Smith Normal Form – a possible basis for an SVD – like code construction?

(Semester Project I)

Name: **Abdul Wakeel**

Majors: **Communication Systems and Electronics**

Supervisor: **Prof. Dr. Werner Henkel**

Semester: **Fall 2008**

Institute: **Jacobs University Bremen, Germany**

Contents

Chapter 1

Introduction

RS codes can be defined using a DFT matrix which is known to diagonolize a Toeplitz matrix. This property is commonly used in multi-carrier modulation, since the channel realises a convolution which can be represented by a Toeplitz matrix. A more general diagonolization for parallel decomposition of a channel is provided by SVD. The question is now, if there is another way to obtain a discrete code construction other than SVD what would be the properties of such a code, especially if it guarantees a certain minimum Hamming distance? In order to check for another option , the so-called Smith Normal Form (Invariant Factor Theorem) is considered. Similar to Singular Value Decomposition, the Smith Normal Form is used to decompose a matrix into two unimodular matrices and a diagonal matrix. However, such type of diagonolization is different from the one provided by the Singular Value Decomposition. Elementary row and column operations are used to diagonolize a matrix. The aim of this project is to study the properties of the unimodular matrices, and the possibility of a code construction using the Smith Normal Form.

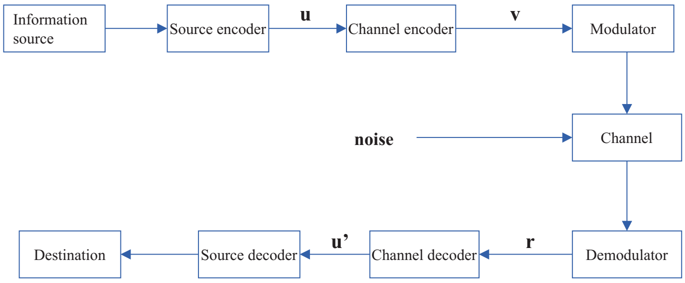
This report is structured as follow. Chapter **2** contains a brief introduction to some topics related to the project. In Chapter **3** the Smith Normal Form is described in detail along with some examples of integer matrix diagonolization. The results of the project are finally summed up as conclusions at the end of this report.

Chapter 2

Diagonolization in coding and transmission systems

This chapter will provide an overview of basic coding definitions and the distance measure called *metrics*. RS codes can be defined using a DFT matrix which is known to diagonolize a Toeplitz matrix. This property is commonly used in multi-carrier modulation, since the channel realises a convolution which can be represented by a Toeplitz matrix. The channel for multi-carrier (OFDM) systems with circular convolution is diagonolized with discrete Fourier transform. In similar way, a more generalised diagonolization for parallel decomposition of Multiple Input Multiple Output (MIMO) channel is provided by singular value decomposition, resulting in pre and post processing unitary matrices. A similar decomposition of matrix can also be obtained with the so-called Smith Normal Form.

2.1 Transmission system model



Block diagram of Transmission System Model

As shown in the figure [8], the *information source* may either be a person or a machine. The *Source encoder* transforms the source output into binary dig-

its called the information sequence *u*. The*Channel encoder* transforms the information sequence *u* into a discrete encoded sequence *v* called a code-word. The *modulator* transforms each output symbols of the channel encoder into a waveform suitable for transmission. This waveform enters the *channel* and is corrupted by noise. The channel may either be wireless or wire-line.
The *demodulator* processes each received waveform and results in either a discrete or a continuous valued output. The sequence of demodulator outputs corresponding to sequence *v* is called the received sequence *r*. The *channel decoder* transforms the received sequence *r* into a binary sequence *u'* called the estimated information sequence. The *source decoder* transforms the estimated information sequence *u'* into an estimate of the source output and delivers this estimate to the *destination.*

2.2 Metrics

In mathematics, *metric* is a function which defines a distance between elements of a set. The same term has been applied to the coding theory in a similar way. Different distance functions are used in coding theory:

- Euclidean distance,
- Hamming distance.

The *Euclidean distance* d_E [7] between two vectors a and b of length n with components a_i, b_i is given by

$$d_E^2 = \sum_{i=0}^{n=1} (a_i - b_i)^2 \tag{2.1}$$

The *Hamming distance* d_H [7] between two vectors a and b of length n with components a_i and b_i that may be elements of an arbitrary number field, are given as the number of different components,

$$d_H = |M| \qquad \text{of the set M} = \{j|a_j \neq b_j\} \ . \tag{2.2}$$

Definition:*Hamming weight*. The Hamming weight w_H of a vector is the number of non-zero components [7], i.e.,

$$w_H = |M| \qquad \text{with M} =\{j \ |a_j \neq 0\} \ . \tag{2.3}$$

2.3 Discrete Fourier Transform

Let $x[n]$, $0 \leq n \leq N-1$, denotes a discrete time sequence. The N-point DFT of $x[n]$ is defined as [10]

$$DFT\{x[n]\} = X[i] = \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} x[n] e^{-j\frac{2\pi n i}{N}} \ , \quad 0 \leq i \leq N-1 \ . \tag{2.4}$$

The sequence $x[n]$ can be recovered from its DFT using the IDFT:

$$IDFT\{X[i]\} = x[n] = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} X[i] e^{j\frac{2\pi n i}{N}} \ , \quad 0 \leq n \leq N-1 \ . \tag{2.5}$$

For convenience (matrix representation) the formula's derived for DFT and IDFT can also be written as

$$X[i] = \sum_{n=0}^{N-1} x[n] W^{in} \ , \quad \text{where } i = 0, 1, \ldots\ldots, N-1 \ . \tag{2.6}$$

$$x[n] = \frac{1}{N} \sum_{n=0}^{N-1} X[i] W^{-in} \ , \quad \text{where } n = 0, 1, \ldots\ldots, N-1 \ . \tag{2.7}$$

where by definition

$$W = e^{\frac{-j2\pi}{N}}$$

The DFT is widely used in digital signal processing and related fields to analyse the frequency contents in a sampled signal, to solve partial differential equation and to perform other operations such as fast convolution . The matrix representation (Vandermonde) of DFT is given by

$$\mathbf{W} = 1/\sqrt{N} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & W & W^2 & \ldots & W^{N-1} \\ 1 & W^2 & W^4 & \ldots & W^{2(N-1)} \\ \vdots & \ddots & \ddots & \ldots & \ldots \\ 1 & W^{N-1} & \ldots & \ldots & W^{(N-1)(N-1)} \end{pmatrix} \tag{2.8}$$

$\mathbf{W}$ is a symmetric matrix.

