Universität des Saarlandes

Fachrichtung 6.1 – Mathematik

Preprint Nr. 330

Point configurations on the projective line over a finite field

Ernst-Ulrich Gekeler

Saarbrücken 2013

Fachrichtung 6.1 – Mathematik
Universität des Saarlandes

Preprint No. 330
submitted: April 2, 2013

Point configurations on the projective line over a finite field

Ernst-Ulrich Gekeler

Saarland University
Department of Mathematics
Campus E2 4
66123 Saarbrücken
Germany
gekeler@math.uni-sb.de

Edited by
FR 6.1 – Mathematik
Universität des Saarlandes
Postfach 15 11 50
66041 Saarbrücken
Germany

Fax: + 49 681 302 4443
e-Mail: preprint@math.uni-sb.de
WWW: http://www.math.uni-sb.de/

1

POINT CONFIGURATIONS ON THE PROJECTIVE LINE OVER A FINITE FIELD

ERNST-ULRICH GEKELER

Abstract. We study n-point configurations in $\mathbb{P}^1(\mathbb{F}_q)$ modulo projective equivalence. For $n = 4$ and 5, a complete classification is given, along with the numbers of such configurations with a given symmetry group. Using Polya's coloring theorem, we investigate the behavior of the numbers $C(n, q)$ of classes of n-configurations resp. $C^{\mathrm{spec}}(n, q)$ of classes with nontrivial symmetry group. Both are described by rational polynomials in q which depend on q modulo $\lambda(n) = \mathrm{lcm}\{m \in \mathbb{N} \mid m \leq n\}$.

MSC 2010: 05A15, 14N10, 11T99

0. Introduction.

Let $K = \mathbb{F}_q$ be a finite field with q elements, of characteristic p. An *n-point configuration* (or briefly n-configuration) on the projective line $\mathbb{P}^1(K)$ is an n-element subset C of $\mathbb{P}^1(K)$. We are interested in the classification on n-configurations up to projective equivalence, that is, up to the action of the group $G := \mathrm{GL}(2, K)$ on $\mathbb{P}^1(K)$ through fractional linear transformations $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)(z) = \frac{az+b}{cz+d}$. Note that G operates through its quotient group $\overline{G} := \mathrm{PGL}(2, K)$, whose action is faithful.

Given an n-configuration C, its symmetry group is

$$\mathrm{Aut}(C) := \{\overline{\sigma} \in \overline{G} \mid \overline{\sigma}(C) = C\}.$$

Typical questions are:

(1) Given n and q, which subgroups A of the symmetric group S_n occur as symmetry groups of n-configuarations?
(2) Determine the number of configurations with fixed symmetry group A, and
(3) the number $C(n, q)$ of classes of n-configuarations up to the action of G!
(4) Describe the asymptotic behavior of $C(n, q)$ for n or q tending to infinity!

These arise from intrinsic combinatorial interest, but are also related to various problems in algebraic geometry, for example the description of

[1]Ernst-Ulrich Gekeler, FR 6.1 Mathematik, Campus E2 4,
Universität des Saarlandes, D-66123 Saarbrücken, gekeler@math.uni-sb.de
Tel.:+49 (0) 681 302 2494, Fax: +49 (0) 681 302 3973

algebraic curves covering $\mathbb{P}^1$ with specified ramification (see, e.g. [6] Ch. IV), or the classification of elliptic surfaces over K or over its algebraic closure ([3] part 2, [4]). Of course, these questions are well-established topics of classical invariant theory, where one considers configurations of points, lines, ... in projective spaces over the complex numbers. Here one usually studies quotients of quasi-projective varieties by algebraic groups: see [8] and its references.

Our approach is more modest, but also more concrete. As $\overline{G}$ acts sharply 3-transitive on $\mathbb{P}^1$, our questions are trivial for $n \leq 3$. Similarly, the case $n = 4$ is rather simple; it is related to the fact that ordered 4-configurations are classified through their cross-ratio [5]. The result, i.e., the answer to questions (1), (2), (3) for $n = 4$, is given in Theorem 3.11. Although it is certainly known to many people, and is for example mentioned in [4] 10.1, we present it here in detail since we heavily use it in the sequel.

Our focus is on the case of 5-configurations, which is remarkably complex. We succeed in solving questions (1), (2), (3): See Theorem 4.31. The possible symmetry groups are the alternating group A_5, the affine group $\mathrm{Aff}(\mathbb{F}_5)$ of order 20 over $\mathbb{F}_5$, the dihedral group D_5 of order 10, the symmetric group S_3, the two groups of order 4, the group of order 2, and the trivial group, depending on the characteristic. The main difficulty is the counting of configurations C with $|\mathrm{Aut}(C)| = 2$ in characteristic $p \neq 2$; it is overcome by counting pairs (C, ι) of configurations C equipped with an involution ι, which relates C with a 4-configuration.

Determining the number $C(n, q)$ may be regarded as a coloring problem (coloring the n distinguished points among the $q+1$ points of $\mathbb{P}^1(K)$), and so Polya's coloring theorem (see [1] Ch. 6) applies.

We briefly recall Polya's theorem in Section 1, in a form suitable for our purposes. In Section 2 we calculate the cycle index $Z_{G,\mathbb{P}^1(K)}$ for the action of G on $\mathbb{P}^1(K)$, a polynomial with rational coefficients in variables $X_1, X_2, \ldots, X_{q+1}$. It is described in Theorem 2.9. Questions (1), (2), (3) for $n \geq 5$ are dealt with in Sections 3 and 4.

The results: Theorem 3.11 and 4.31 are independent of Polya's theorem and give better insight, as the Polya theorem fails to provide information about symmetries of configurations. In Section 5, through evaluating the cycle index, we describe $C(n, q)$ and its behavior for $q \to \infty$, for fixed $n \geq 5$. The result is Theorem 5.13; it states that there are polynomials $f_n(X)$, $g_{n,\overline{q}}(X) \in \mathbb{Q}[X]$, where $\overline{q}$ is the residue class of q modulo $\lambda(n) = \mathrm{lcm}\{m \in \mathbb{N} \mid m \leq n\}$, such that

$$C(n, q) = f_n(q) + g_{n,\overline{q}}(q).$$

The degrees and leading coefficients are given by $\deg(f_n) = n-3$, $\mathrm{lcoeff}(f_n) = \frac{1}{n!}$, $\deg(g_{n,\bar{q}}) = \nu - 1$, $\mathrm{lcoeff}(g_{n,\bar{q}}) = \frac{1}{2^\nu \nu!}$ with $\nu = [\frac{n}{2}]$. Furthermore, $g_{n,\bar{q}}(q)$ describes the order of magnitude of the number $C^{\mathrm{spec}}(n,q)$ of classes of special configurations C (those with symmetry groups $\mathrm{Aut}(C) \neq \{1\}$). Therefore, as $\deg(g_{n,\bar{q}}) < \deg(f_n)$ for $n \geq 5$, "most" configurations are generic, that is, have no symmetries (Corollary 5.18).

Throughout, we use the following

Notation.

$\mathbb{N} = \{1,2,3,\ldots\}$, $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$,
$a|b$ denotes divisibility of b by a, $|X|$ is the cardinality of the finite set X,
$\varphi:\ \mathbb{N} \to \mathbb{N}$ is Euler's function: $\varphi(1) = 1$, $\varphi(n) = |\mathbb{Z}/n)^*|$ for $n > 1$,
$[x]$ = largest integer not exceeding $x \in \mathbb{R}$.
If the group G acts (from the left) on the set X, we write $G \setminus X$ for the orbit space.

Some groups we are dealing with are

- S_n, A_n the symmetric and alternating groups on n letters;
- D_n, the dihedral group with $2n$ elements;
- μ_n, the group of n-th roots of unity, regarded as a subgroup of the multiplicative group of a field K, e.g., $K = \mathbb{F}_q$;
- $\mathrm{Aff}(K)$, the affine group of the field K, which is the group of transformations $z \longmapsto az+b$ ($a,b \in K$, $a \neq 0$). It is isomorphic with the subgroup of matrices $\binom{a\,b}{0\,1}$ of $\mathrm{GL}(2,K)$.

Finally, ρ_n denotes a primitive n-th root of unity. More specifically, $\rho := \rho_3$ and $\tau := \rho_6 = -\rho_3$ are primitive 3^{rd} and 6^{th} roots of unity.

1. Polya's theorem.

For the reader's convenience, we present Polya's theorem about the cycle index, in a version suitable for our purposes. More details and proofs may be found in [1] Ch. 6; see also Polya's original paper [9].

Let G be a finite group that acts on the finite set $\mathfrak{X}$ with N elements.

1.1 Definition

(i) *For $\sigma \in G$, let $\underline{c}(\sigma) = (c_1(\sigma), \ldots, c_N(\sigma))$ be the* cycle type *of σ on $\mathfrak{X}$, i.e.,*

$$c_i(\sigma) \ := \ \textit{number of } i\textit{-cycles of the permutation of } \mathfrak{X} \textit{ induced by } \sigma,\ i = 1,2,\ldots,N.$$

(ii) *For each i, let X_i be an indeterminate. The polynomial*

$$Z_{G,\mathfrak{X}}(X_1,\ldots,X_N) := \frac{1}{|G|}\sum_{\sigma\in G} X_1^{c_1(\sigma)}\cdots X_N^{c_N(\sigma)} \in \frac{1}{|G|}\mathbb{Z}[X_1,\ldots,X_N]$$

is called the cycle index *of G on $\mathfrak{X}$.*

1.2 Remarks. (i) As $\underline{c}(\sigma)$ depends only on the conjugacy class of σ, we usually write

$$Z_{G,\mathfrak{X}} = \frac{1}{|G|}\sum_{\sigma\in S} \ell(\sigma) X_1^{c_1(\sigma)}\cdots X_N^{c_N(\sigma)},$$

where S is a set of representatives for the conjugacy classes of G and $\ell(\sigma)$ the length of the class determined by σ.
(ii) If X_i is endowed with the weight i, $Z_{G,\mathfrak{X}}$ is isobaric of weight N in the X_i.
(iii) Some X_i appears in $Z_{G,\mathfrak{X}}$ if and only if i is a cycle length of some $\sigma \in G$.
(iv) In the description above of the cycle type $\underline{c}(\sigma)$, we have $\sum_i ic_i(\sigma) = N$. Alternatively, we may describe it as

$$\underline{c}(\sigma) = (\underbrace{1,1,\ldots,1}_{c_1(\sigma)},\underbrace{2,\ldots,2}_{c_2(\sigma)},\ldots),$$

in which case the entries sum up to N. We use both formats, where the meaning will always be clear from the context.

