SAPIENZA UNIVERSITÀ DI ROMA

Dipartimento di Matematica, Dipartimento di Metodi e Modelli Matematici per le Scienze Applicate

ISTITUTO NAZIONALE DI ALTA MATEMATICA "FRANCESCO SEVERI"

RENDICONTI DI MATEMATICA

E DELLE SUE APPLICAZIONI

Serie VII - Volume 30 - Fascicolo I - 2010

Le modalità per la presentazione dei lavori e le condizioni di vendita si trovano alla web page.

Submission of papers and subscription rate information could be found on the web page.

ADDRESS:
RENDICONTI DI MATEMATICA
DIPARTIMENTO DI MATEMATICA - PIAZZALE A. MORO, 2 - 00185 ROMA, ITALIA

Fax.: +39 06 49913052
e-mail: rendmat@mat.uniroma1.it
web page: www.dmmm.uniroma1.it/~rendiconti

Direttore Responsabile: Prof. ALESSANDRO SILVA

Autorizzazione del Tribunale di Roma del 22-11-2005 (n. 456/05)

Composizione tipografica effettuata con il programma TEX © dalla
CompoMat – Loc. Braccone – 02040 Configni (RI) – Telefax 39 0746 672240

Stampato a cura del *Centro Stampa d'Ateneo* della Sapienza Università di Roma

Rendiconti di Matematica, Serie VII
Volume 30, Roma (2010), 1–21

Primitive Semifields and Fractional Planes of order q^5

MINERVA CORDERO – VIKRAM JHA

Dedicated to Professor Marialuisa de Resmini

ABSTRACT: *The dimension of an affine plane π of order n, relative to a subplane π_0 of order m, is specified by $\dim_{\pi_0} \pi = \log_m n$. The exotic embeddings of a plane in another plane of the "wrong" characteristic, pioneered by H. Neumann, and systematically considered by de Resmini and her associates, yield planes with transcendental dimensions. On the other hand, infinitely many rational but non-integral dimensional, or fractional, planes were discovered relatively recently and all known examples of such planes are among semifield planes. Such semifield planes must have order $\geq p^5$, p prime. We show:*

Theorem A: Let π be a semifield plane of order p^5, that contains no fractional subplanes. Then for sufficiently large p, every semifield coordinatizing π is right primitive and left primitive.

Here, a semifield $(D, +, \circ)$ is considered right primitive if every non-zero element in D is the right principal power of some $\omega_R \in D$; left primitivity is defined analogously. G. P. Wene Conjectured that all fractional semifields are right primitive. If the fractional hypothesis on π is dropped, counterexamples to the Conjecture are known to arise in semifield planes of order 2^5 and 2^6, as shown by I. F. Rúa and I. R. Hentzel. These are the only known orders for which the Wene Conjecture fails. We provide further support for the Wene Conjecture.

Theorem B: All semifields coordinatizing semifield flock spreads are right primitive.

We also prove the 3-dimensional analogue of this result.

Theorem C: Let π be a semifield spread in $PG(5, q)$ such that $\pi \supset \mathcal{R}$, a regulus of degree $q + 1$ such that the shears axis $Y \in \mathcal{R}$. Then for all sufficiently large q, every semifield coordinatizing π is right primitive.

This result extends a Theorem of Rúa who showed that semifields D of order q^3 that are three-dimensional over the center Z, hence, by Menichetti's Theorem, are Albert semifields with center $GF(q)$, are right primitive and left primitive. The Theorem above is not restricted to such Albert systems.

KEY WORDS AND PHRASES: *Semifields – Spreads – Flocks – Loops – Translation planes*
A.M.S. CLASSIFICATION: 51A40, 17A35.

1 – Introduction

In this paper, we consider two properties of a finite affine plane π that might be considered as reflecting the extent to which π differs from, or is similar to, a Desarguesian plane of the same order. One of these properties, related to the "dimension" that π may have relative to its subplanes, identifies planes that have subplanes of unexpected orders. The other property, which is algebraic in nature, is concerned with the loop structure of the "best" planar ternary rings, that coordinatize any considered π. The basic question here is whether planar ternary rings that are "closest" to fields, viz., quasifields and semifields, have multiplicative loops that are "cyclic", hence share the "primitivity" property of finite fields.

We begin with a brief survey of the notion of dimension, and how it derives from Professor de Resmini's pioneering investigations concerning exotic embeddings of one plane in another.

– Fractional-Dimensional Planes

Bearing in mind that the dimension of a finite field $F = GF(q^n)$, over a subfield $K = GF(q)$, is the integer $\log_{|K|} |F|$, one may more generally define the dimension of an arbitrary finite plane with respect to any subplane. For our convenience we state the Definition for affine rather than projective planes.

DEFINITION 1.1. Let Π be an affine plane of order n, with an affine subplane Ψ of order m. Then the dimension of Π relative to Ψ is specified by $\dim_\Psi \Pi = \log_m n$.

In particular, Π has transcendental dimension, fractional dimension, or integer dimension, relative to Ψ, according to whether $\log_m n$ is transcendental, rational (but not an integer), or an integer.

Similarly if D is a planar ternary ring with a subplanar ternary ring E then $\dim_E D = \log_{|E|} |D|$; D is transcendental, fractional or integer dimensional, relative to E, according to whether $\dim_E D$ is transcendental, rational but not an integer, or an integer.

In the 1950's, H. Neumann [19], showed that any projective Hall plane Π of odd order contains Fano subplanes. It follows that infinitely many affine planes are transcendental dimensional over suitable subaffine planes.

PROPOSITION 1.2. *To each square integer p^{2n}, p an odd prime, corresponds an affine Hall plane Π that contains an affine Fano subplane Φ. Hence $\dim_\Phi \Pi = \theta$, a transcendental number.*

PROOF. Let π be a projective Hall plane of order p^{2n} and ϕ one of its Fano subplanes, whose existence is guaranteed by Neumann, ibid. Choose an affine Hall plane $\Pi = \pi^\ell$ such that the infinite line ℓ is a secant to a Fano plane ϕ, so $\Phi = \phi^\ell$ is a subaffine plane of Π. Hence $\dim_\Phi \Pi = \theta$ where θ satisfies the condition $2^\theta = p^{2n}$. But, by the Gelfond-Schneider Theorem, Schneider [22,23], if $1 < M < N$ are integers, then the equation $M^x = N$ is satisfied by $x > 0$ only if x is rational or transcendental. The result follows since $(2, p) = 1$. □

Following Neumann, Professor de Resmini pioneered what might be considered the study of planes admitting transcendental dimensions. She and her coworkers discovered spectacular examples of such phenomena. For instance, they showed that the Hughes plane of order 25, and also its derivative, the Ostrom-Rosati plane, admit subplanes of order 2 and 3, de Resmini and Puccio,[20], de Resmini and Leone, [17].

Further examples of transcendental affine planes have been obtained in this century by generalizing Neumann's contruction, Proposition 1.2. Thus, by carefully deriving Hall planes, so as not to lose at least one of its Fano subplanes, one obtains a range of translation planes, corresponding to subregular spreads, that contain Fano subplanes, as demonstrated by Fisher and Johnson, [7]. There are also other translation planes that are transcendental dimensional relative to suitable subplanes, Johnson [13].

Thus, transcendental dimensions signal an exotic embedding of one type of plane in a quite different type plane, one with the "wrong" characteristic. By way of contrast, if we consider any affine translation plane $\Pi = \pi^{\ell_\infty}$ (with ℓ_∞ the translation axis of π) of order p^n, then its dimension relative to any affine subplane Π_0, is always a rational number n/m, where p^m is the order of Π_0. Recent work, suggested by Theorems such as those indicated above, has concentrated on the contrasting question: are there planes that are neither transcendental-dimensional nor (as in the overwhelming majority of the known cases) integral-dimensional, that is: *Is it possible for a plane to be fractional dimensional?*

Until a very few years ago, only one fractional dimensional plane was known(1): the Knuth semifield plane of order 32. In the last five years or so, Wene discovered other sporadic examples of fractional dimensional semifield planes, again of characteristic 2. Then Johnson and the second author found infinitely many fractional-dimensional semifields, [11], again of even order. In recent work, the authors of the present paper have shown that infinitely many semifield planes of characteristic 3 are fractional dimensional, Cordero-Jha, [4].

In all these cases, the planes shown to be fractional-dimensional are among various classes of known planes (due to Knuth, Kantor, Coulter-Matthews, Ding-

(1) And possibly only to one person — R. J. Walker, who had classified the semifields of order 32, almost 50 years ago, in his independent verification of the Knuth classification of the semifield planes of order 32, [24].

Yuan, cf. the survey by Kantor, [15]). Thus, in the study of fractional dimensions, as for transcendental dimensions, the aim is not so much to find new planes, but to find subplanes Π_0 of possibly "known" planes Π, that have fractional (or transcendental) dimension, $\dim_{\Pi_0} \Pi$.

Note that *all known fractional-dimensional planes* Π *are semifield planes*, and they are only known to be fractional dimensional relative to some subsemifield plane Π_0 of order p^2. (Thus Π_0 is Desarguesian and its projective closure includes the shears point of Π.) In particular, by the Baer condition, Π has order $\geq p^5$.

Actually, this minimality condition concerning the existence of fractional sub-semifield planes Π_0, of a semifield plane Π, may be formulated more generally for semifield planes Π of order q^n that are n-dimensional over a central subplane[(2)], coordinatized by $GF(q)$. Thus, by the Baer condition:

REMARK 1.3. Let Π be a semifield plane of order q^n with center $GF(q)$ such that Π has fractional dimension relative to a subsemifield plane Π_0 that contains a central subplane of Π. Then the integer $n \geq 5$, and, when $n = 5$, the fractional subplane Π_0 has order q^2 (and hence must be Desarguesian).

COROLLARY 1.4. *A semifield plane of order p^n, p prime, is fractional dimensional relative to a subsemifield plane Π_0 only if $n \geq 5$ and, when $n = 5$, Π_0 has order p^2.*

NOTE. In all cases known to us, any fractional dimensional *translation* plane of order p^5 satisfies *all* the hypotheses of Corollary 1.4 above.

One of our main goals is to show that, in a suitable asymptotic sense, *semifield planes Π of order p^5, or more generally in the 'minimal' semifield planes of order q^5 considered in Remark 1.3, the absence of fractional subplanes guarantees that all the semifields D that coordinatize Π are "primitive"*, in a sense analogous to finite fields, see Corollary A, p.6, (also cf. Theorem 5.6 and Corollary 5.7). Before stating our result explicitly, we define primitivity and a related Conjecture of Wene, to which our result may be seen as an explicit contribution.

– Primitive Semifields and the Wene Conjecture

An algebraic, measure of how "close" a plane is to being Desarguesian is to examine the structure of the "best" planar ternary ring that coordinatizes the plane. We consider this approach when applied to the multiplicative loops of semifields (finite non-associative fields). Following Wene and others, [25, 26,

(2) The center of a semifield is a plane invariant, thus all semifields coordinatizing a plane have centers isomorphic to the same $GF(q)$.

21, 9], we consider whether finite semifields have "cyclic" multiplicative loops, in a sense analogous to fields but taking into account the non-associative nature of their multiplicative loops.

DEFINITION 1.5. Let $\mathcal{D} = (D, +, \circ)$ be a semifield. Then $\mathcal{D}$ is a right primitive semifield if the multiplicative loop $(D^*, \circ)$ contains an element $\omega \in D$ such that every $d \in D^*$ is a right principal power $d = \omega^{k)}$, for some $k \geq 1$, where $\omega^{i)}$ is defined recursively by

$$\omega^{1)} = \omega, \omega^{i+1)} = \omega^{i)} \circ \omega.$$

Similarly, $\mathcal{D}$ is left primitive if every element of $(D^*, \circ)$ is a left principal power $\mu^{(k}$, $k \geq 1$, where the left principal power $\mu^{(i}, i \geq 1$ are defined analogously:

$$\mu^{(1} = \mu, \mu^{(i+1} = \mu \circ \mu^{(i}, i \geq 1.$$

The semifield $\mathcal{D}$ is *primitive* if it is both left primitive and right primitive.

NOTE. One can define primitive and right/left primitivity in exactly the same way for arbitrary finite planar ternary rings. The authors have shown, [3], that there are infinitely many finite quasifields (coordinatizing translation planes) that are primitive, and also infinitely many finite quasifields that are not primitive.

On the basis of a specific class of semifields and some computer-based investigations of small cases, Wene [25, 26] suggested:

CONJECTURE 1.6. (Wene, [26]) Every finite semifield is right primitive.

Rúa, [21], has shown that Conjecture 1.6 is false for the Knuth commutative semifield of order 32: this is neither left primitive nor right primitive. Moreover, Rúa also showed (ibid.) that some of the semifields of order $n = 2^5$ are left primitive but not right primitive and vice-versa (by duality). Hentzel and Rúa, [9], have established that the Wene Conjecture 1.6 does not hold for some semifields of order $n = 2^6$, and again there are semifields of order 64 that are left primitive but not right primitive and vice versa. But there are no known violations of the Wene conjecture for semifields of order $n \neq 2^5, 2^6$.

Since semifields of order q^2 with center $\supseteq GF(q)$ are fields, the first case of interest are semifields of order q^3 with center $GF(q)$. All such semifields are known: they are either fields or the twisted fields of Albert, as established by a celebrated Theorem of Menichetti [18]. Rúa, [21], has shown the Wene conjecture holds for these semifields. The present author's have given a different proof of Rúa's Theorem, Cordero-Jha, [3], without assuming Menichetti's classification, [18].

In this paper, one of our main concerns is whether 5-dimensional semifields, with center $GF(q)$, are primitive. Note that Menichetti's Theorem does not apply here since the Coulter-Matthews and the Ding-Yuan commutative semifields,

[15], have orders 3^n, $n \geq 5$ odd; also, the failure of the Wene conjecture for the case 2^5 needs to be taken into account.

The Knuth commutative semifield D of order 2^5, which violates the Wene Conjecture 1.6, coordinatizes a fractional dimensional semifield plane. On the other hand, the Coulter-Matthews plane of order 3^5 is fractional dimensional but does not violate the Wene conjecture.

