Computing the Performance of Unitary Space-Time Group Constellations from their Character Table

Amin Shokrollahi

Bell Laboratories, Room 2C-381, Lucent Technologies
600 Mountain Avenue, Murray Hill, NJ 07974
amin@research.bell-labs.com

June 14, 2000

Abstract

Multiple antennas can greatly increase the data rate and reliability of a wireless communication link in a fading environment. It is well-known that unitary matrices can be used to design differentially modulated space-time constellations. These constellations have a particularly efficient description if they form a finite group under matrix multiplication. In this paper we will show how to compute parameters of such groups crucial for their use as space-time constellations, using only the character table of the group. Since character tables for many groups are known and tabulated, this method could be used to quickly test, for a given group, which of its irreducible representations can be used to design good unitary space-time constellations. We demonstrate our method by computing the eigenvalues of all the irreducible representations of the special linear group $\mathrm{SL}_2(\mathbb{F}_q)$ over a finite prime field $\mathbb{F}_q$ of odd characteristic, and study in detail the performance of a particular 8-dimensional representation of $\mathrm{SL}_2(\mathbb{F}_{17})$.

1 Introduction

Multiple-antenna wireless communication links promise very high data rates with low error probabilities, especially when the channel is known at the receiver [2, 3]. But the design of so-called space-time codes that achieve these promises is still in its infancy. In [4] some trellis-based codes for known channels are developed. However, the assumption that the channel is known is questionable in a rapidly changing mobile environment, or when many transmitter antennas are employed, since this requires extensive training. In [5, 6], some information-theoretic and signal constellation

design issues are considered for channels that are known neither to the transmitter nor the receiver. In particular, a class of signals called *unitary space-time signals* is developed where the transmitted signal matrices that form a constellation are all unitary. Further justification for using unitary space-time signals is given in [7], where it is shown that these signals can form their own channel code and achieve arbitrary reliability over a single fading coherence interval with a large number of transmitter antennas.

In this paper, a unitary space time constellation is a collection of unitary $M \times M$-matrices. The transmission model is the following: within each coherence interval a matrix is transmitted by sending its (i, j)-entry over the jth channel at the ith time step within the coherence interval. The decoding of the received signals is performed by computing the most likely matrix in the constellation from the received matrix. The probability of mistaking a signal V with a signal W in the constellation for this Maximum Likelihood Decoder has been bounded from above by an expression involving the eigenvalues of the difference $V - W$. (See [4] for the known channel and [6] for the unknown channel case, and also Section 2.) The constellation is said to be *fully diverse* if all these eigenvalues are nonzero for all matrices V, W in the constellation, $V \neq W$. In that case, the formulas for the pairwise error probability suggest that, for high signal to noise ratio, a constellation $\mathcal{V}_1$ is superior to another one $\mathcal{V}_2$ if the minimum of $|\det(V - W)|$ for V and W ranging over pairwise distinct elements in $\mathcal{V}_1$ is larger than the same expression for $\mathcal{V}_2$. Although fully diverse constellations are generally preferable, the formulas for the error probability suggest that the performance of a not fully diverse constellation could still be reasonably good if there are only a few pairs V, W for which $V - W$ has zero eigenvalues, and if for such pairs $V - W$ has high rank.

In this paper we will concentrate on constellations which form a group under matrix multiplication. There are many advantages to having a constellation with a group structure: in the differential setting [8], one has to multiply the matrices in the constellation, and this can be greatly simplified by using a multiplication table for the group, rather than actual multiplication (which could lead to additional computational noise); further, through their high symmetry, constellations from groups can be decoded more efficiently than non-structured constellations. In [1] all fully diverse group constellations were completely classified. Although they have excellent performance, group constellations are few and far between. Hence, given a target constellation size, one may have to look elsewhere for obtaining a good design.

In this paper, we will introduce computational methods to study the performance of general

groups. More precisely, given a finite group G and its *character table*, our procedure is able to quickly compute, for any irreducible representation Δ of G, an upper bound for the pairwise error probability of the maximum likelihood decoder for the constellation $\Delta(G)$. Given the character table and some additional data on the group, our algorithm runs in time $O(hd^2)$ where h is the number of *conjugacy classes* of the group and d is the degree of the representation in question. For non-abelian groups, the class number h can be much less than the size of the group, and hence, lead to substantial savings in the running time. Using fast algorithms, the running time can be further reduced to $O(hd\log(d))$, but we will not emphasize this aspect in this paper, since for practical purposes d is typically small.

How can our methods be used? Character tables for various classes of finite groups are widely accessible, while irreducible representations are not (and are typically more elaborate to compute). Using the methods of this paper, one can identify those groups and those irreducible representations thereof for which the corresponding constellation promises to have good performance, based on the upper bound of the pairwise error probability. Once these groups are identified, one can compute the representations, and hence the constellations. The method is demonstrated for the group $\mathrm{SL}_2(\mathbb{F}_5)$. In [1] it was shown that this group has a fixed-point-free 2-dimensional representation; this means that the image of that representation is a fully diverse constellation. In our example, we will discuss all the irreducible representations of $\mathrm{SL}_2(\mathbb{F}_5)$ and study their properties for use as space-time constellations. Since the groups $\mathrm{SL}_2(\mathbb{F}_q)$ for odd prime q seem very promising, we will elaborate on all these groups and obtain explicit data with which we can compute upper bounds for the pairwise error probability of corresponding constellations. It turns out that, for prime $q < 20$, the most promising groups are those for the values $q = 3, 5, 17$. Here, "promising" means that these groups have representations which only have a small number of eigenvalues 1. The cases $\mathrm{SL}_2(\mathbb{F}_3)$ and $\mathrm{SL}_2(\mathbb{F}_5)$ were already considered in [1]. We therefore study in detail an 8-dimensional irreducible representation of $\mathrm{SL}_2(\mathbb{F}_{17})$ and obtain explicit formulas for the average pairwise error probabilities of the corresponding constellation.

2 Multiple antenna space-time modulation

2.1 The Rayleigh flat fading channel

Consider a communication link with M transmitter antennas and N receiver antennas operating in a Rayleigh flat-fading environment. The nth receiver antenna responds to the symbol sent on the

mth transmitter antenna through statistically independent multiplicative complex-Gaussian fading coefficients h_{mn}. The received signal at the nth antenna is corrupted at time t by additive complex-Gaussian noise w_{tn} that is statistically independent among the receiver antennas and also independent from one symbol to the next. We assume that time is discrete, $t = 0, 1, \ldots$.

It is convenient to group the symbols transmitted over the M antennas in blocks of M channel uses. We use $\tau = 0, 1, \ldots$ to index these blocks; within the τth block, $t = \tau M, \ldots, \tau M + M - 1$. The transmitted signal is written as an $M \times M$ matrix S_τ whose mth column contains the symbols transmitted on the mth antenna as a function of time; equivalently, the rows contain the symbols transmitted on the M antennas at any given time. The fading coefficients h_{mn} are assumed to be constant over these M channel uses.

Similarly, the received signals are organized in $M \times N$ matrices X_τ. Since we have assumed that the fading coefficients are constant within the block of M symbols, the action of the channel is given by the simple matrix equation

$$X_\tau = \sqrt{\rho}\, S_\tau\, H_\tau + W_\tau \quad \text{for} \quad \tau = 0, 1, \ldots. \tag{1}$$

Here $H_\tau = (h_{mn})$ and $W_\tau = (w_{tn})$ are $M \times N$ matrices of independent $\mathcal{CN}(0, 1)$-distributed random variables. Because of the power normalization, ρ is the expected SNR at each receiver antenna.

2.2 Known Channel Modulation

We first discuss the case where the receiver knows the channel H_τ. We assume that the data to be transmitted is a sequence $z_0, z_1, \ldots$ with $z_\tau \in \{0, \ldots, L-1\}$. The data dictates which matrix is transmitted, via $S_\tau = V_{z_\tau}$. Each transmitted matrix occupies M time samples of the channel, implying that transmitting at a rate of R bits per channel use requires a constellation $\mathcal{V} = \{V_1, \ldots, V_L\}$ of $L = 2^{RM}$ unitary signal matrices.

The quality of a constellation $\mathcal{V}$ is determined by the probability of error of mistaking one symbol of $\mathcal{V}$ for another, using the Maximum Likelihood Decoding. In [4, 6] it is shown that pairwise probability of mistaking V_ℓ for $V_{\ell'}$ with a known channel is given by

$$P_{V_\ell, V_{\ell'}} \leqslant \frac{1}{2} \prod_{m=1}^{M} \left[1 + \frac{\rho}{4}\sigma_m^2(V_\ell - V_{\ell'})\right]^{-N},$$

where $\sigma_m(V_\ell - V_{\ell'})$ is the mth singular value of the $M \times M$ matrix $V_\ell - V_{\ell'}$ (in some ordering).

2.3 Differential Modulation

When the receiver does not know the channel, one can communicate using multiple-antenna differential modulation [8]. Here, we transmit an $M \times M$ unitary matrix that is the product of the previously transmitted matrix and a unitary data matrix taken from the constellation. In other words, $S_\tau = V_{z_\tau} S_{\tau-1}$ for $\tau = 1, 2, \ldots$, with $S_0 = I_M$. In [8] the pairwise probability of error under the Maximum Likelihood Decoding was shown to satisfy

$$P_{\mathcal{V}_\ell, V_{\ell'}} \leqslant \frac{1}{2} \prod_{m=1}^{M} \left[1 + \frac{\rho^2}{4(1+2\rho)} \sigma_m^2 (V_\ell - V_{\ell'}) \right]^{-N}.$$

At high SNR, both bounds above depend primarily on the product of the nonzero singular values of $V_\ell - V_{\ell'}$. Let $\mathrm{Sing}^*(A)$ denote the (multi-)set of nonzero singular values of the matrix A, counted with multiplicities. The size of $\mathrm{Sing}^*(A)$ is thus equal to the rank $\mathrm{rk}(A)$ of A, if A is a square matrix. Then, for high SNR we may write

$$P_{V_\ell, V_{\ell'}} \leq \frac{1}{2} \left(\frac{\alpha}{\rho} \right)^{N \mathrm{rk}(V_\ell - V_{\ell'})} \cdot \prod_{\lambda \in \mathrm{Sing}^*(V_\ell - V_{\ell'})} \lambda^{-2N}, \tag{2}$$

where in the known channel case, $\alpha = 4$ and in the unknown channel case $\alpha = 8$, and the inequality is to be understood in an asymptotic sense. This expression can be related to the characteristic polynomial of $V_{\ell'} V_\ell^*$.

Lemma 1. *Let $T(x)$ be the characteristic polynomial of $V_{\ell'} V_\ell^*$, and suppose that $T(x) = (x-1)^k \tilde{T}(x)$ for some $k \geq 0$ such that $\tilde{T}(1) \neq 0$. Then we have for large SNR ρ*

$$P_{V_\ell, V_{\ell'}} \leq \frac{1}{2} \left(\frac{\alpha}{\rho} \right)^{N \deg(\tilde{T}(x))} \cdot |\tilde{T}(1)|^{-2N}.$$

Proof. First, note that in expression (2), we can replace $V_\ell - V_{\ell'}$ by $I_M - V_{\ell'} V_\ell^*$. Let A denote the matrix $V_{\ell'} V_\ell^*$. λ is a nonzero singular value of $I_M - A$ if and only if λ^2 is $|\omega|^2$ for some eigenvalue ω of A which is not equal to 1. Hence,

$$\prod_{\lambda \in \mathrm{Sing}^*(V_\ell - V_{\ell'})} \lambda^{-2N} = \prod_{\omega \in \mathrm{Spec}'(A)} |1 - \omega|^{-2N},$$

where $\mathrm{Spec}'(A)$ if the set of eigenvalues of A unequal to 1, counted with multiplicities. It is easy to see that the latter product is $|\tilde{T}(1)|^{-2N}$. □

A constellation $\mathcal{V}$ is called *fully diverse* if for any two matrices V_ℓ and $V_{\ell'}$ the difference $V_\ell - V_{\ell'}$ has full rank. For such a constellation, the *diversity product* was defined in [1] to be

$$\zeta_{\mathcal{V}} = \frac{1}{2} \min_{0 \leqslant \ell < \ell' < L} |\det (V_\ell - V_{\ell'})|^{1/M}. \tag{3}$$

If the constellation forms a group, then, as above, we can rewrite the diversity product in the form

$$\zeta_{\mathcal{V}} = \frac{1}{2} \min_{A \neq I} |T_A(1)|,$$

where $T_A(x)$ is the characteristic polynomial of the matrix A. The diversity product measures the quality of $\mathcal{V}$ if it is nonzero, and says little if it is zero. In the latter case, one can use the formula in the previous lemma to compute pairwise error probabilities for a given SNR ρ.

If $\mathcal{V}$ forms a group, then for any V and W in V the matrix VW^* is also in V, and an upper bound on $P_{V,W}$ can be computed from the characteristic polynomial of the various group elements. We will show in Section 4 how to do this efficiently. For that we will need some results on the representation theory of groups which will be recalled in the next section.

3 A few facts from representation and character theory

Following the approach in [1], we will view the group constellation $\mathcal{V}$ as the image of an abstract group under a unitary representation. Recall that a unitary representation of degree M of a finite group G is a homomorphism of G into the group $U_M(\mathbb{C})$ of unitary $M \times M$-matrices. Two representations Δ and Δ' are called *equivalent* if there is a unitary matrix T such that $\Delta(g) = T\Delta'(g)T^*$ for all elements g of G. The direct sum of two representations Δ and Δ' is the representation $\Delta \oplus \Delta'$ whose value at a group element g is the block diagonal matrix having the block diagonal entries $\Delta(g)$ and $\Delta'(g)$. A representation is called *irreducible* if it is not equivalent to a direct sum of two representations.

