International Journal of Mathematics Research.
ISSN 0976-5840 Volume 8, Number 3 (2016), pp. 193-198
© International Research Publication House
http://www.irphouse.com

Establishing Role of Rank–Metric Codes for Error Correction in Random Network Coding

Ajeet Singh[1] **and Shefali Kapoor**[1]

[1] *Department of Mathematics, Lingaya's University, Faridabad-121002*

Abstract

In this paper is we establish the role of Rank-metric Codes for error correction in Random network Coding. For this, first we try to understand the process of communication and its components. Thereafter, describing the problem in achieving error free communication and making necessary assumptions, we arrive at the conclusion.

Keywords: Rank-metric code, Error correction, Network coding, transmitter, Receiver, Channel, Topology.

INTRODUCTION

The fundamental problem of communication is that of reproducing exactly same messages from one point to another point of a network. However spreading information throughout the network is prone to transmission errors.

For example, a single corrupt packet of information when transmitted may contaminate all packets of information in the network at various successive links. A network hacker may jam a network by injecting corrupt packet.

This problem can be overcome by Random Network Coding using small Metric codes.

Random Network Coding is a practical and effective technique to achieve highest capacity of a network.

Process of Communication and Elements of a Communication System:

Before we proceed to establish the role of rank- metric codes for error correction, for better appreciation, first it is necessary to understand the process of communication and the elements thereof.

Process of Communication:

Communication involves the transmission of information from one point to another through a succession of processes. Various processes involved therein are described below:

i. Generation of a message signal: voice, music, picture, or computer data.
ii. Description of that message signal with a certain measure of precision, by a set of symbols which can be electrical, aural, or visual.
iii. The encoding of these symbols in a form that is suitable for transmission over a physical medium.
iv. The transmission of the encoded symbols to the desired destination.
v. The decoding and reproduction of the original symbols.
vi. The re-creation of the original message signal, defining the degradation in quality if any.

Elements of a Communication System:

Now we study the variouselements of a communication system. There are three basic elements to every communication system, namely, transmitter, channel, and receiver. The transmitter is located at one point in space, the receiver is located at some other point separate from the transmitter, and the channel is the physical medium that connects them.

Elements of a Communication System are depicted in Figure 1 below.

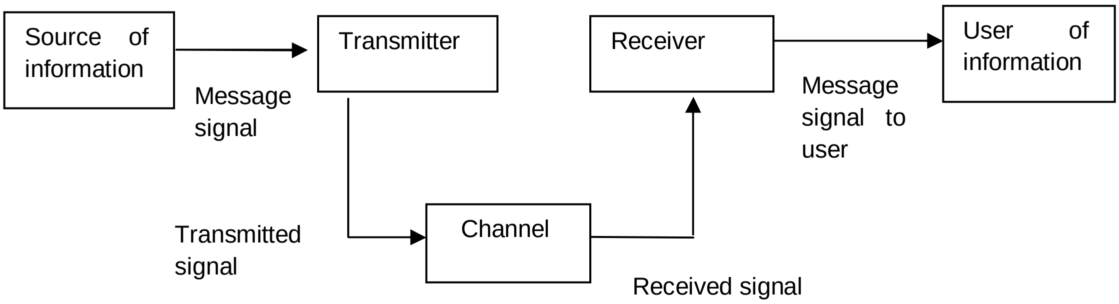

Figure I: Elements of a Communication System

The purpose of a Transmitter:

The purpose of transmitter is to convert the message signal produced by the source of information into a form suitable for transmission over the channel.

Need of Channel:

Channel is the physical medium that connects the transmitter and receiver. As the transmitted signal propagates along the channel, it is distorted due to channel imperfections. Moreover, noise and interfering signals (originating from other sources) are added to the channel output, with the result that the received signal is a corrupted version of the transmitted signal.

Task of the Receiver:
The receiver has the task of operating on the received signal so as to reconstruct a recognizable form of the original message signal for a user.
Having understood "Communication", We now proceed to our main objective i.e. to establish role of Rank–Metric Codes for Error Correction in Random Network Coding.

Assumptions:
We consider the use of random linear network coding in a point- to- point communication network with a single source and multiple destinations.
We assume that neither the source nor any of the destinations have any global knowledge of the network topology or then network code used.
We restrict attention to a single destination since every destination faces essentially the same problem.

Topology of the Network:
The topology of the network may very over time, as nodes join & leave, and connections are established & lost. However, such issues can be resolved by splitting the information stream to be transmitted by the source into chunks of 'n' packets.

Description:
We assume that each packet consists of N symbols over a finite field Fq.
Each internal node in the network performs classical distributed network coding: whenever a node has a transmission opportunity, it produces an outgoing packet as a random F_q-linear combination of all the packets it has until then received.

Let $x_1, \ldots, x_n$ denote the n packets transmitted by the source node,
and let $y_1, \ldots, y_n'$ denote the n ′ packets received by the destination node.

Stacking packets $x_1, \ldots, x_n$ as the rows of the transmitted matrix $x = [x_{ij}]$, where the subscript x_{ij} denotes the j-th entry of packet x_i,
and doing similarly for the received matrix $y = [y_{ij}]$,
we can relate x and y according **to y = Gx,**
where G is an $n' \times n$ matrix over F_q corresponding to the overall transfer function of the network from source to destination.

We now assume that packets may be received in error over any link in the network, then the model becomes:

$$\mathbf{y = Gx + Hz,} \qquad \textbf{- (I)}$$

where $z = [z_1, \ldots, z_t]$ is a matrix consisting of all the erroneous packets introduced, and H is the $n' \times t$ overall transfer matrix from these packets to the destination.

