The slanted expanding system is shown in Fig. 8. To explicate
the mechanisms involved, we consider again the juxtaposition of
patterns 1 and 22 of Table IV. Table IX shows the four nonadjacent
patterns on S1 obtained by modifying input bits on the interface.

Fig. 8. Slanted expanding system.

TABLE IX
<table>
<thead>
<tr>
<th>Input</th>
<th>Output</th>
<th>Input</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>0000</td>
<td>0000</td>
<td>0000</td>
<td>0000</td>
</tr>
<tr>
<td>0000</td>
<td>0000</td>
<td>0000</td>
<td>0000</td>
</tr>
<tr>
<td>0100</td>
<td>0111</td>
<td>0111</td>
<td>0111</td>
</tr>
<tr>
<td>1111</td>
<td>1111</td>
<td>1111</td>
<td>1111</td>
</tr>
<tr>
<td>0000</td>
<td>0000</td>
<td>0000</td>
<td>0000</td>
</tr>
<tr>
<td>0000</td>
<td>0000</td>
<td>0000</td>
<td>0000</td>
</tr>
<tr>
<td>0000</td>
<td>0000</td>
<td>0000</td>
<td>0000</td>
</tr>
<tr>
<td>0000</td>
<td>0000</td>
<td>0000</td>
<td>0000</td>
</tr>
<tr>
<td>0101</td>
<td>0111</td>
<td>0111</td>
<td>0111</td>
</tr>
<tr>
<td>1111</td>
<td>1111</td>
<td>1111</td>
<td>1111</td>
</tr>
<tr>
<td>1111</td>
<td>1111</td>
<td>1111</td>
<td>1111</td>
</tr>
</tbody>
</table>

The best lower bound we have obtained in this way is
\[ G_0 \geq 0.43723 \]
by using the results of the stripe expansion problem.

0018-9448/90/0100-0180$01.00 ©1990 IEEE
We prove that $R_{\text{comp}} = R_0$ for pairwise reversible (PR) multiaccess channels. A channel is said to be PR if for all pairs of input letters $x$ and $x'$

$$\sum_{y: P_N(y|x') > 0} \sqrt{P(y|x) P(y|x')} \log \frac{P(y|x)}{P(y|x')} = 0 \quad (1)$$

where $P(y|x)$ denotes the channel transition probability, i.e., the conditional probability that output letter $y$ is received given that input letter $x$ is transmitted. For a multiaccess channel, $x$ stands for a vector with one component for each user. For example, for a twoaccess channel, $x = (u, v)$ where $u$ is transmitted by user 1 and $v$ by user 2.

Pairwise reversibility was first defined in [2] in the context of reliability exponents for block codes. The class of PR channels includes many channels of theoretical and practical interest. Examples of ordinary (one-user) PR channels are the binary symmetric channel, the erasure-type channels defined in [3], the class of additive gaussian noise channels (by extension to continuous alphabets), and more generally, all additive noise channels for which the noise density function is symmetric around the median. Examples of PR multiaccess channels are the additive gaussian noise channel, the AND and OR channels, and more generally, all deterministic multiaccess channels.

Following Jacobs and Berlekamp [4], we lowerbound the computational complexity of sequential decoding in terms of lower bounds to the average list size $\lambda$ for block coding. In Section II we lowerbound $\lambda$ for ordinary PR channels, and in Section III for PR twoaccess channels. These bounds may be of interest in their own right, with possible applications to the list decoding schemes discussed by Elias [5] and Forney [3].

