[8] N. R. Goodman, "Statistical analysis based on a certain multivariate complex Gaussian distribution (An introduction)," *Ann. Math. Statist.*, vol. 34, pp. 152–177, 1963.

[9] A. Gupta and D. Nagar, *Matrix Variate Distributions*. New York: Chapman & Hall, 2000.

[10] B. M. Hochwald, T. L. Marzetta, and V. Tarokh, "Multiple-antenna channel-hardening and its implications for rate feedback and scheduling," *IEEE Trans. Inf. Theory*, vol. 50, no. 9, pp. 1893–1909, Sep. 2004.

[11] A. T. James, "Distributions of matrix variate and latent roots derived from normal samples," *Ann. Math. Statist.*, vol. 35, pp. 475–501, 1964.

[12] C. G. Khatri, "On certain distribution problems based on positive definite quadratic functions in normal vectors," *Ann. Math. Statist.*, vol. 37, pp. 468–479, 1966.

[13] ——, "Non-central distributions of ith largest characteristic roots of three matrices concerning complex multivariate normal populations," *Ann. Inst. Statist. Math.*, vol. 21, pp. 23–32, 1969.

[14] M. Kiessling and J. Speidel, "Exact ergodic capacity of MIMO channels in correlated Rayleigh fading environments," in *Proc. Int. Zurich Seminar on Communication*, Zurich, Switzerland, Feb. 2004, pp. 128–131.

[15] I. G. Macdonald, *Symmetric Functions and Hall Polynomials*. New York: Oxford Univ. Press, 1995.

[16] R. K. Mallik, "The pseudo-Wishart distribution and its application to MIMO systems," *IEEE Trans. Inf. Theory*, vol. 49, no. 10, pp. 2761–2769, Oct. 2003.

[17] R. J. Muirhead, *Aspects of Multivariate Statistical Theory*. New York: Wiley, 1982.

[18] T. Ratnarajah, R. Vaillancourt, and M. Alvo, "Complex random matrices and Rayleigh channel capacity," *Commun. Inf. Syst.*, vol. 3, no. 2, pp. 119–138, Oct. 2003.

[19] T. Ratnarajah and R. Vaillancourt, "Complex singular Wishart matrices and applications," *Comp. Math. Applic.*, to be published.

[20] ——, "Quadratic forms on complex random matrices and multiple-antenna channel capacity," in *Proc. 12th Annu. Workshop Adaptive Sensor Array Processing*, MIT Lincoln Labs., Lexingtin, MA, Mar. 2004.

[21] ——, "Quadratic forms on complex random matrices and channel capacity," in *Proc. IEEE Int. Conf. Acoustics, Speech, and Signal Processing*, vol. 4, Montreal, QC, Canada, May 17–21, 2004, pp. 385–388.

[22] T. Ratnarajah, R. Vaillancourt, and M. Alvo, "Eigenvalues and condition numbers of complex random matrices," *SIAM J. Matrix Anal. Applic.*, vol. 26, no. 2, pp. 441–456, Jan. 2005.

[23] ——, "Complex random matrices and Rician channel capacity," *Probl. Inform. Transm.*, vol. 41, no. 1, pp. 1–22, Jan. 2005.

[24] M. Sellathurai and G. Foschini, "A stratified diagonal layered space-time architecture: Information theoretic and signal processing aspects," *IEEE Trans Signal Process.*, vol. 51, no. 11, pp. 2943–2954, Nov. 2003.

[25] H. Shin and J. H. Lee, "Capacity of multiple-antenna fading channels: Spatial fading correlation, double scattering, and keyhole," *IEEE Trans. Inf. Theory*, vol. 49, no. 10, pp. 2636–2647, Oct. 2003.

[26] D. S. Shiu, G. F. Foschini, M. G. Gans, and J. M. Kahn, "Fading correlation and its effect on the capacity of multielement antenna systems," *IEEE Trans. Commun.*, vol. 48, no. 3, pp. 502–513, Mar. 2000.

[27] S. H. Simon and A. L. Moustakas, "Eigenvalue density of correlated complex random Wishart matrices," *Phys. Rev.*, vol. E 69 065101(R), 2004.

[28] İ. E. Telatar, "Capacity of multi-antenna Gaussian channels," *Europ. Trans. Telecommun.*, vol. 10, pp. 585–595, 1999.

STBC-Schemes With Nonvanishing Determinant for Certain Number of Transmit Antennas

Kiran T., *Student Member, IEEE,* and
B. Sundar Rajan, *Senior Member, IEEE*

***Abstract*—A space–time block-code scheme (STBC-scheme) is a family of STBCs $\{\mathcal{C}(\mathrm{SNR})\}$, indexed by the signal-to-noise ratio (SNR) such that the rate of each STBC scales with SNR. An STBC-scheme is said to have a *nonvanishing determinant* if the coding gain of every STBC in the scheme is lower-bounded by a fixed nonzero value. The nonvanishing determinant property is important from the perspective of the diversity multiplexing– gain (DM-G) tradeoff: a concept that characterizes the maximum diversity gain achievable by any STBC-scheme transmitting at a particular rate. This correspondence presents a systematic technique for constructing STBC-schemes with nonvanishing determinant, based on cyclic division algebras. Prior constructions of STBC-schemes from cyclic division algebra have either used transcendental elements, in which case the scheme may have vanishing determinant, or is available with nonvanishing determinant only for two, three, four, and six transmit antennas. In this correspondence, we construct STBC-schemes with nonvanishing determinant for the number of transmit antennas of the form $2^k, 3 \cdot 2^k, 2 \cdot 3^k$, and $q^k(q-1)/2$, where q is any prime of the form $4s+3$.**

For cyclic division algebra based STBC-schemes, in a recent work by Elia *et al.*, the nonvanishing determinant property has been shown to be sufficient for achieving DM-G tradeoff. In particular, it has been shown that the class of STBC-schemes constructed in this correspondence achieve the optimal DM-G tradeoff. Moreover, the results presented in this correspondence have been used for constructing optimal STBC-schemes for arbitrary number of transmit antennas, by Elia *et al.*.

***Index Terms*—Cyclic division algebra, diversity-multiplexing gain (DM-G) tradeoff, multiple-input multiple-output (MIMO) channel, nonvanishing determinant, number field, space–time block code (STBC), STBC-scheme.**

I. Introduction and Mathematical Preliminaries

A quasi-static Rayleigh-fading multiple-input multiple-output (MIMO) channel with n_t transmit and n_r receive antennas is modeled as

$$\boldsymbol{Y}_{n_r \times l} = \boldsymbol{H}_{n_r \times n_t} \boldsymbol{X}_{n_t \times l} + \boldsymbol{W}_{n_r \times l}$$

where $\boldsymbol{Y}_{n_r \times l}$ is the received matrix over l channel uses, $\boldsymbol{X}_{n_t \times l}$ is the transmitted matrix, $\boldsymbol{H}_{n_r \times n_t}$ is the channel matrix, and $\boldsymbol{W}_{n_r \times l}$ is the additive noise matrix, with the subscripts denoting the dimension of the matrices. The matrices $\boldsymbol{H}_{n_r \times n_t}$ and $\boldsymbol{W}_{n_r \times l}$ have entries which are independent and identically distributed (i.i.d.), complex circularly symmetric Gaussian random variables. The collection of all possible transmit codewords $\boldsymbol{X}_{n_t \times l}$ forms a space–time block code (STBC).

While most of the initial STBC constructions in the literature concentrated either on codes with maximum diversity alone [1]–[10], or on

Manuscript received August 7, 2004; revised January 24, 2005. This work was supported through grants to B.S. Rajan; in part by the IISc-DRDO program on Advanced Research in Mathematical Engineering, and in part by the Council of Scientific and Industrial Research (CSIR, India) under Research Grant (22(0365)/04/EMR-II). A part of the material in this correspondence was accepted for presentation at the IEEE International Symposium on Information Theory (ISIT 2005) to be held in Adelaide, Australia, September 4–9, 2005.

The authors are with the Department of Electrical Communication Engineering, Indian Institute of Science, Bangalore 560012, India (e-mail: kirant@ece.iisc.ernet.in; bsrajan@ece.iisc.ernet.in).

Communicated by R. R. Müller, Associate Editor for Communications.
Digital Object Identifier 10.1109/TIT.2005.851772

codes with maximum possible data rate alone [11], [12], the work by Zheng and Tse [13] shows that both diversity as well as data rate can be simultaneously achieved, albeit with a tradeoff between them. An optimal diversity multiplexing–gain tradeoff (DM-G) curve for the richly scattered Rayleigh-fading quasi-static MIMO channel is presented, which can be used to evaluate the performance of any coding scheme. To be more precise, if $p_{\rm out}(R)$ denotes the outage probability of the MIMO channel at a rate R bits/s/Hz, then the DM-G tradeoff of a MIMO quasi-static Rayleigh fading channel is the curve $(r, d^*(r))$, where

$$d^*(r) = -\lim_{\mathsf{SNR}\to\infty} \frac{\log p_{\rm out}(R)}{\log \mathsf{SNR}}$$

is the maximum *diversity gain* achievable at a rate $R = r \log \mathsf{SNR}$. The normalized rate of transmission r is called the *multiplexing gain*. When $l \geq n_t + n_r - 1$, the optimal DM-G tradeoff curve is $d^*(r) = (n_t - r)(n_r - r)$ at integral values of r; with the $d^*(r)$ at nonintegral intermediate values of r being obtained by linear interpolation through the integral ones. For the case $l < n_t + n_r - 1$, the optimal DM-G tradeoff is not known and it is only shown that $d^*(r) \leq (n_t - r)(n_r - r)$, an upper bound for the optimal DM-G curve.

In order to evaluate the performance of any code against the fundamental DM-G tradeoff of the channel, the rate of the code R must scale with signal-to-noise ratio (SNR). Therefore, the DM-G tradeoff performance is defined not for a single STBC, but for an *STBC-scheme*: a family of STBCs $\{\mathcal{C}(\mathsf{SNR})\}$, indexed by the SNR value such that the rate of $\mathcal{C}(\mathsf{SNR})$ which is denoted as $R(\mathsf{SNR})$, scales with SNR. An STBC-scheme is said to achieve a multiplexing gain r and a diversity gain d if

$$R(\mathsf{SNR}) = r \log \mathsf{SNR} \quad \text{and} \quad d = -\lim_{\mathsf{SNR}\to\infty} \frac{\log P_e(R)}{\log \mathsf{SNR}} \qquad (1)$$

where P_e denotes the probability of codeword error. An STBC-scheme is said to achieve the optimal DM-G tradeoff (or DM-G tradeoff optimal) if $(r, d) = (r, d^*(r))$ for all possible values of r.

Remark 1: From the pairwise error probability (PEP) point of view, it is well known [14] that the performance of a space–time code at high SNR is dependent on two parameters: *diversity gain* and *coding gain*. Diversity gain is the minimum of rank of the difference matrix $\left(\boldsymbol{X}_{n_t\times l} - \boldsymbol{X}'_{n_t\times l}\right)$, for any $\boldsymbol{X}_{n_t\times l} \neq \boldsymbol{X}'_{n_t\times l} \in \mathcal{C}$, also called the rank of code $\mathcal{C}$. When $\mathcal{C}$ is full rank, the coding gain is proportional to the determinant of $\left(\boldsymbol{X}_{n_t\times l} - \boldsymbol{X}'_{n_t\times l}\right)\left(\boldsymbol{X}_{n_t\times l} - \boldsymbol{X}'_{n_t\times l}\right)^H$.

