REFERENCES

[1] C. P. M. J. Baggen and L. M. G. M. Tolhuizen, "On diamond codes," *Probl. Inform. Transm.*, vol. 43, pp. 1400–1411, Sept. 1997.
[2] E. R. Berlekamp, "Elongated burst trapping," U.S.Patent 4 916 702, Apr. 10, 1990.
[3] R. E. Blahut, *Theory and Practice of Error Control Codes*. Reading, MA: Addison-Wesley, 1984.
[4] M. Blaum and H. C. A. van Tilborg, "Enhanced decoding of interleaved correcting codes," *Proc. 1995 IEEE Int. Symp. Information Theory*, pp. 412–412, Sept. 1995.
[5] E. L. Blokh and V. V. Zyablov, "Coding of generalized concatenated codes," *Probl. Inform. Transm.*, vol. 10, pp. 218–222, 1974.
[6] H. O. Burton and E. J. Weldon, Jr., "Cyclic product codes," *IEEE Trans. Inform. Theory*, vol. IT-11, pp. 433–439, July 1965.
[7] J. Chen and P. Owsley, "A burst-error-correcting algorithm for Reed-Solomon codes," *IEEE Trans. Inform. Theory*, vol. 38, pp. 1807–1812, Nov. 1992.
[8] D. T. Chi, "A new algorithm for correcting single burst errors with Reed-Solomon codes," *Proc. 1991 IEEE Military Communications Conf.*, pp. 1254–1258, Nov. 1991.
[9] G.-L. Feng and K. K. Tzeng, "A generalization of the Berlekamp–Massey algorithm for multisequence shift-register synthesis with applications to decoding cyclic codes," *IEEE Trans. Inform. Theory*, vol. 37, pp. 1274–1287, Sept. 1991.
[10] G. D. Forney, Jr., *Concatenated Codes*. Cambridge, MA: MIT Press, 1966.
[11] ——, "Burst-correcting codes for the classic bursty channel," *IEEE Trans. Commun. Technol.*, pt. 2, vol. COM-19, pp. 772–781, Oct. 1971.
[12] C. R. P. Hartmann and K. K. Tzeng, "Decoding beyond the BCH bound using multiple sets of syndrome sequences," *IEEE Trans. Inform. Theory*, vol. IT-20, pp. 292–295, Mar. 1974.
[13] S. Hirasawa, M. Kasahara, Y. Sugiyama, and T. Namekawa, "Modified product codes," *IEEE Trans. Inform. Theory*, vol. IT-30, pp. 299–306, Mar. 1984.
[14] V. Y. Krachkovsky and Y. X. Lee, "Decoding for interleaved Reed-Solomon coding schemes," *IEEE Trans. Magn.*, vol. 33, pp. 2740–2743, Sept. 1997.
[15] V. Y. Krachkovsky, Y. X. Lee, and H. K. Garg, "Decoding of parallel RS codes with applications to product and concatenated codes," *Proc. 1998 IEEE Int. Symp. Information Theory*, p. 55, Aug. 1998.
[16] J. Maucher, V. V. Zyablov, and M. Bossert, "On the equivalence of generalized concatenated codes and generalized error location codes," *IEEE Trans. Inform. Theory*, vol. 46, pp. 642–649, Mar. 2000.
[17] T. Narahara, S. Kobayashi, M. Hattori, Y. Shimpuku, G. J. van den Enden, J. A. H. M. Kahlman, M. van Dijk, and R. van Woudenberg, "Optical disc system for digital video recording," *Jpn. J. Appl. Phys.*, pt. 1, vol. 39, no. 2B, pp. 912–919, 2000.
[18] R. M. Roth and G. Seroussi, "Reduced-redundancy product codes for burst error correction," *IEEE Trans. Inform. Theory*, vol. 44, pp. 1395–1406, July 1998.
[19] K. Sakakibara, "Performance analysis of the error-forecasting decoding for interleaved block codes on Gilbert-Eliott channels," *IEEE Trans. Commun.*, vol. 48, pp. 386–395, Mar. 2000.
[20] L. B. Vries and K. Odaka, "CIRC—The error-correcting code for the compact disc digital audio system," in *Collected Papers AES Premiere Conference*. Rye, NY: Audio Eng. Soc., 1982, pp. 177–178.
[21] S. P. Wicker, *Error Control Systems for Digital Communication and Storage*. Englewood-Cliffs, NJ: Prentice Hall, 1995.
[22] J. K. Wolf and B. Elspas, "Error locating codes – A new concept in error control," *IEEE Trans. Inform. Theory*, vol. IT-9, pp. 113–117, Apr. 1963.
[23] J. K. Wolf, "On codes derivable from the tensor product of check matrices," *IEEE Trans. Inform. Theory*, vol. IT-11, pp. 281–284, Apr. 1965.
[24] S. I. Zhegalov, "Linear block codes that correct multiple bursts and independent errors," *Probl. Inform. Transm.*, vol. 13, pp. 54–61, 1977.
[25] V. A. Zinoviev, "Generalized cascade codes," *Probl. Inform. Transm.*, vol. 12, pp. 2–9, 1976.
[26] ——, "Generalized concatenated codes for channels with error bursts and independent errors," *Probl. Inform. Transm.*, vol. 17, pp. 53–56, 1981.
[27] V. A. Zinoviev and V. V. Zyablov, "Correcting bursts and independent errors by generalized concatenated codes," *Probl. Inform. Transm.*, vol. 15, pp. 125–134, 1979.