2.4 Orthogonal Frequency Division Multiplexing (OFDM) and Diagonolization of a Toeplitz matrix.

Orthogonal Frequency Division Multiplexing (OFDM) decomposes the wideband channel into a set of narrow band orthogonal sub-channels with a different QAM symbol sent over each sub channel. Let $X[N] = (X[0], X[1], \ldots, X[N-1])$ be the input data stream. After IFFT and cyclic prefix addition, the input data is $\tilde{x}[n]$=$\tilde{x}[-\mu], \ldots, \tilde{x}[N-1]$ =$(x[N-\mu], \ldots, x[0], \ldots, x[N-1])$. This input data is filtered by the channel impulse response $h(n)$ and corrupted by additive noise n, so that the received signal is $y(t) = \tilde{x}(n) * h(n) + n$. Denote the nth element of these sequences as $h_n = h[n]$, $\tilde{x_n} = \tilde{x}[n]$, and $y_n = y[n]$. The channel output can be written as

$$\mathbf{y} = \mathbf{H}\mathbf{x} + \mathbf{n} \ . \tag{2.9}$$

The received symbols $y_{-1}, \ldots, y_{-\mu}$ are affected by ISI from the prior data block and are discarded. The last μ symbols of $x[n]$ correspond to the cyclic prefix. From this, the received symbols in matrix form can equivalently be written as [10]

$$\begin{pmatrix} y_{N-1} \\ y_{N-2} \\ \vdots \\ \vdots \\ \vdots \\ y_0 \end{pmatrix} = \begin{pmatrix} h_0 & h_1 & \ldots & h_\mu & 0 & \ldots & 0 \\ 0 & h_0 & h_1 & \ldots & h_{\mu-1} & \ldots & 0 \\ \vdots & \vdots & \ddots & & & \ddots & \vdots \\ 0 & \ldots & 0 & h_0 & h_1 & \ldots & h_\mu \\ \vdots & \vdots & \ddots & & & \ddots & \vdots \\ h_2 & h_3 & \ldots & h_{\mu-2} & \ldots & h_0 & h_1 \\ h_1 & h_2 & \ldots & h_{\mu-1} & \ldots & 0 & h_0 \end{pmatrix} \begin{pmatrix} x_{N-1} \\ x_{N-2} \\ \vdots \\ \vdots \\ x_0 \end{pmatrix} + \begin{pmatrix} n_{N-1} \\ n_{N-2} \\ \vdots \\ \vdots \\ n_0 \end{pmatrix} . \tag{2.10}$$

we abbreviate

$$\mathbf{y} = \tilde{H}\mathbf{x} + \mathbf{n} , \tag{2.11}$$

where $\tilde{H}$ is $N \times N$ circulant convolution channel matrix over the N samples. This channel matrix $\tilde{H}$ has the eigenvalue decomposition

$$\tilde{H} = M\Lambda M^H ; \tag{2.12}$$

where Λ is the diagonal matrix with eigenvalues of $\tilde{H}$ and M^H is a unitary matrix whose rows comprise the eigenvectors of $\tilde{H}$. The DFT operation on $x[n]$ can be represented by matrix multiplication as

$$X = W_N x ; \tag{2.13}$$

where $X = (X[0], X[1], \ldots, X[N-1])^T$, $x = (x[0], x[1], \ldots, x[N-1])^T$ and W_N is the Vandermonde DFT matrix. Moreover,

$$W_N^{-1} = W_N^H . \tag{2.14}$$

The IDFT can be similarly represented as

$$x = W_N^H X . \tag{2.15}$$

Let $\mathbf{v}$ be the eigenvector of $\mathbf{H}$ with eigenvalue λ. Then

$$\lambda\mathbf{v} = \mathbf{H}\mathbf{v} ; \tag{2.16}$$

The unitary matrix M^H has rows that are the eigenvectors of $\mathbf{H}$, i.e., $\lambda_i m_i^T {=} H m_i^T$ for $i = 0, 1, \ldots, N-1$, where m_i denotes the ith row of M^H. Moreover $W_N = M^H$ and $W_N^H = M$. Thus, we have [10]

$$\begin{aligned} Y &= W_N \, y \qquad (2.17) \\ &= W_N[\tilde{H}x + n] \\ &= W_N[\tilde{H}W_N^H X + n] \end{aligned}$$

$$
\begin{aligned}
&= W[M\lambda M^H W_N^H X + n] \\
&= WM\lambda M^H W_N^H X + Wn \\
&= M^H M\lambda M^H M X + W_N n \\
&= \lambda X + W_N n
\end{aligned} \tag{2.18}
$$

since W_N is unitary, $W_N n$ is still white and Gaussian with unchanged average noise power.

