so the bound in (22) applies with $\epsilon = \sqrt{\frac{1}{2}\log D/\log q}$. Plugging this value of ϵ into (22) and manipulating the resulting expression, we obtain the bound of the theorem. □

Acknowledgment

The authors are grateful to the anonymous reviewers for their suggestions which led to a significantly improved presentation of the results in the correspondence and to Dr. Marc P. C. Fossorier for handling the manuscript. The authors would also like to thank Stefan Laendner and Daniel Bennett for helping with some of the simulations.

References

[1] F. Behrend, "On the sets of integers which contain no three in arithmetic progression," *Proc. Nat. Acad. Sci.*, vol. 23, pp. 331–332, 1946.

[2] C. Berge, *Hypergraphs: Combinatorics of Finite Sets*. Amsterdam, The Netherlands: North-Holland, Mathematical Library, 1989, vol. 45.

[3] N. Biggs, *Algebraic Graph Theory*, 2nd ed. Cambridge, U.K.: Cambridge Univ. Press, 1993.

[4] A. Bosznay, "On the lower estimation of nonaveraging sets," *Acta Math. Hung.*, vol. 53, pp. 155–157, 1989.

[5] J. L. Fan, "Array codes as low-density parity-check codes," in *Proc. 2nd Int. Symp. Turbo Codes and Related Topics*, Brest, France, Sep. 2000, pp. 553–556.

[6] M. P. C. Fossorier, "Quasi-cyclic low-density parity-check codes from circulant permutation matrices," *IEEE Trans. Inf. Theory*, vol. 50, no. 8, pp. 1788–1794, Aug. 2004.

[7] P. Frankl, R. L. Graham, and V. Rödl, "Quantitative theorems for regular systems of equations," *J. Combin. Theory Ser. A*, vol. 47, pp. 246–261, 1988.

[8] R. G. Gallager, *Low-Density Parity-Check Codes*. Cambridge, MA: MIT Press, 1963.

[9] R. L. Graham, B. L. Rothschild, and J. H. Spencer, *Ramsey Theory*, 2nd ed. New York: Wiley-Interscience, 1990.

[10] M. Greferath, M. E. O'Sullivan, and R. Smarandache, "Construction of good LDPC codes using dilation matrices," in *Proc. IEEE Intl. Symp. Information Theory*, Chicago, IL, Jun./Jul. 2004, p. 235.

[11] S. Hoory, "The size of bipartite graphs with a given girth," *J. Comb. Theory Ser. B*, vol. 86, no. 2, pp. 215–220, 2002.

[12] S. Johnson and S. R. Weller, "Regular low-density parity-check codes from combinatorial designs," in *Proc. Information Theory Workshop (ITW 2001)*, Cairns, Australia, Jan. 2001, pp. 90–92.

[13] J.-L. Kim, U. Peled, I. Perepelitsa, V. Pless, and S. Friedland, "Explicit construction of families of LDPC codes with no 4-cycles," *IEEE Trans. Inf. Theory*, vol. 50, no. 10, pp. 2378–2388, Oct. 2004.

[14] Y. Kou, S. Lin, and M. P. C. Fossorier, "Low-density parity-check codes based on finite geometries: A rediscovery and new results," *IEEE Trans. Inf. Theory*, vol. 47, no. 7, pp. 2711–2736, Nov. 2001.

[15] B. Landman and A. Robertson, *Ramsey Theory on the Integers*. Providence, RI: AMS , 2004.

[16] F. Lazebnik and V. A. Ustimenko, "Explicit construction of graphs with arbitrary large girth and of large size," *Discr. Appl. Math.*, vol. 60, pp. 275–284, 1997.

[17] D. J. C. MacKay, *Information Theory, Inference, and Learning Algorithms*. Cambridge, U.K.: Cambridge Univ. Press, 2003.

[18] D. J. C. MacKay and M. C. Davey, , B. Marcus and J. Rosenthal, Eds. , "Evaluation of Gallager codes for short block length and high rate applications," in *Codes, Systems and Graphical Models*. New York: Springer-Verlag, 2000, vol. 123, IMA Volumes in Mathematics and its Applications, pp. 113–130.

[19] G. A. Margulis, "Explicit constructions of graphs without short cycles and low density codes," *Combinatorica*, vol. 2, no. 1, pp. 71–78, 1982.

[20] O. Milenkovic, K. Prakash, and B. Vasic, "Regular and irregular low-density parity-check codes for iterative decoding," in *Proc. 41st Allerton Conf. Communication, Control and Computing*, Monticello, IL, Sep. 2003, pp. 1700–1701.

[21] L. Moser, "On nonaveraging sets of integers," *Canadian J. Math.*, vol. 5, pp. 245–252, 1953.

[22] J. K. Moura, J. Lu, and H. Zhang, "Structured LDPC codes with large girth," *IEEE Signal Process. Mag.*, vol. 21, no. 1, pp. 42–55, Jan. 2004.

[23] K. O'Bryant, "Sidon sets and Beatty sequences," Ph.D. dissertation, Univ. Illinois at Urbana-Champaign, Urbana, IL, 2002.

[24] A. M. Odlyzko and R. P. Stanley, Some Curious Sequences Constructed With the Greedy Algorithm 1978 [Online]. Available: www.dtc.umn.edu/~odlyzko/unpublished/greedy.sequence.ps, unpublished

[25] R. A. Rankin, "Sets of integers containing not more than a given number of terms in arithmetic progression," *Proc. Roy. Soc. Edinburgh Sect. A*, vol. 65, pp. 332–344, 1962.

[26] J. Rosenthal and P. O. Vontobel, "Constructions of regular and irregular LDPC codes using Ramanujan graphs and ideas from Margulis," in *Proc. Int. Symp. Information Theory*, Washington, DC, Jun. 2001, p. 4.

[27] R. M. Tanner, D. Sridhara, and T. Fuja, "A class of group-structured LDPC codes," in *Proc. 6th Int. Symp. Communication Theory and Applications* , Ambleside, U.K., Jul. 2001, pp. 365–370.

[28] R. M. Tanner, "A recursive approach to low complexity codes," *IEEE Trans. Inf. Theory*, vol. IT-27, no. 5, pp. 533–548, Sep. 1981.

[29] B. Vasic and O. Milenkovic, "Combinatorial constructions of LDPC codes," *IEEE Trans. Inf. Theory*, vol. 50, no. 6, pp. 1156–1176, Jun. 2004.

[30] B. Vasic, K. Pedagani, and M. Ivkovic, "High-rate girth-eight LDPC codes on rectangular integer lattices," *IEEE Trans. Commun.*, vol. 52, no. 8, pp. 1248–1252, Aug. 2004.

Geometrical and Numerical Design of Structured Unitary Space–Time Constellations

Guangyue Han and Joachim Rosenthal, *Senior Member, IEEE*

***Abstract*—There exist two important design criteria for unitary space time codes. In the situation where the signal-to-noise ratio (SNR) is large the *diversity product* (DP) of a constellation should be as large as possible. It is less known that the *diversity sum* (DS) is a very important design criterion for codes working in a low SNR environment. So far, no general method to design good-performing constellations with large diversity for any number of transmit antennas and any transmission rate exists.**

In this correspondence, we propose constellations with suitable structures, which allow one to construct codes with excellent diversity using geometrical symmetry and numerical methods. The presented design methods work for any dimensional constellation and for any transmission rate.

***Index Terms*—Diversity product, diversity sum, multiple antennas, space–time coding, space–time constellations.**

I. Introduction and Model

One way to acquire reliable transmission with high transmission rate on a wireless channel is to use multiple transmit or receive antennas. Either because of rapid changes in the channel parameters or because of limited system resources, it is reasonable to assume that both the transmitter and the receiver do not know about the channel state information (CSI), i.e., the channel is noncoherent.

Manuscript received December 3, 2003; revised September 27, 2005. This work was supported in part by the National Science Foundation inder Grants DMS-00-72383 and CCR-02-05310. The work of G. Han was also supported by a fellowship from the Center of Applied Mathematics at the University of Notre Dame. The material in this correspondence was presented in part at the 40th Annual Allerton Conference on Communication, Control, and Computing, Monticello, IL, October 2002 and the IEEE International Symposium on Information Theory, Yokohama, Japan, June/July 2003.

G. Han is with the Department of Mathematics, The University of British Columbia, Vancouver, BC V6T 1Z2, Canada (e-mail: ghan@math.ubc.ca).

J. Rosenthal is with the Department of Mathematics, University of Zürich, CH-8057 Zürich, Switzerland (e-mail: rosen@math.unizh.ch).

Communicated by B. Hassibi, Associate Editor for Communications.

Digital Object Identifier 10.1109/TIT.2006.878107

In [14], Hochwald and Marzetta study unitary space–time modulation. Consider a wireless communication system with M transmit antennas and N receive antennas operating in a Rayleigh flat-fading channel. We assume time is discrete and at each time slot, signals are transmitted simultaneously from the M transmit antennas. We can further assume that the wireless channel is quasi-static over a time block of length T.

A signal constellation $\mathcal{V} := \{\Phi_1, \ldots, \Phi_L\}$ consists of L matrices having size $T \times M$ and satisfying $T \geq M$ and $\Phi_k^* \Phi_k = I_M$. The last equation simply states that the columns of Φ_k form a "unitary frame," i.e., the column vectors all have unit length in the complex vector space $\mathbb{C}^T$ and the vectors are pairwise orthogonal. The scaled matrices $\sqrt{T}\Phi_k, k = 1, 2, \ldots, L$, represent the codewords used during the transmission. It is known that the transmission rate is determined by L and T

$$\mathtt{R} = \frac{\log_2(L)}{T}.$$

Let ρ represent the expected signal-to-noise ratio (SNR) at each receive antenna. The basic equation between the received signal R and the transmitted signal $\sqrt{T}\Phi$ is given through

$$R = \sqrt{\frac{\rho T}{M}} \Phi H + W$$

where the $M \times N$ matrix H accounts for the multiplicative complex Gaussian fading coefficients and the $T \times N$ matrix W accounts for the additive white Gaussian noise. The entries $h_{m,n}$ of the matrix H as well as the entries $w_{t,n}$ of the matrix W are assumed to have a statistically independent normal distribution $\mathcal{CN}(0, 1)$. In particular, it is assumed that the receiver does not know the exact values of either the entries of H or W (other than their statistical distribution).

The decoding task asks for the computation of the most likely sent codeword Φ given the received signal R. Denote by $\| \ \|_F$ the Frobenius norm of a matrix. If $A = (a_{i,j})$ then the Frobenius norm is defined through $\|A\|_F = \sqrt{\sum_{i,j} |a_{i,j}|^2}$. Under the assumption of the above model the maximum-likelihood (ML) decoder will have to compute

$$\Phi_{ML} = \arg \max_{\Phi_l \in \{\Phi_1, \Phi_2, \ldots, \Phi_L\}} \|R^* \Phi_l\|_F$$

for each received signal R (see [14]).

Let $\delta_m(\Phi_l^* \Phi_{l'})$ be the mth singular value of $\Phi_l^* \Phi_{l'}$. It has been shown in [14] that the pairwise probability of mistaking Φ_l for $\Phi_{l'}$ using ML decoding satisfies

$$\begin{aligned} P_{\Phi_l, \Phi_{l'}} &= \mathrm{Prob}\,(\text{choose } \Phi_{l'} \mid \Phi_l \text{transmitted})\,(\rho) \\ &= \mathrm{Prob}\,(\text{choose } \Phi_l \mid \Phi_{l'} \text{ transmitted})\,(\rho) \\ &\leq \frac{1}{2} \prod_{m=1}^{M} \left[1 + \frac{(\rho T/M)^2 (1 - \delta_m^2(\Phi_l^* \Phi_{l'}))}{4(1 + \rho T/M)} \right]^{-N}. \end{aligned} \quad (1.1)$$

It is a basic design objective to construct constellations $\mathcal{V} = \{\Phi_1, \ldots, \Phi_L\}$ such that the pairwise probabilities $P_{\Phi_l, \Phi_{l'}}$ are as small as possible. Mathematically, we are dealing with an optimization problem with unitary constraints:

Minimize $\max_{l \neq l'} P_{\Phi_l, \Phi_{l'}}$ with the constraints $\Phi_i^* \Phi_i = I$ where $i = 1, 2, \ldots, L$.