Any finite group has, up to equivalence, a finite number of irreducible representations. The number of such representations is equal to the *class number* h of G, which we will explain in the following. Two elements g and g' of G are called *conjugate* if there is an element s of G such that $g' = sgs^{-1} =: g^s$. For any element g in G, the *conjugacy class* of g, denoted by $[g]$, is the set of all

elements in G conjugate to G. The class number of G is the number of conjugacy classes of G; we usually denote the class number by h, and the conjugacy classes by $C_1, \ldots, C_h$.

The *character* of a representation Δ is the mapping χ from the group to $\mathbb{C}$ such that $\chi(g)$ equals the trace of $\Delta(g)$, for any group element $g \in G$. Since the trace of a matrix is unaffected by conjugation, a character is a *class function*, i.e., its value is constant on conjugacy classes. As a result, two equivalent representations have the same character. A representation whose character equals a given character χ is called a representation *affording* χ. Of course, two equivalent representations afford the same character, hence there are, in general, infinitely many representations affording a character χ.

We call a character *irreducible* if its corresponding representation is irreducible. The *degree of a character* is the degree of its corresponding representation. Much of the information on the irreducible representations is contained in the *character table* of G: the character table is an $h \times h$-matrix whose rows are indexed by the irreducible characters, and whose columns are indexed by the conjugacy classes of G. The entry (i, j) of this matrix is the value of the ith irreducible character on the jth conjugacy class. One of the many informations the character table contains is information on the degrees of the irreducible representations: let C_1 be the conjugacy class of the identity element of G (which consists of the identity element only), and let χ be a character of G. Then $\chi(C_1)$ is the degree of χ. Indeed, let Δ be a representation affording χ. Then Δ evaluated at the identity element of G is the identity matrix I_M of dimension M, the degree of Δ. Hence, the character χ of Δ evaluated at C_1 has value M, the trace of I_M.

In the next section we will show that we can compute the eigenvalues of a representation of G if we know the values of its character on the conjugacy classes of G, and if we know, for every j and k, which class corresponds to C_j^k. Here, we define C_j^k to be the class generated by the kth power of any generator of C_j. The map $\pi\colon \{1, \ldots, h\}^2 \to \{1, \ldots, h\}$ defined as

$$C_j^k =: C_{\pi(j,k)},$$

is called the *power-map function of* G. In general, the values of this function cannot be obtained from the character table of the group and requires computations in the group.

4 Obtaining information from the character table

Let G be a finite group, $C_1, \ldots, C_h$ be the conjugacy classes of G, and $\chi_1, \ldots, \chi_h$ be its irreducible characters. By $\Delta_1, \ldots, \Delta_h$ we denote irreducible representations of G affording the characters $\chi_1, \ldots, \chi_h$, respectively. We would like to study the quality of the constellation $\Delta_i(G)$ when used in a multiple antenna flat Rayleigh fading channel. Lemma 1 shows that, for computing the pairwise error probability of mistaking two elements of the group, we need to find the characteristic polynomials of the matrices $\Delta_i(g)$ for all the elements $g \in G$.

In many situations, the representations Δ_i are not known, and are generally hard to compute, while the character table of G is known. In such cases, it would be convenient to have a procedure to compute an upper bound on the pairwise probability of error without computing the representation (and hence the signal constellation) itself. If it turns out that the error probability is reasonably low, then one would invest the effort into actually computing the representation. Our aim in this section is to devise such a method, i.e., a procedure to compute the quality of a representation based on the knowledge of its character table and certain other invariants of the group.

Suppose that A is a $d \times d$-matrix over $\mathbb{C}$, with eigenvalues $\omega_1, \ldots, \omega_d$. Further, suppose that we know the power-sums $s_i := \omega_1^i + \cdots + \omega_d^i$, for $i = 1, \ldots, d$. Then we can recover the characteristic polynomial $T_A(x)$ of A in the following manner: we know that $T_A(x) = x^d - \sigma_1 x^{d-1} + \cdots + (-1)^d \sigma_d$, where σ_i is the ith elementary symmetric polynomial evaluated at $(\omega_1, \ldots, \omega_d)$. Let $f_A(x)$ be the reciprocal polynomial of $T_A(x)$, i.e.,

$$f_A(x) = (-1)^d \sigma_d x^d + (-1)^{d-1} \sigma_{d-1} x^{d-1} + \cdots - \sigma_1 x + 1 =: \tau_d x^d + \cdots + \tau_1 x + 1.$$

To recover the τ_i, and hence the σ_i from the s_i, we use the *Newton relations*, given as

$$f_A(x) \left(s_1 + s_2 x + \cdots + s_d x^{d-1} \right) \equiv -\frac{\mathrm{d} f_A}{\mathrm{d} x} \bmod x^d,$$

see, e.g. [9, Th. 2.24, pp. 46].

The above equation represents a system of linear equations for the unknown values $\sigma_1, \ldots, \sigma_d$ in terms of the known values $s_1, \ldots, s_d$. (Note that actually the value of σ_1 is known, since it is equal to s_1. For simplicity, we will ignore this fact in our presentation.) The explicit description of this

system is as follows:

$$\begin{pmatrix} 1 & 0 & 0 & \cdots & 0 & 0 \\ s_1 & 2 & 0 & \cdots & 0 & 0 \\ s_2 & s_1 & 3 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ s_{d-1} & s_{d-2} & s_{d-3} & \cdots & s_1 & d \end{pmatrix} \begin{pmatrix} \tau_1 \\ \tau_2 \\ \tau_3 \\ \vdots \\ \tau_d \end{pmatrix} = - \begin{pmatrix} s_1 \\ s_2 \\ s_3 \\ \vdots \\ s_d \end{pmatrix}, \tag{4}$$

where, as above, $\tau_i = (-1)^i \sigma_i$. Note that the above system is uniquely solvable, as the defining matrix has nonzero determinant. We note in passing that, since the matrix defining the system of equations is Toeplitz, we can actually solve the system with $O(d \log d)$ operations (rather than the naive $O(d^2)$), see, e.g., [10, Chap. 2, Problem 5.3], or [9, Cor. 2.23].

Now, let $A := \Delta_i(x_j)$. Then $s_1, \ldots, s_{d_j}$ equal $\chi_i(x_j), \chi_i(x_j^2), \ldots, \chi_i(x_j^{d_j})$, respectively. Hence, if we know, for all k and j, which class equals C_j^k, i.e., if we know the power-map function π, then we can look up the values $s_k = \chi_j(C_{\pi(j,k)})$ from the character table of G, and solve the system of equations (4). The computation of the characteristic polynomials would take $O(hd^2)$ operations.

The function π depends of course on the underlying group, and, in general, cannot be obtained from the character table alone. In the following, we will give some examples of using our method for some specific groups and representations.

5 The group $\mathrm{SL}_2(\mathbb{F}_5)$

The group $\mathrm{SL}_2(\mathbb{F}_5)$ is defined as the group of all 2×2-matrices over the field $\mathbb{F}_5$ with determinant 1. It has nine conjugacy classes $A, B, C_1, D_1, D_2, E_1, E_{-1}, F_1, F_{-1}$ described as follows:

$$A = \left[\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right], \quad B = \left[\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right], \quad C_1 = \left[\begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix} \right]$$

$$D_1 = \left[\begin{pmatrix} \theta & 0 \\ 0 & \theta^{-1} \end{pmatrix} \right], \quad D_2 = \left[\begin{pmatrix} \theta^2 & 0 \\ 0 & \theta^{-2} \end{pmatrix} \right], \quad E_1 = \left[\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right],$$

$$E_{-1} = \left[\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \right], \quad F_1 = \left[\begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix} \right], \quad F_{-1} = \left[\begin{pmatrix} -1 & 2 \\ 0 & -1 \end{pmatrix} \right],$$

where θ is a primitive 6th root of unity in $\mathbb{F}_{25}$. Note that the generators of D_1 and D_2 do not belong to $\mathrm{SL}_2(\mathbb{F}_5)$. However, they are conjugate to the matrices

$$\begin{pmatrix} 0 & -1 \\ 1 & \theta^i + \theta^{-i} \end{pmatrix}, i = 1, 2$$

which does belong to $\mathrm{SL}_2(\mathbb{F}_5)$.

The following table describes the power-map function; the ith entry in the row corresponding to the class C is the class C^i.

	1	2	3	4	5	6
A	A	A	A	A	A	A
B	B	A	B	A	B	A
C_1	C_1	B	C_1	A	C_1	B
D_1	D_1	D_2	B	D_2	D_1	A
D_2	D_2	D_2	A	D_2	D_2	A
E_1	E_1	E_{-1}	E_{-1}	E_1	A	E_1
E_{-1}	E_{-1}	E_1	E_1	E_{-1}	A	E_{-1}
F_1	F_1	E_{-1}	F_{-1}	E_1	B	E_1
F_{-1}	F_{-1}	E_1	F_1	E_{-1}	B	E_{-1}

The character table of $\mathrm{SL}_2(\mathbb{F}_5)$ is as follows [11, pp. 155]:

	A	B	C_1	D_1	D_2	E_1	E_{-1}	F_1	F_{-1}
χ_1	6	-6	0	0	0	1	1	-1	-1
χ_2	5	5	1	-1	-1	0	0	0	0
χ_3	4	4	0	1	1	-1	-1	-1	-1
χ_4	4	-4	0	-1	1	-1	-1	1	1
χ_5	3	3	-1	0	0	$-\varphi$	$\overline{\varphi}$	$-\varphi$	$\overline{\varphi}$
χ_6	3	3	-1	0	0	$\overline{\varphi}$	$-\varphi$	$\overline{\varphi}$	$-\varphi$
χ_7	2	-2	0	1	-1	$-\overline{\varphi}$	φ	$\overline{\varphi}$	$-\varphi$
χ_8	2	-2	0	1	-1	φ	$-\overline{\varphi}$	$-\varphi$	$\overline{\varphi}$
χ_9	1	1	1	1	1	1	1	1	1

,

where we have set

$$\varphi := \frac{-1+\sqrt{5}}{2}, \qquad \overline{\varphi} := \frac{1+\sqrt{5}}{2} = \frac{1}{\varphi}. \tag{5}$$

The following set of tables summarizes the results of the computations for $\mathrm{SL}_2(\mathbb{F}_5)$. Each table corresponds to one character. The rows of the table are parameterized by classes A–F_{-1}; the first column

gives the characteristic polynomial $T_{\mathcal{C}}(x)$ of the corresponding representation on the conjugacy class $\mathcal{C}$. The second column gives the value $|\tilde{T_{\mathcal{C}}}(1)|$, where $T_{\mathcal{C}}(x) = (x-1)^k \tilde{T_{\mathcal{C}}}(x)$ and $\tilde{T_{\mathcal{C}}}(1) \neq 0$. The third column equals $\deg(\tilde{T_{\mathcal{C}}}(x))$.

χ_1:

$(x-1)^6$	1	0
$(x+1)^6$	64	6
$(x^2+1)^3$	8	6
$(x^3+1)^2$	8	6
$(x^3-1)^2$	9	4
$(x^5-1)(x-1)$	5	4
$(x^5-1)(x-1)$	5	4
$(x^5+1)(x+1)$	4	6
$(x^5+1)(x+1)$	4	6

χ_2:

$(x-1)^5$	1	0
$(x-1)^5$	1	0
$(x^2-1)^2(x-1)$	4	2
$(x^2+x+1)(x^3-1)$	9	4
$(x^2+x+1)(x^3-1)$	9	4
x^5-1	5	4
x^5-1	5	4
x^5-1	5	4
x^5-1	5	4

χ_3:

$(x-1)^4$	1	0
$(x-1)^4$	1	0
$(x^2-1)^2$	4	2
$(x^2-1)(x^2+x+1)$	6	3
$(x^2-1)(x^2+x+1)$	6	3
$x^4+x^3+x^2+x+1$	5	4
$x^4+x^3+x^2+x+1$	5	4
$x^4+x^3+x^2+x+1$	5	4
$x^4+x^3+x^2+x+1$	5	4

χ_4:

$(x-1)^4$	1	0
$(x+1)^4$	16	4
$(x^2+1)^2$	4	4
$(x^3+1)(x+1)$	4	4
$(x-1)^2(x^2+x+1)$	6	2
$x^4+x^3+x^2+x+1$	5	4
$x^4+x^3+x^2+x+1$	5	4
$x^4-x^3+x^2-x+1$	1	4
$x^4-x^3+x^2-x+1$	1	4

χ_5:

$(x-1)^3$	1	0
$(x-1)^3$	1	0
$(x^2-1)(x+1)$	4	2
x^3-1	3	2
x^3-1	3	2
$x^3+\varphi x^2-\varphi x-1$	$\varphi+3$	2
$x^3+\varphi x^2-\varphi x-1$	$\varphi+3$	2
$x^3-\overline{\varphi}x^2+\overline{\varphi}x-1$	$3-\overline{\varphi}$	2
$x^3-\overline{\varphi}x^2+\overline{\varphi}x-1$	$3-\overline{\varphi}$	2

χ_6:

$(x-1)^3$	1	0
$(x-1)^3$	1	0
$(x^2-1)(x+1)$	4	2
x^3-1	3	2
x^3-1	3	2
$x^3-\overline{\varphi}x^2+\overline{\varphi}x-1$	$3-\overline{\varphi}$	2
$x^3+\varphi x^2-\varphi x-1$	$\varphi+3$	2
$x^3-\overline{\varphi}x^2+\overline{\varphi}x-1$	$3-\overline{\varphi}$	2
$x^3+\varphi x^2-\varphi x-1$	$\varphi+3$	2

χ_7:

$(x-1)^2$	1	0
$(x+1)^2$	4	2
x^2+1	2	2
x^2-x+1	1	2
x^2+x+1	3	2
$x^2+\overline{\varphi}x+1$	$\frac{1}{2}(5+\sqrt{5})$	2
$x^2-\varphi x+1$	$\frac{1}{2}(5-\sqrt{5})$	2
$x^2-\overline{\varphi}x+1$	$\frac{1}{2}(3-\sqrt{5})$	2
$x^2+\varphi x+1$	$\frac{1}{2}(3+\sqrt{5})$	2

χ_8:

$(x-1)^2$	0	2
$(x+1)^2$	4	2
x^2+1	2	2
x^2-x+1	1	2
x^2+x+1	3	2
$x^2-\varphi x+1$	$\frac{1}{2}(5-\sqrt{5})$	2
$x^2+\overline{\varphi}x+1$	$\frac{1}{2}(5+\sqrt{5})$	2
$x^2+\varphi x+1$	$\frac{1}{2}(3+\sqrt{5})$	2
$x^2-\overline{\varphi}x+1$	$\frac{1}{2}(3-\sqrt{5})$	2

χ_9:

$x-1$	$x-1$	$x-1$	$x-1$	$x-1$	$x-1$	$x-1$	$x-1$	$x-1$
0	0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1	1

We infer that only the 2-dimensional representations given by χ_8 and χ_7 are fixed-point-free, i.e., that these are the only representations such that no nontrivial matrix in their image has eigenvalue 1. The corresponding ζ-value (see (3)) of these representations equals

$$\frac{1}{2}\sqrt{\frac{3-\sqrt{5}}{2}} \sim 0.309.$$

This is in agreement with the results of [1]. We also see that the representation χ_4 is *almost fixed-point-free*, in that its ζ-value is zero on one nontrivial class only (the class D_2), and has high ζ-value

on other classes (equal to 0.5).