1.3 Definition

(i) *An* r-coloring *of $\mathfrak{X}$ is a map γ from $\mathfrak{X}$ to $\{1,2,\ldots,r\}$. We put* $\mathrm{Col}(r,\mathfrak{X})$ *for the set of all r-colorings.*
(ii) *The* color scheme *of γ is $\underline{d}(\gamma) = (d_1(\gamma),\ldots,d_r(\gamma))$, where $d_j(\mathfrak{p})$ is "the number of points of $\mathfrak{X}$ with color j", i.e., $d_j(\gamma) = |\gamma^{-1}(j)|$. For each color scheme $\underline{d} = (d_1,\ldots,d_r)$, where $\sum d_j = N$, let* $\mathrm{Col}(r,\underline{d},\mathfrak{X})$ *denote the set of r-colorings with scheme $\underline{d}$.*

The group G also acts on $\mathrm{Col}(r,\mathfrak{X})$ and on the $\mathrm{Col}(r,\underline{d},\mathfrak{X})$. We are interested in the number of G-inequivalent r-colorings (perhaps with a fixed color scheme) of $\mathfrak{X}$, i.e., the number of G-orbits on $\mathrm{Col}(r,\mathfrak{X})$ resp. $\mathrm{Col}(r,\underline{d},\mathfrak{X})$. The answer is provided by the following result of Polya.

1.4 Theorem.

(i) *The number of G-inequivalent r-colorings is given by $Z_{G,\mathfrak{X}}(r,\ldots,r)$.*
(ii) *The number of G-inequivalent r-colorings with color scheme $\underline{d}$ is obtained as follows. For each j $(1 \le j \le r)$ let Y_j be an indeterminate, and let*

$$P_K(\underline{Y}) = P_K(Y_1,\ldots,Y_r) := \sum_{1\le j\le r} Y_j^k$$

be the k-th power sum of the Y_j. Expand the polynomial

$$Z_{G,\mathfrak{X}}(P_1(\underline{Y}),\dots,P_N(\underline{Y})) = \sum_{\underline{d}\in\mathbb{N}_0^r} a(\underline{d})\underline{Y}^{\underline{d}},$$

where $\underline{d}=(d_1,\dots,d_r)$ satisfies $\sum d_j = N$, $\underline{Y}^{\underline{d}} = y_1^{d_1}\cdots y_r^{d_r}$, and $a(\underline{d})\in\mathbb{Q}$. Then

$$a(\underline{d}) = |G\setminus \mathrm{Col}(r,\underline{d},\mathfrak{X})|,$$

i.e., the number of G-inequivalent r-colorings of scheme $\underline{d}$.

2. The cycle index of $\mathrm{GL}(2,\mathbb{F}_q)$ on $\mathbb{P}^1(\mathbb{F}_q)$.

In what follows, K always denotes the finite field $\mathbb{F}_q$ with q elements, and G is the group $\mathrm{GL}(2,K)$, which acts as usual through fractional linear transformations on $\mathfrak{X} := \mathbb{P}^1(K) = K\cup\{\infty\}$. We determine the cycle index $Z_{G,\mathfrak{X}}$. We also let $\overline{G} := \mathrm{PGL}(2,K)$, the factor group of G through which it acts effectively on $\mathfrak{X}$, and $\sigma \longmapsto \overline{\sigma}$ is the canonical map from G to $\overline{G}$.

First, we need a description of the conjugacy classes of G. This is well-known and comes out by considering the possible characteristic polynomials.

2.1 Proposition.

(i) *Each element of G is conjugate to exactly one of the following matrices:*

$$\mathrm{I}_a = \begin{pmatrix} a & 0 \\ 0 & a\end{pmatrix};\ \mathrm{II}_a = \begin{pmatrix} a & 1 \\ 0 & a\end{pmatrix};\ \mathrm{III}_{a,b} = \begin{pmatrix} a & 0 \\ 0 & b\end{pmatrix};\ \mathrm{IV}_{a.b} = \begin{pmatrix} 0 & -b \\ 1 & -a\end{pmatrix}.$$

Here, a runs through $K^* = K\setminus\{0\}$ in types I *or* II*, (a,b) runs through the set of ordered pairs of distinct elements of K^* in* III*, where one of (a,b), (b,a) is selected, and X^2+aX+b runs through the set of irreducible monic quadratic K-polynomials in* IV.

(ii) *The numbers of such conjugacy classes are $q-1$, $q-1$, $(q-1)(q-2)/2$, $q(q-1)/2$, respectively, in cases* I, II, III, IV.

(iii) *The sizes of the conjugacy classes of types* I, …, IV *are 1, q^2-1, q^2+q, q^2-q, respectively.*

Next, we determine the cycle types of $\sigma\in G$ on $\mathbb{P}^1(K)$. It suffices to consider the matrices described in Proposition 2.1.

(2.2) As the matrices of type I act trivially, the cycle type is $(1,1,\dots,1)$.

(2.3) The matrix II_a fixes $\infty = (1:0)$ and acts as shift $a\longmapsto Z+a^{-1}$ on

$K \hookrightarrow \mathbb{P}^1(K)$. Hence the cycle type is $(1, \underbrace{p, \ldots, p}_{q/p})$, where $p = \mathrm{char}(K)$.

(2.4) Given the matrix $\sigma = \mathrm{III}_{a,b}$, let m be the order of a/b in K^*. Then $2 \leq m|(q-1)$, σ fixes 0 and ∞, and acts without fixed points on $K^* \hookrightarrow \mathbb{P}^1(K)$. Therefore the cycle type is $(1, 1, \underbrace{m, \ldots, m}_{(q-1)/m})$.

(2.5) Let L be the quadratic extension of K and $\alpha \in L \setminus K$ with minimal polynomial $X^2 + aX + b$. The choice of the K-basis $\{1, \alpha\}$ for L yields an embedding $L^* \hookrightarrow G$, in which α corresponds to the matrix $\mathrm{IV}_{a,b}$. Further, multiplication by α on $\underset{u+v\alpha}{L^*/K^*} \underset{\longmapsto}{\xrightarrow{\cong}} \underset{(u:v)}{\mathbb{P}^1(K)}$ corresponds to the action of $\mathrm{IV}_{a,b}$ on $\mathbb{P}^1(K)$. Therefore, if m denotes the order of the residue class $\overline{\alpha}$ of α in L^*/K^*, the cycle type of $\mathrm{IV}_{a,b}$ on $\mathbb{P}^1(K)$ is $(\underbrace{m, m, \ldots, m}_{(q+1)/m})$.

(2.6) Let m be a divisor $q-1$. The number of elements of precise order m in the cyclic group K^* of order $q-1$ is $\varphi(m)$ with Euler's function φ. Hence there are

$$\frac{1}{2} \sum_{\substack{c \in K^* \\ \mathrm{ord}(c) = m}} |\{(a,b) \in (K^*)^2 | ab^{-1} = c\}| = \frac{1}{2}\varphi(m)(q-1)$$

matrices $\mathrm{III}_{a,b}$ of order m in $\overline{G}$.

2.7 Lemma. *Let ω be the mapping from the set of monic irreducible quadratic polynomials over K to $\{m \in \mathbb{N} \mid 2 \leq m|(q+1)\}$ which to each f associates the order of a zero $\alpha \in L$ of f in the multiplicative group L^*/K^*. Then ω is onto and $|\omega^{-1}(m)| = \frac{1}{2}\varphi(m)(q-1)$.*

Proof. The canonical map $L^* \longrightarrow L^*/K^*$ is surjective with kernel of order $q-1$. As L^*/K^* is cyclic, there are $\varphi(m)(q-1)$ elements α of L^* with order m in L^*/K^*, grouped in $\frac{1}{2}\varphi(m)(q-1)$ pairs with the same minimal polynomial, provided that $m \geq 2$. □

The orders of G and $\overline{G}$ are given by

$$(2.8) \qquad |G| = q(q-1)(q^2-1), \; |\overline{G}| = q(q-1)(q+1).$$

Plugging in the data obtained in (2.1)–(2.8), we find the following expression for the cycle index $Z_{G,\mathfrak{X}}(X_1, \ldots, X_{q+1})$, where $G = \mathrm{GL}(2, K)$, $\mathfrak{X} = \mathbb{P}^1(K)$.

2.9 Theorem.

$$Z_{G,\mathfrak{X}}(X_1,\dots,X_{q+1}) = \frac{1}{|\overline{G}|}X_1^{q+1} + \frac{1}{q}X_1X_p^{q/p} +$$
$$\frac{1}{2(q-1)}\sum_{2\le m|(q-1)}\varphi(m)X_1^2X_m^{(q-1)/m} + \frac{1}{2(q+1)}\sum_{2\le m|(q+1)}\varphi(m)X_m^{(q-1)/m}$$

Here the four terms correspond to the conjugacy classes of G of types I, II, III, IV*, respectively.*

3. n-point configurations: the cases $n \le 4$.

