This paper appeared in J. Mult.-Valued Logic Soft Comput. **34** (2020), 239–259.

BASES FOR THE SPACE OF FIXED POINTS OF THE REED-MULLER-FOURIER TRANSFORM

TAMÁS WALDHAUSER

Abstract. We prove that the space of fixed points of the Reed-Muller-Fourier transform of n-variable functions on a p-element domain always has a basis. For odd p our proof is constructive and it proves the conjecture of C. Moraga, R. S. Stanković, M. Stanković and S. Stojković about the number of fixed points presented at ISMVL 2017. For even p we give a nonconstructive proof that relies on our earlier proof of the above mentioned conjecture.

1. Introduction

The Reed-Muller-Fourier transform (RMF transform, for short) was defined in [10] as a generalization of the Fourier transform of Gibbs [2] from Boolean functions to multiple-valued functions. It also coincides with the Reed-Muller transform [7, 8, 16, 17] in the Boolean case, hence it can be regarded as a common generalization of the Reed-Muller and Fourier transforms. (Note that the Reed-Muller transform has other extensions to the multiple-valued case [3].) For functions of one variable, the RMF transform also agrees with the Pascal transform [1, 4]. For more information on the RMF and other transforms we refer the reader to [11, 12, 13].

The eigenfunctions of the Reed-Muller transform of Boolean and multiple-valued functions have been studied in [9] and [6], respectively. For the RMF transform, the study of the eigenfunctions has been initiated in [5], and the following conjecture has been formulated (note that it agrees with the result of [9] for $p = 2$).

Conjecture 1 ([5])**.** For every $p \geq 2$ and $n \geq 1$, the number of fixed points of the Reed-Muller-Fourier transform of n-variable functions defined on a p-element domain is $p^{\lfloor p^n/2 \rfloor}$ if n is odd, and it is $p^{\lceil p^n/2 \rceil}$ if n is even.

We proved this conjecture for odd values of p as well as for $n = 1$ (with arbitrary p) in [15], and we settled the case of even p in [14]. This paper is an extended version of [15], so we do not include here results of [14] (which was written later than [15] and contains some more general results). Instead, we focus on the existence of bases in the space of fixed points, not merely on the number of fixed points. Our main theorem is the following.

Theorem 2. *For every $p \geq 2$ and $n \geq 1$, the space of fixed points of the Reed-Muller-Fourier transform of n-variable functions defined on a p-element domain has a basis of cardinality $\lfloor p^n/2 \rfloor$ if n is odd, and it has a basis of cardinality $\lceil p^n/2 \rceil$ if n is even.*

Clearly, Theorem 2 implies Conjecture 1. For odd values of p, our proof of Theorem 2 does indeed provide a self-contained proof for Conjecture 1. However, for even values of p we perform a kind of "reverse engineering": we use from [14]

Key words and phrases. Reed-Muller-Fourier transform, eigenvector, eigenvalue, basis, fixed point, functions of several variables.

This study was supported by the Hungarian National Research, Development and Innovation Office (NKFIH grant no. K115518).

the fact that the number of fixed points is $p^{p^n/2}$ to prove that the space of fixed points has a basis (and then it is obvious that the basis has cardinality $p^n/2$).

After presenting the required definitions and tools in Section 2, we settle the case $n = 1$ (both for odd and even p) in Section 3. Besides the fixed points (eigenfunctions with eigenvalue 1), we also consider eigenfunctions with eigenvalue -1, and we prove that both eigenspaces have bases. We show in Section 4, assuming that p is odd, how to build bases for the eigenspaces of n-variable functions corresponding to the eigenvalues 1 and -1 from one-variable functions. In Section 5 we discuss why the case of even p's is substantially different, and we give an (unfortunately nonconstructive) proof for the existence of bases in both eigenspaces.

2. Preliminaries

The Reed-Muller-Fourier transform is defined in terms of the Gibbs convolution, but it can also be given explicitly as follows. Let $T_1 = (t_{ij})_{i,j=0}^{p-1} \in \mathbb{Z}_p^{p\times p}$ be the $p \times p$ matrix over the ring $\mathbb{Z}_p$ of modulo p residue classes of integers with entries

$$t_{ij} = (-1)^{j+1} \cdot \binom{i}{j}, \tag{1}$$

using the convention $\binom{i}{j} = 0$ whenever $i < j$. As an example, see the left half of the matrix of Table 1, which shows T_1 for $p = 8$. Note that we number rows and columns starting from zero; in particular, we refer to the top row of the matrix as "row 0". Two important properties of this matrix are that it is triangular and self-inverse, i.e., $T_1^2 = I$. (Here and in the sequel, I denotes the identity matrix; the size of the matrix shall be clear from the context.) If $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$ is a one-variable function over $\mathbb{Z}_p$, then we can associate the column vector $\mathbf{v}_f = (f(0), \dots, f(p-1))^T \in \mathbb{Z}_p^p$ to f, which we shall call the value vector of f. Then the RMF transform of f is the function whose value vector is $T_1\mathbf{v}_f$. Before presenting the definition for functions of several variables (see Definitions 5 and 6), let us recall some notions of linear algebra.

Working with the RMF transform means that we deal with matrices and vectors over $\mathbb{Z}_p$. If p is a prime, then $\mathbb{Z}_p$ is a field and $\mathbb{Z}_p^m$ is a vector space over $\mathbb{Z}_p$ for every natural number m. However, if p is a composite number, then $\mathbb{Z}_p$ is not a field and $\mathbb{Z}_p^m$ is not a vector space (but a module), and in this case we cannot use all the standard linear algebraic tools. Therefore, we state precisely those definitions and facts that we shall need, and we point out what does (not) remain true when p is composite. We will still use the more familiar linear algebraic terminology, e.g., we talk about subspaces instead of submodules.

Let $\mathcal{V} = \{\mathbf{v}_1, \dots, \mathbf{v}_k\}$ be a set of (column) vectors in $\mathbb{Z}_p^m$. By a *linear combination* of $\mathcal{V}$ we mean a sum of the form $\alpha_1\mathbf{v}_1 + \dots + \alpha_k\mathbf{v}_k$ with coefficients $\alpha_1, \dots, \alpha_k \in \mathbb{Z}_p$. We say that $\mathcal{V}$ is *linearly independent* if the zero vector can be obtained from $\mathcal{V}$ only in a trivial way, i.e., $\alpha_1\mathbf{v}_1 + \dots + \alpha_k\mathbf{v}_k = \mathbf{0}$ implies $\alpha_1 = \dots = \alpha_k = 0$. Equivalently, $\mathcal{V}$ is linearly independent iff every vector of $\mathbb{Z}_p^m$ has at most one representation as a linear combination of $\mathcal{V}$. However, linear independence is not equivalent to the property that no element of $\mathcal{V}$ can be expressed as a linear combination of the others (see Example 3). If a set $U \subseteq \mathbb{Z}_p^m$ is closed under linear combinations, then U is a *subspace* of $\mathbb{Z}_p^m$. If $\mathcal{V} \subseteq U$ and every element of U is a linear combination of $\mathcal{V}$, then we say that $\mathcal{V}$ *generates* the subspace U. If in addition $\mathcal{V}$ is linearly independent, then $\mathcal{V}$ is a *basis* of U. If U has a basis of cardinality k, then every element of U has a unique representation as a linear combination of the basis vectors, hence $|U| = p^k$. This implies that every basis of U has the same size k, and in this case U is called a *k-dimensional* subspace. As the following example illustrates, a subspace does not always have a basis.

Example 3. Let $\mathbf{v}_1 = (2,0)\,,\ \mathbf{v}_2 = (0,2) \in \mathbb{Z}_4^2$. Clearly, no element of $\mathcal{V} = \{\mathbf{v}_1, \mathbf{v}_2\}$ is a linear combination of the other, yet $\mathcal{V}$ is not linearly independent, as $2\mathbf{v}_1 + 2\mathbf{v}_2 = \mathbf{0}$. The subspace generated by $\mathcal{V}$ is $U = \{\mathbf{0}, \mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_1 + \mathbf{v}_2\}$, and this subspace has no basis. In fact, no subset of U is linearly independent, not even the one-element subsets, since $2\mathbf{u} = \mathbf{0}$ holds for every $\mathbf{u} \in U$.

If $A \in \mathbb{Z}_p^{m\times m}$ is an $m \times m$ matrix and $\mathbf{v} \in \mathbb{Z}_p^m$ is a nonzero column vector such that $A\mathbf{v} = \lambda\mathbf{v}$ with some $\lambda \in \mathbb{Z}_p$, then $\mathbf{v}$ is an *eigenvector* of A and λ is the corresponding *eigenvalue*. The set of all eigenvectors corresponding to λ together with the zero vector form the *eigenspace* $U_\lambda = \left\{\mathbf{v} \in \mathbb{Z}_p^m : A\mathbf{v} = \lambda\mathbf{v}\right\}$, which is always a subspace of $\mathbb{Z}_p^m$ (but it may fail to have basis; see Example 8).

