Linear codes from projective spaces

Michel Lavrauw and Leo Storme and Geertrui Van de Voorde

***Abstract*— The finite projective space $\mathrm{PG}(n,q)$, $q=p^h$, p prime, $h\geq 1$, is also investigated from a coding-theoretical point of view. The linear code $\mathrm{C}_{s,t}(n,q)$ of s-spaces and t-spaces in a projective space $\mathrm{PG}(n,q)$, $q=p^h$, p prime, $h\geq 1$, is defined as the vector space spanned over $\mathbb{F}_p$ by the rows of the incidence matrix of s-spaces and t-spaces. This linear code can be investigated purely for its coding-theoretical importance, but the properties of this linear code are also of interest for the finite projective space $\mathrm{PG}(n,q)$ itself. Some of the best results on substructures of finite projective spaces $\mathrm{PG}(n,q)$ have been obtained by using their corresponding codes. Recently, there has been a new incentive on the study of the minimum distance of these linear codes and their duals. In this paper, we summarize what is currently known about the minimum distance and small weight codewords of these linear codes and their duals.**

I. INTRODUCTION

Let $\mathbb{F}_q$ denote the finite field with q elements, where $q=p^h$, p prime, $h\geq 1$. Let $\mathrm{V}(n+1,q)$ denote the vector space of dimension $n+1$ over $\mathbb{F}_q$.

The *projective space* $\mathrm{PG}(n,q)$ is the incidence structure with as *points* the vector spaces of rank 1 of $\mathrm{V}(n+1,q)$ and as *lines* the vector spaces of rank 2 of $\mathrm{V}(n+1,q)$. The m-*dimensional* subspaces of $\mathrm{PG}(n,q)$ correspond to the vector subspaces of rank $m+1$ of $\mathrm{V}(n+1,q)$. The number of points in $\mathrm{PG}(n,q)$ is equal to $(q^{n+1}-1)/(q-1)$ and will be denoted by θ_n. The *Gaussian coefficient* $\begin{bmatrix} t \\ s \end{bmatrix}_q$ denotes the number of $(s-1)$-subspaces in $\mathrm{PG}(t-1,q)$, i.e.,

$$\begin{bmatrix} t \\ s \end{bmatrix}_q = \frac{(q^t-1)(q^{t-1}-1)\cdots(q^{t-s+1}-1)}{(q^s-1)(q^{s-1}-1)\cdots(q-1)}.$$

The subspaces of $\mathrm{PG}(n,q)$ of dimension $0,1,2$, and $n-1$ are called *points*, *lines*, *planes*, and *hyperplanes* respectively. A t-dimensional subspace is often called a *t-space*.

We define the *incidence matrix* $A=(a_{ij})$ of s-spaces and t-spaces in the projective space $\mathrm{PG}(n,q)$ as the matrix whose rows are indexed by the t-spaces of $\mathrm{PG}(n,q)$ and whose columns are indexed by the s-spaces of $\mathrm{PG}(n,q)$, and with entry

$$a_{ij}=\begin{cases} 1 & \text{if } s\text{-space } j \text{ is contained in } t\text{-space } i,\\ 0 & \text{otherwise.}\end{cases}$$

M. Lavrauw is with Department of Mathematics, Ghent University, Krijgslaan 281 - Building S22, 9000 Ghent, Belgium ml@cage.ugent.be, http://cage.ugent.be/∼ml

L. Storme is with Department of Mathematics, Ghent University, Krijgslaan 281 - Building S22, 9000 Ghent, Belgium ls@cage.ugent.be, http://cage.ugent.be/∼ls

G. Van de Voorde is with Department of Mathematics, Ghent University, Krijgslaan 281 - Building S22, 9000 Ghent, Belgium gvdvoorde@cage.ugent.be, http://cage.ugent.be/∼gvdvoorde

An $[N,k,d]$-code C over $\mathbb{F}_q$ is a k-dimensional subspace of the N-dimensional vector space $V(N,q)$ over $\mathbb{F}_q$ of minimum distance d, i.e., the minimum number of positions in which two distinct codewords of C differ is equal to d.

