

REDUNDANT RESIDUE NUMBER SYSTEM BASED  
SPACE-TIME BLOCK CODES

by

AVIK SENGUPTA

B.Tech., West Bengal University of Technology, 2010

---

A THESIS

submitted in partial fulfillment of the  
requirements for the degree

MASTER OF SCIENCE

Department of Electrical and Computer Engineering  
College of Engineering

KANSAS STATE UNIVERSITY

Manhattan, Kansas

2012

Approved by:

Major Professor  
Balasubramaniam Natarajan

# Copyright

Avik Sengupta

2012

# Abstract

Space-time coding (STC) schemes for Multiple Input Multiple Output (MIMO) systems have been an area of active research in the past decade. In this thesis, we propose a novel design of Space-Time Block Codes (STBCs) using Redundant Residue Number System (RRNS) codes, which are ideal for high data rate communication systems. Application of RRNS as a concatenated STC scheme to a MIMO wireless communication system is the main motivation for this work. We have optimized the link between residues and complex constellations by incorporating the “Direct Mapping” scheme, where residues are mapped directly to Gray coded constellations. Knowledge of apriori probabilities of residues is utilized to implement a probability based “Distance-Aware Direct Mapping” (DA) scheme, which uses a set-partitioning approach to map the most probable residues such that they are separated by the maximum possible distance. We have proposed an “Indirect Mapping” scheme, where we convert the residues back to bits before mapping them. We have also proposed an adaptive demapping scheme which utilizes the RRNS code structure to reduce the ML decoding complexity and improve the error performance. We quantify the upper bounds on codeword and bit error probabilities of both Systematic and Non-systematic RRNS-STBC and characterize the achievable coding and diversity gains assuming maximum likelihood decoding (MLD). Simulation results demonstrate that the DA Mapping scheme provides performance gain relative to a Gray coded direct mapping scheme. We show that Systematic RRNS-STBC codes provide superior performance compared to Non-systematic RRNS-STBC, for the same code parameters, owing to more efficient binary to residue mapping. When compared to other concatenated STBC and Orthogonal STBC (OSTBC) schemes, the proposed system gives better performance at low SNRs.

# Table of Contents

<b>Table of Contents</b>	<b>iv</b>
<b>List of Figures</b>	<b>vi</b>
<b>List of Tables</b>	<b>viii</b>
<b>Acknowledgements</b>	<b>ix</b>
<b>Dedication</b>	<b>x</b>
<b>1 Introduction</b>	<b>1</b>
1.1 MIMO Wireless Communication . . . . .	2
1.2 Space-Time Coding . . . . .	5
1.3 RNS and RRNS based Channel coding . . . . .	7
1.4 Overview of Thesis . . . . .	8
1.5 Key Contributions . . . . .	9
1.6 Organization . . . . .	12
<b>2 Residue Number System and Redundant Residue Number System</b>	<b>13</b>
2.1 RNS and RRNS Arithmetic . . . . .	13
2.1.1 Residue Number System . . . . .	13
2.1.2 Redundant Residue Number System . . . . .	15
2.1.3 Decoding of RNS and RRNS . . . . .	16
2.2 RRNS based Error Correcting Codes: . . . . .	20
2.2.1 Non-systematic Encoding . . . . .	20
2.2.2 Systematic Encoding . . . . .	21
2.3 Error Detection and Correction with RRNS . . . . .	23
2.4 Summary . . . . .	25
<b>3 Direct and Indirect Mapping Schemes</b>	<b>26</b>
3.1 Direct Mapping Scheme . . . . .	27
3.1.1 Direct Mapping Scheme . . . . .	27
3.2 Indirect Mapping Scheme . . . . .	31
3.3 Adaptive Demapping Scheme . . . . .	32
3.4 Summary . . . . .	36

<b>4</b>	<b>Redundant Residue Number System based STBC Design</b>	<b>37</b>
4.1	System Model . . . . .	37
4.2	Performance Analysis . . . . .	38
4.2.1	STC Pairwise Error Probability . . . . .	40
4.2.2	Non-Systematic RRNS-STBC . . . . .	42
4.2.3	Systematic RRNS-STBC . . . . .	46
4.3	Complexity of RRNS-STBC . . . . .	51
4.4	Summary . . . . .	52
<b>5</b>	<b>Performance of RRNS-STBC: Analysis of Simulation Results</b>	<b>53</b>
5.1	Simulation Parameters . . . . .	53
5.2	Simulation Results . . . . .	54
5.2.1	Non-Systematic RRNS-STBC . . . . .	54
5.2.2	Systematic RRNS-STBC . . . . .	70
5.3	Summary . . . . .	76
<b>6</b>	<b>Conclusions</b>	<b>77</b>
6.1	Summary of Key Contributions . . . . .	77
6.2	Future Work . . . . .	81
	<b>Bibliography</b>	<b>82</b>
<b>A</b>		<b>89</b>
A.1	Proof of Lemma 2: . . . . .	89
<b>B</b>		<b>91</b>
B.1	Proof of Lemma 5: . . . . .	91
B.1.1	Calculation of Upper Bound for $P_{E1}^s$ . . . . .	91
B.1.2	Calculation of Upper Bound for $P_{E2}^s$ . . . . .	92

# List of Figures

1.1	Multiple Input Multiple Output System . . . . .	3
1.2	Space-time block code - Alamouti's transmit diversity scheme . . . . .	6
2.1	Encoding procedure for Non-Systematic RRNS . . . . .	20
2.2	Encoding procedure for Systematic RRNS . . . . .	21
3.1	System Block for Direct Mapping . . . . .	27
3.2	Gray Coded Direct Mapping for QPSK . . . . .	28
3.3	Probability Based Distance-Aware Mapping Scheme for 16-QAM. . . . .	29
3.4	Probability mass function for $m_o = \{5, 7, 9\}$ and $m_r = \{11, 13, 16\}$ . . . . .	30
3.5	System Block for Indirect Mapping . . . . .	31
3.6	Probability Mass Function for Systematic RRNS(6, 3)-STBC with moduli set $m_o = \{5, 7, 9\}$ ; $m_r = \{11, 13, 16\}$ . . . . .	32
3.7	Probability based DA Mapping and Smart Demapping Scheme for 16-QAM .	33
3.8	Gray coded Direct Mapping and Adaptive Demapping scheme for 16-QAM using modulus 7. . . . .	35
4.1	The block diagram of RRNS-STBC coded $2 \times 2$ MIMO system . . . . .	37
4.2	The block diagram for performance analysis of RRNS-STBC coded $2 \times 2$ MIMO system . . . . .	39
5.1	BER performance of RRNS (5,3)- STBC with moduli set of $m_o = \{7, 9, 11\}$ , $m_r = \{13, 16\}$ . . . . .	55
5.2	Comparison of BER performance of Full Diversity Non-systematic RRNS(6,3)- STBC ( $T = 6$ ), with prior probability based Distance-Aware mapping and Gray coded mapping and Indirect Mapping with ML decoding assuming equal priors . . . . .	57
5.3	Comparison of BER performance of Spatially Multiplexed Non-systematic RRNS-STBC with Direct and Distance-Aware mapping and with different $\chi$	58
5.4	Comparison of BER performance of Non-systematic RRNS(6,3)- Alamouti with prior probability based Distance-Aware mapping, Gray coded mapping and Indirect mapping assuming equal priors . . . . .	60
5.5	Comparison of BER performance of RRNS(4,2)-Alamouti ( $T = 2$ ) with Non-systematic RS(15, 5)-Alamouti and Non-systematic (15, 5)-Cyclic code- Alamouti with 16-QAM. . . . .	61
5.6	Comparison of PMFs for different RRNS codes . . . . .	63
5.7	Comparison of BER performance of different RRNS codes . . . . .	64

5.8	Performance of DA Mapping Scheme over a SISO channel using RRNS (6,2) encoding with moduli set of $m_o = \{5, 7\}$ , $m_r = \{9, 11, 13, 16\}$ . . . . .	66
5.9	Performance of Indirect Mapping Scheme using RRNS (5,3) encoding with moduli set of $m_o = \{9, 11, 13\}$ , $m_r = \{16, 17\}$ . . . . .	67
5.10	Comparison in BER performance of Systematic and Non-systematic RRNS (6,3)- STBC with moduli set of $m_o = \{5, 7, 9\}$ , $m_r = \{11, 13, 16\}$ for the case of Adaptive Demapping. . . . .	68
5.11	Comparison in BER performance of Non-systematic RRNS (6,3)- STBC with moduli set of $m_o = \{5, 7, 9\}$ , $m_r = \{11, 13, 16\}$ for the case of Gray coded Direct Mapping and naive vs. Adaptive Demapping. . . . .	69
5.12	BER performance of Systematic and Non-systematic RRNS (5,3)- STBC with moduli set of $m_o = \{7, 9, 11\}$ , $m_r = \{13, 16\}$ . . . . .	70
5.13	Comparison in BER performance of Systematic and Non-systematic RRNS (5,3)- STBC with moduli set of $m_o = \{7, 9, 11\}$ , $m_r = \{13, 16\}$ , for the case of Direct Mapping and Probability based Distance Aware Mapping. . . . .	72
5.14	BER performance of Systematic RRNS (6,3)- STBC with moduli set of $m_o = \{5, 7, 9\}$ , $m_r = \{11, 13, 16\}$ , for the case of Direct Mapping and Probability based Distance Aware Mapping. . . . .	73
5.15	Comparison BER performance of Systematic and Non-systematic RRNS (4,2)-STBC with moduli set of $m_o = \{7, 9\}$ , $m_r = \{13, 16\}$ with Systematic and Non-systematic RS-STBC Schemes for the case of Indirect Mapping. . . . .	74
5.16	Comparison BER performance of Systematic and Non-systematic RRNS (4,2)-STBC with moduli set of $m_o = \{7, 9\}$ , $m_r = \{13, 16\}$ with RS-STBC Schemes for the case of Direct Mapping. . . . .	75

# List of Tables

2.1	RNS REPRESENTATION OF INTEGER MESSAGES . . . . .	14
2.2	RRNS REPRESENTATION OF INTEGER MESSAGES . . . . .	15
2.3	MAPPING OF INFORMATION BITS TO RESIDUES FOR SYSTEMATIC RRNS ENCODING . . . . .	22
3.1	DIRECT RESIDUES TO COMPLEX SYMBOLS MAPPING USING MODULUS 4 . .	27
5.1	CHOICE OF MODULI FOR DIFFERENT RRNS CODES . . . . .	65



# Acknowledgments

I would like to express my heartfelt gratitude to my advisor, Dr. Bala Natarajan, whose patient support and encouragement has been the driving force behind this work. Under his guidance, I have learnt how to set goals, to stretch the horizons of the mind and scale the targets I set for myself. I would like to thank him for always believing in me and teaching me the essence of research. Not only on a professional level, I have also had the fortune to interact with him and his family on a personal level and cherish every one of these moments. He has always been a caring and understanding mentor and has always made an effort to make me feel comfortable so far away from home. As I set out towards a career in research, his valuable comments will always help me on my way. I would also like to thank Dr. William Kuhn and Dr. Sanjoy Das for agreeing to be a part of my committee and donating their valuable time to review this work.

Being a part of WiCom research group has been the best part of my time here at K-State. I would like to thank all the members, past and present, for their helpful comments and motivation. They made Wicom more of a family than a group. I would especially like to thank Sidd, who has been like an elder brother and mentor. Thanks for always listening to my rants and providing the most insightful of comments and giving the soundest advice possible. To Nick, thanks for patiently listening to my research ideas and giving intelligent feedback and insights. You are an awesome scientist and working with you has been a privilege. Finally I would like to raise a toast to my roommates and my friends in Manhattan, who have made my stay here a lot of fun. You guys rock!

# Dedication

I would like to dedicate this work to my Parents, cousins, my dear nephew and my special group of friends. They have been a constant source of support and have always believed in me. Thank you for standing by me and always encouraging me in whatever I have wanted to do. Without your love and support this would have remained a dream...

# Chapter 1

## Introduction

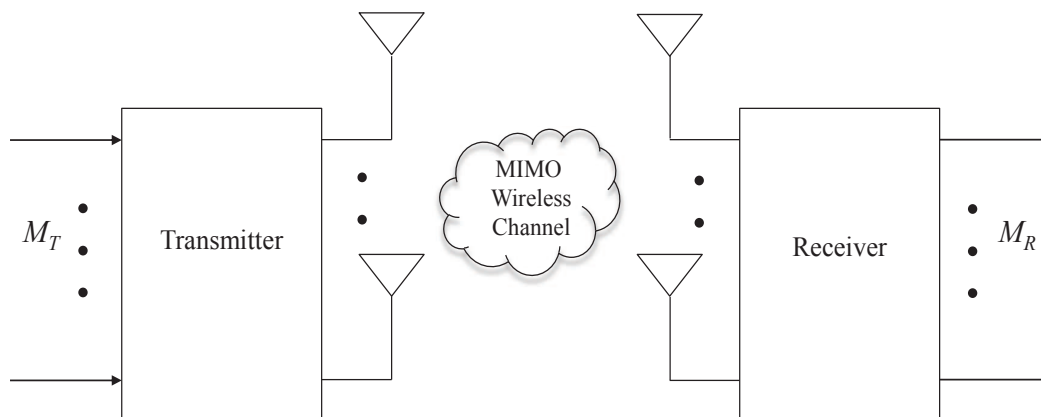
Wireless communication systems have become an indispensable part of our lives. Mobile phones have become the most important means of personal communication, while Wireless LAN, Wifi, Bluetooth, IRDA (infrared data communication) dominate the world of information exchange and computing. It has brought about a radical change in the way people interact and explore leading to an ever increasing demand for further research and development. Apart from applications in telephony and computing, wireless communication systems have found wide ranging applications in remote sensing and wireless sensor networks [1], [2], battle field communications [3], mapping inaccessible terrains, remote health monitoring [4], security, surveillance, home networking, global positioning systems [5] and literally any portable or hand-held device. Wireless systems are even used for transfer of power, without the use of wires, from the power source [6]. Wireless communications systems have enabled us to widen our horizons and conquer previously insurmountable barriers. Space exploration and missions to Mars and other planets employing deep-space radio communication [7],[8] are shining examples of the advancements made in wireless systems. With increasing applications the demand of increased capacity and support of higher data rates is omnipresent. Achieving theoretical performance limits and improving the performance of present wireless systems has been the main objective of research in this area. One of the major breakthroughs in wireless communication research has been Space-time wireless communication, which exploits the spatial dimension to increase fidelity and data rate. Conventional wire-

less systems use only a single antenna at both transmitter and receiver. Space-time systems on the other hand use multiple antennas at receiver and transmitter. In this chapter, we first introduce the concept of multiple input multiple output (MIMO) wireless communication systems and space-time coding. Residue Number System and Redundant Residue Number System are discussed next. Finally, we expound on the prior work, motivation and contributions of this thesis.

## 1.1 MIMO Wireless Communication

In wireless communication systems, the use of multiple antennas at the transmitter and receiver is known as MIMO (multiple-input multiple output) systems. In recent years, the use of MIMO systems for space-time communication have gained popularity owing to its enhanced performance capabilities which caters to the ever increasing demands of higher data rates and better transmission fidelity. The main challenges in designing a wireless communication system is to counter the effects of multi-path fading (angle spread, delay spread and Doppler spread) in the wireless channel and satisfy the constraints posed by limited transmission power and scarcity of frequency bandwidth. MIMO technology is a breakthrough in communication system design. It offers benefits that help mitigate the impairments in wireless channels as well as the challenges in resource management. Apart from the temporal and frequency dimensions, MIMO systems enable the exploitation of the spatial dimension. MIMO systems offer higher data rates at much lower signal-to-noise ratio (SNR) and no additional power or bandwidth expenditure as compared to single input single output (SISO) antenna systems. For example, at a target receive SNR of 25 dB, a conventional SISO system can deliver a data rate of 0.7 Mbps. However, with 2 and 4 transmit antennas, data rates of 1.4 and 2.8 Mbps can be achieved [9], provided orthogonal channels are used. The benefits provided by MIMO technology can be attributed to *array gain*, *spatial diversity gain*, *spatial multiplexing gain* and *interference reduction*.

**Array Gain:** Array gain is the increase in receive SNR due to coherent combining of wireless signals at the receiver, which provides improved resistance to noise. This in turn improves coverage and network range. In MIMO systems, channel state information at the transmitter (CSIT) is required to fully exploit the array gain.



**Figure 1.1:** *Multiple Input Multiple Output System*

**Diversity Gain:** Spatial diversity gain mitigates fading and is a result of transmitting multiple copies of the same signal in space, frequency or time. With an increasing number of independent copies of the transmitted signal at the receiver, the probability of at least one of the copies not experiencing deep fade increases. A MIMO channel with  $M_T$  transmit antennas and  $M_R$  receive antennas can provide a maximum spatial diversity up to the order of  $M_R M_T$ .

**Multiplexing Gain:** Spatial Multiplexing gain results from transmitting multiple independent data streams within the bandwidth of operation, which leads to an increase in data rate. Multiplexing increases the channel capacity by a multiplicative factor equal to the number of independent data streams, provided that the streams can be separated reliably at the receiver. In general, the number of reliable data streams equals  $\min \{M_T, M_R\}$ . There have been many attempts at exploiting the transmit diversity by precoding. The delay diversity schemes [10]-[12] are a classic example.

**Interference Reduction:** Interference in wireless networks results from multiple users sharing the same frequency and temporal resources. MIMO systems also offer improved interference mitigation by exploiting the spatial dimension to increase the separation between users. This can be achieved by directing signal energy towards the intended user and minimizing interference to other users. In presence of interference, the array gain increases the noise tolerance and the signal-to-interference-noise ratio (SINR) improves. Schemes like dirty paper coding (DPC) for MIMO channels exploits the channel knowledge at the transmitter to mitigate interference resulting from the multiple channels [13],[14]. DPC uses a successive interference cancellation framework to cancel out multi-channel interference.

In general it may not be possible to exploit all the benefits simultaneously due to conflicting demands on spatial degrees of freedom but some combination of these benefits provides a considerable improvement in coverage, capacity and reliability [9]. Thus MIMO technology has found increasing applications in wireless cellular networks and ad-hoc networks. MIMO systems form the core of many wireless standards e.g., IEEE 802.11n(Wifi), IEEE 802.16 (WMAN), 4G, 3GPP Long term evolution (LTE), WiMAX (Worldwide Interoperability for Microwave Access) and HSPA+ (Evolved High-Speed Packet Access).

In particular, LTE aims to exploit the advantages offered by MIMO technology. LTE is the next generation for mobile communications, where data usage in handheld devices holds a much greater importance than before. All major wireless telecom service providers e.g., Verizon, AT&T, Sprint etc have started migrating their networks to LTE. LTE Release 8(2010) specifies  $2 \times 2$  MIMO as a standard. Different MIMO modes used are Spatial Multiplexing, MIMO Beamforming and Transmit Diversity. Spatial Multiplexing is preferred in high SINR conditions to increase throughput and spectral efficiency. The use of both open loop(for robustness in high speed scenarios) and closed loop SM(for low speed scenarios with accurate channel feedback) is specified in Release 8. On the other hand, Transmit Diversity is preferred in low SINR conditions to improve coverage. Space Frequency Block Coding (SFBC) and Cyclic Delay Diversity schemes are used for diversity transmission.

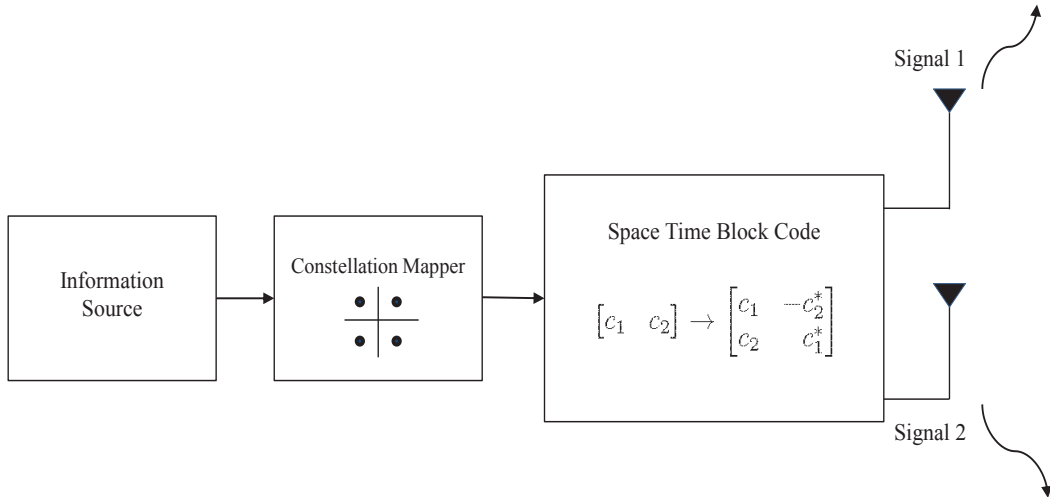
LTE specifies adaptive selection of MIMO modes to maximize performance in the downlink. In the uplink however, only virtual Multi-user MIMO (MU-MIMO) is presently supported. LTE Release 10(2012) i.e., LTE-Advanced specifies upto 8 Tx antennas in downlink and upto 4 Tx antennas in the uplink. Theoretically, the use of higher order MIMO systems are predicted to push the data rates upto 1 Gbps. However, present LTE networks offers data only upto 20Mbps. The implementation of uplink MIMO is still subject to device compatibility and research continues on ways to solve the existing problems and push the actual data rates towards the theoretical boundaries.

## 1.2 Space-Time Coding

Space-time codes (STC) exploit the transmit diversity of the MIMO system which pushes the system performance close to the theoretical performance limits. STCs have been an area of considerable research in the past decade due to its many advantages. Firstly, STC improves the downlink performance without necessitating the use of multiple antennas at the receiver. STCs have been applied to wideband code-division multiple access (WCDMA) techniques [15], which resulted in considerable capacity gains due to smoother fading which makes power control more effective, thereby reducing transmit power. Secondly, STCs can be combined with channel codes [16], which help in realizing an additional coding gain on top of the available diversity gain. Thirdly, STCs operate in an open-loop mode as it does not necessitate the use of channel state information at the transmitter (CSIT). Thus it saves frequency resources by eliminating the need for feedback to the transmitter, which is often unreliable in case of a fast fading channel. Finally, STCs have been shown to be highly robust in non-ideal operating conditions [17], [18].

The two basic space-time coding scheme are - *Space-Time Block Codes* proposed by Alamouti [19] and *Space-Time Trellis Code* proposed by Tarokh *et al.*[16], which introduce spatial and temporal correlation into signals transmitted from different transmit antennas, without increasing the total transmit power or the transmission bandwidth. In this thesis

we concern ourselves with the design of space time block codes.



**Figure 1.2:** *Space-time block code - Alamouti's transmit diversity scheme*

**Space-Time Block Codes** Over the years many variants of space-time block codes (STBC) has been developed. Tarokh *et al.* extended the concept of Alamouti's orthogonal STBC (OSTBC), which was proposed for a  $2 \times 2$  MIMO system, to higher order MIMO systems [20] at the cost of a loss in rate. Alamouti's OSTBC was a simple yet revolutionary step in design of modern wireless communication systems as it provided maximum diversity gain and has been adopted in several wireless standards like WCDMA and CDMA2000. Non-orthogonal STBCs have also been developed, where the orthogonality constraint was relaxed but polynomial decoding complexity was maintained. Linear dispersion codes [21] are an example, where orthogonality is relaxed. But this comes at the expense of constellation expansion and cannot guarantee maximum diversity gains. This reflects the inherent trade-off in STBC design which suggests that to increase diversity gain, the multiplexing gain has to be bounded and vice versa [22]. In this thesis we examine the design of a new, simple STBC scheme which employs an outer forward error correcting code (FEC) concatenated with constellation mapping and inner spatial multiplexing to extract better diversity order. We use a special class of channel codes based on the Residue Number System (RNS).



### 1.3 RNS and RRNS based Channel coding

RNS is a non-weighted, carry-free number system with applications in high-speed parallel signal processing and digital hardware implementations [23]-[28]. The RNS employs carry-free arithmetic which ensures that operations related to the different residue digits are independent. The errors during multiplication, addition and subtraction operations, or due to transmission or processing noise do not propagate and remain confined to their original residue digits and do not contaminate other residue digits [27]-[31]. Thus RNS arithmetic simplifies computations by decomposing a problem into a set of parallel residue computations. The properties of RNS motivate the use of redundant residue number system (RRNS) for robust self-checking, error detection and error correction. The lack of ordered significance among the residues implies that some redundant residue digits can be discarded without affecting the result, as long as a sufficiently high dynamic range is maintained by the retained residues of the reduced RNS so that the information symbols can be described without ambiguity.

The use of RRNS as an error correcting code was initially proposed by [25],[26],[29]. But prior efforts in application of RRNS as a channel coding scheme have been limited due to the complexity of decoding. But recent advances in computing has enabled the use of RRNS as a channel code to improve error detection and correction [23],[27],[30]-[38]. The theoretic framework of RRNS as a channel coding scheme and its error detection and correction capabilities has been investigated in detail by [27][30]-[32]. The applications of RRNS based codes in OFDM based communication systems has been discussed in [33][38], while its application and performance in DS-CDMA systems has been studied in [34]. An adaptive RRNS based multi-carrier modulation scheme for combating effects of frequency selective fading channels has been discussed in [35]. The performance of systematic and non-systematic RRNS codes and near-optimal decoding algorithms for soft decision decoding has been proposed in [37]. The similarities and advantages of RRNS over other non-binary codes like Reed-Solomon (RS) codes has been discussed in detail in [23],[25]-[27],[30]-[38].

Although some prior research has been done on applications of RRNS as channel code, strategies to incorporate RRNS techniques in MIMO has not received any consideration. Analyzing and quantifying the role of systematic and non-systematic RRNS based STBC design for MIMO wireless communications is the main objective of this work.

## 1.4 Overview of Thesis

In this thesis, both systematic and non-systematic RRNS codes [27][37] along with *direct mapping* and *indirect mapping* schemes are formulated as space-time block codes (STBCs) to support high performance, high-rate transmission. In contrast to orthogonal space-time block codes (OSTBCs) [20][19], RRNS-STBC does not require the channel to remain constant during its coding/decoding period. In our proposed scheme, information bits are first mapped to integers and based upon a predetermined moduli set, the corresponding residues are calculated. Then, the obtained residues are mapped to complex constellation symbols using the *direct mapping* (DM) scheme which is similar to the one discussed in [39]. While mapping information bits to residues, not all residue digits occur with equal probability. The unequal a priori probabilities of residues can be effectively exploited by the direct mapping scheme as it maps residues directly to constellation points. We propose a unique prior probability based distance-aware direct mapping (DA) scheme. In this scheme residues are mapped to complex symbol constellations in a distance aware manner using a set-partitioning approach, based on their a priori probabilities. Alternately, we also propose an *indirect mapping*(IM) scheme. In the proposed scheme, the residues are once again converted back to bits and then modulated by any  $M$ -ary complex constellation. Finally, the mapped symbols are constructed as space-time block codes and transmitted over multiple antennas. At the receiver, inverse operations including the use of Chinese Remainder Theorem (CRT)[30] to convert residues back to integers are implemented to recover the original information. We have derived upper bounds on the codeword and bit error probability of both non-systematic and systematic RRNS-STBC assuming ML detection and  $M$ -ary QAM

constellation. We also propose an Adaptive demapping scheme, which utilizes the RRNS code structure to decrease the ML decoding complexity and increase the error performance of the system. The analytical results clearly illustrate the achievable coding and diversity gains.