On the Nonexistence of Rate-One Generalized Complex Orthogonal Designs

Xue-Bin Liang, *Member, IEEE*, and
Xiang-Gen Xia, *Senior Member, IEEE*

***Abstract*—Orthogonal space–time block coding proposed recently by Alamouti [1] and Tarokh, Jafarkhani, and Calderbank [4] is a promising scheme for information transmission over Rayleigh-fading channels using multiple transmit antennas due to its favorable characteristics of having *full* transmit diversity and a *decoupled* maximum-likelihood (ML) decoding algorithm. Tarokh, Jafarkhani, and Calderbank extended the theory of classical orthogonal designs to the theory of generalized, real, or complex, linear processing orthogonal designs and then applied the theory of generalized orthogonal designs to construct space–time block codes (STBCs) with the maximum possible diversity order while having a simple decoding algorithm for any given number of transmit and receive antennas. It has been known that the STBCs constructed in this way can achieve the maximum possible rate of one for *every number* of transmit antennas using any arbitrary *real* constellation and for *two* transmit antennas using any arbitrary *complex* constellation. Contrary to this, in this correspondence we prove that there does *not* exist rate-one STBC from generalized complex linear processing orthogonal designs for *more than two* transmit antennas using any arbitrary *complex* constellation.**

***Index Terms*—Alamouti scheme, complex orthogonal designs, full rate, generalized complex orthogonal designs, Hurwitz–Radon theory, orthogonal designs, space–time block codes (STBCs), transmit diversity.**

I. INTRODUCTION

In the recent paper [4], Tarokh, Jafarkhani, and Calderbank proposed a new scheme, termed "space–time block coding," for transmission over wireless Rayleigh-fading channels using multiple transmit antennas. This approach can be thought of as a generalization of the Alamouti scheme [1], which allows transmission using two transmit antennas, to an arbitrary number of transmit antennas. From the perspective of transmission with multiple transmit antennas, Tarokh, Jafarkhani, and Calderbank [4] established a theoretical framework of generalized orthogonal designs based on the theory of classical orthogonal designs and then employed their theory of generalized orthogonal designs to construct space-time block codes (STBCs) for any given number of transmit antennas. Due to the underlying orthogonal and decoupled structure of STBCs, they possess full diversity order and a decoupled maximum-likelihood (ML) decoding algorithm which avoids the exponential complexity of the ML decoding, in terms of the number of transmitted information symbols within the given decoding delay, at the receiver.

In [4], Tarokh, Jafarkhani, and Calderbank first demonstrated that the theory of classical orthogonal designs can be used as codes for multiple-antenna wireless communications systems, which have full transmit diversity and have a fast ML decoding algorithm at the receiver. However, according to Radon's classical results [2] on

Manuscript received March 13, 2001; revised June 20, 2003. This work was supported in part by the Air Force Office of Scientific Research under Grants F49620-00-1-0086 and F49620-02-1-0157, and the National Science Foundation under Grants MIP-9703377 and CCR-0097240.

X.-B. Liang is with the Department of Electrical and Computer Engineering, Louisiana State University, Baton Rouge, LA 70803 USA (e-mail: xbliang@ee.lsu.edu).

X.-G. Xia is with the Department of Electrical and Computer Engineering, University of Delaware, Newark, DE 19716 USA (e-mail: xxia@ee.udel.edu).

Communicated by R. Urbanke, Associate Editor for Coding Techniques.
Digital Object Identifier 10.1109/TIT.2003.818396

real square orthogonal designs, these designs only exist in the set of dimensions $1, 2, 4,$ and 8. Then, in [4], the authors extended Radon's results to both rectangular and complex orthogonal designs. They showed that there exist full-rate generalized real orthogonal designs for any given number of transmit antennas. Therefore, the STBCs from generalized real orthogonal designs can achieve the maximum possible rate for any given number of transmit antennas using any arbitrary real constellations such as pulse-amplitude modulation (PAM). Subsequently, in [4], the authors extended these schemes from real signal constellations to complex signal constellations such as phase-shift keying (PSK) and quadrature-amplitude modulation (QAM). They introduced the concepts of *generalized complex linear processing orthogonal design* and its *rate* as the ratio of the number of transmitted information symbols to the decoding delay of these symbols at the receiver for any given number of transmit antennas using any complex signal constellations. The STBCs constructed from generalized complex linear processing orthogonal designs were shown to have full transmit diversity and a simple decoupled ML decoding algorithm. If the STBCs from the generalized complex linear processing orthogonal designs can achieve full rate, namely, one, then the codes have no loss in bandwidth in the sense that the STBCs can provide the maximum possible transmission rate at full diversity (see [4] and [3, Corollay 3.3.1, p. 756]). The complex orthogonal design in dimension 2, i.e., the Alamouti scheme for transmission with two antennas [1], is such an example of rate-one design. Therefore, a natural question arises whether or not there exist rate-one generalized *complex* linear processing orthogonal designs for transmission with more than two antennas.

In this correspondence, we prove that there does *not* exist any rate-one generalized complex linear processing orthogonal design for more than two transmit antennas, irrespective of any amount of decoding delay allowed at the receiver. This nonexistence result is in sharp contrast to the existence of rate-one generalized *real* orthogonal designs for any given number of transmit antennas and rate-one complex orthogonal designs for two transmit antennas.

II. Nonexistence of Rate-One STBCs for Transmission With More Than Two Antennas Using Any Arbitrary Complex Constellation

In this section, we will present some preliminaries about the STBCs based on the theory of generalized orthogonal designs established in [4] and then give the main nonexistence result of rate-one STBCs for more than two transmit antennas using any arbitrary complex signal constellation.

A. STBCs From Generalized Complex Linear Processing Orthogonal Designs

The following preliminaries in the theory of generalized orthogonal designs are adopted from [4] and its minor correction [5] but stated here in a compact way.

A *real orthogonal design* $\mathcal{O}$ of size n is an $n \times n$ matrix whose nonzero entries are the indeterminates $x_1, x_2, \ldots, x_n$ over the real field $\mathbb{R}$ or their negative $-x_1, -x_2, \ldots, -x_n$ such that

$$\mathcal{O}^{\mathsf{T}}\mathcal{O} = (x_1^2 + x_2^2 + \cdots + x_n^2) I_{n\times n}$$

where the superscript T represents the transpose of a matrix and $I_{n\times n}$ is the $n \times n$ identity matrix. Radon [2] provided a complete answer to the existence problem of such an orthogonal design, i.e., that the real orthogonal design $\mathcal{O}$ of size n exists if and only if the dimension n is $1, 2, 4,$ or 8.

A *generalized real orthogonal design* $\mathcal{G}$ of size n is a $p \times n$ matrix with entries

$$0, x_1, x_2, \ldots, x_k, -x_1, -x_2, \ldots, -x_k$$

where $x_1, x_2, \ldots, x_k$ are indeterminates over $\mathbb{R}$, satisfying

$$\mathcal{G}^{\mathsf{T}}\mathcal{G} = (x_1^2 + x_2^2 + \cdots + x_k^2) I_{n\times n}.$$

The rate of $\mathcal{G}$ is defined as $R = k/p$.

