International Mathematical Forum, Vol. 7, 2012, no. 14, 687 - 694

Valuation and Discrete Valuation Codes

M. Hosseinyazdi and A. Ashour

Department of Mathematics
Payame Noor University
P. O. Box 19395-4697, Tehran, Iran
myazdi@spnu.ac.ir, Azam.Ashor@yahoo.com

Abstract

In this paper we defined codes over a finitely generated commutative valuation rings. First we defined field encoding and after that defined valuation code over valuation rings and discrete valuation code over discrete valuation rings.

Keywords: valuation code, discrete valuation code, valuation ring, discrete valuation, coding theory

1 Introduction and preliminaries

Over the last 70 years, algebraic coding has become one of the most important and widely applied aspect of abstract algebra. Coding theory forms the basis of modern communication systems and is the key to another area of study, Information theory, which lies in the intersection of probability and coding theory. Algebraic code are now used in essentially all hardware-level implementations of smart and intelligent machine, such as scanner, optical devices, and telecom equipment. It is only with algebraic code that we are able to communicate over long distances or are able achieve megabit bandwidth over a wireless channel. Algebraic coding is most prevalent in communication system and has been developed and engineered because of one inescapable fact of communication: noise. Noise will always be a part of communications and has the potential to corrupt data and voice due to its presence. Noise, comes from practically an infinite number of sources, from cosmic background radiation (affecting space based communication), from an inductive motor in a vending machine down the hall, and can even be generated by the user, themselves by induced signal reflections in the environment. The implications of destructive interference in communication is obvious: mission critical communique, potentially could not be trusted and decision based on those communications could not be made. (see [1])

One can recourse [2, 3, 4], for more information about category algebra coding, cryptography and their applications.
In this paper we will introduce valuation codes. These codes use valuation ring and discrete valuation ring.
In Section 2, we start, with a description of basic algebra, definition of a valuation ring ,discrete valuation and discrete valuation ring.

In section 3, we will define a code from a field encoding over valuation ring and present some theorem in this topic. These codes are called valuation codes.

In section 4, we will define a code from a valuation ring encoding over discrete valuation and give some theorem. These codes are called discrete valuation codes.

2 Valuation and Discrete Valuation Rings

In this section we give some basic, necessary definitions and results on valuation ring. For further details of valuation ring and related algebra, see [5].

Definition 2.1. *Let R be an integral domain. R is a valuation ring if every element x of its field of fraction K satisfies:*

$$x \notin R \Rightarrow x^{-1} \in R$$

Theorem 2.2. *Suppose R is a valuation ring. Then, for any two ideal I, J of R either $I \subset J$ or $J \subset I$.*

Proof:
Suppose $I \not\subseteq J$. Then, there exists $x \in I$ such that $x \notin J$. Hence, for any $0 \neq y \in J$ we have $x/y \notin R$. Otherwise, $x = y(x/y) \in J$; is a contradiction. So, $y/x \in R$ and $y = x(y/x) \in I$. Therefore, $J \subset I$. ■

Note that, the set of all ideals of R form a totally order set, by Theorem 2.2. In particular, R has only one maximal ideal. So, R is a local ring. We denote the unique maximal ideal of R by m. It is easy to verify that, $K \diagdown R = \{x \in K^* | x^{-1} \in m\}$, where K^* is the multiplicative group $K \backslash \{0\}$ (see [5]). Thus, R is determined by K and m.
If R is valuation ring of field K, then any ring R' with $R \subset R' \subset K$ is obviously also a valuation ring. (See [5].)

Definition 2.3. *Let K be a field, $K^* = K \backslash \{0\}$ be the multiplicative group of K and $\mathbb{Z}$ be the set of integer numbers. The extender map $\nu : K^* \to \mathbb{Z}$ is*

called a discrete valuation of K, if it satisfies the following conditions:
1. $\nu(xy) = \nu(x) + \nu(y)$
2. $\nu(x + y) \geq min\{\nu(x), \nu(y)\}$
One can show easily the set $\sum = \{x \in K^* | \nu(x) \geq 0\} \bigcup \{0\}$ is a valuation ring over the field K(See [5]).

Remark 2.4. *(i) If we add the condition*

$$\nu(x) = \infty \Leftrightarrow x = 0$$

to conditions of Definition 2.3, we can extend ν from K onto $\mathbb{Z}$. Therefore

$$\Sigma = \{x \in K | \nu(x) \geq 0\}$$

and it is called the valuation ring of ν.
(ii) For each discrete valuation ν, we have $\nu(1) = \nu(1.1) = \nu(1) + \nu(1)$. So, $\nu(1) = 0$.