Thus, part of the motivation for this paper was to examine how these facts concerning semifields of order p^5, which seem to be pulling in opposite directions, may be reconciled. Thus, we established the following asymptotic result.

COROLLARY A. (cf. Corollary 5.7) *For all sufficiently large primes p, the semifields coordinatizing a semifield plane Π of order p^5 are all primitive (right and left) if Π does not contain any proper subplane Π_0 of order $> p$.*

NOTE.

(1) More generally, cf. Theorem 5.6, suppose $q = p^r$, with r fixed. Then **there is an integer N_r such that for all $p > N_r$ any semifield plane Π of order q^5 with center $GF(q)$ is coordinatized only by semifields that are (left and right) primitive, whenever Π has no fractional subplanes.**
(2) In the p^5-case the non-existence of fractional subplanes is equivalent to the assertion that Π has no proper subplanes.
(3) It is conceivable that the theorem holds for all primes p, rather than for "sufficiently large" p. (Although the commutative semifield plane of order 2^5 admits coordinatization by a non-primitive semifield, the corresponding Knuth plane admits fractional subplanes, so the hypothesis of the above corollary does not apply.)

The key to the proofs of our results is the structure of the slope maps of *regulus* quasifields of low-dimension.

– Primitivity of Low-Dimensional Regulus Semifields

So far we have considered semifields D that have dimension n over the *center* $K = GF(q)$. We now turn to the more general case when K is the subfield of the left nucleus $N_\ell(D)$, or *kern*, that commutes multiplicatively with D. We refer to such subfields as regulus subfields of D. Every semifield is a regulus semifield over its central fields, but often has other regulus subfields as well.

DEFINITION 1.7. Let D be a semifield with a subfield

$$K = \{k \in N_\ell : k \circ d = d \circ k \forall k \in N_\ell\}.$$

If $\dim_K D = n$, then D is a *regulus semifield* of dimension n relative to the regulus subfield K.

NOTE.

(1) Every semifield D of order p^n is a regulus semifield over every subfield in the center $Z(D)$, hence over $GF(p)$.
(2) More generally, *a quasifield Q is a regulus quasifield if its kern contains a subfield K that commutes with K multiplicatively.* We determine the slope structure of Q for the cases $\dim_K Q \leq 5$, $k \neq 4$, cf. Theorem 3.8, and use the information to establish the right primitivity of semifields of dimension $n \leq 5, n \neq 4$.
(3) The n-dimensional regulus semifields D, of order q^n over a regulus field $GF(q)$, are precisely the semifields that coordinatize a semifield spread $\mathcal{S} < PG(2n-1,q)$ such that there is a regulus $\mathcal{R} \subset \mathcal{S}$ of degree $q+1$ with the shears axis $Y \in \mathcal{R}$.
(4) The 2-dimensional regulus semifields are precisely the semifields that coordinatize the flock semifields in $PG(3,q)$, *e.g.*, Gevaert and Johnson, [8]. Infinitely many 2-dimensional regulus semifields exist (including the Kantor-Knuth semifield flocks). Only the semifield flocks of even order q have been classified: the corresponding 2-dimensional regulus semifields are fields, *i.e.*, the flocks are linear, Johnson [14]. Thus for odd q only, the 2-dimensional *regulus* semifields form a strictly larger class than the 2-dimensional *central* semifields (which are merely fields). Moreover, each non-linear flocks is coordinatizable by several non-isomorphic regulus semifields.
(5) Although the semifields D of dimension 3 over the center $GF(q)$ have been classified by Menichetti, the 3-dimensional *regulus* semifield planes have not been classified.

By considering 2-dimensional regulus semifields and using note (4), we will show:

THEOREM. (cf. Corollary 7.3) *All the semifields coordinatizing conical flocks are right primitive.*

NOTE. The duals of non-linear flock semifields are not flock semifields, unless the semifields are fields. Hence, we may only assert that the duals are left primitive: we do not know if they are right primitive.

For dimension 3 we prove an extension of Rúa's Theorem: thus we prove Wene's Conjecture, Conjecture 1.6, for *regulus* semifields that are 3-dimensional over a regulus field $GF(q)$, provided q is large enough.

THEOREM. (cf. Theorem 6.2) *Let π be a semifield spread in $PG(5,q)$ such that $\pi \supset \mathcal{R}$, a regulus of degree $q+1$ such that the shears axis $Y \in \mathcal{R}$. Then for all sufficiently large q, every semifield coordinatizing π is right primitive.*

The above are proved by determining the slope maps of regulus quasifields for dimension ≤ 5 (but not dimension 4 — where different arguments seem necessary), cf. paragraph 3. These results are implicit in Theorem 3.8, and the argument used in proving it.

2 – Preliminaries

We assume the reader to be familiar with affine translation planes and their coordinatization by quasifields, particularly semifields, [10], and their connections with spread sets and spreads, *e.g.*, [12, pp. 36–48], or [1]. To fix our notation, particularly in regard to the non-standard notion of a "regulus" quasifield/semifield, we recall some terminology. Quasifields obey the right distributive law: $(a+b)\circ c = a\circ c + b\circ c$.

DEFINITION 2.1 **(Slope Maps and Regulus Quasifields)** Let Q is a finite quasifield. Then its kern is the field

$$\{k \in Q : \forall a, b \in Q : k\circ(a+b) = k\circ a + k\circ b, k\circ(a\circ b) = (k\circ a)\circ b\},$$

and any (sub)field $K \cong GF(q)$ of Q is a *kern (sub)field* of Q; now $|Q| = q^n$ for some integer $n \geq 1$, since Q is a K vector space.

The *slope* [map] of any non-zero $m \in Q$ is $T_m \in GL(Q, K)$ specified by $T_m : x \mapsto x\circ m, x \in Q$. Thus, T_m may (when convenient) be identified with a non-singular K-matrix of order $n \times n$, which depends on the choice of the K-basis for Q. Also the *slope set* for Q (regarding T_0 as is the zero map) is $\tau_Q = \{T_m : m \in Q\}$.

If the slopes of the elements $k \in K$ are the scalar elements $k\mathbf{1}_5$, then Q is a *regulus quasifield*, and K a *regulus* subfield. (Equivalently, a kern field K is a regulus field if each $k \in K$ commute multiplicatively with every $d \in Q$.)

NOTE. The regulus quasifields, as described above, are the quasifield that coordinatize the spreads $\mathcal{S}$ in $PG(2n-1, q)$ that contain a regulus $\mathcal{R}$ of degree $q+1$: regulus quasifields arise when the coordinatizing triad of components defining the quasifield are selected from among the components in any regulus $\mathcal{R} \subset \mathcal{S}$.

The above attributes of quasifields and semifields are also assigned to the spread sets that they define.

DEFINITION 2.2. Let V be a vector space of dimension n over a field $K \cong GF(q)$, $q = p^r$. Then a set of linear maps

$$\tau \subset GL(V, K) \cup \{\mathbf{0}_n\} := \overline{GL(n, K)},$$

is a *spread set* on the K-space V if $|\tau| = |V| = q^n$, $\tau \supset \{\mathbf{0}_n, \mathbf{1}_n\}$, and

$$A, B \in \tau \implies A - B \in GL(n, K).$$

(1) τ is a *regulus* spread-set if $\tau \supset \mathcal{K}$, where $\mathcal{K} = k\mathbf{1}_n : k \in K$.
(2) τ is *additive* if it is closed under addition (equivalently, τ is an additive group of order $|V|$, with all non-zero elements non-singular and including $\mathbf{1}_V$).
(3) An additive spread set τ is *linear* if τ is a K-subspace of the ring $\mathrm{Hom}(V, +, K)$.

The following properties relating quasifields/semifields to their spread sets are obvious.

REMARK 2.3.
(1) If Q is a quasifield then its slope set τ_Q is a spread set.
(2) If Q is a regulus quasifield, relative to a field K, then τ_Q is a regulus spread set, *i.e.*, τ_Q contains the scalar subfield $\mathcal{K} \cong K$.
(3) If $(D, +, \circ)$ is a semifield containing a field $K \subset N_\ell(D)$ then
   (a) $\tau_D \subset GL(D, K) \cup \{\mathbf{0}\}$ is an additive spread set;
   (b) If D is a regulus semifield over K then the additive spread set τ_D is a K-regulus spread set;
   (c) If D has K in its center (so K is a subfield of the nucleus $N(D) = N_\ell(D) \cap N_m(D) \cap N_r(D)$ such that D centralizes K multiplicatively) then τ_D is a K-linear vector space.

Note that an obvious "converse" of each part of Remark 2.3 is also valid, but we shall only use the fact that every additive spread set is the slope set of a semifield, cf. Remark 4.1.

3 – Slope Map Structure for 5-Dimensional Regulus Quasifields

The slope maps of the non-zero elements of an n-dimensional quasifield Q, over a kern field $K = GF(p^r)$, are elements of $GL(n, q)$. Constraints on the permitted structure of the non-zero slope maps $A \in \tau_Q$ obviously influences the structure of Q, hence also on the geometry of the associated translation plane. We consider the case when Q is a regulus quasifield over K, so

$$\tau_Q \subset GL(n, K), \tau_Q \supset \mathcal{K} = \{k\mathbf{1}_n : k \in K\}.$$

When $n = 3$, we showed, in, [3], that each non-scalar maps $A \in \tau_Q$ is irreducible, thus yielding an alternative proof to Rúa Theorem, establishing the primitivity of all semifields of order q^3 with center $GF(q)$. The key step was to show $(|A|, p) = 1$.

Here we consider the analogous problem for regulus quasifields Q of order q^5. It turns out, that now there are more possibilities than in the q^3-case: A still has order relatively prime to p, but A might not be irreducible. Our goal here is to describe the slope structure for 5-dimensional regulus quasifields, Definition

2.1; in a later section we will specialize to the case when Q is a semifield to obtain a criterion for Q to be a fractional semifield.

We begin with some Lemmas without imposing the dimensional restriction. Thus, we consider a quasifield Q of order q^n, characteristic p, that contains a regulus subfield $K = GF(q)$.

LEMMA 3.1. *Let A be a slope map of a regulus quasifield Q over $GF(q)$, Definition* 2.1. *Then A cannot leave invariant any one-space over $GF(q)$, unless A is one of the scalar slopes of Q.*

PROOF. Otherwise, A has a $GF(q)$-eigenvector, and hence a corresponding eigenvalue λ in $GF(q)$. So there is a matrix X such that XAX^{-1} is a matrix with first column λe_1, and now $X(A-\lambda I_n)X^{-1}$ is singular, hence so is $A-\lambda I_n$, which means A and λI_n cannot both be slope maps in the same spread set unless $A = \lambda I_n$. □

We use $\langle A\rangle$ to denote the multiplicative group generated by any non-singular matrix A.

COROLLARY 3.2. *Let Q be a regulus quasifield over a subfield K. Let A be the slope map of any element of $Q \setminus K$. Then, regarding Q as a vector space over K:*

(1) *A does not fix any one-space or hyperplane of Q.*
(2) *No subgroup S of $\langle A\rangle$ fixes a unique one-space or a unique hyperplane of Q.*

PROOF. Consider the first part. Lemma 3.1 states A cannot fix a one-dimensional K-space. Hence A cannot fix a hyperplane, since the number of fixed one-spaces is the number of fixed hyperplanes, *e.g.*, [5, 12, p. 81]Dembowski. The second part follows since $\langle A\rangle$ is abelian. □

Unless the contrary is indicated, A denotes the slope of some element of the quasifield Q that does *not* lie in the scalar field $I_nK = GF(q)$. So the cyclic group $\langle A\rangle = P \oplus R$, where P denotes the (possibly trivial) p-Sylow subgroup of $\langle A\rangle$ and R is its Hall p'-subgroup. Much of our effort will be devoted to showing that P is often the trivial group. As a default assume P is non-trivial, so $Fix(P) := F_P$ is a non-trivial K-subspace of Q. So R, which centralizes P, leaves F_P invariant. We count the set of Maschke R-complements of F_P.

LEMMA 3.3. [# P-complements] *Suppose P is non-trivial, with fixed space F_P. Then for some integer $k \geq 1$, R has kp distinct Maschke-complements C of P, on the K-space Q. Also, R is completely reducible on F_P*

PROOF. Note that P can't leave invariant any R-complement C of F_P, since P would then fix non-zero points on C. Hence each of the Maschke complements of F_P, for the p'-group R, must lie in a non-trivial P-orbit. The final sentence holds because R is a p'-group that leaves F_P invariant. □

COROLLARY 3.4. 1) *R cannot fix a 1-space in F_P;* 2) *F_P cannot be a 1-space.*

PROOF. 1) Suppose R fixes a 1-space of F_P. Then so does A since R and P must both fix this space and hence so must the group they generate, viz., $A \in R \oplus P = \langle A \rangle$. But now the eigenvalue argument, Lemma 3.1, yields a contradiction so 1) follows. Part 2) is a special case since A, hence also R, leaves F_P invariant. □

Up to now we have not imposed any restrictions on the dimension on the dimension of regulus quasifield Q. For the remainder of the section we restrict ourselves to the 5-dimensional case: Thus, *Q is a quasifield of order q^5 with a regulus subfield K such that $dim_K Q = 5$, so $|Q| = q^5$.* So by Corollary 3.2 above, we may assume F_P has rank three or two: we consider each case in turn.

