Non prefix-free codes for constrained sequences

Marco Dalai & Riccardo Leonardi
Department of Electronics for Automation
University of Brescia, Italy
Email: {marco.dalai, riccardo.leonardi}@ing.unibs.it

Abstract—In this paper we consider the use of variable length non prefix-free codes for coding constrained sequences of symbols. We suppose to have a Markov source where some state transitions are impossible, i.e. the stochastic matrix associated with the Markov chain has some null entries. We show that classic Kraft inequality is not a necessary condition, in general, for unique decodability under the above hypothesis and we propose a relaxed necessary inequality condition. This allows, in some cases, the use of non prefix-free codes that can give very good performance, both in terms of compression and computational efficiency. Some considerations are made on the relation between the proposed approach and other existing coding paradigms.

I. INTRODUCTION

Variable length codes are usually considered to have to satisfy the Kraft inequality (11), as it was proved that this is a necessary condition for unique decodability in [2]. Unique decodability is always defined as a characteristic of the set of code words only, and no reference to the type of source is considered. Thus, imposing unique decodability we are requiring any sequence of symbols being distinguishable. This fact is clearly perfectly acceptable if the source can produce any sequence of symbols with non-null probability as, for example, in the memoryless source case. But what happens if the source is not memoryless and, more precisely, not all sequences are allowed? Consider for example a source with three symbols A, B and C, and suppose that symbol A can never be followed by B. This fact is a characteristic of the source that we can consider known for the encoding problem, as we actually do in the classic Shannon paradigm where no bits are assigned to null-probability events. Thus, the decoder is usually supposed to know that an event is not possible, at least from the fact that that no code word is assigned to that event. Thus, suppose we use the codewords ‘0’, ‘1’ and ‘01’ for our source symbols A, B and C respectively. It is easy to see that any sequence of symbols that can be generated by the source is uniquely specified by concatenating the codewords of every single symbol. This is because with this code one may only confuse sequences of symbols with sequences that our source cannot generate. The objective of this paper is to propose the notion of unique decodability of a set of codewords relatively to a specific information source. We show simple examples of Markov sources that can be efficiently encoded by non-prefix free codes. Our examples also show that there are sources for which a coding technique exists such that the expected number of bits of the code for the first n symbols of the source is strictly smaller than the entropy of those first n symbols (for every n). This fact is often erroneously considered impossible, and this error arises from considering the Kraft inequality a necessary condition for any type of sources.

II. A CURIOUS MARKOV CHAIN EXAMPLE

Suppose, so as to analyze more thoroughly the example of the introduction, we have a source generating symbols $X_1, X_2, X_3, \ldots$ extracted from the set $\mathcal{X} = \{A, B, C\}$ following the Markov chain graphically shown in figure 1. In formulae, if we call $S_i$ the probability distribution row vector on $\mathcal{X}$ at step $i$, we have $S_{i+1} = S_i P$, where $P$ is the transition probability matrix

$$P = \begin{bmatrix} 1/2 & 0 & 1/2 \\ 1/4 & 1/2 & 1/4 \\ 1/4 & 1/2 & 1/4 \end{bmatrix}$$

(1)

If we suppose the initial state has uniform probability $S_1 = [1/3, 1/3, 1/3]$, it is easy to verify that the process is stationary, i.e. $S_i = S_1$ for every $i$. Thus, the entropy $H(X_1, X_2, \ldots, X_k)$ of the first $k$ symbols can be easily computed. We have

$$H(X_1, X_2, \ldots, X_k) = H(X_1) + H(X_2 | X_1) + \cdots + H(X_k | X_{k-1}) =$$

$$H(X_1) + H(X_2 | X_1)(k - 1) = \log(3) + \frac{4}{3}(k - 1)$$

Let us consider now the codeword assignment $A \rightarrow 0, B \rightarrow 1, C \rightarrow 01$. This code is clearly not prefix-free but, as explained in the introduction, when used for this source no ambiguity can arise. If $l(X)$ is the length of the code associated to $X$, we can compute the expected number of bits in coding the

Fig. 1. Graph, with transition probabilities, for a Markov Chain.
first $k$ symbols as
\[
E[l(X_1X_2X_3 \cdots X_k)] = E \left[ \sum_{i=1}^{k} l(X_i) \right] = \sum_{i=1}^{k} E[l(X_i)] = k \left( \frac{1}{3} + \frac{1}{3} + \frac{2}{3} \right) = \frac{4}{3} k
\]

It is easy to verify that this value is strictly smaller than the entropy $H(X_1, X_2, \ldots, X_k)$ above computed. What happens with our coding procedure? And what happens when the number of symbols goes to infinity? Looking carefully at our example, we note that our coding strategy uses an expected number of symbols goes to infinity. Looking carefully at our unique decodability of a set of much more intriguing.

