Constant Composition Distribution Matching

Patrick Schulte and Georg Böcherer, Member, IEEE

Abstract—Distribution matching transforms independent and Bernoulli(\(\frac{1}{2}\)) distributed input bits into a sequence of output symbols with a desired distribution. Fixed-to-fixed length, invertible, and low complexity encoders and decoders based on constant composition and arithmetic coding are presented. Asymptotically in the blocklength, the encoder achieves the maximum rate, namely the entropy of the desired distribution. Furthermore, the normalized divergence of the encoder output and the desired distribution goes to zero in the blocklength.

I. INTRODUCTION

A distribution matcher transforms independent Bernoulli(\(\frac{1}{2}\)) distributed input bits into output symbols with a desired distribution. We measure the distance between the matcher output distribution and the desired distribution by normalized informational divergence [1] p. 7. Informational divergence is also known as Kullback-Leibler divergence or relative entropy [2] Sec. 2.3. A dematcher performs the inverse operation and recovers the input bits from the output symbols. A distribution matcher is a building block of the bootstrap scheme [3] that achieves the capacity of arbitrary discrete memoryless channels [4]. Distribution matchers are used in [5] Sec. VI for rate adaption and in [6] to achieve the capacity of the additive white Gaussian noise channel.

Prefix-free distribution matching was proposed in [7] Sec. IV.A. In [8], [9] Huffman codes are used for matching. Optimal variable-to-fixed and fixed-to-variable length distribution matchers are proposed in [10] and [11], respectively. The codebooks of the matchers in [8]–[11] must be generated offline and stored. This is infeasible for large codeword lengths, which are necessary to achieve the maximum rate. This problem is solved in [12], [13] by using arithmetic coding to calculate the codebook online. The matchers proposed in [12], [13] are asymptotically optimal. All approaches [8]–[13] are variable length, which can lead to varying transmission rate, large buffer sizes, error propagation and synchronization problems [8] Sec. I. Fixed-to-fixed (f2f) length codes do not have these issues. The author of [14] Sec. 4.8 suggests to concatenate short codes and the authors of [4] employ a forward error correction decoder to build an f2f length matcher. The dematchers of [4], [14] cannot always recover the input sequence with zero error. Hence systematic errors are introduced that cannot be corrected by the error correction code or by retransmission. The thesis [15] proposes an invertible f2f length distribution matcher called adaptive arithmetic distribution matcher (adadm). The algorithm is computationally complex.

This work was supported by the German Ministry of Education and Research in the framework of an Alexander von Humboldt Professorship.

The authors are with the Institute for Communications Engineering, Technische Universität München, München, Germany.

In this work we propose practical, invertible, f2f length distribution matchers. They are asymptotically optimal and are based on constant composition codes indexed by arithmetic coding. The paper is organized as follows. In Section II we formally define distribution matching. We analyze constant composition codes in Section III. In Section IV we show how a constant composition distribution matcher (ccdm) and dematcher can be implemented efficiently by arithmetic coding.

II. PROBLEM STATEMENT

The entropy of a discrete random variable \(\mathcal{A}\) with alphabet \(\mathcal{A}\) and distribution \(P_{\mathcal{A}}\) is

\[
\mathbb{H}(\mathcal{A}) = \sum_{a \in \text{supp}(P_{\mathcal{A}})} -P_{\mathcal{A}}(a) \log_2 P_{\mathcal{A}}(a)
\]

(1)

where \(\text{supp}(P_{\mathcal{A}}) \subseteq \mathcal{A}\) is the support of \(P_{\mathcal{A}}\). The informational divergence of two distributions on \(\mathcal{A}\) is

\[
\mathcal{D}(P_{\tilde{\mathcal{A}}}/P_{\mathcal{A}}) = \sum_{a \in \text{supp}(P_{\mathcal{A}})} P_{\mathcal{A}}(a) \log_2 \frac{P_{\mathcal{A}}(a)}{P_{\tilde{\mathcal{A}}}(a)}.
\]

(2)

