Space-Time Codes from Groups

Jarkko Hiltunen

Turku Centre for Computer Science TUCS,
Lemminkäisenkatu 14 A, 5th floor,
FIN-20520 Turku, Finland
e-mail: jakahi@utu.fi

Jyrki Lahtonen

Department of Mathematics,
University of Turku,
FIN-20014 Turku, Finland
e-mail: lahtonen@utu.fi

Anu Nikkanen

Turku Centre for Computer Science TUCS,
Lemminkäisenkatu 14 A, 5th floor,
FIN-20520 Turku, Finland
e-mail: anu.nikkanen@utu.fi

Turku Centre for Computer Science
TUCS Technical Report No 513
February 2003

ISBN 952-12-1127-x
ISSN 1239-1891

Abstract

The basic principle of diversity in the wireless communication is to provide multiple copies of information for a receiver, which can select or combine the received informations to obtain the best quality for reception. Diversity is commonly introduced in either the space, time, or frequency domain.

Space-time coding is a method in which the diversity is introduced in both the time and space domains by utilizing multiple transmit antennas. The data transmitted from multiple antennas is also spread in time supplying the receiver with a sum of the transmitted signals passed over independent fading channels.

In this report we consider the design of space-time block codes for 2 and 4 transmit antennas which are based on the theory of group. Especially we use the representations of the groups to design space-time codes with full diversity.

This report based on the report on the subproject "Applications of algebra in space-time coding" within the project "Telecommunications applications of discrete mathematics" funded by TEKES and Nokia Research Center.

Keywords: space-time coding, product distance, group

TUCS Laboratory
Discrete Mathematics for Information Technology Laboratory
Coding Theory Group

Contents

1 Introduction

In this chapter we give the definitions and the notations needed in the design of the space-time codes. We also present the design criteria of the space-time codes in the Rayleigh fading channel (details from the Rayleigh fading channel you can see [1]).

1.1 The System Model and Performance Criteria in the Rayleigh Fading Channel

In this section we will describe a basic model for a communication system that employs ST coding with N_t transmit antennas and N_r receive antennas. In this system, the message $\mathbf{m} \in \mathcal{M}$ are encoded by function σ to the code matrix $\sigma(\mathbf{m}) \in M_{N_\times L}(\mathcal{A}) \subseteq M_{N_\times L}(\mathbb{C})$, where $\mathcal{A}$ is the constellation alphabet.

We will assume that the encoding function σ maps message $\mathbf{m}$ to the matrix

$$\sigma(\mathbf{m}) = \begin{pmatrix} c_{11} & c_{12} & \cdots & c_{1L} \\ c_{21} & c_{22} & \cdots & c_{2L} \\ \vdots & \vdots & \ddots & \vdots \\ c_{N_t1} & c_{N_t2} & \cdots & c_{N_tL} \end{pmatrix}.$$

At each time slot t, signals $c_{it},\ i = 1, 2, ..., N_t$ are transmitted simultaneously from the N_t transmit antennas. The fading coefficient h_{ij} is the path gain from transmit antenna i to receive antenna j (we have N_tN_r independent fading channels). The wireless channel is assumed to be quasi-static, i.e., the path gains are constant over a frame of length L, and vary from frame to frame. At time slot t the received signal r_{tj} at antenna j is given by

$$r_{tj} = \sum_{i=1}^{N_t} h_{ij} c_{it} \sqrt{E_s} + n_{tj},$$

where n_{tj} is AWGN noise sample for receive antenna j at time slot t and the scale factor $\sqrt{E_s}$ has chosen so that the average energy of the constellation elements is 1. The noise samples are independent samples of a zero-mean complex Gaussian random variable with variance $\frac{N_0}{2}$ per dimension.

In matrix notation, we have

$$\overline{R} = \sqrt{E_s}\overline{H}^T \sigma(\mathbf{m}) + \overline{N}$$

where

$$\overline{R} = \begin{pmatrix} r_{11} & r_{21} & \dots & r_{L1} \\ r_{12} & r_{22} & \dots & r_{L2} \\ \vdots & \vdots & \ddots & \vdots \\ r_{1N_r} & r_{2N_r} & \dots & r_{LN_r} \end{pmatrix},$$

$$\overline{H} = \begin{pmatrix} h_{11} & h_{12} & \dots & h_{1N_r} \\ h_{21} & h_{22} & \dots & h_{2N_r} \\ \vdots & \vdots & \ddots & \vdots \\ h_{N_t1} & h_{N_t2} & \dots & h_{N_tN_r} \end{pmatrix},$$

$$\overline{N} = \begin{pmatrix} n_{11} & n_{21} & \dots & n_{L1} \\ n_{12} & n_{22} & \dots & n_{L2} \\ \vdots & \vdots & \ddots & \vdots \\ n_{1N_r} & n_{2N_r} & \dots & n_{LN_r} \end{pmatrix}.$$

The receiver knows $\overline{H}$ and computes the maximum likelihood estimate of the transmitted data as

$$\hat{\mathbf{m}} = \arg\min_{\mathbf{e}\in\mathcal{M}} \parallel \overline{R} - \sqrt{E_s}\overline{H}^T\sigma(\mathbf{e}) \parallel,$$

where the matrix norm is the Frobenius norm.

Definition 1.1. An $N_t \times L$ space-time code $\mathcal{C}$ of size K is the subset of $M_{N_t\times L}(\mathbb{C})$ of size K.

1.1.1 Performance Criteria in the Rayleigh Fading Channel

Next we shall consider in the Rayleigh fading channel the probability that a maximum-likelihood receiver decides erroneously in favor of a matrix

$$E = \begin{pmatrix} e_{11} & e_{12} & \dots & e_{1L} \\ e_{21} & e_{22} & \dots & e_{2L} \\ \vdots & \vdots & \ddots & \vdots \\ e_{N_t1} & e_{N_t2} & \dots & e_{N_tL} \end{pmatrix} \in \mathcal{C}$$

assuming that

$$C = \begin{pmatrix} c_{11} & c_{12} & \dots & c_{1L} \\ c_{21} & c_{22} & \dots & c_{2L} \\ \vdots & \vdots & \ddots & \vdots \\ c_{N_t1} & c_{N_t2} & \dots & c_{N_tL} \end{pmatrix} \in \mathcal{C}$$

was transmitted.

Assuming ideal channel state information, the probability of transmitting C and deciding in favor of E at the decoder is well upper bounded by [4]

$$P(C \to E \mid h_{ij},\ i = 1, ..., N_t,\ j = 1, ..., N_r) \leq \exp(-d^2(C, E)E_s/4N_0) \quad (1)$$

where $N_0/2$ is noise variance per dimension and

$$d^2(C, E) = \| \overline{H}^T C - \overline{H}^T E) \|^2 . \quad (2)$$

We observe that

$$d^2(C, E) = \mathrm{Tr}((\overline{H}^T (C - E)(C - E)^* (\overline{H}^T)^*). \quad (3)$$

Since $A(C, E) = (C - E)(C - E)^*$ is Hermitian, there exist a unitary matrix V and a real diagonal matrix D such that $VA(C, E)V^* = D$. The rows $(\mathbf{v_1}, ..., \mathbf{v_{N_t}})$ of V are a complete orthonormal basis of $\mathbb{C}^n$ given by eigenvectors of $A(C, E)$. The diagonal elements of D are the eigenvalues λ_i, $i = 1, 2, ..., N_t$ of $A(C, E)$ counting multiplicities. The matrix

$$C - E = \begin{pmatrix} c_{11} - e_{11} & c_{12} - e_{12} & \dots & c_{1L} - e_{1L} \\ c_{21} - e_{21} & c_{22} - e_{22} & \dots & c_{2L} - e_{2L} \\ \vdots & \vdots & \ddots & \vdots \\ c_{N_t1} - e_{N_t1} & c_{N_t2} - e_{N_t2} & \dots & c_{N_tL} - e_{N_tL} \end{pmatrix} \quad (4)$$

is clearly a square root of $A(C, E)$. Thus the eigenvalues of $A(C, E)$ are nonnegative real numbers.

Now we get the upper bound on the average pairwise error probability (see [2])

$$E(P(C \to E)) \leq \left(1/ \prod_{i=1}^{N_t} (E_s \lambda_i / 4N_0 + 1) \right)^{N_r} . \quad (5)$$

Let k denote the rank of matrix $A(\mathbf{c}, \mathbf{e})$ and for large SNR values

$$E(P(C \to E)) \leq [E_s/4N_0]^{-kN_r} \left(\prod_{i=1}^{k} \lambda_i \right)^{-N_r} . \quad (6)$$

Thus a diversity advantage of $N_r k$ and a coding advantage of $(\lambda_1 \lambda_2 \cdots \lambda_k)^{1/k}$ is achieved. Note that $\lambda_1 \lambda_2 \cdots \lambda_k$ is the absolute value of the sum of determinant of all principal $k \times k$ cofactors of $A(C, E)$. Moreover it is easy to see that the ranks of the matrices $A(C, E)$ and $C - E$ are equal.

Remark. 1.1. We note that the diversity advantage is the power of SNR in the denominator of the expression for the pairwise error probability derived above. The coding advantage is an approximate measure of the gain over an uncoded system operating with the same diversity advantage.

To get $E(P(C \to E))$ as low as possible we try to minimize the right-hand side of (6) and thus we arrive at the following design criterion.

The Rank Criterion: To minimize $[E_s/4N_0]^{-kN_r}$ we have to achieve the maximum diversity N_tN_r, the matrix $C - E$ has to be full rank for any distinct code matrices C and E. Otherwise a diversity of kN_r is achieved.

The Product Distance Criterion: To minimize $\left(\prod_{i=1}^{k} \lambda_i\right)^{-N_r}$ we have to maximize the coding advantage $(\lambda_1, \lambda_2, ..., \lambda_k)^{\frac{1}{k}}$ over all pairs of distinct code matrices C and E. For a diversity of N_tN_r, the minimum of the determinant of $A(C, E)$ taken over all pairs of distinct code words C and E must be maximized.

The rank criterion is the more important of the two as it determines the asymptotic slope of the performance curve as a function of E_s/N_0. The product distance criterion is of secondary importance and, ideally should be optimized after the diversity advantage is maximized. The product distance criterion will motivate us to the next definition.