2.5 Reed-Solomon Codes

A *Reed-Solomon (RS) code* [6] of length N and minimum Hamming distance d_{Hm} is a set of vectors, whose components are the values of a polynomial $C(x)$ of degree $\leq K-1 = N - d_{Hm}$ at the positions z^j,with z being an element of order N from an arbitrary number field, i.e., $z \in \mathrm{GF}(P^m)$, $z^N = 1$, $z^j \neq 1$ for $0 < j < N$.

$$c = (c_0, c_1, \ldots, c_{N-1}), c_j = C(x = z^j)\ . \tag{2.19}$$

Let us consider the polynomial $C(x)$ to be full degree $N-1$ then the polynomial at positions z^j can well be formulated using the discrete Fourier transform

$$c_j = C(x = z^j) = \sum_{k=0}^{N-1} C_k z^{jk}\ . \tag{2.20}$$

Theorem Let $C(x)$ be a polynomial of degree $K-1 = N-M-1$ with arbitrary coefficients from a field $\mathbf{F}$. If we compute the values of the polynomial at N different positions $x = x_j$, $x_j \in \mathbf{F}$, $j = 0, 1, \ldots, N-1$. The vectors of N samples have minimum weight $w_{Hm} = M+1 = N-K+1$ [6]. Moreover sum of two such vectors is equivalent to the sum of the corresponding polynomial coefficients, the sum of vectors fulfil the degree limitation, too. Thus, it is a linear code. The minimum distance is equal to the minimum weight.
Theorem: A polynomial $C(x) = C_0 + C_1 x + C_2 x^2 + \ldots + C_{K-1} x^{K-1}$ of degree $K-1$ has at most $K-1$ different roots x_j [6].
Definition A *Maximum Distance Separable* code fulfils the Singleton bound ($d_{Hm} \leq M+1 = N-M+1$) with equality [7].
Let us recall some important properties of the discrete Fourier transform especially the convolution and shift properties. In the Galois field, replacing x by a power of an element of order N, i.e., x has the property $x^N = 1$. This allows to compute $\mathrm{mod}(x^N - 1)$, i.e., x^N can be replaced by 1.

Consider two polynomials $a(x)$ and $b(x)$. The multiplication of $a(x)$ and $b(x)$ under $\mathrm{mod}(x^N-1)$ is

$$(a_0+a_1x+\ldots+a_{N-1}x^{N-1}).(b_0+b_1x+\ldots+b_{N-1}x^{N-1}) = (c_0+c_1x+\ldots+c_{N-1}x^{N-1}) \tag{2.21}$$

$$c_0 = b_0a_0 + b_1a_{N-1} + b_2a_{N-2} \ldots + b_{N-1}a_1$$

$$c_1 = b_0a_1 + b_1a_0 + b_2a_{N-1} \ldots + b_{N-1}a_2 \ ,$$

$$\vdots$$

$$cj = \sum_{l=0}^{N-1} b_l \cdot a_{j-l \bmod N} \ . \tag{2.22}$$

The result obtained is the cyclic convolution of the coefficients of vector a and b [7], i.e.,

$$a \star b \equiv a(x) \cdot b(x)\mathrm{mod}(x^N - 1) \ . \tag{2.23}$$

From the cyclic convolution and shift theorem (minimum distance is preserved) in DFT domain, RS codes can be reformulated as
Definition *Reed-Solomon (RS) code* [6] of length N and minimum Hamming distance d_{Hm} is a set of vectors, whose components are the values of a polynomial $C(x) = x^j \cdot C^{'}(x)$ of degree $\{C^{'}(x)\} \leq K - 1 = N - d_{Hm}$ at position z^k with z being and element of order N from an arbitrary number field.

$$c = (c_0, c_1, \ldots, c_{N-1}), c_j = C(x = z^j) \ , \tag{2.24}$$

where N and K mean the length of the code-word and the number of information symbols, respectively.

2.5.1 Encoding of RS-codes in DFT domain

Let K be the information, then this information can be put into $K = N - 2t$ subsequent positions in DFT domain.We write the IDFT as a matrix operation.

$$\mathbf{c} = C. \begin{pmatrix} 1 & 1 & 1 & 1 & \ldots \\ 1 & z^1 & z^2 & z^3 & \\ 1 & z^2 & z^4 & z^6 & \\ 1 & z^3 & z^6 & z^9 & \\ \vdots & & & & \ddots \end{pmatrix} \tag{2.25}$$

Let the information be C $= (I_0, I_1, \ldots, I_{K-1}, 0, \ldots, 0)$. This yields the set of linear equations [6]

$$\mathbf{c} = (I_0, I_1, \ldots, I_{K-1}) \begin{pmatrix} 1 & 1 & 1 & 1 & \ldots & 1 \\ 1 & z^1 & z^2 & z^3 & \ldots & z^{N-1} \\ 1 & z^2 & z^4 & z^6 & \ldots & z^{2(N-1)} \\ 1 & z^3 & z^6 & z^9 & & \vdots \\ \vdots & & & & \ddots & \vdots \\ 1 & z^{K-1} & z^{2(K-1)} & z^{3(K-1)} & \ldots & z^{(N-1)(K-1)} \end{pmatrix} \tag{2.26}$$

Since the DFT differs from the IDFT only in the factor of N^{-1} and the sign on the exponent of the element of order N, the same matrix description applies also to C_j=$N^{-1} \cdot c(x = z^{N-j})$

Let us now consider code properties in terms of the minimum Hamming distance from a matrix viewpoint. The usual matrix perspective would be to consider the maximum number of linearly independent columns in the parity check matrix. Since parity-check and generator matrices of an RS code are DFT matrices, the number of linearly independent columns of the $M \times N$ parity-check matrix is M, leading to a minimum Hamming distance of $M + 1$. Conversely, one can also consider the generator matrix in the following small example.

$$\left(\begin{array}{ccccc} 1 & 1 & 1 & 1 & 1 \\ 1 & z^1 & z^2 & z^3 & z^4 \\ 1 & z^2 & z^4 & z^6 & z^8 \\ \hline 1 & z^3 & z^6 & z^9 & z^{12} \\ 1 & z^4 & z^8 & z^{12} & z^{16} \end{array}\right) \tag{2.27}$$

$=(\underbrace{00 \neq 0}_{K} | \underbrace{\neq 0 \neq 0}_{M})$ which shows that we will only be able to force two position to zero leaving a weight of 3.