If $A = (a_{ij}) \in \mathbb{Z}_p^{m\times n}$ and $B = (b_{ij}) \in \mathbb{Z}_p^{r\times s}$ are matrices of arbitrary sizes, then their *Kronecker product* is the $mr \times ns$ block matrix

$$A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B & \cdots & a_{1n}B \\ a_{21}B & a_{22}B & \cdots & a_{2n}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1}B & a_{m2}B & \cdots & a_{mn}B \end{pmatrix}.$$

The Kronecker product is associative but not commutative, it distributes over sums, and it satisfies the following mixed product identity (for arbitrary matrices A, B, C, D of appropriate sizes so that both sides are defined):

$$(A \otimes B)\,(C \otimes D) = (AC) \otimes (BD)\,. \tag{2}$$

If $\mathbf{x} \in \mathbb{Z}_p^r$ and $\mathbf{y} \in \mathbb{Z}_p^s$ are column vectors, then we can interpret their Kronecker product $\mathbf{x} \otimes \mathbf{y}$ by regarding $\mathbf{x}$ and $\mathbf{y}$ as an $r \times 1$, respectively $s \times 1$ matrix:

$$\mathbf{x} \otimes \mathbf{y} = (x_1y_1, x_1y_2, \ldots, x_1y_s, x_2y_1, \ldots, x_ry_s)^T\,.$$

We will need the following fact about the Kronecker product of two linearly independent sets of vectors.

Fact 4. *Suppose that* $\{\mathbf{x}_1, \ldots, \mathbf{x}_k\} \subseteq \mathbb{Z}_p^r$ *and* $\{\mathbf{y}_1, \ldots, \mathbf{y}_\ell\} \subseteq \mathbb{Z}_p^s$ *are linearly independent sets of vectors. Then* $\{\mathbf{x}_i \otimes \mathbf{y}_j : i = 1, \ldots, k,\ j = 1, \ldots, \ell\} \subseteq \mathbb{Z}_p^{rs}$ *is also linearly independent.*

With the help of the Kronecker product we can now define the RMF transform for functions of several variables.

Definition 5. Let $f\colon \mathbb{Z}_p^n \to \mathbb{Z}_p$ be an n-variable function over $\mathbb{Z}_p$. The *value vector* of f is the column vector $\mathbf{v}_f \in \mathbb{Z}_p^{p^n}$ consisting of the values $f(\mathbf{x})$ listed in the lexicographic order of $\mathbf{x} \in \mathbb{Z}_p^n$:

$$\mathbf{v}_f = (f(0,0,\ldots,0)\,, f(0,0,\ldots,1)\,, \ldots, f(p-1,\ldots,p-1))^T\,.$$

Definition 6. For all natural numbers n, we define the RMF transform matrix T_n as the n-th Kronecker power of the matrix T_1 defined by (1):

$$T_n = T_1^{\otimes n} = \underbrace{T_1 \otimes \cdots \otimes T_1}_{n}.$$

The *Reed-Muller-Fourier transform* of a function $f\colon \mathbb{Z}_p^n \to \mathbb{Z}_p$ is the function $\mathrm{RMF}(f) : \mathbb{Z}_p^n \to \mathbb{Z}_p$ whose value vector is $T_n\mathbf{v}_f$:

$$\mathbf{v}_{\mathrm{RMF}(f)} = T_n\mathbf{v}_f.$$

It is not hard to verify that T_n is a triangular matrix, and the mixed product identity (2) shows that $T_1^2 = I$ implies $T_n^2 = I$.

Remark 7. The Kronecker product of vectors has the following simple "functional" interpretation. Let f and g be functions of r and s variables, respectively, and define the function $h\colon \mathbb{Z}_p^{r+s} \to \mathbb{Z}_p$ by $h(x_1, \ldots, x_{r+s}) := f(x_1, \ldots, x_r) \cdot g(x_{r+1}, \ldots, x_{r+s})$. Then we have $\mathbf{v}_h = \mathbf{v}_f \otimes \mathbf{v}_g$.

Our main objects of study are the fixed points of the RMF transformation; these are (apart from the zero vector) exactly the eigenvectors of T_n with eigenvalue 1. For arbitrary $\lambda \in \mathbb{Z}_p$, let $U_\lambda^{(n)}$ denote the eigenspace of T_n corresponding to the eigenvalue λ:

$$U_\lambda^{(n)} = \left\{ \mathbf{v} \in \mathbb{Z}_p^{p^n} : T_n \mathbf{v} = \lambda \mathbf{v} \right\}.$$

Then the number of fixed points of the RMF transform of n-variable functions on $\mathbb{Z}_p$ is $\left|U_1^{(n)}\right|$. We will see that in order to find a basis in $U_1^{(n)}$, we also need to consider the eigenspace $U_{-1}^{(n)}$. Our main results are Theorem 12 and Theorem 15, which state that the subspaces $U_1^{(n)}$ and $U_{-1}^{(n)}$ have bases, and the cardinalities of these bases will also be determined.

The existence of bases in eigenspaces is not trivial: as the following example illustrates, some eigenspaces do not have bases.

Example 8. Let us consider the eigenspaces corresponding to $\lambda = 2$ and $\lambda = 3$ for $p = 6$ and $n = 1$:

$$\begin{aligned} U_2^{(1)} &= \left\{ (x_0, -x_0, x_2, -x_0, x_4, -x_0 - x_2 + x_4) : x_0, x_2, x_4 \text{ are even} \right\}; \\ U_3^{(1)} &= \left\{ (0, x_4, x_4, x_3, x_4, x_5) : x_3, x_4, x_5 \text{ are divisible by } 3 \right\}. \end{aligned}$$

Here $U_2^{(1)}$ has size 3^3 and $U_3^{(1)}$ has size 2^3, and neither of these numbers is a power of 6, hence these two eigenspaces have no bases.

3. Functions in one variable

As an illustration, let us first consider the case $p = 8$, $n = 1$. The eigenvectors of T_1 with eigenvalue $\lambda = \pm 1$ can be found by solving $T_1 \mathbf{x} = \lambda I \mathbf{x}$ $\left(\mathbf{x} \in \mathbb{Z}_8^8\right)$, which is a system of 8 linear equations over $\mathbb{Z}_8$ with 8 unknowns. We could write this system in the form $(T_1 - \lambda I)\mathbf{x} = \mathbf{0}$, but the patterns appearing in the coefficients will be more clear if keep the system in the original form, i.e., we consider the 8×16 matrix $(T_1 \mid \lambda I)$, and, for the same reason, we do not reduce the numbers modulo 8 (see Table 1). Here, and in the following computations, one can see the matrix corresponding to $p = 7$ by ignoring the gray entries; we use this to emphasize the difference between the cases of even and odd p.

Now we start an elimination procedure. We could transform the left half of the matrix to a diagonal form, but then the right half would become too complicated. Thus one must be careful to perform "just enough" elimination so that both halves of the matrix become manageable. First we subtract from each row the row immediately above it, but we stop at row 2: we subtract row 6 from row 7, …, row 1 from row 2 (recall that we number the rows from 0 to 7). Then we obtain the matrix shown in Table 2. Next we subtract again from each row the row above it, but this time we stop already at row four: we subtract row 6 from row 7, …, row 3 from row 4 (see Table 3). Finally, we subtract row 6 from row 7 and row 5 from row 6 (see Table 4). This matrix represents a system of linear equations that is equivalent to the original system $T_1 \mathbf{x} = \lambda I \mathbf{x}$. Let us subtract the right hand side of each equation from the left hand side, so that we get a system of homogeneous linear equations corresponding to the matrix of Table 5.