Definition 1.2. The minimum product distance of the space-time code $\mathcal{C}$ is the parameter

$$pd_{\min}(\mathcal{C}) = \min_{C,C' \in \mathcal{C}, C \neq C'} \det((C - C')(C - C')^*)^{\frac{1}{N_t}} \tag{7}$$

2 The Design of the Space-Time Group codes

In this report we consider the space-time codes which are based on the theory of groups. The classical group code in the real Gaussian channel is gotten by letting the elements g of a chosen group G act on a chosen (row) vector X, i.e. the code consists of all the vectors Xg (see [7]). If we make the natural restriction that the group consists of complex unitary (or real orthogonal) matrices, then we immediately see that these codes have the desirable property of geometric uniformity, the code "looks exactly the same from each code block". This makes the analysis of the code much easier, as instead of comparing two arbitrary different code matrices, it suffices to study the "distance" from the generator to any other code block (see the equation (9) below).

In this chapter we look for space-time group codes that have all of the following properties: full diversity, a desirable size (power of 2), a good minimum product distance and an efficient ML-decoding algorithm.

The extension of the group code idea into space-time setting is relatively straightforward. We simply use one generator vector for each transmit antenna, or more conveniently, we have a $N_t \times L$ generator matrix X that is acted from the right by multiplication with complex unitary $L \times L$-matrices g forming a finite group G.

Definition 2.1. If $G = \{g | g$ is complex unitary $L \times L$ matrix$\}$ is a finite group and X is $N_t \times L$ "generator" matrix then the set

$$\mathcal{C}(G, X) = \{Xg | g \in G\}$$

is an $N_t \times L$ space-time group code.

Lemma 2.1. *If A and B are such matrices that the matrix product AB can be define then*

$$rank(AB) \leq \min(rank(A), rank(B)).$$

Especially

$$rank(AB) = \begin{cases} rank(A) & \text{if } B \text{ is invertible} \\ rank(B) & \text{if } A \text{ is invertible} \end{cases}$$

Proof. See [5]. □

For space-time code we require that they satisfy the full diversity criterion: the difference between any two code matrices must have full rank. By lemma 2.1 it is easy to see that for any $Xg,\ Xg' \in \mathcal{C}(G, X)$ $g \neq g'$

$$\begin{aligned} \text{rank}(Xg - Xg') &= \text{rank}(X(g - g')) \\ &= \text{rank}(X(I - g'g^{-1})g) \\ &= \text{rank}(X(I - g'')) \quad (g'' = g'g^{-1} \in G \setminus \{I\}). \\ &\leq \min(\text{rank}(X), \text{rank}(I - g'')). \end{aligned} \tag{8}$$

By inequality (8) we must have the inequality $N_t \leq L$ and the generator matrix X must be of a full rank.

It is easy to see that the matrices $X(I - g'')$ have a full rank for all $g'' \in G \setminus \{I\}$ if and only if the rowspace V (a N_t-dimensional subspace of $\mathbb{C}^L$) of X must not contain any eigenvectors belonging to the eigenvalue 1 for any group element $g'' \neq I$.

Thus the full diversity criterion is now equivalent to the requirement: We must have the inequality $N_t \leq L$ and the generator matrix X must be of a full rank. Moreover the rowspace V of X must not contain any eigenvectors belonging to the eigenvalue 1 for any group element $g \neq I$.

Remark. 2.1. From equation (8) we get that the multiplicity of 1 as an eigenvalue must not exceed $L - N_t$. Below we will refer to this criterion as the multiplicity criterion.

After we have chosen a group G of the prescribed parameters N_t, L and the number of elements which satisfies the multiplicity criterion, we must still be careful in our choice of the generator matrix X. We are really selecting a N_t-dimensional subspace V (the rowspace of X) and a orthonormal basis for it (the rows of X).

Remark. 2.2. It is worth emphasizing that (as in the single transmit antenna Gaussian channel case) a group code combines both modulation and coding. This is in sharp contrast to the use of orthogonal designs, where one is free to choose the modulation alphabet (the collection of all the values taken by the variables c_i) after having constructed the design. Also, in using an orthogonal design one usually will select the combinations of the symbols c_i so that they form words of a code (either a block code or a convolutional code). When a group code approach is used both the modulation alphabet (the collection of all the entries of all the matrices in the code) as well as the code (a subset of all "legal" combinations of alphabets) are created simultaneously.

Furthermore in comparing two group codes (gotten either from two different groups of the same size or the same group but different generator matrix) the minimum product distance must be maximized. Because the group codes have the property of geometric uniformity, the minimum product distance can be calculated very simply as

$$\begin{aligned}
pd_{min}(\mathcal{C}(G,X)) &= \min_{g,g' \in G, g \neq g'} \det\left((Xg - Xg')(Xg - Xg')^*\right)^{\frac{1}{N_t}} \\
&= \min_{g,g' \in G, g \neq g'} \det\left((Xg - Xg')(g^*X^* - g'^*X^*)\right)^{\frac{1}{N_t}} \\
&= \min_{g,g' \in G, g \neq g'} \det\left((X - Xg'g^*)gg^*(X^* - gg'^*X^*)\right)^{\frac{1}{N_t}} \\
&= \min_{g,g' \in G, g \neq g'} \det X\left((I - g'g^*)(I - gg'^*)X^*\right)^{\frac{1}{N_t}} \\
&= \min_{g'' \in G, g'' \neq I} \det X\left((I - g'')(I - g'')X^*\right)^{\frac{1}{N_t}}. \qquad (9)
\end{aligned}$$

From the point of view of group theory, the case $N_t = L$, i.e. the study of fixed-point-free representations (see [8]) is interesting. In this case the space V must be all of $\mathbb{C}^L$, so we may as well choose $X = I_L$ or any other unitary matrix (e.g. a Walsh-Hadamard matrix, if we want to spread the signal power more evenly in both time and space).

2.1 Fixed-Point-Free Groups

Definition 2.2. If ρ is such representation of the group G that for any $g \in G$, $g \neq 1_G$, the $\rho(g)$ does not have an eigenvalue at unity then we say that ρ is fixed-point-free representation. We call a group fixed-point-free if it has a fixed-point-free representation. Moreover we call a group fixed-point-free p-group if G is fixed-point-free and $|G| = p^k$, $p \in \mathbb{P},\ k > 0$.

We start out with a class of groups that are always fixed-point-free: the class of cyclic groups. We denote a cyclic group G, generated by an element σ, as $G = \langle\sigma\rangle$. If G has order n, then $G = \{\sigma^k | k = 0, ..., n-1\}$. It suffices to consider the irreducible fixed-point-free representations, since the irreducible constituents of a fixed-point-free representation have to be fixed-point-free themselves. But fixed-point-free irreducible representations of cyclic groups are trivial: Irreducible representations of Abelian groups are one-dimensional (see [6]), i.e., they are characters of the group. A character is fixed-point-free if and only if it is primitive.

The cyclic group G has n characters given by

$$\chi_u(\sigma^k) = e^{\frac{2\pi i u k}{n}}, \text{ for } u = 0, ..., n-1,$$

but the character χ_u is primitive if and only if $\gcd(u, n) = 1$. Thus there are $\phi(n)$ primitive characters in the cyclic group G. An M-dimensional representation ρ of G is built as a direct sum of M characters

$$\begin{aligned}\rho(\sigma) &= \begin{pmatrix} \chi_{u_1}(\sigma) & 0 & \cdots & 0 \\ 0 & \chi_{u_2}(\sigma) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \chi_{u_M}(\sigma) \end{pmatrix} \\ &= \begin{pmatrix} \omega^{u_1} & 0 & \cdots & 0 \\ 0 & \omega^{u_2} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \omega^{u_M} \end{pmatrix}, \quad \omega = e^{\frac{2\pi i}{n}}.\end{aligned}$$

Now it is easy to see that

$$\rho(\sigma^k) = \begin{pmatrix} \omega^{ku_1} & 0 & \cdots & 0 \\ 0 & \omega^{ku_2} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \omega^{ku_M} \end{pmatrix}, \quad k = 0, ..., n-1,$$

thus the representation ρ is fixed-point-free if and only if $\gcd(n, u_m) = 1$ for all $m = 1, ..., M$.

If G is Abelian but not cyclic, then

$$G = C_{g_1} \times \cdots C_{g_r} =< s_1 > \times \cdots < s_r >$$

where $\gcd(g_1, ..., g_r) > 1$. The Abelian group G has $g_1 \cdots g_r$ characters given by

$$\chi_{m_1,...,m_r}(s_1^{k_1}, ..., s_r^{k_r}) = e^{2\pi i(\frac{k_1 m_1}{g_1} + \cdots + \frac{k_r m_r}{g_r})}, \quad 0 \le k_i, m_i \le g_i - 1.$$

It is easy to see that for all characters of G $\mathrm{Im}(\chi_{m_1,...,m_r}) \subseteq \langle e^{\frac{2\pi i}{(g_1 \cdots g_r)/\gcd(g_1,...,g_r)}} \rangle$. Now $|\mathrm{Im}(\chi_{m_1,...,m_r})| < |G|$ and therefore $\chi_{m_1,...,m_r}$ can't be injection. We conclude that an Abelian group is fixed-point-free if and only if it is cyclic.

It is well known (see [8]) that the only fixed-point-free 2-groups are the so called generalized quaternion groups. If ω is a primitive root of unity of order 2^{k-1}, then the monomial 2×2-matrices

$$\sigma = \begin{pmatrix} \omega & 0 \\ 0 & \overline{\omega} \end{pmatrix}, \quad \text{and} \quad \tau = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

of orders 2^{k-1} and 4 respectively generate a fixed-point-free group Q_{2^k} called the generalized quaternion group of 2^k elements. Now the Alamouti with QPSK alphabet is the union of two codes, which are gotten by using two different generator matrices and the group Q_8 (see the next example 2.1). Similarly Alamouti with 8-PSK alphabet is a union of 4 orbits of the group Q_{16}.