The p-ary *linear code of s-spaces and t-spaces* of $\mathrm{PG}(n,q)$, $q=p^h$, p prime, $h\geq 1$, is the linear code generated by the rows of the incidence matrix of s-spaces and t-spaces in $\mathrm{PG}(n,q)$ and is denoted by $\mathrm{C}_{s,t}(n,q)$. In the particular case that $s=0$, we denote the p-ary linear code of points and t-spaces of $\mathrm{PG}(n,q)$, $q=p^h$, p prime, $h\geq 1$, by $\mathrm{C}_t(n,q)$. The p-ary linear code of points and lines of the projective plane $\mathrm{PG}(2,q)$, $q=p^h$, p prime, $h\geq 1$, will be denoted by $\mathrm{C}_1(2,q)$.

We will identify the support of a codeword of $\mathrm{C}_t(n,q)$ with the corresponding set of points of $\mathrm{PG}(n,q)$, in order to be able to describe the results on the support of a codeword in a geometrical way. Furthermore, if T is a set of points of $\mathrm{PG}(n,q)$, then the incidence vector of this set is also denoted by T.

The parameters s,t, and n will always satisfy $n\geq 2$, $0\leq s<t\leq n-1$, unless indicated differently.

II. THE MINIMUM DISTANCE AND SMALL WEIGHTS OF THE LINEAR CODES ARISING FROM PROJECTIVE SPACES

A. MINIMUM DISTANCE AND SMALL WEIGHTS OF THE LINEAR CODES $\mathrm{C}_{s,t}(n,q)$

One of the main problems in the theory of the linear $[N,k,d]$-codes is to find the parameters N, k, and d of a certain code. Clearly, the length N of $\mathrm{C}_{s,t}(n,q)$ is the number of s-spaces in $\mathrm{PG}(n,q)$, i.e. $N=\begin{bmatrix} n+1 \\ s+1 \end{bmatrix}_q$. For results on the dimension of the linear codes $\mathrm{C}_{s,t}(n,q)$, we refer to [11].

In this section, we discuss the problem of determining the minimum distance and the small weight codewords of the code $\mathrm{C}_{s,t}(n,q)$. The minimum distance d of a linear $[N,k,d]$-code C is a very important parameter since it determines the number of errors that can be corrected using the code C.

For all linear codes $\mathrm{C}_{s,t}(n,q)$, the minimum weight and the exact description of the minimum weight codewords of $\mathrm{C}_{s,t}(n,q)$ is known as the next theorem shows. Let $\Delta_{s,t}$ denote the incidence system whose points and blocks are the s-spaces and t-spaces in $\mathrm{PG}(n,q)$, respectively, and the incidence is inclusion.

ISBN 978-963-311-370-7

Theorem 2.1: [2, Theorem 1] The minimum weight of $\mathrm{C}_{s,t}(n,q)$ is $\begin{bmatrix} t+1 \\ s+1 \end{bmatrix}_q$, and the minimum weight vectors are the scalar multiples of incidence vectors of the blocks of $\Delta_{s,t}$.

For $\mathrm{C}_t(n,q)$, this result was known before and reduces to the following statement.

Theorem 2.2: [1, Proposition 5.7.3] The minimum weight codewords of $\mathrm{C}_t(n,q)$ are the scalar multiples of the incidence vectors of the t-spaces.

After the minimum weight and the exact description of the minimum weight codewords of the linear codes $\mathrm{C}_{s,t}(n,q)$ were known, the attention of researchers was drawn to finding the exact weights of the small weight codewords of $\mathrm{C}_{s,t}(n,q)$ and the exact description of the corresponding small weight codewords.

We now present the main results in the order as they were found, since the following stated results always inspired other researchers to obtain the subsequent results.

Theorem 2.3: [4],[5] There are no codewords in $\mathrm{C}_1(2,p)$, p prime, with weight in the closed interval $[p+2, 2p-1]$.

This result of Chouinard inspired Fack et al. to obtain a larger interval for p prime.