Now we consider the cases $\lambda = 1$ and $\lambda = -1$ separately. If $\lambda = 1$, then our matrix is

$$\begin{pmatrix} -2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & -2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -2 & 4 & -2 & 0 & 0 & 0 \\ 0 & 0 & -1 & 2 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & -6 & 6 & -2 & 0 \\ 0 & 0 & 0 & 1 & -3 & 3 & -1 & 0 \end{pmatrix}.$$

Here every second row is the double of the next one, so we can delete them. However, if $p = 7$, then we cannot delete the last row (it is not the double of the next row, simply because the next row does not exist). Thus, we obtain the following matrices:

$$p = 8: \quad \begin{pmatrix} -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 2 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & -3 & 3 & -1 & 0 \end{pmatrix};$$

$$p = 7: \quad \begin{pmatrix} -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 2 & -1 & 0 & 0 \\ 0 & 0 & 0 & 2 & -6 & 6 & -2 \end{pmatrix}.$$

In both cases the first $4 = \lceil p/2 \rceil$ variables can be expressed uniquely from the last $\lfloor p/2 \rfloor$ variables. (Note that if $p = 7$, then we can divide the last equation by 2, as 2 is relatively prime to 7. We cannot (and do not need to) perform such a division when $p = 8$.) Thus the solutions of our systems of equations are the following:

$$p = 8: \quad \begin{cases} x_0 &= 0 \\ x_1 &= 5x_4 + 2x_5 + 2x_6 \\ x_2 &= 5x_4 + 2x_5 + 2x_6 \\ x_3 &= 3x_4 + 5x_5 + x_6 \\ x_4 &\in \mathbb{Z}_8 \\ x_5 &\in \mathbb{Z}_8 \\ x_6 &\in \mathbb{Z}_8 \\ x_7 &\in \mathbb{Z}_8 \end{cases}$$

$$p = 7: \quad \begin{cases} x_0 &= 0 \\ x_1 &= 5x_4 + x_5 + 2x_6 \\ x_2 &= 5x_4 + x_5 + 2x_6 \\ x_3 &= 3x_4 + 4x_5 + x_6 \\ x_4 &\in \mathbb{Z}_7 \\ x_5 &\in \mathbb{Z}_7 \\ x_6 &\in \mathbb{Z}_7 \end{cases}$$

From these solutions we can get a basis of $U_1^{(1)}$ by giving the value 1 to one of the free variables and 0 to the others. The size of the basis is $\lfloor p/2 \rfloor$ in both cases (see Table 6).

Now let us consider the case $\lambda = -1$. Then our matrix is

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & -3 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 4 & -5 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & -5 & 9 & -7 & 2 \end{pmatrix}.$$

Here every second row is constant 0, so we can delete them:

$$p = 8 : \quad \begin{pmatrix} -1 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & -3 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 4 & -5 & 2 & 0 & 0 \\ 0 & 0 & 0 & 1 & -5 & 9 & -7 & 2 \end{pmatrix};$$

$$p = 7 : \quad \begin{pmatrix} -1 & 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & -3 & 2 & 0 & 0 & 0 \\ 0 & 0 & -1 & 4 & -5 & 2 & 0 \end{pmatrix}.$$

In both cases the first $\lfloor p/2 \rfloor$ variables can be expressed uniquely from the last $4 = \lceil p/2 \rceil$ variables. Thus the solutions of our systems of equations are the following:

$$p = 8 : \quad \begin{cases} x_0 = 6x_4 + 4x_6 \\ x_1 = 3x_4 + 4x_5 + 6x_6 + 4x_7 \\ x_2 = 7x_4 + 6x_5 + 4x_6 \\ x_3 = 5x_4 + 7x_5 + 7x_6 + 6x_7 \\ x_4 \in \mathbb{Z}_8 \\ x_5 \in \mathbb{Z}_8 \\ x_6 \in \mathbb{Z}_8 \\ x_7 \in \mathbb{Z}_8 \end{cases}$$

$$p = 7 : \quad \begin{cases} x_0 = 6x_3 + 5x_4 + 5x_5 \\ x_1 = 3x_3 + 6x_4 + 6x_5 \\ x_2 = 4x_3 + 2x_4 + 2x_5 \\ x_3 \in \mathbb{Z}_7 \\ x_4 \in \mathbb{Z}_7 \\ x_5 \in \mathbb{Z}_7 \\ x_6 \in \mathbb{Z}_7 \end{cases}$$

From these solutions we can get a basis of $U_{-1}^{(1)}$ by giving the value 1 to one of the free variables and 0 to the others. The size of the basis is $\lceil p/2 \rceil$ in both cases (see Table 6).

One can obtain bases of $U_1^{(1)}$ and $U_{-1}^{(1)}$ in a similar manner for arbitrary p. Table 6 shows such bases for $p \leq 8$. We can see some regularities in the basis vectors; e.g., the first component is always 0 for the basis vectors for $U_1^{(1)}$, and $(0, \ldots, 0, 1)$ is included in the basis of $U_{-1}^{(1)}$ whenever p is odd, and these facts are not difficult to verify for every p. However, it is not clear how to write up a general formula for the basis vectors. Still, at least we can see a nice pattern of binomial coefficients in the $p \times 2p$ matrix that was the result of the elimination process (see Table 4). We use this observation in the next theorem to prove the existence of a basis of $U_1^{(1)}$ as well as for $U_{-1}^{(1)}$, and we also determine their cardinalities. This proves Conjecture 1 for $n = 1$.

Theorem 9. *For every $p \geq 2$, the subspaces $U_1^{(1)}, U_{-1}^{(1)} \leq \mathbb{Z}_p^p$ have bases of cardinalities $\lfloor \frac{p}{2} \rfloor$ and $\lceil \frac{p}{2} \rceil$, respectively.*

Proof. We need to determine the set of vectors $\mathbf{x} \in \mathbb{Z}_p^p$ satisfying $(T_1 - \lambda I)\,\mathbf{x} = \mathbf{0}$ for $\lambda = 1$ and for $\lambda = -1$. We apply the elimination procedure presented above to the $p \times 2p$ matrix $(T_1 \mid \lambda I)$. More precisely, we perform the following elimination steps:

- subtract row $p-2$ from row $p-1$, ..., row 1 from row 2;
- subtract row $p-2$ from row $p-1$, ..., row 3 from row 4;
- subtract row $p-2$ from row $p-1$, ..., row 5 from row 6;
- ...
- subtract row $p-2$ from row $p-1$, and if p is even, then also subtract row $p-3$ from row $p-2$.

The pattern of binomial coefficients occurring during the elimination is quite clear, so we omit the proof (which is a straightforward computation using elementary properties of binomial coefficients); we only give the formula for the entries of the matrix $(L \mid R)$ that we obtain at the end of the process (cf. Table 4):

$$\ell_{ij} = (-1)^{j+1} \cdot \binom{\lceil i/2 \rceil}{i-j} \quad \text{and} \quad r_{ij} = (-1)^{i-j} \cdot \binom{\lfloor i/2 \rfloor}{i-j} \cdot \lambda$$

for $i, j = 0, 1, \dots, p-1$. Let us mention that the above formulas also follow from Lemma 4.2 of [14], where the elimination was done at once by multiplying from the left by a suitable matrix. Subtracting the right hand side from the left hand side, we get (the system of homogeneous linear equations corresponding to) the matrix $H := L - R$ with entries

$$\begin{aligned} h_{ij} &= (-1)^{j+1} \cdot \binom{\lceil i/2 \rceil}{i-j} - (-1)^{i-j} \cdot \binom{\lfloor i/2 \rfloor}{i-j} \cdot \lambda \\ &= (-1)^{j+1} \cdot \left(\binom{\lceil i/2 \rceil}{i-j} + (-1)^{i} \cdot \binom{\lfloor i/2 \rfloor}{i-j} \cdot \lambda \right). \end{aligned} \tag{3}$$

From this point on, we treat the cases $\lambda = 1$ and $\lambda = -1$ separately.

If $\lambda = 1$ and $i = 2k$, then $h_{ij} = (-1)^{j+1} \cdot 2 \cdot \binom{k}{i-j}$ and $h_{i+1,j} = (-1)^{j+1} \cdot \left(\binom{k+1}{i+1-j} - \binom{k}{i+1-j} \right) = (-1)^{j+1} \cdot \binom{k}{i-j}$, where the last equality is justified by the basic recurrence relation of the Pascal triangle. We see that $h_{ij} = 2 \cdot h_{i+1,j}$ whenever i is even and $i < p-1$, hence we can drop the even-numbered rows from H (except for row $p-1$ when p is odd) without changing the set of solutions of the system $H\mathbf{x} = \mathbf{0}$. If p is even, then we obtain a $(p/2) \times p$ matrix of the following shape:

$$\begin{pmatrix} -1 & * & \cdots & * & * & \cdots & * \\ 0 & 1 & \cdots & * & * & \cdots & * \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & (-1)^{p/2} & * & \cdots & * \end{pmatrix}.$$

This matrix is in row echelon form, hence we can see that in the corresponding system of linear equations the last $p/2$ variables are free, and the first $p/2$ variables can be uniquely determined from the free variables. Thus $U_1^{(1)}$ has a basis of cardinality $p/2$ (the basis vectors correspond to the free variables). If p is odd, then we cannot delete the last row hence we obtain a $\lceil p/2 \rceil \times p$ matrix of the following shape:

$$\begin{pmatrix} -1 & * & \cdots & * & * & * & \cdots & * \\ 0 & 1 & \cdots & * & * & * & \cdots & * \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & (-1)^{\lfloor p/2 \rfloor} & * & * & \cdots & * \\ 0 & 0 & \cdots & 0 & (-1)^{\lceil p/2 \rceil} \cdot 2 & * & \cdots & * \end{pmatrix}.$$

Since p is odd, 2 is relatively prime to p, hence we can multiply the last row by the multiplicative inverse of 2 so that the first nonzero entry becomes ± 1. Then, similarly to the previous case, we can conclude that the last $\lfloor p/2 \rfloor$ variables are free, therefore $U_1^{(1)}$ has a basis of cardinality $\lfloor p/2 \rfloor$.