– **Case: F_P has rank 3.**

We require a Corollary to:

LEMMA 3.5. *Suppose $(m, n) = 1$ and that q is any prime power. Then an irreducible abelian group $G < GL(n, q)$ cannot be isomorphic to an irreducible subgroup of $GL(m, q)$.*

PROOF. Since G is abelian, by Schur's Lemma G is in a field $GF(q^n)$, but not in any subfield of it. Hence $|G|$ divides $q^n - 1$ but not $q - 1$. However,

$$(q^m - 1, q^n - 1) = q^{(m,n)} - 1 = q - 1,$$

shows that $|G|$ does not divide $q^m - 1$, the order of the multiplicative subgroup of $GF(q^m)$. However, if G were an abelian irreducible subgroup of $GL(m, q)$ then, by Schur again, G would also be an irreducible subgroup of $GF(q^m)$, contradicting the fact that $|G|$ does not divide $q^m - 1$. □

COROLLARY 3.6. *For any prime power q, an irreducible abelian subgroup G of $GL(3, q)$ cannot be isomorphic to any subgroup of $GL(2, q)$.*

PROOF. By the Lemma above, we need merely exclude the possibility that G acts reducibly on the vector space $V_2(q)$. By Maschke, G diagonalizes hence $|G|$ divides $(q-1)^2$, contradicting the irreducibility of G on $V_3(q)$. □

If R fixes a one-space on $Fix(P)$ then so does A, contradicting Corollary 3.2. If R fixes a 2-space T in $Fix(P)$ then it still fixes a one-space, the Maschke complement of T in $Fix(P)$, so we have the same contradiction. Hence R acts irreducibly on $Fix(P)$. Now any R-complement S of F_P, has rank two, and since, by Corollary 3.6, R cannot be faithful on a two-space, being irreducible on a 3-space, a non-trivial subgroup R_1 of R fixes S elementwise. Hence $S_1 = Fix(R_1) \geq S = Fix(R)$ is P-invariant. There are the following cases to consider: i) $S_1 = S$ implies P leaves S invariant and hence fixes non-zero vectors in S contradicting the fact that S is a complement to F_P; ii) $S_1 > S$ so $S_1 \cap F_P$ is a non-trivial proper subspace of F_P since $S \oplus F_P = Q$, and now we contradict the fact that S acts irreducibly on F_P. So the case F_P has rank 3 can never occur.

– **Case: F_P has rank 2.**

By Corollary 3.2 again, R has at least p distinct Maschke complements of the subspace F_P. Since these have rank 3 any two of them, say X and Y, must intersect. Now if $H := X \cap Y$ has rank 2 then $X + Y$ has rank 4, and either $X + Y$ intersects F_P in a one-space, contrary to the eigenvalue argument, or F_P is a rank 2 subspace of the 4-space $X + Y$ and now F_P is too large to be in a complement of X in $X + Y$: recall this is required because F_P has X as a complement.

Thus, H must have rank one, and $F_P < X + Y$, since $X + Y$ has rank 5 because $H = X \cap Y$ has rank one. Since R fixes H, a rank one-space, and R acts irreducibly on F_P, by the eigenvalue argument, we conclude $H \cap F_P$ is trivial. But since now R is irreducible on the rank 2 vector space F_P, of order q^2, and moreover the rank one vector space H of order q is R invariant, it follows that a non-trivial subgroup R_1 of R acts trivially on H, since no scalar group, hence of order dividing $q - 1$, can be irreducibly on F_P since this is 2-dimensional over $K = GF(q)$. Note that since the p-group P, centralizes $R_1 < R$, P must leave $F_1 = FixR_1$ invariant, and hence fix non-zero points on it. Hence $F_1 \cap F_P \neq 0$. If $F_1 \cap F_P$ is a one-space then R fixes this one-space, a possibility already excluded (because A, generated by R and P, would be forced to fix this one-space, contrary to Corollary 3.2). Hence $F_1 \geq F_P$ but then $F_1 > F_P$, since $F_1 > H$ and $H \cap F_P = 0$.

Hence F_1 must have rank 3: otherwise R_1 fixes a hyperplane elementwise which is A-invariant, since R_1 is centralized by A, contrary to Corollary 3.2(1). Now if R leaves invariant at least two rank-one subspaces of F_1 that complement F_P, say C_i, $i = 1, 2$, then $C_1 \oplus C_2$ meets F_P in a rank-one subspace fixed by R, contradicting the fact that R is irreducible on the 2-space F_P. Thus R leaves

invariant the unique complement C of F_P in F_1. Since A centralizes R_1, it leaves F_1 invariant, and hence the unique complement C of F_1, contrary to Corollary 3.2. So F_P is not a rank 2 space.

Hence, since we have ruled out all putative dimensions for F_P, we have shown the order of A is not divisible by p:

PROPOSITION 3.7. *A is a p'-element in all cases, i.e. $\langle A\rangle = R$.*

So either (1) A is irreducible, or (2) A has a $3+2$-split, Corollary 3.2. So we have

THEOREM 3.8. *Let D be a quasifield of order q^5, with regulus field $K = GF(q)$. Then the order of any slope map $A := T_d$, for $d \in D \setminus K$, is not divisible by p. Hence any A is either scalar, irreducible or has a decomposition into irreducible subspaces $V_3 \oplus V_2$, where V_d denotes a K-subspace of D with rank d.*

COROLLARY 3.9. *The slope-map $A = T_d$ not reducible if and only if $|A|^{q^5-1} = 1$.*

PROOF. If A is irreducible or scalar then A lies in $GF(q^2)$, hence in both cases $|A|^{q^5-1} = 1$. If A is reducible but non-scalar then by Theorem 3.8 $A|V_3$ is irreducible hence by Schur's Lemma $|A|$ is divisible by a p-primitive divisor v of q^3-1. But since $(q^3-1, q^5-1) = q-1$, it follows that $|A|^{q^5-1} \neq 1$. □

4 – Primitive Spread Sets

Any spread set is the slope set of some quasifield. The case when the spread set is additive is of special relevance:

REMARK 4.1. Let $\mathcal{S} \subset GL(V,K) \cup \{\mathbf{0}\}$ be an additive spread set, on the finite vector space $(V,+)$ over a field K. Then for each non-zero choice of $e \in V$, there is a semifield $\mathcal{D}_e = (V,+,\circ)$ with slope set $\mathcal{S}$, and multiplicative identity e.

PROOF. Define $x \circ y = xT_y$, where $T_y \in \mathcal{D}$ is chosen such that $y = eT_y$. □

NOTE.

The semifields D_e, as e varies over V^*, are all isomorphic only if $\mathcal{S}$, equivalently D_e, are all fields.

Suppose D_e is a semifield, coordinatizing a semifield plane Π, when the unit point e is chosen on (fixed) unit line Z. The following Lemma implies that if D is right primitive then all the semifields D_f, based on choosing unit point $f \in Z$,

are right primitive, cf. Corollary 4.4. The Lemma will be used in the proof of our main result, Theorem 5.6.

LEMMA 4.2. *Let $\mathcal{S}$ be an additive spread set of order q^n, over any finite field $K = GF(q)$. Then the following are equivalent*

(1) *Some $\Omega \in \mathcal{S}$ has order $q^n - 1$.*
(2) *Every semifield D with slope set $\tau_D = \mathcal{S}$ is right cyclic.*
(3) *Some semifield D with slope set $\tau_D = \mathcal{S}$ is right cyclic.*

PROOF. (1) $\Longrightarrow$ (2). Some $\Omega \in \mathcal{S}$ has order $q^n - 1$. Let D be any semifield with slope set $\tau_D = \mathcal{S}$, and multiplicative identity e. Let $e\Omega = \omega$. Thus, by Remark 4.1,

$$\begin{aligned} e \circ \omega, (e \circ \omega) \circ \omega, ((e \circ \omega) \circ \omega) \circ \omega, \ldots &= e\Omega, (e\Omega)\Omega, ((e\Omega)\Omega)\Omega, \ldots \\ &= e\Omega, e\Omega^2, e\Omega^3, \ldots, e\Omega^{p^n-1}, \ldots \end{aligned}$$

However, since the cyclic group $\langle \Omega \rangle \subset GL(n, K)$ is the multiplicative group of a matrix field $\cong GF(q^n)$, the group $\langle \Omega \rangle$ is sharply 1-transitive on the non-zero elements of the K-space K^n. So the above sequence imcludes all the $p^n - 1$ non-zero elements of K^n, which means the right powers of ω:

$$\omega, (\omega \circ \omega), ((\omega \circ \omega)) \circ \omega, (((\omega \circ \omega)) \circ \omega) \circ \omega, \ldots,$$

run over all of D^*: so D is right primitive. Thus, (1) $\Longrightarrow$ (2) holds. (2) $\Longrightarrow$ (3) is immediate. (3) $\Longrightarrow$ (1). Suppose D is right primitive, and $\tau_D = \mathcal{S}$ its slope set. Let ω be a right primitive element of D, and $\Omega = T_\omega$ be its (right) slope map. Then, as above, it is easy to see that Ω has order $p^n - 1$.

Since right primitive semifields are those that admit a primitive matrix as a slope map, Lemma 4.2(1), and the fact that duals of right primitive semifields are left primitive Lemma 4.2 yields:

COROLLARY 4.3. *Let Π be a semifield plane. Then the following conditions are equivalent.*

(1) *All semifields D coordinatizing Π are right primitive.*
(2) *All semifields D coordinatizing the dual plane of Π are left primitive.*
(3) *All semifields D coordinatizing Π^t the transpose plane of Π are right primitive.*

As indicated earlier, p.5, the work of Rúa, and Hentzel-Rúa, [21, 9], shows that left primitivity and right primitivity for a semifield are not mutually equivalent concepts, for semifields, of order 16 and 64. Lemma 4.2, suggests a possible approach for finding further examples. Thus, applying Lemma 4.2 to a commutative semifield D which is right primitive, hence also left primitive, we obtain a chain of semifields of type:

left & right primitive $\rightarrow$ right primitive [transpose]$\rightarrow$ left primitive [dualize],

and the middle semifield might only be right primitive in which case the final semifield would be left primitive but not right primitive.

Lemma 4.2 also yields the following geometric characterization of planes all whose coordinatizing semifields are right primitive semifields.

COROLLARY 4.4. *Let Π be an affine semifield plane with shears axis Y. Suppose Π is coordinatized by a semifield based on choosing any axis $X \neq Y$ as the x-axis and unit point $e \in Z$, where $Z \notin \{X, Y\}$ is any fixed line through $O = X \cap Y$. Then the semifield D_e coordinatizing Π with the above choices is primitive iff every semifield D_f, based on unit point $f \in Z \setminus \{O\}$, is right primitive.*

PROOF. Interpret the claim in terms of spreads. Thus π is a spread specified by a spread set $\mathcal{S}$ such that line Z is identified with $y = x\mathbf{1}$, $\mathbf{1} \in \mathcal{S}$. Now the semifields D_f and D_e have the same slope set. □

5 – Proof of Main Theorem

In this section we prove Theorem 5.6 . The proof of the following Lemma implicitly describes a technique for detecting fractional subplanes of a given semifield plane. Given a 5-dimensional semifield D, not necessarily fractional, with slope set τ_D, the Lemma shows how to replace D by a fractional semifield D', such that D' is fractional and $\tau_{D'} = \tau_D$, whenever such a D' exists. An elaboration of this method is used to construct fractional dimensional planes of odd order in Cordero and Jha, [3]. Note that the argument makes crucial use of the fact that D is 5-dimensional over a subfield field $K = GF(q)$ in the *center* of D, rather than merely requiring that D be a regulus subfield over K.

LEMMA 5.1. *Let $\mathcal{D} := (D, +, \circ)$ be a 5-dimensional semifield over its center $K = GF(q)$, with slope-set $\mathcal{S} \subset GL(D, K)$. Then either there is a fractional semifield $\mathcal{D}^* := (D, +, *)$ relative to a field $(F, +, *) \cong GF(q^2)$, with center $Z(\mathcal{D}^*) \subset (F, +, *)$, such that $\mathcal{S}$ is also the slope-set of $\mathcal{D}^*$, or every non-scalar element $m \in D \setminus K$ has irreducible slope map $T_m \in \mathcal{S}$.*

PROOF. Suppose the irreducible condition fails. So there is an $m \in D \setminus K$ such that its slope-map $A := T_m$ is not irreducible. Then by Theorem 3.8, A admits a decomposition $V_2 \oplus V_3$, where V_2 and V_3 are irreducible A-invariant subspaces of D that, as K-subspaces, are of dimensions 2 and 3 respectively. By Remark 2.3((c)), $\mathcal{S}$ is closed under both addition, and *multiplication* by the scalar field $\mathcal{K} \subset \mathcal{S}$, $\mathcal{K} \cong GF(q)$. So $\mathcal{S} \supset \mathcal{K} + \mathcal{K}A$, and this additively closed partial spread set, of size q^2, leaves V_2 invariant and hence, by counting, $\mathcal{K} + \mathcal{K}A$ clearly induces an additive spread on V_2. Fix any non-zero $e \in V_2$. Then, cf. Remark 4.1, define a new semifield $(D, +, *)$ by the rule $x * y = x\theta_y$ where $\theta_y \in \mathcal{S}$ such that $e\theta_y = y$. It is straightforward to verify that $(D, +, *)$ is a semifield with center $(K, +, *)$, and obviously $\tau_{D^*} = \tau_D = \mathcal{S}$. Moreover, since V_2 is invariant under $\mathcal{K} + \mathcal{K}A \subset \mathcal{S}$, $(V_2, *)$ is multiplicatively closed, hence by finiteness, the multiplicative loop of $(D^*, *)$ induces a loop on $(V_2, *)$. Thus $(D, +, *)$ is a semifield with a sub-semifield $(V_2, +, *)$. Put $K_2 = (e)\mathcal{K}$ and observe that $V_2 \supset K_2$ and that K_2 is in the center of $(D, +, *)$: K_2 is actually the full center of $(D, +, *)$, by the Baer condition. Thus, since $\dim_{K_2} V_2 = 2$, V_2 must be a field, since semifields that are 2-dimensional extensions over a field are field. So choosing $F := V_2$, completes the proof. □

We require a fundamental Theorem of Davenport, which we describe using the following:

NOTATION 5.2. Let F be finite field. So for any subfield $G < F$, and $x \in F^*$ the ring $G[x]$, of x-polynomials over G, is the subfield of F generated by $G \cup \{x\}$. We consider $G[x]$ to be the FIELD GENERATED BY x OVER G.

