequences can be applied concurrently, thus the whole circuit can be tested within 16 steps.

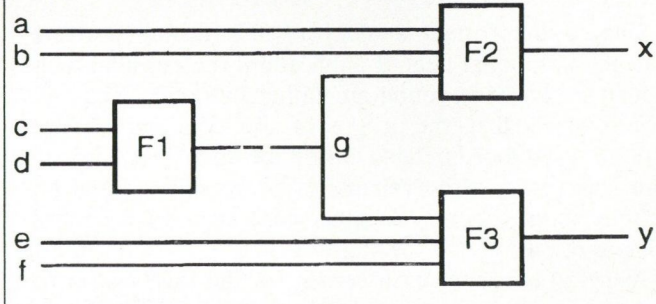


Fig. 4.

The test sequence can be further reduced by the serial decomposition of F1-F2 (F1-F3). Four test vectors and the sensitization of g through F2 are sufficient for testing F1,F2 and F3, both having 3 inputs to be tested with a total of 8 vectors. If the logic function of F1,F2,F3 are known, some of the first four vectors can be applied surely concurrently with some of the second eight ones, thus the test would contain less then 12 steps.

With this decomposition method we can check

- every single stuck-at fault,
- every multiple stuck-at fault in the circuit,
- bridging-fault within the modules,

but we cannot detect the multiple stuck-at-faults and bridging-faults between the modules. As shown in the example, the decomposition of a gate-structured circuit

led to a testing, which was not exhaustive in the whole n dimensional space, but only on its — not necessarily disjoint subspaces of dimensions $k_1, k_2 \ldots k_m$.

It is possible to find the proper k_i subspaces by a thorough examination of any individual circuit, but usually it is much more easy to determine the maximal dimension ($k = k_{max}$) of them, hence a test being exhaustive for all k-subspaces of the n dimensional space of input variables can be used. The problem in general is solved by the $[n, k, T]$ pseudoexhaustive codes. These are code sets containing of total T binary m-tuples exhaustively covering every k-subspace. The pseudoexhaustive codes can be efficiently used also testing parasitic cell coupling faults in registers and memories. RAM tests, which check every pair of cells in all four combinations are widely used.

Up till now no general solution exists for finding an optimal $[n, k, T]$ code. An optimal solution means practically the minimum number (T) of necessary test vectors for a given n and k. Pseudoexhaustive codes described in the literature are not aimed to be optimal, only to be more or less effective. In the following, we will describe some of the interesting code constructions.

a) Optimal code for $k = n - 1$ [20].

Code construction: every combination of the $k = n-1$ bits is enlisted in $T = 2^k$ rows. The n^{th} column is calculated as the modulo 2 parity sum of the other columns (see Fig. 5).

S_1	S_2	$S_3 = S_1 \oplus S_2$
0	0	0
0	1	1
1	0	1
1	1	0

Fig. 5. An optimal code for $k = n - 1$ ($V = [3, 2, 4]$)

b) Optimal code for $k = 2$ [21].

In case of $k = 2$ the all-zero and all-one codes contain the combinations 00 and 11 for each pair of bits, respectively. To include the combinations 01 and 10, any two columns must be unordered. Binary vectors **a** and **b** are unordered, if there exist such bit positions i and j, that $a_i = 0$ and $b_i = 1$, while $a_j = 1$ and $b_j = 0$, respectively. An effective way of selecting unordered codes for the columns is to choose those of a constant weight. Thus the optimal code construction is the following (Fig. 6): Let the first element of any s_i column code be 0. The next $T - 1$ elements ($T - 1$ being an odd number) are forming a code of weight $T/2$. The maximal number of such columns $n_{max} = \binom{T-1}{T/2}$, equals the maximal length of the code. Note, that this method generates the 11 combinations without containing the all-one code.