6 Power map for the group $\mathrm{SL}_2(\mathbb{F}_q)$, for odd prime q

To carry out the program exemplified in the last section for all the groups $\mathrm{SL}_2(\mathbb{F}_q)$, we first need to compute the power maps of this group; in other words, if $C_1, \ldots, C_h$ denote the different conjugacy classes of $\mathrm{SL}_2(\mathbb{F}_q)$, we want to find the power map function $\pi\colon \{1, \ldots, h\}^2 \mapsto 1, \ldots, h$ defined by $C_j^k = C_{\pi(j,k)}$.

We first recall some basic facts about the conjugacy classes of $\mathrm{SL}_2(\mathbb{F}_q)$, and use [11] as a reference. This group has $q+4$ conjugacy classes which we denote by

$$A,\ B,\ C_1,\ \ldots,\ C_{(q-3)/2},\ D_1,\ \ldots,\ D_{(q-1)/2},\ E_1,\ E_{-1},\ F_1,\ F_{-1}.$$

To introduce generators for these conjugacy classes, let ω denote a generator of $\mathbb{F}_q^\times$, and let θ be a primitive $(q+1)$st root of unity over $\mathbb{F}_{q^2}$. Then we have

$$\begin{aligned}
A &= \left[\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right], \quad B = \left[\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}\right], \\
C_i &= \left[\begin{pmatrix} \omega^i & 0 \\ 0 & \omega^{-1} \end{pmatrix}\right], \quad i = 1, \ldots, \frac{q-3}{2}, \\
D_j &= \left[\begin{pmatrix} \theta^j & 0 \\ 0 & \theta^{-j} \end{pmatrix}\right], \quad j = 1, \ldots, \frac{(q-1)}{2}, \\
E_1 &= \left[\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\right], \quad E_{-1} = \left[\begin{pmatrix} 1 & \omega \\ 0 & 1 \end{pmatrix}\right] \\
F_1 &= \left[\begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix}\right], \quad F_{-1} = \left[\begin{pmatrix} -1 & \omega \\ 0 & -1 \end{pmatrix}\right].
\end{aligned}$$

A word of caution is in order. Obviously, the matrix that defines D_j does not belong to $\mathrm{SL}_2(\mathbb{F}_q)$

since θ does not belong to $\mathbb{F}_q$. However, the Frobenius companion matrix of that matrix, namely

$$\begin{pmatrix} 0 & -1 \\ 1 & \theta^i + \theta^{-i} \end{pmatrix}$$

is conjugate (in $\mathrm{SL}_2(\mathbb{F}_{q^2})$) to the said matrix and belongs to $\mathrm{SL}_2(\mathbb{F}_q)$. Stated more precisely, D_i is the conjugacy class of this matrix. However, we find it more convenient to work with the diagonal matrix given above.

The sizes of these conjugacy classes are given as follows [11, pp. 155]:

$$|A| = |B| = 1, \quad |C_i| = q(q+1), \quad |D_i| = q(q-1), \quad |E_{\pm 1}| = F_{\pm 1} = \frac{q^2-1}{2}. \tag{6}$$

The power-map function is given in the following theorem, for which we need to introduce one more piece of notation. Let $r_a(b)$ denote the smallest residue of a modulo b in absolute value. For example, $r_5(3) = -2$, $r_4(2) = 2$, and $r_7(3) = 3$.

Theorem 1. *Let $C_0 := A$, $C_{(q-1)/2} := B$, $D_0 := A$, $D_{(q+1)/2} := B$, $D_0 := A$, $F_0 := B$, and let $\left(\frac{a}{b}\right)$ be the Legendre symbol of a and b. Then we have the following results for $0 \le k < 2p$:*

(a) $A^k = A$.

(b) $B^k = B$ *for odd* k, *and* $B^k = A$ *for even* k.

(c) $C_i^k = C_{|r_{q-1}(ik)|}$.

(d) $D_i^k = D_{|r_{q+1}(ik)|}$.

(e) $E_1^k = E_{\left(\frac{k}{q}\right)}$.

(f) $E_{-1}^k = E_{-\left(\frac{k}{q}\right)}$.

(g) $F_1^k = E_{\left(\frac{-k}{q}\right)}$ *if* k *is even, and* $F_1^k = F_{\left(\frac{-k}{q}\right)}$ *if* k *is odd.*

(h) $F_{-1}^k = E_{-\left(\frac{-k}{q}\right)}$ *if* k *is even, and* $F_{-1}^k = F_{-\left(\frac{-k}{q}\right)}$ *if* k *is odd.*

Proof. (a) and (b) are clear.

Let M_i be the diagonal matrix with diagonal entries ω^i, ω^{-i}. Then M_{q-1-i} is the diagonal matrix with entries ω^{-i}, ω^i, hence is conjugate to M_i as is easily seen. Since $M_i^k = M_{ik}$, we see that M_i^k is conjugate to $M_{|r_{q-1}(ik)|}$, and part (c) follows.

Part (d) is proved analogously. The proofs of parts (e) and (f) are similar, so we only prove (e). Let M be the matrix

$$M := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Then M^k is the upper triangular matrix having ones on the diagonal and k in the upper right corner. We claim that M^k is conjugate to $E_{\left(\frac{k}{q}\right)}$. Suppose that $\left(\frac{k}{q}\right) = 1$, and let a be a square root of $1/k$. Then, it is easily seen that

$$\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix},$$

which shows that M^k and M are conjugate. If $\left(\frac{k}{q}\right) = -1$, then let a be a square root of ω/k and repeat the above argument. This shows that M^k is conjugate to $\begin{pmatrix} 1 & \omega \\ 0 & 1 \end{pmatrix}$.

The cases (g) and (h) are also similar, so we concentrate on (g) only. Let M be the matrix

$$M := \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix}.$$

Then

$$M^k = (-1)^k \begin{pmatrix} 1 & -k \\ 0 & 1 \end{pmatrix}.$$

If k is even, we see that the conjugacy class of M^k is $E_{\left(\frac{-k}{q}\right)}$. If k is odd, then we see in a similar fashion as above that the conjugacy class of M^k is $F_{\left(\frac{-k}{q}\right)}$. □

For later use, we need to study which power of the above conjugacy classes equal A or B. In the following, for a prime number ℓ and an integer a let $\nu_\ell(a)$ denote the maximum number s such ℓ^s divides a. For example, $\nu_2(12) = 2$, and $\nu_2(5) = 0$. Further, the *order* of a conjugacy class C is the smallest positive integer d such that C^d is the class of the identity matrix. In other words, the order of C is the order of any generator of C in the group.

Proposition 1. *Let $C_i, D_i, E_1, E_{-1}, F_1, F_{-1}$ be the conjugacy classes defined above. Then we have:*

(a) *The order of B is 2.*

(b) *For* $1 \leq i < (q-1)/2$ *the order of* C_i *is* $(q-1)/\gcd(i, q-1)$.

(c) *For* $1 \leq i < (q+1)/2$ *the order of* D_i *is* $(q+1)/\gcd(i, q+1)$.

(d) *The order of* E_1 *and* E_{-1} *is* q.

(e) *The order of* F_1 *and* F_{-1} *is* $2q$.

(f) *There exists no* d *such that* $E_{\pm 1}^d = B$.

(g) *The smallest positive* d *with* $F_{\pm 1}^d = B$ *is* $d = q$.

(h) *There exists* d *such that* $C_i^d = B$ *if and only if* $\nu_2(i) < \nu_2(q-1)$. *In that case the smallest such positive number is* $d = (q-1)/(2\gcd(i, q-1))$.

(i) *There exists* d *such that* $D_i^d = B$ *if and only if* $\nu_2(i) < \nu_2(q+1)$. *In that case the smallest such positive number is* $d = (q+1)/(2\gcd(i, q+1))$.

Proof. (a) is obvious. For (b), let M be the diagonal matrix with diagonal entries ω^i, ω^{-i}. C_i is the conjugacy class of this matrix. The order of M is the smallest positive integer d such that $id \equiv 0 \bmod (q-1)$. Obviously, this is equal to $(q-1)/\gcd(i, q-1)$. The proof of (c) is similar. As for (e), let M be the upper triangular matrix with 1's in the diagonal and 1 in position $(1, 2)$. Then M^k has a k in position $(1, 2)$, hence M^k is the identity matrix if and only if $k \equiv 0 \bmod q$. As a result, the order of M is q. This proves that E_1 has order q and that no power of E_1 is B; the proof for E_{-1} is analogous. As for (f), let T be the upper triangular matrix with -1's in the diagonal and 1 at position $(1, 2)$. Then $T = -M^{-1}$, and $T^k = (-1)^k M^{-k}$, hence the order of T is $2q$ and the smallest power of F_1 equal to B is T^d. A similar assertion holds for F_{-1} with a similar proof, which takes care of parts (f) and (g).

We now concentrate on (h). Again, let M be the diagonal matrix with diagonal entries ω^i, ω^{-i}. Then M^d is the negative identity matrix if and only of $id \equiv (q-1)/2 \bmod (q-1)$. For this congruence to be solvable for d we must have $\gcd(i, (q-1)/2) = \gcd(i, q-1)$ which is equivalent to $\nu_2(i) < \nu_2(q-1)$. Part (i) is proved analogously. □

7 Eigenvalues of irreducible representations of $\mathrm{SL}_2(\mathbb{F}_q)$

In this section we compute the eigenvalues of the irreducible representations of $\mathrm{SL}_2(\mathbb{F}_q)$ on the various conjugacy classes based on the characters of these representations as computed in [11, pp. 155]. For

this we need some preliminary definitions. A *character* α of $\mathbb{F}_q^\times$ is a multiplicative map from $\mathbb{F}_q^\times$ into the field of complex numbers. Obviously, the values of any such character are $(q-1)$st roots of unity. Similarly, let μ_{q+1} denote the group of the $(q+1)$st roots of unity in $\mathbb{F}_{q^2}$. A character β of this group is a multiplicative mapping from this group into the field of complex numbers. The values of β are obviously $(q+1)$st roots of unity.

Let α_0 denote the character of $\mathbb{F}_q^\times$ that maps the squares in $\mathbb{F}_q^\times$ to 1 and the non-squares to -1. It is well-known that $\alpha_0(-1) = \left(\frac{-1}{q}\right)$. Similarly, let β_0 be the character of μ_{q+1} which maps squares to 1 and non-squares to -1. Then $\beta_0(-1) = -\left(\frac{-1}{q}\right)$.

With these notations, the character table of $\mathrm{SL}_2(\mathbb{F}_q)$ is given by [11, pp. 155]

	A	B	C_i	D_i	E_1	E_{-1}	F_1	F_{-1}
Id	1	1	1	1	1	1	1	1
$R_T^G(\alpha)$	$q+1$	$\alpha(-1)(q+1)$	$\alpha(\omega^i)+\alpha(\omega^{-i})$	0	1	1	$\alpha(-1)$	$\alpha(-1)$
St	q	q	1	-1	0	0	0	0
$-R_{T_s}^G(\beta)$	$q-1$	$\beta(-1)(q-1)$	0	$-\beta(\theta^i)-\beta(\theta^{-i})$	-1	-1	$-\beta(-1)$	$-\beta(-1)$
$\chi^\varepsilon_{\alpha_0}$	$\frac{q+1}{2}$	$\alpha_0(-1)\frac{q+1}{2}$	$\alpha_0(\omega^i)$	0	η_1	$\overline{\eta}_1$	η_{-1}	$\overline{\eta}_{-1}$
$\chi^\varepsilon_{\beta_0}$	$\frac{q-1}{2}$	$\beta_0(-1)\frac{q-1}{2}$	0	$-\beta_0(\theta^i)$	υ_1	$\overline{\upsilon}_1$	υ_{-1}	$\overline{\upsilon}_{-1}$

where

$$\eta_i := \frac{\alpha_0(i)}{2}\left(1+\varepsilon\alpha_0(i)\sqrt{\alpha_0(-1)q}\right), \quad \overline{\eta}_i := \frac{\alpha_0(i)}{2}\left(1-\varepsilon\alpha_0(i)\sqrt{\alpha_0(-1)q}\right),$$

and

$$\upsilon_i := \frac{\beta_0(i)}{2}\left(-1+\varepsilon\alpha_0(i)\sqrt{\alpha_0(-1)q}\right), \quad \overline{\upsilon}_i := \frac{\beta_0(i)}{2}\left(-1-\varepsilon\alpha_0(i)\sqrt{\alpha_0(-1)q}\right),$$

for $i = 1, -1$. Here, α runs over a set of inequivalent characters of $\mathbb{F}_q^\times$, where we define two characters equivalent if they are the inverse of each other. Similarly, β runs over a set of inequivalent characters of μ_{q+1}. ε runs over the set $\{-1, 1\}$.

