This paper appeared in Acta Cybernetica **23** (2018), 959–979.

ON EIGENVECTORS OF THE PASCAL AND REED-MULLER-FOURIER TRANSFORMS

TAMÁS WALDHAUSER

Dedicated to the memory of Csanád Imreh

Abstract. In their paper at the International Symposium on Multiple-Valued Logic in 2017, C. Moraga, R. S. Stanković, M. Stanković and S. Stojković presented a conjecture for the number of fixed points (i.e., eigenvectors with eigenvalue 1) of the Reed-Muller-Fourier transform of functions of several variables in multiple-valued logic. We will prove this conjecture, and we will generalize it in two directions: we will deal with other transforms as well (such as the discrete Pascal transform and more general triangular self-inverse transforms), and we will also consider eigenvectors corresponding to other eigenvalues.

1. Introduction

In multiple-valued logic, one of the main objects of study is functions of several variables defined on a finite set of logical values. If the number of values is h, then it is natural to represent them as elements of $\mathbb{Z}_h$, the ring of residue classes of integers modulo h, so that arithmetical operations can be performed. The case $h = 2$ corresponds to Boolean functions, which can be represented by polynomials over the two-element field $\mathbb{Z}_2$. This Reed-Muller representation [**?**, **?**] of Boolean functions (also discovered earlier by Zhegalkin [**?**, **?**]) has several generalizations to the multiple-valued case, one of them being the Reed-Muller-Fourier transform [**?**], which is also an extension of the instant Fourier transform of Gibbs [**?**]. We give the definition of the Reed-Muller-Fourier transform in Section 2; and for more information, we refer the reader to [**?**, **?**, **?**].

Aburdene and Goodman defined a seemingly unrelated transform, the so-called discrete Pascal transform [**?**], which has applications in image and signal processing [**?**, **?**, **?**]. It was noticed in [**?**] that the above two transforms are strongly related: the Reed-Muller-Fourier transform of one-variable functions is essentially the same as the Pascal transform (see Section 2 for details).

A common feature of the two transforms is that they can be given by lower triangular self-inverse matrices over $\mathbb{Z}_h$, i.e., they are of the form $\mathbf{v} \mapsto S\mathbf{v}$, where $\mathbf{v} \in \mathbb{Z}_h^N$, and $S \in \mathbb{Z}_h^{N\times N}$ is a lower triangular matrix such that $S^2 = I_N$. This implies that if $\mathbf{v}$ is an eigenvector corresponding to the eigenvalue λ, then $\mathbf{v} = S^2\mathbf{v} = \lambda^2\mathbf{v}$. Therefore, it is natural to consider eigenvalues λ such that $\lambda^2 = 1$, although other eigenvalues might also exist (see Example 2.1 and Table 8). The self-inverse property means that the (permutation of $\mathbb{Z}_h^N$ induced by the) transform consists of cycles of length 2 and 1; therefore, the number of fixed points completely determines the cycle structure.

The eigenfunctions of the Reed-Muller transform of Boolean and multiple-valued functions were examined in [**?**] and [**?**], respectively. For the Reed-Muller-Fourier transform, the study of the eigenfunctions was initiated in [**?**], and the following conjecture was formulated about the number of fixed points (note that it agrees with the result of [**?**] for $h = 2$).

Key words and phrases. Reed-Muller-Fourier transform, discrete Pascal transform, eigenvector, eigenvalue, fixed point, multiple-valued logic, functions of several variables.

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

Conjecture 1.1 ([**?**])**.** For all natural numbers $h \geq 2$ and $n \geq 1$, the number of fixed points of the Reed-Muller-Fourier transform of n-variable functions defined on an h-element domain is $h^{\lfloor h^n/2 \rfloor}$ if n is odd, and it is $h^{\lceil h^n/2 \rceil}$ if n is even.

The main goal of this study is to prove the above conjecture, and, more generally, determine the number of eigenvectors corresponding to eigenvalues λ with $\lambda^2 = 1$. After presenting the required definitions and tools in Section 2, we will prove in Section 3 that if h is odd and $\lambda \in \mathbb{Z}_h$ satisfies $\lambda^2 = 1$, then the number of eigenvectors corresponding to the eigenvalue λ of an arbitrary triangular self-inverse matrix $S \in \mathbb{Z}_h^{N \times N}$ depends only on the diagonal entries of S (Theorem 3.1). This result already proves Conjecture 1.1 for odd h. Let us add that this case was also settled in [**?**] using a different method. The results of [**?**] also indicate that the space of fixed points has a basis, which is not true for arbitrary subspaces of $\mathbb{Z}_h^N$ (see Example 2.1). The proof presented here does not provide the existence of a basis, but it is simpler and more general than the proof in [**?**].

One can easily find examples showing that if h is even, then it is not sufficient to know the diagonal entries of S in order to determine the number of eigenvectors. Therefore, in sections 4 and 5 we deal with the Pascal transform and the Reed-Muller-Fourier transform separately. The main results are Theorem 4.1 and Theorem 5.1, which give the number of eigenvectors of these transforms corresponding to eigenvalues λ such that $\lambda^2 = 1$. As a corollary, we get the number of fixed points of the Reed-Muller-Fourier transform (Corollary 5.1), which in turn proves Conjecture 1.1.

2. Preliminaries

We will work with vectors and matrices over $\mathbb{Z}_h$, the ring of integers modulo h (with $h \geq 2$); thus, our methods will be of a linear algebraic flavor. However, if h is a composite number, then $\mathbb{Z}_h$ is not a field, and $\mathbb{Z}_h^N$ is not a vector space, but just a module, and some familiar facts from linear algebra do not hold in this case. Nevertheless, we will use the more familiar linear algebraic terminology; for instance, we will talk about subspaces instead of submodules. By a *subspace* of $\mathbb{Z}_h^N$ we mean a set $U \subseteq \mathbb{Z}_h^N$ that is closed under *linear combinations*, i.e., $\alpha_1 \mathbf{u}_1 + \cdots + \alpha_k \mathbf{u}_k \in U$ for all $\mathbf{u}_1, \ldots, \mathbf{u}_k \in U$ and $\alpha_1, \ldots, \alpha_k \in \mathbb{Z}_h$. Example 2.1 demonstrates that there exist subspaces that do not have a basis. If a subspace U does have a basis of cardinality d, then $|U| = h^d$, since every element of U can be expressed uniquely as a linear combination of the basis vectors. This shows that the size of the basis (if it exists) is uniquely determined.

We shall not make any sharp distinction between an integer $a \in \mathbb{Z}$ and the modulo h residue class $a \in \mathbb{Z}_h$ containing a; we will use the same notation for them, but the context should make it clear which one is meant. If, occasionally, we need to use residues with respect to a modulus different from h, then we will write congruence instead of equality, indicating the modulus explicitly. We will use the following elementary fact without further mention: A linear equation $ax = b$ has a solution $x \in \mathbb{Z}_h$ if and only if $\gcd(a, h)$ divides b, and then the number of solutions is $\gcd(a, h)$. In particular, an element $a \in \mathbb{Z}_h$ has a multiplicative inverse if and only if a and h are relatively prime, and the inverse is unique. Consequently, if the determinant of a matrix $S \in \mathbb{Z}_h^{N \times N}$ is relatively prime to h, then S has an inverse matrix $S^{-1} \in \mathbb{Z}_h^{N \times N}$. In particular, if S is a (lower or upper) triangular matrix such that each entry on its diagonal is ± 1, then S has an inverse.

We say that a nonzero vector $\mathbf{u} \in \mathbb{Z}_h^N$ is an *eigenvector* of $S \in \mathbb{Z}_h^{N \times N}$ corresponding to the *eigenvalue* $\lambda \in \mathbb{Z}_h$, if $S\mathbf{u} = \lambda \mathbf{u}$. (Here, and in the sequel, all vectors will be considered as column vectors.) The set of all eigenvectors corresponding to λ together with the zero vector $\mathbf{0}$ form the *eigenspace* $U_\lambda(S) = \{\mathbf{u} \in \mathbb{Z}_h^N : S\mathbf{u} = \lambda \mathbf{u}\} \leq \mathbb{Z}_h^N$. (We will often omit the matrix S from the notation, when there is no risk of ambiguity.)

Let P_N be the matrix obtained by arranging the first N rows of the Pascal triangle in a lower triangular matrix with every second column multiplied by -1 (see Table 1).