An *n-point configuration* on $\mathfrak{X} = \mathbb{P}^1(K)$ is an n-point subset of $\mathfrak{X}$. We regard it as a 2-coloring of $\mathfrak{X}$ of color scheme $(n, q+1-n)$, and we always tacitly assume that $n \le q+1$. The set $\mathrm{Col}(2,(n,q+1-n),\mathfrak{X})$ of all n-point configurations will be denoted by $\mathcal{C}(n,\mathfrak{X})$. According to Polya's theorem, we get the number

$$C(n,q) := |G \setminus \mathcal{C}(n,\mathfrak{X})| \tag{3.1}$$

of G-inequivalent n-configurations as the coefficient of $Y_1^nY_2^{q+1-n}$ in $Z_{G,\mathfrak{X}}(Y_1+Y_2, Y_1^2+Y_2^2,\dots,Y_1^{q+1}+Y_2^{q+1})$. This is on the one hand quite explicit and satisfactory; on the other hand it fails to provide insight into the geometric nature of such configurations.

Given $C \in \mathcal{C}(n,\mathfrak{X})$, we let

$$\mathrm{Aut}(C) := \{\sigma \in \overline{G} \mid \sigma(C) = C\} \tag{3.2}$$

be its symmetry group. In the present and the next section, we give - without using the Polya theorem - a direct classification of n-point configurations for $n \le 5$ with respect to their symmetry groups.

The case of $n \le 3$ is completely settled by the following well-known fact.

3.3 Proposition. *Let (x_1,x_2,x_3) and (y_1,y_2,y_3) be triples of pairwise different elements of $\mathfrak{X} = \mathbb{P}^1(K)$. There exists a unique element σ of $\overline{G} = \mathrm{PGL}(2,K)$ such that $\sigma(x_i) = y_i$ $(1 \le i \le 3)$.*

Hence $C(n,q) = 1$ for $n \le 3$, i.e., all n-point configurations are G-equivalent if $n \le 3$.

Let $W \subset \overline{G}$ be the stabilizer of the 3-configuration $\{0,1,\infty\} \subset \mathfrak{X}$. According to (3.3), it is isomorphic with the symmetric group S_3, and is represented by the matrices (by abuse of notation, we use the equality sign):

(3.4)

$$W = \left\{ \begin{pmatrix}1&0\\0&1\end{pmatrix}, \begin{pmatrix}0&1\\1&0\end{pmatrix}, \begin{pmatrix}-1&1\\0&1\end{pmatrix}, \begin{pmatrix}-1&0\\-1&1\end{pmatrix}, \begin{pmatrix}0&1\\-1&1\end{pmatrix}, \begin{pmatrix}-1&1\\-1&0\end{pmatrix} \right\}.$$

Note that the present description makes sense in any characteristic. Let now $\{a, b, c, d\}$ be any 4-configuration. Again by (3.3) it is G-equivalent with $\{0, 1, \infty, z\}$, for some $z \in \mathbb{P}^1(K) \setminus \{0, 1, \infty\} =: P$. We note in passing that, depending on a convenient ordering of $\{a, b, c, d\}$, the quantity z equals the classical cross-ratio of (a, b, c, d), see [5] p. 7. Changing the ordering of $\{0, 1, \infty\}$ replaces z by some W-equivalent element z' of P. Thereby, the set of G-classes of 4-point configurations is in canonical bijection

$$G \setminus \mathcal{C}(4, \mathfrak{X}) \xrightarrow{\cong} W \setminus P \tag{3.5}$$

with the orbit space of P under W.

The W-orbit of $z \in P$ is $\{z, z^{-1}, 1-z, \frac{z}{z-1}, \frac{1}{1-z}, \frac{z-1}{z}\}$, usually of order 6, with the following easily verified exceptions.

(3.6) Suppose that $p \neq 2, 3$. Then $\{2, \frac{1}{2}, -1\}$ is a W-orbit of length 3.

(3.7) Suppose that $p \neq 2, 3$ and $q \equiv 1 \pmod 3$ (then in fact $q \equiv 1 \pmod 6$), and let $\tau = \rho_6$ be a primitive 6-th root of unity in $K = \mathbb{F}_q$. Then $\{\tau, \tau^{-1}\}$ is a W-orbit of length 2.

(3.8) Suppose that $p = 3$. Then $\{2\}$ is a W-orbit of length 1.

(3.9) Suppose that $p = 2$ and $q \equiv 1 \pmod 3$ (i.e., q is an even power of 2), and let $\rho = \rho_3$ be a primitive 3^{rd} root of unity in K. Then $\{\rho, \rho^{-1}\}$ is a W-orbit of length 2.

3.10 Proposition. *Let a, b, c, d be four distinct points of $\mathfrak{X}$. There exists a unique $\sigma \in \overline{G}$ such that $\sigma(a) = b$, $\sigma(b) = a$, $\sigma(c) = d$, $\sigma(d) = c$. In particular, the symmetry group* $\mathrm{Aut}(C)$ *of any 4-configuration C contains a Klein 4-group.*

Proof. Uniqueness of σ is obvious from (3.3). For the existence of σ, we may assume that $(a, b, c, d) = (0, 1, \infty, z)$. Then σ is represented by the matrix $\begin{pmatrix} z & -z \\ 1 & -z \end{pmatrix}$. $\square$

We summarize the preceding observations in the next assertion, which is certainly well-known, see e.g [4], 10.1. Some 4-configuration C is *special* if the order $|A|$ of $A = \mathrm{Aut}(C)$ is strictly larger than 4. In each case, we give the numbers $C(4, q)$ of all G-classes and $C^{\mathrm{spec}}(4, q)$ of all classes of special 4-configuarations, along with a representative C for each special class, and the size $|A|$.

3.11 Theorem. *The G-classes of 4-configurations on $\mathfrak{X} = \mathbb{P}(K)$ with $K = \mathbb{F}_q$ of characteristic p are described as follows.*

case	$C(4,q)$	$C^{\text{spec}}(4,q)$	representative of special 4-configuration	$\lvert A\rvert$
$p \neq 2,3,\quad q \equiv 1(\text{mod}3)$	$\frac{q+5}{6}$	2	$\{0,1,\infty,2\}$ $\{0,1,\infty,\tau\}$	8 12
$q \equiv 2(\text{mod}3)$	$\frac{q+1}{6}$	1	$\{0,1,\infty,2\}$	8
$p = 3$	$\frac{q+3}{6}$	1	$\{0,1,\infty,2\}$	24
$p = 2\quad q = 2^{2k}$	$\frac{q+2}{6}$	1	$\{0,1,\infty,\rho\}$	12
$q = 2^{2k+1}$	$\frac{q-2}{6}$	0	–	–

Here the special configurations correspond to the exceptions (3.6)–(3.9). Writing "$\sim$" for G-equivalence, the extra symmetries are emphasized by noting that

$$\begin{array}{lcll} \{0,1,\infty,2\} & \sim & \{0,1,-1,\infty\} & \text{if } p \neq 2; \\ \{0,1,\infty,\tau\} & \sim & \{0,1,\rho,\rho^{-1}\} & \text{if } p \neq 2,3,\ \rho = \rho_3; \\ \{0,1,\infty,\rho\} & \sim & \{0,1,\rho,\rho^{-1}\} & \text{if } q = 2^{2k}. \end{array}$$

4. Five points.

We now perform a similar analysis for 5-configurations in $\mathfrak{X}$, where we make heavy use of the case $n = 4$. Given $C \in \mathcal{C}(5,q)$, we let $A = \text{Aut}(C)$ be its symmetry group. C splits into orbits under A, of possible shape

(4.1) (1) $C = C_5$; (2) $C = C_4 \cup C_1$; (3) $C = C_3 \cup C_2$;
(4) $C = C_2 \cup C_2' \cup C_1$; (5) $C = C_1 \cup C_1' \cup \cdots \cup C_1^{(4)}$; (6) $C = C_3 \cup C_1 \cup C_1'$;
(7) $C = C_2 \cup C_1 \cup C_1' \cup C_1''$,
where all the unions are disjoint and a subscript i denotes cardinality, i.e., $|C_i| = i$.

Case (7) states that any element of A has 3 fixed points and is therefore reduced to identity (cf. (3.3)). So that case cannot occur.

4.2 Proposition. *Case* (6) *in* (4.1) *is excluded, too.*

Proof. Any element of A has two fixed points, without restriction, the points 0 and ∞ of $\mathfrak{X} = \mathbb{P}(K)$. Hence A contains a 3-group which acts through multiplications with $\rho = \rho_3$, and C is G-equivalent with $\{0,1,\rho,\rho^2,\infty\}$. (Note that this already excludes the case of $p = 3$!) But the symmetry group of such a configuration interchanges 0 and ∞. Hence this case is excluded. □

4.3 Proposition. *In case* (4)*, the symmetry group A has two elements.*

Proof. Any $1 \neq \sigma \in A$ must act nontrivially on C_2 and on C_2'. □

Case (5), which says that $A = \{1\}$, will turn out to be typical, cases (1)–(4) exceptional, in that they occur with smaller order of magnitude, see (5.17) and (5.18).

We now discuss the cases (1) to (4), where (4) will be the most complicated. Before, we introduce some notation.

(4.6) If $\sigma \in G$ with $1 \neq \overline{\sigma} \in \overline{G}$ has order prime to p, it is semisimple and either of type $\mathrm{III}_{a,b}$ (cf. (2.1)) and has two fixed points on $\mathfrak{X}$, in which case it is called *split semisimple*, or it is of type $\mathrm{IV}_{a,b}$, has no fixed points, and is called *non-split semisimple*. In the latter case, its eigenvalues generate the quadratic extension L of K, and description (2.5) applies. If $\overline{\sigma}$ has order a power of p, then the order of $\overline{\sigma}$ is exactly p, σ is of type II_a, $\overline{\sigma}$ is *unipotent*, and has precisely one fixed point on $\mathfrak{X}$. We further use $C \sim C'$ to denote G-equivalence of the configurations C and C'.