RESULT 5.3.(Davenport, [6, Theorem 1].) There exists a positive integer function, $\delta : \mathbb{P} \to \mathbb{P}$, such that in any field $F = GF(p^k) > GF(p) = Z_p$, for $k \leq r$ the following holds: if $\theta \in F$ generates F over Z_p then there exists $\alpha \in Z_p$ such that $\theta - \alpha$ is a primitive element of F.

We require a consequence of this result for which the subfield chosen is not necessarily Z_p. The proof makes extensive use of notation 5.2.

LEMMA 5.4. *Let $F = GF(q^d) > GF(q) = K$, where d is prime and $q = p^r$, and assume that the prime $p > \delta(rd)$. Then to each $t \in F \setminus K$ correspond $\alpha, \beta \in K$ such that $\beta t + \alpha$ is a primitive element of F.*

PROOF. Let $Z_p \leq K$ be the prime subfield of F. Since the dimension $[F : K] = d$ is prime, for any $T \in F \setminus K$ we have $F = K[T]$. Let $F_T = Z_p[T] = GF(p^t)$ for some $t > 1$. By Davenport, result 5.3, $T + z$ is a primitive element of F_T, hence the result holds unless neither of the fields K and F_T contains the other field. So $T + z \notin K$, hence without loss of generality we may assume T itself is a primitive element of F_T. Let ω be a primitive element of the maximal subfield K, so $T\omega$ is not in $K \cup F_T$, and $(p^r - 1)(p^t - 1)$ is an exponent of $T\omega$. We concentrate on the main case:

Case: Neither K nor F_T has order p^2 when $p+1=2^x$.

Let ρ and τ be respectively p-primitive divisor of p^r-1 and p^t-1. Now ω^{p^t-1}, a power of ωT, has order divisible by ρ; for if not then ρ divides p^t-1 so an element of F_T is a generator of K, over Z_p, so $F_T > K$ a contradiction. Hence $Z_p[\omega^{p^t-1}] = K$, so $Z_p[\omega T] \supseteq K$.

By a similar argument, T^{p^s-1}, also a power of ωT, has order divisible by τ (otherwise τ divides p^s-1 and K contains an element of order τ so $K \supseteq F_T$, a contradiction), and hence $Z_p[\omega T] \supseteq F_T$.

Hence we have shown the field $Z_p[\omega T]$ includes $K \cup T$, hence, since K is maximal in F, $F = Z_p[\omega T]$. But now by Davenport again, result 5.3, for some $\alpha \in Z_p$, $\omega T + \alpha$ is a primitive of F. This is the required result.

We turn to the exceptional case when one of the fields K or F_T has no p-primitive divisors. Note that since p is large we may assume $p > 64$. Thus we need only consider:

Case: $p+1=2^x$, and exactly one of $K, F_T \cong GF(p^2)$.

Consider the case $K = GF(p^2)$, $p+1=2^x$, and $F_T = GF(p^t)$, $t > 1$ odd. So ωT has exponent $(p^2-1)(p^t-1)$, and $(\omega T)^{(p^t-1)} = \omega^{(p^t-1)}$. But since $\gcd(p^2-1, p^t-1) = p-1$, implies $p^t-1 = (p-1)\nu$, ν an odd integer > 1, it follows that $\omega^{(p^t-1)} = \omega^{(p-1)\nu} \notin Z_p$, since $\omega^{(p-1)\nu}$ is a 2-element, of order $p+1$. Hence $K = Z_p[\omega^{(p^t-1)}] \subseteq Z_p[\omega T]$.

It remains to rule out the case $K = GF(p^w)$, and $F_T = GF(p^2), p+1=2^x$, $t > 1$ odd. Arguing as before, $p^t-1 = (p-1)\nu$, ν odd, and now ωT has exponent $(p^2-1)(p^w-1)$, so $(\omega T)^{(p^w-1)} = T^{(p^w-1)}$, where $T^{(p^w-1)} = T^{(p-1)\nu} \notin Z_p$. Hence $F_T = Z_p[T^{(p^w-1)}] \subseteq Z_p[\omega T]$. □

We will use the special case of the Lemma, when $F = GF(q^5)$.

Corollary 5.5. *Let $F = GF(q^5) > GF(q) = K$, where $q = p^r$. Then there is a function $\Delta(r), r \in \mathbb{P}$, such that for all $p > \Delta(r)$, to every $t \in F \setminus K$ correspond $\alpha, \beta \in K$ such that $\beta t + \alpha$ is a primitive element of F.*

Theorem 5.6. *Let Π be any semifield plane of order q^5 with center $GF(q), q = p^r$, with r fixed. Suppose the prime $p > \Delta(r)$, where the function Δ is a Davenport function, as in Corollary 5.5. Then all the semifields coordinatizing Π are right primitive and left primitive, whenever Π contains no fractional subplanes Ψ [that contain a central subplane of Π] .*

Proof. We suppose Ψ does not exist. Let D be any semifield coordinatizing Π, with center $K \cong GF(q)$, and let τ_D denote the slope set of D. Thus τ_D is an additive spread set that includes the scalar field $\{\mathcal{K} = k\mathbf{1} : k \in K\}$, and in fact τ_D is a linear spread set over the field $\mathcal{K} \cong GF(q)$. Let π be the corresponding spread on $D \oplus D$; thus $X = D \oplus \mathbf{0} \in \pi$ and $Y = \mathbf{0} \oplus D \in \pi$, where Y is

the shears axis. Suppose $T_d \in \tau_D \setminus \mathcal{K}$ is reducible. Then by Lemma 5.1, Π may be recoordinatized by a fractional semifield E, that contains $GF(q)$ in its center, so the plane Π_E coordinatized by E has a fractional central subplane, but since $\Pi = \Pi_E$ we contradict our assumption that contains no fractional central subplane.

Hence, every non-scalar in τ_D is irreducible. Choose any non-scalar $T \in \tau$. Then since T is irreducible, Schur's Lemma implies that there is a field Θ of K-linear maps containing $\{\mathcal{K}, T\}$, and since D must be a vector space over Θ, it follows that $GF(q^5) \cong \Theta \supset \mathcal{K}$. Hence T, viewed as a $\mathcal{K}$-linear map, is an irreducible element of the field Θ, over the subfield $\mathcal{K}$. So by Corollary 5.5, there are elements $\alpha, \beta \in \mathcal{K}$ such that $W = \alpha T + \beta \in GL(D, K)$ is a primitive element of the field Θ, hence W, as an element $GL(D, K)$, has multiplicative order $|W| = q^5 - 1$. Moreover, since τ_D is a $\mathcal{K}$-linear set, we also have $W \in \tau_D$. But then, by Lemma 4.2(1), D is right-primitive. We still need to check that all such D are left primitive.

Consider the dual plane Π' of Π. Suppose, if possible, that Π' has a fractional subplane, containing a central subplane. So there is a semifield $\mathcal{D}' := (D, +, *)$, with center $K = GF(q)$, coordinatizing Π' such that $\mathcal{D}' := (D, +, *)$ contains a subfield $\mathcal{F} := (F, +, *) > (K, +, *)$, with $\mathcal{F} \cong GF(q^2)$. Now the dual semifield, of $\mathcal{D}' := (D, +, *)$, is a semifield $\mathcal{D} := (D, +, \circ)$ (thus $x \circ y = y * x, x, y \in D$), with center $(K, +, *)$, and this contains the subfield $(F, +, \circ) = (F, +, *) \cong GF(q^2)$, hence the corresponding plane $\Pi(D)$ is fractional relative to the central plane $\Pi(F)$. However, $\Pi(D) \cong \Pi$, which has no fractional subplane. This contradiction shows that Π' cannot be coordinatized by a fractional subplane. Hence, by what has been proved above, the semifields coordinatizing Π' are right primitive, so the semifields coordinatizing Π are left primitive. Thus all the semifields coordinatizing Π are both right primitive and left primitive. □

COROLLARY 5.7. *Let Π be any semifield plane of order p^5. If Π does not admit fractional planes, and p is sufficiently large, then every semifield coordinatizing Π is right primitive and left primitive.*

6 – Generalization of Rúa's Theorem to Regulus Semifields in $PG(7, q)$

Recall that Rúa has shown that semifields of order q^3 with center $GF(q)$ are both right primitive and left primitive. However, in view of the Menichetti classification of such semifields, [18], this result is essentially a result concerning the Albert semifields of order q^3, with center $GF(q)$.

On the other hand, 3-dimensional *regulus* semifields have yet to be classified. These semifields are precisely the semifields that coordinatize semifield spreads $\mathcal{S}$ in $PG(7, q)$ that contain a regulus $\mathcal{R}$ of degree $q + 1$. We show that such semifields are right primitive if q is sufficiently large, Theorem 6.2. For this we require a stronger form of Lemma 5.4, for $q^d = q^3$, due to Mills and McNay.

RESULT 6.1. (Mills and McNay, [16, Paragraph 5]) Suppose $GF(q^3) \cong F > K \cong GF(q)$. Then for sufficiently large values of q, to each $\theta \in F \setminus K$, corresponds an element $k \in K$ such that $\theta + k$ is a primitive element of F.

We may now generalize Rúa's Theorem, [21, Theorem 4], by establishing the right primitivity of semifields 3-dimensional over a regulus subfield $GF(q)$, as opposed to a central subfield $GF(q)$.

THEOREM 6.2. *Let D be a semifield of order q^3 with kern $K = GF(q)$ such that K centralizes D multiplicatively. Then for sufficiently large q, D is right primitive.*

PROOF. Let τ_D be the (additive) spread set of D, and $\mathcal{K}$ be the scalar field in $GL_K(D,+) \cup \{\mathbf{0}\}$, associated with the slope set of K. Then any $T \in \tau_D \setminus \mathcal{K}$ is irreducible. This follows by noting that by the "eigenvalue-argument", Lemma 3.1, T fixes no one-space of the projective plane $PG(D,K)$, hence also no "hyperplane". Thus, by Schur's Lemma, the centralizer of T in $GL_K(D,+) \cup \{\mathbf{0}\}$ is a field $\mathcal{F}_T \supset \{T\} \cup \mathcal{K}$, whenever $T \notin \mathcal{K}$. Since $\mathcal{F}_T \cong GF(q^3)$ and $\mathcal{K} \cong GF(q)$, Mills and McNay, result 6.1, shows that $T + \kappa$, for some $\kappa \in \mathcal{K}$, has multiplicative order $q^3 - 1$. Since, by the additivity of τ_D, $T + \kappa \in \tau_D$, we have τ_D contains a primitive matrix, so $(D,+,\circ)$ is right primitive by Lemma 4.2. □

7 – Right Primitivity of Flock Semifields

The following result is part of a slightly more general Theorem due to S. D. Cohen:

RESULT 7.1. (Cohen, [2].) Let $F = GF(q^2) \supset GF(q) = K$, q any prime power. Then to each $\theta \in F \setminus K$ there correspond $\alpha \in K$ such that $\theta + \alpha$ is a primitive element of F, hence of multiplicative order $q^2 - 1$.

LEMMA 7.2. *Let $\mathcal{D} := (D,+,\circ)$ be a semifield with kern K such that K commutes multiplicatively with D and $\dim_K Q = 2$. Then D is right primitive.*

PROOF. The slope set τ_D may be regarded as an additive group in $GL(2,q) \cup \{\mathbf{0}_2\}$, acting on the K-space $(D,+)$, such that $\tau_D \supset \mathcal{K}$, where $\mathcal{K}$ is the scalar field $\{k\mathbf{1}_2 : k \in K\}$. Let $T \in \tau_D \setminus \mathcal{K}$. Now T is $\mathcal{K}$-linear and acts irreducibly on $(D,+)$, by the "eigenvalue-argument", Lemma 3.1, so by Schur's Lemma the centralizer of T in $Hom_(D,+)$ is a field $\mathcal{F}_T \supset T \cup \mathcal{K}$. Evidently, we have shown the field $\mathcal{F}_T \cong GF(q^2)$, contains $\mathcal{K} \cong GF(q)$, with $T \in \mathcal{F} \setminus \mathcal{K}$. Hence, by Cohen's Theorem, result 7.1, we have $T + A$, for some $A \in \mathcal{K}$, is a primitive element of $\mathcal{F}_T$. However, as τ_D is an additive group $T + A \in \tau_D$ is an element in $GL(2,q)$ with multiplicative order $q^2 - 1$. Hence $(D,+,\circ)$ is right primitive by Lemma 4.2. □

The semifields D that are 2-dimensional over their central kern are precisely the semifields that coordinatize the flock semifield planes. Thus, Lemma 7.2 is equivalent to:

COROLLARY 7.3. *The semifields coordinatizing a flock semifield plane are are all right primitive.*

Note that any non-Desarguesian flock semifield plane admits coordinatization by several non-isomorphic semifields, and all these are flock semifields hence right primitive. However, it is not clear to us whether they are left primitive.

NOTE. The duals of flock semifields are always left primitive, by Corollary 7.3. But the duals of flock semifields are not flock semifields unless the semifield is a field.

Acknowledgement

The second author thanks Flaminio Flamini and the other researchers at the University of Rome for their tremendous support. The work was done when the second author was a visiting professor at the University of Texas at Arlington, 2008-9. The author expresses his cordial thanks to Professors Jianping Zu and the mathematics department at UTA

REFERENCES

[1] M. BILIOTTI – V. JHA – N. L. JOHNSON: *Foundations of Translation Planes*, Marcel Dekker, Inc., New York, Basel.

[2] S. D. COHEN: *Primitive roots in the quadratic extension of a finite field*, J. London Math. Soc., **27** (1983) 221–228.

[3] M. CORDERO – V. JHA: *On the multiplicative structure of quasifields and semifields, cyclic and acyclic loops*, submitted.

[4] M. CORDERO – V. JHA: *Fractional dimensional semifield planes of odd order*, submitted.

[5] P. DEMBOWSKI: *Finite Geometries*, Springer Verlag, Berlin, Heidelberg, New York, 1968.

[6] H. DAVENPORT: *On primitive roots in finite fields*, Quarterly J Math (Oxford), **8** (1937) 308–312.

[7] J. C. FISHER – N. L. JOHNSON: *Fano planes in subregular spreads*, Advances in Geometry, to appear.