Formally,

$$P_N = (p_{ij})_{i,j=0}^{N-1} \in \mathbb{Z}_h^{N\times N}, \text{ where } p_{ij} = (-1)^j \cdot \binom{i}{j}.$$

Note that we start the numbering of rows and columns by zero; in particular, we refer to the top row of a matrix as "row 0 ". The *discrete Pascal transform* is simply the linear transformation $\mathbb{Z}_h^N \to \mathbb{Z}_h^N$, $\mathbf{u} \mapsto P_N\mathbf{u}$ induced by the matrix P_N. It is not hard to see that P_N is a *self-inverse* matrix, i.e., $S_N^2 = I_N$, where I_N denotes the $N \times N$ identity matrix.

For the definition of the Reed-Muller-Fourier transform, we need the notion of the Kronecker product of matrices. If $A = (a_{ij}) \in \mathbb{Z}_h^{m\times n}$ and $B = (b_{ij}) \in \mathbb{Z}_h^{r\times s}$ 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 is distributive 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):

$$(A \otimes B)(C \otimes D) = (AC) \otimes (BD). \tag{1}$$

We will need the following technical lemma about eigenspaces of certain Kronecker products.

Lemma 2.1. *Let p be a prime number, and let $A \in \mathbb{Z}_p^{n\times n}$ be a lower triangular matrix such that every diagonal entry of A is 1. Then for every square matrix $B \in \mathbb{Z}_p^{m\times m}$ and $\lambda \in \mathbb{Z}_p$, we have the following inequality between the dimensions of the eigenspaces of B and of $A \otimes B$:*

$$\dim U_\lambda(A \otimes B) \le n \cdot \dim U_\lambda(B).$$

Proof. We are working over $\mathbb{Z}_p$, which is a field, so we can use standard linear algebra; in particular, we can speak of the dimension of a subspace, as every subspace has a basis. Let us denote the rank of the matrix $B - \lambda I_m$ by r. Note that the eigenspace $U_\lambda(B)$ is the kernel (nullspace) of $B - \lambda I_m$, and its dimension is called the nullity of $B - \lambda I_m$. The so-called rank-nullity theorem asserts that the sum of the rank and the nullity of $B - \lambda I_m$ equals m, thus $\dim U_\lambda(B) = \dim\ker(B - \lambda I_m) = m - r$.

Since $\operatorname{rank}(B - \lambda I_m) = r$, one can choose rows $i_1, \ldots, i_r$ and columns $j_1, \ldots, j_r$ of $B - \lambda I_m$ such that the $r \times r$ submatrix S of $B - \lambda I_m$ that is formed by the intersections of these rows and columns has a nonzero determinant. Let us choose the corresponding rows of $A \otimes B - \lambda I_{nm}$ in each "copy" of B:

$$i_1, \ldots, i_r,\ i_1 + m, \ldots, i_r + m, \ldots, i_1 + (n-1)\,m, \ldots, i_r + (n-1)\,m.$$

Similarly, let us choose the following columns:

$$j_1, \ldots, j_r,\ j_1 + m, \ldots, j_r + m, \ldots, j_1 + (n-1)\,m, \ldots, j_r + (n-1)\,m.$$

The intersections of these rows and columns of $A \otimes B - \lambda I_{nm}$ (see the gray squares in Figure 1) form an $nr \times nr$ submatrix $\tilde{S}$ that has the following structure (each 0_r denotes an $r \times r$ zero matrix):

$$\tilde{S} = \begin{pmatrix} S & 0_r & \cdots & 0_r \\ * & S & \cdots & 0_r \\ \vdots & \vdots & \ddots & \vdots \\ * & * & \cdots & S \end{pmatrix}. \tag{2}$$

The assumption that each entry on the diagonal of A is 1 implies that $A \otimes B$ has n copies of B on its diagonal, hence $A \otimes B - \lambda I_{nm}$ has n copies of $B - \lambda I_m$ on its diagonal. Therefore, $\tilde{S}$ indeed has n copies of S on its diagonal, as shown in (2).

We see that the matrix $A \otimes B - \lambda I_{nm}$ has the $nr \times nr$ submatrix $\tilde{S}$ with $\det(\tilde{S}) = \det(S)^n \neq 0$, hence $\operatorname{rank}(A \otimes B - \lambda I_{nm}) \geq nr$. Using the rank-nullity theorem for $A \otimes B - \lambda I_{nm}$, we see that

$$\begin{aligned}\dim U_\lambda(A \otimes B) &= \dim \ker(A \otimes B - \lambda I_{nm}) \\ &= nm - \operatorname{rank}(A \otimes B - \lambda I_{nm}) \\ &\leq nm - nr = n(m-r) = n \cdot \dim U_\lambda(B).\end{aligned}$$

□

Let $T_h = -P_h$ (see Table 2), and let $T_h^{\otimes n} \in \mathbb{Z}_h^{h^n \times h^n}$ be the n-fold Kronecker product of T_h with itself: $T_h^{\otimes n} = T_h \otimes \cdots \otimes T_h$ (see tables 3, 4 and 5 for some examples). The entries of T_h are

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

for an explicit formula for the entries of $T_h^{\otimes n}$, see the proof of Proposition 2.1 below. The mixed product identity (1) shows that $T_h^{\otimes n}$ is also a self-inverse matrix.

Listing all values of an n-variable function $f\colon \mathbb{Z}_h^n \to \mathbb{Z}_h$, we obtain a vector of length h^n, which uniquely determines f. More precisely, let us define the *value vector* of f as the column vector $\mathbf{v}_f \in \mathbb{Z}_h^{h^n}$ consisting of the values $f(\mathbf{x})$ listed in the lexicographic order of $\mathbf{x} \in \mathbb{Z}_h^n$:

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

The *Reed-Muller-Fourier transform* of f is then defined as the unique function $\operatorname{RMF}(f) : \mathbb{Z}_h^n \to \mathbb{Z}_h$ whose value vector is $T_h^{\otimes n}\mathbf{v}_f$:

$$\mathbf{v}_{\operatorname{RMF}(f)} = T_h^{\otimes n}\mathbf{v}_f.$$

Lucas' theorem about binomial coefficients modulo a prime implies that if h is a prime number, then the relationship between the Reed-Muller-Fourier transform and the Pascal transform stated in [**?**] for $n = 1$ holds in fact for every n.

Proposition 2.1. *If h is a prime number, then $T_h^{\otimes n} = (-1)^n \cdot P_{h^n}$ for all natural numbers n.*

Proof. Let us consider the representation of $i, j \in \{0, 1, \ldots, h^n - 1\}$ in the h-ary number system: $i = i_0 + i_1 h + \cdots + i_{n-1}h^{n-1}$ and $j = j_0 + j_1 h + \cdots + j_{n-1}h^{n-1}$, where $i_k, j_k \in \{0, 1, \ldots, h-1\}$ for $k = 0, 1, \ldots, n-1$. It follows from the definition of the Kronecker product that $\left(T_h^{\otimes n}\right)_{ij} = t_{i_0 j_0} \cdot t_{i_1 j_1} \cdot \ldots \cdot t_{i_{n-1} j_{n-1}}$. Therefore,

$$\begin{aligned}\left(T_h^{\otimes n}\right)_{ij} &= (-1)^{j_0+1} \cdot \binom{i_0}{j_0} \cdot (-1)^{j_1+1} \cdot \binom{i_1}{j_1} \cdot \ldots \cdot (-1)^{j_{n-1}+1} \cdot \binom{i_{n-1}}{j_{n-1}} \\ &= (-1)^{j_0+j_1+\cdots+j_{n-1}+n} \cdot \binom{i_0}{j_0} \cdot \binom{i_1}{j_1} \cdot \ldots \cdot \binom{i_{n-1}}{j_{n-1}}.\end{aligned}$$

By a theorem of Lucas ([**?**], see also [**?**]), if h is a prime, then the product of binomial coefficients in the above formula is congruent to $\binom{i}{j}$ modulo h. Thus, we have

$$\left(T_h^{\otimes n}\right)_{ij} = (-1)^n \cdot (-1)^{j_0+j_1+\cdots+j_{n-1}} \cdot \binom{i}{j}.$$

Now if h is odd, then $j = j_0 + j_1 h + \cdots + j_{n-1}h^{n-1} \equiv j_0 + j_1 + \cdots + j_{n-1} \pmod 2$, hence $\left(T_h^{\otimes n}\right)_{ij} = (-1)^n \cdot (-1)^j \cdot \binom{i}{j} = (-1)^n \cdot p_{ij}$, as claimed. If $h = 2$, then $1 \equiv -1 \pmod h$, so the signs do not matter at all in this case, hence $\left(T_h^{\otimes n}\right)_{ij} = \binom{i}{j} = (-1)^n \cdot p_{ij}$. □

We will study the number of eigenvectors of the Pascal and Reed-Muller-Fourier transforms, and, more generally of self-inverse triangular matrices. If $S \in \mathbb{Z}_h^{N \times N}$ is a self-inverse matrix and $\mathbf{0} \neq \mathbf{u} \in \mathbb{Z}_h^N$ is an eigenvector of S corresponding to the eigenvalue $\lambda \in \mathbb{Z}_h$, then $\mathbf{u} = S^2\mathbf{u} = \lambda S\mathbf{u} = \lambda^2\mathbf{u}$. Now if h is a prime number, then this implies that $\lambda^2 = 1$. As the next example shows, if h is a composite number, then there might be eigenvalues λ such that $\lambda^2 \neq 1$.