Later in Appendix A we will prove the following Theorem which gives the eigenvalues for all the irreducible representations of $\mathrm{SL}_2(\mathbb{F}_q)$.

Theorem 2. *The eigenvalues of the irreducible representations of* $\mathrm{SL}_2(\mathbb{F}_q)$ *for prime odd* q *are given in Table 1.*

To be able to read the table, we need to introduce some notation.

- For a character χ, we define

$$e_{\chi,i,d} := \begin{cases} \chi(-1), & \text{if } \nu_2(i) < \nu_2(d), \\ 1, & \text{otherwise.} \end{cases}$$

- For $i = 1, \ldots, (q-3)/2$ we define

$$t_i := \begin{cases} \dfrac{q-1}{2\gcd(i, q-1)}, & \text{if } \nu_2(i) < \nu_2(q-1), \\ \\ \dfrac{q-1}{\gcd(i, q-1)}, & \text{if } \nu_2(i) = \nu_2(q-1). \end{cases}$$

- For $i = 1, \ldots, (q-1)/2$ we define

$$r_i := \begin{cases} \dfrac{q+1}{2\gcd(i, q+1)}, & \text{if } \nu_2(i) < \nu_2(q+1), \\ \\ \dfrac{q+1}{\gcd(i, q+1)}, & \text{if } \nu_2(i) = \nu_2(q+1). \end{cases}$$

- We set $\eta_{\alpha,i} := \alpha(\omega^i)$, and $\eta_{\beta,i} := \beta(\theta^i)$.

- We set $\gamma_q := \mathrm{e}^{2\pi i/q}$.

The interested reader may want to verify the results of Section 5 using Table 1.

8 Example: an 8-dimensional representation of $\mathrm{SL}_2(\mathbb{F}_{17})$

A look at Table 1 and some calculation reveals that, for odd prime q less than 20, the only groups $\mathrm{SL}_2(\mathbb{F}_q)$ which have an irreducible representation without "too many" eigenvalues 1 are $\mathrm{SL}_2(\mathbb{F}_3)$, $\mathrm{SL}_2(\mathbb{F}_5)$, and $\mathrm{SL}_2(\mathbb{F}_{17})$. The two first groups in this list are in fact fixed-point-free, and were already considered in [1]. For $\mathrm{SL}_2(\mathbb{F}_{17})$ the representations without too many eigenvalues 1 are $\chi^1_{\beta_0}$ and $\chi^{-1}_{\beta_0}$. Therefore, we will in this section apply the results of the previous section to compute the characteristic polynomials of a irreducible representation corresponding to $\chi^1_{\beta_0}$ for the group $\mathrm{SL}_2(\mathbb{F}_{17})$. Using that, we will derive upper bounds for the probability of error of the differential space-time codes obtained from this representation for arbitrary SNR's.

$\mathrm{SL}_2(\mathbb{F}_{17})$ has 21 different conjugacy classes. They are (in the notation of the previous section) A, B, $C_1, \ldots, C_7$, $D_1, \ldots, D_8$, $E_{\pm 1}$, and $F_{\pm 1}$. The characteristic polynomial of $\chi^1_{\beta_0}$ on these classes will be computed using Table 1.

Note that $\beta_0(-1) = -1$ since $17 \equiv 1 \bmod 4$. As a result, the characteristic polynomial of $\chi^1_{\beta_0}$ on B is $(x+1)^8$.

For all $i = 1, \ldots, 7$ we have that $\nu_2(i) < \nu_2(17-1) = 4$, hence $e_{\beta_0,i,16} = \beta_0(-1) = -1$, and $t_i = 8/\gcd(i,16)$. So, the characteristic polynomial of $\chi^1_{\beta_0}$ on C_i is x^8+1 if i is odd, it is $(x^4+1)^2$ if $i \equiv 2 \bmod 4$, and it is $(x^2+1)^4$ for $i = 4$.

To compute $e_{\beta_0,i,18}$ and r_i for $i = 1, \ldots, 8$ we proceed as follows. If i is odd, then $\nu_2(i) < \nu_2(18)$, hence $r_i = 9/\gcd(i,18)$ and $e_{\beta_0,i,18} = -1$. So, $r_1 = r_5 = r_7 = 9$, and $r_3 = 3$. If i is even, then $r_i = 18/\gcd(i,18)$ and $e_{\beta_0,i,18} = 1$. So, $r_2 = r_4 = r_8 = 9$, and $r_6 = 3$. As a result, the characteristic polynomial of $\chi^1_{\beta_0}$ on D_i is $(x^9+1)/(x+1)$ for $i = 1,5,7$, it is $(x^3+1)^3/(x+1)$ for $i = 3$, it is $(x^9-1)/(x-1)$ for $i = 2,4,8$, and it is $(x^3-1)^3/(x-1)$ for $i = 6$.

The characteristic polynomial of $\chi^1_{\beta_0}$ on E_1 is $\prod_{(\frac{k}{17})=1}(x-\gamma^k)$, where $\gamma = \mathrm{e}^{2\pi i/17}$. This polynomial can be represented in closed form in the following way:

$$\begin{aligned}\prod_{(\frac{k}{17})=1}(x-\gamma^k) &= x^8 + \frac{1-\sqrt{17}}{2}x^7 + \frac{5-\sqrt{17}}{2}x^6 + \frac{7-\sqrt{17}}{2}x^5 + \\ &\quad (2-\sqrt{17})x^4 + \frac{7-\sqrt{17}}{2}x^3 + \frac{5-\sqrt{17}}{2}x^2 + \frac{1-\sqrt{17}}{2}x + 1 \\ &=: T_{E_1}(x). \end{aligned} \tag{7}$$

Similarly, we have

$$\begin{aligned}\prod_{(\frac{k}{17})=-1}(x-\gamma^k) &= x^8 + \frac{1+\sqrt{17}}{2}x^7 + \frac{5+\sqrt{17}}{2}x^6 + \frac{7+\sqrt{17}}{2}x^5 + \\ &\quad (2+\sqrt{17})x^4 + \frac{7+\sqrt{17}}{2}x^3 + \frac{5+\sqrt{17}}{2}x^2 + \frac{1+\sqrt{17}}{2}x + 1 \\ &=: T_{E_{-1}}(x), \end{aligned} \tag{8}$$

$$\begin{aligned}\prod_{(\frac{k}{17})=1}(x+\gamma^k) &= x^8 - \frac{1-\sqrt{17}}{2}x^7 + \frac{5-\sqrt{17}}{2}x^6 - \frac{7-\sqrt{17}}{2}x^5 + \\ &\quad (2-\sqrt{17})x^4 - \frac{7-\sqrt{17}}{2}x^3 + \frac{5-\sqrt{17}}{2}x^2 - \frac{1-\sqrt{17}}{2}x + 1 \\ &=: T_{F_1}(x), \end{aligned} \tag{9}$$

$$\prod_{(\frac{k}{17})=-1}(x+\gamma^k) = x^8 - \frac{1+\sqrt{17}}{2}x^7 + \frac{5+\sqrt{17}}{2}x^6 - \frac{7+\sqrt{17}}{2}x^5 +$$

$$(2+\sqrt{17})x^4 - \frac{7+\sqrt{17}}{2}x^3 + \frac{5+\sqrt{17}}{2}x^2 - \frac{1+\sqrt{17}}{2}x + 1 \qquad (10)$$

$$=: \quad T_{F_{-1}}(x).$$

In summary, we have the following.

Proposition 2. *Let $T_C(x)$ denote the characteristic polynomial of $\chi^1_{\beta_0}$ on the conjugacy class C of $\mathrm{SL}_2(\mathbb{F}_{17})$. Then the following hold:*

(a) $T_A(x) = (x-1)^8$, $T_B(x) = (x+1)^8$.

(b) $T_{C_i}(x) = (x^8+1)$ *for* $i = 1,3,5,7$, $T_{C_i}(x) = (x^4+1)^2$ *for* $i = 2,6$, *and* $T_{C_4}(x) = (x^2+1)^4$.

(c) $T_{D_i}(x) = (x^9+1)/(x+1)$ *for* $i = 1,5,7$; $T_{D_3}(x) = (x^3+1)^3/(x+1)$; $T_{D_i}(x) = (x^9-1)/(x-1)$ *for* $i = 2,4,8$, *and* $T_{D_6}(x) = (x^3-1)^3/(x-1)$.

(d) $T_{E_{\pm 1}}(x)$ *and* $T_{F_{\pm 1}}(x)$ *are given in (7)–(10) above.*

In the next section we will investigate the representation corresponding to $\chi^1_{\beta_0}$ from the point of view as using it for the design of unitary multiple antenna space-time signal constellations.

9 Unitary differential space-time constellations from $\chi^1_{\beta_0}$

Let $\mathcal{V}$ be a group of L unitary $M \times M$-matrices and let V_1 be a matrix in V. Using the results of Section 2, the probability $P_{V,W}$ of mistaking a matrix W with a matrix V when sent over the Rayleigh fading channel with M transmitter and N receiving antennas at a signal to noise ratio (SNR) ρ satisfies

$$P_{V,W} \leq \frac{1}{2} \prod_{m=1}^{M} \left[1 + f(\rho)\sigma_m^2(V-W)\right]^{-N},$$

where $f(\rho) = \rho/4$ in case the channel is known, and $f(\rho) = \rho^2/(4(1+2\rho))$ in case of an unknown channel, and $\sigma_m(V-W)$, $m = 1,\ldots,M$, are the singular values of the matrix $V-W$. By the union bound, the error probability P_e of mistaking V with another element of the constellation satisfies

$$P_e \leq \sum_{W \in \mathcal{V}} P_{V,W}.$$

It is our aim to obtain an upper bound for this error-probability when using the representation of $\mathrm{SL}_2(\mathbb{F}_{17})$ corresponding to $\chi^1_{\beta_0}$ as the set $\mathcal{V}$.

To this end, note first that we may assume V to be the identity matrix, since $\sigma_m(V-W) = \sigma_m(I-V^{-1}W)$, and $V^{-1}W$ belongs to $\mathcal{V}$ as the latter is a group. Further, $\sigma_m^2(I-W) = \lambda_m((I-W)(I-W)^*)$, where $\lambda_m(A)$ is the mth eigenvalue of the matrix A (in some ordering), and B^* denotes the Hermitian conjugate of the matrix B. As a result, since W is unitary, $\sigma_m^2(I-W) = 2 - 2\mathrm{Re}(\lambda_m(W))$, where $\mathrm{Re}(z)$ is the real part of the complex number z. This shows that

$$P_{I,W} \leq \frac{1}{2} \prod_{m=1}^{M} \left[1 + 2f(\rho) - 2f(\rho)\mathrm{Re}(\lambda_m(W))\right]^{-N}.$$

Next, observe that $\lambda_m(W)$ is constant when W runs over a conjugacy class C of $\mathrm{SL}_2(\mathbb{F}_{17})$; in this case, we abbreviate $\lambda_m(W)$ by $\lambda_m(C)$. Then, we obtain the following formula for the average pairwise error probability P_e:

$$P_e \leq \sum_{C \in \mathcal{C}} \left\{ |C| \prod_{m=1}^{M} \Big[1 + 2f(\rho)\Big(1 - \mathrm{Re}(\lambda_m(C))\Big)\Big]^{-N} \right\},$$

where $\mathcal{C}$ is the set of conjugacy classes of the group. In our case, we already know the sizes of the various conjugacy classes (6): $|A| = |B| = 1$, $|C_i| = 17 \cdot 18$, $|D_i| = 17 \cdot 16$, and $|E_{\pm 1}| = |F_{\pm 1}| = (q^2-1)/2$. The real parts of the eigenvalues of C can be computed from the results of the previous section. These results are summarized as follows. In all cases, m runs over the integers from 1 to 8.

- $C = A$: $\mathrm{Re}(\lambda_m(C)) = 1$.
- $C = B$: $\mathrm{Re}(\lambda_m(C)) = -1$.
- $C = C_i$:
  - $\mathrm{Re}(\lambda_m(C_i)) = \cos(2\pi(2m-1)/16)$ for $i = 1, 3, 5, 7$.
  - $\mathrm{Re}(\lambda_m(C_i)) = \cos(2\pi(2m-1)/8)$ for $i = 2, 6$.
  - $\mathrm{Re}(\lambda_m(C_4)) = \cos(2\pi(2m-1)/4)$.
- $C = D_i$:
  - $\mathrm{Re}(\lambda_m(D_i)) = \cos(2\pi(2m+9)/18)$ for $i = 1, 5, 7$.
  - $\mathrm{Re}(\lambda_m(D_i)) = \cos(2\pi m/9)$ for $i = 2, 4, 8$.
  - $\mathrm{Re}(\lambda_m(D_3)) = \cos(2\pi(2m+9)/6)$.

- $\mathrm{Re}(\lambda_m(D_6)) = \cos(2\pi m/3)$.

- $C = E_1$ or $C = F_1$: $\mathrm{Re}(\lambda_m(C)) = \cos(2\pi m^2/17)$.

- $C = E_{-1}$ or $C = F_{-1}$: $\mathrm{Re}(\lambda_m(C)) = \cos(2\pi 3m^2/17)$.

