number of recodings by orders of magnitude without compromising performance.

The performance of order reprocessing in terms of list error probability has been investigated in [14]. In the future we plan to analytically study the list error probability of the proposed adaptive skipping rule and, in particular, to determine the range of values for parameter $\lambda$ (in the adaptive skipping rule) that result in smaller error probability than the list error probability of order reprocessing, rendering performance degradation negligible.

## Acknowledgment

The authors would like to acknowledge the reviewers for constructive comments that helped shape the results and the presentation of this paper.

## References

[1] S. G. Wilson, *Digital Modulation and Coding*. Upper Saddle River, NJ: Prentice-Hall, 1996.

[2] J. K. Wolf, "Efficient maximum likelihood decoding of linear block codes using a trellis," *IEEE Trans. Inf. Theory*, vol. 24, pp. 76–80, Jan. 1978.

[3] G. D. Forney, Jr, "Generalized minimum distance decoding," *IEEE Trans. Inf. Theory*, vol. 12, pp. 125–131, Apr. 1966.

[4] D. Chase, "A class of algorithms for decoding block codes with channel measurement information," *IEEE Trans. Inf. Theory*, vol. 18, pp. 170–181, Jan. 1972.

[5] B. G. Dorsch, "A decoding algorithm for binary block codes and $J$-ary output channels," *IEEE Trans. Inf. Theory*, vol. 20, pp. 391–394, May 1974.

[6] A. Valembois and M. Fossorier, "A comparison between most reliable basis reprocessing strategies," *IEICE Tran. Fund.*, vol. E85—A, pp. 1727–1741, Jul. 2002.

[7] ——, "An improved method to compute lists of binary vectors that optimize a given weight function with application to soft decision decoding," *IEEE Commun. Lett.*, vol. 5, pp. 456–458, Nov. 2001.

[8] M. P. C. Fossorier and S. Lin, "Soft-decision decoding of linear block codes based on ordered statistics," *IEEE Trans. Inf. Theory*, vol. 41, pp. 1379–1396, Sep. 1995.

[9] ——, "Computationally efficient soft decision decoding of linear block codes based on ordered statistics," *IEEE Trans. Inf. Theory*, vol. 42, pp. 738–750, May 1996.

[10] D. Gazelle and J. Snyders, "Reliability-based code-search algorithms for maximum-likelihood decoding of block codes," *IEEE Trans. Inf. Theory*, vol. 43, pp. 239–249, Jan. 1997.

[11] Y. S. Han, C. R. P. Hartmann, and C.-C. Chen, "Efficient priority-first search maximum-likelihood soft-decision decoding of linear block codes," *IEEE Trans. Inf. Theory*, vol. 39, pp. 1514–1523, Sep. 1993.

[12] C.-C. Shih, C. R. Wulff, C. R. P. Hartmann, and C. K. Mohan, "Efficient heuristic search algorithms for soft-decision decoding of linear block codes," *IEEE Trans. Inf. Theory*, vol. 44, pp. 3023–3038, Nov. 1998.

[13] Y. Wu and D. Pados, "An adaptive two-stage algorithm for ML and sub-ML decoding of binary linear block codes," *IEEE Trans. Inf. Theory*, vol. 49, pp. 261–269, Jan. 2003.

[14] M. Fossorier and S. Lin, "Error performance analysis for reliability-based decoding algorithms," *IEEE Trans. Inf. Theory*, vol. 48, pp. 287–293, Jan. 2002.

# Generally Dimensional and Constellation Expansion Free Space–Time Block Codes for QAM With Full Diversity

Ming-Yang Chen, Chiang-Yu Chen, *Student Member, IEEE*,
Hua-Chieh Li, Soo-Chang Pei, *Fellow, IEEE*, and
Hsuan-Jung Su, *Member, IEEE*

***Abstract*—This correspondence presents new rate-1 space–time block codes (STBCs) attending full diversity over every quadrature amplitude modulation (QAM) constellation when the number of Tx antennas is a power of two. From the simulation results, our design performs very closely to the quasi-orthogonal code with constellation rotation over 4-QAM and 16-QAM in the case of four Tx antennas over quasi-static Rayleigh fading channels. Moreover, the proposed codes would not cause any constellation expansion over QAM symbols in contrast with the quasi-orthogonal codes with constellation rotations.**

***Index Terms*—Algebraic codes, generalized quaternion groups, representations of finite groups, space–time block codes (STBCs), transmit diversity.**

## I. Introduction

It is well known that using multiple antennas to create a multiple-input multiple-output (MIMO) channel can significantly increase the transmit diversity of communication systems in fading environments. Among various MIMO transmission and receiving techniques, space–time block codes (STBCs) constitute a powerful scheme because the resulted bit error rates (BERs) are lowered dramatically by simple transmission schemes (see [9] and those references therein). When designing STBCs, an orthogonal design is desirable to achieve full diversity. The received signals for an orthogonal STBC can be decoupled to scalar channels and the maximum-likelihood (ML) detection can be done linearly by decoding the transmitted signals individually. Alamouti first analyzed the STBC from orthogonal design for two Tx antennas in [1] as

$$\begin{pmatrix} z_1 & z_2 \\ -z_2^* & z_1^* \end{pmatrix} \tag{1}$$

where $z^*$ stands for the complex conjugate of $z$. Tarokh, Jafarkhani, and Calderbank [8] presented a formal setting for orthogonal designs by defining a $T \times M_T$ unitary matrix with each entry coming from the set

$$\{0\} \cup \left\{ \cup_{i=1}^{N} \{\pm z_i, \pm z_i^*\} \right\}$$

where $T$ and $M_T$ represent the block length and the number of Tx antennas, respectively. In particular, a design is of rate-1 if $N = T$.

Manuscript received September 1, 2005; revised March 27, 2006. This work was supported by the National Science Council, R.O.C., under Contracts NSC 91-2219-E-002-044 and NSC 93-2752-E-002-006-PAE. The material in this correspondence was presented in part at the IEEE International Conference on Communications, Seoul, Korea, May16–20, 2005, and the 16th Annual IEEE International Symposium on Personal Indoor and Mobile Radio Communications, Berlin, Germany, September 2005.

M.-Y. Chen was with the Department of Electrical Engineering, National Taiwan University, Taipei, Taiwan 106, R.O.C. He is now with the Department of Electrical Engineering and Computer Sciences, University of California at Berkeley, Berkeley, CA 94720 USA (e-mail: roc3@eecs.berkeley.edu).

C.-Y. Chen is with the Department of Electrical Engineering, Stanford University, Stanford, CA 94305 USA (e-mail: Chiangyu.Chen@stanford.edu).

H.-C. Li is with the Department of Mathematics, National Taiwan Normal University, Taipei, Taiwan 116, R.O.C. (e-mail: li@math.ntnu.edu.tw).

S.-C. Pei and H.-J. Su are with the Department of Electrical Engineering, National Taiwan University, Taipei, Taiwan 106, R.O.C. (e-mail: pei@cc.ee.ntu.edu.tw; hjsu@cc.ee.ntu.edu.tw).

Communicated by Ø. Ytrehus, Associate Editor for Coding Technique.

Digital Object Identifier 10.1109/TIT.2006.889023

It is proved in [8] that a rate-1 orthogonal design exists only for systems with two Tx antennas over complex constellations, wherefore researchers turned to seek code designs that provide partial diversity. A famous example is the quasi-orthogonal space–time block codes (QOSTBCs) proposed by Jafarkhani [5]. A QOSTBC is a rate-1 $4 \times 4$ STBC that divides the four columns of transmission matrix into two pairs, where the columns within each pair are not orthogonal while different pairs are orthogonal to each other. It can be observed that a QOSTBC achieves half the maximum diversity. The received signals would no longer be decoupled to scalar channels and the corresponding ML detection is thus implemented by searching symbol pairs. According to [5], the BER performance of QOSTBCs is better than that of orthogonal STBCs with rates less than 1 at low signal-to-noise ratios (SNRs). Nevertheless, QOSTBCs are surpassed by orthogonal codes at high SNRs because of the lower transmit diversity.