Theorem 2.4: [6, Theorem 4] The only codewords c, with $0 < wt(c) \leq 2p+(p-1)/2$, in $\mathrm{C}_1(2,p)$, $p \geq 11$ prime, are:

(i) codewords with weight $p+1$: $\alpha\ell$, with ℓ a line of $\mathrm{PG}(2,p)$, $\alpha \in \mathbb{F}_p \setminus \{0\}$,
(ii) codewords with weight $2p$: $\alpha(\ell_1 - \ell_2)$, with ℓ_1 and ℓ_2 two distinct lines of $\mathrm{PG}(2,p)$, $\alpha \in \mathbb{F}_p \setminus \{0\}$,
(iii) codewords with weight $2p+1$: $\alpha\ell_1 + \beta\ell_2$, $\beta \neq -\alpha$, $\alpha, \beta \in \mathbb{F}_p \setminus \{0\}$, with ℓ_1 and ℓ_2 two distinct lines of $\mathrm{PG}(2,p)$.

Similarly, this result inspired Gács, Szőnyi, and Weiner in [7] to obtain a large improvement.

Theorem 2.5: [7] A codeword c in $\mathrm{C}_1(2,q)$, $q = p^h$, p prime, $h \geq 1$, with $wt(c) < \lceil\sqrt{q}\rceil q + 1 + (q - \lceil\sqrt{q}\rceil^2)$ is a linear combination of $\lceil \frac{wt(c)}{q+1} \rceil$ lines, when q is large and $h > 2$.

The preceding results regard small weight codewords for the linear codes $\mathrm{C}_1(2,q)$. We now present results on the small weight codewords for the linear codes $\mathrm{C}_t(n,q)$.

Theorem 2.6: [12, Theorem 12] There are no codewords in $\mathrm{C}_t(n,q) \setminus \mathrm{C}_{n-t}(n,q)^\perp$, $q = p^h$, $p > 5$ prime, $h \geq 1$, with weight in the open interval $]\theta_t, 2q^t[$.

Theorem 2.6 does not say anything about the codewords that are contained in $\mathrm{C}_t(n,q) \cap \mathrm{C}_{n-t}(n,q)^\perp$. In the next theorem, these kinds of codewords are permitted.

Theorem 2.7: [2] There are no codewords in $\mathrm{C}_t(n,q)$, $q = p^h$, $p > 5$ prime, $h \geq 1$, with weight in the open interval $]\theta_t, 2(\frac{q^n-1}{q^t-1}(1-\frac{1}{p})+\frac{1}{p})[$.

The interval in the following theorem is sharp since θ_{n-1} is the weight of a codeword arising from the incidence vector of a hyperplane and $2q^{n-1}$ is the weight of a codeword arising from the difference of the incidence vectors of two distinct hyperplanes.

Theorem 2.8: [12, Corollary 20] There are no codewords with weight in the open interval $]\theta_{n-1}, 2q^{n-1}[$ in the code $\mathrm{C}_{n-1}(n,q)$, $q = p^h$, $p > 5$ prime, $h \geq 1$.

Also in the prime case, we have a sharp interval.

Theorem 2.9: [12, Corollary 21] There are no codewords with weight in the open interval $]\theta_t, 2p^t[$ in the code $\mathrm{C}_t(n,p)$, $p > 5$ prime.

B. MINIMUM WEIGHT OF THE DUAL CODES $\mathrm{C}_t(n,q)^\perp$

After discussing the minimum weight and the small weight codewords of the linear codes $\mathrm{C}_{s,t}(n,q)$, we now focus on the minimum weight of the dual codes $\mathrm{C}_{s,t}(n,q)^\perp$.

Theorem 2.10: [2, Theorem 3] The minimum distance d of $\mathrm{C}_{s,t}(n,q)^\perp$ satisfies:

$$2\left(\frac{q^{n-s}-1}{q^{t-s}-1}(1-\frac{1}{p})+\frac{1}{p}\right) \leq d \leq 2q^{n-t}.$$

If the lower bound is attained, then $t = s+1$.

For q prime and $t = s+1$, the upper and lower bound in the previous theorem coincide, hence, the minimum distance of $\mathrm{C}_{s,s+1}(n,p)^\perp$, p prime, is equal to $2p^{n-s-1}$. In the case that $s = 0$, Bagchi and Inamdar also describe the codewords of minimum weight $2p^{n-1}$ in $\mathrm{C}_1(n,p)^\perp$.