This results in the following upper bound for P_e:

$$\begin{aligned}
P_e \quad \leq \quad & (1+4f(\rho))^{-N} + 4\cdot 17\cdot 18\cdot \prod_{m=1}^{8}\left\{1+2f(\rho)\left(1-\cos\left(\frac{2\pi(2m-1)}{16}\right)\right)\right\}^{-N} \\
& +2\cdot 17\cdot 18\prod_{m=1}^{8}\left\{1+2f(\rho)\left(1-\cos\left(\frac{2\pi(2m-1)}{8}\right)\right)\right\}^{-N} \\
& +17\cdot 18\prod_{m=1}^{8}\left\{1+2f(\rho)\left(1-\cos\left(\frac{2\pi(2m-1)}{4}\right)\right)\right\}^{-N} \\
& +3\cdot 17\cdot 16\prod_{m=1}^{8}\left\{1+2f(\rho)\left(1-\cos\left(\frac{2\pi(2m+9)}{18}\right)\right)\right\}^{-N} \\
& +3\cdot 17\cdot 16\prod_{m=1}^{8}\left\{1+2f(\rho)\left(1-\cos\left(\frac{2\pi m}{9}\right)\right)\right\}^{-N} \\
& +17\cdot 16\prod_{m=1}^{8}\left\{1+2f(\rho)\left(1-\cos\left(\frac{2\pi(2m+9)}{6}\right)\right)\right\}^{-N} \\
& +17\cdot 16\prod_{m=1}^{8}\left\{1+2f(\rho)\left(1-\cos\left(\frac{2\pi m}{3}\right)\right)\right\}^{-N} \\
& +2\frac{17^2-1}{2}\prod_{m=1}^{8}\left\{1+2f(\rho)\left(1-\cos\left(\frac{2\pi m^2}{17}\right)\right)\right\}^{-N} \\
& +2\frac{17^2-1}{2}\prod_{m=1}^{8}\left\{1+2f(\rho)\left(1-\cos\left(\frac{2\pi 3m^2}{17}\right)\right)\right\}^{-N}.
\end{aligned}$$

In Figure 1 we have plotted the logarithm of the (upper bound on the) error probability P_e as a function of SNR (which equals $10\log_{10}(\rho)$ and is measured in dB).

In the next section, we will compute a unitary representation affording $\chi^1_{\beta_0}$ and elaborate on simulation results using the corresponding set of matrices.

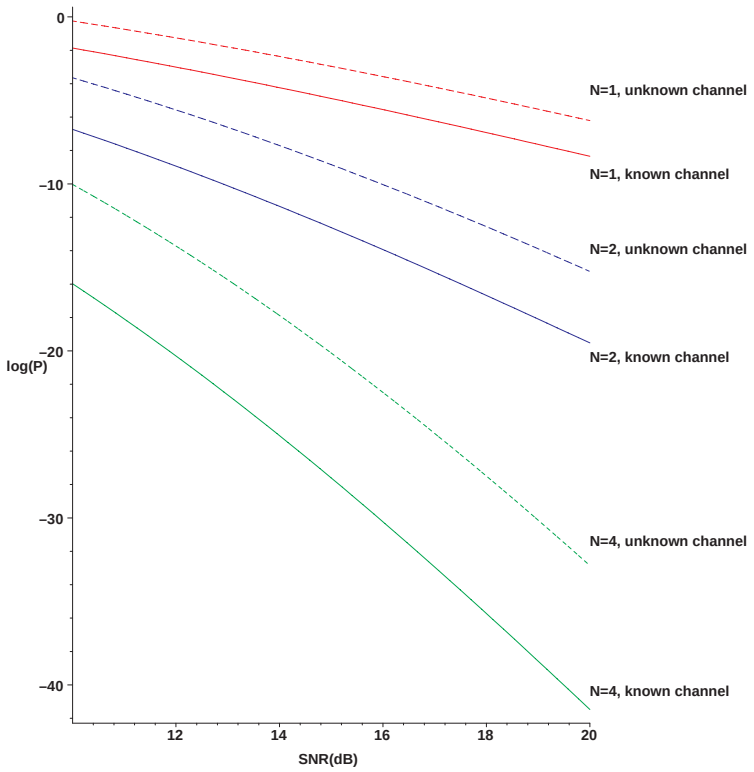


Figure 1: Logarithm of the probability of error versus SNR for the 8-dimensional representation of $\mathrm{SL}_2(\mathbb{F}_{17})$ for the coherent channel and the unknown channel cases. N denotes the number of receiving antennas

10 The Representation and Simulation Results

In this section we will compute a unitary representation affording $\chi^1_{\beta_0}$. The details are rather technical, and can be found in Appendix B.

Let B denote the subgroup of $\mathrm{SL}_2(\mathbb{F}_q)$ consisting of upper triangular 2×2-matrices with ones on the diagonal, and T be the subgroup of upper triangular 2×2-matrices of determinant one over $\mathbb{F}_q$. Further, let D be the subgroup of diagonal 2×2-matrices of determinant one. It is easily seen that any matrix in T can be written uniquely as a product db of a matrix $d \in D$ and a matrix $b \in B$.

Let g be the matrix

$$g = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{F}_q).$$

It is well-known (and easy to prove) that

$$\mathrm{SL}_2(\mathbb{F}_q) = T \sqcup TgB, \tag{11}$$

i.e., any matrix in $\mathrm{SL}_2(\mathbb{F}_q)$ is either in T, or it can be written uniquely as a product tgb with $t \in T$ and $b \in B$. Indeed, for $c \neq 0$ we have

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} -c^{-1} & -a \\ 0 & -c \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 1 & d/c \\ 0 & 1 \end{pmatrix},$$

and if the matrix on the left hand side had two different representations of this form, then this would imply the contradiction $g \in T$.

Thus, a representation Δ of $\mathrm{SL}_2(\mathbb{F}_q)$ is uniquely determined by $\Delta(t)$ for $t \in T$, and $\Delta(g)$. We can compress the description of Δ even further: Note that

$$D = \left\langle \begin{pmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{pmatrix} \right\rangle, \qquad B = \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle,$$

where ω is a primitive root of $\mathbb{F}_q^\times$. Hence, to present Δ, we only need to know the value of Δ at the two matrices above, as well as $\Delta(g)$.

Let these values be denoted by M_D, M_B, and M_g, respectively. Then the constellation corresponding to Δ is the set

$$\left\{ M_D^k M_B^j \mid 0 \leq k < q-1, 0 \leq j < q \right\} \bigsqcup \left\{ M_D^k M_B^j M_g M_B^\ell \mid 0 \leq k < q-1, 0 \leq j < q, 0 \leq \ell < q-1 \right\}. \tag{12}$$

With these preparations, we can now describe a representation affording $\chi^1_{\beta_0}$ and its corresponding constellation:

Theorem 3. *A unitary representation Δ affording the character $\chi^1_{\beta_0}$ of $\mathrm{SL}_2(\mathbb{F}_{17})$ is given by*

$$\begin{aligned} \Delta\left(\begin{pmatrix} 3 & 0 \\ 0 & 6 \end{pmatrix}\right) &= e^{2\pi i/16} Z_8 =: M_D \\ \Delta\left(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\right) &= \mathrm{diag}\left(\gamma, \gamma^2, \gamma^{2^2}, \gamma^{2^3}, \gamma^{2^4}, \gamma^{2^5}, \gamma^{2^6}, \gamma^{2^7}\right) =: M_B \end{aligned}$$

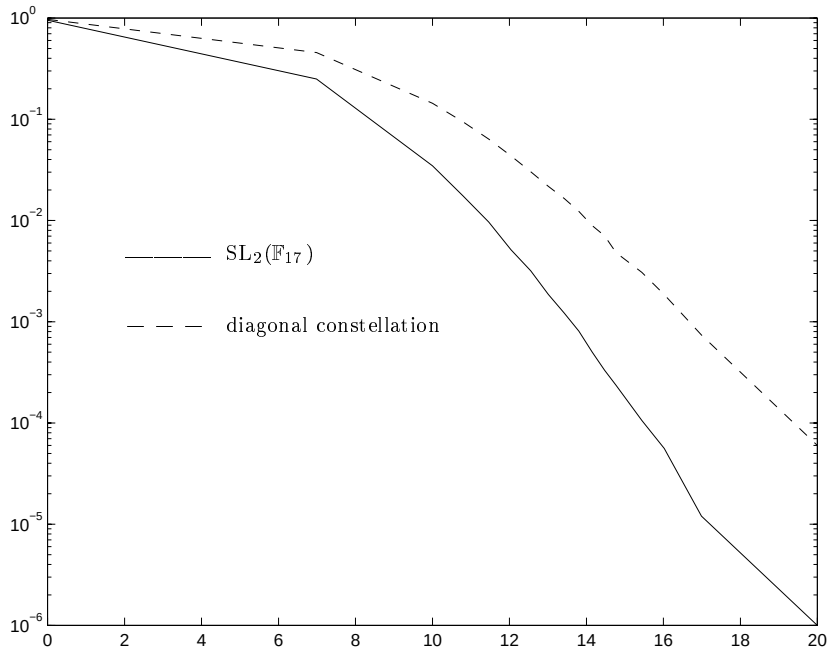


Figure 2: Block-error rate performance of the group $\mathrm{SL}_2(\mathbb{F}_{17})$ versus a good diagonal constellation for $M = 8$ transmitter antennas and $N = 1$ receiver antenna. Both constellations have $L = 4896$ unitary matrices ($R \approx 1.53$).

$$\Delta\left(\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\right) \quad = \quad \frac{2i}{17}\left(e^{2\pi i(k-j)/16}\mathrm{Im}(\alpha_{jk} + \theta\alpha_{jk}^2 + \alpha_{jk}^3 + \alpha_{jk}^4 - \alpha_{jk}^7)\right)_{1\le j,k,\le 8} =: M_g,$$

where Z_8 *is the* shift matrix

$$Z_8 := \begin{pmatrix} 0 & I_7 \\ 1 & 0 \end{pmatrix},$$

(I_7 *is the* 7×7 *identity matrix),* $\gamma = e^{2\pi i/17}$, $\alpha_{jk} = \gamma^{2^{k-1}3^{j-k}}$, $\theta = (-1+\sqrt{17})/2$ *if* $i-j$ *is even, and* $\theta = (-1-\sqrt{17})/2$ *if* $i-j$ *is odd, and* $\mathrm{Im}(z)$ *is the imaginary part of the complex number* z*. The signal constellation corresponding to this representation is given in (12).*

A proof of this theorem can be found in Appendix B.

We have simulated the performance of this constellation on the computer. The results are given in Figure 2.

Acknowledgment

I would like to thank Babak Hassibi, Bert Hochwald, and Thomas Marzetta for interesting discussions concerning the performance of $\mathrm{SL}_2(\mathbb{F}_{17})$, Wim Sweldens for providing the diagonal constellation of

Figure 2, and Carl Pomerance for several number theoretic discussions. I am grateful to Michael Clausen and Salahoddin Shokranian for pointing out the reference [12].

References

[1] B. Hassibi, B. Hochwald, A. Shokrollahi, and W. Sweldens, "Representation theory for high-rate multiple-antenna code design," tech. rep., Bell Laboratories, Lucent Technologies, 2000.

[2] I. E. Telatar, "Capacity of multi-antenna gaussian channels," tech. rep., Bell Laboratories, Lucent Technologies, 1995.

[3] G. J. Foschini, "Layered space-time architecture for wireless communication in a fading environment when using multi-element antennas," *Bell Labs. Tech. J.*, vol. 1, no. 2, pp. 41–59, 1996.

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

[5] T. L. Marzetta and B. M. Hochwald, "Capacity of a mobile multiple-antenna communication link in Rayleigh flat fading," *IEEE Trans. Info. Theory*, vol. 45, pp. 139–157, 1999.

[6] B. M. Hochwald and T. L. Marzetta, "Unitary space-time modulation for multiple-antenna communication in Rayleigh flat-fading," *to appear in IEEE Trans. Info. Theory*, Mar. 2000.

[7] B. Hassibi, B. Hochwald, and T. Marzetta, "Space-time autocoding," *submitted to IEEE Trans. Info. Theory*, 1999.

[8] B. Hochwald and W. Sweldens, "Differential unitary space time modulation," tech. rep., Bell Laboratories, Lucent Technologies, Mar. 1999. Also submitted to *IEEE Trans. Comm.*

[9] P. Bürgisser, M. Clausen, and A. Shokrollahi, *Algebraic Complexity Theory*, vol. 315 of *Grundlehren der Mathematischen Wissenschaften*. Springer Verlag, Heidelberg, 1996.

[10] D. Bini and V. Pan, *Polynomial and Matrix Computations: Fundamental Algorithms*. Birkhäuser, Boston, 1994.

[11] F. Digne and J. Michel, *Representations of Finite Groups of Lie Type.* No. 21 in London Mathematical Society Student Texts, Cambridge University Press, 1991.

[12] A. Silberger, "An elementary construction of the representations of $SL(2, GF(q))$," *Osaka J. Math.*, vol. 6, pp. 329–338, 1969.

[13] E. Landau, *Elementary Number Theory.* Chelsea Publishing Company, New York, 1955.