Notice that the definition of diversity gain by Zheng and Tse deviates from the classical definition of diversity as the exponent of SNR in the PEP. Instead, it is defined as the exponent of SNR in the actual codeword error probability P_e. Further, the DM-G analysis being an asymptotic (in SNR) analysis, it captures only the exponent of SNR disregarding any constant multipliers. These constant multipliers which play a crucial role (analogous to the coding gain of PEP) when comparing the actual codeword error performance, have no role as far as DM-G tradeoff is considered. Thus, it is possible that two $n_t \times l$ STBC-schemes are both DM-G tradeoff optimal, yet differ in the actual codeword error performance. Our focus in this correspondence is only DM-G tradeoff and not the *true* codeword error performance.

Among the various methods of construction, codes from division algebra [9] and the threaded-algebraic space–time (TAST) codes [10] seem to be the only known systematic methods for constructing the full-rate, full-rank codes for arbitrary number of transmit antennas. Similar to the Alamouti code [1] which can be described by a 2×2 matrix with two complex variables and their conjugates, these codes can be described by a *design* which is defined as follows.

Definition 1: A rate-k/l, $n_t \times l$ *design* over a subfield $\mathbb{K}$ of the complex field $\mathbb{C}$, is an $n_t \times l$ matrix $\boldsymbol{M}(x_1, x_2, \ldots, x_k)$, with entries which are $\mathbb{K}$-linear combinations of x_i's and their conjugates. We call $\boldsymbol{M}(x_1, x_2, \ldots, x_k)$ a full-rank design over the field $\mathbb{F}$ if every finite subset of the set

$$E = \{\boldsymbol{M}(f_1, f_2, \ldots, f_k) \mid f_i \in \mathbb{F}\ \forall i\}$$

is a full-rank STBC. The design is said to have full rate if $k = n_t l$.

An STBC can be obtained from the design $\boldsymbol{M}(x_1, x_2, \ldots, x_k)$ by specifying a signal set $\mathcal{S} \subset \mathbb{F}$ from which the variables x_i draw values. If the design has full rate, then the STBC so obtained is said to be a full-rate code.

For codes that can be described using a design over $\mathbb{F}$, a simple way of building an STBC-scheme is to have a family of signal sets $\mathcal{S}(\mathsf{SNR}) \subset \mathbb{F}$ and then $\mathcal{C}(\mathsf{SNR})$ is obtained by allowing the variables in the design to draw values from the signal set $\mathcal{S}(\mathsf{SNR})$.

The work by Zheng and Tse has now opened up an important research problem, which is the construction of STBC-schemes that are optimal in the sense of achieving the optimal DM-G tradeoff [15]–[17]. In [18], the authors only prove **the existence** of lattice-based STBC-schemes that achieve optimal DM-G tradeoff for $l \geq n_t + n_r - 1$ and in [13] it is shown that the STBC-scheme based on the Alamouti code [1] is optimal for $n_r = 1$, but falls short of the optimal DM-G tradeoff for $n_r = 2$. For $n_t = n_r = l = 2$, there are two schemes that have been **proved to achieve** the optimal DM-G tradeoff: the tilted-QAM code [15] and the "Golden code" [19]. The proof for the former in [15] actually shows that the scheme achieves the upper bound of the optimal DM-G curve, thus proving that the upper bound given by Zheng and Tse (when $l < n_t + n_r - 1$) is the actual tradeoff curve for $n_t = n_r = l = 2$. The DM-G optimality of Golden code is proved in [20], where the authors give certain bounds on the achievable DM-G of few existing STBC-schemes, including the ones from cyclic division algebras for two, three, and four transmit antennas in [21]. In all these proofs, the authors make use of the fact that the coding gain of any of the codes $\mathcal{C}(\mathsf{SNR})$ in the scheme does not fall below a certain positive value i.e, there exists a value $d_{\min} \neq 0$ such that the coding gain of all the codes $\mathcal{C}(\mathsf{SNR})$ in the scheme is at least equal to $d_{\min}$. Schemes with this property are said to have a nonvanishing coding gain, and for schemes that are obtained using a design over $\mathbb{F}$, having a nonvanishing coding gain is equivalent to saying that the determinant of the design is always lower-bounded by $d_{\min}$, irrespective of the values that the variables draw from $\mathbb{F}$. In the rest of this correspondence, STBC-schemes from designs with this property are said to have a *nonvanishing determinant*.

In summary, the known results on the DM-G tradeoff imply that, for a $n_t = n_r = l = 2$ STBC-scheme employing M-QAM signal sets, having a symbol rate equal to 2 and a nonvanishing coding gain is **sufficient to achieve the** optimal DM-G tradeoff. For $n_t > 2$, such a result is not known. However, the results in [20] do indicate that STBC-schemes employing M-QAM signal sets, with symbol-rate equal to n_t and having the nonvanishing coding gain is **sufficient to achieve a part** of the optimal DM-G tradeoff curve. In particular, they achieve $(r, d^*(r))$ for r in the range $\min(n_t, n_r) - 1 \leq r \leq \min(n_t, n_r)$. This is the motivation for the constructions that will be presented in this correspondence. Our aim is to give a general technique for constructing STBC-schemes for $n_t \geq 2$, with nonvanishing coding gain and symbol rate equal to n_t. Recently, few codes with these properties have been constructed in [19], [21], [22], but the focus in these papers is only on improving the coding gain (and hence the true codeword error probability), and not on the DM-G tradeoff. The fact that these codes achieve part of the DM-G tradeoff is the result by Elia *et al.* in [20]. It seems to us that the technique used in [19], [22] is different from the one used in [21] (this will be made precise in a subsequent subsection). The construction in [21] is more in-line with [9], the only difference being the choice between an algebraic number in [21] against a transcendental number in [9]. While a transcendental number has been used for constructing cyclic division algebra of arbitrary degree in [9], the authors in

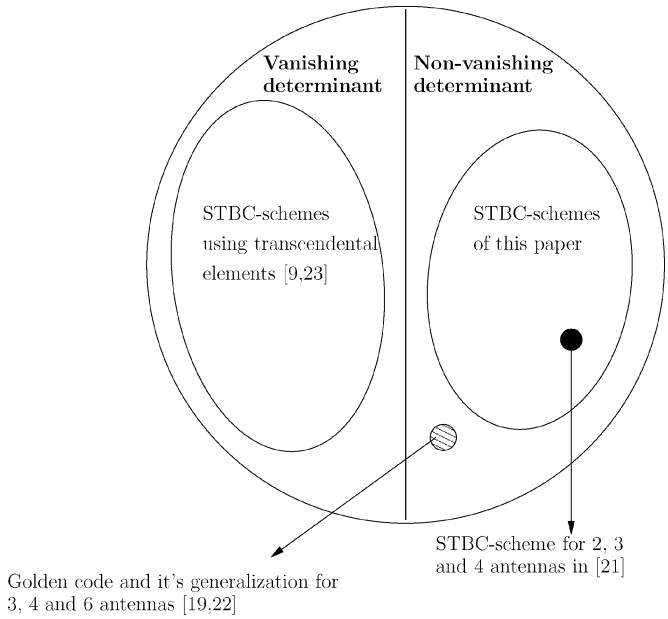

Fig. 1. STBC-schemes from cyclic division algebras.

[21] recognize that this may lead to a vanishing determinant code and hence propose to replace the transcendental element by an appropriate algebraic element without loosing the full-rank property. Although the authors of [21] discuss nonvanishing determinant codes from cyclic division algebra point of view, explicit code construction is only provided for few sporadic values of n_t (for two, three, and four transmit antennas) and a general construction technique for such codes is not available.

In this correspondence, by using an appropriate representation of a cyclic division algebra over a maximal subfield as a design, we construct STBC-schemes with nonvanishing determinant for the number of transmit antennas of the form 2^k or $3 \cdot 2^k$ or $2 \cdot 3^k$ or $q^k(q-1)/2$, where q is a prime of the form $4s+3$ and s is any arbitrary integer. In particular, we are able to construct STBC-schemes with nonvanishing determinant for $n = 2^k$ (resp., $n = 3^k$) transmit antennas, using the algebraic integer $2+i$ (resp., $3+\omega_3$) and a signal set family which is a collection of quadrature amplitude modulation (QAM) constellations (resp., a collection of finite subsets of the hexagonal lattice $\mathbb{Z}[\omega_3]$). Following the results of [20], all these codes achieve part of the optimal DM-G tradeoff corresponding to $\min(n_t, n_r) - 1 \le r \le \min(n_t, n_r)$. In Fig. 1, based on the vanishing/nonvanishing determinant property, we classify the various known STBC-scheme constructions from cyclic division algebra along with the STBC-schemes of this correspondence. The codes for two, three, and four transmit antennas constructed in [21] are obtained as a special case of our construction technique.

Remark 2 (Recent Results): After submitting this correspondence, there have been some important recent developments on codes achieving the optimal DM-G tradeoff [24], [25]. An extended analysis of the DM-G tradeoff is provided in [24], where it is proved that codes with nonvanishing coding gain achieve the optimal DM-G tradeoff. In [25], the authors have improved upon their previous results [20] and prove that nonvanishing determinant is a sufficient condition for full-rate STBC-schemes from cyclic division algebra to achieve the upper bound on optimal DM-G tradeoff; thus proving that the upper bound itself is the optimal DM-G tradeoff for any values of $n_t = l$ and n_r. In particular, it **has been shown that the class of STBC-schemes constructed in this correspondence for $n_t \in \{2^k, 2 \cdot 3^k, 2^k \cdot 3, q^k(q-1)/2\}$ are all optimal**. Moreover, in [25], the results presented in this correspondence have been used for constructing STBC-schemes with nonvanishing determinant for arbitrary values of n_t.

We emphasize that the determinant criterion which is based on the worst case PEP analysis at high SNR is insufficient to determine the true performance. More refined design criteria have been investigated for improving the performance [26]–[29]. However, as mentioned above, nonvanishing determinant is a sufficient criterion (with full rate) as far as the DM-G tradeoff is considered.

In the next subsection, we recollect the main principle used in [9] for constructing full-rate and full-rank STBCs from cyclic division algebra.