Using simulations, we compare the performance of systematic and non-systematic RRNS-STBC with OSTBC i.e., Alamouti scheme for a  $2 \times 2$  MIMO system and other concatenated STCs e.g., RS-STBC (Reed Solomon Codes concatenated with STBC). The simulation results clearly show the improvement provided by RRNS-STBC. With DA mapping, a further improvement in SNR (signal to noise ratio) of about 2dB for spatially multiplexed case and about 1dB for full diversity transmission case is obtained. The IM scheme also gives an improvement in SNR of about 1.5dB over DM. It is important to note that this gain comes at the cost of increased receiver complexity as compared to the Alamouti's scheme. The systematic RRNS-STBC is shown to give an improvement in performance over the non-systematic RRNS-STBC scheme for the same set of moduli.

The main advantage of the proposed schemes over other schemes like concatenated Reed-Solomon Codes as in [40] is that the hardware implementation in case of RRNS is highly modular i.e., same hardware can encode and decode codes with different parameters. The complexity of the CRT is of a higher order as compared to other schemes like the Mixed Radix Conversion(MRC) and Base Extension (BEX) [37]. In [41], decoding schemes having lower complexity have also been introduced. The complexity in our scheme is comparable to other concatenated STBCs as in [40],[42].

## 1.5 Key Contributions

Key contributions of this thesis are as follows:

- *Novel application of RRNS based channel codes as STBC:* We propose an unique application of Redundant Residue Number system based channel coding scheme coupled with direct mapping based M-ary modulation to design Space-time Block codes which

have a higher degree of freedom with respect to design parameters. This is a non-binary concatenated coding scheme which can be used in high data rate systems. The carry free property of RRNS ensures that error propagation within a codeword is eliminated. The concatenated code parameters can be changed to encode different block lengths without extensive change in hardware, thus making the implementation highly modular. In our paper [43], we design a system which enables the application of this scheme for encoding binary data streams.

- *Proposal of the unique probability based distance aware direct mapping (DA) scheme:* The direct mapping scheme optimizes the link between coded non-binary information symbols and complex constellation points. We propose a unique probability based distance aware (DA) direct mapping scheme. The scheme and associated performance improvements are discussed in detail in our papers [43]-[45]. This scheme takes advantage of the a priori probability distribution of the coded data symbols to map them intelligently to complex constellation points such that maximum distance separation is obtained between the symbols having highest probability of occurrence. We demonstrate the results for a 16-QAM constellation but the scheme in general can be extended to any complex constellation. The unique properties of RRNS channel codes make it possible to determine the probability of occurrence of residues, which is unique for a particular code. It is also shown that code parameters can be chosen so as to maximize the separation between highest probability sets of residues so that maximum utilization of the DA mapping scheme can be achieved.
- *Proposal of Indirect Mapping Scheme with modified IM scheme to improve transmission efficiency:* We also propose an alternative Indirect Mapping (IM) scheme where residues are converted back to bits before being mapped to the complex constellation using Gray coded bit assignment. A modified IM scheme has also been formulated in order to increase transmission efficiency by transmitting lesser number of bits than in the naive IM scheme. This is advantageous in cases where the difference between

the minimum and maximum residues in the residue set is quite large. We have shown that the IM scheme shows improvement in performance similar to the DA mapping scheme.

- *Proposal of an Adaptive Demapping Scheme:* We propose an adaptive demapping scheme [45], which exploits the RRNS code structure to decrease the total number of ML searches during hard decision decoding and improve the performance of the concatenated system. We have shown that the adaptive demapping scheme gives a 0.5 – 1.5 dB improvement in performance. We have also shown that the relative error performance, using DA mapped constellations is better than when a Gray coded direct mapped constellation is used. This implies that the adaptive demapping scheme can exploit the DA mapping scheme further and improve the error performance.
- *Upper bounds on the codeword error probability of both non-systematic and systematic RRNS-STBC are derived:* We analyze and quantify the probability of error performance of RRNS-STBC codes. We expound on the code construction for both non-systematic [43],[44] and systematic RRNS-STBC [45] and derive bounds on the codeword and bit error probability. We draw analogies with Reed Solomon (RS) codes and provide conditions under which RRNS codes can be approximated as RS codes. The expressions of probability bounds throw further light on advantages of the proposed RRNS-STBC scheme.
- *Achievable maximum diversity and coding gain assuming maximum likelihood decoding (MLD) are characterized:* We assume equal gain combining and maximum likelihood (ML) detection at the receiver to quantify the achievable performance of the RRNS-STBC schemes, which is treated in great detail in our papers [43]-[45]. RRNS introduces a new parameter in the STBC design which helps us to maximize the diversity gain based on the RRNS code parameters.
- *Performance gain relative Alamouti scheme and other concatenated space-time cod-*

*ing schemes is achieved:* In our papers, [43]-[45], it has been shown with the help of simulation results that the proposed RRNS-STBC scheme outperforms the Alamouti scheme. Other concatenated schemes like RS-STBC are also outperformed at low SNRs. The application of DA mapping brings about further improvement in RRNS-STBC schemes.

## 1.6 Organization

This thesis is divided into 6 chapters. In Chapter 2, the principles of RNS and RRNS arithmetic, encoding and decoding of binary information using RNS and RRNS, and their application as a channel code are discussed. Applications of RRNS encoding as error correcting codes and their decoding techniques are discussed and illustrated with examples. Chapter 3 introduces the direct and indirect mapping schemes. The DA mapping and adaptive demapping schemes are proposed and explained with suitable examples. In Chapter 4, we introduce the concept of RRNS based STBC design. We analyze the performance of both the Systematic and Non-systematic RRNS-STBC coding scheme and quantify the achievable coding and diversity gains. In Chapter 5, using simulation results, the performance of RRNS-STBC with OSTBC and other concatenated STBC schemes are compared. The performance of direct and indirect mapping schemes are also illustrated. Finally we conclude the thesis with Chapter 6, which summarizes the key contributions and conclusions and throws light on future work that can be done in this area.

# Chapter 2

## Residue Number System and Redundant Residue Number System

In this chapter, we introduce the mathematical framework for the RNS and RRNS. We introduce the concept of RRNS as a channel coding scheme and discuss the Non-systematic and Systematic approaches to RRNS encoding. We further discuss the decoding of RRNS based channel codes with the help of Chinese Remainder Theorem (CRT) and more practically viable alternative techniques like Base Extension Algorithm (BEX) and Mixed Radix Conversion (MRC). Examples are cited to illustrate the error detecting and correcting properties of RRNS codes.

### 2.1 RNS and RRNS Arithmetic

This section introduces the basic mathematical tools for converting any weighted number system to RNS and RRNS. The inverse transformation from RNS and RRNS back to the original number system is also introduced. For the inverse transform, conventional techniques using the CRT as well as alternative techniques like BEX and MRC are used.

#### 2.1.1 Residue Number System

RNS can be used to represent any weighted number system as a  $u$ -tuple residue sequence. It is defined by the choice of  $u$  number of positive integers  $m_i$  ( $i = 1, 2, \dots, u$ ), referred to as

**Table 2.1:** RNS REPRESENTATION OF INTEGER MESSAGES

Message $X$	RNS		
	$r_1$	$r_2$	$r_3$
$X_1 = 2$	2	2	2
$X_2 = 5$	0	5	5
$X_3 = 17$	2	3	8
$X_4 = 56$	1	0	2
$X_5 = 108$	3	3	0
$X_6 = 274$	4	1	4

moduli [29],[46]. Let  $N$  be any non- negative integer number in the range  $0 \leq N \leq \varrho^n$ , where  $\varrho$  is the radix of the weighted number system.  $N$  can be represented in weighted number system as  $N = \{b_{n-1}b_{n-2} \cdots b_2b_1b_0\} = \sum_{j=0}^{n-1} b_j \varrho^j$ , where  $b \in \{1, 2, \dots, \varrho - 1\}$ . If  $\varrho = 2$ , then it represents the weighted binary representation. Henceforth, in this thesis, we will assume that  $\varrho = 2$ , i.e., the weighted binary system will be used as we deal with information bits in binary and encoding of binary bits with non-binary channel codes.

The dynamic range of the RNS is defined by the interval  $[0, M_r - 1]$  where  $M_r = \prod_{i=1}^u m_i \geq \varrho^n$ . If all the moduli are pairwise relative primes to each other, any integer  $N$  which falls in the dynamic range can be uniquely and unambiguously denoted by the  $u$ -tuple residue sequence  $\{r_1, r_2, \dots, r_u\}$ , where  $r_i = N \bmod \{m_i\} = N - \lfloor \frac{N}{m_i} \rfloor m_i$  for  $i = \{1, 2, \dots, u\}$ ,  $\lfloor x \rfloor$  represents the largest integer not exceeding  $x$  and  $0 \leq r_i \leq m_i - 1$ . Thus the RNS representation of any integer  $N$  can be defined as:

$$\begin{aligned}
N &\Leftrightarrow (r_1, r_2, r_3, \dots, r_u), \quad 0 \leq N \leq M_r \\
r_i &= N \pmod{m_i}, \quad i = 1, 2, \dots, u.
\end{aligned} \tag{2.1}$$

**Example 2.1.1.** *In this example, we assume that the moduli set used for the RNS representation is  $m_1 = 5$ ,  $m_2 = 7$  and  $m_3 = 9$ . Table(2.1) illustrates the RNS representation of integer messages  $N$ . The dynamic range is  $[0, 314]$ , since  $M_r = (5 \times 7 \times 9) = 315$ . Thus any integer in this range can be unambiguously represent by the RNS, as shown in the table.*



**Table 2.2:** RRNS REPRESENTATION OF INTEGER MESSAGES

Message $X$	Non-redundant Residues			Redundant Residues		
	$r_1$	$r_2$	$r_3$	$r_4$	$r_5$	$r_6$
$X_1 = 2$	2	2	2	2	2	2
$X_2 = 5$	0	5	5	5	5	5
$X_3 = 17$	2	3	8	6	4	1
$X_4 = 56$	1	0	2	1	4	8
$X_5 = 274$	4	1	4	10	1	2
$X_6 = 320$	0	5	5	1	8	0

### 2.1.2 Redundant Residue Number System

An RNS can be designed not only for data representation but also for protection of data. In order to incorporate the capability of self checking and error control, RNS has to be designed with certain number of redundant moduli. A redundant RNS (RRNS) representation is obtained by appending  $(u - v)$  number of moduli  $\{m_{v+1}, m_{v+2}, \dots, m_u\}$  to the RNS consisting of  $v$  number of moduli. The RRNS representation consists of  $u$  positive, pairwise relative prime moduli, where  $\min\{m_{v+1}, m_{v+2}, \dots, m_u\} \geq \max\{m_1, m_2, \dots, m_v\}$  must hold. Now, the integer  $N$  is represented by a residue sequence  $\{r_1, r_2, \dots, r_u\}$  based on  $u$  number of moduli, forming a so-called RRNS( $u, v$ ) code. In this case the moduli  $m_1, m_2, m_3, \dots, m_v$  are called the information moduli, while  $m_{v+1}, m_{v+2}, \dots, m_u$  are the redundant moduli. The integer  $N$  is limited to the information dynamic range or the legitimate range  $[0, M_r]$ , where  $M_r = \prod_{i=1}^v m_i \geq \varrho^n$  and  $v \leq u$ . The range  $[M_r, M_r M_u]$ , where  $M_u = \prod_{i=v+1}^u m_i$ , is called the illegitimate range of the RRNS representation.

**Example 2.1.2.** *In his example, we illustrate the RRNS representation of an integer information  $X$ . To the moduli set used in Example(2.1.1), we append the redundant moduli  $m_4 = 11$ ,  $m_5 = 13$  and  $m_6 = 16$ . The legitimate range of the RRNS representation is still  $[0, 314]$ , while the illegitimate range is given by  $[315, 720720]$  since  $M_u = 11 \times 13 \times 16 = 2228$  and  $M_r M_u = 720720$ . Table(2.2) illustrates the RRNS representation. It can be seen that*

both  $X = 5$  and  $X = 320$  have the same Non-redundant Residue representation but different Redundant Residue. This is because the integer  $X = 320$  is in the illegitimate range and thus has no unique representation by the information moduli, i.e.,  $m_1, m_2, m_3$ .

### 2.1.3 Decoding of RNS and RRNS

To recover the integer information  $N$ , from the  $u$ -tuple residue representation of RNS and RRNS, Chinese Remainder Theorem (CRT)[29] is generally used. Since the implementation of CRT is computationally exhaustive, other methods such as the BEX along with MRC[47] are generally used. RRNS has a very important property, namely, that the integer information represented by the  $u$ -tuple residue digits can be recovered from any combination of  $v$  out of the total of  $u$  residues and their corresponding moduli. In the following subsections, CRT as well as BEX and MRC are discussed in detail.

#### Chinese Remainder Theorem

The CRT [28]-[30] is an important implementation of the reverse transformation from RNS and RRNS to the conventional weighted number system. According to the CRT, any  $u$ -tuple residue representation  $(r_1, r_2, \dots, r_u)$ , where  $0 \leq r_i \leq m_i$  for  $i = 1, 2, \dots, u$ , there exists one and only one integer  $N$  such that  $0 \leq N \leq M_r$  and  $r_i = N(\text{mod}m_i)$ . The numerical value of  $N$  can be computed according to the equation [23],[31]:

$$N = \sum_{i=1}^u r_i T_i M_i (\text{mod} M_r) \quad (2.2)$$

where,  $M_i = \frac{M_r}{m_i}$  and the coefficients  $T_i$  are computed apriori by the solving the congruences

$$T_i M_i = 1 (\text{mod} m_i) \quad (2.3)$$

$T_i$  are referred to as the multiplicative inverses of  $M_i$ . The congruence given in equation(2.3) can be simplified by the equation [46]:

$$\frac{T_i M_i}{m_i} - \left\lfloor \frac{T_i M_i}{m_i} \right\rfloor - \frac{1}{m_i} = 0 \quad (2.4)$$

After calculating  $M_i$  and  $T_i$ , the integer information  $N$  can be easily recovered using equation(2.2), given the residue sequence  $(r_1, r_2, \dots, r_u)$ .

**Example 2.1.3.** *The residue digits for representing the integer  $X_6 = 274$  are given, from Table(2.1), by  $r_1 = 4$ ,  $r_2 = 1$  and  $r_3 = 4$ . We use the CRT to recover the decimal value from the given residue representation. First,  $M_1$ ,  $M_2$  and  $M_3$  are calculated:*

$$\begin{aligned} M_1 &= \frac{M_r}{m_1} = \frac{5 \times 7 \times 9}{5} = 7 \times 9 = 63 \\ M_2 &= \frac{M_r}{m_2} = \frac{5 \times 7 \times 9}{7} = 5 \times 9 = 45 \\ M_3 &= \frac{M_r}{m_3} = \frac{5 \times 7 \times 9}{9} = 5 \times 7 = 35 \end{aligned}$$

The corresponding multiplicative inverses can be calculated by solving equation(2.3) or equation(2.4) for the corresponding  $M - i$  values:

$$M_1 = 63 \rightarrow T_1 = 2$$

$$M_2 = 45 \rightarrow T_1 = 5$$

$$M_3 = 35 \rightarrow T_1 = 8$$

Then using equation(2.2), we can recover  $X_6$  :

$$\begin{aligned} N &= [4 \times (63 \times 2) + 1 \times (45 \times 5) + 4 \times (35 \times 8)](\text{mod}315) \\ &= [504 + 225 + 1120](\text{mod}315) \\ &= [1849](\text{mod}315) \\ &= 274 \end{aligned}$$

which is the same integer  $X_6$  from Table(2.1)

For the case of RRNS we illustrate, with an example, the property of recovering integer information from a combination of any  $v$  residues of the total  $u$  residues.

**Example 2.1.4.** In this example we consider the RRNS representation of the integer  $X_6 = 274$  given in Table(2.2). The residues are given by  $r_1 = 4, r_2 = 1, r_3 = 4, r_4 = 10, r_5 = 1$  and  $r_6 = 2$ . We consider the  $v = 3$  residues  $r_1 = 4, r_3 = 4, r_6 = 2$  and their corresponding moduli  $m_1 = 5, m_3 = 9$  and  $m_6 = 16$ . Here we use  $M = 5 \times 9 \times 16 = 720$  in place of  $M_r = 315$  for solving the congruences. We use the CRT to recover the decimal value from the given residue representation. First,  $M_1, M_3$  and  $M_6$  are calculated:

$$\begin{aligned} M_1 &= \frac{M}{m_1} = 144 \\ M_3 &= \frac{M}{m_3} = 80 \\ M_6 &= \frac{M}{m_6} = 45 \end{aligned}$$

The corresponding multiplicative inverses can be calculated by solving equation(2.3) or equation(2.4) for the corresponding  $M - i$  values:

$$\begin{aligned} M_1 &= 144 \rightarrow T_1 = 4 \\ M_3 &= 80 \rightarrow T_1 = 8 \\ M_6 &= 45 \rightarrow T_1 = 5 \end{aligned}$$

Then using equation(2.2), we can recover  $X_6$  :

$$\begin{aligned} N &= [4 \times (144 \times 4) + 4 \times (80 \times 8) + 2 \times (45 \times 5)](\text{mod}720) \\ &= [5314](\text{mod}720) \\ &= 274 \end{aligned}$$

which is the same integer  $X_6$  from Table(2.2). Thus if we compare the results from example(2.1.3) with that from example(2.1.4), it can be seen that any  $v$ -tuple from the  $u$ -tuple residue and their corresponding moduli can be used to recover the integer information  $N$ , in case of an RRNS provided that  $0 \leq N < M_r$ .

## Base Extension Algorithm and Mixed Radix Conversion

CRT is a classical algorithm but its implementation is computationally intensive for large moduli values as deals with modular operations with a large value of  $M_r$ . Thus to avoid processing large numbers, the use of base extension (BEX) operation in conjunction with mixed radix conversion [47] has been frequented. Using mixed radix conversion, the integer information  $N$  can be represented in the form:

$$N = a_1 + a_2 m_1 + a_3 m_1 m_2 + \cdots + a_k \prod_{i=1}^{k-1} m_i + \cdots + a_u \prod_{i=1}^{u-1} m_i, \quad (2.5)$$

where,  $0 \leq a_k < m_k$  for  $k = 1, 2, \dots, u$  are the mixed radix digits and we have  $\prod_{i=1}^0 m_i = 1$ .

The mixed radix digits for a given residue sequence  $(r_1, r_2, \dots, r_u)$  can be computed as:

$$\begin{aligned} a_1 &= r_1, \\ a_2 &= ((r_2 - a_1)/m_1)(\text{mod}m_2), \\ a_3 &= (((r_3 - a_1)/m_1 - a_2)/m_2)(\text{mod}m_3) \\ &\dots \\ a_u &= (((\cdots((r_u - a_1)/m_1 - a_2)/m_2 - \cdots) - a_{u-1})/m_{u-1})(\text{mod}m_u) \end{aligned} \quad (2.6)$$

It has been shown that MRC is independent of large integer  $M_r$  and all operations are related to relatively small operands which are of the order of the moduli values. The following example illustrates the recovery of the same integer  $X_6 = 274$  from Table(2.1) using equation(2.5) and equation(2.6).

**Example 2.1.5.** *Using equation(2.6), we have:*

$$\begin{aligned} a_1 &= r_1 = 4 \\ a_2 &= ((r_2 - a_1)/m_1)(\text{mod}m_2) \\ &= ((1 - 4)/5)(\text{mod}7) \Leftrightarrow 5a_2 = -3(\text{mod}7) \rightarrow a_2 = 5 \\ a_3 &= ((r_3 - a_1)/m_1 - a_2)/m_2)(\text{mod}m_3) \\ &= ((4 - 4)/5 - 5)/7)(\text{mod}9) \Leftrightarrow 7a_3 = -5(\text{mod}9) \rightarrow a_3 = 7 \end{aligned}$$

Now, using equation(2.5), the integer information can be recovered:

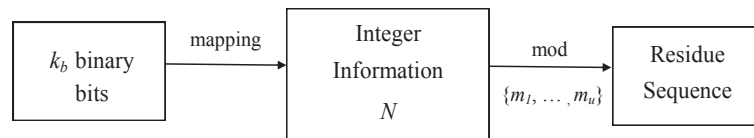
$$\begin{aligned}
 N &= a_1 + a_2m_1 + a_3m_1m_2 \\
 &= 4 + 5 \times 5 + 7 \times 5 \times 7 \\
 &= 274
 \end{aligned}$$

Thus it can be seen that the integer information can be retrieved without having to modulo operators large numbers when compared to the previous examples. All the integer operands are of the order of the moduli involved in RNS.

## 2.2 RRNS based Error Correcting Codes:

RRNS based  $u$ -tuple residue representation of any non-negative integer has the advantage that the original integer can be recovered from any combination of  $v$  out of the total  $u$  number of moduli. This property is the basis for the design of the RRNS based error correction codes. An RRNS scheme having  $v$  number of information moduli and  $u - v$  number of redundant moduli is denoted as an RRNS( $u, v$ ) code. The encoding operation of binary information bits using RRNS( $u, v$ ) code can be implemented using groups of bits to form binary coded decimal integers, which are then operated upon to generate the non-redundant and redundant residues. There are two encoding schemes, namely, the Non-systematic encoding and the Systematic encoding scheme.

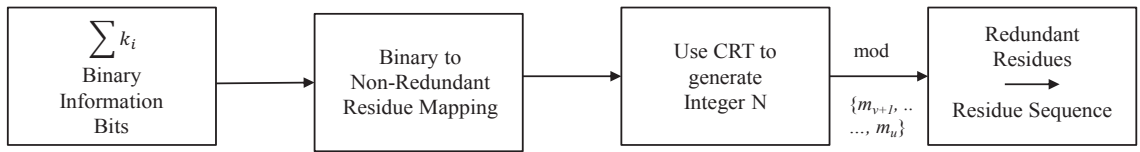
### 2.2.1 Non-systematic Encoding



**Figure 2.1:** Encoding procedure for Non-Systematic RRNS

Figure 2.1 shows the block diagram of the encoding procedure non-systematic RRNS i.e. binary to RRNS conversion. In the encoder,  $k_b$  bits are mapped to one integer  $N$ , where  $k_b = \lfloor \log_2 M_r \rfloor$  and  $\lfloor x \rfloor$  denotes the largest integer smaller than  $x$ . Then, corresponding residues are obtained by taking the modulus of  $N$  based upon the chosen set of moduli.

## 2.2.2 Systematic Encoding



**Figure 2.2:** *Encoding procedure for Systematic RRNS*

In Systematic RRNS, the information bits are mapped directly to residues. Figure 2.2 illustrates the systematic encoding scheme. For a moduli set  $\{m_1, \dots, m_u\}$ , the number of bits required to represent the residue corresponding to each modulus is given by  $k_i = \lfloor \log_2 m_i \rfloor$  for  $i = 1, 2, \dots, u$ . The input information bits are grouped into  $k_i$  binary bits and these bits from binary represented integers  $\{\mathcal{I}_i\} = 0, 1, 2, \dots, 2^{k_i} - 1$ . These integers are mapped to residue digits  $\{r_i\} = 0, 1, 2, \dots, m_i - 1$  according to the following rule:

- If a binary represented integer,  $\mathcal{I}_i$ , is in the range  $0 \leq \mathcal{I}_i \leq m_i - 1$ , then we assign residue  $r_i = \mathcal{I}_i$
- If a binary represented integer,  $\mathcal{I}_i$ , is in the range  $m_i \leq \mathcal{I}_i \leq 2^{k_i} - 1$ , then we assign residue  $r_i = 2^{k_i} - \mathcal{I}_i - 1$

Table(2.3) illustrates the mapping scheme. It can be seen that residues in the range  $[0, 2^{k_i} - m_i - 1]$  correspond to two different binary represented integers thus giving rise to a  $2 \rightarrow 1$  mapping. The remaining residues are  $1 \rightarrow 1$  mapped. In case of  $2 \rightarrow 1$  mapping, the hamming distance between two binary represented integers is maximized i.e.,  $k_i$ , thus

**Table 2.3:** MAPPING OF INFORMATION BITS TO RESIDUES FOR SYSTEMATIC RRNS ENCODING

Residue Digits	Binary represented integer	Binary Represented integer	
0	000...00	111...11	$2^{k_i} - m_i$ $2 \rightarrow 1$ mapping
1	000...01	111...10	
2	000...10	111...01	
...	.....	.....	
$2^{k_i} - m_i - 1$	.....	.....	$2m_i - 2^{k_i}$ $1 \rightarrow 1$ mapping
$2^{k_i} - m_i$	.....		
...	.....		
$m_i - 1$	.....		

the decoder can reliably differentiate between the two. The  $v$  residues thus obtained from the mapping and their corresponding moduli are used to generate an integer  $N$  with the help of CRT. This integer is then modulo divided by the  $u - v$  redundant moduli to obtain the redundant residues i.e.,  $r_i = N \bmod \{m_i\}$  for  $i = v, v + 1, \dots, u$ . Thus with the help of the systematic mapping scheme an information block of length  $\sum_{i=1}^k k_i$  is encoded into a Systematic RRNS( $u, v$ ) code.

The decoding of RRNS channel codes incorporating error detection and correction are discussed in the following section.

**Note:** For decoding the Systematic RRNS, two stages are required. In the 1st-stage decoding, the redundant and non-redundant residues are used to correct errors using CRT. In the 2nd-stage decoding, the non-redundant residues are mapped back to the binary information using the mapping as shown in Table(2.3). In case of residues with  $2 \rightarrow 1$  mapping, the binary represented integer with least hamming distance to the received binary representation of the given residue is selected.



## 2.3 Error Detection and Correction with RRNS

The unique properties of RRNS make it possible to use RRNS codes for efficient error detection and correction. Error correction decoding of RRNS codes has been studied in detail by Mandelbaum [48], Barsi and Maestrini [25], Sun, Lin and Krishna [28]-[30] and also by Hanzo et al [23],[27],[46]. Barsi and Maestrini developed the theory for single residue digit error correction while Sun, Lin and Krishna addressed the problem of double residue digit errors and simultaneous detection of multiple residue errors. The theory of RRNS( $u, v$ )-codes in terms of their error correcting capabilities have been consolidated into the so-called minimum distance decoding algorithm.

