Algebraic Number Precoding for Space-Time Block Codes

Zhihong Hong, Ke Liu, Nigel Boston, and Akbar M. Sayeed

***Abstract*— We propose a space-time block coding framework based on linear precoding. The codes for P transmit antennas are formed by transmitting the information vector (with P independent information symbols) L times where each time it is rotated by a distinct precoding matrix. The framework generalizes conventional spatial multiplexing techniques and facilitates tradeoff between rate and diversity. We propose a simple construction for precoding matrices whose parameters are chosen to guarantee maximal diversity using algebraic number theory. Our codes exhibit circular structure, which greatly simplifies the performance analysis and facilitates linear decoding. Theoretical analysis and numerical simulations demonstrated excellent performance of the proposed algebraic precoding framework.**

***Index Terms*— MIMO, algebraic number theory, cyclotomic fields, Diophantine approximation, space-time codes, spatial multiplexing, circular matrices**

I. Introduction

Multiple-input multiple-output (MIMO) communication systems, which employ multi-antenna arrays at the transmitter and receiver, have been shown to significantly improve the capacity and reliability of wireless communication links. Several distinct bandwidth-efficient MIMO techniques have been developed to exploit the spatial degrees of freedom in MIMO channels, including space-time coding [1], [2], [3], [4], [5] and spatial multiplexing [6]. These techniques entail a fundamental tradeoff between multiplexing gain and diversity as captured in [7], although complexity is often another important factor in practical schemes. For example, spatial multiplexing achieves high rate but less diversity by transmitting independent data streams from all transmit antennas. On the other hand, space-time codes, such as the orthogonal space-time block codes (STBC) [3], [2], focus on the transmit diversity advantage of MIMO systems but often at the cost of rate.

Recently there have been a series of works focusing on algebraic space-time codes (see e.g. [8], [9], [10], [11]). These algebraic codes exploit the algebraic properties of the underlining signal constellation. Powerful constructions such as [10], [11] achieve full "multiplexing" rate at full diversity. The multiplexing rate refers to the number of information symbols being transmitted in one channel use. Note that such a notion of full-rate, full-diversity codes is not in conflict with the information theoretic study of the multiplexing gain versus diversity tradeoff in [7] which is an asymptotic characterization in the limit of high signal-to-noise ratio (SNR) and the multiplexing gain is defined as a normalized capacity with respect to SNR. Nevertheless, the algebraic approach represents a major improvement over the earlier space-time code designs.

The construction of space-time codes proposed in this paper is in the spirit of the above algebraic method. It is inspired by our earlier work [12] on spatial multiplexing for correlated channels, where the transmitted vectors are precoded or rotated to avoid the channel "null space" due to spatial correlation. Its algebraic structure is inspired by the diagonal algebraic space-time codes (DAST) [9] and the threaded algebraic space-time codes (TAST) [10]. In DAST, the idea of constellation rotation, first developed in the context of signal space diversity [13] for single-input single-output fading channels, is further extended to MIMO channels. By exploiting the algebraic property of the signal constellation, DAST and TAST are able to achieve full diversity.

In this paper, we leverage the constellation rotation insight for designing space-time block codes from a different perspective. In the literature of space-time code design, diversity gain is optimized by maximizing the rank of the error codeword matrices, which is equivalent to maximizing the number of linearly independent error vectors. When two vectors are linearly independent, there is a nonzero angle between them. This can be easily achieved by rotating the same vector by two different precoding matrices. We thus propose a space-time block coding framework in which codes are designed using a set of $L \leq P$ precoding matrices, where P is the number of transmit antennas. Unlike DAST and TAST, our focus is on designing a code that is flexible in term of the tradeoff between rate and diversity. Using the theory of *cyclotomic fields* and *Diophantine approximation* in algebraic number theory, we construct precoding matrices that achieve L-fold transmit diversity and rate of P/L symbols/channel use. A prominent feature of our algebraic construction is the circular structure of the codewords. In particular, when $L = P$, the codewords are circular square matrices. The spectral representation of circular matrices greatly facilitates performance analysis and encoding/decoding of our proposed codes. We give closed-form expressions for codeword eigenvalues and bound the diversity and coding gain of the codes. Moreover, the proposed codes facilitate the use of (sub-optimal) linear receivers that exploit the circular structure of codewords to reduce the decoding complexity when $L = P$.

The organization of the rest of this paper is as follows.

Dr. Hong (zhihong.hong@crc.ca) is affiliated with Communications Research Centre Canada, 3701 Carling Ave., Box 11490, Station H, Ottawa, Ontario K2H 8S2. Dr. Liu (kel@qualcomm.com) is with Qualcomm Inc., 5775 Morehouse Drive, San Diego, CA 92121. Prof. Boston (boston@engr.wisc.edu) and Prof. Sayeed (akbar@engr.wisc.edu) are with Department of Electrical and Computer Engineering at the University of Wisconsin-Madison, 1415 Engineering Drive, Madison, WI 53706. This work was supported in part by the Office of Naval Research under grant #N00014-01-1-0825 and by the National Science Foundation grant CRCD.

The channel model, along with the space-time code design criteria, are briefly discussed in Section II. We present the proposed coding framework based on precoding matrices in Section III. The algebraic construction approach for the precoding matrices is studied in Section IV, followed by discussions and numerical examples of the algebraic codes in Section V. Finally, the concluding remarks are provided in Section VI.

II. Channel Model for Space-Time Block Codes

Consider a discrete-time MIMO channel with P transmit antennas and Q receive antennas. An STBC codeword can been seen as a $P \times L$ matrix $[x_{nt}]$ ($n = 0, \cdots, P-1$ and $t = 0, \cdots, L-1$), where the symbol x_{nt}, drawn from a complex alphabet $\mathcal{D}$, is transmitted from the n-th transmit antenna during the t-th discrete time instance. We assume the quasi-static fading scenario where the channel remains constant within the duration of one codeword transmission. The $Q \times L$ received signal in the presence of noise can be written in a matrix form as

$$\mathbf{Y} = \sqrt{\rho}\mathbf{H}\mathbf{X} + \mathbf{N} \tag{1}$$

where the $Q \times P$ channel matrix $\mathbf{H}$, perfectly known at the receiver but not at the transmitter, has i.i.d. complex Gaussian entries of zero mean and unit variance. Without loss of generality, the spatially and temporally white additive complex Gaussian noise is assumed to be of unit variance. The transmit power ρ is normalized, $\rho = \rho_t/P$, such that the total transmit power is ρ_t regardless of P.