A. Space–Time Codes From Cyclic Division Algebras [9], [23]

Let $\mathbb{F}$ be a subfield of the complex field $\mathbb{C}$, and $\mathbb{K}$ be a finite cyclic Galois extension of $\mathbb{F}$. A cyclic algebra $D = (\mathbb{K}/\mathbb{F}, \sigma, \gamma)$ over the field $\mathbb{F}$ is an algebra that has $\mathbb{F}$ as the center ($\mathbb{F} = \{x \mid dx = xd \ \forall d \in D\}$) and $\mathbb{K}$ as a maximal subfield, with the Galois group $\mathrm{Gal}(\mathbb{K}/\mathbb{F}) = \langle \sigma \rangle$ being cyclic. D is naturally a right vector space over $\mathbb{K}$, with the degree or the index of D being defined as the dimension of the vector space D over $\mathbb{K}$. If n is the degree of D, then $|\mathrm{Gal}(\mathbb{K}/\mathbb{F})| = n$ and D can be decomposed as

$$D = \mathbb{K} \oplus z\mathbb{K} \oplus z^2\mathbb{K} \oplus \cdots \oplus z^{n-1}\mathbb{K}$$

where z is some element of D and the multiplication operation in D is completely defined by the relations

$$kz = z\sigma(k), \quad \forall k \in \mathbb{K} \quad \text{and} \quad z^n = \gamma, \quad \text{for some } \gamma \in \mathbb{F}^*.$$

Let $N_{\mathbb{K}/\mathbb{F}}(k) = \prod_{i=0}^{n-1} \sigma^i(k)$ denote the relative algebraic norm of an element $k \in \mathbb{K}$. Then the cyclic algebra D is a division algebra if γ satisfies the condition

$$\gamma^i \notin N_{\mathbb{K}/\mathbb{F}}(\mathbb{K}), \quad \text{for } 1 \le i < n \quad \text{and} \quad \gamma^n \in N_{\mathbb{K}/\mathbb{F}}(\mathbb{K}). \tag{2}$$

The division algebra D can be isomorphically embedded inside the ring of invertible $n \times n$ matrices $GL(n, \mathbb{K})$, by a map that takes the element $\sum_{i=0}^{n-1} z^i k_i$ to the matrix [9]

$$\begin{bmatrix} k_0 & \gamma\sigma(k_{n-1}) & \gamma\sigma^2(k_{n-2}) & \cdots & \gamma\sigma^{n-1}(k_1) \\ k_1 & \sigma(k_0) & \gamma\sigma^2(k_{n-1}) & \cdots & \gamma\sigma^{n-1}(k_2) \\ k_2 & \sigma(k_1) & \sigma^2(k_0) & \cdots & \gamma\sigma^{n-1}(k_3) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ k_{n-1} & \sigma(k_{n-2}) & \sigma^2(k_{n-3}) & \cdots & \sigma^{n-1}(k_0) \end{bmatrix}. \tag{3}$$

Since $\mathbb{K}$ is an nth-degree extension of $\mathbb{F}$, any element $k_i \in \mathbb{K}$ can be expressed as $k_i = \sum_{j=0}^{n-1} f_{i,j} t_j$, where $\{t_0, \ldots, t_{n-1}\}$ is a basis of $\mathbb{K}$ over $\mathbb{F}$ and $f_{i,j} \in \mathbb{F}$ for all i, j. Therefore, using the above matrix representation over $\mathbb{K}$ as a template, any element $d \in D$ can now be represented in the matrix form (4) at the bottom of the page.

$$\begin{bmatrix} \sum_{j=0}^{n-1} f_{0,j}t_j & \gamma\sigma\left(\sum_{j=0}^{n-1} f_{n-1,j}t_j\right) & \gamma\sigma^2\left(\sum_{j=0}^{n-1} f_{n-2,j}t_j\right) & \cdots & \gamma\sigma^{n-1}\left(\sum_{j=0}^{n-1} f_{1,j}t_j\right) \\ \sum_{j=0}^{n-1} f_{1,j}t_j & \sigma\left(\sum_{j=0}^{n-1} f_{0,j}t_j\right) & \gamma\sigma^2\left(\sum_{j=0}^{n-1} f_{n-1,j}t_j\right) & \cdots & \gamma\sigma^{n-1}\left(\sum_{j=0}^{n-1} f_{2,j}t_j\right) \\ \sum_{j=0}^{n-1} f_{2,j}t_j & \sigma\left(\sum_{j=0}^{n-1} f_{1,j}t_j\right) & \sigma^2\left(\sum_{j=0}^{n-1} f_{0,j}t_j\right) & \cdots & \gamma\sigma^{n-1}\left(\sum_{j=0}^{n-1} f_{3,j}t_j\right) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \sum_{j=0}^{n-1} f_{n-1,j}t_j & \sigma\left(\sum_{j=0}^{n-1} f_{n-2,j}t_j\right) & \sigma^2\left(\sum_{j=0}^{n-1} f_{n-3,j}t_j\right) & \cdots & \sigma^{n-1}\left(\sum_{j=0}^{n-1} f_{0,j}t_j\right) \end{bmatrix}. \tag{4}$$

The set of all matrices of the type (4), with the n^2 elements $f_{i,j} \in \mathbb{F}$ forms a division algebra. Using (4) as a rate-n design over $\mathbb{F}$, we can get a full-rank STBC for n transmit antennas by letting the n^2 variables take values from a signal set which is a finite subset of $\mathbb{F}$. Further, this code is called full rate, which means the symbol rate is n symbols per channel use since n^2 symbols $f_{i,j}, 0 \leq i, j < n-1$ are transmitted in n channel uses. An STBC-scheme can be constructed using the above design by considering a family of signal sets that are subsets of $\mathbb{F}$.

Proposition 1: Let $\mathcal{C}$ be a full-rate STBC constructed from a cyclic division algebra $(\mathbb{K}/\mathbb{F}, \sigma, \gamma)$ with codeword matrices of the form (4). Then, the coding gain of the code $\mathcal{C}$ is equal to

$$\min_{\boldsymbol{f} \neq \boldsymbol{f}'} \left|(-1)^{n-1} N_{\mathbb{K}/\mathbb{F}}(\Delta k_{n-1})\gamma^{n-1} + \cdots + N_{\mathbb{K}/\mathbb{F}}(\Delta k_0)\right|^{2/n}$$

where

$$\boldsymbol{f} = [f_{0,0}, \ldots, f_{0,n-1}, \ldots, f_{n-1,0}, \ldots, f_{n-1,n-1}]$$

and

$$\boldsymbol{f}' = [f'_{0,0}, \ldots, f'_{0,n-1}, \ldots, f'_{n-1,0}, \ldots, f'_{n-1,n-1}]$$

are two distinct sets of values of the n^2 variables in the design, and

$$\Delta k_i = \sum_{j=0}^{n-1} (f_{i,j} - f'_{i,j}) t_j.$$

Proof: The proof follows from the expression for the determinant of a matrix of the form (4), which is available in [30, Ch. 16]. □

Remark 3: When $n > 2$, unlike the constant term and the coefficient of γ^{n-1}, the coefficients of the remaining γ^i's in the coding gain expression of Proposition 1 are not simple expressions like $(-1)^i N_{\mathbb{K}/\mathbb{F}}(\Delta k_i)$, but involve complicated homogeneous polynomial expressions in the variables Δk_i and their conjugates. Nevertheless, the expression within $|.|$ is still an element of $\mathbb{F}$ [30].

Constructing a cyclic division algebra involves finding $\gamma \in \mathbb{F}$ satisfying condition (2) which is quite difficult. In [9], the authors overcome this difficulty by choosing $\gamma = \delta$, transcendental over $\mathbb{K}$ which will ensure that $(\mathbb{K}(\delta)/\mathbb{F}(\delta), \sigma, \delta)$ is a division algebra. While this method does yield full-rank STBCs, the coding gain given by the expression in Proposition 1 tends toward zero as the size of the signal set (any subset of $\mathbb{F}$) keeps increasing. This was first observed by Belfiore *et al.* in [21], where they are able to construct STBCs with *nonvanishing determinant* property for some specific values of n_t (equal to $2, 3,$ and 4). In order to get nonvanishing determinant codes from cyclic division algebras, they propose the following.

1) The element γ satisfying condition (2) should belong to $\mathfrak{O}_{\mathbb{F}}$, the algebraic integer ring in $\mathbb{F}$.
2) The basis $\{t_0, t_1, t_2, \ldots, t_{n-1}\}$ of $\mathbb{K}$ over $\mathbb{F}$ must be an integral basis, i.e., $t_i \in \mathfrak{O}_{\mathbb{K}}$ for all i.
3) The variables $f_{i,j}$ should take values from $\mathfrak{O}_{\mathbb{F}}$, which implies that the signal sets that can be used are subsets of the algebraic integer ring $\mathfrak{O}_{\mathbb{F}}$.

Since the algebraic norm map $N_{\mathbb{K}/\mathbb{F}}(\cdot)$ maps an algebraic integer in $\mathbb{K}$ to an algebraic integer in $\mathbb{F}$, these modifications will ensure that the determinant of the design (2) is an algebraic element in $\mathbb{F}$. If $\mathfrak{O}_{\mathbb{F}}$ **is a discrete subset of** $\mathbb{C}$, then there exists $d_{\min}(\mathfrak{O}_{\mathbb{F}})$: the smallest Euclidean distance between any two elements of $\mathfrak{O}_{\mathbb{F}} \subset \mathbb{C}$ when viewed as complex numbers. In such a case, the above modifications together with Proposition 1 ensure that the STBC using design (4) and any subset of $\mathfrak{O}_{\mathbb{F}}$ will have a nonvanishing determinant. Therefore, STBC-schemes obtained by a family of signal sets that are subsets of $\mathfrak{O}_{\mathbb{F}}$ and the design in (4) will have nonvanishing coding gain.

In this correspondence, we continue with this setup and construct STBCs from cyclic division algebras satisfying all the modifications mentioned above. We give a technique for finding γ satisfying the condition in (2), using which it is possible to get STBCs for arbitrary number of antennas by simply replacing the transcendental element with a suitable γ for all the codes in [9]. Doing this alone will not ensure the nonvanishing determinant property because $\mathfrak{O}_{\mathbb{F}}$ needs to be a discrete subset of $\mathbb{C}$ which is not true for all $\mathbb{F}$. This, coupled with the difficulty that finite cyclic extensions of arbitrary number field $\mathbb{F}$ are not well known, limits the number of transmit antennas for which we are able to construct STBC-schemes with nonvanishing determinant.

Remark 4 (Recent Result): The choice of γ and basis $\{t_i\}$ would affect the actual performance of the code. As far as nonvanishing coding gain is considered, these need to satisfy the conditions mentioned above. The codes for $n_t = 2, 3, 4,$ and 6 transmit antennas in [19], [22] satisfy these conditions and more (as indicated in Fig. 1, these are not covered under the general construction technique that is proposed in this correspondence). These codes are now known as perfect STBCs [31]: a class of codes which need to satisfy the four requirements for nonvanishing determinant listed earlier and **more** (see [31] for details). For instance, an additional requirement is that $|\gamma| = 1$. These additional requirements ensure a very good error probability performance, but as far as DM-G tradeoff is considered, these do not give any additional benefits. They, in fact, turn out to be restrictive because perfect STBCs exist only for $n_t = 2, 3, 4,$ and 6.

The remaining part of this correspondence is organized as follows. In the next subsection, we develop the necessary background on the ideals and their factorization in number fields. The main theorem (Theorem 1) of this correspondence is proved in Section II and in Section III, we discuss few constructions of nonvanishing determinant STBC-schemes for various number of transmit antennas and illustrate them through examples.