Although there is no rate-1 complex orthogonal design for more than two Tx antennas, it does not imply that there is no full-diversity code for a specific constellation. Motivated by this, some approaches have aimed to achieve full diversity through quasi-orthogonal designs or other algebraic methodologies. The first instance is to improve QOSTBCs through constellation rotations [7]. Full diversity can be provided by finding the optimal rotation angles and rotating the constellations for half the input variables. Since the codes are based on QOSTBCs, after rotations the receivers can still maintain the same decoding complexity as a normal QOSTBC. Even so, the tradeoff is the need of some additional constellations, e.g., for quadrature amplitude modulations (QAMs) the optimal rotation angle is $\pi/4$. On the other hand, Damen, Abed-Meraim, and Belfiore [4] developed the diagonal algebraic space–time (DAST) block codes that combine the rotated constellations and Hadamard transform in order to attend full diversity over QAM and pulse-amplitude modulations. In simulations, the DAST block codes have higher BERs than the QOSTBCs with constellation rotations in the case of four Tx antennas over quasi-static Rayleigh-fading channels. Furthermore, the DAST block codes are not quasi-orthogonal. Although the ML decoding complexity can be reduced without loss of diversity by sphere decoders [10], it is still a concern in implementations.

This correspondence presents a general and new set of rate-1 STBCs. Each of the new codes forms a ring and is derived explicitly via a group-theoretic methodology on the generalized quaternion group of order $4N$. The graceful properties of ring structures enable us to show that these codes achieve full diversity over every QAM constellation when $N$ is a power of two. Because all the entries in transmission matrices are selected from

$$\cup_{i=1}^{N} \{\pm z_i, \pm \mathbf{i} z_i, \pm z_i^*, \pm \mathbf{i} z_i^*\}$$

($\mathbf{i} = \sqrt{-1}$), the resulted schemes would not cause any constellation expansion over QAM symbols. Moreover, the columns of each new design can be divided into two equally sized sets such that those coming from different sets are orthogonal pairwise, thus reducing the ML decoding complexity. In particular, as $N = 4$, our code is quasi-orthogonal and performs better BERs not only than the previous QOSTBC [5], but also superior to the DAST block code [4] over quasi-static Rayleigh fading channels. Compared with the QOSTBC with constellation rotation [7], their performance comes very closely to each other.

The rest of this article is organized as follows. Section II shows the algebraic constructions for our new STBCs with some companionate properties, which help to prove the satisfaction of full diversity as well as some performance issues over QAM in Section III. The simulation results are discussed in Section IV. Finally, the conclusions are drawn in Section V.

*Remark (Recent Results)*

After submitting this correspondence, an analogous development for phase-shift keying (PSK) modulations is provided in [2]. When the number of Tx antennas is four, the proposed codes in this article reach full diversity without any constellation expansion over 4-PSK. Otherwise, one has to select the entries in transmission matrices from

$$\cup_{i=1}^{N} \left\{\pm z_i, \pm e^{\mathbf{i}2\pi/m} z_i, \pm e^{-\mathbf{i}2\pi/m} z_i\right\}$$

(up to a conjugation) in order to get constellation expansion free QOSTBCs for $m$-PSK modulations, $m \geq 8$.

## II. Code Constructions

The formal definition of a size $N$ complex rate-1 STBC $\mathbf{S}(z_1, \ldots, z_N)$ in [8] is an $N \times N$ matrix with entries the indeterminates $\pm z_1, \ldots, \pm z_N$, their conjugates $\pm z_1^*, \ldots, \pm z_N^*$, or multiples of them by $\mathbf{i}$. Without loss of generality, the first row of $\mathbf{S}(z_1, \ldots, z_N)$ is set to $(z_1, \ldots, z_N)$. Let $\mathbf{e}_i$ be the row vector $(z_1, \ldots, z_N)$ with $z_i = 1$ and $z_j = 0$ for $j \neq i$, and $\mathbf{e}'_i$ be the row vector $(z_1, \ldots, z_N)$ with $z_i = \mathbf{i}$ and $z_j = 0$ for $j \neq i$. The following Lemma 2.1 guarantees that only finite groups of order $4N$ are needed to exploit if one wants to construct STBCs of size $N$ with ring structures.

*Lemma 2.1:* If the set

$$\mathbb{G} := \left\{\pm \mathbf{S}(\mathbf{e}_1), \pm \mathbf{S}(\mathbf{e}'_1), \ldots, \pm \mathbf{S}(\mathbf{e}_N), \pm \mathbf{S}(\mathbf{e}'_N)\right\}$$

is a multiplicative group, then

$$\mathbb{S} := \{\mathbf{S}(z_1, \ldots, z_N) \mid z_1, \ldots, z_N \in \mathbb{C}\}$$

is a ring with identity $\mathbf{S}(\mathbf{e}_1)$ over the conventional matrix addition and multiplication, where $\mathbb{C}$ is the field of complex numbers.

*Proof:* Note that $\mathbb{S}$ is closed under addition because every entry of $\mathbf{S}(z_1, \ldots, z_N)$ is linear. For arbitrary $\mathbf{S}(z_1, \ldots, z_N)$, $\mathbf{S}(z'_1, \ldots, z'_N) \in \mathbb{S}$

$$\begin{aligned}
&\mathbf{S}(z_1, \ldots, z_N) \cdot \mathbf{S}(z'_1, \ldots, z'_N)\\
&= \left(\sum_{i=1}^{N} \Re(z_i)\mathbf{S}(\mathbf{e}_i) + \Im(z_i)\mathbf{S}(\mathbf{e}'_i)\right)\\
&\quad \cdot \left(\sum_{i=1}^{N} \Re(z'_i)\mathbf{S}(\mathbf{e}_i) + \Im(z'_i)\mathbf{S}(\mathbf{e}'_i)\right)\\
&= \sum_{i,j=1}^{N} \Re(z_i)\Re(z'_j)\mathbf{S}(\mathbf{e}_i) \cdot \mathbf{S}(\mathbf{e}_j)\\
&\quad + \sum_{i,j=1}^{N} \Re(z_i)\Im(z'_j)\mathbf{S}(\mathbf{e}_i) \cdot \mathbf{S}(\mathbf{e}'_j)\\
&\quad + \sum_{i,j=1}^{N} \Im(z_i)\Re(z'_j)\mathbf{S}(\mathbf{e}'_i) \cdot \mathbf{S}(\mathbf{e}_j)\\
&\quad + \sum_{i,j=1}^{N} \Im(z_i)\Im(z'_j)\mathbf{S}(\mathbf{e}'_i) \cdot \mathbf{S}(\mathbf{e}'_j)
\end{aligned}$$

where $\Re(z)$ and $\Im(z)$ represent the real and imaginary parts of $z \in \mathbb{C}$. Since $\mathbb{G}$ is closed under multiplication, it turns out that

$$\mathbf{S}(\mathbf{e}_i) \cdot \mathbf{S}(\mathbf{e}_j), \mathbf{S}(\mathbf{e}_i) \cdot \mathbf{S}(\mathbf{e}'_j), \mathbf{S}(\mathbf{e}'_i) \cdot \mathbf{S}(\mathbf{e}_j), \mathbf{S}(\mathbf{e}'_i) \cdot \mathbf{S}(\mathbf{e}'_j)$$

all lie in $\mathbb{G}$ and thus in $\mathbb{S}$ for every $i, j = 1, \ldots, N$. $\mathbb{S}$ is closed under multiplication, i.e.

$$\mathbf{M}_1 \cdot \mathbf{M}_2 \in \mathbb{S}$$

for every $\mathbf{M}_1, \mathbf{M}_2 \in \mathbb{S}$. Hence to evaluate $\mathbf{M}_1 \cdot \mathbf{M}_2$ one only needs to know what its first row is. In fact, if the $i$-th row of $\mathbf{M} \in \mathbb{S}$ is $(x_1, \ldots, x_N)$, then the first row of $\mathbf{S}(\mathbf{e}_i) \cdot \mathbf{M}$ is $(x_1, \ldots, x_N)$ and

$$\mathbf{S}(\mathbf{e}_i) \cdot \mathbf{M} = \mathbf{S}(x_1, \ldots, x_N). \qquad (2)$$