From the perspective of coding theory, the properties of RRNS( $u, v$ )-codes having  $v$ -information moduli and  $(u - v)$  redundant moduli can be summarized as follows:

- The Hamming weight of a code vector  $\mathbf{x}$  in an RRNS code is the number of non-zero residue components in  $\mathbf{x}$ .
- The Hamming distance between two RRNS codewords,  $d(\mathbf{x}_i, \mathbf{x}_j)$ , is the number of positions in which  $\mathbf{x}_i$  and  $\mathbf{x}_j$  differ.
- The maximum possible minimum Hamming distance  $\delta$  of an RRNS( $u, v$ )-code is defined as  $\delta = u - v + 1$ , provided  $\{m_1 < m_2 < \dots < m_v < m_{v+1} < \dots < m_u\}$ , i.e., the largest non-redundant residue is smaller than the smallest redundant residue.
- An RRNS( $u, v$ )-code can detect up to two  $(u - v)$  residue digit errors and correct up to  $t = \lfloor \frac{u-v}{2} \rfloor$  residue digit errors.

The error detection and correction capabilities of the RRNS( $u, v$ )-code can be explained with the help of the two following examples. The mechanisms of error correction are illustrated invoking the use of CRT, in general, the principle remains unchanged even if BEX and MRC are used.

**Example 2.3.1. Error Detection in RRNS:** Let's consider the moduli set  $\{3, 4, 5, 7\}$ , where  $\{3, 4, 5\}$  are the information moduli and 7 is the redundant modulus. The information dynamic range i.e., the legitimate range of the code is  $[0, M_r)$  where  $M_r = 3 \times 4 \times 5 = 60$ . Let the integer message to be encoded be  $N = 21$  which has the corresponding residue representation  $\{0, 1, 1, 0\}$ . Supposing there is an error in the residue digit  $r_3$  during transmission and it is changed from 1 to 3, i.e. the received residue sequence is  $\{0, 1, \tilde{3}, 0\}$ , then, following the CRT approach, using equation(2.2), we obtain:

$$\begin{aligned} N &= [20 \times (0 \times 2) + 15 \times (1 \times 3) + 12 \times (3 \times 3)](\text{mod } 60) \\ &= 33 \end{aligned}$$

However, we can verify that  $N = 33(\text{mod } 7) \neq r_4$ , hence we can conclude that there were errors in the RRNS representation. Hence and RRNS code with one redundant modulus can detect the residue digit error in  $r_3$ .

**Example 2.3.2. Error Correction in RRNS:** For this example, we invoke another redundant modulus, 11, such that information moduli set is  $\{3, 4, 5\}$  and redundant moduli set is  $\{7, 11\}$ . Encoding the same integer information  $N = 21$  with this RNS(5, 3) code yields the residue representation  $\{0, 1, 1, 0, 10\}$ . As in the previous example we suppose  $r_3$  has been changed from 1 to 3 due to transmission error such that the received residue set becomes  $\{0, 1, \tilde{3}, 0, 10\}$ . According to CRT, any integer in the information range i.e.,  $[0, 60)$  can be recovered by using any 3 of the moduli and their corresponding residues, if no errors are present.

We consider all possible combinations of 3 out of 5 moduli and their corresponding

residues in an attempt to recover  $N$ :

$$\begin{aligned}
(r_1, r_2, r_3) &= (0, 1, 3) &\Leftrightarrow X_{123} &= 33(\text{mod } 60), \\
(r_1, r_2, r_4) &= (0, 1, 0) &\Leftrightarrow X_{124} &= 21(\text{mod } 60), \\
(r_1, r_2, r_5) &= (0, 1, 10) &\Leftrightarrow X_{125} &= 21(\text{mod } 60), \\
(r_1, r_3, r_4) &= (0, 3, 0) &\Leftrightarrow X_{134} &= 63(\text{mod } 60), \\
(r_1, r_3, r_5) &= (0, 3, 10) &\Leftrightarrow X_{135} &= 153(\text{mod } 60), \\
(r_1, r_4, r_5) &= (0, 0, 10) &\Leftrightarrow X_{145} &= 21(\text{mod } 60), \\
(r_2, r_3, r_4) &= (1, 3, 0) &\Leftrightarrow X_{234} &= 133(\text{mod } 60), \\
(r_2, r_3, r_5) &= (1, 3, 10) &\Leftrightarrow X_{235} &= 153(\text{mod } 60), \\
(r_2, r_4, r_5) &= (1, 0, 10) &\Leftrightarrow X_{245} &= 21(\text{mod } 60), \\
(r_3, r_4, r_5) &= (3, 0, 10) &\Leftrightarrow X_{345} &= 98(\text{mod } 60),
\end{aligned}$$

where,  $X_{ijk}$  corresponds to the integer recovered using the  $i$ -th,  $j$ -th and  $k$ -th moduli and their corresponding residues. From the results we can observe that  $X_{134}, X_{135}, X_{234}, X_{235}$  and  $X_{345}$  are all in the illegitimate range i.e., their values are out the range  $[0, 60)$ . In the remaining cases, 4 out of 5 give the result 21. It can also be observed that all these results were recovered from 3 moduli without including the moduli  $m_3$ . Thus, we conclude that 21 is the correct result and that the residue corresponding to  $m_3$  i.e.,  $r_3$  is in error. The correct value for  $r_3$  can be easily computed as  $\hat{r}_3 = 21(\text{mod } 5) = 1$ .

## 2.4 Summary

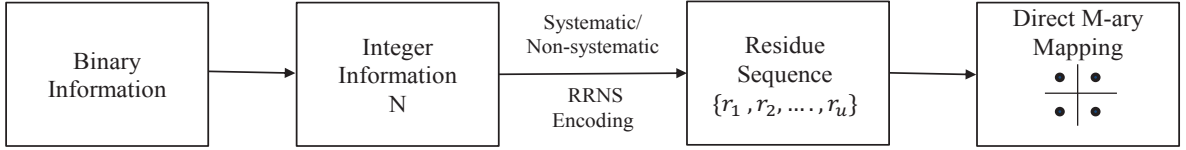
This chapter introduces the concept Residue Number System representation of non-negative integers and gives an outline of the mathematical operations involved in conversion of any weighted number system representation to RNS. The inverse transformation of RNS back to the weighted number system, using Chinese Remainder Theorem as well as BEX and MRC has been discussed. We also introduced the concept of error-checking and error-correction through the use of Redundant Residue Number System. The concept of RRNS as channel codes has been introduced and systematic and non-systematic encoding procedures have been investigated. A coding theory framework for RRNS based channel codes has been laid and error detection and error correction using RRNS codes has been illustrated with the aid of simple examples.

# Chapter 3

## Direct and Indirect Mapping Schemes

In this chapter, the methods for mapping non-binary information symbols to complex constellations for transmission over wireless channels are discussed. The link between information symbols and  $M$ -ary complex signal constellations is optimized by using the direct mapping scheme, where the symbols are mapped directly to constellation points using a one to one mapping. If the probability of occurrence of the information symbols are known a priori, then this information can be exploited to further optimize the mapping scheme. We propose an unique prior probability based distance aware (DA) direct mapping scheme, which exploits the probability of occurrence of residues in an RRNS channel coding scheme. We also propose an Indirect mapping scheme whereby, the residues are converted back to binary bits before being mapped to the  $M$ -ary constellation using binary bit assignment strategy.

In this chapter we discuss the mapping schemes from the perspective of being applied to RRNS based channel coded systems which is pertinent to the context of the thesis. We also propose an adaptive demapping scheme which exploits the code structure of the RRNS( $u, v$ )-code to reduce the complexity of the ML decoding and increase the error performance of the system.



**Figure 3.1:** *System Block for Direct Mapping*

### 3.1 Direct Mapping Scheme

In Figure 3.1, the binary information is first mapped to integer information and then encoded using non-systematic or systematic RRNS technique as discussed sections 2.2.1 and 2.2.2. The calculated residues are then mapped to  $M$ -ary complex constellation points before transmission. We discuss two different  $M$ -ary direct mapping schemes, namely, naive direct mapping and the proposed probability based distance aware(DA) direct mapping.

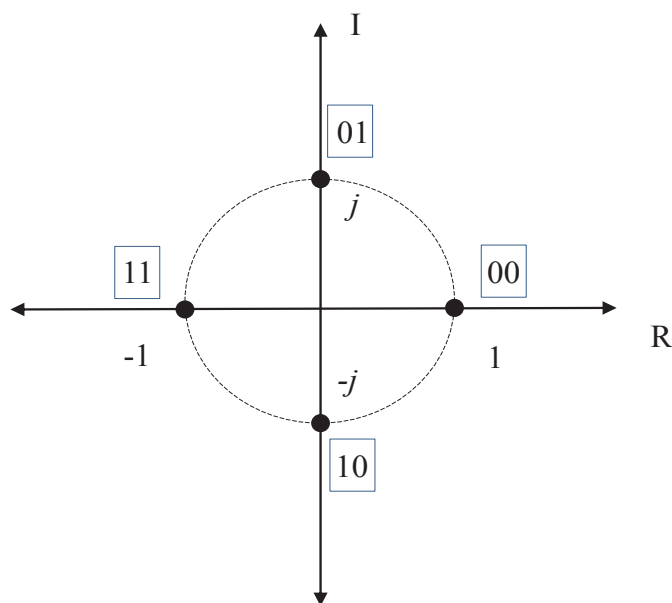
#### 3.1.1 Direct Mapping Scheme

In the direct mapping scheme, the calculated residues are directly mapped to complex constellation points. We notice that the available residue digits are in the range of  $[0, \max\{m_1, \dots, m_u\} - 1]$ . Therefore, we propose to map residue digits directly to  $M$ -ary (PSK/QAM) complex constellation points forming the so-called “direct-mapping” scheme. Here,  $M \geq \max\{m_1, \dots, m_u\} - 1$  must hold. Consequently, complex symbols corresponding to each of the residue digits are transmitted over wireless channels.

**Table 3.1:** DIRECT RESIDUES TO COMPLEX SYMBOLS MAPPING USING MODULUS 4

Residues	Bit Assignment	QPSK Symbols
0	00	1
1	01	$j$
2	10	$-j$
3	11	$-1$

**Example 3.1.1.** One illustrative example is given in Table(3.1) to characterize the “direct mapping” scheme in the case of  $\max\{m_1, \dots, m_u\} - 1 = 3$ . Since the maximum modulus value is 4, QPSK ( $M = 4$ ) and gray coded mapping is considered. The residues are mapped directly to the constellation points such that the  $\log_2 M$ -bit binary value of the residue is equal to binary gray coded bit assignment of the constellation point. The mapping is illustrated in Figure 3.2



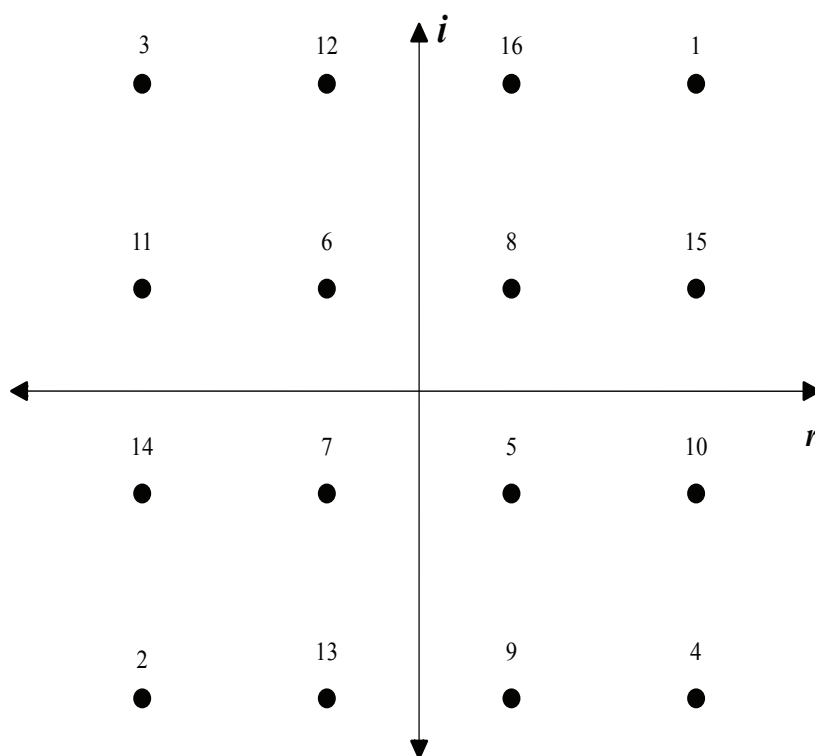
**Figure 3.2:** Gray Coded Direct Mapping for QPSK

### Probability Based Distance-Aware Direct Mapping

In case of non-systematic RRNS( $u, v$ ) code, when a random bit sequence is given as input and the residues are calculated as shown in Figure 3.1, the probability of occurrence of each of the  $u$  residues corresponding to each decimal integer information mapped from  $k_b$  bits, is different for every unique set of  $u$  moduli. In case of Systematic RRNS( $u, v$ ) code the probability of occurrence of  $v$  non-redundant residues and the  $u - v$  redundant residues corresponding to  $\sum_{i=1}^v k_i$  bit information block is considered. Thus for every RRNS( $u, v$ ) code, the range of possible residues is given by  $[0, \max(m_1, m_2, \dots, m_u) - 1]$ . The probabilities

of occurrence of these residues can be calculated apriori for a predetermined set of  $v$  primary moduli and  $u - v$  redundant moduli.

We exploit the apriori probability of occurrence of the residues by proposing a unique probability based distance-aware (DA) direct mapping scheme. After calculation of apriori probabilities, the residues are ranked in order of their probabilities, with the highest ranked residue being the one with the highest probability of occurrence. A set-partitioning approach is used to decompose constellation points into sets with maximum separation for the highest ranked residues according to their probability of occurrence.

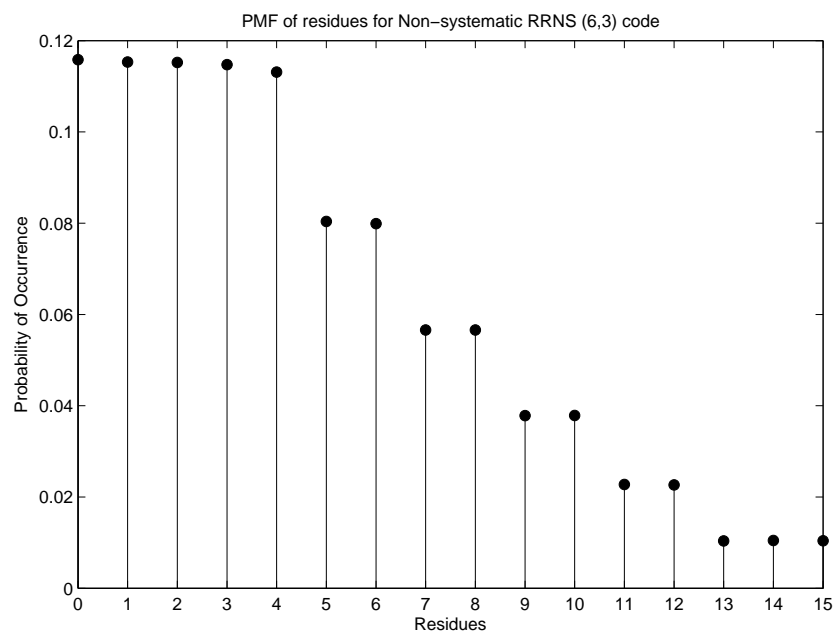


**Figure 3.3:** *Probability Based Distance-Aware Mapping Scheme for 16-QAM.*

Figure 3.3 illustrates the mapping scheme for 16-QAM. The numbers correspond to the probability of occurrence i.e., the rank of the particular residue. Number 1 denotes the most probable and 16 the least probable residue/symbol. The set of four most probable residues are mapped to the four corners of the constellation. The next set of four residues

are mapped diagonally across from them such that the least probable in this set is nearest to the most probable in the first set thus maintaining maximum distance possible among the most probable residues. The next two residue sets are mapped to points such that the convention is followed and the least probable surround the most probable residues from the first set. The scheme is general for any  $M$ -ary QAM constellation. For an 8-PSK constellation, the first set of four residues are mapped to points on the four axes and the next four are again mapped to the remaining constellation points such that the two least probable ones surround the most probable residue. For QPSK and BPSK, the same mapping scheme is applicable and the extension is trivial.

**Example 3.1.2.** For example, we consider a moduli set where  $m_o = \{5, 7, 9\}$  and  $m_r = \{11, 13, 16\}$ . The pmf (probability mass function) of the residues in the case of non-systematic RRNS(6,3) code is shown in Figure 3.4.



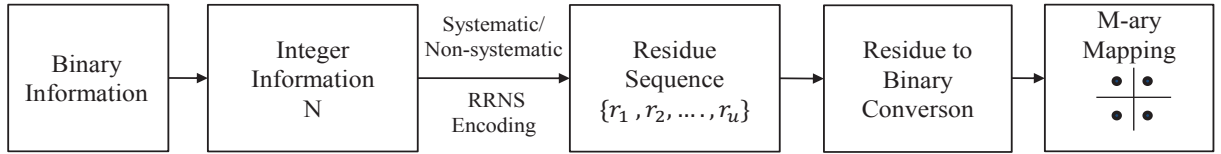
**Figure 3.4:** Probability mass function for  $m_o = \{5, 7, 9\}$  and  $m_r = \{11, 13, 16\}$ .

It can be seen from Figure 3.4, that the residues can be ranked according to probability



in the order  $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 10, 9, 11, 12, 14, 15, 13\}$ , where the position of each residue in the set is its rank. Here, we see that  $\max\{r\} = \max\{m_1, \dots, m_u\} - 1 = 15$ . Thus, for this case, we can use a 16-QAM constellation for mapping the residues. Thus the residue 0, which has highest probability of occurrence has the highest rank i.e 1 and the residue 13 with the lowest probability of occurrence has the lowest rank, 16. The mapping scheme is illustrated in Figure 3.3.

## 3.2 Indirect Mapping Scheme



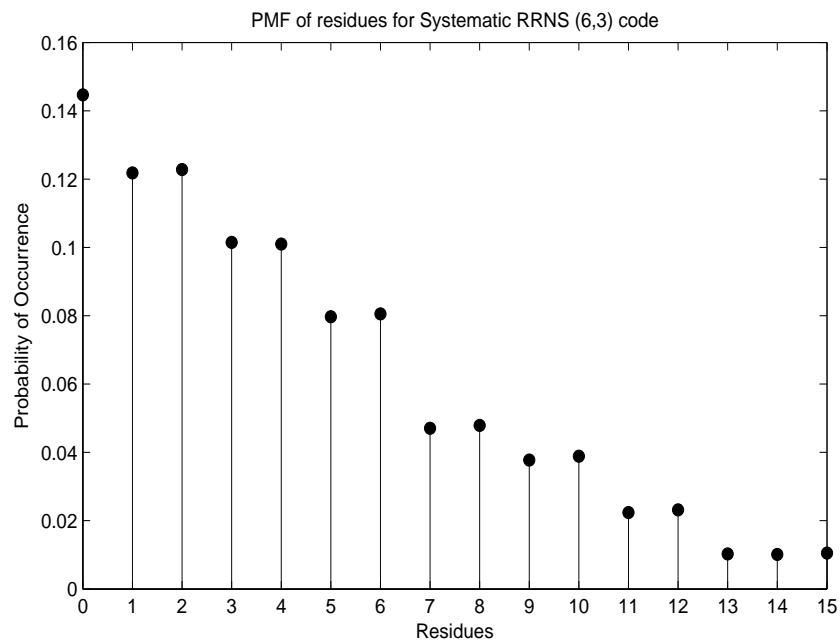
**Figure 3.5:** System Block for Indirect Mapping

An alternative to the direct mapping scheme is the indirect mapping scheme (IM). In this scheme, we convert the residues back into bits before mapping them to complex constellations as illustrated in Figure 3.5. Each residue is converted into an “ $n$ ” bit binary number, where  $n = \lceil \log_2(\max\{m_1, \dots, m_u\}) \rceil$ . After conversion to bits, the bit sequence is modulated by any  $M$ -ary scheme using Gray coded bit assignment. There are no limitations to the scheme chosen in this case as “ $M$ ” has no relation to the  $\max\{m_1, \dots, m_u\}$ . Thus in this scheme we can use any moduli set for the RRNS( $u, v$ ) code with any given  $M$ -ary modulation scheme. This scheme provides better performance than the naive direct mapping scheme owing to the fact that the a priori probability of residues has a lesser effect after conversion to binary before mapping to  $M$ -ary constellation. However this comes at the cost of greater number of transmitted symbols as opposed to the Direct and DA mapping schemes.

In the case of RRNS coding schemes, one alternative is to modify the IM scheme such that

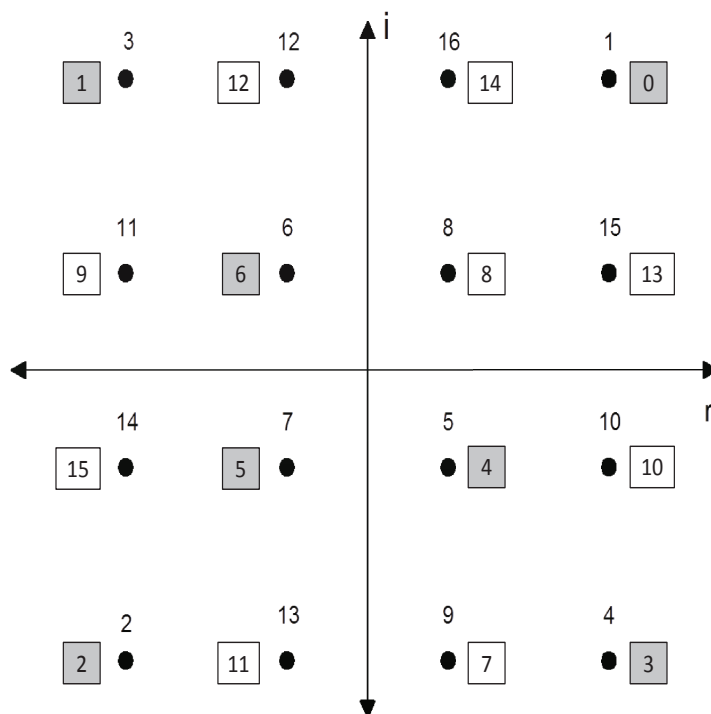
all residues are not converted back to “ $n$ ”-bit binary numbers. We can exploit the coding structure and modularity of the RRNS to optimize the number of symbol transmissions. Since the moduli for an RRNS( $u, v$ ) code are fixed, the residue  $r_i$  corresponding to moduli  $m_i$  can have a maximum value  $m_i - 1$ . Thus the residue corresponding to moduli  $m_i$  can be represented by  $n_i = \lceil \log_2(m_i) \rceil$  bits for  $i = 1, \dots, u$ . Thus residues corresponding to each moduli can be represented by less than  $n$  bits. Using this scheme, we save  $n - n_i$  bits,  $i = 1, \dots, u$ , for each residue to binary conversion before  $M$ -ary mapping. This gives fewer symbols than the original IM scheme. This is especially true if the range of the moduli set is large and the largest modulus is much larger than the smallest one. In this case  $n$  would be much larger than the  $n_i$  for the smaller moduli and we would transmit redundant bits thereby decreasing transmission efficiency and wasting valuable power resources.

### 3.3 Adaptive Demapping Scheme



**Figure 3.6:** Probability Mass Function for Systematic RRNS(6, 3)-STBC with moduli set  $m_o = \{5, 7, 9\}$ ;  $m_r = \{11, 13, 16\}$

The receiver detects the Direct mapped and DA mapped residues using an ML decoder. After the noise corrupted symbol is received, the ML decoder searches for the nearest point in the  $M$ -ary constellation by searching for shortest among  $M$  distances[43],[44]. We use 16-QAM as an example. We consider a Systematic RRNS(6,3)-STBC, having moduli set  $m_o = \{5, 7, 9\}$  and  $m_r = \{11, 13, 16\}$ . The residues are mapped to the QAM constellation using DA mapping scheme as discussed in 3.1.1. In this section, we propose an adaptive  $M$ -ary demapping scheme that can reduce the complexity of ML decoding while increasing error performance relative to the DA mapping scheme without adaptive demapping. Figure 3.6, shows the probability mass function (pmf) of the RRNS(6,3)-STBC. The residues have different apriori probabilities of occurrence and can be ranked according to decreasing probability of occurrence, in the order:  $\{0, 2, 1, 3, 4, 6, 5, 8, 7, 10, 9, 12, 11, 15, 13, 14\}$ .

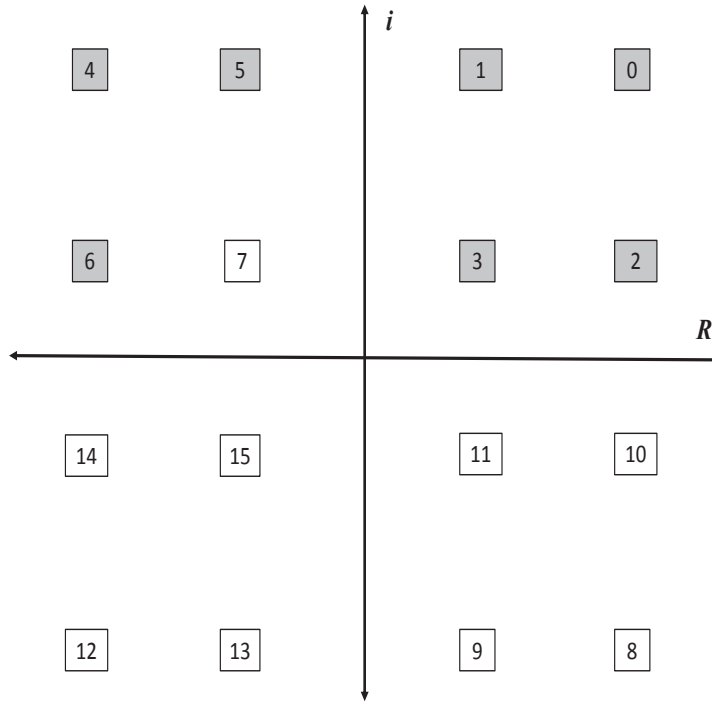


**Figure 3.7:** *Probability based DA Mapping and Smart Demapping Scheme for 16-QAM*

Figure 3.7 shows the scheme for DA mapping and adaptive demapping. The numbers

beside the constellation points denote the rank of the residues, while the numbers in the boxes are the actual residues. For the adaptive demapping scheme, we use the coding structure of the RRNS( $u, v$ ) code to reduce the number of ML searches. The receiver keeps track of the number of blocks, each consisting of  $u$  received residues. In each block, the 1st residue corresponds to the modulus  $m_1$  and so on, i.e., the  $u$ -th residue corresponds to the last modulus  $m_u$ . For example, we consider the 2nd residue of the block. For the RRNS(6,3)-STBC, this corresponds to the modulus  $m_2 = 7$ . Thus the range of residues resulting from this modulus is  $[0, m_i - 1] \rightarrow [0 - 6]$ . In the adaptive demapping scheme, for every 2nd residue in the block of 6 received residues, we search only for the points in the constellation corresponding to mapped residues, which are in the range of possible values for that particular position i.e., 0 – 6. In Figure 3.7, the points marked by gray boxes are the residues which are used for the ML search for each received residue which corresponds to  $m_2 = 7$ . Thus, in general, we reduce the number of ML searches for each received residue from  $M$  to  $m_i$  for the  $i$ -th residue in every block of  $u$  received residues. For every block i.e., codeword, we have  $\sum_{i=1}^u (M - m_i)$  number of *less* searches compared to exhaustive ML decoding. By not searching for the non-occurring residues, this scheme eliminates more errors in the demapping than traditional ML decoders. This, in turn, leads CRT (or MRC/BEX) to correct more errors for a particular RRNS( $u, v$ ) code when adaptive demapping is used. As a result adaptive demapping effectively and dynamically increases the free distance of the RRNS( $u, v$ ) code and accounts for better performance. The simulation results for both Systematic and Non-systematic RRNS-STBC in Chapter 5 justify our claim.