B. Ideal Factorization in Number Fields: A Brief Overview

In this subsection, we briefly review some important concepts from the theory of algebraic number fields which are necessary for our purposes. A number field $\mathbb{K}$ is a finite extension of the field of rationals $\mathbb{Q}$ and it is always of the form $\mathbb{Q}(\alpha)$ for some algebraic integer α. The set of all algebraic integers in $\mathbb{K}$ form a ring, called the ring of algebraic integers, and is denoted by $\mathfrak{O}_{\mathbb{K}}$. In general, the ring $\mathfrak{O}_{\mathbb{K}}$ is not a unique factorization domain (UFD) for an arbitrary $\mathbb{K}$, but it is always a Dedekind domain, which means that

- every prime ideal in $\mathfrak{O}_{\mathbb{K}}$ is a maximal ideal, and
- every ideal uniquely factorizes into a product of prime ideals.

These are two important properties that we are going to exploit in the later sections. Further, every ideal in $\mathfrak{O}_{\mathbb{K}}$ is generated by at most two elements, i.e., every ideal $\mathfrak{a}$ is of the form $\langle a_1, a_2 \rangle$, for some $a_1, a_2 \in \mathfrak{O}_{\mathbb{K}}$. The sum of two ideals $\mathfrak{a} + \mathfrak{b}$, also called the greatest common divisor (GCD) of $\mathfrak{a}$ and $\mathfrak{b}$, is the smallest ideal containing both the ideals. The ideals $\mathfrak{a}$ and $\mathfrak{b}$ are said to be coprime if $\mathfrak{a} + \mathfrak{b} = \mathfrak{O}_{\mathbb{K}}$. The product of two ideals $\mathfrak{a}\mathfrak{b}$ is the ideal generated by all finite sums of the form $\sum_i a_i b_i, a_i \in \mathfrak{a}$ and $b_i \in \mathfrak{b}$. We use the notation $a\mathfrak{O}_{\mathbb{K}}$ and $\langle a \rangle$ interchangeably to mean the principal ideal generated by $a \in \mathfrak{O}_{\mathbb{K}}$. An ideal $\mathfrak{a}$ is said to divide ideal $\mathfrak{b}$, if there exists another ideal $\mathfrak{c}$ such that $\mathfrak{b} = \mathfrak{a}\mathfrak{c}$, alternately, if $\mathfrak{a} \subset \mathfrak{b}$. If both these ideals are principal ideals, i.e., $\mathfrak{a} = \langle a \rangle$, $\mathfrak{b} = \langle b \rangle$ for some $a, b \in \mathfrak{O}_{\mathbb{K}}$, then the ideal division $\mathfrak{a}$ dividing $\mathfrak{b}$ is equivalent to the element a dividing b. The norm of an ideal $\mathfrak{a}$, denoted as $\|\mathfrak{a}\|$, is defined to be the index of $\mathfrak{a}$ in the additive Abelian group $\mathfrak{O}_{\mathbb{K}}$. If $\mathfrak{a} = \langle a \rangle$ for some $a \in \mathfrak{O}_{\mathbb{K}}$, then $\|\mathfrak{a}\| = \left|N_{\mathbb{K}/\mathbb{Q}}(a)\right|$.

Let $\mathbb{F}$ be a number field and $\mathbb{K}$ be a finite algebraic extension of $\mathbb{F}$. If $\mathfrak{p}$ is a prime ideal in $\mathfrak{O}_{\mathbb{F}}$, $\mathfrak{p}\mathfrak{O}_{\mathbb{K}}$ may no longer be a prime ideal in the ring $\mathfrak{O}_{\mathbb{K}}$. It factorizes uniquely into a product of prime ideals:

$\mathfrak{p}\mathfrak{O}_{\mathbb{K}} = \mathfrak{P}_1^{e_1}\mathfrak{P}_2^{e_2}\cdots\mathfrak{P}_r^{e_r}$. We will say that each prime ideal $\mathfrak{P}_i$ that appears in the factorization *lies over* the prime ideal $\mathfrak{p}$, or $\mathfrak{p}$ *lies under* $\mathfrak{P}_i$. Notice that $\mathfrak{P}_i \cap \mathfrak{O}_{\mathbb{F}} = \mathfrak{p}$, and therefore every prime ideal in $\mathfrak{O}_{\mathbb{K}}$ is over a unique prime ideal in $\mathfrak{O}_{\mathbb{F}}$. This means, if $\mathfrak{P}_i$ is a prime factor of $\mathfrak{p}\mathfrak{O}_{\mathbb{K}}$ then it cannot be a prime factor to any other ideal $\mathfrak{q}\mathfrak{O}_{\mathbb{K}}$ where $\mathfrak{q}$ is a prime ideal in $\mathfrak{O}_{\mathbb{F}}$ different from $\mathfrak{p}$. The exponent of any $\mathfrak{P}_i$ that appears in the factorization of $\mathfrak{p}\mathfrak{O}_{\mathbb{K}}$ is called the *ramification index* of $\mathfrak{P}_i$ over $\mathfrak{p}$, denoted as $e(\mathfrak{P}_i|\mathfrak{p}) = e_i$. Since every prime ideal in $\mathfrak{O}_{\mathbb{K}}$ is a maximal ideal, the quotient ring $\mathfrak{O}_{\mathbb{K}}/\mathfrak{P}_i$ is a field. It turns out that this is an extension of the finite field $\mathfrak{O}_{\mathbb{F}}/\mathfrak{p}$ with characteristic p, where p is the unique prime that lies under $\mathfrak{p}$ in $\mathbb{Z}$. The degree of the extension field $\mathfrak{O}_{\mathbb{K}}/\mathfrak{P}_i$ over $\mathfrak{O}_{\mathbb{F}}/\mathfrak{p}$ is called the *inertial degree* of $\mathfrak{P}_i$ over $\mathfrak{p}$, denoted as $f(\mathfrak{P}_i|\mathfrak{p}) = f_i$. This means that the norm of the ideal $\mathfrak{P}_i$, $\|\mathfrak{P}_i\|$, is equal to $\|\mathfrak{p}\|^{f_i}$. The ramification indices and the inertial degrees satisfy the relation $\sum_{i=1}^{r} e_i f_i = [\mathbb{K}:\mathbb{F}]$ and

$$f(\mathfrak{P}_i|p) = f(\mathfrak{P}_i|\mathfrak{p})f(\mathfrak{p}|p) \quad \text{and} \quad e(\mathfrak{P}_i|p) = e(\mathfrak{P}_i|\mathfrak{p})e(\mathfrak{p}|p).$$

We call the primes $p, \mathfrak{p}, \mathfrak{P}_i$ that lie one below the other as a prime triplet $(p;\mathfrak{p};\mathfrak{P}_i)$.

Our interest being in cyclic Galois extensions, it is important to mention that when $\mathbb{K}$ is Galois over $\mathbb{F}$, if $\mathfrak{P}_i, 1 \le i \le r$ are all the prime ideals that lie above $\mathfrak{p}$ as denoted above, then the ramification index of all the prime ideals are equal and so is the inertial degree. If e and f denote these common values then we have the relation $efr = [\mathbb{K}:\mathbb{F}]$ and $\|\mathfrak{P}_i\| = \|\mathfrak{p}\|^f$ for all $i = 1, 2, \ldots, r$.

Lemma 1: Let $\mathbb{K}$ be a degree-n Galois extension of a number field $\mathbb{F}$. If $\mathfrak{p}$ is a prime ideal in $\mathfrak{O}_{\mathbb{F}}$ such that the ideal $\mathfrak{P} = \mathfrak{p}\mathfrak{O}_{\mathbb{K}}$ is prime in $\mathfrak{O}_{\mathbb{K}}$, then $\|\mathfrak{P}\| = \|\mathfrak{p}\|^n$.

Proof: If $\mathfrak{P} = \mathfrak{p}\mathfrak{O}_{\mathbb{K}}$ is the only prime above $\mathfrak{p}$, then we have $r = 1$ and also $e(\mathfrak{P}|\mathfrak{p}) = 1$. Therefore, $f = [\mathbb{K}:\mathbb{F}]/(re) = n$. □

A prime $\mathfrak{p}$ of the form in Lemma 1 is said to be *inert* in $\mathbb{K}$, otherwise, we say it either *ramifies* (or is ramified) in $\mathbb{K}$ when $e_i > 1$ for some $i = 1, 2, \ldots, r$ or *splits* in $\mathbb{K}$ when $e_i = 1$ for all i and $r > 1$. If $\mathfrak{p} \subset \mathfrak{O}_{\mathbb{F}}$ is inert in $\mathbb{K}$, then $\mathfrak{P} = \mathfrak{p}\mathfrak{O}_{\mathbb{K}}$ is the unique prime that lies over $\mathfrak{p}$.

Example 1: Let $\mathbb{F} = \mathbb{Q}$ and $\mathbb{K} = \mathbb{Q}(i)$. It is well known that the primes of the form $4k+1$ split in $\mathbb{Z}[i]$, whereas the primes of the form $4k+3$ remain prime (or inert) in $\mathbb{Z}[i]$. Since $\mathbb{Z}[i]$ is a UFD, the factorization of elements is equivalent to the factorization of the ideals generated by the corresponding element. For example, $5 = (2+i)(2-i)$, which implies the ideal $\langle 5\rangle = \langle 2+i\rangle\langle 2-i\rangle$ in $\mathbb{Z}[i]$, whereas $\langle 3\rangle$ is itself a prime ideal in $\mathbb{Z}[i]$.

II. Main Result: Principle for Finding Suitable γ

In Example 1, the splitting of a rational prime p in $\mathbb{Z}[i]$ is equivalent to the possibility of expressing this prime as a sum of two squares ($5 = (2+i)(2-i) = 2^2 + 1^2$). For any $x + iy \in \mathbb{Q}(i)$, $x^2 + y^2 = N_{\mathbb{Q}(i)/\mathbb{Q}}(x+iy)$ and, therefore, we can say that a prime p splits in $\mathbb{Z}[i]$ if and only if $p \in N_{\mathbb{Q}(i)/\mathbb{Q}}(\mathbb{Q}[i])$. Because we are interested in finding an element γ which is not in the image of a norm map $N_{\mathbb{K}/\mathbb{F}}(\cdot)$, this observation led us to the study of prime ideal factorization in arbitrary extension fields. In this section, we present our main result (Theorem 1) which is a generalization of the above argument in $\mathbb{Z}[i]$ to integer rings of arbitrary number fields.

Lemma 2 ([32, Ch. 3, Exercise Problem 11]): Let $\mathfrak{I}$ be an ideal in a number field $\mathbb{K}$. Then, $\|\mathfrak{I}\|$ divides $N_{\mathbb{K}/\mathbb{Q}}(a)$ for all $a \in \mathfrak{I}$ and $\|\mathfrak{I}\| = \left|N_{\mathbb{K}/\mathbb{Q}}(a)\right|$ if and only if $\mathfrak{I} = \langle a\rangle$.