Since the first row of $\mathbf{S}(x_1, \ldots, x_N)$ is $(x_1, \ldots, x_N)$, we get

$$\mathbf{S}(\mathbf{e}_1) \cdot \mathbf{S}(x_1, \ldots, x_N) = \mathbf{S}(x_1, \ldots, x_N).$$

Equivalently speaking, $\mathbf{S}(\mathbf{e}_1)$ is the identity matrix and thus the identity of both $\mathbb{G}$ and $\mathbb{S}$. Combining with the addition and multiplication of matrices implies that $\mathbb{S}$ is a ring with identity $\mathbf{S}(\mathbf{e}_1)$. □

The following derivations show an algorithm for deciding the entries of $\mathbf{S}(z_1, \ldots, z_N)$ if the multiplication rules of $\mathbb{G}$ are given. Suppose that

$$\mathbf{S}(\mathbf{e}_i) \cdot \mathbf{S}(\mathbf{e}_k) = \pm \mathbf{S}(\mathbf{e}_j).$$

Then the $i$-th row of $\mathbf{S}(\mathbf{e}_k)$ is $\pm \mathbf{e}_j$. In other words, there is no entry in the $i$-th row of $\mathbf{S}(z_1, \ldots, z_N)$ related with $z_k$ except the $(i, j)$-th entry that is $\pm z_k$ or $\pm z_k^*$. This implies that

$$\mathbf{S}(\mathbf{e}_i) \cdot \mathbf{S}(\mathbf{e}'_k) = \pm \mathbf{S}(\mathbf{e}'_j).$$

More precisely, the $(i, j)$th entry of $\mathbf{S}(z_1, \ldots, z_N)$ corresponding to the following four cases:

$$\begin{aligned}
&(\mathbf{a}) \left\{ \begin{array}{l} \mathbf{S}(\mathbf{e}_i) \cdot \mathbf{S}(\mathbf{e}_k) = \mathbf{S}(\mathbf{e}_j) \\ \mathbf{S}(\mathbf{e}_i) \cdot \mathbf{S}(\mathbf{e}'_k) = \mathbf{S}(\mathbf{e}'_j) \end{array} \right. \\
&(\mathbf{b}) \left\{ \begin{array}{l} \mathbf{S}(\mathbf{e}_i) \cdot \mathbf{S}(\mathbf{e}_k) = -\mathbf{S}(\mathbf{e}_j) \\ \mathbf{S}(\mathbf{e}_i) \cdot \mathbf{S}(\mathbf{e}'_k) = -\mathbf{S}(\mathbf{e}'_j) \end{array} \right. \\
&(\mathbf{c}) \left\{ \begin{array}{l} \mathbf{S}(\mathbf{e}_i) \cdot \mathbf{S}(\mathbf{e}_k) = \mathbf{S}(\mathbf{e}_j) \\ \mathbf{S}(\mathbf{e}_i) \cdot \mathbf{S}(\mathbf{e}'_k) = -\mathbf{S}(\mathbf{e}'_j) \end{array} \right. \\
&(\mathbf{d}) \left\{ \begin{array}{l} \mathbf{S}(\mathbf{e}_i) \cdot \mathbf{S}(\mathbf{e}_k) = -\mathbf{S}(\mathbf{e}_j) \\ \mathbf{S}(\mathbf{e}_i) \cdot \mathbf{S}(\mathbf{e}'_k) = \mathbf{S}(\mathbf{e}'_j) \end{array} \right.
\end{aligned}$$

are $(\mathbf{a}) : z_k$, $(\mathbf{b}) : -z_k$, $(\mathbf{c}) : z_k^*$, $(\mathbf{d}) : -z_k^*$, respectively. Analogously, if

$$\mathbf{S}(\mathbf{e}_i) \cdot \mathbf{S}(\mathbf{e}_k) = \pm \mathbf{S}(\mathbf{e}'_j)$$

then the $i$th row of $\mathbf{S}(\mathbf{e}_k)$ is $\pm \mathbf{e}'_j$. Thus the $i$-th row of $\mathbf{S}(\mathbf{e}'_k)$ is $\pm \mathbf{e}_j$ followed by

$$\mathbf{S}(\mathbf{e}_i) \cdot \mathbf{S}(\mathbf{e}'_k) = \pm \mathbf{S}(\mathbf{e}_j).$$

The $(i, j)$th entry of $\mathbf{S}(z_1, \ldots, z_N)$ corresponding to the following four cases:

$$\begin{aligned}
&(\mathbf{e}) \left\{ \begin{array}{l} \mathbf{S}(\mathbf{e}_i) \cdot \mathbf{S}(\mathbf{e}_k) = \mathbf{S}(\mathbf{e}'_j) \\ \mathbf{S}(\mathbf{e}_i) \cdot \mathbf{S}(\mathbf{e}'_k) = -\mathbf{S}(\mathbf{e}_j) \end{array} \right. \\
&(\mathbf{f}) \left\{ \begin{array}{l} \mathbf{S}(\mathbf{e}_i) \cdot \mathbf{S}(\mathbf{e}_k) = -\mathbf{S}(\mathbf{e}'_j) \\ \mathbf{S}(\mathbf{e}_i) \cdot \mathbf{S}(\mathbf{e}'_k) = \mathbf{S}(\mathbf{e}_j) \end{array} \right. \\
&(\mathbf{g}) \left\{ \begin{array}{l} \mathbf{S}(\mathbf{e}_i) \cdot \mathbf{S}(\mathbf{e}_k) = \mathbf{S}(\mathbf{e}'_j) \\ \mathbf{S}(\mathbf{e}_i) \cdot \mathbf{S}(\mathbf{e}'_k) = \mathbf{S}(\mathbf{e}_j) \end{array} \right. \\
&(\mathbf{h}) \left\{ \begin{array}{l} \mathbf{S}(\mathbf{e}_i) \cdot \mathbf{S}(\mathbf{e}_k) = -\mathbf{S}(\mathbf{e}'_j) \\ \mathbf{S}(\mathbf{e}_i) \cdot \mathbf{S}(\mathbf{e}'_k) = -\mathbf{S}(\mathbf{e}_j) \end{array} \right.
\end{aligned}$$

are $(\mathbf{e}) : \mathbf{i}z_k$, $(\mathbf{f}) : -\mathbf{i}z_k$, $(\mathbf{g}) : \mathbf{i}z_k^*$, $(\mathbf{h}) : -\mathbf{i}z_k^*$, respectively.

The generalized quaternion group of order $4N$ is generated by two elements $a$ and $b$, where $a$ is of order $2N$ and $b$ is of order 4 with the relations

$$a^N = b^2 \text{ and } ab = ba^{-1}.$$

Explicitly, it can be written as

$$\left\{ 1, b, a, ab, a^2, a^2 b, \ldots, a^{2N-1}, a^{2N-1} b \right\}.$$

Note that $a^N$ is the only element of order 2 in this multiplicative group. We may assume that $N = 2L$ is even because of the following concern: the columns of a transmission matrix can be split up into two equally sized sets such that those coming from different sets are orthogonal pairwisely, and so the ML decoding is implemented more efficiently.[1] Applying similar arguments as the impacts of (2), it can be obtained that

$$\mathbf{S}(\mathbf{e}'_i) \cdot \mathbf{M} = \mathbf{S}(\mathbf{i}\mathbf{e}_i) \cdot \mathbf{M} = \mathbf{S}(\mathbf{i}x_1, \ldots, \mathbf{i}x_N)$$

if the $i$-th row of $\mathbf{M} \in \mathbb{S}$ is $(x_1, \ldots, x_N)$. In particular

$$\mathbf{S}(\mathbf{e}'_1) \cdot \mathbf{S}(\mathbf{e}_i) = \mathbf{S}(\mathbf{i}\mathbf{e}_i) = \mathbf{S}(\mathbf{e}'_i). \qquad (3)$$

