The Dual Code of Points and t-Spaces in the Projective Space

Maarten De Boeck

The Dual Code of Points and t-Spaces in the Projective Space

Maarten De Boeck*

Ghent University, Department of Mathematics,
Krijgslaan 281 - Building S22, 9000 Ghent, Belgium
mdeboeck@cage.ugent.be

Abstract. The most important results on $C_t^{\perp}(n,q)$, the dual code of points and t-spaces in $\mathrm{PG}(n,q)$ are presented. We focus on the minimum distance and on the small weight codewords. In the third section, a recent result about the classification of the small weight codewords in $C_{n-1}^{\perp}(n,q)$, q even, is given.

Keywords: Linear codes; Projective spaces; Small weight codewords

1 Introduction

In the 1970's, the p-ary code of points and lines in a projective plane was introduced. In the same decade, also the study of the linear code $C_t(n,q)$ generated by the points and t-spaces (t-dimensional subspaces) of the projective space $\mathrm{PG}(n,q)$ began. The dimensions and minimum distances of these codes have been found and their minimum weight codewords were classified. However, there remain unanswered questions, even in the case of the projective plane $\mathrm{PG}(2,q)$. Also in the case of the linear codes of non-Desarguesian projective planes, there are still many open problems.

The dual code $C_t^{\perp}(n,q)$ of these codes has been studied as well, but, in general, less is known about them. The question about the minimum distance has only been answered in some specific cases. We will start by introducing these codes.

Definition 1. *The incidence matrix $M_{n,q,t}$ of the points and the t-spaces in the projective space $\mathrm{PG}(n,q)$ is the $\{0,1\}$-matrix whose columns are indexed by the points and whose rows are indexed by the t-spaces, and such that the entries fulfill*

$$(M_{n,q,t})_{i,j} = \begin{cases} 1 & \text{if the } i\text{-th } t\text{-space contains the } j\text{-th point} \\ 0 & \text{otherwise} \end{cases}. \tag{1}$$

Definition 2. *The p-ary code $C_t(n,q)$, $q=p^h$ and p prime, is the linear code over $\mathbb{F}_p$ generated by the rows of $M_{n,q,t}$.*

* The research of the author is supported by FWO-Vlaanderen (Fund for Scientific Research - Flanders).

The dimension of the codes $C_t(n,q)$, and hence of their duals, is known by a theorem of Hamada.

Theorem 1 ([6]). *Let $q = p^h$ and let k be the dimension of the p-ary code $C_t(n,q)$, $0 < t < n$. Then:*

$$k = \sum_{s_0} \cdots \sum_{s_{h-1}} \prod_{j=0}^{h-1} \sum_{i=0}^{L(s_{j+1},s_j)} (-1)^i \binom{n+1}{i} \binom{n + s_{j+1}p - s_j - ip}{n}, \qquad (2)$$

with $s_h = s_0$. The summation indices fulfill

$$t+1 \leq s_j \leq n+1 \qquad \text{and} \qquad 0 \leq s_{j+1}p - s_j \leq (n+1)(p-1),$$

with

$$L(s_{j+1}, s_j) = \left\lfloor \frac{s_{j+1}p - s_j}{p} \right\rfloor.$$

For the case $t = n-1$, i.e. the code of points and hyperplanes, the dimension was known earlier and is given by the following, easier, formula.

Theorem 2 ([5]). *The dimension of the p-ary code $C_{n-1}(n,q)$, $q = p^h$ and p prime, equals*

$$\binom{n+p-1}{n}^h + 1 . \qquad (3)$$

2 Minimum distance and small weight codewords for q odd

In this case, the minimum distance is not known in general. However, some theorems giving bounds on these minimum distances or giving relations between these minimum distances, were proven.

