Combinatorial Entropy Encoding

Abu Bakar Siddique* and Muhammad Umar Farooq†
*Department of Electrical Engineering, RCET
†University of Engineering and Technology Lahore, Pakistan
*abubakar@uet.edu.pk, †mufarooq40@gmail.com

Abstract—This paper proposes a novel entropy encoding technique for lossless data compression. Representing a message string by its lexicographic index in the permutations of its symbols results in a compressed version matching Shannon entropy of the message. Commercial data compression standards make use of Huffman or arithmetic coding at some stage of the compression process. In the proposed method, like arithmetic coding entire string is mapped to an integer but is not based on fractional numbers. Unlike both arithmetic and Huffman coding no prior entropy model of the source is required. Simple intuitive algorithm based on multinomial coefficients is developed for entropy encoding that adaptively uses low number of bits for more frequent symbols. Correctness of the algorithm is demonstrated by an example.

Index Terms—Data Compression, Shannon Information, Huffman Coding, Entropy Coding

I. INTRODUCTION

Efficient storage and communication of ever growing digital content has kept researchers busy designing new techniques for compressing this information efficiently. The ubiquitous presence of multimedia enabled communication devices produce enormous amount of data to be stored and communicated efficiently. Research in bio-informatics has introduced whole new dimension where large amount of DNA information has to be processed. The handling, storage and transmission of these data is already beyond current available resources.

The science of data compression originated with Shannon’s famous paper on information theory [1] where he introduced entropy as measure of the information. Considering the source generating discrete set of symbols each of which is independent and identically distributed random variable, he showed that it is not possible to compress the source coding rate (average bits per symbol) below the Shannon entropy of the source and be able to reconstruct the original message without the loss of information. To define entropy suppose that a message is made up of $t$ alphabets in set $A = \alpha_1, \alpha_2, \cdots, \alpha_t$. If the alphabet frequencies are $f_1, f_2, \cdots, f_t$ respectively with message length $n = f_1 + f_2 + \cdots + f_t$ then Shannon entropy of the message is

$$H = \sum_{i=1}^{t} p_i \log_2 1/p_i$$

$$= - \sum_{i=1}^{t} p_i \log_2 p_i$$

where $p_i = f_i/n$

Shannon, along with Fano, invented a variable length prefix coding scheme to compress data by assigning shorter codes to more frequent symbols and longer codes to rarely occurring symbols. A slightly improved version was presented by Huffman [2] that constructed the code assignment tree from leaves to the root, in contrast to the Shannon-Fano coding tree that built from root to the leaves. Huffman encoding is sometimes used directly to compress the data while more often it is used as final step to compress symbols after other compression algorithms have taken place. Tools like PKZIP, JPEG, MP3, BZIP2 make use of Huffman coding. For efficient compression, in the original Huffman encoding, it is required that the character probabilities be known at the start of the compression process. This can come either from an accurate estimate of the information source or from statistical pre-processing of the data before putting it to compression algorithm. This encoding approaches the Shannon limit when the data size, $n$, is large and the character probabilities are powers of $1/2$. It is least efficient when the data consists of binary symbols since each Huffman symbol is integer number of bits in size. Such is the problem with other prefix codes such as Golomb, Elias and unary coding as only rarely symbol probabilities obey this condition in practice.

To solve the problem of inefficient Huffman encoding due to integer bits another statistical based data compression scheme known as arithmetic encoding [3] was introduced. Though theoretically promising, its use remained initially limited because of the patent issues. It encodes all the data into one fractional number, represented by bits no more than the Shannon limit. It’s beauty is that it works even for binary alphabet, assigning fractional bits to symbol. One drawback is that the complete message is processed with no inter-alphabet boundaries. Since digital computers are more comfortable working with integers, the fractional ranges have to be frequently converted to integer ranges in practice. Some of these limitations were solved by range coding [4]. However these are still costly because of multiplication operations.