For ergodic sources). But this fact is somehow interesting; our code assigns to the first symbol a number of bits smaller than its entropy, using the memory properties of the source, without affecting unique decodability. Thus, if we consider the case when only a finite number of symbols are given the problem of finding the optimal coding strategy arises. Furthermore, we should consider that in the more general case, when higher order constraint are eventually present, the problem becomes much more intriguing.

III. KRAFT INEQUALITY FOR CONSTRAINED SEQUENCES

McMillan showed in [2] that a necessary condition for the unique decodability of a set of $n$ codewords is that their lengths $l_1, l_2, \ldots, l_n$ satisfy the Kraft inequality
\[
\sum_{i=1}^{n} 2^{-l_i} \leq 1
\]

Karush ([3]) gave a simple proof of this fact by considering that for every $k > 0$ the following inequality must be satisfied
\[
\left( \sum_{i} 2^{-l_i} \right)^k \leq kl_{\text{max}}
\]

The term on the left hand side of (3) can be written as the sum of weights of codes of possible sequences of $k$ symbols. For example, a sequence starting with $x_1, x_3, x_2, \ldots$ gives a term $2^{-l_1}2^{-l_3}2^{-l_2} \ldots$ in the expansion of the left hand side of (3). In order to have only one sequence assigned to every code the above inequality is necessary. But if we only want to distinguish between the possible sequences generated by a constrained source, we may rewrite the condition in a less stringent form. Let us consider once more as an example the source of fig. 1 with $l_1, l_2$ and $l_3$ lengths assigned respectively to $A, B$ and $C$. Thus, terms on the expansion of left hand side of (3) that contains $\ldots 2^{-l_1}2^{-l_2} \ldots$ should not be considered as $B$ cannot follow $A$ in a source sequence. Let us consider the matrix
\[
Q = \begin{bmatrix}
2^{-l_1} & 0 & 2^{-l_1} \\
2^{-l_2} & 2^{-l_2} & 2^{-l_2} \\
2^{-l_3} & 2^{-l_3} & 2^{-l_3}
\end{bmatrix}
\]

it is possible to verify that the really necessary correspondent of eq. 3 for our source should be written, for $k > 0$, as
\[
\left[ \begin{array}{ccc}
1 & 1 & 1
\end{array} \right] Q^{k-1} \begin{bmatrix}
2^{-l_1} \\
2^{-l_2} \\
2^{-l_3}
\end{bmatrix} \leq kl_{\text{max}}
\]

It is possible to show that a necessary condition for this inequality to be satisfied for every $k$ is that the matrix $Q$ has spectral radius\(^1\) at most equal to 1. We state and prove this fact in the general case.

Theorem 1: Let $P$ be an irreducible $n \times n$ stochastic matrix and $1 = [l_1, l_2, \ldots, l_n]$ a vector of $n$ integers. Let $Q$ be the $n \times n$ matrix such that
\[
Q_{ij} = \begin{cases} 
0 & \text{if } P_{ij} = 0 \\
2^{-l_i} & \text{if } P_{ij} > 0
\end{cases}
\]

Then, a necessary condition for the codeword lengths $l_1, l_2, \ldots, l_n$ to be lengths of a uniquely decodable code for a Markov source with transition probability matrix $P$ is that $\rho(Q) \leq 1$, where $\rho(Q)$ is the spectral radius of $Q$.