Theorem: Any minor $|F|$ of any size $K \times K$ of an $N \times N$ Fourier (DFT) matrix W with components $W_{k,i} = z^{ik}$, where z $= e^{\pm j2\pi/N}$ and adjacent rows (or columns) is non-zero [6].

Proof: Such a minor is given by

$$\mathbf{det}(\mathbf{F}) = |\mathbf{F}| = \begin{vmatrix} z^{k_1 l} & z^{k_2 l} & \ldots & z^{k_{K-1} l} \\ z^{k_1(l+1)} & z^{k_2(l+2)} & \ldots & z^{k_{K-1}(l+1)} \\ \vdots & \ddots & & \vdots \\ z^{k_1(l+k-1)} & z^{k_2(l+K-1)} & \ldots & z^{k_{K-1}(l+K-1)} \end{vmatrix}$$

$$= z^{k_1 l + k_2 l \ldots + k_{K-1} l} . \begin{vmatrix} 1 & 1 & \ldots & 1 \\ z^{k_1} & z^{k_2} & \ldots & z^{k_{K-1}} \\ \vdots & \ddots & & \vdots \\ z^{k_1(k-1)} & z^{k_2(K-1)} & \ldots & z^{k_{K-1}(K-1)} \end{vmatrix}$$

$$= z^{k_1 l + k_2 l \ldots + k_{K-1} l} . \prod_{i<l\leq(K-1)} (z^{kl} - z^{ki}) \neq 0. \tag{2.28}$$

The last step follows from the well-known determinant of a Vandermonde matrix. Moreover, the non-singularity of the considered submatrices ensures that at most $K-1$ zeros can be achieved, leaving at least $N-K+1$ non-zero values in the time domain, which is then the minimum Hamming weight and the minimum Hamming distance (linearity).
OFDM makes use of an IFFT and a cyclic prefix (CP) addition at the transmitter and a (CP) elimination and an FFT at the receiver. The CP, which is used for inter-symbol interference cancellation makes the channel convolution to appear cyclic and the IFFT/FFT pair diagonolizes the channel. Practically, usually some consecutive carriers are left unused, thereby realising an analog RS code.

2.6 MIMO systems, Diagonolization of MIMO systems by Singular Value Decomposition.

Multiple Input Multiple Output systems use multiple transmitters and multiple receivers for transmission and reception, respectively. Consider a MIMO system consisting of M_t transmit and M_r receive antennas respectively. Let $h_{11}, h_{12} \ldots, h_{M_r M_t}$ be the channel gains from transmit antenna M_t to receive antenna M_r. Let $x_1, x_2, \ldots, x_{Mt}$, are M_t-dimensional transmit symbols. These symbols, when transmitted over the channel, are filtered by $h_{11}, h_{12}, \ldots, h_{M_r M_t}$ the channel impulse responses, and corrupted by noise modelled to occur at the receiver. If $n_1, n_2, \ldots, n_{Mr}$ are the noise samples at the receiver, then in matrix form the channel output is [10]

$$\begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_{Mr} \end{pmatrix} = \begin{pmatrix} h_{11} & h_{12} & \ldots & h_{1Mt} \\ h_{21} & h_{22} & \ldots & h_{2Mt} \\ \vdots & & \ddots & \vdots \\ h_{Mr1} & h_{Mr2} & \ldots & h_{MrMt} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_{Mt} \end{pmatrix} + \begin{pmatrix} n_1 \\ n_2 \\ \vdots \\ n_{Mr} \end{pmatrix} \tag{2.29}$$

In more compact form we write

$$\mathbf{y} = \mathbf{H}\ \mathbf{x} + \mathbf{n}. \tag{2.30}$$

where $\mathbf{H}$ is the $M_r \times M_t$ channel gain matrix, $\mathbf{x}$ and $\mathbf{y}$ are M_t and M_r dimensional column vectors.The channel gain matrix $H_{M_r M_t}$ can be decomposed using Singular Value Decomposition (SVD), in the form

$$H = UDV^H \tag{2.31}$$

where the $M_r \times M_r$ matrix $\mathbf{U}$ and the $M_t \times M_t$ matrix $\mathbf{V}$ are unitary matrices and $\mathbf{D}$ is an $M_r \times M_t$ diagonal matrix with singular values δ_i of $\mathbf{H}$. These singular values δ_i have the property that $\delta_i = \sqrt{\lambda_i}$ for λ_i the ith eigenvalue of

HH^H and R_H of these singular values are nonzero, where R_H is the rank of the matrix $\mathbf{H}$, $R_H \leq min(M_t, M_r)$. If $\mathbf{H}$ is full rank, then $R_H = min(M_t, M_r)$. The decomposition of the channel is obtained by defining a transformation on the channel input and output $\mathbf{x}$ and $\mathbf{y}$ through transmit pre-coding and receiver post processing. In transmit pre-coding the input to the antennas is generated through a linear transformation on the input vector $\tilde{x}$ as $x = V\tilde{x}$. Receiver post processing performs a similar operation at the receiver by multiplying the channel output $\mathbf{y}$ with U^H. The parallel decomposition of MIMO system using SVD is given as [10]

$$\begin{aligned}
\tilde{y} &= U^H(Hx + n) \qquad (2.32)\\
&= U^H(UDV^Hx + n)\\
&= U^H(UDV^HV\tilde{x} + n)\\
&= U^HUDV^HV\tilde{x} + U^Hn\\
&= U^HUDV^HV\tilde{x} + U^Hn\\
&= D\tilde{x} + \tilde{n} \qquad (2.33)
\end{aligned}$$

where $\tilde{n} = U^Hn$.