The author was unable to find a statistical encoding scheme that mentions or uses combinatorics to compress the data. Previously the source statistics are defined in terms of the symbol probabilities, the fractional numbers. Our point of view is to consider a message as one permutation of its constituent symbols. Given the symbols and their frequencies in the message, we can represent the input data with a small integer denoting the lexicographic position of the message in list of permutations of its symbols. This index takes far fewer bits than the original message and achieves perfect compression.
Contribution of this paper is also to develop an algorithm that calculates the dictionary index of a message as permutation of its constituent symbols with given frequencies for message encoding and vice versa for decoding. The index calculated this way remains below the Shannon entropy of the message.

The paper presents a data compression technique that to the best knowledge of the author has not been presented before. The message compression is achieved by combinadics, a mixed radix numbering system. The algorithm treats the input message as one permutation of its constituent symbols. Like both Huffman encoding and Arithmetic encoding an alphabet frequency list is needed for decompression of the message. The compression however does not need pre-processing or statistical modeling of the information source. Rather the frequency of each letter encountered at the time of compression is incremented and the compression process continues at the mean time. Compression has linear time complexity O(n) while decompression is O(t · n).

In this paper n represents the message length, t represents the alphabet size. The set of alphabets \( A = (\alpha_1, \alpha_2, \ldots, \alpha_t) \) is replaced with set \( (0, 1, 2, \ldots, t - 1) \) to use with message encoding examples. Each occurrence of an alphabet is termed as a message symbol. There are \( n \) symbols in \( n \) length message.

II. COMPRESSION

The data compression is treated as combinatorics problem in this paper. When alphabet frequencies in the message are not known then for a message length \( n \) and alphabet size \( t \) the number of all possible messages is \( n^t \). For example if message length is six \( (n = 6) \) and three alphabets \( (t = 3) \) are used from set \( A = (0, 1, 2) \), the number of possible messages would be \( 3^6 = 243 \). The binary bits required to represent the message can be calculated as \( \log_2(3^6) = 9.5098 \). With 6 symbols long message, the average information per symbol is 9.5098/6 = 1.5850 bits/symbol. The message can not be decodeably represented with fewer than 10 bits if no other statistics information is available.

If the probabilities of the alphabets are known in advance then the number of bits required to span all possible messages would be much lower as given by Shannon source coding limit. If the alphabets \( (0, 1, 2) \) appear in the message with probabilities 3/6, 1/6, 2/6 respectively, the optimum symbol size by Shannon source coding theorem in Equation[1]

\[
H = - \left( \frac{3}{6} \log_2 \left( \frac{3}{6} \right) + \frac{1}{6} \log_2 \left( \frac{1}{6} \right) + \frac{2}{6} \log_2 \left( \frac{2}{6} \right) \right) \\
= 1.4591 \text{Bits/Symbol}
\]

(2)

Reducing the average information per symbol to the Shannon limit is the goal of every compression method.

Compression ratio is a measure of efficiency for a compression method. It is the ratio

\[
\text{Compression Ratio} = \frac{\text{Uncompressed Size}}{\text{Compressed Size}}
\]

(3)

A closely related measure quantifying the percentage amount of space saved by the compression method is

\[
\text{Space Saving (\%age)} = \left( 1 - \frac{\text{Compressed Size}}{\text{Uncompressed Size}} \right) \times 100
\]

(4)

The compression ratio in our case is 1.5850/1.4591 = 1.0863 percent or 7.94% reduction in the amount of space needed to store the message.

This paper treats the compression as a combinatorial problem. We evaluate the total permutations of the message given the alphabets used and their respective occurrence frequencies in the message. The same statistical information is used by Shannon, Huffman and arithmetic encoding as alphabet probability of occurrence in the message. Instead of working with alphabet probabilities we work with the alphabet frequencies. Taking the previous example further, calculate the number of permutations of 6-symbol message formed by three alphabets, appearing in the message with frequencies three, one and two say. The permutations calculation is the same as combinatorial problem of placing 6 balls: say three red, two green and one blue, in 6 urns. The enumerations are calculated using the multinomial formula

\[
P(n, f_1, f_2, \cdots, f_t) = \frac{n!}{f_1!f_2!\cdots f_t!}
\]

(5)

where

\[
n = f_1 + f_2 + \cdots + f_t
\]

The number of permutations for the example using Equation[5] would be

\[
\left( \begin{array}{c} 6 \\ 3, 1, 2 \end{array} \right) = \frac{6!}{3! \cdot 1! \cdot 2!} = \frac{6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1}{(3 \cdot 2 \cdot 1) \cdot (1 \cdot 2 \cdot 1)} = 60
\]

A unique ID can be attributed to each of these 60 permutations using \( \log_2(60) = 5.9069 \). Because a binary number can not have fractional number of bits therefore 6-bits would suffice to uniquely identify each permutation. As a comparison, this is much smaller than the Shannon length \( 6 \times 1.4591 = 8.7546 \) = 9-bits. It achieves the space saving of ratio 1/1.5850 = 63.09%.