The normalized informational divergence for length \(n\) random vectors \(\tilde{\mathcal{A}}^n = \tilde{A}_1 \ldots \tilde{A}_n\) and \(\mathcal{A}^n\) is defined as

\[
\mathcal{D}(P_{\tilde{\mathcal{A}}^n}/P_{\mathcal{A}^n}) = \frac{1}{n} \sum_{a \in \text{supp}(P_{\mathcal{A}})} P_{\mathcal{A}}(a) \log_2 \frac{P_{\mathcal{A}}(a)}{P_{\tilde{\mathcal{A}}}(a)}.
\]

(3)

For random vectors with independent and identically distributed (iid) entries, we write

\[
P_{\mathcal{A}}(a^n) = \prod_{i=1}^{n} P_{\mathcal{A}}(a_i).
\]

(4)

A one-to-one f2f distribution matcher is an invertible function \(f\). We denote the inverse function by \(f^{-1}\). The mapping imitates a desired distribution \(P_{\mathcal{A}}\) by mapping \(m\) Bernoulli(\(\frac{1}{2}\)) distributed bits \(B^m\) to length \(n\) strings \(\tilde{A}^n = f(B^m) \in \mathcal{A}^n\). The output distribution is \(P_{\tilde{\mathcal{A}}^n}\). The concept of one-to-one f2f distribution matching is illustrated in Fig. 1.

Fig. 1. Matching a data block \(B^m = B_1 \ldots B_m\) to output symbols \(\tilde{A}^n = \tilde{A}_1 \ldots \tilde{A}_n\) and reconstructing the original sequence at the dematcher. The rate is \(\frac{m}{n}\). The matcher can be interpreted as emulating a discrete memoryless source \(P_{\mathcal{A}}\).

This work was supported by the German Ministry of Education and Research in the framework of an Alexander von Humboldt Professorship.

The authors are with the Institute for Communications Engineering, Technische Universität München, München, Germany.
**Definition 1.** A matching rate \( R = m/n \) is achievable for a distribution \( P_A \) if for any \( \alpha > 0 \) and sufficiently large \( n \) there is an invertible mapping \( f : \{0, 1\}^m \rightarrow A^n \) for which

\[
\mathbb{D}(P_f(B^n) \mid |P_A^n|) \leq \alpha. \tag{5}
\]

The following proposition in [16] relates the rate \( R \) and \( \alpha \).

**Proposition 1 (Converse, [16] Proposition 8).** There exists a positive-valued function \( \beta \) with

\[
\beta(\alpha) \xrightarrow{\alpha \to 0} 0 \tag{6}
\]

such that \( \mathbb{D}(P_f(B^n) \mid |P_A^n|) \leq \beta(\alpha) \).

Proposition 1 bounds the maximum rate that can be achieved under condition (5). Since \( \mathbb{H}(B) = 1 \) we have

\[
R \leq \mathbb{H}(A) \tag{8}
\]

for any achievable rate \( R \).

**III. Constant Composition Distribution Matching**

The empirical distribution of a vector \( c \) of length \( n \) is defined as

\[
P_{\hat{A}c}(a) = \frac{n_a(c)}{n} \tag{9}
\]

where \( n_a(c) = \{|i : c_i = a\} \) is the number of times symbol \( a \) appears in \( c \). The authors of [17] Sec. 2.1 call \( \hat{P}_{\hat{A}c} \) the type of \( c \). An \( n \)-type is a type based on a length \( n \) sequence. A codebook \( C_{ccdm} \subseteq A^n \) is called a constant composition code if all codewords are of the same type, i.e., \( n_a(c) \) does not depend on the codeword \( c \). We will write \( n_a \) in place of \( n_a(c) \) for a constant composition code.

**A. Approach**

We use a constant composition code with \( n_a \approx P_Aa \). As all \( n_a \) need to be integers and add up to \( n \), there are multiple possibilities to choose the \( n_a \). We use the allocation that solves

\[
P_A = \arg\min_{P_A} \mathbb{D}(P_{\hat{A}} \mid P_A) \tag{10}
\]

subject to \( P_A \) is \( n \)-type.