2.7 The Smith Normal Form

*For an $m \times n$ matrix **A** with entries from Principle Ideal Domain(PID), there exist unimodular matrices $U_{m\times m}$ and $V_{n\times n}$ such that UAV is a diagonal matrix, with positive diagonal elements $\delta_1, \delta_2, \delta_3, \ldots, \delta_r$ where $\delta_1|\delta_2|\ldots|\delta_r$* [2]. Moreover $\delta_1, \delta_2, \delta_3, \ldots, \delta_r$ are the invariant factors of the matrix $\mathbf{A}$.
We can write $\quad \mathbf{B} = \text{UAV}$
where $\mathbf{U}$ and $\mathbf{V}$ are unimodular matrices with $+1$ and -1 determinant.
Example:

$$\mathbf{A} = \begin{pmatrix} 2 & 3 & 4 \\ -6 & 6 & 12 \\ 10 & -4 & -16 \end{pmatrix}$$

The Smith Normal Form is

$$\mathbf{B} = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 6 & 0 \\ 0 & 0 & 12 \end{pmatrix}$$

and the unimodular matrices U and V are

$$\mathbf{U} = \begin{pmatrix} 1 & 0 & 0 \\ 2 & -1 & -1 \\ -3 & 4 & 3 \end{pmatrix}$$

and

$$\mathbf{V} = \begin{pmatrix} 1 & -2 & -2 \\ 0 & 1 & -2 \\ 0 & 0 & -1 \end{pmatrix}$$

The unimodular matrices, **U** and **V** are permutation matrices obtained as a result of elementary row and column operations on matrix **A**. Matrix **U** is the pre-multiplication matrix obtained from the row operations on an identity matrix, as a result of diagonolization of the matrix **A**, whereas matrix **V** is the post-multiplication matrix obtained as a result of column operations. The Smith Normal Form is treated in detail in chapter 3

Chapter 3

Detailed treatment of the possibilities to use Smith's Normal Form for coding

3.1 Introduction

Let us consider two rectangular matrices **A** and **B** of same size $m \times n$ over the Principal Ideal Domain (PID). **B** is said to be equivalent to **A**, if there exist invertible unimodular matrices **U** and **V** such that $B = UAV$. **B** is a $m \times n$ diagonal matrix with $\delta_1, \delta_2, \delta_3, \ldots, \delta_r$ on its leading diagonal $(0 \leq r \leq min(m, n))$ and zero elsewhere, and $\delta_1|\delta_2|\ldots|\delta_r$. Moreover $\delta_1, \delta_2, \ldots, \delta_r$ are the diagonal elements, and are also known as invariant factors of **A** over Principle Ideal Domain (PID). This process is often also referred to as Invariant Factor theorem.
Theorem *For an $m \times n$ matrix $\boldsymbol{A}$ with entries from PID, there exist unimodular matrices $U_{m\times m}$ and $V_{n\times n}$ such that UAV is a diagonal matrix with positive diagonal elements $\delta_1, \delta_2, \delta_3, \ldots, \delta_r$, where $\delta_1|\delta_2|\ldots|\delta_r$* [2]. Moreover, $\delta_1, \delta_2, \delta_3, \ldots, \delta_r$ are the invariant factors of the matrix **A**.
We can write

$$B = UAV \tag{3.1}$$

where **U** and **V** are unimodular matrices with $+1$ and -1 determinant. As the absolute value of $|U|$ and $|V|$ is 1, we can thus write as

$$|UAV| = |B| = \delta_1 \cdot \delta_2 \cdot \delta_3 \cdot \ldots \cdot \delta_r \ . \tag{3.2}$$

Example:

$$\mathbf{A} = \begin{pmatrix} 2 & 4 & 4 \\ -6 & 6 & 12 \\ 10 & -4 & -16 \end{pmatrix}$$

The Smith Normal Form is

$$\mathbf{B} = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 6 & 0 \\ 0 & 0 & 12 \end{pmatrix}$$

and the unimodular matrices **U** and **V** are

$$\mathbf{U} = \begin{pmatrix} 1 & 0 & 0 \\ 2 & -1 & -1 \\ -3 & 4 & 3 \end{pmatrix}$$

and

$$\mathbf{V} = \begin{pmatrix} 1 & -2 & -2 \\ 0 & 1 & -2 \\ 0 & 0 & -1 \end{pmatrix} .$$

It is also noteworthy to describe the two important terms, the determinantal divisor and the Elementary divisor of matrix **A**

Determinantal divisor

Consider an $m \times n$ rectangular matrix **A** from PID. Let k be any integer such that $(0 \leq k \leq n)$. Now choose k row and k column subscripts. Compute the determinant of the sub-matrices constructed from the k choices. Finally, find the greatest common divisor of all the determinants. This number is known as k_{th} determinantal divisor and is denoted by $d_k(A)$. From the determinantal divisor, two matrices are said to be equivalent if and only if they have the same determinantal divisors [3]. Moreover, if the rank of **A** is r, then only r elements on the diagonal will be different from zeros.

The relationship between the determinantal divisor and the invariant factors is given by

$$d_k(A) = \delta_1(A) \cdot \delta_2(A) \cdot \delta_3(A) \ldots \delta_k(A) \; , \qquad (1 \leq k \leq n) \; . \tag{3.3}$$

Or

$$\delta_k(A) = d_k(A)/d_k - 1(A) \; , \qquad (1 \leq k \leq n) \; . \tag{3.4}$$

Elementary Divisor

The theory about elementary divisor arises from primes. For integer numbers Z, every number can be written as a product of prime numbers. Thus any of the invariant factors on the diagonal can be expressed as the product of distinct primes power. The set of such prime powers for all invariant factors is then another invariant factor. Any such prime power is called as elementary Divisor. Thus in terms of elementary Divisor, two matrices are said to be equivalent if and only if they have they same elementary Divisors [3].