Proof: By definition, $\|\mathfrak{I}\|$ is the cardinality of the additive quotient group $\mathfrak{O}_{\mathbb{K}}/\mathfrak{I}$. For any $a \in \mathfrak{I}$, the ideal $\langle a\rangle$ is an additive subgroup of $\mathfrak{I}$ and hence $\mathfrak{O}_{\mathbb{K}}/\mathfrak{I}$ is a subgroup of $\mathfrak{O}_{\mathbb{K}}/\langle a\rangle$. Therefore, $\|\mathfrak{I}\|$ divides $\|\langle a\rangle\| = \left|N_{\mathbb{K}/\mathbb{Q}}(a)\right|$. □

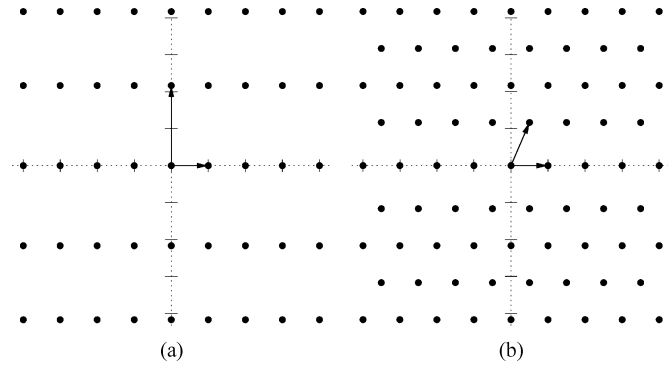

Fig. 2. Lattice structure of the integer ring of an imaginary quadratic field. (a) Rectangular lattice when $\boldsymbol{d \equiv 2, 3 \bmod 4}$. (b) Isosceles triangular lattice when $\boldsymbol{d \equiv 1 \bmod 4}$.

Theorem 1 (Main Theorem): Let $\mathbb{K}$ be a degree-n Galois extension of a number field $\mathbb{F}$ and let $\mathfrak{p}$ be a prime ideal in $\mathfrak{O}_{\mathbb{F}}$ that is below the prime ideal $\mathfrak{P} \subset \mathfrak{O}_{\mathbb{K}}$ such that $\|\mathfrak{P}\| = \|\mathfrak{p}\|^f$. If γ is any element of $\mathfrak{p} \setminus \mathfrak{p}^2$, then $\gamma^i \notin N_{\mathbb{K}/\mathbb{F}}(\mathbb{K})$ for any $i = 1, 2, \ldots, f-1$.

In particular, if $\mathrm{Gal}(\mathbb{K}/\mathbb{F}) = \langle\sigma\rangle$ with $[\mathbb{K}:\mathbb{F}] = n$, then the cyclic algebra $(\mathbb{K}/\mathbb{F}, \sigma, \gamma)$ is a division algebra if $\gamma \in \mathfrak{p} \setminus \mathfrak{p}^2$ for some prime triplet $(p;\mathfrak{p};\mathfrak{P})$ with $f(\mathfrak{P}|\mathfrak{p}) = n$.

Proof: Recall that $\|\mathfrak{P}\| = \|\mathfrak{p}\|^f$. Now, if we assume that $\gamma^i = N_{\mathbb{K}/\mathbb{F}}(x)$ for some $x \in \mathbb{K}$, then x has to be in $\mathfrak{P}$ and according to Lemma 2, $\|\mathfrak{p}\|^f$ divides $N_{\mathbb{K}/\mathbb{Q}}(x) = N_{\mathbb{F}/\mathbb{Q}}(\gamma)^i$. But this is a contradiction since $\gamma \in \mathfrak{p} \setminus \mathfrak{p}^2$ implies $\|\mathfrak{p}\|$ divides $N_{\mathbb{F}/\mathbb{Q}}(\gamma)$, whereas $\|\mathfrak{p}\|^2$ does not. □

To construct cyclic division algebra $(\mathbb{K}/\mathbb{F}, \sigma, \gamma)$, Theorem 1 along with Lemma 1 suggest that we need to look for a prime ideal $\mathfrak{p}$ in $\mathfrak{O}_{\mathbb{F}}$ that remains inert in $\mathfrak{O}_{\mathbb{K}}$.

Example 2 (Example 1 Continued): Let $\mathfrak{p} = \langle 3\rangle \subset \mathbb{Z}$. Since $\mathfrak{p}$ is inert in $\mathbb{Z}[i]$, according to Lemma 1, we have $\|\mathfrak{P}\| = \|\mathfrak{p}\|^2 = 3^2$. The element $\gamma = 3$ belongs to the set $\gamma \in \langle 3\rangle \setminus \langle 3^2\rangle$ and it cannot belong to $N_{\mathbb{Q}(i)/\mathbb{Q}}(\mathbb{Q}(i))$ because 3^2 cannot divide 3.

In general, it is not easy to find the parameters e, f, and r, let alone the factorization of an ideal $p\mathfrak{O}_{\mathbb{K}}$ in an arbitrary number field $\mathbb{K}$. But in this correspondence and also in [9], [21], STBC constructions from cyclic division algebra $(\mathbb{K}/\mathbb{F}, \sigma, \gamma)$ consider $\mathbb{K}$ to be a cyclotomic extension of $\mathbb{Q}$, for which there exist results on finding e, f, and r for any rational prime p. Further, all our constructions in this correspondence assume the field $\mathbb{F}$ to be a quadratic extension of $\mathbb{Q}$. For both classes of extension fields, there exist results on finding e, f, and r, which are given in the following two subsections.

A. Factorization in a Quadratic Extension of $\mathbb{Q}$

A number field $\mathbb{F} = \mathbb{Q}(\sqrt{d})$, d a square-free integer in $\mathbb{Z}$, is said to be a quadratic extension of $\mathbb{Q}$. The degree $[\mathbb{F}:\mathbb{Q}]$ is always 2 and the Galois group $\mathrm{Gal}(\mathbb{F}/\mathbb{Q}) = \langle\sigma\rangle$, with $\sigma(\sqrt{d}) = -\sqrt{d}$. The integer ring of $\mathbb{F}$ is $\mathbb{Z}\left[\sqrt{d}\right]$ when $d \equiv 2, 3 \bmod 4$, otherwise, it is $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$. When $d < 0$, $\mathbb{F}$ is an imaginary quadratic extension field, in which case, the ring $\mathfrak{O}_{\mathbb{F}}$ forms a lattice in the complex plane. This lattice, which is shown in Fig. 2, is rectangular if $d \equiv 2, 3 \bmod 4$ and it is "isosceles triangular" when $d \equiv 1 \bmod 4$ (see [33, Ch. 11]).

In this correspondence, in all the cyclic division algebras $(\mathbb{K}/\mathbb{F}, \sigma, \gamma)$ that are used for STBC-scheme construction, we consider the field $\mathbb{F}$ to be an imaginary quadratic extension. Thus, the

signal sets used are always subsets of either a rectangular lattice or an isosceles triangular lattice. In the special case when $d = -1$ and $d = -3$, the integer ring is the Gaussian ring (square lattice) and the hexagonal lattice (equilateral triangular lattice), respectively.

Theorem 2 ([32, p. 74]): Let $\mathbb{F} = \mathbb{Q}(\sqrt{d})$. Suppose d is odd, then the ideal $2\mathfrak{O}_{\mathbb{F}}$ factorizes as

- $\langle 2, 1+\sqrt{d}\rangle^2$ if $d \equiv 3 \bmod 4$;
- $\langle 2, \frac{1+\sqrt{d}}{2}\rangle\langle 2, \frac{1-\sqrt{d}}{2}\rangle$ if $d \equiv 1 \bmod 8$;
- $2\mathfrak{O}_{\mathbb{F}}$ (remains prime) if $d \equiv 5 \bmod 8$.

Further, if p is an odd prime such that $\gcd(p, d) = 1$, then the ideal $p\mathfrak{O}_{\mathbb{F}}$ factorizes as

- $\langle p, x+\sqrt{d}\rangle\langle p, x-\sqrt{d}\rangle$ if $x^2 \equiv d \bmod p$ for some $x \in \mathbb{Z}$;
- $p\mathfrak{O}_{\mathbb{F}}$ (remains prime) if $x^2 \not\equiv d \bmod p$ for any $x \in \mathbb{Z}$.

When the integer ring $\mathfrak{O}_{\mathbb{Q}(\sqrt{d})}$ is a Euclidean domain with respect to the norm map of $\mathbb{Q}(\sqrt{d})$, then it is also a UFD and hence a principal ideal domain (PID), which means all ideals are generated by single elements. In such a case, the ideal $\langle p, x+\sqrt{d}\rangle$ in Theorem 2 is generated by π; a factor of p. For instance, the rings $\mathbb{Z}[i]$ as well as $\mathbb{Z}[\omega_3]$ are both Euclidean domains.

B. Factorization in a Cyclotomic Field

A number field $\mathbb{K} = \mathbb{Q}(\omega_m)$ is said to be an mth cyclotomic extension field if ω_m is a primitive mth root of unity. The degree of $\mathbb{Q}(\omega_m)$ is $[\mathbb{Q}(\omega_m) : \mathbb{Q}] = \varphi(m)$, where $\varphi(.)$ denotes the Euler totient function and the ring of algebraic integers is $\mathbb{Z}[\omega_m]$. This field is Galois over $\mathbb{Q}$, with

$$\mathrm{Gal}(\mathbb{K}/\mathbb{Q}) = \{\sigma_j : \sigma_j(\omega_m) = \omega_m^j \mid \gcd(m, j) = 1\}$$

which is isomorphic to the group of units in $\mathbb{Z}/m\mathbb{Z}$, denoted as $U(\mathbb{Z}/m\mathbb{Z})$.

Theorem 3 ([32, p. 78]): If $\gcd(p, m) = 1$, then the ideal $p\mathbb{Z}[\omega_m]$ splits into $\varphi(m)/f$ distinct prime ideals in $\mathbb{Z}[\omega_m]$, where f is the multiplicative order of p modulo m.

III. STBC-Schemes With Nonvanishing Determinant

In this section, we construct STBC-schemes with nonvanishing determinant from cyclic division algebras. We will first treat the $n = 2^k$ antenna case separately by going through the detailed process of finding a suitable value for γ. The odd prime power case will be taken up in the subsequent subsection.

A. STBC-Scheme for $n = 2^k$ Transmit Antennas Over QAM Signal Sets

Let $m = 2^{k+2}$, $k \geq 1$, and $\mathbb{K} = \mathbb{Q}(\omega_m)$. The Galois group $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^k\mathbb{Z}$ and $\mathbb{F} = \mathbb{Q}(i)$ is the subfield fixed by the cyclic subgroup $\mathbb{Z}/2^k\mathbb{Z}$. Therefore, $\mathbb{K}/\mathbb{F}$ is cyclic with $[\mathbb{K} : \mathbb{F}] = n = \varphi(m)/2 = 2^k$. Now, to construct division algebra $(\mathbb{Q}(\omega_m)/\mathbb{Q}(i), \sigma, \gamma)$, we need to find a prime triplet $(p; \mathfrak{p}; \mathfrak{P})$, $\mathfrak{p} \subset \mathbb{Z}[i]$ and $\mathfrak{P} \subset \mathbb{Z}[\omega_m]$ such that $f(\mathfrak{P}|\mathfrak{p}) = n = 2^k$. In the following theorem, we prove that $p = 5$ is a suitable choice.