Example 2.1. The eigenspace $U_3 \leq \mathbb{Z}_6^6$ of the matrix T_6 corresponding to the eigenvalue $\lambda = 3$ is

$$U_3 = \{(0, a, a, b, a, c) : a, b, c \in \{0, 3\}\}.$$

This eigenspace has 8 elements, which is not a power of $h = 6$, hence U_3 does not have a basis.

One can see other examples in Table 8, which lists the sizes of the eigenspaces of T_h for $h \leq 12$. In contrast, we will consider only λ eigenvalues with $\lambda^2 = 1$. This certainly includes the cases $\lambda = 1$ (fixed points) and $\lambda = -1$, but in general there might be more such eigenvalues (for example, if $h = 12$, then $\lambda = 5$ and $\lambda = 7$ also satisfy $\lambda^2 = 1$). It was proved in [**?**] that if h is odd, then $\mathbb{Z}_h^{h^n}$ has a basis consisting of eigenvectors of $T_h^{\otimes n}$ corresponding to the eigenvalues 1 and -1. If h is a prime (i.e., if $\mathbb{Z}_h$ is a field), then this implies that there are no other eigenvalues. However, as we can see in Table 8, if h is a composite number, then this is not true: for $h = 9$ there exists eigenvectors corresponding to $\lambda = 2$, 4, 5, 7.

3. Triangular self-inverse transforms over domains of odd size

If h is odd and $S \in \mathbb{Z}_h^{N \times N}$ is a triangular self-inverse matrix, then we can get a quite general formula for the number of eigenvectors of S corresponding to an eigenvalue $\lambda \in \mathbb{Z}_h$ with $\lambda^2 = 1$. Actually, the size of the eigenspace depends only on the diagonal entries of S (and, of course, on h and λ as well). The key observation is that $\mathbb{Z}_h^N$ is the direct sum of the subspaces U_λ and $U_{-\lambda}$.

Lemma 3.1. *Assume that h is odd and S is an $N \times N$ matrix over $\mathbb{Z}_h$ such that $S^2 = I_N$. If $\lambda \in \mathbb{Z}_h$ and $\lambda^2 = 1$, then $\mathbb{Z}_h^N$ is the direct sum of the eigenspaces of S corresponding to the eigenvalues λ and $-\lambda$, i.e., $\mathbb{Z}_h^N = U_\lambda \oplus U_{-\lambda}$.*

Proof. For arbitrary $\mathbf{v} \in \mathbb{Z}_h^N$, let $\mathbf{v}^+ = \frac{1}{2}(\mathbf{v} + \lambda S\mathbf{v})$ and $\mathbf{v}^- = \frac{1}{2}(\mathbf{v} - \lambda S\mathbf{v})$. Note that these expressions are well defined, because h is odd, thus 2 has a multiplicative inverse in $\mathbb{Z}_h$. Clearly, we have $\mathbf{v} = \mathbf{v}^+ + \mathbf{v}^-$; moreover, $\mathbf{v}^+ \in U_\lambda$ and $\mathbf{v}^- \in U_{-\lambda}$ follow from the fact that $S^2 = I_N$ and $\lambda^2 = 1$:

$$S\mathbf{v}^+ = \frac{1}{2}\left(S\mathbf{v} + \lambda S^2\mathbf{v}\right) = \frac{1}{2}\left(\lambda^2 S\mathbf{v} + \lambda\mathbf{v}\right) = \lambda\mathbf{v}^+;$$
$$S\mathbf{v}^- = \frac{1}{2}\left(S\mathbf{v} - \lambda S^2\mathbf{v}\right) = \frac{1}{2}\left(\lambda^2 S\mathbf{v} - \lambda\mathbf{v}\right) = -\lambda\mathbf{v}^-.$$

This means that $\mathbb{Z}_h^N = U_\lambda + U_{-\lambda}$. It remains to be proved that $U_\lambda \cap U_{-\lambda} = \{\mathbf{0}\}$. If $\mathbf{u} \in U_\lambda \cap U_{-\lambda}$, then $S\mathbf{u} = \lambda\mathbf{u} = -\lambda\mathbf{u}$, hence $2\lambda\mathbf{u} = \mathbf{0}$. Since $\lambda^2 \equiv 1 \pmod{h}$, we have $\gcd(h, \lambda) = 1$; moreover, 2 is also relatively prime to h, as h is odd. Therefore we may conclude that $\mathbf{u} = \mathbf{0}$, and this completes the proof. □

We still need a simple number-theoretical lemma before we can prove our main theorem about the number of eigenvectors.

Lemma 3.2. *If h is an odd natural number, and $\lambda, s \in \mathbb{Z}$ are such that $\lambda^2 \equiv s^2 \equiv 1 \pmod{h}$, then $\gcd(h, s - \lambda) \cdot \gcd(h, s + \lambda) = h$.*

Proof. Let $h = \prod p_i^{e_i}$ be the prime power factorization of h, where each p_i is an odd prime and each e_i is a positive exponent. Since $\lambda^2 \equiv 1 \pmod{h}$, we have $p_i^{e_i} \mid (\lambda - 1)(\lambda + 1)$ for every i. This implies that either $p_i^{e_i} \mid \lambda - 1$ or $p_i^{e_i} \mid \lambda + 1$, as $\gcd(\lambda - 1, \lambda + 1) \leq 2$ and p_i is odd. Thus $\lambda \equiv \pm 1 \pmod{p_i^{e_i}}$, and a similar argument shows that $s \equiv \pm 1 \pmod{p_i^{e_i}}$ for every i. Therefore, one of $s - \lambda$ and $s + \lambda$ is congruent to ± 2 and the other one is congruent to 0 modulo $p_i^{e_i}$. Thus one of $\gcd(h, s - \lambda)$ and $\gcd(h, s + \lambda)$ is divisible by $p_i^{e_i}$ and the other one is not divisible by p_i. This is true for every prime divisor p_i of h, and no other primes can occur as a divisor of $\gcd(h, s - \lambda) \cdot \gcd(h, s + \lambda)$, hence we may conclude that $\gcd(h, s - \lambda) \cdot \gcd(h, s + \lambda) = \prod p_i^{e_i} = h$. □

Theorem 3.1. *Assume that h is odd and $S = (s_{ij})_{i,j=0}^{N-1}$ is a lower triangular $N \times N$ matrix over $\mathbb{Z}_h$ such that $S^2 = I_N$. If $\lambda \in \mathbb{Z}_h$ and $\lambda^2 = 1$, then the size of the eigenspace $U_\lambda(S)$ of S corresponding to the eigenvalue λ is*

$$|U_\lambda(S)| = \gcd(h, s_{00} - \lambda) \cdot \ldots \cdot \gcd(h, s_{N-1,N-1} - \lambda).$$

Proof. The elements of U_λ are the solutions of the system $(S - \lambda I_N)\,\mathbf{x} = \mathbf{0}$ of homogeneous linear equations. The first equation (written as a modulo h congruence) is $(s_{00} - \lambda)\,x_0 \equiv 0 \pmod h$. This linear congruence has $\gcd(h, s_{00} - \lambda)$ many solutions modulo h, thus there are $\gcd(h, s_{00} - \lambda)$ possible values for $x_0 \in \mathbb{Z}_h$. The second equation is equivalent to $s_{10}x_0 + (s_{11} - \lambda)\,x_1 \equiv 0 \pmod h$. If we have already chosen the value of x_0, then this can be viewed as a linear congruence $(s_{11} - \lambda)\,x_1 \equiv -s_{10}x_0 \pmod h$ for the unknown x_1. Depending on the value of x_0, this linear congruence may or may not have a solution, but if there is a solution, then the number of solutions modulo h is $\gcd(h, s_{11} - \lambda)$. Thus the number of choices for $x_1 \in \mathbb{Z}_h$ is either 0 or $\gcd(h, s_{11} - \lambda)$. Continuing in this manner, having assigned values to $x_0, \ldots, x_{i-1}$, we can treat the i-th equation as a linear congruence $(s_{ii} - \lambda)\,x_i \equiv -s_{i0}x_0 - \cdots - s_{i,i-1}x_{i-1} \pmod h$ for the unknown x_i, which has either 0 or $\gcd(h, s_{ii} - \lambda)$ many solutions in $\mathbb{Z}_h$. This provides an upper estimate for the size of the eigenspace U_λ:

$$|U_\lambda| \le \gcd(h, s_{00} - \lambda) \cdot \ldots \cdot \gcd(h, s_{N-1,N-1} - \lambda). \tag{3}$$