Example 2.1. Let $L = N_t = 2$. Let G be the quaternion group generated by the matrix

$$A = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

so

$$G = \{I, A, A^2 = -I, A^3 = A^{-1}, B, BA, BA^2, BA^3\}.$$

Now a good choice for the generator matrix is

$$X_1 = \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}$$

and the entire code consists of the following 8 matrices

$$\begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}, \begin{pmatrix} i & 1 \\ -1 & -i \end{pmatrix}, \begin{pmatrix} -1 & -i \\ -i & -1 \end{pmatrix}, \begin{pmatrix} -i & -1 \\ 1 & i \end{pmatrix},$$

$$\begin{pmatrix} -i & 1 \\ -1 & i \end{pmatrix}, \begin{pmatrix} -1 & i \\ i & -1 \end{pmatrix}, \begin{pmatrix} i & -1 \\ 1 & -i \end{pmatrix}, \begin{pmatrix} 1 & -i \\ -i & 1 \end{pmatrix}.$$

We observe that this one half of the code gotten from the Alamouti scheme using the 4-phase alphabet $\{1, i, -1, -i\}$. We get the other half by using the generator matrix

$$X_2 = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}.$$

We emphasize that the quaternion groups have the very desirable property that the differences between any two matrices within the group have the equal singular eigenvalue property called for in [9], i.e. the rows of a difference matrix have the same norm and are orthogonal to each other. Thus they may turn out to be useful in other ST code constructions as well.

2.2 Building Groups of Monomial Matrices

A monomial matrix is a square matrix with exactly one non-zero entry on each row and column. We further restrict ourselves to such monomial matrices, where the non-zero entries are roots of unity. Monomial matrices are desirable for the reason that postmultiplication of a generator matrix by a monomial matrix results in first simply permuting the entries on each row and then multiplying them by various roots of unity. Thus we have a complete control of the modulation alphabet, when we use monomial matrices. Furthermore the classification of fixed-point-free groups tells that most fixed-point-free groups can be written as groups of monomial matrices, which strongly suggests that monomial matrices are a natural first testing ground.

A monomial matrix M can be written as a product $M = DP$ of a diagonal matrix D and a permutation matrix P. If the vector of the diagonal entries of D is $(d_1, d_2, ..., d_n)$, and postmultiplication of the vector $(x_1, x_2, ..., x_n)$ by P gives the permuted vector $(x_{\pi(1)}, x_{\pi(2)}, ..., x_{\pi(n)})$ for some permutation π on n letters, we will use the shorthand notation $M = (d_1\pi(1), d_2\pi(2), ..., d_n\pi(n))$ to compactly write a monomial matrix.

Example 2.2. The matrices

$$\sigma = \begin{pmatrix} \omega & 0 \\ 0 & \overline{\omega} \end{pmatrix}, \quad \text{and} \quad \tau = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

can be written compactly using notation $\sigma = (\omega, 2\overline{\omega})$ and $\tau = (-2, 1)$.

Observe that as the elements of D are roots of unity, this can never result in any confusion. Thus $M = (-3, 4, -1, 2, 6, -5, -8, 7)$ is the linear transformation that maps the vector $(x_1, x_2, ..., x_n)$ to the vector $(-x_3, x_4, -x_1, x_2, x_6, -x_5, -x_8, x_7)$. We observe that it is very easy to compute the multiplicity of 1 as an eigenvalue of such a monomial matrix. We simply multiply the numbers d_i where i ranges over a cycle of π. Do this for all the cycles and conclude that the desired multiplicity is equal to the number of times 1 occured as such a product.. E.g. the cycles in the above matrix M are $(13), (24), (56)$ and (78). The respective products are $d_1d_3 = 1, d_2d_4 = 1, d_5d_6 = -1$ and $d_7d_8 = -1$, so we conclude that the multiplicity of 1 as an eigenvalue for this linear transformation is 2.

Let us study building blocks for groups G consisting of monomial matrices only. Let U be the "group alphabet" (the collection of the non-zero matrix entries, usually consists of roots of unity of a small order). The diagonal matrices in G form a normal subgroup C called the block code of G (= a linear block code with alphabet U written multiplicatively (see the next example)).

Example 2.3. We can identify $\mathbb{Z}_4$-word $\mathbf{s} = (s_1, ..., s_L) \in (\mathbb{Z}_4)^L$ with the matrix $M(\mathbf{s}) = \mathrm{diag}(i^{s_1}, ..., i^{s_L})$. Now it is easy to see that $M(\mathbf{s} + \mathbf{s}') = M(\mathbf{s})M(\mathbf{s}')$.

The quotient group $\Sigma = G/C$ is the group of permutations of G. We identify these permutations with their permutation matrices even though the corresponding permutation matrices don't necessarily appear in the group G as "pure" permutations (i.e. as monomial matrices with 1 in the non-zero entries).

Now all the elements of the group G can be written in the form $\mathrm{diag}(c_1, ..., c_L)\sigma$, where $\sigma \in \Sigma$ and $\mathrm{diag}(c_1, ..., c_L)$. If we multiply $g = \mathrm{diag}(c_1, ..., c_L)\sigma \in G$ by $g' = \mathrm{diag}(c'_1, ..., c'_L)\sigma' \in G$ we get

$$\begin{aligned} gg' &= \mathrm{diag}(c_1, ..., c_L)\sigma\mathrm{diag}(c'_1, ..., c'_L)\sigma' \\ &= \mathrm{diag}(c_1, ..., c_L)\sigma\mathrm{diag}(c'_1, ..., c'_L)\sigma^{-1}\sigma\sigma' \\ &= \mathrm{diag}(c_1, ..., c_L)\mathrm{diag}(c'_{\sigma(1)}, ..., c'_{\sigma(L)})\sigma\sigma' \\ &= \mathrm{diag}(c_1c'_{\sigma(1)}, ..., c_nc'_{\sigma(L)})\sigma\sigma'. \end{aligned}$$

Now $\sigma\sigma' \in \Sigma$, but $\mathrm{diag}(c_1c'_{\sigma(1)}, ..., c_nc'_{\sigma(L)}) \in C$ if and only if $\mathrm{diag}(c'_{\sigma(1)}, ..., c'_{\sigma(L)}) \in C$. This imply that $\Sigma \subseteq \mathrm{Aut}(C)$.

A natural way to construct G is to extend a block code C by a subgroup Σ of its automorphism group, i.e. we require that $C^\sigma =_{def} \sigma C \sigma^{-1} = C$ for any pure permutation $\sigma \in \Sigma$. In order for the group G to meet the multiplicity criterion, we must require that the minimum Hamming weight of C is at least $L - N_t$, for otherwise the multiplicity criterion is trivially violated by a low weight matrix in C.

The simplest way of constructing $G = \Sigma \ltimes C$ as a semidirect product of the two component groups is often not optimal, as the pure permutations have 1 as an eigenvalue of a relatively high multiplicity (see the section 2.2). We get better diversity by constructing G as the union of sets of the form $\sigma f(\sigma)$, for all pure permutations $\sigma \in \Sigma$, where $f(\sigma) \in U^L/C$ is a carefully chosen coset of C. Now

$$\sigma f(\sigma)\tau f(\tau) = \sigma\tau\tau^{-1} f(\sigma)\tau f(\tau),$$

so for the set $\cup_{\sigma\in\Sigma}\sigma f(\sigma)$ to be a group it is necessary and sufficient that $f(\sigma\tau) = f(\sigma)^\tau * f(\tau)$ for all $\sigma, \tau \in \Sigma$, i.e. the map $f : \Sigma \mapsto U^L/C$ is a so called crossed homomorphism.

Using this construction idea, the game will be to first find a good block code whose automorphism group has a large 2-Sylow subgroup, and then to try to find a suitable crossed homomorphism so that the resulting group satisfies the desired multiplicity criterion.

Example 2.4. Here we may use the overall parity check code C of length $L = 4$ in the group alphabet U. Any permutation of the 4 symbol positions is obviously an automorphism, so we choose Σ to be the dihedral group generated by the permutations (12) and (13)(24). We only need to worry about the 2-cycles in the group. Choosing the obvious crossed homomorphism

$$f(\sigma) = \begin{cases} C & \text{if } \sigma \text{ is an even permutation} \\ \mathrm{diag}(-1,1,1,1) * C, & \text{otherwise} \end{cases}$$

gives us a group $P(U) \bullet D_4 = \cup_{\sigma\in\Sigma}\sigma f(\sigma)$ of cardinality $8 * (\sharp U)^3$ that meets the multiplicity criterion for diversity two (see example 3.1). Thus the resulting constellations have a bandwith efficiency of $3(1 + \log_2(\sharp U))/4$ bits/s/Hz.

If $U = \{1, -1\}$ then the generator matrix

$$X = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i & 1 & 1 \\ 1 & 1 & -1 & i \end{pmatrix}$$

give us the minimum product distance 2.

If $U = \{1, -1, i, -i\}$ then the generator matrix

$$X = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & w & 1 & 1 \\ 1 & 1 & -1 & -w^* \end{pmatrix}, \text{ where } w = \frac{1+i}{\sqrt{2}}$$

give us the minimum product distance $\sqrt{6 - 4\sqrt{2}}$.

3 Trellis Representations of Groups

Assume that the receiver has perfect channel state information available. The task for the decoder (assume a single receiver antenna for the sake simplicity) is to find the group element g that gives the best match (= the smallest Euclidean separation) between the received vector $\mathbf{r}$ and the vector $\mathbf{y} = HXg$ (here H is the channel vector). The brute force method of doing this is to try all the group elements in sequence, and simply record the best match.

In all decoding, where soft information (here the individual components of $\mathbf{y}$ and $\mathbf{r}$) is available, significant savings to the brute force -method can be achieved by taking into account common parts of the code vectors (here common columns of the group matrices). The following is an exact analog of the familiar BCJR-trellis representation of linear block codes (see [10]).

Assume that an ordered orthonormal basis $v_1, v_2, ..., v_L$ for the ambient space is given. For any relevant j let $V_{j,i}$ be the subspace spanned by the initial vectors $v_1, v_2..., v_j$, and let $V_{j,f}$ be its orthogonal complement spanned by the final vectors $v_{j+1}, v_{j+2}, ..., v_L$. Let $G_{j,i}$ (resp. $G_{j,f}$) be the subgroups that act trivially on $V_{j,i}$ (resp. $V_{j,f}$).

