BULGARIAN ACADEMY OF SCIENCIES
INSTITUTE OF MATHEMATICS AND INFORMATICS

PASKAL NIKOLAEV PIPERKOV

DESCRETE TRANSFORMS AND THEIR APPLICATION IN CODING THEORY AND COMBINATORICS

Summary of Dissertation
for Award of Educational and Scientific Degree PhD
Code of the Professional Field: 4.5. Mathematics
Code of the Scientific Speciality:
01.01.02. Algebra and Number Theory

Supervisor:
Prof. D.Sc. Iliya Bouyukliev

Sofia
2022

The PhD thesis examines the discrete transforms and some of their applications in the calculations of the parameters of linear codes. Developed in the 1960s, the fast transforms play a key role for the efficiency of computational algorithms. Although widespread in noise protection coding and signal processing, the fast discrete transforms still have illimitable potential for application in various fields of science and technology.

Preface

The core nature of some discrete transforms is the multiplication of a matrix by vector. The specific character of a particular transformation depends on what type of matrix is used. For the purposes of fast algorithms the main transform matrix has been represented as a product of sparse matrices whose rows consist mostly of zeros except a few elements, for example with value 1 or -1. This leads to algorithms that are much more effective than the usual matrix by vector multiplication [11, 14, 26]. A survey of fast transforms and their applications can be found in [5, 12, 19, 27].

Historically, Walsh functions arose as a discrete analogue of the orthonormal system of trigonometric functions, and the Walsh-Hadamard transform—as an analogue of the Fourier transform [30]. The Walsh-Hadamard transform is applied to the study of combinatorial configurations such as the Boolean and vector Boolean functions [8, 9], binary linear codes [17] and others.

The Vilenkin-Chrestenson functions [10, 29] and their corresponding transform are a generalization of Walsh functions and Walsh transform in complex numbers. They take as a base a q-th primitive complex root of unity. The transform is applicable in combinatorial configurations over prime finite fields [17, 18].

It is appropriate to use the trace transform for linear codes over composite finite fields [1, 18]. A primitive complex root of unity of degree characteristic of the field is taken as a base. In calculations, instead of the inner product, its trace is used.

The problem set to be solved by the dissertation thesis is to find effective algorithms for calculating the weight distribution and the covering radius of a linear code over a finite field by using a characteristic vector.

The linear codes are defined as linear subspaces of the n-dimensional linear space over a finite field. They are constructed and used in the terms of generator matrix whose rows are a basis of the subspace. Computing the parameters of the code (weight distribution, minimal distance, covering radius) using a given generator (or parity check) matrix presents the basic problem in many aspects of Coding Theory. Detecting (correcting) errors in information transmission is one of the

goals in Coding Theory, and the determining factor for this is the minimum weight and covering radius of the chosen linear code. Coding Theory is systematically constructed, for example in [2, 4, 15, 22, 24].

The study was motivated by the results and ideas of Mark Karpovsky [17, 18] on applying fast discrete transforms to find the weight distribution and covering radius of a linear code. For binary linear codes, Karpowsky applies the Walsh-Hadamard transform. As a generalization for non-binary linear codes, he suggests the application of the Vilenkin-Chrestenson transform (for prime fields) and the trace transform (for composite fields).

A significant contribution of the present work is that the calculations have been done over a maximal set of nonproportional vectors. On the one hand this is enough for determining the weight enumerator and other parameters of the linear code, on the other hand it decreases the complexity of the algorithms and the size of used memory. For the purpose, the generator (parity check) matrix that determines the linear code is represented by the characteristic vector of of the columns of the matrix by counting the number of the columns belonging to the respective points of projective geometry. The construction is rather useful when the number of the rows of the matrix is substantially smaller than the numbers of the columns.

In **Chapter 1** the basic concepts are described. In Section 1, some definitions and propositions for finite fields are introduced—such as trace, self-dual basis etc. In Section 2, basic definitions and propositions for linear codes are given. In Section 3, Walsh-Hadamard transform is shown. In Section 4, methods for representation of Kroneker product as a product of sparse matrices are given. This technique is the basis for fast transforms and the corresponding butterfly algorithms. In Section 5, Vilenkin-Chrestenson transform is described. In Section 6, trace transform is described.

In **Chapter 2** a developed algorithm for calculating the weight distribution of a linear code over finite prime filed is described. In Section 1, a special type of a generator matrix of the simplex code is described and a concept of characteristic vector with respect to the simplex code is defined. In Section 2, the concept of characteristic distribution is defined and its properties are deduced. The relation between the characteristic distribution and the weight distribution is shown. In Section 3, the developed algorithm for computing the characteristic distribution is described in details. In Section 4, the concept of reduced characteristic distribution is defined and the relation between the reduced characteristic distribution and the weight distribution is given. The reduced characteristic distribution is a generalization of the Walsh spectra. In Section 5, the complexity of the proposed algorithm is computed and an experimental results are presented.

In **Chapter 3** methods for computing the weight distribution where the linear

code is over composite finite field are considered. In Section 1, the problem is reduced to the problem for computing the weight distribution of a linear code over a prime field by the concept of trace code. In the other sections, the trace transform [1] is used as a base. In section 2, the standard approach by trace transform of extended characteristic vector is commented. A more effective algorithm when the elements of the field are lexicographically ordered with respect to a self-dual basis are shown. In Sections 3 and 4, an improved algorithm for computing the trace transform is described. This algorithm uses the characteristic vector with respect to the simplex code. In Section 3, the improved algorithm is motivated analytically on a base of matrices and, in Section 4, a detailed description is given and the complexity is computed.

In **Chapter 4** some methods for computing the covering radius of a linear code by discrete transforms are described. The decision proposed by Karpovsky for binary codes [18] is generalized and improved. The concept of reduced distribution of a vector is defined. It is a variant of generalization of Walsh-Hadamard transform. In Section 1, focus is put on linear codes over prime finite fields and the Vilenkin-Cherestenson transform is applied. In Section 2, some results for composite finite fields are described and the trace transform is applied.

Acknowledgments

I want to express my sincere thanks to all my teachers and mentors over the years Stefka Todorova, Emil Petrov, prof. D.Sc. Dimiter Vakarelov and assoc. prof. PhD Dimiter Petrov. I am much indebted to my supervisor prof. D.Sc. Iliya Bouyukliev who has showed a lot of patience and perseverance, and unreservedly believed in my abilities and led me to the completion of this work. My thanks also go to prof. D.Sc. Stefka Bouyuklieva for the support and hard work as a co-author. I want to thank Tatsuya Maruta who agreed me as a co-author. My deep and sincere gratitude to the directors of Institute of Mathematics and Informatics acad. Julian Revalski, acad. Vesselin Drensky and prof. D.Sc. Peter Boyvalenkov for the support and trust they invested in me. My thanks to the colleagues from the department of Mathematical Foundations of Informatics and its heads prof. D.Sc. Emil Kolev and assoc. prof. PhD Hristo Kostadinov for supporting me throughout my research work. To the participants in the National Seminar in Coding Theory "Prof. Stefan Dodunekov" and the colleagues from the Faculty of Mathematics and Informatics of St. Cyril and St. Methodius University of Veliko Tarnovo my appreciation for their support and constructive ideas.

1 Preliminaries

1.1 Finite fields

Let $\mathbb{F}_q$ be a finite field with q elements and the prime p be its characteristic. Theory of finite fields is systematically built for example in [21, 23].

Definition 1.1. Let $K = \mathbb{F}_q$, $F = \mathbb{F}_{q^m}$ and $\alpha \in F$. The *trace* $\mathrm{Tr}_{F/K}(\alpha)$ of $\alpha \in F$ over K is defined by

$$\mathrm{Tr}_{F/K}(\alpha) = \alpha + \alpha^q + \alpha^{q^2} + \ldots + \alpha^{q^{m-1}}.$$

If K is the prime subfield of F, then $\mathrm{Tr}_{F/K}(\alpha)$ is called the *absolute trace* of α and denoted by $\mathrm{Tr}_F(\alpha)$.

In the dissertation only absolute trace is used and for short it will be called the *trace*. If the subfield is clear then the trace will be denoted by $\mathrm{Tr}(\alpha)$.

Definition 1.2. Two bases $\beta_1, \ldots, \beta_m \in F$ and $\beta'_1, \ldots, \beta'_m \in F$ of the field F over the field K are called *dual*, if for $1 \leq i, j \leq m$

$$\mathrm{Tr}_{F/K}(\beta_i \beta'_j) = \begin{cases} 0, & \text{if} \quad i \neq j, \\ 1, & \text{if} \quad i = j. \end{cases}$$

The basis that is dual to itself is called *self-dual*.

For every basis there exists an uniquely determined dual basis.

Theorem 1.1 ([25]). *There exists a self-dual basis of the field $F = \mathbb{F}_{q^m}$ over $K = \mathbb{F}_q$ iff q is even or both q and m are odd.*

For the purposes of the dissertation, the elements of the field $\mathbb{F}_q$ are denoted respectively by $\alpha_0 = 0, \alpha_1, \ldots, \alpha_{q-1}$. Let they are ordered lexicographically over a fixed basis of the field over its prime subfield.

If $x \in \mathbb{F}_q^k$ then the coordinates of x are denoted by subscripts, i.e. $x = (x_1, x_2, \ldots, x_k)$. If two vectors x and x' belong to the linear space $\mathbb{F}_q^k$, then their *Euclidean scalar product* is $\langle x, x' \rangle = x_1 x'_1 + x_2 x'_2 + \cdots + x_k x'_k$ where the operations are in the field $\mathbb{F}_q$. In the dissertation only Euclidean scalar product is used so it will be called simply the *scalar product*.

1.2 Linear codes

Definition 1.3. Every k-dimensional linear subspace C of the linear space $\mathbb{F}_q^n$ is called *q-ary linear $[n,k]$ code* (or *linear $[n,k]_q$ code*). The parameters n and k are called the *length* and *dimension* of C, respectively, and the vectors in C are called the *codewords*.

Definition 1.4. The (*Hamming*) *weight* $\mathrm{wt}(x)$ of the vector $x \in \mathbb{F}_q^n$ is the number of its nonzero coordinates.

Definition 1.5. For a given linear $[n,k]_q$ code C, the least nonzero weight of a codeword is called the *minimum weight* of the code C and is denoted by d. If A_w is the number of the codewords with length w in C, $w = 0, 1, \ldots, n$, then the sequence $(A_0, A_1, \ldots, A_n)$ is called the *weight distribution* of C and the polynomial $W(z) = \sum_{w=0}^{n} A_w z^w$ is called the *weight enumerator* of the code C.