Proof: We follow Karush's proof of McMillan theorem. Suppose without loss of generality that the set of our source symbols is $\mathcal{X} = \{1, 2, \ldots, n\}$, and call $\mathcal{X}^{(k)}$ the set of all sequences of $k$ symbols that can be produced by the source. Let us set $L = 2^{-1} = [2^{-l_1}, 2^{-l_2}, \ldots, 2^{-l_n}]$ and define, for $k > 0$,
\[
V_k^T = Q^{k-1}L^T.
\]

Then it is easy to see by induction that the $i$-th component of $V_k$ is written as
\[
V_k^i = \sum_{x_1, x_2, \ldots, x_k} 2^{-l_{x_1} - l_{x_2} \cdots - l_{x_k}}
\]

where the sum runs over all elements $(x_1, x_2, \ldots, x_k)$ of $\mathcal{X}^{(k)}$ with $x_1 = i$. So, if we call $1_n$ the row vector composed of $n$ 1’s, we have
\[
1_n Q^{k-1}L^T = \sum_{x_1, x_2, \ldots, x_k} 2^{-l_{x_1} - l_{x_2} \cdots - l_{x_k}}
\]

where the sum now runs over all elements of $\mathcal{X}^{(k)}$. Thus, reindexing the sum with respect to the total length $l = l_{x_1} + l_{x_2} + \cdots + l_{x_k}$ and calling $c_l$ the number of sequences to which correspond a code of length $l$, we have
\[
1_n Q^{k-1}L^T = \sum_{l=1}^{k \text{max}} c_l 2^{-l}
\]

where $l_{\text{min}}$ and $l_{\text{max}}$ are respectively the maximum and the minimum of the values $l_i, i = 1, 2, \ldots, n$. Since the code

\(^1\)The spectral radius of a matrix is defined as the greatest modulus of its eigenvalues.
is uniquely decodable, all $c_l$ sequences of length $l$ must be different and so they are at most $2^l$. This implies that, for every $k > 0$, we must have

$$1_nQ^{k-1}L^T \leq \sum_{l=k_{\text{min}}}^{k_{\text{max}}} 2^l 2^{-l} = k(l_{\text{max}} - l_{\text{min}} + 1) \quad (11)$$

Now, note that the irreducible matrix $Q$ is also nonnegative. Thus, for the Perron-Frobenius theorem (see [4] for details), its spectral radius $\rho(Q)$ is also an eigenvalue with algebraic multiplicity 1 and with positive associated eigenvector. As the vectors $1_n$ and $L$ are both positive, this implies that the term on the left hand side of eq. (11) asymptotically grows like $\rho(Q)^{k-1}$. On the contrary, the right hand side term only grows linearly with $k$; so, taking the limit as $k \to \infty$ in eq. (11) we conclude that $\rho(Q) \leq 1$.

We note that if the $P$ matrix has all strictly positive entries, the matrix $Q$ reduces to have all equal columns, and its spectral radius is exactly $\sum 2^{-l}$. Thus, for non-constrained sequences, we obtain the classic Kraft inequality. Furthermore, as the spectral radius of a nonnegative positive matrix increases if any of the elements increases, we note that the situation $\rho(Q) = 1$ is a strong condition on $P$ and $I$. In the sense that if for a given matrix $P$ there is a decodable code with codeword lengths $l_i, i = 1, \ldots, n$ such that $\rho(Q) = 1$, then there is no decodable code with lengths $l'_i$ if $l'_i < l_i$ for some $i$. Also, it is not possible to remove constraints from the Markov chain while keeping unique decodability property.

The most important remark, however, concerns the non-sufficiency of the stated condition. In fact, while the classic Kraft inequality is a necessary and sufficient condition for the existence of a uniquely decodable code for an unconstrained sequence, the found inequality $\rho(Q) \leq 1$ is unfortunately only necessary, and not sufficient. We discuss this point in the next section, where we propose an extension of the Sardinas Patterson test for testing the unique decodability of a code for a constrained sequence.

