A modular equality for Cameron-Liebler line classes

Alexander L. Gavrilyuk

Research Center for Pure and Applied Mathematics, Graduate School of Information Sciences, Tohoku University, Sendai 980-8579, Japan
and
N.N. Krasovsky Institute of Mathematics and Mechanics UB RAS, Kovalevskaya str., 16, Ekaterinburg 620990, Russia

Klaus Metsch

Justus-Liebig-Universität, Mathematisches Institut, Arndtstraße 2, D-35392 Gießen, Germany
and
Department of Pure Mathematics and Computer Algebra, Ghent University, Krijgslaan 281-S22, 9000 Gent, Belgium

Abstract

In this paper we prove that a Cameron-Liebler line class $\mathcal{L}$ in $\mathrm{PG}(3,q)$ with parameter x has the property that $\binom{x}{2}+n(n-x)\equiv 0 \mod q+1$ for the number n of lines of $\mathcal{L}$ in any plane of $\mathrm{PG}(3,q)$. It follows that the modular equation $\binom{x}{2}+n(n-x)\equiv 0 \mod q+1$ has an integer solution in n. This result rules out roughly at least one half of all possible parameters x. As an application of our method, we determine the spectrum of parameters of Cameron-Liebler line classes of $\mathrm{PG}(3,5)$. This includes the construction of a Cameron-Liebler line class with parameter 10 in $\mathrm{PG}(3,5)$ and a proof that it is unique up to projectivities and dualities.

Keywords: Cameron-Liebler line class, tight sets, hyperbolic quadric, intriguing set, completely regular code, Grassmann graph
2000 MSC: 51E20, 05B25, 05E30

1. Introduction

A *Cameron-Liebler line class* [4, 16] of the finite projective space $\mathrm{PG}(3,q)$ is a set of lines that shares a constant number x of lines with every regular spread of $\mathrm{PG}(3,q)$. The number x is called the *parameter* of the Cameron-Liebler line class. These classes appeared in connection with an attempt by Cameron and

Email addresses: `alexander.gavriliouk@gmail.com` (Alexander L. Gavrilyuk), `klaus.metsch@math.uni-giessen.de` (Klaus Metsch)

Dedicated to the memory of Frédéric Vanhove.

Liebler [4] to classify collineation groups of $PG(n, q)$, $n \geqslant 3$, that have equally many orbits on lines and on points.

An empty set of lines is a Cameron-Liebler line class with parameter $x = 0$. An example with $x = 1$ consists of all lines on a point, a second one of all lines in a plane. If the point is not in the plane, then the union of the previous two examples gives a Cameron-Liebler line class with parameter $x = 2$. There are no other examples with $x \in \{1, 2\}$, see [4]. As the complement of a Cameron-Liebler line class with parameter x is a Cameron-Liebler line class with parameter $q^2 + 1 - x$, there exist also examples with $x = q^2 + 1$, $x = q^2$ and $x = q^2 - 1$. It was conjectured [4] that these are the only Cameron − Liebler line classes. The first counterexamples were constructed by Drudge [8] (in $PG(3, 3)$ with $x = 5$), by Bruen and Drudge [3] (for all odd q, in $PG(3, q)$ with $x = (q^2 + 1)/2$), the examples are closely related to elliptic quadrics of $\mathrm{PG}(3, q)$, and later by Govaerts and Penttila [10] (in $PG(3, 4)$ with $x = 7$). Despite much effort, see e.g. [18], there is no infinite series known with $x \neq 0, 1, 2, \frac{1}{2}(q^2+1), q^2-1, q^2, q^2+1$.

Connecting Cameron-Liebler line classes to blocking sets, many non-existence results have been proved, see e.g. [6, 8, 11]. One of the strongest results obtained from the theory of blocking sets is by Govaerts and Storme [11] who showed that $2 < x \leq q$ is impossible when q is a prime. This was improved to the non-existence for $2 < x \leq q$ and all prime powers q [14]. Using a different technique, it was shown in [15] that there exists a constant c such that $x \leq 2$ or $x \geq cq^{4/3}$ for any prime power q. The main results of the present paper is the following modular equation connecting the parameter x with the number of lines of a Cameron-Liebler line class in the planes of $\mathrm{PG}(3, q)$ or dually the number of lines on a point.

Theorem 1.1. *Suppose $\mathcal{L}$ is a Cameron-Liebler line class with parameter x of* $\mathrm{PG}(3, q)$. *Then for every plane and every point of* $\mathrm{PG}(3, q)$

$$\binom{x}{2} + n(n - x) \equiv 0 \mod q + 1 \tag{1}$$

where n is the number of lines of $\mathcal{L}$ in the plane respectively through the point.

It is known, see Result 2.2 in Section 2, that a Cameron-Liebler line class $\mathcal{L}$ with parameter x of $\mathrm{PG}(3, q)$ has the following property. If P is a point and π a plane of $\mathrm{PG}(3, q)$ with $P \in \pi$, then the number of lines of $\mathcal{L}$ through P plus the number of lines of $\mathcal{L}$ in π is congruent to x modulo $q + 1$. Thus, if n is the number of lines of $\mathcal{L}$ in some plane, then every plane has congruent to n modulo $q+1$ lines of $\mathcal{L}$, and the number of lines of $\mathcal{L}$ through any point is congruent to $x - n$ modulo $q + 1$.

Corollary 1.2. *Suppose* $\mathrm{PG}(3, q)$ *has a Cameron-Liebler line class with parameter x. Then* (1) *has a solution for n in the set $\{0, 1, \ldots, q\}$.*

This corollary is a strong non-existence result for Cameron-Liebler line classes. In Section 3 we shall see for any given space $\mathrm{PG}(3, q)$ that it rules out roughly at least half of the possible parameters x of a Cameron-Liebler line class. This proves a conjecture stated in [9]. The technique used to prove this result is based on ideas of the papers [9] and [15]. As an application of our technique, we determine the spectrum for the parameter x of a Cameron-Liebler line class in $\mathrm{PG}(3,5)$.

Theorem 1.3. *A Cameron-Liebler line class with parameter x exists in* $\mathrm{PG}(3,5)$ *if and only if* $x \in \{0,1,2,10,12,13,14,16,24,25,26\}$.

For the proof of this theorem we also provide a construction for a new Cameron-Liebler line class with parameter 10 in $\mathrm{PG}(3,5)$, starting from one of the two complete 20-caps of $\mathrm{PG}(3,5)$ that were constructed by Abatangelo, Korchmaros and Larato in [1]. We also show that any two Cameron-Liebler line classes of $\mathrm{PG}(3,5)$ with parameter 10 are either projectively equivalent or dual to each other. Note that the spectra of parameters of Cameron-Liebler line classes in $\mathrm{PG}(3,q)$ with $q \leq 4$ were determined earlier, see [8, 10, 9].

In this paper, we do not study a question whether Cameron-Liebler line classes in $\mathrm{PG}(3,5)$ with parameter $x \in \{12,13\}$ found by Rodgers [18], and Bruen and Drudge [3] respectively, are unique. To our best knowledge the example with $x = 13$ is not unique.

The notion of Cameron − Liebler line classes in $PG(3,q)$ can be naturally generalized to that in $PG(n,q)$, $n > 3$, see [7]. The only known examples (up to their complement) are trivial, i.e., with parameter $x \in \{0,1,2\}$. For small values $q = 2,3,4$, it is shown that there are no other examples, see [7], [9]. We leave the corresponding question for $q = 5$ outside the scope of the present paper, though it should be solvable in the same manner as in [7], [9].

Finally, it is worthwhile to note that Cameron-Liebler line classes are equivalent or give rise to the following objects (besides the tight sets of the hyperbolic quadric $Q^+(5,q)$, see Section 2):

- projective two-weight codes, two-character sets (and thus, by the well-known Delsarte construction, strongly regular graphs) [17],
- completely regular codes (equitable partition, intriguing sets [5]) of the Grassmann graphs $J_q(4,2)$ with strength 1, which are essentially the same as the tight sets of the hyperbolic quadric $Q^+(5,q)$, whose the collinearity graph is the Grassmann graph $J_q(4,2)$,
- tight sets in generalised quadrangles $Q(4,q)$ [2].