	S_1	S_2	S_3	S_4	S_5	S_6	S_7	S_8	S_9	S_{10}
0	0	0	0	0	0	0	0	0	0	0
T/2 out-of (T-1) codes	0	0	0	0	1	1	1	1	1	1
	0	1	1	1	0	0	0	1	1	1
	1	0	1	1	0	1	1	0	0	1
	1	1	0	1	1	0	1	0	1	0
	1	1	1	0	1	1	0	1	0	0

Fig. 6. Optimal code for $k = 2$ ($V = [10, 2, 6]$)

c) Systematic code for $k = 2$

Code construction: Let the i-th column code be $s_i = 0[i]1[\neg i]$ where $[i]$ denotes the binary expression for i and $[\neg i]$ is the 1's complement of (Fig. 7). Having T as an even number test vectors of the length of $n_{max} = 2^{T/2-1}$ bits can be encoded.

S_i	S_0	S_1	S_2	S_3
0	0	0	0	0
i	0	0	1	1
	0	1	0	1
1	1	1	1	1
$\neg$i	1	1	0	0
	1	0	1	0

Fig. 7. Systematic code for the $k = 2$ case

d) Constant weight codes [22].

Code construction: Let $V = [n, k, T]$ be a code containing every vector v_i of weight(s) w such, that $w = c \bmod (n - k + 1)$ for a constant c, where $0 \leq c \leq n - k$. For $k = n - 1$ this method provides the optimal code. Thus, in this case $w = c \bmod 2$, if $c = 0$, then all codes of even weights, if $c = 1$, then all codes of odd weights are included in V.

An example for $k = 2$:

Let $c = 0$,	then $w_1 = 0$,	$w_2 = n - 1$
Let $c = 1$,	then $w_1 = 1$,	$w_2 = n$
Let $c = 2$,	then $w = 2$	
Let $c = n - 2$,	then w=n-2.	

The best cases of these are when $c = 0$ or $c = 1$. If $c = 0$, then V includes the all-zero vector and all the vectors containing only one zero. In this case $T = n + 1$, which is considerably worse than the optimal solution. For $k = 3$ the best choice is to take all the codes containing a single zero, and all the codes containing single one ($w_1 = 1$, $w_2 = n - 1$). The number of necessary vectors equals $T = 2k$, as shown in Fig. 8.

n	Number of test vectors	
	Effective code	Constant weight code
3		8
4	8	8
8	14	16
16	22	32
32	32	64

Fig. 8. Number of test vectors for $k = 3$

e) Effective systematic code for $k = 2$ [23]. A code for arbitrary n and $k = 2$ can be obtained from a $V_0 = [3, 2, 4]$ pseudoexhaustive code by the following algorithm: Let remove from V_0 the all-zero code and denote the columns of the remaining code with s_0, s_1 and s_2 respectively. To construct the i-th column code in the n dimensional space, let us rewrite the index i into the ternary number system and denote its digits with $a_0 \ldots a_q$. The i-th column of in the extended code will be $S_i = 0[s_{a_0}][s_{a_1}] \ldots [s_{a_q}]$, as illustrated in Fig. 9. E.g. the fifth column will be constructed as $S_5 = S_{12_3} = 0[s_1][s_2]$.

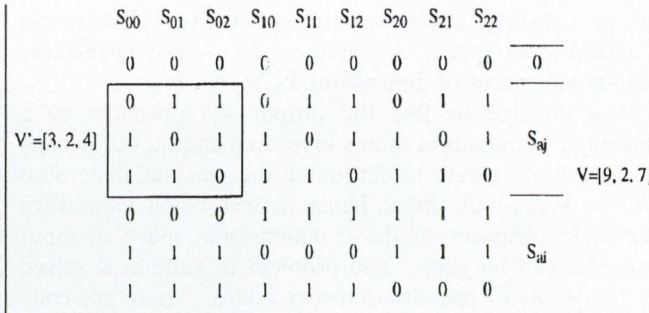


Fig. 9. A systematic $V = [9, 2, 7]$ code

f) Effective code construction for $k = 3$ [23] .

Let $V_2 = [n, 2, T/2]$ be the systematic code containing columns of the form $s_i = 0[i]1[\neg i]$ as described in Section c) above. In this case, the $V_3 = V_2 \oplus V_2$ code (the $\oplus$ operation between codes has to be executed between all ordered pairs of code-words of them) will form a pseudoexhaustive code for $k = 3$. The effectiveness of this construction is shown in Fig. 8. where it is compared with the constant weight code described in Section d).

