A UNIFIED FRAMEWORK FOR CONSTRUCTING DMT-OPTIMAL FAST-DECODABLE CODES FOR N RELAYS*

C. HOLLANTI† AND N. MARKIN‡

Abstract. In this paper, we give a general construction for DMT-optimal fast-decodable lattice codes for the nonorthogonal amplify-and-forward (NAF) [1], [2] multiple-input multiple-output (MIMO) channel. The constructions are based on quaternion division algebras. When satisfying certain properties, these algebras provide us with codes whose structure naturally reduces the decoding complexity. The proposed codes are also suitable for the parallel MIMO channel.

Key words. Amplify-and-forward, complexity, distributed space-time codes, division algebras, DMT, fast-decodable, lattices, less than minimum delay, MIMO, NAF protocol, QR decomposition, quaternion algebras, relay, sphere decoder.

AMS subject classifications. 16H05, 11R52, 94B75

1. Introduction.

The quality of wireless long distance communications can be significantly improved by using cooperative diversity techniques. Cooperating relays can be positioned between the source station and the destination to aid the transmission by either amplifying and forwarding (AF) or decoding and forwarding (DF) the signal. Spatially separated terminals will allow an increment in the diversity in a distributed manner. Depending on the application, a one-hop or multi-hop transmission is called for. Here, we consider multi-hop distributed space-time codes employing a half-duplex NAF protocol [1], [2]. It is known [2] that the NAF protocol outperforms all other AF protocols since, as opposed to orthogonal protocols, it can keep transmitting also during the transmission of the relays. In addition, the AF protocols are less complex than the DF protocols. This type of low cost relay systems are called for in *e.g.* digital video broadcasting (DVB) [6].

In [3, 4] and [5], Yang *et al.* and Hollanti *et al.* proposed block-diagonal space-time code constructions for the asymmetric MIMO channel with or without relays. The constructions arise from cyclic division algebras constructed over a higher degree center. A nonvanishing determinant (NVD) is then achieved by forming a block-diagonal matrix consisting of the left regular representation of the algebra and its Galois conjugates from the center to the base field. It was also shown [4, Theorem 4] that a block-diagonal structure together with the NVD property is enough to achieve the diversity-multiplexing gain tradeoff (DMT) of a relay MIMO NAF channel also in the asymmetric case, where the number of transmit antennas is strictly bigger than the number of receive antennas, and hence the corresponding lattice is not full. Motivated by this and the urge for complexity reduction of MIMO codes in general, we impose further properties that the algebras and the constructions should satisfy in order to reduce the complexity. This paper can be seen as a generalization to [7].

Related work has been carried out by, among others, Rajan *et al.* (see e.g. [8]). They considered fast-decodable distributed space-time codes arising from Clifford

*The research of C. Hollanti is supported by the Emil Aaltonen Foundation's Young Researcher's Project, and by the Academy of Finland grant #131745.
N. Markin's work was supported by the Singapore National Research Foundation under Research Grant NRF-CRP2-2007-03.

†C. Hollanti is with the Aalto University, Department of Mathematics and System Ananlysis, P.O.Box 11100, FI-00076 Aalto, Finland. camilla.hollanti@aalto.fi.

‡N. Markin is with the Nanyang Technological University, School of Phys. and Math. Sciences, 21 Nanyang Link, Singapore 637371. nadyaomarkin@gmail.com

algebras. Our work differs from theirs in that our codes achieve the NVD property and hence the DMT of the asymmetric relay NAF channel. The codes proposed in this paper moreover have a nice algebraic structure which makes analyzing the codes easier in general. Let us finish this introductory section by giving a couple essential definitions.

DEFINITION 1.1. *If the code $\mathcal{C}$ consisting of matrices X satisfies*

$$\min_{0\neq X\in\mathcal{C}} \det(X^\dagger X) > \kappa > 0,$$

we say that $\mathcal{C}$ has the nonvanishing determinant property *(NVD). In case of square matrices, we simply refer to* $\det(X)$ *when talking about NVD.*

There are multiple definitions of rate, but we will consistently use the following.

DEFINITION 1.2. *Let $B_1,\dots,B_k \in M_{n_t\times T}(\mathbb{C})$ be the generator matrices (over $\mathbb{R}$) of a rank k code $\mathcal{C}$ with n_t transmit antennas, so*

$$\mathcal{C} = \sum_{i=1}^{k} B_i g_i,$$

where $g_i \in \mathbb{Z}$, e.g. *PAM symbols. The* rate R *of the code is then*

$$R = k/T$$

(real) dimensions per channel use (dpcu).