II. AVERAGE LIST SIZE FOR ORDINARY PAIRWISE REVERSIBLE CHANNELS

The discussion in this section is restricted to one-user discrete memoryless channels. We denote the input alphabet of such a channel by $X$, the output alphabet by $Y$, and the transition probabilities by $P(y|x)$. We denote transition probabilities over blocks of $N$ channel uses by $P_N(y|x)$. This is the conditional probability that the output word $y = (y_1, \ldots, y_N)$ is received given that the input word $x = (x_1, \ldots, x_N)$ is transmitted. Since the channel is assumed memoryless, $P_N(y|x) = \prod_x P_N(y|x)$. Consider a block code with $M$ codewords and blocklength $N$. Let $x_m$ be the codeword for message $m, 1 \leq m \leq M$. The average list size for such a code is defined as

$$\lambda = \frac{1}{M} \sum_{m=1}^{M} \sum_{x_m} P_{\text{max}}, \quad (2)$$

where $P_{\text{max}}$ is the conditional probability, given that $m$ is the true (transmitted) message, that a channel output is received that makes message $m'$ appear at least as likely as message $m$. More precisely

$$P_{\text{max}} = \sum_{y: P_N(y|x_m) \geq P_N(y|x_{m'})} P_N(y|x_m). \quad (3)$$

Thus, $\lambda$ is the expected number of messages that appear, to a maximum-likelihood decoder, at least as likely as the true message. The following result from [2] (which is essentially the Chernoff bound [7, p. 130] tailored for this application) is the key to lowerbounding $\lambda$ for PR channels.

**Lemma 1:** For any two codewords $x_m$ and $x_{m'}$ on a pairwise reversible channel

$$P_{\text{max}} + P_{\text{max}} \geq 2g(N) \sum_{y} \left[ P_N(y|x_m) P_N(y|x_{m'}) \right] \quad (4)$$

where $g(N) = (1/8) \exp((2N \ln P_{\text{max}})$ and $P_{\text{max}}$ is the smallest nonzero transition probability for the channel.

Summing the two sides of inequality (4) over all pairs of messages, we obtain

$$\lambda \geq \frac{1}{M} \sum_{m=1}^{M} \sum_{x_m} P_N(y|x_m) P_N(y|x_m). \quad (5)$$

To simplify this, we consider a probability distribution $Q$ on $X^N$ such that, for each $x \in X^N$, $Q(x) = \left( \text{the fraction of messages } m \text{ such that } x_m = x \right)$. Thus, $Q(x) = k/M$ if $x$ is the codeword for exactly $k$ messages. We shall refer to such probability distributions as code compositions. Now, inequality (5) can be rewritten as

$$\lambda \geq g(N) \sum_{x} Q(x) Q(x') \sum_{y} P_N(y|x_m) P_N(y|x_{m'}). \quad (6)$$

and thus we obtain Theorem 1.

**Theorem 1:** For block coding on pairwise reversible channels, the average list size satisfies

$$\lambda \geq g(N) \exp N \left( R - R_0 \right) \quad (7)$$

where $R = (1/N) \ln M$ is the rate, $N$ the blocklength, and $Q$ the composition of the code, and we have defined

$$R_0 = -\frac{1}{N} \ln \sum_{x} Q(x) \left[ \sum_{y} P_N(y|x) \right]^2. \quad (8)$$

This theorem gives a nontrivial lower bound to $\lambda$ whenever the code rate $R$ exceeds the code-channel parameter $R_0$. To obtain a lower bound that is independent of code compositions, we recall the following result by Gallager [7, pp. 149–150].

**Lemma 2:** For every probability distribution $Q$ on $X^N$ (where $N$ is arbitrary and $Q$ is not necessarily a code composition),

$$\lambda \geq g(N) \exp N \left( R - R_0 \right) \quad (9)$$

where we have by definition

$$R_0 = \max_{Q} \left\{ -\frac{1}{N} \ln \sum_{x} Q(x) \left[ \sum_{y} P_N(y|x) \right]^2 \right\}. \quad (10)$$

The maximum is over (single-letter) probability distributions $Q$ on $X$.

Combining Theorem 1 and Lemma 2, we have Theorem 2.

