Dual transform and projective self-dual codes

Iliya Bouyukliev* and Stefka Bouyuklieva†

Abstract

We present and analyze the relationship between different linear codes through the (projective) dual transform. The considered codes are represented by a generator matrix or a characteristic vector. We pay special attention to projective self-dual codes and present constraints on the lengths and dimensions of these codes over the prime and composite finite fields.

1 Introduction

There is a natural duality between points and hyperplanes in the projective geometry $PG(k-1,q)$: any point $a=(a_1,a_2,\ldots,a_k)$ defines a hyperplane H_a which consists of all points $x=(x_1,x_2,\ldots,x_k)$ such that $(a,x)=\sum a_ix_i=0$. This duality (known as projective duality or Delsarte duality) is useful in the study of two-weight codes (see [3, 5, 7]). A generalization of the projective duality was given by Dodunekov and Simonis in [6].

The authors use different definitions of dual transformation depending on the purpose for which they use it. Usually the transform is defined constructively in terms of projective geometry [3, 6, 8], or by matrices [1, 3]. In [2], we used a new perspective that allows algebraic proofs of the statements. The linear codes are presented by their characteristic vector, and the characteristic vector of the projective dual of a linear code is obtained as a product of a special matrix by the characteristic vector of the input code. Using the same matrix we can easily calculate the weights of the linear code and its projective dual code and to prove formulas for the length and dimension. We apply this approach to prove more properties of the projective dual codes and more applications of the projective dual transform.

In Section 2 we define the projective dual transform and give the main statements and formulas. Section 3 is devoted to the projective self-dual codes.

*I. Bouyukliev is with the Institute of Mathematics and Informatics, Bulgarian Academy of Sciences, P.O. Box 323, Veliko Tarnovo, BULGARIA. Email: iliyab@math.bas.bg

†S. Bouyuklieva is with the Faculty of Mathematics and Informatics, St. Cyril and St. Methodius University of Veliko Tarnovo, BULGARIA. Email: stefka@ts.uni-vt.bg. The research of this author was supported, in part, by a Bulgarian NSF contract KP-06-N32/2-2019.

2 Dual transform

Let q be a prime power and C be a linear $[n,k;q]$ code over the finite field $\mathbb{F}_q$ with nonzero weights w_1, $w_2,\ldots,w_t$. Let G be an $m\times n$ matrix that generate the code C ($m\geq k$, $\mathrm{rank}(G)=k$). Obviously, any column from the matrix G can be considered as a point in the projective geometry $PG(m-1,q)$. If we put all points of $PG(m-1,q)$ in a matrix S_m as columns, then S_m generates the simplex code $\mathcal{S}_{m,q}$ of length $\theta(m,q)=\frac{q^m-1}{q-1}$, dimension m and only one nonzero weight q^{m-1}.

Further, we consider the matrix $M_m=S_m^T\cdot S_m$, where the multiplication is over $\mathbb{F}_q$. The rows of M_m are nonproportional codewords in the simplex code $\mathcal{S}_{m,q}$. Since $M_m^T=(S_m^T\cdot S_m)^T=S_m^T\cdot S_m=M_m$, M_m is a symmetric q-ary $\theta(m,q)\times\theta(m,q)$ matrix. Let $\mathcal{N}(M_m)$ be the matrix obtained from M_m by replacing all nonzero elements by 1. Then the elements of $\mathcal{N}(M_m)^2$ are equal to $a_i\cdot a_j$, where a_i are the rows of the matrix, $i=1,\ldots,\theta(m,q)$, and $a_i\cdot a_j$ is the inner product of two rows over $\mathbb{Z}$. It turns out that

$$a_i\cdot a_i=\mathrm{wt}(a_i)=q^{m-1}, i=1,\ldots,\theta(m,q),$$
$$a_i\cdot a_j=(q-1)q^{m-2},\quad 1\leq i<j\leq\theta(m,q).$$

Hence $\det(\mathcal{N}(M_m)^2)=q^{m+\theta(m,q)(m-2)}\neq 0$ and $\mathcal{N}(M_m)$ is invertible.

Definition 1. *The characteristic vector of the $[n,k;q]$-code C with respect to the matrix G is*

$$\chi(C,G)=(\chi_1,\chi_2,\ldots,\chi_{\theta(m,q)})\in\mathbb{Z}^{\theta(m,q)} \tag{1}$$

where χ_i is the number of the columns of G that are equal or proportional (with nonzero coefficients) to the i-th column of the matrix S_m.

When the code C and the matrix G are clear from the context, we will write briefly χ. Note that $\sum_{i=1}^{\theta(m,q)}\chi_i=n$, where n is the length of C. A code C can have different characteristic vectors depending on the matrix G and the considered generator matrix S_m of the simplex code $\mathcal{S}_{m,q}$. If we permute the columns of the matrix G we will obtain a permutation equivalent code to C having the same characteristic vector. Moreover, from a characteristic vector one can restore the columns of the generator matrix G, possibly in a different order and/or multiplied by nonzero elements of the field.