Determinantal and elementary divisors are used to check either two matrices are equivalent to each other or not. Thus, two matrices are said to be equivalent if they have the same determinantal divisors / elementary divisors. This project is carried out to check the Smith Normal Form for code construction, the main concern is the unimodular matrices. These two terms explains a property of the diagonal matrix, which is beyond the scope of this project and are skipped for further discussion.

3.2 Algorithm

In the computation of the Smith Normal Form, first of all the invertible matrices **U** and **V** are to be computed such that UAV will be diagonal. Once invertible matrices **U** and **V** are obtained, it is then easy to put the matrix into Smith Normal Form. The unimodular matrices **U** and **V** are permutation matrices obtained by elementary row (column) operations on the matrix **A**. Any row operation made in matrix **A** is reflected on the left by **U**, the pre-multiplying matrix, and any column operation in matrix **A** is reflected on the right by **V**, the post multiplying matrix [4]. Thus, **U** and **V** matrices are obtained by repeatedly applying transformations that replace a row (column) by another row (column) or a linear combination of rows (columns)
Elementary row operations are

1. to interchange row j and row k,
2. to multiply row j by q (integer),
3. to add q times row k to row j.

   The elementary column operations are

4. to interchange column j and column k,
5. to multiply column j by q (integer),
6. to add q times column k to column j.

In order to keep track of the transformations, row operations are performed on an identity matrix to represent the pre-multiplication matrix **U** and corresponding column operations on another identity matrix to represent the post multiplication matrix **V**.
In order to find out the Smith Normal Form of a matrix, the first stage is to produce a diagonolization of the matrix in the following steps (algorithm from [2])

1. Step 1: Check for the element with the smallest absolute value. Interchange rows and column such that a_{11} is the element of smallest absolute value among all non-zero elements in the first row and the first column of the matrix.

2. Step 2: If a_{11} divides a_{1j} $(a_{11} \mid a_{1j})$, for $j = 2, 3, \ldots, n$, go to step 3, otherwise for some k, let $a_{1k} = qa_{11} + r$ where q, r are integers and $0 < r < a_{11}$. Let $A[1,k]$ denote the k_{th} column of $\mathbf{A}$. Replace $A[1,k]$ by $A[1,k]$ - $qA[1,1]$. Go to step 1.

3. Step 3: If a_{11} divides a_{l1} $(a_{11} \mid a_{l1})$, for $l = 2, 3, \ldots, n$, go to step 4, otherwise for some k, let $a_{k1} = qa_{11} + r$ where q, r are integers and $0 < r < a_{11}$. Let $A[k,1]$ denote the k_{th} row of $\mathbf{A}$. Replace $A[k,1]$ by $A[k,1] - qA[1,1]$. Go to step 1.

4. Step 4: $a_{11} \mid a_{1j}$ for $j = 2, 3, \ldots, n$, and $a_{11} \mid a_{1l}$ for $l = 2, 3, \ldots, n$.
   Either assume $a_{1j} = qa_{11}$, then replace $A[1,j]$ by $A[1,j] - qA[1,1]$ for $j = 2, 3, \ldots, n$. This will ensure that the first row of the matrix has only the first element non-zero.
   Assume $a_{l1} = qa_{11}$, then replace $A[l,1]$ by $A[l,1] - qA[l,1]$ for $l = 2, 3, \ldots, n$. This will ensure that the first column of the matrix has only the first element non-zero.

5. Step 5: The matrix is now of the form

$$\begin{pmatrix} a_{11} & 0 & \ldots & 0 \\ 0 & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & a_{n2} & \ldots & a_{nn} \end{pmatrix}$$

   Step 1 to 4 are now applied to the sub-matrix

$$\begin{pmatrix} a_{22} & \ldots & a_{2n} \\ \vdots & \ddots & \vdots \\ a_{n2} & \ldots & a_{nn} \end{pmatrix}$$

   and the process continues until the matrix is completely diagonolized.
   It is also necessary to memorize that if the numbers are getting larger, then step 1 and/or 4 can be omitted as follows. If in a row or column two or more elements has the same absolute value, then the one which will keep numbers down the most will be selected.
   The diagonal matrix so obtained is

$$\begin{pmatrix} x_1 & 0 & \ldots & 0 & 0 \\ 0 & x_2 & \ldots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \\ 0 & \ldots & \ldots & x_r & 0 \\ 0 & \ldots & \ldots & 0 & 0 \end{pmatrix}$$

6. Step 6: The aim of Steps $1 - 5$ was to diagonolize a matrix. Once the diagonolization of a matrix is obtained, the next step is to find out the

invariant factors of the diagonal matrix. If $x_1|x_k$ for $k = 2, 3, \ldots, n$, then check $x_2|x_k$ for $k = 3, 4, \ldots, n$, continue this process until $x_l \nmid x_k$ for $0 < l < k$. Row k is added to row l and the process is repeated for a new x_l of smaller value.

Example: Let the diagonal matrix obtained be

$$\begin{pmatrix} 3 & 0 & 0 \\ 0 & 8 & 0 \\ 0 & 0 & 12 \end{pmatrix}$$

The invariant factors for this matrix can be found in the following steps. Since 3 is not a factor of 8 thus according to Step 6, row 2 (R_2) is added to row 1 (R_1)

$$\mathbf{R_1 + R_2} \Rightarrow \begin{pmatrix} 3 & 8 & 0 \\ 0 & 8 & 0 \\ 0 & 0 & 12 \end{pmatrix},$$

using Step 2, multiply column 1 (C_1) by 2 and subtract from column 2 (C_2), i.e.,

$$\mathbf{C_2 - 2C_1} \Rightarrow \begin{pmatrix} 3 & 2 & 0 \\ 0 & 8 & 0 \\ 0 & 0 & 12 \end{pmatrix},$$