Definition 1.6. Every $k \times n$ matrix G whose rows form a basis of the linear $[n,k]_q$ code C is called the *generator matrix* of the code C.

Definition 1.7. The matrix H with size $(n-k) \times n$ that determines C in a sense

$$C = \{x \in \mathbb{F}_q^n | Hx^{\mathrm{T}} = 0\},$$

is called the *parity check matrix* of the code C.

Definition 1.8. For the linear $[n,k]_q$ code C and an arbitrary vector $x \in \mathbb{F}_q^n$ the set $x + C = \{x + c | c \in C\}$ is called a *coset* of the code C. The *weight of a coset* is the least weight of a vector in the coset and some vector with this the least weight in the coset is called the *coset leader*.

Definition 1.9. The *syndrome* of the vector $x \in \mathbb{F}_q^n$ with respect to the check matrix H of a given linear $[n,k]_q$ code C is the vector $syn(x) = Hx^{\mathrm{T}} \in \mathbb{F}_q^{n-k}$.

Definition 1.10. The maximal among the weights of the cosets of a linear $[n,k]_q$ code C is called the *covering radius* of C and is denoted by $R(C)$.

Theorem 1.2 ([15], Theorem 1.12.5)**.** *$R(C)$ is the smallest integer s such that every nonzero syndrome is a linear combination of s or fewer columns of the parity check matrix H, and some syndrome requires s columns.*

Definition 1.11. A *linear code of full length* is a linear code without zero columns in its generator matrix.

The maximal number of pairwise linearly independent vectors in the linear space $\mathbb{F}_q^k$ is $\theta(q,k) = \frac{q^k-1}{q-1}$. This is the number of 1-dimensional linear subspaces of $\mathbb{F}_q^k$.

Definition 1.12. The matrix with size $k \times \theta(q,k)$ whose columns are pairwise linear independent vectors in $\mathbb{F}_q^k$ generate a linear $[\theta(q,k),k]_q$ code that is called the *simplex code* and is denoted by $\mathcal{S}_{q,k}$.

1.3 Discrete Walsh-Hadamard transform

Definition 1.13 ([17])**.** Let f be a Boolean function of k variables. The *discrete Walsh-Hadamard transform* of f is the function $\widehat{f} : \mathbb{F}_2^k \to \mathbb{Z}$ defined by

$$\widehat{f}(\omega) = \sum_{x \in \mathbb{F}_2^k} f(x)(-1)^{\langle x,\omega \rangle}, \quad \omega \in \mathbb{F}_2^k. \tag{1}$$

Truth table of the function $\widehat{f}$ is called *Walsh spectrum* of the function f and is denoted by W_f.

Transform matrices are defined inductively as follows

$$H_1 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad H_k = \begin{pmatrix} H_{k-1} & H_{k-1} \\ H_{k-1} & -H_{k-1} \end{pmatrix}, \, k > 1. \tag{2}$$

Theorem 1.3. *If f is a Boolean function of k variables then $W_f = H_k \cdot TT_f$.*

Naturally, the definition 1.13 can be generalized for pseudo-Boolean functions, i.e. the functions $f : \mathbb{F}_q^k \to \mathbb{Z}$ that satisfy

$$\widehat{f}(\omega) = \sum_{x \in \mathbb{F}_2^k} f(x)(-1)^{\langle x,\omega \rangle}, \quad \omega \in \mathbb{F}_2^k. \tag{3}$$

Let G be a generator matrix of a linear $[n,k]_2$ code and $f : \mathbb{F}_2^k \to \mathbb{Z}$ be a characteristic function such that $f(x)$ is the number of the columns of G that is equal to x. In this case the Walsh-Hadamard transform $\widehat{f}$ corresponds to the weight of the codeword ωG as follows

$$\mathrm{wt}(\omega G) = \frac{n - \widehat{f}(\omega)}{2}, \quad \omega \in \mathbb{F}_2^k. \tag{4}$$

This fact is mentioned by Karpovsky [17] in the case when there exists no zero columns and repeated columns in G, i.e. when the dual code has minimum weight greater than 2.

1.4 Kroneker product. Fast transforms

The *Kroneker product* of matrices $A = (a_{ij})_{s_1 \times t_1}$ and $B = (b_{ij})_{s_2 \times t_2}$ is the $s_1 s_2 \times t_1 t_2$ matrix

$$A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B & \dots & a_{1t_1}B \\ a_{21}B & a_{22}B & \dots & a_{2t_1}B \\ \dots & & & \\ a_{s_1 1}B & a_{s_1 2}B & \dots & a_{s_1 t_1}B \end{pmatrix}.$$

The operation Kroneker product is not commutative.

For square matrix M the k-th Kroneker power $\otimes^k M$ is defined by the recurrent formulae:

$$\otimes^2 M = M \otimes M, \quad \otimes^{k+1} M = M \otimes \left(\otimes^k M\right), k > 1.$$

Good [14] shows that Kroneker product can be represented as usual product of rare matrices. The following theorem is a reformulation to the case of Kroneker power.

Theorem 1.4. *Let M be a square matrix of order t and k be a positive integer. Then*

$$\otimes^k M = B_1 \cdot B_2 \cdots B_k \tag{5}$$

where $B_l = I_{t^{l-1}} \otimes M \otimes I_{t^{k-l}}$, $1 \le l \le k$ and I_s is the identity matrix of order s.

Lechner [20] applies (5) to Walsh-Hadamard transform, but in reverse order of multipliers, and mentiones that factors commute. This is the statement of the following theorem.

Theorem 1.5. *Factors in* (5) *commute. So their order does not matter.*

1.5 Discrete Vilenkin-Chrestenson transform

Let ξ be a primitive complex q-th root of unity. The Vilenkin-Chrestenson matrices of order k are defined recurrently as follows:

$$V_1 = \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \xi & \xi^2 & \dots & \xi^{q-1} \\ 1 & \xi^2 & \xi^4 & \dots & \xi^{2(q-1)} \\ & \vdots & \vdots & & \vdots \\ 1 & \xi^{q-1} & \xi^{2(q-1)} & \dots & \xi^{(q-1)^2} \end{pmatrix}, \; V_{k+1} = V_1 \otimes V_k, \; k \in \mathbb{Z}, \, k \ge 1, \tag{6}$$

where $\otimes$ denotes Kroneker product. The elements of the matrix V_k are of the type $v_\omega(x) = \xi^{\langle \omega, x \rangle}$ where $\omega, x \in \mathbb{Z}_q^k$ (the row and column indexes respectively) are lexicographically ordered.

Definition 1.14. Let $f : \mathbb{Z}_q^k \to \mathbb{C}$ be a function. The *Vilenkin-Chrestenson transform* of f is the function $\widehat{f} : \mathbb{Z}_q^k \to \mathbb{C}$ defined by

$$\widehat{f}(\omega) = \sum_{x \in \mathbb{Z}_q^k} f(x) v_\omega(x), \quad \omega \in \mathbb{Z}_q^k. \tag{7}$$

A detailed information for this transform and other transforms related to Fourier transform can be found for example in [3, 13, 19].

Let TT_f be a value vector of the function f when the elements of $\mathbb{Z}_q^k$ are lexicographically ordered. This is an analogue of the truth table of Boolean functions, but here the coordinates of $TT_{\widehat{f}}$ are complexes. The value vectors of the functions f and $\widehat{f}$ are connected by the equality

$$TT_{\widehat{f}} = V_k \cdot TT_f.$$

In this way the Vilenkin-Chrestenson transform turns into matrix by vector multiplication.

Let q be a prime, G be a generator matrix of a linear $[n, k]_q$ code with full length and the function $f : \mathbb{F}_q^k \to \mathbb{Z}$ be defined by the number of the columns of G that are proportional (with nonzero coefficient) to x. In this case the Vilenkin-Chrestenson transform $\widehat{f}$ corresponds to the weight of the codeword ωG as follows

$$\mathrm{wt}(\omega G) = \frac{(q-1)n - \widehat{f}(\omega)}{q}, \quad \omega \in \mathbb{F}_q^k. \tag{8}$$

1.6 Trace transform

A generalization of Walsh-Hadamard transform that is applied to linear codes over composite finite fields is proposed by Karpovsky [18]. He suggests to use this transform for computing the weight distribution of cosets.

Let $\mathbb{F}_q$ be a composite finite field where $q = p^m$ and p be a prime.

In trace transform, the absolute trace of the scalar product is used instead of the scalar product in Vilenkin-Chrestenson transform [1, p. 367].

Let ζ be a primitive complex p-th root of unity and

$$\tau_\omega(x) = \zeta^{\mathrm{Tr}(\langle \omega, x \rangle)} \tag{9}$$

for arbitrary $\omega, x \in \mathbb{F}_q^k$. As it was earlier mentioned, the natural homomorphism between $\mathbb{F}_p$ and complexes with absolute value 1 are used. The transform is determined by the matrix $T_k = (\tau_\omega(x))$ with size $q^k \times q^k$ where the indexes $\omega, x \in \mathbb{F}_q^k$ are lexicographically ordered. By (9) transform of Fourier type is defined [1] that is called trace transform.

Definition 1.15. Let $\mathbb{F}_q$ be a finite field with q elements, $q = p^m$ where p is a prime and ζ be a primitive complex p-th root of unity. The *trace transform* of the function $f : \mathbb{F}_q^k \to \mathbb{C}$ is the function $\widehat{f} : \mathbb{F}_q^k \to \mathbb{C}$ that is defined by

$$\widehat{f}(\omega) = \sum_{x \in \mathbb{F}_q^k} f(x)\tau_\omega(x) = \sum_{x \in \mathbb{F}_q^k} f(x)\zeta^{\mathrm{Tr}(\langle \omega, x \rangle)}, \quad \omega \in \mathbb{F}_q^k. \tag{10}$$

The value tables of f and $\widehat{f}$ are related by the equality

$$TT_{\widehat{f}} = T_k \cdot TT_f.$$

For the matrices T_k the following recurrence relation holds $T_{k+1} = T_1 \otimes T_k$ and $T_k = \otimes^k T_1$ for $k \in \mathbb{N}$.

Definition 1.16. The value of the *characteristic function* $f_G(x)$ of a linear $[n, k]_q$ code C with a generator matrix G is the number of the columns of G that are proportional (by nonzero coefficient) to x, for $x \in \mathbb{F}_q^k$.