[8] H. GEVAERT – N. L. JOHNOSN: *Flocks of quadratic cones, generalized quadrangles and translation planes*, Geom. Dedicata, **27** (1981) 301–317.

[9] I. R. HENTZEL – I. F. RÚA: *Primitivity of finite semifields with 64 and 81 elements*, International J. Algebra and Computation, **17** (2007) 1411–1429.

[10] D. R. Hughes – F. C. Piper: *Projective Planes*, Springer Verlag, New York, 1973.

[11] V. Jha – N. L. Johnson: *The dimension of a subplane of a translation plane*, Bulletin of the Belgian Math. Soc. to appear.

[12] N. L. Johnson – V. Jha – M. Biliotti: *Handbook on Translation Planes*, Taylor and Francis Group, 2007.

[13] N. L. Johnson: *Fano configurations in translation planes*, Note di Mathematica **27** (2007) 21–38.

[14] N. L. Johnson: *Semifield flocks of quadratic cones*, Simon Stevin, **61** (1987) 313–324.

[15] W. Kantor: *Finite semifields*, Proc. Conf. at Pingree Park, (2005) 103–114.

[16] D. Mills – G. McNay: *Primitive roots in cubic extensions of finite fields*, Finite fields with applications to coding theory, cryptography and related areas (Oaxaca, 2001), (2002) 239–250, Springer, Berlin.

[17] A. O. Leone – M. J. de Resmini: *Subplanes of the derived Hughes planes of order 25*, Simon Stevin, **67** (1993) 289–322.

[18] G. Menichetti: *On a Kaplansky Conjecture concerning three-dimensional division algebras over a finite field*, J. Algebra, **47** (1977) 400–410.

[19] H. Neumann: *On some finite non-desarguesian planes*, Arch. Math., **6** (1955) 36–40.

[20] L. Puccio – M. J. de Resmini: *Subplanes of the Hughes planes of order 25*, Arch. Math. (Basel), (1987) 151–165.

[21] I. F. Rúa: *Primitive and non-primitive finite semifields*, Communications in Algebra, **22** (2004) 791–803.

[22] T. Schneider: *Transzendenzuntersuchen periodischer Funktionen I*, J. Reine Angew, Math, **172** (1934) 65–69.

[23] T. Schneider: *Transzendenzuntersuchen periodischer Funktionen II*, J. Reine Angew, Math, **172** (1934)b 70–74.

[24] R. J. Walker: *Determination of division algebras with 32 elements*, Proc. Symposia Appl. Math., **15** (1962) 83–85.

[25] G. P. Wene: *On the multiplicative structure of finite division rings*, Aequationes Math., **41** (1991) 222–233.

[26] G. P. Wene: *Semifields of dimension* $2n$*,* $n \geq 3$*, over* $GF(p^m)$ *that have left primitive elements*, Geom. Dediciata, **41** (1992) 1–3.

Lavoro pervenuto alla redazione il 10 marzo 2010
ed accettato per la pubblicazione il 15 marzo 2010.
Bozze licenziate il 20 aprile 2010

Indirizzo degli Autori:

Minerva Cordero – Mathematics Department – University of Texas – Arlington, TX
E-mail:cordero@uta.edu

Vikram Jha – 2 Marchmont Terrace – Glasgow, G12 9LT – Scotland
E-mail: vjha267@googlemail.com

Rendiconti di Matematica, Serie VII
Volume 30, Roma (2010), 23-32

Some results on Spreads and Ovoids

LAURA BADER

Dedicated to Professor Marialuisa de Resmini

ABSTRACT: *We survey some results on ovoids and spreads of finite polar spaces, focusing on the ovoids of $H(3,q^2)$ arising from spreads of $PG(3,q)$ via indicator sets and Shult embedding, and on some related constructions. We conclude with a remark on symplectic spreads of $PG(2n-1,q)$.*

1 – Introduction

Let q be any prime power and let $PG(2n-1,q)$ be the projective space of dimension $2n-1$ over the Galois field $GF(q)$. A $(n-1)$-spread $\mathcal{S}$ of $PG(2n-1,q)$ is a set of q^n+1 mutually skew $(n-1)$-dimensional subspaces; hence the elements of $\mathcal{S}$ partition the pointset of $PG(2n-1,q)$. Spreads of $PG(2n-1,q)$ define translation planes of order q^n , with kernel containing $GF(q)$, embedding $PG(2n-1,q)$ as a hyperplane in a $PG(2n,q)$ and using the well known André-Bruck/Bose construction, and conversely. This relationship is probably the main motivation for the study of spreads, and the most studied case is $n=2$.

Bruck in [8] introduced indicator sets in finite desarguesian projective planes of square order, and their links with line spreads of projective 3-spaces have been studied in the next years by Bruck himself in [9] and by Bruen in [10]; a few years later, Lunardon in [15] further studied that relationship, mainly from

KEY WORDS AND PHRASES: *Spread – Indicator set – Linear representation – Hermitian variety*
A.M.S. CLASSIFICATION: Primary 51A50, Secondary 51E20, 51A40.

the synthetic geometric point of view: with any spread of $PG(3,q)$ a family of indicator sets is associated. Indicator sets have been somehow aside for many years, until Shult in [19] proved that a suitable set of lines, presently called a Shult set, defines a locally Hermitian ovoid of the Hermitian variety via the so-called Shult embedding, and conversely.

As a Shult set is the point-line dual of an indicator set, there immediately followed a link between spreads of $PG(3,q)$ and families of locally Hermitian ovoids of $H(3,q^2)$, which was first studied by Cossidente, Ebert, Marino and Siciliano in [11] focusing on those associated with the regular spread, the so called classical and semiclassial ovoids of the Hermitian variety. In the subsequent paper [12] Cossidente, Lunardon, Marino and Polverino classified the ovoids arising from the regular spread and from a (proper) semifield spread via the above construction, while in [2] Bader, Marino, Polverino and Trombetti further studied the collineation group of the translation ovoids constructed via a Shult embedding and pointed out that two constructions which could be performed (a family of ovoids of the Klein quadric from the given family of locally Hermitian ovoids of the Hermitian variety via a construction of Lunardon [17] and a family of line spreads from the given family of Shult sets via a construction of Thas [21]) do not produce any new example.

Here we deal with these results and we conclude the paper with a remark linking symplectic spreads of $PG(2n-1,q)$ and Thas maximal arcs in projective planes of order q^n and kernel containing $GF(q)$.

2 – Spreads of $PG(3,q)$, ovoids of $H(3,q^2)$ and some related constructions

2.1 – Spreads, indicator sets, Shult sets

View $\Sigma = PG(3,q)$ as a canonical subgeometry of a $\Sigma^* = PG(3,q^2)$; let σ be the collineation of Σ^* fixing Σ pointwise (hence $\sigma^2 = id$) and let $\mathcal{S}$ be any spread of Σ. Fix a line l in $\mathcal{S}$. A plane $\pi \cong PG(2,q^2)$ of Σ^* is an *indicator plane* of $\mathcal{S}$ if $\pi \cap \Sigma = l$; the *indicator set* of $\mathcal{S}$ in π is $I_\pi(\mathcal{S}) = \{m^* \cap \pi | m \in \mathcal{S}\}$, where m^* denotes the unique line of Σ^* containing m. The set $I_\pi(\mathcal{S})$ has size q^2 and none of its secants contains points of l; conversely, any set I' of points of π satisfying the previous two properties canonically defines a spread, namely $\mathcal{S}' = \{< Q, Q^\sigma > \cap \Sigma \mid Q \in I'\} \cup \{l\}$ and $I_\pi(\mathcal{S}') = I'$. Hence, with any spread $\mathcal{S}$ a family is associated of indicator sets $I_\pi(\mathcal{S})$. Furthermore, the spread $\mathcal{S}$ is regular if and only if any $I_\pi(\mathcal{S})$ is either an affine line (*classical indicator set*) or an affine Baer subplane (*semiclassical indicator set*). For more details, see *e.g.* [8], [9], [10] and [15].

Let $\Sigma = PG(3,q), \Sigma^* = PG(3,q^2)$, the plane π and the line l be as above, and denote by l^* the line of Σ^* containing l. Let $\hat{\pi}$ be the dual plane of π and let P denote the point of $\hat{\pi}$ corresponding to the line l^*. The points of l are

mapped to the lines of a cone $\hat{l}$ of $\hat{\pi}$ having vertex P. Let $\mathcal{F}$ be the set of lines of $\hat{\pi}$ corresponding to the points of the indicator set I. Then: (i) $\hat{\pi}$ is a projective plane with a distinguished degenerate Hermitian variety (the Baer subpencil $\hat{l}$ with vertex P); (ii) $\mathcal{F}$ is a set of q^2 lines of $\hat{\pi}$, none of which contains P; (iii) any two distinct lines of $\mathcal{F}$ intersect in a point not on the Baer subpencil. Any set of lines satisfying the above three properties is called a *Shult set*. Conversely, a Shult set defines, by any polarity of its plane, an indicator set. In conclusion, with any line spread a family of indicator sets or, equivalently, a family of Shult sets is associated.

2.2 – Shult embedding

A Hermitian surface $\mathcal{H} = H(3, q^2)$ of $PG(3, q^2)$ is the set of all isotropic points of a non-degenerate unitary polarity. A line of $PG(3, q^2)$ meets $\mathcal{H}$ in 1 (*tangent*) or $q + 1$ (*hyperbolic line*) or $q^2 + 1$ (*generator*) points. The hyperbolic lines intersect $\mathcal{H}$ in Baer sublines which are called *chords*.

An ovoid $\mathcal{O}$ of $\mathcal{H}$ is a set of $q^3 + 1$ points such that any generator of $\mathcal{H}$ contains exactly one point of $\mathcal{O}$. The Hermitian curve $H(2, q^2)$, intersection of $\mathcal{H}$ with any of its secant planes, is the *classical* ovoid. An ovoid is called *locally Hermitian* with respect to a point P if it is the union of q^2 chords of $\mathcal{H}$ through P and is called *translation* with respect to a point P if there is a collineation group of $\mathcal{H}$ fixing P, all the generators through P, and acting regularly on the points of $\mathcal{O} \setminus \{P\}$. Note that any translation ovoid is locally Hermitian ([7]) but not conversely, and a classical ovoid of $\mathcal{H}$ is a translation ovoid with respect to each of its points.

Start off with a spread $\mathcal{S}$ of $PG(3, q)$, fix a line l in $\mathcal{S}$, an indicator plane π through l as above, construct the indicator set and polarize to a Shult set $\mathcal{F}$ with respect to the subpencil $\hat{l}$ in the plane $\hat{\pi} = PG(2, q^2)$; embed the plane $\hat{\pi}$ in a $PG(3, q^2)$ containing a Hermitian surface $\mathcal{H}$ such that $\hat{\pi}$ is the tangent plane to $\mathcal{H}$ at P and $\hat{l} = \mathcal{H} \cap \hat{\pi}$; denote by ρ be the polarity defined by $\mathcal{H}$. Then Shult has proved in [19] that $\mathcal{O}_\pi(\mathcal{S}) = \bigcup\{L^\rho | L \in \mathcal{F}\}$ is an ovoid of $\mathcal{H}$, which is, by construction, locally Hermitian with respect to its point P. The above construction is presently called a *Shult embedding* following [11].

We explicitly note that on the other hand, via the so-called *Hermitian embedding* defined by Cossidente, Ebert, Marino and Siciliano in [11], symplectic spreads of $PG(3, q)$ are characterised as those corresponding to indicator sets embedded in a Hermitian variety $\mathcal{H}$, and conversely. Namely, let δ be a symplectic polarity commuting with the unitary polarity ρ associated with $\mathcal{H} = H(3, q^2)$. The map $\sigma = \delta \circ \rho = \rho \circ \delta$ is a (non-linear) collineation, fixing $q^3 + q^2 + q + 1$ points on $\mathcal{H}$ but no point off $\mathcal{H}$, and leaving invariant $q^3 + q^2 + q + 1$ generators of $\mathcal{H}$. Also, noting that any fixed point (invariant generator resp.) is incident with $q + 1$ invariant generators (fixed points resp.), yields a symmetric configuration

which extends in a suitable way to a symplectic polar space $\mathcal{W} = W(3,q)$ embedded in a subgeometry $\Sigma = PG(3,q)$ of the starting Σ^* containing $\mathcal{H}$. In this context, the totally isotropic lines of Σ with respect to δ are exactly the lines of $\mathcal{W}$. Let $\mathcal{S}$ be a spread of Σ whose lines are isotropic with respect to δ. Let l be a line of $\mathcal{S}$ and denote by l^* the line of Σ^* containing l, which is a generator of $\mathcal{H}$. Fix a point $P \in l^* \setminus l$, hence $P^\rho \cap \mathcal{W} = l$. The indicator set is contained in $\mathcal{H}$ and consists of the points in which all the extended lines of $\mathcal{S}$ meet P^ρ. The construction above can be reversed. Unfortunately, the Hermitian embedding does not produce any locally Hermitian ovoid (whereas the Shult embedding does) because the dual lines of the starting Hermitian indicator set not necessarily are hyperbolic lines of $\mathcal{H}$.

2.3 – Semiclassical ovoids of $H(3,q^2)$

In [11] the Shult embedding is used to construct the classical ovoid and two semiclassical ovoids of $\mathcal{H}(3,q^2)$ arising from classical and semiclassical indicator sets, respectively. Also, the groups of those ovoids are computed, proving that if $q > 3$ there exist at least two (non isomorphic) semiclassical ovoids of $\mathcal{H}(3,q^2)$, depending on the elliptic quadric $\mathbb{Q} = Q^-(3,q)$, image of the points of the indicator set being permutable or not, i.e. the polarity defined by the $Q^+(5,q)$ containing $\mathbb{Q}$ commutes with the unitary polarity associated with the Hermitian variety. The first one, called the p-*semiclassical ovoid* (permutable semiclassical ovoid), has an elementary abelian p-group ($q = p^r$).