Formula (1.1) is sometimes referred to as "Chernoff's bound." Researchers have been searching for constructions where the maximal pairwise probability of $P_{\Phi_l, \Phi_{l'}}$ is as small as possible. Of course the pairwise probabilities depend on the chosen SNR ρ and the construction of constellations has therefore to be optimized for particular values of the SNR.

The design objective is slightly simplified if one assumes that transmission operates at high-SNR situations. In [13], a design criterion for high SNR is presented and the problem has been converted to the design of a finite set of unitary matrices whose diversity product is as large as possible. In this special situation, several researchers [2], [22]–[24] came up with algebraic constructions and we will say more about this in the next section.

The main purpose of this correspondence is to present structured constellation and to develop geometrical and numerical procedures which allow one to construct unitary constellations with excellent diversity for any set of parameters M, N, T, L and for any SNR ρ. The correspondence is structured as follows. In Section II, we illustrate unitary space–time constellation design criteria and present certain example constellations.

In Section III, we parameterize constellations which will be efficient for numerical search algorithms. For this purpose, we introduce the concept of a weak group structure and we classify all weak group structures whose elements are normal and positive.

In Section IV, we investigate an algebraic structure which led to some of the best constellations which we were able to derive. We also show that in the good-performing codes the distance spectrum profile for both the diversity sum and the diversity product are important.

Section V is one of the main sections of this correspondence. We first explain a general method on how one can efficiently design excellent constellations for any set of parameters M, N, T, L, and ρ. For this we review the Cayley transform. We conclude this section with an extensive table where we publish a large set of codes having some of the best diversity sums and diversity products in their parameter range. More extensive lists of codes with large diversity can be found on the website [6].

Finally, in Section VI, we explain how the algebraic structure which underlies most of the derived codes can be used to have a fast decoding algorithm. Our simulations indicate that in the design of codes more attention should be given to the diversity sum which previously has not been fully studied.

II. Constellation Design Criteria and Examples

In this correspondence, we will be concerned with the construction of constellations where the right-hand side in (1.1), maximized over all pairs l, l' is as small as possible for fixed numbers of T, M, N, L. This task depends on the SNR the system is operating. We consider designing constellations for high- and low-SNR cases.

A. Design Criterion for High-SNR Channel

In high-SNR scenario, namely, when ρ is large, maximizing the constellation performance boils down to designing a constellation with large diversity product:

Definition 2.1: (See [13]) The *diversity product* of a unitary constellation $\mathcal{V}$ is defined as

$$\prod \mathcal{V} = \min_{l \neq l'} \left(\prod_{m=1}^{M} (1 - \delta_m(\Phi_l^* \Phi_{l'})^2) \right)^{\frac{1}{2M}}.$$

An important special case occurs when $T = 2M$. In this situation, it is customary to represent all unitary matrices Φ_k in the form

$$\Phi_k = \frac{\sqrt{2}}{2} \begin{pmatrix} I \\ \Psi_k \end{pmatrix}. \quad (2.1)$$

Note that by definition of Φ_k, the matrix Ψ_k is an $M \times M$ unitary matrix. The diversity product as defined in Definition 2.1 has then a nice form in terms of the unitary matrices. For this, let λ_m be the mth eigenvalue of a matrix, then

$$\begin{aligned}1-\delta_m^2(\Phi_{l'}^*\Phi_l) &= \frac{1}{4}\lambda_m(2I_M-\Phi_l^*\Phi_{l'}-\Phi_{l'}^*\Phi_l)\\ &= \frac{1}{4}\delta_m^2(I_M-\Psi_{l'}^*\Psi_l)=\frac{1}{4}\delta_m^2(\Psi_{l'}-\Psi_l).\end{aligned}$$

So we have

$$\begin{aligned}\prod_{m=1}^{M}(1-\delta_m^2(\Phi_{l'}^*\Phi_l))^{\frac{1}{2M}} &= \frac{1}{2}\prod_{m=1}^{M}\delta_m(\Psi_{l'}-\Psi_l)^{\frac{1}{M}}\\ &= \frac{1}{2}|\det(\Psi_{l'}-\Psi_l)|^{\frac{1}{M}}.\end{aligned}$$

When $T=2M$ and the constellation $\mathcal{V}$ is defined as above, then the formula of the diversity product assumes the simple form

$$\prod\mathcal{V}=\frac{1}{2}\min_{0\le l<l'\le L}|\det(\Psi_l-\Psi_{l'})|^{\frac{1}{M}}. \tag{2.2}$$

We call a constellation $\mathcal{V}$ a fully diverse constellation if $\prod\mathcal{V}>0$. A lot of efforts have been taken to construct constellations with large diversity product. (See e.g., [13], [17], [8], [7], [22]–[24].) For the particular situation $T=2M$ with special form (2.1) the design asks for the construction of a discrete subset $\mathcal{V}=\{\Psi_1,\ldots,\Psi_L\}$ of the set of $M\times M$ unitary matrices $U(M)$. When this discrete subset has the structure of a discrete subgroup of $U(M)$ then the condition that $\mathcal{V}$ is fully diverse is equivalent to the condition that the identity matrix is the only element of $\mathcal{V}$ having an eigenvalue of 1. In other words, the constellation $\mathcal{V}$ is required to operate fixed point free on the vector space $\mathbb{C}^M$. Using a classical classification result of fixed point free unitary representations by Zassenhaus [26], Shokrollahi *et al.* [22], [23] were able to study the complete list of fully diverse finite group constellations inside the unitary group $U(M)$. Some of these constellations have the best known diversity product for given fixed parameters M, N, L.

In most of the literature mentioned above, researchers focus their attention on constellations having the special form (2.1). Unitary differential modulation [13] is used to avoid sending the identity (upper part of every element in the constellation) redundantly. This increases the transmission rate by a factor of 2 to

$$\mathtt{R}=\frac{\log_2(L)}{M}=2\frac{\log_2(L)}{T}.$$

Because of this reason we will also focus ourselves in the later part of the correspondence on the special form (2.1) as well. The numerical techniques presented in this correspondence work in all situations.

B. Design Criterion for Low-SNR Channel

At low-SNR regime, we consider diversity sum as the design criterion for unitary space time constellation.

Definition 2.2: The *diversity sum* of a unitary constellation $\mathcal{V}$ is defined as

$$\sum\mathcal{V}=\min_{l\ne l'}\sqrt{1-\frac{\|\Phi_l^*\Phi_{l'}\|_F^2}{M}}.$$

Again one has the important special case where $T=2M$ and the matrices Φ_k take the special form (2.1). In this case, one verifies that

$$\begin{aligned}\|\Phi_l^*\Phi_{l'}\|_F^2 &= \frac{1}{4}\|I+\Psi_l^*\Psi_{l'}\|_F^2=\frac{1}{4}\mathrm{tr}\,((I+\Psi_{l'}^*\Psi_l)(I+\Psi_l^*\Psi_{l'}))\\ &= \frac{1}{4}\mathrm{tr}\,(2I+\Psi_{l'}^*\Psi_l+\Psi_l^*\Psi_{l'})\\ &= \frac{1}{4}(4M-(2M-\mathrm{tr}\,(\Psi_{l'}^*\Psi_l+\Psi_l^*\Psi_{l'})))\\ &= \frac{1}{4}(4M-\mathrm{tr}\,((\Psi_l-\Psi_{l'})^*(\Psi_l-\Psi_{l'})))\\ &= \frac{1}{4}(4M-\|\Psi_l-\Psi_{l'}\|_F^2).\end{aligned}$$

For the form (2.1), the diversity sum assumes the following simple form:

$$\sum\mathcal{V}=\min_{l,l'}\frac{1}{2\sqrt{M}}\|\Psi_l-\Psi_{l'}\|_F. \tag{2.3}$$

Without mentioning the term, the concept of diversity sum was used in [12]. Liang and Xia [17, p. 2295] explicitly defined the diversity sum in the situation when $T=2M$ using (2.3). Definition 2.2 naturally generalizes the definition to arbitrary constellations.

Hochwald and Marzetta [14] calculate the noncoherent space–time channel capacity and indicate that unitary signal constellation are capacity achieving signal sets only for high-SNR scenarios. For the low-SNR case, the transmitting power should be allocated unsymmetrically, i.e., unitary constellations are not capacity achieving in the first place. However, unitary signal sets are easily manageable and one can take advantage of differential modulation technique [13] to speed up the transmission. Moreover, our simulation results indicate that codes with near optimal diversity sum tend to perform significantly better compared to the currently existing ones optimized for the diversity product for low- and even moderate-SNR scenarios. So it is quite reasonable and more toward the practical use to construct unitary constellations with good diversity sum. Interestingly, for constellations inside the special unitary group $SU(2)$, we have $\prod\mathcal{V}=\sum\mathcal{V}$.

C. Four Illustrative Examples

The diversity sum governs at low-SNR regimes, while the diversity product governs at high-SNR regimes. Codes optimized at these extreme values of the SNR-axis do not necessarily perform well on the "other side of the spectrum." In this subsection, we illustrate the introduced concepts on four examples. All examples have about equal parameters, namely, $T=4$, $M=2$, and the size L is 121 (respectively, 120). The first two examples are well studied examples from the literature. We derived the third and the fourth examples by geometrical design and numerical methods, respectively.

Orthogonal Design: This constellation has been considered by several authors [2], [23]. For our purpose, we simply define this code as a subset of $SU(2)$

$$\left\{\frac{\sqrt{2}}{2}\begin{pmatrix}e^{\frac{2m\pi i}{11}} & e^{\frac{2n\pi i}{11}}\\ -e^{-\frac{2n\pi i}{11}} & e^{-\frac{2m\pi i}{11}}\end{pmatrix}|m,n=0,1,\ldots,10\right\}.$$

The constellation has 121 elements and the diversity sum and the diversity product are both equal to 0.1992.

Unitary Representation of $SL_2(\mathbb{F}_5)$: Shokrollahi *et al.* [23] derived a constellation using the theory of fixed point free representations whose diversity product is near optimal. This constellation appears as a unitary representation of the finite group $SL_2(\mathbb{F}_5)$ and we will refer to this constellation as the $SL_2(\mathbb{F}_5)$-constellation. The finite group $SL_2(\mathbb{F}_5)$ has 120 elements and this is also the size of the constellation. The constellation has rate $R=3.45$ and

$$\prod SL_2(\mathbb{F}_5)=\sum SL_2(\mathbb{F}_5)=\frac{1}{2}\sqrt{\frac{(3-\sqrt{5})}{2}}\sim 0.3090.$$

The diversity product of this constellation is truly outstanding.

Numerically Derived Constellation: Using simulated annealing algorithm we found after short computation a constellation with very

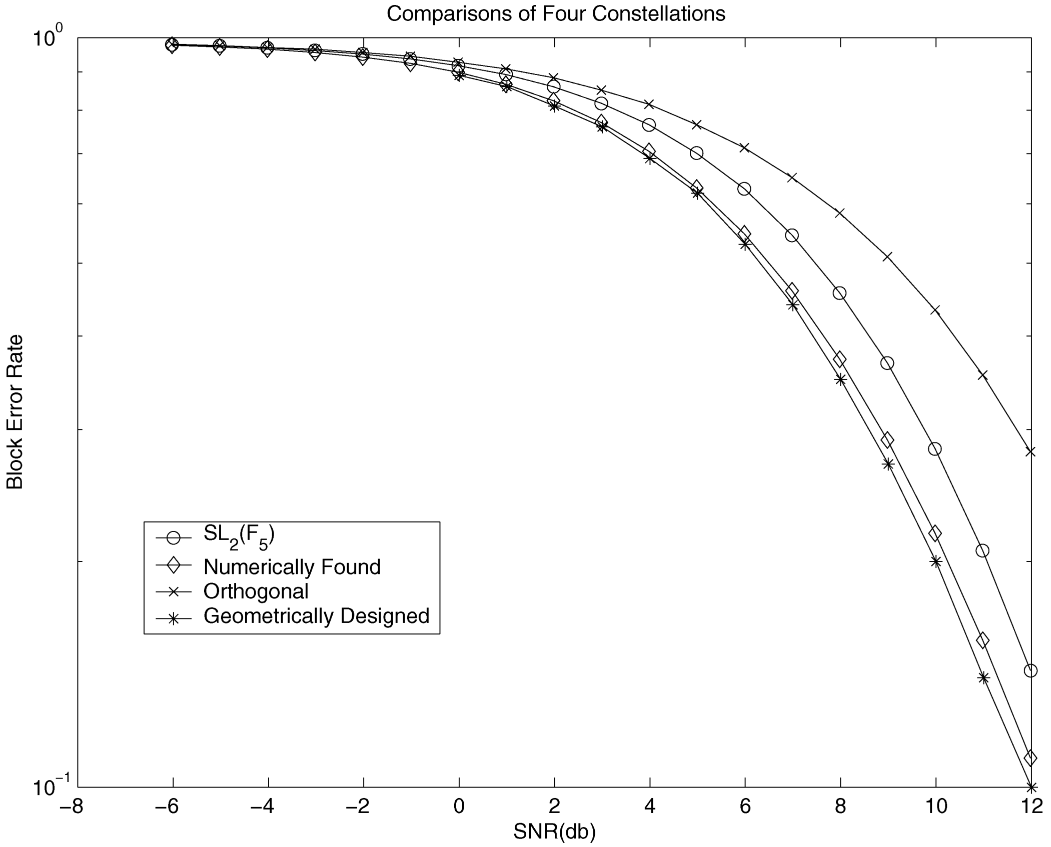

Fig. 1. Simulations of four constellations having sizes $T = 4$, $M = 2$, and $L = 120$ (respectively, $L = 121$).