It essentially means that we need a mechanism to establish bijection between the message permutation and its order in the list of all the permutations of given alphabet with given frequency counts. That number represented in binary format would correspond to the original message. The best selection would be the entry number in the dictionary of all permutations of the original message. Algorithms exist that can find the next permutation in lexicographic order given the present permutation. However, to the best of the author’s knowledge, no algorithm has been presented in literature that can find the permutation lexicographic position given the message or vice versa. This paper presents origional algorithm to map a message to and from its lexicographic order with simple method. A mixed radix number system consisting of multinomial coefficients is developed to perform this mapping.

The reader might get skeptic of getting a bit representation smaller than the Shannon limit in our toy example. The combinatorial compression would approaches the Shannon
Fig. 1: Binary source data compression using the Pascal’s triangle. In this directed acyclic graph, node pascal coefficient gives the number of paths from the root node. Powers of a and b tell the frequencies of these binary symbols in the message and correspond to number of left and right turns, respectively, taken to reach from root node. Starting at root node 1 and traversing the graph by taking a left turn on each a and right turn for each b, the sum of edge weights gives lexicographic order of the message. For example the message “aabb” would lead to node 6a²b² and maps to lexicographic index 0 + 0 + 2 + 3 = 5. The message “bbaa” would map to 0 + 0 + 0 + 0 = 0.

Limit as $n$ approaches $\infty$ for uniform alphabet frequencies but remaining always below the Shannon limit.

For a comparison the Shannon formula can be re-arranged to enumerate the corresponding patterns for given alphabet probabilities $p_1, p_2, \ldots, p_i$,

$$H = p_1 \log_2(1/p_1) + p_2 \log_2(1/p_2) + \cdots + p_i \log_2(1/p_i)$$

$$= \log_2\left(\frac{1}{p_1^{f_1} \cdot p_2^{f_2} \cdots p_i^{f_i}}\right)$$

As $H$ is the average length per symbol, $n \cdot H$ would give the total message length and $2^{n \cdot H}$ will give the total number of possible messages with $nH$ bits.

$$n \cdot H = n \cdot \log_2\left(\frac{1}{p_1^{f_1} \cdot p_2^{f_2} \cdots p_i^{f_i}}\right)$$

$$2^{n \cdot H} = \left(\frac{1}{p_1^{f_1} \cdot p_2^{f_2} \cdots p_i^{f_i}}\right)^n$$

$$2^{n \cdot H} = \left(\frac{1}{p_1^{f_1} \cdot p_2^{f_2} \cdots p_i^{f_i}}\right)$$

Using the relation between alphabet frequency and its probability $p_i = f_i/n$

$$2^{n \cdot H} = \frac{1}{(f_1/n)^{f_1} \cdot (f_2/n)^{f_2} \cdots (f_i/n)^{f_i}}$$

$$2^{n \cdot H} = \frac{1}{f_1^{f_1} \cdot f_2^{f_2} \cdots f_i^{f_i}}$$

$$2^{n \cdot H} = \frac{n!}{f_1! \cdot f_2! \cdots f_i!}$$

It is trivial to prove that Equation [14] is always greater than Equation [5] for all $n$ and $f_i$.

**Lemma 1.**

$$\frac{n^n}{f_1^{f_1} \cdot f_2^{f_2} \cdots f_i^{f_i}} > \frac{n!}{f_1! \cdot f_2! \cdots f_i!}$$

for all $n$ and $f_i$. Where $\sum_{i=1}^{l} f_i = n$

**Proof:** The inequality can be rearranged to the form

$$n^n > \frac{n!}{f_1! \cdot f_2! \cdots f_i!} f_1^{f_1} \cdot f_2^{f_2} \cdots f_i^{f_i}$$

Clearly [17] is true because right hand side is a term in the expansion of left hand side. Q.E.D.