5. CONCLUSIONS

The application of error-correcting codes plays an increasingly important role in digital hardware testing. However as shown in the previous illustrative examples the strict limitations in hardware and time redundancy require new solutions and prohibit a simple transplantation of the well-proven solution from the field of telecommunication. The development of new, effective encoding procedures for testing purposes is still a topic of vivid research activities.

REFERENCES

[1] Hohl, W.; Michel, E.; Pataricza, A.: Hardware Support for Error Detection in Multiprocessor Systems — A Case Study. Microprocessors and Microsystems, Vol 17., No. 4., May 1993., pp. 201-206.

[2] Goodman, R.M.; Sayano, M.: The Reliability of Semiconductor RAM Memories with On-Chip Error-Correction Coding, *IEEE Trans. on Information Theory*, Vol. IT-37, No. 3, May 1991, pp. 884-896.

[3] Rao, T.R.N.; Fujiwara, E.: Error-Control Coding for Computer Systems, Prentice-Hall International, Inc. Englewood Cliffs, NJ, 1989.

[4] Györfi, L.; Vajda, I.: A hibajavíto kódolás és a nyilvános kulcsú titkosítás elemei Budapesti Műszaki Egyetem, 1991.

[5] MacWilliams,F.J., Sloane, N.J.A.: The Theory of Error-Correcting Codes, North Holland, Amsterdam, 1977.

[6] Abramovici, M.; Breuer, M.A.; Friedman, A.D.: Digital systems testing and testable design, *Computer Science Press*, 1990.

[7] Benowitz, N. et al.: An Advanced Fault Isolation System for Digital Logic. *IEEE Trans. on Computers*, Vol. C-24., No. 5., May 1975., pp. 489-497.

[8] Lake, R.: A Fast 20K Gate Array with On-Chip Test System, VLSI System Design, Vol. 7, No. 6, June 1986, pp. 46-66

[9] LeBlanc, J.: LOCST:A Built-In Self Test Technique, *IEEE Design and Test of Computers*, Vol. 1, No. 4, Nov. 1984, pp. 42-52

[10] Konemann, B. et al.: Built-In Test for Complex Digital Integrated Circuits, *Digest of Papers* 1979 Test Conference, pp. 37-41.

[11] Butt, H.H.; El-Ziq, Y.M.: Impact on Mixed-Mode Self-Test of Life-Cycle Cost of VLSI Based Designs *Proc. Int. Test Conf.*, 1984, pp. 103-111.

[12] Iwasaki, K., Arakawa, F.: An Analysis of the Aliasing Probability of Multiple-Input Signature Registers in the case of a 2m-ary Symmetric Channel. *IEEE Trans. on Computer Aided Design*, Vol. 9., No. 4., Apr. 1990., pp. 427-438.

[13] Iwasaki, K.: Analysis and Proposal of Signature Circuits for LSI Testing. *IEEE Trans. on Computer Aided Design*, Vol. 7., No. 1., Jan. 1988., pp. 84-90.

[14] Pataricza, A.: An Improved Signature Analysis Based CPU Self-Test. Microprocessing and Microcomputing, *The EUROMICRO Journal*, Vol. 23., 1988., pp. 167-172.

[15] Smith, J.E.: Measures of Effectiveness of Fault Signature Analysis. *IEEE Trans. on Computers*, Vol. C-29., No. 6., June 1980., pp. 510-514.

[16] Saluja, K.K., Karpovsky, M.: Testing Computer Hardware through Data Compression in Space and Time. IEEE 1983 International Test Conference, 1983., pp. 83-88.

[17] Hassan, S.Z. et al.: Parallel Signature Analyzers Detection Capability and Extensions. *IEEE Compcon Spring*, 1983., pp. 440-445.

[18] Pataricza, A.: An Optimal Input-Transformation Based Signature Analyzer Structure for Multi-Output Circuits. Proc. FTSD-11., Suhl, 1988., pp. 240-245.