Definition 2.5. *If P is a prime ideal of R, then the length of a chain*

$$P = P_0 \supsetneqq P_1 \supsetneqq ... \supsetneqq P_n$$

going down from P, of proper inclusions of prime ideals, is shown by, $ht(P) = n$. The Krull dimension of R, is denoted by K-dim(R), and is defined as $sup(ht(P))$, where supermum is taken over all prime ideals of R.

Definition 2.6. *Suppose R is an integral domain. Then, R is a discrete valuation ring, if there exists a discrete valuation ν from quotient field $K = S^{-1}R$ ($S = R \diagdown \{0\}$) on to $\mathbb{Z}$ (the set of all integers) such that R is the valuation ring of ν. Hence, $R = \{x \in K : \nu(x) \geq 0\}$.*

Theorem 2.7.([5]) *Suppose R is a discrete evaluation ring with discrete evaluation ν of its quotient field $K = S^{-1}R$ $(S = R\backslash\{0\})$ on to Z. Then :*
1. R is a local ring with maximal ideal $m = \{x \in K | \nu(x) > 0\}$.
2. If $x, y \in R$ and $\nu(x) = \nu(y)$, then the ideal generated by x and the ideal generated by y are equal, i.e., $< x >=< y >$.
3. If I is a non-zero ideal of R, then there exists an integer k and $x \in I$ such that $\nu(x) = k$. Thus, $y \in R$ and $\nu(y) \geq k$ implies $y \in I$, i.e., $I = \{y \in R | \nu(y) \geq k\}$.
4. There exists $x \in m$ such that $\nu(x) = 1$, $m =< x >$ and if $m_k = \{y \in R | \nu(y) \geq k\}$ then $m_k =< x^k >$ for some $k \geq 1$.
5. m is the unique non-zero prime ideal of R.

Theorem 2.8. *Let R be a discrete valuation ring. For ever $x \in R$, $\nu(x) = 0$ if and only if x is unit in R.*

Proof:
Suppose $\nu(x) = 0$. Thus, $x \notin m$ ($m = \{x \in K|\nu(x) > 0\}$). Hence, $x \in R\diagdown m$, by Theorem 2.8. Since R is a local ring, x is unit in R.
Conversely, suppose x is unit in R, then $x, x^{-1} \in R$. We know $\nu(1) = \nu(1.1) = \nu(1) + \nu(1)$ Thus $\nu(1) = 0$. Now, $\nu(1) = \nu(xx^{-1}) = \nu(x) + \nu(x^{-1}) = 0$. Then, $\nu(x) = -\nu(x^{-1})$. As, $x, x^{-1} \in R$, $\nu(x) = \nu(x^{-1}) = 0$. ■

Theorem 2.9.([5]) *Suppose R is a local integral domain with $dimR = 1$. Also, let m be the maximal ideal of R and $K = R/m$ be the quotient field of R. Then, the following conditions are equivalent:*
1. R is integrally closed.
2. R is a PDI.
3. R is discrete valuation ring.

3 Valuation Codes

In this section we defined valuation codes over finitely generated valuation ring.
Suppose R generated by $S = \{r_1, ..., r_n\}$. Then, for each $r \in R$ there exists $a_i \in R$ $(1 \leq i \leq n)$ such that $r = \sum_{i=1}^{n} a_i r_i$. Now, we define $\underline{r} := (a_1, ..., a_n)$.

Definition 3.1. *Let R be a valuation ring, generated by $S = \{r_1, ..., r_n\}$, $K = S^{-1}R, (S = R\diagdown\{0\})$. Also, let A be a subset of K and $r \in K$ be given. A " field encoding" is mapping $f_r : A \to K$ such that $f_r(x) = rx$.*

A code ζ is the image of a field encoding; i.e, for a given $r \in K$, $\zeta_r = \{f_r(x)|x \in A\}$. Suppose R is valuation ring, then R is integral domain and $S = R\diagdown\{0\}$. Therefore $S^{-1}R$ includes R.
Let R be a finitely generated valuation ring and $A = R$ in Definition 3.1. Then,

$$\zeta_r = \{rx|x \in R\}$$

Also, we can consider A as an ideal of R. Thus, $\zeta_r = \{rx|x \in I\}$.

Theorem 3.2. *Suppose R is a finitely generated valuation ring , I is an ideal of R , $A = I$ in Definition 3.1 and $\zeta_r = \{rx|x \in I\}$. Then ζ_r is an ideal of R.*

proof:
Note that, for all $t_1, t_2 \in \zeta_r$ there exist $x_1, x_2 \in I$ such that $t_1 = rx_1$ and $t_2 = rx_2$. Hence, $t_1 + t_2 = rx_1 + rx_2 = r(x_1 + x_2)$ and $I \trianglelefteq R$, we have $t_1 + t_2 \in \zeta_r$
Also, for all $t \in \zeta_r$ and $s \in R$ there exists $x \in I$ such that $t = rx$. Hence,