**Theorem 2:** If a block code with rate $R$ and blocklength $N$ is used on a pairwise reversible channel, then the average list size satisfies

$$\lambda \geq g(N) \exp N \left( R - R_0 \right). \quad (11)$$

Thus, at rates above the channel parameter $R_0$, the average list size $\lambda$ goes to infinity exponentially in the blocklength $N$, regardless of how the code is chosen. Theorem 2 is actually a special case of a general result, proved in [6], which states that, for block coding on any discrete memoryless channel, $\lambda > \exp N \left( R - R_0 - o(N) \right)$, where $o(N)$, here and elsewhere, denotes a positive quantity that goes to zero as $N$ goes to infinity. Known proofs of this result involve sphere-packing lower bounds to the probability of decoding error for block codes, and are far more complicated than the proof of Theorem 2. What makes the proof easy for PR channels is Lemma 1, which fails to hold for arbitrary channels.

There is a well-known upper bound on $\lambda$, which completes Theorem 2: For block coding on any discrete memoryless channel, there exist codes such that $\lambda < 1 + \exp N \left( R - R_0 \right)$. This result is known as the Bhattacharyya or the union bound, and can be proved by random-coding methods [7, pp. 131–133]. Thus, $R_0$ has fundamental significance as a threshold: At rates $R > R_0$, $\lambda$ must go to infinity as the blocklength $N$ is increased.
at rates \( R < R_n \), there exist codes for which \( \lambda \) stays around 1, even as \( N \) goes to infinity.

At first sight, Theorem 2 may seem to contradict Shannon's noisy-channel coding theorem. One may expect that it should be possible to keep \( \lambda \) around 1 at all rates below the channel capacity \( C \), since the probability of error can be made as small as desired at such rates. To discuss this point, let \( L \) denote the list-size random variable. Let \( P_e = \text{Prob}(L > 1) \). It follows by Theorem 2 that, at rates \( R > R_n \), \( P_e \) goes to infinity in \( N \). It is also true that, at rates \( R < C \), \( P_e \) cannot go to zero as fast as \( \lambda \) goes to infinity. In other words, for rates \( R_{01} < R < C \), one can ensure that \( L \) is seldom larger than 1; but whenever \( L \) is larger than 1, it is likely to be so large that \( \lambda = E(L) \) cannot be kept small as the blocklength is increased.

### III. THE TWOACCESS CASE

To keep the notation simple, we consider only multiaccess channels with two users. (Generalizations are straightforward and can be found in [8].) We denote the input alphabet of user 1 by \( U \), the input alphabet of user 2 by \( V \), and the channel output alphabet by \( Y \). \( P(y | u,v) \) denotes the conditional probability that \( y \) is received at the channel output given that users 1 and 2 transmit \( u \) and \( v \), respectively.

To define the average list size for the twoaccess case, consider a twoaccess block code with blocklength \( N \) and \( M \) messages for each user. Let \( u_m, v_l \) denote the codeword for message \( m \) of user 1, and \( v_l \) the codeword for message \( l \) of user 2. The average list size is then given by

\[
\lambda = \frac{1}{M-1} \sum_{m=1}^{M} \sum_{l=1}^{L} P(u_m, v_l),
\]

where \( P(u_m, v_l) \) is the conditional probability, given that \((m,l)\) is the true message, that a channel output is received that makes \((u_m, v_l)\) at least as likely as message \((m,l)\).

We now make some observations that relate the twoaccess case here to the one-user case of Section II, and thereby shorten the proofs of certain results in this section. First, consider associating to each twoaccess channel a one-user channel with input alphabet \( X = UV \) (the cartesian product of \( U \) and \( V \)), output alphabet \( Y \), and transition probabilities \( P(y | x) = P(y | u,v) \), where \( x = (u,v) \). The only real difference between these two channels is that the inputs to the twoaccess channel must be independently encoded. The important point for our purposes is that one of the two channels is PR iff the other is.