[19] McCluskey, E.J.; Bozorgui-Nesbat, S.: Design for Autonomous Test, *IEEE Trans. on Computers*, Vol. C-30., No. 11., Nov. 1981., pp. 866-875.

[20] McCluskey, E.J.: Verification Testing. 19th Annual Design

Automation Conference. Las Vegas, Nevada, June 14-16 1982., pp. 495-500.
[21] McCluskey, E.J.: Verification Testing — A Pseudoexhaustive Test Technique. *IEEE Trans. on Computers*, Vol. C-33., No. 6., June 1984.
[22] Tang, D.; Woo, L.S.: Exhaustive Test Pattern Generation with Constant Weight Vectors. *IEEE Trans. on Computers*, Vol. C-32., No. 12., Dec. 1983., pp. 1145-1150.
[23] Selényi, E.: New Methods for Pseudoexhaustive Testing. *Periodica Polytechnica*. Series Electrical Engineering, Vol. 31., No. 1-2., 1987., pp. 11-20.

András Pataricza received his diploma in electrical engineering from the Technical University of Budapest in 1977. Since then he is with the Department of Measurement and Instrument Engineering of this institution, currently as associate professor. He defended his Candidate of Technical Science (Ph.D.) thesis entitled "Signature analyzers for maximal error detection" in 1988. He is currently for a year with the University of Erlangen-Nürnberg Institute of Informatics as visiting lecturer in the framework of the Konrad Zuse program of the DAAD. His research fields include the theory of hardware testing, especially the use of information compaction methods and fault-tolerant computer architectures. He is author of by about 40 papers in this fields.

Endre Selényi is full professor at the Technical University of Budapest, Department of Measurement and Instrument Engineering. He defended his Doctor of Technical Science thesis in the field of system level testing of multiprocessor systems in 1987. In 1985 he won the highest Hungarian award for scientific research, the State Prize for his work as principal investigator in the development of the MMT Microprocessor Application System. His research fields include the theory of error-correcting codes and their application in fault-tolerant hardware synthesis and the testing and testable design of microprocessor-based systems. He serves as head of the Committee for Informatics Education at the Faculty of Electrical Engineering and Informatics of the TUB supervising the teaching and curriculum development of this branch of the faculty and as head of the Hungarian Accreditation Board on Technical Informatics.

CLARIFYING MAGYARCOM'S INVESTMENT STRATEGIES AND PRIORITIES FOR MATÁV: THE SHARED VISION FOR HUNGARY

December 22, 1993 signalled a new era in the history of telecommunications in Hungary and in Central and Eastern Europe for this is the day that the concession agreements were signed, money was transferred, and MagyarCom became the owner of 30 % of the Hungarian Telecommunications Company (HTC) or MATÁV. For 875 million US dollars, we gained the right to provide public telephone service in Hungary as the National Concession Holder. As to its value, it was the largest privatization transaction and the most important foreign working capital investment carried out, not only in Hungary, but in the whole Central and Eastern European region. Keeping in mind the importance of the telecom sector in developed economies and, seeing that even compared to the overall state of the Hungarian economy this industry can be considered a weak area, we can begin to understand how the event in December really did signal a whole new era in the history of telecommunications in Hungary.

Last fall I helped put together the MagyarCom consortium formed by Deutsche Bundespost Telecom and Ameritech which was chosen by the Hungarian Government to be the choice strategic partner for the privatization of MATÁV. As a new Executive Director of MATÁV, I am anxious for them to become a "world class" telecommunications company comparable with any of those in the Western Countries of Europe. I would imagine that those of you from other Central and Eastern European countries may have a similar goal.

I would like to talk this afternoon about MagyarCom and the role we will be playing in the near-term development of MATÁV. To do that, I will first very clearly paint the picture of what the shared vision is that we have for Hungary. I will then describe the plans that MagyarCom has to enhance the value of MATÁV including some of our detailed strategies in the technical, marketing, human resource and other areas.

