International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 4, Issue 8
August 2017

A Note on Codes Arising from the Evaluation Maps

Avinash J. Kamble
Department of Applied Sciences and Humanities,
Pillai HOC College ofEngineering and Technology, Rasayani, Panvel, Maharashtra, India.

Abstract :
The aim of this paper is to discuss the codes arising from the evaluation maps.
AMS Mathematics Subject Classification(2010) : 94B05
Keywords : Finite fields, Linear codes, Evaluation map, Evaluation code.

1. Introduction :

Coding theory is concerned with reliability of communication over noisy channel. Error-correcting codes are used in a wide range of communication systems from deep space communication, to quality of sound in a compact discs. The message to be communicated is first "encoded", i.e. turned into a codeword, by adding "redundancy". The codeword is then sent through the channel and received message is "decoded" by the receiver into a message resembling, as closely as possible, the original message. The degree of resemblance will depend on how good the code is in relation to the channel. The basic problem of coding theory is that of communication over an unreliable channel that results in errors in the transmitted message. Generally, all communication channels have errors, and thus codes are widely used.

This expository note is an attempt to give a nice sketch of constructing a vector space arising out of a function and then relate the constructed vector space for coding theory problems, via evaluation maps. Simple evaluation codes are discussed which arises from evaluation maps. The motivation stems from the simple set-theoretic considerations.

2. Pre-requisites :

In this section, we gather some basic facts required for our subsequent section.

Let X be a set, countable or finite and P be a subset of X . If P is finite, let $P=\{x_1,...,x_k\}$, for a unique integer k .If P is countable then $P=\{x_1,x_2,...\}$. By a function we mean a mapping $f:X\to K$, where K is some scalar field. In fact we are interested in fixing this K to be some finite field F_q , where $q=P^n$, for some prime P and $n>1$. Then for each i, $x_i \mapsto f(x_i)\in K$

A k-tuple $(f(x_1),...,f(x_k))\in K^k$. An evaluation map e_X is a map that evaluates all such functions f, given by $e_X(f)=(f(x_1),f(x_2),...)$. We shall construct a vector space of these functions and exploit for coding theory problems.

Definition 2.1:A code is any non-empty subset of F_q^n. The code is called linear, if it an F_q-linear subspace of F_q^n. The number n is the length of the code.

Definition 2.2:A field F is said to be finite, if it is of prime characteristic and isomorphic to Z_p, for prime $p>1$. The next class of finite fields are the fields with prime power. Generally, we denoteaprime field by F_q, for some prime power q .

International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 4, Issue 8
August 2017

From linear algebra we know that, every field F is a vector space over itself and further, if F is a vector space, then so is $F^n : \underbrace{F \times ... \times F}_{n-times}$, over F. In particular, If $F = F_q$, a finite field with prime power elements, then $F_q^n = F_q \times ... \times F_q \ (n - times)$ is a vector space over F_q

Proposition 2.3 : The finite fields F_q^m and F_q^n are isomorphic if and only if, $m = n$.

3. Vector spaces and Evaluation maps:

This section deals with the main result of this paper. Let X be topological space or a geometric object (such as smooth n-manifold or an algebraic variety).Let $K = F_q$, where $q = P^n$, for some prime $P > 1$. To this end, we construct a vector space as follows :

Let V be a vector space over F_q consisting of functions defined on X and taking values in F_q. Thus, $f \in V$ mean, $f : X \to F_q$ and the vector space operations are given by $f, g \in V \ (f + g)(x) := f(x) + g(x)$, for each $x \in X$.**(3.1.1)**

Now, for $\sim \in F_q$, $x \in X$, define $f(\sim x) := \sim \cdot f(x)$, $\forall f \in V$.**(3.1.2)**

For this X and V we define the evaluation map with respect to X, for the functions defined on V evaluated at each $x_i \in X$ as follows :

$eval_X : V \to F_q^n$, $eval_X(f) = (f(x_1),...,f(x_n))$.