(4.7) **Case (1) of (4.1).** Here A contains an element $\overline{\sigma}$ of order 5. If $\boxed{p = \mathrm{char}(K) = 5}$, then $\overline{\sigma}$ is unipotent and has one fixed point $z \in \mathfrak{X}$, without restriction, $z = \infty$. Then $C \sim \{0,1,2,3,4\} = \mathbb{F}_5 \hookrightarrow \mathfrak{X}$, and A is isomorphic with $\mathrm{Aff}(\mathbb{F}_5)$, the affine group of order 20.

Suppose now that $\boxed{p \neq 5}$. Then σ is semisimple. If σ is split semisimple, it has two fixed points, without restriction: the points 0 and ∞. Then $C \sim \mu_5 \hookrightarrow K^* \hookrightarrow \mathfrak{X}$, which occurs if and only if $q \equiv 1(\mathrm{mod} 5)$. If σ is non-split (which occurs if and only if $5|(q+1)$, i.e., $q \equiv 4(\mathrm{mod} 5)$), then $C \sim \mu_5 \hookrightarrow L^*/K^* \xrightarrow{\cong} \mathfrak{X}$. In both cases, the inversion $z \longmapsto z^{-1}$ on $\mathfrak{X}$ stabilizes C, which gives an embedding of the dihedral group $D_5 \hookrightarrow A = \mathrm{Aut}(C)$. If moreover $\boxed{p \neq 2}$ then $D_5 = A$, as follows from Proposition 4.8. It remains to consider the subcase $\boxed{p = 2}$. If $q = 2^k$ with $k \equiv 1,3(\mathrm{mod}\ 4)$ then $q \equiv 2,3(\mathrm{mod}\ 5)$ and no such 5-configuration C exists in $\mathfrak{X}$. If $k \equiv 2(\mathrm{mod}\ 4)$ then $q \equiv 4(\mathrm{mod}\ 5)$, $K = \mathbb{F}_q$ contains $\mathbb{F}_4$, and $C \sim \mathbb{P}^1(\mathbb{F}_4) \hookrightarrow \mathfrak{X}$, which gives $A \cong \mathrm{PGL}(2,\mathbb{F}_4) \cong A_5$. If $k \equiv 0(\mathrm{mod}\ 4)$ then $q \equiv 1(\mathrm{mod}\ 5)$, $C \sim \mu_5$ as seen above, but also $C \sim \mathbb{P}^1(\mathbb{F}_4)$ as there is only one such class, so again $A \cong \mathrm{PGL}(2,\mathbb{F}_4) \cong A_5$.

Hence case (1) occurs if and only if $p = 5$, in which case $A \cong \mathrm{Aff}(\mathbb{F}_5)$, $p = 2$ and $q = 2^{2k}$, in which case $A \cong A_5$, or $p \neq 2,5$ and $q \equiv 1,4(\mathrm{mod}\ 5)$, in which case $A \cong D_5$. In each case, there is precisely one such C up to G-equivalence.

4.8 Proposition. *Suppose that $p \neq 2,5$ and C is a 5-configuration of type (1) in (4.1). Then $A = \mathrm{Aut}(C) \cong D_5$.*

Proof. We must show that A is not larger than D_5. The subgroups of S_5 of order divisible by $10 = |D_5|$ have orders 20, 60, 120 and are isomorphic with $\mathrm{Aff}(\mathbb{F}_5)$, A_5, S_5, respectively. Now $A \not\cong S_5$ by Proposition 3.3, and $A \not\cong \mathrm{Aff}(\mathbb{F}_5)$ since $\mathrm{Aff}(\mathbb{F}_5)$ doesn't embed into $\overline{G}$ ([7], XI, Theorem 2.3). Suppose that $A \cong A_5$. If $C = \{a,b,c,d,e\}$

then any of the involutions $(ab)(cd)$, $(ac)(bd)$ and $(ad)(bc)$ must fix the point e. But this is excluded by Proposition 4.9. $\square$

4.9 Proposition. *Let $p \neq 2$ and $\{a, b, c, d\}$ be any 4-configuration. The fixed point sets of the 3 involutions $(ab)(cd)$, $(ac)(bd)$, $(ad)(bc)$ (see* (3.10)*) are mutually disjoint.*

Proof. Without restriction, $\{a, b, c, d\} = \{0, 1, \infty, z\}$. The 3 involutions are represented by the matrices $\begin{pmatrix} z & -z \\ 1 & -z \end{pmatrix}$, $\begin{pmatrix} 0 & z \\ 1 & 0 \end{pmatrix}$ and $\begin{pmatrix} 1 & -z \\ 1 & -1 \end{pmatrix}$. Their fixed points are, respectively, $z \pm \sqrt{z^2 - z}$, $\pm\sqrt{z}$, and $1 \pm \sqrt{1-z}$, from which we get the result. $\square$

(4.10) **Case (2) of (4.1).** We have $C = C_4 \cup C_1$ with $C_1 = \{x\}$, where x is a fixed point of A. Up to G-conjugation, x may be taken as $\infty \in \mathfrak{X}$. We first assume $\boxed{p = 2}$. Then A is a subgroup of $\mathrm{Aff}(K)$, and its 2-Sylow group a subgroup of the group of transformations $z \longmapsto z + b$, $b \in K$. Hence C_4 is a residue class in K modulo a subgroup of order 4, that is, an affine subspace of dimension 2 of the $\mathbb{F}_2$-vector space $K = \mathbb{F}_q$.

4.11 Proposition. *Let $q \geq 4$ be a power of* 2.

(i) *The number of $\mathbb{F}_2$-subvector spaces V of K of dimension 2 is $(q-1)(q-2)/6$.*
(ii) *The number of affine $\mathbb{F}_2$-subspaces U of K of dimension 2 is $q(q-1)(q-2)/24$.*
(iii) *Each U as in (ii) is $\mathrm{Aff}(K)$-equivalent with some V as in (i).*
(iv) *The stabilizer subgroup in $\mathrm{Aff}(K)$ of some V as in (i) is isomorphic with V, if V is not K^*-equivalent with $\mathbb{F}_4 \hookrightarrow K$, and is isomorphic with the group $\{z \longmapsto az + b \mid a \in \mathbb{F}_4^*, b \in V\} \cong \mathrm{Aff}(\mathbb{F}_4)$, if V is K^*-equivalent with $\mathbb{F}_4$ (which occurs if and only if $q = 2^{2k}$).*
(v) *The number of $\mathrm{Aff}(K)$-orbits on $\{U \mid U$ affine $\mathbb{F}_2$-subspace of K of dimension $2\}$ is $(q+2)/6$ for $q = 2^{2k}$ and $(q-2)/6$ for $q = 2^{2k+1}$.*

Proof. (i) Count the number of ordered bases! (ii) For each V as in (i), there are $q/4$ residue classes U. (iii) and (iv) are obvious, and (v) results from counting. $\square$

Note that the special orbit in (v), $q = 2^{2k}$, represented by $U = V = \mathbb{F}_4$, yields the 5-configuration $C = C_4 \cup C_1 = \mathbb{F}_4 \cup \{\infty\} = \mathbb{P}^1(\mathbb{F}_4)$, which has $A = \mathrm{Aut}(C) = \mathrm{PGL}(2, \mathbb{F}_4) \cong A_5$, and is not of type (2). Hence there remain $(q-4)/6$ (if $q = 2^{2k}$) resp. $(q-2)/6$ (if $q = q^{2k+1}$) $\mathrm{Aff}(K)$-classes of U's, which give the same number of $\overline{G}$-classes of 5-configurations of type (2), all with $A = V$ elementary abelian of order 4.

Now assume $\boxed{p \neq 2}$. If C_4 is a generic 4-configuration (that is, $\mathrm{Aut}(C_4)$

is a Klein 4-group) or $C_4 \sim \{0, 1, \infty, \tau\}$ (see (3.11)) and $C = C_4 \cup \{x\}$, then x must be a fixed point of all the three involutions in $\mathrm{Aut}(C_4)$, which is impossible by Proposition 4.9. Therefore, $\mathrm{Aut}(C_4)$ contains an element $\overline{\sigma}$ of order 4, which has x as a fixed point. Up to conjugation in $\overline{G}$, the fixed points of $\overline{\sigma}$ are $x = \infty$ and $y = 0$, that is $\overline{\sigma}$ acts as multiplication with ρ_4 and $C = C_4 \cup \{x\} \sim \mu_4 \cup \{\infty\}$. This occurs if and only if $q \equiv 1 (\mathrm{mod}\ 4)$.

If $\boxed{p = 5}$ then $C \sim \mu_4 \cup \{\infty\} \sim \mu_4 \cup \{0\} = \mathbb{F}_5 \hookrightarrow \mathfrak{X}$, and we find C of type (1). Thus case (2) is impossible for $p = 5$. If $\boxed{p \neq 2, 5}$ then $\mathrm{Aut}(\mu_4 \cup \{\infty\}) = \mathrm{Aut}(\mu_4) \cap \mathrm{Aff}(K) \cong \mu_4$. Here the last isomorphism is obvious for $p > 5$, and requires a small - omitted - calculation for $p = 3$, due to the fact that $\mu_4 \sim \mathbb{P}^1(\mathbb{F}_3)$ has a large automorphism group, cf. (3.11). Hence for $p \neq 2, 5$ and $q \equiv 1 (\mathrm{mod}\ 4)$ there exists one G-class of 5-configurations of type (2), represented by $C = \mu_4 \cup \{\infty\}$, and with $\mathrm{Aut}(C) = \mu_4$, which acts on C by multiplication. Case (2) doesn't occur if $q \not\equiv 1 (\mathrm{mod}\ 4)$.