I would first like to take a few minutes to talk about MagyarCom and the role we will play in the near-term development of MATÁV. Together, Deutsche Bundespost Telekom and Ameritech have begun to demonstrate their shared commitment to develop MATÁV into a world-class telecommunications company. Through the shared vision for Hungary that I have already mentioned plus a unique combination of skills and strengths, each of the members of our Consortium is committed to assisting MATÁV in exceeding its development goals.

As one of the world's leading telecommunications providers, Ameritech possesses technical and operating experience, and serves residential and business customers in the United States with the most advanced telecommunications services available today. Headquartered in Chicago, Illinois, Ameritech employs 70 000 people and attained 1993 revenues of almost USD 12 billion.

DBP Telekom is one of the world's largest telecommunications companies and is a leader of technologicaI innovation. It has recently transformed the telecommunications system of Eastern Germany, and through this has gained invaluable experience in rapid and extensive network development. DBP Telekom is currently involved in projects of regional co-operation with MATÁV and other Central and Eastern European operators, such as the Trans European Link and the International Network Management System.

The combination of Deutsche Bundespost Telekom and Ameritech brings a harmonised set of individual skills experiences know-how, strategic intent and commitment to MATÁV. Together, MagyarCom's shared vision for Hungary offers:

A unique combination of skills, including:
- large scale project management and network development expertise
- international presence, facilities and hubbing experience
- competitive successes in all types of regulatory environments
- a singular focus on meeting customer's needs
- and technical excellence and leadership in telecommunications services.

It also offers a demonstrable commitment to Hungary with:
- jointly, over 7 years of activity in Hungary seeking participation in the privatization and operation of MATÁV
- a common belief in Hungary's potential for rapid economic growth
- and a shared vision of Hungary's future in the heart of Europe and the European Community.

I keep referring to this shared vision so let me briefly describe what it is. MagyarCom's vision for the year 2000 places MATÁV as the leader in telecommunications service provision throughout Central and Eastern Europe and places Hungary in a position to reap the rewards of international trade and culture.

By the year 2000, MATÁV will have:
- An extensive, technically advanced telecommunications network.
- A highly skilled and motivated workforce.
- A corporate culture responsive to customers' needs.
- And a leading role in the setting of quality standards in Hungary.

In return, by the year 2000, Hungary will have:

- A business community equipped with the telecommunications services needed to compete effectively in the European Community
- It will have a choice of the latest advanced services throughout the country.
- And an accessible telephony service providing quality and affordability at the level of the European Community.

MagyarCom plans to enhance the value of the company through a variety of strategies and plans which build on the foundation started by MATÁV. MagyarCom will enhance MATÁV's value through the implementation of an aggressive business plan which includes:

- development of an advanced network infrastructure and Network Management
- improvements in quality and efficiency through the deployment of modern Operations Support Systems
- development of an international, commercial and telecommunications hub in Hungary
- transformation from a network driven company to a customer focused company
- implementation of creative marketing and sales techniques
- co-operation with regulators and other communications operators
- and development of human resources.

MagyarCom will enhance the value of MATÁV by transferring skills and knowledge to MATÁVs employees and increasing the productivity and performance levels of the workforce. This will be accomplished through enhanced management practices, greater employee mobility and skill rebalancing.

MagyarCom is committed to value enhancement for MATÁV and believes this can be achieved through the implementation of our very aggressive business plan. The starting point of the development plan is rapid line installation and a network upgrade programme. The technological improvements in the system in terms of quality, efficiency, and capability, as well as the satisfaction of presently unmet demand will boost profitability and equity value over time. At the same time, the development plan to enhance, MATÁVs value will include continuous emphasis on technical and operational advancement, international hub implementation, regulatory management, culture change, human resources development, and marketing innovation.

Looking specifically at the strategy and implementation plans of MagyarCom, we have made a commitment to apply the best technologies available to provide telecommunication services in Hungary. In terms of new technology, MATÁV now has the following plans for the future:

- Introduce advanced network management
- Rapidly complete the SS7 network
- Continue the digitalization of exchanges
- Introduce ISDN in Budapest
- Deploy digital loop carrier systems
- Increase usage of fibre in the local loop
- Install wireless loops to meet the most urgent demand
- Enhance the planning process for all network elements
- Implement Operator Services Networks and Operations Support Systems.