The notion of commuting polarities was introduced by Tits in 1955, and Segre in 1965 studied Hermitian geometry over finite fields, also investigating the polarities commuting with a unitary one. Starting with Segre's results, recently Cossidente, de Resmini and Marino in [13] have studied various geometrical and combinatorial properties of permutable polarities, with special regard to unitary polarities commuting with orthogonal ones, focusing on the relationship between (regular) symplectic spreads of $PG(3,q)$ and some remarkable subsets of the Hermitian curve $H(2,q^2)$, the so-called C_F-sets after Donati and Durante. Furthermore, in [13] they discuss symplectic polarities commuting with unitary polarities.

In order to compute the number of non isomorphic ovoids of $\mathcal{H}(3,q^2)$ arising via the Shult embedding, the following definition has been introduced by Cossidente, Lunardon, Marino and Polverino in [12]: two indicator sets I_1 and I_2 in the same Σ^* lying on the indicator planes π_1 and π_2, respectively, passing through the line l^*, are said *isomorphic* if the associated spreads of Σ are, and they are said *equivalent* if there is a collineation of Σ^* mapping I_1 to I_2 and fixing the Baer subline l. Note that equivalent indicator sets are isomorphic, whereas it is worth noting that isomorphic indicator sets may be non equivalent. With this approach, they can prove that two locally Hermitian ovoids of $\mathcal{H}(3,q^2)$ are

isomorphic if and only if the corresponding indicator sets are equivalent, and consequently show that the number θ of non isomorphic semiclassical ovoids of $\mathcal{H}(3,q^2)$ is $\frac{q-3}{2}+1$ if q is a prime with $q \geq 3$, whereas the following bounds hold for any q : $2 \leq \theta \leq \frac{q-2}{2}$ if q is even and $q > 2$, and $2 \leq \theta \leq \frac{q-3}{2}+1$ if q is odd and $q > 3$. For further details, see [12].

2.4 – Translation ovoids and their group

To obtain futher information on the collineation group of the ovoids arising from the Shult embedding, we specialize to a distinguished class of spreads, namely semifield spreads. A spread $\mathcal{S}$ is a *semifield spread* with respect to its line ℓ_∞ if there exists a group fixing the line ℓ_∞ pointwise and acting regularly on the set of the q^2 lines of $\mathcal{S}$ different from ℓ_∞. Moreover, if $\mathcal{S}$ is a semifield spread with respect to the line ℓ_∞ then, for any choice of the indicator plane π such that $\ell_\infty \subset \pi$, the ovoid $\mathcal{O}_\pi(\mathcal{S})$ is a translation ovoid with respect to the point P, and conversely.

Choose homogeneous projective coordinates (x_0,x_1,x_2,x_3) in such a way that $\mathcal{S} = \{\ell_\infty, \ell_{u,v} | u,v \in GF(q)\}$ with $\ell_\infty : x_0 = x_1 = 0$, and $\ell_{u,v} = \{(a,b,c,d) : (c,d) = (a,b)X_{u,v},\ a,b \in GF(q)\}$ where $X_{u,v} = \begin{pmatrix} v & h(u,v) \\ u & k(u,v) \end{pmatrix}$ with $h,k : GF(q) \times GF(q) \to GF(q)$, $h(0,0) = k(0,0) = 0$. Since $\mathcal{S}$ is a semifield spread, then $\{X_{u,v} | u,v \in GF(q)\}$ is closed under addition hence h and k are additive functions.

If $\pi_\lambda : x_1 = \lambda x_0$ is any indicator plane through ℓ_∞, where $\lambda \in GF(q^2) \setminus GF(q)$, then $I_{\pi_\lambda}(\mathcal{S}) = I_\lambda(\mathcal{S}) = \{(1,\lambda, v+\lambda u, h(u,v)+\lambda k(u,v)) : u,v \in GF(q)\}$ and

$$\mathcal{O}_\lambda(\mathcal{S}) = \{(1, -v-\lambda^q u, h(u,v)+\lambda^q k(u,v), \alpha + \lambda(vk(u,v) - uh(u,v))) : u,v,\alpha \in GF(q)\} \cup \{P = (0,0,0,1)\}$$

is the locally Hermitian ovoid (with respect to P) of $\mathcal{H}(3,q^2) : y_0 y_3^q - y_3 y_0^q + y_2 y_1^q - y_1 y_2^q = 0$ arising via the Shult embedding (for more details, see [12]).

Let $PGU(4,q^2)$ be the group of the linear collineations of $PG(3,q^2)$ leaving $\mathcal{H}$ invariant. The subgroup E of $PGU(4,q^2)$ fixing P and leaving invariant all the generators through P has size q^5 ([18]) and direct computations show that E consists of the matrices

$$\begin{pmatrix} 1 & \alpha & \beta & c-\alpha\beta^q \\ 0 & 1 & 0 & -\beta^q \\ 0 & 0 & 1 & \alpha^q \\ 0 & 0 & 0 & 1 \end{pmatrix}, \alpha,\beta \in GF(q^2), c \in GF(q).$$

The subgroup of E acting as translation group on the ovoid $\mathcal{O}_\lambda(\mathcal{S})$ is explicitly computed in [2] as

$$G = \left\{ \begin{pmatrix} 1 & -v-\lambda^q u & h(u,v)+\lambda^q k(u,v) & c+(v+\lambda^q u)(h(u,v)+\lambda k(u,v)) \\ 0 & 1 & 0 & -h(u,v)-\lambda k(u,v) \\ 0 & 0 & 1 & -v-\lambda u \\ 0 & 0 & 0 & 1 \end{pmatrix}; \right. \left. u,v,c \in F_q \right\}.$$

As $H(3,q^2)$ can also be viewed as an elation generalised quadrangle, which can be represented as a coset geometry with elation group $(\tilde{E},\circ)$ where $\tilde{E} = GF(q^2) \times GF(q) \times GF(q^2)$ and $(\alpha,c,\beta)\circ(\alpha',c',\beta') = (\alpha+\alpha', c+c'+Tr(\alpha'\beta^q), \beta+\beta')$ with $\alpha,\beta \in GF(q^2)$ and $c \in GF(q)$ (see *e.g.* [3]), the map

$$\psi : (\alpha,c,\beta) \in \tilde{E} \to \begin{pmatrix} 1 & \alpha & \beta & c-\alpha\beta^q \\ 0 & 1 & 0 & -\beta^q \\ 0 & 0 & 1 & \alpha^q \\ 0 & 0 & 0 & 1 \end{pmatrix} \in E$$

is an isomorphism and the translation group of any translation ovoid $\mathcal{O}_\lambda(\mathcal{S})$ arising from a semifield spread $\mathcal{S}$ via the Shult embedding is isomorphic to the preimage of G

$$\tilde{G} = \psi^{-1}(G) = \{(-v-\lambda^q u, \alpha, h(u,v)+\lambda^q k(u,v)) : \ u,v,\alpha \in GF(q)\}$$

which turns out to be abelian if and only if $\mathcal{O}_\lambda(\mathcal{S})$ is p-semiclassical (see [2]).

Recall that the permutable semiclassical ovoid was the only translation ovoid constructed in [11] admitting an elementary abelian p-group , $q = p^r$, and in [12] it is proved that the $q+1$ p-semiclassical translation ovoids arising from a given regular spread are all isomorphic. Hence there exists (up to isomorphism) a unique translation ovoid of $H(3,q^2)$ with an abelian translation group, namely the p-semiclassical. For more details, see [2].

2.5 – Ovoids of $Q^+(5,q)$ from indicator sets

Let $\mathcal{S}$ be any spread of $\Sigma = PG(3,q)$ containing the lines ℓ_∞ and ℓ_0 and defined by the functions h and k as in Section 2.4. Here, as $\mathcal{S}$ may not be a semifield spread, hence h and k may not be additive.

Then $\mathcal{O}_\lambda(\mathcal{S})$ are the locally Hermitian ovoids of the Hermitian surface $\mathcal{H}$: $x_0x_3^q - x_0^q x_3 + x_2x_1^q - x_2^q x_1 = 0$ of $\Gamma = PG(3,q^2)$ arising from $\mathcal{S}$, as λ varies in $GF(q^2) \setminus GF(q)$.

The projective plane $\pi = PG(V, q^2)$ is the lattice of the $GF(q^2)-$ subspaces of the 3-dimensional vector space V (over $GF(q^2)$); as V can also be viewed as a 6-dimensional vector space over $GF(q)$, a 5-dimensional projective space $= PG(V, q) = PG(5, q)$ arises. A point (line resp.) of π is defined by a $GF(q^2)-$subspace of dimension 1 (2 resp.), which can be considered as a $GF(q)-$subspace of dimension 2 (4 resp.); hence the pointset of π is mapped to a lineset of Ω, which is a normal spread $\mathcal{R}_\lambda$, and any line of π is mapped to a 3-space with a regular spread consisting of the images of the points of the line itself . The pair $(\Omega, \mathcal{R}_\lambda)$ is the *F_q-linear representation* of π with respect to the basis $\{1, \lambda\}$ (for more details see [2]).

Embed the above $(\Omega, \mathcal{R}_\lambda)$ in $\Omega' = PG(6, q)$ as a hyperplane and define the point-line geometry $\pi(\Omega', \Omega, \mathcal{R}_\lambda)$ as follows. The points are either the points of $\Omega' \setminus \Omega$ or the elements of $\mathcal{R}_\lambda$. The lines are either the planes of Ω' which intersect Ω in a line of $\mathcal{R}_\lambda$ or the regular spreads of the 3-dimensional projective spaces $\langle A, B\rangle$, where A and B are distinct lines of $\mathcal{R}_\lambda$; the incidence is the natural one. As $\mathcal{R}_\lambda$ is normal, $\pi(\Omega', \Omega, \mathcal{R}_\lambda)$ is isomorphic to a $PG(3, q^2)$ containing π, and the isomorphism extends the linear representation. This is the *Barlotti-Cofman representation* of $PG(3, q^2)$ (for more details see [5]).

Lunardon in [17] has shown that the image of a Hermitian variety having π as a tangent plane, in the Barlotti-Cofman representation, is a cone having vertex in Ω and basis a suitable $Q^+(5, q)$ of Ω', and that any locally Hermitian ovoid $\mathcal{O}_\pi(\mathcal{S})$ with respect to P of $\mathcal{H}$ is mapped to an ovoid, say $\mathbb{O}_\lambda$, of the hyperbolic quadric $Q^+(5, q)$, and conversely; if $\mathcal{O}_\pi(\mathcal{S})$ is a translation ovoid, then $\mathbb{O}_\lambda$ is too.

On the other hand, to the line spread $\mathcal{S}$ there corresponds, via the Klein map, an ovoid $\mathcal{O}(\mathcal{S})$ of the Klein quadric. Answering a question posed in [17], in [2] it is shown that the ovoid $\mathcal{O}(\mathcal{S})$ is isomorphic to any $\mathbb{O}_\lambda$, for any choice of the indicator plane π, therefore no new ovoids of $Q^+(5, q)$ can be constructed in this way.

2.6 – Spreads from indicator sets via locally Hermitian spreads of $Q^-(5, q)$

Let $\mathcal{S}$ be any spread of $\Sigma = PG(3, q)$. Embed Σ in $\Sigma^* = PG(3, q^2)$ in such a way that $\Sigma = Fix(\sigma)$, where σ is an involutory collineation of Σ^*. Let π be an indicator plane of $\mathcal{S}$ in $PG(3, q^2)$. Denote by l the line of $\mathcal{S}$ such that l is in π and by $I_\pi(\mathcal{S})$ the indicator set of $\mathcal{S}$ in the plane π. Consider the point-line dual plane of π: this is a plane $\tilde{\pi}$, in which l^* (the extension of l in Σ^*) is represented by a point P, the Baer subline l by a Baer subpencil $\tilde{l}$ through P and $I_\pi(\mathcal{S})$ by a set $\mathcal{F}$ of q^2 lines not containing P, any two of which intersect at a point of $\tilde{\pi} \setminus \tilde{l}$. (The set of lines $\mathcal{F}$ is the associated Shult set.) Fix a Hermitian surface $\mathcal{H} = H(3, q^2)$ in such a way that $P \in \mathcal{H}$ and $\tilde{\pi} \cap \mathcal{H} = \tilde{l}$. Let ρ be the polarity defined by $\mathcal{H}$. The elements of $\mathcal{F}^\rho$ are hyperbolic lines of $\mathcal{H}$ through P, hence the set $\mathcal{O}_\pi = \bigcup_{m \in \mathcal{F}} (m^\rho \cap \mathcal{H})$ is a locally Hermitian ovoid of $\mathcal{H}$. (Note that the ovoid

depends on the choice of the indicator plane π.) The ovoid $\mathcal{O}$ corresponds, via the Klein map κ, to a locally Hermitian spread $\mathbb{S}_\pi$ of $Q^-(5,q)$ with respect to the line $L = P^\kappa$. Let $\Lambda = L^\perp$, where $\perp$ is the orthogonal polarity induced by $Q^-(5,q)$. If M is a line of $\mathbb{S}_\pi$ different from L then $m_{L,M} = \langle L, M\rangle^\perp$ is a line of Λ disjoint from $\langle L, M\rangle$. Moreover the set of lines $\mathcal{S}'_\pi = \{m_{L,M} : M \in \mathbb{S}, M \neq L\} \cup \{L\}$ turns out to be a spread of Λ as proved by Thas in [21]. If the spread $\mathcal{S}$ is a semifield spread then the spread $\mathcal{S}'_\pi$ also is. In [2] it is proved that $\mathcal{S}$ and $\mathcal{S}'_\pi$ are isomorphic for any choice of the indicator plane π, the proof being obtained by reviewing the above construction embedding the involved spreads in the same 3-dimensional projective space over $GF(q^2)$. In the case $\mathcal{S}$ is a semifield spread, the question on the relation between $\mathcal{S}$ and $\mathcal{S}'_\pi$ was posed in [17, Par. 4.3].

3 – Symplectic spreads and Thas arcs

Let $PG(2n-1,q)$ be the projective $(2n-1)-$dimensional space over F_q. A *spread* of $PG(2n-1,q)$ is a set of q^n+1 pairwise disjoint $(n-1)-$dimensional subspaces which partition the pointset of $PG(2n-1,q)$. A spread is *symplectic* if all of its elements are totally isotropic with respect to some polarity of the space, defined by a nonsingular alternating bilinear form of the underlying vector space. For more details, the reader is referred *e.g.* to [14].