TABLE I
PARAMETERS OF THE FOUR CONSTELLATIONS

	Orthogonal design	$SL_2(\mathbb{F}_5)$	Numerically derived	Geometrically designed
Number of elements	121	120	121	120
diversity sum	0.1992	0.309	0.3886	0.4156
diversity product	0.1992	0.309	0.0278	0.1464

good diversity sum. The constellation is given through a set of 121 matrices shown at the bottom of the page. As we explain in Section VI, the ML decoding of this constellation admits a simple decoding algorithm: sphere decoding.

Geometrically Designed Constellation: A geometrically designed constellation can be described as follows:

$$\left\{\Psi_k := A^k B^k | A = \begin{pmatrix} e^{17\pi/60i} & 0 \\ 0 & e^{13\pi/60i} \end{pmatrix}, \right.$$
$$\left. B = \begin{pmatrix} \cos(22\pi/60) & \sin(22\pi/60) \\ -\sin(22\pi/60) & \cos(22\pi/60) \end{pmatrix}, \ k = 0, 1, \ldots, 119 \right\}.$$

This constellation has superb diversity sum and reasonably good diversity product. One can also use sphere decoding to implement ML decoding of this constellation.

Fig. 1 provides simulation results for each of the four constellations of Table I. Note that the numerically designed code who has a very bad diversity product is performing very well nevertheless due to the exceptional diversity sum. One can see that up to 12-dB numerically derived codes outperform the group code by about 1 dB. In fact, our simulation results show that until 35 dB, the numerical one is still performing much better than the orthogonal one. However, at around 18 dB, the group constellation surpasses the numerical one due to exceptional diversity product. The geometrically designed constellation has better diversity sum and diversity product than the numerical one, therefore, its performance is better than the numerical one (our results show

$$\left\{\Psi_{k,l} := A^k B^l | A = \begin{pmatrix} -0.9049 + 0.3265 * i & 0.1635 + 0.2188 * i \\ 0.0364 + 0.2707 * i & -0.8748 + 0.4002 * i \end{pmatrix}, \right.$$
$$\left. B = \begin{pmatrix} -0.1596 + 0.9767 * i & -0.1038 + 0.0994 * i \\ 0.0833 - 0.1171 * i & -0.9432 + 0.2995 * i \end{pmatrix}, \ k, l = 0, 1, \ldots, 10 \right\}.$$

that their performance curves are quite close, although the geometrical one is slightly better). These simulation results give an indication that the diversity sum is a very important parameter for a unitary constellation at low-SNR regime.

III. Constellations With Algebraic Structure

In the sequel, we are going to investigate structured constellations and explain how one can restrict the parameter space to judiciously chosen subsets and how one can convert ML decoding to lattice decoding by using structured constellations.

Consider a general constellation of square unitary matrices

$$\mathcal{V} = \{\Psi_1, \Psi_2, \ldots, \Psi_L\}.$$

In order to calculate the diversity product, one needs to do $\frac{L(L-1)}{2}$ calculations: $|\det(\Psi_i - \Psi_j)|$ for every different pair i, j. The same statement can be made about the diversity sum, however, for simplicity we only show the diversity product case in the sequel unless specified otherwise.

As shown in [23], if one deals with a group constellation then one needs only to calculate $L-1$ such determinant calculations. This is a direct consequence of

$$|\det(\Psi_i - \Psi_j)| = |\det(\Psi_i)\det(I - \Psi_i^*\Psi_j)| = |\det(I - \Psi_i^*\Psi_j)|$$

where $\Psi_i^*\Psi_j$ is still in the group. Group constellations are, however, very restrictive about what the algebraic structure is concerned, and the constellations found by this approach [23] are really few and far between. In the following, we are going to present some constellations which have some small number of generators and whose diversity can be efficiently computed. This will ensure that the total parameter space to be searched is limited as well. We start with an example:

Example 3.1: Consider the constellation

$$\mathcal{V} = \{A^k B^l | A, B \in U(M),\ k = 0, \ldots, p,\ l = 0, \ldots, q\}.$$

(We remark that a more specified constellation of this type has been considered in [23].) The parameter space for this constellation is $U(M) \times U(M)$, this is a manifold of dimension $2M^2$ and the number of elements in $\mathcal{V}$ is $(p+1)(q+1)$. If one has to compute $|\det(\Psi_i - \Psi_j)|$ for every distinct pair, this would require $\binom{(p+1)(q+1)}{2}$ determinant calculations. We will show in the following that the same result can be obtained by doing $2pq + p + q$ determinant computations.

Let Ψ_i and Ψ_j be two distinct elements having the form $A^{k_1}B^{l_1}$ and $A^{k_2}B^{l_2}$ respectively. We have now several cases. When $k_1 = k_2$, then necessarily $l_1 \neq l_2$ and the distance is computed as

$$|\det(A^{k_1}B^{l_1} - A^{k_2}B^{l_2})| = |\det(I - B^{|l_2 - l_1|})|,$$

where $|l_2 - l_1|$ is an integer between 1 and q. If $l_1 = l_2$, then we have $k_1 \neq k_2$ and the distance is computed as

$$|\det(A^{k_1}B^{l_1} - A^{k_2}B^{l_2})| = |\det(I - A^{|k_2 - k_1|})|$$

where $|k_2 - k_1|$ is an integer between 1 and p. If ($k_1 < k_2$ and $l_1 < l_2$) or ($k_1 > k_2$ and $l_1 > l_2$), we have

$$|\det(A^{k_1}B^{l_1} - A^{k_2}B^{l_2})| = |\det(I - A^{|k_2 - k_1|}B^{|l_2 - l_1|})$$

where $1 \leq |k_2 - k_1| \leq p$ and $1 \leq |l_2 - l_1| \leq q$. Similarly, if ($k_1 < k_2$ and $l_1 > l_2$) or ($k_1 > k_2$ and $l_1 < l_2$) then

$$|\det(A^{k_1}B^{l_1} - A^{k_2}B^{l_2})| = |\det(A^{|k_2 - k_1|} - B^{|l_2 - l_1|})|,$$

with $1 \leq |k_2 - k_1| \leq p$ and $1 \leq |l_2 - l_1| \leq p$. The total number of distances to be computed is in total equal to $2pq + p + q$.

In the sequel, we are going to loosen the constraints imposed by the group structures. As demonstrated in Example 3.1, it is desirable to have a small-dimensional manifold (in Example 3.1 it was $U(M) \times U(M)$) which parameterizes a set of potentially interesting constellations. Having such a parameterization will help to avoid the problem of "dimension explosion." The set of constellations parameterized by $U(M) \times U(M)$ in Example 3.1 are interesting as we are not required to compute all pairwise distances in order to compute the diversity product (sum).

Definition 3.2: Let X be the set $\{x_1, x_2, \ldots, x_n\}$ and F be the free group on the set X. A subset $G \subset U(M)$ is called *freely generated* if there are elements $\{g_1, g_2, \ldots, g_n\} \subset G$ such that the homomorphism $\phi : F \longrightarrow G$ with $\phi(x_i) = g_i$ is an isomorphism.

An immediate consequence of this definition is that every element in G can be uniquely written as a product of g_i's and g_i^{-1}'s. The elements g_i are called the generators of G. A freely generated subset G is simply parameterized by the set

$$\left\{a_1^{p_1} a_2^{p_2} \cdots a_k^{p_k} \mid a_i \text{ is one of } g_i's,\ p_i \in \mathbb{Z}\right\}.$$

Take an element $g \in G$ with its representation $g = \prod_{i=1}^k a_i^{p_i}$, we say that the presentation is *reduced* whenever $a_i \neq a_{i+1}$ for $i = 1, \ldots, n-1$. Observe that taking the product of distinct matrices $\prod_{i=1}^n A_i$ is numerically expensive, however, taking the power of one matrix A^k is much easier (note that for $A = U \sum U^{-1}$ with $\sum$ diagonal, we have $A^k = U \sum^k U^{-1}$). Moreover, by considering the powers of one matrices, we are able to impose the lattice structure to the constellation, which makes sphere decoding of structured constellations possible. (see Section VI) Therefore, we are interested in "normal" elements of G.

Definition 3.3: We say that an element $g = \prod_{i=1}^k a_i^{p_i}$ in reduced form is a *normal element* whenever $a_i \neq a_j$ for $i \neq j$. A subset $\mathcal{V}$ of the freely generated set G is said to be a *normal constellation* if every nonidentity element in $\mathcal{V}$ is normal.

In the following we limit our searches to positive constellations:

Definition 3.4: An element g in G with the reduced form $g = \prod_{i=1}^k a_i{}^{p_i}$ is said to be a *positive element* if $p_i > 0$ for $i = 1, 2, \ldots, k$. A subset $\mathcal{V}$ of the freely generated set G is said to be a *positive constellation* if every nonidentity element in $\mathcal{V}$ is positive.

Positive normal constellations are desirable for numerical searches as they can be efficiently parameterized and searched. If one wants to compute the diversity product (or sum) of an arbitrary positive constellation with L elements one still has to compare a total of $\binom{L}{2}$ pairs of matrices. In the sequel, we will impose more structure on a constellation $\mathcal{V} \subset G$ which will guarantee that only $L-1$ pair of elements have to be compared during the diversity product (sum) computation.

Definition 3.5: Two unitary matrices $A, B \in G$ are said to be *equivalent* (denote by $A \sim B$) if there is a unitary matrix $U \in G$ such that $A = UBU^{-1}$ or $A = UB^{-1}U^{-1}$. $[A]$ will denote all the matrices that are equivalent to A. For a constellation $\mathcal{V} \subset G$, we say that $\mathcal{V} = \{\Psi_1, \Psi_2, \ldots, \Psi_L\}$ has a weak group structure if for any two distinct elements Ψ_i, Ψ_j the product $\Psi_i^{-1}\Psi_j$ is equivalent to some Ψ_k.

The reader can verify that we indeed defined an equivalence relation. Note also that $\mathcal{V}$ has a group structure as soon as $\Psi_i^{-1}\Psi_j$ is always another element of $\mathcal{V}$ and this explains our wording.

Lemma 3.6: Let $\mathcal{V} = \{\Psi_0 = I, \Psi_1, \Psi_2, \ldots, \Psi_{L-1}\}$ be a constellation with a weak group structure. In order to compute the diversity product (sum) it is enough to do $L-1$ distance computations.

Proof:

$$|\det(\Psi_i - \Psi_j)| = |\det(I - \Psi_i^{-1}\Psi_j)| = |\det(I - B)|$$

where $B \in \mathcal{V}$ is an element in $\mathcal{V}$ equivalent to $\Psi_i^{-1}\Psi_j$. This shows the result for the diversity product. If one is concerned with the diversity sum, then the same argument still holds if the absolute value of the determinant $|\det(\cdot)|$ is replaced by the Frobenius norm $\| \, . \, \|_F$. □

Based on this lemma, we are interested in finite constellations inside G whose elements have a weak group structure and are all normal. The following theorem provides a complete characterization of all these constellations.