The solution of (10) can be found efficiently by [18] Algorithm 2. Suppose the output length \( n \) is fixed and we can choose the input length \( m \). Let \( T^n_{\hat{P}_A} \) be the set of vectors of type \( \hat{P}_A \), i.e., we have

\[
T^n_{\hat{P}_A} = \{ v \mid v \in A^n, \frac{n_a(v)}{n} = \hat{P}_A(a) \ \forall a \in A \}. \tag{11}
\]

The matcher is invertible, so we need at least as many codewords as input blocks. The input blocklength must thus not exceed \( \log_2 |T^n_{\hat{P}_A}| \). We set the input length to \( m = \lceil \log_2 |T^n_{\hat{P}_A}| \rceil \) and we define the encoding function

\[
f_{ccdm} : \{0, 1\}^m \rightarrow T^n_{\hat{P}_A} \tag{12}
\]

The actual mapping \( f_{ccdm} \) can be implemented efficiently by arithmetic coding, as we will show in Section IV. The constant composition codebook is now given by the image of \( f_{ccdm} \), i.e.,

\[
C_{ccdm} = f_{ccdm}(\{0, 1\}^m). \tag{13}
\]

Since \( f_{ccdm} \) is invertible, the codebook size is \(|C_{ccdm}| = 2^m\).

**B. Analysis**

We show that \( f_{ccdm} \) asymptotically achieves all rates satisfying (5). We can bound \( m \) by

\[
m = \lceil \log_2 |T_{\hat{P}_A}\rceil \geq \log_2 |T_{\hat{P}_A}| - 1. \tag{14}
\]

Recall that the matcher output distribution is \( P_{\hat{A}a} \). We have

\[
\mathbb{D}(P_{\hat{A}a} \mid |P_A^n|) = \sum_{a \in C_{ccdm} \subseteq T_{\hat{P}_A}} 2^{-m} \log_2 P_{\hat{A}a}(a) \tag{15}
\]

For Term 1 we obtain

\[
\mathbb{D}(P_{\hat{A}a} \mid |P_A^n|) = \sum_{a \in C_{ccdm} \subseteq T_{\hat{P}_A}} 2^{-m} \log_2 \prod_{i \in A} P_{\hat{A}a}(i)^{n_i} = \sum_{a \in C_{ccdm}} 2^{-m} \log_2 \frac{2^m}{2^{n \mathbb{H}(A)}} = n \mathbb{H}(\hat{A}) - m. \tag{16}
\]

Using (16) in (15) and dividing by \( n \) we have

\[
\mathbb{D}(P_{\hat{A}a} \mid |P_A^n|) < \mathbb{H}(\hat{A}) - R. \tag{17}
\]

The choice (10) of \( P_A \) guarantees (see [18] Proposition 4) that for the third term in (17) we have

\[
\mathbb{D}(P_{\hat{A}a} \mid |P_A^n|) < \frac{k}{\min_{a \in \text{supp}(P_A)} P_A(a)n^2} \tag{18}
\]

where \( k = |A| \) is the alphabet size. Consequently, we know that this term vanishes as the blocklength approaches infinity, i.e., we have

\[
\lim_{n \to \infty} \mathbb{D}(P_{\hat{A}a} \mid |P_A^n|) = 0. \tag{19}
\]

We now relate the input and output lengths to understand the asymptotic behavior of the rate. By [17] Lemma 2.2, we have

\[
|T_{\hat{P}_A}| \geq \binom{n+k-1}{k-1}^{-1} 2^{n \mathbb{H}(\hat{A})} \geq (n+k)^{-k} 2^{n \mathbb{H}(\hat{A})}. \tag{20}
\]

Taking the logarithm to the base 2 and dividing by \( n \) we have

\[
\frac{\log_2 |T_{\hat{P}_A}|}{n} \geq -k \log_2 (n+k) + \mathbb{H}(\hat{A}) - \frac{1}{n} \tag{21}
\]

For the rate, we obtain

\[
R = \frac{m}{n} \geq \frac{\log_2 |T_{\hat{P}_A}|}{n} - \frac{1}{n} \geq -k \log_2 (n+k) + \mathbb{H}(\hat{A}) - \frac{1}{n} \tag{22}
\]

and in the asymptotic case

\[
\lim_{n \to \infty} R = \mathbb{H}(\hat{A}). \tag{23}
\]
We describe the output model by a random vector $\tilde{\mathbf{A}}$. Fig. 2 shows the normalized divergence and rate of ccdm over output blocklength for $P_n = (0.0722, 0.1654, 0.3209, 0.4415)$. For comparison, the performance of optimal f2f [14, Sec. 4.4] and aadm [15] is displayed. Because of limited computational resources, we could calculate the performance of optimal f2f only up to a blocklength of $n = 90$.