$st = srx = rsx$ and $sx \in I$ implies $st \in \zeta_r$. So, ζ_r is an ideal of R. ■

Theorem 3.3. *Suppose R is a finitely generated valuation ring , I and J are two ideals of R, $\zeta_{1_r} = \{rx|x \in I\}$ and $\zeta_{2_r} = \{rx|x \in J\}$. Then $\zeta_{1_r} \subset \zeta_{2_r}$ or $\zeta_{2_r} \subset \zeta_{1_r}$.*

proof:
Suppose I, J are two ideals of R. Then, ζ_{1_r}, ζ_{2_r} are two ideal of R, by Theorem 3.2. Hence, $\zeta_{1_r} \subset \zeta_{2_r}$ or $\zeta_{2_r} \subset \zeta_{1_r}$, by Theorem 2.2. ■

Definition 3.4. *Let R be a valuation ring, P be a prime ideal of R and $A = P$ in Definition 3.1. Then $\zeta_r = \{rx|x \in P\}$ is called prime code.*

Definition 3.5. *Let R be a ring and I be an ideal of R. The radical of I is denoted by $r(I)$ or $\sqrt{I}$, and defined as follows:*

$$r(I) = \sqrt{I} = \{a \in R|a^n \in I \ for \ some \ n > 0\}$$

Note that, $r(I)$ is an ideal of R.

Theorem 3.6. *Suppose R is a finitely generated valuation ring and I is proper ideal of R. Then $\zeta_r = \{rx|x \in r(I)\}$ is a prime code, where $r(I)$ is the radical of I.*

proof:
Suppose, I is a proper ideal of R. For all $ab \in r(I)$, there exists $n \in N$ such that $a^n b^n \in I$. We have $Ra \subseteq Rb$ or $Rb \subseteq Ra$. If $Ra \subseteq Rb$ then $b^{2n} \in Rb^n Rb^n \subseteq Ra^n Rb^n = Ra^n b^n$. Thus, $b \in r(I)$. If $Rb \subseteq Ra$ then, in the same way, $a \in r(I)$. Therefore, $r(I)$ is prime ideal of R. Hence ζ_r is a prime code. ■

4 Discrete Valuation Codes

In this section we define discrete valuation code, when $A = \Sigma$ in Definition 3.1, $\zeta_r = \{rx|x \in \Sigma\}$ is discrete valuation code. (Σ as Definition 2.3).

Theorem 4.1. *If ζ_r is a discrete valuation code then, $\zeta_r = \{rx|\nu(x) \geq 0\}$.*
Proof:
We know $\Sigma = \{x \in K|\nu(x) \geq 0\}$. Clearly, $\zeta_r = \{rx|\nu(x) \geq 0\}$. ■

Theorem 4.2. *Suppose $\nu(x) = \nu(y)$. Then we have:*

$$\{f_r(z)|z \in < x >\} = \{f_r(z)|z \in < y >\}$$

Proof:

It is clear by Theorem 2.7(2). ■

Theorem 4.3. *Suppose m is a maximal ideal of Σ. If $A = m$ in Definition 3.1 and $\zeta_r = \{rx|x \in m\}$ is prime a code then, $\zeta_r = \{rz|\nu(z) \geq 1\}$.*

Proof:
It is sufficient to show $m =< x >= \{y \in \Sigma|\nu(y) \geq 1\}$. Let $m' = \{y \in \Sigma|\nu(y) \geq 1\}$. Now, we show $m' =< x >$.
For each $y \in< x >$, there exists $t \in \Sigma$ such that, $y = tx \in m$. Thus, $\nu(tx) = \nu(t) + \nu(x) \geq 1$. Then, $< x >\subseteq m'$. On the other hands, for each $y \in m'$ there exists k such that, $\nu(y) = k \geq 1$. Also, we know that, $\nu(x^k) = k$. Then, $< y >=< x^k >$. Therefore, there exists $s \in \Sigma$ such that $y = sx^k$ which implies $y \in< x >$. So, $m' =< x >$. Now, it is clear that $\zeta = \{rz|\nu(z) \geq 1\}$.■

Theorem 4.4. *Let m_k be the ideal of Σ as in Theorem 2.7(4) and $\zeta_r = \{ry|y \in m_k\}$. Then, there exist $x \in \Sigma$ and $k \in Z$ such that $\zeta_r = \{ry|y \in< x^k >\} = \{ry|\nu(y) \geq k\}$.*

Proof:
It is clear by Theorem 2.7(4). ■

Theorem 4.5. *Suppose R is a valuation ring of its field of fractions K and $\zeta_r = \{rx|x \in K\}$. Then, $\zeta_r = \{rx|x \in R\} \bigcup \{rx|x \in R^{-1}\}$.*
Proof:
If we consider R^{-1} as the set of inverses of all non-zero elements of R, then $R \bigcup R^{-1} = K$. (See [5]). Therefore, $\zeta_r = \{rx|x \in R\} \bigcup \{rx|x \in R^{-1}\}$.■