Remark 1.1. Karpovsky [18] considers the extended matrix

$$G' = (\alpha_1 G | \alpha_2 G | \ldots | \alpha_{q-1} G) \tag{11}$$

where G has no pairwise proportional columns, i.e. the minimum weight of the dual code is greater than 2. In this case the characteristic function in the classic sense $f' : \mathbb{F}_q^k \to \mathbb{F}_2$, that for every vector x shows if it is the column of G', is the same as the above defined function f_G.

Theorem 1.6. *Let G be a generator matrix of a linear $[n, k]_q$ code with full length C. Then the weights of the codewords of C*

$$\mathrm{wt}(\omega G) = \frac{(q-1)n - \widehat{f}(\omega)}{q}, \quad \omega \in \mathbb{F}_q^k, \tag{12}$$

where $\widehat{f}$ is the trace transform of the characteristic function f_G of the code C.

2 An algorithm for computing the weight distribution of a linear code over a prime finite field using characteristic vector

In this chapter the prime finite field $\mathbb{F}_q = \mathbb{Z}_q = \{0, 1, 2, \ldots, q-1\}$ with fixed order of its elements $\alpha_0 = 0, \alpha_1 = 1, \alpha_2, \ldots, \alpha_{q-1}$ is considered.

By $\boldsymbol{\alpha}$ the vector $(\alpha, \alpha, \ldots, \alpha) = \alpha(1, 1, \ldots, 1)$ with length by default and consisting of the same coordinates is denoted.

2.1 Characteristic vector of linear code

A special type of a generator matrix of the simplex code $\mathcal{S}_{q,k}$ that will mainly be used in dissertation is recurrently defined by the equalities:

$$G_1 = (1)\,, \quad G_{k+1} = \begin{pmatrix} \mathbf{0} & \boldsymbol{\alpha_1} & \boldsymbol{\alpha_2} & \dots & \boldsymbol{\alpha_{q-1}} & 1 \\ G_k & G_k & G_k & & G_k & \mathbf{0}^{\mathrm{T}} \end{pmatrix}\,,\ k \in \mathbb{N}. \tag{13}$$

Definition 2.1. *The characteristic vector* of the linear $[n,k]_q$ code C with respect to a generator matrix G is the vector

$$\chi(C,G) = (\chi_1, \chi_2, \dots, \chi_{\theta(q,k)}) \in \mathbb{Z}^{\theta(q,k)} \tag{14}$$

where χ_u is the number of the columns of G that are equal to proportional (by nonzero coefficient) to the u-th column of the matrix G_k, $u = 1, 2, \dots, \theta(q,k)$.

Below the characteristic vector is denoted for short by χ only, if the code C and the generator matrix G are clear from context.

For computing the weight distribution of the code C, it is enough to calculate the weights of the rows of the matrix $G_k^{\mathrm{T}} \cdot G$.

Let $M_k = G_k^{\mathrm{T}} \cdot G_k$, $k \in \mathbb{N}$, where multiplication is over $\mathbb{F}_q$. Below by $\mathcal{N}(M_k)$ the matrix obtained from M_k by replacing the all nonzero elements by 1 is denoted. This matrix is called *normalized matrix*.

Lemma 2.1. *Let C be a linear $[n,k]_q$ code with a generator matrix G and χ be a characteristic vector of C with respect to G. Then the Hamming weight of the i-th row of the matrix $G_k^{\mathrm{T}} \cdot G$ (multiplication is over $\mathbb{F}_q$) is the i-th element of the column vector $\mathcal{N}(M_k) \cdot \chi^{\mathrm{T}}$ (multiplication is over $\mathbb{Z}$), $i = 1, \dots, \theta(q,k)$.*

From (13) the recurrence relation of the matrices M_k is obtained, namely: $M_1 = (1)$ and for all $k \in \mathbb{Z}, k \geq 2$

$$M_k = \begin{pmatrix} M_{k-1} & M_{k-1} & \dots & M_{k-1} & \mathbf{0}^{\mathrm{T}} \\ M_{k-1} & M_{k-1} + J & \dots & M_{k-1} + \alpha_{q-1} J & \mathbf{1}^{\mathrm{T}} \\ M_{k-1} & M_{k-1} + \alpha_2 J & \dots & M_{k-1} + \alpha_2 \alpha_{q-1} J & \boldsymbol{\alpha_2}^{\mathrm{T}} \\ \vdots & & & & \\ M_{k-1} & M_{k-1} + \alpha_{q-1} J & \dots & M_{k-1} + \alpha_{q-1}^2 J & \boldsymbol{\alpha_{q-1}}^{\mathrm{T}} \\ \mathbf{0} & \mathbf{1} & \dots & \boldsymbol{\alpha_{q-1}} & 1 \end{pmatrix}. \tag{15}$$

The matrix J in the furmula above is $\theta(q,k-1) \times \theta(q,k-1)$ matrix consisting of ones.

2.2 Characteristic distribution

Definition 2.2. Let $\chi = (\chi_1, \ldots, \chi_t) \in \mathbb{Z}^t$ and $b = (b_1, \ldots, b_t) \in \mathbb{F}_q^t$, $t \in \mathbb{N}$. The *characteristic distribution* of a vector b with respect to χ is the vector

$$b^{[\chi]} = (\mu_0, \mu_1, \ldots, \mu_{q-1}) \in \mathbb{Z}^q$$

where μ_j is the sum of the coordinates χ_u of the vector χ such that $b_u = \alpha_j$, $1 \le u \le t$, $j = 0, 1, \ldots, q-1$. If no coordinate of b that is equal to α_j then $\mu_j = 0$.

Definition 2.3. Let $s, t \in \mathbb{N}$, $\chi \in \mathbb{Z}^t$, $B \in \mathbb{F}_q^{s \times t}$ and $B_1, \ldots, B_s$ be the rows of the matrix B. The *characteristic distribution* of the matrix B with respect to the vector χ is the matrix $B^{[\chi]} \in \mathbb{Z}^{s \times q}$ whose rows are $B_1^{[\chi]}, \ldots, B_s^{[\chi]}$.

Theorem 2.2. *Let C be a linear $[n,k]_q$ code of full length and χ be a characteristic vector of the code C with respect to an its generator matrix. The i-th coordinate of $\mathcal{N}(M_k) \cdot \chi^{\mathrm{T}}$ is equal to $n - \mu_0$ where μ_0 is the first coordinate of the characteristic distribution $c_i^{[\chi]} = (\mu_0, \mu_1, \ldots, \mu_{q-1})$ of the i-th row c_i of the matrix M_k with respect to χ.*

Let the characteristic vector χ of a linear $[n,k]_q$ code C be split to $q+1$ parts as follows

$$\chi = \left(\chi^{(0)} | \chi^{(1)} | \ldots | \chi^{(q-1)} | \chi^{(q)}\right) \tag{16}$$

where $\chi^{(j)} \in \mathbb{Z}^{\theta(q,k-1)}$, $j = 0, \ldots, q-1$ и $\chi^{(q)} \in \mathbb{Z}$. It is known that $\theta(q,k) = q\theta(q,k-1) + 1$. Then the following recurrence relation holds:
$M_k^{[\chi]} =$

$$\begin{pmatrix}
M_{k-1}^{[\chi^{(0)}]} & + & M_{k-1}^{[\chi^{(1)}]} & + \cdots + & M_{k-1}^{[\chi^{(q-1)}]} & + & \mathbf{0}^{\mathrm{T}[\chi^{(q)}]} \\
M_{k-1}^{[\chi^{(0)}]} & + & \mathrm{SR}(M_{k-1}^{[\chi^{(1)}]}) & + \cdots + & \mathrm{SR}_{\alpha_{q-1}}(M_{k-1}^{[\chi^{(q-1)}]}) & + & \mathbf{1}^{\mathrm{T}[\chi^{(q)}]} \\
M_{k-1}^{[\chi^{(0)}]} & + & \mathrm{SR}_{\alpha_2}(M_{k-1}^{[\chi^{(1)}]}) & + \cdots + & \mathrm{SR}_{\alpha_2\alpha_{q-1}}(M_{k-1}^{[\chi^{(q-1)}]}) & + & \boldsymbol{\alpha_2}^{\mathrm{T}[\chi^{(q)}]} \\
 & & & \vdots & & & \\
M_{k-1}^{[\chi^{(0)}]} & + & \mathrm{SR}_{\alpha_{q-1}}(M_{k-1}^{[\chi^{(1)}]}) & + \cdots + & \mathrm{SR}_{\alpha_{q-1}^2}(M_{k-1}^{[\chi^{(q-1)}]}) & + & \boldsymbol{\alpha_{q-1}}^{\mathrm{T}[\chi^{(q)}]} \\
\mathbf{0}^{[\chi^{(0)}]} & + & \mathbf{1}^{[\chi^{(1)}]} & + \cdots + & \boldsymbol{\alpha_{q-1}}^{[\chi^{(q-1)}]} & + & 1^{[\chi^{(q)}]}
\end{pmatrix} \tag{17}$$

where by SR the operation *circular shift right* is denoted.

Thus one cam use only permutations and additions to calculate $M_k^{[\chi]}$ from $M_{k-1}^{[\chi^{(0)}]}, M_{k-1}^{[\chi^{(1)}]}, \ldots, M_{k-1}^{[\chi^{(q-1)}]}$ and $\chi^{(q)}$. Moreover $\mathbf{1}^{[\chi]}, \ldots, \boldsymbol{\alpha_{q-1}}^{[\chi]}$ can be obtained from $\mathbf{0}^{[\chi]}$ by the operation SR.

Definition 2.4. Let $k \in \mathbb{N}$ and $\chi = (\chi_1, \ldots, \chi_{\theta(q,k)}) \in \mathbb{Z}^{\theta(q,k)}$. The *partial characteristic distribution* $M_k^{[\chi]}(l)$ for $l = 1, \ldots, k$ is recursively defined as follows

1. $M_k^{[\chi]}(k) = M_k^{[\chi]}$.

2. If $1 \leq l < k$ and the vector χ is split to the $q+1$ part as in (16) then $M_k^{[\chi]}(l)$ is calculated by the formula

$$M_k^{[\chi]}(l) = \begin{pmatrix} M_{k-1}^{[\chi^{(0)}]}(l) \\ M_{k-1}^{[\chi^{(1)}]}(l) \\ \ldots \\ M_{k-1}^{[\chi^{(q-1)}]}(l) \\ M_1^{[\chi^{(q)}]} \end{pmatrix}.$$

The matrix $M_k^{[\chi]}(1)$ is with size $\theta(q,k) \times q$ and rows $M_1^{[\chi_u]}$, $u = 1, \ldots, \theta(q,k)$. Because of $M_1 = (1)$, so the columns of the matrix $M_k^{[\chi]}(1)$ are zero vectors except the second that equals to χ^{T}.