Theorem 3.7: Let $\mathcal{V} \subset G$ be a finite positive normal constellation (including identity element) with $L \geq 3$ elements. If $\mathcal{V}$ has a weak group structure then $\mathcal{V}$ takes one of the following forms:

- $\{I, A, A^2, \ldots, A^{L-1}\}$;
- $\{I, AB, A^2B^2, \ldots, A^{L-1}B^{L-1}\}$.

where $A = g_i^{p_i}$, $B = g_j^{p_j}$ for some $i \neq j$.

The proof of Theorem 3.7 is rather involved. In order to make it more understandable we will divide it in several definitions and lemmas.

Definition 3.8: For any element $\Psi \in G$, we define the length of $\Psi = \prod_{i=1}^{k} a_i{}^{p_i}$ to be

$$\text{length}\,(\Psi) = \sum_{i=1}^{k} p_i.$$

It is a routine to check that the definition is wel defined and does not depend on the representation of the element. For the identity element, one will have length $(I) = 0$. One immediate consequence from this definition is that if $A \sim B$, one will have $|\text{length}\,(A)| = |\text{length}\,(B)|$. The following lemma claims that any freely generated positive weak group constellation "approximately" takes cyclic form.

Lemma 3.9: Let $\mathcal{V} = \{\Psi_0 = I, \Psi_1, \Psi_2, \ldots, \Psi_{L-1}\} \subset G$ be a positive constellation of the freely generated set $G \subset U(M)$. Suppose length $(\Psi_i) \leq$ length (Ψ_j) for $i < j$. If $\mathcal{V}$ is a weak group constellation, then

$$\Psi_i \in [\Psi_1]^i$$

where $[\Psi_1]^i = \{a_1 a_2 \cdots a_i | a_1, a_2, \ldots, a_i \in [\Psi_1]\}$.

Proof: We first show that length $(\Psi_i) <$ length (Ψ_j) for $i < j$: Indeed, if length $(\Psi_i) =$ length (Ψ_j), then length $(\Psi_i^{-1}\Psi_j) =$ length $(\Psi_j) -$ length $(\Psi_i) = 0$. That means $\Psi_i^{-1}\Psi_j \sim I$, equivalently one will have $\Psi_i^{-1}\Psi_j = I$, i.e., $\Psi_i = \Psi_j$. That contradicts the fact that Ψ_i and Ψ_j are distinct.

Consider $\Psi_1^{-1}\Psi_2$. Since

$$\begin{aligned} 0 &< \text{length}\,(\Psi_1^{-1}\Psi_2) \\ &= \text{length}\,(\Psi_2) - \text{length}\,(\Psi_1) < \text{length}\,(\Psi_2) \end{aligned}$$

therefore, $\Psi_1^{-1}\Psi_2 = \bar{\Psi}_1$ where $\bar{\Psi}_1 \sim \Psi_1$. So $\Psi_2 = \Psi_1\bar{\Psi}_1 \in [\Psi_1]^2$. Proceeding by induction, one can show $\Psi_k^{-1}\Psi_{k+1} = \bar{\Psi}_2$ where $\bar{\Psi}_2 \sim \Psi_1$. So $\Psi_{k+1} = \Psi_k\bar{\Psi}_2 \in [\Psi_1]^{k+1}$ by induction. □

Remark 3.10: An immediate observation is that

$$\text{length}\,(\Psi_i) = i * \text{length}\,(\Psi_1).$$

Take two positive normal elements in G with their reduced forms

$$\Psi_1 = a_1^{p_1} a_2^{p_2} \cdots a_m^{p_m} \qquad \Psi_2 = b_1^{q_1} b_2^{q_2} \cdots b_n^{q_n}.$$

We define the shift operator S_k on the reduced form of a positive normal element Ψ by induction: $S_1(\Psi) = S_1(a_1^{p_1} a_2^{p_2} \cdots a_m^{p_m}) = a_2^{p_2} \cdots a_m^{p_m} a_1^{p_1}$ and $S_{k+1} = S_k \circ S_1$. We assume that $S_0(\Psi) = \Psi$, then apparently for a fixed element Ψ the shift operator is periodic. We have the following lemma.

Lemma 3.11: $\Psi_1 \sim \Psi_2$ if and only if $\Psi_1 = S_k(\Psi_2)$ for some k.

Proof: The sufficiency part of this lemma is straightforward. So we have to prove the necessity part. Since $\Psi_1 \sim \Psi_2$, according to the definition of equivalence there exists c such that $c\Psi_1 c^{-1} = \Psi_2$ or $c\Psi_1 c^{-1} = \Psi_2^{-1}$. However, since length $(c\Psi_1 c^{-1}) =$ length $(\Psi_2) > 0$ and length $(\Psi_2^{-1}) < 0$, the second case will not happen. The only possibility is $c\Psi_1 c^{-1} = \Psi_2$. We assume that c is generated by only one generator and further assume $c = c_1^{l_1}$ with $l_1 > 0$, then we will have

$$c_1^{l_1} a_1^{p_1} a_2^{p_2} \cdots a_m^{p_m} c_1^{-l_1} = b_1^{q_1} b_2^{q_2} \cdots b_n^{q_n}.$$

So $c_1 = a_m$ and $l_1 \leq p_m$ follows, otherwise, the left-hand side of the equation above will have negative power, while the right-hand side only has positive power. This will contradict the uniqueness of the representation of the same element. In fact, $l_1 = p_m$, since otherwise, $\Psi_2 = c_1^{l_1} a_1^{p_1} a_2^{p_2} \cdots c_1^{p_m - l_1}$. This will contradict the fact that Ψ_2 is a normal element. So with

$$a_m^{p_m} a_1^{p_1} \cdots a_{m-1}^{p_{m-1}} = b_1^{q_1} b_2^{q_2} \cdots b_n^{q_n}$$

one can check $m = n$ and $\Psi_2 = S_{m-1}(\Psi_1)$.

Proceeding by induction, suppose c has the reduced form $c = c_1^{l_1} c_2^{l_2} \cdots c_{k+1}^{l_{k+1}}$, then the following equation follows:

$$c_1^{l_1} c_2^{l_2} \cdots c_{k+1}^{l_{k+1}} a_1^{p_1} a_2^{p_2} \cdots a_m^{p_m} c_{k+1}^{-l_{k+1}} \cdots c_2^{-l_2} c_1^{-l_1} = b_1^{q_1} b_2^{q_2} \cdots b_n^{q_n}.$$

Without loss of generality, we assume $l_{k+1} > 0$ and apply the same argument as in the one-generator case. One proves $a_m = c_{k+1}$ and $l_{k+1} = p_m$. Therefore, we reach the following equation:

$$c_1^{l_1} c_2^{l_2} \cdots c_k^{l_k} S_{m-1}(\Psi_1) c_k^{-l_k} \cdots c_2^{-l_2} c_1^{-l_1} = b_1^{q_1} b_2^{q_2} \cdots b_n^{q_n}.$$

By induction, $\Psi_2 = S_{k_1} \circ S_{m-1}(\Psi_1) = S_{k_1+m-1}(\Psi_1)$ for some k_1. □

Proof of Theorem 3.7: Pick any two distinct elements $\Psi_i, \Psi_j \in \mathcal{V}$ having length $(\Psi_i) <$ length (Ψ_j). We claim that if $\Psi_i = a_1 a_2 \cdots a_m$, then either there exists $1 \leq k \leq m-1$ such that

$$\Psi_j = a_1 a_2 \cdots a_k b_1 b_2 \cdots b_l a_{k+1} \cdots a_m$$

or

$$\Psi_j = b_1 b_2 \cdots b_l a_1 a_2 \cdots a_m$$

or

$$\Psi_j = a_1 a_2 \cdots a_m b_1 b_2 \cdots b_l$$

for some $l > 0$.

Suppose that the claim is not true, then for $\Psi_j = c_1 c_2, \dots c_p$, there exist k_1, k_2 such that $0 \leq k_1 \leq m, 1 \leq k_2 \leq m+1$, and $k_1 < k_2 - 1$ and Ψ_j will take the following form:

$$\Psi_j = a_1 a_2 \cdots a_{k_1} b_1 b_2 \cdots b_l a_{k_2} \cdots a_m$$

where $b_1 \neq a_{k_1+1}$ and $b_l \neq a_{k_2-1}$. (For the special case $k_1 = 0$, we assume $c_1 \neq a_1$. For the special case $k_2 = m+1$, we assume $c_p \neq a_m$.) Then $\Psi_i^{-1}\Psi_j$ would be equivalent to $a_{k_2-1}^{-1} \cdots a_{k_1+1}^{-1} b_1 b_2 \cdots b_l$, which in any case will not be equivalent to any positive element $\Psi_k = d_1 d_2 \cdots d_q$ or I. That contradicts the fact that $\mathcal{V}$ is equipped with a weak group structure.

As explained above we can further assume that

$$\text{length}\,(I) < \text{length}\,(\Psi_1) < \cdots < \text{length}\,(\Psi_{L-1}).$$

If Ψ_1 is generated by only one generator, i.e., $\Psi_1 = g_i^{p_i}$ for some i. Since Ψ_2 is a normal element, according to the claim, either $\Psi_2 = \Psi_1 \tilde{\Psi}_2$ or $\Psi_2 = \tilde{\Psi}_2 \Psi_1$ for some $\tilde{\Psi}_2$. In either case, $\tilde{\Psi}_2$ will be equivalent to Ψ_1, while Lemma 3.11 will guarantee $\tilde{\Psi}_2 = \Phi_1$. Therefore, we will have $\Psi_2 = g_i^{2p_i}$. Proceeding by induction, it can be checked that $\Psi_l = g_i^{lp_i}$ for every l. So the constellation will take the first form in the theorem.

If Φ_1 is generated by two generators, i.e., $\Psi_1 = g_i^{p_i} g_j^{p_j}$ for some i, j. According to the claim, we will have $\Psi_2 = \Psi_1 \tilde{\Psi}_2$ or $\Psi_2 = \tilde{\Psi}_2 \Psi_1$ or $\Psi_2 = g_i^{p_i} \tilde{\Psi}_2 g_j^{p_j}$. Because $\tilde{\Psi}_2$ is equivalent to Ψ_1, $\tilde{\Psi}_2$ is a shifted version of Ψ_1. Exhausting all the possibilities, the first two cases would make Ψ_2 a non-normal element, so the only possibility is the third case. Consider two shifted versions of Ψ_1: $S_0(\Psi_1) = g_i^{p_i} g_j^{p_j}$ and $S_1(\Psi_1) = g_j^{p_j} g_i^{p_i}$. Only $S_0(\Psi_1)$ will satisfy the condition that Ψ_2 is a normal element. So the analysis above shows that

$$\Psi_2 = g_i^{p_i} \Psi_1 g_j^{p_j} = g_i^{2p_i} g_j^{2p_j}.$$

By induction it can be shown that

$$\Psi_{k+1} = g_i^{p_i} \Psi_k g_j^{p_j} = g_i^{(k+1)p_i} g_j^{(k+1)p_j}.$$

So in this case, the constellation will take the second form in the theorem.

However, the constellation does not exist if Ψ_1 is generated by more than three elements. Indeed, suppose with the reduced form $\Psi_1 = a_1^{p_1} a_2^{p_2} \cdots a_m^{p_m}$ with $m \geq 3$, then Ψ_2 will take one of the following forms: $\tilde{\Psi}_2 a_1^{p_1} a_2^{p_2} \cdots a_m^{p_m}, a_1^{p_1} \tilde{\Psi}_2 a_2^{p_2} \cdots a_m^{p_m}, \dots, a_1^{p_1} a_2^{p_2} \cdots a_m^{p_m} \tilde{\Psi}_2$ with $\tilde{\Psi}_2$ being a shifted version of Ψ_1. But Ψ_2 would not be a normal element for any of the above form, so there does not exist weak group constellation for this case. □

A weak group constellation is very group like, while it is not exactly a group. It does keep the advantage of a group constellation: for example, for any weak group constellation $\mathcal{V}$ taking the second form in the theorem, only $L-1$ computations $|\det(I - A^k B^k)|$ for $k = 1, 2, \dots, L-1$ are needed to calculate the diversity product. Contrary to group codes, the generators can freely be chosen. Moreover, the restriction to code elements in normal form is very advantageous during sphere decoding. In the next section, we will mainly use the second weak group structure as described in Theorem 3.7. Before we describe these search procedures we would like to illustrate some alternative methods.