A Eigenvalues of irreducible representations of $\mathrm{SL}_2(\mathbb{F}_q)$

Lemma 2. *Let $\gamma_1, \ldots, \gamma_d$ be roots of unity over the rationals, and denote by s_i the power-sum $\gamma_1^i + \cdots + \gamma_d^i$. Further, let $T(x)$ denote the polynomial $(x-\gamma_1)\cdots(x-\gamma_d)$. Suppose that $s_t = d$ or $s_t = -d$. Then the γ_j are determined uniquely up to ordering by the values $s_1, \ldots, s_t$. Moreover, suppose that t is the smallest positive integer such that $s_t = \pm d$, and that there exists an $r < t$ such that each $s_i = \sum_{j=1}^r \gamma_j^i$ for $i = 1, \ldots, t-1$. Then $d \equiv r \bmod t$ and $T(x) = (x^t - e)^{(d-r)/t} \prod_{j=1}^r (x - \gamma_j)$, where $e = 1$ if $s_t = d$, and $e = -1$ if $s_t = -d$.*

Proof. First, note that by the triangle inequality $|s_i| \leq d$, with equality holding if and only if $\gamma_j^i = \pm 1$ for all $j = 1, \ldots, d$. This shows that if $s_t = (-)d$, then $\gamma_j^t = (-)1$ for all $j = 1, \ldots, d$. Further, the γ_j are uniquely determined by the values $s_1, \ldots, s_d$ by (4), and the values s_{t+i} for $i \geq 0$ are uniquely determined by $s_1, \ldots, s_t$. As a result, the γ_j are uniquely determined by $s_1, \ldots, s_t$.

Next, suppose that $s_i = \sum_{j=1}^r \gamma_j^i$ for $i = 1, \ldots, t-1$, where t is the smallest positive integer such that $s_t = \pm d$. First, assume that $s_i = 0$ for $i = 1, \ldots, t-1$, and that $s_t = \pm d$. For simplicity, let us further suppose that $s_t = d$ (the other case is handled analogously). We will show that then $d \equiv 0 \bmod t$, and that $T(x) = (x^t - 1)^{d/t}$. To this end, suppose first that $d \equiv k \bmod t$, with $0 < k < t$. Let us look at (4). Because of our assumption on the s_i, we see that $\tau_{d-\ell} = 0$ if $\ell \not\equiv 0 \bmod t$, i.e., if $\tau_u \neq 0$, then $u \equiv d \bmod t$. Now, let us look at the last equation in the system (4):

$$s_d \tau_d + \cdots + s_1 \tau_1 = -d.$$

Since $s_i = 0$ for $i \not\equiv 0 \bmod t$, we have obtain $\sum_{\ell=1}^{\lfloor d/t \rfloor} s_{\ell t} \tau_{\ell t} = -d$. From the above, we see that $\tau_{\ell t} = 0$, unless $\ell t \equiv d \bmod t$, i.e., unless $d \equiv 0 \bmod t$, which does not hold by assumption. Hence, we obtain the impossible equation $0 = -d$, which contradicts the assumption $d \not\equiv 0 \bmod t$. So, we see that $d \equiv 0 \bmod t$. Further, setting $\eta_j := \gamma^{j \bmod t}$ for $j = 1, \ldots, d$, where γ is a primitive tth root of unity,

we see that the powersums of the η_j coincide with the powersums s_i, hence, up to reordering, $\gamma_j = \eta_j$ and $T(x) = \prod_{j=1}^{d}(x - \eta_j) = (x^t - 1)^{d/t}$.

If $s_t = -d$, we similarly obtain that $d \equiv 0 \bmod t$, and setting $\eta_j := \gamma^{(2j-1) \bmod 2t}$, where γ is a primitive $2t$th root of unity, shows in an analogous manner that $T(x) = (x^t + 1)^{d/t}$.

Altogether this shows that the second statement of the lemma is true if $r = 0$. In case of arbitrary r, replace d by $d - r$, and γ_j by γ_{j+r} for $j = 1, \ldots, d - r$. Then the powersums s_i of the new γ_j are 0 if $i \not\equiv 0 \bmod t$, and they are $\pm(d - r)$ otherwise. The above results then show that $\prod_{j=r+1}^{d}(x - \gamma_j) = (x^t - e)^{(d-r)/t}$, which completes the proof. □

In the remainder of this section, we will prove Theorem 2. We will frequently use the previous lemma and the terminology introduced there.

A.1 The trivial character Id

The values of Id are given by

A	B	C_i	D_i	E_1	E_{-1}	F_1	F_{-1}
1	1	1	1	1	1	1	1

Applying Lemma 2 with $d = t = 1$, $r = 0$, and $e = 1$ gives the characteristic polynomial $T(x) = x - 1$.

A.2 The Character $R_T^G(\alpha)$

For any character α of $\mathbb{F}_q^\times$, the character $R_T^G(\alpha)$ of $\mathrm{SL}_2(\mathbb{F}_q)$ is given by

A	B	C_i	D_i	E_1	E_{-1}	F_1	F_{-1}
$q+1$	$\alpha(-1)(q+1)$	$\alpha(\omega^i) + \alpha(\omega^{-i})$	0	1	1	$\alpha(-1)$	$\alpha(-1)$

Note that $R_T^G(\alpha)$ and $R_T^G(\alpha^{-1})$ are the same characters. To compute the characteristic polynomial of this character, we apply Lemma 2 to each of the conjugacy classes. In all cases $d = q + 1$, the degree of $R_T^G(\alpha)$.

On A: we have $t = 1$, since $s_1 = q + 1 = d$. As a result, $T(x) = (x - 1)^{q+1}$.

On B: here we have $t = 1$ since $s_1 = \alpha(-1)(q + 1)$. Hence, $T(x) = (x - e)^{q+1}$, where $e = \alpha(-1)$.

On C_i: the smallest t such that $s_t = \pm d$ is the smallest t such that $C_i^t \in \{A, B\}$. To compute t, we use Proposition 1. Suppose that $\nu_2(i) < \nu_2(q - 1)$. Then, by Part (h) of that proposition, $t = (q - 1)/(2\gcd(i, q - 1))$. Furthermore, in the notation of Lemma 2 $r = 2$, since s_j can be written

as the sum of two roots of unity if $C_i^j \notin \{A, B\}$. Hence, $T(x) = (x^t - e)^{(q-1)/t}(x - \eta)(x - \overline{\eta})$, where $\eta = \alpha(\omega^i)$ and $e = \alpha(-1)$. Suppose now that $\nu_2(i) = \nu_2(q-1)$. Then by Proposition 1(h) we have $t = (q-1)/\gcd(i, q-1)$, and again $r = 2$. By the previous lemma we obtain $T(x) = (x^t - 1)^{(q-1)/t}(x - \eta)(x - \overline{\eta})$.

On D_i: again, we use Proposition 1 to compute t. From part (i) of that proposition we infer that if $\nu_2(i) < \nu_2(q+1)$, then $t = (q+1)/(2\gcd(i, q+1))$. Furthermore, we clearly have $r = 0$, and so $T(x) = (x^t - e)^{(q+1)/t}$ by the previous lemma, where $e = \alpha(-1)$. If $\nu_2(i) = \nu_2(q+1)$, then by the proposition $t = (q+1)/\gcd(i, q+1)$; further, $r = 0$ and so $T(x) = (x^t - 1)^{(q+1)/t}$.

On $E_{\pm 1}$: to determine t, we use Proposition 1(d) and see that $t = q$. Further, $r = 1$, since s_j is equal to the root of unity 1, for $j < q$, and $e = 1$, since $E_{\pm 1}^t = A$. Hence, $T(x) = (x^q - 1)(x - 1)$.

On $F_{\pm 1}$: again, $t = q$ and $r = 1$, but $e = \alpha(-1)$, since $F_{\pm 1}^t = B$. So, $T(x) = (x^q - e)(x - e)$.

A.3 The Steinberg Character St

The *Steinberg character* is a q-dimensional character whose values on the various conjugacy classes is given as:

A	B	C_i	D_i	E_1	E_{-1}	F_1	F_{-1}
q	q	1	-1	0	0	0	0

In this case, $d = q$ and, since the value of the character on A and B is the same, $e = 1$.

On A and B: obviously, $t = 1$, so $r = 0$ and $T(x) = (x-1)^q$.

On C_i: by Proposition 1, if $\nu_2(i) < \nu_2(q-1)$, then $t = (q-1)/(2\gcd(i, q-1))$, otherwise $t = (q-1)/\gcd(i, q-1)$. In both cases $r = 1$ since the powersums equal 1, and $T(x) = (x-1)(x^t-1)^{(q-1)/t}$.

On D_i: by Proposition 1 $t = (q+1)/(2\gcd(i, q+1))$ if $\nu_2(i) < \nu_2(q+1)$, and $t = (q+1)/\gcd(i, q+1)$ otherwise. Further, in both cases $r = t - 1$, since $s_i = \gamma^i + \gamma^{2i} + \cdots, \gamma^{(t-1)i}$, where γ is a primitive tth root of unity. Applying the previous lemma, we obtain $T(x) = (x^t - 1)^{(q+1)/t}/(x-1)$.

On $E_{\pm 1}$ and $F_{\pm 1}$: by the previous proposition $t = q$, and obviously $r = 0$. Hence $T(x) = (x^q - 1)$.

A.4 The Character $-R_{T_s}^G(\beta)$

For any character β of the group μ_{q+1} of the $(q+1)$st roots of unity over $\mathbb{F}_q$, the character $-R_{T_s}^G(\beta)$ is defined as

A	B	C_i	D_i	E_1	E_{-1}	F_1	F_{-1}
$q-1$	$\beta(-1)(q-1)$	0	$-\beta(\theta^i) - \beta(\theta^{-i})$	-1	-1	$-\beta(-1)$	$-\beta(-1)$

.

Note that $-R_{T_s}(\beta)$ and $-R_{T_s}(\beta^{-1})$ are identical. In this case $d = q-1$.

On A: in this case $t = 1$, so $r = 0$, and $T(x) = (x-1)^{q-1}$.

On B: in this case $t = 1$, so $r = 0$. Since the value of the character on B is $\beta(-1)$ times its value on A, we have $e = \beta(-1)$, and $T(x) = (x-e)^{q-1}$.

On C_i: since the character values are all zero, we have $r = 0$. To compute t, we again use Proposition 1 to deduce that $t = (q-1)/(2\gcd(i, q-1))$ if $\nu_2(i) < \nu_2(q-1)$, in which case $T(x) = (x^t - e)^{(q-1)/t}$, where $e = \beta(-1)$. If $\nu_2(i) = \nu_2(q-1)$, then $t = (q-1)/gcd(i, q-1)$ and $T(x) = (x^t - 1)^{(q-1)/t}$.

On D_i: if $\nu_2(i) < \nu_2(q+1)$, then $t = (q+1)/(2\gcd(q+1, i))$. Note that $-\beta(\theta^i) - \beta(\theta^i)$ is the sum of all the tth roots of unity except for $\beta(\theta^i)$ and $\beta(\theta^{-i})$. Hence, $r = t-2$, and we have $T(x) = (x^t - e)^{(q+1)/t}/((x-\gamma)(x-\overline{\gamma})$ where $\gamma = \beta(\theta^i)$. If $\nu_2(i) = \nu_2(q+1)$, then we similarly obtain $r = t-2$ and $T(x) = (x^t-1)^{(q+1)/t}/((x-\gamma)(x-\overline{\gamma}))$ where $t = (q+1)/\gcd(t, q+1)$.

On $E_{\pm 1}$: in this case $t = q$. Let s_i denote the character value on $E^i_{\pm 1}$. Then $s_1 = \ldots = s_{q-1} = -1$. Note that -1 is the sum of all qth roots of unity except for 1, hence $r = q-1$ and $T(x) = (x^q - 1)/(x-1)$.

On $F_{\pm 1}$: if $e = \beta(-1) = 1$, then we are back in the previous case and $T(x) = (x^q-1)/(x-1)$. So suppose that $e = -1$. Again, let s_i denote the character value on $F^i_{\pm 1}$. Then $s_1 = \ldots = s_{q-1} = 1$. Note that 1 is the sum of all $2q$th roots of unity that are not qth roots, and are not -1. Hence, $r = q-1$ and $T(x) = (x^q+1)/(x+1)$. Altogether, we obtain in this case $T(x) = (x^q - e)/(x-e)$.

A.5 The Characters $\chi^{\varepsilon}_{\alpha_0}$

Recall that α_0 is the unique character of order 2 of $\mathbb{F}_q^{\times}$. Then, for $\varepsilon = \pm 1$, $\chi^{\varepsilon}_{\alpha_0}$ is a $(q+1)/2$-dimensional character defined as

A	B	C_i	D_i	E_1	E_{-1}	F_1	F_{-1}
$\frac{q+1}{2}$	$\alpha_0(-1)\frac{q+1}{2}$	$\alpha_0(\omega^i)$	0	η_1	$\overline{\eta}_1$	η_{-1}	$\overline{\eta}_{-1}$

where

$$\eta_i := \frac{\alpha_0(i)}{2}\left(1 + \varepsilon\alpha_0(i)\sqrt{\alpha_0(-1)q}\right), \quad \overline{\eta}_i := \frac{\alpha_0(i)}{2}\left(1 - \varepsilon\alpha_0(i)\sqrt{\alpha_0(-1)q}\right),$$

for $i = 1, -1$. In this case $d = (q+1)/2$.

On A: here $t = 1$, so $r = 0$ and, since $e = 1$, $T(x) = (x-1)^{(q+1)/2}$.

On B: again, $t = 1$ and $r = 0$. But $e = \alpha_0(-1)$, since the value of the character on B is $\alpha_0(-1)$ times its value on A. So, we have $T(x) = (x - e)^{(q+1)/2}$.

On C_i: in this case, s_j, the character value on C_i^j, equals $\alpha_0(\omega^i)^j$ if C_i^j is neither A nor B. Hence, $r = 1$. Suppose that $\nu_2(i) < \nu_2(q-1)$. Then $t = (q-1)/(2\gcd(i, q-1))$, and we obtain $T(x) = (x^t - e)^{(q-1)/t}(x - \gamma)$ where $e = \alpha_0(-1)$ and $\gamma = \alpha_0(\omega^i)$, i.e., $\gamma = 1$ if i is even, and $\gamma = -1$ otherwise. If $\nu_2(i) = \nu_2(q-1)$, then we obtain in a similar fashion $T(x) = (x^t - 1)^{(q-1)/t}(x - \gamma)$, where $t = (q-1)/\gcd(i, q-1)$.