Denote by $\mathbf{E} = \mathbf{X} - \hat{\mathbf{X}}$ the error codeword matrix between two codewords $\mathbf{X}$ and $\hat{\mathbf{X}}$. The associated error covariance matrix is defined as $\mathbf{R}_\mathbf{E} = \mathbf{E}\mathbf{E}^\dagger$ where $\dagger$ denotes the Hermitian transpose. The *pairwise error probability* (PEP) between $\mathbf{X}$ and $\hat{\mathbf{X}}$ is well characterized in [1] for quasi-static fading

$$\begin{aligned} P(\mathbf{X} \to \hat{\mathbf{X}}) &\le |\mathbf{I} + \frac{\rho}{4}\mathbf{E}\mathbf{E}^\dagger|^{-Q} \\ &\approx \Big(\prod_{l=0}^{\nu-1} \lambda_l(\mathbf{R}_\mathbf{E})\Big)^{-Q} (\rho/4)^{-\nu Q} \end{aligned} \tag{2}$$

where $\lambda_l(\mathbf{R}_\mathbf{E})$, $l = 0, \cdots, \nu-1$, are the *nonzero* eigenvalues of $\mathbf{R}_\mathbf{E}$, and the approximation is fairly accurate for medium to high SNR.

It thus follows the well-known rank and determinant criteria [1] for space-time codes. The diversity advantage of the code is defined as

$$\nu = \min_{\mathbf{E} \in \mathcal{E}} \operatorname{rank}(\mathbf{R}_\mathbf{E}) = \min_{\mathbf{E} \in \mathcal{E}} \operatorname{rank}(\mathbf{E}) \tag{3}$$

where $\mathcal{E}$ is the set of all possible codeword error matrices. (The total diversity gain achieved by such code is νQ due to multiple receive antennas.) Moreover, the coding gain is quantified as

$$\eta = \min_{\mathbf{E} \in \mathcal{E}} \Big(\prod_{l=0}^{\nu-1} \lambda_l(\mathbf{R}_\mathbf{E})\Big)^{1/\nu}. \tag{4}$$

III. Cyclic Extension for Spatial Multiplexing

Throughout this paper the block length L is limited by the number of transmit antennas ($L \le P$). We start with a straightforward extension of spatial multiplexing. The codeword is constructed as

$$\mathbf{X} = \begin{bmatrix} \mathbf{W}_0\mathbf{x} & \mathbf{W}_1\mathbf{x} & \cdots & \mathbf{W}_{L-1}\mathbf{x} \end{bmatrix} \tag{5}$$

where $\mathbf{x} = [x_0, \cdots, x_{P-1}]^T$ is a vector of P independent information symbols and $\mathbf{W}_l$'s are the unitary precoding matrices. Since the same symbol vector $\mathbf{x}$ is spread over L transmissions, the *multiplexing rate* is $R = P/L$ (symbols per channel use). The above design offers a trade-off between rate and diversity via different choices of L. When $L = 1$ it becomes the conventional spatial multiplexing which achieves the highest multiplexing rate but with no (transmit) diversity advantage. By increasing L it is possible to have higher diversity, albeit lowering multiplexing rate.

Our aim is to design precoding matrices $\mathbf{W}_l$'s that guarantee full diversity L while at the same time allow analytical study of the code properties. We consider precoding matrices of the following form[1]

$$\mathbf{W}_l = \mathbf{P}^l \operatorname{diag}(\theta_0, \theta_1, \cdots, \theta_{P-1}) = \mathbf{P}^l\mathbf{D} \tag{6}$$

where $0 \le l \le L-1$, and $\mathbf{P}$ is the $P \times P$ permutation matrix

$$\mathbf{P} = \begin{bmatrix} 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{bmatrix}. \tag{7}$$

The design parameters θ_k ($|\theta_k| = 1, \forall k$) represent phase rotation for input symbol vector $\mathbf{x}$. Without loss of generality, we can always set $\theta_0 = 1$.

The design in (6) induces a circular structure on codewords. In particular, for $L = P$, the codeword matrix can be written as

$$\mathbf{X} = \begin{bmatrix} x_0 & \theta_{P-1}x_{P-1} & \cdots & \theta_1 x_1 \\ \theta_1 x_1 & x_0 & \cdots & \theta_2 x_2 \\ \vdots & \vdots & \ddots & \vdots \\ \theta_{P-1}x_{P-1} & \theta_{P-2}x_{P-2} & \cdots & x_0 \end{bmatrix}. \tag{8}$$

One can view the above as a cyclic extension of spatial multiplexing: The transmit symbols first go through phase rotation and then are cyclically shifted across antennas during the successive transmission. This significantly simplifies the encoder at the transmitter. As we shall see later, the cyclic structure also allows efficient decoding at the receiver for the maximum diversity case.

The circular codeword admits special eigenvalue decomposition

$$\mathbf{X} = \mathbf{A}_T \mathbf{S} \mathbf{A}_T^\dagger \tag{9}$$

[1]Our reviewers have brought to our attention a later work [11] that achieves full-rate full-diversity using $\mathbf{W}_l = (\mathbf{P}\mathbf{D})^l$. This is a noted improvement over our design proposed in this paper. Here we use $\mathbf{W}_l = \mathbf{P}^l\mathbf{D}$ to ensure the DFT structure of our code which is further exploited to reduce encoding and decoding complexity.

where $\mathbf{A}_T = \left[e^{j2\pi kn/P}\right]$ is the $P \times P$ unitary DFT matrix and $\mathbf{S}$ is a diagonal matrix whose diagonal elements are given by

$$s_k = \sum_{n=0}^{P-1} \theta_n x_n e^{-j2\pi kn/P}. \tag{10}$$

or as a matrix form,

$$\mathbf{s} = \mathbf{A}_T^\dagger \mathbf{D}\mathbf{x} \tag{11}$$

where $\mathbf{s} = (s_0, \ldots, s_{P-1})^T$ is the vector of eigenvalues s_k of the codeword, $\mathbf{D} = \mathrm{diag}(\theta_0, \ldots, \theta_{P-1})$ is the diagonal phase matrix used in linear precoding, and $\mathbf{x} = (x_0, \ldots, x_{P-1})^T$ is the spatial multiplexing symbols. Correspondingly, the error codeword matrix becomes

$$\mathbf{E} = \begin{bmatrix} e_0 & \theta_{P-1}e_{P-1} & \cdots & \theta_1 e_1 \\ \theta_1 e_1 & e_0 & \cdots & \theta_2 e_2 \\ \vdots & \vdots & \ddots & \vdots \\ \theta_{P-1}e_{P-1} & \theta_{P-2}e_{P-2} & \cdots & e_0 \end{bmatrix} = \mathbf{A}_T \mathbf{\Lambda} \mathbf{A}_T^\dagger \tag{12}$$

where $\mathbf{\Lambda}$ is again a diagonal matrix whose diagonal elements are the eigenvalues of $\mathbf{E}$. Due to the circular structure, the eigenvalues can be written explicitly in close form

$$\lambda_k(\mathbf{E}) = \sum_{n=0}^{P-1} \theta_n e_n e^{-j2\pi kn/P} \tag{13}$$

The matrix $\mathbf{E}$ has rank P when every $\lambda_k \neq 0$, $0 \leq k \leq P-1$. In the following, we leverage algebraic number theory to guarantee that all λ_k are nonzero, thus achieving full diversity.