Theorem 4: Let k be a positive integer. For $n = 2^k$ transmit antennas, the scheme constructed using a family of M-QAM signal sets and the design (4) based on the cyclic division algebra $(\mathbb{Q}(\omega_{2^{k+2}})/\mathbb{Q}(i), \sigma, 2+i)$ has a nonvanishing determinant.

Proof: We will continue to use the notations used in the earlier paragraph, where we already showed that the extension $\mathbb{K}/\mathbb{F}$ is a cyclic extension of degree 2^k. It is well known that the Gaussian integer ring $\mathbb{Z}[i]$ is a discrete subset of $\mathbb{C}$. Therefore, it remains to prove that $\gamma = 2 + i$ satisfies the condition (2), which follows from the argument below.

1) Let $\mathfrak{P}_1$ be one of the primes in $\mathbb{Z}[\omega_m]$ which lies above $p = 5$. The multiplicative order of 5 modulo 2^{k+2} is equal to $f(\mathfrak{P}_1|p) = 2^k$ (see [34, Ch. 4, Theorem 2′]).
2) Since $\gcd(5, m) = 1$ in $\mathbb{Z}[\omega_m]$, the ideal $5\mathbb{Z}[\omega_m]$ splits into $\varphi(2^{k+2})/f(\mathfrak{P}_1|p) = 2$ distinct prime ideals, $\mathfrak{P}_1$ and $\mathfrak{P}_2$.
3) If $\mathfrak{p} = \mathfrak{P}_1 \cap \mathbb{Z}[i]$ is the unique prime in $\mathbb{Z}[i]$ below $\mathfrak{P}_1$, since we know that $5 = (2+i)(2-i)$ in $\mathbb{Z}[i]$, $\mathfrak{p}$ has to be equal to either $(2+i)\mathbb{Z}[i]$ or $(2-i)\mathbb{Z}[i]$. Without loss of generality, we assume $\mathfrak{p} = (2+i)\mathbb{Z}[i]$. Further, since 5 splits into two factors and $[\mathbb{Q}(i) : \mathbb{Q}] = 2$, we have $f(\mathfrak{p}|p) = 1$.
4) Therefore, $(5; (2+i)\mathbb{Z}[i]; \mathfrak{P}_1)$ is a prime triplet with

$$f(\mathfrak{P}_1|\mathfrak{p}) = f(\mathfrak{P}_1|p)/f(\mathfrak{p}|p) = 2^k/1 = 2^k.$$

From Theorem 1, this argument proves that $(\mathbb{Q}(\omega_m)/\mathbb{Q}(i), \sigma, 2+i)$ is a cyclic division algebra and hence the STBC-scheme under consideration has a nonvanishing determinant. □

Example 3:

i) Let $n = 2$ be the number of transmit antennas. The field $\mathbb{K} = \mathbb{Q}(\omega_8)$ is a degree 2 cyclic extension of $\mathbb{Q}(i)$ with $\{1, \sqrt{i}\}$ as a basis. The design of (4) takes the form

$$\boldsymbol{X} = \begin{bmatrix} f_{0,0} + f_{0,1}\sqrt{i} & \gamma(f_{1,0} - f_{1,1}\sqrt{i}) \\ f_{1,0} + f_{1,1}\sqrt{i} & f_{0,0} - f_{0,1}\sqrt{i} \end{bmatrix}$$

where $\gamma = 2+i$. This design is a full-rank design over $\mathbb{Q}(i)$ and an STBC-scheme can be constructed for two transmit antennas using this design along with a family of M-QAM signal sets.

ii) For $n = 4$ transmit antennas, the design takes the form

$$\boldsymbol{X} = \begin{bmatrix} a_{0,0} & \gamma a_{1,3} & \gamma a_{2,2} & \gamma a_{3,1} \\ a_{0,1} & a_{1,0} & \gamma a_{2,3} & \gamma a_{3,2} \\ a_{0,2} & a_{1,1} & a_{2,0} & \gamma a_{3,3} \\ a_{0,3} & a_{1,2} & a_{2,1} & a_{3,0} \end{bmatrix}$$

where $\gamma = 2+i$ and $a_{j,k} = \sum_{l=0}^{3} f_{k,l}(i^j\omega_{16})^l$ and $f_{j,k} \in \mathbb{Z}(i)$ for $j, k = 0, 1, 2, 3$. An STBC-scheme can be constructed for four transmit antennas using this design along with a family of M-QAM signal sets.

In the above construction, there is a restriction on the number of transmit antennas (n of the type 2^k) because of the difficulty in constructing cyclic extension fields of arbitrary degree over $\mathbb{Q}(i)$. For designing STBCs from cyclic division algebra for n not of the type 2^k, we have to change to a different base field $\mathbb{F} \neq \mathbb{Q}(i)$. This, in turn, means that we will have to forgo the standard QAM signal set for some nonstandard signal sets. In all cases, the procedure to find suitable γ would be exactly the same as we did here: to find a rational prime p such that the number of prime factors of $p\mathfrak{O}_{\mathbb{F}}$ in $\mathfrak{O}_{\mathbb{F}}$ is the same as the number of prime factors of $p\mathfrak{O}_{\mathbb{K}}$ in $\mathfrak{O}_{\mathbb{K}}$. This will ensure $f(\mathfrak{P}|\mathfrak{p}) = [\mathbb{K} : \mathbb{F}]$; a consequence of a general theorem on factorization of ideals and a corollary to this theorem which is given in the Appendix.

B. STBC-Schemes for $n = q^k(q-1)/2$ Transmit Antennas

We will now generalize the construction of the previous subsection to $n = \varphi(q^{k+1})/2$ number of transmit antennas, where q is a rational prime of the form $4s + 3$.

Theorem 5: Let q be a rational prime of the form $4s + 3$, and $m = q^{k+1}$ for some arbitrary rational integer $k \geq 0$ ($k > 0$ when

$q = 3$). Consider the STBC-scheme for $n = \varphi(q^{k+1})/2$ transmit antennas that can be constructed using a family of signal sets that are subsets of $\mathbb{Z}\left[\frac{1+\sqrt{-q}}{2}\right]$ and the design (4) from the cyclic division algebra $(\mathbb{Q}(\omega_m)/\mathbb{Q}(\sqrt{-q}), \sigma, \gamma)$. This scheme has a nonvanishing determinant if $\gamma \in \mathfrak{p} \setminus \mathfrak{p}^2$ for the prime triplet $(p; \mathfrak{p}; \mathfrak{P})$ chosen such that $\gcd(p, q) = 1$, and

- $p = 2$ if $-q \equiv 1 \bmod 8$, else p is chosen such that $x^2 \equiv -q \bmod p$ for some integer x;
- $\sigma_p : \sigma_p(\omega_m) = \omega_m^p$ is a generator of the cyclic Galois group

$$\langle \sigma \rangle = \mathrm{Gal}(\mathbb{Q}(\omega_m)/\mathbb{Q}(\sqrt{-q})).$$

Proof: For $m = q^{k+1}$, the Galois group $\mathrm{Gal}(\mathbb{Q}(\omega_m)/\mathbb{Q})$ is $U(\mathbb{Z}/q^k\mathbb{Z})$, which is known to be a cyclic group for any k. Therefore, if d is any positive divisor of $\varphi(m)$, then there is a unique subfield of degree d. When q is of the form $4s+3$, the unique degree 2 subfield of $\mathbb{Q}(\omega_m)$ is $\mathbb{Q}(\sqrt{-q})$ (see [32, Ch. 2, Exercise problem 8]), whose integer ring $\mathbb{Z}\left[\frac{1+\sqrt{-q}}{2}\right]$ is always a discrete subset of $\mathbb{C}$. From Theorem 2, the first condition implies that the ideal $\langle p \rangle$ splits into two prime factors $\mathfrak{p}$ and $\mathfrak{p}'$ in $\mathbb{Z}\left[\frac{1+\sqrt{-q}}{2}\right]$, while the second condition is equivalent to saying that the multiplicative order of p modulo m is

$$f(\mathfrak{P}|p) = [\mathbb{K} : \mathbb{F}] = \varphi(q^{k+1})/2 = q^k(q-1)/2. \qquad \square$$

As an example of this theorem, we consider STBCs for $n = 3^k$ transmit antennas over a constellation that is a subset of the hexagonal lattice

$$\mathbb{Z}[\omega_3] = \mathbb{Z}[\omega_6] = \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$$

where $\omega_6 = \frac{1+\sqrt{-3}}{2}$ and $\omega_3 = -\omega_6$.

Example 4 (Scheme for 3^k Antennas Over Hexagonal Lattice): This construction is similar to that of $n = 2^k$ antenna STBC; the only difference being the various fields and the prime p that are involved in the construction. Let $m = 3^{k+1}$ and $\mathbb{K} = \mathbb{Q}(\omega_m)$. The extension $\mathbb{K}/\mathbb{Q}$ is cyclic Galois, with

$$\mathrm{Gal}(\mathbb{K}/\mathbb{Q}) \cong U(\mathbb{Z}/3^{k+1}\mathbb{Z}) \quad \text{and} \quad [\mathbb{K} : \mathbb{Q}] = \varphi(3^{k+1}) = 3^k 2.$$

Now, the field $\mathbb{F} = \mathbb{Q}(\omega_3)$ is a subfield of $\mathbb{K}$, with $[\mathbb{K} : \mathbb{F}] = 3^k$ and the extension $\mathbb{K}/\mathbb{F}$ is also cyclic Galois.

Let $p = 7$. This satisfies the first condition of Theorem 5 because $2^2 \equiv -3 \bmod 7$; it splits in $\mathbb{Z}[\omega_3]$ as $7 = (3+\omega_3)(2-\omega_3)$ and, therefore, $7\mathbb{Z}[\omega_3] = \langle 3+\omega_3 \rangle \langle 2-\omega_3 \rangle$. This implies that the inertial degree of $\mathfrak{p} = \langle 3+\omega_3 \rangle$ is $f(\mathfrak{p}|p) = 1$. Further, let $\mathfrak{P}$ be a prime over $\mathfrak{p}$ in $\mathbb{Z}[\omega_m]$; since the multiplicative order of 7 modulo 3^{k+1} is equal to $f(\mathfrak{P}|p) = 3^k$ for any $k > 0$, the ideal $7\mathbb{Z}[\omega_m]$ splits into $\varphi(3^{k+1})/f(\mathfrak{P}|p) = 2$ distinct prime ideals. This implies $\mathfrak{P}$ is the only prime over $\mathfrak{p}$ in $\mathbb{Z}[\omega_m]$ which means $\mathfrak{p} = \langle 3+\omega_3 \rangle$ is inert in $\mathbb{Z}[\omega_m]$. Thus, $(\mathbb{Q}(\omega_m)/\mathbb{Q}(\omega_3), \sigma, 3+\omega_3)$ is a cyclic division algebra for any $k > 0$.