According to Step 1, to check for an element of smaller absolute value in the first row and the first column, interchange (C_2) and (C_1) (column operation), i.e.,

$$\mathbf{C_1 \sim C_2} \Rightarrow \begin{pmatrix} 2 & 3 & 0 \\ 8 & 0 & 0 \\ 0 & 0 & 12 \end{pmatrix},$$

using Step 2, since 2 is not a factor of 3, thus subtraction of column 1 (C_1) from column 2 (C_2) leads to,

$$\mathbf{C_2 - 2C_1} \Rightarrow \begin{pmatrix} 2 & 1 & 0 \\ 8 & -8 & 0 \\ 0 & 0 & 12 \end{pmatrix}.$$

According to Step 1, again to check for an element of smaller absolute value in the first row and the first column, interchange C_1 and C_2 (column operation),

$$\mathbf{C_1 \sim C_2} \Rightarrow \begin{pmatrix} 1 & 2 & 0 \\ -8 & 8 & 0 \\ 0 & 0 & 12 \end{pmatrix}.$$

Now according to Step 2, all the elements except a_{11} in the first row must be zero. Thus, subtracting 2 times C_1 from C_2, i.e.,

$$\mathbf{C_2 - 2C_1} \Rightarrow \begin{pmatrix} 1 & 0 & 0 \\ -8 & 36 & 0 \\ 0 & 0 & 12 \end{pmatrix}.$$

Similarly Step 3 implies that all elements in the first column except a_{11} must be zero, thus adding 8 times R_1 to R_2 results in

$$\mathbf{R_2 + 8R1} \Rightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 36 & 0 \\ 0 & 0 & 12 \end{pmatrix} .$$

Now, since 1 is a factor of both 36 and 12, thus it remains unchanged. In the matrix above $a_{22} > a_{33}$, thus according to Step 6 R_3 is added to R_2, i.e.,

$$\mathbf{R_2 + R_3} \Rightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 36 & 12 \\ 0 & 0 & 12 \end{pmatrix} .$$

Following Step 1, to check for an element of smaller absolute value in the second row and the second column interchange column 3 and column 2 (column operation)

$$\mathbf{C_2 \sim C_3} \Rightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 12 & 36 \\ 0 & 12 & 0 \end{pmatrix}$$

According to Step 2 and Step 3, the second row and second column must have only 2nd element non-zero. Thus subtracting 3 times columns 2 from column 3 and row 2 from row 3 leads to

$$\mathbf{C_3 - 3C_2} \Rightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 12 & 0 \\ 0 & 12 & -36 \end{pmatrix} ,$$

$$\mathbf{R_3 - R_2} \Rightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 12 & 0 \\ 0 & 0 & -36 \end{pmatrix} .$$

Multiplying column 3 by (-1)

$$(\mathbf{-1})\mathbf{C_2} \Rightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 12 & 0 \\ 0 & 0 & 36 \end{pmatrix}$$

The invariant factors are [1,12,36].

3.3 The Smith Normal Form of Integer Matrices

The Smith Normal Form of the integer matrices can well be explained from the solution of the following matrix. Example [4]:

$$\mathbf{A} = \begin{pmatrix} 7 & 8 & 9 \\ 4 & 5 & 6 \\ 1 & 2 & 3 \end{pmatrix}$$

According to Step 1, a_{11} must be the element of smallest absolute value. Thus interchanging row 1 (R_1) with row 3 ($R-3$) (row operation). Moreover to keep the track of transformations, performing the same operation on an identity matrix and pre-multiply.

$$\mathbf{R_1} \sim \mathbf{R_3} \Rightarrow \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}. \tag{3.5}$$

Since 1 is a factor of all the elements in the first row and column, thus according to Step 4, subtracting 2 times column 1 (C_1) from column 2 (C_2), and 3 times column 1 (C_1) from column 3 (C_3) and performing the same operations on post-multiplication identity matrix results in,

$$\begin{matrix}\mathbf{C_2 - 2C_1} \\ \mathbf{C_3 - 3C_1}\end{matrix} \Rightarrow \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 4 & -3 & -6 \\ 7 & -6 & -12 \end{pmatrix} \begin{pmatrix} 1 & -2 & -3 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}. \tag{3.6}$$

Similarly following Step 4, subtracting 4 times row 1 (R_1) from row 2 (R_2) and 7 times row 1 (R_1) from row 3 (R_3). Perform the same operations on the pre-multiplication matrix.

$$\begin{matrix}\mathbf{R_2 - 4R_1} \\ \mathbf{R_3 - 7R_1}\end{matrix} \Rightarrow \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & -4 \\ 1 & 0 & -7 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & -3 & -6 \\ 0 & -6 & -12 \end{pmatrix} \begin{pmatrix} 1 & -2 & -3 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}. \tag{3.7}$$

As obvious from the matrix, 3 has the minimum absolute value and is also a factor of all the elements of the sub matrix, thus using Step 4 again, subtracting 2 times C_2 from C_3 implies,

$$\mathbf{C_3 - 2C_2} \Rightarrow \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & -4 \\ 1 & 0 & -7 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & -3 & 0 \\ 0 & -6 & 0 \end{pmatrix} \begin{pmatrix} 1 & -2 & 1 \\ 0 & 1 & -2 \\ 0 & 0 & 1 \end{pmatrix}. \tag{3.8}$$

Now to make all the elements of column 2, except a_{22}, equal to zero (Step 4), subtracting 2 times R_2 from R_3,

$$\mathbf{R_3 - 2R_2} \Rightarrow \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & -4 \\ 1 & -2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & -3 & 0 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & -2 & 1 \\ 0 & 1 & -2 \\ 0 & 0 & 1 \end{pmatrix}. \tag{3.9}$$

The invariant factors theorem states that all the diagonal elements must be positive, thus multiplying C_2 by -1,

$$(\mathbf{-1})\mathbf{C_2} \Rightarrow \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & -4 \\ 1 & -2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 2 & 1 \\ 0 & -1 & -2 \\ 0 & 0 & 1 \end{pmatrix}. \tag{3.10}$$