It has been shown in [4] that, for any given number n of transmit antennas, there exists a rate-one $p \times n$ generalized real orthogonal design with the smallest possible decoding delay p depending only upon n (see [4, Corollary 4.1.2, p. 1461]). The STBCs from this full-rate generalized orthogonal design have entries of the form $x_1, x_2, \ldots, x_p, -x_1, -x_2, \ldots, -x_p$.

A *complex orthogonal design* $\mathcal{O}_c$ of size n is an $n \times n$ matrix whose nonzero entries are

$$x_1, x_2, \ldots, x_n, -x_1, -x_2, \ldots, -x_n$$

or their conjugates

$$x_1^*, x_2^*, \ldots, x_n^*, -x_1^*, -x_2^*, \ldots, -x_n^*$$

or the products of the above ones with $\boldsymbol{j} \overset{\text{def}}{=} \sqrt{-1}$, the imaginary unit in the complex field $\mathbb{C}$, where $x_1, x_2, \ldots, x_n$ are indeterminates over $\mathbb{C}$, satisfying

$$\mathcal{O}_c^{\mathsf{H}}\mathcal{O}_c = (|x_1|^2 + |x_2|^2 + \cdots + |x_n|^2) I_{n\times n}$$

where the superscript H represents the Hermitian transpose or complex conjugate transpose of a complex matrix.

The Alamouti scheme [1] for transmission with double transmit antennas employed the following 2×2 complex orthogonal design

$$\begin{pmatrix} x_1 & x_2 \\ -x_2^* & x_1^* \end{pmatrix}.$$

However, it was proved in [4] that a complex orthogonal design $\mathcal{O}_c$ of size n exists only when the dimension n is 1 or 2. This conclusion remains true even if the complex linear processing is allowed at the transmitter in the sense that the entries of the complex orthogonal designs can be complex linear combinations of the complex variables $x_1, x_2, \ldots, x_n$ and their conjugates $x_1^*, x_2^*, \ldots, x_n^*$ (see [4, Theorem 5.4.2, p. 1463]). Such an orthogonal design is called a *complex linear processing orthogonal design*.

A *generalized complex orthogonal design* $\mathcal{G}_c$ of size n is a $p \times n$ matrix with entries

$$0, x_1, x_2, \ldots, x_k, -x_1, -x_2, \ldots, -x_k$$

or their conjugates by ignoring the zero

$$x_1^*, x_2^*, \ldots, x_k^*, -x_1^*, -x_2^*, \ldots, -x_k^*$$

or the products of the above ones with the imaginary unit $\boldsymbol{j}$, where $x_1, x_2, \ldots, x_k$ are indeterminates over $\mathbb{C}$, satisfying

$$\mathcal{G}_c^{\mathsf{H}}\mathcal{G}_c = (|x_1|^2 + |x_2|^2 + \cdots + |x_k|^2) I_{n\times n}.$$

Furthermore, if the complex linear processing is allowed at the transmitter, i.e., that the entries of $\mathcal{G}_c$ are relaxed to be complex linear combinations of the complex variables $x_1, x_2, \ldots, x_k$ and their conjugates $x_1^*, x_2^*, \ldots, x_k^*$, then the design $\mathcal{G}_c$ is called a *generalized complex linear processing orthogonal design*. The rate of $\mathcal{G}_c$ is defined as $R = k/p$.

As an illustrative example, we present a family of *generalized complex orthogonal designs* with a special recursive structure for all $n \geq 1$ transmit antennas as follows.

Let $\mathcal{S}_1 = (x_1)$ and

$$\mathcal{S}_2 = \begin{pmatrix} x_1 & x_2 \\ -x_2^* & x_1^* \end{pmatrix}$$

be the first two generalized complex orthogonal designs for a single and two transmit antennas, respectively. For all $n \geq 1$, let

$$p = p_n \stackrel{\text{def}}{=} n(n-1)/2 + 1.$$

We can define the $p \times n$ matrix $\mathcal{S}_n$ for all $n \geq 3$ in the following recursive way:

$$\mathcal{S}_{n+1} = \left(\begin{array}{c|c} \mathcal{S}_n & \begin{matrix} x_{n+1} \\ 0 \\ \vdots \\ 0 \end{matrix} \\ \hline -x_{n+1}^* I_{n \times n} & \begin{matrix} x_1^* \\ x_2^* \\ \vdots \\ x_n^* \end{matrix} \end{array}\right), \qquad \text{for } n = 2, 3, \ldots$$

where $x_1, x_2, \ldots, x_n$ are indeterminates over $\mathbb{C}$ and in the last column of $\mathcal{S}_{n+1}$ there are $p_n - 1$ zero entries between x_{n+1} and x_1^*. Then, the $p \times n$ matrix $\mathcal{S}_n$ for all $n \geq 1$ recursively defined above is a generalized complex orthogonal design satisfying

$$\mathcal{S}_n^{\mathsf{H}} \mathcal{S}_n = (|x_1|^2 + |x_2|^2 + \cdots + |x_n|^2) I_{n \times n}$$

for which the proof is given in Appendix A. It is seen that the rate of the generalized complex orthogonal design $\mathcal{S}_n$ for $n \geq 1$ transmit antennas is $R = n/p_n = 2n/(n^2 - n + 2)$.

Tarokh, Jafarkhani, and Calderbank [4] demonstrated that the STBCs from generalized complex linear processing orthogonal designs can achieve full diversity order and have a simple decoupled ML decoding algorithm which is based only on linear processing at the receiver. It is the remarkable merit of the STBCs constructed in this way that renders the space–time block coding a preferable scheme for information transmission over wireless fading channels with multiple transmit antennas. Clearly, a fundamental and challenging task in STBCs within the theoretical framework of generalized orthogonal designs is to construct high-rate generalized complex linear processing orthogonal designs while taking into account the minimization of the decoding delay at the receiver for any given number of transmit antennas.