For $n = 3$ transmit antennas we use $\{1, \omega_9, \omega_9^2\}$ as a basis of $\mathbb{Q}(\omega_9)$ over $\mathbb{Q}(\omega_3)$, and the design in (4) takes the form

$$\boldsymbol{X} = \begin{bmatrix} a_{0,0} & \gamma a_{1,2} & \gamma a_{2,1} \\ a_{0,1} & a_{1,0} & \gamma a_{2,2} \\ a_{0,2} & a_{1,1} & a_{2,0} \end{bmatrix}$$

where $\gamma = 3 + \omega_3$ and $a_{j,k} = \sum_{l=0}^{2} f_{k,l}(\omega_3^j \omega_9)^l$ for $j, k = 0, 1, 2$. An STBC-scheme for three transmit antennas can be obtained using this design along with signal sets from $\mathbb{Z}[\omega_3]$. This is the same scheme that is obtained in [21] for three transmit antennas.

Example 5 (STBC-Scheme for Five Transmit Antennas): Let $\mathbb{K} = \mathbb{Q}(\omega_{11})$, which contains $\mathbb{F} = \mathbb{Q}(\sqrt{-11})$ as a subfield with $[\mathbb{K} : \mathbb{F}] = 5$. We have

$$\mathfrak{O}_{\mathbb{F}} = \mathbb{Z}\left[\frac{1+\sqrt{-11}}{2}\right]$$

where $p = 3$ factorizes as $\left(\frac{1+\sqrt{-11}}{2}\right)\left(\frac{1-\sqrt{-11}}{2}\right)$ (notice that $2^2 \equiv -11 \bmod 3$). Following Theorem 3, we find that the multiplicative order of 3 modulo 11 is $5 = [\mathbb{K} : \mathbb{F}]$ and so p splits into $\varphi(11)/5 = 2$ distinct prime ideals in $\mathbb{Z}[\omega_{11}]$. Thus, choosing $\gamma = \frac{1+\sqrt{-11}}{2}$, we get a degree 5 cyclic division algebra $\left(\mathbb{Q}(\omega_{11})/\mathbb{Q}(\sqrt{-11}), \sigma, \gamma\right)$.

Example 6 (STBC-Scheme for 11 Transmit Antennas): Let $\mathbb{K} = \mathbb{Q}(\omega_{23})$, which contains $\mathbb{F} = \mathbb{Q}(\sqrt{-23})$ as a subfield with $[\mathbb{K} : \mathbb{F}] = 11$. The algebraic integer ring

$$\mathfrak{O}_{\mathbb{F}} = \mathbb{Z}\left[\frac{1+\sqrt{-23}}{2}\right]$$

is not a PID, but from Theorem 2, we find that $\langle p \rangle = \langle 2 \rangle$ factorizes as $\langle 2, \frac{1+\sqrt{-23}}{2} \rangle \langle 2, \frac{1-\sqrt{-23}}{2} \rangle$ in $\mathfrak{O}_{\mathbb{F}}$ (notice that $-23 \equiv 1 \bmod 8$). Following Theorem 3, we find that the multiplicative order of 2 modulo 23 is $11 = [\mathbb{K} : \mathbb{F}]$ and so 2 splits into $\varphi(23)/11 = 2$ distinct prime ideals in $\mathbb{Z}[\omega_{23}]$. Thus, by choosing $\gamma = \frac{1+\sqrt{-23}}{2}$, we get a degree 11 cyclic division algebra $\left(\mathbb{Q}(\omega_{23})/\mathbb{Q}(\sqrt{-23}), \sigma, \gamma\right)$.

In both the classes of STBC-schemes that we have constructed so far, we made use of the fact that $\mathbb{K}/\mathbb{F}$ is cyclic. With this knowledge, we used an inert prime ideal to get a γ satisfying condition (2). All the proofs and techniques that we have used so far rely on a general theorem (stated in the Appendix) that actually says that existence of inert prime ideal implies that $\mathbb{K}/\mathbb{F}$ is cyclic. We make use of this to construct STBC-schemes for n that is of the form $2 \cdot 3^k$ or $3 \cdot 2^k$.

C. STBC-Scheme for $n = 2 \cdot 3^k$ or $n = 3 \cdot 2^k$ Antennas

Theorem 6: Let $m = 4 \cdot 3^{k+1}$ and $n = \varphi(m)/2 = 2 \cdot 3^k$. For n transmit antennas, the STBC-scheme obtained using a family of signal sets that are subsets of $\mathbb{Z}[\omega_3]$, and the design (4) based on the cyclic division algebra $(\mathbb{Q}(\omega_m)/\mathbb{Q}(\omega_3), \sigma, 3+\omega_3)$ has a nonvanishing determinant.

Proof: Let $p = 7$. Since $\mathbb{K} = \mathbb{Q}(\omega_m)$ is a cyclotomic extension field, any subgroup of $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ is a normal group and hence we can use the results of Corollary 1 in the Appendix. Since 7 splits into $\mathfrak{p} = \langle 3+\omega_3 \rangle \langle 2-\omega_3 \rangle$ in $\mathbb{F} = \mathbb{Q}(\omega_3)$ and there is no other subfield of $\mathbb{F}$, the field $\mathbb{F}$ must be the decomposition field of $p = 7$. Therefore, it is enough to show that n is the multiplicative order of 7 modulo m. This is straightforward because

$$7^f \equiv 1 \mod 4 \cdot 3^{k+1} \Rightarrow \begin{cases} 7^f \equiv 1 \mod 4 \\ 7^f \equiv 1 \mod 3^{k+1} \end{cases}$$

and if f is the smallest integer satisfying the preceding equation, f must be the least common multiple of f_1 and f_2, where $f_1 =$ order of $7 \bmod 4 = 2$, and $f_2 =$ order of $7 \bmod 3^{k+1} = 3^k$ for all $k > 0$. $\square$

By considering $m = 9 \cdot 2^{k+1}$ and $p = 5$, we can give a similar proof as above, to show that $(\mathbb{Q}(\omega_m)/\mathbb{Q}(i), \sigma, 2+i)$ is a division algebra

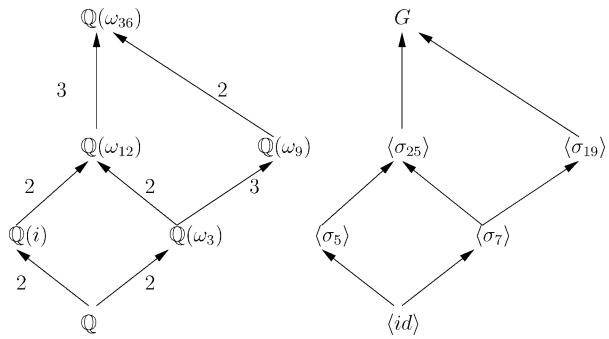

Fig. 3. Subfield tower of $\mathbb{Q}(\omega_{36})$.

of degree $\varphi(m)/2 = n = 3 \cdot 2^k$. Thus, STBC-scheme with nonvanishing determinant can be constructed using this division algebra along a family of signal sets from $\mathbb{Z}[i]$.

Example 7 (STBC for Six Transmit Antennas): Let $\mathbb{K} = \mathbb{Q}(\omega_{36})$ for which $\mathrm{Gal}(\mathbb{K}/\mathbb{Q}) = \{\sigma_i : \gcd(i, 36) = 1\}$, and σ_i is determined by $\sigma_i(\omega_{36}) = \omega_{36}^i$. We have the tower of subfields and the subgroups of $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ fixing them as shown in Fig. 3.

Notice that the $\mathbb{Q}(\omega_{36})/\mathbb{Q}(i)$ is cyclic with $\mathrm{Gal}(\mathbb{Q}(\omega_{36})/\mathbb{Q}(i)) = \langle\sigma_5\rangle$. We can now say that the decomposition field of 5 in $\mathbb{K}$ is $\mathbb{Q}(i)$ and the inertial field is $\mathbb{K}$ itself. Thus, the ideal $(2+i)\mathbb{Z}[i]$ remains inert in every extension between $\mathbb{K}$ and $\mathbb{Q}(i)$ and we have: a degree 6 cyclic division algebra $(\mathbb{K}/\mathbb{Q}(i), \sigma_5, 2+i)$.

Similarly, $\mathbb{Q}(\omega_{36})/\mathbb{Q}(\omega_3)$ is cyclic with $\mathrm{Gal}(\mathbb{Q}(\omega_{36})/\mathbb{Q}(\omega_3)) = \langle\sigma_7\rangle$ and we get a sixth-degree cyclic division algebra $(\mathbb{K}/\mathbb{Q}(\omega_3), \sigma_7, 3+\omega_3)$.

D. Bound on the Coding Gain

The coding gain of an $n \times n$ full-rank STBC $\mathcal{C}$ is known [14] to be equal to

$$\min_{\boldsymbol{C}_1 \neq \boldsymbol{C}_2 \in \mathcal{C}} |Det\,(\boldsymbol{C}_1 - \boldsymbol{C}_2)|^{2/n}.$$

For the STBCs considered in this correspondence, we have the following result on the coding gain.

Theorem 7: Let $\mathcal{C}$ be an $n \times n$ STBC constructed using the design (4) and any of the cyclic division algebras $\left(\mathbb{Q}(\omega_m)/\mathbb{Q}(\sqrt{d}), \sigma, \gamma\right)$, discussed in the previous subsections. If κ denotes the scaling factor used on each codeword as part of power constraint, then the coding gain of $\mathcal{C}$ is always greater than or equal to κ^2.

Proof: From Proposition 1, and the fact that $Det(\kappa\boldsymbol{C}) = \kappa^n Det(\boldsymbol{C})$, it is clear that the coding gain is lower-bounded by $(\kappa^n d_{\min})^{2/n}$, where $d_{\min}$ denotes the minimum Euclidean distance of the integer ring $\mathfrak{O}_{\mathbb{Q}(\sqrt{d})}$. The cyclic division algebras considered in this correspondence are over an imaginary quadratic field $\mathbb{Q}(\sqrt{d})$, where $d = -1$ or $d = -q$, q is of the form $4s+3$. So, the ring of integers is either the Gaussian integer ring or some isosceles triangle lattice, and for both these lattices the minimum Euclidean distance is 1. □

The need for κ arises when comparing the performance of two different codes that are using the same signal set. If both the codes are described through designs, then κ depends only on the respective designs to make sure that both codes are using the same average energy. Therefore, κ is independent of the signal set size, and hence the STBC-scheme constructed using our design and a family of signal sets that are subsets of either the Gaussian integer ring or the isosceles triangle lattice, has a nonvanishing determinant.

IV. Conclusion

In this correspondence, we have presented a general construction technique for STBC-schemes with nonvanishing determinant for the number of transmit antennas (n_t) of the form 2^k or $3 \cdot 2^k$ or $2 \cdot 3^k$ or $q^k(q-1)/2$, where q is a prime of the form $4s+3$ and s is any arbitrary integer. The proposed STBC-schemes are based on cyclic division algebras. We provide a technique for finding suitable γ so that the determinant of the design based on cyclic division algebra $(\mathbb{K}/\mathbb{F}, \sigma, \gamma)$ is always a nonzero element in the integer ring of $\mathbb{F}$. This technique is general and can be used for any cyclic extension $\mathbb{K}/\mathbb{F}$ of arbitrary degree. But in this correspondence, we have only been able to use this for the above mentioned values of n_t, because these are the only values for which we could manage to satisfy the twin restrictions: the integer ring of $\mathbb{F}$ should be discrete in $\mathbb{C}$ and $\mathbb{K}/\mathbb{F}$ should be cyclic.