Note that the commonly used rate in complex dimensions per channel use is $R/2$ when using the above notation.

2. System model for the NAF relay channel. For ease of notation, we only define the single-relay model, the generalization to multi-hop is straightforward. Following [3], let us denote by X_i the signals transmitted from the source, and by Y_r the signal received by the relay which the relay then amplifies and forwards as BY_r. The number of relays and the number of antennas at the source, relays and destination are denoted by N, n_s, n_r, n_d, respectively. We assume n_r is the same for all relays $r = 1,\dots,N$. Note that we then have $n_t = N(n_s + n_r)$. To be realistic, we assume $n_s \geq n_r$. The destination is observing Y_1 and Y_2 in consecutive time instances, and we have

$$\begin{aligned} Y_1 &= \sqrt{\pi_1\, SNR}\, F X_1 + V_1 \\ Y_r &= \sqrt{\pi_1 \rho\, SNR}\, H X_1 + W \\ Y_2 &= \sqrt{\pi_3\, SNR}\, G(BY_r) + \sqrt{\pi_2\, SNR}\, F X_2 + V_2, \end{aligned}$$

where V_i, W are the additive white gaussian noise matrices and F, H, G are the Rayleigh distributed channel matrices. The power allocation π_i factors are chosen so that SNR denotes the received SNR per receive antenna at the destination. We assume perfect channel state information (CSI) at the receivers, while the transmitters have none.

The above channel model can be equivalently presented as a virtual (vectorized) single-user MIMO channel, so the channel to be considered in the actual code construction becomes the typical one with

$$y = \sqrt{SNR}\, \tilde{H} x + z,$$

where the $\tilde{H}$ has a specific structure arising from the different relay paths, and z represents the noise. For more details on this equivalent virtual channel, we refer to [3].

We can now formulate:

The code construction problem: It was shown in [4, Theorem 4] that a DMT-optimal code for the NAF MIMO channel can be constructed from a block-diagonal single-user code that has a suitable rate. To this we add the requirement of fast decodability, *i.e.*, we moreover want the equivalent channel matrix $\tilde{H}$ to result in a specific R-matrix structure when the QR-decomposition is performed on $\tilde{H}$. To this end, let us define what we mean by fast-decodability and, in particular, by *(conditional) g-group decodability.*

DEFINITION 2.1 ([9]). *A space-time code is said to be* fast-decodable *if its R matrix has the following form:*

$$R = \begin{bmatrix} \Delta & B_1 \\ 0 & R_2 \end{bmatrix},$$

where Δ is a diagonal matrix and R_2 is upper-triangular.

The authors of [9] give criteria when the zero structure of R coincides with that of M, where M is a matrix capturing information about orthogonality relations of the basis elements of B_i:

$$M_{k,l} = ||B_k^\dagger B_l + B_l^\dagger B_k||_F. \tag{2.1}$$

In particular, [9, Lemma 2] shows that if M has the structure $M = \begin{bmatrix} \Delta & B_1 \\ B_2 & B_3 \end{bmatrix}$, where Δ is diagonal, then $R = \begin{bmatrix} \Delta & B_1 \\ 0 & R_1 \end{bmatrix}$. We could thus rephrase Defnition 2.1 in terms of M.

DEFINITION 2.2. *A space-time code of dimension K is called* g-group decodable *if there exists a partition of $\{1, \ldots, K\}$ into g nonempty subsets $\mathcal{J}_1, \ldots, \mathcal{J}_g$, so that the matrix $M_{l,k} = 0$ when l, k are in disjoint subsets $\mathcal{J}_i, \mathcal{J}_j$.* In this case, as shown in [9], the matrix R has the form

$$R = \begin{bmatrix} R_1 & 0 & 0 \\ 0 & \cdots & 0 \\ 0 & 0 & R_g \end{bmatrix},$$

where each R_i is a square upper triangular matrix. Hence, the symbols x_k and x_l can be decoded independently when their corresponding basis matrices B_k and B_l belong to disjoint subsets of the partition.