Theorem 3 ([11, Theorem 10]). *If $n \geq 2$ and $1 \leq t \leq n-1$, then $d\left(C_t^{\perp}(n,q)\right) = d\left(C_1^{\perp}(n-t+1,q)\right)$, with $q = p^h$ and p prime.*

Theorem 4 ([1, Proposition 1]). *If $n \geq 2$ and $1 \leq t \leq n-1$, then $(q+p)\,q^{n-t-1} \leq d\left(C_t^{\perp}(n,q)\right) \leq 2q^{n-t}$, with $q = p^h$ and p prime.*

Combining these results, the minimum distance can be determined when $q = p$.

Corollary 1. *If $n \geq 2$, $1 \leq t \leq n-1$ and p prime, $d\left(C_t^{\perp}(n,p)\right) = 2p^{n-t}$.*

Since the minimum distances are unknown in general, the codewords of minimum weight cannot be studied. However, if $q = p$, not only the minimum distances are known, but also the codewords of minimum weight were classified.

Theorem 5 ([11, Theorem 12]). *Let c be a codeword of $C_t^{\perp}(n,p)$, $n \geq 2$, $1 \leq t \leq n-1$ and p prime, with $\mathrm{wt}(c) = 2p^{n-t}$. Then, $c = \alpha(c' - c'')$ with c' and c'' the incidence vectors of two $(n-k)$-spaces intersecting each other in an $(n-k-1)$-space, and with $\alpha \in \mathbb{F}_p^*$.*

The construction used in this theorem, consisting of the difference of the incidence vectors of two $(n-k)$-spaces with a maximal intersection, was also used in the proof of Theorem 4 to construct a codeword of $C_t^{\perp}(n,q)$, with weight $2q^{n-t}$, thus giving the upper bound for the minimum distance.

The upper and lower bound of Theorem 4 were improved using various techniques. This first theorem is proven by looking at the number of different symbols occurring in the codeword.

Theorem 6 ([11, Theorem 14, Theorem 15]). *If $n \geq 2$, $1 \leq t \leq n-1$ and $q = p^h$ is odd, with p prime, then $d\left(C_t^{\perp}(n,q)\right) \geq \frac{1}{3}(4\theta_{n-t}(q)+2)$. Moreover, if $p = 7$, respectively $p > 7$, then $d\left(C_t^{\perp}(n,q)\right) \geq \frac{1}{7}(12\theta_{n-t}(q)+2)$, respectively $d\left(C_t^{\perp}(n,q)\right) \geq \frac{1}{7}(12\theta_{n-t}(q)+6)$.*

Hereby, we used the notation $\theta_i(q) = \frac{q^{i+1}-1}{q-1}$.

The upper bound was improved by constructing a codeword with weight smaller than $2q^{n-t}$, if q is not a prime. Such a codeword was constructed using a minimal blocking set of Rédei type.

Theorem 7 ([10, Theorem 4.13, Theorem 4.14]). *There exists a minimal $(n-t)$-blocking set B in $\mathrm{PG}(n,q)$ of size $|B| = q^{n-t} + \delta$, such that there is a $(n-t)$-space τ with $|B \cap \tau| = \delta = q^{n-t-1}\frac{q-1}{p-1} + \frac{q^{n-t-1}-1}{q-1}$. Denote the incidence vector of B by c_B and the incidence vector of τ by c_τ. Then $c_B - c_\tau \in C_t^{\perp}(n,q)$ and $\mathrm{wt}(c_B - c_\tau) = 2q^{n-t} - \frac{q-p}{p-1}q^{n-t-1}$.*

Corollary 2 ([10, Corollary 4.15]). *If $n \geq 2$, $1 \leq t \leq n-1$ and $q = p^h$ with $p \neq 2$ prime, then $d\left(C_t^{\perp}(n,q)\right) \leq 2q^{n-t} - \frac{q-p}{p-1}q^{n-t-1}$.*

Apart from the case $q = p$, the exact minimum distance of $C_t^{\perp}(n,q)$ is only known for $q = p^2$, $n = 2$, $t = 1$, $p \in \{3,5\}$, if q is odd.

Theorem 8 ([7], [2, Corollary 1.2], [8, Theorem 1]).

