INTEGER TO INTEGER KARHUNEN LOÉVE TRANSFORM OVER FINITE FIELDS

Güneş Z. Karabulut[1], Daniel Panario[2], Abbas Yongaçoḡlu[1]

[1]School of Information Technology and Eng.
University of Ottawa
K1N 6N5, Ontario, Canada

[2]School of Mathematics and Statistics
Carleton University
K1S 5B6, Ontario, Canada

ABSTRACT

In communications system design, it is frequently assumed that source symbols are equiprobable. However in real life applications this is not the case since most sources produce Gaussian samples. In this paper, we introduce a Karhunen Loéve Transform (KLT) based integer to integer transform, I$_2$I KLT, over $GF(q)$ that will force the symbols to uniform distribution. This transform can be used as interface between sources with different distributions and communication systems designed according to uniform distributions.

1. INTRODUCTION

A communication system connects a source to a destination through a channel. A typical communication system is shown in Fig.1. Due to today's increasing data demands, this process has to be reliable, i.e. robust to any channel imperfections or source statistics, and efficient i.e. use the least possible amount of resources like power and bandwidth. These goals make the communication system design a challenging problem.

Considering discrete sources, the majority of the communication systems are designed according to the uniform input distribution assumption, i.e, the probabilities of discrete source outputs are constant. This assumption is frequently used when there is no apriori knowledge about the data, which is the case for many source outputs.

The source distribution is important in the sense that, in a communication system, the receiver is designed according to a particular source distribution. For example, optimum decision region in a binary system depends on the probabilities of 1's and 0's. For example the system designs proposed in [1, 2] assume that source output symbols are equally likely. Therefore, their designs are optimum only with these assumptions. Furthermore, it is known that a communication system works optimally for symmetric channels when the input probability distributions are fixed ([3], Lemma 8).

However uniform input distribution is rarely the case in real life. For instance, due to correlation, output symbols of a digital camera most likely will not be equally likely. Most but not all source outputs in practice are Gaussian distributed. In this paper, we introduce a Karhunen Loéve transform based integer to integer transform (I$_2$I KLT) over finite fields that will produce uniformly distributed outputs, regardless of the input distribution. This transform is fast and invertible, since the operations are performed over a finite field avoiding floating point arithmetic.

We propose to use the I$_2$I KLT as shown in Fig.2 so that the inputs of the communication system are uniformly distributed, and the communication system design assumptions hold. Since this is a fast and lossless process, it can be added to previously designed communication system in order to assure the uniform distribution.

The paper is organized as follows. A brief summary of the KLT over $\mathcal{R}$ and the transform coding is given in Section 2. The proposed I$_2$I KLT is presented in Section 3. In Section 4, experiment results are shown. Conclusions are given in Section 5.

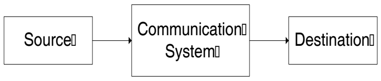

Fig. 1. A communication system model

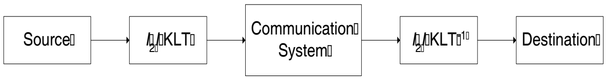

Fig. 2. A modified communication system model

0-7803-8484-9/04/$20.00 ©2004 IEEE

2. TRANSFORM CODING AND KARHUNEN LOÉVE TRANSFORM OVER $\mathcal{R}$

In classical communication theory, a transform coder is used for data compression. One of the frequently used transform coding techniques is Karhunen Loéve Transform (KLT). In this section we summarize the transform coding and the KLT over $\mathcal{R}$.

A transform coder decomposes a signal using an orthogonal basis and quantizes the decomposition coefficients. For an n dimensional signal vector $\mathbf{x}_i$, $i = 1, 2, ..., M$ and a unitary transform matrix $\mathbf{A}$ of dimension $n \times n$, we have the analysis equation

$$\mathbf{y}_i = \mathbf{A}\mathbf{x}_i, \tag{1}$$

where $\mathbf{y}_i$ is the vector of transformed coefficients. Assuming $\mathbf{A} = [\mathbf{a}_1, \mathbf{a}_2, ..., \mathbf{a}_n]$, the synthesis equation that is used to reconstruct the original signals $\mathbf{x}_i$ is

$$\mathbf{x}_i = \mathbf{A}^{\mathrm{T}}\mathbf{y}_i = \sum_{j=1}^{n} y_{i,j}\mathbf{a}_j \simeq \sum_{j=1}^{n} \hat{y}_{i,j}\mathbf{a}_j \tag{2}$$

where $y_{i,j}$, $j = 1, 2, ..., n$, $i = 1, 2, ..., M$, are the transform coefficients and $\hat{y}_{i,j}$ are the quantized coefficients. This quantization process distorts the bijective relation between $\mathbf{x}_i$, and $\mathbf{y}_i$, resulting in the quantization noise.