Lemma 3.1. *The subgroup generated by groups $G_{j,i}$ and $G_{j,f}$ is their direct product $G_j = G_{j,i} \times G_{j,f}$.*

Proof. It is easy to see that $G_{j,i} \cap G_{j,f} = \{I\}$. Now we have to prove that any elements of $G_{j,i}$ commutes with every elements of $G_{j,f}$.

Let's assume that $g \in G_{j,i},\ v \in V_{j,f}$ and $g(v) = \sum_{k=1}^{L} a_k v_k$. Since the group is finite there is such m, that $g^m = I$. Now

$$v = g^m(v) = g^{m-1}(\sum_{k=1}^{L} a_k v_k) = \sum_{k=1}^{j} a_k v_k + g^{m-1}(\sum_{k=j+1}^{L} a_k v_k)$$

thus $a_k = 0,\ k = 1, ..., j$. This give us that if $g \in G_{j,i}$ and $v \in V_{j,f}$ then $g(v) \in V_{j,f}$. Similarly we get that if $g \in G_{j,f}$ and $v \in V_{j,i}$, then $g(v) \in V_{j,i}$. Now it is easy to see that $gg'(v_k) = g'g(v_k)$ for all $g \in G_{j,i},\ g' \in G_{j,f}$ and $k = 1, ..., L$. $\square$

For two different splitting points $j < j'$ we have the obvious subgroup inclusions $G_{j',i} \leq G_{j,i}$, $G_{j,f} \leq G_{j',f}$ and consequently $G_{j',i} \times G_{j,f} \leq G_j \cap G_{j'}$. The motivation to these definitions comes from the following observations. The decoder knows the channel state H and the generator matrix X. Hence decoder can compute the reference vector $\widetilde{\mathbf{r}} = HX$ that corresponds to the transmission of the identity element. The decoder can also compute the coordinates of $\widetilde{\mathbf{r}}$ with respect to our basis (normally we use the natural basis, so the coordinates are really the samples of the received signal, so there is nothing to compute here)

$$\widetilde{\mathbf{r}} = \sum_{i=1}^{L} \widetilde{r}_i v_i.$$

The coordinates of the vector

$$\widetilde{\mathbf{r}}g = \sum_{j=1}^{L} \widetilde{r}_j(g) v_j$$

can be computed as inner products

$$\begin{aligned}
\widetilde{r}_j(g) &= \langle v_j | \widetilde{\mathbf{r}}g \rangle \\
&= v_j (\widetilde{\mathbf{r}}g)^* \\
&= v_j g^* \widetilde{\mathbf{r}}^* \\
&= \langle v_j g^* | \widetilde{\mathbf{r}} \rangle \\
&\overset{g^*=g^{-1}}{=} \langle v_j g^{-1} | \widetilde{\mathbf{r}} \rangle.
\end{aligned}$$

Thus, if the inverses of two group elements g and g' map the basis vector v_j to the same vector, then the corresponding coordinates $\widetilde{r}_j(g)$ and $\widetilde{r}_j(g')$ are equal. In order to save computations we want to make as many decisions based on as few of the coordinates as possible. The key ideas we copy from the BCJR-trellis construction are that

1. two distinct group elements g and g' may correspond to the same initial sequence i.e. $\widetilde{r}_i(g) = \widetilde{r}_i(g')$ for all $i = 1, ..., j$, and that

2. two distinct initial sequences may have identical sets of possible futures $\widetilde{r}_{j+1}, ..., \widetilde{r}_L$.

Lemma 3.2. *The coordinate sequences corresponding to the two group elements have the same initial part, if and only if the group elements g and g' belong to the same left coset of the group $G_{j,i}$.*

Proof.

$$\begin{array}{llll}
 & v_i g^{-1} & = v_i g'^{-1} & \text{for all } i = 1, ..., j \\
\Leftrightarrow & v_i & = v_i g'^{-1} g & \text{for all } i = 1, ..., j \\
\Leftrightarrow & g'^{-1} g & \in G_{j,i} & \\
\Leftrightarrow & g & \in g' G_{j,i} &
\end{array}$$

□

Lemma 3.3. *The future parts of two coordinate sequences agree, iff the group elements lie in the same left coset of the group* $G_{j,f}$.

Proof.

$$\begin{array}{llll} & v_i g^{-1} & = v_i g'^{-1} & \text{for all } i = j+1, ..., L \\ \Leftrightarrow & v_i & = v_i g'^{-1} g & \text{for all } i = j+1, ..., L \\ \Leftrightarrow & g'^{-1} g & \in G_{j,f} & \\ \Leftrightarrow & g & \in g' G_{j,f} & \end{array}$$

□

Lemma 3.4. *Two coordinate sequences coincide in the range from* $j+1$ *to* j'*, whenever the two group elements are in the same left coset of the group* $G_{j',i} \times G_{j,f}$.

Proof.

$$\begin{array}{llll} & v_i g^{-1} & = v_i g'^{-1} & \text{for all } i = j+1, ..., j' \\ \Leftrightarrow & v_i & = v_i g'^{-1} g & \text{for all } i = j+1, ..., j' \\ \Leftrightarrow & g'^{-1} g & \in G_{j',i} \times G_{j,f} & \\ \Leftrightarrow & g & \in g'(G_{j',i} \times G_{j,f}) & \end{array}$$

□

Lemma 3.5. *If* $g, g' \in G$, $g \neq g'$ *and* $gG_j = g'G_j$ *then there is such* $g'' \in G$ *that* $g'' \in gG_{j,f} \cap g'G_{j,i}$.

Proof. If $g, g' \in G$, $g \neq g'$ and $gG_j = g'G_j$ then $g = g' g_{j,i} g_{j,f}$, where $g_{j,i} \in G_{j,i}$ and $g_{j,f} \in G_{j,f}$. Now

$$\begin{array}{lcll} g g_{j,f}^{-1}(v_k) & = & g' g_{j,i}(v_k) = g'(v_k), & k = 1, ..., j \\ & & \text{and} & \\ g g_{j,f}^{-1}(v_k) & = & g(v_k), & k = j+1, ..., L. \end{array}$$

Thus $g g_{j,f}^{-1} \in gG_{j,f} \cap g'G_{j,i}$. □

By lemmas 3.2, 3.3, 3.4 and 3.5 we can form our (time-varying) trellis as follows. We sectionalize the trellis by choosing an increasing sequence of splitting points $0 = j_0 < j_1 < \cdots < j_k = L$, so our trellis will have k sections. We identify the states at a splitting point j with the left cosets of G_j. The edges connecting state gG_j with the state $g'G_{j'}$ (here j and j' are two consecutive splitting points) are in a one-to-one correspondence with the cosets of $G_{j',i} \times G_{j,f}$ contained in the intersection $gG_j \cap g'G_{j'}$. By the above observations all the elements $h \in G$ within such a coset share the coordinate sequence in the range $\widetilde{r}_{j+1}(h), ..., \widetilde{r}_{j'}(h)$ allowing us to assign as the cost of this edge the squared Euclidean distance of this partial vector from the corresponding part of the received vector. So a group element g corresponds to the path going thru the states gG_j for all $j = j_0, ..., j_k$ consisting of the edges associated with the cosets $g(G_{j_{m+1},i} \times G_{j_m,f})$. Finally by lemma 3.5 there are one to one correspondence between the paths of trellis and the elements of G.

In order to minimize the state complexity of this group trellis we must look for an ordered basis that maximizes the size of the various groups G_j. In order to get significant savings we probably need to require that at the mid-point (j about $\frac{L}{2}$), both the initially trivial and the finally trivial subgroups should be non-trivial. This demand to an extent conflicts with the multiplicity criterion, as multiplicities at least j and $L-j$ then occur. Thus we must require that L is at least $2N_t$. In what follows we will concentrate on the simplest case $L = 2N_t$. In this case both the subgroups $G_{N_t,i}$ and $G_{N_t,f}$ must be fixed-point-free 2-groups, i.e. either cyclic or the generalized quaternion groups.

Example 3.1. Let $N_t = 2$, $N_r = 1$ and $L = 4$. Now $HX = (h_1, h_2)X = (\widetilde{r}_1, \widetilde{r}_2, \widetilde{r}_3, \widetilde{r}_4)$ and the group G is such that for any $g \in G$

$$\widetilde{\mathbf{r}}g = (\epsilon_{i(1)}\widetilde{r}_{i(1)}\epsilon_{i(2)}\widetilde{r}_{i(2)}\epsilon_{i(3)}\widetilde{r}_{i(3)}\epsilon_{i(4)}\widetilde{r}_{i(4)})$$

where

$$i \in D_4 = \langle (12), (13)(24) \rangle \leq S_4, \ \epsilon_i \in U \subseteq \mathbb{C}.$$

and

$$\epsilon_1\epsilon_2\epsilon_3\epsilon_4 \mathrm{sign}(i) = +1.$$

We will denote G by $P(U) \bullet D_4$.

If $U = \{1, -1\}$ (resp. $U = \{1, -1, i, -i\}$), then the number of elements in the group G is 64 (resp. 512).

Now we study the trellis representation of the group $P(\{1, -1\}) \bullet D_4$.

Let v_1, v_2, v_3, v_4 be natural basis of $\mathbb{C}^4$. Now (notations are like in the section 2.2)

$$
\begin{aligned}
G_{0,i} &= G \\
G_{0,f} &= \{1_G\} \\
G_{1,i} &= \{1_G, (1,2,4,-3), (1,2,-4,3), (1,2,-3,-4), (1,-2,-3,4), \\
&\quad (1,-2,3,-4), (1,-2,-4,-3), (1,-2,4,3)\} \\
G_{1,f} &= \{1_G\} \\
G_{2,i} &= \{1_G, (1,2,4,-3), (1,2,-4,3), (1,2,-3,-4)\} \\
G_{2,f} &= \{1_G, (-1,-2,3,4), (2,-1,3,4), (-2,1,3,4)\} \\
G_{3,i} &= \{1_G\} \\
G_{3,f} &= \{1_G, (-1,-2,3,4), (2,-1,3,4), (-2,1,3,4), (1,-2,-3,4), \\
&\quad (-1,2,-3,4), (2,1,-3,4), (-2,-1,-3,4)\} \\
G_{4,i} &= \{1_G\} \\
G_{4,f} &= G
\end{aligned}
$$

and thus groups

$$
\begin{aligned}
G_0 &= G \\
G_1 &= G_{1,i} \\
G_2 &= G_{2,i} \times G_{2,f} \\
G_3 &= G_{3,f} \\
G_4 &= G
\end{aligned}
$$

have orders $64, 8, 16, 8, 64$ respectively.