IV. NON SUFFICIENCY AND SARIDNAS PATTERSON TEST

In the preceding sections we have shown that the classic Kraft inequality is not, in general, a necessary condition for the unique decodability of a constrained sequence, and we have found a necessary condition under this hypothesis. Unfortunately, the found condition is not sufficient and trivial examples show this fact. We note that the only parameter determining the matrix $Q$ are the length vector $I$ and the graph associated to the Markov chain, i.e. the state pairs with positive transition probability. Thus, we only consider the transition graphs of the sources without taking into account the value of the transition probabilities. Consider for example a source with three symbols $A, B$ and $C$ with transition graph as shown in fig. 2(a). It is easy to see that if $I = [1, 1, 1]$ then $\rho(Q) = 1$; anyway, it is clearly impossible to decode the sequences of the source if we assign only one bit to every symbol. In general, we may consider that it is not possible to have a decodable code with more than $2^l$ codewords of length $l$, because otherwise even the initial state cannot be recovered. Anyway, still imposing this additional condition does not suffice. Take for example a code with $I = [1, 1, 2]$ for a source with transition graph as shown in fig. 2(b) we have $\rho(Q) < 1$, only two codewords of 1 bit and one codeword of 2 bits, but still a decodable code with those lengths does not exist ($A \to 0$ imposes $B \to 1$, and consequently $C \to 11$, but $BCB$ and $CC$ have the same code).

The above examples show that the question of finding a sufficient condition for the unique decodability of codes for constrained sequences appears to be more complicated than with unconstrained sequences. A positive fact is that it is possible to extend the Sardinas Patterson (SP) test ([5]) to the case of our interest. Given a set of codewords, the SP test allows to establish in a finite number of steps if the code is uniquely decodable for unconstrained sequences. Here we modify the classic algorithm for the case of constrained ones. The generalization is straightforward so that we do not give here a formal proof, as it would merely be a rewriting of that for the classic SP test, for which we refer the reader to [6, th. 2.2.1].

Suppose our source symbol set is $X = \{1, 2, \ldots, n\}$ and let us call $W = \{W_i\}_{i=1,\ldots,n}$ the set of associated codewords. For $i = 1, 2, \ldots, n$ we call $F_i = \{W_j | P_{ij} > 0\}$ the subset of $W$ containing all codewords that can follow $W_i$ in a source sequence. We construct a sequence of sets $S_1, S_2, \ldots$ in the following way. To form $S_1$ we consider all pairs of codewords of $W$; if a codeword $W_i$ is a prefix of another codeword $W_j$, i.e. $W_j = W_iA$ we put the suffix $A$ into $S_1$. In order to consider only the possible sequences, we have to remember the codewords that have generated every suffix; thus, let us say that we mark the obtained suffix $A$ with two labels, thus we indicate it with $iA_j$. We do this for every $i$ and $j$. Then, for $n > 1$, $S_n$ is constructed by comparing elements of $S_{n-1}$ and elements of $W$; for a generic element $iB_m$ of $S_{n-1}$ we consider the subset $F_i$ of $W$:

a) If a codeword $W_k \in F_i$ is equal to $iB_m$ the algorithm stops and the code is not decodable,

b) if $iB_m$ is prefix of a codeword $W_r = iB_mC$ we put the

\[ \begin{align*}
2 & \text{Note that in general the spectral radius is not an eigenvalue as it is defined as the maximum of } |\lambda| \text{ over all eigenvalues } \lambda.
\end{align*} \]
respectively, and the initial state is uniformly distributed. For this source the entropy of the first $k$ symbols is $(3k + 1)/2$ while our code uses on average $3k/2$ bits. Thus we cannot say that, even for stationary ergodic processes, the minimum average length of the code for the first $k$ symbols is greater than or equal to their entropy. The only thing we can say is about the entropy rate.

Given a Markov source $X_1, X_2, X_3, \ldots$ with transition matrix $P$, let $\mu = [\mu_1, \mu_2, \ldots, \mu_n]$ be the stationary distribution, and $\mathcal{H}$ the entropy rate. Using the asymptotic equipartition property for ergodic sources (Shannon-McMillan theorem, [7]), we deduce that for every uniquely decodable code we must use at least $\mathcal{H}$ bits per symbol on average and thus $1 \cdot \mu^T \geq \mathcal{H}$. Note that this does not imply that $E[l(X_1)] \geq \mathcal{H}(X_1)$, nor, in general, that for some fixed $n$ we have $E[l(X_1, X_2, \ldots, X_k)] \geq H(X_1, X_2, \ldots, X_k)$ (see [8, Th. 5.4.2]), and our examples precisely show that in fact this is not true. The point is that for sources with memory we can use codes that do not respect the classic Kraft inequality and thus the inequality $E[l(X)] \geq H(X)$ cannot be proved. Thus, we should be careful in formulating the converse theorem for variable length codes.