IV. Algebraic Number Theoretic Constructions

In the following, the symbols $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ denote positive natural numbers, rational integers, rationals, reals and complex numbers, respectively. Let R be a ring with identity, the symbol $R[X]$ denotes the polynomial ring with coefficients in R. We begin with a few basic terminologies in algebraic number theory. Readers are referred to [14], [15], [16] for a detailed exposition of algebraic number theory and abstract algebra.

Definition 1: A number $a \in \mathbb{C}$ is called an algebraic number if it satisfies a nonzero polynomial $p(X)$ in $\mathbb{Q}[X]$, that is,

$$0 = p(a) = b_n a^n + \cdots + b_1 a + b_0. \tag{14}$$

Definition 2: A number $z \in \mathbb{C}$ is called an algebraic integer if it satisfies a monic polynomial in $\mathbb{Z}[X]$, i.e., a polynomial with the highest order coefficient being 1.

It follows trivially from the definitions that algebraic integers are algebraic numbers. Examples of algebraic numbers and algebraic integers abound. In fact, $\mathbb{Q}$ and $\mathbb{Z}$ consist of algebraic numbers and algebraic integers. Other examples include $j = \sqrt{-1}$ which is a root of $X^2 + 1$ and $e^{j2\pi/n}$ which is a root of $X^n - 1$.

Let $\mathbb{A}$ be the set of all algebraic numbers. It can be shown that $\mathbb{A} \subseteq \mathbb{C}$ is a field so that field operations such as sum and division between two algebraic numbers yield algebraic numbers. Similarly the set of all algebraic integers, $\mathbb{O}$, is a ring.

Given $s \in S$ where $R \subseteq S$ is a unitary overring of R, the (canonical) *evaluation homomorphism* $\rho_s : R[X] \to S$ is defined as $\rho_s(p) = p(s)$. Its image is denoted by $R[s]$, which can be viewed as extension of R by adjoining s.

Definition 3: Let $F \subseteq E$ be a field extension. The field E can be viewed as a vector space over F. The dimension of this vector space is call the degree of the field extension, denoted by $|E : F|$.

Definition 4: An element $e \in E \supseteq F$ is said to be algebraic over F if it satisfies a nonzero polynomial in $F[X]$. There is a monic one with minimal degree among all such polynomials, called the minimal polynomial over F of e, denoted by $\min_F(e)$. The degree of $\min_F(e)$, $\deg \min_F(e)$, is called the degree of e over F. A field extension $F \subseteq E$ is called an algebraic extension over F if every element of E is algebraic over F.

Definition 5: A complex number ϵ is an n-th root of unity if $\epsilon^n = 1$ for some $n \in \mathbb{N}$, and it is a *primitive* n-th root of unit if $\epsilon^m \neq 1$ for $1 \leq m < n$.

A. Algebraic Integer Constellations

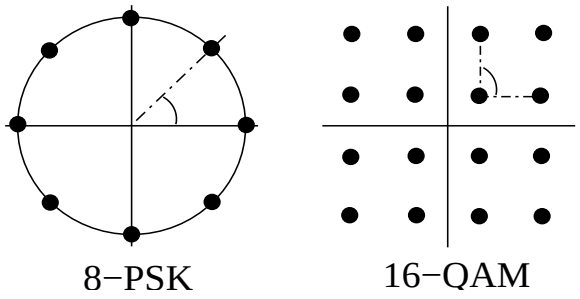


Fig. 1. Illustrations of signal constellations. The signal points in the complex plane are generated by multiplications in the amplitude and rotations in the phase. The base phase rotation is $\frac{\pi}{4}$ for the 8-PSK and $\frac{\pi}{2}$ for the 16-QAM constellation, respectively.

Fig. 1 depicts the signal constellations of Phase Shift Keyings (PSK) and Quadrature Amplitude Modulation (QAM). It demonstrates a certain regularity of the signal points in commonly used constellations. More specifically, signal points are discrete in the complex plane, and there exists multiplication in the amplitude as well as rotation in the phase angle. Under scale normalization, the amplitude can be modeled as multiplication by $\mathbb{Z}$, whereas the phase rotation can be seen as multiplication by $e^{j2\pi/A}$ where $2\pi/A$ is the minimal rotation with $A > 0$ a natural number. Therefore, one can generally assume that the signal constellation comes from the integer ring $\mathbb{Z}[e^{j2\pi/A}]$. For instance, the 8-PSK constellation can be represented by $\mathbb{Z}[e^{j2\pi/8}]$ with $A = 8$, and similarly, $\mathbb{Z}[j]$ with $A = 4$ for the QAM constellation.

Note that $\mathbb{Z}[e^{j2\pi/A}] \subset \mathbb{Q}[e^{j2\pi/A}]$, the A-th *cyclotomic field* (often denoted as $\mathbb{Q}_A$). So the signal constellation can be regarded as lying in the cyclotomic field as well. The following essential result regarding cyclotomic fields can be found in [14].

Theorem 1: Let $\langle \mathbb{Q}_A, \mathbb{Q}_B \rangle$ be the compositum of $\mathbb{Q}_A$ and $\mathbb{Q}_B$ in $\mathbb{C}$, that is, the minimal subfield of $\mathbb{C}$ that contains both

$\mathbb{Q}_A$ and $\mathbb{Q}_B$. The following hold.

$$\begin{aligned} |\mathbb{Q}_A : \mathbb{Q}| &= \deg \min_{\mathbb{Q}}(e^{j2\pi/A}) = \varphi(A) \\ \langle \mathbb{Q}_A, \mathbb{Q}_B \rangle &= \mathbb{Q}_{\mathrm{lcm}(A,B)} \\ \mathbb{Q}_A \cap \mathbb{Q}_B &= \mathbb{Q}_{\gcd(A,B)} \end{aligned} \tag{15}$$

where lcm and $\gcd$ stand for the least common multiple and the greatest common divisor, respectively. The Euler function $\varphi(n)$ is defined to be the number of integers $0 \le i \le n-1$ that are coprime to n, i.e., $\gcd(i,n) = 1$.