It is possible to increase the number of generators to obtain new structures. For example

$$\mathcal{V} = \{A^k B^l C^m | A, B, C \in U(M), \quad k = 0, \dots, p,\ l = 0, \dots, q,\ m = 0, \dots, r\}.$$

For a unitary constellation $\mathcal{V} = \{\Phi_i | i = 1, \dots, L\}$, we call $\mathcal{V}_s = \{U \Phi_i V | i = 1, \dots, L\}$ shifted version of $\mathcal{V}$. It will be straightforward to prove that $\mathcal{V}_s$ has the same complexity as $\mathcal{V}$ when one calculates the diversity. $\{A^k C B^k | A, B, C \in U(M),\ k = 0, \dots, L-1\}$ is a shifted copies of the second weak group structure in Theorem 3.7. To see this, note that $A^k C B^k = A^k C B^k C^{-1} C = A^k (C B C^{-1})^k C$. It can checked that $A^k B^{L+1-k} = A^k (B^{-1})^k B^{L+1}$, therefore,

$$\{A^k B^{L+1-k} | A, B \in U(M),\ k = 1, \dots, L\}$$

is also a shifted version of the second form weak group structure.

Also, we can consider the "combination" or the "product" of two structures. For example, $\{I, A, AB, ABA, ABAB, ABABA, \dots\}$ is the union of $\{(AB)^k | k = 0, \dots\}$ and its shifted version $\{(AB)^k A | k = 0, \dots\}$. Another example is the product case: let $\mathcal{V}_1 = \{I, C, C^2, C^3, \dots\}$ and $\mathcal{V}_2 = \{I, A, AB, ABA, \dots\}$ and consider the Cartesian product constellation

$$\mathcal{V} = \mathcal{V}_1 \times \mathcal{V}_2 = \{AB | A \in \mathcal{V}_1, B \in \mathcal{V}_2\}.$$

IV. Geometrical Design of Unitary Constellations With Good Diversity

For low-dimensional constellations, one may further specify the generators in the proposed structure. Observe that for both forms of weak group constellations in Theorem 3.7, one can always assume A is diagonal. In the sequel, we design codes using the second form and further assume that B is real orthogonal, i.e., we consider the following two-dimensional constellation

$$\mathcal{V} = \left\{A^k B^k \middle| A = \begin{pmatrix} e^{ix} & 0 \\ 0 & e^{iy} \end{pmatrix}, \right. \quad \left. B = \begin{pmatrix} \cos z & \sin z \\ -\sin z & \cos z \end{pmatrix},\ k = 0, 1, \dots, L-1 \right\}. \tag{4.1}$$

There are several ways to design constellations with good diversity from this specific structure. A natural idea is to do brute-force search using fine step size. Another approach is to design the constellation with the help of geometrical intuition. Note that a 2×2 complex matrix can be viewed as a vector in $\mathbb{C}^4$. In this context, A and B can be viewed as "rotation transforms" (induced by regular matrix multiplication) acting on $\mathbb{C}^4$. A constellation of the form (4.1) can be viewed as a set of rotated vectors under the transforms $A^k B^k, k = 0, 1, \dots, L-1$. Intuition tells us that good constellations can be found if the rotation angle is symmetrical. Based on that idea and assuming that x, y, z are the multiples of $2\pi/L$, we found a lot of good codes resulting from this geometrical symmetry (see the tables in Section V).

The two-dimensional constellation design has been studied in [17]. In that paper, Liang *et al.* proposed very interesting parametric codes and many codes with excellent diversity were found. The codes shown in [17] can be achieved by our design as well. In fact, most of Liang's codes belong to a special form of our parameterization (4.1). To the best of our knowledge, most of our codes shown on the website [6] are the best codes ever found or never found before.

Example 4.1: A very interesting code with 120 elements is found using this approach

$$\mathcal{V} = \left\{A^k B^k \middle| A = \begin{pmatrix} e^{\pi/30i} & 0 \\ 0 & e^{11\pi/30i} \end{pmatrix}, \right. \quad \left. B = \begin{pmatrix} \cos \pi/4 & \sin \pi/4 \\ -\sin \pi/4 & \cos \pi/4 \end{pmatrix},\ k = 0, 1, \dots, 119 \right\}.$$

It can be checked that $\prod \mathcal{V} = \sum \mathcal{V} = \frac{1}{2}\sqrt{\frac{(3-\sqrt{5})}{2}}$, i.e., the diversity product and the diversity sum are identical to the ones of the

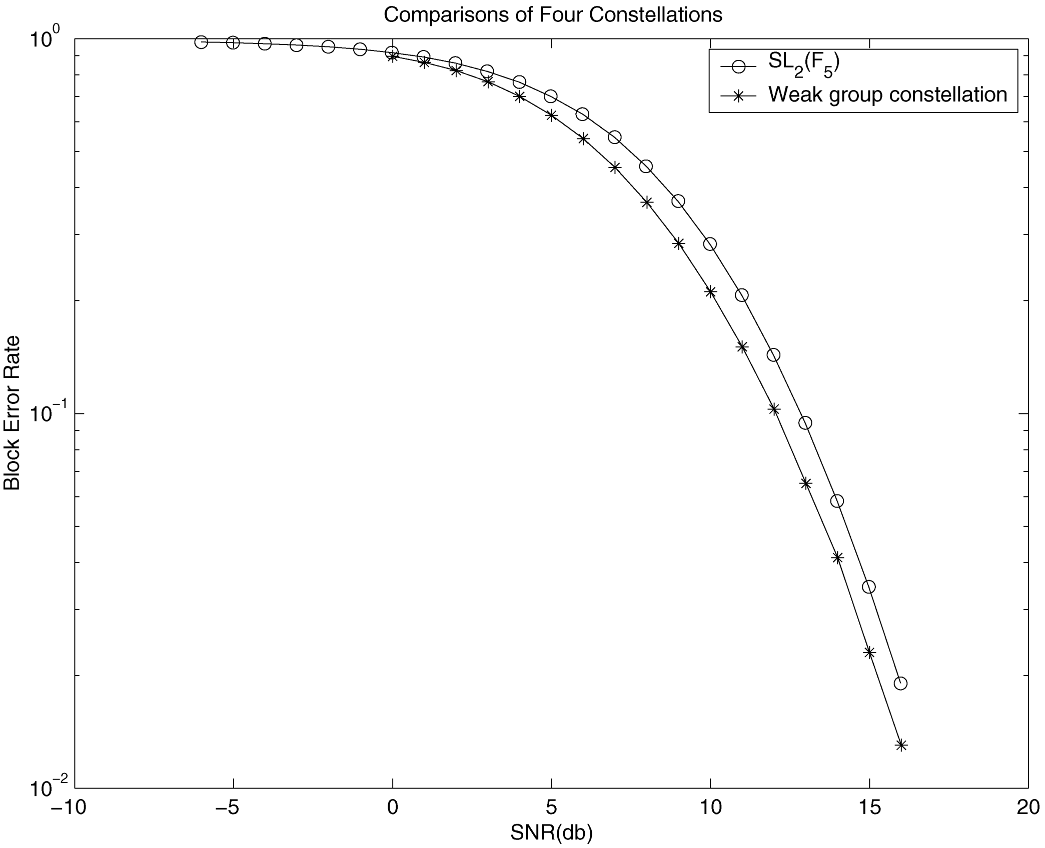

Fig. 2. Two-dimensional weak group constellations and group constellation.

TABLE II
WEAK GROUP CONSTELLATION DP DISTANCE SPECTRUM

distance	distribution
0.3090	360
0.3136	480
0.3895	480
0.3931	1440
0.4402	240
0.5000	120
0.5878	120
0.6360	1440
0.6787	480
0.7071	600
0.8090	360
0.8430	480
0.8660	120
0.8979	240
0.9511	120
1	60

TABLE III
WEAK GROUP CONSTELLATION DS DISTANCE SPECTRUM

distance	distribution
0.3090	120
0.4402	240
0.5000	120
0.5023	480
0.5457	240
0.5878	120
0.6367	480
0.6502	240
0.7071	3000
0.7598	240
0.7711	240
0.8090	120
0.8380	240
0.8647	480
0.8660	120
0.8979	240
0.9511	120
1	60

$SL_2(\mathbb{F}_5)$-constellation. We simulated the performance of this code and compared it with the performance of the $SL_2(\mathbb{F}_5)$-constellation. To our great surprise, our new code performed considerably better than the $SL_2(\mathbb{F}_5)$-constellation. The constellation $\mathcal{V}$ with sphere decoding outperformed the $SL_2(\mathbb{F}_5)$-constellation by about *1 dB* (see Fig. 2). As the SNR goes higher, the two curves are coming closer though.

In order to understand the difference in the performance of the two seemingly similar constellations, we investigated the *distance spectrum* for the diversity product (DP) and diversity sum (DS) for each of the constellations. In Tables II and III, we provide the number of pairs of codewords, which have a certain distance. As we explained before, for a unitary constellation with L elements, $L(L-1)/2$ distance calculations may produce distances with multiplicities. For example, consider $\mathcal{V}$ as above, 360 out of 7140 pairs of elements have distance 0.3090 (see DP distance spectrum in Table II) .

One can check that the DP distance spectrum of the $SL_2(\mathbb{F}_5)$-constellation is identical to the DS distance spectrum. Table IV shows that the DS distance spectrum for the $SL_2(\mathbb{F}_5)$-constellation has denser small distance distribution compared to DS spectrum of our constellation and this explains the considerable worse performance of this constellation in our simulations.

Although we have concentrated so far on the design of two-dimensional constellations there is actually no restriction with our approach.

TABLE IV
$SL_2(\mathbb{F}_5)$-Constellation DP (and DS) Distance Spectrum

distance	distribution
0.3090	720
0.5000	1200
0.5878	720
0.7071	1800
0.8090	720
0.8660	1200
0.9511	720
1	60

A similar "rotation" idea can be applied to other low-dimensional constellation designs. For instance, we can make further specifications to a three-dimensional weak group constellations

$$\mathcal{V} = \{A^kB^k | A = \begin{pmatrix} \cos x & \sin x & 0 \\ -\sin x & \cos x & 0 \\ 0 & 0 & e^{iy} \end{pmatrix}, \quad B = \begin{pmatrix} e^{iz} & 0 & 0 \\ 0 & \cos w & \sin w \\ 0 & -\sin w & \cos w \end{pmatrix}, \ k = 0, 1, \ldots, L-1\}.$$

where x, y, z, w is assumed to take the multiple of $2\pi/L$. Apparently, algebraic design based on geometrical symmetry can be applied to any other structure as well. For instance consider the following specified structures:

$$\mathcal{V} = \{A^kB^l | A = \begin{pmatrix} e^{ix} & 0 \\ 0 & e^{iy} \end{pmatrix}, \quad B = \begin{pmatrix} \cos z & \sin z \\ -\sin z & \cos z \end{pmatrix}, \ k = 0, 1, \ldots, p-1, \ l = 0, 1, \ldots, q-1\}$$

where we can take x, y to be multiple of $2\pi/p$ and z to be multiple of $2\pi/q$. Some of the two-dimensional geometrically found constellations will be listed together with those numerically found in Tables V and VI. We also refer to [6] for the designed low-dimensional constellations from these approaches.

V. Numerical Design of Constellations With Good Diversity

In order to numerically design constellations, it will be necessary to have a good parameterization for the set of unitary constellations having size L, operating with M transmit antennas. In this section, we show how one can use the classical Cayley transform and Simulated Annealing algorithm to obtain such a parameterization.

A. Cayley Transformation

There are several ways to represent a unitary matrix in a very explicit way. One elegant way makes use of the classical Cayley transformation. In order for the correspondence to be self-contained we provide a short summary. More details are given in [21, Sec. 22] and [10].