NOTE: It is to be noted that the adaptive demapping exploits the DA mapping scheme in a better manner. For the case discussed here, we can see the the possible residues are distributed in a manner that they are separated by the maximum possible distance. In case of a Direct Mapping scheme however, the residues are mapped according to a Gray coded scheme and the residues 0 – 6, as in the example, will not be separated by the maximum



**Figure 3.8:** *Gray coded Direct Mapping and Adaptive Demapping scheme for 16-QAM using modulus 7.*

possible distance. In this case, most of them will lie in the 1st and 2nd quadrants of the constellation map. This is illustrated in Figure 3.8. The colored boxes indicate the residues that will be searched in the ML decoding corresponding to the modulus 7. On comparing Figures 3.7 and 3.8, it can be seen that the DA mapping scheme offers wider separation between the chosen residues than the naive Gray coded scheme. This would result in a relatively lesser performance improvement in the case when adaptive demapping is applied to Gray coded direct mapped constellations as compared to a DA mapped constellation. However, even in this case, it reduces the decoding complexity by reducing the number of ML searches, but gives around 0.5dB improvement in performance as illustrated in Chapter 5.

## 3.4 Summary

This chapter discussed the methods for mapping residue digits to complex  $M$ -ary constellation. Two basic mapping methods were introduced - the DM scheme and the IM scheme. The DM scheme optimizes the link between the residue digits and the complex constellation points by mapping residue directly on a one to one basis. We have proposed an unique prior probability based DA mapping scheme which exploits the unique prior probability of occurrence of residues for a given moduli set, to provide maximum separation between residues with highest probability of occurrence. The direct mapping however imposes a restriction on the dimension of constellation that can be used, based on the maximum moduli value of the RRNS( $u, v$ ) code. The IM scheme removes this restriction, by converting the residues back to binary bits and then mapping the bits to complex constellations. We have also proposed an adaptive  $M$ -ary demapping scheme, which reduces the complexity of the ML decoding and increases the error performance of the concatenated code.

# Chapter 4

## Redundant Residue Number System based STBC Design

In this chapter, we discuss the application of RRNS based channel codes to the design of space-time block codes (STBC) for MIMO wireless Communications. The system model used for the analysis of RRNS-STBC is described and the design parameters are identified. The performance of both non-systematic and systematic RRNS-STBC is quantified and the effect of using RRNS is analyzed from the perspective of coding and diversity gain of the system. The RRNS-STBC introduces a new parameter for quantifying the diversity gain of the MIMO system.

### 4.1 System Model



**Figure 4.1:** *The block diagram of RRNS-STBC coded  $2 \times 2$  MIMO system*

The RRNS-STBC scheme is a concatenated channel code [49], with *M-ary* modulation and STBC together acting as the inner code and RRNS being the outer code. Figure 4.1 illustrates the system block for RRNS-STBC based  $2 \times 2$  MIMO system. The binary information is first mapped to integers. For non-systematic RRNS,  $k_b$  bits are grouped

together and converted to decimal integer  $N$ , while for systematic RRNS,  $\sum_{i=1}^v k_i$  bits are grouped together to form integer information  $N$ . The integer  $N$  is then encoded using RRNS( $u, v$ ) channel code. The residues from RRNS( $u, v$ ) encoding are mapped to complex symbols using any of the three aforementioned mapping schemes. The symbols are then grouped together into blocks of  $M_T \times T$ , where  $T$  is the number of time slots used for the RRNS-STBC code and  $M_T$  is the number of transmit antennas. At the receiver the received codeword is of dimension  $M_R \times T$ , where  $M_R$  is the total number of receive antennas. At the receiver, the inverse operations are performed. Firstly, Maximum Likelihood decoding and STBC demapping is performed. Then the complex symbols are demapped to residue digits using the exact inverse of the mapping operation, based whichever mapping scheme among DM, DA mapping or IM is used. The residues are then decoded into integer information using RRNS decoding schemes as discussed in Chapter 2. Finally the integer information is converted back into binary bits.

Different transmission mechanisms are used to transmit the RRNS-STBC over wireless channels. In case of spatially multiplexed RRNS-STBC, all the  $M_T \times T$  symbols are unique. However, in case of full diversity transmission, the code block is formed by choosing  $T$  symbols and transmitting the same  $T$  symbols across  $M_T$  antennas. Other conventional STBC techniques such as the Alamouti scheme [19] and higher order orthogonal schemes for  $M > 2$ , as in [20], can be used as the inner code without any loss of generality.

## 4.2 Performance Analysis

In this section, we analyze the performance of RRNS based STBC coded MIMO systems. We denote the transmitted  $M_T \times T$  codeword as  $\mathbf{X}$ . The received  $M_R \times T$  block code  $\mathbf{Y}$  is then given by,

$$\mathbf{Y} = \mathbf{H}\mathbf{X} + \mathbf{N}, \quad (4.1)$$

where,  $\mathbf{H}$  is the  $M_R \times M_T$  channel matrix with each entry distributed according to  $\mathcal{CN}(0, 1)$ ;  $\mathbf{N}$  is a  $M_R \times T$  complex Gaussian noise matrix with each entry distributed according to



$\mathcal{CN}(0, \frac{1}{2}N_0)$ .

For Direct and Indirect mapping using Gray coded QAM/PSK constellations, it is assumed that the mapped symbols are equiprobable. At the receiver, assuming maximum likelihood decoding (MLD), the output codeword  $\hat{\mathbf{X}}$  corresponds to

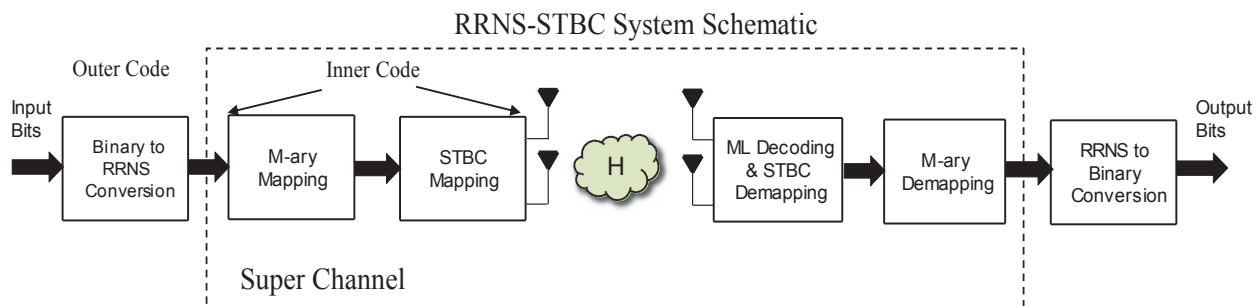
$$\hat{\mathbf{X}} = \arg \min_{\mathbf{X} \in \mathcal{R}^{M_T \times T}} \|\mathbf{Y} - \mathbf{H}\mathbf{X}\|^2, \quad (4.2)$$

where the minimization is taken over all possible input STBCs  $\mathcal{R}^{M_T \times T}$ .

For the case of DA mapping, the fact that the  $M$  symbols are not equiprobable, as a result of RRNS coding, is taken into account. Therefore the output codeword  $\hat{\mathbf{X}}$  corresponds to

$$\hat{\mathbf{X}} = \arg \min_{\mathbf{X} \in \mathcal{R}^{M_T \times T}} \|\mathbf{Y} - \mathbf{H}\mathbf{X}\|^2 - 2\sigma^2 \ln P(\mathbf{X}), \quad (4.3)$$

where,  $\sigma^2$  is the variance of the channel noise and  $P(\mathbf{X})$  is the apriori probability of generation of the codeword  $\mathbf{X}$ .



**Figure 4.2:** The block diagram for performance analysis of RRNS-STBC coded  $2 \times 2$  MIMO system

From Figure 4.2, it can be seen that for the proposed RRNS-STBC scheme, the STC acts as the inner code and the RRNS as the outer code. The mapping scheme and modulation together with the inner STC serves as a super channel for the RRNS encoder. The pairwise error probability of the STC is evaluated and this is used as the symbol error probability of the super channel, for evaluation of the RRNS codeword error probability. In subsection 4.2.1, the upper bound on the STC pairwise codeword error probability is evaluated. The

average codeword error probability and bit error probability of the Non-systematic and Systematic RRNS-STBC, for error correction only, is analyzed in subsections 4.2.2 and 4.2.3 respectively.

### 4.2.1 STC Pairwise Error Probability

Assuming  $M$ -QAM constellation, the probability that the transmitted codeword  $\mathbf{X}_i$  is mistaken for another codeword  $\mathbf{X}_j$  (also known as the pairwise error probability (PEP)) [16] is

$$P(\mathbf{X}_i, \mathbf{X}_j | \mathbf{H}) = Q \left( \sqrt{\frac{\rho \|\mathbf{H}\mathbf{E}_{i,j}\|_F^2}{2M_T}} \right), \quad (4.4)$$

where,  $\mathbf{E}_{i,j} = \mathbf{X}_i - \mathbf{X}_j$  is the  $M_T \times T$  codeword difference matrix,  $Q(\cdot)$  is the  $Q$ -function, and  $\rho = \frac{E_b k_b}{u N_0}$  is the average SNR at the receive antenna in a SISO fading link, which accounts for the change in SNR due to redundancy in the RRNS code. Applying Chernoff bound and averaging over all channel realizations, (4) can be upper bounded as [16]

$$P(\mathbf{X}_i, \mathbf{X}_j) \leq \prod_{k=1}^{r(\mathbf{G}_{i,j})} \left( \frac{1}{1 + \rho \lambda_k(\mathbf{G}_{i,j})/4M_T} \right)^{M_R}, \quad (4.5)$$

where,  $\lambda_k$  is the  $k$ -th non-zero eigenvalue of  $\mathbf{G}_{i,j} = \mathbf{E}_{i,j} \mathbf{E}_{i,j}^H$ , and  $r(\mathbf{G}_{i,j})$  is the rank of  $\mathbf{G}_{i,j}$ . Hence, the symbol/residue error probability,  $P_s$ , can be upper bounded as [50],[51]

$$P_s \leq \sum_{i=1}^{N_c} P(\mathbf{X}_i) \sum_{j \neq i}^{N_c} P(\mathbf{X}_i, \mathbf{X}_j), \quad (4.6)$$

where,  $N_c$  is the total number of codewords and  $P(\mathbf{X}_i)$  is the probability that the codeword  $\mathbf{X}_i$  is transmitted. When the codewords are equiprobable, equation (4.6) reduces to:

$$P_s \leq \frac{1}{N_c} \sum_{i=1}^{N_c} \sum_{j=1, j \neq i}^{N_c} P(\mathbf{X}_i, \mathbf{X}_j), \quad (4.7)$$

When the DA mapping scheme is used, the union bound in equation (4.6) changes as we utilize unequal prior probabilities of occurrence of the residues. Therefore, the  $P(\mathbf{X}_i)$  are different for each codeword. As a result, during symbol by symbol ML detection, the

decision boundaries are scaled according to the prior probabilities of each symbol. Thus, in the DA mapping case,  $\hat{\mathbf{X}}$  becomes more accurate and the performance bound is lowered. As a result, the DA mapping scheme is expected to provide better error performance than normal gray coded QAM mapping with ML decoding.

**Lemma 1.** *The number of possible codewords  $N_c^s$ , in case of Systematic RRNS, is greater than the number of possible codewords,  $N_c^{ns}$ , in Non-Systematic RRNS, when the same set of moduli are used.*

**Proof:** This is accounted for by the fact that in Systematic mapping the whole range of legitimate codewords i.e.,  $M_r$  is used. This gives  $N_c^s = M_r$ . Whereas in case of Non-Systematic mapping,  $N_c^{ns} = 2^{\lceil \log_2 M_r \rceil}$ . Thus we have,

$$N_c^{ns} = 2^{\lceil \log_2 M_r \rceil} \leq 2^{\log_2 M_r} \leq N_c^s \quad (4.8)$$

The equality holds when the legitimate range  $M_r$  is a perfect square number. ■

The total range, including the illegitimate range, of the RRNS code is given by  $M_T = \prod_{i=1}^u m_i$ . It is also clear that both Systematic and Non-Systematic RRNS codeword sets cannot be comprised of all possible combinations of residues  $0 \leq r_i \leq \max\{m_i\} - 1$  for  $i = 1 \cdots u$ . Depending on the integers operated upon, the combinations of residues in the codeword are determined. This differentiates RRNS from other non-binary block codes like RS codes.

Since  $N_c^s \geq N_c^{ns}$ , the bound in equation(4.6) becomes more accurate for Systematic RRNS than for Non-Systematic RRNS. The  $\mathbf{E}_{i,j}$  are calculated on a larger codeword set in Systematic than on Non-Systematic leading to lesser  $P_s$  in the Systematic case. Now,  $N_T - N_c^s \leq N_T - N_c^{ns}$ . Thus, the number of codewords that can be erroneously detected in case of Systematic RRNS-STBC is less than Non-Systematic RRNS-STBC and hence, the performance in the case of Systematic is better than Non-Systematic RRNS-STBC.

## 4.2.2 Non-Systematic RRNS-STBC

### Codeword Error Probability

Let the error probability of the residue digit corresponding to each moduli  $m_i$  for  $i = 1 \cdots u$ , in the RRNS-STBC codeword be defined as  $p_i(e)$ . For an RRNS( $u, v$ ) code,  $t = \lfloor \frac{1}{2}(d_{min} - 1) \rfloor$  is the maximum number of errors that can be corrected by the code and  $d_{min} = \chi = u - v + 1$  is the maximum possible minimum-distance of the RRNS ( $u, v$ ) code. The probability of correct decoding in the case of Non-systematic RRNS-STBC can be expressed as [27] :

$$P_C^{ns} = \sum_{\lambda=0}^t \left\{ \sum_{Q(\lambda)} \left[ \underbrace{\prod_{\{\alpha\}_\lambda} p_\alpha(e)}_{\lambda \text{ terms}} \underbrace{\prod_{\{\beta\}, \{\beta\} \neq \{\alpha\}} (1 - p_\beta(e))}_{(u-\lambda) \text{ terms}} \right] \right\}, \quad (4.9)$$

where  $Q(\lambda)$  represents  $\lambda$  errors out of the  $u$  received residue digits in a codeword,  $\sum_{Q(\lambda)}$  represents all possible combinations of  $\lambda$  elements out of possible  $1, 2, \dots, u$ . Also,  $\{\alpha\}_\lambda$  represents the set of residue digits corresponding to the positions of the  $\lambda$  errors while  $\{\beta\}$  represents the set of residue digits corresponding to the positions of  $(n - \lambda)$  residue digits which are not in error. We define  $\prod_{\{\alpha\}_\lambda} (\cdot) = 1$ , when the set  $\{\alpha\}_\lambda$  is empty i.e. there are no residue digit errors. For minimum-distance decoding, the received vector is decoded to an incorrect codeword, only if the vector is within the incorrect codeword's error-correction decoding sphere. Apart from the correct codeword's error-correction decoding sphere, there are  $(N_c^{ns} - 1)$  other legitimate decoding spheres, corresponding to  $N_c^{ns}$  legitimate information messages. The number of *all* vectors having a distance ' $i$ ' from a transmitted codeword is given by:

$$V_i = \sum_{Q(\lambda)} \prod_{\{\beta\}_i} (m_\beta - 1), \quad (4.10)$$

and distance is calculated by the number of positions in which the vector differs with the codeword. The set  $\{\beta\}_i$  contains the positions corresponding to the  $i$  number of residues for each of the  $Q(\lambda)$  combinations. In the incorrect decoding sphere, the total number of

vectors can be expressed as [27]:

$$S_{IC}^{ns} = (N_c^{ns} - 1) \sum_{\alpha=0}^t \sum_{Q_{(\alpha)}^{(u)}} \prod_{\{\beta\}_{\alpha}} (m_{\beta} - 1), \quad (4.11)$$

and the total number of  $M_T$  vectors in the coding space, except those within the error-correction decoding sphere of the correct codeword, can be expressed as [27]:

$$S = M_T - \sum_{\alpha=0}^t \sum_{Q_{(\alpha)}^{(u)}} \prod_{\{\beta\}_{\alpha}} (m_{\beta} - 1), \quad (4.12)$$

where, the set  $\{\beta\}_{\alpha}$  contains the positions corresponding to the  $\alpha$  number of residues for each of the  $Q_{(\alpha)}^{(u)}$  combinations. Thus the codeword error probability is given as:

$$P_E^{ns} = \frac{S_{IC}^{ns}}{S} (1 - P_C^{ns}), \quad (4.13)$$

where  $P_C^{ns}$  is given by equation(4.9). The RRNS  $(u, v)$  code is similar to RS Codes provided  $\min\{m_{v+1}, \dots, m_u\} \geq \max\{m_1, m_2, \dots, m_v\}$  holds [27]. If the moduli are relatively close to each other i.e. they can be approximated by using their average value, the weight distribution of RRNS codes can be approximated using the weight distribution of RS codes [30]. For “error-correction-only” [27],[46] the codeword error probability in equation(4.13) can be simplified by replacing each moduli,  $m_1, m_2, \dots, m_u$ , by their average value  $q$  and error probabilities of the residue corresponding to each modulus, i.e.,  $p_1(e), p_2(e), \dots, p_u(e)$  by value of the channel symbol error probability,  $P_s$ . Thus equation(4.13) simplifies to:

$$P_E^{ns} = \frac{S_{IC}^{ns}}{S} \sum_{\lambda=t+1}^u \binom{u}{\lambda} P_s^{\lambda} (1 - P_s)^{u-\lambda} \quad (4.14)$$

**Lemma 2.** *The codeword error probability of Non-Systematic RRNS-STBC can be upper bounded by:*

$$P_E^{ns} \leq \frac{S_{IC}^{ns}}{S} (N_c^{ns} - 1) 2^u P_s^{\chi/2}, \quad (4.15)$$

**Proof:** See Appendix(A). ■

**Lemma 3.** *The codeword error probability  $P_C^{ns}$  for the case of equiprobable codewords can be further simplified in the high SNR region as:*

$$P_E^{ns} \leq \frac{S_{IC}^{ns} (N_c^{ns} - 1) 2^u [N_c^{ns} (N_c^{ns} - 1)]^{r(\mathbf{G}_{i,j})}}{S \left[ \prod_{k=1}^{r(\mathbf{G}_{i,j})} \lambda_k(\mathbf{G}_{a,b}) \right]^{M_R}} \times \left( \frac{\rho}{4M_T} \right)^{-r(\mathbf{G}_{i,j}) M_{RX}/2}. \quad (4.16)$$

**Proof:** By substituting equation (4.7),(4.5) into equation(4.15), we have:

$$\begin{aligned} P_E^{ns} &\leq \frac{S_{IC}^{ns}}{S} (N_c^{ns} - 1) 2^u P_s^{\chi/2} \\ &\leq \frac{S_{IC}^{ns}}{S} (N_c^{ns} - 1) 2^u \times \left[ \frac{1}{N_c^{ns}} \sum_{i=1}^{N_c^{ns}} \sum_{j=1, j \neq i}^{N_c^{ns}} P(\mathbf{X}_i, \mathbf{X}_j) \right] \\ &\leq \frac{S_{IC}^{ns}}{S} (N_c^{ns} - 1) 2^u \times \left[ \sum_{j=1}^{N_c^{ns}} \sum_{i=1, i \neq j}^{N_c^{ns}} \prod_{k=1}^{r(\mathbf{G}_{i,j})} \left( \frac{1}{1 + \rho \lambda_k(\mathbf{G}_{i,j}) / 4M_T} \right)^{M_R} \right]^{\chi/2} \\ &\leq \frac{S_{IC}^{ns}}{S} (N_c^{ns} - 1) 2^u \times \prod_{k=1}^{r(\mathbf{G}_{i,j})} \left[ \sum_{j=1}^{N_c^{ns}} \sum_{i=1, i \neq j}^{N_c^{ns}} \left( \frac{1}{1 + \rho \lambda_k(\mathbf{G}_{a,b}) / 4M_T} \right)^{M_{RX}/2} \right] \\ &\leq \frac{S_{IC}^{ns}}{S} (N_c^{ns} - 1) 2^u [N_c^{ns} (N_c^{ns} - 1)]^{r(\mathbf{G}_{i,j})} \times \prod_{k=1}^{r(\mathbf{G}_{i,j})} \left[ \left( \frac{1}{1 + \rho \lambda_k(\mathbf{G}_{a,b}) / 4M_T} \right)^{M_{RX}/2} \right], \end{aligned} \quad (4.17)$$

where,

$$\lambda_k(\mathbf{G}_{a,b}) = \min_{1 \leq i, j \leq N_c^{ns}, i \neq j} \lambda_k(\mathbf{G}_{i,j}).$$

In high SNR regime,  $\rho \gg 1$  and equation(4.17) can be further simplified as equation(4.16). ■

From equation (4.16), we observe that for RRNS( $u, v$ )-STBC, the coding gain mainly depends on the term  $\left[ \prod_{k=1}^{r(\mathbf{G}_{i,j})} \lambda_k(\mathbf{G}_{a,b}) \right]^{M_R}$ , while  $r(\mathbf{G}_{i,j}) M_{RX}/2$  determines the achievable diversity gain. In contrast to OSTBC,  $\mathbf{G}_{i,j}$  in RRNS( $u, v$ )-STBC can not be guaranteed to be full rank. However, the additional term  $\chi/2$  introduces a new degree of freedom

for designing STBC. This is consistent with the results discussed in [52], which analyses a concatenated system based on Convolution codes and STBC.

**Lemma 4.** *For a  $M_T \times M_R$  MIMO system, the best RRNS code is one with  $d_{min} = 2M_T$ . Thus for a  $2 \times 2$  MIMO system, the best code is the one with  $d_{min} = \chi = 4$*

**Proof:** From (4.16) we see that the diversity gain of the RRNS-STBC is dependent on the factor  $M_R\chi/2$ . The maximum achievable diversity order for an  $M_T \times M_R$  MIMO system is  $M_R M_T$ .

This implies that

$$\begin{aligned} \frac{\chi}{2} r(\mathbf{G}_{a,b}) M_R &\leq M_R M_T \\ \Rightarrow \chi &\leq \frac{2M_T}{r(\mathbf{G}_{a,b})} \end{aligned} \quad (4.18)$$

Now,  $\min r(\mathbf{G}_{a,b}) = 1$  and  $\max r(\mathbf{G}_{a,b}) = M_T$ . Thus for  $r(\mathbf{G}_{a,b}) = M_T$  an RRNS code with  $d_{min} = \chi = 2$  will be sufficient to extract maximum diversity order. But since full rank cannot be guaranteed in case of RRNS-STBC design, thus for  $r(\mathbf{G}_{a,b}) = 1$ , a code with  $d_{min} = \chi = 2M_T$  will be able to achieve maximum possible diversity order. Codes with  $d_{min} \geq 2M_T$  will only achieve extra coding gain without any change in diversity order. ■

### Bit Error Probability

An RRNS code is designed with  $d = u - v$  redundant moduli, meaning that  $d$  number of moduli can be dropped from each codeword, that is, even if there are errors in  $d$  number of moduli, we can still decode the decimal number correctly. As a result, there will be an error in decoding  $k_b$  bits only when there are more than  $d$  residue errors per RRNS codeword. The probability that a symbol is not recovered correctly after the residue to  $k_b$  binary bit conversion is denoted by  $P_s(E)$  and is upper bounded as [39]

$$P_{Es}^{ns} \leq 1 - \sum_{k=0}^d \binom{u}{k} (P_s)^k (1 - P_s)^{u-k} P(d, k) \quad (4.19)$$

where,  $P_s$ , given in equation (4.6), is the upper bound on the symbol error probability of the inner STBC of the concatenated scheme, and  $P(d, k)$  is the probability that there are

$k$  residue errors out of the possible  $d$ .  $P(d, k)$  depends on the error probability of a single residue digit. We have considered an  $M$ -ary QAM modulation and Rayleigh fading channel for our analysis. The probability of a single residue digit error is determined based on the performance of the  $M$ -ary QAM in Rayleigh fading channel.

The average probability of error of  $M$ -ary QAM in fading channel is given as [53]:

$$\begin{aligned} \bar{P}_{QAM} &= \frac{4}{\pi} \left(1 - \frac{1}{\sqrt{M}}\right) \int_0^{\pi/2} \mathcal{M}_{\gamma_s} \left(-\frac{g}{\sin^2\phi}\right) d\phi \\ &\quad - \frac{4}{\pi} \left(1 - \frac{1}{\sqrt{M}}\right)^2 \int_0^{\pi/4} \mathcal{M}_{\gamma_s} \left(-\frac{g}{\sin^2\phi}\right) d\phi, \end{aligned} \quad (4.20)$$

where  $g = 1.5/(M - 1)$  is a function of the  $M$ -ary QAM constellation size.

$$\mathcal{M}_{\gamma_s} \left(-\frac{g}{\sin^2\phi}\right) = \left(1 + \frac{g\bar{\gamma}_s}{\sin^2\phi}\right)^{-1}, \quad (4.21)$$

is the moment generating function (MGF) of the Rayleigh fading channel and  $\bar{\gamma}_s$  is the average SNR per symbol.

Using the above result, the probability  $P(d, k)$  is obtained as

$$P(d, k) = \sum_{n=0}^{d-k} \binom{u-k}{m} (\bar{P}_{QAM})^m (1 - \bar{P}_{QAM})^{u-k-m}, \quad (4.22)$$

where  $d$  represents the number of redundant moduli. Thus using the above expression in equation (10), the probability of correct symbol detection  $P_s(C)$  can be evaluated. Then the approximate average BER is given by

$$P_{Eb}^{ns} \approx \frac{2^{k_b-1}}{2^{k_b} - 1} P_{Es}^{ns}. \quad (4.23)$$

Our analysis in this section is based on  $M$ -ary QAM and Rayleigh fading channel. However this approach is applicable to any  $M$ -ary modulation scheme and any fading channel provided the MGF can be determined for the channel distribution.

### 4.2.3 Systematic RRNS-STBC

#### Codeword Error Probability

In the case of Systematic RRNS-STBC, there exists a number of ambiguous  $2 \rightarrow 1$  mappings, which depend on the choice of moduli. Thus a decoded symbol can still be in error due



incorrect decoding of  $2 \rightarrow 1$  mapping even if it is correctly RRNS decoded. This is the so-called  $2 \rightarrow 1$  *mapping problem*. It is to be noted that only the successfully error corrected symbols associated with the systematic information part of the systematic RRNS codeword exhibit this problem. If a non-redundant residue digit is corrected by RRNS decoding, referred to as the *1st stage decoding*, then this corrected residue digit must be decoded to one of its two possible binary representations, referred to as *2nd stage decoding*. Residue digits which have a  $1 \rightarrow 1$  mapping are also exempt from this problem.