By setting

$$\begin{gathered}
-\mathbf{S}(\mathbf{e}_1) = a^{2L}, \mathbf{S}(\mathbf{e}'_1) = a^L, \mathbf{S}(\mathbf{e}_1) = 1, \mathbf{S}(\mathbf{e}_{L+1}) = b \\
\mathbf{S}(\mathbf{e}_2) = a, \mathbf{S}(\mathbf{e}_{L+2}) = ab, \mathbf{S}(\mathbf{e}_3) = a^2, \mathbf{S}(\mathbf{e}_{L+3}) = a^2 b \\
\ldots, \mathbf{S}(\mathbf{e}_L) = a^{L-1}, \mathbf{S}(\mathbf{e}_{2L}) = a^{L-1} b
\end{gathered}$$

the multiplication rules of $\mathbb{G}$ can be completely determined by (3) and the fact that $-\mathbf{S}(\mathbf{e}_1)$ is the minus of identity matrix. In virtue of the consequences $(\mathbf{a}) \sim (\mathbf{h})$ above, the corresponding STBC is

$$\begin{aligned}
&\mathbf{S}_1(z_1, \ldots, z_{2L}) \\
&\quad := \begin{pmatrix} \mathbf{C}_1(z_1, \ldots, z_L) & \mathbf{C}_1(z_{L+1}, \ldots, z_{2L}) \\ -\mathbf{C}_1(z_{L+1}, \ldots, z_{2L})^H & \mathbf{C}_1(z_1, \ldots, z_L)^H \end{pmatrix} \qquad (4)
\end{aligned}$$

where $\mathbf{M}^H$ means the Hermitian of $\mathbf{M}$ and

$$\mathbf{C}_1(z_1, \ldots, z_L) := \begin{pmatrix} z_1 & z_2 & z_3 & \cdots & z_{L-1} & z_L \\ \mathbf{i}z_L & z_1 & z_2 & \cdots & z_{L-2} & z_{L-1} \\ \mathbf{i}z_{L-1} & \mathbf{i}z_L & z_1 & \cdots & z_{L-3} & z_{L-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \mathbf{i}z_2 & \mathbf{i}z_3 & \mathbf{i}z_4 & \cdots & \mathbf{i}z_L & z_1 \end{pmatrix}.$$

Analogously, applying

$$\begin{gathered}
-\mathbf{S}(\mathbf{e}_1) = a^{2L}, \mathbf{S}(\mathbf{e}'_1) = a^L, \mathbf{S}(\mathbf{e}_1) = 1, \mathbf{S}(\mathbf{e}_{L+1}) = b, \\
\mathbf{S}(\mathbf{e}_2) = a, \mathbf{S}(\mathbf{e}_{L+2}) = ba, \mathbf{S}(\mathbf{e}_3) = a^2, \mathbf{S}(\mathbf{e}_{L+3}) = ba^2, \\
\ldots, \mathbf{S}(\mathbf{e}_L) = a^{L-1}, \mathbf{S}(\mathbf{e}_{2L}) = ba^{L-1}
\end{gathered}$$

the corresponding STBC is

$$\mathbf{S}_2(z_1, \ldots, z_{2L}) := \begin{pmatrix} \mathbf{C}_1(z_1, \ldots, z_L) & \mathbf{C}_2(z_{L+1}, \ldots, z_{2L}) \\ -\mathbf{C}_2(z_{L+1}, \ldots, z_{2L})^* & \mathbf{C}_1(z_1, \ldots, z_L)^* \end{pmatrix}$$

[1] In [3], it is proved that $\mathbb{G}$ must contain a cyclic normal subgroup of order 4. Since there is no cyclic normal subgroup of order 4 in any generalized quaternion group of order $4N$ with odd $N$, it is impossible to construct an STBC under this case.

where $\mathbf{M}^*$ denotes the conjugate matrix of $\mathbf{M} = (\alpha_{ij})$ by replacing each entry with its complex conjugate and

$$\mathbf{C}_2(z_{L+1}, \ldots, z_{2L}) := \begin{pmatrix} z_{L+1} & z_{L+2} & \cdots & z_{2L-2} & z_{2L-1} & z_{2L} \\ z_{L+2} & z_{L+3} & \cdots & z_{2L-1} & z_{2L} & \mathbf{i}z_{L+1} \\ z_{L+3} & z_{L+4} & \cdots & z_{2L} & \mathbf{i}z_{L+1} & \mathbf{i}z_{L+2} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ z_{2L} & \mathbf{i}z_{L+1} & \cdots & \mathbf{i}z_{2L-3} & \mathbf{i}z_{2L-2} & \mathbf{i}z_{2L-1} \end{pmatrix}.$$

Some properties about $\mathbf{S}_1(z_1, \ldots, z_{2L})$ and $\mathbf{S}_2(z_1, \ldots, z_{2L})$ are listed in the following Lemma 2.2.

*Lemma 2.2:* For $j = 1, 2$, if a matrix $\mathbf{M} \in \mathbb{S}_j$ then $\mathbf{M}^H \in \mathbb{S}_j$, where

$$\mathbb{S}_j := \{\mathbf{S}_j(z_1, \ldots, z_{2L}) \mid z_1, \ldots, z_{2L} \in \mathbb{C}\}.$$

Moreover, all the first $L$ columns of $\mathbf{S}_j(z_1, \ldots, z_{2L})$ are orthogonal to the others.

*Proof:* The truthfulness of the first claim is not hard to see by direct observations. Let $\mathbf{P}_1 = \mathbf{C}_1(z_1, \ldots, z_L)$ and $\mathbf{P}_2 = \mathbf{C}_1(z_{L+1}, \ldots, z_{2L})$. From

$$\mathbf{S}_1(z_1, \ldots, z_{2L})^H \cdot \mathbf{S}_1(z_1, \ldots, z_{2L}) = \begin{pmatrix} \mathbf{P}_1^H \cdot \mathbf{P}_1 + \mathbf{P}_2 \cdot \mathbf{P}_2^H & \mathbf{P}_1^H \cdot \mathbf{P}_2 - \mathbf{P}_2 \cdot \mathbf{P}_1^H \\ \mathbf{P}_2^H \cdot \mathbf{P}_1 - \mathbf{P}_1 \cdot \mathbf{P}_2^H & \mathbf{P}_2^H \cdot \mathbf{P}_2 + \mathbf{P}_1 \cdot \mathbf{P}_1^H \end{pmatrix}$$

to prove that all the first $L$ columns of $\mathbf{S}_1(z_1, \ldots, z_{2L})$ are orthogonal to the others is equivalent to show that

$$\mathbf{P}_1^H \cdot \mathbf{P}_2 - \mathbf{P}_2 \cdot \mathbf{P}_1^H = \mathbf{P}_2^H \cdot \mathbf{P}_1 - \mathbf{P}_1 \cdot \mathbf{P}_2^H = 0.$$

Note that

$$\mathbf{P}_1, \mathbf{P}_2, \mathbf{P}_1^H, \mathbf{P}_2^H \in \{\mathbf{C}_1(x_1, \ldots, x_L) \mid x_1, \ldots, x_L \in \mathbb{C}\}.$$

It suffices to verify that

$$\{\mathbf{C}_1(x_1, \ldots, x_L) \mid x_1, \ldots, x_L \in \mathbb{C}\}$$

is a commutative ring. Since $\mathbf{C}_1(x_1, \ldots, x_L)$ is obtained by assigning the set

$$\{\pm\mathbf{S}(\mathbf{e}_1), \ldots, \pm\mathbf{S}(\mathbf{e}_L)\}$$

to the cyclic group of order $4L$,

$$\left\{1, a, \ldots, a^{4L-1}\right\},$$

an abelian subgroup of the generalized quaternion group of order $8L$, the corresponding subring

$$\{\mathbf{C}_1(x_1, \ldots, x_L) \mid x_1, \ldots, x_L \in \mathbb{C}\}$$

of $\mathbb{S}_1$ must be commutative by Lemma 2.1.