Next, we consider associating to each \((N,M,L)\) code a one-user code that has blocklength \( N \) and \( M \) codewords, namely, the codeword \( x_{m,l} = (u_m, v_l) \) for message \((m,l)\). Note that the \( \lambda \) for a twoaccess code over a twoaccess channel equals the \( \lambda \) for the associated one-user code over the associated one-user channel. Also note that if, for a twoaccess block code, \( Q_1 \) and \( Q_2 \) are the compositions of the codes of users 1 and 2, respectively, then the composition of the associated one-user code is given by the product-form probability distribution \( Q = Q_1 Q_2 \). Now the following result is immediate.

**Theorem 3:** Consider an \((N,M,L)\) code for a pairwise reversible twoaccess channel. Let \( Q_1 \) and \( Q_2 \) denote the code compositions for the codes of users 1 and 2, respectively. Then the average list size satisfies

\[
\lambda \geq g(N) ML \exp - N R_0(Q_1, Q_2),
\]

where

\[
R_0(Q_1, Q_2) = -\frac{1}{N} \ln \left( \sum_{u,v} Q_1(u) Q_2(v) P_n(y | u,v) \right)^2.
\]

To prove this, apply Theorem 1 to the associated one-user code, noting that \( R_0(Q) \), as defined in Section II, equals \( R_0(Q_1, Q_2) \) when \( Q = Q_1 Q_2 \).

Next, we develop a result that gives the critical rate region for \( \lambda \) in the case of PR twoaccess channels. We define, for arbitrary probability distributions \( Q_1 \) on \( U^N \) and \( Q_2 \) on \( V^N \),

\[
R_0(Q_1, Q_2) = -\frac{1}{N} \ln \left( \sum_{u,v} Q_1(u) Q_2(v) P_n(y | u,v) \right)^2.
\]

We define \( R_n \) as the region of all points \((R_1, R_2)\) such that, for some \( N \geq 1 \) and some pair of probability distributions, \( Q_1 \) on \( U^N \) and \( Q_2 \) on \( V^N \), the following are satisfied:

\[
0 \leq R_1 \leq R_0(Q_1, Q_2), \quad 0 \leq R_2 \leq R_0(Q_1, Q_2).
\]

The significance of \( R_n \) is brought out by the following result.

**Theorem 4:** For block coding on pairwise reversible twoaccess channels at rates strictly outside \( R_n \), the average list size \( \lambda \) goes to infinity exponentially in the code blocklength.

**Proof:** The proof uses only definitions:

\[
ML \exp - N R_0(Q_1, Q_2) = \sum_{m=1}^{M} \sum_{l=1}^{L} \left( \sum_{y} P_n(y | u_m, v_l) P_n(y | u_m, v_l) \right)
\]

\[
\geq \frac{1}{M} \sum_{i=1}^{M} \sum_{m=1}^{M} \left( \sum_{y} P_n(y | u_m, v_l) P_n(y | u_m, v_l) \right)
\]

\[
= M \exp - N R_0(Q_1, Q_2).
\]

This proves inequality (18). Inequality (19) follows similarly. Inequalities (20) and (21) now follow from Theorem 3.
and \( Q_2 \) on \( N^\tau \), we have either \( R_1 \geq R_0 (Q_2 | Q_1) + \beta \), or \( R_1 \geq R_0 (Q_2 | Q_1) + \beta \). Thus it is true in particular when \( Q_1 \) and \( Q_2 \) are the compositions of an \((N, M, L)\) code. It follows then, by Theorem 3 and Lemma 3, that for every \((N, M, L)\) code the average list size satisfies \( \lambda \geq g(N) \exp N \beta \), whenever \( M \geq \exp NR_1 \) and \( N \geq \exp NR_2 \) (i.e., whenever the code has rate \( \geq (R_1, R_2) \)).

Theorem 4, unlike Theorem 2, is not a special case of a known general result: it is not known if the statement of Theorem 4 holds for twoaccess channels that are not pairwise reversible.