(4.12) **Case (3) of (4.1).** We have $C = C_3 \cup C_2$, without restriction: $C = \{0, 1, \infty\} \cup \{a, b\}$. In this case, $A \hookrightarrow W$ with the group W of (3.4), and A acts transitively on both $\{0, 1, \infty\}$ and $\{a, b\}$. This implies $A = W$, and a, b are fixed points of the elements $\begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}$, $\begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}$ of order 3 of W. This is equivalent with a, b being roots of $X^2 - X + 1$. If $\boxed{p = 2}$, $a, b \in \mathbb{F}_4$ and $C = \mathbb{P}^1(\mathbb{F}_4)$ is of type (1); if $\boxed{p = 3}$ then $X^2 - X + 1 = (X + 1)^2$ has only one root; so case (3) doesn't occur for $p = 2$ or 3. If $\boxed{p > 3}$ then a, b are primitive 6^{th} roots of unity, which is only possible if $q \equiv 1 (\mathrm{mod}\ 3)$. In this case, any 5-configuration C of type (3) is G-equivalent with $\{0, 1, \infty, \tau, \tau^{-1}\} \sim \mu_3 \cup \{0, \infty\}$, and has symmetry group $A = \mathrm{Aut}(C) \cong W \cong S_3$.

(4.13) In order to handle the remaining and most complicated **case (4) of (4.1)**, let us introduce some more notation.

We put

$$\begin{aligned} &\mathcal{C}(4) = \mathcal{C}(4, \mathfrak{X}),\ \mathcal{C}(5) = \mathcal{C}(5, \mathfrak{X}), \\ &\mathcal{C}^{\mathrm{spec}}(5) = \{C \in \mathcal{C}(5) \mid |\mathrm{Aut}(C)| > 1\} = \textstyle\bigcup_{1 \leq i \leq 4} \mathcal{C}(5, i), \end{aligned}$$

where $\mathcal{C}(5, i)$ consists of the 5-configurations of type (i) (see (4.1)). Moreover we define

$$\begin{aligned} \tilde{\mathcal{C}}(4) &:= \{(C, \iota) \mid C \in \mathcal{C}(4) \text{ and } \iota \in \mathrm{Aut}(C) \text{ an involution of type } (2,2)\}, \\ \tilde{\mathcal{C}}(5) &:= \{(C, \iota) \mid C \in \mathcal{C}(5) \text{ and } \iota \in \mathrm{Aut}(C) \text{ an involution of type } (2,2,1)\}. \end{aligned}$$

That is, $\iota \in \mathrm{Aut}(C)$ has order 2 and has no (resp. one) fixed point in C. The group G acts via its quotient group $\overline{G}$ on all the mentioned configuration sets. We relate the 5-configurations of type (4) with the 4-configurations on $\mathfrak{X}$ through the following commutative diagram:

$$
(4.14)\qquad
\begin{array}{ccccccc}
\mathcal{C}(4) & \xleftarrow{\kappa} & \tilde{\mathcal{C}}(4) & \xleftarrow{\varphi} & \tilde{\mathcal{C}}(5) & \xrightarrow{\psi} & \mathcal{C}^{\mathrm{spec}}(5) \\
\downarrow & & \downarrow & & \downarrow & & \downarrow \\
\overline{G}\setminus\mathcal{C}(4) & \xleftarrow{\overline{\kappa}} & \overline{G}\setminus\tilde{\mathcal{C}}(4) & \xleftarrow{\overline{\varphi}} & \overline{G}\setminus\tilde{C}(5) & \xrightarrow{\overline{\psi}} & \overline{G}\setminus\mathcal{C}^{\mathrm{spec}}(5)
\end{array}
$$

Here ψ and κ are the natural forgetful mappings, φ maps (C,ι) to $(C_4,\iota|_{C_4})$ if $C=C_4\cup\{x\}$ with the fixed point x of ι, the unlabelled vertical maps are the canonical projections, and the lower row maps are derived from the upper row. We first suppose that the characteristic p is larger than 5 and later make the necessary adaptations to $p=2,3,5$.

$\boxed{p>5}$ The fiber $\psi^{-1}(C)$ of some $C\in\mathcal{C}^{\mathrm{spec}}(5)$ has m elements, where m is the number of involutions in $A=\mathrm{Aut}(C)$, since each such involution ι is necessarily of type $(2,2,1)$. Hence $m=5,1,3,1$ for $C\in\mathcal{C}(5,i)$, $i=1,2,3,4$, as $A=D_5$, μ_4, S_3,μ_2, respectively. Now in all four cases, all the involutions in A are A-conjugate, which implies:

(4.15) $\overline{\psi}$ is injective, and thus bijective.

Let $\tilde{\mathcal{C}}(5,i)$ be the inverse image $\psi^{-1}(\mathcal{C}(5,i))$ and let $(C,\iota)\in\tilde{\mathcal{C}}(5,i)$. The stabilizer of (C,ι) in $\overline{G}$ equals the centralizer of ι in $A=\mathrm{Aut}(C)$, which is $\{1,\iota\}$ for $i=1,3,4$, and $A=\mu_4$ for $i=2$. Therefore:

(4.16) The fibers $\tilde{C}(5)\longrightarrow\overline{G}\setminus\tilde{\mathcal{C}}(5)$ have $|\overline{G}|/2$ elements in $\tilde{\mathcal{C}}(5,i)$, $i=1,3,4$, and $|\overline{G}|/4$ elements for $i=2$. Note that there is at most one exceptional fiber of length $|\overline{G}|/4$.

Next, let (C,ι) be an element of $\tilde{C}(4)$. As ι is semisimple, it has 2 or 0 fixed points on $\mathfrak{X}$, which gives $|\varphi^{-1}((C,\iota))|=2$ or 0, respectively. If C is G-equivalent with $\{0,1,\infty,z\}$, its three involutions ι_1,ι_2,ι_3 are represented by the matrices $\begin{pmatrix} z & -z\\ 1 & -z\end{pmatrix}$, $\begin{pmatrix} 0 & z\\ 1 & 0\end{pmatrix}$, $\begin{pmatrix} 1 & -z\\ 1 & -1\end{pmatrix}$. From the proof of Proposition 4.9 we see that

$$
(4.17)\qquad
\begin{array}{rclcrcl}
|\varphi^{-1}((C,\iota_1))| & = & 2 & \Leftrightarrow & (\frac{1-z^{-1}}{q}) & = & 1\\
|\varphi^{-1}((C,\iota_2))| & = & 2 & \Leftrightarrow & (\frac{z}{q}) & = & 1\\
|\varphi^{-1}((C,\iota_3))| & = & 2 & \Leftrightarrow & (\frac{1-z}{q}) & = & 1.
\end{array}
$$

Here $(\frac{\cdot}{q})$ is the quadratic symbol in $K=\mathbb{F}_q$; $(\frac{a}{q})=1,-1,0$ if $a\in K$ is a non-zero square/nonsquare/zero in K, respectively. If one of these symbols takes the value -1, the corresponding fiber is empty.

Again, the stabilizer of (C,ι) in $\overline{G}$ is the centralizer of ι in $\mathrm{Aut}(C)$.

Now (see (3.11)) $\mathrm{Aut}(C)$ is a subgroup of order 4, 8 or 12 of S_4, the

Klein 4-group V_4, a 2-Sylow group isomorphic with D_4, or the alternating group A_4. All the involutions in $\mathrm{Aut}(C)$ are of type (2,2) if $\mathrm{Aut}(C) = V_4$ or A_4, and then the centralizer of ι is V_4. If, on the other hand, $\mathrm{Aut} \cong D_4$, there are three involutions of type (2,2), among which two have a centralizer V_4 and one a centralizer D_4. This implies:

(4.18) The fibers of $\tilde{\mathcal{C}}(4) \longrightarrow \overline{G}\backslash\tilde{\mathcal{C}}(4)$ are all but one of size $|\overline{G}|/4$, with the exceptional fiber of size $|\overline{G}|/8$.

4.19 Proposition. *The map $\overline{\varphi}$ is injective. If $(C,\iota) \in \tilde{\mathcal{C}}(4)$ is G-equivalent with $(\{0,1,\infty,z\},\iota_k)$ as in* (4.17)*, then its class belongs to the image of $\overline{\varphi}$ if and only if the corresponding quadratic symbol $(\frac{1-z^{-1}}{q})$, $(\frac{z}{q})$, $(\frac{1-z}{q})$ has value* 1*.*

Proof. First note that the exceptional fiber of $\tilde{\mathcal{C}}(5) \longrightarrow \overline{G}\backslash\tilde{\mathcal{C}}(5)$ (which exists if and only if $q \equiv 1(\mathrm{mod}\ 4)$, and is then represented by $C = \mu_4 \cup \{\infty\}$ with its involution $\iota : \ z \longmapsto -z$) maps under φ to the exceptional fiber of $\tilde{\mathcal{C}}(4) \longrightarrow \overline{G}\backslash\tilde{\mathcal{C}}(4)$, represented by $\{0,1,\infty,-1\}$ and the involution $x \longmapsto -x^{-1}$ given by the matrix $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. This results from an explicit calculation, which we omit. Now the assertion comes out by comparing fibers in the middle square of diagram (4.14). $\square$

The fibers of κ are all of size 3. As the fibers of $\mathcal{C}(4) \longrightarrow \overline{G} \setminus \mathcal{C}(4)$ are all but at most two of length $|\overline{G}|/4$ (one of length $|\overline{G}|/8$, and, if $q \equiv 1(\mathrm{mod}\ 3)$, one of length $|\overline{G}|/12$), we find:

4.20 Proposition. *All the fibers of $\overline{\kappa}$ are of size* 3*, except for the fibers over the orbits represented by $C = \{0,1,\infty,-1\}$, which contains two elements, and, if $q \equiv 1(\mathrm{mod}\ 3)$, $C = \{0,1,\infty,\tau\}$, which contains one element.*

Proof. This results from considering the left square in (4.14). Note that the inverse image of the class of $\{0,1,\infty,-1\}$ in $\tilde{C}(4)$ splits into two $\overline{G}$-orbits, one of size $|\overline{G}|/4$, the other of size $|\overline{G}|/8$. $\square$

Now, as we control the maps in (4.14), we may express $\overline{G} \setminus \mathcal{C}^{\mathrm{spec}}(5)$ through the known quantity $\overline{G} \setminus \mathcal{C}(4)$.