**Theorem 2.** Let a source stream of independent identically distributed random variables of length $n$, of which each symbol comes from the set $A = \{\alpha_1, \alpha_2, \ldots, \alpha_t\}$ with frequencies $(f_1, f_2, \cdots, f_i)$ respectively. It is possible to compress the
Fig. 2: Encoding for binary messages of length \( n = 4 \). Traversal starts at root node. For the input stream we starts from Least Significant Bit (LSB). If a one is encountered in the input stream Right (R) turn is taken in graph traversal and Left (L) turn for a zero. Because all six streams have 2 zeroes (a’s) and 2 ones (b’s), we end up at node 6a^2b^2 in each case. Unlike Huffman/Arithmatic/Range encoding, no prior source model or alphabet probability knowledge is required. Rather respective alphabet frequency counters are incremented for each new symbol arrival.

**Proof:** Given the alphabet frequencies \((f_1, f_2, \ldots, f_t)\), due to basic combinatorics there cannot be more than \(\binom{n}{f_1, f_2, \ldots, f_t}\) permutations of the to-be-compressed-message. If a bijection is established between each permutation of the message and a number representing the lexicographic order of the permutation, no more than \(\log_2(\binom{n}{f_1, f_2, \ldots, f_t})\) would be needed to represent any of the permutations. This lexicographic position along with alphabet frequencies would accurately regenerate the original message. Due to Lemma-1, \(1/n \log_2(\binom{n}{f_1, f_2, \ldots, f_t})\) is always smaller than \(H\). The difference is more prominent for small \(n\). It is also substantial when one or two alphabets occur more frequently than others. For large \(n\) and uniform \(f_i\), the lemma approximates equality.

### III. Data Compression for Binary Source

The data compression for combinatoric encoding is first explained by a binary source with alphabet \(A = \{a = 0, b = 1\}\). Figure 4 shows a few examples of combinatorial encoding.

The figure proves the bijection of message permutations and its lexicographic order using the Pascal’s triangle. Each node in the directed acyclic graph can be reached from root in \(\binom{n}{f_0, f_1}\) ways, where \(n\) is the level of the node in the graph and \(f_0\) and \(f_1\) are the number of left and right turn needed to reach the node, respectively. Here the binomial coefficient is written in more generic form using \(\binom{n}{k} = \binom{n}{n-k}\). It will help extend the discussion to multinomial coefficients.

The edge weights between two nodes are given by the equation

\[
W_{\text{Left Turn}} \left\{ \left( \binom{n-1}{f_0-1, f_1} \rightarrow \binom{n}{f_0, f_1} \right) \right\} = \text{Zero} \quad (18)
\]

\[
W_{\text{Right Turn}} \left\{ \left( \binom{n-1}{f_0, f_1-1} \rightarrow \binom{n}{f_0, f_1} \right) \right\} = \binom{n-1}{f_0-1, f_1}
\]

Each path traversed with above edge weights will give a unique path cost, referred to here as lexicographic number of the path.

Compression is achieved by calculating the lexicographic order of the input message. For example if the input message is [11011100101], its lexicographic order or the compressed
Algorithm 1: Combinatorics Encoder for Binary Alphabet

Data: Source message $S$ of length $n$
Output: Lexicographic index: $L_i$, Frequencies: $f_0$, $f_1$

$L_i \leftarrow 0$
$f_0 \leftarrow 0$
$f_1 \leftarrow 0$

for $i \leftarrow 0$ to $n - 1$ do
  if $S[i] == 1$ then
    $L_i \leftarrow L_i + \binom{i}{f_1}$
    $f_1 \leftarrow f_1 + 1$
  else
    $f_0 \leftarrow f_0 + 1$

representation can be computed using Algorithm 1.

$$L_i = \binom{10}{7} + \binom{9}{6} + \binom{7}{5} + \binom{6}{4} + \binom{5}{3} + \binom{2}{2} + \binom{0}{1}$$

$$= 120 + 84 + 21 + 15 + 10 + 1 + 0$$

$$= 251$$

The number 251 can be represented with 8-bits, a saving of three bits. For decompression we will need the information ($L_i = 251$, $f_1 = 7$, $f_0 = 4$).