Definition 2. *Let α and β be rational numbers such that $\alpha w_i+\beta\in\mathbb{Z}$ for any nonzero weight w of a codeword in C. The projective dual code $D_{\alpha,\beta,m}(C)$ of C is the linear code with characteristic vector $\chi_{\alpha,\beta,m}=\alpha\chi\mathcal{N}(M_m)+\beta\mathbf{1}$, where $\mathbf{1}$ is the all-ones vector of the corresponding length.*

Example 1. Let C be the linear ternary code generated by the matrix $G=\begin{pmatrix}1&0&1&1\\0&1&1&2\\1&1&2&0\end{pmatrix}$. A characteristic vector of this code with respect to G is $\chi=(0,0,1,0,0,1,0,0,1,0,1,0,0)$. Then

$$\chi_D=\chi\cdot\mathcal{N}(M_m)=(3,3,3,3,3,3,3,3,0,3,3,3,3).$$

The dimension of C is 2 and therefore χ_D contains a zero coordinate.

Take $\alpha = 1/3$ and $\beta = 1$. Then

$$\chi_{1/3,1,3} = \frac{1}{3}\chi \cdot \mathcal{N}(M_m) + \mathbf{1} = \frac{1}{3}\chi_D + \mathbf{1} = (2,2,2,2,2,2,2,2,2,1,2,2,2,2).$$

So the projective dual code $D_{1/3,1,3}(C)$ is a ternary linear code of length 25 generated by the matrix

$$\begin{pmatrix} 0000000011111111111111111 \\ 0011111100001111100222222 \\ 1100112200110011222002211 \end{pmatrix}.$$

Similarly, the code $D_{1/3,0,3}(C)$ is the $[12,3,8]_3$ code generated by the matrix

$$\begin{pmatrix} 000011111111 \\ 011100110222 \\ 101201012021 \end{pmatrix}.$$

Let see when β may not be an integer. Obviously, if $\alpha \in \mathbb{Z}$ then $\beta \in \mathbb{Z}$. Suppose that $\alpha = a/b \notin \mathbb{Z}$, where a and b are coprime integers, and C has at least two nonzero weights $0 < w_1 < w_2$. Then

$$\frac{a}{b}w_1 + \beta \in \mathbb{Z},\ \frac{a}{b}w_2 + \beta \in \mathbb{Z}\ \Rightarrow \frac{a}{b}(w_2 - w_1) \in \mathbb{Z} \Rightarrow b \mid w_2 - w_1.$$

Since $w_2 - w_1 = w \in C$ then $\frac{a}{b}w + \beta \in \mathbb{Z}$ and $\frac{a}{b}w \in \mathbb{Z}$ which gives $\beta \in \mathbb{Z}$. Moreover, $\frac{a}{b}w \in \mathbb{Z}$ for all nonzero weights of C and therefore if C is a Δ-divisible code than $b \mid \Delta$.

Let us explain the meaning of the coefficients α and β. Taking a positive integer β, we extend the matrix $G_{\alpha,0,m}$ generating the dual code $D_{\alpha,0,m}$ with β copies of S_m. Conversely, a negative integer β (if possible according to Definition 1) corresponds to removing $-\beta$ copies of S_m from $G_{\alpha,0,m}$. If all weights in C are divisible by an integer t , then each column in the matrix $G_{\alpha,0,m}$ is repeated at least t times. Therefore, it is convenient to take $\alpha = 1/t$ and then $G_{1/t,0,m}$ will have t times fewer columns than $G_{\alpha,0,m}$.

If two linear codes are equivalent then their projective dual codes for given α, β and mk are also equivalent [1]. The length of $D_{\alpha,\beta,m}(C)$ is $n_D = \alpha n q^{m-1} + \beta\theta(q,m)$ [1]. From this formula we obtain that if $\alpha = \frac{a}{b}$ with $\gcd(a,b) = 1$, then $b \mid nq^{m-1}$. If C is a projective linear code then its dual code has at most two nonzero weights, namely $w_1 = \alpha q^{m-2}(q-1)n + \beta q^{m-1}$ and $w_2 = \alpha q^{m-2} + w_1$.

We are going to summarize the new and known results for applying the projective dual transform to codes related to Griesmer and Grey-Rankin bounds.

3 Projective self-dual codes

The linear code C is projective self-dual if it is equivalent to its projective dual code for some α, β, and $m = k$.

The following lemma is important in the study of projective self-dual codes.

