An Implementation of Elias Coding for Input-Restricted Channels

ERDAL ARIKAN, MEMBER, IEEE

Abstract—An implementation of Elias coding for input-restricted channels is presented and analyzed. This is a variable-to-fixed length coding method that uses finite-precision arithmetic and can work at rates arbitrarily close to channel capacity as the precision is increased. The method offers a favorable tradeoff between complexity and coding efficiency. For example, in experiments with the [2, 7] runlength constrained channel, a coding efficiency of 0.9977 is observed, which is significantly better than what is achievable by other known methods of comparable complexity.

I. INTRODUCTION

Ever since Shannon [1, p. 36] formulated and studied input-restricted channels, many coding methods have been proposed for such channels; the reference section provides a partial list. We present another method, based on Elias coding, which may be of interest since it can achieve extremely high coding efficiencies using little memory and computation.

The idea of using Elias coding for input-restricted channels is not new, though the earlier codes were presented under the name of arithmetic coding [4], [5], [6]. The primary interest in [4], [5] was in fixed-rate implementations. Here, we consider a variable-to-fixed-length implementation that is fixed-rate only in a certain asymptotic sense. It return for giving up the strict fixed-rate property, a favorable tradeoff is obtained between coding complexity and efficiency, as demonstrated by experimental and analytical results.

The relation between Elias coding and the code here is a special case of the duality between source coding (data compaction) and coding for input-constrained channels (data translation). The decoder for a data-translation code is an encoder for a data-compaction code: it removes the structural redundancy that is present in the constrained channel sequence. This relationship was stated and exploited in [4], [5], and more recently in [16]. For the code here, the decoder is an Elias encoder, more exactly a finite-precision floating-point implementation of Elias coding, similar in some respects to that in [15]. (For Elias coding and its variants, see [14].)

The main results of this correspondence are contained in Section IV. Sections II and III contain definitions, conventions, and some background results. Section V contains complementary remarks on the algorithm.

II. CONVENTIONS AND DEFINITIONS

We consider only input-restricted channels that can be presented by finite state diagrams. An example of such a channel is the [2, 7] runlength constrained channel, presented by the state diagram in Fig. 1. (Runlength constraints arise, e.g., in magnetic recording applications. For details, see, e.g., [13].) Each edge in Fig. 1 is labeled by a 0 or a 1, the input letters for this channel. A 0–1 sequence is admissible as an input to the [2, 7] channel if it can be generated by a walk through the state diagram. It will be noted that runlengths of 0 in admissible sequences are bounded between 2 and 7, and being in state \( i \) implies that the current runlength of 0 is \( i - 1 \).

There may be several reasonable ways of presenting an input-restricted channel by a state diagram. For our purposes any such presentation is acceptable as long as it has the properties of being simple and deterministic. A state diagram is said to be simple if for each pair of (not necessarily distinct) states \( i \) and \( j \), there is at most one edge from state \( i \) to state \( j \). A state diagram is said to be deterministic if, for each state, the labels on edges emerging from that state are distinct.

Note that, if one is given a sequence of edge-labels through a deterministic state diagram and the initial state is known, one can then determine the sequence of states visited by the walk. (This notion was expressed by the terms unifilar in [2] and, in a somewhat weaker form, by right-resolving in [9].)

It is easy to see that if an input-restricted channel can be presented by a finite state diagram, so can it be by a simple, deterministic one. So, the restrictions we have imposed on state diagram presentations do not exclude any channels. We shall, however, exclude from consideration those channels that cannot be presented by irreducible state diagrams. A state diagram is said to be irreducible if there exists a directed path from each state to each other state. Channels that are not irreducible are not of particular interest; they are best studied in terms of their irreducible components. Henceforth, we shall assume that the state diagram under consideration is finite, simple, deterministic, and irreducible.

Let us note that the restriction to simple state diagrams is made only to simplify the notation; the coding method presented here can be applied to nonsimple state diagrams after minor changes. The restriction to deterministic state diagrams is essential for decodability, though that too can be relaxed somewhat (to what is called right-resolving in [9]).

We shall label the states by integers 1 through \( S \), where \( S \) denotes the number of states. We shall let \( t_{i,j}, 1 \leq i, j \leq S \), denote the number of edges from state \( i \) to state \( j \). Thus, \( t_{i,j} \) will be either 0 or 1 since we consider only simple state diagrams. The matrix \( T = (t_{i,j}) \) will be called the state transition matrix. We shall let \( l_{i,j} \) denote the channel symbol labeling the edge from state \( i \) to state \( j \); if there is no such edge, \( l_{i,j} \) will be undefined.