The last row of the matrix $M_k^{[\chi]}(l)$ is the same for $l = 1, \ldots, k-1$, namely $M_1^{[\chi^{(q)}]}$. Furthermore, the row before the last one in $M_k^{[\chi]}(l)$ is the same for $l = 1, \ldots, k-2$. Actually, for all $l < k$ there are some rows that save themselves in all matrices $M_k^{[\chi]}(l')$ for $1 \leq l' < l$. These rows are called *inactive rows*. There exist exactly $\theta(q, k-l)$ inactive rows in $M_k^{[\chi]}(l)$, $l = 2, \ldots, k-1$.

2.3 An algorithm for computing the characteristic distribution

In this section the developed algorithm for computing $M_k^{[\chi]}$ by consequently calculating $M_k^{[\chi]}(1)$, $M_k^{[\chi]}(2)$,..., $M_k^{[\chi]}(k-1)$, $M_k^{[\chi]}(k)$ is presented.

The algorithm consists of three main transformations that are called Add0, LastRow and AllRows. These transformations are explained for $l = k$ below. The computation begins by

1. Add0: First, the operation circular shift left over the last row of the matrix $M_k^{[\chi]}(k-1)$ is applied. The resulted vector $\mathrm{lcs}(M_1^{[\chi^{(q)}]}) = (\chi^{(q)}, 0, \ldots, 0) = 0^{[\chi^{(q)}]}$ is added to every row of the matrix $M_{k-1}^{[\chi^{(1)}]}$.

2. LastRow: The last row of the matrix $M_k^{[\chi]}(k)$ that is equal to

$$\begin{aligned} M_k^{[\chi]}last &= \left(\mathbf{0}^{[\chi^{(0)}]} + \mathbf{1}^{[\chi^{(1)}]} + \cdots + \boldsymbol{\alpha_{q-1}}^{[\chi^{(q-1)}]} + 1^{[\chi^{(q)}]}\right) \\ &= \left(\sum_{u=1}^{\theta_0} \chi_u,\ \chi^{(q)} + \sum_{u=\theta_0+1}^{2\theta_0} \chi_u, \ldots,\ \sum_{u=\theta_1-\theta_0}^{\theta_1-1} \chi_u\right), \end{aligned}$$

has been calculated, where $\theta_0 = \theta(q, k-1)$ and $\theta_1 = \theta(q, k)$.

3. AllRows: In the core of this transformation q rows AllRows$[j]$, $j = 0, 1, \ldots, q-1$, of the matrix $M_k^{[\chi]}$ have been computed. For this purpose, a help array TEMP with size $q \times q$ has been used. The vectors AllRows$[j]$ have been calculated fron TEMP by the formulae

$$\begin{aligned} \text{AllRows}[0](\text{TEMP}) &= \text{TEMP}[0]+\text{TEMP}[1] + \cdots + \text{TEMP}[q-1], \\ \text{AllRows}[j](\text{TEMP}) &= \text{TEMP}[0]+SR_{\alpha_j}(\text{TEMP}[1]) + \cdots + \\ &\quad SR_{\alpha_j\alpha_{q-1}}(\text{TEMP}[q-1]),\ j > 0, \end{aligned}$$

where TEMP[0], TEMP[1], ..., TEMP$[q-1]$ are the rows of TEMP.

In the calculation of $M_k^{[\chi]}(l)$ from $M_k^{[\chi]}(l-1)$, inactive rows have been left unchanged and above formulae have been applied for obtaining the matrix $M_l^{[\chi']}(l)$ from the matrix $M_l^{[\chi']}(l-1)$ where χ' is a suitable part of χ.

To explain more formally the main algorithm one can introduce a matrix representation of the transform steps between the partial characteristic distributions.

Let all the rows of the matrix $M_k^{[\chi]}(l)$ be ordered in one vector with length $q\theta(q,k)$ that will be denoted by $\widetilde{M}_k^{[\chi]}(l)$, $l = 1, \ldots, k$. For shortness the notations $\widetilde{M}_k^{[\chi]} = \widetilde{M}_k^{[\chi]}(k)$ and $\widetilde{\chi} = \widetilde{M}_k^{[\chi]}(1)$ are used below.

In the next theorem the matrices of a few types are used, namely:

- The identity matrices I_s of size $s \times s$.
- The permutation matrices P_j of size $q \times q$ that realize the permutations SR_{α_j} respectively. In particular, $P_0 = I_q$, $P_1 = \begin{pmatrix} \mathbf{0} & 1 \\ I_{q-1} & \mathbf{0}^{\mathrm{T}} \end{pmatrix}$ and $P_j = P_1^j$.
- The matrices E_j of size $q \times q$, $j = 0, 1, \ldots, q-1$, for which the $j+1$-st row of E_j consists of 1's only and the other rows consist of 0's.
- The matrices O consisting of 0's only, with default size.
- The matrices $T_{k,l}$ for $k, l \in \mathbb{Z}$, $2 \le l \le k$, that are inductively defined by the following rules:

1. if $k = l = 2$ then

$$T_{2,2} = \begin{pmatrix} I_q & I_q & I_q & \dots & I_q & P_1^{-1} \\ I_q & P_1 & P_{\alpha_2} & \dots & P_{\alpha_{q-1}} & I_q \\ I_q & P_{\alpha_2} & P_{\alpha_2^2} & \dots & P_{\alpha_2\alpha_{q-1}} & P_{\alpha_2}P_1^{-1} \\ \vdots & & & & & \\ I_q & P_{\alpha_{q-1}} & P_{\alpha_{q-1}\alpha_2} & \dots & P_{\alpha_{q-1}^2} & P_{\alpha_{q-1}}P_1^{-1} \\ E_0 & E_1 & E_2 & \dots & E_{q-1} & E_1 \end{pmatrix}; \tag{18}$$

2. if $k > l$ then

$$T_{k,l} = \begin{pmatrix} I_q \otimes T_{k-1,l} & O \\ O & I_q \end{pmatrix}; \tag{19}$$

3. if $k = l > 2$ then

$$T_{k,k} = \begin{pmatrix} I_{\theta(q,k-1)} \otimes I_q & I_{\theta(q,k-1)} \otimes I_q & \dots & I_{\theta(q,k-1)} \otimes I_q & \mathbf{1} \otimes P_1^{-1} \\ I_{\theta(q,k-1)} \otimes I_q & I_{\theta(q,k-1)} \otimes P_1 & \dots & I_{\theta(q,k-1)} \otimes P_{\alpha_{q-1}} & \mathbf{1} \otimes I_q \\ I_{\theta(q,k-1)} \otimes I_q & I_{\theta(q,k-1)} \otimes P_{\alpha_2} & \dots & I_{\theta(q,k-1)} \otimes P_{\alpha_2\alpha_{q-1}} & \mathbf{1} \otimes P_2 \cdot P_1^{-1} \\ \vdots & & & & \\ I_{\theta(q,k-1)} \otimes I_q & I_{\theta(q,k-1)} \otimes P_{\alpha_{q-1}} & \dots & I_{\theta(q,k-1)} \otimes P_{\alpha_{q-1}^2} & \mathbf{1} \otimes P_{\alpha_{q-1}} \cdot P_1^{-1} \\ E_0 \;\; O & E_1 \;\; O & \dots & E_{q-1} \;\; O & I_q \end{pmatrix}. \tag{20}$$

Theorem 2.3. *Let χ be the characteristic vector of a linear $[n,k]_q$ code. Then*

$$\left(\widetilde{M}_k^{[\chi]}(l)\right)^{\mathrm{T}} = T_{k,l} \cdot \left(\widetilde{M}_k^{[\chi]}(l-1)\right)^{\mathrm{T}}, \quad l = 2, \dots, k, \tag{21}$$

and

$$\left(\widetilde{M}_k^{[\chi]}\right)^{\mathrm{T}} = T_{k,k} \cdot T_{k,k-1} \cdots T_{k,2} \cdot \widetilde{\chi}^{\mathrm{T}}. \tag{22}$$

2.4 Reduced characteristic distribution

Definition 2.5. Let $\chi \in \mathbb{Z}^t$ and $b \in \mathbb{F}_q^t$, $t \in \mathbb{N}$. The *reduced characteristic distribution* of the vector b with respect to χ is the vector

$$b^{[\chi]_r} = (\mu_0 - \mu_1, \dots, \mu_0 - \mu_{q-1}) \in \mathbb{Z}^{q-1},$$

where $b^{[\chi]} = (\mu_0, \mu_1, \dots, \mu_{q-1})$ is the characteristic distribution of b with respect to χ.

Lemma 2.4. *If $\chi \in \mathbb{Z}^t$ and $b \in \mathbb{F}_q^t$, $t \in \mathbb{N}$ then*

$$(b^{[\chi]_r})^{\mathrm{T}} = \begin{pmatrix} 1 & -1 & 0 & \cdots & 0 & 0 \\ 1 & 0 & -1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & 0 & 0 & \cdots & -1 & 0 \\ 1 & 0 & 0 & \cdots & 0 & -1 \end{pmatrix} \cdot (b^{[\chi]})^{\mathrm{T}}.$$

Analogously to what was described in the previous section, the notions reduced characteristic distribution of matrices, partial reduced characteristic distribution and its vector representation can be introduced.

Lemma 2.5. *Let χ be the characteristic vector of a linear $[n,k]_q$ code with full length. So the sum of coordinates of $\widetilde{M}_k^{[\chi]_r}$ is $-n$.*

2.5 Complexity of the algorithms and experimental results

The total complexity of the described algorithm is

$$\sum_{l=2}^{k} \frac{q^{k+2} - q^{k+2-l} + q^{k-1} - q^{k-l}}{q-1} = (k-1)\frac{q^{k+2} + q^{k-1}}{q-1} - \frac{(q^2+1)(q^{k-1}-1)}{(q-1)^2}.$$

This gives that for a fixed q the complexity of the algorithm is $O(kq^k)$. When k and q are considered as variables, the running time is $O(kq^{k+1})$.

Remark 2.1. Comparison between the approved algorithm and Algorithm 9.8 (Walsh transform over a prime finite field $\mathbb{F}_p$) in [16] was done. According to Joux, the complexity of the second algorithm if p varies is $O(kp^{k+2})$.

The presented approach is implemented in a C/C++ program [6]. To compare the efficiency, the C program is used where the algorithm described in [7] is embedded. The efficiency of the last algorithm is as the Gray code algorithms. The input data are randomly generated linear codes with lengths 30, 300, 3000, 30000 and different dimensions over finite fields with 2, 3, 4, 5 and 7 elements. For the same parameters, results that are obtained using Magma V2.25-2 by online Magma Calculator are presented.