Let us write down the corresponding estimate for $-\lambda$, and use Lemma 3.2 (observe that $S^2 = I_N$ implies that $s_{ii}^2 = 1$ for every i, since S is a lower triangular matrix):

$$|U_\lambda| \cdot |U_{-\lambda}| \le \gcd(h, s_{00} - \lambda)\gcd(h, s_{00} + \lambda) \cdot \ldots \\ \cdot \gcd(h, s_{N-1,N-1} - \lambda)\gcd(h, s_{N-1,N-1} + \lambda) = h^N.$$

By Lemma 3.1, every element of $\mathbb{Z}_h^N$ can be uniquely expressed as a sum of a vector from U_λ and a vector from $U_{-\lambda}$. This implies that $|U_\lambda| \cdot |U_{-\lambda}| = \left|\mathbb{Z}_h^N\right| = h^N$, hence the inequality above is in fact an equality, so we have equality in (3) as well. □

4. The Pascal transform

Next, we will determine the number of eigenvectors of P_N corresponding to eigenvalues $\lambda \in \mathbb{Z}_h$ with $\lambda^2 = 1$ (note that Theorem 4.1, the main result of this section, overlaps with Theorem 3.1 if h is odd). Since $T_h = -P_h$, this includes as a special case the results of [**?**], where one-variable eigenfunctions of the Reed-Muller-Fourier transform were considered with the eigenvalues ± 1. An elimination procedure was used in [**?**], but its correctness was not rigorously proved (although the patterns of binomial coefficients appearing in the matrices were clear enough). Here we provide a proof, and instead of a step-by-step procedure, we do the elimination at once, by multiplying by a suitable invertible matrix.

Let $A_N = (a_{ij})_{i,j=0}^{N-1} \in \mathbb{Z}_h^{N \times N}$ be the matrix given by the entries

$$a_{ij} = (-1)^{i+j} \cdot \binom{\lfloor i/2 \rfloor}{i-j}.$$

As an example, the matrix A_8 is shown in Table 6. We will determine the number of solutions of $(P_N - \lambda I_N)\,\mathbf{x} = \mathbf{0}$ by multiplying by A_N on the left. The following combinatorial identity is required to compute the product $A_N P_N$. Such identities can be proved automatically by a computer [**?**], but a "human" proof might still be of interest.

Lemma 4.1. *For all natural numbers ℓ, r and m, we have*

$$\sum_{k=0}^{r} (-1)^k \cdot \binom{r}{k} \cdot \binom{\ell + r - k}{m} = \binom{\ell}{m - r}. \tag{4}$$

Proof. We give a combinatorial interpretation of the identity, and, to make the proof more vivid, we present it in the setting of a fantasy story. Assume that there is a group of r orcs and ℓ elves wandering together in Middle-earth. They learn about a wizard forging magic rings, and they decide to steal some of those rings. A set of m members of the group is to be chosen for this mission, such that all the orcs are included (they are good fighters). Thus it suffices to choose the $m-r$ elves that are going with the orcs, and the number of such choices is obviously $\binom{\ell}{m-r}$.

Now we count the number of possibilities once more, with the help of the inclusion-exclusion principle, and this will result in the left hand side of (4). Let E and O denote the set of elves and orcs (thus $|E|=\ell$ and $|O|=r$), and let $\mathcal{G}$ stand for the set of "good" choices for the mission:

$$\mathcal{G}=\{M\subseteq E\cup O : |M|=m \text{ and } O\subseteq M\}.$$

We saw in the previous paragraph that $|\mathcal{G}|=\binom{\ell}{m-r}$. For every orc $o\in O$, let $\mathcal{B}_o$ denote the set of choices that are "bad", because the orc o is not sent to the mission:

$$\mathcal{B}_o=\{M\subseteq E\cup O : |M|=m \text{ and } o\notin M\}.$$

Given k orcs $o_1,\dots,o_k\in O$, the cardinality of $\mathcal{B}_{o_1}\cap\dots\cap\mathcal{B}_{o_k}$ is $\binom{\ell+r-k}{m}$, and there are $\binom{r}{k}$ possibilities for the set $\{o_1,\dots,o_k\}$. Therefore, by the inclusion-exclusion principle, we have

$$|\mathcal{G}|=\sum_{k=0}^{r}(-1)^k\cdot\binom{r}{k}\cdot\binom{\ell+r-k}{m},$$

which is indeed the left hand side of (4). □

Lemma 4.2. *The entries of the matrix A_NP_N are the following:*

$$(A_NP_N)_{ij}=(-1)^j\cdot\binom{\lceil i/2\rceil}{i-j}\qquad(i,j=0,1,\dots,N-1).$$

Proof. From the definitions of the matrices A_N and P_N, we have

$$\begin{aligned}(A_NP_N)_{ij}=\sum_{k=0}^{N-1}a_{ik}\cdot p_{kj}&=\sum_{k=0}^{N-1}(-1)^{i+k}\cdot\binom{\lfloor i/2\rfloor}{i-k}\cdot(-1)^j\cdot\binom{k}{j}\\&=(-1)^j\cdot\sum_{k=0}^{\lfloor i/2\rfloor}(-1)^k\cdot\binom{\lfloor i/2\rfloor}{k}\cdot\binom{i-k}{j}.\end{aligned}$$

(In the last step we changed the summation variable from k to $i-k$, and we omitted those terms where the first binomial coefficient is zero.) Applying Lemma 4.1 with $r=\lfloor i/2\rfloor$, $\ell=\lceil i/2\rceil$ and $m=j$, we get $(-1)^j\cdot\binom{\lceil i/2\rceil}{j-\lfloor i/2\rfloor}=(-1)^j\cdot\binom{\lceil i/2\rceil}{i-j}$, hence the lemma is proved. □

Theorem 4.1. *For every natural number h and $\lambda\in\mathbb{Z}_h$ with $\lambda^2=1$, the eigenspace $U_\lambda(P_N)\leq\mathbb{Z}_h^N$ of the discrete Pascal transform P_N has cardinality*

$$|U_\lambda(P_N)|=\begin{cases}h^{\lfloor N/2\rfloor}\cdot\gcd(1-\lambda,h), & \text{if } N \text{ is odd;}\\ h^{N/2}, & \text{if } N \text{ is even.}\end{cases}$$

Proof. We need to determine the set of vectors $\mathbf{x}\in\mathbb{Z}_h^N$ satisfying $(P_N-\lambda I_N)\,\mathbf{x}=\mathbf{0}$. Since the matrix A_N is triangular and all of its entries on the main diagonal are 1, we have $\det(A_N)=1$, hence A_N has an inverse in $\mathbb{Z}_h^{N\times N}$. Therefore, the solutions of $(P_N-\lambda I_N)\,\mathbf{x}=\mathbf{0}$ are the same as the solutions of $A_N(P_N-\lambda I_N)\,\mathbf{x}=\mathbf{0}$. We will prove that we can omit (roughly) every second equation from this system of linear equations: row i of the matrix $A_N(P_N-\lambda I_N)=A_NP_N-\lambda A_N$ is a scalar multiple of row $i+1$ whenever i is even and $i<N-1$.

Letting $i = 2k$, the j-th entries of row i and of row $i+1$ are, by Lemma 4.2 and by the definition of the matrix A_N,

$$(A_N P_N - \lambda A_N)_{2k,j} = (-1)^j \cdot (1-\lambda) \cdot \binom{k}{2k-j}, \tag{5a}$$

$$(A_N P_N - \lambda A_N)_{2k+1,j} = (-1)^j \cdot \left(\binom{k+1}{2k+1-j} + \lambda \cdot \binom{k}{2k+1-j} \right). \tag{5b}$$

Multiplying (5b) by $1-\lambda$ and taking into account the fact that $\lambda^2 = 1$ (and also using the usual recurrence for the Pascal triangle), we indeed get (5a):

$$\begin{aligned}
(1-\lambda) \cdot (A_N P_N - \lambda A_N)_{2k+1,j} &= \\
&= (-1)^j \cdot \left((1-\lambda) \cdot \binom{k+1}{2k+1-j} + (\lambda - \lambda^2) \cdot \binom{k}{2k+1-j} \right) \\
&= (-1)^j \cdot (1-\lambda) \cdot \left(\binom{k+1}{2k+1-j} - \binom{k}{2k+1-j} \right) \\
&= (-1)^j \cdot (1-\lambda) \cdot \binom{k}{2k-j} \\
&= (A_N P_N - \lambda A_N)_{2k,j}.
\end{aligned}$$

Therefore, the (equations corresponding to the) even-numbered rows can be omitted without changing the set of solutions. Let us distinguish two cases based on the parity of N.