2. Preliminaries

We make use of the Klein-correspondence from $\mathrm{PG}(3,q)$ to the hyperbolic quadric $Q^+(5,q)$. The reader who is not familiar with this concept is referred to [13] for properties of the hyperbolic quadric and to Section 15.4 of [12] for the Klein-correspondence.

The ambient space of $Q^+(5,q)$ is $\mathrm{PG}(5,q)$, the related polarity is denoted by $\perp$. It is known that the planes of the quadric $Q^+(5,q)$ fall into two classes such that different planes are in the same class if and only if they meet in a point. As usual we call the planes of one class *Greek planes* while the other planes are called *Latin planes*. A *tight set* with *parameter* x of $Q^+(5,q)$ is defined to be a set of points that meets every elliptic quadric $Q^-(3,q)$ of $Q^+(5,q)$ in exactly x points. As the Klein-correspondence maps the regular spreads of $\mathrm{PG}(3,q)$ to the elliptic quadrics $Q^-(3,q)$ of $Q^+(5,q)$, then it translates Cameron-Liebler line classes with parameter x of $\mathrm{PG}(3,q)$ to tight sets of $Q^+(5,q)$ with the same parameter. Thus there are two different environments to study Cameron-Liebler line classes and we shall make use of both.

We start with a collection of some important results for tight sets, which of course correspond to equivalent results on Cameron-Liebler line classes.

Result 2.1 ([4]). *Let M be a tight set with parameter x of $Q^+(5,q)$. Then*

1. $|M| = x(q^2+q+1)$.
2. *For every point $P \in M$ we have $|P^\perp \cap M| = q^2 + x(q+1)$.*
3. *For every point $P \in Q^+(5,q) \setminus M$ we have $|P^\perp \cap M| = x(q+1)$.*

Result 2.2 ([16]). *Let M be a tight set of $Q^+(5,q)$ and ℓ a line of the ambient space* $\mathrm{PG}(5,q)$. *Then $|\ell^\perp \cap M| = q|\ell \cap M| + x$. In particular, if ℓ is a line of the quadric $Q^+(5,q)$ and π and τ are the planes of the quadric on ℓ, then*

$$|\pi \cap M| + |\tau \cap M| = (q+1)|\ell \cap M| + x.$$

Let M be a tight set and P a point of $Q^+(5,q)$. It is well-known that P lies in $q+1$ Latin planes $\tau_0, \dots, \tau_q$ and $q+1$ Greek planes $\pi_0, \dots, \pi_q$. Define the square matrix $T = (t_{ij})$ of size $q+1$ with integer entries $t_{ij} := |((\tau_i \cap \pi_j) \setminus \{P\}) \cap M|$, $0 \le i,j \le q$. The set consisting of the matrix T, its transpose, and every matrix obtained from one of these two by a permutation of the rows and a permutation of the columns is called the *pattern* of P with respect to M. We represent each pattern by one of its matrices. By slight abuse of notation we also call each matrix of this set the pattern for P. This concept has been introduced in [9] where the important equalities of part (d) of the following proposition have been proved.

Proposition 2.3. *Let M be a tight set of $Q^+(5,q)$, let P be a point of the quadric, and $T = (t_{ij})$ the pattern of P.*

(a) *The planes of $Q^+(5,q)$ on P correspond one-to-one to the columns and rows of T, and each column sum and each row sum is the number of points of $M \setminus \{P\}$ in the corresponding plane.*

(b) *For all $k,l \in \{0,\dots,q\}$*

$$\sum_{i=0}^{q} t_{il} + \sum_{j=0}^{q} t_{kj} = \begin{cases} x + (q+1)t_{kl} & \text{if } P \notin M \\ x + (q+1)(t_{kl}+1) - 2 & \text{if } P \in M. \end{cases}$$

(c) $t_{kl} + t_{rs} = t_{ks} + t_{rl}$ *for all $k,l,r,s \in \{0,\dots,q\}$.*

(d)

$$\sum_{i,j=0}^{q} t_{ij}^2 = \begin{cases} x(q+x) & \text{if } P \notin M \\ q^3 + q^2 + (x-1)^2 + q(x-1) & \text{if } P \in M. \end{cases}$$

Proof. (a) This is a consequence of the definition of the pattern of P, using that each Latin or Greek plane on P is the union of the lines in which it intersects the $q+1$ Greek respectively Latin planes on P.

(b) This is a reformulation of Result 2.2 for the lines of $Q^+(5,q)$ on P.

(c) This is an immediate consequence of part (b).

(d) This was proved in [9], but we mention that it follows from Result 2.2 by counting pairs (R,S) of points of M with $S \sim R \sim P \not\sim S$ in the collinearity graph of $Q^+(5,q)$. □

For the construction of a Cameron-Liebler line class in the last section we need the notion of caps in projective space. A *k-cap* in $\mathrm{PG}(3,q)$ is a set of k points, no three of which are collinear. A k-cap is called *complete* if it is not contained in a $(k+1)$-cap.

The maximum value of k, for which there exists a k-cap in $\mathrm{PG}(3,q)$, $q \geq 3$, is q^2+1, and if q is odd such a cap consists of the points of an elliptic quadric, see [13]. The size of the second largest complete cap (usually denoted by $m_2'(3,q)$) is only known for some small values of q. Fortunately, in [1], it is shown that $m_2'(3,5) = 20$ and that there are, up to isomorphism, only two complete 20-caps in $\mathrm{PG}(3,5)$. We start with one of these 20-caps to construct a new Cameron-Liebler line class in $\mathrm{PG}(3,5)$ with parameter $x = 10$.

3. Proof and discussion of Theorem 1.1

We start with the proof of Theorem 1.1, which we formulate in terms of tight sets. Then we discuss the modular condition (1) of the theorem.

Theorem 3.1. *If M is a tight set of $Q^+(5,q)$ with parameter x, then for any plane π of $Q^+(5,q)$ we have*

$$\binom{x}{2} + n(n-x) \equiv 0 \mod q+1$$

where n is the number of points of M in the plane.

Proof. We first consider the case that the plane π in question is not completely contained in M. Consider a point P of π with $P \notin M$ and its pattern $T = (t_{ij})$. We may assume that the first column of T corresponds to π, so that the number n of points in π is equal to $\sum_{i=0}^{q} t_{i0}$. Proposition 2.3 (d) gives

$$\sum_{i,j=0}^{q} t_{ij}^2 = x(q+x)$$

and part (c) of the same proposition shows that $t_{ij} = t_{i0} + t_{0j} - t_{00}$ for $i,j \geq 1$, thus

$$t_{00}^2 + \sum_{i=1}^{q} t_{i0}^2 + \sum_{j=1}^{q} t_{0j}^2 + \sum_{i,j=1}^{q} (t_{i0} + t_{0j} - t_{00})^2 = x(q+x).$$

Defining $E := \sum_{i=1}^{q} t_{i0}$ and $F := \sum_{j=1}^{q} t_{0j}$, this can be written as

$$(q^2+1)t_{00}^2 + (q+1)(\sum_{i=1}^{q} t_{i0}^2 + \sum_{j=1}^{q} t_{0j}^2) + 2EF - 2t_{00}q(E+F) = x(q+x).$$

Modulo 2 we have $t^2 \equiv t$ for every integer t, so $\sum_{i=1}^{q} t_{i0}^2 \equiv E$ and $\sum_{j=1}^{q} t_{0j}^2 \equiv F$. Hence

$$(q^2+1)t_{00}^2 + (q+1)(E+F) + 2EF + 2(E+F)t_{00} \equiv x(q+x) \mod 2(q+1). \quad (2)$$

Proposition 2.3 (b) shows that $E + F = t_{00}(q-1) + x$. Modulo $2(q+1)$ we therefore have

$$\begin{aligned} 2(E+F)t_{00} &\equiv 2t_{00}(x - 2t_{00}), \\ 2EF &\equiv 2E(t_{00}(q-1) + x - E) \equiv 2E(x - 2t_{00} - E), \\ (q+1)(E+F) &\equiv (q+1)(t_{00}(q-1) + x). \end{aligned}$$

Using this in (2) gives

$$(q^2-1)t_{00}(t_{00}+1) - 2(E+t_{00})(E+t_{00}-x) \equiv x(x-1) \mod 2(q+1).$$

The first term on the left hand side is divisible by $2(q+1)$, hence

$$2(E+t_{00})(E+t_{00}-x) + x(x-1) \equiv 0 \mod 2(q+1). \quad (3)$$

Since $n = \sum_{i=0}^{q} t_{i0} = E + t_{00}$, this proves Theorem 1.1 in the considered case.