Definition 5.1: For a complex $M \times M$ matrix Y which has no eigenvalues at -1, the Cayley transform of Y is defined to be

$$Y^c = (I + Y)^{-1}(I - Y)$$

where I is the $M \times M$ identity matrix.

Note that $(I + Y)$ is nonsingular whenever Y has no eigenvalue at -1. One immediately verifies that $(Y^c)^c = Y$. This is in analogy to the fact that the linear fractional transformation $f(z) = \frac{1-z}{1+z}$ has the property that $f(f(z)) = z$. Recall that a matrix M is skew-Hermitian whenever $A^* = -A$. The set of $M \times M$ skew-Hermitian matrices forms a linear subspace of $\mathbb{C}^{M \times M} \cong \mathbb{R}^{2M^2}$ having real dimension M^2. The main property of the Cayley transformation is summarized in the following theorem (see, e.g., [10], [21]).

Theorem 5.2: When A is a skew-Hermitian matrix then $(I + A)$ is nonsingular and the Cayley transform $V := A^c$ is a unitary matrix. On the other hand, when V is a unitary matrix which has no eigenvalues at -1 then the Cayley transform V^c is skew-Hermitian.

This theorem allows one to parameterize the open set of $U(M)$ consisting of all unitary matrices whose eigenvalues do not include -1 through the linear vector space of skew-Hermitian matrices. Most optimization methods require us to consider the neighborhood of one element in $U(M)$, Therefore, the Cayley transformation is very important for the numerical design of constellations because it makes the local topology of $U(M)$ clear.

B. Simulated Annealing (SA) Algorithm

In our numerical experiments we have considered several methods. Because there are a large number of target functions, the best known optimization algorithms such as Newton's methods [4], [19] and the Conjugate Gradient method [4], [19] are difficult to implement. Surprisingly, the Simulated Annealing (SA) algorithm turned out to be very practical for this problem. For more details about this algorithm, we refer the reader to [1], [25], [20]. Our implementation of the algorithm can be summarized in the following way: one can find a sample program on our website [6].

1) Choose a proposed algebraic structure for the constellation.
2) Generate initial generators of the whole constellation. One can either take an existing constellation as the start point or just take the initial point randomly.
3) First apply Cayley transform to the old unitary constellation to obtain the corresponding skew-Hermitian constellation, then select a new skew-Hermitian constellation in the neighborhood of the old skew-Hermitian constellation according to Gaussian distribution (with decreasing variances as the algorithm progresses). Next apply Cayley transform again to the new skew-Hermitian constellation to obtain the new unitary constellation.
4) Calculate the diversity product (or sum) of the newly constructed constellation.
5) If the new constellation has better diversity product (or sum), then accept the new constellation. If not, reject the new constellation and keep the old constellation (or accept it according to Metropolis's criterion [18]).
6) Check the stopping criterion, if satisfied, then stop, otherwise go to 2) and continue the iteration.

Example 5.3: As we mentioned before, one can either choose an existing constellation as the starting point for our numerical method or just take the initial point randomly. In the sequel, we use the group constellation $G_{21,4}$ in [23]

$$\mathcal{V}_1 = \{A^kB^l | A = \begin{pmatrix} \eta & 0 & 0 \\ 0 & \eta^4 & 0 \\ 0 & 0 & \eta^{16} \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ \eta^7 & 0 & 0 \end{pmatrix}, \ k = 0, 1, \ldots, 20, \ l = 0, 1, 2\}.$$

One can verify that $\prod \mathcal{V}_1 = 0.3851$.

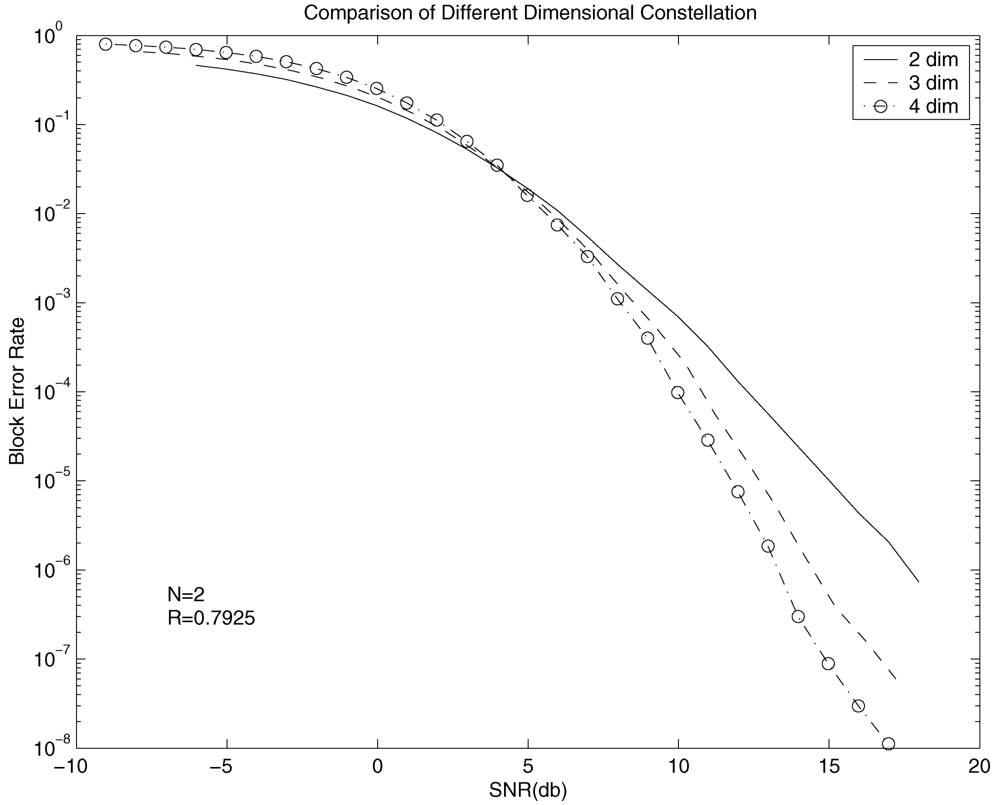

Fig. 3. Performance of different dimensional constellations with the same rate.

It seems that $G_{21,4}$ is already a very good constellation, our algorithm only improves a little (see $\mathcal{V}_2$ below). However, one can check for most of the cases, the algorithm will improve much compared to the original group constellation

$$\mathcal{V}_2 = \{A^k B^l | k = 0, 1, \ldots, 20,\ l = 0, 1, 2\},$$

where we get the matrices at the bottom of the page. One verifies that $\prod \mathcal{V}_2 = 0.3874$.

Example 5.4: Note that codes based on the proposed structure are flexible and can be optimized for dimension and any SNR efficiently in the same way as for extreme SNR cases. Fig. 3 shows the comparison of three constellations with different dimensions with two receiver antennas.

The first one is a two-dimensional constellations with three elements ($R = 0.7925$) and optimal diversity product 0.8660 and optimal diversity sum 0.8660. The second constellation is a three-dimensional constellation which has five elements ($R = 0.7740$) with diversity product 0.7183 and diversity sum 0.7454. The third constellation is a four-dimensional one consisting of nine elements ($R = 0.7925$) with diversity product 0.5904 and diversity sum 0.6403. Here based on the structure $A^k B^k$ we used Simulated Annealing to optimize the constellation at 6 dB to obtain the last two constellations.

In [9], packing problems on compact Lie groups are analyzed and the upper bound for the diversity sum and the diversity product are derived. Fig. 4 shows the limiting behavior of the two numerically found dimensional structured constellations compared to the upper bound. One can check [6] for the comparisons for other dimensions.

C. Constellations With Large Diversity

In Tables V and VI we list the best two-dimensional constellations we found with the techniques described in Sections IV and V. (For results on the higher dimensional unitary constellation design, one can check the web site [6].) The tabulated constellations have some of the best diversity sums and diversity products published so far. All the constellations searched by SA were based on the $A^k B^k$ structure. For constellations with L elements and parameters x, y, z being multiples of $2\pi/L$, they are found by geometrical methods using the parameterization (4.1). For constellations with L elements and parameters x, y, z being decimals, they are found by brute force with step size 0.1000 based on the same parameterization (4.1).

$$A = \begin{pmatrix} 0.9415 + 0.3155 * i & 0.0573 - 0.0222 * i & 0.0496 + 0.0882 * i \\ 0.0160 - 0.0555 * i & 0.4005 + 0.9136 * i & 0.0326 - 0.0212 * i \\ 0.0579 + 0.0855 * i & -0.0312 - 0.0099 * i & 0.1384 - 0.9844 * i \end{pmatrix}$$

$$B = \begin{pmatrix} 0.0175 + 0.0095 * i & 0.9997 + 0.0111 * i & 0.0079 + 0.0042 * i \\ 0.0086 + 0.0100 * i & -0.0082 + 0.0040 * i & 0.9999 + 0.0036 * i \\ -0.4836 + 0.8750 * i & 0.0004 - 0.0198 * i & -0.0045 - 0.0126 * i \end{pmatrix}.$$

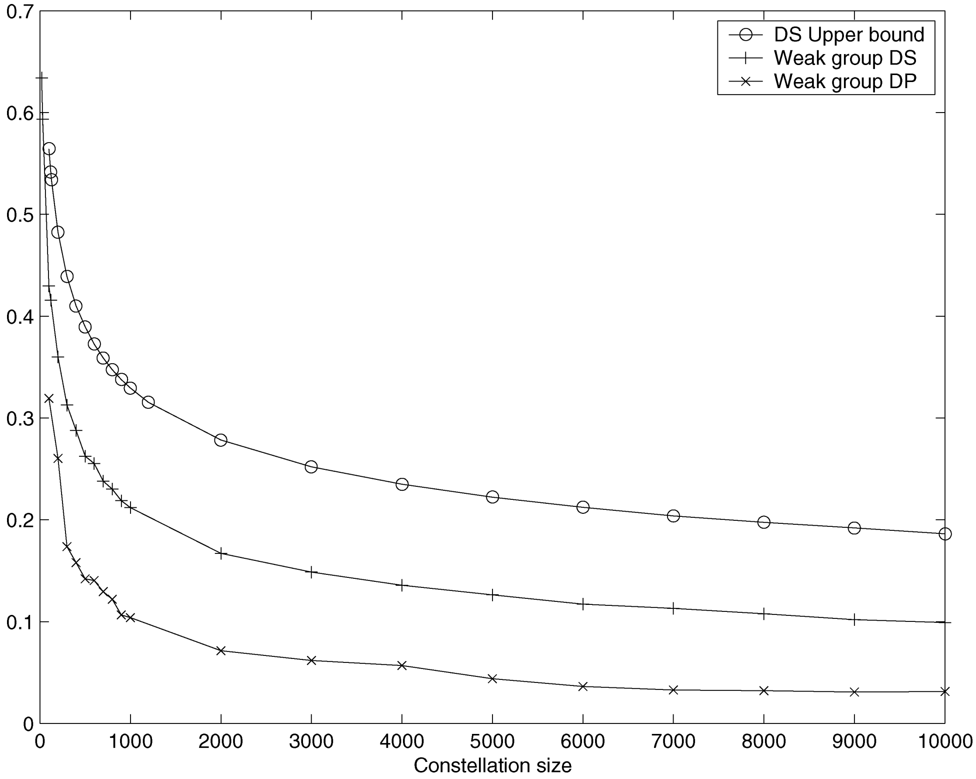

Fig. 4. Two-dimensional weak group constellations and upper bound.