For easy hand calculations the above algorithm can be summarized as follows:

- Index message bits from zero starting at Least Significant Bit (LSB) of the message. Let $i$ be the bit index.
- Start a counter $j$ from LSB side and increment whenever a ONE is encountered. If LSB start with ONE then first value of $j$ would be one.
- Compute lexicographic order of the message as $\sum_{i=0}^{n-1} b_i \binom{i}{j}$, where $b_i$ is the $i$th bit and $\binom{i}{j} = 0$ for $i < j$

It should be noted lexicographic order remains unchanged for any number of zeros on left of message MSB. It helps in representing the bits in more compact form. However zeros to the right of LSB are significant and they effect the lexicographic order.

For lossless decompression of the message we need the lexicographic order of the message with given frequencies of the alphabets.

Using Algorithm 2 the compressed data ($L_i = 251$, $f_1 = 7$, $f_0 = 4$) can be decompressed as follows.

Algorithm 2: Data Reconstruction Algorithm

Input: Lexicographic index: $L_i$, Frequencies: $f_0$, $f_1$
Output: Data array $S[n]$

while $(f_0 + f_1) \geq 0$ do
  $n \leftarrow (f_0 + f_1 - 1)$
  if $L_i \geq \binom{n}{f_1}$ then
    $L_i \leftarrow L_i - \binom{n}{f_1}$
    $S[n] \leftarrow 1$
  else
    $S[n] \leftarrow 0$
  $f_0 \leftarrow f_0 - 1$

IV. DATA COMPRESSION FOR T-ALPHABET SOURCE

The data compression for multi alphabet source is achieved on the same principles as used by the binary source. An acyclic directed graph can be constructed in this case also. The major difference is that there are now $t$ outwards paths from each node, connecting to next $t$ nodes. Edge weights are weighted multinomial coefficients instead of binomial coefficients. If we have the alphabet as $(0, 1, 2, \ldots, t - 1)$, then each node in the directed graph has the data string $(f_1, f_2, \ldots, f_t)\alpha_1 f_1 \alpha_2 f_2 \cdots \alpha_t f_t$. Figure 3 shows the graph for three alphabet case.

The nodes on each level have labels

$$\sum_{f_1 + f_2 + \cdots + f_t = n} \binom{n}{f_1, f_2, \ldots, f_t} \alpha_1 f_1 \alpha_2 f_2 \cdots \alpha_t f_t$$

(19)

The weight of the directed edge connecting two nodes $(f_1, \ldots, f_k, \ldots, f_t)\alpha_1 f_1 \alpha_2 f_2 \cdots \alpha_k f_k \cdots \alpha_t f_t$ is given by
Fig. 3: Messages constructed by t-alphabet are encoded using acyclic directed graph of Pascal simplex in t-dimensions. For three alphabet we get a tetrahedron.

\[
W(f_1, \ldots, f_{n-1}, f_t) = \sum_{j=1}^{k-1} \binom{n-1}{f_1, \ldots, f_j - 1, \ldots, f_t}
\]

A. Encoding Example for Tertiary Alphabet: B A N A N A

All possible permutations of the letters in BANANA are

\[
P(n, f_1, f_2, f_3) = \binom{6}{3, 1, 2} = \frac{6!}{3!2!1!} = \frac{6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1}{3 \cdot 2 \cdot 1 \cdot 2 \cdot 1 \cdot 1} = 60
\]

So there are merely 60 different permutations. If we consider dictionary entry number of each of these permutations, any permutation can be represented by a binary number of no more than 6-bits length. That corresponds to one bit per symbol which is considerable compression as compared to 2-bits/symbol required for ordinary binary encoding.