Consider now the case that π is completely contained in M. Then we can argue in two ways. Firstly, we could repeat the above argument for any point P of π. As P lies in M this time, there will be slight differences, but in the end, we will find

$$2(E+t_{00}+1)(E+t_{00}+1-x) + x(x-1) \equiv 0 \mod 2(q+1).$$

This time $E+t_{00}+1$ is the number n of points of M in π, so we are done again. Alternatively, we can consider $M' := M \setminus \pi$, which is a tight set with parameter $x-1$ (since $\pi \subseteq M$) with $n' := |\pi \cap M'| = 0$, so that we can apply (3) to π and M' giving $(x-1)(x-2) \equiv 0 \mod 2(q+1)$. As $n = q^2+q+1$, this is equivalent to $2n(n-x) + x(x-1) \equiv 0 \mod 2(q+1)$. □

Reducing (1) to prime powers p^k that divide $2(q+1)$ one obtains interesting corollaries. We mention the ones for $p^k \in \{4, 5, 8\}$.

Corollary 3.2. PG$(3, q)$, *q odd, does not have a Cameron-Liebler line class with parameter* $x \equiv 3 \mod 4$.

Corollary 3.3. PG$(3, q)$, $q \equiv 4 \mod 5$ *odd, does not have a Cameron-Liebler line class with parameter* $x \equiv 3 \mod 5$ *or* $x \equiv 4 \mod 5$.

Corollary 3.4. PG$(3,q)$, $q \equiv 3 \mod 4$ *odd, does not have a Cameron-Liebler line class with parameter* x *congruent to* 3, 4, 6 *or* 7 *modulo* 8.

We now investigate the solutions of equation (1) in general. We write the equation in the form

$$x(x-1) + 2n(n-x) \equiv 0 \mod 2(q+1) \tag{4}$$

and wish to determine the number of integers $x \in \{0, 1, \ldots, q^2+1\}$ for which this modular equation has a solution in n. First of all, it suffices to consider integers x with $0 \le x < 2(q+1)$. Let $2(q+1) = p_1^{k_1} \ldots p_s^{k_s}$ be the prime factorization of $2(q+1)$. If we consider x and q as fixed and (4) as an equation for n, then the Chinese Remainder Theorem states that (4) has a solution in n, if each of the equations

$$x(x-1) + 2n(n-x) \equiv 0 \mod p_i^{k_i} \tag{5}$$

has a solution. Also, if w_i is the number of integers x with $0 \le x < p_i^{k_i}$ such that (5) has a solution in n, then $w_1 \ldots w_s$ is the number of integers x with $0 \le x < 2(q+1)$ such that (4) has a solution in n.

It will turn out that (5) with $k_i > 1$ is only slightly more restrictive than (5) with $k_i = 1$. Note that (5) gives no condition when $p_i = 2$ and $k_i = 1$. We now analyze first the situation $k_i = 1$ and $p_i \neq 2$.

Lemma 3.5. *For an odd prime* p*, the number of integers* x *with* $0 \le x < p$ *such that there exists an integer* n *satisfying*

$$x(x-1) + 2n(n-x) \equiv 0 \mod p$$

is $\frac{1}{2}(p+1)$ *when* $p \equiv 1 \mod 4$ *and* $\frac{1}{2}(p+3)$ *when* $p \equiv 3 \mod 4$.

Proof. Instead of performing calculations modulo p, we consider the equation over the finite field $\mathbb{F}_p$. As p is odd, we write $x = 2y$, so that the equation reads as

$$2y(2y-1) + 2n(n-2y) = 0.$$

Dividing by 2, this is equivalent to

$$\left(y + \frac{p-1}{2}\right)^2 = \left(\frac{p-1}{2}\right)^2 - (n-y)^2.$$

We try to find all y that satisfy this equation for some n. We can therefore replace $(n-y)^2$ in the last equation by n^2 and consider:

$$\left(y + \frac{p-1}{2}\right)^2 = \left(\frac{p-1}{2}\right)^2 - n^2.$$

The number of feasible y thus depends on the number of squares in $\mathbb{F}_p$ that can be written as a difference of a given square and an arbitrary square n^2. It is well-known in number theory as well as in algebra that there are $\frac{1}{4}(p+3)$

such squares n^2 when $p \equiv 1 \mod 4$ and there are $\frac{1}{4}(p+5)$ such squares when $p \equiv 3 \mod 4$. Each square corresponds to two feasible values of y, except that $n^2 = \left(\frac{p-1}{2}\right)^2$ corresponds only to one feasible value for x. The assertion follows. $\square$

Remark. If $q+1$ is not a power of 2, so that $q+1$ has an odd prime divisor, then roughly half of the integers x with $0 \le x \le q^2+1$ are excluded by this lemma and Corollary 1.2 as parameters of Cameron-Liebler line classes in $\mathrm{PG}(3,q)$. When $q+1$ has more than one prime divisor, then usually more than half of the parameters x are ruled out by our results. If $q \in \{2^2, 2^4, 2^8, 2^{16}\}$ then $q+1$ is a prime congruent to 1 mod 4, so only slightly less than one half of the integers x with $0 \le x \le q^2+1$ are excluded by our results.

Next we study the solutions of (5) with $k_i > 1$. It is convenient to use the following notation for positive integers z:

$$Z(z) := \{0, \dots, z-1\},$$
$$S(z) := \{x \in Z(z) \mid x(x-1) + 2n(n-x) \equiv 0 \mod z \text{ for some integer } n\}.$$

Note that $0, 1, 2 \in S(z)$ for all z, reflecting the fact that there are Cameron-Liebler line classes with parameters 0, 1, and 2.

Lemma 3.6. *Let p be an odd prime and $k \ge 1$ an integer.*

(a) *An element $\tilde{x} \in Z(p^{k+1})$ that is not congruent to 0 or 2 mod p^k lies in $S(p^{k+1})$ if and only if $\tilde{x} \mod p^k$ lies in $S(p^k)$.*
(b) *If k is odd, then $S(p^{k+1})$ contains 0 and 2 but no other integers congruent to 0 or 2 modulo p^k.*
(c) *If k is even, then the integers in $S(p^{k+1})$ that are congruent 0 or 2 mod p^k are $2\gamma^2 p^k \mod p^{k+1}$ and $2(1-\gamma^2 p^k) \mod p^{k+1}$ with $\gamma \in Z(p)$.*

Proof. (a) Let $\tilde{x} \in Z(p^{k+1})$, let x be the integer of $Z(p^k)$ with $\tilde{x} \equiv x \mod p^k$ and suppose that $x \ne 0$ and $x \ne 2$. Clearly if $\tilde{x} \in S(p^{k+1})$, then $x \in S(p^k)$. To see the converse assume that $x \in S(p^k)$ and let n be an integer such that

$$x(x-1) + 2n(n-x) \equiv 0 \mod p^k. \tag{6}$$

We have to show that there exists an integer $\tilde{n}$ satisfying

$$\tilde{x}(\tilde{x}-1) + 2\tilde{n}(\tilde{n}-\tilde{x}) \equiv 0 \mod p^{k+1}. \tag{7}$$

Put $j := \lceil \frac{k}{2} \rceil$. We claim that p^j does not divide $2n-x$. Assume on the contrary that $p^j \mid 2n-x$. Then

$$0 \equiv x(x-1) + 2n(n-x) \equiv 2n(2n-1) + 2n(n-2n) \equiv 2n(n-1) \mod p^j$$

so n is congruent to 0 or 1 modulo p^j.