According to the above discussion, there exist rate-one generalized real orthogonal designs for any given number of transmit antennas and rate-one complex orthogonal design for two transmit antennas. However, it remains unknown whether or not there exists a rate-one generalized complex linear processing orthogonal design for more than two transmit antennas. Our main result in the current correspondence is that *no* such rate-one generalized complex orthogonal design exist for more than two transmit antennas, irrespective of the amount of decoding delay allowed at the receiver, as demonstrated in the following.

B. A Nonexistence Result of Rate-One STBCs for More Than Two Transmit Antennas Using Complex Constellations

The main result in this correspondence is Theorem 1, the proof of which is placed at the end of this section.

Theorem 1: Let $p \geq n \geq 3$ and $\mathcal{E}_c$ be a $p \times n$ matrix whose entries are the complex linear combinations of the complex variables $x_1, x_2, \ldots, x_k$ and their conjugates $x_1^*, x_2^*, \ldots, x_k^*$. If there exist $n \times n$ positive diagonal matrices $D_1, D_2, \ldots, D_k$ such that

$$\mathcal{E}_c^{\mathsf{H}} \mathcal{E}_c = |x_1|^2 D_1 + |x_2|^2 D_2 + \cdots + |x_k|^2 D_k \tag{1}$$

then we have

$$k \leq p - 1. \tag{2}$$

By setting $D_1 = D_2 = \cdots = D_k = I_{n \times n}$ in Theorem 1, we know that there do *not* exist rate-one generalized complex linear processing orthogonal designs for more than two transmit antennas. In particular, by setting $p = n = k$, it is seen that *no* complex linear processing orthogonal design exists for more than two transmit antennas, which coincides with the result obtained in [4, Theorem 5.4.2, p. 1463]. Theorem 1 indicates further that no rate-one STBCs exist within the theoretical framework of generalized orthogonal designs for more than two transmit antennas using complex constellations even if the complex linear processing at the transmitter and *any* amount of decoding delay $p \geq n \geq 3$ at the receiver are allowed. In other words, the result obtained in [4, Theorem 5.4.2, p. 1463] only implies the nonexistence of rate-one complex *square* $(p = n \geq 3)$ orthogonal designs for more than two transmit antennas, while Theorem 1 demonstrates that any rate-one generalized complex orthogonal design for more than two transmit antennas is nonexistent irrespective of whether the generalized complex orthogonal design itself is *square or rectangular* $(p \geq n \geq 3)$.

It is worth noting that, in the context of STBCs based on the theory of generalized orthogonal designs, the inequality (2) provides an upper bound on the number k of information symbols which can be transmitted within the decoding delay p using $n \geq 3$ transmit antennas, i.e., $k \leq p - 1$. In [4], two STBCs of rate $R = k/p = 3/4$ were constructed from generalized complex linear processing orthogonal designs for $p \times n = 4 \times 3$ and 4×4, respectively, where in both cases we have $k = 3$. Therefore, the above upper bound is *reached* when $p = 4$ and $n = 3$ or 4, i.e., $k = p - 1 = 3$. Consequently, we have the following.

Corollary 1: The rate $R = 3/4$ is the highest possible rate of STBCs from generalized complex linear processing orthogonal designs for three and four transmit antennas given the decoding delay of four, i.e., $p = 4$, at the receiver.

We would like to mention that the $p \times n$ matrix $\mathcal{E}_c$ with the property (1) given in Theorem 1 was originally proposed in [4] within the theoretical framework of generalized orthogonal designs. If the positive diagonal matrices $D_1, D_2, \ldots, D_k$ in Theorem 1 are equal, then $\mathcal{E}_c$ can be reduced by a linear transformation to a generalized complex linear processing orthogonal design $\mathcal{G}_c$ as previously defined (see [5]).

C. Proof of Theorem 1

The following lemma is crucial in our proof.

Lemma 1: Let A, B, and C be three $m \times m$ $(m \geq 1)$ complex constant matrices. For any m-dimensional complex-variable vector $x = (x_1, x_2, \ldots, x_m)^{\mathsf{T}} \in \mathbb{C}^m$, we denote its conjugate by

$$\overline{x} = (x_1^*, x_2^*, \ldots, x_m^*)^{\mathsf{T}}$$

and conjugate transpose

$$x^{\mathsf{H}} = (x_1^*, x_2^*, \ldots, x_m^*).$$

If the three matrices A, B, and C satisfy

$$x^{\mathsf{H}} A x + x^{\mathsf{H}} B \overline{x} + x^{\mathsf{T}} C x = 0, \qquad \text{for all } x \in \mathbb{C}^m$$

then we have

$$A = B + B^{\mathsf{T}} = C + C^{\mathsf{T}} = 0_{m \times m},$$

where $0_{m \times m}$ denotes the $m \times m$ all-zero matrix.

Proof: See Appendix B. □

In the sequel, we present the proof of Theorem 1 by the contradiction method. Assume to the contrary that there exists a $p \times n$ matrix $\mathcal{E}_c$ satisfying the properties in the theorem with $k \geq p$. We can further assume $k = p$ without loss of generality, since in the case $k > p$ we can set the complex variables $x_{p+1} = \cdots = x_k = 0$ and, consequently, obtain again a $p \times n$ matrix $\mathcal{E}_c$ satisfying the properties in the theorem with $k = p$.

We denote the $n \times n$ positive diagonal matrices in the theorem by

$$D_i = \mathrm{diag}(d_{i1}, d_{i2}, \ldots, d_{in}) > 0, \qquad \text{for } i = 1, 2, \ldots, p.$$

We define the $p \times p$ positive diagonal matrices as

$$\Lambda_\ell = \mathrm{diag}(d_{1\ell}, d_{2\ell}, \ldots, d_{p\ell}) > 0, \qquad \text{for } \ell = 1, 2, \ldots, n.$$

Then, the $p \times n$ matrix $\mathcal{E}_c$ satisfies

$$\mathcal{E}_c^{\mathsf{H}} \mathcal{E}_c = \mathrm{diag}(x^{\mathsf{H}}\Lambda_1 x, x^{\mathsf{H}}\Lambda_2 x, \ldots, x^{\mathsf{H}}\Lambda_n x), \tag{3}$$

where the p-dimensional complex-variable vector

$$x = (x_1, x_2, \ldots, x_p)^{\mathsf{T}} \in \mathbb{C}^p$$

with its conjugate transpose $x^{\mathsf{H}} = (x_1^*, x_2^*, \ldots, x_p^*)$.