As discussed in [27], this problem can be addressed by assuming that the value of the  $k_i$ -bit information symbol used for generation of the  $i$ -th non-redundant residue is uniformly distributed in the range  $[0, 2^{k_i} - 1]$ . Thus with reference to Table(2.3), these values can be given as:

$$2 \rightarrow 1 \text{ mapping : } P(x_i) = \frac{1}{2^{k_i-1}} \quad (4.24)$$

$$1 \rightarrow 1 \text{ mapping : } P(x_i) = \frac{1}{2^{k_i}} \quad (4.25)$$

Let  $p_{e1}(x_i)$  denote the probability of error for the 1st stage decoding error probability for the  $i$ -th residue digit. In the case of Systematic RRNS-STBC, the average 1st stage decoding error probability,  $\bar{p}_{e1} = P_s$ , i.e., the symbol error probability of the super-channel given by equation(4.7). The symbol error probability of the 2nd stage decoding is denoted by  $p_{e2}(x_i)$ . In case a residue digit is in error and is corrected by 1st stage decoding, but there is no second stage decoding as  $1 \rightarrow 1$  mapping was used i.e.,  $x_i \geq 2^{k_i} - m_i$ , then  $p_{e2}(x_i) = 0$ . For any  $x_i \leq 2^{k_i} - m_i - 1$ , the error probability is given by the probability of error of the minimum-distance decoding i.e.,  $p_{e2}(x_i) = Q(\sqrt{2k_i\gamma_b R_c})$ , where  $\gamma_b$  is the SNR per bit and  $R_c$  is the code rate of the systematic RRNS given by [37]:

$$R_c^s = \sum_{i=1}^v k_i / \sum_{j=1}^u k_j \quad (4.26)$$

The average error probability of the second stage for the corrected residue digit  $x_i$ ,  $i = 1, 2, \dots, u$  is given by [27]:

$$\bar{p}_{e2}(x_i) = \frac{2^{k_i} - m_i}{2^{k_i-1}} Q\left(\sqrt{2k_i\gamma_b R_c}\right) \quad (4.27)$$

For error-correction-only decoding of Systematic RRNS-STBC codes, we consider the probability of correct decoding,  $P_C^s$ , the probability of incorrect decoding due 2nd-stage decoding errors,  $P_{IC}^s$  and the codeword error probability  $P_E^s$ . The 1st-stage error probability is denoted by  $p_{\epsilon 1}(x_i)$  and the average 2nd-stage error probability is denoted by  $\bar{p}_{\epsilon 2}(x_i)$ , where  $x_i$  are the residues and  $i = 1, 2, \dots, u$ .  $\bar{p}_{\epsilon 2}(x_i) = 0$  for  $i = v + 1, \dots, u$  since there is no  $2 \rightarrow 1$  mapping for redundant residue digits. For successful decoding, the residue digits corrected by the 1st-stage RRNS decoding are successfully mapped back to their corresponding information bits by 2nd-stage decoding. The probability for systematic RRNS-STBC correcting upto  $t$  errors, is given by:

$$\begin{aligned}
P_C^s &= \sum_{\lambda=0}^t [\text{Probability of } \lambda \text{ residue digits in error}] \\
&\quad \times [\text{Probability that the } \lambda \text{ errors are corrected by 2nd-stage decoding}] \\
&= \sum_{\lambda=0}^t \left\{ \sum_{Q(\lambda)} \left[ \underbrace{\prod_{\{\alpha\}_\lambda} p_{\epsilon 1}(x_\alpha)(1 - \bar{p}_{\epsilon 2}(x_\alpha))}_{\lambda \text{ terms}} \underbrace{\prod_{\{\beta\}, \{\beta\} \neq \{\alpha\}} (1 - p_{\epsilon 1}(x_\beta))}_{(u-\lambda) \text{ terms}} \right] \right\} \quad (4.28)
\end{aligned}$$

$$(1 - P_C^s) = \sum_{\lambda=t+1}^u \left\{ \sum_{Q(\lambda)} \left[ \underbrace{\prod_{\{\alpha\}_\lambda} p_{\epsilon 1}(x_\alpha)(1 - \bar{p}_{\epsilon 2}(x_\alpha))}_{\lambda \text{ terms}} \underbrace{\prod_{\{\beta\}, \{\beta\} \neq \{\alpha\}} (1 - p_{\epsilon 1}(x_\beta))}_{(u-\lambda) \text{ terms}} \right] \right\} \quad (4.29)$$

where the notations are same as in equation(9). The probability of incorrect decoding due to 2nd-stage decoding errors is given by:

$$P_{IC2}^s = \sum_{\lambda=0}^t \left\{ \sum_{Q(\lambda)} \left[ \underbrace{\prod_{\{\alpha\}_\lambda} p_{\epsilon 1}(x_\alpha)\bar{p}_{\epsilon 2}(x_\alpha)}_{\lambda \text{ terms}} \underbrace{\prod_{\{\beta\}, \{\beta\} \neq \{\alpha\}} (1 - p_{\epsilon 1}(x_\beta))}_{(u-\lambda) \text{ terms}} \right] \right\} \quad (4.30)$$

where the product over  $\alpha_\lambda$  is zero when the set is empty. If we apply the same approximations as in the case of Non-systematic RRNS codes i.e., replace the moduli,  $m_1, m_2, \dots, m_u$ , with an average value  $q$ . Taking this further, if we replace the values  $k_i$  for  $i = 1, \dots, v$  with an

average value  $k_{avg}$ , then we can substitute the error probability defined by equation(4.27) with an average value for all residue digits,  $\bar{p}_{e2}$ . Also the average 1st-stage decoding error probability over all residue digits is given by  $\bar{p}_{e1} = P_s$ . Substituting these in equation(4.29 and 4.30), we have:

$$(1 - P_C^s) = P_{E1}^s = \sum_{\lambda=t+1}^u \binom{u}{\lambda} \{\bar{p}_{e1}(1 - \bar{p}_{e2})\}^\lambda \{1 - \bar{p}_{e1}\}^{u-\lambda} \quad (4.31)$$

$$P_{IC2}^s = P_{E2}^s = \sum_{\lambda=0}^t \binom{u}{\lambda} \{\bar{p}_{e1}\bar{p}_{e2}\}^\lambda \{1 - \bar{p}_{e1}\}^{u-\lambda} \quad (4.32)$$

The probability of error due 1st-stage decoding is given by:

$$P_{IC1}^s = \frac{S_{IC}^s}{S} (1 - P_C^s - P_{IC2}^s) \quad (4.33)$$

where,  $S$  is given by equation(4.12) and  $S_{IC}^s$  is given by [27]:

$$S_{IC}^s = (N_c^s - 1) \sum_{\alpha=0}^t \sum_{Q(\alpha)} \prod_{\{\beta\}_\alpha} (m_\beta - 1), \quad (4.34)$$

The codeword error probability for the Systematic RRNS-STBC can be then expressed as:

$$\begin{aligned} P_E^s &= P_{IC1}^s + P_{IC2}^s \\ &= \frac{S_{IC}^s}{S} (1 - P_C^s) + \frac{S - S_{IC}^s}{S} P_{IC2}^s \end{aligned} \quad (4.35)$$

$$\begin{aligned} &= \frac{S_{IC}^s}{S} \sum_{\lambda=t+1}^u \binom{u}{\lambda} \{\bar{p}_{e1}(1 - \bar{p}_{e2})\}^\lambda \{1 - \bar{p}_{e1}\}^{u-\lambda} \\ &\quad + \frac{S - S_{IC}^s}{S} \sum_{\lambda=0}^t \binom{u}{\lambda} \{\bar{p}_{e1}\bar{p}_{e2}\}^\lambda \{1 - \bar{p}_{e1}\}^{u-\lambda} \end{aligned} \quad (4.36)$$

**Lemma 5.** *The codeword error probability for Systematic RRNS-STBC can be upper bounded as:*

$$P_E^s \leq (N_c^s - 1) 2^u (\bar{p}_{e1})^{\chi/2} \left[ \frac{S_{IC}^s}{S} (1 - \bar{p}_{e2})^{\chi/2} + \frac{S - S_{IC}^s}{S} (\bar{p}_{e2})^{\chi/2} \right] \quad (4.37)$$

where  $\chi = u - v + 1$  and  $\bar{p}_{e1} = P_s$ .

**Proof:** See Appendix(B). ■

Using the fact that  $\bar{p}_{\epsilon 1} = P_s$ , and following the same method as in Lemma 5, we can derive an expression for the upper bound on Systematic RRNS-Codeword error probability given by:

$$\begin{aligned}
P_E^s &\leq (N_c^s - 1)2^u(P_s)^{\chi/2} \left[ \frac{S_{IC}^s}{S}(1 - \bar{p}_{\epsilon 2})^{\chi/2} + \frac{S - S_{IC}^s}{S}(\bar{p}_{\epsilon 2})^{\chi/2} \right] \\
&\leq 2^u(N_c^s - 1)[N_c^s(N_c^s - 1)]^{r(\mathbf{G}_{i,j})} \frac{\left[ \frac{S_{IC}^s}{S}(1 - \bar{p}_{\epsilon 2})^{\chi/2} + \frac{S - S_{IC}^s}{S}(\bar{p}_{\epsilon 2})^{\chi/2} \right]}{\left[ \prod_{k=1}^{r(\mathbf{G}_{i,j})} \lambda_k(\mathbf{G}_{a,b}) \right]^{M_R}} \\
&\quad \times \left( \frac{\rho}{4M_T} \right)^{-r(\mathbf{G}_{i,j})M_R\chi/2}
\end{aligned} \tag{4.38}$$

It can be seen that similar to Non-systematic RRNS-STBC, the Systematic code also provides the same degree of freedom for design of STBC.

### Bit Error Probability

The bound on the bit error probability of Systematic RRNS-STBC can be obtained in similar manner to Non-Systematic RRNS-STBC. When there is a codeword error the corresponding symbol error probability,  $P_{Es}^s$ , is given by:

$$\begin{aligned}
P_{Es}^s &\leq \underbrace{\left[ 1 - \sum_{k=0}^d \binom{u}{k} \{\bar{p}_{\epsilon 1}\bar{p}_{\epsilon 2}\}^k \{1 - \bar{p}_{\epsilon 1}\}^{u-k} P(d, k) \right]}_{1st\text{-stage decoding}} \\
&\quad + \underbrace{\left[ 1 - \sum_{k=0}^d \binom{u}{k} \{(1 - \bar{p}_{\epsilon 1})\bar{p}_{\epsilon 2}\}^k \{1 - \bar{p}_{\epsilon 2}\}^{u-k} P(d, k) \right]}_{2nd\text{-stage decoding}}
\end{aligned} \tag{4.39}$$

where  $P(d, k)$  is calculated in the same way as for non-systematic RRNS and is given by equation(4.22). The corresponding bit error probability is given by:

$$P_{Eb}^s = \frac{2^{\sum k_i - 1}}{2^{\sum k_i} - 1} P_{Es}^s \tag{4.40}$$

where  $\sum k_i; i = 1, 2, \dots, v$  represents the size of the information block in bits which was initially encoded to form non-redundant residues.

The code rate of the Non-systematic RRNS-STBC is given by [37]:

$$R_c^{ns} = k_b / \sum_{j=1}^u k_{b_j} \quad (4.41)$$

where  $k_b = \lceil \log_2 M_r \rceil$  and  $k_{b_j} = \lceil \log_2 m_j \rceil$ , where  $m_j, \{j = 1, 2 \dots u\}$  are the moduli. Comparing equation(4.26) and equation(4.41), it can be seen that for the same moduli set, systematic RRNS has a higher code rate i.e.,  $R_c \geq R_c'$ . This results from the more efficient binary to residue mapping in case of Systematic RRNS as well as the result stated in Lemma 1.

### 4.3 Complexity of RRNS-STBC

Implementation of the CRT with exhaustive Maximum Likelihood search results in a complexity of  $\mathcal{O}(N^3)$ , where  $N$  is number of non-redundant moduli. However, several methods of lower complexity also exist in literature. In [54], an implementation of CRT using systolic array has been proposed which has a complexity of  $\theta(\log NP)$ , where  $N$  is the number of moduli and  $P$  is the number of bits. The Base Extension algorithm is used in [30], [31] with a complexity of  $\mathcal{O}(N^2)$ , where  $N$  is number of non-redundant moduli used in RRNS. In [55], Mixed Radix Conversion algorithm is used which yields a time complexity of  $\mathcal{O}(N)$ . VLSI architectures capable of decoding RRNS with time complexity of  $\theta(N)$  has been proposed in [56]. In [41] and even lower complexity scheme, having a complexity of  $\theta(\log N)$ , is proposed. The decoding in this case is achieved using carry-save adders (CSA) and modulo adders (MA). Thus, the complexity of RRNS-STBC compares favourably with other concatenated STC schemes like the RS-STBC discussed in [40],[42].

## 4.4 Summary

In this chapter present the system model for an RRNS-STBC coded  $2 \times 2$  MIMO System. The STBC mapping and modulation scheme together act as the inner code forming a super channel, while the RRNS based channel code acts as the outer code. Thus the proposed RRNS-STBC is a concatenated coding scheme. The performance of both systematic and non-systematic RRNS-STBC schemes is quantified and the bounds on the Symbol Error rate and BER are derived. The Pairwise error probability of the inner STBC is used as the channel error probability of the super channel. This is in turn used for deriving the performance bounds on the RRNS-STBC schemes. We also comment on the complexity of the RRNS-STBC concatenated coding scheme and see that it is similar to other concatenated schemes like RS-STBC. In the next chapter, we simulate the RRNS-STBC codes and compare the performance with other concatenated coding schemes.

# Chapter 5

## Performance of RRNS-STBC: Analysis of Simulation Results

In this chapter, we simulate different RRNS-STBC codes and analyze their performance over a Rayleigh fading environment. The different RRNS-STBC schemes are compared with OSTBC and other Concatenated coding schemes. The results derived in Chapter 4 are illustrated and justified. The performance of the different mapping schemes discussed in Chapter 3 are also illustrated with the help of simulations. We first discuss the simulation parameters and then expound on the simulation results and their implications.

### 5.1 Simulation Parameters

A  $2 \times 2$  MIMO system is considered for the simulation. We assume a Rayleigh fading channel. Block fading is assumed i.e., the channel is considered to be constant over the duration of block length,  $T$ , of the codeword (given each codeword is  $M_T \times T$ ). It is also assumed that channel state information (CSI) is available at the receiver. Alamouti scheme [19] is simulated as an example of OSTBC. In order to develop a fair comparison between Alamouti scheme and RRNS  $(u, v)$ -STBC, we use global coding efficiency [40] as a standardizing metric. The global coding efficiency is defined as the product of the spatial and temporal coding rates of the concatenated code, i.e.,  $\eta_G = R_c R_s$ , where  $R_c$  is the coding rate of the outer error correcting code (RRNS in this case) and  $R_s$  is the space time coding

rate. Space time coding rate [40] is defined as the number of useful modulation symbols over the number of space time coded symbols used in the STBC. In case of the OSTBC, i.e., Alamouti's scheme for a  $2 \times 2$  MIMO system, each set of two symbols are coded into four different symbols. Thus,  $R_s$  becomes 0.5. In the case of other space time coding schemes like simple spatial multiplexing,  $R_s$  is unity.

We set the same  $\eta_G$  for both RRNS( $u, v$ )-STBC and OSTBC. Secondly, modulation scheme used in RRNS-STBC is set to be the same as in OSTBC. For our simulations we have assumed 16-QAM without any loss of generality. Bit error rate (BER) performance of different mapping schemes is evaluated and compared. The bound on the BER, given by equation (4.23) for Non-Systematic RRNS and by equation(4.40) for Systematic RRNS, is an union bound on the average bit error probability and it can tightened further by removing error sequences that are multiples of lower weight error sequences [51].

## 5.2 Simulation Results

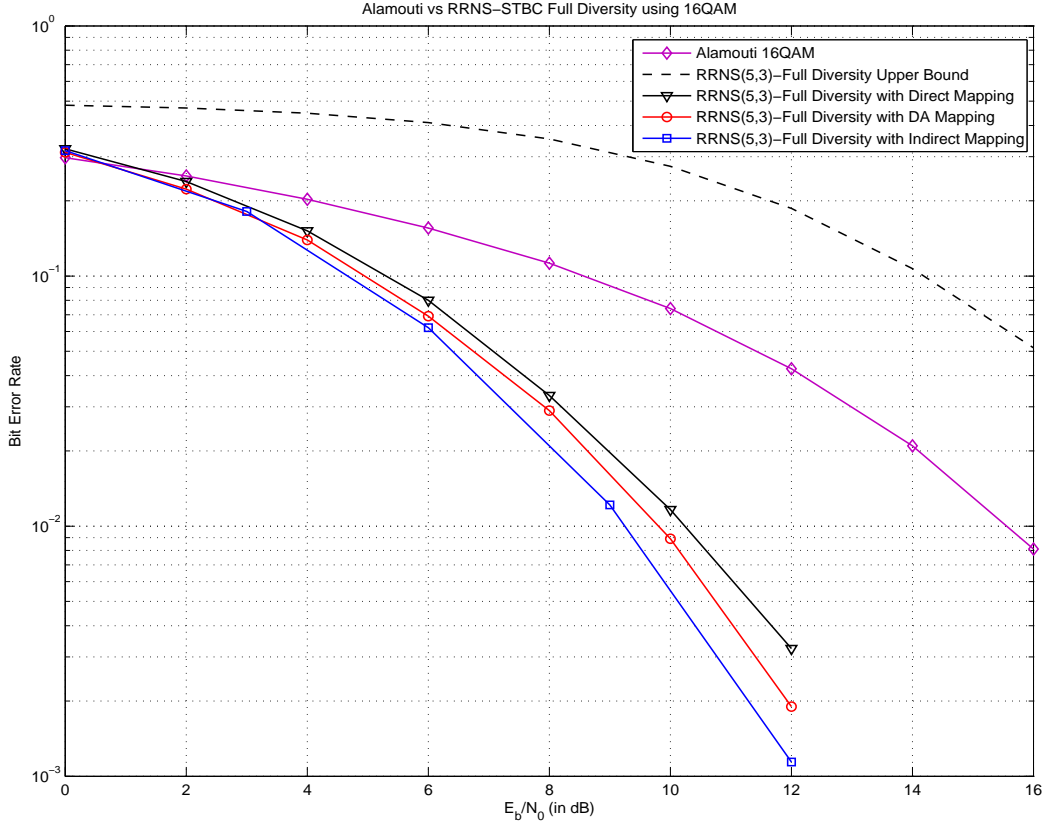
The simulation results based on both Non-Systematic and Systematic RRNS-STBC are discussed in detail in the following subsections.

### 5.2.1 Non-Systematic RRNS-STBC

#### Non-Systematic RRNS-STBC vs. OSTBC

In Figure 5.1, BER performance of Non-systematic RRNS (5, 3)-STBC using full diversity transmission and Alamouti coding scheme is compared. In case of full diversity transmission, the same symbol is transmitted on the  $M_T$  transmit antennas at each time slot. In case of Spatial Multiplexing, we transmit  $M_T$  distinct symbols for each time slot. In the case of RRNS-STBC system with full diversity transmission, the condition of channel invariance across block length can be relaxed. Even if the channel varies for each time slot, the performance does not differ as we suppose that identical symbols are transmitted on the  $M_T$  antennas for a given time slot and CSI is available at the receiver. The moduli set



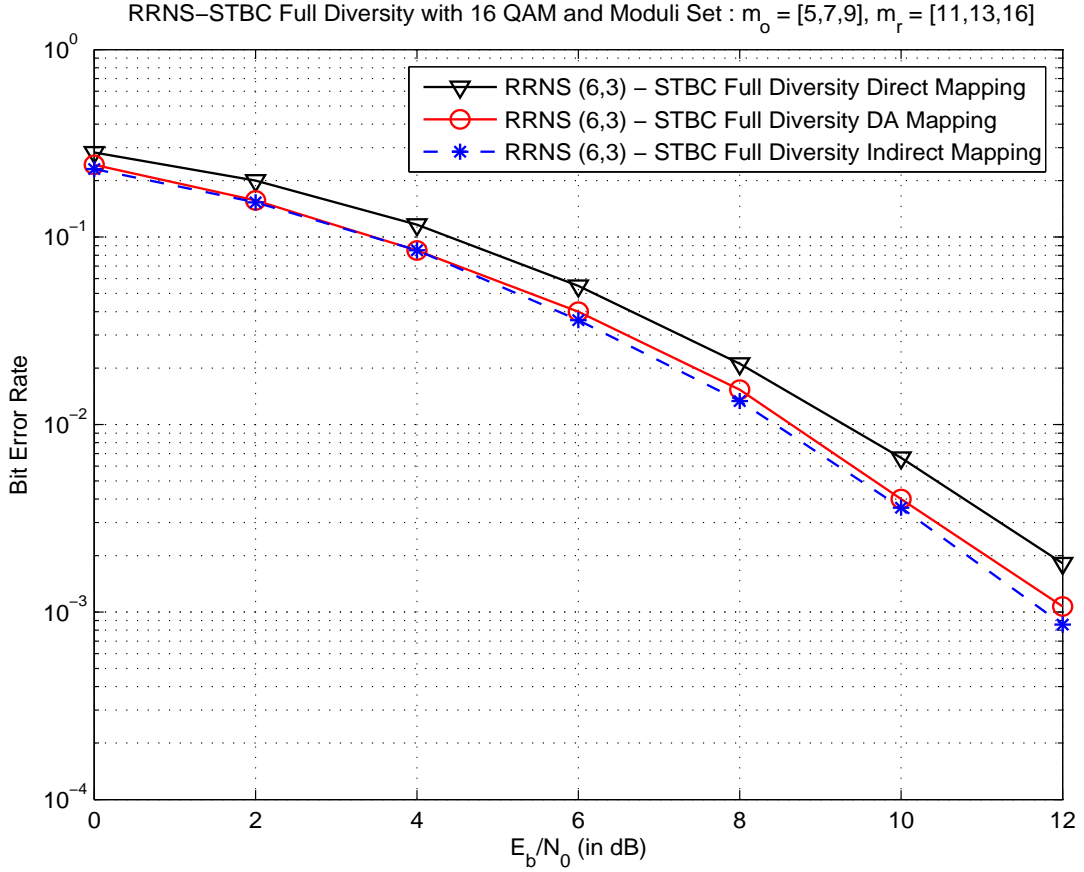


**Figure 5.1:** BER performance of RRNS (5,3)-STBC with moduli set of  $m_o = \{7, 9, 11\}$ ,  $m_r = \{13, 16\}$ .

that is used in case of Direct and DA mapped RRNS (5,3)-STBC is  $\{7, 9, 11, 13, 16\}$ , where  $m_o = \{7, 9, 11\}$  and  $m_r = \{13, 16\}$  correspond to the original moduli set and redundant moduli set, respectively. 16-QAM modulation scheme is applied in both RRNS (5,3)-STBC and Alamouti scheme. The global codes efficiency of RRNS (5,3)-STBC ( $R_c R_s = 0.5 \times 1 = 0.5$ ) is the same as Alamouti coding ( $R_c R_s = 1 \times 0.5 = 0.5$ ). The  $R_c$  for Non-systematic RRNS-STBC is given by equation(4.41). It is observed that RRNS (5,3)-STBC outperforms Alamouti coding scheme in terms of BER. This is expected as in this case,  $\chi/2 = 1.5$ . Therefore, the contribution of the additional term  $\chi/2$  provides a similar diversity order relative to Alamouti scheme. Furthermore, RRNS-STBC exploits extra coding gain while

Alamouti coding has no coding gain. All these features are clearly revealed in Figure 5.1. For the RRNS-STBC with Indirect Mapping, the basis of this comparison is the transmission rate given by bits per channel use. Here the moduli set of the RRNS-STBC is chosen as  $m_o = \{9, 11, 13\}$ ,  $m_r = \{16, 17\}$ . This yields a code rate  $R_c = 0.48$  and  $k_b = 10$ . Thus in this case the  $\eta_G \approx 0.5$ . Since we are using block length  $T = 5$ , the bits per channel use in case of this code is 4. This is because we are transmitting 10 bits using 5 complex symbols. Thus for a  $2 \times 2$  system, 20 bits are transmitted using 5 channel uses or time slots. Thus for the RRNS(5,3)-STBC, transmission rate is 4 bits per channel use. The Alamouti code also transmits at 4 bits per channel use. We can see that the RRNS-STBC still outperforms the Alamouti scheme when bits per channel use is used as a metric for comparison. The RRNS-STBC uses the Chinese Remainder Theorem for decoding the codewords. The CRT is computationally intensive as compared to the simple Alamouti scheme. Thus the gain using RRNS-STBC comes at the cost of increased receiver complexity. However in terms of complexity, our implementation is comparable to [40] where RS codes have been used as STBC. Also, RRNS decoding methods having much lower complexity can be used, as discussed in [41],[54]-[56] etc. The use of DA mapping also gives an improvement of 0.5dB in BER performance for the RRNS(5,3)-STBC as seen from Fig.4. This gain due to the DA mapping scheme obtained as a result of the decision boundaries in the signal space being scaled according to the probability of occurrence of a symbol, i.e., the most probable symbol having the largest decision region. This leads to a consistent improvement in error performance of the RRNS-STBC when DA mapping is used.