III. MAXENTROPIC PROBABILITIES AND CHANNEL CAPACITY

Let \( \lambda \) be the largest positive eigenvalue of \( T \), the state-transition matrix for some input-restricted channel. Let \( (B_i, 1 \leq i \leq S) \) be an eigenvector belonging to \( \lambda \): \( TB = \lambda B \) (By the Frobenius theorem for irreducible, nonnegative matrices [3, p. 53], \( B \) is unique up to a scaling constant, and one may assume that \( B_i > 0 \) for all \( i \)).

Shannon [1, p. 58] showed that the entropy of the input to an input-restricted channel is maximized by a source that visits the states of the constraint diagram according to the following Markovian transition probabilities:

\[
 p_{i,j} = t_{i,j} B_i \lambda^{-1}/B_j.
\]
These transition probabilities are called maxentropic, and the resulting maximum entropy is calculated to be $\log A$.

Shannon [1, p. 37] also showed that the capacity of an input-restricted channel is given by $C = \log A$. Thus, in order to use this noiseless channel at the maximum possible rate $C$, one must maximize the entropy of the channel input. This suggests that the output of an encoder working at a rate close to channel capacity should, in some sense, approximate the maxentropic Markov chain. The algorithm presented in the next section tries to achieve this as best it can under the limitations of finite-precision arithmetic.

IV. THE ALGORITHM

The algorithm presented here is a variable-to-fixed-length sliding-block code, which in each encoding cycle accepts a variable number $n$ of new data bits into the encoder and sends out one channel symbol. The encoder thus maps a data sequence $x_0, x_1, \ldots, x_n$ to a code sequence $y_0, y_1, \ldots, y_M$. The decoder processes the code sequence $y_0, y_1, \ldots, y_M$ and generates $d_0, d_1, \ldots, d_M$, the original data sequence except for a tail of $d$ bits. Since we shall be appending to the original data sequence a fixed tail of $r$ bits, one can ensure the decodability of all data bits. Since we shall be primarily interested in the asymptotic performance of the algorithm as $L$ goes to infinity, we shall ignore these end-effects.

In order to apply the algorithm to an input-restricted channel, we first fix a state-diagram presentation. Then, we choose a matrix of transition probabilities $(p_{ij})$ on this state-diagram so that $p_{ii} = 0$ whenever $i = 0$, and $\sum_{j=1}^{N} p_{ij} = 1$, all $i$. The algorithm can work with any such set of transition probabilities, but what is intended is to choose the $(p_{ij})$ as close to the maxentropic probabilities as possible within finite precision. It is aimed to have the encoder behave like a Markov chain (in its transitions from one state to another during the encoding process) with the chosen transition probabilities when the encoder input is a symmetric Bernoulli process (independent, equiprobable bits).

A pseudocode for the algorithm is shown next.

```plaintext
procedure encode((F, \rho), (l, \alpha), r, s_0);
begin
begin[initialization]
    s := s_0;  \ y := 0;  \ z := 2^r - 1;  \ w := z - y;
    u := \sum_{i=0}^{K} d_{i} 2^{-i};
end[initialization]

while not end-of-data do
begin[encodingcycle]
determine the least i such that \ F_{s_{i}} - \ F_{s_{i-1}} \geq u;
output the next code letter \ x := l_{i};
\ z := y + |wF_{s_{i-1}}|;
\ y := y + |wF_{s_{i-1}}|;
\ t := t(y, z);
shift t 0's into register \ y;
shift t 1's into register \ z;
shift the next t data bits into register \ w;
\ w := z - y;  \ s := i;
end[encodingcycle]

begin[decodingcycle]
\ s := s_0;  \ y := 0;  \ z := 2^r - 1;  \ w := z - y;
end[decodingcycle]
while not end-of-code do
begin[decodingcycle]
determine the state \ i \ such that \ l_{i} = s;
\ z := y + |wF_{s_{i-1}}|;
\ y := y + |wF_{s_{i-1}}|;
\ t := t(y, z);
output the leftmost t bits of register \ y;
shift t 0's into register \ y;
shift t 1's into register \ z;
\ w := z - y;  \ s := i;
end[decodingcycle]
end;
```

By convention, we take $F_{0} = 0$ for all $i$.