In the following, we assume that $\Lambda_1 = I_{p\times p}$, which can be obtained by a linear variable transformation of replacing $x \in \mathbb{C}^p$ by $\Lambda_1^{-1/2}x$.

Since the entries of the $p \times n$ matrix $\mathcal{E}_c$ are all complex linear combinations of the complex variables $x_1, x_2, \ldots, x_p$ and their conjugates $x_1^*, x_2^*, \ldots, x_p^*$, each column vector of $\mathcal{E}_c$ can be written as the form of $Px + Q\overline{x}$, where P and Q are $p \times p$ complex constant matrices in $\mathbb{C}^{p\times p}$ and $\overline{x} = (x_1^*, x_2^*, \ldots, x_p^*)^{\mathsf{T}} \in \mathbb{C}^p$ is the conjugate vector of x.

We denote the first column vector of $\mathcal{E}_c$ by

$$Ax + B\overline{x} \in \mathbb{C}^p$$

where A and B are $p \times p$ constant matrices in $\mathbb{C}^{p\times p}$. It follows from (3) that

$$(Ax + B\overline{x})^{\mathsf{H}}(Ax + B\overline{x}) = x^{\mathsf{H}}\Lambda_1 x = x^{\mathsf{H}}x, \qquad \text{for all } x \in \mathbb{C}^p.$$

That is,

$$x^{\mathsf{H}}(A^{\mathsf{H}}A + B^{\mathsf{T}}\overline{B} - I_{p\times p})x + x^{\mathsf{H}}A^{\mathsf{H}}B\overline{x} + x^{\mathsf{T}}B^{\mathsf{H}}Ax = 0$$

for all $x \in \mathbb{C}^p$, where $\overline{B}$ is the $p \times p$ conjugate matrix of B. Therefore, applying Lemma 1 gives

$$A^{\mathsf{H}}A + B^{\mathsf{T}}\overline{B} = I_{p\times p} \quad \text{and} \quad A^{\mathsf{H}}B + B^{\mathsf{T}}\overline{A} = 0_{p\times p} \tag{4}$$

where $\overline{A}$ is the $p \times p$ conjugate matrix of A. Let the $2p \times 2p$ matrix

$$W \stackrel{\text{def}}{=} \begin{pmatrix} A & B \\ \overline{B} & \overline{A} \end{pmatrix} \in \mathbb{C}^{2p\times 2p}.$$

Then, by using (4), we obtain

$$W^{\mathsf{H}}W = \begin{pmatrix} A^{\mathsf{H}}A + B^{\mathsf{T}}\overline{B} & A^{\mathsf{H}}B + B^{\mathsf{T}}\overline{A} \\ B^{\mathsf{H}}A + A^{\mathsf{T}}\overline{B} & B^{\mathsf{H}}B + A^{\mathsf{T}}\overline{A} \end{pmatrix} = I_{2p\times 2p},$$

which means that W is a $2p \times 2p$ square unitary matrix under the preceding assumption $k = p$.

For any given p-dimensional complex-variable vector

$$y = (y_1, y_2, \ldots, y_p)^{\mathsf{T}} \in \mathbb{C}^p$$

and its conjugate vector

$$\overline{y} = (y_1^*, y_2^*, \ldots, y_p^*)^{\mathsf{T}}$$

we make the following variable transformation:

$$x = A^{\mathsf{H}}y + B^{\mathsf{T}}\overline{y} \in \mathbb{C}^p. \tag{5}$$

Then, we have

$$\begin{pmatrix} x \\ \overline{x} \end{pmatrix} = \begin{pmatrix} A^{\mathsf{H}} & B^{\mathsf{T}} \\ B^{\mathsf{H}} & A^{\mathsf{T}} \end{pmatrix} \begin{pmatrix} y \\ \overline{y} \end{pmatrix} = W^{\mathsf{H}} \begin{pmatrix} y \\ \overline{y} \end{pmatrix}.$$

By the unitarity of the square matrix W, it follows that

$$\begin{pmatrix} y \\ \overline{y} \end{pmatrix} = W \begin{pmatrix} x \\ \overline{x} \end{pmatrix} = \begin{pmatrix} Ax + B\overline{x} \\ \overline{B}x + \overline{A}\overline{x} \end{pmatrix}.$$

Therefore, under the variable transformation (5), the $p \times n$ matrix $\mathcal{E}_c$ in the theorem will have entries all of which are complex linear combinations of the complex variables $y_1, y_2, \ldots, y_p$ and their conjugates $y_1^*, y_2^*, \ldots, y_p^*$. Furthermore, by noting that the number of columns in $\mathcal{E}_c$ is $n \geq 3$, we see that the first three column vectors of $\mathcal{E}_c$ can be represented by $y = Ax + B\overline{x}$, $Cy + D\overline{y}$, and $Ey + F\overline{y}$, respectively, where C, D, E, and F are all $p \times p$ constant matrices in $\mathbb{C}^{p\times p}$.

Since the column vectors of $\mathcal{E}_c$ are mutually complex orthogonal, we have

$$y^{\mathsf{H}}(Cy + D\overline{y}) = y^{\mathsf{H}}Cy + y^{\mathsf{H}}D\overline{y} = 0, \qquad \text{for all } y \in \mathbb{C}^p$$

where $y^{\mathsf{H}} = (y_1^*, y_2^*, \ldots, y_p^*)$ is the conjugate transpose of y. According to Lemma 1, the above fact gives

$$C = 0_{p\times p} \quad \text{and} \quad D = -D^{\mathsf{T}}.$$

By using a similar argument, we can also get

$$E = 0_{p\times p} \quad \text{and} \quad F = -F^{\mathsf{T}}.$$

Then, the first three column vectors of $\mathcal{E}_c$ are y, $D\overline{y}$, and $F\overline{y}$, respectively.