B. Full Diversity Codes

The algebraic structure of a signal constellation can be exploited to construct full diversity codes. We assume that the signal constellation in question is $\mathbb{Z}[e^{j2\pi/A}]$ where $A > 0$ is a natural number determined by the signal constellation as above. The full diversity criterion applied to the precoding amounts to requiring that any nonzero $P \times L$ error codeword matrix $\mathbf{E}$ has full rank. Since a $P \times L$ codeword matrix consists of the first L columns of the corresponding $P \times P$ codeword matrix, it suffices to focus on the case when $L = P$. In this case, the eigenvalues of error codeword matrix are given by

$$\lambda_k(\mathbf{E}) = \sum_{n=0}^{P-1} \theta_n e_n e^{-j2\pi kn/P}, \quad 0 \le k \le P-1. \tag{16}$$

The full diversity design is to seek θ_n with $|\theta_n| = 1$, a total of P points on the unit circle in the complex plane, such that $\lambda_k(\mathbf{E}) \neq 0$ for all $0 \le k \le P-1$ and all $\mathbf{E} \neq \mathbf{0}$.

Note $e^{-j2\pi n/P}$ appearing in (16) are P-th roots of unity. Hence, the eigenvalue λ_k can be seen as a linear combination of θ_n's with coefficients in

$$\mathbb{Z}[e^{j2\pi/A}][e^{j2\pi/P}] = \mathbb{Z}[e^{j2\pi/\,\mathrm{lcm}(A,P)}] \subset \mathbb{Q}_{\mathrm{lcm}(A,P)}. \tag{17}$$

Then the full diversity condition that $\lambda_k \neq 0$ unless all coefficients vanish translates exactly to the notion of *free basis*, or linearly independent basis. So we have just proved

Proposition 1: The full diversity is achieved when θ_n for $0 \le n \le P-1$ are free over the ring $\mathbb{Z}[e^{j2\pi/\,\mathrm{lcm}(A,P)}]$.

A canonical choice of θ_n is to set $\theta_n = \phi^n$ where $|\phi| = 1$ is the design parameter. Then (16) becomes

$$\lambda_k(\mathbf{E}) = \sum_{n=0}^{P-1} \phi^n e_n e^{-j2\pi kn/P}, \quad 0 \le k \le P-1 \tag{18}$$

which can be regarded as polynomials in the variable ϕ. The highest order of these polynomials is $P-1$, corresponding to the case when $e_{P-1} \neq 0$. This interpretation establishes a natural connection with field extensions.

Theorem 2: The full diversity is achieved when ϕ is a primitive m-th root of unity where m satisfies

$$\varphi(m) \ge \varphi\big(\gcd(m, \mathrm{lcm}(A,P))\big)P. \tag{19}$$

In particular, if m is coprime to both A and P, then (19) simplifies to

$$\varphi(m) \ge P, \tag{20}$$

which further simplifies to

$$m \ge P+1 \tag{21}$$

provided that m is prime. Note that all primitive m-th roots of unity are given by $e^{j2\pi k/m}$ where $\gcd(k,m) = 1$.

Proof: The polynomial coefficients in (18) belong to $\mathbb{Q}_{\mathrm{lcm}(A,P)}$. The full diversity condition will force ϕ to satisfy none of polynomials in $\mathbb{Q}_{\mathrm{lcm}(A,P)}[X]$ with degree less than P. This is equivalent to

$$\deg \min_{\mathbb{Q}_{\mathrm{lcm}(A,P)}}(\phi) = |\mathbb{Q}_{\mathrm{lcm}(A,P)}[\phi] : \mathbb{Q}_{\mathrm{lcm}(A,P)}| \ge P.$$

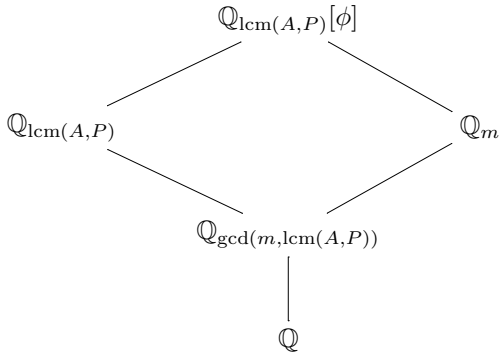
Since ϕ is a primitive m-th root of unity, one has $\mathbb{Q}[\phi] = \mathbb{Q}_m$. It follows from Theorem 1 that

$$\mathbb{Q}_{\mathrm{lcm}(A,P)} \cap \mathbb{Q}_m = \mathbb{Q}_{gcd(m,\mathrm{lcm}(A,P))}.$$

Furthermore, it is obvious to see that

$$\langle \mathbb{Q}_m, \mathbb{Q}_{\mathrm{lcm}(A,P)} \rangle = \mathbb{Q}_{\mathrm{lcm}(A,P)}[\phi].$$

Consider the following field extensions (read from bottom to top):



Since $\mathbb{Q}_m$ is Galois over $\mathbb{Q}$, it follows from the theorem of Natural irrationalities [14, Theorem 18.22] that

$$\begin{aligned} |\mathbb{Q}_{\mathrm{lcm}(A,P)}[\phi] : \mathbb{Q}_{\mathrm{lcm}(A,P)}| &= |\mathbb{Q}_m : \mathbb{Q}_{\gcd(m,\mathrm{lcm}(A,P))}| \\ &= \frac{\varphi(m)}{\varphi(\gcd(m, \mathrm{lcm}(A,P)))} \\ &\ge P \end{aligned}$$

which proves (19). If m is coprime to both A and P, then $\gcd(m, \mathrm{lcm}(A,P)) = 1$ and hence (20) follows. □

Table I lists the values of m for various combinations of dimension P and signal constellations.

TABLE I
VALUES OF m THAT SATISFY THEOREM 2

P	A	$m \le 10$
2	8 (8-PSK)	3, 5, 6, 7, 9, 10
	4 (QAM)	3, 5, 6, 7, 8, 9, 10
4	8 (8-PSK)	5, 7, 9, 10
	4 (QAM)	5, 7, 9, 10

C. Coding Gain Analysis

We will focus on the $P \times P$ case where the eigenvalues of the error codeword matrix are given in (18). The coding parameter ϕ is chosen according to Theorem 2 so that full

diversity is guaranteed. Hence, the coding gain associated with the algebraic number precoding is given by

$$\eta = \min_{\mathbf{E}\neq\mathbf{0}} \left(\prod_{k=0}^{P-1} |\lambda_k(\mathbf{E})| \right)^{2/P} \tag{22}$$

where the minimization is over all nonzero error codeword matrices. Note that $\lambda_k(\mathbf{E}\mathbf{E}^\dagger) = |\lambda_k(\mathbf{E})|^2$ is used in the derivation of (22).