If N is even, then we keep row i for $i = 1, 3, \ldots, N-1$. From (5b) we see that the first nonzero entry in row $2k+1$ is $(A_N P_N - \lambda A_N)_{2k+1,k} = (-1)^k$. Therefore, after deleting the even-numbered rows, we get an $(N/2) \times N$ matrix with the following form:

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

This matrix is in row echelon form, hence we can see that in the corresponding system of linear equations the last $N/2$ variables (namely $x_{N/2}, \ldots, x_{N-1}$) are free, and the first $N/2$ variables (namely $x_0, \ldots, x_{N/2-1}$) can be uniquely determined from the free variables. Since we have h choices for each of the free variables $x_{N/2}, \ldots, x_{N-1}$, the cardinality of U_λ is $h^{N/2}$.

Now let us assume that N is odd. In this case we cannot delete row $N-1$ even though $N-1$ is even, because this is the last row in the matrix (hence it cannot be a scalar multiple of the next row, as the next row does not exist). Thus we keep row i for $i = 1, 3, \ldots, N-2, N-1$, hence we get an $\lceil N/2 \rceil \times N$ matrix. Computing the first nonzero entry in each row with the help of (5a) and (5b), we see that our matrix has the following form:

$$\begin{pmatrix}
1 & * & \cdots & * & * & * & \cdots & * \\
0 & -1 & \cdots & * & * & * & \cdots & * \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots \\
0 & 0 & \cdots & (-1)^{(N-3)/2} & * & * & \cdots & * \\
0 & 0 & \cdots & 0 & (-1)^{(N-1)/2} \cdot (1-\lambda) & * & \cdots & *
\end{pmatrix}.$$

By (5a), each element in the last row in the above matrix (row $N-1$ in the original matrix before deleting every second row) has a factor $1-\lambda$. Thus the last row can be divided by $1-\lambda$, but then we obtain a modulo $h/\gcd(1-\lambda, h)$ congruence (instead of a modulo h congruence). Therefore, $x_{\lfloor N/2 \rfloor}$ is determined by the free variables $x_{\lceil N/2 \rceil}, \ldots, x_{N-1}$ only modulo $\gcd(1-\lambda, h)$, so there are $\gcd(1-\lambda, h)$ possibilities for $x_{\lfloor N/2 \rfloor}$ in $\mathbb{Z}_h$. The variables $x_0, \ldots, x_{\lfloor N/2 \rfloor - 1}$ are then uniquely determined (modulo h). We may conclude that the number of solutions is $h^{\lfloor N/2 \rfloor} \cdot \gcd(1-\lambda, h)$. □

Corollary 4.1. *For all natural numbers $h \geq 2$ and $n \geq 1$, the number of fixed points of the discrete Pascal transform P_N on $\mathbb{Z}_h^N$ is $h^{\lceil N/2 \rceil}$.*

Proof. We just need to apply Theorem 4.1 with $\lambda = 1$ and note that if N is odd, then $|U_1| = h^{\lfloor N/2 \rfloor} \cdot \gcd(1-\lambda, h) = h^{\lfloor N/2 \rfloor} \cdot \gcd(0, h) = h^{\lfloor N/2 \rfloor} \cdot h = h^{\lceil N/2 \rceil}$. □

5. The Reed-Muller-Fourier transform

If h is odd, then the results of Section 3 apply to the Reed-Muller-Fourier transform. By Proposition 2.1, Section 4 also covers the Reed-Muller-Fourier transform when h is a prime number.

From now on, we will assume that h is even, and we consider eigenvectors of $T_h^{\otimes n}$ corresponding to an eigenvalue $\lambda \in \mathbb{Z}_h$ such that $\lambda^2 = 1$. (Note that this implies that λ is odd and relatively prime to h.) In this case $\mathbb{Z}_h^{h^n}$ is not the direct sum of the eigenspaces U_λ and $U_{-\lambda}$, but we can still determine the cardinalities of $U_\lambda + U_{-\lambda}$ and $U_\lambda \cap U_{-\lambda}$ (see Lemma 5.2 and Lemma 5.3).

Lemma 5.1. *If h is an even natural number, then the number of vectors $\mathbf{u} \in \mathbb{Z}_2^{h^n}$ satisfying $T_h^{\otimes n}\mathbf{u} \equiv \mathbf{u} \pmod 2$ is $2^{h^n/2}$.*

Proof. Let us replace each entry of T_h by its residue modulo 2, and let $B_h \in \mathbb{Z}_2^{h \times h}$ denote the resulting matrix over $\mathbb{Z}_2$. Then $T_h^{\otimes n} \equiv B_h^{\otimes n} \pmod 2$, and our task is to prove that $\dim U_1\left(B_h^{\otimes n}\right) = h^n/2$. Since $B_h^{\otimes n}$ is a lower triangular matrix with ones on its diagonal, we can use Lemma 2.1 repeatedly to prove that

$$\dim U_1\left(B_h^{\otimes n}\right) \leq h^{n-1} \cdot \dim U_1\left(B_h\right). \tag{6}$$

Note that B_h is none other than P_h taken modulo 2, hence applying Corollary 4.1 (substituting N with h and h with 2), we see that the number of fixed points of B_h is $2^{h/2}$. This means that $\dim U_1(B_h) = h/2$, and then (6) gives $\dim U_1\left(B_h^{\otimes n}\right) \leq h^n/2$.

To prove the reverse inequality, observe that $\left(B_h^{\otimes n} - I_{h^n}\right)^2 = \left(B_h^{\otimes n}\right)^2 - 2B_h^{\otimes n} + I_{h^n} = 0_{h^n}$, since $B_h^{\otimes n}$ is a self-inverse matrix and the matrices are considered modulo 2. This implies that the range of $B_h^{\otimes n} - I_{h^n}$ is contained in its kernel, hence $\operatorname{rank}\left(B_h^{\otimes n} - I_{h^n}\right) \leq \dim\ker\left(B_h^{\otimes n} - I_{h^n}\right)$. By the rank-nullity theorem, we have

$$\begin{aligned} h^n &= \operatorname{rank}\left(B_h^{\otimes n} - I_{h^n}\right) + \dim\ker\left(B_h^{\otimes n} - I_{h^n}\right) \\ &\leq 2 \cdot \dim\ker\left(B_h^{\otimes n} - I_{h^n}\right) = 2 \cdot \dim U_1\left(B_h^{\otimes n}\right), \end{aligned}$$

and this proves that $\dim U_1\left(B_h^{\otimes n}\right) \geq h^n/2$. □

Lemma 5.2. *If h is an even natural number, $\lambda \in \mathbb{Z}_h$ and $\lambda^2 = 1$, then the cardinality of the sum of the eigenspaces $U_\lambda, U_{-\lambda} \leq \mathbb{Z}_h^{h^n}$ of $T_h^{\otimes n}$ is*

$$|U_\lambda + U_{-\lambda}| = \frac{h^{h^n}}{2^{h^n/2}}.$$

Proof. We claim that

$$U_\lambda + U_{-\lambda} = \left\{\mathbf{v} \in \mathbb{Z}_h^{h^n} : T_h^{\otimes n}\mathbf{v} \equiv \mathbf{v} \pmod 2\right\}. \tag{7}$$

If $\mathbf{v} = \mathbf{v}^+ + \mathbf{v}^-$ with $\mathbf{v}^+ \in U_\lambda, \mathbf{v}^- \in U_{-\lambda}$, then $T_h^{\otimes n}\mathbf{v} = \lambda\mathbf{v}^+ - \lambda\mathbf{v}^- \equiv \mathbf{v}^+ + \mathbf{v}^- \equiv \mathbf{v} \pmod 2$, as λ is odd. Now assume that $T_h^{\otimes n}\mathbf{v} \equiv \mathbf{v} \pmod 2$. Then each entry of $\mathbf{v} + \lambda T_h^{\otimes n}\mathbf{v}$ is even (again, we make use of the fact that λ is odd), hence it makes sense to write $\mathbf{v}^+ = \frac{1}{2}\left(\mathbf{v} + \lambda T_h^{\otimes n}\mathbf{v}\right)$. Similarly, we can let $\mathbf{v}^- = \frac{1}{2}\left(\mathbf{v} - \lambda T_h^{\otimes n}\mathbf{v}\right)$. It is clear that $\mathbf{v} = \mathbf{v}^+ + \mathbf{v}^-$, and the same argument as in the proof of Lemma 3.1 shows that $\mathbf{v}^+ \in U_\lambda$ and $\mathbf{v}^- \in U_{-\lambda}$. Therefore, $\mathbf{v} \in U_\lambda + U_{-\lambda}$, and this proves (7).