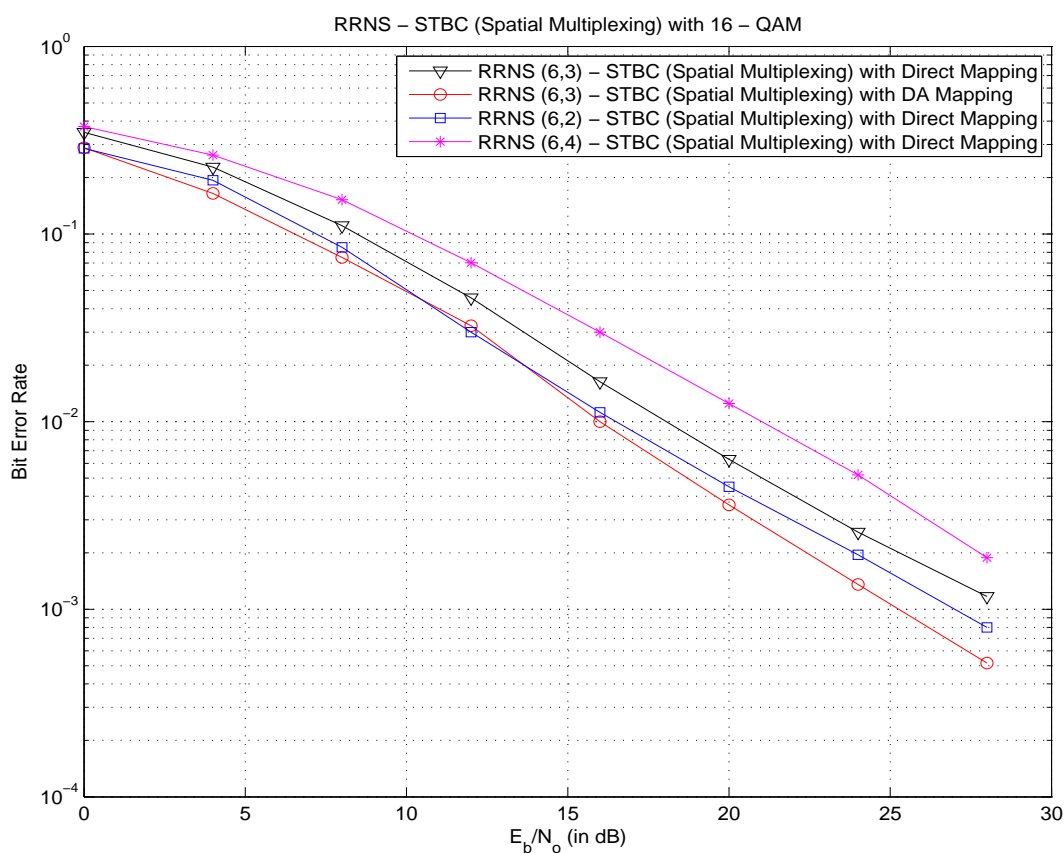
## RRNS-STBC schemes using Direct, DA and Indirect Mapping



**Figure 5.2:** Comparison of BER performance of Full Diversity Non-systematic RRNS(6,3)-STBC ( $T = 6$ ), with prior probability based Distance-Aware mapping and Gray coded mapping and Indirect Mapping with ML decoding assuming equal priors

In Figure 5.2, the comparison between normal gray coded mapping and the new probability based DA mapping for an RRNS (6, 3)-STBC, as considered in Example(3.1.2), is shown. Here,  $m_o = \{5, 7, 9\}$  and  $m_r = \{11, 13, 16\}$  and full diversity transmission scheme is used i.e., each antenna transmits the same symbol over the same time period. At the receiver end, equal gain combining (EGC) is used along with ML detection. Thus, in this case,  $R_s = 1$ . It can be seen that the DA mapping scheme gives a consistent improvement of about 1dB in BER performance over the normal gray coded QAM mapping scheme. The

IM scheme is shown to give nearly the same performance as the DA mapping scheme at very low SNR and slightly better performance as SNR increases. Thus, this scheme can be used as an alternative to DA mapping. It removes the limitations on the modulation scheme used. However, it comes at the cost of transmitting more complex symbols as compared to DA and also the extra decimal to binary conversion at the encoder after RRNS coding and vice-versa at the receiver.

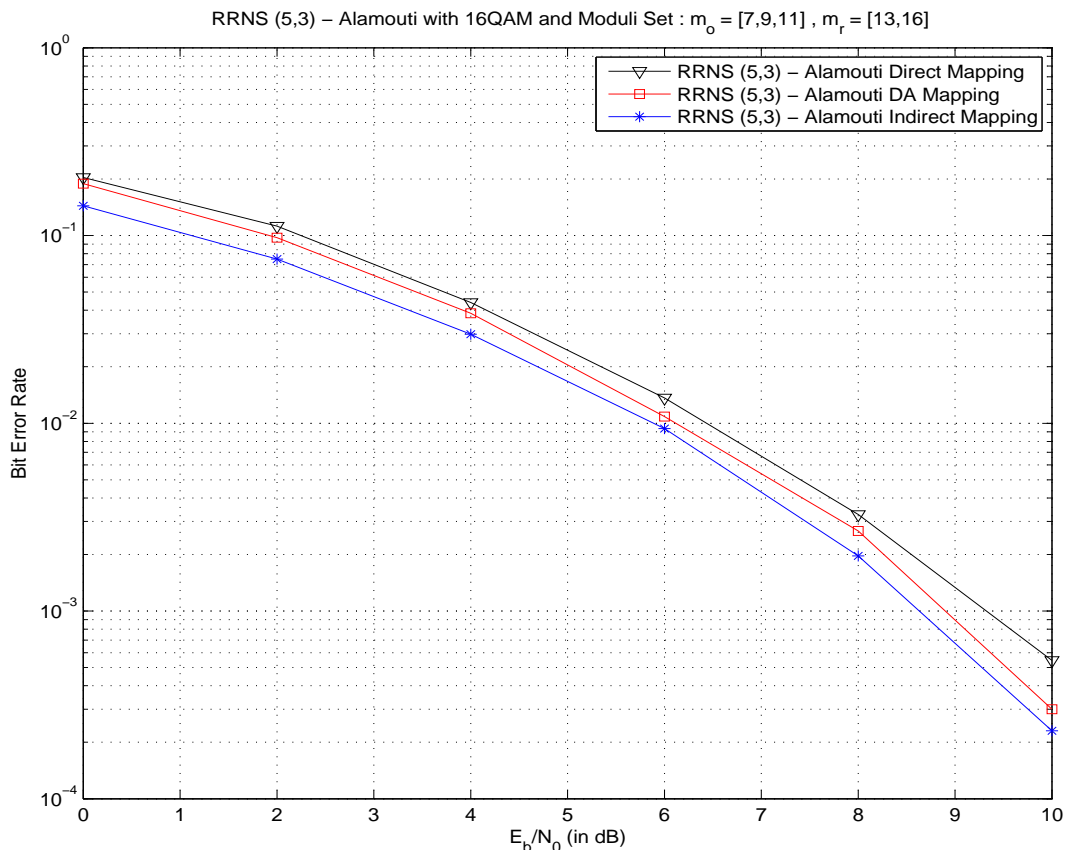


**Figure 5.3:** Comparison of BER performance of Spatially Multiplexed Non-systematic RRNS-STBC with Direct and Distance-Aware mapping and with different  $\chi$

Figure 5.3 shows the comparison in BER performance in case of a spatial multiplexing scheme with the same Non-systematic RRNS(6, 3) channel code. The moduli set used for RRNS(6, 3)-STBC is  $m_o = \{5, 7, 9\}$  and  $m_r = \{11, 13, 16\}$  and code rate is 0.36. Here the two antennas transmit a pair of different symbols at each time instant and ML detection at the receiver is based on detecting a symbol pair instead of symbol by symbol detection. Thus, as expected the performance degrades from that of full diversity scheme. It can be seen in this case also that a performance improvement of about 2dB is obtained by using the DA mapping scheme over the normal Gray coded scheme.

Figure 5.3 also illustrates the fact that with increase in  $\chi$ , the diversity gain is bounded at  $M_R \times M_T$ . The RRNS(6, 2)-STBC code is used with moduli set  $m_o = \{5, 7\}$ ,  $m_r = \{9, 11, 13, 16\}$  and code rate 0.22. For RRNS(6, 3)-STBC and RRNS(6, 2)-STBC, the block length is  $T = 3$ . We can see from the figure that the diversity order for the three schemes at high SNR is almost same. The factor  $\chi/2$  contributes to achieving the maximum possible diversity order for the given code set. But beyond  $d_{min} = \chi = 4$ , i.e.,  $M_R \times M_T$  for the  $2 \times 2$  system, the only thing that changes is coding gain. The diversity remains unchanged. The RRNS(6, 4)-STBC with moduli set  $m_o = \{5, 7, 9, 11\}$  and  $m_r = \{13, 16\}$  is also simulated. In this case  $d_{min} = \chi = 3$ . It can be observed that this case has a slight decrease in diversity compared the others. But the factor  $\chi$  contributes to make it almost equal to the other two.

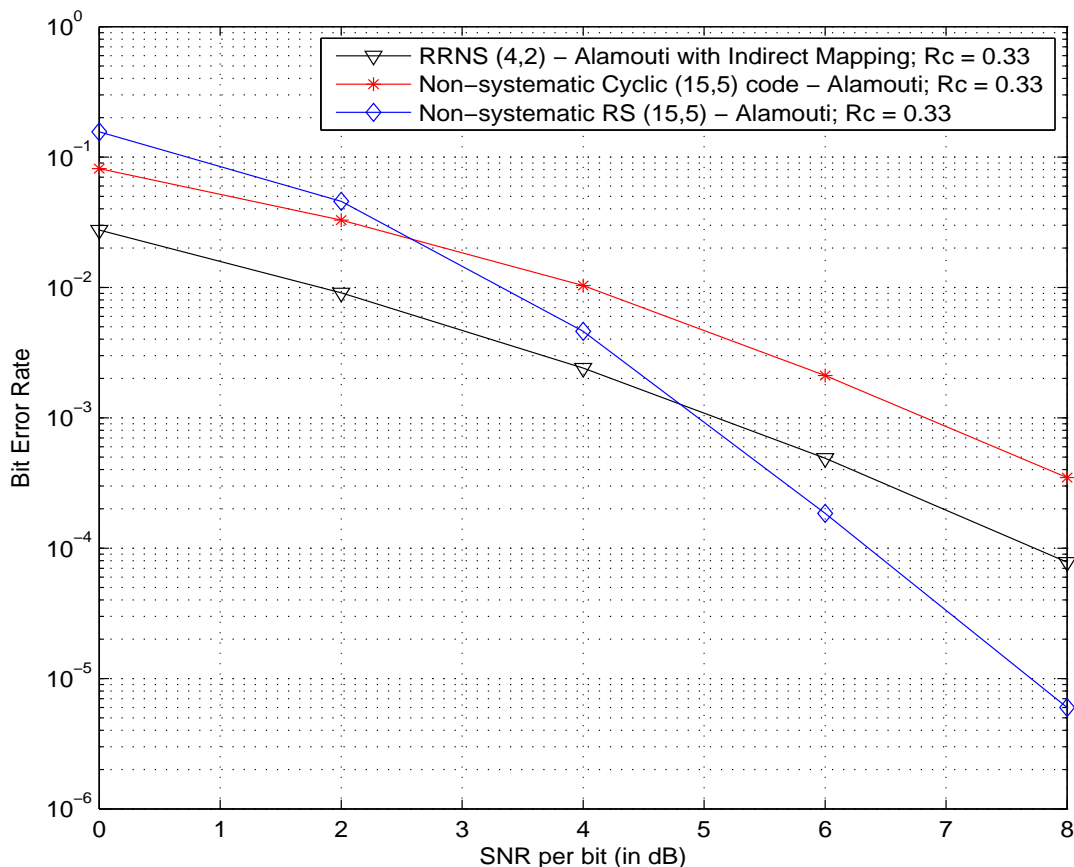
## Non-systematic RRNS-OSTBC Schemes



**Figure 5.4:** Comparison of BER performance of Non-systematic RRNS(5,3)- Alamouti with prior probability based Distance-Aware mapping, Gray coded mapping and Indirect mapping assuming equal priors

Figure 5.4 shows the BER performance of a Non-systematic RRNS(5,3)-OSTBC scheme. Here the Alamouti scheme is used as the inner STBC of the concatenated scheme. This scheme gives a better performance as compared to the full diversity scheme as the  $\eta_G$  is lesser in this case. It can be seen here that the DA mapping scheme gives a 0.5 dB improvement in performance. The IM scheme shows a further 0.5 dB performance improvement. However in case of OSTBC,  $R_s = 0.5$ . As a result, this improvement comes at the cost of more transmitted symbols as compared to the other two schemes.

## Non-systematic RRNS-OSTBC vs. Concatenated OSTBC schemes



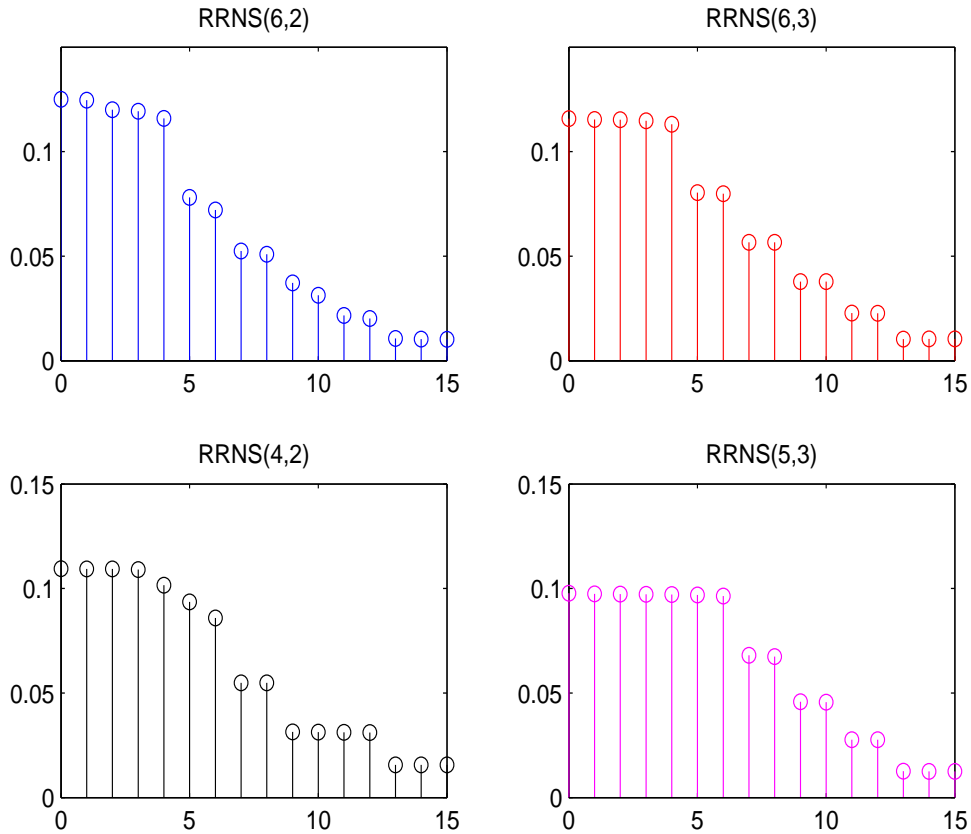
**Figure 5.5:** Comparison of BER performance of RRNS(4,2)-Alamouti ( $T = 2$ ) with Non-systematic RS(15,5)-Alamouti and Non-systematic (15,5)-Cyclic code-Alamouti with 16-QAM.

Figure 5.5 shows the comparison of the Non-systematic RRNS (4,2)-Alamouti scheme with a binary non-systematic (15,5)-Cyclic code concatenated with Alamouti as the inner OSTBC and the Non-systematic (15,5)-RS code concatenated with the Alamouti scheme. The modulation scheme used is 16QAM. It can be seen clearly that the RRNS-OSTBC outperforms the Cyclic code of same rate. The RS-OSTBC is generally very good in the high SNR region, but the RRNS-OSTBC provides appreciable performance improvement

over the RS-OSTBC in the low SNR region of 0 – 5 dB. For fairness in comparison, non-systematic RS code was chosen as the RRNS considered in this paper is also non-systematic. Systematic RS codes give a better performance than non-systematic RS codes in the low SNR region [57], but its comparison with non-systematic RRNS is not fair.



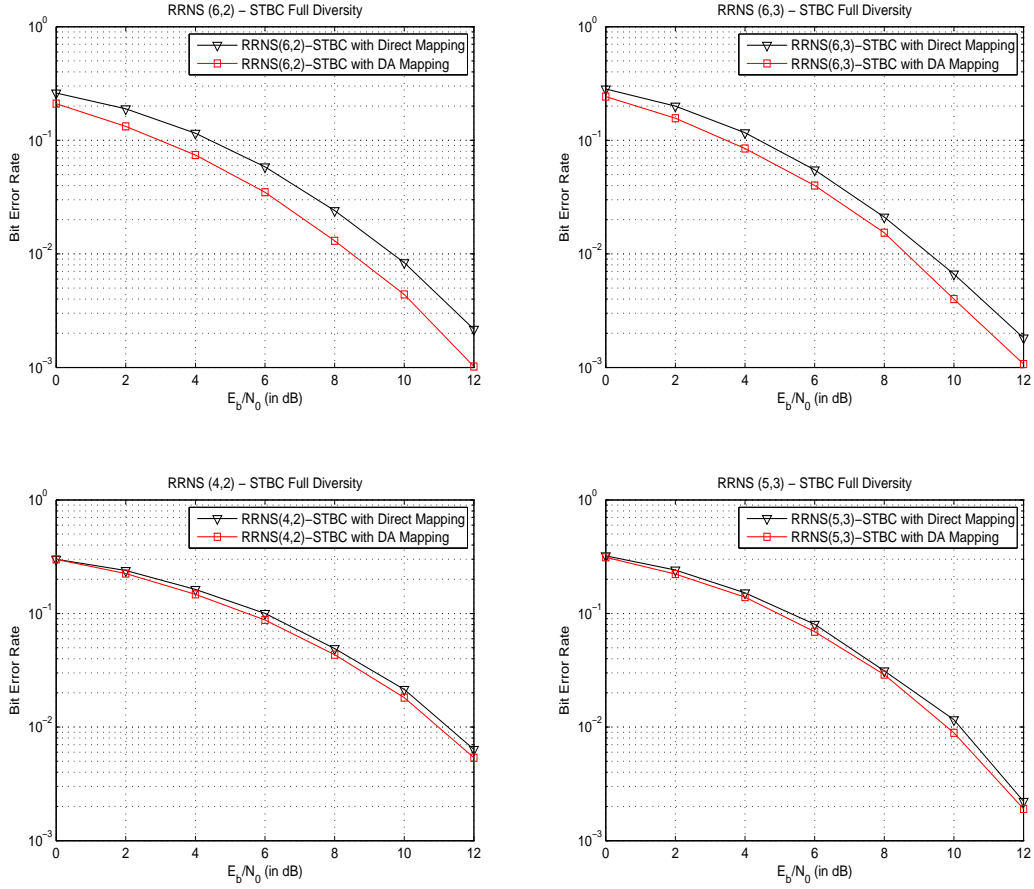
## Performance of DA Mapping scheme



**Figure 5.6:** Comparison of PMFs for different RRNS codes

From Figure 5.1, we observe that the improvement due to DA mapping is less than 0.5dB over normal Gray coded mapping. But as redundancy in RRNS is increased, the improvement given by the DA mapping scheme also increases as seen from Figure 5.2, where the relative gain in performance is about 1dB. Thus it can be observed that the DA mapping performance improvement increases as the coding rate decreases.

A formal explanation for this can be observed from Figure 5.6 and Figure 5.7. Here we compare the pmf of the residues for different RRNS schemes. It can be seen that that separation between the sets of residues used in the set partitioned scheme for DA mapping



**Figure 5.7:** Comparison of BER performance of different RRNS codes

is different for different choice of moduli i.e. for different RRNS codes.

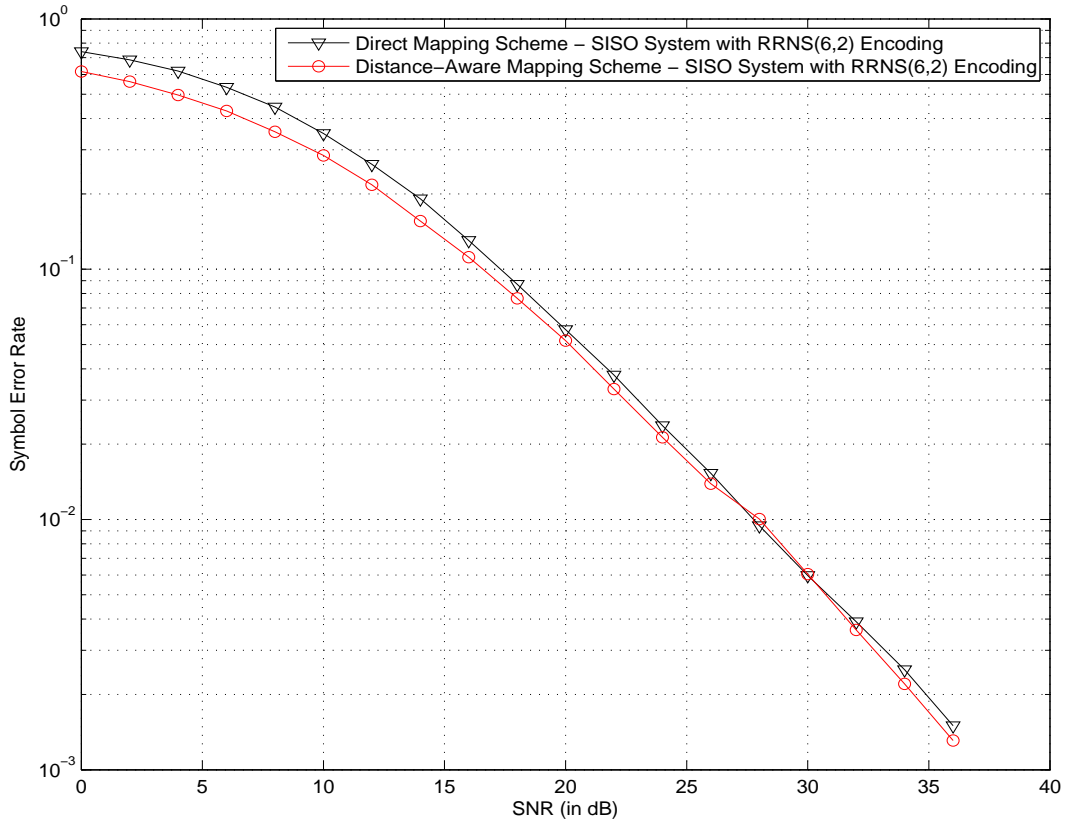
The choice of moduli in the codes in Figure 5.6 is given in Table(5.1). It can be seen clearly from Figure 5.6 that for RRNS(6,2) and RRNS(6,3) code, the residues in the sets (of 4 residues each) having the highest probability are separated by a wider margin from the remaining residues. In the case of RRNS(5,3) and RRNS(4,2) code, the separation is not as distinct and the first two sets of four residues are almost equiprobable. As the separation of the sets of residues increases in terms of probability, the decision boundaries for the residues in the most probable set become larger in case of ML detection. This scaling of decision

**Table 5.1:** CHOICE OF MODULI FOR DIFFERENT RRNS CODES

RRNS Code	$\mathbf{m}_o$	$\mathbf{m}_r$
RRNS(6,2) Code	5,7	9,11,13,16
RRNS(6,3) Code	5,7,9	11,13,16
RRNS(4,2) Code	7,9	13,16
RRNS(5,3) Code	7,9,11	13,16

boundaries, thus suggests that the codes having better set separation should perform better when DA mapping is used. This is observed in the performance improvement obtained using DA mapping.

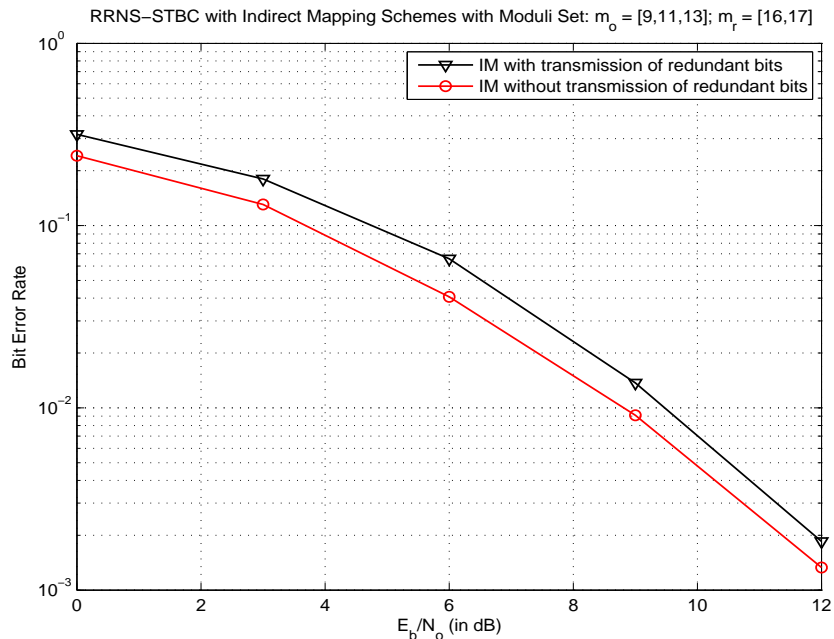
We simulate the RRNS-STBC schemes with parameters given in Table(5.1), for a full diversity transmission case. The results are illustrated in Figure 5.7. Here, we can clearly see that for DA mapping scenario, the RRNS(6, 2)-STBC and RRNS(6, 3)-STBC provides a better performance than the other two. Another observation is that in case of the DA mapping RRNS(6, 2) performs better than RRNS(6, 3). The increase in redundancy, for the same set of moduli, leads to the decrease of the legitimate range  $M_r$ . Thus the lower residues digits are more likely to occur than higher ones. This can be observed from Figure 5.7 where the probability values for the most probable residue set are higher in the case of RRNS(6, 2) code. Thus we can conclude that as redundancy increases, i.e., the legitimate range of RRNS decreases, the DA mapping scheme gives better gain in BER performance. This also implies that as the coding rate decreases, the DA mapping scheme provides better performance gain compared to a Gray coded mapping scheme. But trade off lies in the fact that as coding rate decreases, the decrease in legitimate range leads to generation of residues which are much less than  $\max\{m_1, \dots, m_u\}$  leading to inefficient mapping and unused codewords and constellation symbols. It is to be noted that the coding performances of the different RRNS schemes shown in Fig.9 cannot be compared with one another on basis of coding rate alone. In order to provide a fair comparison of the different RRNS schemes, the bits per residue i.e.  $k_b/u$  for the RRNS( $u, v$ ) codes has to be equal to one another.



**Figure 5.8:** Performance of DA Mapping Scheme over a SISO channel using RRNS (6,2) encoding with moduli set of  $m_o = \{5, 7\}$ ,  $m_r = \{9, 11, 13, 16\}$ .

Figure 5.8 shows another important observation in case of the DA mapping scheme. It can be seen that at low SNRs, the DA scheme provides an appreciable improvement in performance of about 1dB SNR. However at very high SNRs, the performance of DA mapping scheme is almost same as the the Direct mapping. This is because as SNR increases, the effect of additive noise displaces symbols from their original position in the constellation by lesser distances as compared to low SNR (when noise is much higher). As a result the decoding spheres needed for accurate decoding shrink in size. Thus DA mapping ceases to provide any appreciable advantage in comparison to normal Gray coded mapping scheme. This inference can be extended to a MIMO case without any loss in generality.