Let <A> denote the row space of a matrix A.
In order to communicate under this model, we consider that a message generated at the source is encoded as a subspace X of the vector space F_q^N, which is then transmitted over the network as the row space of x , i.e. X = <x> . The destination receives Y = <y>, the row space of y.
From this received subspace Y , the destination tries to infer X.

What we have is a channel where a subspace X is transmitted and a subspace Y is received.
At this point, it is intuitive that a notion of closeness between X and Y exists.

The following distance function is introduced to make this notion precise:

Definition 1:
Let X and Y be subspaces of a finite dimensional vector space.
The distance between X and Y is defined as:

$$\mathbf{d_S(X, Y) = dimension\ (X) + dimension\ (Y) - 2\ dimension\ (X \cap Y)}$$

It can be shown that this function is a metric.

Proceeding in this manner, the problem of error correction in random network coding can be rephrased as the problem of finding the subspace X that is at the smallest distance from the received subspace Y .

More precisely, we define the Grassmannian graph $Gr_{n,N}(Fq)$ as the set of all n-dimensional subspaces of Fq^N. A code ß in the Grassmannian graph is any subset of $Gr_{n},_{N}(F_q)$. The decoding problem proposed above, from now on referred to as subspace decoding, is the following:

$$\mathbf{Minimize\ d_s\ (X,Y)\ where\ X \in ß - (\ II)}$$

Connection between Rank-metric Codes & the Codes in the Grassmannian Graph:
We now develop the connection between rank metric codes and codes in the Grassmannian graph and show how the subspace decoding problem can be solved by techniques for the rank metric.

Let F_q^{nXm} be the set of all n × m matrices over F_q.
A matrix code C is defined as any subset of F_q^{nXm}.

The following distance function is known to be a metric:
Definition 2:
Therank distance between matrices a, b $\in F_q^{nXm}$ is defined as:

$$\mathbf{d_R(a, b) = rank\ (b - a)}$$

A rank-metric code is simply a matrix code used in the context of the rank distance metric.
For any $C \subseteq F_q^{nXm}$, let $C^* = \{[I\ c], c \in C\}$, where I denotes an identity matrix.

We assume the special case of problem (II), where the code ß in the Grassmannian graph is of the form:
$ß = ß^* = \{<x>, x \in C^*\}$ for some $C \subseteq F_q^{nXm}$,
i.e., ß* consists of the row spaces of all matrices in C with an identity matrix appended on the left.

The subspace decoding problem then becomes:

$$\textbf{Minimize } d_S (<x>, <y>) \textbf{ where } x \in C^* \textbf{ - (III)}$$

We can now solve the above subspace decoding problem by using a rank-metric decoder.
A solution c returned by such a decoder will give exactly a solution x = [I c] to the problem (III).

CONCLUSION

In this paper, we have established a strong connection between codes in the Grassmannian graph and codes in the Rank-Metric. This connection enables us to convert the error correction problem in random network coding into a generalized decoding problem for rank-metric codes. Thus the role of Rank-Metric codes for error correction in Random network coding has been established.

REFERENCES

[1] Y. Akwaiwa and Y.Nagata, "Highly efficient digital mobile communications with a linearmodulation method," IEEE journal on selected areas in communication, Vol. SAC-5, pp.890-895, 1987.

[2] R.W Chang, "Synthesis of band-limited orthogonal signals for multichannel data transmission," Bell system Tech.J., vol.45 , pp. 1775-1796, 1996.

[3] R.C. Bose and D.K. Ray Chaudhari, "On a class of error correcting binary group codes," Information and control, vol.3 , pp. 68-79, 1960.

[4] J.Adamek, Foundations of Coding (New York: Wiley, 1991).

[5] N. Abramson, Information Theory and Coding (New York: McGraw-Hill, 1963).

[6] J.B.Anderson and S.Mohan, Source and Channel Coding: An Algorithm Approach (Boston, Mass: Kluwer Academic,1991).

[7] J.B. Anderson, Digital Transmission Engineering (Piscataway, N.J.: IEEE Press,1999).

[8] R.B.Ash, Information Theory (New York: Wiley, 1965).

[9] E.R. Berlekamp, Algebraic Coding Theory (New York: McGraw-Hill, 1968).

[10] R.E.Blahut, Digital Transmissions of Information (Reading, Mass.: Addison-Wesley,1990).

[11] Y.Akaiwa, Introduction to Digital Mobile Communication.(New York: Wiley, 1997).

[12] G.D.Forney, M.V.Eyuboglu, "Combined equalization and coding using precoding," IEEE Communications Magazine, Vol.29, no. 12, pp.25-34,1991.

[13] J.P.Costas, "Poisson, Shannon and the radio amateur," Proceedings of the IRE, Vol.47, pp.2058-2068, 1959.

[14] V.K. Bharagava, "Forward error correction schemes for digital communications," IEEE Communications Magazine, vol.21, no.1, pp. 11-19, 1983.

[15] C.E.Shannon, "A mathematical theory of communication," Bell System Tech.J., vol.27, pp.379-423, 623-656,1948.

[16] M.J.E Golay, "Note on digital coding," Proceedings of the IRE, vol.37, p.657, 1949

[17] D.J.C Mackay, "Good error-correcting codes based on very sparse matrices," IEEE Transactions on Information Theory, vol. 45, pp. 399-431, 1999.

[18] I.M Jacobs, "Practical applications of coding," IEEE Transactions on Information Theory, vol. IT-20, pp.305-310,1974.

[19] T.A.Welch, "A technique of high performance data compression," Computer, vol.17, no.6, pp.8-19, 1984.

[20] B. Sklar, "A primer on turbo code concepts," IEEE Communications Magazine, vol.35, pp. 94-102, December 1997.