The above arguments show that we need to count the vectors $\mathbf{v} \in \mathbb{Z}_h^{h^n}$ for which there exists some $\mathbf{u} \in \mathbb{Z}_2^{h^n}$ such that $T_h^{\otimes n}\mathbf{u} \equiv \mathbf{u} \pmod 2$ and $\mathbf{v} \equiv \mathbf{u} \pmod 2$. By Lemma 5.1, there are $2^{h^n/2}$ possibilities for $\mathbf{u}$. Once $\mathbf{u}$ us given, we have $(h/2)^{h^n}$ choices for $\mathbf{v}$: if $u_i = 0$, then $v_i \in \{0, 2, \ldots, h\}$, and if $u_i = 1$, then $v_i \in \{1, 3, \ldots, h-1\}$ for $i = 1, 2, \ldots, h^n$. We may conclude that the number of $\mathbf{v} \in \mathbb{Z}_h^{h^n}$ with $T_h^{\otimes n}\mathbf{v} \equiv \mathbf{v} \pmod 2$ is $2^{h^n/2} \cdot (h/2)^{h^n}$, and this completes the proof. □

Lemma 5.3. *If h is an even natural number, $\lambda \in \mathbb{Z}_h$ and $\lambda^2 = 1$, then the cardinality of the intersection of the eigenspaces $U_\lambda, U_{-\lambda} \leq \mathbb{Z}_h^{h^n}$ of $T_h^{\otimes n}$ is*

$$|U_\lambda \cap U_{-\lambda}| = 2^{h^n/2}.$$

Proof. We claim that

$$U_\lambda \cap U_{-\lambda} = \left\{ \mathbf{v} \in \mathbb{Z}_h^{h^n} : \exists \mathbf{u} \in \mathbb{Z}_2^{h^n} \text{ such that } \mathbf{v} = \frac{h}{2} \cdot \mathbf{u} \text{ and } T_h^{\otimes n}\mathbf{u} \equiv \mathbf{u} \pmod 2 \right\}. \tag{8}$$

If $\mathbf{v} \in U_\lambda \cap U_{-\lambda}$, then $T_h^{\otimes n}\mathbf{v} = \lambda\mathbf{v} = -\lambda\mathbf{v}$, hence $2\lambda\mathbf{v} = \mathbf{0}$. Since λ is relatively prime to h, the condition $2\lambda\mathbf{v} = \mathbf{0}$ is equivalent to $\mathbf{v} \equiv \mathbf{0} \pmod{h/2}$, i.e., each component of $\mathbf{v}$ is either 0 or $h/2$. Therefore, $\mathbf{v}$ can be written as $h/2 \cdot \mathbf{u}$, where $u_i = 0$ if $v_i = 0$ and $u_i = 1$ if $v_i = h/2$. Now $T_h^{\otimes n}\mathbf{v} = \lambda\mathbf{v}$ can be reformulated as $h/2 \cdot T_h^{\otimes n}\mathbf{u} = h/2 \cdot \lambda\mathbf{u}$, which is equivalent to $T_h^{\otimes n}\mathbf{u} \equiv \lambda\mathbf{u} \equiv \mathbf{u} \pmod 2$, as λ is odd. Next, assume that $\mathbf{v} = h/2 \cdot \mathbf{u}$ for some $\mathbf{u} \in \mathbb{Z}_2^{h^n}$ such that $T_h^{\otimes n}\mathbf{u} \equiv \mathbf{u} \pmod 2$. Then we have $T_h^{\otimes n}\mathbf{v} = h/2 \cdot T_h^{\otimes n}\mathbf{u}$; furthermore, $T_h^{\otimes n}\mathbf{u} \equiv \mathbf{u} \pmod 2$ implies that $h/2 \cdot T_h^{\otimes n}\mathbf{u} \equiv h/2 \cdot (\pm\lambda\mathbf{u}) \pmod h$, since λ is odd. Thus we have $T_h^{\otimes n}\mathbf{v} \equiv h/2 \cdot (\pm\lambda\mathbf{u}) \equiv \pm\lambda\mathbf{v} \pmod h$, and this proves (8).

Since $\mathbf{v}$ is uniquely determined by $\mathbf{u}$ in (8), we may conclude that $|U_\lambda \cap U_{-\lambda}| = \left|\left\{\mathbf{u} \in \mathbb{Z}_2^{h^n} : T_h^{\otimes n}\mathbf{u} \equiv \mathbf{u} \pmod 2\right\}\right|$, and this is $2^{h^n/2}$ by Lemma 5.1. □

Lemmas 5.2 and 5.3 allow us to determine the product $|U_\lambda| \cdot |U_{-\lambda}|$ (see the first paragraph of the proof of Theorem 5.1). This will give the cardinalities of the eigenspaces if we manage to prove that $|U_\lambda| = |U_{-\lambda}|$. To achieve this, we use an auxiliary matrix $C_h = (c_{ij})_{i,j=0}^{h-1} \in \mathbb{Z}_h^{h \times h}$ given by

$$c_{ij} = (-1)^{j+1} \cdot 2^{j-i} \cdot \binom{h-1-i}{j-i}.$$

As an illustration, see Table 7, which shows this matrix for $h = 8$. Just like that with the matrix A_h in Section 4, a combinatorial identity is required to compute the products C_hT_h and T_hC_h. It should be mentioned that the algorithms of [**?**] tell us that the sums in (9) below do not have a closed form.

Lemma 5.4. *For all natural numbers ℓ, r and m, we have*

$$\sum_{k=0}^{\ell} (-1)^k \cdot \binom{\ell}{k} \cdot \binom{\ell+r-k}{m} \cdot 2^{\ell-k} = \sum_{k=0}^{r} (-1)^k \cdot \binom{r}{k} \cdot \binom{\ell+r-k}{m-k} \cdot 2^{m-k}. \tag{9}$$

Proof. Let us visit the elves and orcs of Lemma 4.1 once more. They managed to fetch a generous supply of magic rings; in principle, each member of the group could wear one. However, such artefacts can be dangerous, so they should be used with care. Therefore, when a set M of m members of the group are chosen for the next adventure, some rules must be observed regarding the set R of ring-bearers. First, orcs should not wear magic rings, because they do not have the mental skills required to handle them safely. Second, those staying at home should not wear magic rings, since they will not need them. We will prove that both sides of (9) give the cardinality of the following set of good assignments:

$$\mathcal{G} = \{(M, R) : M, R \subseteq E \cup O,\ |M| = m \text{ and } R \subseteq E \cap M\}.$$

We will use the inclusion-exclusion principle in two different ways to count the elements of $\mathcal{G}$. Let us spell(!) out the requirements on the pair (M, R) in detail:

(i) if $e \in E \setminus M$, then $e \notin R$;
(ii) if $o \in O \cap M$, then $o \notin R$;
(iii) if $o \in O \setminus M$, then $o \notin R$.

First, let $\mathcal{B}_e$ denote the set of assignments where conditions (ii) and (iii) are satisfied but (i) is not, because an elf $e \in E$ gets a ring, even though (s)he stays at home:

$$\mathcal{B}_e = \{(M, R) : M, R \subseteq E \cup O,\ |M| = m \text{ and } e \in R \subseteq E\}.$$

Given k elves $e_1, \ldots, e_k \in E$, the cardinality of $\mathcal{B}_{e_1} \cap \cdots \cap \mathcal{B}_{e_k}$ is $\binom{\ell+r-k}{m} \cdot 2^{\ell-k}$. Indeed, there are $\binom{\ell+r-k}{m}$ possibilities for M, as $e_1, \ldots, e_k \notin M$, and we can distribute

the rings to the elves (other than $e_1, \dots, e_k$, who already received their rings) in $2^{\ell-k}$ many ways. There are $\binom{\ell}{k}$ options for the set $\{e_1, \dots, e_k\}$, thus the inclusion-exclusion principle gives the left hand side of (9) for $|\mathcal{G}|$.