DEFINITION 2.3. *Recall from [10] that a code is called* conditionally g-group decodable *if there exists a partition of the indices $\{1, \ldots, K\}$ of basis elements into $g+1$ disjoint subsets $\mathcal{J}_1$, ..., $\mathcal{J}_g$, $\mathcal{J}^C$ such that*

$$\|B_l^\dagger B_m + B_m^\dagger B_l\|_F = 0 \quad \forall l \in \mathcal{J}_i, \forall m \in \mathcal{J}_j, i \neq j.$$

In this case, the sphere decoding complexity order reduces to $|S|^{|\mathcal{J}^C| + \max_{1 \leq i \leq g} |\mathcal{J}_i|}$.

REMARK 1. *Note that a simple computation shows that the zero structure of M is stable under premultiplication of B_i by a channel matrix H. In general, the same does not hold for R.*

By the above discussion, in order to demonstrate fast-decodability (resp. (conditional) g-group decodability), it suffices to find an ordering on the basis elements B_i, which results in the desired zero structure of M.

3. General framework for constructing fast-decodable N-relay codes for $n_s = n_r = 1$ and $n_d \geq 2$. Let us consider the following tower of subfields of a quaternion division algebra $Q = (-a, -b)$. Methods for checking whether a certain quaternion algebra is division can be found in [11]. We assume that θ is totally real and that K' includes a totally imaginary number field $K = \mathbb{Q}(\sqrt{-m})$ for some square free $m \in \mathbb{Z}_+$.

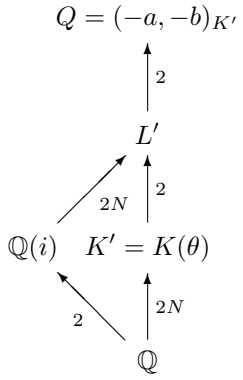


FIG. 3.1. *Quaternion construction.*

We will next prove that the rate four codes we obtain are conditionally 4-group decodable and have NVD. In the proposition, we assume Q is division to start with. Techniques for construction a division quaternion algebra can be found in [11], see especially [11, Theorem 7.1].

PROPOSITION 3.1. *Define the code*

$$\mathcal{C} = \{\alpha_\tau(X)\} = \left\{ \begin{bmatrix} X & 0 & \cdots & 0 \\ 0 & \tau(X) & \cdots & 0 \\ & & \ddots & \\ 0 & \cdots & 0 & \tau^{N-1}(X) \end{bmatrix}, X \in \psi(\Lambda) \right\},$$

where $X = \psi(x)$ is the left regular matrix representation of an element x from an order Λ of the quaternion division algebra $Q = (-a, -b)_{K'}$, suitably conjugated for energy balance. The conjugation does not affect NVD but does actually aid fast-decodability. More precisely,

$$X = \begin{bmatrix} c & -\sqrt{b}\sigma(d) \\ \sqrt{b}d & \sigma(c) \end{bmatrix},$$

with $c, d \in \mathcal{O}_{L'}$, $\sigma : i \mapsto -i$ and $\langle\tau\rangle = \mathrm{Gal}(K'/K)$.

Then the code $\mathcal{C}$ is of rank $8N$ giving it rate four (real dimensions per channel use). The code has the NVD property and is hence DMT-optimal (cf. [4, Theorem 4]). There further exists an ordering of the basis matrices such that the decoding complexity is $|S|^{5N}$, where S is the underlying PAM alphabet, hence reducing the decoding cost by 37.5% as opposed to the worst-case sphere decoding complexity $|S|^{8N}$.

Proof. Let $K = \mathbb{Q}(\sqrt{-m})$, $K' = K(\theta)$ (cf. Fig. 3). To simplify the notation, assume K' has an integral power basis $\{1, \theta, \ldots, \theta^{N-1}\}$ over K. Firstly, Q has the following K'-basis:

$$\left\{ q_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, q_2 = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, q_3 = \begin{bmatrix} 0 & \sqrt{b}i \\ \sqrt{b}i & 0 \end{bmatrix}, q_4 = \begin{bmatrix} 0 & -\sqrt{b} \\ \sqrt{b} & 0 \end{bmatrix} \right\}.$$