The variables $u, v, z$ and $r$ represent $r$-bit, right-to-left shift-registers. Register $u$ holds a window of $r$ data bits: $u = d_{i-r}, \ldots, d_{i},$ where $K$ is the number of bits that have been processed by the encoder until then, and left the system. The contents of register $u$ are also treated as the integer $u = \sum_{i=0}^{K} d_{i} 2^{-i}$. In the same manner, registers $v$ and $z$ are treated as both bit sequences and integers. Thus, setting $z = 2^r - 1$ is equivalent to loading register $v$ with $r$ 1’s. Likewise, setting $u = \sum_{i=0}^{K} d_{i} 2^{-i}$ loads register $u$ with the first $r$ data bits.

The function $t(y, z)$ gives the length of the common (left) prefix of registers $y$ and $z$ (e.g., if $y = 001001$ and $z = 001110$ (with $r = 6$), the common prefix is 001 and $t(y, z) = 3$).

The shift operation on registers is best explained by an example: If $u = 001010$ ($r = 6$), then executing "shift 111 into register $u"$ results in $u = 011110$.

To explain how the algorithm works, let us indicate the value of a variable at the end of encoding cycle $n$ by the subscript $n$ (e.g., $y_n, s_n, etc.$). Let the subscript 0 indicate initial values. The algorithm works by generating, in effect, a sequence of intervals $I_{n} = \{y_{n}, z_{n}\}$, $u \geq 0$, with the property that $y_{i} \leq u \leq z_{i}$. In the $n$th encoding cycle, the initial interval $I_{0} = \{y_{0}, z_{0}\}$ is divided into subintervals so that there is one subinterval for each state. The subinterval for state $i$ is empty if

$$p_{n}(i) = F_{n+1,i} - F_{n+1,i-1} = 0; \quad \text{otherwise, it equals}$$

$$\left[y_{n+1} + \left\lfloor w_{n+1} \frac{F_{n+1,i} - F_{n+1,i-1}}{u} \right\rfloor, y_{n+1} + \left\lfloor w_{n+1} \frac{F_{n+1,i} - F_{n+1,i-1}}{u} \right\rfloor \right].$$

What is aimed here is to allocate a fraction $p_{n,i}$ of the initial interval to state $i$. These subintervals may overlap at their endpoints, but what matters is that they cover all integers in $I_{n+1}$. (With a more complicated rule, one could guarantee disjoint subintervals and slightly improve the coding efficiency.) The encoder sets $s_n$ equal to the least $i$ such that $s_{n+1,i}$ lies in the subinterval for state $i$. The symbol $x_n = l_{n,s_n}$ is then sent to the channel.

Let us now look at the situation from the decoder’s point of view. Suppose that the decoder has kept up with the encoder and

$$s := s_0;  \ y := 0;  \ z := 2^r - 1;  \ w := z - y.$$
is in possession of \( y_{n-1}, z_{n-1}, \) and \( s_{n-1} \). After observing \( x_n \), the decoder can determine \( s_n \) (since the state diagram is deterministic), and hence, \( y_n, z_n \), and the leftmost

\[ t_n = \left( y_{n-1} + [w_{n-1}F_{s_{n-1},y_{n-1}}], y_{n-1} + [w_{n-1}F_{s_{n-1},y_{n-1}}] \right) \]  

bits of \( u_{n-1} \). This explains why the encoder can drop, as it does, the leftmost \( t_n \) bits of register \( u \), thus making room for the upcoming \( t_n \) data bits. The updating rule for registers \( y \) and \( z \) ensures that the inequality \( y_n \leq u_n \leq z_n \) is satisfied going into the next cycle; so the process can continue indefinitely.

Thus the number of data bits that the decoder is able to decode after observing the first \( n \) code letters is given by \( T_n = t_1 + \cdots + t_n \). The question that arises is whether the code here is asymptotically fixed-rate, i.e., whether \( R_n = T_n/N \) converges as \( n \) goes to infinity to a fixed rate \( R \) for all data sequences. (In such limits, we assume that \( L \), the number of data bits, is infinite.) Unfortunately, this is not so. However, we shall see later in this section that, if each data sequence of a fixed finite length is assumed equally likely, then the set of all infinite-length data sequences for which the previous statement is false has total probability zero.

A. An Experimental Result

We applied the algorithm to the [2, 7] runlength constrained channel presented in Fig. 1. The numbers \( F_{j, k} \) were based on the following transition probabilities: \( p_{1, 1} = 0.34, p_{1, 4} = 0.36, p_{5, 1} = 0.40, p_{6, 1} = 0.46, p_{7, 1} = 0.59 \), which were obtained by rounding off the maxentropic transition probabilities. The register length was \( r = 8 \).

We carried out the experiment 100 times. In each run the input to the encoder was a simulated symmetric Bernoulli sequence. The encoder was run until it produced \( N = 10000 \) code letters, which were then processed by the decoder, and the number \( T_n \) of decoded bits was recorded. Fig. 2 shows the frequency of occurrence of the observed values of \( T_n \).