- $d\left(C_1^{\perp}(2,9)\right) = 15$,
- $d\left(C_1^{\perp}(2,25)\right) = 45$,
- $88 \leq d\left(C_1^{\perp}(2,49)\right) \leq 91$.

The lower bound given for $p = 7$ is better than any of the lower bounds derived before. The upper bound coincides with the upper bound of Corollary 2.

3 Minimum distance and small weight codewords for q even

In this case, the minimum distances are known. Moreover, we have a result on the codewords of minimal weight.

Theorem 9 ([1, Theorem 1]). *Let $q = 2^h$ and $0 < t < n$, then $d\left(C_t^{\perp}(n,q)\right) = (q+2)\,q^{n-t-1}$.*

Theorem 10 ([11, Theorem 11]). *Consider a codeword $c \in C_t^{\perp}(n,q)$, $0 < t < n$, such that $\mathrm{wt}(c) = d\left(C_t^{\perp}(n,q)\right)$. Then $\mathrm{supp}(c)$ is contained in an $(n-t+1)$-space of $\mathrm{PG}(n,q)$.*

Definition 3. *A hyperoval is a point set H in $\mathrm{PG}(2,q)$, q even, such that every line in $\mathrm{PG}(2,q)$ intersects H in 0 or 2 points.*

The proof of Theorem 9 has two parts. In the first part, it is proven that $(q+2)\,q^{n-t-1}$ is a lower bound on the minimum distance, using earlier work of Delsarte. In the second part, it is proven that this lower bound is sharp by constructing a codeword of weight $(q+2)\,q^{n-t-1}$ in the following way. Let V be a plane and σ an $(n-t-2)$-space skew to it, and let H be a hyperoval in V. Consider the cone σH, with σ as vertex and H as base. Then the incidence vector of $\sigma H \setminus \sigma$ is a codeword $c \in C_t^{\perp}(n,q)$, with $\mathrm{wt}(c) = (q+2)\,q^{n-t-1}$.

The codewords constructed above are codewords of minimum weight. It is however not proven that all codewords of minimum weight can be constructed in this way. For the geometrical interpretation of codewords of minimum weight in $C_t^{\perp}(n,q)$, we can only rely on Theorem 10. About the codewords of small, non-minimum weight, nothing is known in general.

Recently however, the classification of the small weight codewords was done for the case $t = n-1$; this is the dual code of points and hyperplanes. If we look at the codewords of minimum weight $q+2$ in this code, we know by Theorem 10 that the support of such a codeword is contained in a plane. It can easily be seen that their support must be a hyperoval. Hyperovals are examples of even sets.

Definition 4. *An even set is a point set S in $\mathrm{PG}(2,q)$, q even, such that every line in $\mathrm{PG}(2,q)$ intersects S in an even number of points.*

Other examples of even sets are the symmetric difference of an even number of lines, the symmetric difference of hyperovals and the so-called $(q+t)$-arcs of type $(0,2,t)$ (see [4, 9, 12]). By an easy counting argument, one can see that the number of points of an even set is always even.

It is obvious that the incidence vector of an even set in a plane of $\mathrm{PG}(n,q)$ is a codeword of $C_{n-1}^{\perp}(n,q)$. One might expect that all the small weight codewords are the incidence vector of an even set in a plane of the projective space. The following two theorems state that this turns out to be true. However the width of the interval of weights for which all codewords are the incidence vector of an

even set depends on the fact whether q is a square. If q is a non-square, this width is at least $\sqrt[3]{q^2}$. If q is a square, this width is $2\sqrt{q}-3$. In this case, a second possibility for the geometrical interpretation of the codewords pops up as soon as the weight of the codewords exceeds $q+2\sqrt{q}-1$. The support of the next codewords is contained in a 3-space.