Case 1. We consider the situation when $n \equiv 0 \mod p^j$. Then $x \equiv 2n \equiv 0 \mod p^j$, so $2n(n-x) \equiv 0 \mod p^{2j}$. As $2j \ge k$, it follows from (6) that

$$0 \equiv x(x-1) + 2n(n-x) \equiv x(x-1) \mod p^k.$$

Since $p^j \mid x$ where $j \geq 1$ and since $x \in Z(p^k)$, this implies that $x = 0$, contradicting the choice of $\tilde{x}$ in the beginning of the proof.

Case 2. We consider the situation when $n \equiv 1 \mod p^j$. Then $x \equiv 2n \equiv 2 \mod p^j$, so $p^j \mid n+1-x$. Thus $p^{2j} \mid (n-1)(n+1-x)$. As $2j \geq k$, it follows from (6) that

$$0 \equiv x(x-1) + 2n(n-x) - 2(n-1)(n+1-x) \equiv (x-1)(x-2) \mod p^k.$$

As $x \equiv 2 \mod p^j$ and $j \geq 1$, it follows that $x \equiv 2 \mod p^k$. Since $x \in Z(p^k)$, it follows that $x = 2$, but again this is a contradiction.

Thus we have shown that p^j does not divide $2n - x$. Let p^i be the largest power of p dividing $2n - x$. Then $0 \leq i < \frac{k}{2}$. We now claim that there is an integer $\tilde{n}$ of the form $\tilde{n} = n + \beta p^{k-i}$ with $\beta \in Z(p)$ that satisfies (7). To see this, we use that $\tilde{x} \equiv x \mod p^k$, so that $\tilde{x} = x + \alpha p^k$ for some $\alpha \in Z(p)$. Then condition (7) for an integer $\tilde{n}$ of the form $\tilde{n} = n + \beta p^{k-i}$ with $\beta \in Z(p)$ is equivalent to

$$x(x-1) + 2n(n-x) + \alpha(2x-1-2n)p^k + 2\beta p^{k-i}(2n-x) \equiv 0 \mod p^{k+1}. \quad (8)$$

In view of (6) and since p^i is the highest power of p dividing $2n - x$, one can divide by p^k and finds a condition on β modulo p, where the coefficient of β is coprime to p. Hence there exists a unique $\beta \in Z(p)$ satisfying the condition.

(b) and (c) Clearly $0, 2 \in S(p^{k+1})$. For $0 \neq \alpha \in Z(p)$ we have $\alpha p^k \in S(p^{k+1})$ if and only if there exists an integer n with

$$\alpha p^k(\alpha p^k - 1) + 2n(n - \alpha p^k) \equiv 0 \mod p^{k+1}. \quad (9)$$

If there exists such an n at all, then p^k must divide $2n^2$ but p^{k+1} does not. This can happen only if k is even and then n must have the form $\gamma p^{k/2}$. Then (9) holds if and only if $\alpha = 2\gamma^2$. A similar argument can be used to investigate the integers of $Z(p^{k+1})$ that are congruent to 2 mod p^k. □

Proposition 3.7. *For an odd prime p, we have*

$$|S(p^k)| = p^{k-1}s - \frac{p^k + (-1)^k p}{p+1} + \frac{3 + (-1)^k}{2}$$

where $s = \frac{1}{2}(p-1)$ when $p \equiv 1 \mod 4$ and $s = \frac{1}{2}(p+1)$ when $p \equiv 3 \mod 4$.

Proof. This follows by induction on k. For $k = 1$, the assertion was proved in Lemma 3.5. For the induction step we use from Lemma 3.6 that

$$|S(p^{k+1})| = (|S(p^k)| - 2)p + 2 \qquad \text{if } k \text{ is odd}$$

$$|S(p^{k+1})| = (|S(p^k)| - 2)p + 2 \cdot \frac{p+1}{2} \qquad \text{if } k \text{ is even}$$

The induction step is obtained by an easy calculation. □

Proposition 3.8. *We have* $|S(2)| = 2$, $|S(4)| = 3$, $|S(8)| = 4$ *and*

$$|S(2^k)| = 2^{k-2} + 3 + \frac{1}{3}(2^{k-3} + (-1)^k)$$

for $k \geq 4$.

Proof. This is very similar to the previous proposition. The statement for $S(2^k)$ with $k \leq 6$ follows easily by hand. We assume from now on that $k \geq 7$. The statement follows by induction on k once we have shown that $|S(2^{k+1})| = 2|S(2^k)| - 2$ when k is odd, and $|S(2^{k+1})| = 2|S(2^k)| - 4$ when k is even. To do so, we first remark that $\tilde{x} \in S(2^{k+1})$ implies that $\tilde{x} \mod 2^k$ lies in $S(2^k)$. Thus it suffices to determine for each element x of $S(2^k)$ whether or not x and $x + 2^k$ lie in $S(2^{k+1})$. We shall see that both lie in $S(2^{k+1})$ for almost all x.

Since $x \in S(2^k)$, there exists an integer n such that

$$x(x-1) + 2n(n-x) \equiv 0 \mod 2^k. \tag{10}$$

Let $\tilde{x}$ be one of the integers x and $x + 2^k$. We have to investigate whether the equation

$$\tilde{x}(\tilde{x}-1) + 2\tilde{n}(\tilde{n}-\tilde{x}) \equiv 0 \mod 2^{k+1} \tag{11}$$

has a solution in $\tilde{n}$. Put $j = \lceil \frac{k-1}{2} \rceil$. We consider two cases.

Case 1. We assume that 2^j does not divide $2n - x$ and show $\tilde{x} \in S(2^{k+1})$. We have $\tilde{x} = x + \alpha 2^k$ with $\alpha \in \{0, 1\}$. Let 2^i be the largest power of 2 dividing $2n - x$. Then $0 \leq i < \frac{k-1}{2}$. We now claim that there is an integer $\tilde{n}$ of the form $\tilde{n} = n + \beta 2^{k-i-1}$ with $\beta \in \{0, 1\}$ that satisfies (11). In fact, if we substitute $\tilde{x} = x + \alpha 2^k$ and $\tilde{n} = n + \beta 2^{k-i-1}$, then condition (11) is equivalent

$$x(x-1) + 2n(n-x) - \alpha 2^k + \beta 2^{k-i}(2n - x) \equiv 0 \mod 2^{k+1}. \tag{12}$$

In view of (10) and since 2^i is the largest power of 2 dividing $2n - x$, one can divide by 2^k and finds a condition on β modulo 2, where the coefficient of β is 1. Hence there exists a unique $\beta \in \{0, 1\}$ satisfying the condition.

Case 2. We assume that 2^j divides $2n - x$. As in the proof of Lemma 3.6 this implies that 2^j divides $2n(n-1)$. Hence 2^{j-1} divides $n - e$ for some $e \in \{0, 1\}$. Then $x \equiv 2n \equiv 2e \mod 2^j$, so $2(n-e)(n+e-x) \equiv 0 \mod 2^{2j-1}$. As $2j - 1 \leq k$, then (10) implies that

$$0 \equiv x(x-1) + 2n(n-x) - 2(n-e)(n+e-x) \equiv (x-1)(x-2e) \mod 2^{2j-1}.$$

As $x \equiv 2e \mod 2^j$ and $j > 0$, it follows that $x \equiv 2e \mod 2^{2j-1}$. We also have $0 \leq x < 2^k$ and $e \in \{0, 1\}$. If k is even, then $2j - 1 = k - 1$, and thus $x \in E(k) := \{0, 2, 2^{k-1}, 2 + 2^{k-1}\}$, and if k is odd, then $2j - 1 = k - 2$, so $x \in O(k) := \{r \cdot 2^{k-2}, 2 + r \cdot 2^{k-2} \mid r = 0, 1, 2, 3\}$.