Next we assume that $\lambda = -1$. In this case (3) implies that $h_{ij} = 0$ whenever i is even, so we can delete the even-numbered rows from H (here it does not matter whether p is even or odd). The remaining rows form a $\lfloor p/2 \rfloor \times p$ matrix of the following shape:

$$\begin{pmatrix} -1 & * & \cdots & * & * & \cdots & * \\ 0 & 1 & \cdots & * & * & \cdots & * \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & (-1)^{\lfloor p/2 \rfloor} & * & \cdots & * \end{pmatrix}.$$

Just as before, this means that we have $\lceil p/2 \rceil$ free variables, hence $U_{-1}^{(1)}$ has a basis of cardinality $\lceil p/2 \rceil$. □

4. Functions over domains of odd cardinality

We use an inductive argument to determine bases in the eigenspaces $U_1^{(n)}$ and $U_{-1}^{(n)}$. The initial step of the induction is provided by Theorem 9. In the induction step we will rely on the fact that $\mathbb{Z}_p^{p^n}$ is the direct sum of $U_1^{(n)}$ and $U_{-1}^{(n)}$, which is true unfortunately only when p is odd (see Section 5). In general, we say that $\mathbb{Z}_p^m$ is the *direct sum* of the subspaces U and $\tilde{U}$ (notation: $\mathbb{Z}_p^m = U \oplus \tilde{U}$) if $\mathbb{Z}_p^m = U + \tilde{U}$ and $U \cap \tilde{U} = \{\mathbf{0}\}$. There are several characterizations of direct sum decompositions of vector spaces over fields; however, we must take special care when applying these, since if p is not a prime, then $\mathbb{Z}_p$ is not a field, and some subspaces of $\mathbb{Z}_p^m$ do not even have a basis. Therefore, we provide the proof of the following lemma, even though it consists of very standard arguments of linear algebra.

Lemma 10. *If $\mathbb{Z}_p^m$ is the direct sum of the subspaces U and $\tilde{U}$, then the following hold.*

(i) *Every element of $\mathbb{Z}_p^m$ can be uniquely written as a sum of a vector from U and a vector from $\tilde{U}$.*

(ii) *If $\mathcal{B}$ is a basis of U and $\tilde{\mathcal{B}}$ is a basis of $\tilde{U}$, then $\mathcal{B} \cup \tilde{\mathcal{B}}$ is a basis of $\mathbb{Z}_p^m$.*

(iii) *If $\mathcal{B} \subseteq U$, $\tilde{\mathcal{B}} \subseteq \tilde{U}$, and $\mathcal{B} \cup \tilde{\mathcal{B}}$ is a basis of $\mathbb{Z}_p^m$, then $\mathcal{B}$ is a basis of U and $\tilde{\mathcal{B}}$ is a basis of $\tilde{U}$.*

Proof. Suppose that $\mathbb{Z}_p^m = U \oplus \tilde{U}$. By definition, this immediately implies that $\mathbb{Z}_p^m = U + \tilde{U}$, thus every $\mathbf{v} \in \mathbb{Z}_p^m$ can be written as $\mathbf{v} = \mathbf{u} + \tilde{\mathbf{u}}$ with $\mathbf{u} \in U, \tilde{\mathbf{u}} \in \tilde{U}$. Assume that $\mathbf{v} = \mathbf{w} + \tilde{\mathbf{w}}$ is another such decomposition of $\mathbf{v}$ with $\mathbf{w} \in U, \tilde{\mathbf{w}} \in \tilde{U}$. Then we have $\mathbf{u} - \mathbf{w} = \tilde{\mathbf{w}} - \tilde{\mathbf{u}} \in U \cap \tilde{U} = \{\mathbf{0}\}$, as the left hand side belongs to U and the right hand side belongs to $\tilde{U}$. We can conclude that $\mathbf{u} = \mathbf{w}$ and $\tilde{\mathbf{u}} = \tilde{\mathbf{w}}$, and this proves (i).

For (ii), let $\mathcal{B} = \{\mathbf{u}_1, \ldots, \mathbf{u}_r\}$ be a basis of U and let $\tilde{\mathcal{B}} = \{\tilde{\mathbf{u}}_1, \ldots, \tilde{\mathbf{u}}_s\}$ be a basis of $\tilde{U}$. From $\mathbb{Z}_p^m = U + \tilde{U}$ it follows that $\mathcal{B} \cup \tilde{\mathcal{B}}$ generates $\mathbb{Z}_p^m$. To prove linear independence, assume that $\alpha_1\mathbf{u}_1 + \cdots + \alpha_r\mathbf{u}_r + \tilde{\alpha}_1\tilde{\mathbf{u}}_1 + \cdots + \tilde{\alpha}_s\tilde{\mathbf{u}}_s = \mathbf{0}$ for some $\alpha_i, \tilde{\alpha}_j \in \mathbb{Z}_p$. Then we have $\alpha_1\mathbf{u}_1 + \cdots + \alpha_r\mathbf{u}_r = -\tilde{\alpha}_1\tilde{\mathbf{u}}_1 - \cdots - \tilde{\alpha}_s\tilde{\mathbf{u}}_s \in U \cap \tilde{U} = \{\mathbf{0}\}$, hence $\alpha_1\mathbf{u}_1 + \cdots + \alpha_r\mathbf{u}_r = \mathbf{0}$ and $\tilde{\alpha}_1\tilde{\mathbf{u}}_1 + \cdots + \tilde{\alpha}_s\tilde{\mathbf{u}}_s = \mathbf{0}$. Since $\mathcal{B}$ is linearly independent, $\alpha_1\mathbf{u}_1 + \cdots + \alpha_r\mathbf{u}_r = \mathbf{0}$ implies that $\alpha_1 = \cdots = \alpha_r = 0$, and similarly we have $\tilde{\alpha}_1 = \cdots = \tilde{\alpha}_s = 0$.

In order to prove (iii), let us assume that $\mathcal{B} = \{\mathbf{u}_1, \ldots, \mathbf{u}_r\} \subseteq U$ and $\tilde{\mathcal{B}} = \{\tilde{\mathbf{u}}_1, \ldots, \tilde{\mathbf{u}}_s\} \subseteq \tilde{U}$ such that $\mathcal{B} \cup \tilde{\mathcal{B}}$ is a basis of $\mathbb{Z}_p^m$. Then $\mathcal{B} \cup \tilde{\mathcal{B}}$ is linearly independent, thus $\mathcal{B}$ and $\tilde{\mathcal{B}}$ are linearly independent, too. It remains to prove that $\mathcal{B}$ generates U and $\tilde{\mathcal{B}}$ generates $\tilde{U}$. For arbitrary $\mathbf{u} \in U$, we have $\mathbf{u} = \alpha_1\mathbf{u}_1 + \cdots + \alpha_r\mathbf{u}_r + \tilde{\alpha}_1\tilde{\mathbf{u}}_1 + \cdots + \tilde{\alpha}_s\tilde{\mathbf{u}}_s$ with suitable coefficients $\alpha_i, \tilde{\alpha}_j \in \mathbb{Z}_p$, as $\mathcal{B} \cup \tilde{\mathcal{B}}$ generates $\mathbb{Z}_p^m$. Now $\mathbf{u} - \alpha_1\mathbf{u}_1 - \cdots - \alpha_r\mathbf{u}_r = \tilde{\alpha}_1\tilde{\mathbf{u}}_1 + \cdots + \tilde{\alpha}_s\tilde{\mathbf{u}}_s \in U \cap \tilde{U} = \{\mathbf{0}\}$, hence $\mathbf{u} - \alpha_1\mathbf{u}_1 - \cdots - \alpha_r\mathbf{u}_r = \mathbf{0}$. Therefore, $\mathbf{u} = \alpha_1\mathbf{u}_1 + \cdots + \alpha_r\mathbf{u}_r$, i.e., $\mathcal{B}$ indeed generates U. An analogous argument shows that $\tilde{\mathcal{B}}$ generates $\tilde{U}$, and this completes the proof. □