There is a converse to Theorem 4: For any fixed rate strictly inside \( R_0 \), there exists a code with that rate for which \( c \leq 1 + o(N) \). This result holds for general twoaccess channels, and is proved by random-coding \([9], [10]\). Thus for PR twoaccess channels, \( R_0 \) is the critical region for \( c \). (Whether the same holds in general remains unsettled.)

We have defined \( R_0 \) as the union of an uncountable number of regions. Unfortunately no simpler characterization of \( R_0 \) (such as the single-letter characterization that exists in the case of ordinary channels) has been found. The difficulty here is that for twoaccess channels no analog of Lemma 2 exists. For more on open problems in this area, see [10] and [8].

IV. APPLICATIONS TO SEQUENTIAL DECODING

Consider sequential decoding of a tree code on a one-user channel. Assume that the tree code is infinite in length and that each path in the tree is equally likely to be the true (transmitted) path. Let \( C_n \) denote the expected number of computational steps as the single-letter characterization that exists in the case of twoaccess channels no analog of Lemma 2 exists. For more on computation for sequential decoding, \( [7\), p. 279]). Thus, Lemma 4, together with this achievability result, establishes that \( R_{comp} \geq R_0 \) for PR channels.

It is in fact true that \( R_{comp} = R_0 \) in general. However without the assumption of pairwise reversibility, the inequality \( R_{comp} \geq R_0 \) appears to be considerably harder to prove (see [6] for such a general proof).

We now briefly consider the twoaccess case. An explanation of sequential decoding on twoaccess channels can be found in [1], [10]. For twoaccess sequential decoding, there is an achievable rate region \( R_{comp} \) defined as the closure of the region of all rates at which sequential decoding is possible within bounded average computation per correctly decoded digit. At present, the main unsettled question about twoaccess sequential decoding is whether in general \( R_{comp} = R_0 \). It has been proven [1] that \( R_{comp} \) is at least as large as \( R_0 \). Also, no example is known for which \( R_{comp} \) is larger than \( R_0 \). For PR twoaccess channels, the following theorem settles this question.

**Theorem 5:** For pairwise reversible twoaccess channels

\[
R_{comp} = R_0.
\]

To prove this theorem, one only needs to show that \( R_{comp} \) is not larger than \( R_0 \) for any PR twoaccess channel (because, as previously mentioned, \( R_{comp} \) contains \( R_0 \) in general). This follows immediately once one establishes that Lemma 4, which was stated for ordinary channels, holds also for twoaccess channels. Such a proof, though straightforward, requires a lengthy description of twoaccess sequential decoding, and hence is omitted here. A complete proof can be found in [8].

REFERENCES


Some New Optimum Golomb Rulers

JAMES B. SHEARER

Abstract—By exhaustive computer search, the minimum length Golomb rulers (or \( B_2 \)-sequences or difference triangles) containing 14, 15, and 16 marks are found. They are unique and of length 127, 151, and 177, respectively.

A Golomb ruler \( \{B_1, B_2, \ldots, B_n\} \) is defined as a set of \( m \) integers \( 0 = a_0 < a_1 < \ldots < a_m \), such that the \( (m-1) \) differences \( a_i - a_j \), \( 1 \leq i < j \leq m \) are distinct. Note this condition is equivalent to requiring that the \( \binom{m}{2} + m \) sums \( a_0 + a_j \), \( 1 \leq j \leq m \) be distinct. We say the ruler contains \( m \) marks and is of length \( a_m \). Previous investigators have found the optimum (minimum length) rulers for \( m \leq 13 \) marks \([1], [2], [4], [5], [6]\). In Table 1 we present the unique minimum length rulers for \( m = 14, 15, 16 \) all found by exhaustive computer search. For \( m = 15 \) and 16 the best previously known rulers were of length 153 and

Manuscript received January 3, 1989.

The author is with the Department of Mathematical Sciences, IBM Research Division, T. J. Watson Research Center, P.O. Box 218, Yorktown Heights, NY 10598.

IEEE Log Number 8933108.