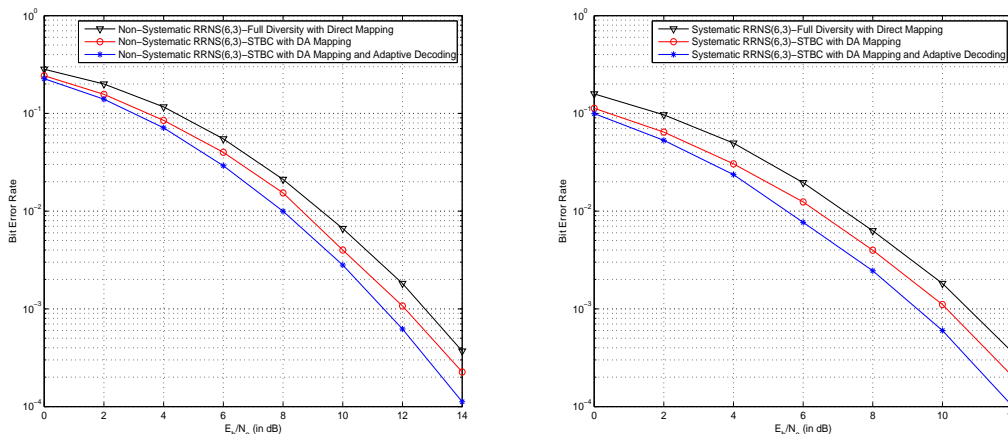
## Performance of Indirect Mapping Scheme



**Figure 5.9:** Performance of Indirect Mapping Scheme using RRNS (5,3) encoding with moduli set of  $m_o = \{9, 11, 13\}$ ,  $m_r = \{16, 17\}$ .

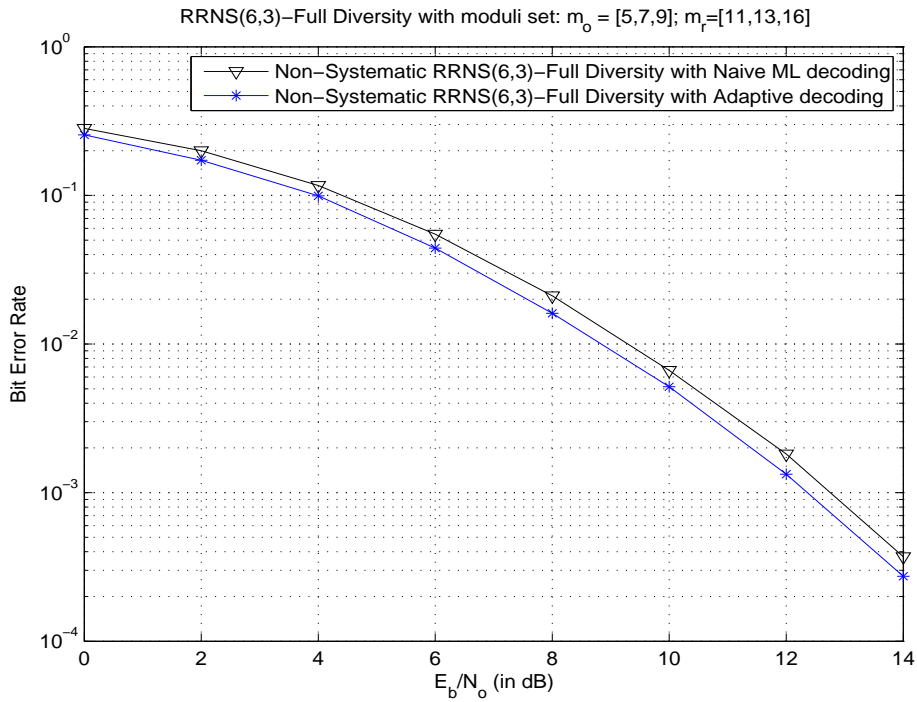
Figure 5.9 shows the comparison in performance of Indirect mapping scheme. In one case we use the transmission where each residue is converted back to  $n = \lceil \log_2(\max\{m_1, \dots, m_u\}) \rceil$  bits i.e., redundant bits are transmitted. In the second case we use the scheme in which each residue  $r_i$ , corresponding to moduli  $m_i$ , is converted into  $n_i = \lceil \log_2(m_i) \rceil$  bits for  $i = 1, \dots, u$ . We can see that for the case in which lower number of bits are transmitted, the performance improves. On an average, we use lower number of bits for transmission of each residue. Thus when we we have a residue digit error, it translates to lesser number of bit errors. This reflects in the performance improvement.

## Performance of the Adaptive Demapping Scheme



**Figure 5.10:** Comparison in BER performance of Systematic and Non-systematic RRNS (6,3)- STBC with moduli set of  $m_o = \{5, 7, 9\}$ ,  $m_r = \{11, 13, 16\}$  for the case of Adaptive Demapping.

Figure 5.10 shows the performance of both Systematic and Non-Systematic RRNS(6, 3)-STBC schemes when the proposed Adaptive demapping is used. It can be seen that the adaptive demapping scheme offers a further 1 dB - 1.5 dB performance improvement over the DA mapping scheme when exhaustive search based ML decoding is used. In case of adaptive demapping, we eliminate some of the residue which are not valid choices corresponding to a particular modulus. This increases the inter-symbol distance of the constellation for the corresponding modulus. This decreases the symbol error probability of the super channel. This in turn leads to better error detection and correction in the RRNS decoding stage. This improvement is reflected in Figure 7. The added advantage in the adaptive case is the lesser number of comparisons which decreases complexity.

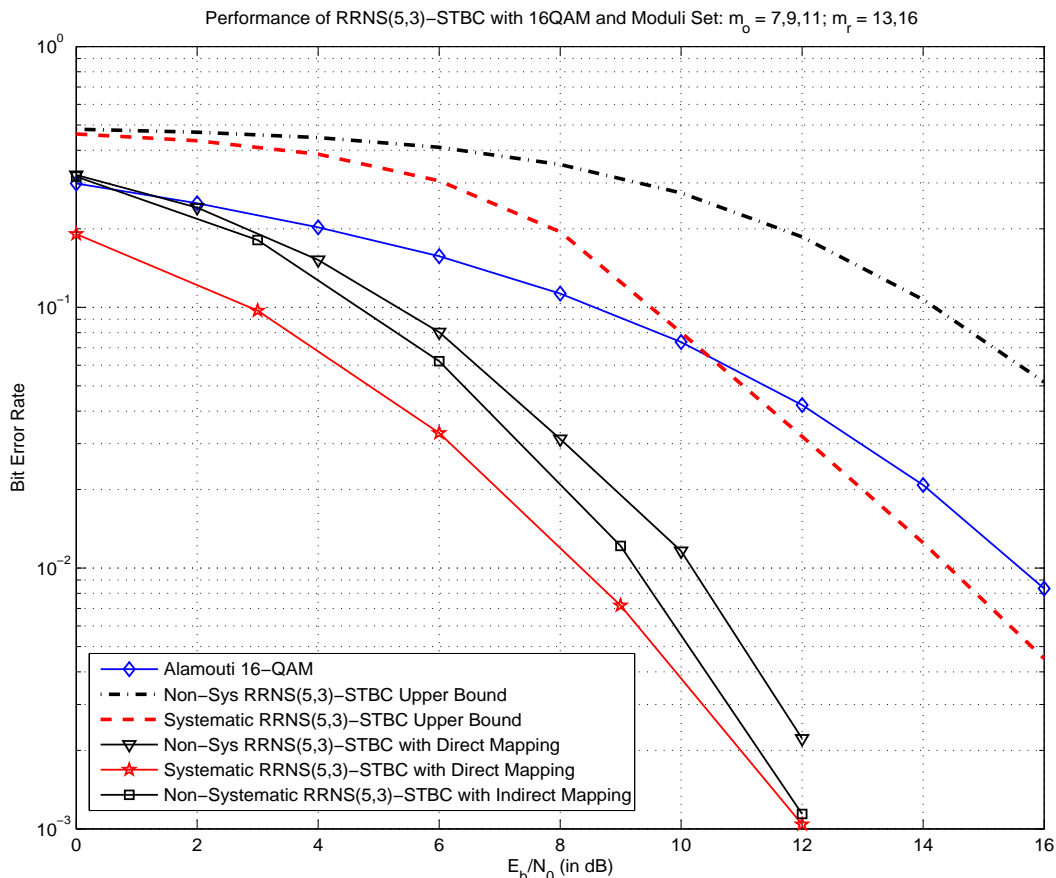


**Figure 5.11:** Comparison in BER performance of Non-systematic RRNS (6,3)- STBC with moduli set of  $m_o = \{5, 7, 9\}$ ,  $m_r = \{11, 13, 16\}$  for the case of Gray coded Direct Mapping and naive vs. Adaptive Demapping.

Figure 5.11 shows that the adaptive demapping scheme, when applied to a Gray coded direct mapped constellation, give a relatively lesser improvement in performance. However, we get a comparable, even slightly better performance with lesser number of ML searches. So this demapping method should be preferred over exhaustive ML decoding.

## 5.2.2 Systematic RRNS-STBC

### Systematic RRNS-STBC vs. Non-Systematic RRNS-STBC & OSTBC



**Figure 5.12:** BER performance of Systematic and Non-systematic RRNS (5,3)- STBC with moduli set of  $m_o = \{7, 9, 11\}$ ,  $m_r = \{13, 16\}$ .

In Figure 5.12, BER performance of RRNS (5, 3)-STBC using full diversity transmission and Alamouti coding scheme is compared. The theoretical upper bounds are simulated. The moduli set that is used in case of Systematic and Non-systematic RRNS (5, 3)-STBC is  $\{7, 9, 11, 13, 16\}$ , where  $m_o = \{7, 9, 11\}$  and  $m_r = \{13, 16\}$  correspond to the original moduli set and redundant moduli set, respectively. 16-QAM modulation scheme is applied in both RRNS (5, 3)-STBC and Alamouti scheme. The global codes efficiency of RRNS (5, 3)-STBC

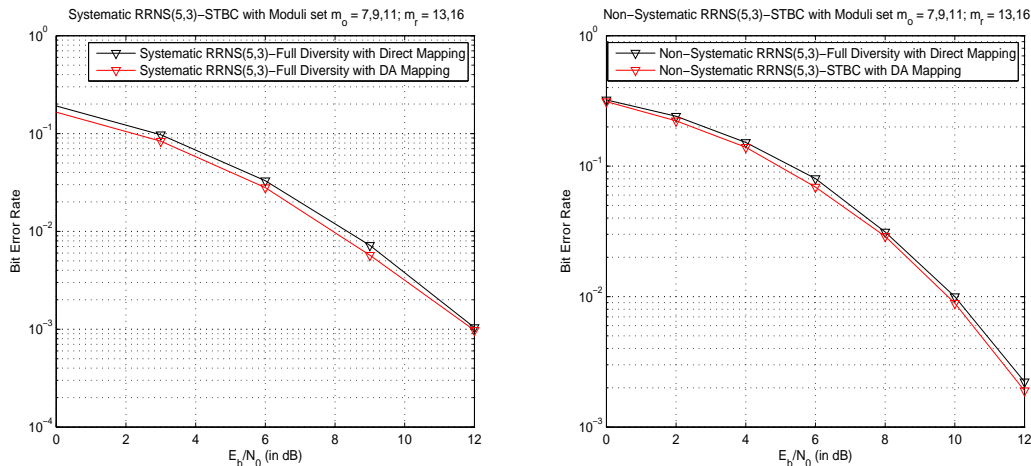


( $R_c R_s = 0.5 \times 1 = 0.5$ ) is the same as Alamouti coding ( $R_c R_s = 1 \times 0.5 = 0.5$ ). The coding rate of systematic RRNS-STBC is given by equation(4.26).

It is observed that both systematic and non-systematic RRNS (5, 3)-STBC outperforms Alamouti coding scheme in terms of BER. This is expected as in this case,  $\chi/2 = 1.5$ . Therefore, the contribution of the additional term  $\chi/2$  provides a similar diversity order relative to Alamouti scheme. Furthermore, RRNS-STBC exploits extra coding gain while Alamouti coding has no coding gain. All these features are clearly revealed in Figure 5.12. For the RRNS-STBC with Indirect Mapping, the basis of comparison is the transmission rate given by bits per channel use. Here the moduli set of the RRNS-STBC is chosen as  $m_o = \{9, 11, 13\}$ ,  $m_r = \{16, 17\}$ . This yields a code rate  $R_c = 0.48$  and  $k_b = 10$ . Thus in this case the  $\eta_G \approx 0.5$ . Since we are using block length  $T = 5$ , the bits per channel use in case of this code is 4. This is because we are transmitting 10 bits using 5 complex symbols. Thus for a  $2 \times 2$  system, 20 bits are transmitted using 5 channel uses or time slots. Thus for the RRNS(5, 3)-STBC, transmission rate is 4 bits per channel use. The Alamouti code also transmits at 4 bits per channel use. We can see that the RRNS-STBC still outperforms the Alamouti scheme when bits per channel use is used as a metric for comparison.

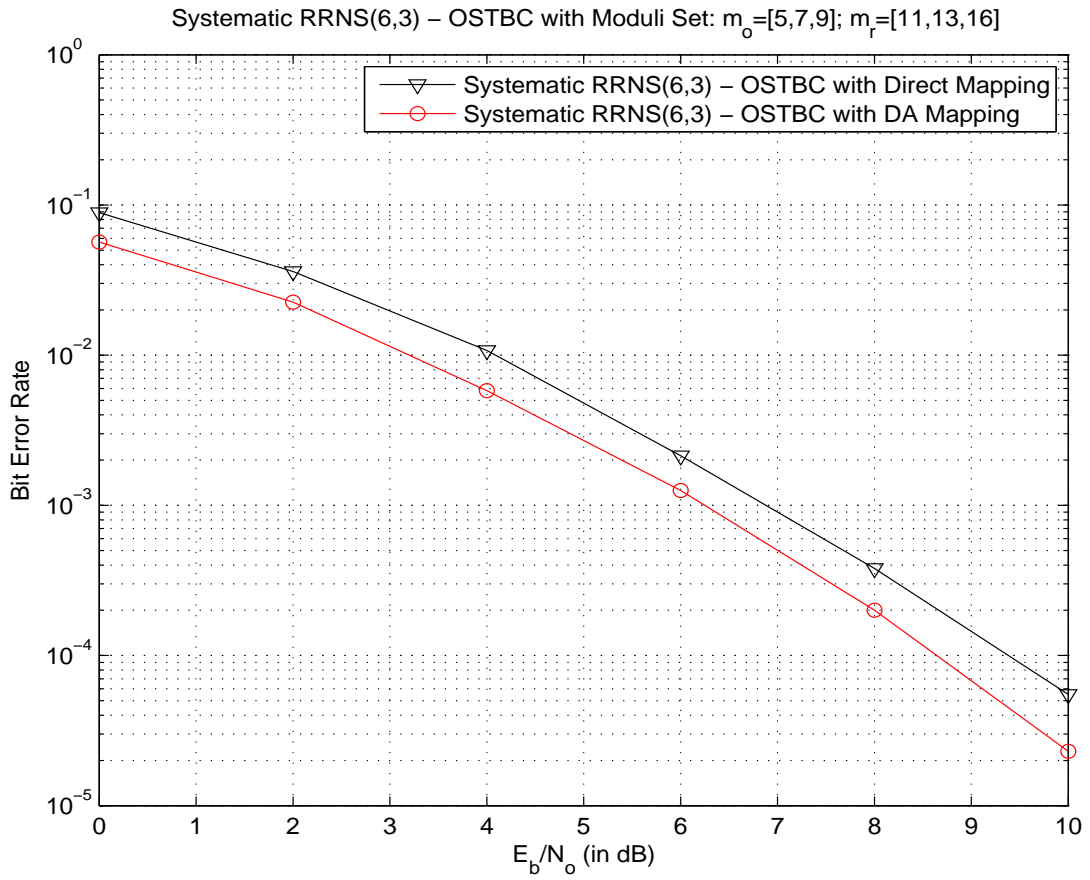
It is also seen from Figure 5.12, the Systematic RRNS-STBC outperforms the Non-Systematic RRNS-STBC which corroborates the theoretical results and discussions. Also, the theoretical upper bounds are seen to be a bit loose but that results from the approximations and assumptions made in Chapter 4. However, the theoretical BER curves still show that systematic RRNS-STBC outperforms non-systematic RRNS-STBC.

## Systematic RRNS-STBC with Direct and DA Mapping



**Figure 5.13:** Comparison in BER performance of Systematic and Non-systematic RRNS (5,3)- STBC with moduli set of  $m_o = \{7, 9, 11\}$ ,  $m_r = \{13, 16\}$ , for the case of Direct Mapping and Probability based Distance Aware Mapping.

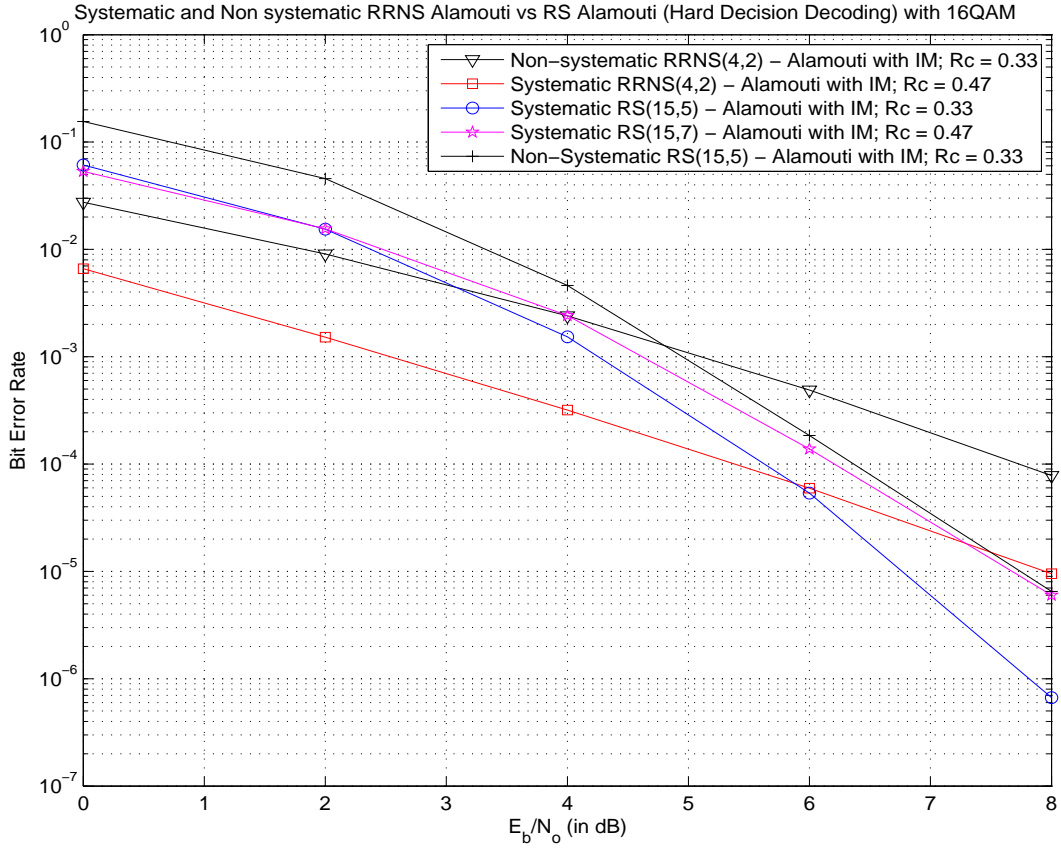
In Figure 5.13, the improvement in performance obtained by use of DA mapping in case of Systematic and Non-systematic RRNS-STBC is shown. The use of DA mapping gives an improvement of 0.5dB in BER performance. It can also be seen that for the same code parameters, the performance of the Systematic RRNS is better than the Non-systematic RRNS. This result is a direct implication of Lemma(1) and discussions at the end of Section 4.2.3 in Chapter 4. Also, as discussed in 5.2.1, the DA mapping performance can be seen to approach the Direct mapping case for high SNRs.



**Figure 5.14:** BER performance of Systematic RRNS (6,3)- STBC with moduli set of  $m_o = \{5, 7, 9\}$ ,  $m_r = \{11, 13, 16\}$ , for the case of Direct Mapping and Probability based Distance Aware Mapping.

Figure 5.14 shows the improvement in performance in the case of Alamouti's scheme being used as the inner OSTBC. It is seen that the DA Mapping scheme provides a improvement of 1 dB SNR at a bit error rate of  $10^{-2}$ .

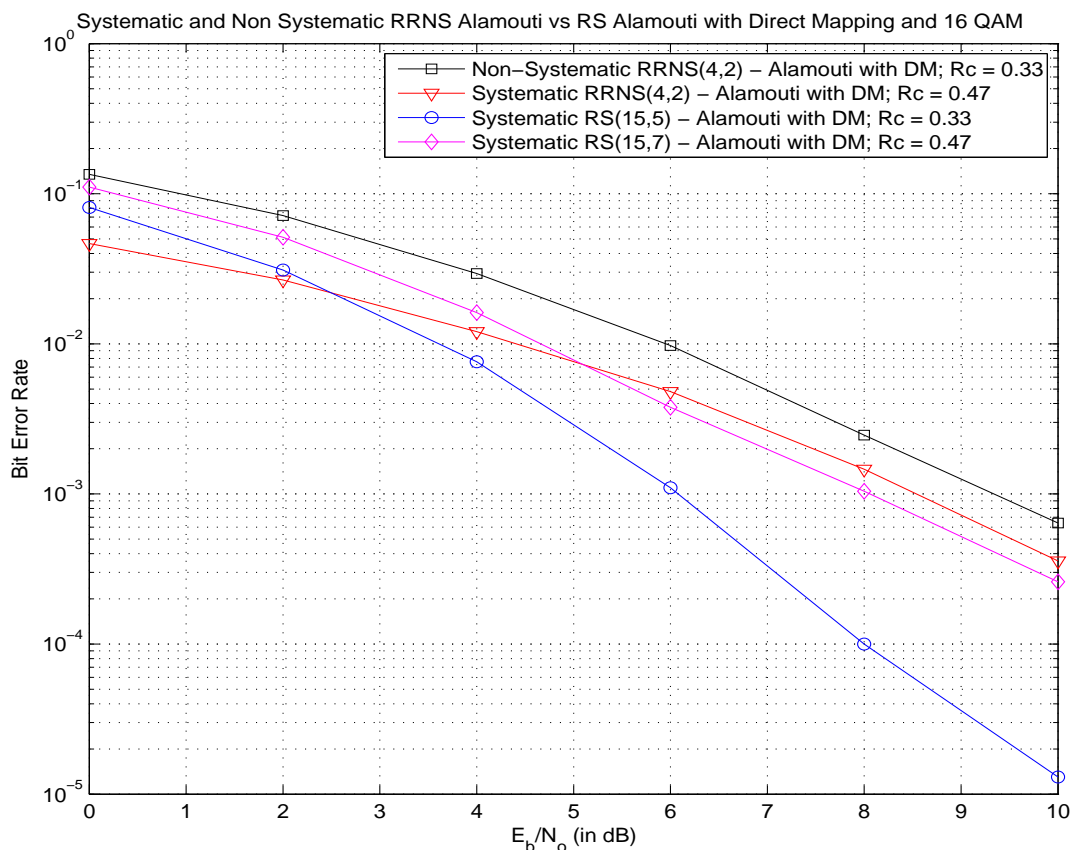
## Systematic & Non-Systematic RRNS-OSTBC vs. Concatenated OSTBC schemes



**Figure 5.15:** Comparison BER performance of Systematic and Non-systematic RRNS (4,2)- STBC with moduli set of  $m_o = \{7, 9\}$ ,  $m_r = \{13, 16\}$  with Systematic and Non-systematic RS-STBC Schemes for the case of Indirect Mapping.

In Figure 5.15, the proposed schemes are compared with concatenated RS-Alamouti codes. It can be seen that at low SNR region the Non-systematic RRNS-Alamouti outperforms both the Systematic and Non-systematic (15,5)RS-Alamouti codes which have the same rate i.e.,  $R_c = 0.33$ . For the same set of moduli, the Systematic RRNS-Alamouti has a higher coding rate i.e.,  $R_c = 0.47$ . It can be seen that in low SNR region, the Systematic RRNS-Alamouti outperforms both the systematic and non-systematic (15,5)RS-Alamouti as well as the (15,7)RS-Alamouti. Despite having the higher coding rate, the Systematic

RRNS performs better than the Non-Systematic RRNS due to more efficient binary to residue mapping.



**Figure 5.16:** Comparison BER performance of Systematic and Non-systematic RRNS (4,2)- STBC with moduli set of  $m_o = \{7, 9\}$ ,  $m_r = \{13, 16\}$  with RS-STBC Schemes for the case of Direct Mapping.

Figure 5.16 shows the comparison of the systematic and Non-Systematic RRNS-Alamouti with the Systematic RS-Alamouti for the case of Direct Mapping. As expected the Systematic RS codes outperform the Non-systematic RRNS but the Systematic RRNS-Alamouti shows similar performance to the (15,7)RS-Alamouti at higher SNRs and slightly better performance at low SNR range of 0 – 5 dB.

### 5.3 Summary

In this chapter, we have analyzed the simulation results with respect to both Non-systematic and Systematic RRNS-STBC schemes. The results corroborate the theoretical performance analysis in Chapter 4. It has been clearly shown that the RRNS-STBC schemes outperform the Alamouti scheme and other concatenated STBC scheme like the RS-STBC and Cyclic-STBC codes at low SNRs. The DA mapping scheme also brings about an appreciable improvement, in order of 1- 2 dB, for SNR regions of interest i.e., 0-10 dB. The DA mapping can be further optimized by selecting moduli sets which have more separation among the moduli in terms of prior probability of occurrence. The Systematic RRNS-STBC has been shown to outperform the Non-systematic RRNS-STBC owing to its more efficient binary to residue mapping as discussed in Chapter 2. The adaptive demapping scheme gives an improvement in performance for both Systematic and Non-systematic RRNS-STBC, even with a reduction in the number of ML searches.

# Chapter 6

## Conclusions

In this thesis, we have proposed a unique RRNS based STBC design. The main objective behind our research is to provide an application of RRNS based concatenated space-time code to a MIMO wireless communication system. Chapters 3, 4 and 5 form the core of our research. In this chapter, we provide a concise summary of the contributions of our research and the conclusions drawn. We also discuss the future work that can be done to further optimize the performance of the proposed RRNS-STBC system.

### 6.1 Summary of Key Contributions

We have proposed an application of RRNS based channel coding scheme coupled with Direct Mapping of residues to complex constellations to design Space-time Block codes which have a higher degree of freedom with respect to design parameters. The proposed RRNS-STBC scheme is a non-binary concatenated coding scheme which is highly modular and can be used in high data rate systems. The carry free property of RRNS ensures that error propagation within a codeword is eliminated. The concatenated code parameters can be changed to encode different block lengths without extensive change in hardware, thus making the implementation highly modular.

In Chapter 2, we show that the Systematic RRNS-STBC scheme has a more efficient mapping scheme than the Non-systematic RRNS-STBC. We confirm our conjectures through the simulation results, where we show that the Systematic RRNS-STBC performs better

than the Non-systematic RRNS-STBC for the same set of moduli. We show that the proposed RRNS-STBC scheme outperforms the Alamouti scheme. Other concatenated schemes like RS-STBC are also outperformed at low SNRs. The application of DA mapping brings about further performance improvement in RRNS-STBC schemes. The decoding of RRNS-STBC is more complex than OSTBC when CRT is used. But we can use alternatives like MRC and BEX, as discussed in Chapter 2, to decrease complexity.