(4.21) By the results of Section 3 (see Theorem 3.11), the elements of $\overline{G} \setminus \mathcal{C}_4$ are represented through $\{0,1,\infty,z\}$, with z taken

- one out of $\{-1,\frac{1}{2},2\}$, say, $z=-1$;
- if $q \equiv 1(\mathrm{mod}\ 3)$: one out of τ,τ^{-1} (recall that $\tau = \rho_6$ is a primitive 6^{th} root of unity);
- one out of each W-orbit on $K \setminus \{0,1,-1,\frac{1}{2},2,\tau,\tau^{-1}\} =: H$, where the group W is described in (3.4).

We now discuss the contributions to $\overline{G} \setminus \mathcal{C}^{\text{spec}}(5)$ in diagram (4.14).

(4.22) The three involutions on $C = \{0, 1, \infty, -1\}$ give rise to three quadratic symbols $(\frac{2}{q})$, $(\frac{-1}{q})$, $(\frac{2}{q})$ (see (4.17)); the coincidence of two of the symbols corresponds to the fact that $\overline{\kappa}^{-1}(C)$ has only two elements. Hence, by (4.19), C gives a contribution of 1 to $|\overline{G}\setminus\mathcal{C}^{\text{spec}}(5)|$ if $(\frac{-1}{q}) = 1$, i.e., if $q \equiv 1(\text{mod } 4)$, and another 1 if $(\frac{2}{q}) = 1$, i.e., if $q \equiv 1, 7(\text{mod } 8)$; altogether a contribution of $2, 1, 0$ if $q \equiv 1, 5$ or $7, 3(\text{mod } 8)$, respectively.

(4.23) Now consider $C = \{0, 1, \infty, \tau)$ (in case $q \equiv 1(\text{mod } 3)$). The relevant quadratic symbols are $(\frac{1-\tau^{-1}}{q})$, $(\frac{\tau}{q})$, $(\frac{1-\tau}{q})$. But, with $\rho = \rho_3 = -\tau = (\rho^2)^2$, $(\frac{1-\tau^{-1}}{q}) = (\frac{1+\rho^{-1}}{q}) = (\frac{-\rho^2}{q}) = (\frac{-1}{q})$, $(\frac{\tau}{q}) = (\frac{-1}{q})$, $(\frac{1-\tau}{q}) = (\frac{1+\rho}{q}) = (\frac{-\rho^2}{q}) = (\frac{-1}{q})$. (Again the coincidence of the three values is predicted by $|\overline{\kappa}^{-1}(C)| = 1$.) Hence C contributes to $|\overline{G}\setminus\mathcal{C}^{\text{spec}}(5)|$ by 1 if $(\frac{-1}{q}) = 1$, i.e., if $q \equiv 1(\text{mod } 12)$, and by 0 otherwise.

(4.24) Finally, we consider $C = \{0, 1, \infty, z\}$ with $z \in H = K \setminus \{0, 1, -1, \frac{1}{2}, 2, \tau, \tau^{-1}\}$. By (4.19) and (4.20) to such a C there correspond $\frac{1}{2}(3 + (\frac{1-z^{-1}}{q}) + (\frac{z}{q}) + (\frac{1-z}{q}))$ many elements of $\overline{G}\setminus\mathcal{C}^{\text{spec}}(5)$. Note that $z, 1-z, 1-z^{-1}$ along with their reciprocals $z^{-1}, (1-z)^{-1}, z(z-1)^{-1}$ form the W-orbit of z.

Assume $\boxed{q \equiv 1(\text{mod } 3)}$. Then $|H| = q - 7$, and the total contribution of such C to $|\overline{G} \setminus C^{\text{spec}}(5)|$ is

$$\begin{aligned}
&\tfrac{1}{2}\textstyle\sum_{z\in W\setminus H}(3 + (\frac{z}{q}) + (\frac{1-z}{q}) + (\frac{1-z^{-1}}{q})) = \tfrac{3}{2}(\frac{q-7}{6}) + \tfrac{1}{4}\textstyle\sum_{z\in W\setminus H}\sum_{w\in W}(\frac{w(z)}{q}) \\
&= \tfrac{q-7}{4} - \tfrac{1}{4}\textstyle\sum_{z\in\{1,-1,2,\frac{1}{2},\tau,\tau^{-1}\}}(\frac{z}{q}) \quad (\text{ as } \sum_{z\in K^*}(\frac{z}{q}) = 0) \\
&= \tfrac{q-7}{4} - \tfrac{1}{4}(1 + (\frac{-1}{q})) - \tfrac{1}{2}(\frac{2}{q}) - \tfrac{1}{2}(\frac{\tau}{q}).
\end{aligned}$$

Similarly, we get for $\boxed{q \equiv 2(\text{mod } 3)}$ the contribution $\frac{q-5}{4} - \frac{1}{4}(1+(\frac{-1}{q})) - \frac{1}{2}(\frac{2}{q})$.

The values of these formulas depend on $q(\text{ mod } 8)$ and $q(\text{ mod } 12)$, that is, on $q(\text{mod } 24)$. The table below shows the contributions of $C = \{0, 1, \infty, z\}$ to $|\overline{G}\setminus\mathcal{C}^{\text{spec}}(5)|$, where $z \in W \setminus H$, $z = -1$, $z = \tau$, depending on $q(\text{mod } 24)$.

4.25 Table. $\overline{G} \setminus \mathcal{C}^{\text{spec}}(5)$ and its fibering over $\overline{G} \setminus \mathcal{C}(4)$

type of z / $q(\mathrm{mod}\ 24)$	$z \in H \setminus W$	$z=-1$	$z=\tau$	$\lvert\overline{G}\setminus\mathcal{C}^{\mathrm{spec}}(5)\rvert$
1	$(q-13)/4$	2	1	$(q-1)/4$
5	$(q-5)/4$	1	0	$(q-1)/4$
7	$(q-7)/4$	1	0	$(q-3)/4$
11	$(q-3)/4$	0	0	$(q-3)/4$
13	$(q-9)/4$	1	1	$(q-1)/4$
17	$(q-9)/4$	2	0	$(q-1)/4$
19	$(q-3)/4$	0	0	$(q-3)/4$
23	$(q-7)/4$	1	0	$(q-3)/4$

We remark that the number $|\overline{G}\setminus\mathcal{C}^{\mathrm{spec}}(5)|$ of special 5-configurations C (i.e., of those C with $A=\mathrm{Aut}(C)\neq\{1\}$) is $(q-1)/4$ (resp. $(q-3)/4$) for $q\equiv 1$ resp. $3(\mathrm{mod}\ 4)$, and in particular depends only on $q(\mathrm{mod}\ 4)$. The total number of classes of 5-configurations of type (4) in (4.1) comes out as $|\overline{G}\setminus\mathcal{C}^{\mathrm{spec}}(5)|$ minus the now known numbers of classes of types (1), (2) and (3).

4.26 Definition. *We define characteristic functions as follows: For $q,a,b\in\mathbb{N}$ put*

$$\chi(q,a,b):=\begin{cases}1, & \text{if } q\equiv a(\mathrm{mod}\ b)\\ 0, & \text{otherwise.}\end{cases}$$

Further, for $S\subset\mathbb{N}$,

$$\chi(q,S,b):=\sum_{s\in S}\chi(q,s,b),$$

and for a prime power $q=p^k$,

$$\chi(q):=\begin{cases}1, & k \text{ even}\\ 0, & k \text{ odd.}\end{cases}$$

Then, as results from (4.7) – (4.12), the number 5-configurations of type (i) is

(4.27) $\chi(q,\{1,4\},5)$ for $i=1$, $\chi(q,1,4)$ for $i=2$, $\chi(q,1,3)$ for $i=3$, $(q-2+(\frac{-1}{q}))/4-\chi(q,\{1,4\},5)-\chi(q,1,4)-\chi(q,1,3)$ for $i=4$, as long as $p>5$.

It remains to discuss case (4) of (4.1) for the "bad" characteristics $p=2,3,5$.

(4.28) Let now $\boxed{p=5}$. As described before (cf. (4.10)), case (2) doesn't occur, and there exists one class of 5-configurations of type (1), with automorphism group $A\cong\mathrm{Aff}(\mathbb{F}_5)$. That group contains 5 involutions, all of type $(2,2,1)$, and all conjugate in A. Hence the map $\overline{\psi}$ in (4.14) is still bijective. The rest of the discussion of (4.14) remains unchanged.

That is $|\overline{G}\backslash\mathcal{C}^{\rm spec}(5)| = (q-1)/4$, as $q \equiv 5 \equiv 1(\bmod 4)$, and the number of classes of C's of type (i) is 1 for $i = 1$, 0 for $i = 2$, $\chi(q, 1, 3) = \chi(q)$ for $i = 3$, $(q-5)/4 - \chi(q)$ for $i = 4$.

(4.29) Next, we study $\boxed{p = 3}$. As only cases (1), (2), (4) of (4.1) may occur, where all the relevant involutions in A are A-conjugate, the map $\overline{\psi}$ is still bijective. Also the mapping properties of the middle square in (4.14) are the same as for the case $p > 5$, as is the case for the map $\kappa : \tilde{\mathcal{C}}(4) \longrightarrow \mathcal{C}(4)$, which is $3:1$. On the other hand, fibers of $\mathcal{C}(4) \longrightarrow \overline{G} \setminus \mathcal{C}(4)$ now all have size $|\overline{G}|/4$ except for one, which has $|G|/24$ elements. It results that $\overline{\kappa} : \overline{G} \setminus \tilde{\mathcal{C}}(4) \longrightarrow \overline{G} \setminus \mathcal{C}(4)$ has fibers of size 3, except for the distinguished element of $\overline{G} \setminus \mathcal{C}(4)$ represented by $\mathbb{P}^1(\mathbb{F}_3)$, which has a fiber with one point. With a calculation similar to (4.24), we get $|\overline{G}\backslash\mathcal{C}^{\rm spec}(5)| = (q-2+(\frac{-1}{q}))/4 = (q-3+2\chi(q))/4$, and for the number of classes of 5-configurations C of type (i): $\chi(q, \{1, 4\}, 5) = \chi(q)$ for $i = 1$, $\chi(q, 1, 4) = \chi(q)$ for $i = 2$, 0 for $i = 3$, $(q-3-6\chi(q))/4$ for $i = 4$.