Analyzing (10) one can check for $k \geq 7$ that $E(k) \subseteq S(2^k)$ when k is even, and that $O(k) \cap S(2^k) = O'(k) := \{0, 2, 2^{k-2}, 2 + 3 \cdot 2^{k-2}\}$ when k is odd. As an example we show that 2^{k-1} is not in $S(2^k)$, when k is odd. Assume on the contrary that there exists an integer n such that (10) is satisfied, that is

$$2^{k-1}(2^{k-1}-1)+2n(n-2^{k-1})\equiv 0 \mod 2^k. \tag{13}$$

It follows that $2^{k-1} \mid 2n^2$. As k is odd, this implies that $2^{k-1} \mid n^2$, that is $2^k \mid 2n^2$. As $2(k-1)\geq k$ (since $k\geq 7$), then (13) gives $2^{k-1}\equiv 0 \mod 2^k$, which is absurd.

If k is even, then $x\in E(k)$ implies that $\tilde{x}\in\{x, 2^k+x\}$, so $\tilde{x}\in O(k+1)$. We know that only four of the eight numbers of $O(k+1)$ lie in $S(2^{k+1})$. Hence, the four possibilities for x give eight possibilities for $\tilde{x}$, but only four of these lie in $S(2^{k+1})$. Hence $|S(2^{k+1})| = 2|S(2^k)|-4$, if $k\geq 8$ is even.

Now assume that k is odd and $x\in O'(k)$. If $x=0$, then $\tilde{x}\in\{0,2^k\}$ and thus $\tilde{x}\in E(k+1)\subseteq S(2^{k+1})$. The same is true for $x=2$. Next let $x=2^{k-2}$, so that $\tilde{x}\in\{2^{k-2}, 2^k+2^{k-2}\}$. Analyzing (11), one sees that only 2^{k-2} lies in $S(2^{k+1})$. Similarly, if $x=2+3\cdot 2^{k-2}$, then $\tilde{x}\in\{2+3\cdot 2^{k-2}, 2^k+2+3\cdot 2^{k-2}\}$, but only $2^k+2+3\cdot 2^{k-2}$ lies in $S(2^{k+1})$. Hence, the four possibilities for x give eight possibilities for $\tilde{x}$, but only six of these lie in $S(2^{k+1})$. Hence $|S(2^{k+1})| = 2|S(2^k)|-2$, when $k\geq 7$ is odd. □

The number of integers x with $0\leq x<2(q+1)$ such that equation (4) or equivalently (1) has a solution in n is equal to the product of the numbers $|S(p_i^{k_i})|$ for $i=1,\ldots,s$, where $2(q+1)=p_1^{k_1}\ldots p_s^{k_s}$ is the prime factorization of $2(q+1)$.

4. Tight Sets in $Q^+(5,5)$

In the remaining two sections of the paper, we want to determine the spectrum of parameters of all tight sets of $Q^+(5,q)$ with $q=5$. As the complement of a tight set with parameter x is a tight set with parameter q^2+1-x, it suffices to consider the integers $x\leq\frac{1}{2}(q^2+1)=13$. It is known that Cameron-Liebler line classes of $\mathrm{PG}(3,q)$ exist for $x\in\{0,1,2,12,13\}$. The one with $x=0$ is the empty set, examples with $x=1$, $x=2$ and $x=13$ have been mentioned in the introduction, and an example with $x=12$ was found by M. Rodgers [18]. For the non-existence results, we have $x\neq 3,4$, which probably appears first in [16], we have $x\neq 3,4,5$ by [11], and $x\neq 7,11$ by Theorem 1.1. Thus the open values are 6, 8, 9 and 10. We shall show in this section that $x\in\{6,8,9\}$ is impossible. In the next section we will construct a tight set with parameter $x=10$.

Our strategy is to compute all possible patterns for points of $Q^+(5,5)$ by enumerating all (6×6)-matrices with entries from $\{0,1,\ldots,5\}$ that satisfy the conditions of Proposition 2.3. As each pattern matrix $T=(t_{ij})$ is determined by the 10 entries t_{i0}, $i=1,\ldots,5$ and t_{0j}, $j=1,\ldots,5$, this can be easily be managed with a computer. Thus in each of the following lemmas we use a computer program to determine all admissible patterns. We notice that the cases $x\in\{3,4,5\}$ can be excluded easily by the same technique.

Lemma 4.1. *If M is a tight set with parameter x of $Q^+(5,q)$ with $q=5$, then $x \neq 6$.*

Proof. Assume that $x=6$. Then there is only one possible pattern for points in M, which is the first one in Table 1, and two possible patterns for points outside M, which are the second and third in the same table. As the first pattern has

$$\begin{pmatrix} 0&0&0&1&3&4\\ 0&0&0&1&3&4\\ 0&0&0&1&3&4\\ 0&0&0&1&3&4\\ 1&1&1&2&4&5\\ 1&1&1&2&4&5 \end{pmatrix} \begin{pmatrix} 0&0&0&1&1&1\\ 0&0&0&1&1&1\\ 0&0&0&1&1&1\\ 0&0&0&1&1&1\\ 1&1&1&2&2&2\\ 2&2&2&3&3&3 \end{pmatrix} \begin{pmatrix} 0&0&0&0&1&2\\ 0&0&0&0&1&2\\ 0&0&0&0&1&2\\ 1&1&1&1&2&3\\ 1&1&1&1&2&3\\ 1&1&1&1&2&3 \end{pmatrix}$$

Table 1: Patterns in the case $x=6$

column sum 26 in its last column, every point of M lies on a plane of $Q^+(5,q)$ that meets M in 27 points, see Proposition 2.3(a). Since a plane with 27 points in M has also a point not in M, there exist points outside M that lie in a plane with 27 points in M. But no column or row sum in the two patterns for points of $Q^+(5,q) \setminus M$ is 27, contradicting Proposition 2.3(a). □

Lemma 4.2. *If M is a tight set with parameter x of $Q^+(5,q)$ with $q=5$, then $x \neq 8$.*

Proof. Assume that there exists a tight set M with parameter $x=8$. Then the possible patterns for the points in $Q^+(5,q) \setminus M$ are the first three in Table 2, and the ones for points in M the last two in the same table. The two possible

$$\begin{pmatrix} 0&0&1&1&1&1\\ 0&0&1&1&1&1\\ 0&0&1&1&1&1\\ 0&0&1&1&1&1\\ 2&2&3&3&3&3\\ 2&2&3&3&3&3 \end{pmatrix} \begin{pmatrix} 0&0&0&1&1&2\\ 0&0&0&1&1&2\\ 0&0&0&1&1&2\\ 1&1&1&2&2&3\\ 1&1&1&2&2&3\\ 2&2&2&3&3&4 \end{pmatrix} \begin{pmatrix} 0&0&0&0&2&2\\ 0&0&0&0&2&2\\ 1&1&1&1&3&3\\ 1&1&1&1&3&3\\ 1&1&1&1&3&3\\ 1&1&1&1&3&3 \end{pmatrix} \begin{pmatrix} 0&0&0&3&3&3\\ 0&0&0&3&3&3\\ 0&0&0&3&3&3\\ 1&1&1&4&4&4\\ 1&1&1&4&4&4\\ 1&1&1&4&4&4 \end{pmatrix} \begin{pmatrix} 0&0&1&1&3&4\\ 0&0&1&1&3&4\\ 0&0&1&1&3&4\\ 1&1&2&2&4&5\\ 1&1&2&2&4&5\\ 1&1&2&2&4&5 \end{pmatrix}$$

Table 2: Patterns in the case $x=8$

patterns for points in M have 21 as a column sum, so every point of M lies on a plane of $Q^+(5,q)$ that meets M in 22 points. But no one of the three patterns for the points of $Q^+(5,q) \setminus M$ has column or row sum 22, contradicting Proposition 2.3(a).