Lemma 1. [2] *If C is a linear q-ary code, then C is the projective dual code to $D_{\alpha,\beta,m}(C)$ for $\lambda = \frac{1}{\alpha q^{m-2}}$ and $\mu = -\frac{\alpha(q-1)n+\beta q}{\alpha}$.*

We use also the following proposition from [6]:

Proposition 2. *Let C be q-ary $[n,k,d]$ projective self-dual code. If C is not a replicated simplex code, then*

$$\alpha = \pm q^{1-\frac{k}{2}}, \quad \beta = -\frac{q-1}{1+q^{k-1}\alpha}n. \tag{2}$$

After converting the formula (2) we get

$$\alpha = \frac{\epsilon}{q^{\frac{k}{2}-1}}, \quad \beta = -\frac{q-1}{q^{k/2}+\epsilon}n, \tag{3}$$

where $\epsilon = \pm 1$.

Since for a projective self-dual code β is an integer, then $\frac{(q-1)n}{q^{k/2}+1} \in \mathbb{Z}$ or $\frac{(q-1)n}{q^{k/2}-1} \in \mathbb{Z}$. This means that for an even integer k

- if q is even then $\theta(k/2,q) = \frac{q^{k/2}-1}{q-1} \mid n$ or $q^{k/2}+1 \mid n$, and
- if q is odd then $\theta(k/2,q) = \frac{q^{k/2}-1}{q-1} \mid n$ or $\frac{q^{k/2}+1}{2} \mid n$.

For the weights of the code we have

$$w_1 = q^{k/2-1}\frac{(q-1)n}{q^{k/2}+\epsilon}, \quad w_2 = q^{k/2-1}\frac{(q-1)n+\epsilon q^{k/2}+1}{q^{k/2}+\epsilon}$$

If $k = 2k_1$ then we consider the following cases:

- Case 1) $n = (q^{k_1}+1)u$, $w_1 = q^{k_1-1}(q-1)u$, $w_2 = q^{k_1-1}((q-1)u+1)$.
- Case 2) $n = (q^{k_1}+1)u/2$, q and u are odd integers, $w_1 = q^{k_1-1}(q-1)u/2$, $w_2 = q^{k_1-1}((q-1)u/2+1)$.
- Case 3) $n = \frac{q^{k_1}-1}{q-1}u$, $w_1 = q^{k_1-1}\frac{(q-1)n}{q^{k_1}-1} = q^{k_1-1}u$, $w_2 = q^{k_1-1}(u-1)$. In this case $w_1 > w_2$.

In the three cases $d = q^{k_1-1}d_1$, where $d_1 = (q-1)u$, $(q-1)u/2$, or $u-1$. Moreover, in the first two cases $n = \frac{q^{k_1}+1}{q-1}d_1$.

Consider as an example the codes over $\mathbb{F}_4$. Looking at the above conditions, we have that: (1) $\frac{4^{k/2}-1}{3} \mid n$ or $4^{k/2}+1 \mid n$ for an even k, and (2) $\frac{2^k+1}{3} \mid n$ or $2^k-1 \mid n$ for an odd integer k. Hence

- If $k = 3$ then n must be a multiple of 3 or 7. Projective self-dual $[6,3,4]$, $[7,3,4]$ and $[9,3,6]$ are known.
- If $k = 4$ then n must be a multiple of 5 or 17. Projective self-dual codes for $n = 5m$ for $m = 2,3,\ldots,8$ and $n = 17$ and 34 have been constructed (see [4]).

- If $k = 5$ then n must be a multiple of 11 or 31.
- If $k = 6$ then n must be a multiple of 21 or 65.
- If $k = 7$ then n must be a multiple of 43 or 127.

References

[1] I. Bouyukliev, Classification of Griesmer Codes and Dual Transform, *Discrete Mathematics*, **309 (12)**, 4049-4068, 2009.

[2] S. Bouyuklieva and I. Bouyukliev, Dual Transform through Characteristic Vectors, Proceedings of the International Workshop OCRT, Sofia, Bulgaria, pp.43–48, 2017.

[3] A.E. Brouwer and E. van Eupen, The correspondence between projective codes and 2-weight codes, *Des., Codes and Crypt.*, **11**, 262–266, 1997.

[4] A. R. Calderbank, W. M. Kantor, The geometry of two-weight codes, Bull. London Math. Soc. 18 (1986) pp. 97-122.

[5] P. Delsarte, Weights of linear codes and strongly regular normed spaces, *Discrete Math.,* **3**, 47–64, 1972.

[6] S. Dodunekov and J. Simonis, Codes and projective multisets, *Electron. J. Combin.*, 5(1), 1998.

[7] R. Hill, Caps and codes, *Discrete Math.*, **22**, 111–137, 1978.

[8] D. Nogin, Weight/multiplicity duality, in *Proc. Sixth Int. Workshop ACCT, Pskov, Russia, 1998*, 195–198.