Anyway, the examples shown in this and in preceding sections leave many open questions. We have shown examples of transition graphs with associated codeword lengths such that the obtained code is uniquely decodable. For every one of these graphs we have shown that there is a transition probability matrix $P$ such that the entropy rate of the source exactly equals the average length per symbol of our code. We should ask if this is only a coincidence or if it is the rule. Furthermore, we may ask what happens in terms of efficiency with our code for a generic matrix $P$ on a given graph; is it possible to find an optimal codeword assignment as we do with Huffman codes in the classic framework? Again, what happens if we consider blocks of more than one symbols? We clearly obtain a different transition graph and the efficiency cannot be lower; but is there a gain in some cases or not?

V. ENTROPY RATE AND AVERAGE LENGTHS

In the second section we have seen an example of Markov chain that is efficiently encoded with a non-prefix-free code. Here we note that the same thing happens with the sources of fig. 3 with the indicated codewords if the transition probability matrix associated are

$$P = \begin{bmatrix}
1/2 & 0 & 1/2 & 0 \\
0 & 1/2 & 0 & 1/2 \\
1/4 & 1/4 & 1/4 & 1/4 \\
1/4 & 1/4 & 1/4 & 1/4
\end{bmatrix}$$

and

$$P = \begin{bmatrix}
1/2 & 0 & 1/4 & 1/4 \\
0 & 1/2 & 1/4 & 1/4 \\
0 & 1/2 & 1/4 & 1/4 \\
1/2 & 0 & 1/4 & 1/4
\end{bmatrix}$$

VI. SOME CONSIDERATIONS

It is interesting to consider the proposed coding approach from the point of view of the encoding complexity. Consider for example the stationary Markov chain with transition matrix of eq. (12) and uniform initial distribution. Note that it is possible to encode the first $k$ symbols of the source using exactly as many bits as the entropy of those symbols using Huffman codes. Two bits are used for the first symbol, which correspond to its entropy. Then, at every step we use a different Huffman code, depending on the preceding step, and use on average $H(X_{k+1}|X_k) = \mathcal{H} = 3/2$ bits. Note that this technique actually fits with the conditional entropy idea in the sense that it really encodes each symbol given the preceding one. This implies that the encoder must trace the state of the source and choose the code for the new symbol. On the

3Note that in this paper we have considered only stationary processes; for nonstationary processes there may be still more surprising results.
contrary, the non prefix-free codeword assignment indicated in fig. 6 allows a very simple encoding phase, as there is a fixed mapping from symbols to code bits, with the same (slightly better) compression performance. The point is that we are making a different use of the decoder knowledge about possible transitions. Note that, even for the Huffman code, we are supposing that the decoder exactly knows what transitions are possible and what are not. The difference is that with the non prefix-free code we are making the decoder more active. This relates the presented idea to other developed coding paradigms. We should note in fact, that in practice the proposed approach was already used in other contexts. One of the oldest examples may be that of modulo-PCM codes ([9]) for numerical sequences; here only the modulo-4 value of every sample is encoded, leaving to the decoder the task of understanding the original value using its knowledge on the memory of the source. In that case the used code is even a singular code 4 but under certain hypothesis this does not affect the decodability. Similar ideas are then used in the recently reemerged theme of distributed source coding (see for example [10] and references therein). Let us consider for a moment the problem of noiseless separated coding of dependent sequences. The well known Slepian-Wolf theorem ([11]) says that two correlated memoryless sources, X and Y, can be separately lossless coded at rates R(X) and R(Y) respectively when jointly decoded, if \( R(X) \geq H(X|Y) \), \( R(Y) \geq H(Y|X) \) and \( R(X) + R(Y) \geq H(H, Y) \). Cover extended the result to the case of general ergodic sources in [12]. Roughly speaking, the used encoding process at every encoder consists on considering large blocks of symbols; the set of all such blocks is split into disjoint bins and only the index of the bin that contains the extracted block is encoded. At the decoder the original block for both sequences X and Y is recovered by extracting from the pair of specified bins the only pair of jointly typical blocks. It is interesting to note that this encoding technique actually uses singular codes in order to achieve compression, leaving to the decoder the task of disambiguating, based on the joint statistic of the two sources.