MagyarCom's strategy is focused on the optimization of the existing network capacity and its rapid expansion to meet customer demand as early as possible. The availability of SS7 and SDH throughout the entire network paves the way for the implementation of advanced network technology such as Intelligent Network and ISDN.

Accelerating the digitalization and electronization of exchanges will enhance network quality and efficiency. With the appearance of more and more services, the need for advanced operations support systems and operator services networks increases dramatically. MagyarCom will bring its extensive experience in these areas and systems to MATÁV.

The expansion of the local loop requires significant investment to provide the required rate of 15,5 % per year increase in new customer lines. Our first priority is to increase the utilization of switch capacity and redirect much needed investment into rapid expansion of the local loop. Our second objective is to maintain a close match between increased switch capacity and local loop capacity to meet projected customer demand and the requirements of the Concession Contract. This is a complex and demanding process, absorbing over 70 % of the projected capital investment, and requiring strong, revenue related project management, coupled with state-of the-art installation techniques.

In addition to the expansion of the traditional copper network throughout the concession area, optical fibre cable will be deployed in the feeder network. MagyarCom's experience in establishing fibre networks will lead to a highly sophisticated, reliable and "future proof" local network. The application of digital loop carrier systems (DLC) both on existing copper plant and on newly installed optical fibre cables will ensure a capability to connect new customers rapidly in the most economic manner.

The installation of fibre as feeder lines to the cross connection cabinets in the local loop will increase the capability to provide new digital services. In the business centres of Hungary, an all-fibre overlay network connecting large customers on high-bit-rate-streams to the network will fuel the telecommunications business.

Radio access technologies will play an important role both as a temporary solution and as the ultimate solution in remote areas. MagyarCom will assist MATÁV in implementing these systems throughout the concession area to meet the government's requirements for reducing connection times and the waiting list.

MATÁV's planning tools, already in place, will be complemented by even more advanced computer aided planning and design tools. These will be an integrated part of a fully automated telecommunications administration and management system. We will assist MATÁV with planning and implementation expertise in order to accelerate all current projects. We propose a network architecture following modern design principles to ensure an efficient combination of existing facilities with the newest technologies. Close co-operation with local governments and municipalities will ensure rapid installation and expansion of local loops. By 1998, full geographic coverage will be

reached in order to meet the government's objectives for connection of new customers.

Our strategy is to ensure that all subscribers connected to the network will receive high quality service. Rapid replacement of manual switches and party lines will decrease the number of faults and increase the usefulness of the network. Furthermore, the deployment of a digital telecommunications infrastructure and advanced OSS and Network Management tools will make achieving a high quality network a practical reality.

MagyarCom is also devoted to transforming MATÁV into a customer focused service provider. MATÁV must respond rapidly and effectively to the changing needs of its customers. This involves not only an increase in the capacity and quality of the network and the expansion of service offerings, but the transition to a customer-focused company and the implementation of creative marketing techniques.

Changing to a customer-focused company requires full corporate commitment beginning with top management and spreading throughout the entire company. This commitment is predicated on the belief that the customer is paramount and that customer desires and expectations will now drive MATÁVs investment and resource deployment decisions. The members of MagyarCom have undergone similar transitions in their home markets. In each situation, this change has begun with restructuring the company to respond to customer's needs. MagyarCom will draw from its considerable experience to assist MATÁV in implementing a new structure. In the new MATÁV, there will be entrepreneurially independent units equipped with the means and authority to conduct business successfully.

The needs of specific customer groupings will replace traditional operating organizations. All employees of MATÁV must refocus their energies on serving the customer, while the corporation as a whole must be flexible, responsive and supportive. This will also be stimulated by MATÁVs Employee Share Ownership Programme.

One example of restructuring is in network planning, which will be the responsibility of a single unit providing maximum integration and deploying the services customers require. The day-to-day interface with customers will be decentralised, allowing maximum flexibility and responsiveness. Specific regional plans will be developed, taking into account unique requirements and circumstances.