Theorem 11 ([3, Theorem 5.3]). *Let c be a codeword in $C_{n-1}^{\perp}(n,q)$, q even, with $\mathrm{wt}(c) \leq q+\sqrt[3]{q^2}+1$.*

- *If q is a non-square or $q \in \{4,16\}$, then c is the incidence vector of an even set in a plane of $\mathrm{PG}(n,q)$.*
- *If q is a square and $q \geq 64$, then c is the incidence vector of an even set in a plane of $\mathrm{PG}(n,q)$ or the incidence vector of a set in a 3-dimensional Baer subgeometry B in $\mathrm{PG}(n,q)$ such that the restriction of c to the positions indexed by the points of B is a codeword of $C_1^{\perp}\left(3,\sqrt{q}\right)$.*

Theorem 12 ([3, Corollary 4.13]). *Let c be a codeword in $C_{n-1}^{\perp}(n,q)$, $q=2^h \geq 64$ a square, such that $\mathrm{wt}(c) < q+2\sqrt{q}$. Then, it is the incidence vector of an even set in a plane of $\mathrm{PG}(n,q)$.*

The proof of both theorems relies on the classification of the small blocking sets. We have a closer look at the second possibility occurring in the case $q \geq 64$ square.

Theorem 13 ([3, Theorem 4.12]). *If $\overline{c} \in C_1^{\perp}\left(3,\sqrt{q}\right)$, q even, is completed to a vector c by zeros on the positions indexed by the points of $\mathrm{PG}(n,q)\setminus B$, with B a 3-dimensional Baer subgeometry in $\mathrm{PG}(n,q)$, then $c \in C_{n-1}^{\perp}(n,q)$.*

Hence, the bound of Theorem 12 is sharp. It corresponds with the bound $d\left(C_1^{\perp}(3,\sqrt{q})\right) = q+2\sqrt{q}$, given by Theorem 9.

References

1. Calkin, N.J., Key, J.D., de Resmini, M.J.: Minimum Weight and Dimension Formulas for Some Geometric Codes. Des. Codes Cryptogr. 17, 105-120 (1999)
2. Clark, K.L., Hatfield, L.D., Key, J.D., Ward, H.N.: Dual codes of projective planes of order 25. Adv. Geom. 3, S140-S152 (2003)
3. De Boeck, M.: Small weight codewords in the dual code of points and hyperplanes in $\mathrm{PG}(n,q)$, q even. Submitted to Des. Codes Cryptogr.
4. Gács, A., Weiner, Zs.: On $(q+t)$-arcs of type $(0,2,t)$. Des. Codes Cryptogr. 29, 131-139 (2003)
5. Goethals, J.M., Delsarte, P.: On a class of majority-logic decodable cyclic codes. IEEE Trans. Inform. Theory 14, 182-188 (1968)
6. Hamada, N.: The rank of the incidence matrix of points and d-flats in finite geometries. J. Sci. Hiroshima Univ., Ser. A-I 32, 381-396 (1969)
7. Key, J.D., de Resmini, M.J.: Ternary dual codes of the plane of order nine. J. Statist. Plann. Inference 95, 229-236 (2001)

8. Key, J.D., Ngwane, F.F.: A lower bound for the minimum weight of the dual 7-ary code of a projective plane of order 49. Des. Codes Cryptogr. 44, 133-142 (2007)
9. Korchmáros, G., Mazzocca, F.: On $(q+t)$-arcs of type $(0,2,t)$ in a desarguesian plane of order q. Math. Proc. Camb. Phil. Soc. 108, 445-459 (1990)
10. Lavrauw, M., Storme, L., Van de Voorde, G.: Linear codes from projective spaces. In: Bruen, A.A., Wehlau, D.L. (Eds.), Error-Correcting Codes, Finite Geometries, and Cryptography. AMS Contemporary Mathematics (CONM) book series, vol. 523, pp. 185-202. American Mathematical Society (2010)
11. Lavrauw, M., Storme, L., Van de Voorde, G.: On the code generated by the incidence matrix of points and k-spaces in PG (n,q) and its dual. Finite Fields Appl. 14, 1020-1038 (2008)
12. Vandendriessche, P.: Codes of Desarguesian projective planes of even order, projective triads and $(q+t,t)$-arcs of type $(0,2,t)$. Submitted to Finite Fields Appl.