(4.3) Now finally let $\boxed{p = 2}$. This is quite simple, as the case (4) of (4.1) doesn't occur. For, let $C = \{a, b\} \cup \{c, d\} \cup \{e\}$ be a 5-configuration, and $\overline{\sigma} \in \mathrm{Aut}(C)$ an involution which interchanges a, b and c, d, and fixes e. Without restriction, $e = \infty$, $a = 0$. Then $\overline{\sigma}$ is of shape $z \longmapsto z + b$ and $d = c + b$. But then $\overline{\gamma} : z \longmapsto z + c$ also stabilizes C, a, b, c, d are $\mathrm{Aut}(C)$-equivalent, and C is not of type (4). Therefore the number of classes of type (i) is $\chi(q, \{1, 4\}, 5) = \chi(q)$ for $i = 1$, $(q-2-2\chi(q))/6$ for $i = 2$, and 0 for $i = 3$ or 4.

We collect what has been proven in the next theorem, which is analogous with Theorem 3.11. The table gives, depending on the nature of q, the number $C(5, q, i) = |\overline{G} \setminus \mathcal{C}(5, \mathfrak{X}, i)|$ of G-classes of 5-configurations of type (i), for $1 \leq i \leq 4$, along with the corresponding symmetry groups A, and the total number $C^{\rm spec}(5, q) = |\overline{G} \setminus \mathcal{C}^{\rm spec}(5, \mathfrak{X})|$ of all classes of special 5-configurations C (i.e, those with $|\mathrm{Aut}(C)| > 1$). We postpone to the next section giving the number $C(5, q) = |\overline{G} \setminus \mathcal{C}(5, \mathfrak{X})|$ of all classes.

4.31 Theorem. *The numbers of classes of special* 5*-configurations on* $\mathfrak{X} = \mathbb{P}^1(\mathbb{F}_q)$ *modulo the action of* $G = \mathrm{GL}(2, \mathbb{F}_q)$ *are given by the following table.*

type i / char p	$C(5,q,1)$ A	$C(5,q,2)$ A	$C(5,q,3)$ A	$C(5,q,4)$ A	$C^{spec}(5,q)$
$p>5$	$\chi(q,\{1,4\},5)$ D_5	$\chi(q,1,4)$ μ_4	$\chi(q,1,3)$ S_3	see (4.27) μ_2	$\frac{(q-2+(\frac{-1}{q}))}{4}$
$p=5$	1 $\mathrm{Aff}(\mathbb{F}_5)$	0 -	$\chi(q)$ S_3	$\frac{(q-5)}{4}-\chi(q)$ μ_2	$\frac{(q-1)}{4}$
$p=3$	$\chi(q)$ D_5	$\chi(q)$ μ_4	0 -	$(\frac{(q-3-6\chi(q))}{4}$ μ_2	$\frac{(q-3+2\chi(q))}{4}$
$p=2$	$\chi(q)$ A_5	$\frac{q-2-2\chi(q))}{6}$ $\mathbb{F}_2\times\mathbb{F}_2$	0 -	0 -	$\frac{(q-2+4\chi(q))}{6}$

Representatives C of classes of a given symmetry type are given in (4.7)–(4.12).

5. The numbers $C(n,q)$, $n\geq 5$.

Note that the results of the last two sections are independent of the determination of the cycle index in Section 2. They allow to determine $C(5,q)=|\overline{G}\setminus\mathcal{C}(5,q)|$, but this would require an enormous amount of case considerations. Instead, we now use the cylce index to find a precise formula for $C(5,q)$, and asymptotic results for $C(n,q)$, $n\geq 5$.

By the discussion around (3.1), we have

$$C(5,q)=\text{coefficient of } Y_1^5Y_2^{q-4} \text{ in } Z_{G,\mathfrak{X}}(P_1(Y_1,Y_2),\ldots,P_{q+1}(Y_1,Y_2)),$$

that is, of

$$(5.1)\qquad \begin{aligned} &|\overline{G}|^{-1}(Y_1+Y_2)^{q+1}+q^{-1}(Y_1+Y_2)(Y_1^p+Y_2^p)^{q/p}\\ &+\tfrac{1}{2(q-1)}\textstyle\sum_{2\leq m|(q-1)}\varphi(m)(Y_1+Y_2)^2(Y_1^m+Y_2^m)^{(q-1)/m}\\ &+\tfrac{1}{2(q+1)}\textstyle\sum_{2\leq m|(q+1)}\varphi(m)(Y_1^m+Y_2^m)^{(q+1)/m}. \end{aligned}$$

We label the four terms by I, II, III, IV.

(5.2) The contribution to $C(5,q)$ of term I is

$$\frac{1}{|\overline{G}|}\binom{q+1}{5}=\frac{(q-2)(q-3)}{5!}.$$

In the following, we first assume $\boxed{p>5}$. Then term II doesn't contribute.

The share of term III comes from the summands to $m=2,3,4,5$, namely, for

$m=2$: $\frac{1}{2(q-1)}\varphi(2)\cdot 2\binom{(q-1)/2}{2}=(q-3)/8$;

$m=3$ (if $q\equiv 1(\mathrm{mod}\ 3)$, which is taken into account by the factor $\chi(q,1,3)$): $\frac{\chi(q,1,3)}{2(q-1)}\varphi(3)(q-1)/3=\chi(q,1,3)/3$

$m = 4$: $\frac{\chi(q,1,4)}{2(q-1)}\varphi(4) \cdot 2\frac{q-1}{4} = \chi(q,1,4)/2$

$m = 5$: $\frac{\chi(q,1,5)}{2(q-1)}\varphi(5)\frac{q-1}{5} = \frac{2}{5}\chi(q,1,5)$.

Term IV may only contribute through its summand for $m = 5$, by

$$\frac{\chi(q,4,5)}{2(q+1)}\varphi(5)\frac{q+1}{5} = \frac{2}{5}\chi(q,4,5).$$

Making similar calculations for $p = 2, 3, 5$ (where also term II may contribute) and collecting the results, we find the wanted numbers. Recall that $\chi(q) = 1$ (resp. 0) if q is (is not) a square. This allows to simplify the expression $\chi(q,a,b)$ for $q = 2, 3, 5$.

5.3 Theorem. *The number $C(5,q)$ of G-equivalent 5-point configurations in $\mathfrak{X}$ is given by*

(i) $C(5,q) = \frac{1}{120}(q^2 + 10q - 39) + \frac{1}{3}\chi(q,1,3) + \frac{1}{2}\chi(q,1,4) +$
$+\frac{2}{5}\chi(q,\{1,4\},5)$, *if* $p = \mathrm{char}(\mathbb{F}_q) > 5$;

(ii) $C(5,q) = \frac{1}{120}(q^2 + 10q + 45) + \frac{1}{3}\chi(q)$ *if* $p = 5$;

(iii) $C(5,q) = \frac{1}{120}(q^2 + 10q - 39) + \frac{9}{10}\chi(q)$ *if* $p = 3$;

(iv) $C(5,q) = \frac{1}{120}(q^2 + 10q - 24) + \frac{11}{15}\chi(q)$ *if* $p = 2$.

5.4 Remarks. (i) The formulas of Theorem 5.3 also appear in the 2012 Bachelor's thesis of Marius Bohn [2].
(ii) $C(5,q) = \frac{1}{120}q^2 + \frac{1}{12}q + O(1)$, where the constant $O(1)$-term depends only on q modulo $60 = 3 \cdot 4 \cdot 5$. This will soon be generalized.

Now we analyze the behavior of $C(n,q)$ for arbitrary $\boxed{n \geq 5}$. Again we have a look to the coefficient of $Y_1^n Y_2^{q+1-n}$ in the terms I,... IV of (5.1), always assuming that $q + 1 \geq n$.

(5.5) The coefficient of $Y_1^n Y_2^{q+1-n}$ in term I of (5.1) is

$$f_n(q) := \frac{1}{|\overline{G}|}\binom{q+1}{n} = \frac{1}{n!}(q-2)(q-3)\cdots(q-n+2).$$

Here $f_n(X) \in \frac{1}{n!}\mathbb{Z}[X]$ is a polynomial of degree $n - 3$ with leading coefficient $\frac{1}{n!}$.

(5.6) Term II of (5.1) contributes to $C(n,q)$ if and only if $n \equiv 0$ or $1 (\mathrm{mod}\ p)$. In case $n = \nu p$ the contribution is

$$\frac{1}{q}\binom{q/p}{\nu} = \frac{1}{q}p^{-\nu}\frac{q(q-p)\cdots(q-(\nu-1)p)}{\nu!} = \frac{1}{p^\nu \nu!}(q-p)\cdots(q^{-(\nu-1)}p),$$

a polynomial in q of degree $\nu - 1 = [n/p] - 1$ with leading coefficient $\frac{1}{p^\nu \nu!}$. In case $n = \nu p + 1$, the contribution is the same.