Similarly, let $\mathbf{P}_3 = \mathbf{C}_2(z_{L+1}, \ldots, z_{2L})$. From

$$\mathbf{S}_2(z_1, \ldots, z_{2L})^H \cdot \mathbf{S}_2(z_1, \ldots, z_{2L}) = \begin{pmatrix} \mathbf{P}_1^H \cdot \mathbf{P}_1 + \mathbf{P}_3^T \cdot \mathbf{P}_3^* & \mathbf{P}_1^H \cdot \mathbf{P}_3 - \mathbf{P}_3^T \cdot \mathbf{P}_1^* \\ \mathbf{P}_3^H \cdot \mathbf{P}_1 - \mathbf{P}_1^T \cdot \mathbf{P}_3^* & \mathbf{P}_3^H \cdot \mathbf{P}_3 + \mathbf{P}_1^T \cdot \mathbf{P}_1^* \end{pmatrix}$$

to prove that all the first $L$ columns of $\mathbf{S}_2(z_1, \ldots, z_{2L})$ are orthogonal to the others is equivalent to show that

$$\mathbf{P}_1^H \cdot \mathbf{P}_3 - \mathbf{P}_3^T \cdot \mathbf{P}_1^* = \mathbf{P}_3^H \cdot \mathbf{P}_1 - \mathbf{P}_1^T \cdot \mathbf{P}_3^* = 0,$$

where $\mathbf{M}^T$ is the transpose of $\mathbf{M}$. Since $\mathbf{S}_2(z_1, \ldots, z_{2L})^H$ lies in the ring $\mathbb{S}_2$

$$\mathbf{P}_1^H \cdot \mathbf{P}_3 - \mathbf{P}_3^T \cdot \mathbf{P}_1^*$$

and

$$\mathbf{P}_3^H \cdot \mathbf{P}_1 - \mathbf{P}_1^T \cdot \mathbf{P}_3^*$$

are of the forms $\mathbf{C}_2(x_1, \ldots, x_L)$ and $-\mathbf{C}_2(x_1, \ldots, x_L)^*$, respectively, with $(x_1, \ldots, x_L)$ the first row of

$$\mathbf{P}_1^H \cdot \mathbf{P}_3 - \mathbf{P}_3^T \cdot \mathbf{P}_1^*.$$

Whereas it can be easily detected that every entry in the first row of

$$\mathbf{P}_1^H \cdot \mathbf{P}_3 - \mathbf{P}_3^T \cdot \mathbf{P}_1^* = \mathbf{P}_1^H \cdot \mathbf{P}_3 - \mathbf{P}_3 \cdot \mathbf{P}_1^*$$

is zero ($\mathbf{P}_3$ is symmetric), we get

$$\mathbf{P}_1^H \cdot \mathbf{P}_3 - \mathbf{P}_3^T \cdot \mathbf{P}_1^* = \mathbf{P}_3^H \cdot \mathbf{P}_1 - \mathbf{P}_1^T \cdot \mathbf{P}_3^* = 0.$$

□

The special cases of $\mathbf{S}_1(z_1, \ldots, z_{2L})$ and $\mathbf{S}_2(z_1, \ldots, z_{2L})$ with $L = 1$ exactly coincide with the Alamouti's scheme (1), and in the sense of designing square matrices, the obtained new codes can be treated as the generalizations of (1). In essence, what we provide so far is two new schemes for constructing STBCs such that the columns of every transmission matrix can be partitioned into two equally sized sets, where those coming from different sets are orthogonal pairwisely. One is of the form

$$\begin{pmatrix} \mathbf{M}_1 & \mathbf{M}_2 \\ -\mathbf{M}_2^H & \mathbf{M}_1^H \end{pmatrix}$$

with

$$\mathbf{M}_1 \cdot \mathbf{M}_2 = \mathbf{M}_2 \cdot \mathbf{M}_1$$

and the other is

$$\begin{pmatrix} \mathbf{M}_3 & \mathbf{M}_4 \\ -\mathbf{M}_4^* & \mathbf{M}_3^* \end{pmatrix}$$

with

$$\mathbf{M}_3^H \cdot \mathbf{M}_4 - \mathbf{M}_4^T \cdot \mathbf{M}_3^* = 0$$

or equivalently $\mathbf{M}_3^H \cdot \mathbf{M}_4$ is symmetric. We are going to give a further analysis about the performance issues in the upcoming Section III.

## III. Diversity and Coding Gains Over QAM

The proof for our new STBCs achieving full diversity over every QAM constellation is based upon the following Lemma 3.1.

*Lemma 3.1:* $\mathbf{C}_1(z_1, \ldots, z_L)$ is full rank for every choice of

$$z_1, \ldots, z_L \in \mathbb{Q}(\mathbf{i}) := \{x_1 + x_2\mathbf{i} \mid x_1, x_2 \in \mathbb{Q}\}$$

with $z_1, \ldots, z_L$ not all zeros if and only if $L$ is a power of two, where $\mathbb{Q}$ is the field of rational numbers.

*Proof:* The case that $L$ is a power of two follows Propositions 3 and 5 in [6]. Suppose that $L = 2^m n$ with $n$ an odd number greater than one. When $m = 0$, we give a nonzero solution of the equation

$$\lambda(z_1, z_2, \ldots, z_L) = (\mathbf{i} z_L, z_1 \ldots, z_{L-1})$$

so the first and second rows of $\mathbf{C}_1(z_1, \ldots, z_L)$ are linearly dependent. Let $z_1 = 1$. Then $\lambda = \mathbf{i} z_L, z_2 = \lambda^{-1}, \ldots, z_L = \lambda^{-L+1}$ that implies $\lambda^L = \mathbf{i}$. This system has a particular solution as follows:

$$\begin{aligned}
&\text{if } L \equiv 1 \pmod 4\\
&\text{then } \lambda = \mathbf{i}, z_i = \begin{cases} 1, & \text{if } i \equiv 1 \pmod 4\\ -\mathbf{i}, & \text{if } i \equiv 2 \pmod 4\\ -1, & \text{if } i \equiv 3 \pmod 4\\ \mathbf{i}, & \text{if } i \equiv 0 \pmod 4 \end{cases};\\
&\text{if } L \equiv 3 \pmod 4\\
&\text{then } \lambda = -\mathbf{i}, z_i = \begin{cases} 1, & \text{if } i \equiv 1 \pmod 4\\ \mathbf{i}, & \text{if } i \equiv 2 \pmod 4\\ -1, & \text{if } i \equiv 3 \pmod 4\\ -\mathbf{i}, & \text{if } i \equiv 0 \pmod 4 \end{cases}.
\end{aligned}$$

For $m > 0$, simply let $z_i = 0$ if $i \not\equiv 1 \pmod{2^m}$ and consider the first and $(2^m + 1)$th rows in $\mathbf{C}_1(z_1, \ldots, z_L)$. It reduces back to the case of $m = 0$ and hence the proof is complete. □

*Corollary 3.2:* $\mathbf{C}_1(z_1, \ldots, z_L)^H$ and $\mathbf{C}_1(z_1, \ldots, z_L)^*$ are full rank for every $z_1, \ldots, z_L \in \mathbb{Q}(\mathbf{i})$ with $z_1, \ldots, z_L$ not all zeros if and only if $L$ is a power of two.

*Proposition 3.3:* Denote

$$\begin{aligned}\mathbf{D}_j &= \mathbf{S}_j(z_1, \ldots, z_{2L}) - \mathbf{S}_j(z_1', \ldots, z_{2L}')\\ &= \mathbf{S}_j(z_1 - z_1', \ldots, z_{2L} - z_{2L}')\end{aligned}$$

as the difference matrix of $\mathbf{S}_j(z_1, \ldots, z_{2L})$. For $j = 1, 2$,

a) $\mathbf{D}_j$ is full rank for every $z_1, z_1', \ldots, z_{2L}, z_{2L}' \in \mathbb{Q}(\mathbf{i})$ with $(z_1, \ldots, z_{2L}) \neq (z_1', \ldots, z_{2L}')$ if and only if $L$ is a power of two;

b) if $L$ is a power of two

$$\min_{\substack{z_1, z_1', \ldots, z_{2L}, z_{2L}' \in \mathbb{Z}(\mathbf{i})\\ (z_1, \ldots, z_{2L}) \neq (z_1', \ldots, z_{2L}')}} \left\{\det\left(\mathbf{D}_j \cdot \mathbf{D}_j^H\right)\right\} = 1$$

where

$$\mathbb{Z}(\mathbf{i}) := \{x_1 + x_2 \mathbf{i} \mid x_1, x_2 \in \mathbb{Z}\}$$

with $\mathbb{Z}$ the collections of integers.