We map the residues directly to complex constellation points using the Direct Mapping scheme, which optimizes the link between coded non-binary information symbols and complex constellation points. In Chapter 3, we have proposed a unique probability based distance aware direct mapping scheme. The DA mapping scheme takes advantage of the a priori probability distribution of the coded data symbols to map them intelligently to complex constellation points. The mapping is done using a set partitioning scheme such that maximum distance separation is obtained between the symbols having highest probability of occurrence. We show that code parameters can be chosen so as to maximize the separation between highest probability sets of residues so that maximum utilization of the DA mapping scheme can be achieved. We have also shown that the DA mapping scheme ceases to provide appreciable improvement over the naive Gray coded mapping when the SNR is very high. This is because the decoding spheres for each constellation point becomes smaller as SNR increases. We also propose an alternative IM scheme where residues are converted back to bits before being mapped to the complex constellation. A modified IM scheme has also been formulated in order to increase transmission efficiency by transmitting lesser number of bits than in the naive IM scheme. This is advantageous in cases where the difference between the minimum and maximum moduli in the moduli set is large. We have shown that the IM scheme shows improvement in performance similar to the DA mapping scheme but comes at the cost of more transmitted bits. Thus we can conclude that DA mapping scheme is a more efficient scheme. We have also proposed an adaptive demapping scheme, which exploits the RRNS code structure to decrease the total number of ML searches during hard



decision decoding and improve the performance of the concatenated system. We have shown that the adaptive demapping scheme gives a 0.5 – 1.5 dB improvement in performance. We have also shown that the relative error performance, using DA mapped constellations is more than when a Gray coded direct mapped constellation is used. This implies that the adaptive demapping scheme can exploit the DA mapping scheme further and improve the error performance. The adaptive demapping scheme provides performance improvement in the case of both Systematic and Non-systematic RRNS-STBC, which is justified by the simulation results.

In Chapter 4, we have designed a system which enables the application of RRNS-STBC scheme for encoding binary data streams. The RRNS acts as the outer code while the STBC and the  $M$ -ary mapping scheme together form the inner code. We have analyzed the probability of error performance of both Systematic and Non-systematic RRNS-STBC codes. We give a detailed discussion on code construction for both Non-systematic and Systematic RRNS-STBC and derive bounds on the codeword and bit error probability. We draw analogies with Reed Solomon (RS) codes and show conditions under which RRNS codes can be approximated as RS codes. We assume equal gain combining and maximum likelihood (ML) detection at the receiver to quantify the achievable performance of the RRNS-STBC schemes. The expressions of probability bounds throw further light on advantages of the proposed RRNS-STBC scheme. From the bounds on the BER we can see that use of RRNS gives us an extra factor,  $\chi/2$ , which can help us optimize the coding and diversity gain. The factor  $\chi/2$  can be controlled directly by varying the coding parameters of the RRNS-STBC, which is a very interesting observation. We have shown that the diversity gain is bounded by the factor  $M_T \times M_R$ . Beyond this the diversity gain becomes constant and the coding gain increases.

In Chapter 5, we demonstrate the results for a 16-QAM constellation but the scheme, in general, can be extended to any complex constellation. It is shown that the results and conclusions from the previous chapters are corroborated by the simulation results.

We have investigated the performance of the RRNS-STBC over a  $2 \times 2$  MIMO wireless channel in a Rayleigh fading environment. In the next section we discuss future work with the goal of further optimizing the system performance.

## 6.2 Future Work

Some interesting areas which can be investigated with respect to extending the present work:

- An interesting area of work in extension to the original DA mapping scheme, would be to quantify the choice of moduli which can produce the optimum code with respect to separation of the moduli based on the apriori probability. We can identify the exact distribution of the apriori probability mass function of the residues. The code parameters which generate residues according to the optimum probability distribution can be identified. This will generalize the choice of moduli for DA mapping which can give maximum possible improvement in performance.
- We can also extend the DA mapping algorithm to non-square constellations like 32-QAM. We can also investigate further receiver architectures to decrease complexity while maintaining near optimal performance.
- Another area worth investigating would be characterize the achievable capacity that can be obtained by use of Systematic and Non-systematic RRNS-STBC.
- Different suboptimal decoding schemes including sphere decoding, soft decision decoding and turbo decoding as in [37] can be implemented to counter the complexity of hard ML decoding.

# Bibliography

- [1] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “Wireless sensor networks: a survey,” *Computer Networks*, vol. 38, no. 4, pp. 393 – 422, 2002. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S1389128601003024>
- [2] C.-Y. Chong and S. Kumar, “Sensor networks: evolution, opportunities, and challenges,” *Proceedings of the IEEE*, vol. 91, no. 8, pp. 1247 – 1256, aug. 2003.
- [3] A. Davies, “Ww2 british army battlefield wireless communications equipment,” in *History of Telecommunications Conference, 2008. HISTELCON 2008. IEEE*, sept. 2008, pp. 83 –90.
- [4] Z. Li, G. Feng, F. Liu, J. Dong, R. Kamoua, and W. Tang, “Wireless health monitoring system,” in *Applications and Technology Conference (LISAT), 2010 Long Island Systems*, may 2010, pp. 1 –4.
- [5] E. Lassiter, “Navstar global positioning system: A satellite based microwave navigation system,” in *Microwave Symposium, 1975 IEEE-MTT-S International*, may 1975, p. 334.
- [6] A. Kurs, A. Karalis, R. Moffatt, J. Joannopoulos, P. Fisher, and M. Soljagic, “Wireless power transfer via strongly coupled magnetic resonances,” *Science*, vol. 317, pp. 83–86, July 2007.
- [7] D. Bagri, J. Statman, and M. Gatti, “Proposed array-based deep space network for nasa,” *Proceedings of the IEEE*, vol. 95, no. 10, pp. 1916 –1922, oct. 2007.
- [8] D. Antsos, “Mars technology program communications and tracking technologies for mars exploration,” in *Aerospace Conference, 2006 IEEE*, 0-0 2006, p. 20 pp.

- [9] E. Biglieri, R. Calderbank, A. Constantinides, A. Goldsmith, A. Paulraj, and H. V. Poor, *MIMO Wireless Communications*. New York, NY, USA: Cambridge University Press, 2010.
- [10] P. Morgensen, “Gsm base-station antenna diversity using soft decision combining on up-link and delayed-signal transmission on down-link,” in *Vehicular Technology Conference, 1993 IEEE 43rd*, may 1993, pp. 611 –616.
- [11] N. Seshadri and J. Winters, “Two signaling schemes for improving the error performance of frequency-division-duplex (fdd) transmission systems using transmitter antenna diversity,” in *Vehicular Technology Conference, 1993 IEEE 43rd*, may 1993, pp. 508 –511.
- [12] D. Gore, S. Sandhu, and A. Paulraj, “Delay diversity codes for frequency selective channels,” in *Communications, 2002. ICC 2002. IEEE International Conference on*, vol. 3, 2002, pp. 1949 – 1953 vol.3.
- [13] M. Costa, “Writing on dirty paper (corresp.),” *Information Theory, IEEE Transactions on*, vol. 29, no. 3, pp. 439 – 441, may 1983.
- [14] N. Jindal and A. Goldsmith, “Dirty-paper coding versus tdma for mimo broadcast channels,” *Information Theory, IEEE Transactions on*, vol. 51, no. 5, pp. 1783 – 1794, may 2005.
- [15] S. Parkvall, M. Karlsson, M. Samuelsson, L. Hedlund, and B. Goransson, “Transmit diversity in wcdma: link and system level results,” in *Vehicular Technology Conference Proceedings, 2000. VTC 2000-Spring Tokyo. 2000 IEEE 51st*, vol. 2, 2000, pp. 864 –868 vol.2.
- [16] V. Tarokh, N. Seshadri, and A. Calderbank, “Space-time codes for high data rate wireless communications: Performance criterion and code construction,” *Information Theory, IEEE Transactions on*, vol. 44, no. 2, pp. 744–765, March 1998.

- [17] A. Naguib, V. Tarokh, N. Seshadri, and A. Calderbank, “A space-time coding modem for high-data-rate wireless communications,” *Selected Areas in Communications, IEEE Journal on*, vol. 16, no. 8, pp. 1459–1478, oct 1998.
- [18] V. Tarokh, A. Naguib, N. Seshadri, and A. Calderbank, “Space-time codes for high data rate wireless communication: performance criteria in the presence of channel estimation errors, mobility, and multiple paths,” *Communications, IEEE Transactions on*, vol. 47, no. 2, pp. 199–207, feb 1999.
- [19] S. Alamouti, “A simple transmit diversity technique for wireless communications,” *Selected Areas in Communications, IEEE Journal on*, vol. 16, no. 8, pp. 1451–1458, oct 1998.
- [20] V. Tarokh, H. Jafarkhani, and A. Calderbank, “Space-time block codes from orthogonal designs,” *Information Theory, IEEE Transactions on*, vol. 45, no. 5, pp. 1456–1467, jul 1999.
- [21] B. Hassibi and B. Hochwald, “High-rate codes that are linear in space and time,” *Information Theory, IEEE Transactions on*, vol. 48, no. 7, pp. 1804–1824, jul 2002.
- [22] L. Zheng and D. Tse, “Diversity and multiplexing: a fundamental tradeoff in multiple-antenna channels,” *Information Theory, IEEE Transactions on*, vol. 49, no. 5, pp. 1073–1096, may 2003.
- [23] L. L. Yang and L. Hanzo, “Redundant residue number system based error correction codes,” in *Vehicular Technology Conference, 2001. VTC 2001 Fall. IEEE VTS 54th*, vol. 3, 2001, pp. 1472–1476 vol.3.
- [24] R. Cosentino, “Fault tolerance in a systolic residue arithmetic processor array,” *Computers, IEEE Transactions on*, vol. 37, no. 7, pp. 886–890, jul 1988.

- [25] F. Barsi and P. Maestrini, "Error correcting properties of redundant residue number systems," *Computers, IEEE Transactions on*, vol. C-22, no. 3, pp. 307 – 315, march 1973.
- [26] S.-S. Yau and Y.-C. Liu, "Error correction in redundant residue number systems," *Computers, IEEE Transactions on*, vol. C-22, no. 1, pp. 5 – 11, jan. 1973.
- [27] L. Yang and L. Hanzo, "Coding theory and performance of redundant residue number system codes," August 1999. [Online]. Available: [http://www-mobile.ecs.soton.ac.uk/lly/papers/RRNS\\_code.pdf](http://www-mobile.ecs.soton.ac.uk/lly/papers/RRNS_code.pdf)
- [28] H. Krishna and J.-D. Sun, "On theory and fast algorithms for error correction in residue number system product codes," *Computers, IEEE Transactions on*, vol. 42, no. 7, pp. 840 –853, jul 1993.
- [29] R. Watson and C. Hastings, "Self-checked computation using residue arithmetic," *Proceedings of the IEEE*, vol. 54, no. 12, pp. 1920 – 1931, dec. 1966.
- [30] H. Krishna, K.-Y. Lin, and J.-D. Sun, "A coding theory approach to error control in redundant residue number systems - Part I: Theory and single error correction," *Circuits and Systems II: Analog and Digital Signal Processing, IEEE Transactions on*, vol. 39, no. 1, pp. 8 –17, jan 1992.
- [31] J.-D. Sun and H. Krishna, "A coding theory approach to error control in redundant residue number systems. ii. multiple error detection and correction," *Circuits and Systems II: Analog and Digital Signal Processing, IEEE Transactions on*, vol. 39, no. 1, pp. 18 –34, jan 1992.
- [32] V. T. Goh and M. Siddiqi, "Multiple error detection and correction based on redundant residue number systems," *Communications, IEEE Transactions on*, vol. 56, no. 3, pp. 325 –330, march 2008.

- [33] T. Keller, T. Liew, and L. Hanzo, "Adaptive rate RRNS coded OFDM transmission for mobile communication channels," in *Vehicular Technology Conference Proceedings, 2000. VTC 2000-Spring Tokyo. 2000 IEEE 51st*, vol. 1, 2000, pp. 230 –234 vol.1.
- [34] L. Yang and L. Hanzo, "Performance of residue number system based ds-cdma over multipath fading channels using orthogonal sequences," *European Transactions on Telecommunications*, vol. 9, p. 525536, Nov.-Dec 1998.
- [35] T. Keller, T. Liew, and L. Hanzo, "Adaptive redundant residue number system coded multicarrier modulation," *Selected Areas in Communications, IEEE Journal on*, vol. 18, no. 11, pp. 2292 –2301, nov 2000.
- [36] T. Liew, L. Yang, and L. Hanzo, "Soft-decision redundant residue number system based error correction coding," in *Vehicular Technology Conference, 1999. VTC 1999 - Fall. IEEE VTS 50th*, vol. 5, 1999, pp. 2546 –2550 vol.5.
- [37] T. Liew, L.-L. Yang, and L. Hanzo, "Systematic redundant residue number system codes: Analytical upper bound and iterative decoding performance over AWGN and rayleigh channels," *Communications, IEEE Transactions on*, vol. 54, no. 6, pp. 1006 –1016, june 2006.
- [38] T. Shahana, B. Jose, R. James, K. Jacob, and S. Sasi, "RRNS-convolutional encoded concatenated code for ofdm based wireless communication," in *Networks, 2008. ICON 2008. 16th IEEE International Conference on*, dec. 2008, pp. 1–6.
- [39] L.-L. Yang and L. Hanzo, "Residue number system arithmetic assisted m-ary modulation," *Communications Letters, IEEE*, vol. 3, no. 2, pp. 28 –30, feb 1999.
- [40] M. Lalam, K. Amis, and D. Leroux, "On the use of reed-solomon codes in space-time coding," in *Personal, Indoor and Mobile Radio Communications, 2005. PIMRC 2005. IEEE 16th International Symposium on*, vol. 1, sept. 2005, pp. 31 –35.



- [41] K. Elleithy and M. Bayoumi, “Fast and flexible architectures for rns arithmetic decoding,” *Circuits and Systems II: Analog and Digital Signal Processing, IEEE Transactions on*, vol. 39, no. 4, pp. 226 –235, apr 1992.
- [42] C. Zhong, H. Xia, and J. Cruz, “On the serial concatenation of soft rs codes and space-time block codes over quasistatic fading channels,” in *Signals, Systems and Computers, 2004. Conference Record of the Thirty-Eighth Asilomar Conference on*, vol. 1, nov. 2004, pp. 1262 – 1265 Vol.1.
- [43] A. Sengupta, D. Zhu, and B. Natarajan, “On the performance of redundant residue number system codes assisted STBC design,” in *Computing, Networking and Communications (ICNC), 2012 International Conference on*, Jan. 30 - Feb. 2 2012, pp. 1051 –1055.
- [44] A. Sengupta and B. Natarajan, “Redundant residue number system based space-time block codes,” *European Transactions on Telecommunications (under review)*, 2012.
- [45] —, “Performance of systematic RRNS based space-time block codes with probability-aware adaptive demapping,” *Wiley Wireless Communications and Mobile Computing Journal (under review)*, 2012.
- [46] L. Hanzo, L. Yang, E. Kuan, and K. Yen, *Single and multi-carrier DS-CDMA: Multi-user detection, space-time spreading, synchronization and standards*. John Wiley and Sons,Ltd, 2003.
- [47] W. Jenkins and E. Altman, “Self-checking properties of residue number error checkers based on mixed radix conversion,” *Circuits and Systems, IEEE Transactions on*, vol. 35, no. 2, pp. 159 –167, feb 1988.
- [48] D. Mandelbaum, “Error correction in residue arithmetic,” *Computers, IEEE Transactions on*, vol. C-21, no. 6, pp. 538 –545, june 1972.

- [49] T. Liew and L. Hanzo, “Space-time codes and concatenated channel codes for wireless communications,” *Proceedings of the IEEE*, vol. 90, no. 2, pp. 187–219, feb 2002.
- [50] S. Sandhu and A. Paulraj, “Union bound on error probability of linear space-time block codes,” in *Acoustics, Speech, and Signal Processing, 2001. Proceedings. (ICASSP '01). 2001 IEEE International Conference on*, vol. 4, 2001, pp. 2473–2476 vol.4.
- [51] ———, “Unified design of linear space-time block codes,” in *Global Telecommunications Conference, 2001. GLOBECOM '01. IEEE*, vol. 2, 2001, pp. 1073–1077 vol.2.
- [52] S. Ali and B. Woerner, “Error performance of convolutionally concatenated space-time block codes,” in *SoutheastCon, 2006. Proceedings of the IEEE*, 31 2005-april 2 2006, pp. 181–187.
- [53] A. Goldsmith, *Wireless Communication*. Cambridge University Press, 2005.
- [54] S. Bandyopadhyay, G. Jullien, and A. Sengupta, “A systolic array for fault tolerant digital signal processing using a residue number system approach,” in *Systolic Arrays, 1988., Proceedings of the International Conference on*, may 1988, pp. 577–586.
- [55] C. Koc and P. Cappello, “Systolic arrays for integer chinese remaindering,” in *Computer Arithmetic, 1989., Proceedings of 9th Symposium on*, sep 1989, pp. 216–223.
- [56] R. Capocelli and R. Giancarlo, “Efficient vlsi networks for converting an integer from binary system to residue number system and vice versa,” *Circuits and Systems, IEEE Transactions on*, vol. 35, no. 11, pp. 1425–1430, nov 1988.
- [57] L. Hanzo, T. Liew, and B. Yeap, *Turbo Coding, Turbo Equalisation and Space-Time Coding for Transmission over Fading Channels*. Wiley-IEEE Press, 2003.

# Appendix A

## A.1 Proof of Lemma 2:

For an RRNS( $u, v$ )-STBC,  $d_{min} = \chi = u - v + 1$  and the maximum number of correctable errors is  $t = \lfloor \frac{u-v}{2} \rfloor$ . We define a variable  $\mathbf{X}_i$  for  $i = 1, 2, \dots, u$  such that

$$\mathbf{X}_i = \begin{cases} 1, & \text{with probability } P_s \text{ i.e. an error;} \\ -1, & \text{with probability } (1 - P_s) \text{ i.e. no error;} \end{cases} \quad (\text{A.1})$$

Now, given a transmitted codeword, the RRNS( $u, v$ )-STBC code can correct  $t$  number of errors, i.e., there is a codeword error if there are more than  $t$  symbol errors i.e. if

$$\sum_{i=1}^u \mathbf{X}_i \geq -v \quad (\text{A.2})$$

Now, using Chernoff bound, we have,

$$P \left( \frac{1}{u} \sum_{i=1}^u \mathbf{X}_i \geq \delta_m \right) \leq [e^{-\hat{w}\delta_m} E(e^{\hat{w}\mathbf{X}})]^u, \quad (\text{A.3})$$

where  $\hat{w}$  is the solution of the equation

$$E(Xe^{wX}) - \delta_m E(e^{wX}) = 0 \quad (\text{A.4})$$

For our case, we choose  $\delta_m = -\frac{v}{u}$ . This gives

$$P \left( \sum_{i=1}^u \mathbf{X}_i \geq -v \right) \leq \left[ e^{\frac{\hat{w}v}{u}} E(e^{\hat{w}\mathbf{X}}) \right]^u, \quad (\text{A.5})$$

where  $\hat{w}$  is the solution of

$$\begin{aligned}
& E(Xe^{wX}) - \left(-\frac{v}{u}\right)(e^{wX}) = 0 \\
\Rightarrow & -(1 - P_s)e^{-w} + P_s e^w - \left(-\frac{v}{u}\right) [(1 - P_s)e^{-w} + P_s e^w] = 0 \\
\Rightarrow & \left(1 - \frac{v}{u}\right) [P_s e^w - (1 - P_s)e^{-w}] = 0 \\
\Rightarrow & \hat{w} = \ln\left(\sqrt{\frac{1 - P_s}{P_s}}\right) = \ln(\theta)
\end{aligned} \tag{A.6}$$

Using this result, the bound in equation(A.5) is given as

$$\begin{aligned}
P(\sum_{i=1}^u \mathbf{X}_i \geq -v) & \leq [e^{-\ln(\theta)\delta_m} E(e^{\ln(\theta)\mathbf{X}})]^u, \\
& \leq \left[ e^{\ln\theta \frac{v}{u}} \{(1 - P_s)e^{-\ln\theta} + P_s e^{\ln\theta}\} \right]^u, \\
& \leq \theta^{(u+v)} 2^u P_s^u, \\
& \leq 2^u (1 - P_s)^{\frac{u+v}{2}} P_s^{\frac{u-v}{2}}, \\
& \leq 2^u P_s^{\chi/2}
\end{aligned}$$

By applying the union bound using equation(A.7) we get the desired result

$$P_E^{ns} \leq \frac{S^{ns}}{S} (N_c^{ns} - 1) 2^u P_s^{\chi/2} \tag{A.7}$$

# Appendix B

## B.1 Proof of Lemma 5:

To prove this Lemma, we follow the same procedure as in Appendix A. We use a Chernoff Bound to derive upper bounds for the expressions  $P_{E1}^s$  and  $P_{E2}^s$  from equations(4.31 and 4.32).

### B.1.1 Calculation of Upper Bound for $P_{E1}^s$

We model the problem as follows. We define a variable  $\mathbf{X}_i$  for  $i = 1, 2, \dots, u$  such that

$$\mathbf{X}_i = \begin{cases} 1, & \text{with probability } \bar{p}_{\epsilon 1}(1 - \bar{p}_{\epsilon 2}) \text{ i.e. an error;} \\ -1, & \text{with probability } (1 - \bar{p}_{\epsilon 1}) \text{ i.e. no error;} \end{cases} \quad (\text{B.1})$$

Now, given a transmitted codeword, the RRNS( $u, v$ )-STBC code can correct  $t$  number of errors, i.e., there is a codeword error if there are more than  $t$  symbol errors i.e. if

$$\sum_{i=1}^u \mathbf{X}_i \geq -v \quad (\text{B.2})$$

Now, using Chernoff bound, we have,

$$P\left(\frac{1}{u} \sum_{i=1}^u \mathbf{X}_i \geq \delta_m\right) \leq [e^{-\hat{w}\delta_m} E(e^{\hat{w}\mathbf{X}})]^u, \quad (\text{B.3})$$

where  $\hat{w}$  is the solution of the equation

$$E(Xe^{wX}) - \delta_m E(e^{wX}) = 0 \quad (\text{B.4})$$

For our case, we choose  $\delta_m = -\frac{v}{u}$ . This gives

$$P\left(\sum_{i=1}^u \mathbf{X}_i \geq -v\right) \leq \left[e^{\frac{\hat{w}v}{u}} E(e^{\hat{w}\mathbf{X}})\right]^u, \quad (\text{B.5})$$

where  $\hat{w}$  is the solution of

$$\begin{aligned} E(Xe^{wX}) - \left(-\frac{v}{u}\right)(e^{wX}) &= 0 \\ \Rightarrow -(1 - \bar{p}_{\epsilon 1})e^{-w} + \bar{p}_{\epsilon 1}(1 - \bar{p}_{\epsilon 2})e^w - \left(-\frac{v}{u}\right)[(1 - \bar{p}_{\epsilon 1})e^{-w} + \bar{p}_{\epsilon 1}(1 - \bar{p}_{\epsilon 2})e^w] &= 0 \\ \Rightarrow \left(1 - \frac{v}{u}\right)[\bar{p}_{\epsilon 1}(1 - \bar{p}_{\epsilon 2})e^w - (1 - \bar{p}_{\epsilon 1})e^{-w}] &= 0 \\ \Rightarrow \hat{w} = \ln\left(\sqrt{\frac{1 - \bar{p}_{\epsilon 1}}{\bar{p}_{\epsilon 1}(1 - \bar{p}_{\epsilon 2})}}\right) &= \ln(\theta) \end{aligned} \quad (\text{B.6})$$

Using this result, the bound in equation(B.5) is given as

$$\begin{aligned} P(\sum_{i=1}^u \mathbf{X}_i \geq -v) &\leq \left[e^{-\ln(\theta)\delta_m} E(e^{\ln(\theta)\mathbf{X}})\right]^u, \\ &\leq \left[e^{\ln\theta \frac{v}{u}} \{(1 - \bar{p}_{\epsilon 1})e^{-\ln\theta} + \bar{p}_{\epsilon 1}(1 - \bar{p}_{\epsilon 2})e^{\ln\theta}\}\right]^u \\ &\leq \theta^{(u+v)} 2^u [\bar{p}_{\epsilon 1}(1 - \bar{p}_{\epsilon 2})]^u \\ &\leq 2^u (1 - \bar{p}_{\epsilon 1})^{\frac{u+v}{2}} [\bar{p}_{\epsilon 1}(1 - \bar{p}_{\epsilon 2})]^{\frac{u-v}{2}} \\ &\leq 2^u \bar{p}_{\epsilon 1}^{\chi/2} (1 - \bar{p}_{\epsilon 2})^{\chi/2} \end{aligned}$$

By applying the union bound we get:

$$P\left(\sum_{i=1}^u \mathbf{X}_i \geq -v\right) \leq 2^u (\bar{p}_{\epsilon 1})^{\chi/2} (1 - \bar{p}_{\epsilon 2})^{\chi/2} \quad (\text{B.7})$$

Applying the union bound, we get

$$P_{E1}^s \leq (N_c^s - 1) 2^u (\bar{p}_{\epsilon 1})^{\chi/2} (1 - \bar{p}_{\epsilon 2})^{\chi/2} \quad (\text{B.8})$$

### B.1.2 Calculation of Upper Bound for $P_{E2}^s$

Again we define a variable  $\mathbf{X}_i$  for  $i = 1, 2, \dots, u$  such that

$$\mathbf{X}_i = \begin{cases} 1, & \text{with probability } \bar{p}_{\epsilon 1}\bar{p}_{\epsilon 2} \text{ i.e. an error;} \\ -1, & \text{with probability } (1 - \bar{p}_{\epsilon 1}) \text{ i.e. no error;} \end{cases} \quad (\text{B.9})$$

Following the same steps as in Appendix A, we have:

$$P\left(\sum_{i=1}^u \mathbf{X}_i \geq -v\right) \leq 2^u (\bar{p}_{\epsilon 1})^{\chi/2} (1 - \bar{p}_{\epsilon 2})^{\chi/2} \quad (\text{B.10})$$

Applying the union bound, we get

$$P_{E2}^s \leq (N_c^s - 1)2^u (\bar{p}_{\epsilon 1})^{\chi/2} (\bar{p}_{\epsilon 2})^{\chi/2} \quad (\text{B.11})$$

Therefore the upper bound on the codeword error probability is given by:

$$\begin{aligned} P_E^s &\leq \frac{S_{IC}^s}{S} (N_c^s - 1) 2^u (\bar{p}_{\epsilon 1})^{\chi/2} (1 - \bar{p}_{\epsilon 2})^{\chi/2} + \frac{S - S_{IC}^s}{S} (N_c^s - 1) 2^u (\bar{p}_{\epsilon 1})^{\chi/2} (\bar{p}_{\epsilon 2})^{\chi/2} \\ &\leq (N_c^s - 1) 2^u (\bar{p}_{\epsilon 1})^{\chi/2} \left[ \frac{S_{IC}^s}{S} (1 - \bar{p}_{\epsilon 2})^{\chi/2} + \frac{S - S_{IC}^s}{S} (\bar{p}_{\epsilon 2})^{\chi/2} \right] \end{aligned} \quad (\text{B.12})$$