On D_i: Here $r = 0$. Further, $t = (q+1)/(2\gcd(i, q+1))$ if $\nu_2(i) < \nu_2(q+1)$, and $T(x) = (x^t - e)^{(q+1)/(2t)}$. If $\nu_2(i) = \nu_2(q+1)$, then $t = (q+1)/\gcd(i, q+1)$, and $T(x) = (x^t - 1)^{(q+1)/(2t)}$.

To compute the characteristic polynomial of the representation on $E_{\pm 1}$ and $F_{\pm 1}$ we use the following result, due to Gauss.

Proposition 3. *Let γ be a primitive q-th root of unity where q is a prime. Then*

$$\sum_{k, \left(\frac{k}{q}\right)=1} \gamma^k = -\frac{1}{2}\left(1 - \sqrt{\alpha_0(-1)q}\right).$$

Proof. A theorem of Gauss asserts that

$$\sum_{k=1}^{p-1} \left(\frac{k}{p}\right)\gamma^k = \sqrt{\left(\frac{-1}{p}\right)p},$$

see [13, Chap. IV, Th. 211]. The result follows now by noting that $\sum_{k=1}^{p-1} \gamma^k = -1$. □

This shows that $\eta_1 = 1 + \sum_{k, \left(\frac{k}{q}\right)=\varepsilon} \gamma^k$, and $\overline{\eta}_1 = 1 + \sum_{k, \left(\frac{k}{q}\right)=-\varepsilon} \gamma^k$, since the sum of all qth roots of unity is 0.

On $E_{\pm 1}$: we have $r = (q+1)/2$, $t = q$, and the characteristic polynomial on E_i is

$$T(x) = (x - 1) \prod_{k, \left(\frac{k}{q}\right)=i\varepsilon} (x - \gamma^k).$$

On $F_{\pm 1}$: if $e = \alpha_0(-1) = 1$, then the characteristic polynomials on E_1 and on F_1 coincide, as do the characteristic polynomials on E_{-1} and F_{-1}. If $\alpha_0(-1) = -1$, an argument similar to the shows that on F_1 the characteristic polynomial is $T(x) = (x+1)\prod_{k, \left(\frac{k}{q}\right)=\varepsilon}(x + \gamma^k)$, while it is

$T(x) = (x+1)\prod_{k,\left(\frac{k}{q}\right)=-\varepsilon}(x+\gamma^k)$ on F_{-1}. Combining all these cases into a single statement, we see that the characteristic polynomial on F_i equals

$$T(x) = (x - \alpha_0(-1)) \prod_{k,\left(\frac{k}{q}\right)=i\varepsilon} (x - \alpha_0(-1)\gamma^k).$$

A.6 The Characters $\chi^{\varepsilon}_{\beta_0}$

Recall that β_0 is the unique character of order 2 of μ_{q+1}, the group of $(q+1)$st roots of unity. Then, for $\varepsilon = \pm 1$, $\chi^{\varepsilon}_{\beta_0}$ is a $(q-1)/2$-dimensional character defined as

A	B	C_i	D_i	E_1	E_{-1}	F_1	F_{-1}
$\frac{q-1}{2}$	$\beta_0(-1)^{\frac{q-1}{2}}$	0	$-\beta_0(\theta^i)$	υ_1	$\overline{\upsilon}_1$	υ_{-1}	$\overline{\upsilon}_{-1}$

where

$$\upsilon_i := \frac{\beta_0(i)}{2}\left(-1 + \varepsilon\alpha_0(i)\sqrt{\alpha_0(-1)q}\right), \quad \overline{\upsilon}_i := \frac{\beta_0(i)}{2}\left(-1 - \varepsilon\alpha_0(i)\sqrt{\alpha_0(-1)q}\right),$$

for $i = 1, -1$. In this case $d = (q-1)/2$.

On A: again, $t = 1$, $r = 0$, $e = 1$, and we have $T(x) = (x-1)^{(q-1)/2}$.

On B: as above, $t = 1$, so $r = 0$; further, $e = \beta_0(-1)$ and we have $T(x) = (x-e)^{(q-1)/2}$.

On C_i: here, $r = 0$. Further, $t = (q-1)/(2\gcd(i, q-1))$ if $\nu_2(i) < \nu_2(q-1)$, and $T(x) = (x^t - e)^{(q-1)/(2t)}$. If $\nu_2(i) = \nu_2(q-1)$, then $t = (q-1)/\gcd(i, q-1)$, and $T(x) = (x^t-1)^{(q-1)/(2t)}$.

On D_i: in this case, s_j, the character value on D_i^j, equals $\beta_0(\theta^i)^j$ if D_i^j is neither A nor B. If i is odd, then $\beta_0(\theta^i)$ is -1. Let s_j denote the character value on D_i^j. Since i is odd, $D_i^t = B$ for $t = (q+1)/(2\gcd(i, q+1))$ and we have $s_1 = 1, s_2 = -1, \ldots, s_{t-1} = (-1)^t$ and $s_t = \beta_0(-1)(q-1)/2$. We distinguish two cases. First, suppose that $\beta_0(-1) = -1$, i.e., $q \equiv 1 \bmod 4$. Let $\gamma_1, \ldots, \gamma_{t-1}$ be the $2t$th roots of unity that are neither -1 nor a tth root of unity. Then the sum of the γ_i^{2j} equals 1, if $2j < t$, and the sum of the γ_i^{2j+1} equals -1 if $2j+1 < t$. Hence, we see that $r = t-1$, and $T(x) = (x^t+1)^{(q+1)/(2t)}/(x+1)$. Next, suppose that $\beta_0(-1) = 1$, i.e., $q \equiv -1 \bmod 4$. Note that, since i is odd, $t = (q+1)/(2\gcd(i, q+1))$ is even. Let $\gamma_1, \ldots, \gamma_{t-1}$ be all the tth roots of unity except for -1. Then, it is easily seen that $s_i = \sum_j \gamma_j^i$ for $i < t$, hence $r = t-1$ and $T(x) = (x^t-1)^{(q+1)/(2t)}/(x+1)$. Altogether, in case of odd i we obtain $T(x) = (x^t-e)^{(q+1)/(2t)}/(x+1)$, where $t = (q+1)/(2\gcd(i, q+1))$.

Suppose now that i is even. Then $\beta_0(\theta^i) = 1$. Again, we distinguish two cases. First, assume

that $\beta_0(-1) = 1$, i.e., $q \equiv -1 \bmod 4$. Let s_j denote the value of the character on D_i^j. Then $s_1 = \cdots = s_{t-1} = -1$, $s_t = (q-1)/2$, where $t = (q+1)/(2\gcd(i, q+1))$ if $\nu_2(i) < \nu_2(q+1)$, and $t = (q+1)/\gcd(i, q+1)$ if $\nu_2(i) = \nu_2(q+1)$. As above, it is now easy to show that $r = t-1$ and $T(x) = (x^t-1)^{(q+1)/(2t)}/(x-1)$. On the other hand, if $\beta_0(-1) = -1$, then $q \equiv 1 \bmod 4$, hence $\nu_2(i) = \nu_2(q+1)$ since i is even. As a result, D_i^j is never equal to B, which shows that the values of the character on D_i^j equal $s_1 = \cdots = s_{t-1} = -1$, $s_t = (q-1)/2$, i.e., $T(x) = (x^t-1)^{(q+1)/(2t)}/(x-1)$, where $t = (q+1)/\gcd(i, q+1)$.

On $E_{\pm 1}$: as above, it is easy to show that the characteristic polynomial of the representation on E_i equals

$$T(x) = \prod_{k, \left(\frac{k}{q}\right) = i\varepsilon} (x - \gamma^k),$$

where γ is a primitive qth root of unity.

On $F_{\pm 1}$: suppose that $\beta_0(-1) = 1$. Then $\alpha_0(-1) = -1$, and $\upsilon_1 = (1 - \varepsilon\sqrt{-q})/2$. This value is the sum of γ^k where $\left(\frac{k}{q}\right) = -\varepsilon$. If $\beta_0(-1) = -1$, then $\upsilon_{-1} = -(1 + \varepsilon\sqrt{q})/2$ which equals the sum of $-\gamma^k$ where $\left(\frac{k}{q}\right) = \varepsilon$. Following the details outlined previously, we obtain the following characteristic polynomial on F_i:

$$T(x) = \prod_{k, \left(\frac{k}{q}\right) = \alpha_0(-1) i\varepsilon} (x + \alpha_0(-1)\gamma^k).$$

B Proof of Theorem 3

The representations of $\mathrm{SL}_2(\mathbb{F}_q)$ for odd q have been essentially computed by many authors. To make this paper as self-contained as possible, and since the description of the representations found in the literature is not as specific as in Theorem 3, we choose to rederive the computation in this appendix, following the ideas in [12].

We will derive the representation Δ as an extension of an irreducible 8-dimensional representation F of the subgroup T. To do this, we use the following simple result which, in a more general form, is contained in [12, Lemma 4.4].

Lemma 3. *Let Δ be a unitary representation of $\mathrm{SL}_2(\mathbb{F}_{17})$ affording $\chi^1_{\beta_0}$, and assume that the re-*

striction F of Δ to T is irreducible. Then, for any $u \in \mathrm{SL}_2(\mathbb{F}_{17})$ we have

$$\Delta(u) = \frac{1}{34} \sum_{t \in T} F(t) \chi^1_{\beta_0}(t^{-1}u).$$

Thus, if we can prove that F is irreducible, and if we know $F(t)$ for all $t \in T$, then we can construct Δ.

Let us first focus on proving that F is irreducible.

Lemma 4. *Let Δ be a representation of $\mathrm{SL}_2(\mathbb{F}_{17})$ affording $\chi^1_{\beta_0}$. Then $\Delta \downarrow T$ is irreducible.*

Proof. This statement is easily proved using Frobenius reciprocity. Let $\chi := \chi^1_{\beta_0}$. Recall that $\chi \downarrow T$ is irreducible if and only if

$$\frac{1}{|T|} \sum_{t \in T} \chi(t)\chi(t^{-1}) = 1.$$

To evaluate this sum, we need to compute the conjugacy classes of various elements in T. First, consider the elements

$$\begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix},$$

where a is not in $\{\pm 1\}$. This matrix is clearly conjugate to $\mathrm{diag}\,(a, a^{-1})$ since it has two different eigenvalues, so its conjugacy class is C_i for some i. Since χ vanishes on C_i, the value of χ at all such matrices is zero.

We may thus focus on matrices of the form $\pm \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$. If b is zero, then the conjugacy class of such a matrix is clear. If b is nonzero, then we easily see that

$$\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \in E_{(\frac{b}{17})}, \quad \begin{pmatrix} -1 & b \\ 0 & -1 \end{pmatrix} \in F_{(\frac{b}{17})}.$$

Consulting the character table of $\mathrm{SL}_2(\mathbb{F}_{17})$, we thus see that

$$\begin{aligned} \frac{1}{|T|} \sum_{t \in T} \chi(t)\chi(t^{-1}) &= \frac{(17-1)^2}{4} + \frac{(17-1)^2}{4} + \frac{(17-1)}{2}\upsilon_1 + \\ &\quad \frac{(17-1)}{2}\bar{\upsilon}_1 + \frac{(17-1)}{2}\upsilon_{-1} + \frac{(17-1)}{2}\bar{\upsilon}_{-1} \\ &= 1. \end{aligned}$$

This shows that $\chi \downarrow T$, and hence $\Delta \downarrow T$, is irreducible. ∎

Next, we focus on the representation theory of T. Let F be the representation of T given by

$$\begin{aligned} F\left(\begin{pmatrix} 3 & 0 \\ 0 & 6 \end{pmatrix}\right) &:= \mathrm{e}^{2\pi i/16}\begin{pmatrix} 0 & I_7 \\ 1 & 0 \end{pmatrix}, \\ F\left(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\right) &:= \mathrm{diag}\,(\gamma, \gamma^2, \gamma^{2^2}, \gamma^{2^3}, \gamma^{2^4}, \gamma^{2^5}, \gamma^{2^6}, \gamma^{2^7}), \end{aligned}$$

where $\gamma = \mathrm{e}^{2\pi i/17}$. We leave it to the reader to show that this assignment is, in fact, a representation of T, i.e., satisfies the relations in T. Further, the character of this representation coincides with $\chi^1_{\beta_0}$, hence F is indeed the restriction of a representation Δ of $\mathrm{SL}_2(\mathbb{F}_{17})$ affording $\chi^1_{\beta_0}$ to T.[1]

We can now apply Lemma 3 to compute $\Delta(g)$. For this, we need two pieces of information. First, we need to know the value of F at an arbitrary matrix in T.