Lemma 11. *For every odd $p \geq 2$ and $n \geq 1$, we have $\mathbb{Z}_p^{p^n} = U_1^{(n)} \oplus U_{-1}^{(n)}$, i.e., each element of $\mathbb{Z}_p^{p^n}$ can be expressed uniquely in the form $\mathbf{u}^+ + \mathbf{u}^-$ with $\mathbf{u}^+ \in U_1^{(n)}, \mathbf{u}^- \in U_{-1}^{(n)}$.*

Proof. First we prove that $\mathbb{Z}_p^{p^n} = U_1^{(n)} + U_{-1}^{(n)}$. For arbitrary $\mathbf{u} \in \mathbb{Z}_p^{p^n}$, let $\mathbf{u}^+ = \frac{1}{2}(\mathbf{u} + T_n\mathbf{u})$ and $\mathbf{u}^- = \frac{1}{2}(\mathbf{u} - T_n\mathbf{u})$. Here $\frac{1}{2}$ denotes the multiplicative inverse of 2 modulo p (it exists, because 2 and p are relatively prime). Clearly, we have $\mathbf{u} = \mathbf{u}^+ + \mathbf{u}^-$; moreover, $\mathbf{u}^+ \in U_1^{(n)}$, $\mathbf{u}^- \in U_{-1}^{(n)}$ follow from the fact that $T_n^2 = I$:

$$
\begin{aligned}
T_n\mathbf{u}^+ &= \frac{1}{2}\left(T_n\mathbf{u} + T_n^2\mathbf{u}\right) = \frac{1}{2}\left(T_n\mathbf{u} + \mathbf{u}\right) = \mathbf{u}^+;\\
T_n\mathbf{u}^- &= \frac{1}{2}\left(T_n\mathbf{u} - T_n^2\mathbf{u}\right) = \frac{1}{2}\left(T_n\mathbf{u} - \mathbf{u}\right) = -\mathbf{u}^-.
\end{aligned}
$$

Now assume that $\mathbf{w} \in U_1^{(n)} \cap U_{-1}^{(n)}$. Then we have $T_n\mathbf{w} = \mathbf{w} = -\mathbf{w}$, hence $2\mathbf{w} = 0$. Since p is odd, $\mathbf{w} = 0$ follows, and this proves that $U_1^{(n)} \cap U_{-1}^{(n)} = \{\mathbf{0}\}$. □

Using the above lemma, we can now prove that $U_1^{(n)}$ and $U_{-1}^{(n)}$ have bases, and we can determine the sizes of their bases. Note that in the induction step we need to use the induction hypothesis for both $U_1^{(n)}$ and $U_{-1}^{(n)}$, thus we have to treat the two cases in parallel.

Theorem 12. *For every odd $p \geq 2$ and $n \geq 1$, the subspaces $U_1^{(n)}$ and $U_{-1}^{(n)}$ have bases $\mathcal{B}_1^{(n)}$ and $\mathcal{B}_{-1}^{(n)}$ respectively, such that $\mathcal{B}_1^{(n)} \cup \mathcal{B}_{-1}^{(n)}$ is a basis of $\mathbb{Z}_p^{p^n}$. The sizes of the bases are*

$$
\left|\mathcal{B}_1^{(n)}\right| = \begin{cases} \lfloor p^n/2 \rfloor, & \text{if } n \text{ is odd,}\\ \lceil p^n/2 \rceil, & \text{if } n \text{ is even;} \end{cases}
$$

$$
\left|\mathcal{B}_{-1}^{(n)}\right| = \begin{cases} \lceil p^n/2 \rceil, & \text{if } n \text{ is odd,}\\ \lfloor p^n/2 \rfloor, & \text{if } n \text{ is even.} \end{cases}
$$

Proof. We prove the theorem by induction on n. For the initial step $n = 1$, Theorem 9 guarantees that there exist bases $\mathcal{B}_1^{(1)}$ of $U_1^{(1)}$and $\mathcal{B}_{-1}^{(n)}$ of $U_{-1}^{(1)}$; moreover, we have and $\left|\mathcal{B}_1^{(1)}\right| = \left\lfloor \frac{p}{2} \right\rfloor$ and $\left|\mathcal{B}_{-1}^{(1)}\right| = \left\lceil \frac{p}{2} \right\rceil$. Lemma 10 and Lemma 11 show that $\mathcal{B}_1^{(1)} \cup \mathcal{B}_{-1}^{(1)}$ is indeed a basis of $\mathbb{Z}_p^p$.

For the induction step, assume that $\mathcal{B}_1^{(n)}$ is a basis of $U_1^{(n)}$ and $\mathcal{B}_{-1}^{(n)}$ is a basis of $U_{-1}^{(n)}$, as stated in the theorem; in particular, $\mathcal{B}_1^{(n)} \cup \mathcal{B}_{-1}^{(n)}$ is a basis of $\mathbb{Z}_p^{p^n}$. Let us put

$$\begin{aligned}\mathcal{B}_1^{(n+1)} &:= \left(\mathcal{B}_1^{(n)} \otimes \mathcal{B}_1^{(1)}\right) \cup \left(\mathcal{B}_{-1}^{(n)} \otimes \mathcal{B}_{-1}^{(1)}\right) \quad \text{and} \\ \mathcal{B}_{-1}^{(n+1)} &:= \left(\mathcal{B}_1^{(n)} \otimes \mathcal{B}_{-1}^{(1)}\right) \cup \left(\mathcal{B}_{-1}^{(n)} \otimes \mathcal{B}_1^{(1)}\right).\end{aligned}$$

We are going to prove that these are bases in $U_1^{(n+1)}$ and $U_{-1}^{(n+1)}$, respectively. It follows from the mixed product identity (2) that if $T_n\mathbf{u} = \lambda\mathbf{u}$ and $T_1\mathbf{v} = \mu\mathbf{v}$, then

$$\begin{aligned}T_{n+1}\left(\mathbf{u} \otimes \mathbf{v}\right) &= \left(T_n \otimes T_1\right)\left(\mathbf{u} \otimes \mathbf{v}\right) = \left(T_n\mathbf{u}\right) \otimes \left(T_1\mathbf{v}\right) \\ &= \lambda\mathbf{u} \otimes \mu\mathbf{v} = \lambda\mu\left(\mathbf{u} \otimes \mathbf{v}\right).\end{aligned}$$

Therefore, $\mathcal{B}_1^{(n+1)} \subseteq U_1^{(n+1)}$ and $\mathcal{B}_{-1}^{(n+1)} \subseteq U_{-1}^{(n+1)}$.

By Fact 4, the system of vectors

$$\mathcal{B}_1^{(n+1)} \cup \mathcal{B}_{-1}^{(n+1)} = \left(\mathcal{B}_1^{(n)} \cup \mathcal{B}_{-1}^{(n)}\right) \otimes \left(\mathcal{B}_1^{(1)} \cup \mathcal{B}_{-1}^{(1)}\right) \subseteq \mathbb{Z}_p^{p^{n+1}}$$

is linearly independent, since, by the induction hypothesis, $\mathcal{B}_1^{(n)} \cup \mathcal{B}_{-1}^{(n)}$ is a basis of $\mathbb{Z}_p^{p^n}$ and $\mathcal{B}_1^{(1)} \cup \mathcal{B}_{-1}^{(1)}$ is a basis of $\mathbb{Z}_p^p$. The cardinality of $\mathcal{B}_1^{(n+1)} \cup \mathcal{B}_{-1}^{(n+1)}$ is

$$\left|\mathcal{B}_1^{(n+1)} \cup \mathcal{B}_{-1}^{(n+1)}\right| = \left|\mathcal{B}_1^{(n)} \cup \mathcal{B}_{-1}^{(n)}\right| \cdot \left|\mathcal{B}_1^{(1)} \cup \mathcal{B}_{-1}^{(1)}\right| = p^n \cdot p = p^{n+1}.$$

Clearly, any linearly independent system of p^{n+1} vectors in $\mathbb{Z}_p^{p^{n+1}}$ is a basis of $\mathbb{Z}_p^{p^{n+1}}$, as p^{n+1} is the dimension of $\mathbb{Z}_p^{p^{n+1}}$. Thus we can conclude that $\mathcal{B}_1^{(n+1)} \cup \mathcal{B}_{-1}^{(n+1)}$ is a basis of $\mathbb{Z}_p^{p^{n+1}}$. Now Lemma 10 and Lemma 11 imply that $\mathcal{B}_1^{(n+1)}$ is a basis of $U_1^{(n+1)}$ and $\mathcal{B}_{-1}^{(n+1)}$ is a basis of $U_{-1}^{(n+1)}$.