From the complex orthogonality between column vectors of $\mathcal{E}_c$, we obtain

$$(D\overline{y})^{\mathsf{H}}F\overline{y} = y^{\mathsf{T}}(D^{\mathsf{H}}F)\overline{y} = 0, \qquad \text{for all } y \in \mathbb{C}^p.$$

Therefore, its conjugate also satisfies

$$y^{\mathsf{H}}(D^{\mathsf{T}}\overline{F})y = 0, \qquad \text{for all } y \in \mathbb{C}^p$$

which implies, by Lemma 1

$$D^{\mathsf{T}}\overline{F} = 0_{p\times p}. \tag{6}$$

On the other hand, we can prove that the $p \times p$ matrices D and F are both of full rank as follows. In fact, according to (3) and (5), we have

$$(D\overline{y})^{\mathsf{H}}D\overline{y} = x^{\mathsf{H}}\Lambda_2 x = (A^{\mathsf{H}}y + B^{\mathsf{T}}\overline{y})^{\mathsf{H}}\Lambda_2(A^{\mathsf{H}}y + B^{\mathsf{T}}\overline{y}). \tag{7}$$

If $0 \neq y \in \mathbb{C}^p$, i.e., $0 \neq \overline{y} \in \mathbb{C}^p$, then, by virtue of the unitarity of the square matrix W

$$W^{\mathsf{H}} \begin{pmatrix} y \\ \overline{y} \end{pmatrix} = \begin{pmatrix} A^{\mathsf{H}}y + B^{\mathsf{T}}\overline{y} \\ B^{\mathsf{H}}y + A^{\mathsf{T}}\overline{y} \end{pmatrix} \neq 0 \in \mathbb{C}^{2p}.$$

Noting that $A^{\mathsf{H}}y + B^{\mathsf{T}}\overline{y}$ and $B^{\mathsf{H}}y + A^{\mathsf{T}}\overline{y}$ are mutually conjugate, we can conclude that

$$A^{\mathsf{H}}y + B^{\mathsf{T}}\overline{y} \neq 0 \in \mathbb{C}^p.$$

Then, by (7), we get $(D\overline{y})^{\mathsf{H}}D\overline{y} > 0$ and, hence, $D\overline{y} \neq 0 \in \mathbb{C}^p$. Therefore, the $p \times p$ complex matrix D is of full rank. In a similar manner, the $p \times p$ complex matrix F can also be shown to have full rank. Consequently, the two $p \times p$ complex matrices D^{T} and $\overline{F}$ are of full rank as well, which is in contradiction to (6). This completes the proof of Theorem 1. $\square$

III. Conclusion

STBCs developed within the theoretical framework of generalized orthogonal designs possess the favorable characteristics of having full diversity order and a fast ML decoding algorithm. While the rate-one STBCs from orthogonal designs exist for any given number of transmit antennas using any arbitrary real constellation and for two transmit antennas using any arbitrary complex constellation, it has been shown that there does not exist rate-one STBC from generalized complex linear processing orthogonal designs for more than two transmit antennas using any arbitrary complex constellation. As a consequence, the rate $3/4$ of the two generalized complex linear processing orthogonal designs for three and four transmit antennas constructed in [4] is the highest possible one, given the decoding delay of four at the receiver.

Appendix A
Proof of $\mathcal{S}_n$ Being Generalized Complex Orthogonal Designs for All $n \geq 1$

The proof can be given by a simple induction in terms of $n \geq 1$. When $n = 1$ and $n = 2$, it is obvious that $\mathcal{S}_1$ and $\mathcal{S}_2$ as defined earlier are both generalized complex orthogonal designs. Assuming that the $p \times n$ matrix $\mathcal{S}_n$ is a generalized complex orthogonal design for some $n \geq 2$, which satisfies

$$\mathcal{S}_n^{\mathsf{H}}\mathcal{S}_n = (|x_1|^2 + |x_2|^2 + \cdots + |x_n|^2)I_{n\times n}, \tag{8}$$

we will show that $\mathcal{S}_{n+1}$ is also as follows.

The Hermitian transpose of $\mathcal{S}_{n+1}$ for all $n \geq 2$ is

$$\mathcal{S}_{n+1}^{\mathsf{H}} = \left(\begin{array}{cccc|cccc} & \mathcal{S}_n^{\mathsf{H}} & & & & -x_{n+1}I_{n\times n} & & \\ \hline x_{n+1}^* & 0 & \cdots & 0 & x_1 & x_2 & \cdots & x_n \end{array}\right)$$

in the last row of which there are $p_n - 1$ zero entries between x_{n+1}^* and x_1. It is easy to see that for all $n \geq 1$, the first row of the $p \times n$ matrix $\mathcal{S}_n$ recursively defined above is $(x_1, x_2, \ldots, x_n)$, i.e., that the first column of the $n \times p$ matrix $\mathcal{S}_n^{\mathsf{H}}$ is $(x_1^*, x_2^*, \ldots, x_n^*)^{\mathsf{T}}$. Hence,

$$\mathcal{M}_1 \stackrel{\text{def}}{=} \mathcal{S}_n^{\mathsf{H}} \begin{pmatrix} x_{n+1} \\ 0_{(p_n-1)\times 1} \end{pmatrix} - x_{n+1}(x_1^*, x_2^*, \ldots, x_n^*)^{\mathsf{T}} = 0_{n\times 1},$$

and equivalently

$$\begin{aligned} \mathcal{M}_2 &\stackrel{\text{def}}{=} \mathcal{M}_1^{\mathsf{H}} \\ &= (x_{n+1}^* \quad 0_{1\times(p_n-1)})\,\mathcal{S}_n - x_{n+1}^*(x_1, x_2, \ldots, x_n) \\ &= 0_{1\times n} \end{aligned}$$

where $0_{s\times t}$ denotes the $s \times t$ all-zero matrix for any $s \geq 1$ and any $t \geq 1$.