The resultant diagonal matrix is

$$\mathbf{B} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 0 \end{pmatrix},$$

where the unimodular matrices **U** and **V** are

$$\mathbf{U} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & -4 \\ 1 & -2 & 1 \end{pmatrix} \qquad \text{and} \qquad \mathbf{V} = \begin{pmatrix} 1 & 2 & 1 \\ 0 & -1 & -2 \\ 0 & 0 & 1 \end{pmatrix}$$

Moreover
$|U| = 1 \cdot (0 \cdot (-2)) + 1 \cdot 1 = 0 + 1 = 1$ and
$|V| = 1 \cdot ((-1) \cdot 1 + 0 \cdot (-2)) = -1 + 0 = -1$
since the matrices **U** and **V** are non-singular, they are thus invertible.

3.3.1 Smith Normal Form of a bigger rectangular matrix

Consider a 5 x 7 matrix [3] as shown,

$$\mathbf{G} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 2 & 4 & 5 & 6 & 1 & 1 & 1 \\ 1 & 4 & 2 & 5 & 2 & 0 & 0 \\ 0 & 0 & 1 & 1 & 2 & 2 & 3 \end{pmatrix}.$$

The resultant diagonal and unimodular matrices are

$$\mathbf{D} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 0 & 0 \end{pmatrix}$$

$$\mathbf{U} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 2 & 0 & -1 & 0 & 0 \\ 2 & 0 & -1 & 0 & -1 \\ 5 & 0 & -2 & -1 & -3 \\ -3 & -1 & 2 & 0 & 0 \end{pmatrix},$$

and

$$\mathbf{V} = \begin{pmatrix} 1 & -3 & 2 & -6 & -14 & 29 & 16 \\ 0 & 0 & 0 & 7 & 15 & -34 & -18 \\ 0 & 1 & -2 & 5 & 10 & -23 & -13 \\ 0 & 0 & 1 & -7 & -14 & 33 & 18 \\ 0 & 0 & 0 & 1 & 2 & -6 & -4 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

The number of invariant factors in the matrix $\mathbf{D}$ on the diagonal are five, thus it means that the rank of the matrix G is 5, i.e., $r = 5$, which also proves that the number of invariant factors equals the rank of a matrix.

3.4 Code construction with Smith Normal Form

The diagonolization of integer matrices with Smith Normal From is discussed in the previous sections. The question is now, is it possible to use the Smith Normal Form as a basis for discrete code construction? In order to check Smith Normal From as a possibility for code construction using the unimodular matrices, let us first work out the minimum Hamming distance /Hamming weight for the unimodular matrices from the matrix view point. The unimodular matrices are sparse permutation matrices which are obtained as a result of various permutations and linear combinations on integer matrix. Consider the 7 × 7 unimodular matrix obtained in 3.37. Let this matrix represent the generator matrix for the code (supposed), if we force the last four positions to zero, i.e.,

$$(\mathbf{C_0 C_1 C_2}|\mathbf{0000}) = \left(\begin{array}{ccccccc} 1 & -3 & 2 & -6 & -14 & 29 & 16 \\ 0 & 0 & 0 & 7 & 15 & -34 & -18 \\ 0 & 1 & -2 & 5 & 10 & -23 & -13 \\ \hline 0 & 0 & 1 & -7 & -14 & 33 & 18 \\ 0 & 0 & 0 & 1 & 2 & -6 & -4 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{array}\right). \qquad (3.11)$$

there is still a possibility to get a zero minor, which is violation to the minimum Hamming distance. Moreover, let us suppose that the rows of the matrix represent the code-words of a code (supposed), then Hamming weight of the last two rows is 1, which means a Hamming distance of 1, which also contradicts the definition of minimum Hamming distance for a code-word. Thus the unimodular matrices so obtained does not fulfils the singleton bound ($d_{Hm} \leq M + 1 = N - M + 1$) so, it is concluded that the Smith Normal Form cannot be used for code construction.

3.5 Conclusion

Any $m \times n$ rectangular integer matrix can be diagonolized by pre and post-multiplication with unimodular matrices. The pre and post-multiplication matrices are obtained from the elementary row and column operations on identity matrices used to keep track of operations performed for diagonolization of the integer matrix. The resulting pre and post-multiplication matrices are sparse matrices, which are obtained as a result of various permutations and linear combinations on the integer matrix. In order to make use of the Smith Normal Form for code construction, certain minimum Hamming distance has to be guaranteed. Due to the sparsity of the resulting pre and post-processing matrices, minors will often be zero, thereby violating the desired minimum Hamming distance. Hence it is concluded that Smith Normal Form cannot be used for discrete code construction.

Bibliography

[1] Patrik J-Morandi, “The smith Normal Form of a matrix”.

[2] V.J Rayward - Smith, “On computing the Smith Normal Form of an integer Matrix”, *ACM Transactions on Mathematical Software, Vol 5, No , December 1979.*

[3] Morris Newman, “The Smith Normal Form”, *Linear algebra and its applications, 254: 367-381 (1997).*

[4] B.Hartley and T.O Hawkes, “Rings, Modules and Linear Algebra”.

[5] Carl D.Meyer, “Matrix Analysis and Applied Linear Algebra”.

[6] Werner Henkel and Ina Kodrasi, “An RS Coding View onto OFDM, MIMO, and Time Frequency uncertainty”.

[7] Werner Henkel,“Channel Coding (Lecture Notes)”.

[8] Shu Lin and Daniel J.Costello Jr., “ Error Control Coding”.

[9] Rolf Johannesson and Kamil Sh.Zigangirov, “Fundamentals of Convolutional Coding”.

[10] Andrea Goldsmith, “Wireless Communications”.