Lemma 5. *Let $F(a)_{jk}$ denote the (j,k)-entry of the matrix $F(a)$, let $\gamma := e^{2\pi i/17}$, and let $\mu := e^{2\pi i/16}$.*

(1) *For $1 \le j,k \le 8$ and $0 \le x \le 15$ we have*

$$F\left(\begin{pmatrix} 3^x & b \\ 0 & 3^{-x} \end{pmatrix}\right)_{jk} = \begin{cases} 0, & \text{if } k \not\equiv j + x \bmod 8 \\ \mu^{k-j}\gamma^{b3^{j-k}2^{k-1}}, & \text{else.} \end{cases}$$

(2) *For $1 \le j,k \le 8$ we have*

$$\sum_{x=0}^{15} F\left(\begin{pmatrix} 3^x & b \\ 0 & 3^{-x} \end{pmatrix}\right)_{jk} = 2i\mu^{k-j}\mathrm{Im}(\gamma^{b3^{j-k}2^{k-1}}).$$

(3) *For $1 \le j,k \le 8$ we have*

$$\sum_{x=0}^{7} F\left(\begin{pmatrix} 3^{2x} & b \\ 0 & 3^{-2x} \end{pmatrix}\right)_{jk} = \begin{cases} 0, & \text{if } j-k \text{ odd} \\ 2i\mu^{k-j}\mathrm{Im}(\gamma^{b3^{j-k}2^{k-1}}), & \text{if } j-k \text{ even} \end{cases}$$

(4) *For $1 \le j,k \le 8$ we have*

$$\sum_{x=0}^{7} F\left(\begin{pmatrix} 3^{2x+1} & b \\ 0 & 3^{-2x+1} \end{pmatrix}\right)_{jk} = \begin{cases} 0, & \text{if } j-k \text{ even} \\ 2i\mu^{k-j}\mathrm{Im}(\gamma^{b3^{j-k}2^{k-1}}), & \text{if } j-k \text{ odd} \end{cases}$$

[1] This representation can be computed from the scratch in various ways, e.g., by realizing T as a semidirect product, or by using the action of T on the irreducible characters of B; we will not elaborate on this problem here. For completeness we mention that T is isomorphic to the group $G_{34,9}$ in the notations of [1].

Proof. (1) First, note that

$$\begin{pmatrix} 3^x & b \\ 0 & 3^{-x} \end{pmatrix} = \begin{pmatrix} 3 & 0 \\ 0 & 3^{-1} \end{pmatrix} \begin{pmatrix} 1 & b3^{-x} \\ 0 & 1 \end{pmatrix}.$$

Further, we have

$$F\left(\begin{pmatrix} 3^x & 0 \\ 0 & 3^{-x} \end{pmatrix}\right) = \mu^x \begin{pmatrix} 0 & I_{(x \bmod 8)+1} \\ I_{7-(x \bmod 8)} & 0 \end{pmatrix},$$

and

$$F\left(\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}\right) = \operatorname{diag}(\gamma^a, \gamma^{2a}, \gamma^{4a}, \ldots, \gamma^{2^7 a}),$$

where we define I_0 to be the empty matrix. Combining these statements, we obtain the assertion.

(2–4) Apply (1), keeping in mind that $\mu^{8+x} = -\mu^x$ and $3^{8+x} = -3^x$ for $x = 0, \ldots, 7$. □

The second piece of information we need to be able to apply Lemma 3 is the knowledge of the "multipliers" $\chi^1_{\beta_0}(t^{-1}g)$. This is done in the following.

Lemma 6. *Let* $t = \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \in T$, *and let* $g = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. *Then we have*

$$\chi^1_{\beta_0}(t^{-1}g) = \begin{cases} 0, & \text{if } b \in \{0, \pm 5, \pm 6, \pm 8\}, \ a \text{ arbitrary}, \\ 1, & \text{if } b \in \{1, 3, 4, -7\}, \ a \text{ arbitrary}, \\ -1 & \text{if } b \in \{-1, -3, -4, 7\}, \ a \text{ arbitrary}, \\ \upsilon_1 & \text{if } b = 2, \ \left(\frac{a}{17}\right) = 1, \\ \bar{\upsilon}_1 & \text{if } b = 2, \ \left(\frac{a}{17}\right) = -1, \\ -\upsilon_1 & \text{if } b = -2, \ \left(\frac{a}{17}\right) = 1, \\ -\bar{\upsilon}_1 & \text{if } b = -2, \ \left(\frac{a}{17}\right) = -1. \end{cases}$$

Proof. First, note that

$$\begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} b & a^{-1} \\ -a & 0 \end{pmatrix} =: M.$$

The characteristic polynomial of the matrix M on the right hand side is $X^2 - bX + 1$. If the discriminant $b^2 - 4$ of this quadratic polynomial is a nonzero square, then the matrix M has two different eigenvalues in $\mathbb{F}_{17}$, and hence it is conjugate to a matrix in C_i for some i. Since, $\chi^1_{\beta_0}$ vanishes on C_i for all i, the multipliers in this case are zero. Noting that $b^2 - 4$ is a nonzero square precisely for the values $b = \pm 4, \pm 5, \pm 8$, we obtain the first assertion.

If $b^2 - 4$ is not a square in $\mathbb{F}_{17}$, then the matrix M is diagonalizable over $\mathbb{F}_{17^2}$ but not over $\mathbb{F}_{17}$, and hence, is conjugate to a matrix in D_i for some i. Since $\chi^1_{\beta_0}(D_i) = (-1)^{i-1}$, we only need to compute the parity of i for each b such that $b^2 - 4$ is a non-square. Let θ be a root of $X^2 - bX + 1$ in $\mathbb{F}_{17^2}$. Then M belongs to D_i for and odd i if and only if $\theta^9 \neq 1$. Note that $\theta^9 = X^9 \bmod (X^2 - bX + 1)$ in $\mathbb{F}_{17}$. A short calculation shows that for $b = 1, 3, 4, -7$ we have that $M \in D_i$ for odd i; and for $b = -1, -3, -4, 7$ we have that $M \in D_i$ for even i. This takes care of the second and the third assertion.

If $b^2 - 4 = 0$, i.e., if $b = \pm 2$, then M has a double eigenvalue which is 1 in case $b = 2$, and is -1 if $b = -2$. We claim that if $b = 2$ and $\left(\frac{a}{17}\right) = 1$, then $M \in E_1$. This is immediately seen from the following identity:

$$\begin{pmatrix} 2 & a^{-1} \\ -a & 0 \end{pmatrix} \begin{pmatrix} -a^{-1} & -1 - a^{-1} \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} -a^{-1} & -1 - a^{-1} \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}.$$

Similarly, we see that if $b = 2$ and $\left(\frac{a}{17}\right) = -1$, then $M \in E_{-1}$, and if $b = -2$, then $M \in F_{\left(\frac{a}{17}\right)}$. Hence, the remaining four assertions follow from $\chi^1_{\beta_0}(E_1) = \upsilon_1$, $\chi^1_{\beta_0}(E_{-1}) = \bar{\upsilon}_1$, $\chi^1_{\beta_0}(F_1) = \upsilon_{-1} = -\upsilon_1$, and $\chi^1_{\beta_0}(F_{-1}) = \bar{\upsilon}_{-1} = -\bar{\upsilon}_1$. □

Now we are able to prove Theorem 3.

Proof. (Of Theorem 3.) By Lemma 4 the restriction F of the irreducible representation Δ affording $\chi := \chi^1_{\beta_0}$ to T is irreducible. Hence, we can use Lemma 3 to compute $\Delta(g)$.

Let $M_{a,b}$ denote the matrix $\begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix}$, and let $S_{a,b}$ denote the matrix $M^{-1}_{a,b} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Then, by Lemma 3

$$\Delta(g) = \frac{1}{34} \sum_{b \in \mathbb{F}_{17}} \sum_{a \in \mathbb{F}_{17}^\times} F(M_{a,b}) \chi(S_{a,b}).$$

We rewrite the right-hand side in the following way, using Lemma 6:

$$\begin{aligned}\Delta(g) \quad = \quad & \frac{1}{34}\sum_{b\in\{0,\pm 5,\pm 6,\pm 8\}} 0\cdot\sum_{a\in\mathbb{F}_{17}^{\times}} F(M_{a,b}) + \\ & \frac{1}{34}\sum_{b\in\{1,3,4,-7\}} \underbrace{\sum_{a\in\mathbb{F}_{17}^{\times}} [F(M_{a,b}) - F(M_{a,-b})]}_{=:I} + \\ & \frac{1}{34}\upsilon_1 \underbrace{\sum_{(\frac{a}{17})=1} [F(M_{a,2}) - F(M_{a,-2})]}_{=:II} + \\ & \frac{1}{34}\bar{\upsilon}_1 \underbrace{\sum_{(\frac{a}{17})=-1} [F(M_{a,2}) - F(M_{a,-2})]}_{=:III}.\end{aligned}$$

Let us study the (j,k)-entry of the contribution terms I, II, and III. By Lemma 5(2), the (j,k)-entry of I equals $4i\mu^{k-j}\mathrm{Im}(\gamma^{b3^{j-k}2^{k-1}}) = 4i\mu^{k-j}\mathrm{Im}(\alpha_{jk}^{b})$, in the notation of Theorem 3. Similarly, by part (3) of the same lemma, the (j,k) entry of II equals $4i\mu^{k-j}\mathrm{Im}(\alpha_{jk}^{2})$ if $j-k$ is even, and the entry is 0 otherwise. By the same token, using part (4) of the lemma shows that the (j,k) entry of III equals 0 if $j-k$ is even, and it equals $4i\mu^{j-k}\mathrm{Im}(\alpha_{jk}^{2})$ otherwise. Putting everything together, we see that the (j,k)-entry of $\Delta(g)$ equals

$$\frac{2}{17}i\mu^{j-k}\mathrm{Im}(\alpha_{jk} + \theta\alpha_{jk}^{2} + \alpha_{jk}^{3} + \alpha_{jk}^{4} - \alpha_{jk}^{7}),$$

where $\theta = \upsilon_1$ if $j-k$ is even, and it is $\bar{\upsilon}_1$ if $j-k$ is odd. This is precisely the statement of the theorem. □

	A	B	C_i
$R_T^G(\alpha)$	$(x-1)^{q+1}$	$(x-\alpha(-1))^{q+1}$	$(x^{t_i}-e_{\alpha,i,q-1})^{\frac{q-1}{t_i}}(x-\eta_{\alpha,i})(x-\overline{\eta}_{\alpha,i})$
St_G	$(x-1)^q$	$(x-1)^q$	$(x-1)(x^{t_i}-1)^{\frac{q-1}{t_i}}$
$-R_{T_s}^G(\beta)$	$(x-1)^{q-1}$	$(x-\beta(-1))^{q-1}$	$(x^{t_i}-e_{\beta,i,q-1})^{\frac{q-1}{t_i}}$
$\chi_{\alpha_0}^{\varepsilon}$	$(x-1)^{\frac{q+1}{2}}$	$(x-\alpha_0(-1))^{\frac{q+1}{2}}$	$(x^{t_i}-e_{\alpha_0,i,q-1})^{\frac{q-1}{2t_i}}(x-(-1)^i)$
$\chi_{\beta_0}^{\varepsilon}$	$(x-1)^{\frac{q-1}{2}}$	$(x-\beta_0(-1))^{\frac{q-1}{2}}$	$(x^{t_i}-e_{\beta_0,i,q-1})^{\frac{q-1}{2t_i}}$
Id_G	$(x-1)$	$(x-1)$	$(x-1)$

	D_i	E_1	E_{-1}
$R_T^G(\alpha)$	$(x^{r_i}-e_{\alpha,i,q+1})^{\frac{q+1}{r_i}}$	$(x^q-1)(x-1)$	$(x^q-1)(x-1)$
St_G	$\dfrac{(x^{r_i}-1)^{\frac{q+1}{r_i}}}{x-1}$	(x^q-1)	(x^q-1)
$-R_{T_s}^G(\beta)$	$\dfrac{(x^{r_i}-e_{\beta,i,q+1})^{\frac{q+1}{r_i}}}{(x-\eta_{\beta,i})(x-\overline{\eta}_{\beta,i})}$	$\dfrac{x^q-1}{x-1}$	$\dfrac{x^q-1}{x-1}$
$\chi_{\alpha_0}^{\varepsilon}$	$(x^{r_i}-e_{\alpha_0,i,q+1})^{\frac{q+1}{2r_i}}$	$(x-1)\prod_{\left(\frac{k}{q}\right)=\varepsilon}(x-\gamma_q^k)$	$(x-1)\prod_{\left(\frac{k}{q}\right)=-\varepsilon}(x-\gamma_q^k)$
$\chi_{\beta_0}^{\varepsilon}$	$\dfrac{(x^{r_i}-e_{\beta_0,i,q+1})^{\frac{q+1}{2r_i}}}{(x-(-1)^i)}$	$\prod_{\left(\frac{k}{q}\right)=\varepsilon}(x-\gamma_q^k)$	$\prod_{\left(\frac{k}{q}\right)=-\varepsilon}(x-\gamma_q^k)$
Id_G	$(x-1)$	$(x-1)$	$(x-1)$

	F_1	F_{-1}
$R_T^G(\alpha)$	$(x^q-\alpha(-1))(x-\alpha(-1))$	$(x^q-\alpha(-1))(x-\alpha(-1))$
St_G	(x^q-1)	(x^q-1)
$-R_{T_s}^G(\beta)$	$\dfrac{x^q-\beta(-1)}{x-\beta(-1)}$	$\dfrac{x^q-\beta(-1)}{x-\beta(-1)}$
$\chi_{\alpha_0}^{\varepsilon}$	$(x-\alpha_0(-1))\prod_{\left(\frac{k}{q}\right)=\varepsilon}(x-\alpha_0(-1)\gamma_q^k)$	$(x-\alpha_0(-1))\prod_{\left(\frac{k}{q}\right)=-\varepsilon}(x-\alpha_0(-1)\gamma_q^k)$
$\chi_{\beta_0}^{\varepsilon}$	$\prod_{\left(\frac{k}{q}\right)=\alpha_0(-1)\varepsilon}(x+\alpha_0(-1)\gamma_q^k)$	$\prod_{\left(\frac{k}{q}\right)=-\alpha_0(-1)\varepsilon}(x+\alpha_0(-1)\gamma_q^k)$
Id_G	$(x-1)$	$(x-1)$

Table 1: Characteristic polynomials of irreducible representations of $\mathrm{SL}_2(\mathbb{F}_q)$ for odd prime q on classes A, B, C_i, D_j, $i = 1, \ldots, (q-3)/2$, $j = 1, \ldots, (q-1)/2$