Proposition 3.1: The evaluation map is linear.

Proof : Enough, if we show that, $eval_X(f + g) = eval_X(f) + eval_X(g)$

and $eval_X(\sim f) = \sim eval_X(f)$ for all $f, g \in V$ and $\sim \in F_q^n$.

From the vector space operations given by (3.1.1) and (3.1.2) . Hence, the proposition follows.

Consequently, the image of $eval_X$ is a subset of F_q^n.

Denoting $\mathrm{Im}(eval_X) = F_q^k$, this is possible, thus $F_q^k \subset F_q^n$, for $k < n$. Which implies that F_q^k and hence $\mathrm{Im}(eval_X)$ is a subspace of F_q^n, as a vector space and can be regarded as a code in F_q^n, a linear code indeed.

4. Evaluation Codes

Definition 4.1

Suppose M is a set of "functions" which acts on a set $S = \{P_1,...,P_n\}$, in the following sense : each $¤ \in M$ maps, each element P_i of P to an element of F_q. Assume that, M carries the structure of an F_q-vector space compatible with the evaluation map. In this situation, we are able to construct a $q - ary$ code of length n, which we will call an *evaluation code* via (M, S, F_q). The exact definition is as follows :

Wemap M to F_q^n via $¤ : M \to F_q^n$, $¤ \mapsto (¤(P_1),...,¤(P_n))$.

The *evaluation code*is the image of this map.

Proposition 4.1.1 : Any linear code is an evaluation code.

International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 4, Issue 8
August 2017

Proposition 4.1.2 : Let C be an evaluation code via (M, S, F_q)

i) The dimension of C is $\dim_{F_q}(M) - \dim_{F_q}(T)$, where T is the subspace of M for which all the function disappear on all the points of S.

ii) Suppose that, all $¤ \in M$ which do not identically disappear on S have the property that they have at most t zeros on S. Then the minimum distance of C is at least $n-t$.

Simple Evaluation Codes 4.2:

Consider M as the dual space of F_2^k, and S as $\{1, \mu, ..., \mu^{n-1}\}$ in F_q, where $q = 2^k$.

If S contains a basis and $n = k$, then the evaluation code is equal to F_2^k, hence trivial. We therefore assume that the elements of S generate F_q as F_2 – space and $n > k$.

Now consider the space of all "binary relations" on S. These are the set of all binary $(a_0, ..., a_{n-1})$such that $\sum_i a_i \mu^i = 0$. This vector space is the dual space of the evaluation code. In fact, if $\sum_i a_i ¤(\mu^i) = 0$ for all linear forms $¤$, then by linearity $\sum_i a_i \mu^i = 0$ and vice-versa.

Lemma 1 : Let C be the evaluation code via (M, S, F_2) as described above. Then $C^\perp$ is the set of all binary polynomials f of degree less than n, such that $f(\mu) = 0$.

Lemma 2 : Suppose that any subset S of size $(n-d+1)$ contains a basis of F_q / F_2, then the minimum distance of the evaluation code is at least d.

4. Conclusion

The present note is an attempt to give a sketch of constructing a vector space arising from a function space and then relate it to construction of codes via evaluation maps.

References

1. Cameron, P.J. and Van Lint, J.H,;*Designs, Graphs and Codes and their Links*. London Math.Soc. Student Texts, Vol. 22, Cambridge University Press, 1991.
2. Rudolf Lidl and Harald Niederreiter, *Introduction to Finite Fields and their Applications*,;Cambridge University Press, Cambridge, 1986.
3. Van Lint, J.H., *Introduction to Coding Theory*. Graduate Texts in Mathematics, Springer-Verlag, New York, 1982.
4. F. J. MacWilliam& N.J.A. Sloane, *The Theory of Error-Correcting Codes* ,(North- Holland, Amsterdam, 1978).