□

Lemma 4.3. *If M is a tight set with parameter x of $Q^+(5,q)$ with $q=5$, then $x \neq 9$.*

Proof. Assume that $x = 9$. Then the possible patterns for the points in $Q^+(5,q) \setminus M$ are the first six in Table 3. As 24 is the largest row or column sum in these matrices, we see that every plane of $Q^+(5,q)$ that is not completely contained in M has at most 24 points in M.

$$\overset{(1)}{\begin{pmatrix} 0&0&2&2&2&3\\ 0&0&2&2&2&3\\ 0&0&2&2&2&3\\ 0&0&2&2&2&3\\ 0&0&2&2&2&3\\ 0&0&2&2&2&3 \end{pmatrix}} \quad \overset{(2)}{\begin{pmatrix} 0&1&1&1&3&3\\ 0&1&1&1&3&3\\ 0&1&1&1&3&3\\ 0&1&1&1&3&3\\ 0&1&1&1&3&3\\ 0&1&1&1&3&3 \end{pmatrix}} \quad \overset{(3)}{\begin{pmatrix} 0&0&1&1&2&2\\ 0&0&1&1&2&2\\ 0&0&1&1&2&2\\ 0&0&1&1&2&2\\ 1&1&2&2&3&3\\ 2&2&3&3&4&4 \end{pmatrix}} \quad \overset{(4)}{\begin{pmatrix} 0&0&0&2&2&2\\ 0&0&0&2&2&2\\ 0&0&0&2&2&2\\ 1&1&1&3&3&3\\ 1&1&1&3&3&3\\ 1&1&1&3&3&3 \end{pmatrix}} \quad \overset{(5)}{\begin{pmatrix} 0&0&1&1&1&3\\ 0&0&1&1&1&3\\ 0&0&1&1&1&3\\ 1&1&2&2&2&4\\ 1&1&2&2&2&4\\ 1&1&2&2&2&4 \end{pmatrix}}$$

$$\overset{(6)}{\begin{pmatrix} 1&1&1&1&1&4\\ 1&1&1&1&1&4\\ 1&1&1&1&1&4\\ 1&1&1&1&1&4\\ 1&1&1&1&1&4\\ 1&1&1&1&1&4 \end{pmatrix}} \quad \overset{(7)}{\begin{pmatrix} 0&0&2&3&3&3\\ 0&0&2&3&3&3\\ 0&0&2&3&3&3\\ 0&0&2&3&3&3\\ 0&0&2&3&3&3\\ 2&2&4&5&5&5 \end{pmatrix}} \quad \overset{(8)}{\begin{pmatrix} 0&0&1&1&3&3\\ 0&0&1&1&3&3\\ 0&0&1&1&3&3\\ 1&1&2&2&4&4\\ 2&2&3&3&5&5\\ 2&2&3&3&5&5 \end{pmatrix}} \quad \overset{(9)}{\begin{pmatrix} 0&0&0&2&3&3\\ 0&0&0&2&3&3\\ 1&1&1&3&4&4\\ 1&1&1&3&4&4\\ 1&1&1&3&4&4\\ 2&2&2&4&5&5 \end{pmatrix}}$$

Table 3: Patterns in the case $x = 9$

For the points in M, there are also six possible patterns, however, three of these have column or row sum equal to 26 or 29, so require planes that meet the quadric in 27 or 30 points, which is not possible; the three remaining patterns are the ones with numbers (7), (8) and (9) in the table.

Each of the three possible patterns of points of M has a row or a column whose entries sum up to 23 and such that some entry in this row or column is equal to 4. This corresponds to a plane with 24 points in M and a line ℓ therein with 5 point in M, which therefore necessarily exist. Consider the unique point of ℓ that is not in M. The pattern for this point must have a column or row whose entries sum up to 24 and such that some entry in the column or row is 5. But from the patterns (1)-(6) only in pattern (6) the last column sum is 24 but there is no entry 5 in this column, contradiction. □

5. Tight sets with parameter $x = 10$ in $Q^+(5,5)$

We start this section with a construction of a Cameron-Liebler line class with parameter 10 of $\mathrm{PG}(3,5)$ and then we show that all Cameron-Liebler line classes with parameter 10 of $\mathrm{PG}(3,5)$ are projectively equivalent.

It was shown in [1] that $\mathrm{PG}(3,5)$ possesses only two projectively inequivalent complete caps with 20 points, one of which is missing 16 planes whereas the other is missing only 11 planes. For the construction we use the complete cap K_1 with 20 points in $\mathrm{PG}(3,5)$ that was constructed in [1]. One of the properties of K_1 proved in [1] is that it is the union of five tetrahedra in the sense that a tetrahedron consists of four points of the cap and such that there are four planes that contain three points of the tetrahedron but no other point of the cap, which can therefore be called facets of the polyhedra. In total, there are 20 planes that meet the cap in just three points and these are the $5 \times 4 = 20$ facets of the five tetrahedra. Another property of K_1 is that it misses exactly 16 planes.

The uniqueness of K_1 implies that all Cameron-Liebler line classes obtained by the construction below are projectively equivalent.

Construction. Let K_1 be a cap of $\mathrm{PG}(3,5)$ with 20 points such that there exist 16 planes missing K_1. Let $\mathcal{L}$ be the set consisting of the following lines.

- the 120 intersection lines of two planes missing K_1,
- the 160 lines that lie in a plane missing K_1 and two planes meeting K_1 in three points.
- the $5 \times 6 = 30$ lines that are edges of the tetrahedra, that is the secant lines to K_1 that lie in two planes meeting K_1 in three points.

Then $\mathcal{L}$ is a Cameron-Liebler line class with parameter $x = 10$. This can be checked by hand, but we omit a proof.

Theorem 5.1. *If $\mathcal{L}$ is a Cameron-Liebler line classes of* $\mathrm{PG}(3,5)$ *with parameter* 10*, then either $\mathcal{L}$ or its dual can be obtained from a complete* 20*-cap as in the above construction.*

We prove this theorem in a series of lemmas. Throughout, $\mathcal{L}$ denotes a Cameron-Liebler line class of $\mathrm{PG}(3,5)$ with parameter 10. We use the results of Section 2 after their translation by the Klein-Correspondence. By Theorem 1.1, the number of lines of $\mathcal{L}$ incident with a given point or plane is congruent to 1 or 3 modulo 6. By switching to the dual space if necessary, Result 2.2 implies that we can assume for all points P and planes π that the number of lines of $\mathcal{L}$ on P is congruent to 3 modulo 6, and the number of lines of $\mathcal{L}$ in π is congruent to 1 modulo 6.

We consider the patterns of the lines ℓ of $\mathrm{PG}(3,5)$ with respect to $\mathcal{L}$, and represent them by matrices such that the rows of the pattern correspond to the planes π on ℓ while the columns correspond to points P of ℓ, and the (π, P)-entry of the pattern is the number of lines of $\mathcal{L} \setminus \{\ell\}$ in the pencil of lines through P and in π. Thus, if $\ell \notin \mathcal{L}$, then each column sum of the matrix gives the number of lines of $\mathcal{L}$ on the point corresponding to the column, and each row sum is the number of lines of $\mathcal{L}$ in the plane corresponding to the row. If $\ell \in \mathcal{L}$, then the row or column sum is one less, as the line ℓ itself is also incident with the corresponding points and planes. By $\overline{\mathcal{L}}$, we denote the set of lines not in $\mathcal{L}$.