Theorem 2.11: [2, Proposition 2] The minimum distance of $\mathrm{C}_1(n,p)^\perp$, p prime, is $2p^{n-1}$. Moreover, the codewords of minimum weight are precisely the scalar multiples of the difference of two hyperplanes.

The fact that the minimum distance of $\mathrm{C}_1(2,p)^\perp$, p prime, is $2p$ was already known since the 1970's, when Assmus and Key derived the following bounds on the minimum distance of $\mathrm{C}_1(2,q)^\perp$.

Theorem 2.12: [1, Theorem 6.4.2] The minimum distance d of $\mathrm{C}_1(2,q)^\perp$, $q = p^h$, p prime, $h \geq 1$, satisfies

$$q + p \leq d \leq 2q,$$

and the lower bound is attained if $p = 2$.

The sharpness of the lower bound follows from the existence of hyperovals in the projective plane $\mathrm{PG}(2,q)$, q even. If q is odd, other lower bounds were known. In 1979, Sachar proved the following result for $\mathrm{C}_1(2,q)^\perp$.

Theorem 2.13: [13, Proposition 2.3] The minimum distance of $\mathrm{C}_1(2,q)^\perp$, $q=p^h$, $p>2$ prime, $h\geq 1$, is at least $4q/3+2$.

Theorem 2.14: [13, Proposition 2.4] Let c be a codeword of $\mathrm{C}_1(2,q)^\perp$, $q=p^h$, p prime, $h\geq 1$, with $p \not| \ wt(c)$. If $p=5$, then $wt(c)\geq 4(2q+3)/5$ and if $p>5$, then $wt(c)\geq (12q+18)/7$.

The divisibility condition in this latter theorem was proven to be unnecessary in [10], where the authors used the same ideas to extend these lower bounds to the code of $\mathrm{C}_t(n,q)^\perp$.

Theorem 2.15: [10, Theorem 14][10, Theorem 15] If $p\neq 2$, then $d(\mathrm{C}_t(n,q)^\perp)\geq (4\theta_{n-t}+2)/3$, if $p=7$, then $d(\mathrm{C}_t(n,q)^\perp)\geq (12\theta_{n-t}+2)/7$ and if $p>7$, then $d(\mathrm{C}_t(n,q)^\perp)\geq (12\theta_{n-t}+6)/7$.

In 1999, Calkin, Key, and de Resmini [3] extended Theorem 2.12 to general dimension.

Theorem 2.16: [3, Proposition 1] The minimum distance d of $\mathrm{C}_t(n,q)^\perp$, $q=p^h$, p prime, $h\geq 1$, satisfies the following:

$$(q+p)q^{n-t-1}\leq d\leq 2q^{n-t}.$$

They again show that for $p=2$, this lower bound is sharp.

Theorem 2.17: [3, Theorem 1] The minimum distance of $\mathrm{C}_t(n,q)^\perp$, q even, is $(q+2)q^{n-t-1}$.

If $q=p$, it follows from Theorem 2.16 that the minimum distance of $\mathrm{C}_t(n,p)^\perp$ is $2p^{n-t}$. In [10], the authors derive this result in a different way; they show that finding the minimum distance of $\mathrm{C}_t(n,q)^\perp$ can be reduced to finding the minimum distance of $\mathrm{C}_1(n-t+1,q)^\perp$.

Theorem 2.18: [10, Theorem 10] $d(\mathrm{C}_t(n,q)^\perp)=d(\mathrm{C}_1(n-t+1,q)^\perp)$.

Using Theorem 2.11 of Bagchi and Inamdar for $\mathrm{C}_1(n,p)^\perp$, p prime, they derive the following result for $\mathrm{C}_t(n,p)^\perp$. Note that it was already shown that the minimum weight of $\mathrm{C}_t(n,p)^\perp$ was $2p^{n-t}$, but the nature of the minimum weight codewords was not known.

Theorem 2.19: [10, Theorem 12] The minimum distance of $\mathrm{C}_t(n,p)^\perp$, p prime, is equal to $2p^{n-t}$, and the codewords of weight $2p^{n-t}$ are the scalar multiples of the difference of two $(n-t)$-spaces intersecting in an $(n-t-1)$-space.