Now let $\mathcal{C}_e$ denote the set of assignments where the requirements (i) and (iii) are met but (ii) is violated, because an orc $o \in O$ taking part in the mission gets a ring:

$$\mathcal{C}_e = \{(M, R) : M, R \subseteq E \cup O,\ |M| = m \text{ and } o \in R \subseteq M\}.$$

Given k orcs $o_1, \dots, o_k \in O$, the cardinality of $\mathcal{C}_{o_1} \cap \dots \cap \mathcal{C}_{o_k}$ is $\binom{\ell+r-k}{m-k} \cdot 2^{m-k}$: we have $\binom{\ell+r-k}{m-k}$ many options to choose those members of $E \cup O$ that will accompany $o_1, \dots, o_k$ on the mission, and we can distribute the rings to the members of M (other than $o_1, \dots, o_k$, who have already received their rings) in 2^{m-k} many ways. There are $\binom{r}{k}$ choices for the set $\{o_1, \dots, o_k\}$, so the inclusion-exclusion principle indeed gives the right hand side of (9) for $|\mathcal{G}|$. □

Lemma 5.5. *If h is an even natural number, then $T_h C_h = -C_h T_h$.*

Proof. Let us compute first the entries of $T_h C_h$ (in the last step we omit terms where the first binomial coefficient is zero):

$$\begin{aligned}(T_h C_h)_{ij} = \sum_{k=0}^{h-1} t_{ik} \cdot c_{kj} &= \sum_{k=0}^{h-1} (-1)^{k+1} \cdot \binom{i}{k} \cdot (-1)^{j+1} \cdot 2^{j-k} \cdot \binom{h-1-k}{j-k} \\ &= (-1)^j \cdot \sum_{k=0}^{i} (-1)^k \cdot \binom{i}{k} \cdot \binom{h-1-k}{j-k} \cdot 2^{j-k}.\end{aligned}$$

This is the same as $(-1)^j$ times the right hand side of (9) with $r = i$, $\ell = h-1-i$ and $m = j$. Similarly, for $C_h T_h$ we find that

$$\begin{aligned}(C_h T_h)_{ij} = \sum_{g=0}^{h-1} c_{ig} \cdot t_{gj} &= \sum_{g=0}^{h-1} (-1)^{g+1} \cdot 2^{g-i} \cdot \binom{h-1-i}{g-i} \cdot (-1)^{j+1} \cdot \binom{g}{j} \\ &= \sum_{g=i}^{h-1} (-1)^{g+j} \cdot \binom{h-1-i}{g-i} \cdot \binom{g}{j} \cdot 2^{g-i}.\end{aligned}$$

Now let us introduce a new summation variable $k = h-1-g$:

$$(-1)^{h-1+j} \cdot \sum_{k=0}^{h-1-i} (-1)^k \cdot \binom{h-1-i}{k} \cdot \binom{h-1-k}{j} \cdot 2^{h-1-i-k}.$$

With the same setting for r, ℓ and m as above, this becomes $(-1)^{h-1+j}$ times the left hand side of (9). Therefore, Lemma 5.4 implies that $(-1)^j \cdot (T_h C_h)_{ij} = (-1)^{h-1+j} \cdot (C_h T_h)_{ij}$. If h is even, then $(-1)^j$ and $(-1)^{h-1+j}$ are of opposite sign, hence $(T_h C_h)_{ij} = -(C_h T_h)_{ij}$. □

Lemma 5.5 allows us to give a bijection between U_λ and $U_{-\lambda}$, proving that $|U_\lambda| = |U_{-\lambda}|$.

Lemma 5.6. *If h is an even natural number, $\lambda \in \mathbb{Z}_h$ and $\lambda^2 = 1$, then the eigenspaces $U_\lambda, U_{-\lambda} \leq \mathbb{Z}_h^{h^n}$ of $T_h^{\otimes n}$ have the same size: $|U_\lambda| = |U_{-\lambda}|$.*

Proof. Let consider the matrix $C_h^{(n)} = I_h \otimes \dots \otimes I_h \otimes C_h = I_h^{\otimes(n-1)} \otimes C_h \in \mathbb{Z}_h^{h^n}$. The mixed product identity and Lemma 5.5 imply that $C_h^{(n)} T_h^{\otimes n} = -T_h^{\otimes n} C_h^{(n)}$:

$$\begin{aligned}T_h^{\otimes n} \cdot C_h^{(n)} &= (T_h \otimes \dots \otimes T_h \otimes T_h) \cdot (I_h \otimes \dots \otimes I_h \otimes C_h) \\ &= (T_h I_h) \otimes \dots \otimes (T_h I_h) \otimes (T_h C_h) \\ &= (I_h T_h) \otimes \dots \otimes (I_h T_h) \otimes (-C_h T_h) \\ &= -(I_h \otimes \dots \otimes I_h \otimes C_h) \cdot (T_h \otimes \dots \otimes T_h \otimes T_h) = -C_h^{(n)} \cdot T_h^{\otimes n}.\end{aligned}$$

We can use this fact to prove that if $\mathbf{v} \in U_\lambda$ then $C_h^{(n)}\mathbf{v} \in U_{-\lambda}$:

$$T_h^{\otimes n} C_h^{(n)} \mathbf{v} = -C_h^{(n)} T_h^{\otimes n} \mathbf{v} = -C_h^{(n)} \lambda \mathbf{v} = -\lambda C_h^{(n)} \mathbf{v}.$$

Therefore, we can define a map $\varphi\colon U_\lambda \to U_{-\lambda}$, $\mathbf{v} \mapsto C_h^{(n)}\mathbf{v}$.

Since C_h is an upper triangular matrix with diagonal entries ± 1, it has an inverse $C_h^{-1} \in \mathbb{Z}_h^{h\times h}$. Consequently, by the mixed product identity (1), the matrix $C_h^{(n)}$ also has an inverse (namely, $I_h \otimes \cdots \otimes I_h \otimes C_h^{-1}$). Taking the inverse of both sides of the equality $C_h^{(n)} T_h^{\otimes n} = -T_h^{\otimes n} C_h^{(n)}$ and recalling that $T_h^{\otimes n}$ is self-inverse, we obtain $T_h^{\otimes n}\big(C_h^{(n)}\big)^{-1} = -\big(C_h^{(n)}\big)^{-1} T_h^{\otimes n}$. Then a similar argument to the one above leads us to infer that if $\mathbf{v} \in U_{-\lambda}$ then $\big(C_h^{(n)}\big)^{-1}\mathbf{v} \in U_\lambda$:

$$T_h^{\otimes n}\big(C_h^{(n)}\big)^{-1}\mathbf{v} = -\big(C_h^{(n)}\big)^{-1} T_h^{\otimes n}\mathbf{v} = -\big(C_h^{(n)}\big)^{-1}(-\lambda\mathbf{v}) = \lambda\big(C_h^{(n)}\big)^{-1}\mathbf{v}.$$

This allows us to define a map $\psi\colon U_{-\lambda} \to U_\lambda$, $\mathbf{v} \mapsto \big(C_h^{(n)}\big)^{-1}\mathbf{v}$. Clearly, φ and ψ are inverses of each other, so both are bijections, and this means that $|U_\lambda| = |U_{-\lambda}|$. □

Now we are ready to prove our main result about the eigenvectors of the Reed-Muller-Fourier transform. It is worth noting that if h is even, then the number of eigenvectors does not depend on the eigenvalue λ (as long as $\lambda^2 = 1$).

Theorem 5.1. *For every natural number h and $\lambda \in \mathbb{Z}_h$ with $\lambda^2 = 1$, the eigenspace $U_\lambda\left(T_h^{\otimes n}\right) \leq \mathbb{Z}_h^{h^n}$ of the Reed-Muller-Fourier transform $T_h^{\otimes n}$ has cardinality*

$$\left|U_\lambda\left(T_h^{\otimes n}\right)\right| = \begin{cases} h^{\lfloor h^n/2\rfloor} \cdot \gcd\left(h, 1+\lambda\right), & \text{if } h \text{ is odd and } n \text{ is odd;} \\ h^{\lfloor h^n/2\rfloor} \cdot \gcd\left(h, 1-\lambda\right), & \text{if } h \text{ is odd and } n \text{ is even;} \\ h^{h^n/2}, & \text{if } h \text{ is even.} \end{cases}$$

Proof. Assume first that h is even. Considering U_λ and $U_{-\lambda}$ as additive subgroups of $\mathbb{Z}_h^{h^n}$, one of the isomorphism theorems (there seems to be no consensus on the numbering) yields $\left(U_\lambda + U_{-\lambda}\right)/U_{-\lambda} \cong U_\lambda/\left(U_\lambda \cap U_{-\lambda}\right)$, which implies with the help of lemmas 5.2 and 5.3 that

$$|U_\lambda| \cdot |U_{-\lambda}| = |U_\lambda + U_{-\lambda}| \cdot |U_\lambda \cap U_{-\lambda}| = \frac{h^{h^n}}{2^{h^n/2}} \cdot 2^{h^n/2} = h^{h^n}.$$

Then we may conclude from Lemma 5.6 that $|U_\lambda| = |U_{-\lambda}| = h^{h^n/2}$.