*Proof:*

a) By setting $z_i = z_i'$ for all $i = L+1, \ldots, 2L$, the case that $L$ is not a power of two is solved by Lemma 3.1. Suppose that $L$ is a power of two. Since all the first $L$ columns of $\mathbf{S}_1(z_1, \ldots, z_{2L})$ are orthogonal to the others by Lemma 2.2, $\mathbf{D}_1 \cdot \mathbf{D}_1^H$ is a block diagonal matrix consisting of two $L \times L$ minors. Emerging with the ring structures of $\mathbb{S}_1$, we have

$$\mathbf{D}_1, \mathbf{D}_1^H, \mathbf{D}_1 \cdot \mathbf{D}_1^H$$

all belong to $\mathbb{S}_1$, which means that those two $L \times L$ minors are of the forms $\mathbf{C}_1(x_1, \ldots, x_L)$ and $\mathbf{C}_1(x_1, \ldots, x_L)^H$, respectively, with

$$x_1 = \sum_{i=1}^{2L} \left|z_i - z_i'\right|^2 > 0.$$

Since $L$ is a power of two, from Lemma 3.1 and Corollary 3.2 these two minors are full rank and their determinants are nonzero. Hence

$$\det\left(\mathbf{D}_1 \cdot \mathbf{D}_1^H\right) \neq 0.$$

Applying similar arguments to $j = 2$, the assertions are complete.

b) Following

$$\det\left(\mathbf{D}_j \cdot \mathbf{D}_j^H\right) = \left|\det\left(\mathbf{D}_j\right)\right|^2$$

and the fact that $\mathbb{Z}(\mathbf{i})$ is closed under addition and multiplication, $\det\left(\mathbf{D}_j \cdot \mathbf{D}_j^H\right)$ is a nonnegative integer for every choice of $z_1, z_1', \ldots, z_{2L}, z_{2L}' \in \mathbb{Z}(\mathbf{i})$. Combining with a), $\det\left(\mathbf{D}_j \cdot \mathbf{D}_j^H\right)$ is a positive integer for every choice of $z_1, z_1', \ldots, z_{2L}, z_{2L}' \in \mathbb{Z}(\mathbf{i})$ with

$$(z_1, \ldots, z_{2L}) \neq (z_1', \ldots, z_{2L}').$$

Setting

$$z_1 - 1 = z_1' = z_2 = z_2' = \cdots = z_{2L} = z_{2L}' = 0$$

achieves the minimum. □

The analytic expressions of performance can be summarized as follows.

*Theorem 3.4:* Denote $d_{\min}$ as the minimum Euclidean distance of an arbitrary QAM constellation $\mathcal{A}$. For $j = 1, 2$:

a) the STBC $\mathbf{S}_j(z_1, \ldots, z_{2L})$ achieves full diversity over every QAM constellation if and only if $L$ is a power of two;

b) if $L$ is a power of two

$$\min_{\substack{z_1, z_1', \ldots, z_{2L}, z_{2L}' \in \mathcal{A}\\ (z_1, \ldots, z_{2L}) \neq (z_1', \ldots, z_{2L}')}} \left\{\det\left(\mathbf{D}_j \cdot \mathbf{D}_j^H\right)\right\} = d_{\min}^{4L}. \quad (5)$$

*Proof:* When $\mathbf{D}_j$ is full rank for every arbitrary choice of $z_1, z_1', \ldots, z_{2L}, z_{2L}' \in \mathbb{Q}(\mathbf{i})$ with $(z_1, \ldots, z_{2L}) \neq (z_1', \ldots, z_{2L}')$, surely $\mathbf{S}_j(z_1, \ldots, z_{2L})$ reaches full diversity over every QAM constellation. On the other hand, if $\mathbf{D}_j$ is not full rank for some $z_1, z_1', \ldots, z_{2L}, z_{2L}' \in \mathbb{Q}(\mathbf{i})$ with

$$(z_1, \ldots, z_{2L}) \neq (z_1', \ldots, z_{2L}')$$

there is always a positive integer $m$ such that

$$m z_i, m z_i' \in \mathbb{Z}(\mathbf{i})$$

for all $i = 1, \ldots, 2L$ by $L$ being finite. Choosing $\mathcal{A}$ as the QAM constellation containing all points

$$m z_1, m z_1', \ldots, m z_{2L}, m z_{2L}'$$

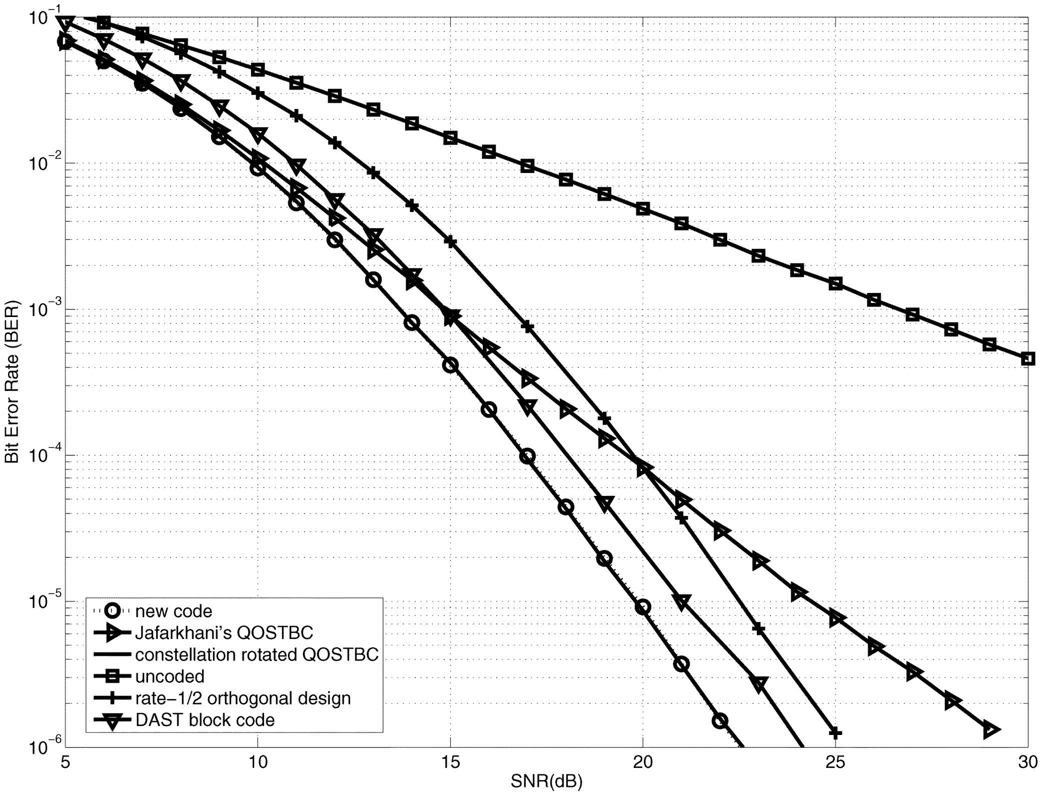

Fig. 1. BER performance for four Tx antennas and one Rx antenna transmission schemes at 2 b/s/Hz.

$\mathbf{S}_j(z_1,\ldots,z_{2L})$ cannot achieve full diversity over $\mathcal{A}$. The rest follows Proposition 3.3. □

Other than $\mathbf{S}_1(z_1,\ldots,z_{2L})$ and $\mathbf{S}_2(z_1,\ldots,z_{2L})$, we can assign the elements of $\mathbb{G}$ to the generalized quaternion group of order $8L$ in different combinations to obtain other STBCs. In fact, if two matrices $\mathbf{M}_1$ and $\mathbf{M}_2$ are representable by the same group, they would just differ by some elementary row operations. More precisely, there exists an invertible matrix $\mathbf{U}$ such that

$$\mathbf{U}^{-1}\cdot\mathbf{M}_1\cdot\mathbf{U}=\mathbf{M}_2$$

with each entry of $\mathbf{U}$ and $\mathbf{U}^{-1}$ coming from $\{\pm 1,\pm\mathbf{i},0\}$. Thus $\mathbf{M}_1$ reaches full diversity for a specific constellation if and only if $\mathbf{M}_2$ does, too, and the determinants of their difference matrices are always identical to each other. Since the coding gain is determined by the determinant of difference matrix, $\mathbf{M}_1$ and $\mathbf{M}_2$ share the same coding gain. In other words, two STBCs representable by a common group have the same diversity and coding gains, i.e., the same asymptotic performance.