We observe that the sample mean of the rate \( R_n = T_n/N \) equals 0.516165, which is within 0.23% of the channel capacity \( C = 0.517370 \ldots \) for the [2, 7] channel (see [13] for the capacity). We also observe that the spread of the observed values of \( T_n \) around the sample mean is, relatively speaking, quite small, suggesting some statistical regularity. The analysis that follows helps to explain these observations.

B. Statistical Analysis of the Algorithm

For the statistical analysis, we assume that the data sequence is a symmetric Bernoulli process. We first sketch a proof that \( R_n \) converges almost surely as \( N \) goes to infinity.

The proof is based on the observation that the sequence \( (\sigma_n : n \geq 0) \), where \( \sigma_n = (u_n, s_n, y_n) \), is a Markov chain with time-invariant transition probabilities. This follows from the facts that \( \sigma_n \) is a function of \( \sigma_{n-1} \) and \( u_{n-1} \), and that \( u_{n-1} \) is uniformly distributed (equally likely to take on any integer value) on the interval \( [y_{n-1}, z_{n-1}] \), regardless of the path taken to reach the state \( \sigma_{n-1} \). (These statements can be proved easily by induction.)

Since the random variable \( t_n \) is a function of \( u_{n-1} \) and \( \sigma_n \), i.e.,

\[ t_n = t(\sigma_{n-1}, \sigma_n) \]

we can write

\[ R_n = 1/N \sum_{1 \leq n \leq N} t_n = \sum_{\sigma \leq N} f_n(\sigma, \sigma') t(\sigma, \sigma') \]

where the random variable \( f_n(\sigma, \sigma') \) equals \( 1/N \) times the number of transitions from state \( \sigma \) to state \( \sigma' \) during the first \( N \) transitions in the sequence \( (\sigma_n) \). Since \( (\sigma_n) \) is a Markov chain with finitely many states, the times at which a transition occurs from state \( \sigma \) to state \( \sigma' \) form a renewal process; hence, we have, almost surely as \( N \) goes to infinity (e.g., [17, p. 290]),

\[ f_n(\sigma, \sigma') \xrightarrow{a.s.} \pi_{\sigma, \sigma'} \]

where \( \pi_{\sigma, \sigma'} \) is the reciprocal of the mean recurrence time of state \( \sigma \), and \( r_{\sigma, \sigma'} \) is the transition probability from state \( \sigma \) to state \( \sigma' \).

From (5) and (6), we have, as \( N \) goes to infinity,

\[ R_n \xrightarrow{a.s.} \pi_{\sigma, \sigma'} t(\sigma, \sigma') \]

We have thus shown that the coding rate asymptotically approaches a constant \( R \) for almost all data sequences.

Next, we present an analysis, though inexact, provides insight into why and under what conditions we may expect \( R \) to be close to the channel capacity. We begin by noting the following recursive relation:

\[ w_n = z_n - y_n \]

\[ = \left( \left[ w_{n-1}F_{s_{n-1},y_{n-1}} \right] - \left[ w_{n-1}F_{s_{n-1},y_{n-1}} \right] \right) 2^n + 2^{n-1} - 1. \]

The algorithm aims at having

\[ w_n = w_{n-1}p_{u_{n-1}y_{n-1}} 2^n \]

within the limitations of finite-precision arithmetic. The idea is to have, as a consequence of the preceding equation,

\[ w_n = w_0p_{u_{n-1}y_{n-1}} 2^{N-1} - 1. \]

For \( (p_{u_{n-1}y_{n-1}}) \) approximately maxentropic, this implies

\[ w_n = w_0(B_{\text{c}}/B_{\text{u}}) 2^{N-1} - 1 \]

where \( C \) is the channel capacity. Since \( 1 \leq w_n \leq 2^n - 1 \), it follows that, for large \( N \),

\[ R_n = T_n/N = C. \]
Thus to the extent that the previous approximations are valid for the state sequence \( (s_i) \) corresponding to a data sequence, the coding rate for that data sequence will be close to the channel capacity. The most effective way of ensuring the validity of these approximations for a large fraction of data sequences is to choose \( r \), the register size, suitably large.

Note that in the limit of infinite precision, the above approximations are exact and the code is truly fixed-rate. The algorithm deviates from being fixed-rate as the precision is decreased. The experimental values of \( R_k \), previously reported suggest that even with a modest precision that deviation may be kept at an insignificant level.