In a recent work [25], the construction techniques and results of this correspondence have been used to construct cyclic division algebra based STBC-schemes with nonvanishing determinant for arbitrary number of transmit antennas. Moreover, it has been proved that all the STBC-schemes constructed in this correspondence achieve the optimal DM-G tradeoff.

Appendix

Theorem 8 ([32, Ch. 4, Theorem 28]): Let $\mathbb{K}$ be a Galois extension of $\mathbb{Q}$ and let $\mathfrak{P}$ be a prime factor of $p\mathfrak{O}_{\mathbb{K}}$ for some rational prime p, with $e(\mathfrak{P}|p) = e$, $f(\mathfrak{P}|p) = f$ and $efr = [\mathbb{K} : \mathbb{Q}]$. Let

$$D = D(\mathfrak{P}|p) = \{\sigma \in \mathrm{Gal}(\mathbb{K}/\mathbb{Q}) : \sigma(\mathfrak{P}) = \mathfrak{P}\}$$

and

$$\begin{aligned} E &= E(\mathfrak{P}|p) \\ &= \{\sigma \in \mathrm{Gal}(\mathbb{K}/\mathbb{Q}) : \sigma(a) + \mathfrak{P} = a + \mathfrak{P} \quad \forall a \in \mathfrak{O}_{\mathbb{Q}}\}. \end{aligned}$$

Then, $E \subset D$ and both D, E are subgroups of $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$, respectively called the *decomposition group* and the *inertia group* of $\mathfrak{P}$ over p. If $\mathbb{K}_D$ and $\mathbb{K}_E$ denote the fixed subfields of D and E, respectively, and $\mathfrak{P}_D = \mathfrak{P} \cap \mathfrak{O}_{\mathbb{K}_D}$, $\mathfrak{P}_E = \mathfrak{P} \cap \mathfrak{O}_{\mathbb{K}_E}$ are the prime ideals below $\mathfrak{P}$ and above p in the respective algebraic integer rings, then we have the following relation among the tower of fields and ideals:

$$\begin{array}{rcl} & \mathbb{K} & \mathfrak{P} \\ [\mathbb{K} : \mathbb{K}_E] = e & \uparrow & \uparrow \; e(\mathfrak{P}|\mathfrak{P}_E) = e \\ & & \quad\;\; f(\mathfrak{P}|\mathfrak{P}_E) = 1 \\ & \mathbb{K}_E & \mathfrak{P}_E \\ [\mathbb{K}_E : \mathbb{K}_D] = f & \uparrow & \uparrow \; e(\mathfrak{P}_E|\mathfrak{P}_D) = 1 \\ & & \quad\;\; f(\mathfrak{P}_E|\mathfrak{P}_D) = f \\ & \mathbb{K}_D & \mathfrak{P}_D \\ [\mathbb{K}_D : \mathbb{Q}] = r & \uparrow & \uparrow \; e(\mathfrak{P}_D|P) = 1 \\ & & \quad\;\; f(\mathfrak{P}_D|p) = 1 \\ & \mathbb{Q} & p \end{array}$$

Further, the extension $\mathbb{K}_E/\mathbb{K}_D$ is always cyclic.

The intermediate fields $\mathbb{K}_E$ and $\mathbb{K}_D$, called the inertial and the decomposition field, respectively, depend on the prime $\mathfrak{P}$ and p. For the same p if we choose a different prime $\mathfrak{P}'$ above p then the associated decomposition field and inertia field can be different. Also, the various ramification and inertial degree values given above is specific to the prime pair p and $\mathfrak{P}$. For example: if $\mathfrak{P}'_D$ is another prime in $\mathbb{K}_D$ above p but below a different ideal $\mathfrak{P}'$, then $e(\mathfrak{P}'_D|p)$ and $f(\mathfrak{P}'_D|p)$ may not be equal to 1. But this disparity in values across $\mathfrak{P}$ and $\mathfrak{P}'$ does not occur for the following special case.

Corollary 1: Suppose D is a normal subgroup of $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$. Then p splits into r different primes in $\mathbb{K}_D$. If E is also a normal subgroup in

$\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$, then each of them remains prime in $\mathbb{K}_E$ and finally, each one becomes an eth power in $\mathbb{K}$.

ACKNOWLEDGMENT

The authors are grateful to the reviewers for their comments, which improved the presentation and the contents of this correspondence. They wish to thank E. Viterbo and P. V. Kumar for sending a preprint version of their papers and also thank Prof. C. R. Pradeep, V. Shashidhar, and Djordje Tujkovic for the helpful discussions on this topic.

REFERENCES

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

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

[3] O. Tirkkonen and A. Hottinen, "Square-matrix embeddable space–time block codes for complex signal constellations," *IEEE Trans. Inf. Theory*, vol. 48, no. 2, pp. 384–395, Feb. 2002.

[4] A. Shokrollahi, B. Hassibi, B. Hochwald, and W. Sweldens, "Representation theory for high-rate multiple-antenna code design," *IEEE Trans. Inf. Theory*, vol. 47, no. 6, pp. 2335–2367, Sep. 2001.

[5] B. Hughes, "Optimal space–time constellations from groups," *IEEE Trans. Inf. Theory*, vol. 49, no. 2, pp. 401–410, Feb. 2003.

[6] ——, "Differential space-time modulation," *IEEE Trans. Inf. Theory*, vol. 46, no. 7, pp. 2567–2578, Nov. 2000.

[7] M. Damen, K. Abed-Meraim, and J.-C. Belfiore, "Diagonal algebraic space–time block codes," *IEEE Trans. Inf. Theory*, vol. 48, no. 3, pp. 628–636, Mar. 2002.

[8] M. Damen, A. Tewfik, and J.-C. Belfiore, "A construction of a space-time code based on number theory," *IEEE Trans. Inf. Theory*, vol. 48, no. 3, pp. 753–760, Mar. 2002.

[9] B. A. Sethuraman, B. S. Rajan, and V. Shashidhar, "Full-diversity, high-rate space-time block codes from division algebras," *IEEE Trans. Inf. Theory*, vol. 49, no. 10, pp. 2596–2616, Oct. 2003.

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

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

[12] G. J. Foschini, "Layered space-time architecture for wireless communications in a fading environment when using multi-element antennas," *Bell Labs. Tech. J.*, vol. 1, no. 2, pp. 41–59, 1996.

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

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

[15] H. Yao and G. Wornell, "Structured space-time block codes with optimal diversity-multiplexing tradeoff and minimum delay," in *Proc. IEEE Global Telecommunications Conf. (GLOBECOM 2003)*, vol. 4, San Francisco, CA, Dec. 2003, pp. 1–5.

[16] V. Shashidhar, B. S. Rajan, and P. V. Kumar, "STBC's with optimal diversity-multiplexing tradeoff for 2,3 and 4 transmit antennas," in *Proc. IEEE Int. Symp. Information Theory*, Chicago, IL, Jun./Jul. 2004, p. 125.

[17] ——, "Asymptotic-information-lossless designs and diversity-multiplexing tradeoff," in *Proc. IEEE Global Telecommunications Conf. (GLOBECOM 2004), Communication Theory Symp.*, Dallas, TX, Nov./Dec. 2004.

[18] H. El Gamal, G. Caire, and M. Damen, "Lattice coding and decoding achieve the optimal diversity-multiplexing tradeoff of MIMO channels," *IEEE Trans. Inf. Theory*, vol. 50, pp. 968–985, Jun. 2004.

[19] J. Belfiore, G. Rekaya, and E. Viterbo, "The golden code: A 2×2 full-rate space-time code with nonvanishing determinants," in *Proc. IEEE Int. Symp. Information Theory*, Chicago, IL, Jun./Jul. 2004, p. 308.

[20] P. Elia, P. V. Kumar, S. Pawar, K. R. Kumar, B. S. Rajan, and H. Lu, "Diversity-multiplexing tradeoff analysis of a few algebraic space-time constructions," in *Proc. 42nd Allerton Conf. Communications, Control and Computing*, Monticello, IL, Sep./Oct. 2004.

[21] J. Belfiore and G. Rekaya, "Quaternionic lattices for space-time coding," in *Proc. Information Theory Workshop*, Paris, France, Mar./Apr. 2003.

[22] G. Rekaya, J. Belfiore, and E. Viterbo, "Algebraic 3×3, 4×4 and 6×6 space-time codes with nonvanishing determinants," in *Proc. IEEE Int. Symp. Information Theory and its Applications (ISITA)*, Parma, Italy, Oct. 2004, pp. 325–329.

[23] V. Shashidhar, B. S. Rajan, and B. A. Sethuraman, "STBC's using capacity achieving designs from cyclic division algebras," in *Proc. IEEE Global Telecommunications Conf. (GLOBECOM 2003), Communication Theory Symp.*, vol. 4, San Francisco, CA, Dec. 2003, pp. 1957–1962.

[24] D. N. C. Tse and P. Viswanath, *Fundamentals of Wireless Communication*. New York: Cambridge Univ. Press, to be published.

[25] P. Elia, K. R. Kumar, S. Pawar, P. V. Kumar, and H. Lu, "Explicit, minimum-delay space-time codes achieving the diversity-multiplexing gain tradeoff," *IEEE Trans. Inf. Theory*. [Online]. Available http://ece.iisc.ernet.in/~vijay, submitted for publication.

[26] D. Ionescu, "New results on space-time code design criteria," in *Proc. Wireless Communications and Networking Conf. (WCNC 1999)*, vol. 2, New Orleans, LA, Sep. 1999, pp. 684–687.

[27] ——, "On space-time code design," *IEEE Trans. Wireless Commun.*, vol. 2, no. 1, pp. 20–28, Jan. 2003.

[28] Z. Chen, J. Yuan, and B. Vucetic, "Improved space-time trellis coded modulation scheme on slow rayleigh fading channels," *Electron. Lett.*, vol. 37, no. 7, pp. 440–441, Mar. 2001.

[29] J. Geng, M. Vajapeyam, and U. Mitra, "Distance spectrum of space-time block codes: A union bound point of view," in *Proc. 36th Asilomar Conf. Signals, Systems and Computers*, vol. 2, Monticello, IL, Nov. 2002, pp. 1132–1136.

[30] R. S. Pierce, *Associative Algebras (Graduate Texts in Mathematics)*. New York: Springer-Verlag, 1982.

[31] F. Oggier, G. Rekaya, J.-C Belfiore, and E. Viterbo, "Perfect space- time block codes," *IEEE Trans. Inf. Theory*. [Online]. Available http://www.comelec.enst.fr/belfiore/publi.html, submitted for publication.

[32] D. A. Marcus, *Number Fields (Universitext)*. New York: Springer-Verlag, 1977.

[33] M. Artin, *Algebra, 3rd Indian Reprint*. New Delhi, India: Prentice-Hall of India Pvt. Ltd., 1996.

[34] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*. New Delhi, India: Springer-Verlag, 2004.