In view of the code construction, one legitimate error pattern is that $e_0 \neq 0$ but $e_n = 0$ for $1 \leq n \leq P-1$, in which case (18) becomes $\lambda_k(\mathbf{E}) = e_0$ for $0 \leq k \leq P-1$. Therefore, the coding gain η is upper bounded by

$$\eta \leq d^2_{\min} \tag{23}$$

where $d_{\min}$ is the minimum distance of the signal constellation.

Lower bounds for the coding gain are, in contrast with upper bounds, elusive to obtain for general values of P due to the presence of higher order terms in (18). But lower bounds are arguably more important to code optimization because they provide a measure for guaranteed performance—error probability of the codes will be smaller than the one corresponding to the lower bounds. Fortunately, exploiting the algebraic structure of underlining signal constellation can lead to such an analysis on lower bounds for $P = 2$, that is, 2 transmit antennas, as we next elaborate.

When $P = 2$, the eigenvalue expression (18) specializes to

$$\lambda_k(\mathbf{E}) = e_0 + \phi e_1(-1)^k, \quad 0 \leq k \leq 1, \tag{24}$$

and hence the coding gain can be expressed as

$$\begin{aligned} \eta &= \min_{(e_0,e_1)\neq(0,0)} |e_0^2 - \phi e_1^2| \\ &= \min\{\min_{e_1=0} |e_0^2 - \phi e_1^2|, \min_{e_1\neq 0} |e_0^2 - \phi e_1^2|\} \\ &= \min\{d^2_{\min}, \eta_1\} \end{aligned} \tag{25}$$

where

$$\begin{aligned} \eta_1 &= \min_{e_1\neq 0} |e_0^2 - \phi^2 e_1^2| \\ &= \min_{e_1\neq 0} |e_1^2| \Big| \phi^2 - \frac{e_0^2}{e_1^2} \Big| \\ &\geq d^2_{\min} \min_{e_1\neq 0} \Big| \phi^2 - \frac{e_0^2}{e_1^2} \Big| \end{aligned} \tag{26}$$

since $|e_1|^2 \geq d^2_{\min}$ for nonzero e_1.

Let $\mathcal{D}$ denote the signal constellation (with finite number of signal points). Let $\mathcal{A}$ be the differences among signal points. The algebraic structure of the signal constellation gives $\mathcal{D} \subset \mathbb{Q}_A$ where A is determined by the minimal phase rotation in the constellation. Since $\frac{e_0^2}{e_1^2}$ only involves field operations, the finite set

$$\mathcal{B} := \Big\{ \frac{e_0^2}{e_1^2} : e_0 \in \mathcal{A}, e_1 \in \mathcal{A}, e_1 \neq 0 \Big\} \tag{27}$$

is still contained in $\mathbb{Q}_A$, that is, $\mathcal{B} \subset \mathbb{Q}_A$.

Our lower bound rests upon a result in [17] regarding approximation by algebraic numbers. Following the notations of [17], we will denote by $H(\beta)$ (*height* of β) the maximum modulus of the coefficients of the minimal polynomial of β over $\mathbb{Q}$ where β is an algebraic number. Further, let $q(\beta)$ be the smallest positive integer such that $q(\beta)\beta$ is an algebraic integer.

Theorem 3 (Lemma 9.1 in [17]): If θ is an algebraic number of degree $n \geq 3$, $k \in \mathbb{N}$ and $\alpha \neq \theta$ is algebraic of degree at most k, then

$$\begin{aligned} |\theta - \alpha| \geq k^{-2}(k+1)^{1-n} q(\theta)^{-kn} (1+|\theta|)^{1-k} \\ \cdot (1 + H(\theta))^{k(1-n)} H(\alpha)^{-n}. \end{aligned} \tag{28}$$

We now specialize the above theorem to the case of $|\phi^2 - b|$ where $b \in \mathcal{B}$ and ϕ is an m-th primitive root of unit. Since ϕ^2 is an algebraic integer, one has $q(\phi^2) = 1$. However, ϕ^2 is now a primitive $m/gcd(m,2)$-th root of unit. The degree of elements in $\mathbb{Q}_A$ is at most $\varphi(A)$. Therefore, a lower bound for the coding gain is given as the following.

Theorem 4: Let $\mathcal{D} \subset \mathbb{Q}_A$ be the signal constellation and ϕ be a primitive m-th root of unity satisfying Theorem 2. Denote by B the maximal height of elements in $\mathcal{B}$, that is, $B = \max_{b\in\mathcal{B}} H(b)$. One has

$$\eta \geq d^2_{\min} \min\{1, C\} \tag{29}$$

where

$$C = k^{-2}(k+1)^{1-n} 2^{1-k} (1 + H(\phi^2))^{k(1-n)} B \tag{30}$$

where $k = \varphi(A)$ and $n = \varphi(m/gcd(m,2))$ is assumed to be no less than 3.

Since ϕ^2 is a root of unity, its minimal polynomial over $\mathbb{Q}$ is related to the so-called *cyclotomic polynomial*.

Definition 6: The n-th cyclotomic polynomial, denoted by $\Phi_n(X)$, is the monic polynomial in $\mathbb{C}[X]$ whose roots are precisely the primitive n-th roots of unity. In other words,

$$\Phi_n(X) = \prod_{0\leq k<n,\ gcd(k,n)=1} (X - e^{2\pi j k/n}). \tag{31}$$

The fact that $\Phi_n(X)$ is the minimal polynomial of a primitive n-th root of unity is established by the following [14].

Theorem 5 (Gauss): The cyclotomic polynomial $\Phi_n(X)$ is irreducible in $\mathbb{Q}[X]$ for all integers $n \geq 1$.