Because we identify the states at a splitting point j with the left cosets of G_j thus $P(C_2) \bullet D_4$ (resp. $P(C_4) \bullet D_4$) has state complexity profile $1, 8, 4, 8, 1$ (resp. $1, 16, 8, 16, 1$). Finally there are one to one correspondence between $g \in G$ and the path

$$G_0 \to gG_1 \to gG_2 \to gG_3 \to G_4.$$

$P(C_2) \bullet D_4$ has the edge complexity profile $8, 16, 16, 8$ (resp. $16, 32, 32, 16$).

If the received vector is

$$\mathbf{r} = (r_1, r_2, r_3, r_4)$$

then by using the knowledge of $\mathbf{r}$ and $HX = (\widetilde{r}_1, \widetilde{r}_2, \widetilde{r}_3, \widetilde{r}_4)$ the maximum likelihood decoder is able to find the minimum weight path from the next trellis.

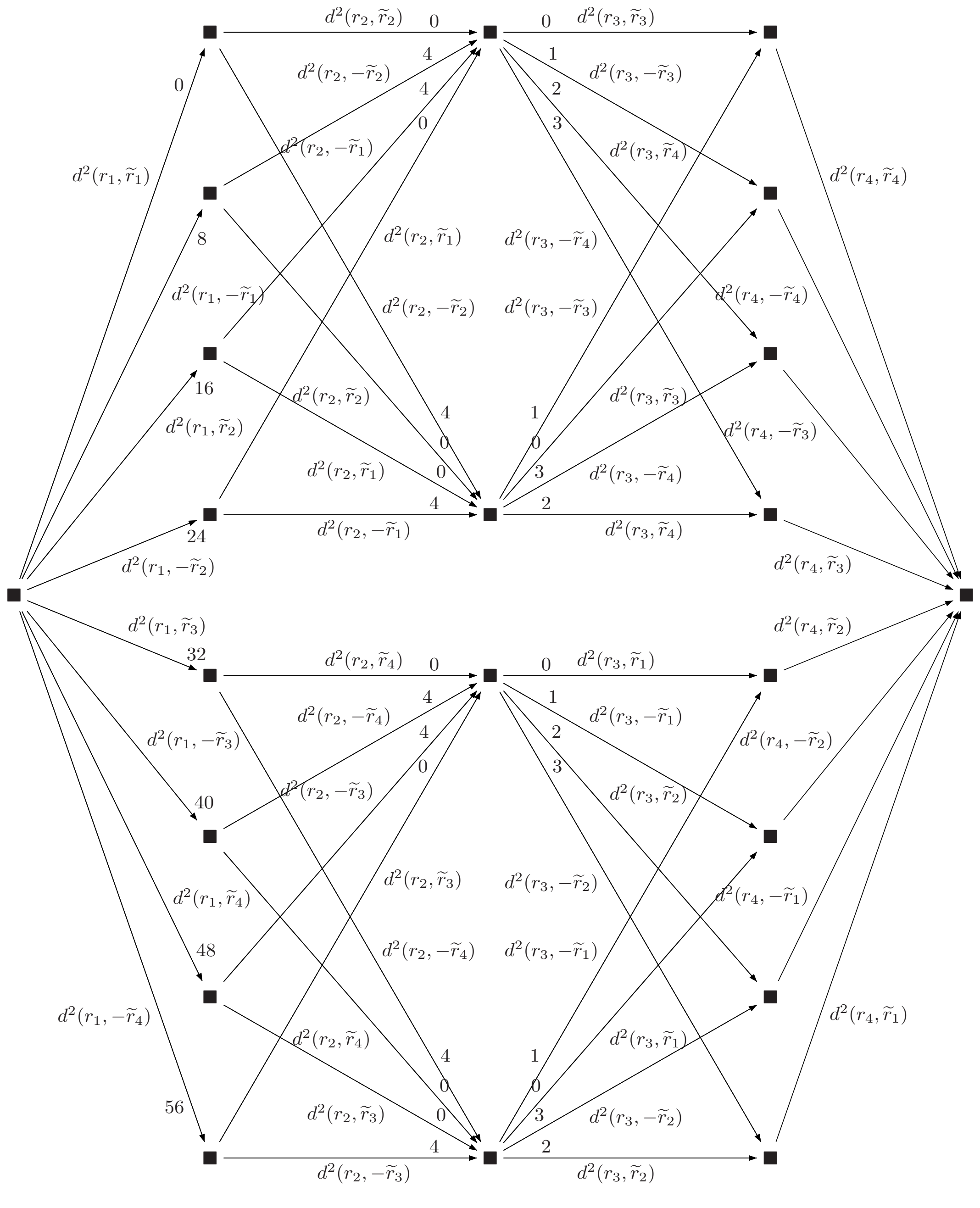

Figure 1: Trellis for the group $P(C_2) \bullet D_4$

4 Differential Space-Time Group Coding

When the receiver does not know the channel coefficients, one can communicate using differential space-time coding (see [12]). In the N_t-antenna (assume a single receiver antenna) differential space-time group coding we transmit an $N_t \times L$ matrix (in the paper [8] the assumption is that $N_t = L$) that is the product of the previously transmitted matrix and a unitary $L \times L$ data matrix taken from the group G. In other words, the transmitter sends the data sequence $g_{i_0}, g_{i_1}, ... \in G$ in the form

$$X_0 = Xg_{i_0},\ X_1 = X_0 g_{i_1}, ..., X_t = X_{t-1} g_{i_t}, ...,$$

where X is the $N_t \times L$ generator matrix. Now all the matrices $X_t,\ t = 0, 1, 2, ...$ belong to the finite set $\mathcal{C}(G, X) = \{Xg | g \in G\}$.

The receiver receives

$$\begin{aligned} \mathbf{r}_0 &= H_0 X_0 + \mathbf{n}_0, \mathbf{r}_1 = H_1 X_1 + \mathbf{n}_1 = H_1 X_0 g_{i_1} + \mathbf{n}_1, ..., \\ \mathbf{r}_t &= H_t X_t + \mathbf{n}_t = H_t X_{t-1} g_{i_t} + \mathbf{n}_t, ... \end{aligned}$$

where $H_t,\ t = 0, 1, 2, ...$ is a $1 \times N_t$ channel vector and $\mathbf{n}_t,\ t = 0, 1, 2, ...$ is a $1 \times L$ vector of additive independent $\mathcal{CN}(0, 1)$ noise.

Now we assume that the fading coefficients are approximately constant over $2L$ time samples ($H_t \approx H_{t-1}$) and thus

$$\begin{aligned} \mathbf{r}_t &= H_t X_t + \mathbf{n}_t \\ &= H_t X_{t-1} g_{i_t} + \mathbf{n}_t \\ &\approx H_{t-1} X_{t-1} g_{i_t} + \mathbf{n}_t \\ &= \mathbf{r}_{t-1} g_{i_t} + (\mathbf{n}_t - \mathbf{n}_{t-1} g_{i_t}) \\ &\underset{\mathbf{n}_t \sim \mathcal{CN}(0,1)^L}{\overset{-\mathbf{n}_{t-1} g_{i_t} \sim \mathcal{CN}(0,1)^L}{=}} \mathbf{r}_{t-1} g_{i_t} + \sqrt{2}\mathbf{n}'_t, \end{aligned}$$

where $\mathbf{n}'_t,\ t = 0, 1, 2, ...$ is a $1 \times L$ vector of additive independent $\mathcal{CN}(0, 1)$ noise.

As shown in [12], the maximum likelihood decoder has the simple structure

$$\hat{g}_{i_t} = \arg\min_{g \in G} \|\mathbf{r}_t - \mathbf{r}_{t-1} g\|. \tag{10}$$

It is easy to see that all the design criterion in the differential case are like in the case of typical space-time group codes (see the section 2). Moreover our trellis decoder of the space-time group coding (see the section 3) will work in the case of the differential space-time group coding, when we use as reference vector $\widetilde{\mathbf{r}}_t = \mathbf{r}_{t-1}$ (instead of $\widetilde{\mathbf{r}} = HX$).

5 Group Codes for Two Transmit Antennas

In this section we list some group codes with parameters $N_t = 2$ and $L = 4$. It turns out that in this case the best constellations are gotten by using the quaternion group of 8 elements as the starting point. This is explained by the close connection between the Alamouti scheme for QPSK alphabet and the group Q_8. Furthermore, there aren't any astonishing block codes of length 4, so not much can be expected from that construction. Indeed, the Alamouti scheme (together with simple coding) gives us constellations with very nice parameters (size vs. minimum product distance), and there is very little hope to find anything better.

Example 5.1. In this example the main point is to use the direct product $Q_8 \times Q_8$ of two generalized quaternion groups. Now we represent the elements of the group $Q_8 \times Q_8$ in the form

$$\begin{pmatrix} q_1 & 0 \\ 0 & q_2 \end{pmatrix},$$

where 2×2 blocks q_1 and q_2 are elements of the generalized quaternion group of 8 elements Q_8 (see the section 2.1). because the group Q_8 is fixed-point-free, we may simple choose

$$X = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$$

as our generator matrix. This give us the minimum product distance 2.

The trellis of the group $Q_8 \times Q_8$ has state complexity profile $1, 8, 1, 8, 1$ and edge complexity profile $8, 8, 8, 8$.

The group $Q_8 \times Q_8$ can be extended to a group $Q_8 \times Q_8 \bullet C_2$ of 128 elements very natural way by including matrices of the following form

$$\begin{pmatrix} 0 & q_1 \\ q_2 & 0 \end{pmatrix},$$

where again 2×2 blocks q_1 and q_2 are elements of Q_8. For this group the generator matrix

$$X = \begin{pmatrix} i & 1 & 1 & 1 \\ -i & 1 & i & -i \end{pmatrix}$$

surprisingly give us the minimum product distance 2.