TABLE V
DIVERSITY PRODUCT OF TWO-DIMENSIONAL CONSTELLATION BASED ON WEAK GROUP STRUCTURE

Number of elements	Diversity Product	Codes and Comments
2	1	$x=\pi, y=\pi, z=0$ (optimal)
3	$\sqrt{3}/2$	$x=2\pi/3, y=2\pi/3, z=0$ (optimal)
4	0.7831	$x=0.6000, y=6.0000, z=4.4000$
5	$\sqrt{5/8}$	$x=2\pi/5, y=8\pi/5, z=4\pi/5$ (optimal)
8	0.7071	$x=2.3562, y=3.9270, z=4.7124$
9	0.6524	SA searched code
10	0.6124	$x=2\pi/5, y=8\pi/5, z=\pi/5$
16	$\sqrt[4]{2}/2$	$x=\pi/4, y=5\pi/4, z=13\pi/8$
17	0.5255	SA searched code
18	0.5207	SA searched code
19	0.5128	SA searched code
20	0.5011	$x=1.6500, y=3.7500, z=4.0500$
24	0.5000	$x=\pi/12, y=5\pi/12, z=\pi/2$
37	0.4461	$x=2\pi/37, y=6\pi/37, z=12\pi/37$
39	0.3984	$x=8\pi/39, y=34\pi/39, z=36\pi/39$
40	0.3931	$x=3\pi/10, y=11\pi/10, z=3\pi/4$
55	0.3874	$x=2\pi/55, y=68\pi/55, z=6\pi/11$
57	0.3764	$x=2\pi/57, y=40\pi/57, z=48\pi/57$
75	0.3535	$x=2\pi/75, y=98\pi/75, z=96\pi/75$
85	0.3497	$x=26\pi/85, y=94\pi/85, z=18\pi/17$
91	0.3451	$x=2\pi/91, y=128\pi/91, z=42\pi/91$
96	0.3192	$x=7\pi/16, y=29\pi/16, z=\pi/6$
105	0.3116	$x=2\pi/105, y=68\pi/105, z=84\pi/105$
120	0.3090	$x=\pi/30, y=11\pi/30, z=\pi/4$
135	0.2869	$x=2\pi/135, y=28\pi/135, z=68\pi/135$
145	0.2841	$x=2\pi/145, y=64\pi/145, z=76\pi/145$
165	0.2783	$x=2\pi/33, y=20\pi/33, z=2\pi/5$
203	0.2603	$x=2\pi/203, y=290\pi/203, z=70\pi/203$
225	0.2499	$x=82\pi/225, y=118\pi/225, z=126\pi/225$
217	0.2511	$x=2\pi/217, y=250\pi/217, z=168\pi/217$
225	0.2499	$x=82\pi/225, y=118\pi/225, z=126\pi/225$
240	0.2239	$x=\pi/40, y=9\pi/40, z=\pi/6$
273	0.2152	$x=2\pi/273, y=208\pi/273, z=142\pi/273$
295	0.2237	$x=14\pi/295, y=104\pi/295, z=22\pi/59$
297	0.1910	$x=242\pi/297, y=548\pi/297, z=54\pi/297$
299	0.1858	$x=8\pi/299, y=220\pi/299, z=18\pi/299$
300	0.1736	$x=\pi/150, y=51\pi/150, z=5\pi/6$

TABLE VI
DIVERSITY SUM OF TWO-DIMENSIONAL CONSTELLATION BASED ON WEAK GROUP STRUCTURE

number of elements	Diversity Sum	Codes and Comments
2	1	$x = \pi, y = \pi, z = 0$ (optimal)
3	$\sqrt{3}/2$	$x = 2\pi/3, y = 2\pi/3, z = 0$ (optimal)
5	$\sqrt{5/8}$	$x = 2\pi/5, y = 8\pi/5, z = 4\pi/5$ (optimal)
9	$3/4$	$x = 10\pi/9, y = 4\pi/3, z = 4\pi/9$ (optimal)
16	$\sqrt{2}/2$	$x = \pi/4, y = 5\pi/4, z = 13\pi/8$ (optimal)
18	0.6614	$x = 4\pi/9, y = 2\pi/3, z = 7\pi/9$
20	0.6338	SA searched code
22	0.6154	SA searched code
24	0.6124	$x = \pi/6, y = \pi/4, z = 5\pi/12$
28	0.5996	$x = 3\pi/8, y = \pi/2, z = 2\pi/7$
30	0.5934	$x = 4\pi/15, y = \pi/3, z = 7\pi/15$
32	0.5734	SA searched code
39	0.5726	$x = 14\pi/39, y = 40\pi/39, z = 18\pi/39$
40	0.5499	$x = 3\pi/20, y = 7\pi/20, z = 3\pi/10$
42	0.5371	$x = 4\pi/7, y = 13\pi/21, z = \pi/3$
45	0.5342	$x = 2\pi/9, y = 4\pi/9, z = 14\pi/15$
52	0.5332	$x = \pi/13, y = 2\pi/13, z = 9\pi/26$
60	0.5000	$x = \pi/15, y = 4\pi/15, z = 3\pi/10$
64	0.4852	$x = 3\pi/16, y = 53\pi/32, z = 55\pi/32$
75	0.4850	$x = 32\pi/75, y = 14\pi/75, z = 2\pi/75$
85	0.4540	$x = 2\pi/17, y = 8\pi/17, z = 14\pi/85$
95	0.4418	$x = 6\pi/19, y = 2\pi/95, z = 36\pi/95$
105	0.4295	$x = 2\pi/105, y = 16\pi/105, z = 28\pi/105$
106	0.4161	$x = 2\pi/53, y = 13\pi/53, z = 12\pi/53$
120	0.4156	$x = \pi/10, y = \pi/6, z = 5\pi/4$
123	0.4077	$x = 188\pi/123, y = 38\pi/123, z = 182\pi/123$
130	0.4071	$x = 26\pi/65, y = 5\pi/13, z = 2\pi/13$
133	0.3971	$x = 2\pi/133, y = 212\pi/133, z = 206\pi/133$
145	0.3949	$x = 138\pi/145, y = 22\pi/145, z = 40\pi/29$
150	0.3758	$x = \pi/15, y = 8\pi/75, z = 19\pi/75$
155	0.3828	$x = 2\pi/5, y = 26\pi/31, z = 58\pi/31$
160	0.3802	$x = 69\pi/80, y = 59\pi/80, z = 37\pi/20$
165	0.3760	$x = 24\pi/165, y = 26\pi/165, z = 34\pi/165$
180	0.3636	$x = \pi/9, y = 97\pi/90, z = 127\pi/90$
208	0.3501	$x = \pi/13, y = 8\pi/13, z = 65\pi/104$
220	0.3459	$x = 19\pi/11, y = 163\pi/110, z = 121\pi/110$
240	0.3371	$x = 71\pi/120, y = 11\pi/10, z = 187\pi/120$
248	0.3291	$x = 103\pi/124, y = 39\pi/31, z = 179\pi/124$
276	0.3237	$x = 23\pi/138, y = 15\pi/69, z = 6\pi/69$
300	0.3126	$x = \pi/75, y = 17\pi/150, z = 9\pi/25$

D. General Form Constellation Numerical Design

As first illustrated in [16], one can construct $T \times M$ unitary constellations by using the first M columns of $T \times T$ unitary constellations. With this idea, the techniques used above for square unitary constellations can also be applied to design general form unitary constellations.. For simplicity, we describe the idea with the assumption $T = 2M$ and consider the following structure:

$$\{A^k B | A \in U(T), B = \begin{pmatrix} I_M \\ 0 \end{pmatrix}, \ k = 0, 1, \ldots, L-1\}.$$

One can check that at most $2L - 1$ distance calculations are needed to derive the diversity product (sum) with this algebraic structure. We list some of the numerically found nonsquare constellations in Table VII. More results can be found in [6].

VI. FAST DECODING OF THE STRUCTURED CONSTELLATION

The complexity of ML decoding for unitary space–time constellations increases exponentially with the number of antennas or the transmission rate. This will preclude its practical use for high transmission rates or for a large number of antennas. Basically our structured constellations can convert the ML decoding to lattice decoding naturally, consequently, they admit fast decoding algorithms.

TABLE VII
DIVERSITY PRODUCT AND DIVERSITY SUM FOR NON-SQUARE CONSTELLATIONS ($T = 5, M = 2$)

Size	DP
3	0.8527
4	0.8152
5	0.7171
6	0.7668
7	0.7493
8	0.7418
9	0.7183
10	0.6608
20	0.6240
30	0.5985
40	0.5552
50	0.5556
60	0.5088
90	0.4487
300	0.3563
600	0.2821
900	0.2472
3000	0.1867
6000	0.1545
9000	0.1296
10000	0.1426

Size	DS
3	0.8693
4	0.8589
5	0.8243
6	0.7976
7	0.7960
8	0.7844
9	0.7659
10	0.7737
20	0.7243
30	0.6837
40	0.6576
50	0.6392
60	0.6237
90	0.5775
300	0.4369
600	0.3687
900	0.3358
3000	0.2461
6000	0.2163
9000	0.1874
10000	0.1735

The principle of sphere decoding [5] is as follows: instead of doing an exhaustive search over all the lattice points, one can limit its search area to a sphere with given radius $\sqrt{C}$ centered at received point. One can check the complexity of this approach in [5] and in [11].

$$\begin{aligned}\|X_\tau - A^k B^l X_{\tau-1}\|_F &= \|A^{-k}X_\tau - B^l X_{\tau-1}\|_F \\ &= \|U\mathrm{diag}\,(e^{-ik\alpha_1}, e^{-ik\alpha_2}, \ldots, e^{-ik\alpha_M})U^* X_\tau - V\mathrm{diag}\,(e^{-il\beta_1}, e^{-il\beta_2}, \ldots, e^{-il\beta_M})V^* X_{\tau-1}\|_F.\end{aligned}$$

We will use the $A^k B^l$ structure to describe how one can apply the sphere decoding algorithm for demodulation based on our constellations. Suppose A has Schur decomposition

$$A = U\mathrm{diag}\,(e^{i\alpha_1}, e^{i\alpha_2}, \ldots, e^{i\alpha_M})U^*$$

similarly assume

$$B = B\mathrm{diag}\,(e^{i\beta_1}, e^{i\beta_2}, \ldots, e^{i\beta_M})B^*.$$

Consider unitary differential modulation [13] and denote with X_τ the received signal at time block τ. The ML demodulation algorithm involves the following minimization problem:

$$(\hat{k}, \hat{l}) = \arg\min_{k,l} \|X_\tau - A^k B^l X_{\tau-1}\|_F.$$

Algebraically one can check the equation at the top of the page. So every entry of $X_\tau - A^k B^l X_{\tau-1}$ is a linear combination of trigonometric functions $\cos$ or $\sin$ in the variables k, l, which can be viewed as lattice points. As demonstrated in [15] and [11], the whole demodulation task has been converted to a least-squares problem. Consequently, our structured constellation will admit the sphere decoding algorithm. In [15], a detailed study of the sphere decoding algorithm applied to constellations from $Sp(2)$ was undertaken.

The complexity (either upper bound or average complexity) of sphere decoding will depend on the dimension of the lattice. This will make the weak group structure $A^k B^k$ more remarkable, because in this case, the algorithm requires considering finding the closest point in a one-dimensional lattice, which is very simple.

In [3], a very interesting fast demodulation approach is proposed for diagonal space–time constellations. The authors use numerical approximation and the Lenstra–Lenstra–Lovász (LLL) basis reduction technique to reduce the decoding complexity. Note that a constellation with the weak group structure A^k essentially is a diagonal constellation (straightforward Schur decomposition will show this), therefore, the same technique can be applied to this structure. Most importantly, some other algebraic structures can employ the techniques as well. For instance, consider the $A^k B^l C^m$ structure. If we let l go over a large interval and let k, m stay within a small interval, the structure will become "almost" diagonal. For efficient decoding, one only has to do exhaustive search for k, m and apply the techniques for diagonal constellations to decode l. Although the decoding complexity will increase a little, our experiments show the performance will output the diagonal one remarkably. Exactly the same "almost" diagonal idea can be applied to other proposed structures.

VII. Conclusion and Future Work

The *diversity product* and the *diversity sum* for unitary constellations are studied from the analysis of the limiting behavior. We propose algebraic structures, which are suitable for constructing a unitary space–time constellation and feature fast decoding algorithms. Based on the presented structure. we construct unitary constellations using geometrical symmetry and numerical methods. For two dimensions, most of our codes are better or equal to the currently existing ones. For higher dimensions, many codes with excellent diversity are found, which were never found before. Future work may involve analyzing the geometric aspects (such as geodesics, gradients, and Hessians of the functions, etc.) on $U(M)$ or the complex Stiefel manifold. Using the optimization techniques on Riemmannian manifold to optimize the distance spectrum of a unitary constellation to further search for good-performing constellations is under close investigation as well.

References

[1] E. H. L. Aarts and J. Korst, "A stochastic approach to combinatorial optimization and neural computing," in *Simulated Annealing and Boltzmann Machines*. Chichester, U.K.: Wiley, 1989, Wiley-Interscience Series in Discrete Mathematics and Optimization.