The results show that the presented approach is faster for codes with large length. The execution time for computing the characteristic vector is negligible.

3 Some methods for computing the weight distribution of a linear code over a composite finite field

3.1 Approach by the trace code

Let $q = p^m$ where p is a prime and $m > 1$.

If G is a generator matrix of a linear $[n,k]_q$ code C then the *extended matrix* $\overline{G} = (\alpha_1 G | \alpha_2 G | \cdots | \alpha_{q-1} G)$ is a generator matrix of a linear $[(q-1)n,k]_q$ code $\overline{C}$. If the minimum weight of C is d then the minimum weight of $\overline{C}$ is $(q-1)d$.

For every vector $x \in \mathbb{F}_q^n$ let $\mathrm{Tr}(x) = (\mathrm{Tr}(x_1), \ldots, \mathrm{Tr}(x_n)) \in \mathbb{F}_p^n$.

Definition 3.1. Let C be a linear $[n,k]_q$ code with generator matrix G. The code $\mathrm{Tr}(C) = \{\mathrm{Tr}(c) | c \in C\}$ is called the *trace code* of C.

$\mathrm{Tr}(C)$ is a linear code over the finite field $\mathbb{F}_p$ with the same length as C but its dimension is less than or equal to mk [28]. Therefore instead of $\mathrm{Tr}(C)$ the trace code of $\overline{C}$ will be considered.

Lemma 3.1. *The dimension of the code* $\mathrm{Tr}(\overline{C})$ *is equal to* mk.

Corollary 3.2. *The codes* C *and* $\mathrm{Tr}(\overline{C})$ *have the same number of codewords, namely* $q^k = p^{mk}$.

Theorem 3.3. *Let* $q = p^m$ *where* p *is a prime and* $m > 1$. *Let* C *be a linear* $[n,k]_q$ *code with weight enumerator* $W(z) = \sum_{w=0}^{n} A_w z^w$. *So* $\mathrm{Tr}(\overline{C})$ *is a linear* $[(q-1)n, mk]_p$ *code with weight enumerator*

$$W_1(z) = \sum_{w=0}^{n} A_w z^{\frac{q(p-1)w}{p}}.$$

According to the theorem above, by applying the algorithm described in the previous chapter the weight distribution of a linear code C over a composite finite field can be obtained from the weight distribution of the linear code $\mathrm{Tr}(\overline{C})$ that is over a finite field. The complexity of calculations for the characteristic vector of $\mathrm{Tr}(\overline{C})$ is $O(mkqn)$ and for the characteristic distribution— $O(mkp^{mk+1}) = O(kmpq^k)$.

3.2 Approach by trace transform

In the rest of this chapter composite finite field with characteristic 2 is considered. This can easily be generalized for an other characteristic of a composite finite field.

Let $q = 2^m$ and $\beta_1, \ldots, \beta_m$ be a self-dual basis of $\mathbb{F}_{2^m}$ over $\mathbb{F}_2$. According to theorem 1.1 there exists such basis. Let by $\lambda(\alpha) = (\lambda_1(\alpha), \ldots, \lambda_m(\alpha))$ be denoted the vector $\lambda(\alpha) \in \mathbb{F}_2^m$, that corresponds to the element

$$\alpha = \lambda_1(\alpha)\beta_1 + \cdots + \lambda_m(\alpha)\beta_m \in \mathbb{F}_q.$$

For the rest of this chapter, let the elements $\alpha_0 = 0, \alpha_1, \ldots, \alpha_{q-1}$ of $\mathbb{F}_q$ be ordered the way so that the corresponding binary vectors $\lambda(0), \lambda(\alpha_1), \ldots, \lambda(\alpha_{q-1})$ are ordered lexicographically.

Let G be a generator matrix of a linear $[n,k]_q$ code C with full length where $q = 2^m$. Let f_G be the characteristic function of C according to definition 1.16. Theorem 1.6 gives the relation between the weight distribution of C and the trace transform of f_G, that by definition 1.15 is the function

$$\widehat{f}(\omega) = \sum_{x \in \mathbb{F}_q^k} f_G(x)\tau_\omega(x) = \sum_{x \in \mathbb{F}_q^k} f_G(x)(-1)^{\mathrm{Tr}(\langle \omega, x \rangle)}, \quad \omega \in \mathbb{F}_q^k. \tag{23}$$

The value vectors of $\widehat{f}$ and f_G relate by equality $TT_{\widehat{f}} = T_k \cdot TT_{f_G}$, where the indexes $\omega, x \in \mathbb{F}_q^k$, that determine the order of the rows and the columns of the matrix $T_k = (\tau_\omega(x))$ respectively, are ordered lexicographically.

Lemma 3.4. *The matrix*

$$T_1 = \left((-1)^{\mathrm{Tr}(\alpha_j \alpha_{j'})}\right)_{j,j'=0}^{q-1}$$

is the transform matrix H_m defined by (2).

The above lemma shows that

$$T_1 = H_m = \otimes^m H_1 = \otimes^m \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \tag{24}$$

Because of the transform matrix T_k is a Kroneker power of T_1, so

$$T_k = \otimes^k T_1 = \otimes^{km} H_1 = \otimes^{km} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{25}$$

and one can use a butterfly algorithm for computing the transform (23). A similar pseudocode is described by Joux [16, Algorithm 9.3].

3.3 Matrix representation of an improved algorithm

An improvement of the calculations can be performed when the transforms act only over a part of the value vector of the characteristic function that corresponds to nonproportional arguments. For the purpose, it is convenient to use the columns of the generator matrix G_k of the simplex code, inductively defined as in the scheme (13). The developed algorithm uses input data with size $\theta(q,k)$ instead of q^k. The complexity of the algorithm is $O(mkq^{k-1})$.

The matrices G_k are defined inductively by the equalities

$$G_1 = (1), \quad G_k = \begin{pmatrix} \mathbf{0} & \boldsymbol{\alpha_1} & \dots & \boldsymbol{\alpha_{q-1}} & 1 \\ G_{k-1} & G_{k-1} & \dots & G_{k-1} & \mathbf{0}^{\mathrm{T}} \end{pmatrix}, \ k \in \mathbb{N}, \ k \geq 2. \tag{26}$$

Let the columns of the matrix G_k be denoted by g_u, $u = 1, \dots, \theta(q,k)$, i. e.

$$G_k = \left(g_1 \dots g_{\theta(q,k)}\right).$$

The extended matrix $\overline{G}_k$ is defiined by the equality

$$\overline{G}_k = (0|\alpha_1 G_k| \dots |\alpha_{q-1} G_k). \tag{27}$$

This matrix consists of the all vectors in $\mathbb{F}_q^k$ as columns and *determines an order* in this set. Let the columns of the matrix $\overline{G}_k$ be denoted by $\bar{g}_t$, $t = 1, \dots, q^k$, i. e.

$$\overline{G}_k = \left(\bar{g}_1 \dots \bar{g}_{q^k}\right).$$

Let G be a generator matrix of a linear $[n,k]_q$ code C with full length where $q = 2^m$. Let f_G be the characteristic function of C according to definition 1.16. The *characteristic vector* $\chi = (\chi_1, \dots, \chi_{\theta(q,k)})$ is defined by the equalities $\chi_u = f_G(g_u)$ за $u = 1, \dots, \theta(q,k)$. The *extended characteristic vector* $\overline{\chi} = (\overline{\chi}_1, \dots, \overline{\chi}_{q^k})$ is defined by the equalities $\overline{\chi}_t = f_G(\bar{g}_t)$ за $t = 1, \dots, q^k$. From (27) it follows that for every $t_1, t_2 \in \mathbb{N}$, such that $1 < t_1 < t_2 \leq q^k$ and $t_2 - t_1$ are devisible by $\theta(q,k)$, the vectors $\bar{g}_{t_1}$ и $\bar{g}_{t_2}$ are proportional and $\overline{\chi}_{t_1} = f_G(\bar{g}_{t_1}) = f_G(\bar{g}_{t_2}) = \overline{\chi}_{t_2}$. This shows that $\overline{\chi} = (0|\chi| \dots |\chi)$.

For explanation of the algorithm the following matrices are needed:

$$\overline{M}_k = \overline{G}_k^{\mathrm{T}} \cdot \overline{G}_k = \left(\langle \bar{g}_{t_1}, \bar{g}_{t_2} \rangle\right)_{t_1,t_2=1}^{q^k},$$

$$M_k = G_k^{\mathrm{T}} \cdot G_k = \left(\langle g_{u_1}, g_{u_2} \rangle\right)_{u_1,u_2=1}^{\theta(q,k)},$$

$$\overline{P}_k = \left((-1)^{\mathrm{Tr}(\langle \bar{g}_{t_1}, \bar{g}_{t_2} \rangle)}\right)_{t_1,t_2=1}^{q^k},$$

$$P_k = \left((-1)^{\mathrm{Tr}(\langle g_{u_1}, g_{u_2}\rangle)}\right)_{u_1,u_2=1}^{\theta(q,k)},$$

$$P_{k,\alpha} = \left((-1)^{\mathrm{Tr}(\alpha\langle g_{u_1}, g_{u_2}\rangle)}\right)_{u_1,u_2=1}^{\theta(q,k)}, \quad \alpha \in \mathbb{F}_q\backslash\{0\},$$

$$\Lambda^{(\alpha)} = \left((-1)^{\mathrm{Tr}(\alpha\alpha_{j_1}\alpha_{j_2})}\right)_{j_1,j_2=0}^{q-1}, \quad \alpha \in \mathbb{F}_q\backslash\{0\}.$$

The matrix $\overline{P}_k$ can be obtained from the matrix T_k by a suitable permutation of some rows and some columns. Let $\widehat{\chi} = (\widehat{\chi}_1, \ldots, \widehat{\chi}_{q^k})$ be the vector determined by the equalities $\widehat{\chi}_t = \widehat{f}(\bar{g}_t)$ for $t = 1, \ldots, q^k$. Hence $\widehat{\chi}^{\mathrm{T}} = \overline{P}_k \cdot \overline{\chi}^{\mathrm{T}}$.

$$\overline{P}_k \cdot \overline{\chi}^{\mathrm{T}} = \begin{pmatrix} (q-1)\sum_{u=1}^{\theta(q,k)} \chi_u \\ \left(\sum_{j=1}^{q-1} P_{k,\alpha_j}\right)\chi^{\mathrm{T}} \\ \left(\sum_{j=1}^{q-1} P_{k,\alpha_j}\right)\chi^{\mathrm{T}} \\ \vdots \\ \left(\sum_{j=1}^{q-1} P_{k,\alpha_j}\right)\chi^{\mathrm{T}} \end{pmatrix}. \tag{28}$$

This means that it is not necessary to use the $2^k \times 2^k$ matrix $\overline{P}_k$ and the larger vector $\overline{\chi}$. To obtain $\widehat{\chi}$ and the weight distribution of the code, it is enough to use the characteristic vector χ, the matrix P_k and the matrices $P_{k,\alpha}$ for $\alpha \in \mathbb{F}_q\backslash\{0\}$.

$$P_k = \begin{pmatrix} & & \boldsymbol{\Lambda_0}^{\mathrm{T}} \\ & T_1 \otimes P_{k-1} & \boldsymbol{\Lambda_{\alpha_1}}^{\mathrm{T}} \\ & & \vdots \\ & & \boldsymbol{\Lambda_{\alpha_{q-1}}}^{\mathrm{T}} \\ \boldsymbol{\Lambda_0} & \boldsymbol{\Lambda_{\alpha_1}} \quad \ldots \quad \boldsymbol{\Lambda_{\alpha_{q-1}}} & \Lambda_1 \end{pmatrix}, \tag{29}$$

where $\Lambda_\alpha = (-1)^{\mathrm{Tr}(\alpha)}$ for $\alpha \in \mathbb{F}_q$ and $\boldsymbol{\Lambda_\alpha}$ is a row vector with default length and the same coordinates Λ_α. The last equality and (24) give possibility to apply a butterfly algorithm for computing $P_k \cdot \chi^{\mathrm{T}}$.