In [20] Thas gave the following construction of a maximal arc, which is called *Thas arc*: let $Q^- = Q^-(2n-1,q)$ be an elliptic quadric of $PG(2n-1,q)$, $n \geq 2$, and let $\mathcal{S}^-$ be a spread of $Q^-(2n-1,q)$. Fix an $(n-1)-$spread $\mathcal{S}$ of $H = PG(2n-1,q)$ intersecting $Q^-(2n-1,q)$ in $\mathcal{S}^-$. Embed $PG(2n-1,q)$ as a hyperplane in $PG(2n,q)$ and fix a point $x \in PG(2n,q) \setminus PG(2n-1,q)$. The set $\{< x,y > | y \in Q^-\} \setminus Q^-$ is a maximal $(q^{2n-1} - q^n + q^{n-1}; q^{n-1})-$arc of the projective plane of order q^n defined by $\mathcal{S}$ via the usual André-Bruck/Bose construction. We recall that, following Barlotti in [4], a $\{k;m\}-$arc in a finite projective plane of order s is a set of k points such that m is the greatest number of collinear points in the set, and an arc is *maximal* if k attains its maximal value, i.e. $k = sm - s + m$. In [6] Blockhuis, Hamilton and Wilbrink proved that no Thas arcs exist for q odd, as conjectured in [20].

Recently, using some intersection properties of symplectic spreads and nonsingular quadrics, it has been proved in [1] that a translation plane of order q^n, q even, with kernel containing $GF(q)$, is defined by a symplectic spread if and only if it contains a Thas arc.

In the following Bibliography a huge number of actually relevant papers and books are missing, for obvious reasons of space. We have just listed some items we explicitly refer to, and we apologize to the Authors of the many missing ones.

REFERENCES

[1] L. Bader: *A remark on symplectic spreads*, Ricerche Mat., to appear.

[2] L. Bader – G. Marino – O. Polverino – R. Trombetti: *Spreads of $PG(3,q)$ and ovoids of polar spaces*, Forum Math., **19** (2007) 1101–1110.

[3] L. Bader – R. Trombetti: *Translation ovoids of flock generalized quadrangles*, Europ. J. Combin., **25** (2004) 65–72.

[4] A. Barlotti: *Sui $\{k;n\}-$archi di un piano lineare finito*, Boll. Un. Mat. Ital., **11** (1956) 553–556.

[5] A. Barlotti – J. Cofman: *Finite Sperner spaces constructed from projective and affine spaces*, Abh. Math. Sem. Univ. Hamburg, **40** (1974) 230–241.

[6] A. Blockhuis – N. Hamilton – H. Wilbrink: *On the non-existence of Thas maximal arcs in odd order projective planes*, Europ. J. Combin., **9** (1998) 413–417.

[7] I. Bloemen – J. A. Thas – H. Van Maldeghem: *Translation ovoids of generalized quadrangles and hexagons*, Geom. Dedicata, **72** (1998) 19–62.

[8] R. H. Bruck: *Construction problems in finite projective spaces*, Combinatorial Mathematics and its applications, Chapel Hill, (1969) 426–514.

[9] R. H. Bruck: *Construction problems in finite projective spaces*, Finite geometric structures and their applications, CIME, (1972) 105–188.

[10] A. A. Bruen: *Spreads and a conjecture of Bruck and Bose*, J. Algebra, **23** (1972) 519–537.

[11] A. Cossidente – G. Ebert – G. Marino – A. Siciliano: *Shult Sets and Translation Ovoids of the Hermitian Surface*, Adv. Geom., **6** (2006) 523–542.

[12] A. Cossidente – G. Lunardon – G. Marino – O. Polverino: *Hermitian indicator sets*, Adv. Geom., **7** (2007) 357–373.

[13] A. Cossidente – M. J. de Resmini – G. Marino: *On the geometry of commuting polarities*, Europ. J. Combin., **28** (2007) 1043–1055.

[14] P. Dembowski: *Finite Geometries*, Springer-Verlag, Berlin Heidelberg New York, 1968.

[15] G. Lunardon: *Insiemi indicatori proiettivi e fibrazioni planari di uno spazio proiettivo finito*, Boll. Un. Mat. Ital., **3** (1984) 717–735.

[16] G. Lunardon: *Normal spreads*, Geom. Dedicata, **75** (1999) 245–261.

[17] G. Lunardon: *Blocking sets and semifields*, J. Comb. Theory Ser. (A), **113** (2006) 1172–1188.

[18] S. E. Payne – J. A. Thas: *Finite Generalized Quadrangles*, Research Notes in Mathematics, 110, Pitman, Boston, 1984.

[19] E. E. Shult: *Problems by the wayside*, Disc. Math., **294** (2005) 175–201.

[20] J. A. Thas: *Construction of Maximal Arcs and Dual Ovals in Translation Planes*, Europ. J. Combin., **1** (1980) 189–192.

[21] J. A. Thas: *Semi-Partial geometries and spreads of classical polar spaces*, J. Comb. Theory Ser. A, **35** (1983) 58–66.

Lavoro pervenuto alla redazione il 10 marzo 2010
ed accettato per la pubblicazione il 15 marzo 2010.
Bozze licenziate il 20 aprile 2010

Indirizzo dell'Autore:

Laura Bader – Università di Napoli Federico II – Dipartimento di Matematica e Applicazioni – Complesso di Monte S. Angelo, Via Cintia, I-80126 Napoli – Italy
E-mail: laura.bader@unina.it

Rendiconti di Matematica, Serie VII
Volume 30, Roma (2010), 33-45

Some remarks on Calabi-Yau manifolds

GILBERTO BINI

Dedicated to Professor Marialuisa de Resmini

Abstract: *Here we focus on the geometry of the "mirror quintic" Y and its generalizations. In particular, we illustrate how to obtain new birational models of Y.*

1 – Introduction

Let X be a complex, compact, connected Kähler manifold. X is said to be a Calabi-Yau variety if i) the canonical bundle is trivial and ii) there are no p-holomorphic forms for $p \neq 0, n$, where n is the complex dimension of X. i) implies that there is a unique (up to scalars) global top degree holomorphic form and ii) can be rephrased in terms of Hodge numbers, that is to say, $h^{p,0} \neq 0$ for p in the range above. We remark that $h^{0,0} = 1$ because X is connected and $h^{n,0} = 1$ because the canonical bundle $K_X = \Omega_X^n$ is trivial.

For applications in Mathematics and Physics it is important to give a definition of singular Calabi-Yau varieties. These are normal compact manifolds with Gorenstein canonical singularities such that the dualizing sheaf is trivial and the Hodge numbers $h^{p,0} \neq 0$ for $p \neq 0, n$. In most of the applications we shall deal with, X will be a global quotient, i.e., a smooth variety with an action of a finite group $G \subset SL(n, \mathbb{C})$.

It is easy to give examples of smooth Calabi-Yau manifold in low dimension. Elliptic curves and K3 surfaces are the only examples of Calabi-Yau manifolds

Key Words and Phrases: *Calabi-Yau Manifolds – Orbifold Cohomology*
A.M.S. Classification: 14H10.

in dimension one and two, respectively. Noticeably, in these cases the condition of being Calabi-Yau uniquely determines the structure of the Hodge diamond. This is no longer true for higher dimensional examples.

We start our talk by going over an intriguing example: a family of quintic threefolds in $\mathbb{P}^4$. This family was introduced by Dwork in the sixties, and has been extensively studied in connection with Number Theory [10] and Physics (see, for instance, [5]). Clearly, a smooth quintic in $\mathbb{P}^4$ is Calabi-Yau by adjunction and the Lefschetz Theorem. Hence, the generic member of the Dwork pencil is a Calabi-Yau manifold. Further, the five singular members are singular Calabi-Yau manifolds according to the definition recalled above.

A group $G \cong (\mathbb{Z}/125\mathbb{Z})^3$ acts on the Dwork pencil X_t. Generically, the quotient has a smooth resolution Y_t, which is a Calabi-Yau manifold. There is a strange duality - first pointed out in [7] - among the Hodge numbers of X_t and those of Y_t for generic t. More specifically, X_t and Y_t are said to be *mirror symmetric*.

Given a family of Calabi-Yau manifolds $\mathcal{F}_t$, it is natural to ask whether $\mathcal{F}_t$ is birational to Y_t or not. In [2] we answer this question for six families. Some of them are birational to Y_t modulo a finite group. One of them is exactly the family investigated in [8].

We finally remark that the Dwork pencil X_t^{n+1} can be generalized to any degree. We investigate its properties in [3]. Here we show how the geometry of X_t^{n+1} can be intricate by describing a special subvariety that exists in even dimensional projective space.

2 – The mirror quintic

Let $X_t \to \mathbb{P}^1$ be the Dwork pencil, where

$$X_t := \left\{ x_1^5 + \ldots + x_5^5 - 5t x_1 \ldots x_5 = 0 \right\}. \tag{1}$$

It is easy to check that for $t^5 \neq 1$, the fiber of the Dwork pencil is a smooth Calabi-Yau manifold. For $t = \infty$ the fiber is a union of hyperplanes.

PROPOSITION 2.1. *For $t^5 = 1$ X_t is a singular Calabi-Yau.*

PROOF. First, notice that the singularities are normal because the singular set has codimension more than one: see [15], p. 76. Moreover, they are Gorenstein by [13], p. 314. Furthermore, an ordinary double point is canonical: see, for instance, [11]. Finally, it is an exercise to show that $h^{i,0}(X_t) = 0$. □

Let us now compute the Hodge numbers of the general fiber of the Dwork pencil. By definition of Calabi-Yau manifold, it suffices to compute $h^{1,1}$ and $h^{2,1}$. The former equals the dimension of $H^2(X_t, \mathbb{C})$ by Lefschetz's Theorem, which is 1. The Euler characteristic of X_t is given by $c_3(X_t)$, which can be computed by the Euler exact sequence and the exact sequence, which defines the tangent space to X. More precisely, we have

$$c(X_t) = \frac{(1+u)^5}{(1+5u)},$$

where $c(X_t)$ is the total Chern polynomial. Hence we get $c_3(X_t) = -200$. This yields $h^{2,1} = 101$.

There is an abelian group that acts on X_t for all t. Set

$$G := \left\{ (a_1, \ldots, a_5) \in (\mathbb{Z}/5\mathbb{Z})^5 : \sum_i a_i \equiv 0 \mod 5 \right\} / < (a,a,a,a,a) > .$$

The group G acts on the projective space $\mathbb{P}^4$ in the following way:

$$(a_1, \ldots, a_5) \cdot (x_1 : \ldots : x_5) = (\zeta^{a_1} x_1 : \ldots : \zeta^{a_5} x_5),\ \zeta^5 = 1, \zeta \neq 1,$$

where ζ is a primitive fifth root of unity. If the a_i's are equal to each other, the action becomes trivial; hence we mod out by the subgroup of diagonal elements. The condition $\sum_i a_i \equiv 0 \mod 5$ preserves the term $x_1 \ldots x_5$; so the group G acts on X_t for any t. Modding out by the subgroup of diagonal elements allows one to set one of the coordinates equal to zero. Since the sum of the remaining coordinates has to be congruent to zero mod 5, the group G depends on three coordinates. Hence it is isomorphic to $(\mathbb{Z}/5\mathbb{Z})^3$, whose order is 125. As proved in [17], the set of 125 nodes is transitive with respect to the action of G for $t^5 = 1$.

The group G acts on X_t with nontrivial stabilizers. Suppose $x_j = x_k = 0$ for $j, k \in \{1, \ldots, 5\}$. Then $\{x_j = x_k = 0\} \cap X_t$ is a plane quintic curve with generic stabilizer isomorphic to $\mathbb{Z}/5\mathbb{Z}$. If three coordinates are equal to zero, then the stabilizer is isomorphic to $(\mathbb{Z}/5\mathbb{Z})^2$.

A monomial $x_1^{k_1} \ldots x_4^{k_4}$ is invariant under G if and only if $k_1 \equiv k_2 \equiv k_3 \equiv k_4 \mod 5$. Thus the quotient map $p : X_t \to X_t/G$ is given by

$$(x_1 : \ldots : x_5) \to (x_1 \ldots x_5 : x_1^5 : \ldots : x_5^5).$$

The quotient is thus a threefold in $\mathbb{P}^5$ which satisfies the following equations:

$$z_1 + z_2 + \ldots + z_5 - 5tz_0 = 0, \qquad z_0^5 = z_1 z_2 z_3 z_4 z_5, \tag{2}$$

where z_i are a system of homogeneous coordinates in $\mathbb{P}^5$.

The image of the curves $\{x_j = x_k = 0\} \cap X_t$ is given by $z_0 = z_j = z_k = 0$ and $z_1 + \ldots + z_5 = 0$, which is isomorphic to $\mathbb{P}^1$. The points with stabilizer $(\mathbb{Z}/5\mathbb{Z})^2$ satisfy the condition $x_i = x_j = x_k = 0$ for distinct $i, j, k \in \{1, 2, 3, 4, 5\}$. For each triple i, j, k they give a point in X_t/G.

The Calabi-Yau manifold X_t has a unique (up to scalars) top degree differential form. It can be written down explicitely as follows:

$$\omega := \mathrm{Res}_{X_t}\left(\frac{\sum_{i=1}^{n}(-1)^i x_i \mathrm{d}x_1 \wedge \ldots \wedge \widehat{\mathrm{d}x_i} \wedge \ldots \wedge \mathrm{d}x_5}{F_t}\right),$$

where $F_t := x_1^5 + \ldots + x_5^5 - 5tx_1 \ldots x_5$.

This form is clearly invariant under the action of G. This means that $G \subset SL(3, \mathbb{C})$; hence the quotient has Gorenstein singularities. For these orbifolds there exists a desingularization, which is a smooth Calabi-Yau threefold Y_t. Moreover, by [19] the Hodge structure of the cohomology of Y_t is the same as the Hodge structure of the orbifold cohomology of X_t/G. Let us briefly recall the definition of these groups.