The trellis of the group $Q_8 \times Q_8 \bullet C_2$ has state complexity profile $1, 16, 2, 16, 1$ and edge complexity profile $16, 16, 16, 16$.

Example 5.2. In this example the starting point is the Alamouti scheme. The first we consider the group code consisting of matrices of the form

$$\frac{1}{\sqrt{2}}\begin{pmatrix} c_1 & -c_2^* & c_3 & -c_4^* \\ c_2 & c_1^* & c_4 & c_3^* \end{pmatrix},$$

wherein the symbols c_i come from QPSK alphabet ($= \{s_0 = \frac{1+i}{\sqrt{2}}, s_1 = \frac{-1+i}{\sqrt{2}}, s_2 = \frac{-1-i}{\sqrt{2}}, s_3 = \frac{1-i}{\sqrt{2}}\}$). The size of code is 256 and the minimum product distance is 1.

ML-decoding is very simple: we use the Alamouti decoding for both Alamouti blocks separately.

Next we consider the group code (coded Alamouti) consisting of matrices of the form

$$\frac{1}{\sqrt{2}}\begin{pmatrix} c_1 & -c_2^* & c_3 & -c_4^* \\ c_2 & c_1^* & c_4 & c_3^* \end{pmatrix},$$

wherein the symbols c_i come from QPSK alphabet and the last symbol c_4 was used as an overall parity check symbol such that in the additive $\mathbb{Z}_4$-presentation of the QPSK-alphabet, the symbols of a code matrix add up to zero (modulo 4). This mean that $(c_1, c_2, c_3, c_4) = (s_{i_1}, s_{i_2}, s_{i_3}, s_{i_4})$, where $i_1 + i_2 + i_3 + i_4 \equiv 0 \pmod 4$. ML-decoding for this code can easily be achieved by using the Alamouti matched filter outputs $(\tilde{r}_1, \tilde{r}_2, \tilde{r}_3, \tilde{r}_4)$ for all the symbols in computing the weights for the $\mathbb{Z}_4$-linear BCJR trellis of the corresponding additive code (see the next page).

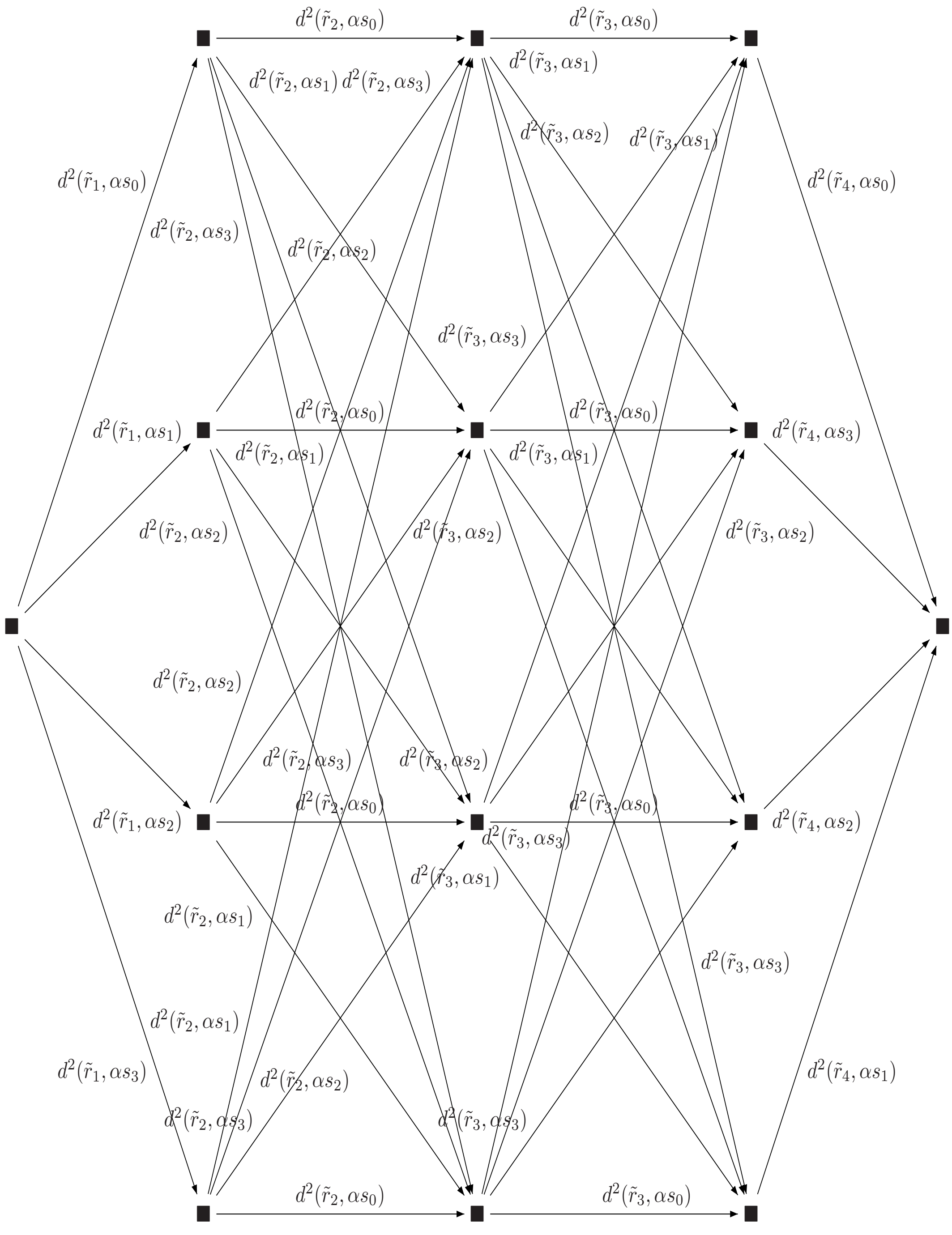

Figure 2: Trellis for the coded Alamouti. Note! $\alpha = |h_1|^2 + |h_2|^2$.

We see that the state complexity profile is $1, 4, 4, 4, 1$ and the edge complexity profile is $4, 16, 16, 4$.

5.1 Parameters of the Codes for 2 Transmit Antennas and Simulation Results

In the table below we see the most important parameters of the codes we have presented in this chapter.

group/ code	size	modulation alphabet	$pd_{\min}$
$P(C_2) \bullet D_4$	64	QPSK	$\sqrt{2}$
$P(C_4) \bullet D_4$	512	8-PSK	$\sqrt{6 - 4\sqrt{2}}$
$Q_8 \times Q_8$	64	QPSK	2
$Q_8 \times Q_8 \bullet C_2$	128	QPSK	2
Coded Alamouti	64	QPSK	2
2∗Alamouti	256	QPSK	1

The simulations were done in a Rayleigh fading channel. As only the block error rate (BLER) performance was studied, and the duration of a single block is 4 time units, the memory characteristics of the channel (e.g. dependence on receiver speed) were neglected. These showed that the group code $Q_8 \times Q_8$ and the coded Alamouti had identical block error rates (see the figure 3). This was hardly surprising in view of the fact that the two codes are more or less rearrangements of each other. As we had optimized the group $P(C_2) \bullet D_4$ with respect to its Euclidean distance distribution (rather than with respect to the product distance), it turned out to be the loser by about 1 dB (see the figure 4).

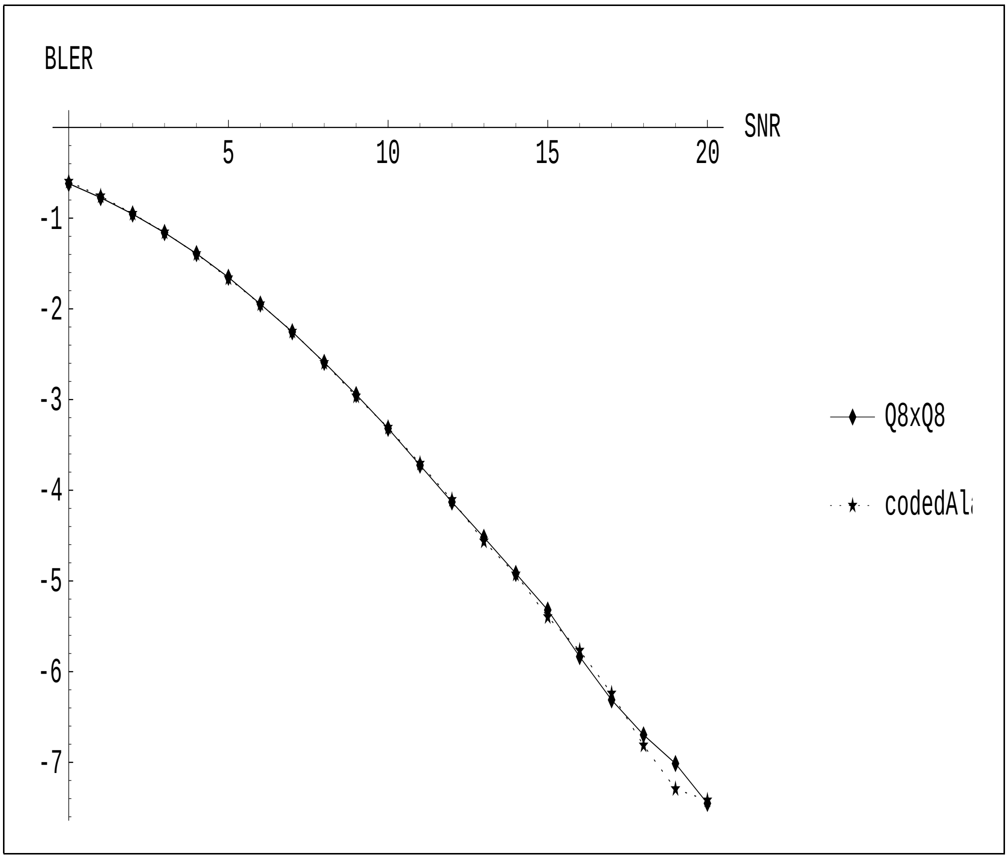

Figure 3: The BLER performance comparison between the coded Alamouti and the group code $Q_8 \times Q_8$ in the Rayleigh fading channel