**C. The Error Propagation Problem**

Suppose that, instead of the entire code sequence \( x_1, x_2, \ldots \), the decoder is given \( x_{n+1}, x_{n+2}, \ldots \). Can the data sequence still be reconstructed correctly allowing a finite number of initial errors? This situation arises when some of the first \( n \) symbols are garbled by noise, or when one wishes to start decoding in the middle of an encoded sequence. In such cases, one would not like to see a catastrophic propagation of decoding errors.

Unfortunately the codes generated by the algorithm may suffer catastrophic error propagation. We now examine this problem in more detail, mention possible remedies, but propose no specific solutions.

Let \( \sigma \) denote, as before, the state of the encoder at the end of encoding cycle \( n \). Let \( \delta \) denote the state of the decoder at the end of decoding cycle \( n \). We may view \( \delta \) as the decoders estimate of \( \sigma \). Assume that \( x_{n+1}, x_{n+2}, \ldots \) is error-free.

From our discussion of the decoding algorithm, it is clear that the output of the decoder at decoding cycles \( > n \) is completely determined by \( (\delta, x_{n+1}, x_{n+2}, \ldots) \). In other words the effect of \( x_{n+1}, \ldots, x_n \) on the future behavior of the decoder is completely summarized by \( \delta \). Thus for each possible value of \( \delta \), there are (finitely many) there is a hypothetical data sequence. One of these sequences, the one for which \( \delta = \sigma \), is the true data sequence. In order to stop error propagation, the decoder must be able to select one of the hypothetical sequences that shares a common suffix with the true sequence. (Two sequences \( \alpha, \beta, \ldots \) and \( \beta, \beta', \ldots \) are said to share a common suffix if there exist \( k, k' \) such that \( \alpha_{i-k} = \beta_{i-k} \) for all \( i \geq 1 \).

A straightforward, but not particularly elegant, solution to this problem is to build some structure into the data sequence (e.g., by inserting parity-check bits) so as to facilitate the elimination of false data sequences. This approach requires no major changes in the algorithm itself. Another approach is to try to modify the algorithm so that both the encoder and the decoder update their states using a next-state function, with finite look-ahead and finite look-back

\[
\sigma = f(x_{n-k}, \ldots, x_{n-k+1}),
\]

where \( k, k' \) are fixed integers. Clearly, an algorithm with such a next-state function is noncatastrophic, with a maximum synchronization delay of \( k + k' + 1 \) symbols. The algorithm here has a next-state function of the form \( \sigma = f(\sigma, x_k) \), which has no look-ahead, but possibly infinite look-back. We have found no clean way of modifying the algorithm so as to eliminate the potentially infinite memory from its next-state function.

We should note that there are algorithms (e.g., [9], [10]), for which the next-state function is in the form (13), with one important difference: for these algorithms, each argument of the next-state function (the terms \( x_{n-k}, x_{n-k+1}, \ldots, x_{n-k+1} \)) is a block of \( q \) symbols (for some fixed integer \( q \)) from the channel alphabet. Unfortunately such a next-state function does not provide protection against misframing (i.e., incorrectly deciding the block boundaries); hence, these codes, too, are subject to catastrophic error propagation.

**V. Conclusion**

Nonfixed-rate codes require buffering if one wishes to use the channel synchronously, and one has to worry about the consequent buffer overflow problems. For this reason there is a bias towards fixed-rate codes in practice. Such a bias is hard to justify in systems where the source sequence is highly redundant and one uses a variable-length source code (such as a Huffman code) to remove part of that redundancy, since buffering is required then whether the channel coding is fixed-rate or not.

Fixed-rate codes do not present a buffer-overflow problem, but they may require considerably more implementation complexity. Consider, for example, the fixed-rate codes proposed in [7], [8], and the ones pioneered by Adler, Haustler, and Coppersmith [9], [10], [11]. These codes are constrained to work at rational rates; and, to construct a code with rate \( p/q \), one needs to work with a \( q \)-step state-diagram for the given channel. Since the \( q \)-step diagram contains on the order of \( 2^q \) states for a channel with capacity \( C \), the implementation complexity of these codes is exponential in \( q \). The constructions in [9], [10], [11] have an even higher complexity because they apply state-splitting (an elegant procedure invented by Marcus [12]) to the \( q \)-step diagram, resulting in a further increase in the total number of states. The fact that the complexity is exponential in \( q \) places a practical limit on how close one can get to the channel capacity with rational rates of the form \( p/q \).

In contrast, the algorithm here never has to deal with extended channels no matter how close the desired coding rate is to channel capacity. In order to achieve higher rates, one need only run the same algorithm using a higher precision.

**References**