Now let us assume that h is odd. Then we can apply Theorem 3.1, as $T_h^{\otimes n}$ is a triangular self-inverse matrix. Denoting the number of ones and zeros on the diagonal of $T_h^{\otimes n}$ by m_1 and m_{-1}, respectively, we see that

(10)
$$|U_\lambda| = \gcd\left(h, 1-\lambda\right)^{m_1} \cdot \gcd\left(h, -1-\lambda\right)^{m_{-1}} = \gcd\left(h, 1-\lambda\right)^{m_1} \cdot \gcd\left(h, 1+\lambda\right)^{m_{-1}}.$$

It is not hard to verify that the diagonal of $T_h^{\otimes n}$ is $(-1, 1, \ldots, 1, -1)$ if n is odd and it is $(1, -1, \ldots, -1, 1)$ if n is even (note that if h is even then the diagonal entries of $T_h^{\otimes n}$ are still ± 1, but not alternately; see tables 3 and 4). In the first case we have $m_1 = \lfloor h^n/2\rfloor, m_{-1} = \lceil h^n/2\rceil$, while in the second case we have $m_1 = \lceil h^n/2\rceil, m_{-1} = \lfloor h^n/2\rfloor$. Therefore, (10) gives with the help of Lemma 3.2 (note that $\lceil h^n/2\rceil = \lfloor h^n/2\rfloor + 1$),

$$|U_\lambda| = \gcd\left(h, 1-\lambda\right)^{\lfloor h^n/2\rfloor} \cdot \gcd\left(h, 1+\lambda\right)^{\lceil h^n/2\rceil} = h^{\lfloor h^n/2\rfloor} \cdot \gcd\left(h, 1+\lambda\right) \text{ if } 2 \nmid n,$$
$$|U_\lambda| = \gcd\left(h, 1-\lambda\right)^{\lceil h^n/2\rceil} \cdot \gcd\left(h, 1+\lambda\right)^{\lfloor h^n/2\rfloor} = h^{\lfloor h^n/2\rfloor} \cdot \gcd\left(h, 1-\lambda\right) \text{ if } 2 \mid n.$$

□

Now, we will conclude our study by proving Conjecture 1.1.

Corollary 5.1. *For all natural numbers $h \geq 2$ and $n \geq 1$, the number of fixed points of the Reed-Muller-Fourier transform on n-variable functions over $\mathbb{Z}_h$ is $h^{\lfloor h^n/2\rfloor}$ if n is odd, and it is $h^{\lceil h^n/2\rceil}$ if n is even.*

Proof. We apply Theorem 5.1 with $\lambda = 1$. If h is even, then there is nothing to do; if h is odd, then observe that $|U_\lambda| = h^{\lfloor h^n/2 \rfloor} \cdot \gcd(h, 1+1) = h^{\lfloor h^n/2 \rfloor} \cdot 1$ when n is odd, and $|U_\lambda| = h^{\lfloor h^n/2 \rfloor} \cdot \gcd(h, 1-1) = h^{\lfloor h^n/2 \rfloor} \cdot h = h^{\lceil h^n/2 \rceil}$ when n is even. □

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

E-mail address: twaldha@math.u-szeged.hu

TABLE 1. The matrix P_8

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & -2 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & -3 & 3 & -1 & 0 & 0 & 0 & 0 \\ 1 & -4 & 6 & -4 & 1 & 0 & 0 & 0 \\ 1 & -5 & 10 & -10 & 5 & -1 & 0 & 0 \\ 1 & -6 & 15 & -20 & 15 & -6 & 1 & 0 \\ 1 & -7 & 21 & -35 & 35 & -21 & 7 & -1 \end{pmatrix}$$

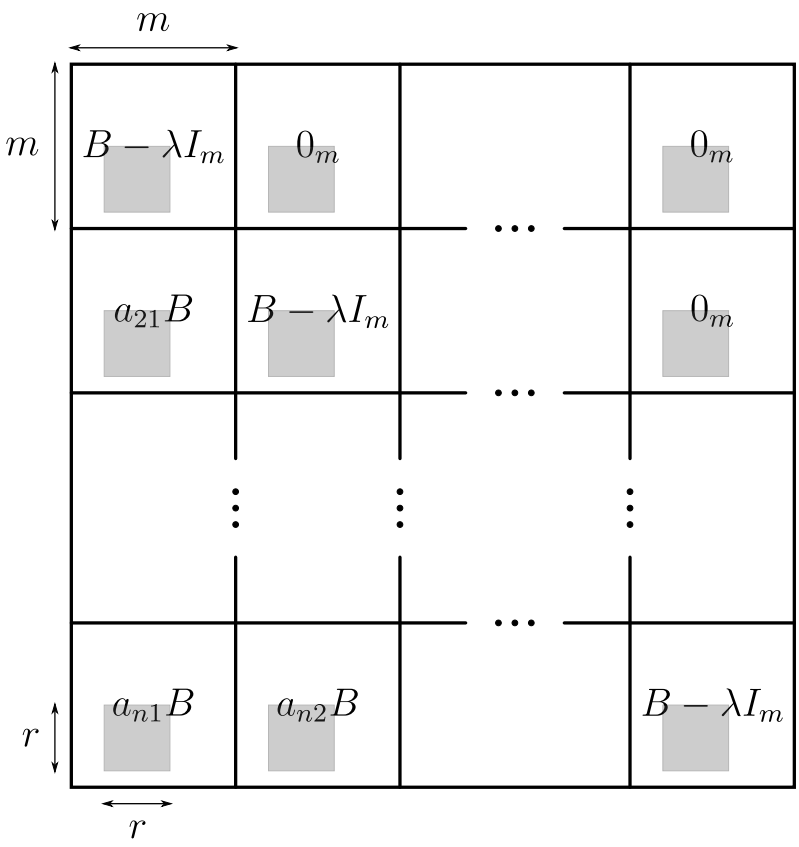

FIGURE 1. The matrix $A \otimes B - \lambda I_{nm}$ in the proof of Lemma 2.1

TABLE 2. The matrix T_8

$$\begin{pmatrix} -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 2 & -1 & 0 & 0 & 0 & 0 & 0 \\ -1 & 3 & -3 & 1 & 0 & 0 & 0 & 0 \\ -1 & 4 & -6 & 4 & -1 & 0 & 0 & 0 \\ -1 & 5 & -10 & 10 & -5 & 1 & 0 & 0 \\ -1 & 6 & -15 & 20 & -15 & 6 & -1 & 0 \\ -1 & 7 & -21 & 35 & -35 & 21 & -7 & 1 \end{pmatrix}$$

TABLE 3. The matrix $T_2^{\otimes 2}$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 1 & 0 & -1 & 0 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

TABLE 4. The matrix $T_2^{\otimes 3}$

$$\begin{pmatrix} -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ -1 & 1 & 1 & -1 & 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 & 1 & -1 & 0 & 0 \\ -1 & 0 & 1 & 0 & 1 & 0 & -1 & 0 \\ -1 & 1 & 1 & -1 & 1 & -1 & -1 & 1 \end{pmatrix}$$

TABLE 5. The matrix $T_3^{\otimes 2}$

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

TABLE 6. The matrix A_8

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

TABLE 7. The matrix C_8

$$\begin{pmatrix} -1 & 14 & -84 & 280 & -560 & 672 & -448 & 128 \\ 0 & 1 & -12 & 60 & -160 & 240 & -192 & 64 \\ 0 & 0 & -1 & 10 & -40 & 80 & -80 & 32 \\ 0 & 0 & 0 & 1 & -8 & 24 & -32 & 16 \\ 0 & 0 & 0 & 0 & -1 & 6 & -12 & 8 \\ 0 & 0 & 0 & 0 & 0 & 1 & -4 & 4 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

TABLE 8. Sizes of eigenspaces of T_h for $h \leq 12$

		h										
		2	3	4	5	6	7	8	9	10	11	12
λ	0	1	1	1	1	1	1	1	1	1	1	1
	1	2	3	2^4	5^2	$2^3 3^3$	7^3	2^{12}	3^8	$2^5 5^5$	11^5	$2^{12} 3^6$
	2		3^2	1	1	3^3	1	1	3^5	1	1	3^6
	3			2^4	1	2^3	1	2^{12}	1	2^5	1	2^{12}
	4				5^3	3^3	1	1	3^4	5^5	1	3^6
	5					$2^3 3^3$	1	2^{12}	3^5	2^5	1	$2^{12} 3^6$
	6						7^4	1	1	5^5	1	1
	7							2^{12}	3^4	2^5	1	$2^{12} 3^6$
	8								3^{10}	1	1	3^6
	9									$2^5 5^5$	1	2^{12}
	10										11^6	3^6
	11											$2^{12} 3^6$