From [19] and [16, Proposition 6] we know that $H(\tilde{\mathbf{A}}) \rightarrow H(A)$ and by [19] and (23) in [17], normalized divergence approaches zero for $n \rightarrow \infty$.

**Example 1.** The desired distribution is

$$P_n = (0.0722, 0.1654, 0.3209, 0.4415).$$

Fig. 2 shows the normalized divergences and rates of ccdm and the optimal f2f length matcher [14, Sec. 4.4]. The empirical performance of aadm [15] is also displayed. For optimal f2f and aadm, the rate is fixed to $H(A)$ bits per symbol. Observe that the ccdm needs about 4 times the blocklength of the optimal scheme to reach an informational divergence of 0.06 bits per symbol. However, the memory for storing the optimal codebook grows exponentially in $m$. For $n = 10$, we already need about $10240$ bits $= 1.25$ kB; for $n = 100$ we would need $1.441 \times 10^{19}$ TB of memory. In this example, ccdm performs better than aadm for short blocklength up to 100 symbols. Fig. 2 also shows the lower and upper bounds (8) and (22), respectively.

**IV. ARITHMETIC CODING**

We use arithmetic coding for indexing sequences efficiently. Our arithmetic encoder associates an interval to each input sequence in $\{0, 1\}^m$ and it associates an interval to each output sequence in $T_n^\mathbf{P}$, see Fig. 3 for an example. The size of an interval is equal to the probability of the corresponding sequence according to the input and output model, respectively. For the input model we choose an iid Bernoulli$(\frac{1}{2})$ process. We describe the output model by a random vector

$$\tilde{\mathbf{A}} = \tilde{A}_1 \tilde{A}_2 \ldots \tilde{A}_n$$

with marginals $P_{\mathbf{A}} = P_{\tilde{\mathbf{A}}}$ and the uniform distribution

$$P_{\mathbf{A}}(a^n) = \frac{1}{|T_n^\mathbf{P}|} \quad \forall a^n \in T_n^\mathbf{P}.$$  

The intervals are ordered lexicographically. All input and output intervals range from 0 to 1 because all probabilities add up to 1.

**Example 2.** Fig. 3 shows input and output intervals with output length $n = 4$ and $P_n(0) = P_n(1) = 0.5$. There are 4 equally probable input sequences and 6 equally probable output sequences. The intervals on the input side are $[0, 0.25), [0.25, 0.5), [0.5, 0.75)$ and $[0.75, 1)$. The intervals on the output side are $[0, \frac{1}{6})$, $[\frac{1}{6}, \frac{2}{6})$, $[\frac{2}{6}, \frac{3}{6})$, $[\frac{3}{6}, \frac{4}{6})$, $[\frac{4}{6}, \frac{5}{6})$ and $[\frac{5}{6}, 1)$.

The arithmetic encoder can link an output sequence to an input sequence if the lower border of the output interval is inside the input interval. In the example (Fig. 3) '00' may link to both '0101' and '0011', while for '01' only a link to '0110' is possible. There are at most two possible choices because by (14) the input interval size is less than twice the output interval size. Both choices are valid and we can perform an inverse operation. In our implementation, the encoder decides for the output sequence with the lowest interval border. As a result, the codebook $C_{\text{cdcm}}$ of Example 2 is $\{0011^\prime, \, 0110, \, 1001', \, '1100\}$. In general $C_{\text{cdcm}}$ has cardinality $2^n$ with $2^n \leq |T_n^\mathbf{P}| < 2^{n+1}$ according to (14). It is not possible to index the whole set $T_n^\mathbf{P}$ unless $2^n = |T_n^\mathbf{P}|$. The analysis of the code (Section III-B) is valid for all codebooks $C_{\text{cdcm}} \subseteq T_n^\mathbf{P}$. The actual subset is implicitly defined by the arithmetic encoder.