The computation of $H(\phi^2)$ can be greatly simplified by the fact that all of the non-vanishing coefficients of $\Phi_n(X)$ are ± 1 for $n \leq 104$ [14]. Therefore, if $\frac{m}{gcd(m,2)} \leq 104$, then $H(\phi^2) = 1$, in which case, the constant C in Theorem 4 reduces to

$$C = k^{-2}(k+1)^{1-n} 2^{1-kn} B. \tag{32}$$

V. Discussions and Numerical Results

A. Efficient Linear Decoding Algorithm

For the maximum diversity case ($L = P$) the DFT eigen-decomposition (9) facilitates efficient decoding of the proposed cyclic extension of spatial multiplexing. Right-multiplying the received signal by $\mathbf{A}_T$, the DFT matrix, one can rewrite the channel equation (1) as

$$\begin{aligned} \tilde{\mathbf{Y}} &= \mathbf{Y}\mathbf{A}_T \\ &= \sqrt{\rho}\mathbf{H}\mathbf{A}_T\mathbf{S}\mathbf{A}_T^\dagger\mathbf{A}_T + \mathbf{N}\mathbf{A}_T \\ &= \sqrt{\rho}\tilde{\mathbf{H}}\mathbf{S} + \tilde{\mathbf{N}} \end{aligned} \tag{33}$$

where $\tilde{\mathbf{H}} = \mathbf{H}\mathbf{A}_T$ and $\tilde{\mathbf{N}} = \mathbf{N}\mathbf{A}_T$. Since $\mathbf{S}$ is a diagonal matrix, the above equation can be further simplified as

$$\tilde{\mathbf{y}} = \begin{bmatrix} \tilde{\mathbf{y}}_0 \\ \vdots \\ \tilde{\mathbf{y}}_{P-1} \end{bmatrix} = \sqrt{\rho} \begin{bmatrix} \tilde{\mathbf{h}}_0 & & \\ & \ddots & \\ & & \tilde{\mathbf{h}}_{P-1} \end{bmatrix} \begin{bmatrix} s_0 \\ \vdots \\ s_{P-1} \end{bmatrix} + \begin{bmatrix} \tilde{\mathbf{n}}_0 \\ \vdots \\ \tilde{\mathbf{n}}_{P-1} \end{bmatrix} = \sqrt{\rho}\mathbf{M}\mathbf{s} + \tilde{\mathbf{n}} \tag{34}$$

where $\tilde{\mathbf{y}}_i$, $0 \le i \le P-1$, is the i-th column of matrix $\tilde{\mathbf{Y}}$ and the similar notations for $\tilde{\mathbf{h}}_i$ and $\tilde{\mathbf{n}}_i$. Substituting (11) into the above equation, one has

$$\tilde{\mathbf{y}} = \sqrt{\rho}\mathbf{M}\mathbf{A}_T^{\dagger}\mathbf{D}\mathbf{x} + \tilde{\mathbf{n}} \tag{35}$$

where $\mathbf{x} = (x_0, \ldots, x_{P-1})^T$ is the multiplexing symbols. Regarding x_k's as user symbols, (35) can be viewed as a multiple access channel, from which zero-forcing (ZF) and minimum mean squares error (MMSE) linear receiver can be derived. In other words, we design linear filter $\mathbf{F}$ so that $\mathbf{F}\tilde{\mathbf{y}}$ approximates the transmit symbol vector $\mathbf{x}$.

For the ZF solution, the filter $\mathbf{F}$ is essentially the channel inverse

$$\mathbf{F} = (\sqrt{\rho})^{-1}\mathbf{D}^{-1}\mathbf{A}_T(\mathbf{M}^{\dagger}\mathbf{M})^{-1}\mathbf{M}^{\dagger}. \tag{36}$$

Thanks to the block-diagonal matrix $\mathbf{M}$ one has

$$\mathbf{M}^{\dagger}\mathbf{M} = \mathrm{diag}(\|\tilde{\mathbf{h}}_0\|^2, \cdots, \|\tilde{\mathbf{h}}_{P-1}\|^2). \tag{37}$$

Since $\mathbf{D}$ is also diagonal, the computation of the filter coefficient matrix $\mathbf{F}$ involves only *scalar* inversion, which can significantly reduce system complexity. Moreover, inversion is carried out with respect to the norm of random channel vector $\|\tilde{\mathbf{h}}_k\|^2$, which provides high level of diversity to combat channel fading.

The MMSE solution is given by

$$\mathbf{F} = (\rho\mathbf{D}^{\dagger}\mathbf{A}_T\mathbf{M}^{\dagger}\mathbf{M}\mathbf{A}_T^{\dagger}\mathbf{D} + \mathbf{I})^{-1}\sqrt{\rho}\mathbf{D}^{\dagger}\mathbf{A}_T\mathbf{M}^{\dagger}. \tag{38}$$

Since the unitary $\mathbf{D}$ is diagonal and $\mathbf{M}^{\dagger}\mathbf{M}$ is diagonal by (37), the MMSE filter is simplified as

$$\mathbf{F} = \mathbf{D}^{-1}\mathbf{A}_T\,\mathrm{diag}(\rho\|\tilde{\mathbf{h}}_0\|^2+1, \cdots, \rho\|\tilde{\mathbf{h}}_{P-1}\|^2+1)^{-1}\sqrt{\rho}\mathbf{M}^{\dagger}. \tag{39}$$

Similar to the ZF receiver, the MMSE receiver eliminates the matrix inversion and exploits channel diversity. Furthermore, it accounts for both signal and noise strength and avoids the problem of noise amplification in the ZF receiver in the low-SNR regime.

B. Rate Diversity Tradeoff

In Section IV, we focus on the case $L = P$ to construct full rank error codeword matrices to achieve the maximum diversity (P). However, the code has the smallest multiplexing rate of 1 symbol per channel use due to its large block length.

Higher rates can be obtained by decreasing the code block length L. This can be seen as truncation of the maximum diversity code by taking the first L columns of the $P \times P$ codewords constructed in Section IV. The truncated code retains L level of transmit diversity because its pairwise error matrix, as a submatrix of its corresponding error matrix of the original full-rank, full-sized ($P \times P$) code, is also full rank. The rate of this code is P/L symbol/channel use and the diversity advantage is L. On the other hand, since the $P \times L$ codewords are no longer square circular matrices, we cannot directly apply the efficient decoding algorithms developed for the $L = P$ case in V-A.

TABLE II

CODING GAINS FOR DIFFERENT CHOICES OF m, $P = 2, 4$, QPSK CONSTELLATION

m	3	5	6	7	8	9	10
$\eta(P=2)$	2	2	2	2	2	2	2
$\eta(P=4)$	-	1.4725	-	1.6167	-	1.1315	1.4725

TABLE III

CODING GAIN COMPARISON FOR DIFFERENT P, QPSK

P	O-STBC	DAST	Proposed Codes
2	2	$2/\sqrt{5}$	2
4	2^1	$\sqrt{2/5}$	1.6167

[1] This orthogonal code only has rate 3/4 symbol/channel use.