Secondly, this means that Q is generated over $K = \mathbb{Q}(\sqrt{-m})$ by the following $4N$ matrices:

$$\Gamma_{i,1} = q_i, \Gamma_{i,2} = q_i(\theta), \ldots, \Gamma_{i,N} = q_i(\theta^{N-1})$$

for $i = 1, \ldots, 4$. Next, we extend this to a $\mathbb{Q}$-basis by letting $\Gamma_{i,j} = \sqrt{-m}\Gamma_{i-4,j}$ for $i = 5, \ldots, 8$. Then a $\mathbb{Z}$-basis of $\mathcal{C}$ can be given by

$$\{\alpha_\tau(\Gamma_{i,j})\}_{1 \le i \le 8, 1 \le j \le N} \tag{3.1}$$

and is of size $8N$. Indeed, the rank of $\mathcal{C}$ is $8N$, since each codeword X is an element of quaternion algebra $(-a, -b)_{K'}$, and hence encodes 4 symbols from $K' = \mathbb{Q}(\zeta_7)$ which, for its part, is of degree $2N$ over $\mathbb{Q}$.

Now let τ be a generator of $\mathrm{Gal}(K'/K)$. When the coefficients of codewords are from the ring of algebraic integers $\mathcal{O}'_L$ of L', the code is NVD. This follows from the fact that

$$\det(X') = \prod_{i=0}^{N-1} \det(\tau^i(X)) = \prod_{i=0}^{N-1} \tau^i(\det(X))) = N_{K'/K}(\det(X)) \in \mathcal{O}_K,$$

since, being the reduced norm of an order element (cf. [12, Prop. 3.3]), $\det(X) \in \mathcal{O}_{K'}$. The field K being an imaginary quadratic field then gives us $\det(X') \ge 1$ (remember Q is division). We remark that this proof is along the same lines as its correspondents in [4, 5].

Finally, we show that $\mathcal{C}$ is conditionally 4-group decodable with complexity $|S|^{5N}$; conditioned on decoding symbols corresponding to $\{\Gamma_{5,1}, \ldots, \Gamma_{8,N}\}$, the complexity of decoding symbols corresponding to $\{\Gamma_{1,1}, \ldots, \Gamma_{4,N}\}$ is at most $|S|^N$, where S is the underlying real alphabet. For that, note that when $A = \Gamma_{i,j}, B = \Gamma_{i',j'}$, for all j, j' and for $i \neq i'$, we have

$$AB^\dagger + BA^\dagger = \mathbf{0}.$$

Same follows for $\alpha_\tau(A), \alpha_\tau(B)$, *i.e.*, we have:

$$\alpha_\tau(A)\alpha_\tau(B)^\dagger + \alpha_\tau(B)\alpha_\tau(A)^\dagger = \mathbf{0}.$$

Let $\Gamma = [\alpha_\tau(\Gamma_{1,1}), \ldots, \alpha_\tau(\Gamma_{8,N})]$ be the list of $8N$ generators of $\mathcal{C}$ from (3.1) in lexicographical order. Then the matrix $M = M_{i,j}$ from Equation (2.1) capturing orthogonality relations on Γ has the following structure:

$$M = \begin{bmatrix} * & 0 & 0 & 0 & * & * & * & * \\ 0 & * & 0 & 0 & * & * & * & * \\ 0 & 0 & * & 0 & * & * & * & * \\ 0 & 0 & 0 & * & * & * & * & * \\ * & * & * & * & * & * & * & * \\ * & * & * & * & * & * & * & * \\ * & * & * & * & * & * & * & * \\ * & * & * & * & * & * & * & * \end{bmatrix} \tag{3.2}$$

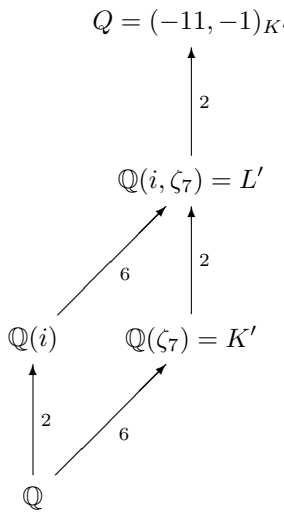
where each coefficient of the matrix above is an $N \times N$ matrix, which is $\mathbf{0}$ when the coefficient is 0. That is, the code is conditionally 4-group decodable (cf. Def. 2.3) with complexity $4N \cdot N = 5N$. □