A point on i lines of $\mathcal{L}$ is called an i-point, and a plane with i lines in $\mathcal{L}$ is called an i-plane.

$$\overset{(1)}{\begin{pmatrix}0&0&3&3&3&3\\0&0&3&3&3&3\\0&0&3&3&3&3\\0&0&3&3&3&3\\1&1&4&4&4&4\\1&1&4&4&4&4\end{pmatrix}}\quad\overset{(2)}{\begin{pmatrix}0&0&0&2&2&2\\0&0&0&2&2&2\\1&1&1&3&3&3\\2&2&2&4&4&4\\2&2&2&4&4&4\\3&3&3&5&5&5\end{pmatrix}}\quad\overset{(3)}{\begin{pmatrix}0&0&1&1&2&2\\0&0&1&1&2&2\\1&1&2&2&3&3\\1&1&2&2&3&3\\3&3&4&4&5&5\\3&3&4&4&5&5\end{pmatrix}}\quad\overset{(4)}{\begin{pmatrix}0&0&0&0&0&0\\1&1&1&1&1&1\\2&2&2&2&2&2\\3&3&3&3&3&3\\4&4&4&4&4&4\\4&4&4&4&4&4\end{pmatrix}}\quad\overset{(5)}{\begin{pmatrix}0&1&1&1&1&2\\0&1&1&1&1&2\\0&1&1&1&1&2\\2&3&3&3&3&4\\3&4&4&4&4&5\\3&4&4&4&4&5\end{pmatrix}}$$

$$\overset{(6)}{\begin{pmatrix}0&0&0&0&0&0\\2&2&2&2&2&2\\2&2&2&2&2&2\\2&2&2&2&2&2\\3&3&3&3&3&3\\5&5&5&5&5&5\end{pmatrix}}\quad\overset{(7)}{\begin{pmatrix}1&1&1&1&1&1\\1&1&1&1&1&1\\1&1&1&1&1&1\\3&3&3&3&3&3\\3&3&3&3&3&3\\5&5&5&5&5&5\end{pmatrix}}\quad\overset{(8)}{\begin{pmatrix}1&1&1&1&4&4\\1&1&1&1&4&4\\1&1&1&1&4&4\\1&1&1&1&4&4\\2&2&2&2&5&5\\2&2&2&2&5&5\end{pmatrix}}\quad\overset{(9)}{\begin{pmatrix}0&1&1&3&3&4\\0&1&1&3&3&4\\0&1&1&3&3&4\\0&1&1&3&3&4\\1&2&2&4&4&5\\1&2&2&4&4&5\end{pmatrix}}\quad\overset{(10)}{\begin{pmatrix}0&0&0&1&2&3\\0&0&0&1&2&3\\2&2&2&3&4&5\\2&2&2&3&4&5\\2&2&2&3&4&5\\2&2&2&3&4&5\end{pmatrix}}$$

Table 4: Patterns for lines of $\mathcal{L}$ in the case $x = 10$

Lemma 5.2. *A line from $\mathcal{L}$ has one of the patterns* (1) – (10) *listed in Table* 4*, and a line from $\overline{\mathcal{L}}$ has one of the patterns* (11) – (16) *listed in Table* 5*.*

Proof. As in the previous section, the lemma is proved with an exhaustive enumeration of all 6×6-matrices admissible by Proposition 2.3. □

Lemma 5.3. *Suppose that π is a 25-plane. Then there exists a conic C in π such that the 15 secant lines of C have pattern* (3)*, and the 10 lines of π missing C have pattern* (2)*. Moreover, the six tangent lines of C are the lines of $\overline{\mathcal{L}}$ of π and these have pattern* (13)*.*

Proof. An inspection of Table 4 and Table 5 shows that every line of $\mathcal{L}$ of π has pattern (2)-(5), while lines of $\overline{\mathcal{L}}$ of π have pattern (13). Looking at the entries of the rows of these patterns that correspond to 25-planes, we see that every point of π lies on at least four lines of $\mathcal{L}$. Thus, each point of π lies inside π on at most two of the six lines of π that are in $\overline{\mathcal{L}}$, that is these six lines form a dual arc of π. The famous theorem of Segre [19] implies that these are the six tangent lines of a conic C of π. They have pattern (13).

A line of π missing C has three points that lie on no tangent of C and three points that are on two tangents of C. Hence, the points of such a line lie inside π in $4, 4, 4, 6, 6, 6$ lines of $\mathcal{L}$. Inspection of the patterns (2)-(5) shows that such a line must have pattern (2), the corresponding row in the pattern is $3, 3, 3, 5, 5, 5$.

Similarly, a secant line to C has points that lie in π on $4, 4, 5, 5, 6, 6$ lines of $\mathcal{L}$, corresponding to a row $3, 3, 4, 4, 5, 5$, so these lines have pattern (3). □

Lemma 5.4. *Patterns* (4) – (10) *and* (14) – (16) *can not be realized.*

$$
\begin{array}{ccc}
(11) & (12) & (13) \\
\begin{pmatrix} 0&0&1&1&2&3\\ 0&0&1&1&2&3\\ 0&0&1&1&2&3\\ 1&1&2&2&3&4\\ 1&1&2&2&3&4\\ 1&1&2&2&3&4 \end{pmatrix} &
\begin{pmatrix} 0&1&1&1&1&3\\ 0&1&1&1&1&3\\ 0&1&1&1&1&3\\ 0&1&1&1&1&3\\ 1&2&2&2&2&4\\ 2&3&3&3&3&5 \end{pmatrix} &
\begin{pmatrix} 1&1&1&1&1&2\\ 1&1&1&1&1&2\\ 1&1&1&1&1&2\\ 1&1&1&1&1&2\\ 1&1&1&1&1&2\\ 4&4&4&4&4&5 \end{pmatrix} \\
(14) & (15) & (16) \\
\begin{pmatrix} 0&0&1&2&2&2\\ 0&0&1&2&2&2\\ 0&0&1&2&2&2\\ 0&0&1&2&2&2\\ 1&1&2&3&3&3\\ 2&2&3&4&4&4 \end{pmatrix} &
\begin{pmatrix} 0&0&0&0&0&1\\ 1&1&1&1&1&2\\ 1&1&1&1&1&2\\ 1&1&1&1&1&2\\ 3&3&3&3&3&4\\ 3&3&3&3&3&4 \end{pmatrix} &
\begin{pmatrix} 0&0&0&0&0&1\\ 0&0&0&0&0&1\\ 2&2&2&2&2&3\\ 2&2&2&2&2&3\\ 2&2&2&2&2&3\\ 3&3&3&3&3&4 \end{pmatrix}
\end{array}
$$

Table 5: Patterns for lines of $\overline{\mathcal{L}}$ in the case $x = 10$

Proof. A line with pattern (8), (9) or (10) requires a 27-plane, as each of these patterns have a row with row sum 26. However, a 27-plane also has lines in $\overline{\mathcal{L}}$, but no line of $\overline{\mathcal{L}}$ has a pattern that requires a 27-plane, since there is no row of patterns (11)-(16) with row sum 27. Hence patterns (8)-(10) do not occur.

A line with pattern (4) or (5) requires a 25-plane, but we have seen in the previous lemma that a 25-plane does not have lines with these patterns, so they also cannot occur.

Assume that there exists a line ℓ with pattern (6) or (7). Then ℓ lies in a 19-plane corresponding to a row $3, 3, 3, 3, 3, 3$ in the pattern of ℓ. Hence every point of ℓ lies in π on four lines of $\mathcal{L}$. This implies that every line of π has a point that lies in π on exactly four lines of $\mathcal{L}$. Inspection of the patterns in Table 4 shows that every line of $\mathcal{L}$ of π has pattern (1), (2), (6), and (7). However patterns (1) and (2) have no entry 3 in a row corresponding to a 19-plane, so every line of π that is in $\mathcal{L}$ has pattern (6) or (7). This gives 19 lines of π, and each point of one of them must be on exactly four of them. Thus these 19 lines cover c points where $4c = 19 \times 6$, that is $c = 57/2$, a contradiction.