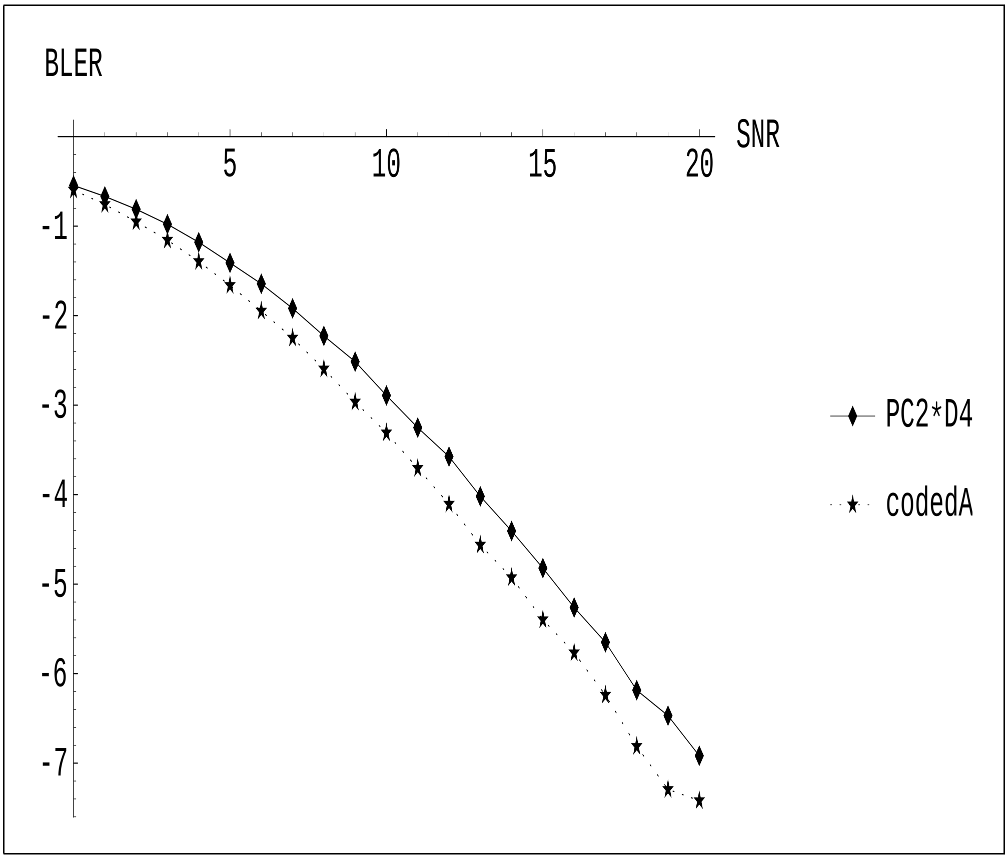

Figure 4: The BLER performance comparison between the coded Alamouti and the group code $P(C_2) \bullet D_4$ in the Rayleigh fading channel

6 Group Codes for Four Transmit Antennas

This time we concentrate on the case $k = 4$, $n = 8$. As there is no Alamouti scheme to compete against, there is some hope that we can find better codes. Instead we use the 4-antenna orthogonal design (see [3]) together with some coding as a reference point. Even though the 4-antenna design is very remarkable also, we now have more elbow room and the extra degrees of freedom in the group setting will enable us to find at least one better codes from the group side (see 6.2 below).

6.1 Groups Built by Extending Quaternion Groups

In our quest for 4-antenna codes we encountered 4-dimensional representations of quaternion groups: Namely the monomial matrices $\sigma = (2, -1, 4, -3)$ and $\tau = (3, -4, -1, 2)$ generate a group isomorphic to Q_8. Similarly the monomial matrices $\sigma = (2i, -3i, 4i, i)$ and $\tau = (-2, 1, 4, -3)$ generate a group isomorphic to the quaternion group Q_{16}. These 4-dimensional fixed-point-free representations are not irreducible, in fact they are direct sums of two 2-dimensional representations. However, they enable the use of roots of unity of a smaller order, which helps to reduce at least the group alphabet (and hopefully also the modulation alphabet) in size. We can now form the following groups of 8×8-matrices meeting the multiplicity criterion for diversity 4. First we get a group of 256 elements consisting of the matrices

$$\begin{pmatrix} q_1 & 0 \\ 0 & q_2 \end{pmatrix}$$

where the 4×4-blocks q_1 and q_2 are elements of the copy of the group Q_{16} described in the previous paragraph. Using a Walsh-Hadamard -like generator matrix

$$X = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \end{pmatrix}$$

results in a code with minimum product distance 4. As in the 2-antenna case we can double the size of this group by also allowing matrices of the form

$$\begin{pmatrix} 0 & q_1 \\ q_2 & 0 \end{pmatrix}.$$

Again we have been able to find a generator matrix for this group that results in a constellation of 512 matrices and minimum product distance 4. One such generator matrix (again normalized to unit column energy) is

$$X = \frac{1}{2}\begin{pmatrix} i & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & -1 & i & -1 & -1 & 1 & 1 \\ 1 & i & -1 & -1 & 1 & -1 & 1 & -1 \\ 1 & -1 & i & -1 & -1 & 1 & 1 & -1 \end{pmatrix}.$$

The reader immediately realizes that the rows of this matrix are not orthogonal. Thus we might improve this code by finding an orthogonal basis for the row space of X. This would result in a very awkward modulation alphabet.

6.2 Groups from Block Codes and Their Automorphisms

Here we split the study according to the group alphabet. In the case of a binary group alphabet and binary block codes, the extended Hamming $[8, 4, 4]$-code stands out as the candidate for the diagonal part of the group. In the interest of minimizing the trellis, we will write the positions in a Reed-Muller order, so the group C is generated by the following four matrices:

$$\begin{aligned} d_1 &= \operatorname{diag}(-1,-1,-1,-1,-1,-1,-1,-1), \\ d_2 &= \operatorname{diag}(1,1,1,1,-1,-1,-1,-1), \\ d_3 &= \operatorname{diag}(1,1,-1,-1,1,1,-1,-1), \\ d_4 &= \operatorname{diag}(1,-1,1,-1,1,-1,1,-1). \end{aligned}$$

All the affine transformations are automorphisms of this code. This group has several 2-Sylow subgroups, of which have chosen to concentrate on Σ, the one generated by the permutations $\sigma_1 = (12)(34)$, $\sigma_2 = (13)(24)$, $\sigma_3 = (15)(26)(37)(48)$, and $\sigma_4 = (12)(56)$. The group Σ has 64 elements. After some trial and error we found a crossed homomorphism f satisfying

$$\begin{aligned} f(\sigma_1) &= \operatorname{diag}(1,-1,1,-1,1,1,1,1) * C, \\ f(\sigma_2) &= \operatorname{diag}(1,-1,-1,1,1,1,1,1) * C, \\ f(\sigma_3) &= C, \\ f(\sigma_4) &= \operatorname{diag}(-1,1,1,1,-1,1,1,1) * C. \end{aligned}$$

and resulting in a group of 1024 elements satisfying the multiplicity criterion for diversity 4. Observe that the image of f consists of all the even weight cosets of the Hamming code. As all this fits together very nicely, I strongly suspect that this construction might be generalized to other cases. Using the notation from section 2.2 we see that our group $G1024$ is generated by a single diagonal matrix d_4 and the monomial matrices

$$\begin{aligned} g_1 &= (2,-1,4,-3,5,6,7,8), \\ g_2 &= (3,-4,-1,2,5,6,7,8), \\ g_3 &= (5,6,7,8,1,2,3,4), \\ g_4 &= (-2,1,3,4,-6,5,7,8). \end{aligned}$$

Here a further computation shows that the group generated by g_3 and g_4 is the finally trivial subgroup $G1024_{4,f}$. This group is actually isomorphic to Q_8 (see section 6.1). Conjugating this subgroup by g_3 gives then the initially trivial subgroup $G1024_{4,i}$. We denote the direct product of these two subgroups by $G_{4,4} = G1024_{4,i} \times G1024_{4,f}$. This is a normal subgroup of index 16 in the whole group $G1024$. Thus in a trellis representation of $G1024$ we have sixteen states at the midpoint. The earlier initially trivial subgroup $G1024_{2,i}$ contains all of $G1024_{4,i}$ and the product g_1g_4, so the order is equal to 32. As $G1024_{2,f}$ is obviously the trivial group, we see that our trellis representation of $G1024$ has 32 states at split point 2. Similarly the trellis has state complexity 32 also at the split point 6.

Altogether the trellis is divided into 4 parallel subtrellises (corresponding to a subgroup $G256$ of order 256 generated by $G_{4,4}$ and g_4 and its cosets). Each subtrellis has state complexity $(1,8,4,8,1)$ and edge complexity $(8,32,32,8)$, so the total edge complexity of the trellis 320. The complexity of the Viterbi algorithm on this trellis is further reduced by the fact at each section there are only 32 different labels on the edges, thus only the costs of 128 edges must be computed (and stored into an array indexed by the section number and the labels). The labels in each section correspond to two columns of the group matrices. Thus e.g. the path corresponding to the group element g_1 above consists of 4 edges labelled $(2,-1)$, $(4,-3)$, $(5,6)$ and $(7,8)$. The two components on any label are integers, have absolute values as in the example and all sign and order combinations appear. Thus the total number of labels is 32 and in the two center sections of the trellis each label appears exactly 4 times. It might be worthwhile to look for a tailbiting trellis representation for $G1024$ as well.

Finding a good generator matrix for a code gotten by using $G1024$ has proven to be quite difficult. To cut down search time we set up a search algorithm looking for such generator matrices that have orthogonal rows using 4-phase modulation alphabet (scaled to squared norm 1/4 so that the column energy is equal to one) and have the extra property that the rows of the generator matrix are gotten from each other by acting with an element of the group $G1024$. I cannot give a compelling reason as to why this would be a good strategy. This seemed to work, when looking for smaller codes, but her this was done simply to cut down search time. The best generator matrix

$$X = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & i & 1 & 1 & i & -1 \\ i & 1 & -1 & -1 & 1 & -i & 1 & 1 \\ 1 & i & -1 & 1 & -i & 1 & -1 & 1 \\ -1 & 1 & i & 1 & 1 & -1 & -1 & i \end{pmatrix}$$

results in a code with minimum product distance 4. Each point in the code has exactly 4 other points at this minimum product distance. There are several other generator matrices resulting in the same minimum product distance, but the others seem to have a worse distribution. This is also supported by the computer simulations.