Corollary 4.6. *Suppose R is an integral domain , $K = S^{-1}R$ ($S = R \setminus \{0\}$) and Σ the valuation ring of ν. Then, $\zeta_r = \{rx|x \in \Sigma\} \bigcup \{rx|x^{-1} \in \Sigma\}$.*

Proof:
It is clear by Theorem 4.5. ■

Theorem 4.7. *Let $\zeta_r = \{rx|x \in \Sigma\}$ and $\zeta_r^{-1} = \{rx|x^{-1} \in \Sigma\}$. Then*

$$\zeta_r \bigcap \zeta_r^{-1} = \{rx|x \quad is \quad unit\}$$

Proof:
For all $t \in \zeta_r \bigcap \zeta_r^{-1}$ there exist $x \in \Sigma$ and $y \in \Sigma$ such that $t = rx$ and $t = ry^{-1}$. Thus, $rx = ry^{-1}$ which implies $\nu(rx) = \nu(ry^{-1})$. Hence, $\nu(r) + \nu(x) = \nu(r) + \nu(y^{-1})$. Therefore, $\nu(x) = \nu(y^{-1})$. Then, 0$= \nu(x) - \nu(y^{-1}) = \nu(x) + \nu(y) = \nu(xy)$. Thus, by Theorem 2.8, xy is unit. Then x and y are units. ■

Corollary 4.8. *Let $\zeta_r = \{rx|x \in \Sigma\}$ and $\zeta_r^{-1} = \{rx|x^{-1} \in \Sigma\}$. Then*

$$\zeta_r \bigcap \zeta_r^{-1} = \{rx|\nu(x) = 0\}.$$

Theorem 4.9. *If ν is a discrete valuation of field K and $\alpha_1, ..., \alpha_n \in K$ such that $\alpha_1 + ... + \alpha_n = 0$ then, there exist two indices i, j such that $i \neq j$ and $\zeta_i = \zeta_j$ where, $\zeta_i = \{rx|x \in <\alpha_i>\}, \zeta_j = \{rx|x \in <\alpha_j>\}$.*

Proof:
It is sufficient, to show there exist indices i and j such that $i \neq j$ and $\nu(\alpha_i) = \nu(\alpha_j)$. Suppose, for each i, j, $\nu(\alpha_i) \neq \nu(\alpha_j)$. Let $\nu(\alpha_j) = min\{\nu(\alpha_1), ..., \nu(\alpha_n)\}$. For each $i \neq j$; if $\nu(\alpha_i) \neq \nu(\alpha_j)$ then, $\nu(\alpha_i + \alpha_j) = min\{\nu(\alpha_i), \nu(\alpha_j)\}$. (see [5]). Hence,

$$\nu(0) = \nu(\alpha_1 + ... + \alpha_n) = min\{\nu(\alpha_1), ..., \nu(\alpha_n)\} = \nu(\alpha_j)$$

Thus, $\infty = \nu(\alpha_j)$. Then, $\nu(\alpha_1) = ... = \nu(\alpha_n) = \nu(\alpha_j)$. It is contradiction with $\nu(\alpha_i) \neq \nu(\alpha_j)$. Then, there exist indices i and j such that $i \neq j$ and $\nu(\alpha_i) = \nu(\alpha_j)$. Now it follows by Theorem 4.2.■

5 Conclusion

In this paper we investigate each code from an ideal of discrete valuation ring R, is generated by $x^k \in R$ such that $\nu(x) = 1$, $k \in \mathbb{Z}$. Therefore, these codes can use in cyclic codes such as BCH, Hamming and Reed-Solomon. By this method, we can consider, the code $\zeta = \{rx|\nu(x) \geq k\}$, for each $k \in \mathbb{Z}$. This code, is generated by x^k such that $\nu(x) = 1$ and we can generate equivalent codes by this method.

References

[1] A. Attarian, A.Hutzel, R. Neal, Algebraic coding theory, MA 407, pp 1-12, 2006.

[2] P. Elias, Error -correcting codes for list decoding, IEEE Transactions on Information Theory, 37(1991), 5-12.

[3] A. Goldaste et. all, An introduction to the fundamentals of encription, Publications of education , reserch institute of defence industries, 1999.

[4] P. Hurey, Codes from zero-divisore and unit in group ring, Int. J. information and coding theory, 1(2009), 57-58.

[5] H. Matsumura, Commutative ring theory, Department of Mathematics, Faculty of Sciences Nagoya University Nogoya Japan, 1980.

[6] V. S. Pless, and W. C. Huffman, Handbook of coding Theory, North Holland, 1998.

Received: September, 2011