(5.7) Next, consider term III and its m-summand

$$\frac{\varphi(m)}{2(q-1)}(Y_1+Y_2)^2(Y_1^m+Y_2^m)^\ell \quad \text{with } q-1=\ell\cdot m.$$

There is a contribution to $C(n,q)$ if and only if $n=km+0$, 1 or 2, and this contribution is

$$\begin{array}{ll} \frac{\varphi(m)}{2(q-1)}\binom{\ell}{k} & \text{for } n=km \text{ or } n=km+2, \text{ and} \\ \frac{\varphi(m)}{q-1}\binom{\ell}{k} & \text{for } n=km+1. \end{array}$$

Now $\frac{1}{q-1}\binom{\ell}{k}=\frac{1}{m^k k!}(q-1-m)(q-1-2m)\cdots(q-1-(k-1)m)$, a polynomial in q of degree $k-1$ with leading coefficient $\frac{1}{m^k k!}$.

If $\boxed{q \text{ is odd}}$ then $m=2$, $k:=\nu:=[n/2]$ yields a contribution which as a polynomial in q has maximal degree $\nu-1$, and that polynomial has leading coefficient $\frac{1}{2}\frac{1}{2^\nu\nu!}$ if n is even and $\frac{1}{2^\nu\nu!}$ if n is odd. Note that all the other possible choices of m and k yield expressions which as polynomials in q have degree strictly smaller than $\nu-1$.

If $\boxed{q \text{ is even}}$ then $m\geq 3$, and the contribution of term III to $C(n,q)$ is a polynomial in q of degree $\leq \frac{n}{3}-1<\nu-1$.

(5.8) Finally, we study the m-summand of term IV of (5.1),

$$\frac{\varphi(m)}{2(q+1)}(Y_1^m+Y_2^m)^\ell, \quad \text{where } q+1=\ell\cdot m,$$

and its contribution to $C(n,q)$. Such a contribution exists if and only if $n=k\cdot m$, and in this case is

$$\frac{\varphi(m)}{2(q+1)}\binom{\ell}{k}=\frac{\varphi(m)}{2m^k k!}(q+1-m)(q+1-2m)\cdots(q+1-(k-1)m).$$

If $\boxed{q \text{ is odd}}$ then $m=2$ yields a contribution if n is even. It is a polynomial in q of degree $\nu-1$, where $\nu=n/2$, with leading coefficient $\frac{1}{2}\frac{1}{2^\nu\nu!}$. If n is odd then the 2-summand of IV doesn't contribute to $C(n,q)$. If $m>2$ or q is even, the contribution is a polynomial in q of degree strictly smaller than $\nu-1$, where $\nu:=[n/2]$.

(5.10) As a conclusion we find: $C(n,q)$ is composed of 4 terms, where the first one, $|\overline{G}|^{-1}\binom{q+1}{n}$, is $f_n(q)$ with a polyomial $f_n\in\frac{1}{n!}\mathbb{Z}[X]$, while the sum of terms II, III, IV is $g_{n,\overline{q}}(q)$, where $g_{n,\overline{q}}(X)$ is a polynomial in $\mathbb{Q}[X]$ which depends only on n and the residue classes of q modulo all the $m\in\mathbb{N}$, $m\leq n$, that is, on the class $\overline{q}$ of q modulo

(5.11) $\lambda(n):=$ least common multiple of $\{m\in\mathbb{N}\mid m\leq n\}$.

5.12 Proposition. *The polynomial $g_{n,\overline{q}}$ has degree $\nu-1$ and leading coefficient $\frac{1}{2^\nu\nu!}$ with $\nu=\nu(n)=[n/2]$.*

Proof. If the characteristic p of $K = \mathbb{F}_q$ is 2, term II has by (5.6) the stated properties, while the terms III and IV have strictly smaller degrees by (5.7) and (5.8). If $p > 2$ and n is even, terms III and IV both have degree $\nu - 1$ and leading coefficient $\frac{1}{2}\frac{1}{2^\nu \nu!}$, while II has smaller degree.

If $p > 2$ and n is odd, III has degree $\nu - 1$ with leading coefficient $\frac{1}{2^\nu \nu!}$, while II and IV have smaller degrees. $\square$

We collect what has been proved.

5.13 Theorem. *Assume $n \geq 5$. The number $C(n, q)$ of G-inequivalent n-point configurations in $\mathfrak{X} = \mathbb{P}^1(K)$ may be described as*

$$C(n, q) = f_n(q) + g_{n,\overline{q}}(q)$$

with polynomials $f_n(X)$, $g_{n,\overline{q}}(X) \in \mathbb{Q}[X]$, where $g_{n,\overline{q}}$ depends only on n and the residue class $\overline{q}$ of q modulo $\lambda(n)$.

The degrees and leading coefficients are given by $\deg f_n = n - 3$, $\deg g_{n,\overline{q}} = \nu(n) - 1$, $\mathrm{lcoeff}(f_n) = \frac{1}{n!}$, $\mathrm{lcoeff}(g_{n,\overline{q}}) = \frac{1}{2^{\nu(n)}\nu(n)!}$. Here $\nu(n) = [n/2]$, $\lambda(n) = \mathrm{lcd}\{m \in \mathbb{N} \mid m \leq n\}$, $f_n(X) = \frac{1}{n!}(X-2)(X-3)\cdots(X-n+2)$, and the $g_{n,\overline{q}}$ are described in (5.6), (5.7), 5.8). $\square$

For $n = 5$, explicit expressions are given in Theorem 5.3.

The symmetry group $\mathrm{Aut}(C)$ of an n-configuration is a subgroup of S_n and therefore has bounded size for n given. We define for each divisor i of $n! = |S_n|$:

$$\begin{aligned} \mathcal{C}_i(n, \mathfrak{X}) &:= \{C \in \mathcal{C}(n, \mathfrak{X}) \mid |\mathrm{Aut}(C)| = i\} \\ C_i(n, q) &:= |\overline{G} \setminus \mathcal{C}_i(n, \mathfrak{X})| \end{aligned} \tag{5.14}$$

Then

$$\begin{aligned} \textstyle\sum_{i \geq 1} C_i(n, q) &= C(n, q) \text{ and} \\ \textstyle\sum_{i \geq 1} C_i(n, q) \frac{|\overline{G}|}{i} &= \binom{q+1}{n}, \end{aligned} \tag{5.15}$$

that is

$$\sum_{i \geq 1} \frac{C_i(n, q)}{i} = \frac{1}{|\overline{G}|}\binom{q+1}{n} = f_n(q). \tag{5.16}$$

By subtracting (5.16) from (5.15), we find

$$g_{n,\overline{q}}(q) = C(n, q) - f_n(q) = \sum_{i \geq 2}(1 - \frac{1}{i})C_i(n, q).$$

Now, as $\frac{1}{2} \leq 1 - \frac{1}{i} < 1$ for $i \geq 2$, we have

$$\frac{1}{2}\sum_{i \geq 2}(C_i(n, q) \leq g_{n,\overline{q}}(q) < \sum_{i \geq 2} C_i(n, q), \text{ i.e.,}$$

$$g_{n,\overline{q}}(q) < \sum_{i\geq 2} C_i(n,q) \leq 2g_{n,\overline{q}}(q). \tag{5.17}$$

Therefore $g_{n,\overline{q}}(q)$, the contribution of terms II, III, IV of (5.1) to $C(n,q)$, describes the order of magnitude of $C^{\mathrm{spec}}(n,q) := \sum_{i\geq 2} C_i(n,q)$, the number of G-classes of special n-configurations, where an n-configuration C is *special* if $|\mathrm{Aut}(C)| > 1$. Otherwise we call C *generic*.

5.18 Corollary. *Given $n \geq 5$, the number $C^{\mathrm{spec}}(n,q)$ is $O(q^{\nu(n)-1})$ with $\nu(n) = [n/2]$.* □

As the number $C(n,q)$ of all G-classes of n-configurations grows like $\frac{q^{n-3}}{n!}$, we may say that "most" classes are generic, i.e., have trivial symmetry groups, provided that $n \geq 5$. This doesn't hold for $n \leq 4$: see (3.10).

Concluding remarks. (i) It is conceivable that an analysis similar to the one of Section 4 may be performed for n-configurations with $n > 5$. However, the number $C^{\mathrm{spec}}(n,q)$ is polynomial in q of degree ≥ 2, and so a count similar to the one presented for $C^{\mathrm{spec}}(5,q)$ will turn out extremely difficult.

(ii) Our n-point configurations correspond to 2-colorings of $\mathfrak{X} = \mathbb{P}^1(\mathbb{F}_q)$. As explained in Section 1, the cycle index $Z_{G,\mathfrak{X}}$ also allows counting of 3,4,...-colorings modulo G-equivalence, which e.g. is relevant for the classification of algebraic curves covering $\mathbb{P}^1$ with distinct types of ramification. Some formulas for 3-colorings have been worked out in [2].

References

[1] M. Aigner: A Course in Enumeration. GTM 238, Springer-Verlag Berlin-Heidelberg 2007.

[2] M. Bohn: Punktkonfigurationen über endlichen Körpern. Bachelor's Thesis, Saarbrücken 2012.

[3] E. Bombieri and D. Husemöller: Classification and Embeddings of Surfaces. Proc. of Symp. in Pure Mathematics 29, Algebraic Geometry Arcata 1974, 329-420, AMS Providence 1975.

[4] E.-U. Gekeler: Automorphe Formen über $\mathbb{F}_q(T)$ mit kleinem Führer. Abh. Math. Sem. Univ. Hamburg 55, 111-146 (1985).

[5] M. Harris: Algebraic Geometry. GTM 133, Springer-Verlag Berlin-Heidelberg-New York 1992.

[6] R. Hartshorne: Algebraic Geometry. GTM 52, Springer-Verlag Berlin-Heidelberg-New York 1977.

[7] S. Lang: Introduction to Modular Forms. Grundlehren der math. Wiss. 222, Springer-Verlag Berlin-Heidelberg-New York 1976.

[8] D. Mumford: Geometric Invariant Theory. Ergeb. d. Mathematik 34, Springer-Verlag Berlin-Heidelberg-New York 1965.

[9] G. Polya: Kombinatorische Anzahlbestimmungen für Gruppen, Graphen und chemische Verbindungen. Acta Math. 68, 145-254 (1937).