To finish the proof, we need to compute the cardinalities of these two bases. If n is even, then we have, by the induction hypothesis

$$\begin{aligned}\left|\mathcal{B}_1^{(n+1)}\right| &= \left|\mathcal{B}_1^{(n)}\right| \cdot \left|\mathcal{B}_1^{(1)}\right| + \left|\mathcal{B}_{-1}^{(n)}\right| \cdot \left|\mathcal{B}_{-1}^{(1)}\right| \\ &= \left\lceil \frac{p^n}{2} \right\rceil \cdot \left\lfloor \frac{p}{2} \right\rfloor + \left\lfloor \frac{p^n}{2} \right\rfloor \cdot \left\lceil \frac{p}{2} \right\rceil = \left\lfloor \frac{p^{n+1}}{2} \right\rfloor,\end{aligned}$$

$$\begin{aligned}\left|\mathcal{B}_{-1}^{(n+1)}\right| &= \left|\mathcal{B}_1^{(n)}\right| \cdot \left|\mathcal{B}_{-1}^{(1)}\right| + \left|\mathcal{B}_{-1}^{(n)}\right| \cdot \left|\mathcal{B}_1^{(1)}\right| \\ &= \left\lceil \frac{p^n}{2} \right\rceil \cdot \left\lceil \frac{p}{2} \right\rceil + \left\lfloor \frac{p^n}{2} \right\rfloor \cdot \left\lfloor \frac{p}{2} \right\rfloor = \left\lceil \frac{p^{n+1}}{2} \right\rceil.\end{aligned}$$

Similarly, if n is odd, then we have

$$\begin{aligned}\left|\mathcal{B}_1^{(n+1)}\right| &= \left|\mathcal{B}_1^{(n)}\right| \cdot \left|\mathcal{B}_1^{(1)}\right| + \left|\mathcal{B}_{-1}^{(n)}\right| \cdot \left|\mathcal{B}_{-1}^{(1)}\right| \\ &= \left\lfloor \frac{p^n}{2} \right\rfloor \cdot \left\lfloor \frac{p}{2} \right\rfloor + \left\lceil \frac{p^n}{2} \right\rceil \cdot \left\lceil \frac{p}{2} \right\rceil = \left\lceil \frac{p^{n+1}}{2} \right\rceil,\end{aligned}$$

$$\begin{aligned}\left|\mathcal{B}_{-1}^{(n+1)}\right| &= \left|\mathcal{B}_1^{(n)}\right| \cdot \left|\mathcal{B}_{-1}^{(1)}\right| + \left|\mathcal{B}_{-1}^{(n)}\right| \cdot \left|\mathcal{B}_1^{(1)}\right| \\ &= \left\lfloor \frac{p^n}{2} \right\rfloor \cdot \left\lceil \frac{p}{2} \right\rceil + \left\lceil \frac{p^n}{2} \right\rceil \cdot \left\lfloor \frac{p}{2} \right\rfloor = \left\lfloor \frac{p^{n+1}}{2} \right\rfloor.\end{aligned}$$

□

Remark 13. The proof of Theorem 12 provides a method to construct the bases of $U_1^{(n)}$ and $U_{-1}^{(n)}$ explicitly from the bases of $U_1^{(1)}$ and $U_{-1}^{(1)}$. Let us illustrate this in the case of $p = 3$. From Table 6 we see that $U_1^{(1)}$ has a basis $\{u\}$ and $U_{-1}^{(1)}$ has a basis $\{v, w\}$, where the functions u, v, w are defined on $\mathbb{Z}_3$ as follows:

$$\begin{aligned} u(0) &= 0, & u(1) &= 1, & u(2) &= 1; \\ v(0) &= 2, & v(1) &= 1, & v(2) &= 0; \\ w(0) &= 0, & w(1) &= 0, & w(2) &= 1. \end{aligned}$$

A basis of $U_1^{(2)}$ can be given by

$$\big(\{u\} \otimes \{u\}\big) \cup \big(\{v, w\} \otimes \{v, w\}\big) = \{u \otimes u, v \otimes v, v \otimes w, w \otimes v, w \otimes w\},$$

where the Kronecker products can be computed by Remark 7 (for example, $v \otimes w$ is the two-variable function $v(x_1) \cdot w(x_2)$). Similarly, $U_{-1}^{(1)}$ has the basis

$$\big(\{u\} \otimes \{v, w\}\big) \cup \big(\{v, w\} \otimes \{u\}\big) = \{u \otimes v, u \otimes w, v \otimes u, w \otimes u\}.$$

In general, the functions $g_1(x_1) \cdot \ldots \cdot g_n(x_n)$ with $g_i \in \{u, v, w\}$ constitute a basis of all n-variable functions over $\mathbb{Z}_3$; those with an even number of g_i-s belonging to $\{v, w\}$ form a basis of $U_1^{(n)}$, while those with an odd number of g_i-s belonging to $\{v, w\}$ form a basis of $U_{-1}^{(n)}$.

5. Functions over domains of even cardinality

If p is even, then the direct sum decomposition given in Lemma 11 is not valid. Indeed, we have

$$U_1^{(n)} \cap U_{-1}^{(n)} = \left\{\mathbf{v} \in \mathbb{Z}_p^{p^n} : T_n\mathbf{v} = \mathbf{v} = -\mathbf{v}\right\} = \left\{\mathbf{v} \in \mathbb{Z}_p^{p^n} : T_n\mathbf{v} = \mathbf{v} \text{ and } 2\mathbf{v} = \mathbf{0}\right\}.$$

Thus $U_1^{(n)} \cap U_{-1}^{(n)}$ consists of those fixed points whose components are all divisible by $p/2$, and this set contains nonzero vectors. For example, with $p = 6$ and $n = 1$ we have

$$U_1^{(1)} \cap U_{-1}^{(1)} = \big\{(0, -x_4, -x_4, x_3, x_4, x_5) : x_3, x_4, x_5 \text{ are divisible by } 3\big\}.$$

This subspace does not even have a basis (its cardinality is 2^3, which is not a power of 6). It is not true either that $U_1^{(n)} + U_{-1}^{(n)} = \mathbb{Z}_p^{p^n}$; again, in the case $p = 6$, $n = 1$ we have

$$U_1^{(1)} + U_{-1}^{(1)} = \big\{(x_0, x_1, x_2, x_3, x_4, x_5) : x_0 \text{ is even, and } x_1 \equiv x_2 \equiv x_4 \pmod 2\big\},$$

and this subspace has no basis either (its cardinality is $3^3 \cdot 6^3$).

The method of constructing bases in $U_1^{(n)}$ and $U_{-1}^{(n)}$ with the help of Kronecker products outlined in Remark 13 does not work either if p is even. For example, let us consider the bases $\mathcal{B}_1^{(1)}$and $\mathcal{B}_{-1}^{(1)}$ of $U_1^{(1)}$ and $U_{-1}^{(1)}$, respectively, given in Table 6 for $p = 4$. Then $\big(\mathcal{B}_1^{(1)} \otimes \mathcal{B}_1^{(1)}\big) \cup \big(\mathcal{B}_{-1}^{(1)} \otimes \mathcal{B}_{-1}^{(1)}\big)$ consists of the following eight vectors in $\mathbb{Z}_4^{16}$:

$$\begin{gathered} (0,0,0,0,0,1,1,0,0,1,1,0,0,0,0,0); \\ (0,0,0,0,0,0,0,1,0,0,0,1,0,0,0,0); \\ (0,0,0,0,0,0,0,0,0,0,0,0,0,1,1,0); \\ (0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1); \\ (0,2,2,0,2,1,3,0,2,3,1,0,0,0,0,0); \\ (0,0,0,2,0,2,0,3,0,2,0,1,0,0,0,0); \\ (0,0,0,0,0,2,2,0,0,0,0,0,2,3,1,0); \\ (0,0,0,0,0,0,0,2,0,0,0,0,0,2,0,1). \end{gathered}$$

This system of vectors is linearly dependent (consider, for instance, their linear combination with all coefficients equal to 2), hence it cannot be a basis in $U_1^{(2)}$.

Due to these difficulties, we can only give a nonconstructive proof for the existence of a basis in $U_1^{(n)}$ and $U_{-1}^{(n)}$ when p is even. We will use Theorem 5.1 of [14] that tells us that if these subspaces have bases, then the bases are of cardinality $p^n/2$.

Lemma 14. *Let p be an even natural number, and let $Q \in \mathbb{Z}_p^{p/2 \times p/2}$ be the matrix formed by the entries in the lower left quarter of T_1:*

$$q_{ij} = (-1)^{j+1} \cdot \binom{i+p/2}{j} \qquad (i,j = 0,1,\ldots,p/2-1)\,.$$

Then Q has an inverse matrix in the ring $\mathbb{Z}_p^{p/2 \times p/2}$.