For the purposes of trellis coded modulation it would be nice to find such a generator matrix X that the two halves of it would be unitary matrices. This is because, then the cosets of the subgroup $G_{4,4}$ would provide a very promising looking partition of this code. As the differences of matrices in $G_{4,4}$ have the equal singular value property, the minimum product distance within such a partition would be 16 allowing the possibility of good coding gain (a similar construction as in [11], but for four antennas, would become possible). The above generator X was selected using the subcode minimum product distance as a secondary criterion. However, as the two halves of X are not unitary, we do not quite achieve this - the minimum product distance within these subcodes turns out to be 9. I leave it as a challenge problem to find a generator matrix X with unitary halves and also achieving the over all minimum product distance 4.

A related constuction achieving full diversity with 4-phase group alphabet is to use the celebrated $Z4$-linear Nordstrom-Robinson code of 256 elements as the diagonal subgroup. Now the group C is generated by the following four matrices:

$$\begin{aligned} d_1 &= \mathrm{diag}(i, -i, i, i, -1, 1, 1, 1), \\ d_2 &= \mathrm{diag}(i, 1, -i, -1, i, 1, i, 1), \\ d_3 &= \mathrm{diag}(i, 1, 1, i, -i, 1, -1, i), \\ d_4 &= \mathrm{diag}(i, 1, 1, -i, 1, i, i, -1). \end{aligned}$$

Nordstrom-Robinson code has a group of 8 permutations (corresponding to translations in the 3-dimensional binary vector space) as a subgroup of its automorphisms. The group Σ of 8 permutations is generated by the permutations $\sigma_1 = (12)(34)(56)(78)$, $\sigma_2 = (13)(24)(57)(68)$, and $\sigma_3 = (15)(26)(37)(48)$. Each permutation ($\neq (1)$) in the group Σ consists of 4 disjoint 2-cycles. From this we get that the multiplicity of 1 as an eigenvalue of the matrix $d\sigma$ is at most 4, when $\sigma \in \Sigma \setminus \{\neq (1)\}$ and $d\ inC$. We know that the Hamming weight of any non-zero word in the Nordstrom-Robinson code is at least 4 and thus the multiplicity of 1 as an eigenvalue of the matrix d, $d \in C$ is at most 4. Now it immediately follows that the semidirect product $\Sigma \ltimes C$ meets the multiplicity criterion. Thus we get a group of order 2048. However, the trellis complexity of this group blows up to 512 at the midpoint, so we haven't really looked for good generator matrices, as the complexity of ML-decoding is pretty bad at this stage of research.

6.3 Parameters of the Codes for Four Transmit Antennas

In the table below we have collected the properties of some of the group codes from above. All these are designed for four transmit antennas and a symbol duration of 8 time units. The coded orthogonal design that is used as a reference point in our simulations is gotten by using two blocks of the 4-antenna design as follows:

$$\begin{pmatrix} c_1 & c_2 & c_3 & 0 & c_4 & c_5 & c_6 & 0 \\ -c_2^* & c_1^* & 0 & c_3 & -c_5^* & c_4^* & 0 & c_6 \\ c_3^* & 0 & -c_1^* & c_2 & c_6^* & 0 & -c_4^* & c_5 \\ 0 & c_3^* & -c_2^* & -c_1 & 0 & c_6^* & -c_5^* & -c_4 \end{pmatrix}$$

Here the 6 QPSK symbols should be scaled to squared norm $= 1/3$, so that the column energy is normalized to unity. The constellation size was cut down to 1024 by using as an overall parity check symbol (so that in the Z4-presentation the symbols sum up to zero). Thus this constellation can be ML-decoded using a trellis with 6 section with state complexity $(1, 4, 4, 4, 4, 4, 1)$ and edge complexity $(4, 16, 16, 16, 16, 4)$ using the penalties provided by the mathced filter detector as weights. This simple coding also enhances the minimum product distance of the resulting constellation, as now the allowed symbol sequences have minimum Hamming distance 2.

group/ code	size	group alphabet	modulation alphabet	$pd_{\min}$
$Q_{16} \times Q_{16}$	256	quaternary	QPSK	4
$Q_{16} \times Q_{16} \bullet C_2$	512	quaternary	QPSK	4
$G1024$	1024	binary	QPSK	4
$G_{4,4}$	64	binary	QPSK	16
Coded Orth. Des.	1024		QPSK	256/81

6.4 Simulation results

The following simulation were done using a complex Rayleigh fading channel model. The channel state was assumed to be constant and known during the transmission of a single symbol. As only the code performances were compared (no coding), a memoryless channel model was sufficient. We see that at SNR 0 dB, the group code has an advantage of about 0.5 dB. As the SNR grows, this advantage gradually disappears and when SNR exceeds 14 dB, the performance of the two codes is within the margin of error. Both codes have full diversity, but the product distance properties of the group code are slightly better, this was to be expected. But it is nevertheless somewhat surprising (to me) that the group code couldn't maintain its edge. A possible explanation is that the product distance properties of the two codes are so close to each other that no difference will show in the high SNR range. However, as the group code doesn't have the equal singular value property [9], lower degree symmetric polynomials of the singular values (e.g. the trace distance distribution that also plays a role) help the group code in the low range. Nevertheless, it seems that the minimum product distance alone doesn't determine the performance for high SNR. Namely an earlier simulation using a different generator matrix achieving the same minimum product distance (but worse product distance distribution) actually started to lose to this orthogonal code (with a worse minimum product distance) in the range SNR $>$ 12 dB. The difference in the complexity of the trellis presentations of the two codes showed in the simulations in that the group simulations required about $2-3$ times more time.

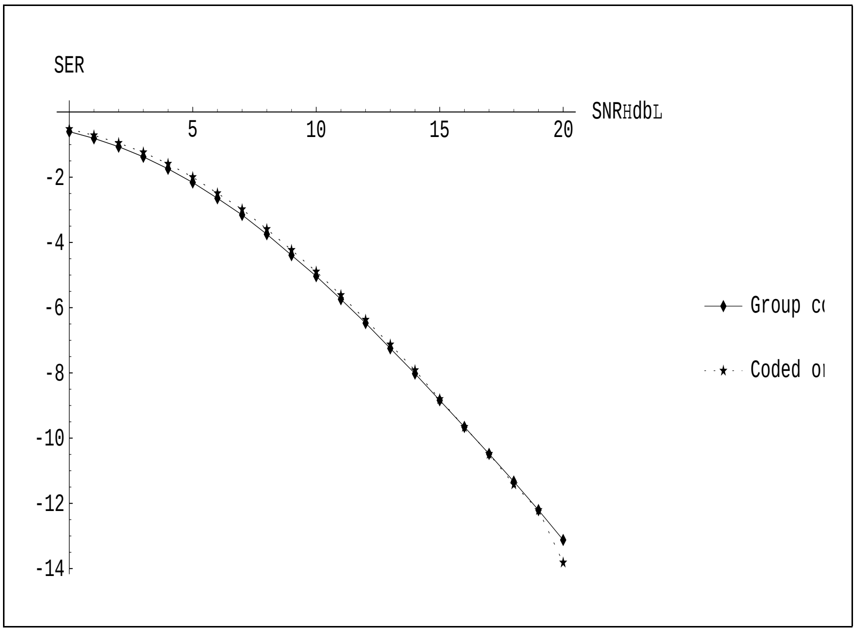

Figure 5: The error probability performance comparison between group constellation and coded orthogonal design in Rayleigh fading channel with QPSK-modulation

References

[1] Hiltunen, J., and Lahtonen, J. (2002). *Space-Time Lattice Codes from Algebraic Number Fields.* Technical Report 489, TUCS, 2002.

[2] Tarokh, V., Seshadri, N., and Calderbank, A. R. (1998). *Space-Time Codes for High Data Rate Wireless Communications: Performance Criterion and Code Construction.* IEEE Transactions on Information Theory, Vol. 44, No. 2, March 1998, pp. 744-765.

[3] Tarokh, V., Jafarkhani, H., and Calderbank, A. R. (1999). *Space-Time Block Codes from Orthogonal Designs.* IEEE Transactions on Information Theory, Vol. 45, No. 5, July 1999, pp. 1456-1467.

[4] Proakis, J. G., (1995). *Digital Communication.* McGraw-Hill.

[5] Metsänkylä, T., (1996). *Matriisilaskenta*, Lecture Note, Turun Yliopisto.

[6] Metsänkylä, T., (1996). *Ryhmäteoria*, Lecture Note, Turun Yliopisto.

[7] Slepian, D., (1968). *Group codes for the Gaussian channel.* Bell Syst. Tech. J., Vol. 47, pp. 575-602, Apr.1968.

[8] Hassibi, B., Hochwald, B. M., Shokrollahi, and A., Sweldens, W.. *Representation Theory for High-rate Multiple-Antenna Code Design.* IEEE Transactions on Information Theory, Vol. 47, No. 6, Sebtember 2001.

[9] Ionescu, D. M.. *New Results on Space-Time Code Design Criteria.*

[10] McEliece, R. J.. *On the BCJR Trellis for Linear Block Codes.* IEEE Transactions on Information Theory, Vol. 42, No. 4,5 July 1996.

[11] Ionescu, D. M., Mukkavilli, K. K., Yan, Z., and Lilleberg, J.. *Improved 8- and 16-State ST Codes for 4PSK with Two Transmit Antennas.* IEEE Communications Letters, vol. 5(7), July 2001.

[12] B. Hochwald, and W. Sweldens. *Differential Unitary Space-Time Modulation.* Tech. rep., Bell Laboratories, Lucent Technologies, Mar. 1999.

Turku Centre for Computer Science
Lemminkäisenkatu 14
FIN-20520 Turku
Finland

http://www.tucs.fi

University of Turku
- **Department of Information Technology**
- **Department of Mathematics**

Åbo Akademi University
- **Department of Computer Science**
- **Institute for Advanced Management Systems Research**

Turku School of Economics and Business Administration
- **Institute of Information Systems Science**