[2] S. M. Alamouti, "A simple transmitter diversity scheme for wireless communications," *IEEE J. Sele. Areas Commun.*, vol. 16, no. 8, pp. 1451–1458, Oct. 1998.

[3] K. L. Clarkson, W. Sweldens, and A. Zheng, "Fast multiple-antenna differential decoding," *IEEE Trans. Commun.*, vol. 49, no. 2, pp. 253–261, Feb. 2001.

[4] A. Edelman, T. A. Arias, and S. T. Smith, "The geometry of algorithms with orthogonality constraints," *SIAM J. Matrix Anal. Appl.*, vol. 20, no. 2, pp. 303–353, 1999.

[5] U. Fincke and M. Pohst, "Improved methods for calculating vectors of short length in a lattice, includ-ing a complexity analysis," *Math. Comput.*, vol. 44, pp. 463–471, Apr. 1985.

[6] G. Han and J. Rosenthal, A Website of Unitary Space Time Constellations With Large Diversity [Online]. Available: http://www.nd.edu/~ecoding/space-time/

[7] ——, "Unitary constellation design and its application to space-time coding," in *Proc. 15th Int. Symp. Mathematical Theory of Networks and Systems*, Notre Dame, IN, Aug. 2002.

[8] ——, "Unitary constellations with large diversity sum and good diversity product," in *Proc. 40th Annu. Allerton Conf. Communication, Control, and Computing*, Monticello, IL, Oct. 2002, pp. 48–57.

[9] ——, Unitary Space Time Constellation Analysis: An Upper Bound for the Diversity 2004 [Online]. Available: http://front.math.ucdavis.edu/math.CO/0401045 E-print math.CO/0401045

[10] B. Hassibi and B. M. Hochwald, "Cayley differential unitary space-time codes," *IEEE Trans. Inf. Theory*, vol. 48, no. 6, pp. 1485–1503, Jun. 2002.

[11] B. Hassibi and H. Vikalo, "On the expected complexity of integer least-squares problems," in *Proc. IEEE Int. Conf. Acoustics, Speech and Signal Processing,*, Orlando, FL, Apr. 2002, pp. 1497–1500.

[12] B. Hochwald, T. Marzetta, T. Richardson, W. Sweldens, and R. Urbanke, "Systematic design of unitary space-time constellations," *IEEE Trans. Inf. Theory*, vol. 46, no. 6, pp. 1962–1973, Sep. 2000.

[13] B. Hochwald and W. Sweldens, "Differential unitary space-time modulation," *IEEE Trans. Commun.*, vol. 48, no. 12, pp. 2041–2052, Dec. 2000.

[14] B. M. Hochwald and T. L. Marzetta, "Unitary space-time modulation for multiple-antenna communications in Rayleigh flat fading," *IEEE Trans. Inf. Theory*, vol. 46, no. 2, pp. 543–564, Mar. 2000.

[15] Y. Jing and B. Hassibi, "Fully-diverse $Sp(2)$ code design," in *Proc. 2003 IEEE Int. Symp. Information Theory*, Yokohoma, Japan, Jun./Jul. 2003, p. 299.

[16] ——, "Unitary space-time modulation via Cayley transform," *IEEE Trans. Signal Process.*, vol. 51, no. 11, pp. 2891–2904, Nov. 2003.

[17] X.-B. Liang and X.-G. Xia, "Unitary signal constellations for differential space-time modulation with two transmit antennas: Parametric codes, optimal designs and bounds," *IEEE Trans. Inf. Theory*, vol. 48, no. 8, pp. 2291–2322, Aug. 2002.

[18] N. Metropolis, A. W. Rosenbluth, M. N. Rosenbluth, A. H. Teller, and E. Teller, "Equation of state calculations by fast computing machines," *J. Chem. Phys.*, vol. 21, no. 6, pp. 1087–1092, 1953.

[19] J. Nocedal and S. J. Wright*, Numerical Optimization*. New York: Springer-Verlag, 1999, Springer Series in Operations Research.

[20] R. H. J. M. Otten and L. P. P. P. van Ginneken*, The Annealing Algorithm*. Boston, MA: Kluwer Academic, 1989, The Kluwer International Series in Engineering and Computer Science. VLSI, Computer Architecture and Digital Signal Processing.

[21] V. V. Prasolov*, Problems and Theorems in Linear Algebra.* Transl.: Russian manuscript by D. A. Leĭtes. Providence, RI: Amer. Math. Soc., 1994, vol. 134, *Translations of Mathematical Monographs*.

[22] A. Shokrollahi, "Computing the performance of unitary space-time group codes from their character table," *IEEE Trans. Inf. Theory*, vol. 48, no. 6, pp. 1355–1371, Jun. 2002.

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

[24] V. Tarokh and H. Jafarkhani, "A differential detection scheme for transmit diversity," *IEEE J. Sel. Areas Commun.*, vol. 18, no. 7, pp. 1169–1174, Jul. 2000.

[25] P. J. M. van Laarhoven and E. H. L. Aarts*, Simulated Annealing: Theory and Applications*. Dordrecht, The Netherlands: Reidel, 1987, vol. 37, *Mathematics and its Applications*.

[26] H. Zassenhaus, "Über endliche Fastkörper," *Abh. Math. Sem. Hamburg*, vol. 11, pp. 187–220, 1936.

On the Dimensions of Certain LDPC Codes Based on q-Regular Bipartite Graphs

Peter Sin and Qing Xiang

***Abstract*—An explicit construction of a family of binary low-density parity check (LDPC) codes called *$LU(3,q)$*, where q is a power of a prime, was recently given. A conjecture was made for the dimensions of these codes when q is odd. The conjecture is proved in this note. The proof involves the geometry of a four-dimensional (4-D) symplectic vector space and the action of the symplectic group and its subgroups.**

***Index Terms*—Generalized quadrangle, incidence matrix, low-density parity check (LDPC) code, symplectic grou.**

I. Introduction

Let V be a four-dimensional (4-D) vector space over the field $\mathbf{F}_q$ of q elements. We assume that V has a nonsingular alternating bilinear form (v, v') and denote by $\mathrm{Sp}(V)$ the group of linear automorphisms of V which preserve this form. We choose a symplectic basis e_0, e_1, e_2, e_3 of V, with $(e_i, e_{3-i}) = 1$, for $i = 0, 1$.

Let $P = \mathbf{P}(V)$ be the set of points of the projective space of V. A subspace of V is said to be *totally isotropic* if $(v, v') = 0$ whenever v and v' are both in the subspace. Let L denote the set of totally isotropic two-dimensional (2-D) subspaces of V, considered as lines in P. The pair (P, L), together with the natural relation of incidence between points and lines, is called the *symplectic generalized quadrangle*. Except for in the appendix, the term "line" will always mean an element of L. It is easy to verify that (P, L) satisfies the following *quadrangle property*. Given any line and any point not on the line, there is a unique line which passes through the given point and meets the given line.

Now fix a point $p_0 \in P$ and a line $\ell_0 \in L$ through p_0. We can assume that we chose our basis so that $p_0 = \langle e_0 \rangle$ and $\ell_0 = \langle e_0, e_1 \rangle$. For $p \in P$, denote by $p^{\perp}$ the set of points on lines through p; $p' \in p^{\perp}$ if and only if the subspace of V spanned by p and p' is isotropic. Consider the set $P_1 = P \setminus p_0^{\perp}$ of points not collinear with p_0, and the set L_1 of lines which do not meet ℓ_0. Then we can also consider the incidence systems $(P_1, L_1), (P, L_1)$, and (P_1, L). Let $M(P, L)$ and $M(P_1, L_1)$ be the binary incidence matrices of the respective incidence systems, with rows indexed by points and columns by lines. The rows and columns of $M(P, L)$ have weight $q + 1$ and, as a consequence of the quadrangle property, those of $M(P_1, L_1)$ have weight q.

If q is odd we know by Theorem 9.4 of [1] that the 2-rank of $M(P, L)$ is $(q^3 + 2q^2 + q + 2)/2$. Here we prove the following theorem.

Theorem 1.1: Assume q is a power of an odd prime. The 2-rank of $M(P_1, L_1)$ equals $(q^3 + 2q^2 - 3q + 2)/2$.

In [2], a family of codes designated $\mathrm{LU}(3, q)$ was defined in the following way. Let P^* and L^* be sets in bijection with $\mathbf{F}_q{}^3$, where q is any prime power. An element $(a, b, c) \in P^*$ is incident with an element $[x, y, z] \in L^*$ if and only if

$$y = ax + b \quad \text{and} \quad z = ay + c. \tag{1}$$

The binary incidence matrix with rows indexed by L^* and columns indexed by P^* is denoted by $H(3, q)$ and the two binary codes having $H(3, q)$ and its transpose as parity check matrices are called $\mathrm{LU}(3, q)$ codes. The name comes from [3], where the bipartite graph with parts P^* and L^* and adjacency defined by the (1) had been studied previously.

It is not difficult to show that the incidence systems (P_1, L_1) and (P^*, L^*) are equivalent. A detailed proof is given in the Appendix. Thus, $M(P_1, L_1)$ is a parity check matrix of the $\mathrm{LU}(3, q)$ code given by the transpose of $H(3, q)$ and Theorem 1.1 has the following immediate corollary.

Corollary 1.2: If q is a power of an odd prime, the dimension of $\mathrm{LU}(3, q)$ is $(q^3 - 2q^2 + 3q - 2)/2$.

The corollary was conjectured in [2]. There it was established that this number is a lower bound when q is an odd prime.

II. Relative Dimensions and a Lower Bound for $\mathrm{LU}(3, q)$

In this section q is an arbitrary prime power.

Let $\mathbf{F}_2[P]$ be the vector space of all $\mathbf{F}_2$-valued functions on P. We can think of such a function as a vector in which the positions are indexed by the points of P, and the entries are the values of the function at the points. For $p \in P$, the characteristic function χ_p is the vector with 1 in the position with index p and zero in the other positions. The set of all characteristic functions of points forms a basis of $\mathbf{F}_2[P]$. Let $\ell \in L$. Its characteristic function $\chi_\ell \in \mathbf{F}_2[P]$ is the function which takes the value 1 at the $q + 1$ points of ℓ and zero at all other points. The subspace of $\mathbf{F}_2[P]$ spanned by all the χ_ℓ is the $\mathbf{F}_2$-code of (P, L), denoted by $C(P, L)$. One can think of $C(P, L)$ as the column space of $M(P, L)$. For brevity, we will sometimes blur the distinction between lines and their characteristic functions and speak, for instance, of the subspace of $\mathbf{F}_2[P]$ spanned by a set of lines. Let $C(P, L_1)$ be the subspace of $\mathbf{F}_2[P]$ spanned by lines in L_1. Let $C(P_1, L_1)$ denote the code of (P_1, L_1), viewed as a subspace of $\mathbf{F}_2[P_1]$, and let $C(P_1, L)$ be the larger subspace of $\mathbf{F}_2[P_1]$ spanned by the restrictions to P_1 of the characteristic functions of all lines of L.

Consider the natural projection map

$$\pi_{P_1} : \mathbf{F}_2[P] \rightarrow \mathbf{F}_2[P_1] \tag{2}$$

given by restriction of functions. Its kernel will be denoted by $\ker \pi_{P_1}$.

Let $Z \subset C(P, L_1)$ be a set of characteristic functions of lines in L_1 which maps bijectively under π_{P_1} to a basis of $C(P_1, L_1)$. Let X be the set of characteristic functions of the $q + 1$ lines of L through p_0 and let $X_0 = X \setminus \{\chi_{\ell_0}\}$. Finally, choose any q lines of L which meet ℓ_0 in the q distinct points other than p_0 and let Y be the set of

Manuscript received May 25, 2005; revised January 1, 2006. The work of Q. Xiang was supported by the NSF under Grant DMS0400411.

P. Sin is with the Department of Mathematics, University of Florida, Gainesville, FL 32611 USA (e-mail: sin@math.ufl.edu).

Q. Xiang is with the Department of Mathematical Sciences, University of Delaware, Newark, DE 19716 USA (e-mail: xiang@math.udel.edu).

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

Digital Object Identifier 10.1109/TIT.2006.878231