Proof. Let us consider the integer matrices A and B of size $p/2 \times p/2$ defined by

$$a_{ij} = \binom{i}{j}, \qquad b_{ij} = (-1)^{j+1} \cdot \binom{p/2}{j-i} \qquad (i,j = 0,1,\ldots,p/2-1)\,.$$

Note that A is lower triangular (it is actually the Pascal matrix), B is upper triangular, and the diagonal entries in both matrices are ±1. This implies that they have unit determinant, and consequently their inverses contain only integer entries. Therefore, A and B are also invertible over $\mathbb{Z}_p$. To prove our lemma, it suffices to verify that $AB = Q$. Let us illustrate this equality for $p = 10$:

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 2 & 1 & 0 & 0 \\ 1 & 3 & 3 & 1 & 0 \\ 1 & 4 & 6 & 4 & 1 \end{pmatrix} \cdot \begin{pmatrix} -1 & 5 & -10 & 10 & -5 \\ 0 & 1 & -5 & 10 & -10 \\ 0 & 0 & -1 & 5 & -10 \\ 0 & 0 & 0 & 1 & -5 \\ 0 & 0 & 0 & 0 & -1 \end{pmatrix} = \begin{pmatrix} -1 & 5 & -10 & 10 & -5 \\ -1 & 6 & -15 & 20 & -15 \\ -1 & 7 & -21 & 35 & -35 \\ -1 & 8 & -28 & 56 & -70 \\ -1 & 9 & -36 & 84 & -126 \end{pmatrix}.$$

The (i,j) entry of AB is

$$\sum_{k=0}^{p/2-1} a_{ik} \cdot b_{kj} = \sum_{k=0}^{p/2-1} \binom{i}{k} \cdot (-1)^{j+1} \cdot \binom{p/2}{j-k} = (-1)^{j+1} \cdot \sum_{k=0}^{i} \binom{i}{k} \cdot \binom{p/2}{j-k}.$$

Thus we need to prove that

$$\sum_{k=0}^{i} \binom{i}{k} \cdot \binom{p/2}{j-k} = \binom{i+p/2}{j}. \tag{4}$$

This identity has an easy combinatorial interpretation. If we have i black balls and $p/2$ white balls, then we can choose j balls in $\binom{i+p/2}{j}$ many ways. On the other hand, we may choose first k black balls for some $k \in \{0,1,\ldots,i\}$ in $\binom{i}{k}$ many ways, and then we can choose $j-k$ white balls in $\binom{p/2}{j-k}$ many ways. This shows that the number of choices is given by the left hand side of (4), and this completes the proof. □

Theorem 15. *For every even $p \geq 2$ and $n \geq 1$, the subspaces $U_1^{(n)}$ and $U_{-1}^{(n)}$ have bases of size $p^n/2$.*

Proof. The subspace $U_\lambda^{(n)}$ is the set of all solutions of $(T_n - \lambda I)\,\mathbf{x} = \mathbf{0}$. This is a system of p^n linear equations in p^n unknowns. Let us consider only the $p^n/2$ equations that correspond to the bottom half of the matrix $T_n - \lambda I$, and let $\hat{U}_\lambda^{(n)}$ denote the solution set of this system of equations. Clearly, we have $\hat{U}_\lambda^{(n)} \supseteq U_\lambda^{(n)}$. We will prove that $\hat{U}_\lambda^{(n)}$ has a basis of cardinality $p^n/2$ for every $\lambda \in \mathbb{Z}_p$, and we will also prove that if $\lambda = 1$ or $\lambda = -1$, then $\hat{U}_\lambda^{(n)} = U_\lambda^{(n)}$.

Let us consider the following schematic view of the matrix $T_n - \lambda I$:

$$\begin{array}{|c|c|}\hline \multicolumn{2}{|c|}{} \\ \hline L & R \\ \hline \end{array}$$

We have split the bottom half of $T_n - \lambda I$ into two submatrices $L, R \in \mathbb{Z}_p^{p^n/2 \times p^n/2}$. Note that $L = Q \otimes T_{n-1}$, where Q is the matrix considered in Lemma 14 (the matrix L does not include any diagonal entries of $T_n - \lambda I$, hence λ does not occur in L). Lemma 14 and the mixed product identity (2) imply that L is invertible in $\mathbb{Z}_p^{p^n/2 \times p^n/2}$, namely, $L^{-1} = Q^{-1} \otimes T_{n-1}^{-1} = Q^{-1} \otimes T_{n-1}$.

Let us split the column vector $\mathbf{x} \in \mathbb{Z}_p^{p^n}$ also into two parts: $\mathbf{x} = (\mathbf{y}, \mathbf{z})$ with $\mathbf{y} = \left(x_0, \ldots, x_{p^n/2-1}\right)$, $\mathbf{z} = \left(x_{p^n/2}, \ldots, x_{p^n-1}\right)$. Now we can write $\hat{U}_\lambda^{(n)}$ in the following form:

$$\hat{U}_\lambda^{(n)} = \{(\mathbf{y}, \mathbf{z}) : L\mathbf{y} + R\mathbf{z} = \mathbf{0}\} = \{(\mathbf{y}, \mathbf{z}) : L\mathbf{y} = -R\mathbf{z}\} = \left\{(\mathbf{y}, \mathbf{z}) : \mathbf{y} = -L^{-1}R\mathbf{z})\right\}.$$

This means that we can treat the variables in $\mathbf{z}$ as free variables, and we can express the variables in $\mathbf{y}$ uniquely from these free variables. Therefore, $\hat{U}_\lambda^{(n)}$ has a basis of cardinality $p^n/2$ (the basis vectors can be obtained by assigning the value 1 to one of the free variables and 0 to the others, just as we did in Section 3). Consequently, we have $\left|\hat{U}_\lambda^{(n)}\right| = p^{p^n/2}$. On the other hand, we know from [14] that $\left|U_\lambda^{(n)}\right| = p^{p^n/2}$ for $\lambda = \pm 1$. Taking into account that $\hat{U}_\lambda^{(n)} \supseteq U_\lambda^{(n)}$, we can conclude that $\hat{U}_\lambda^{(n)} = U_\lambda^{(n)}$, thus the basis of $\hat{U}_\lambda^{(n)}$ is also a basis of $U_\lambda^{(n)}$ for $\lambda = \pm 1$. □

References

1. M. F. Aburdene and T. J. Goodman, *The discrete Pascal transform and its applications*, IEEE Signal Processing Letters **12** (2005), no. 7, 493–495.
2. J. E. Gibbs, *Instant Fourier transform*, Electronics Letters **13** (1977), no. 5, 122–123.
3. D. H. Green and I. S. Taylor, *Multiple-valued switching circuit design by means of generalised Reed-Muller expansions*, Digital Process. **2** (1976), no. 1, 63–81.
4. C. Moraga, R. S. Stanković, and M. Stanković, *The Pascal triangle (1654), the Reed-Muller-Fourier transform (1992), and the discrete Pascal transform (2005)*, Proc. 46th IEEE International Symposium on Multiple-Valued Logic (ISMVL), 2016, pp. 229–234.
5. C. Moraga, R. S. Stanković, M. Stanković, and S. Stojković, *On fixed points of the Reed-Muller-Fourier transform*, Proc. 47th IEEE International Symposium on Multiple-Valued Logic (ISMVL), 2017, pp. 55–60.
6. C. Moraga, S. Stojković, and R. Stanković, *On fixed points and cycles in the Reed Muller domain*, Proc. 38th IEEE International Symposium on Multiple Valued Logic (ISMVL), 2008, pp. 82–87.
7. D. E. Muller, *Application of Boolean algebra to switching circuit design and to error detection*, Transactions of the IRE Professional Group on Electronic Computers **EC-3** (1954), no. 3, 6–12.
8. I. Reed, *A class of multiple-error-correcting codes and the decoding scheme*, Transactions of the IRE Professional Group on Information Theory **4** (1954), no. 4, 38–49.
9. T. Sasao and J. T. Butler, *The eigenfunction of the Reed-Muller transformation*, Proc. Workshop on Applications of the Reed Muller Expansion in Circuit Design and Representations and Methodology of Future Computing Technology, 2007, pp. 31–38.
10. R. S. Stanković, *Some remarks on Fourier transform and differential operators for digital functions*, Proc. 22nd IEEE International Symposium on Multiple-Valued Logic (ISMVL), 1992, pp. 365–370.
11. ———, *The Reed-Muller-Fourier transform—computing methods and factorizations*, Claudio Moraga: A Passion for Multi-Valued Logic and Soft Computing (R. Seising and H. Allende-Cid, eds.), Studies in Fuzziness and Soft Computing, vol. 349, Springer, 2017, pp. 121–151.
12. R. S. Stanković, J. T. Astola, and C. Moraga, *Representation of multiple-valued logic functions*, Synthesis Lectures on Digital Circuits and Systems, vol. 37, Morgan & Claypool, 2012.