We now discuss the online algorithm that processes the input sequentially. Initially, the input interval spans from 0 to 1. As the input model is Bernoulli$(\frac{1}{2})$ we split the interval into two equally sized intervals and continue with the upper interval in case the first input bit is ‘1’; otherwise we continue with the lower interval. After the next input bit arrives we repeat the last step. After $m$ input bits we reach a size $2^{-m}$ interval. After every refinement of the input interval the algorithm checks for a sure prefix of the output sequence, e.g., in Fig. 3 we see that if the input starts with 1 the output must start with 1. Every time we extend the sure prefix by a new symbol, we must calculate the probability of the next symbol given

\[^1\text{Please note that in this case no distribution matcher is needed. However, the invertible mapping is of interest in its own right.}\]
the sure prefix. That means we determine the output intervals within the sure interval of the prefix. The model for calculating the conditioned probabilities is based on drawing without replacement. There is a bag with \( n \) symbols of \( k \) discriminable kinds. \( n_a \) denotes how many symbols of kind \( a \) are initially in the bag and \( n'_a \) is the current number. The probability to draw a symbol of type \( a \) is \( n'_a / n \). If we pick a symbol \( a \) both \( n \) and \( n'_a \) decrement by 1.

**Example 3.** Fig. 4 shows a refinement of the output intervals. Initially there are 2 ’0’s and 2 ’1’s in the bag. The distribution of the first drawn symbol is \( P_{A_1} (0) = P_{A_1} (1) = \frac{1}{2} \). When drawing a ’0’, there are 3 symbols remaining: one ’0’ and two ’1’s. Thus, the probability for a ’0’ reduces to 1/3 while the probability of ’1’ is 2/3. If two ’0’s were picked, two ’1’s must follow. This way we ensure that the encoder output is of the desired type. Observe that the probabilities of the next symbol conditioned on the previous symbols are unequal in general, i.e, we have

\[
P_{A_2 | \bar{A}_1} (0 | 0) \neq P_{A_2 | \bar{A}_1} (0 | 1)
\]  

(25)

in general. However, \( P_{A_1} = \prod_{i=1}^{n} P_{A_1} | a_{i-1} (a_i | a_{i-1}) \) is constant on \( T^n_{\bar{A}_1} \) as we show in the following proposition.

**Proposition 2.** After \( n \) refinements of the output interval the model used for the refinement step stated above creates equally spaced (equally probable) intervals that are labeled with all sequences in \( T^n_{\bar{A}_1} \).

**Proof.** All symbols in the bag are chosen at some point. Consequently only sequences in \( T^n_{\bar{A}_1} \) may appear. All possibilities associated with the chosen string are products of fractions \( n'_a / n \), where \( n \) takes on all values from the initial value to 1 because every symbol is drawn at some point. Thus for each string we obtain for its probability an expression that is independent of the realization itself:

\[
P_{A^n} (a^n) = \frac{n_{a=0} \cdots n_{a=k-1}}{n!} = \frac{1}{|T^n_{\bar{A}_1}|} \forall a^n \in T^n_{\bar{A}_1}. 
\]  

(26)

Numerical problems for representing the input interval and the output interval occur after a certain number of input bits. For this reason we introduce a rescaling each time a new output symbol is known. We explain this next.

A. Scaling input and output intervals

After we identify a prefix, we are no longer interested in code sequences that do not have that prefix. We scale the input and output interval such that the output interval is \([0,1)\). Fig. 5 illustrates the mapping of intervals \([\text{in}_1, \text{out}_1]\) to \([\text{in}_2, \text{out}_2]\). The refinement for the second symbol works as described in Example 3 If the second bit is 0, we know that 10 must be a prefix of the output. The resulting scaling is shown in Fig. 5 as \([\text{in}_2, \text{out}_2]\) to \([\text{in}_3, \text{out}_3]\). A more detailed explanation of scaling for arithmetic coding can be found for instance in [19, Chap. 4]. We provide an implementation of cedn online [20].