It is known that over $\mathcal{R}$ KLT minimizes the geometric mean of the variance of the transformed coefficients [4]. If the process is Gaussian then the coefficients of $\mathbf{y}_i$ are Gaussian using any basis. If the process is not Gaussian, the KLT is not necessarily the optimal transform.

The transform vectors of KLT consist of the eigenvectors of the autocorrelation matrix. The autocorrelation matrix for a random process X, is a matrix $\mathbf{R}$ whose $(k, l)^{th}$ element $[R]_{k,l}$ is given by

$$[R]_{k,l} = E[x_m x_{m+|k-l|}], \tag{3}$$

where x_i is the i^{th} sample of the random process. This procedure is adopted to finite fields in order to obtain a lossless transform which is termed as I$_2$I KLT. This transform is described with further details in the following section.

3. KARHUNEN LOÉVE TRANSFORM OVER FINITE FIELDS: I$_2$I KLT

Let us consider a field with q elements, where q is a power of a prime p. We denote this finite field by $GF(q)$. Using results on linear algebra over $GF(q)$, we can adopt KLT over finite fields.

There are two major differences between KLT over $\mathcal{R}$ and over $GF(q)$. In KLT over $\mathcal{R}$ after a block of data is transformed, it has to be quantized in order to be represented in digital sense. This introduces some noise and distortion to the transform. However, when the transform is from integer to integer, then this noise is eliminated. The second difference is speed. It is known that an integer to integer transform can reduce the required time for a particular application since floating point arithmetics is avoided [5].

The eigenvalues of an $n \times n$ square matrix $\mathbf{R}$ in any field are defined as the roots of

$$|\lambda\mathbf{I} - \mathbf{R}| = \mathbf{0}. \tag{4}$$

This equation leads us to the unique monic polynomial

$$p(\lambda) = \lambda^n + a_1\lambda^{n-1} + a_2\lambda^{n-2} + \cdots + a_{n-1}\lambda + a_n \tag{5}$$

where, eigenvalues satisfy the equality $p(\lambda) = 0$.

The most challenging problem in adopting KLT over $GF(q)$ is the existence of eigenvalues in higher order extension fields. It can be shown that only some (but few) eigenvalues are located within the considered field. Furthermore, not all $n \times n$ matrices have n eigenvalues due to the fact that irreducible polynomials can have any degree, not only degree one. This leads us to the following probabilistic analysis.

3.1. Probability Analysis

The probability that there exist n distinct roots from a given polynomial with degree n over $GF(q)$ can be calculated as

$$P_1 = \frac{1}{q^n}\binom{q}{n}. \tag{6}$$

One can show using generating functions that the probability of having at least one root of the characteristic polynomial in the field of interest is given by

$$P_2 = \sum_{i=1}^{n} (-1)^{i+1}\binom{q}{i} q^{-i}. \tag{7}$$

Moreover, the probability that a polynomial of degree n, has k distinct roots, where $k \leq n$, can be obtained as [6]

$$P_3 = \binom{q}{k} q^{-k} \sum_{i=0}^{n-k} (-1)^i \binom{q-k}{i} q^{-i}. \tag{8}$$

Consider $GF(127)$ and $GF(256)$, and let n be 8. It can be shown that $P_1 = 1.98e^{-5}$, $P_2 = 0.6336$ for

Table 1. P_3 values for $GF(127)$ and $GF(256)$, for $n = 8$

k	$GF(127)$	$GF(256)$	k	$GF(127)$	$GF(256)$
1	0.369	0.368	5	$2.71e^{-3}$	$2.74e^{-3}$
2	0.1847	0.1843	6	$6.12e^{-4}$	$6.52e^{-4}$
3	0.0609	0.061	7	$9.24e^{-6}$	$5e^{-6}$
4	0.0152	0.0154	8	$1.98e^{-5}$	$2.22e^{-5}$

$GF(127)$ and $P_1 = 2.22e^{-5}$, $P_2 = 0.6328$ for $GF(256)$. Furthermore one can show that P_2 values converge to $1 - e^{-1}$ for large q. That is, 63.21% of the time we will have at least one root for the polynomial in (5).

The probability values of P_3 for both fields are tabulated in Table 1. For $k = n$ case, $P_1 = P_3$ as shown in the table. From the values we see that, although the probability that all roots exist is very low for both fields, with high probability we have at least one root existing within that field. These probabilities verify that a fast KLT can be efficiently implemented over $GF(q)$.