Let us take more insightful focuses on the designing process of $\mathbf{S}_1(z_1,\ldots,z_{2L})$, in which a scheme for establishing STBCs of size $2L$ with the form

$$\begin{pmatrix}\mathbf{M}_1 & \mathbf{M}_2\\ -\mathbf{M}_2^H & \mathbf{M}_1^H\end{pmatrix}$$

and

$$\mathbf{M}_1\cdot\mathbf{M}_2=\mathbf{M}_2\cdot\mathbf{M}_1$$

is provided. The most natural thought for constructing STBCs such that $\mathbf{M}_1$ and $\mathbf{M}_2$ are commutative for arbitrary complex values $z_1,\ldots,z_{2L}$ is to look for a size $L$ STBC that is a commutative ring, or equivalently to apply an abelian group of order $4L$ from Lemma 2.1. For instance, $\mathbf{S}_1(z_1,\ldots,z_{2L})$ utilizes the cyclic group of order $4L$ to construct the two $L\times L$ minors $\mathbf{C}_1(z_1,\ldots,z_L)$ and $\mathbf{C}_1(z_{L+1},\ldots,z_{2L})$, or the commutative ring

$$\{\mathbf{C}_1(x_1,\ldots,x_L)\mid x_1,\ldots,x_L\in\mathbb{C}\}.$$

Lemma 3.1 concludes that cyclic groups whose orders are powers of two are feasible to fit this mechanism. For noncyclic abelian groups, the following Theorem 3.5 claims that it is impossible to get a size $L$ full-diversity STBC over every QAM constellation.

*Theorem 3.5:* If $\mathbb{G}$ is an Abelian group of order $4L$, then the size $L$ STBC $\mathbf{S}(z_1,\ldots,z_L)$ constructed through $(\mathbf{a})\sim(\mathbf{h})$ derived in Section II achieves full diversity over every QAM constellation if and only if $\mathbb{G}$ is a cyclic group with $L$ a power of two.

*Proof:* When $\mathbb{G}$ is cyclic, Lemma 3.1 tells that $\mathbf{S}(z_1,\ldots,z_L)$ reaches full diversity over every QAM constellation if and only if $L$ is a power of two.

If $\mathbb{G}$ is noncyclic, by the fundamental theorem for Abelian groups, $\mathbb{G}$ is isomorphic to the direct sum

$$\mathbb{Z}/m_1\mathbb{Z}\oplus\cdots\oplus\mathbb{Z}/m_r\mathbb{Z}$$

with positive integers $m_1,\ldots,m_r$. If there is an $m_i$ that is not a power of two, then $\mathbf{S}(z_1,\ldots,z_L)$ would contain a minor $\mathbf{M}$ that is the same as the STBC constructed by adopting $\mathbb{Z}/m_i\mathbb{Z}$ in Lemma 2.1 and the consequences $(\mathbf{a})\sim(\mathbf{h})$. By Lemma 3.1, $\mathbf{M}$ cannot reach full diversity over every QAM constellation and nor can $\mathbf{S}(z_1,\ldots,z_L)$. Therefore, we only have to consider the case that $m_1,\ldots,m_r$ are all powers of two, in which there are more than one element in $\mathbb{G}$ of order 2. Since $\mathbf{S}(\mathbf{e}_1)$ is the identity matrix, the diagonal entries of $\mathbf{S}(z_1,\ldots,z_L)$ are either $z_1$ or $z_1^*$, and $-\mathbf{S}(\mathbf{e}_1)$ and $\pm\mathbf{S}(\mathbf{e}_1')$ are of order 2 and 4, respectively. Suppose that $\mathbf{S}(\mathbf{e}_i)$ is of order 2 for some $i\neq 1$, i.e.

$$\mathbf{S}(\mathbf{e}_i)\cdot\mathbf{S}(\mathbf{e}_i)=\mathbf{S}(\mathbf{e}_1).$$

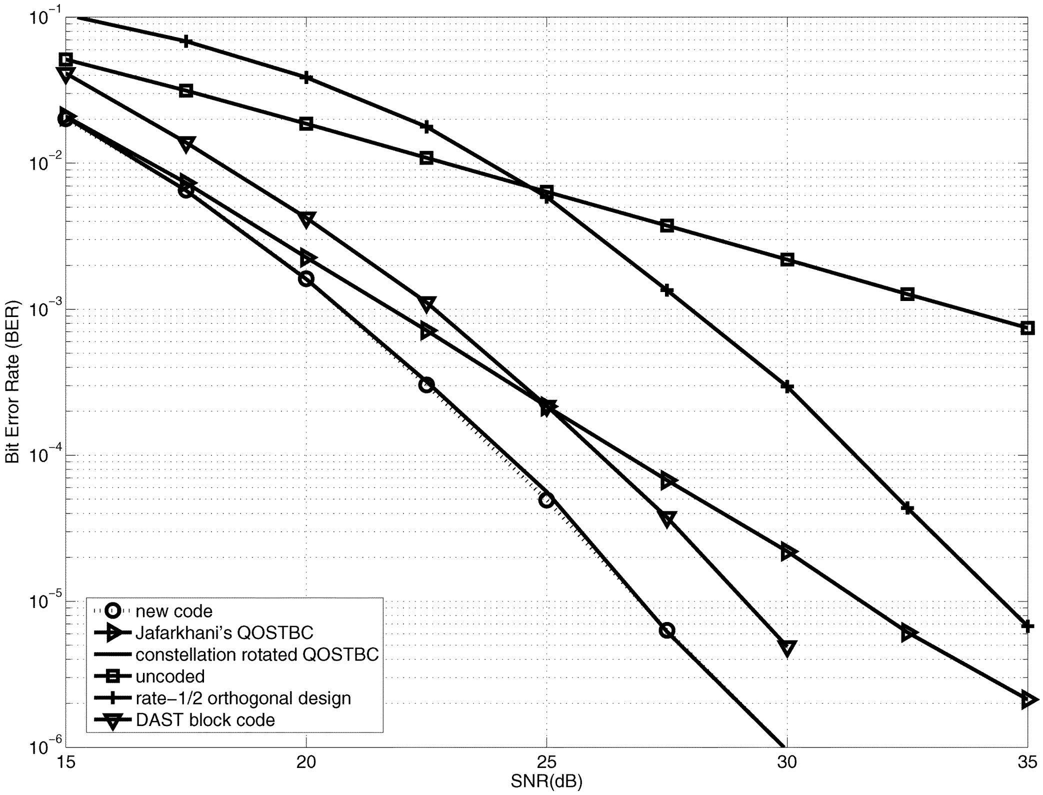

Fig. 2. BER performance for four Tx antennas and one Rx antenna transmission schemes at 4 b/s/Hz.

By $(\mathbf{a}) \sim (\mathbf{h})$, the $(i,1)$-th entry of $\mathbf{S}(z_1,\ldots,z_L)$ is either $z_i$ or $z_i^*$, and there is no entry in the $i$th row related with $z_1$ and $z_i$ except the $(i,1)$th and $(i,i)$-th entries. Setting $z_1 = z_i = 1$ and $z_j = 0$ for $j \neq 1, i$, the first and $i$-th rows of $\mathbf{S}(z_1,\ldots,z_L)$ become simultaneously $\mathbf{e}_1 + \mathbf{e}_i$, which tells that $\mathbf{S}(\mathbf{e}_1 + \mathbf{e}_i)$ is not full rank. Similar results would happen if there exists one element $\mathbf{S}(\mathbf{e}_i')$ whose order is 2 for some $i \neq 1$. □

## IV. Simulation Results and Discussions

In this section, the BER performance of the transmission schemes derived in Section II and [4], [5], [7] as well as the orthogonal design in [8] for $4 \times 1$ MISO systems is presented. Fig. 1 shows the simulation results at 2 b/s/Hz, in which 4-QAM is used for all encoding schemes except applying 16-QAM for the rate-$1/2$ orthogonal design. In Fig. 2, we adopt 16-QAM for all encoding schemes except applying 256-QAM for the rate-$1/2$ orthogonal design. At the receiver side, the ML decoding is implemented to extract diversity provided by the transmitter. Quasi-static Rayleigh and independent fading paths are assumed so the channel gains are modeled by independent zero mean circularly symmetric complex Gaussian random variables. Since two STBCs representable by a common group have the same diversity and coding gains, the new code is selected as the matrix (4) with $L = 2$. For the QOSTBC with constellation rotation, the rotation angle $\phi = \pi/4$ is chosen according to [7]. Hence, in those figures, the codes that do not achieve full diversity are the Jafarkhani's QOSTBC and the uncoded scheme. All the other codes satisfy the rank criterion in [9] and therefore have full diversity.