Noting the above facts and the induction assumption (8), we have

$$\begin{aligned} &\mathcal{S}_{n+1}^{\mathsf{H}}\mathcal{S}_{n+1} \\ &\quad = \left(\begin{array}{c|c} \mathcal{S}_n^{\mathsf{H}}\mathcal{S}_n + |x_{n+1}|^2 I_{n\times n} & \mathcal{M}_1 \\ \hline \mathcal{M}_2 & |x_1|^2 + \cdots + |x_n|^2 + |x_{n+1}|^2 \end{array}\right) \\ &\quad = (|x_1|^2 + |x_2|^2 + \cdots + |x_{n+1}|^2) I_{(n+1)\times(n+1)}. \end{aligned}$$

By the induction principle, we know that for all $n \geq 1$, the $p \times n$ matrix $\mathcal{S}_n$ is a generalized complex orthogonal design. The proof is completed. □

Appendix B
Proof of Lemma 1

Assume that $A = A_1 + \boldsymbol{j}A_2$, $(B + B^{\mathsf{T}})/2 = B_1 + \boldsymbol{j}B_2$, and $(C + C^{\mathsf{T}})/2 = C_1 + \boldsymbol{j}C_2$, where A_i, B_i, and C_i are all $m \times m$ real constant matrices in $\mathbb{R}^{m\times m}$ for $i = 1, 2$. It is obvious that

$$B_1 = B_1^{\mathsf{T}}, \quad B_2 = B_2^{\mathsf{T}}, \quad C_1 = C_1^{\mathsf{T}}, \quad \text{and } C_2 = C_2^{\mathsf{T}}. \tag{9}$$

Then, under the conditions of the lemma, we have

$$\begin{aligned} &x^{\mathsf{H}}Ax + x^{\mathsf{H}}B\overline{x} + x^{\mathsf{T}}Cx && (10) \\ &= x^{\mathsf{H}}Ax + \frac{1}{2}x^{\mathsf{H}}(B + B^{\mathsf{T}})\overline{x} + \frac{1}{2}x^{\mathsf{T}}(C + C^{\mathsf{T}})x \\ &= x^{\mathsf{H}}(A_1 + \boldsymbol{j}A_2)x + x^{\mathsf{H}}(B_1 + \boldsymbol{j}B_2)\overline{x} + x^{\mathsf{T}}(C_1 + \boldsymbol{j}C_2)x \\ &= 0, \qquad \text{for all } x \in \mathbb{C}^m. && (11) \end{aligned}$$

Let $x = a \in \mathbb{R}^m$. From (11), it follows that

$$a^{\mathsf{T}}(A_1 + \boldsymbol{j}A_2)a + a^{\mathsf{T}}(B_1 + \boldsymbol{j}B_2)a + a^{\mathsf{T}}(C_1 + \boldsymbol{j}C_2)a = 0$$

for all $a \in \mathbb{R}^m$. Hence, by equating the real and imaginary parts on the two sides

$$a^{\mathsf{T}}(A_1 + B_1 + C_1)a = 0, \qquad \text{for all } a \in \mathbb{R}^m \tag{12}$$

and

$$a^{\mathsf{T}}(A_2 + B_2 + C_2)a = 0, \qquad \text{for all } a \in \mathbb{R}^m. \tag{13}$$

Let $x = \boldsymbol{j}a$ with $a \in \mathbb{R}^m$. From (11), we obtain

$$-a^{\mathsf{T}}(A_1 + \boldsymbol{j}A_2)a + a^{\mathsf{T}}(B_1 + \boldsymbol{j}B_2)a + a^{\mathsf{T}}(C_1 + \boldsymbol{j}C_2)a = 0$$

for all $a \in \mathbb{R}^m$. This is equivalent to

$$a^{\mathsf{T}}(-A_1 + B_1 + C_1)a = 0, \qquad \text{for all } a \in \mathbb{R}^m \tag{14}$$

and

$$a^{\mathsf{T}}(-A_2 + B_2 + C_2)a = 0, \qquad \text{for all } a \in \mathbb{R}^m. \tag{15}$$

From (12)–(15), we can get

$$a^{\mathsf{T}}A_1a = a^{\mathsf{T}}A_2a = a^{\mathsf{T}}(B_1 + C_1)a = a^{\mathsf{T}}(B_2 + C_2)a = 0 \tag{16}$$

for all $a \in \mathbb{R}^m$. Noting the symmetry of the $m \times m$ real constant matrices B_i and C_i for $i = 1, 2$ as stated in (9), we know from (16) that

$$A_1 = -A_1^{\mathsf{T}}, \quad A_2 = -A_2^{\mathsf{T}}, \quad B_1 = -C_1, \quad \text{and } B_2 = -C_2. \tag{17}$$

Now, let $x = a + \boldsymbol{j}b \in \mathbb{C}^m$, where a and b are any given two real vectors in $\mathbb{R}^m$. By virtue of (9) and (17), from (11) we have

$$\begin{aligned} &x^{\mathsf{H}}Ax + x^{\mathsf{H}}B\overline{x} + x^{\mathsf{T}}Cx && (18) \\ &= (a^{\mathsf{T}} - \boldsymbol{j}b^{\mathsf{T}})(A_1 + \boldsymbol{j}A_2)(a + \boldsymbol{j}b) \\ &\quad + (a^{\mathsf{T}} - \boldsymbol{j}b^{\mathsf{T}})(B_1 + \boldsymbol{j}B_2)(a - \boldsymbol{j}b) \\ &\quad - (a^{\mathsf{T}} + \boldsymbol{j}b^{\mathsf{T}})(B_1 + \boldsymbol{j}B_2)(a + \boldsymbol{j}b) \\ &= 2\boldsymbol{j}a^{\mathsf{T}}(A_1 + \boldsymbol{j}A_2)b - 4\boldsymbol{j}a^{\mathsf{T}}(B_1 + \boldsymbol{j}B_2)b \\ &= 2a^{\mathsf{T}}(2B_2 - A_2)b + 2\boldsymbol{j}a^{\mathsf{T}}(A_1 - 2B_1)b \\ &= 0, \qquad \text{for all } a \in \mathbb{R}^m \text{ and all } b \in \mathbb{R}^m && (19) \end{aligned}$$

which gives

$$a^{\mathsf{T}}(A_1 - 2B_1)b = 0, \qquad \text{for all } a \in \mathbb{R}^m \text{ and all } b \in \mathbb{R}^m$$

and

$$a^{\mathsf{T}}(2B_2 - A_2)b = 0, \qquad \text{for all } a \in \mathbb{R}^m \text{ and all } b \in \mathbb{R}^m.$$

Therefore,

$$A_1 = 2B_1 \quad \text{and} \quad A_2 = 2B_2. \tag{20}$$

From (9) and (17), while A_1 and A_2 are real antisymmetric matrices, B_1 and B_2 are real symmetric ones. Then, from the equality (20), it can be concluded that

$$A_1 = A_2 = B_1 = B_2 = 0_{m\times m}$$

and hence, by (17)

$$C_1 = C_2 = 0_{m\times m}.$$

Thus, we obtain

$$A = B + B^{\mathsf{T}} = C + C^{\mathsf{T}} = 0_{m\times m}$$

as desired. The proof of Lemma 1 is completed. □

REFERENCES

[1] S. Alamouti, "A simple transmit diversity technique for wireless communications," *IEEE J. Select. Areas Commun.*, vol. 16, pp. 1451–1458, Aug. 1998.