V. Conclusion

We presented a practical and invertible f2f length distribution matcher that achieves the maximum rate asymptotically in the blocklength. In contrast to matchers proposed in the literature [8]–[13] the f2f matcher is robust to synchronization and variable rate problems. Error propagation is limited by the blocklength. In future work we plan to investigate f2f length codes that perform well in the finite blocklength regime.

VI. Acknowledgment

We wish to thank Irina Bocharova and Boris Kudryashov for encouraging us to work on the presented approach.

**References**

[1] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*. Cambridge University Press, 2011.

[2] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd ed. John Wiley & Sons, Inc., 2006.

[3] G. Böcherer and R. Mathar, “Operating LDPC codes with zero shaping gap,” in *Proc. IEEE Inf. Theory Workshop (ITW)*, 2011.

[4] M. Mondelli, S. H. Hassani, and R. Urbanke, “How to achieve the capacity of asymmetric channels,” *Proc. Allerton Conf. Commun., Contr., Comput.*, pp. 789–796, Sep. 2014.

[5] D. MacKay, “Good error-correcting codes based on very sparse matrices,” *IEEE Trans. Inf. Theory*, vol. 45, no. 2, pp. 399–431, 1999.

[6] G. Böcherer, P. Schulte, and F. Steiner, “Bandwidth efficient and rate-compatible low-density parity-check coded modulation,” arXiv preprint, 2015. [Online]. Available: [http://arxiv.org/abs/1502.02733](http://arxiv.org/abs/1502.02733)

[7] J. Forney, G., R. Gallager, G. Lang, F. Longstaff, and S. Qureshi, “Efficient modulation for band-limited channels,” *IEEE J. Sel. Areas Commun.*, vol. 2, no. 5, pp. 632–647, 1984.

[8] F. R. Kschischang and S. Pasupathy, “Optimal nonuniform signaling for Gaussian channels,” *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 915–929, 1993.
[9] G. Ungerböck, “Huffman shaping,” in *Codes, Graphs, and Systems*, R. Blahut and R. Koetter, Eds. Springer, 2002, ch. 17, pp. 299–313.
[10] G. Böcherer and R. Mathar, “Matching dyadic distributions to channels,” in *Proc. Data Compression Conf.*, 2011, pp. 23–32.
[11] R. A. Amjad and G. Böcherer, “Fixed-to-variable length distribution matching,” in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, 2013, pp. 1511–1515.
[12] N. Cai, S.-W. Ho, and R. Yeung, “Probabilistic capacity and optimal coding for asynchronous channel,” in *Proc. IEEE Inf. Theory Workshop (ITW)*, 2007, pp. 54–59.
[13] S. Baur and G. Böcherer, “Arithmetic distribution matching,” in *Proc. Int. ITG Conf. Syst. Commun. Coding*, Feb. 2015.
[14] R. A. Amjad, “Algorithms for simulation of discrete memoryless sources,” Master’s thesis, Technische Universität München, 2013.
[15] P. Schulte, “Zero error fixed length distribution matching,” Master’s thesis, Technische Universität München, 2014.
[16] G. Böcherer and R. A. Amjad, “Informational divergence and entropy rate on rooted trees with probabilities,” in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Sep. 2014, pp. 176–180.
[17] I. Csiszár and P. C. Shields, “Information theory and statistics: A tutorial,” *Foundations and Trends in Commun. Inf. Theory*, vol. 1, no. 4, pp. 417–528, 2004.
[18] G. Böcherer and B. C. Geiger, “Optimal quantization for distribution synthesis,” *arXiv preprint*, 2014. [Online]. Available: [http://arxiv.org/abs/1307.6843](http://arxiv.org/abs/1307.6843)
[19] K. Sayood, *Introduction to data compression*. Elsevier, 2006.
[20] “A fixed-to-fixed length distribution matcher in C/MATLAB.” [Online]. Available: [http://beam.to/ccdm](http://beam.to/ccdm)