The same idea is now being used, in order to shift the complexity from the encoder to the decoder, in what may be called “source coding based on distributed source coding principles”. Special attention in this field is being payed to the case of video coding (see for example [13], [14]). In this context the memory of the video source is not exploited in the encoding phase but in the decoding one. Again, roughly speaking, in the encoding phase no motion compensation and prediction is applied and singular codes are used for the data compression task. In the decoding phase, on the contrary, the memory of the source is exploited in order to remove ambiguity by using motion compensation. It is interesting to see that practical architectural specification for this video coding techniques have been presented only in recent years, even if the idea of such an approach to video coding was already patented by Witsenhausen and Wyner in late ’70s ([15]). Moreover, it is also interesting to note that there is not much difference in this approach with respect to the idea behind the modulo-PCM coding above mentioned.

As a final comment on the general problem of finding variable length non prefix-free codes for a given constrained sequence, we note that there are many connections with the area of coding for constrained channels (see for example [16]). The relation between the transition graphs of our sources and the possible codeword assignments may find interesting counterparts (and maybe answers) in that field, where graph theory has already been successfully applied.

References

[1] L.G. Kraft, “A device for quantizing, grouping and coding amplitude modulated pulses,” M.S. thesis, Dept. of Electrical Engg., MIT, Cambridge, Mass., 1949.
[2] B. McMillan, “Two inequalities implied by unique decipherability,” IEEE Trans. Inform. Theory, vol. IT-2, pp. 115–116, 1956.
[3] J. Karush, “A simple proof of an inequality of McMillan,”IRE Trans. Inform. Theory, vol. IT-7, pp. 118, 1961.
[4] H. Minc,Nonnegative Matrices, Wiley, 1988.
[5] A.A. Sardinas and G.W. Patterson, “A necessary and sufficient condition for the unique decomposition of coded messages,” in IRE Convention Record, Part 8, 1953, pp. 104–108.
[6] R.B. Ash,Information Theory, Interscience, New York, 1965.
[7] B. McMillan, “The basic theorems of information theory,”Ann. Math. Stat., vol. 24, pp. 196–219, 1953.
[8] T.M. Cover and J.A. Thomas, Elements of Information Theory, John Wiley, New York, 1990.
[9] T. Ericson and V. Ramamoorthy, “Modulo-PCM: A new source coding scheme,” in Proc. IEEE Int. Conf. Acoustics, Speech, and Signal Processing, Washington, 1979, pp. 419–422.
[10] S.S Pradhan, J. Kusuma, and K. Ramchandran, “Distributed compression in a dense microsensor network.”IEEE Signal Processing Magazine, vol. 19, no. 2, pp. 51–60, March 2002.
[11] D. Slepian and J.K. Wolf, “Noiseless coding of correlated information sources,”IEEE Trans. Inform. Theory, vol. IT-19, pp. 471–480, 1973.
[12] T.M. Cover, “A proof of the data compression theorem of Slepian and Wolf for ergodic sources,”IEEE Trans. Inform. Theory, vol. IT-22, pp. 226–228, 1975.
[13] R Puri and K. Ramchandran, “PRISM: A new robust video coding architecture based on distributed compression principles,” in Proc. Of 40thAllerton Conference on Communication, Control, and Computing, Allerton, IL, 2002.
[14] B. Girod, A. Aaron, S. Rane, and D. Rebollo-Monedero, “Distributed video coding.” inProc. IEEE, 2005, vol. 93, pp. 71–83.
[15] Bell Telephone Laboratories Incorporated, Interframe coder for video signals, US Patent, us 4191970.
[16] D. Lind and B. Marcus, An introduction to Symbolic Dynamics and Coding, Cambridge University Press., 1996.

4In our examples here we have considered only non singular codes with singular extension. The non singularity of the code is required in our setting where we want to be able to decode a sequence composed of one single symbol.