13. R. S. Stanković, C. Moraga, and J. T. Astola, *Reed-Muller expressions in the previous decade*, Journal of Multiple-Valued Logic and Soft Computing **10** (2004), no. 1, 5–28.

14. T. Waldhauser, *On eigenvectors of the Pascal and Reed-Muller-Fourier transforms*, Acta Cybernetica **23** (2018), no. 3, 959–979.

15. ———, *On the number of fixed points of the Reed-Muller-Fourier transform*, Proc. 48th IEEE International Symposium on Multiple-Valued Logic (ISMVL), May 2018, pp. 229–234.

16. I. I. Zhegalkin, *On the techniques of calculating sentences in symbolic logic*, Math. Sb. **34** (1927), 9–28, Russian.

17. ———, *Arithmetic representations for symbolic logic*, Math. Sb. **35** (1928), 311–377, Russian.

(T. Waldhauser) Bolyai Institute, University of Szeged, Aradi vértanúk tere 1, H–6720 Szeged, Hungary

Email address: `twaldha@math.u-szeged.hu`

Table 1. The matrix $(T_1 \mid \lambda I)$ for $p = 8$ and for $p = 7$

$$\left(\begin{array}{cccccccc|cccccccc}
-1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \lambda & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
-1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \lambda & 0 & 0 & 0 & 0 & 0 & 0 \\
-1 & 2 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \lambda & 0 & 0 & 0 & 0 & 0 \\
-1 & 3 & -3 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \lambda & 0 & 0 & 0 & 0 \\
-1 & 4 & -6 & 4 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \lambda & 0 & 0 & 0 \\
-1 & 5 & -10 & 10 & -5 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \lambda & 0 & 0 \\
-1 & 6 & -15 & 20 & -15 & 6 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \lambda & 0 \\
-1 & 7 & -21 & 35 & -35 & 21 & -7 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \lambda
\end{array}\right)$$

Table 2. The matrix $(T_1 \mid \lambda I)$ for $p = 8$ and for $p = 7$, after the first elimination step

$$\left(\begin{array}{cccccccc|cccccccc}
-1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \lambda & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
-1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \lambda & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & -\lambda & \lambda & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & -2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & -\lambda & \lambda & 0 & 0 & 0 & 0 \\
0 & 1 & -3 & 3 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & -\lambda & \lambda & 0 & 0 & 0 \\
0 & 1 & -4 & 6 & -4 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & -\lambda & \lambda & 0 & 0 \\
0 & 1 & -5 & 10 & -10 & 5 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & -\lambda & \lambda & 0 \\
0 & 1 & -6 & 15 & -20 & 15 & -6 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & -\lambda & \lambda
\end{array}\right)$$

Table 3. The matrix $(T_1 \mid \lambda I)$ for $p = 8$ and for $p = 7$, after the second elimination step

$$\left(\begin{array}{cccccccc|cccccccc}
-1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \lambda & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
-1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \lambda & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & -\lambda & \lambda & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & -2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & -\lambda & \lambda & 0 & 0 & 0 & 0 \\
0 & 0 & -1 & 2 & -1 & 0 & 0 & 0 & 0 & 0 & \lambda & -2\lambda & \lambda & 0 & 0 & 0 \\
0 & 0 & -1 & 3 & -3 & 1 & 0 & 0 & 0 & 0 & 0 & \lambda & -2\lambda & \lambda & 0 & 0 \\
0 & 0 & -1 & 4 & -6 & 4 & -1 & 0 & 0 & 0 & 0 & 0 & \lambda & -2\lambda & \lambda & 0 \\
0 & 0 & -1 & 5 & -10 & 10 & -5 & 1 & 0 & 0 & 0 & 0 & 0 & \lambda & -2\lambda & \lambda
\end{array}\right)$$

Table 4. The matrix $(T_1 \mid \lambda I)$ for $p = 8$ and for $p = 7$, after the third elimination step

$$\left(\begin{array}{cccccccc|cccccccc}
-1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \lambda & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
-1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \lambda & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & -\lambda & \lambda & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & -2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & -\lambda & \lambda & 0 & 0 & 0 & 0 \\
0 & 0 & -1 & 2 & -1 & 0 & 0 & 0 & 0 & 0 & \lambda & -2\lambda & \lambda & 0 & 0 & 0 \\
0 & 0 & -1 & 3 & -3 & 1 & 0 & 0 & 0 & 0 & 0 & \lambda & -2\lambda & \lambda & 0 & 0 \\
0 & 0 & 0 & 1 & -3 & 3 & -1 & 0 & 0 & 0 & 0 & -\lambda & 3\lambda & -3\lambda & \lambda & 0 \\
0 & 0 & 0 & 1 & -4 & 6 & -4 & 1 & 0 & 0 & 0 & 0 & -\lambda & 3\lambda & -3\lambda & \lambda
\end{array}\right)$$

TABLE 5. The matrix $T_1 - \lambda I$ for $p = 8$ and for $p = 7$, after the elimination procedure

$$\begin{pmatrix}
-1-\lambda & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
-1 & 1-\lambda & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1+\lambda & -1-\lambda & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & -2+\lambda & 1-\lambda & 0 & 0 & 0 & 0 \\
0 & 0 & -1-\lambda & 2+2\lambda & -1-\lambda & 0 & 0 & 0 \\
0 & 0 & -1 & 3-\lambda & -3+2\lambda & 1-\lambda & 0 & 0 \\
0 & 0 & 0 & 1+\lambda & -3-3\lambda & 3+3\lambda & -1-\lambda & 0 \\
0 & 0 & 0 & 1 & -4+\lambda & 6-3\lambda & -4+3\lambda & 1-\lambda
\end{pmatrix}$$

TABLE 6. Eigenspaces of T_1 for $p \leq 8$

	basis of $U_1^{(1)}$	basis of $U_{-1}^{(1)}$	size of $U_\lambda^{(1)}$
$p = 2$	$(0, 1)$	$(0, 1)$	$\lambda = 1:\ 2$
$p = 3$	$(0, 1, 1)$	$(2, 1, 0)$ $(0, 0, 1)$	$\lambda = 1:\ 3$ $\lambda = 2:\ 9$
$p = 4$	$(0, 1, 1, 0)$ $(0, 0, 0, 1)$	$(2, 3, 1, 0)$ $(0, 2, 0, 1)$	$\lambda = 1:\ 16$ $\lambda = 2:\ 1$ $\lambda = 3:\ 16$
$p = 5$	$(0, 2, 2, 1, 0)$ $(0, 4, 4, 0, 1)$	$(1, 3, 1, 0, 0)$ $(1, 3, 0, 1, 0)$ $(0, 0, 0, 0, 1)$	$\lambda = 1:\ 25$ $\lambda = 2:\ 1$ $\lambda = 3:\ 1$ $\lambda = 4:\ 125$
$p = 6$	$(0, 2, 2, 1, 0, 0)$ $(0, 5, 5, 0, 1, 0)$ $(0, 0, 0, 0, 0, 1)$	$(2, 4, 4, 1, 0, 0)$ $(0, 3, 1, 0, 1, 0)$ $(0, 0, 2, 0, 0, 1)$	$\lambda = 1:\ 216$ $\lambda = 2:\ 27$ $\lambda = 3:\ 8$ $\lambda = 4:\ 27$ $\lambda = 5:\ 216$
$p = 7$	$(0, 5, 5, 3, 1, 0, 0)$ $(0, 1, 1, 4, 0, 1, 0)$ $(0, 2, 2, 1, 0, 0, 1)$	$(6, 3, 4, 1, 0, 0, 0)$ $(5, 6, 2, 0, 1, 0, 0)$ $(5, 6, 2, 0, 0, 1, 0)$ $(0, 0, 0, 0, 0, 0, 1)$	$\lambda = 1:\ 343$ $\lambda = 2:\ 1$ $\lambda = 3:\ 1$ $\lambda = 4:\ 1$ $\lambda = 5:\ 1$ $\lambda = 6:\ 2401$
$p = 8$	$(0, 5, 5, 3, 1, 0, 0, 0)$ $(0, 2, 2, 5, 0, 1, 0, 0)$ $(0, 2, 2, 1, 0, 0, 1, 0)$ $(0, 0, 0, 0, 0, 0, 0, 1)$	$(6, 3, 7, 5, 1, 0, 0, 0)$ $(0, 4, 6, 7, 0, 1, 0, 0)$ $(4, 6, 4, 7, 0, 0, 1, 0)$ $(0, 4, 0, 6, 0, 0, 0, 1)$	$\lambda = 1:\ 4096$ $\lambda = 2:\ 1$ $\lambda = 3:\ 4096$ $\lambda = 4:\ 1$ $\lambda = 5:\ 4096$ $\lambda = 6:\ 1$ $\lambda = 7:\ 4096$