4. Explicit construction for $N = 3$ relays. For illustration, we repeat here the construction proposed in [7].

Let us consider the quaternion algebra $(-11, -1)_{\mathbb{Q}(\zeta_7)}$, which is a division algebra. This follows from the techniques of [11]: we apply [11, Theorem 7.1] while noting that $\mathbb{F}_{11^3}$ contains no element of order 4, *i.e.*, -1 is not a square in $\mathbb{F}_{11^3}$, which is the residue field of the prime 11 in $\mathbb{Q}(\zeta_7)$. We define the relay code

$$\mathcal{C} = \{\alpha_\tau(X)\} = \left\{ \begin{bmatrix} X & 0 & 0 \\ 0 & \tau(X) & 0 \\ 0 & 0 & \tau^2(X) \end{bmatrix} \right\},$$

where X is a matrix of the form $X = \begin{bmatrix} c & -\sqrt{11}\sigma(d) \\ \sqrt{11}d & \sigma(c) \end{bmatrix}$ with $c, d \in \mathbb{Z}(i, \zeta_7)$, $\sigma : i \mapsto -i$, and $\tau : \zeta_7 \mapsto \zeta_7^2$ is the generator of $\mathrm{Gal}(K'/K)$. The code $\mathcal{C}$ is of rank 24 and has (real) decoding complexity $|S|^{15}$. Moreover, it has the NVD property and is therefore DMT-optimal. Following the notation from Fig. 3, we have $K = \mathbb{Q}(\sqrt{-7})$ and $K' = K(\zeta_7 + \zeta_7^{-1})$ as demonstrated by the diagram below.



5. Conclusions and future work. We proposed DMT-optimal relay codes for distributed cooperative communications that are conditionally $4-$group decodable, hence reducing the worst-case sphere decoding complexity by as much as 37.5%. The codes are also suitable for a parallel MIMO channel and have NVD guaranteeing a good coding gain regardless of the constellation size. The codes are suitable for an arbitrary number of relays, however, due to the quaternion algebra structure, they only work with $n_s = n_r = 1$. Future work contains extending the construction methods to an arbitrary number of antennas as well as investigating how the codes perform compared to other distributed codes that either have higher complexity or lack NVD.

REFERENCES

[1] R. Nabar, H. Bolcskei, and F. Kneubuhler, "Fading relay channels: performance limits and space-time signal design," *IEEE Journal on Selected Areas in Communications*, vol. 22, no. 6, pp. 1099 – 1109, aug. 2004.

[2] K. Azarian, H. El Gamal, and P. Schniter, "On the achievable diversity-multiplexing tradeoff in half-duplex cooperative channels," *IEEE Trans. Inf. Theory*, vol. 51, no. 12, pp. 4152 –4172, dec. 2005.

[3] S. Yang and J.-C. Belfiore, "Optimal space-time codes for the MIMO amplify-and-forward cooperative channel," in *International Zürich Seminar on Communications, 2006* , 0-0 2006, pp. 122 –125.

[4] S. Yang and J.-C. Belfiore, "Optimal space-time codes for the MIMO amplify-and-forward cooperative channel," in *IEEE Trans. Inf. Theory*, vol. 53, no. 2, pp. 647–663, 2007.

[5] C. Hollanti and H.-F. Lu, "Construction methods for asymmetric and multi-block space-time codes," *IEEE Trans. Inf. Theory*, vol. 55, no. 3, pp. 1086 – 1103, 2009.

[6] DVB Project, the global standard for digital television, *http://www.dvb.org*.

[7] C. Hollanti and N. Markin, "Algebraic fast-decodable relay codes for distributed communications", *Proc. IEEE Int. Symp. Inform. Theory*, Cambridge, MA, July 2012.

[8] G. Susinder Rajan and B. Sundar Rajan, "Multi-group ML decodable collocated and dis-

tributed space–time block codes," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, July 2010, pp. 3221–3247.

[9] G. R. Jithamithra and B. S. Rajan, "A quadratic form approach to ML decoding complexity of STBCs," preprint available at *arxiv.org/abs/1004.2844*.

[10] L. P. Natarajan and B. S. Rajan, "Fast group-decodable STBCs via codes over GF(4)," *Proc. IEEE Int. Symp. Inform. Theory*, Austin, TX, June 2010.

[11] T. Unger and N. Markin, "Quadratic forms and space-time block codes from generalized quaternion and biquaternion algebras", *IEEE Trans. Inf. Theory*, vol. 57 no. 9, pp. 6148-6156, Sept 2011.

[12] C. Hollanti, J. Lahtonen, and H.-F. Lu, "Maximal orders in the design of dense space-time lattice codes," *IEEE Trans. Inf. Theory*, vol. 54, no.10, pp. 4493–4510, Oct. 2008.