[2] J. Radon, "Lineare scharen orthogonaler matrizen," in *Abhandlungen aus dem Mathematischen Seminar der Hamburgishen Universität*, vol. I, 1922, pp. 1–14.

[3] V. Tarokh, N. Seshadri, and A. R. Calderbank, "Space-time codes for high data rate wireless communication: Performance criterion and code construction," *IEEE Trans. Inform. Theory*, vol. 44, pp. 744–765, Mar. 1998.

[4] V. Tarokh, H. Jafarkhani, and A. R. Calderbank, "Space-time block codes from orthogonal designs," *IEEE Trans. Inform. Theory*, vol. 45, pp. 1456–1467, July 1999.

[5] ——, "Correction to 'Space-time block codes from orthogonal designs'," *IEEE Trans. Inform. Theory*, vol. 46, p. 314, Jan. 2000.

The Rate of Regular LDPC Codes

Gadi Miller and Gérard Cohen, *Senior Member, IEEE*

***Abstract*—We find the rate of of a typical code from the regular low-density parity-check (LDPC) ensemble. We then show that the rate of a code from the ensemble converges to the design rate in quadratic mean and almost surely.**

***Index Terms*—Low-density parity-check (LDPC) codes, rate.**

I. INTRODUCTION

Most results on low-density parity-check (LDPC) codes are concerned with an ensemble of such codes. In particular, the codes comprising the ensemble are not all of the same rate. The most popular way (originating with [2]) to circumvent this difficulty is to argue that a code that has a parity-check matrix of size $L \times N$ has a rate $R \geq R'$ where $R' \triangleq 1 - L/N$ is the *design rate*. This *lower bound* on the rate is often sufficient. Moreover, by providing upper bounds on the maximum-likelihood decoding error probability of the expurgated LDPC ensemble (e.g., [2], [3]), the typical rate of the ensemble can be bounded also *from above* by the capacity of the channel for which reliable communication is attained.

In this correspondence, we find the rate of a typical code in the (c, d) regular LDPC ensemble. This is done by finding the rank of the corresponding LDPC matrix. We show that as the block length increases, the parity-check matrix is almost sure to be full rank for c odd, or with a single degeneracy for c even. We then show that the rate of a code randomly drawn from the ensemble converges to the design rate both in quadratic mean and almost surely.

Manuscript received December 5, 2002; revised May 23, 2003.

The authors are with the École Nationale Supérieure des Télécommunications, 75634 Paris 13, France (e-mail: miller@enst.fr; cohen@enst.fr).

Communicated by S. Litsyn, Associate Editor for Coding Theory.

Digital Object Identifier 10.1109/TIT.2003.818403

II. MAIN RESULT

The (c, d) regular bipartite ensemble is expressed in terms of a bipartite graph with N variable nodes and L parity-check nodes. The variable nodes and parity-check nodes are each assigned c and d sockets, respectively. A random permutation of size $Nc = Ld$ is then drawn uniformly from all $(Nc)!$ possibilities to match variable and parity-check sockets. This ensemble of graphs induces an ensemble of binary LDPC matrices where the element (i, j) in the matrix is one iff the ith parity-check node is connected to the jth variable node an odd number of times, and is zero otherwise. Note that while parallel edges may cause certain rows to have a (Hamming) weight smaller then d, the parity of the weight is conserved.

The main result of this correspondence is expressed as the following two theorems.

Theorem 1: Let $2 < c < d$ be two integers and consider the (c, d) regular ensemble with block length N such that Nc/d is an integer. Let $R(c, d; N)$ be the random variable corresponding to the rate of a randomly drawn code from this ensemble. Then

$$\lim_{N\to\infty} \Pr\left(R(c, d; N) = 1 - \frac{c}{d} + \frac{\text{even }(c)}{N}\right) = 1$$

where even (c) is a function equal to 1 if c is even and to 0 if c is odd.

Since the rate of any code satisfies $0 \leq R \leq 1$ we immediately get the following.

Corollary 1: With the same notations as in Theorem 1

$$\lim_{N\to\infty} \mathrm{E}\left(R(c, d; N) - \left(1 - \frac{c}{d}\right)\right)^2 = 0$$

i.e, $R(c, d; N)$ converges to $1 - c/d$ in quadratic mean, and hence also in probability. The following result, however, does not follow from Theorem 1.

Theorem 2: With the same notations as in Theorem 1, $R(c, d; N)$ converges to $1 - c/d$ almost surely.

Comment: Theorem 2 states that the sequence of random variables converges almost surely regardless to the nature of dependencies (if any) between them.

Proof of Theorem 1: The proof is slightly different for c even and odd. We first assume that c is even, and then describe the modification for the case where c is odd. Let us denote the ensemble of (c, d) regular matrices by $\mathcal{A}(c, d; N)$ and let $A(c, d; N)$ be a matrix randomly drawn from $\mathcal{A}(c, d; N)$. Then

$$\Pr\left(R(c, d; N) = 1 - \frac{c}{d} + \frac{1}{N}\right) = \Pr\left(\operatorname{rank} A(c, d; N) = N\frac{c}{d} - 1\right). \quad (1)$$

We now use the observation

$$\{A : A \in \mathcal{A}(c, d; N)\} = \left\{B^T : B \in \mathcal{A}\left(d, c; Nc/d\right)\right\}$$

to write

$$\begin{aligned}\Pr\left(\operatorname{rank} A(c, d; N) = Nc/d - 1\right) &= \Pr\left(\operatorname{rank} A^T(c, d; N) = Nc/d - 1\right)\\ &= \Pr\left(\operatorname{rank} A\left(d, c; Nc/d\right) = Nc/d - 1\right). \quad (2)\end{aligned}$$