3.2. I$_2$I KLT

Let $\mathbf{x} = [\mathbf{x}_1, \mathbf{x}_2, \cdots, \mathbf{x}_M]$ and $\mathbf{y} = [\mathbf{y}_1, \mathbf{y}_2, \cdots, \mathbf{y}_M]$ be the data and the transform matrices respectively. Inspired from KLT, I$_2$I KLT can be defined as

$$\mathbf{y}_i = \mathbf{A}(\mathbf{x}_i - \mathbf{m_x}), \tag{9}$$

where $\mathbf{m_x}$ is the mean vector of $\mathbf{x}$. However, since the transform is over finite fields, $\mathbf{m_x}$ is calculated over the field of interest $GF(q)$ as

$$\mathbf{m_x} = E_q[\mathbf{x}] = M^{-1} \sum_{i=1}^{M} \mathbf{x}_i, \tag{10}$$

where M^{-1} represents the multiplicative inverse of M in $GF(q)$, and $E_q[\cdot]$ represents the mean calculated according to $GF(q)$ addition rules.

In KLT over $\mathcal{R}$, the rows of the $n \times n$ transform matrix $\mathbf{A}$ are the eigenvectors of the correlation matrix, $\mathbf{R}$. Similar to (10), the correlation matrix $\mathbf{R}$ can be calculated over $GF(q)$ as

$$\mathbf{R} = M^{-1} \sum_{i=1}^{M} \mathbf{x}_i \mathbf{x}_i^T - \mathbf{m_x}. \tag{11}$$

When working over $GF(q)$, some eigenvalues may be in some extension fields. It is likely that this is the case and we have $l \leq n$ eigenvalues that are the roots of polynomial in (5). The probability of this case is given in equations (6) to (8).

Over $GF(q)$ the roots of (5) can be evaluated using a trial and error process known as the Chien search. However this method only shows that for a particular value, if the equality is satisfied, it is a root of order at least one. This prevents us from finding the proper order of the root unless we have exactly n distinct roots.

After obtaining the $l \leq n$ eigenvalues $\{\lambda_1, ..., \lambda_l\}$ that exists within $GF(q)$ one can find the eigenvectors from the null-space of the matrix $\mathbf{M}_k = \lambda_k \mathbf{I} - \mathbf{R}$. From the dimension of the null-space of $\mathbf{M}_k$, the order of the eigenvalue as a root of (5) can be obtained. Let us assume that from a particular $\mathbf{R}$ we have obtained m distinct eigenvectors, where $l \leq m \leq n$, and let them form the rows of the $m \times n$ matrix $\mathbf{E}$.

Since with a high probability we will have $m < n$, we can not implement the optimum KLT that is used in transform coding. One suboptimal method that can solve this problem is to place universal unit basis for eigenvectors of the non-existent eigenvalues. That is, in order to assure invertibility, we can form a suboptimal transform matrix $\mathbf{A}$ as

$$\mathbf{A} = \left[\begin{array}{ccc} & \mathbf{E} & \\ - & - & - \\ \mathbf{0} & | & \mathbf{I} \end{array} \right], \tag{12}$$

where $\mathbf{I}$ is the $(n-m) \times (n-m)$ identity matrix, and 0 is the $(n-m) \times m$ zero matrix. Using this transform if $m = n$, $\mathbf{A} = \mathbf{E}$ we have the optimum KLT over $GF(q)$, and if $m = 0$, we have $\mathbf{A} = \mathbf{I}$.

The original data $\mathbf{x}_i$ can be obtained by using the inverse transform, I$_2$I KLT^{-1}

$$\hat{\mathbf{x}}_i = \mathbf{A}^{-1}\mathbf{y}_i + \mathbf{m_x}, \tag{13}$$

where $\mathbf{A}^{-1}$ is evaluated such that $\mathbf{A}\mathbf{A}^{-1} = \mathbf{I}$ over $GF(q)$. Dividing $\mathbf{A}$ into submatrices as shown in (12), we have the invertibility property, that is we can assure that $\mathbf{A}^{-1}$ exists, and $\hat{\mathbf{x}} = \mathbf{x}$.

Another issue that needs to be checked in I$_2$I KLT is the independence of the variables. Assuming that the source outputs are independent and identically distributed, uniformly distributed data can be obtained via I$_2$I KLT. However, the samples of the transform output may not be independent. This problem can easily be solved by using an interleaver. The size of the interleaver can be very small due to the fact that only m samples may be correlated, and $n - m$ samples remain independent. A small interleaver size introduce only negligible amount of delay to the system.