Bagchi and Inamdar conjecture that, if p is prime, the minimum distance of the dual code $\mathrm{C}_{s,t}(n,p)^\perp$ is $2p^{n-t}$ too. Proving this is still an open problem, except for the cases $s=0$ and $t=s+1$ [2].

Open Problem 2.20: Show that the minimum distance of $\mathrm{C}_{s,t}(n,p)^\perp$, p prime, equals $2p^{n-t}$ or construct a codeword of $\mathrm{C}_{s,t}(n,p)^\perp$ that has smaller weight.

Open Problem 2.21: Determine the minimum distance of $\mathrm{C}_{s,t}(n,q)^\perp$.

We now concentrate on the problem of finding a new upper bound on the minimum distance of $\mathrm{C}_t(n,q)^\perp$. When q is not a prime, there are counterexamples to Theorem 2.19 (with p replaced by q), as the following theorem states.

Theorem 2.22: [10, Theorem 13] Let B be a minimal $(n-t)$-blocking set in $\mathrm{PG}(n,q)$ of size $q^{n-t}+x$, with $x<(q^{n-t}+1)/2$, such that there exists an $(n-t)$-space μ intersecting B in x points. The difference of the incidence vectors of B and μ is a codeword of $\mathrm{C}_t(n,q)^\perp$ of weight $2q^{n-t}+\theta_{n-t-1}-x$.

The authors used in [11] this theorem to correct a wrong upper bound, derived by the authors in [10, Theorem 13].

Theorem 2.23: There exists a small minimal $(n-t)$-blocking set B in $\mathrm{PG}(n,q)$, $q=p^h$, p prime, $h>1$, of size $q^{n-t}+x$ such that there is an $(n-t)$-space μ with $|B\cap\mu|=x$ and with $x=q^{n-t-1}(q-1)/(p-1)+\theta_{n-t-2}$.

Using this theorem, together with Theorem 2.22, yields the following corollary.

Corollary 2.24: The minimum distance of $\mathrm{C}_t(n,q)^\perp$, $q=p^h$, p prime, $h>1$, satisfies the following inequality:

$$d(\mathrm{C}_t(n,q)^\perp)\leq 2q^{n-t}-q^{n-t-1}(q-p)/(p-1).$$

For $n=2$, the codeword constructed was also found in [8].

C. THE MINIMUM DISTANCE OF THE HULL

The *hull* of a linear code C is defined as $\mathrm{C}\cap\mathrm{C}^\perp$. The minimum weight vectors of the hull of $\mathrm{C}_1(2,q)$ are characterised in the following theorem.

Theorem 2.25: [1, Corollary 6.4.4] The hull $\mathrm{C}_1(2,q)\cap\mathrm{C}_1(2,q)^\perp$ has minimum distance $2q$ and the minimum weight vectors are the scalar multiples of the differences of the incidence vectors of any two distinct lines of $\mathrm{PG}(2,q)$.

This was extended to the code of points and hyperplanes in [9].

Theorem 2.26: [9, Theorem 5] The minimum distance of the hull of $\mathrm{C}_{n-1}(n,q)$ is equal to $2q^{n-1}$.

Open Problem 2.27: Determine the minimum distance of the hull of the code $\mathrm{C}_{s,t}(n,q)$, where $(s,t) \neq (0,n-1)$.

Remark 2.28: This summary of the known results on the minimum distances of the linear codes $\mathrm{C}_{s,t}(n,q)$, and their duals, arises from the survey article [11], in which much more information on the minimum distances of the linear codes $\mathrm{C}_{s,t}(n,q)$, and their duals, is presented, including information on the minimum distances of the linear codes of non-Desarguesian projective planes. In [11], also a great number of open problems is presented for the readers interested in doing research on this topic.

III. SUMMARY

TABLE I
KNOWN VALUES AND BOUNDS ON THE MINIMUM DISTANCE OF LINEAR CODES FROM PROJECTIVE SPACES ($q = p^h$, p PRIME, $h \geq 1$).