It is found that the new code, the constellation rotated QOSTBC, and the DAST block code all have the same value of (5). Therefore, those three codes achieve the maximum possible diversity product [7] or the minimum product distance [4] over QAM. The rate-$1/2$ orthogonal design has a smaller value of (5) so its performance is about 3 dB and 7.5 dB worse than the new code at data rates 2 and 4 b/s/Hz, respectively. It is also observed that the new code and the constellation rotated QOSTBC perform about 2 dB better than the DAST block code, which is substantiated by examining the numbers of distinct symbol pairs that have the minimum product distance in Table I.

TABLE I
Numbers of Distinct Symbol Pairs Having the Minimum Product Distance for Full-Diversity Codes

| | 4-QAM | 16-QAM |
|---|---|---|
| new code | 1536 | 901120 |
| constellation rotated QOSTBC | 1536 | 901120 |
| DAST block code | 3136 | 3755136 |

On the other hand, the multiplication with $\mathbf{i}$ on any QAM symbol in the new codes does not generate new constellation points, i.e., all of the transmitted symbols still belong to the original QAM constellation points. Because the optimal rotation angles of QOSTBCs with constellation rotations cannot be $\pi/2$, additional constellations have to be used both at the transmitter and receiver.

As far as the ML decoders are concerned, the DAST block codes only reach full diversity with nonorthogonality. Thus, all the received signals in a block have to be decoded together by the ML decoding and sphere decoders [10] have to be regarded to lower the decoding complexity. Contrarily, the new codes and the QOSTBCs with constellation rotations have less decoding complexity due to their partial orthogonality so that the ML decoders can be done by dividing symbols into sets with smaller cardinalities, as proposed in [5].

## V. Conclusion

Based upon the motivation of designing STBCs having ring structures over the complex number field, a whole new family of rate-1 STBCs is provided via a group-theoretic methodology. They achieve full diversity over every QAM constellation when the number of Tx antennas is a power of two. With an orthogonality-preserving scheme, the computational complexity for the ML decoding at the receiver side can be reduced significantly. Moreover, no extra and irregular constellation has to be used. Hence the proposed code designs certainly provide a method capable of achieving both high performance and simple implementations.

## ACKNOWLEDGMENT

The authors would like to thank the anonymous referees for their helpful comments and suggestions, which greatly improved the correctness as well as the presentation of this correspondence.

## REFERENCES

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

[2] C.-Y. Chen, M.-Y. Chen, and J. M. Cioffi, "Full-diversity quasi-orthogonal space-time block codes for M-PSK modulations," in *Proc. 2005 IEEE Global Telecommun. Conf. GLOBECOM 2005*, St. Louis, MO, Nov.–Dec. 2005, vol. 5, pp. 3022–3026.

[3] M.-Y. Chen, C.-Y. Chen, H.-C. Li, S.-C. Pei, and J. M. Cioffi, "Deriving new quasi-orthogonal space-time block codes and relaxed designing viewpoints with full transmit diversity," in *Proc. 2005 IEEE Int. Conf. Commun., ICC 2005*, Seoul, Korea, May 2005, vol. 5, pp. 2922–2926.

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

[5] H. Jafarkhani, "A quasi-orthogonal space-time block code," *IEEE Trans. Commun.*, vol. 49, pp. 1–4, Jan. 2001.

[6] 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, pp. 2596–2616, Oct. 2003.

[7] W. Su and X.-G. Xia, "Signal constellations for quasi-orthogonal space-time block codes with full diversity," *IEEE Trans. Inf. Theory*, vol. 50, pp. 2331–2347, Oct. 2004.

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

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

[10] E. Viterbo and J. Boutros, "A universal lattice code decoder for fading channels," *IEEE Trans. Inf. Theory*, vol. 45, pp. 1639–1642, Jul. 1999.

# The Moments of a Kloosterman Sum and the Weight Distribution of a Zetterberg-Type Binary Cyclic Code

Marko J. Moisio

***Abstract*—In this correspondence, we give the moments of a Kloosterman sum over $\mathbb{F}_q$ in terms of the frequencies of weights in the binary Zetterberg code of length $q+1$, which are known by the work of Schoof and van der Vlugt. The method is illustrated by giving explicit formulae for the moments up to the tenth moment. As a corollary the weight distribution of a Zetterberg-type binary cyclic code is obtained.**

***Index Terms*—Cyclic code, exponential sum, Kloosterman sum, Pless power moments, weight distribution, Zetterberg code.**

## I. INTRODUCTION

Kloosterman sums over finite fields of characteristic 2 have extensively been studied from various point of views and have been used in solving a variety of problems from coding theory see, e.g., [6], [8], [3], [13], [5].

In this correspondence an old problem concerning the evaluation of moments, or power sums, of a Kloosterman sum is considered. More presicely, let $r \geq 3$ be an integer and let $q = 2^r$. Let $h$ be a nonnegative integer. Let $\mathrm{tr}$ denote the trace function from $\mathbb{F}_q$ onto $\mathbb{F}_2$, and let

$$K_h := \sum_{a \in \mathbb{F}_q^*} k(a)^h \tag{1}$$

denote the $h$th moment of the Kloosterman sum

$$k(a) := \sum_{x \in \mathbb{F}_q^*} (-1)^{\mathrm{tr}(x+ax^{-1})}.$$

Obviously $K_0 = q - 1$. Furthermore, there are elementary proofs for the following formulas:

$$\begin{aligned} &K_1 = 1, \quad K_2 = q^2 - q - 1, \quad K_3 = (-1)^r q^2 + 2q + 1 \\ &K_4 = 2q^3 - 2q^2 - 3q - 1 \\ &K_6 = 5q^4 - (5 + (-1)^r)q^3 - 9q^2 - 5q - 1. \end{aligned}$$

The formulae for $K_1$, $K_2$, $K_3$, and $K_4$ were obtained by Carlitz in [1] (see also [6], [3]), and the sixth moment was evaluated in [13].

In this correspondence we are able to go much further by connecting the moments to the frequencies of weights in the binary Zetterberg code of length $q+1$, which were obtained in [16] in terms of the traces of certain Hecke operators acting on spaces of cusp forms for the congruence subgroup $\Gamma_1(4) \subset SL_2(\mathbb{Z})$.

The explicit formulae for the number of low-weight codewords in the Zetterberg code given in [16, Table 6.2] (see also Remark 2), together with our Theorem 5 below, give, with help of the symbolic manipulation language *Mathematica*, e.g., the following new moments.

*Theorem 1:* Let $q = 2^r$ with $r \geq 3$. Then

$$\begin{aligned} K_5 &= (t_7 + (-1)^r 4)q^3 + 5q^2 + 4q + 1 \\ K_7 &= (t_9 + 6t_7 + (-1)^r 14 + 1)q^4 \\ &\quad + 14q^3 + 14q^2 + 6q + 1 \\ K_8 &= 14q^5 - (15 + (-1)^r 7)q^4 \\ &\quad - 28q^3 - 20q^2 - 7q - 1 \end{aligned}$$

Manuscript received December 27, 2005; revised October 20, 2006.

The author is with the Department of Mathematics and Statistics, University of Vaasa, FIN-65101 Vaasa, Finland (e-mail: mamo@uwasa.fi).

Communicated by R. J. McEliece, Associate Editor for Coding Theory.

Digital Object Identifier 10.1109/TIT.2006.889020