Hence lines with pattern (6) or (7) do not exist. Thus, if there is a plane π with 19 lines in $\mathcal{L}$, then these 19 lines have pattern (1) or (2) and thus no point of π lies in π on exactly four lines of $\mathcal{L}$. This implies that no line l has pattern (14)-(16). □

We now know that the lines of $\mathcal{L}$ have pattern (1), (2) or (3) and those of $\overline{\mathcal{L}}$ pattern (11), (12) or (13). Inspection of these patterns show that every point lies on 3, 9, 15 or 21 lines of $\mathcal{L}$, while planes have 7, 13, 19, or 25 points in $\mathcal{L}$. Let n_i be the number of i-points and m_j the number of j-planes for the four possible values for i and j.

Lemma 5.5. (a) *The set* $\mathcal{L}$ *contains exactly* 30 *lines with pattern* (1)*,* 160 *lines with pattern* (2)*, and* 120 *lines with pattern* (3)*.*

(b) $(n_3, n_9, n_{15}, n_{21}) = (20, 80, 16, 40)$.

(c) $(m_7, m_{13}, m_{19}, m_{25}) = (80, 40, 20, 16)$.

Proof. Assume that there does not exist a 25-plane. Then patterns (2), (3) and (13) can not occur. Hence, every line of $\mathcal{L}$ has pattern (1). Since every plane is incident with a line of $\mathcal{L}$, this implies that all planes are 13-planes or 19-planes. But each of the patterns (11), (12) and (13) of the lines of $\overline{\mathcal{L}}$ requires a plane with less than 13 lines in $\mathcal{L}$, a contradiction.

Hence there exists a 25-plane π. As the pattern of a line ℓ of π determines the number of lines of $\mathcal{L}$ in each plane on ℓ, the known pattern together with the information of Lemma 5.3 on π proves (c). As each line with pattern (2) lies in one 25-plane, then Lemma 5.3 also shows that there are $m_{25} \cdot 10 = 160$ lines with pattern (2). Similarly, lines with pattern (3) lie in two 25-planes, so there are $m_{25} \cdot 15/2 = 120$ lines with pattern (3), so the remaining 30 lines of $\mathcal{L}$ have pattern (1). As each pattern of a line of $\mathcal{L}$ determines the number of i-points on the line for all i, we see that the numbers in (b) can be calculated. For example, pattern (1) requires four 21-points, pattern (2) requires three 21-points, and pattern (3) requires two 21-points. Thus (a) gives $n_{21}21 = 30 \cdot 4 + 160 \cdot 3 + 120 \cdot 2$ giving $n_{21} = 40$. □

Lemma 5.6. *The set* K *of* 3*-points is a complete* 20*-cap* K*. It is projectively equivalent to the cap* K_1 *used in the above construction.*

Proof. We have $|K| = n_3 = 20$. An inspection of the patterns shows that no line has more than two 3-points, so K is a 20-cap. Lemma 5.3 shows that 25-planes only have lines with pattern (2), (3) or (13), an inspection of these pattern show that such a line does not have a 3-point. Hence, the sixteen 25-planes miss the cap. It follows that the cap K is not contained in an elliptic quadric as it then could not miss more than 7 planes. Then the information on caps given in the beginning of the section shows that K is projectively equivalent to the cap K_1. □

Lemma 5.7. (a) *The planes missing* K *are the* 25*-planes.*

(b) *The planes meeting* K *in exactly three points are the* 19*-planes.*

Proof. (a) As K is equivalent to K_1, it misses exactly 16 planes. We have seen in the previous lemma that these are the sixteen 25-planes.

(b) From the patterns we distract the following information. A line of $\overline{\mathcal{L}}$ in a 19-plane π has pattern (12), exactly one of its points is a 3-point and this point lies on exactly two lines of π that are in $\mathcal{L}$ (see the last row of pattern (12)). As a 3-point of π necessarily lies on a line of π that is in $\overline{\mathcal{L}}$ and since π contains 12 lines of $\overline{\mathcal{L}}$, then the number of 3-points of π is $12 \cdot 1/4 = 3$. It follows from [1] that there are exactly 20 planes, each of which contains only 3 points of K (of course this also can be deduced from the pattern), so this proves the second assertion. □

We are now in position to finish the proof of Theorem 5.1. The previous lemma shows that the cap K uniquely determines the 25-planes and the 19-planes. From patterns of the lines we see the following. The lines with pattern (3) are the lines that lie in two 25-planes, the lines with pattern (2) are the lines that lie in one 25-plane and two 19-planes, and the lines with pattern (1) are the secants to K that lie in two 19-planes. This shows that $\mathcal{L}$ is obtained from K as in the above construction.

Acknowledgements. Part of this work was done while the first author was visiting Tohoku University as a JSPS Postdoctoral Fellow. The first author is also supported by the Grant of the President of Russian Federation for young scientists (pr. MK-1719.2013.1) and the RFBR grant (pr. 12-01-31098).

References

[1] Vito Abatangelo, Gabor Korchmaros, and Bambina Larato. Classification of maximal caps in $\mathrm{PG}(3, 5)$ different from elliptic quadrics. *J. Geom.*, 57(1-2):9–19, 1996.

[2] John Bamberg, Maska Law, Tim Penttila. Tight sets and m-ovoids of generalised quadrangles. *Combinatorica*, 29(1):1–17, 2009.

[3] A. A. Bruen and Keldon Drudge. The construction of Cameron-Liebler line classes in $\mathrm{PG}(3, q)$. *Finite Fields Appl.*, 5(1):35–45, 1999.

[4] P. J. Cameron and R. A. Liebler. Tactical decompositions and orbits of projective groups. *Linear Algebra Appl.*, 46:91–102, 1982.

[5] E. van Dam, J.H. Koolen, H. Tanaka. Distance-regular graphs. *Preprint*, May 2014 version.

[6] J. De Beule, A. Hallez, and L. Storme. A non-existence result on Cameron-Liebler line classes. *J. Combin. Des.*, 16(4):342–349, 2008.

[7] Keldon Drudge. Extremal sets in projective and polar spaces. *Ph.D. Thesis*, University of Western Ontario, 1998.

[8] Keldon Drudge. On a conjecture of Cameron and Liebler. *European J. Combin.*, 20(4):263–269, 1999.

[9] Alexander L. Gavrilyuk and Ivan Yu. Mogilnykh. Cameron-Liebler line classes in $\mathrm{PG}(n, 4)$. *Des. Codes Cryptogr.*, DOI 10.1007/s10623-013-9838-z.

[10] Patrick Govaerts and Tim Penttila. Cameron-Liebler line classes in $\mathrm{PG}(3, 4)$. *Bull. Belg. Math. Soc. Simon Stevin*, 12(5):793–804, 2005.

[11] Patrick Govaerts and Leo Storme. On Cameron-Liebler line classes. *Adv. Geom.*, 4(3):279–286, 2004.

[12] J. W. P. Hirschfeld. *Finite projective spaces of three dimensions.* Oxford Mathematical Monographs. The Clarendon Press Oxford University Press, New York, 1985. Oxford Science Publications.

[13] J. W. P. Hirschfeld. *Projective geometries over finite fields.* Oxford Mathematical Monographs. The Clarendon Press Oxford University Press, New York, second edition, 1998.

[14] Klaus Metsch. The non-existence of Cameron-Liebler line classes with parameter $2 < x \leqslant q$. *Bull. Lond. Math. Soc.*, 42(6):991–996, 2010.

[15] Klaus Metsch. An improved bound on the existence of Cameron–Liebler line classes. *J. Combin. Theory Ser. A*, 121:89–93, 2014.

[16] Tim Penttila. Cameron-Liebler line classes in $\mathrm{PG}(3, q)$. *Geom. Dedicata*, 37(3):245–252, 1991.

[17] Morgan J. Rodgers. On some new examples of Cameron-Liebler line classes. *Ph.D. Thesis*, University of Colorado, 2012.

[18] Morgan Rodgers. Cameron-Liebler line classes. *Des. Codes Cryptogr.*, 68(1-3):33–37, 2013.

[19] Beniamino Segre. Ovals in a finite projective plane. *Canad. J. Math.*, 7:414–416, 1955.