C. Code Examples and Numerical Results

We focus on the case $L = P$ and QPSK constellation for systems with $P = 2, 4$ transmit antennas. As stated in Theorem 2, that full diversity is achieved when we choose the algebraic number ϕ to be an m-th primitive root of unitary. As seen in Table I, there are many different values of m satisfying Theorem 2. Furthermore, there are also several primitive m-th roots of unity given by $e^{j2\pi k/m}$ for each value of m, where $\gcd(k, m) = 1$. However, we can simply pick m and k such that the coding gain given in (22) is maximized. The coding gains for different number of m are illustrated in Table II, where the values of m are given in Table I.

In Table II, only the maximum coding gain for each value of m is shown. For example, for $P = 2$, $m = 3$, $e^{j2\pi/3}$ and $e^{j4\pi/3}$ are all primitive roots of unity. They yield the same coding gains. Therefore, we can arbitrarily choose $\phi = e^{j2\pi/3}$. The precoding matrices for this example are

$$\mathbf{W}_0 = \begin{bmatrix} 1 & 0 \\ 0 & e^{j2\pi/3} \end{bmatrix}, \ \mathbf{W}_1 = \begin{bmatrix} 0 & e^{j2\pi/3} \\ 1 & 0 \end{bmatrix}. \tag{40}$$

In Table III, we list the coding gains of our codes with comparison to orthogonal STBC and DAST. For $P = 2$, all three codes have the same rate, our codes achieve the same coding gain as orthogonal STBC. For $P = 4$, DAST and the proposed codes achieve rate 1 symbol/channel use, while orthogonal STBC only has rate $3/4$ symbol/channel use. It is easy to see that the proposed codes have coding gain advantage over DAST in both cases. Note that the coding gain 1.6167 for $P = 4$ is the largest for $m = \{5, 7, 9, 10\}$, but it may be further increased through a larger search space.

In Fig. 2-4, we plot the performance of the proposed codes for systems with $P = 4$ antennas and different number of receive antennas. We also plot the performance of DAST with maximum likelihood (ML) decoding for comparison. In all figures, the proposed codes outperform the DAST due to the improvement in coding gains. As the number of receive

antennas increases, the gap between the ML decoding and suboptimal decodings decreases. For $P = Q = 4$, MMSE and ZF decodings have comparable performance.

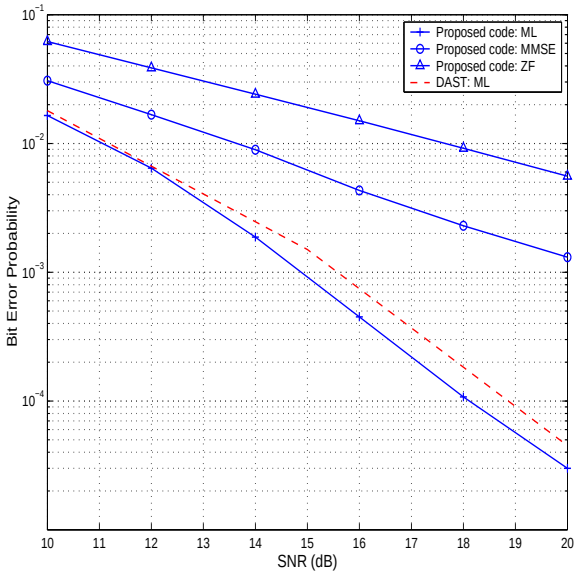


Fig. 2. Performance comparison between proposed code and DAST, $P = 4$, $Q = 1$, $R = 2$ bps/Hz.

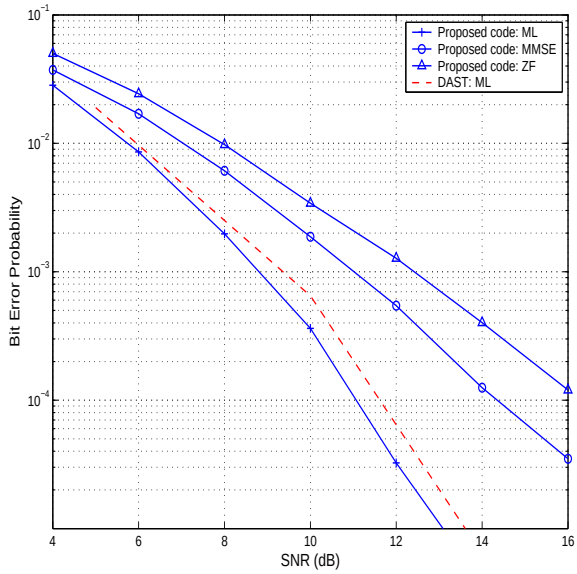


Fig. 3. Performance comparison between proposed code and DAST, $P = 4$, $Q = 2$, $R = 2$ bps/Hz.

VI. Conclusions

We have proposed a space-time block coding framework based on a set of L precoding matrices. It can be regarded as a cyclic extension of the conventional spatial multiplexing. Full diversity is achieved through an algebraic design of the precoding matrices based on cyclotomic numbers. The coding scheme provides a tradeoff between L-fold diversity and P/L multiplexing rate. The cyclic structure of the code is especially simple to implement at the transmitter, whereas there exist low complexity decoding algorithms for the $L = P$ case.

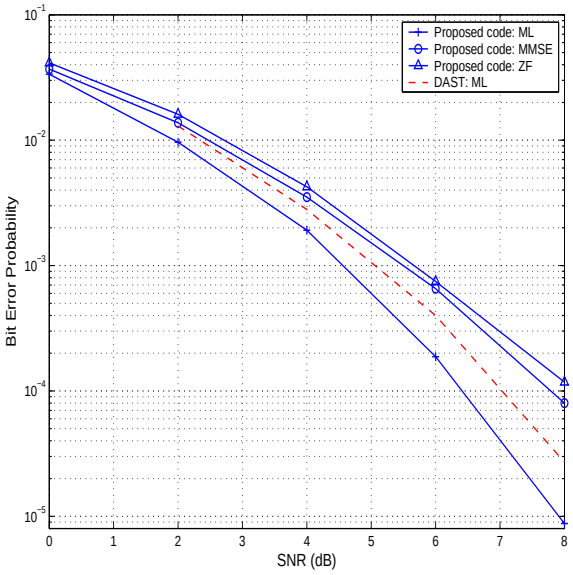


Fig. 4. Performance comparison between proposed code and DAST, $P = 4$, $Q = 4$, $R = 2$ bps/Hz.

Spatial multiplexing with precoding [12] designed for correlated fading can be considered as a special case of the proposed codes in this paper. We believe that with the flexibility of our code design, one can further match the codes to the correlated channel to exploit the available diversity gain and maintain the rate advantage over orthogonal STBCs.