Let the characteristic vector χ be split in parts as follows

$$\chi = (\chi^{(0)}|\chi^{(1)}|\ldots|\chi^{(q-1)}|\chi_{\theta(q,k)}), \tag{30}$$

where $\chi^{(0)}, \chi^{(1)}, \ldots, \chi^{(q-1)} \in \mathbb{Z}^{\theta(q,k-1)}$.

Let $Num(\alpha) \in \{0, 1, \ldots, q-1\}$ be the position of the element α in the order of the field $\mathbb{F}_q$, i. e. $\alpha_{Num(\alpha)} = \alpha$. Therefore

$$P_k \cdot \chi^{\mathrm{T}} = \begin{pmatrix} (T_1 \otimes I_{\theta(q,k-1)}) \cdot \begin{pmatrix} P_{k-1} \cdot {\chi^{(0)}}^{\mathrm{T}} \\ P_{k-1} \cdot {\chi^{(1)}}^{\mathrm{T}} \\ \vdots \\ P_{k-1} \cdot {\chi^{(Num(1))}}^{\mathrm{T}} + \chi_\theta . \mathbf{1}^{\mathrm{T}} \\ \vdots \\ P_{k-1} \cdot {\chi^{(q-1)}}^{\mathrm{T}} \end{pmatrix} \\ \Lambda_0 \sum \chi^{(0)} + \cdots + \Lambda_1 \left(\chi_\theta + \sum \chi^{(Num(1))} \right) + \cdots + \Lambda_{\alpha_{q-1}} \sum \chi^{(q-1)} \end{pmatrix}, \quad (31)$$

where for short $\theta = \theta(q,k)$ and $\sum \chi^{(j)}$ denotes the sum of coordinates of $\chi^{(j)}$, $j = 0, 1, \ldots, q-1$.

For $1 < l < k$ it is hold

$$P_l \cdot {\chi'}^{\mathrm{T}} + \chi_\theta . \mathbf{1}^{\mathrm{T}} = \begin{pmatrix} \left(T_1 \otimes I_{\theta(q,l-1)}\right) \cdot \begin{pmatrix} P_{l-1} \cdot {\chi'^{(0)}}^{\mathrm{T}} + \chi_\theta . \mathbf{1}^{\mathrm{T}} \\ P_{l-1} \cdot {\chi'^{(1)}}^{\mathrm{T}} \\ \vdots \\ P_{l-1} \cdot {\chi'^{(Num(1))}}^{\mathrm{T}} + \chi'_{\theta(q,l-1)} . \mathbf{1}^{\mathrm{T}} \\ \vdots \\ P_{l-1} \cdot {\chi'^{(q-1)}}^{\mathrm{T}} \end{pmatrix} \\ \Lambda_0 \left(\chi_\theta + \sum \chi'^{(0)} \right) + \Lambda_{\alpha_1} \sum \chi'^{(1)} + \ldots \end{pmatrix}, \quad (32)$$

where χ' is a vector with length $\theta(q,l)$ that is a suitable part of χ. From this equality by induction one can prove that for computing $P_{k-1} \cdot {\chi^{(Num(1))}}^{\mathrm{T}} + \chi_\theta . \mathbf{1}^{\mathrm{T}}$ it is enough to add χ_θ only to the first coordinate of the vector $\chi^{(Num(1))}$, previously multiplied by Λ_1. For calculating the last coordinate of $P_k \cdot \chi^{\mathrm{T}}$ one needs add χ_θ to the same coordinate, but without previous multiplication. These observations give the possibility to do some previous operations with the value of χ_θ and with the last coordinates of all blocks $\chi'^{(j)}$, $j = 0, \ldots, q-1$.

Consider the matrices $P_{k,\alpha}$ for $\alpha \in \mathbb{F}_q \backslash \{0\}$. For $k = 1$ the matrices are

$P_{1,\alpha} = (\Lambda_\alpha)$. For the recurrent step it is hold

$$P_{k,\alpha}\cdot\chi^{\mathrm{T}} = \begin{pmatrix} (\Lambda^{(\alpha)}\otimes I_{\theta(q,k-1)})\cdot \begin{pmatrix} P_{k-1,\alpha}\cdot{\chi^{(0)}}^{\mathrm{T}} \\ P_{k-1,\alpha}\cdot{\chi^{(1)}}^{\mathrm{T}} \\ \vdots \\ P_{k-1,\alpha}\cdot{\chi^{(Num(1))}}^{\mathrm{T}} + \chi_\theta.\mathbf{1}^{\mathrm{T}} \\ \vdots \\ P_{k-1,\alpha}\cdot{\chi^{(q-1)}}^{\mathrm{T}} \end{pmatrix} \\ \Lambda_0\sum\chi^{(0)} + \Lambda_{\alpha\alpha_1}\sum\chi^{(1)} + \cdots + \Lambda_\alpha\left(\chi_\theta + \sum\chi^{(Num(1))}\right) + \cdots \end{pmatrix}. \tag{33}$$

The multiplication by $\alpha \neq 0$ can be considered as a permutation of the elements of $\mathbb{F}_q$, so the matrix $\Lambda^{(\alpha)}$ can be obtained from the matrix $T_1 = \Lambda^{(1)}$ by a suitable permutation of rows (and/or columns)). Let $\pi_\alpha \in S_q$ be the permutation defined by the equality $\pi_\alpha(j) = j'$, where $\alpha_{j'} = \alpha\alpha_j$, $j = 0, 1, \ldots, q-1$. The permutation π_α induces a permutation of the blocks of columns in the matrix $T_1 \otimes I_{\theta(q,k-1)}$. Hence

$$P_{k,\alpha}\cdot\chi^{\mathrm{T}} = \begin{pmatrix} (T_1\otimes I_{\theta(q,k-1)})\cdot \begin{pmatrix} P_{k-1,\alpha}\cdot{\chi^{(\pi_\alpha^{-1}(0))}}^{\mathrm{T}} \\ P_{k-1,\alpha}\cdot{\chi^{(\pi_\alpha^{-1}(1))}}^{\mathrm{T}} \\ \vdots \\ P_{k-1,\alpha}\cdot{\chi^{(\pi_\alpha^{-1}(Num(\alpha)))}}^{\mathrm{T}} + \chi_\theta.\mathbf{1}^{\mathrm{T}} \\ \vdots \\ P_{k-1,\alpha}\cdot{\chi^{(\pi_\alpha^{-1}(q-1))}}^{\mathrm{T}} \end{pmatrix} \\ \Lambda_0\sum\chi^{(0)} + \Lambda_{\alpha\alpha_1}\sum\chi^{(1)} + \cdots + \Lambda_\alpha\left(\chi_\theta + \sum\chi^{(Num(1))}\right) + \cdots \end{pmatrix}, \tag{34}$$

where $\pi_\alpha^{-1}(Num(\alpha)) = Num(1)$.

The comparison between the equalities (31) and (34) shows that for calculating the coordinates (without the last one) a multiplication by the same matrix $T_1 \otimes I_{\theta(q,k-1)}$ is used. In the last equality the blocks $P_{k-1,\alpha}\cdot{\chi^{(j)}}^{\mathrm{T}}$ are permuted. By induction, these permutations can be transferred over the coordinates of the vector χ. Likewise, χ_θ and the last elements of the intermediate blocks are added to a determined positions in χ. The modified vector in this way is denoted by $\pi_\alpha(\chi)$ below.

In the improved algorithm, to compute $\left(\sum_{j=1}^{q-1} P_{k,\alpha_j}\right)\chi^{\mathrm{T}}$ directly the sum

$$SP(\chi) = \pi_{\alpha_1}(\chi) + \pi_{\alpha_2}(\chi) + \cdots + \pi_{\alpha_{q-1}}(\chi)$$

is used and in addition only one modification of χ is used.

3.4 Description of the improved algorithm

3.4.1 Precomputation

Let $\rho : \mathbb{Z}_{\theta(q,k)} \to \mathbb{Z}^{k-1}$ be a map defined as follows: if $0 \le z \le \theta(q,k) - 1$ and $\rho(z) = (\rho_1, \ldots, \rho_{k-1})$, then

$$\rho_1 = \left\lfloor \frac{z}{\theta(q,k-1)} \right\rfloor, \quad \rho_t = \left\lfloor \frac{z - \sum_{s=1}^{t-1} \rho_s \theta(q,k-s)}{\theta(q,k-t)} \right\rfloor \text{ за } t = 2, \ldots, k-1.$$

Lemma 3.5. *If $0 \le z \le \theta(q,k) - 1$ and $\rho(z) = (\rho_1, \ldots, \rho_{k-1})$, then*

$$z = \rho_1\theta(q,k-1) + \rho_2\theta(q,k-2) + \cdots + \rho_{k-2}\theta(q,2) + \rho_{k-1},$$

and $0 \le \rho_t \le q$, $t = 1, \ldots, k-1$.