Code	minimum distance d	Theorem
$\mathrm{C}_{s,t}(n,q)$	$\begin{bmatrix} t+1 \\ s+1 \end{bmatrix}_q$	2.1
$\mathrm{C}_t(n,q)$	θ_t	2.2
$\mathrm{C}_{s,t}(n,q)^\perp$	$2\left(\frac{q^{n-s}-1}{q^{t-s}-1}(1-\frac{1}{p})+\frac{1}{p}\right) \leq d$ $d \leq 2q^{n-t}$	2.10
$\mathrm{C}_{s,s+1}(n,p)^\perp$	$2p^{n-s-1}$	2.10
$\mathrm{C}(2,q)^\perp$	$q+p \leq d \leq 2q$	2.12
$\mathrm{C}(2,q)^\perp$, $p>2$	$4q/3+2 \leq d$	2.13
$\mathrm{C}_t(n,q)^\perp$, $p>2$	$(4\theta_{n-t}+2)/3 \leq d$	2.15
$\mathrm{C}_t(n,q)^\perp$	$(q+p)q^{n-t-1} \leq d \leq 2q^{n-t}$, $d = d(\mathrm{C}_1(n-t+1,q)^\perp)$	2.16 2.18
$\mathrm{C}_t(n,q)^\perp$, $p=2$	$(q+2)q^{n-t-1}$	2.17
$\mathrm{C}_t(n,p)^\perp$	$2p^{n-t}$	2.19
$\mathrm{C}_t(n,q)^\perp$	$d \leq 2q^{n-t} - q^{n-t-1}\frac{q-p}{p-1}$	2.24
$\mathrm{C}_{n-1}(n,q) \cap$ $\mathrm{C}_{n-1}(n,q)^\perp$	$2q^{n-1}$	2.26

REFERENCES

[1] E.F. Assmus, Jr. and J.D. Key. Designs and their codes. *Cambridge University Press*, 1992.

[2] B. Bagchi and S.P. Inamdar. Projective Geometric Codes. *J. Combin. Theory, Ser. A* **99** (2002), 128–142.

[3] N.J. Calkin, J.D. Key, and M.J. de Resmini. Minimum weight and dimension formulas for some geometric codes. *Des. Codes Cryptogr.* **17** (1999), 105–120.

[4] K. Chouinard. Weight distributions of codes from planes (PhD Thesis, University of Virginia) (August 1998).

[5] K. Chouinard. On weight distributions of codes of planes of order 9. *Ars Combin.* **63** (2002), 3–13.

[6] V. Fack, Sz.L. Fancsali, L. Storme, G. Van de Voorde, and J. Winne. Small weight codewords in the codes arising from Desarguesian projective planes. *Des. Codes Cryptogr.* **46** (2008), 25–43.

[7] A. Gács, T. Szőnyi, and Zs. Weiner. Private communication (2009).

[8] J.D. Key, T.P. McDonough, and V.C. Mavron. An upper bound for the minimum weight of the dual codes of Desarguesian planes. *European J. Combin.* **30** (2009), 220–229.

[9] M. Lavrauw, L. Storme, and G. Van de Voorde. On the code generated by the incidence matrix of points and hyperplanes in $\mathrm{PG}(n,q)$ and its dual. *Des. Codes Cryptogr.* **48** (2008), 231–245.

[10] M. Lavrauw, L. Storme, and G. Van de Voorde. On the code generated by the incidence matrix of points and k-spaces in $\mathrm{PG}(n,q)$ and its dual. *Finite Fields Appl.* **14** (2008), 1020–1038.

[11] M. Lavrauw, L. Storme, and G. Van de Voorde, Linear codes from projective spaces. *AMS Contemporary Mathematics (CONM) book series*, to appear.

[12] M. Lavrauw, L. Storme, P. Sziklai, and G. Van de Voorde. An empty interval in the spectrum of small weight codewords in the code from points and k-spaces of $\mathrm{PG}(n,q)$. *J. Combin. Theory, Ser. A* **116** (2009), 996–1001.

[13] H. Sachar. The $\mathbb{F}_p$ span of the incidence matrix of a finite projective plane. *Geom. Dedicata* **8** (1979), 407–415.