4. EXPERIMENT RESULTS

In our experiments we used q-ary data points obtained from an approximately Gaussian random process. We

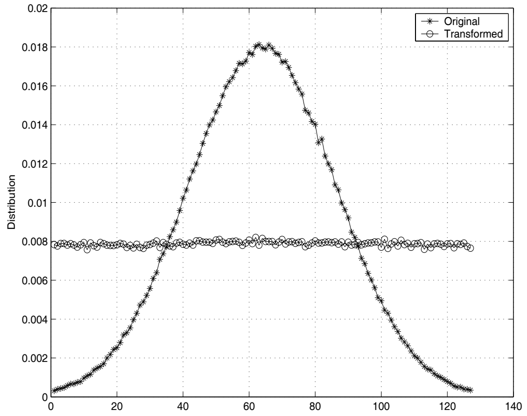

Fig. 3. Probability Distribution 2 before and after I_2I KLT $GF(127)$

selected the process to be bell shaped since most of the sources produce approximately Gaussian outputs. We transformed the random data using I_2I KLT, and also evaluated the inverse transform, I_2I KLT^{-1} in order to verify that there exists no quantization noise in the transform.

For simulations we considered two bell shaped distributions in a prime field $GF(127)$, and in an extension field $GF(256)$. For the I_2I KLT we considered parameters as $n = 8$, $M = 256$. The original and the transformed data probability distributions are shown in Fig. 3 and Fig. 4 respectively. From these figures we can see that large deviations in the distributions are smoothened via the I_2I KLT. The produced input samples were independent, and at 5% level we do not have enough evidence to state that the output samples are dependent [7].

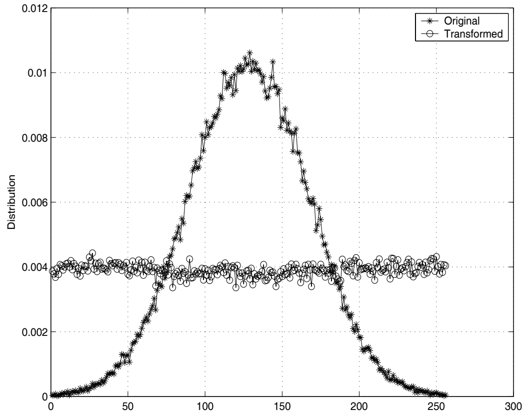

Fig. 4. Probability Distribution before and after I_2I KLT over $GF(256)$

5. CONCLUSIONS

In this paper, a KLT based integer to integer transform over finite fields is introduced. This transform smoothens the probability distributions of discrete variables. It is fast and invertible, causing no data or efficiency loss. Since the transform does not depend on the input distribution, it is very flexible in terms of different source distributions.

Besides the application as a pre-coder suggested in the introduction, this transform has potential applications in signal processing and communications area that may solve system specific problems. The optimum uncoded q-ary communication system is an example [3]. Furthermore, error correcting codes can be another potential application due to the randomization achieved via I_2I KLT.

ACKNOWLEDGMENT

Authors would like to thank Dr. Matias Salibian-Barrera for several statistical suggestions that improved the paper.

6. REFERENCES

[1] M. J. Borran and B. Aazhang, "Multilevel codes and iterative multistage decoding: rate design rules and practical considerations," IEEE Wireless Comm. and Networking Conf., vol. 1, pp. 23–28, Sep 2000.

[2] G. Ungerboeck, "Channel coding with multilevel/phase signals," IEEE Trans. on Info. Theo., vol. IT-28, no. 1, pp. 55–67, Jan 1982.

[3] M. Gastpar, B. Rimoldi, and M. Vetterli, "To code or not to code: Lossy source-channel communication revisited," IEEE Trans. on Info. Theo., vol. 49, no. 5, pp. 1147–1158, May 2003.

[4] K. Sayood, Introduction to Data Compression, Morgan Kaufmann Publishers, 2000.

[5] C.-C. T. Chen, C.-T. Chen, and C.-M. Tsai, "Hard limited Karhunen Loéve transform for text independent speaker recognition," Electronic Letters, vol. 33, no. 24, pp. 2014–2016, Nov 1997.

[6] A. Knopfmacher and J. Knopfmacher, "Counting polynomials with a given number of zeros in a finite field," Linear and Multilinear Algebra, vol. 26, pp. 287–292, 1990.

[7] W. Mendenhall III, R. L. Scheaffer, and D.D. Wackerly, Mathematical Statistics with Applications, Duxbury Advanced Series, 2002.