Corollary 3.6. *The map ρ is injective.*

Lemma 3.7. *If $0 \le z \le \theta(q,k) - 1$, $\rho(z) = (\rho_1, \ldots, \rho_{k-1})$ and there exists an index $t \in \{1, \ldots, k-1\}$ such that $\rho_t = q$ and $\rho_s < q$ за $s = 1, \ldots, t-1$, then $\rho_{t+1} = \cdots = \rho_{k-1} = 0$.*

A small modification of the vector $\rho(z)$ is more convenient for the developed algorithm. For this purpose the map $\nu : \{1, \ldots, \theta(q,k)\} \to \mathbb{Z}^{k-1}$, defined by

$$\nu(z) = \begin{cases} \rho(z), & \text{if } \rho_t < q \text{ for all } t = 1, \ldots, k-1, \\ (\rho_1, \ldots, \rho_{t-1}, q, \ldots, q), & \text{if } \rho_t = q \text{ for some } t \le k-1, \end{cases}$$

is used.

Let $\kappa : \mathbb{F}_q^{k-1} \to \mathbb{Z}$ be the map defined by the equality

$$\kappa(\alpha_{j_1}, \ldots, \alpha_{j_{k-1}}) = \rho^{-1}(j_1, \ldots, j_{k-1}) + 1.$$

Obviously, the images of the vectors in $\mathbb{F}_q^{k-1}$ are positive integers less than or equal to $\theta(q,k)$. Moreover, the different vectors have different images. If u, where $1 \le u \le \theta(q,k)$, is not an image of the map κ, then the corresponding coordinate χ_u of the characteristic vector χ is called an *inactive coordinate*. Indeed, χ_u is an inactive coordinate if the last coordinate of the vector $\nu(u-1)$ is q.

In the developed algorithm three arrays with length $\theta(q,k)$ are used. They are denoted by $\chi(0)$, $\chi(1)$ and S. The arrays $\chi(0)$ and $\chi(1)$ play a role of modified copies of the characteristic vector χ. If the last coordinate of $\nu(u-1)$ is not equal to q, then $\chi(s)[u] = (-1)^s\chi_u$, for $u = 1, \ldots, \theta(q,k)$ and $s = 0, 1$. Inactive coordinates of χ are added to a suitable positions in the copies. The array S serves to form the vector $SP(\chi)$.

3.4.2 Main algorithm

A butterfly algorithm over the sum S and the vector $\chi(0)$ is performed. As a result S takes value $\left(\sum_{j=1}^{q-1} P_{k,\alpha_j}\right)\chi^{\mathrm{T}}$. Throughout the procedure the right places of inactive coordinates are searched. For this purpose suitable permutations are applied. The realization is with the help of the maps σ_l, $\nu^{(l)}$ and ν^{-1}. The butterfly algorithms for S and $\chi(0)$ are similar to the algorithm described in the section 3.2.

3.4.3 Complexity analysis

The total complexity of the improved algorithm is $O(kmq^{k-1})$.

It is easy to see that the complexity of the algorithm from the section 3.2 is $O(kmq^k)$. Furthermore the array with size q^k is used, while the improved algorithm uses three arrays with lengths $\theta(q,k) = (q^k-1)/(q-1)$. The described improved algorithm is more effective than the previous algorithms for computing the weight distribution especially when the length n and/or the number of the elements of the considered field q are large numbers.

4 Computing the covering radius of a linear code over a finite field by discrete transforms

To clarify the relation between the matter considered in this chapter and the algorithms in the previous chapters the following concept is needed.

Definition 4.1. Let $b \in \mathbb{Z}^\theta$ be a vector with length $\theta(q,k)$ and integer coordinates. For every row vector c of the matrix M_k let be defined the vector

$$c^{[b]_r} = (\mu_0 - \mu_1, \ldots, \mu_0 - \mu_{q-1}),$$

where $\mu_0, \mu_1, \ldots, \mu_{q-1}$ are the coordinates of $c^{[b]}$. The matrix $M_k^{[b]_r}$ consists of the vectors $c^{[b]_r}$ as rows. The sum of the columns of $M_k^{[b]_r}$ is called the *reduced distribution* of b and is denoted by $r(b)$.

Lemma 4.1. *The reduced distribution $r(b)$ of the vector $b \in \mathbb{Z}^\theta$ is*

$$r(b) = [(q-1)J - q\mathcal{N}(M_k)]b^T$$

where J is the $\theta \times \theta$ all 1's matrix.

4.1 Computing the covering radius of a linear code over a prime finite field

In this section only prime fields are considered. So q is a prime and $\mathbb{F}_q = \mathbb{Z}_q = \{0, 1, \ldots, q-1\}$.

Let C be a linear $[n,k]_q$ code with a parity check matrix H. The characteristic function of the matrix H is defined by

$$h_H(x) = \begin{cases} 1, & \text{if } x \text{ is proportional to a column of } H, \\ 0, & \text{otherwise,} \end{cases} \tag{35}$$

where the proportion coefficients have to be nonzero. This characteristic function is used to compute the covering radius of the code. The following theorem is hold for prime $q \geq 3$. A similar result is published [18, Theorem 2] for the case $q = 2$.

Theorem 4.2. *Let C be a linear $[n,k]_q$ code with a parity check matrix H, where q is an odd prime, and $\widehat{h} : \mathbb{F}_q^{n-k} \to \mathbb{C}$ be the Vilenkin-Chrestenson transform of the characteristic function $h = h_H$. Then the covering radius $R(C)$ is equal to the smallest positive integer t such that $\widehat{\widehat{h}^t}(y) \neq 0$ for all vectors $y \in \mathbb{F}_q^{n-k}$, $y \neq \mathbf{0}$.*

Remark 4.1. The same method can be used for computing the weight distribution of the coset leaders of a linear code over $\mathbb{F}_q$ for an odd prime q. If $t \geq 2$ is an integer, then the number of the coset leaders of weight t is equal to the number of the vectors $y \in \mathbb{F}_q^{n-k} \backslash \{\mathbf{0}\}$ such that $\widehat{\widehat{h}^t}(y) \neq 0$ and $\widehat{\widehat{h}^{t-1}}(y) = 0$. The number of the coset leaders of weight 1 is equal to the number of the nonzero vectors $y \in \mathbb{F}_q^{n-k}$ such that $h(y) \neq 0$.

Let $g_1, \ldots, g_\theta$ be the columns of the generator matrix G_s of the simplex code defined by (13). It is satisfied

$$\widehat{h}(\mathbf{0}) = \sum_{x \in \mathbb{F}_q^s} h(x) v_{\mathbf{0}}(x) = \sum_{x \in \mathbb{F}_q^s} h(x) = h(\mathbf{0}) + (q-1) \sum_{u=1}^{\theta} h(g_u) \tag{36}$$

and

$$\begin{aligned} \widehat{h}(g_i) &= \sum_{x \in \mathbb{F}_q^s} h(x) v_{g_i}(x) = h(\mathbf{0}) + \sum_{u=1}^{\theta} \sum_{j=1}^{q-1} h(g_u) v_{g_i}(j g_u) \\ &= h(\mathbf{0}) + \sum_{u=1}^{\theta} h(g_u) \sum_{j=1}^{q-1} \left(\xi^{\langle g_i, g_u \rangle}\right)^j, \quad i = 1, \ldots, \theta. \end{aligned} \tag{37}$$

Lemma 4.3. *Let q be an odd prime and $h : \mathbb{F}_q^s \to \mathbb{Z}$ be a function with the property $h(x) = h(\alpha x)$ for all $\alpha \in \mathbb{F}_q \backslash \{0\}$ and $x \in \mathbb{F}_q^s$. If $\widehat{h} : \mathbb{F}_q^s \to \mathbb{C}$ is the Vilenkin-Chrestenson transform of h then $\widehat{h}$ is actually an integer valued function and $\widehat{h}(\omega) = \widehat{h}(\alpha\omega)$ for all $\alpha \in \mathbb{F}_q \backslash \{0\}$ and $\omega \in \mathbb{F}_q^s$.*

Corollary 4.4. *Let C be a linear $[n,k]_q$ code with a parity check matrix H, where q is an odd prime, and $\widehat{h} : \mathbb{F}_q^{n-k} \to \mathbb{C}$ be the Vilenkin-Chrestenson transform of the characteristic function $h = h_H$. Then the covering radius $R(C)$ is equal to the smallest positive integer t such that $\widehat{\widehat{h}^t}(g_i) \neq 0$ for all $i = 1, \ldots, \theta(q, n-k)$.*

The above corollary shows that it is enough to calculate $\widehat{\widehat{h}^t}(\mathbf{0})$ и $\widehat{\widehat{h}^t}(g_i)$ for $i = 1, \ldots, \theta(q, n-k)$. Because of

$$\sum_{j=1}^{q-1} \left(\xi^{\langle g_i, g_u \rangle}\right)^j = \begin{cases} q-1, & \text{if } \langle g_i, g_u \rangle = 0, \\ -1, & \text{if } \langle g_i, g_u \rangle \neq 0, \end{cases} \tag{38}$$

from (37) follows that

$$\widehat{h}(\alpha g_i) = \widehat{h}(g_i) = h(\mathbf{0}) + \sum_{u=1}^{\theta(q,s)} r_{iu} h(g_u),$$

where $\alpha \in \mathbb{F}_q \backslash \{0\}$ ans

$$r_{iu} = \begin{cases} q-1, & \text{if } \langle g_i, g_u \rangle = 0, \\ -1, & \text{if } \langle g_i, g_u \rangle \neq 0. \end{cases}$$

If $b = (h(g_1), \ldots, h(g_\theta))$, then

$$\begin{pmatrix} \widehat{h}(\mathbf{0}) \\ \widehat{h}(g_1) \\ \vdots \\ \widehat{h}(g_\theta) \end{pmatrix} = \begin{pmatrix} \widehat{h}(\mathbf{0}) \\ h(\mathbf{0}).\mathbf{1}^{\mathrm{T}} + \Lambda \cdot b^{\mathrm{T}} \end{pmatrix} = \begin{pmatrix} h(\mathbf{0}) + (q-1)\sum_{u=1}^{\theta} h(g_u) \\ \\ h(\mathbf{0}).\mathbf{1}^{\mathrm{T}} + r(b)^{\mathrm{T}} \end{pmatrix}. \tag{39}$$

To compute $r(b)$ the algorithm described in Chapter 2 is applicable.

4.2 Computing the covering radius of a linear code over a composite finite field

In this section composite fields are considered, i. e. $q = p^m$ where p is a prime, $m \geq 2$ is a positive integer and $\mathbb{F}_p = \mathbb{Z}_p = \{0, 1, \ldots, p-1\}$. The results from the previous section can be reformulated for composite fields by using the trace transform.