The implementation of MATÁV's Key Account programme and the identification of more key accounts is the first step towards segmenting the market. Further development of the Key Account program must be a top priority for MATÁV. In addition to the existing accounts in the government, finance, insurance, and media sectors, MagyarCom will assist in developing target markets for its key account programme, such as:

- large private network operations including transportation, utilities, education, health care and emergency services
- new entrepreneurial sectors such as telemarketing, consultancies international trading companies and retail chains
- the tourist and travel industry

MagyarCom will begin to work immediately to transfer first-hand experience to MATÁV in serving large corporate accounts and will expand MATÁV's market segmentation scheme, focusing on small business owners, entrepreneurs, and high, value residential users to build strong customer relationships.

Understanding and meeting the different needs, expectations and perceptions of individual business and residential users is critical to strengthening MATÁV's reputation as a quality provider of telecommunications services. As validated in our marketing research, customers place a high importance on improved levels of service quality, better responsiveness from MATÁV, and availability of a wider range of services at good value. MagyarCom will assist MATÁV in developing a complete marketing plan which will address the needs of customers.

I began this talk with a statement of our vision for MATÁV and for Hungary in the year 2000 which pictures MATÁV as having an extensive, technically advanced telecommunications network. Its workforce will be highly skilled and motivated and the company will be responsive to customer needs. MATÁV will have a leading role in the setting of quality process in Hungary. Let me just conclude with a re-affirmation that through the plans I have just outlined and through MagyarCom's investment in MATÁV, we will realize that vision.

JOHN L. DRAHEIM
Vice President – Ameritech International
Executive Director – MATÁV

Information for authors

JOURNAL ON COMMUNICATIONS is published monthly, alternately in English and Hungarian. In each issue a significant topic is covered by selected comprehensive papers.

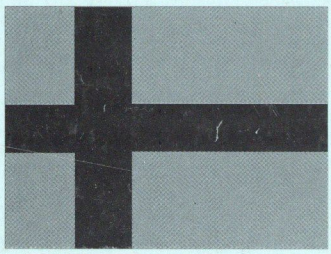
Other contributions may be included in the following sections:

- INDIVIDUAL PAPERS for contributions outside the focus of the issue,
- PRODUCTS-SERVICES for papers on manufactured devices, equipments and software products,
- BUSINESS-RESEARCH-EDUCATION for contributions dealing with economic relations, research and development trends and engineering education,
- NEWS-EVENTS for reports on events related to electronics and communications,
- VIEWS-OPINIONS for comments expressed by readers of the journal.

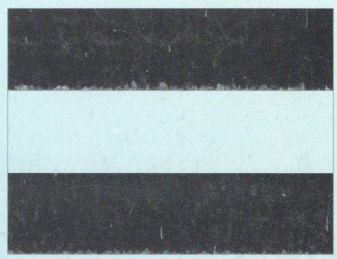
Manuscripts should be submitted in two copies to the Editor in chief (see inside front cover). Papers should have a length of up to 30 double-spaced typewritten pages (counting each figure as one page). Each paper must include a 100–200 word abstract at the head of the manuscript. Papers should be accompanied by brief biographies and clear, glossy photographs of the authors.

Contributions for the PRODUCTS-SERVICES and BUSINESS-RESEARCH-EDUCATION sections should be limited to 16 double-spaced typewritten pages.

Original illustrations should be submitted along the manuscript. All line drawings should be prepared on a white background in black ink. Lettering on drawings should be large enough to be readily legible when the drawing is reduced to one- or two-column width. On figures capital lettering should be used. Photographs should be used sparingly. All photographs must be glossy prints. Figure captions should be typed on a separate sheet.



SVÉDORSZÁG



MAGYARORSZÁG

Digital exchanges
Microwave and optical transmission
Digital mobil telephony
Land mobile radio-systems
Various network elements
Turn-key projects
Software products for telecommunication
Air-conditioning for telecommunication
Power equipment for telecommunication systems

Ericsson Technika Kft.
Budapest X., Venyige u. 3.
Levél: 1475 Budapest, Pf. 154.
Tel.: 147-6590
Fax: 127-6040

ERICSSON

Ericsson Technika