V. Conclusion

An entropy encoding technique based on permutation index representation of the message string is presented. The encoding and decoding algorithms work by assigning integer weights to symbol place value based on multinational coefficients. Encoding process use only addition and subtraction and unlike arithmetic or range encoding require no multiplication or division operations. With pre-calculated binomial or multinomial coefficients the method achieves the compression accuracy of arithmetic coding at the operation speed of Huffman coding. The binary messages need binomial coefficients as digit place values while multinomial coefficients are used for higher cardinality alphabet sets.

REFERENCES

[1] C. E. Shannon, “A mathematical theory of communication,” ACM SIGMOBILE Mobile Computing and Communications Review, vol. 5, no. 1, pp. 3–55, 2001.
[2] D. A. Huffman et al., “A method for the construction of minimum redundancy codes,” Proceedings of the IRE, vol. 40, no. 9, pp. 1098–1101, 1952.
[3] I. H. Witten, R. M. Neal, and J. G. Cleary, “Arithmetic coding for data compression,” Communications of the ACM, vol. 30, no. 6, pp. 520–540, 1987.
[4] G. N. N. Martin, “Range encoding: an algorithm for removing redundancy from a digitised message,” in Proc. Institution of Electronic and Radio Engineers International Conference on Video and Data Recording, 1979.
Fig. 4: Input stream [BANANA] is encoded by traversal in directed acyclic graph of Pascal’s tetrahedron as there are three alphabets, compressed to [10110]. 6 edges are traversed, taking directions according to input alphabet.

TABLE I: All the permutations of word B A N A N A: $\lceil \log_2 \binom{6}{3,1,2} \rceil = 6$ bit long binary code along with knowledge of character frequencies ($f_A = 3, f_B = 1, f_N = 2$) is sufficient to uniquely represent any permutation.

| Lexicographic Index | Permutation | Code | Lexicographic Index | Permutation | Code | Lexicographic Index | Permutation | Code |
|---------------------|-------------|------|---------------------|-------------|------|---------------------|-------------|------|
| 0                   | mbbaaa      | 1    | 20                  | nabana      | 10101| 40                  | nbaaan      | 101001|
| 1                   | nbbaaa      | 10   | 21                  | anbana      | 10110| 41                  | bnaaan      | 101010|
| 2                   | bnbaaa      | 11   | 22                  | banana      | 10111| 42                  | nbaaan      | 101011|
| 3                   | nnabba      | 100  | 23                  | abnana      | 11000| 43                  | anbaan      | 101100|
| 4                   | nanabba     | 101  | 24                  | naabna      | 11001| 44                  | banaan      | 101101|
| 5                   | annbba      | 110  | 25                  | anabna      | 11010| 45                  | abnaan      | 101110|
| 6                   | nbabna      | 111  | 26                  | aanbna      | 11101| 46                  | naaban      | 110111|
| 7                   | bnabna      | 1000 | 27                  | baanana     | 11100| 47                  | anaban      | 110000|
| 8                   | nababa      | 1001 | 28                  | abanana     | 11101| 48                  | aanban      | 110001|
| 9                   | ababba      | 1010 | 29                  | aababna     | 11110| 49                  | baanan      | 110010|
| 10                  | babbba      | 1011 | 30                  | nnaaab      | 11111| 50                  | abanan      | 110011|
| 11                  | ababna      | 1100 | 31                  | nanaab      | 100000| 51                | aababn      | 110100|
| 12                  | naabab      | 1101 | 32                  | anaabab     | 100001| 52                | naanabn     | 110101|
| 13                  | nanabba     | 1110 | 33                  | naanab      | 100010| 53                | aanabbn     | 110110|
| 14                  | annabba     | 1111 | 34                  | aanabab     | 100111| 54                | aanabbn     | 110111|
| 15                  | nanaba      | 10000| 35                  | aannab      | 100100| 55                | aaanbn      | 111000|
| 16                  | ananba      | 10001| 36                  | naaanab     | 1001001| 56              | baanabn     | 111001|
| 17                  | aanabna     | 10010| 37                  | anaanab     | 100110| 57                | abaanbn     | 111010|
| 18                  | nbanaba     | 10011| 38                  | anaanab     | 100111| 58                | aabaan      | 111101|
| 19                  | banaaba     | 10100| 39                  | aaanabbn    | 101000| 59                | aaabbn      | 111100|