Theorem 4.5. *Let C be a linear $[n,k]_q$ code with a parity check matrix H where $q = p^n$ for an odd prime p, and $\widehat{h} : \mathbb{F}_q^{n-k} \to \mathbb{C}$ be the trace transform of the characteristic function $h = h_H$. Then the covering radius $R(C)$ is equal to the smallest positive integer t such that $\widehat{\widehat{h}}^t(y) \neq 0$ for all vectors $y \in \mathbb{F}_q^{n-k}$, $y \neq \mathbf{0}$.*

Theorem 4.6. *Let C be a linear $[n,k]_q$ code with parity check matrix H where $q = 2^m$, and $\widehat{h} : \mathbb{F}_q^{n-k} \to \mathbb{C}$ be the trace transform of the characteristic function $h = h_H$. Let*

$$\varphi_t(\omega) = \sum_{l=1}^{t} \left(\widehat{h}(\omega)\right)^l, \ \omega \in \mathbb{F}_q^{n-k}, \quad t = 1, \ldots, n,$$

and $\widehat{\varphi}_t : \mathbb{F}_q^{n-k} \to \mathbb{C}$ be the trace transform of φ_t. Then the covering radius $R(C)$ is equal to the smallest positive integer t such that $\widehat{\varphi}_t(y) \neq 0$ for all $y \in \mathbb{F}_q^{n-k}$, $y \neq \mathbf{0}$.

Lemma 4.7. *Let $q = p^m$ for a prime p and $h : \mathbb{F}_q^s \to \mathbb{Z}$ be a function with the property $h(x) = h(\alpha x)$ for all $\alpha \in \mathbb{F}_q \backslash \{0\}$ and $x \in \mathbb{F}_q^s$. if $\widehat{h} : \mathbb{F}_q^s \to \mathbb{C}$ is the trace transform of h, than $\widehat{h}$ is actually an integer valued function and $\widehat{h}(\omega) = \widehat{h}(\alpha\omega)$ for all $\alpha \in \mathbb{F}_q \backslash \{0\}$ and $\omega \in \mathbb{F}_q^s$.*

Again, the reduced distribution can be used to compute the covering radius. For this purpose, the algorithms described in the previous chapters are applicable.

Conclusion

Solutions of the problems of computing the weight distribution and the covering radius of a linear code over a finite field are presented in the dissertation. For this purpose the generator (parity check) matrix is represented by a characteristic vector that determines the number of the columns proportional by nonzero coefficient to the columns of a specially chosen generator matrix of the simplex code. Some algorithms are developed depending on the finite field (prime or composite). As a basis of this work, the Walsh-Hadamard transform, Vilenkin-Chrestenson transform and trace transform are used. Due to the transition to a characteristic vector, the proposed algorithms have a less complexity. The algorithms are notably effective to linear codes with large length and to finite fields with the large number of elements.

Scientific contributions

Main scientific contributions in the dissertation are:

1. The knowledge for discrete Walsh-Hadamard transform, discrete Vilenkin-Chrestenson transform and trace transform are studied and systematized. Their application for computing the weight distribution of a linear code is shown.

2. A special type of a generator matrix of the simplex code is defined. This is convenient for determining the characteristic vector of a generator (parity check) matrix of a linear code. These definitions help to obtain natural recurrent relations between transform matrices of different orders.

3. For linear codes over prime fields with characteristic $p > 2$, an algorithm for computing the weight distribution from a given characteristic vector is developed. This algorithm has a complexity $O(kp^{k+1})$, that is p times smaller than the complexity of the algorithms known so far.

4. For linear codes over composite finite fields, a general algorithm for computing the weight distribution from a given extended characteristic vector is developed. This algorithm uses the trace transform and self-dual basis. Thus the considered transform is reduced to the Walsh-Hadamard transform (for characteristic 2) or the Vilenkin-Chrestenson transform. The complexity of the algorithm is $O(kmq^k)$.

5. For linear codes over composite finite fields, an improved algorithm for computing the weight distribution from a given characteristic vector is developed. The complexity is decreasing q times. This algorithm is described in detail for composite fields with characteristic 2.

6. Some methods for computing the covering radius of a linear code over a finite field (prime or composite) from a given characteristic vector of a parity check matrix are developed. These methods are generalizations of the proposed by Karpovsky method for binary linear codes.

7. The developed algorithms are presented by theoretical justifications, descriptions and diagrams.

Dissertation Publications

[P1] Bouyukliev, I., and Piperkov. P. On Walsh transform and matrix factorization. In *Eight International Workshop on Optimal Codes and Related Topics. Jul 10-14, 2017. Sofia, Bulgaria* (2017), pp. 55-60. ISSN 1313-1167.

[P2] Piperkov, P., Bouyukliev, I., and Bouyuklieva, S. An algorithm for computing the weight distribution of a linear code over composite finite field with characteristic 2. In *Recent Topics in Differential Geome-*

try and its Related Fields, T. Adachi and H. Hashimoto, Eds. World Scientific Publishing Company, 2019, pp. 163-181. ISBN 978-981-120-668-9. DOI:10.1142/9789811206696_0011.

[P3] Bouyukliev, I., Bouyuklieva, S., Maruta, T., and Piperkov, P. Characteristic vector and weight distribution of a linear code. *Cryptography and Communications 13*, 2 (2021), 263-282. ISSN 1936-2447. DOI:10.1007/s12095-020-00458-8.

[P4] Piperkov, P., Bouyukliev, I., and Bouyuklieva, S. An algorithm for computing the covering radius of a linear code based on Vilenkin-Chrestenson transform. In *New Horizons in Differential Geometry and its Related Fields,* T. Adachi and H. Hashimoto, Eds. World Scientific Publishing Company, 2022, pp. 105–123. ISBN 978-981-124-809-2. DOI:10.1142/9789811248108_0007.

References

[1] Assmus, E. F., and Mattson, H. F. Coding and combinatorics. *SIAM Review 16*, 1 (1974), 349–388.

[2] Berlecamp, E. R. *Algebraic Coding Theory.* McGraw-Hill, New York, 1968.

[3] Bespalov, M. S. Discrete Chrestenson transform. *Probl. Inf. Transm. 46*, 4 (2010), 353–375.

[4] Betten, A., Braun, M., Fripertinger, H., Kerber, A., Kohnert, A., and Wassermann, A. *Error-Correcting Linear Codes: Classification by Isometry and Applications.* Springer-Verlag, Berlin, 2006.

[5] Blahut, R. E. *Fast Algorithms for Signal Processing.* Cambridge University Press, Cambridge, 2010.

[6] Bouyukliev, I. The program WDHV v1.0 (a module in QextNewEdition). https://zenodo.org/record/3968198#.YpiUrDlBxH5, 2020. Accessed: 2022-06-02.

[7] Bouyukliev, I., and Bakoev, V. A method for efficiently computing the number of codewords of fixed weights in linear codes. *Discret. Appl. Math. 156*, 15 (2008), 2986–3004.

[8] Carlet, C. Boolean functions for cryptography and error-correcting codes. In *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, Y. Crama and P. Hammer, Eds., vol. 134 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, 2010, pp. 257–397.

[9] Carlet, C. Vectorial Boolean functions for cryptography. In *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, Y. Crama and P. Hammer, Eds., vol. 134 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, 2010, pp. 398–470.

[10] Chrestenson, H. E. A class of generalized Walsh functions. *Pacific J. of Math. 5*, 1 (1955), 17–31.

[11] Cooley, J. W., and Tukey, J. W. An algorithm for the machine calculation of complex Fourier series. *Math. Comp. 19* (1965), 297–301.

[12] Elliott, D. F., and Rao, K. R. *Fast Transforms. Algorithms, Analyses, Applications*. Academic Press, London, 1982.

[13] Farkov, Y. A. Discrete wavelets and the Vilenkin-Chrestenson transform. *Math. Notes 89* (2011), 871–884.

[14] Good, I. J. The interaction algorithm and practical Fourier analysis. *J. of the Royal Stat. Soc., Ser. B. 20* (1958), 361–372.

[15] Huffman, W. C., and Pless, V. *Fundamentals of Error-Correcting Codes*. Cambridge Univ. Press, 2003.

[16] Joux, A. *Algorithmic Cryptanalysis*. Chapman and Hall/CRC, Boca Raton, FL 33487-2742, 2009.

[17] Karpovsky, M. G. On the weight distribution of binary linear codes. *IEEE Trans. Inform. Theory 25*, 1 (1979), 105–109.

[18] Karpovsky, M. G. Weight distribution of translates, covering radius, and perfect codes correcting errors of given weights. *IEEE Trans. Inform. Theory 27*, 4 (1981), 462–472.

[19] Karpovsky, M. G., Stanković, R. S., and Astola, J. T. *Spectral Logic and its Applications for the Design of Digital Devices*. John Wiley & Sons Ltd, 2008.

[20] Lechner, R. J. Comment on "Computation of the fast Walsh-Fourier transform". *IEEE Trans. Comp. C-19* (1970), 174.

[21] Lidl, R., and Niederreiter, H. *Introduction to Finite Fields and their Applications*. Cambridge University Press, 1986.

[22] MacWilliams, F. J., and Sloane, N. J. A. *The Theory of Error-Correcting Codes*. Elsevier Science Publishers, 1977.

[23] Mullen, G. L., and Panario, D. *Handbook of Finite Fields*. Chapman and Hall/CRC, Boca Raton, FL 33487-2742, 2013.

[24] Pless, V. S., and Huffman, W. C. *Handbook on Coding Theory*. Elsevier Science B.V., 1998.

[25] Seroussi, G., and Lempel, A. Factorization of symmetric matrices and trace-orthogonal bases in finite fields. *SIAM Journal on Computing 9*, 4 (1980), 758–767.

[26] Shanks, J. L. Computation of the fast Walsh-Fourier transform. *IEEE Trans. Comp. C-18*, 5 (1969), 457–459.

[27] Stanković, R. S., Astola, J. T., and Moraga, C. *Representation of Multiple-Valued Logic Functions*, vol. 37 of *Synthesis Lectures on Digital Circuits and Systems*. Morgan & Claypool, 2012.

[28] Stichtenoth, H. Subfield subcodes and trace codes. In *Algebraic Function Fields and Codes*, vol. 254 of *Graduate Texts in Mathematics*. Springer-Verlag, 2009, pp. 311–326.

[29] Vilenkin, N. On a class of complete orthonormal systems. *Bull. Acad. Sci. URSS. Sér. Math. 11* (1947), 363–400.

[30] Walsh, J. L. A closed set of normal orthogonal functions. *American Journal of Math. 45*, 1 (1923), 5–24.