References

[1] V. Tarokh, N. Seshadri, and A. R. Calderbank, "Space-time codes for high data rate wireless communication: Performance criterion and code construction," *IEEE Trans Inform. Theory*, vol. 44, no. 2, pp. 744–765, March 1998.

[2] V. Tarokh, H. Jafarkhani, and A. R. Calderbank, "Space-time block codes from orthogonal designs," *IEEE Trans. Inform. Theory*, vol. 45, no. 5, pp. 1456–1467, July 1999.

[3] S. M. Alamouti, "A simple transmit diversity technique for wireless communications," *IEEE J. Select. Areas in Commun.*, vol. 16, no. 8, pp. 1451–1458, Oct. 1998.

[4] G. J. Foschini, "Layered space-time architecture for wireless communication in a fading environment when using multiple antennas," *Bell Labs Technical Journal*, vol. 1, no. 2, pp. 41–59, 1996.

[5] B. Hassibi and B. M. Hochwald, "High-rate codes that are linear in space and time," *IEEE Trans. Inform. Theory*, vol. 48, no. 7, pp. 1804–1824, July 2002.

[6] A. Paulraj and T. Kailath, "U.S. Patent #5345599: Increasing capacity in wireless broadcast systems using distributed transmission/directional reception (DTDR)," Sept. 1994.

[7] L. Zheng and D. N. C. Tse, "Diversity and multiplexing: a fundamental tradeoff in multiple-antenna channels," *IEEE Trans. Inform. Theory*, vol. 49, no. 5, pp. 1073–1096, May 2003.

[8] H. E. Gamal and M. O. Damen, "An algebraic number theoretic framework for space-time coding," in *IEEE International Symposium on Information Theory (ISIT'02)*, Lausanne, Switzerland, June 2002, p. 132.

[9] M. O. Damen, K. Abed-Meraim, and J.-C. Belfiore, "Diagonal algebraic space-time block codes," *IEEE Trans. Inform. Theory*, vol. 48, pp. 628–636, Mar. 2002.

[10] H. E. Gamal and M. O. Damen, "Universal space-time coding," *IEEE Trans. Inform. Theory*, vol. 49, no. 5, pp. 1097–1119, May 2003.

[11] F. Oggier, G. Rekaya, J.-L. Belfiore, and E. Viterbo, "Perfect space-time block codes," *IEEE Trans. Inform. Theory*, vol. 52, no. 9, pp. 3885–3902, Sept. 2006.
[12] Z. Hong, K. Liu, J. R. W. Heath, and A. M. Sayeed, "Spatial multiplexing in correlated fading via the virtual channel representation," *IEEE Journal on Select. Areas in Commun.*, vol. 21, no. 5, pp. 856–866, June 2003.
[13] J. Boutros and E. Viterbo, "Signal space diversity: a power- and bandwidth-efficient diversity technique for the Rayleigh fading channel," *IEEE Trans. Inform. Theory*, vol. 44, pp. 1453–1467, July 1998.
[14] I. M. Issacs, *Algebra, a Graduate Course*. Pacific Grove, Calif.: Brooks/Cole Pub. Co., 1994.
[15] I. Stewart and D. Tall, *Algebraic Number Theory and Fermat's Last Theorem*. Natick, Mass.: AK Peters, 2002.
[16] S. Lang, *Algebraic Number Theory*. New York: Springer-Verlag, 1986.
[17] M. A. Bennett, "Rational approximation to algebraic numbers of small height: the Diophantine equation $|ax^n - by^n| = 1$," *J. Reine Angew. Math*, vol. 535, pp. 1–49, 2001.

Zhihong Hong received the B.S. degree from Tsinghua University, Beijing, China, in 1994, and the M.S. and Ph.D. degrees, in 1998 and 2002, respectively, from North Carolina State University, Raleigh, all in electrical engineering. From 1999 to 2002, he was a Research Assistant at the Center for Advanced Computing and Communication (CACC), North Carolina State University. From 2002 to 2003, he was with the University of Wisconsin at Madison, as a Postdoctoral Research Associate. Since August 2003, he has been with Communications Research Centre Canada (CRC) as a research scientist. His research interests include advanced coding and modulation in wireless communications, channel estimation and Doppler mitigation for OFDM systems.

Ke Liu (S'99-M'05) received his B.S. degree (1999) in Electrical Engineering from Tsinghua University, Beijing, China, and the M.S. degree (2001) in Electrical Engineering, the M.A. degree (2002) in Mathematics, and the Ph.D. degree (2004) in Electrical Engineering, all from the University of Wisconsin at Madison, USA.

From 2000-2004, he was a research assistant in the Wireless Communications Laboratory at the University of Wisconsin-Madison. He was a postdoctoral researcher at the Ohio State University (2004-2005). Since 2005 he has been with Qualcomm Inc., working on the next generation wireless systems. His current research interests include wireless communications, wireless networks, information theory, and signal processing.

Dr. Liu received Graduate School Fellowship from 1999 to 2000 and was awarded the Harold A. Peterson Graduate Student Paper Award for his work on space-time coding for multi-antenna systems. He served as reviewer for IEEE communications, signal processing and information theory society.

Nigel Boston received his B.A. from Cambridge University in 1982 and his Ph.D. from Harvard University in 1987, both in mathematics. He holds a split appointment in the Departments of Mathematics and Electrical and Computer Engineering at the University of Wisconsin-Madison. He is currently on leave from Wisconsin and is Stokes Professor of Pure and Applied Algebra at University College Dublin, Ireland.

Akbar M. Sayeed (S'89-M'97-SM'02) is currently Professor of Electrical and Computer Engineering at the University of Wisconsin-Madison. He received the B.S. degree from the University of Wisconsin-Madison in 1991, and the M.S. and Ph.D. degrees from the University of Illinois at Urbana-Champaign in 1993 and 1996, all in Electrical Engineering. He was a postdoctoral fellow at Rice University from 1996 to 1997. His current research interests include wireless communications, statistical signal processing, multi-dimensional communication theory, information theory, learning theory, time-frequency analysis, and applications in wireless communication networks and sensor networks. Dr. Sayeed is a recipient of the Robert T. Chien Memorial Award (1996) for his doctoral work at Illinois, the NSF CAREER Award (1999), the ONR Young Investigator Award (2001), and the UW Grainger Junior Faculty Fellowship (2003). He is a Senior Member of the IEEE and is currently serving on the signal processing for communications technical committee of the IEEE Signal Processing Society. Dr. Sayeed also served as an Associate Editor for the IEEE Signal Processing Letters from 1999-2002, and as the technical program co-chair for the 2007 IEEE Statistical Signal Processing Workshop and the 2008 IEEE Communication Theory Workshop.