2.1 – The orbifold cohomology groups

We briefly summarize some facts on orbifold cohomology: for more details the reader is referred to [4]. Let X be an n-dimensional complex orbifold. Define $\widetilde{X}$ to be the set of pairs $(p, ((g))_{G_p})$ for $p \in X$ and (g) is the conjugacy class of g in the local isotropy group G_p. It is known that $\widetilde{X}$ is an orbifold called the *inertia orbifold*. This orbifold admits a decomposition in connected components, the nontwisted sector X and the twisted sectors $X_{(g)}$ for $g \neq 1$.

Any $g \in G_p$ acts on the tangent space T_pX via a diagonal matrix

$$D = \mathrm{diag}(e^{2\pi i r_1}, \ldots, e^{2\pi i r_n}),$$

where $r_i \in [0, 1)$. The degree shifting number $i_{(g)}$ is defined to be $\sum_i r_i$. If $g \in SL(n, \mathbb{C})$, then $i_{(g)}$ is an integer. Moreover, we have

$$i_{(g)} + i_{(g^{-1})} = n - dim_{\mathbb{C}} X_{(g)}. \tag{3}$$

The d-th orbifold group is defined to be

$$H^d_{orb}(X) := \bigoplus_{(g)} H^{d-2i_{(g)}}(X).$$

In particular, if $X = Y/G$ is a global quotient of a smooth variety Y by a finite group G, then

$$H^d_{orb}(X) := \bigoplus_{(g)\in G_*} H^{d-2i_{(g)}}(Y^g/C(g)),$$

where Y^g is the fixed locus of g, $C(g)$ is the centralizer in G, and G_* is a set of representatives of conjugacy classes in G.

Now, let us compute the Hodge numbers of Y_t. As before, it suffices to compute $h^{1,1}$ and $h^{2,1}$. The whole cohomology ring of the mirror quintic has been computed in [12]. Here we obtain the numbers mentioned above via direct methods.

Since X_t/G is Gorenstein, the degree shifting number is always an integer. The twisted sectors coincide with $Y^g/C(g)$ for $g \neq 1$. They are points or isomorphic to $\mathbb{P}^1$. By (3), the degree shifting number of g is 1 or 2, respectively. Clearly, the degree shifting number of the identity is zero.

A direct computation of the elements of G shows that there are 24 elements that do not fix anything, namely the S_4-orbit of $(1,2,3,4,0) \in G$. If three of the components of $g := (a_1, a_2, a_3, a_4, 0) \in G$ are equal, then g fixes a quintic curve whose image in X_t/G is a $\mathbb{P}^1$. If there are two pairs of the components of g that are equal, then g fixes ten points, which become two points under the quotient map $p : X_t \to X_t/G$.

Lemma 2.2.

i) *There are* 40 *elements* g *in* G *such that* $i_{(g)} = 1$ *and* $i_{(g^{-1})} = 1$.

ii) *There are* 30 *elements* g *in* G *such that* $i_{(g)} = 1$ *and* $i_{(g^{-1})} = 2$.

Proof.

i) We need to count all elements g such that $Y^g/C(g)$ is isomorphic to $\mathbb{P}^1$. As mentioned before, three components in $g = (a_1, a_2, a_3, a_4, 0)$ must be equal. This proves the claim.

ii) Since 24 elements do not move anything, we are left with $125 - 1 - 24 - 40 = 60$ elements. These come in pairs (g, g^{-1}). Therefore, ii) is completely proved. □

Proposition 2.3. *The Hodge numbers* $h^{1,1}(Y_t)$ *and* $h^{2,1}(Y_t)$ *are equal to* 101 *and* 1*, respectively.*

Proof. It suffices to compute $h^2_{orb}(X_t/G)$ and $h^3_{orb}(X_t/G)$. By definition, we have

$$h^2_{orb}(X_t/G) = h^2(X_t)^G \bigoplus_{g \neq 1} h^0(X_t^g/G).$$

We have $h^2(X_t)^G = 1$ since $h^2(X_t)$ is one-dimensional. By Lemma 2.2, we have $h^0(X_t^g/G) = 100$, since the elements in ii) yield two connected components in X_t^g/G. Note that $C(g) = G$ since the group is abelian.

As for $h^3_{orb}(X_t/G)$, we have

$$h^3_{orb}(X_t/G) = h^3(X_t)^G \bigoplus_{g \neq 1} h^1(X_t^g/G).$$

For $g \neq 1$ we have no contribution because X_t^g/G is either a point or a projective line. This leaves us with the computation of $h^3(X_t)^G$. The dimension of the space of invariants can be expressed in terms of the Euler characteristics of the fixed loci (Holomorphic Lefschetz Formula). In particular, we have

$$h^3(X_t)^G = \frac{1}{|G|} \sum_g tr\left(g^* | H^3(X_t)\right),$$

where g^* is the transformation induced by g on $H^3(X_t)$. Further, we have

$$\chi(X_t^g) = \sum_i (-1)^i tr\left(g^* | H^i(X_t)\right) = 4 - tr\left(g^* | H^3(X_t)\right).$$

Hence we have

$$h^3(X_t)^G = 4 - \frac{1}{|G|} \sum_g \chi(X_t^g).$$

On the other hand, X_t^g can be a plane quintic or 10 points. Therefore, we have

$$h^3(X_t)^G = 4 - \frac{1}{|G|} \{-200 + 40(-10) + 60(10)\} = 4.$$

Since $h^{3,0}(Y_t) = 1$, we have

$$h^{2,1}(Y_t) = h^{2,1}_{orb}(X_t/G) = \frac{1}{2}(4-2) = 1.$$

□

2.2 – Generalizations

The Dwork pencil can be generalized to any degree n. More precisely, we can consider the pencil $X_t^{n+1} \to \mathbb{P}^1$, where $X_t^{n+1} = Z(F_t^{n+1}) \subset \mathbb{P}^n$ and

$$F_t^{n+1} := \sum_i^{n+1} x_i^{n+1} - nt \prod_i^{n+1} x_i.$$

In [3] we investigate the geometry of this generalized pencil and its quotients by various automorphism groups. As n varies, the geometry might be rather intricate as the following proposition shows.

Let us consider the following subvariety Z of $\mathbb{P}^n$ for $n \equiv 0 \bmod 2$, namely:

$$\begin{cases} x_1 + \ldots + x_{n+1} = 0 \\ x_1^2 + \ldots + x_{n+1}^2 = 0 \\ \cdots\cdots\cdots \\ x_1^{n/2} + \ldots + x_{n+1}^{n/2} = 0 \end{cases}$$

LEMMA 2.4. *Let $\mathbb{Q}(\lambda)$ be an extension of the rational field. Choose $n-1$ distinct non-zero rational numbers $c_1, \ldots, c_{n-1}$. The determinant V of the Vandermonde matrix $V(\lambda, c_1, \ldots, c_{n-1})$ is not rational.*

PROOF. Suppose, on the contrary, that V is a rational number. If we expand with respect to the column of the powers of λ, it is easy to see that λ satisfies a polynomial with rational coefficients. Hence, the extension $\mathbb{Q}(\lambda)$ is algebraic and the Galois group is finite. If V is rational, it is fixed by any element σ of the Galois group. We thus have

$$\det \begin{pmatrix} 0 & 1 & \ldots & 1 \\ \lambda - \sigma(\lambda) & c_1 & \ldots & c_{n-1} \\ \ldots & \ldots & \ldots & \ldots \\ \lambda^{n-1} - \sigma(\lambda^{n-1}) & c_1 & \ldots & c_{n-1}^{n-1} \end{pmatrix} = 0.$$

The determinant of the matrix

$$\begin{pmatrix} c_1 & \ldots & c_{n-1} \\ \ldots & \ldots & \ldots \\ c_1^{n-1} & \ldots & c_{n-1}^{n-1} \end{pmatrix}.$$

is given by

$$c_1 c_2 \ldots c_{n-1} \prod_{r<s} (c_r - c_s),$$

which is different from zero. This means that the first column of the matrix in (4) is a linear combination with rational coefficients of the other columns, which are rational numbers. Thus, we have $(\sigma - I)(\lambda) = d \in \mathbb{Q}$. Suppose $\sigma^m = I$. If we apply $\sigma^{m-1} + \ldots + I$ to both members, we get $0 = md$; hence $\lambda = \sigma(\lambda)$ for any σ in the Galois group. This would mean that λ is rational against the assumptions. □

THEOREM 2.5. *The subvariety Z is smooth and is contained in X_1^{n+1}.*

PROOF. First of all, we notice that Z is defined by the equations $p_1 = p_2 = \ldots = p_{n/2} = 0$, where the p_j's are the Newton symmetric functions. The elementary symmetric functions e_j can be written in terms of the p_j. It is easy to check that the subvariety Z can be defined via the equations $e_1 = e_2 = \ldots = e_{n/2} = 0$. This said, we recall that X_1^{n+1} is given by $p_{n+1} - (n+1)e_{n+1} = 0$. Since n is even, this equation is equivalent to

$$\sum_{j=1}^{n} (-1)^{n+1-j} p_j e_{n+1-j} = 0. \tag{5}$$

If $e_1 = \ldots = e_{n/2} = 0$, then equation (5) is satisfied.

Second, the jacobian J of the system of equations defining Z is given by

$$\begin{pmatrix} 1 & \ldots & 1 \\ 2x_1 & \ldots & 2x_{n+1} \\ \ldots & \ldots & \ldots \\ \frac{n}{2}x_1^{\frac{n}{2}-1} & \ldots & \frac{n}{2}x_{n+1}^{\frac{n}{2}-1} \end{pmatrix}$$

If we choose any $n/2$ columns, we get a Vandermonde matrix. If a point of Z has at least $n/2$ different coordinates, there exists a minor of J different from zero. We need to show that a point with at most $n/2$ different coordinates does not belong to Z. This implies that Z is smooth. Suppose, on the contrary, that a point $P := [\lambda_0 : \ldots : \lambda_0 : \ldots : \lambda_{\frac{n}{2}-2} : \ldots : \lambda_{\frac{n}{2}-2}]$ belongs to Z. We can assume $\lambda_i \neq \lambda_j$. Let k_i be the number of times λ_i appears as a coordinate of P. Notice that $\sum_i k_i = n+1$. The λ_i's and the k_i's satisfy the following system of equations:

$$\text{(6)} \qquad \begin{cases} k_0 + \ldots + k_{\frac{n}{2}-2} = n+1 \\ \\ k_0\lambda_0 + \ldots + k_{\frac{n}{2}-2}\lambda_{\frac{n}{2}-2} = 0 \\ \\ k_0\lambda_0^2 + \ldots + k_{\frac{n}{2}-2}\lambda_{\frac{n}{2}-2}^2 = 0 \\ \\ \ldots\ldots\ldots\ldots \\ \\ k_0\lambda_0^{n/2} + \ldots + k_{\frac{n}{2}-2}\lambda_{\frac{n}{2}-2}^{n/2} = 0 \end{cases}$$

Let us consider the linear system $\Lambda X = N$, where Λ is the $(n/2+1) \times (n/2-1)$ matrix

$$\begin{pmatrix} 1 & \ldots & 1 \\ \lambda_0 & \ldots & \lambda_{\frac{n}{2}-2} \\ \ldots & \ldots & \ldots \\ \lambda_0^{n/2} & \ldots & \lambda_{\frac{n}{2}-2}^{n/2} \end{pmatrix},$$

X is the column of unknowns and N is the column vector $(n+1, 0, \ldots, 0)^t$. Since $\lambda_i \neq \lambda_j$, the matrix Λ contains a minor V of size $(n/2-1) \times (n/2-1)$ different from zero, so the system has a unique solution, which is given by the integers k_i for any given P. By standard linear algebra, we have

$$\text{(7)} \qquad k_l = (n+1)(-1)^{l+1}\frac{V_l}{\det(V)},$$

where V_l is the determinant of the matrix obtained from V by removing the l-th column.

Notice that if some of the λ_i's coincide, the k_i would be zero, so we would get a smaller system and we could proceed as in the case where $\lambda_i \neq \lambda_j$.

Third, we can assume that λ_i is in $\mathbb{Z}$ for any i. To do this, it suffices to show that under our assumptions all λ_i's are in the rational field. Suppose there exist $\lambda_{i_1}, \ldots, \lambda_{i_f}$ not in $\mathbb{Q}$. If $f \geq 2$, there exist λ_{i_r} and λ_{i_s} not in $\mathbb{Q}$. Then, there exists an element of the Galois group of the extension $\mathbb{Q}(\lambda_{i_1}, \ldots, \lambda_{i_f})$ over $\mathbb{Q}$ which exchanges λ_{i_r} and λ_{i_s}. It is easy to check that under this element k_{i_r} is mapped onto $-k_{i_s}$. Since k_{i_r} is an integer, we must have $k_{i_r} + k_{i_s} = 0$. This means that $k_{i_r} = k_{i_s} = 0$. In other words, we can disregard λ_{i_r} and λ_{i_s}. If f is even, we can disregard all the λ_i's not in $\mathbb{Q}$. If f is odd, we are left with the extension $\mathbb{Q}(\lambda_l)$ over $\mathbb{Q}$. In other words, there is only one λ_l not rational and the other ones are rational numbers. If we take into account k_l, then V_l is rational. Recall that the λ_j are all distinct. If none of them is zero, we reach a contradiction by Lemma 2.4. If one of them is zero (this is the only possible case because the λ's are all distinct), we can cancel a column from the matrix Λ and apply the result of Lemma 2.4.

Let us recap what we have proved so far. If P is a point in Z with at most $(n/2)-1$ different entries, the coordinates of P are integer numbers given by the formula (7). More explicitly, the solutions are given by

$$k_l = (n+1)(-1)^{l+1} \frac{\lambda_0 \ldots \widehat{\lambda_l} \ldots \lambda_t}{\prod_{r<l}(\lambda_r - \lambda_l)\prod_{s>l}(\lambda_l - \lambda_s)},$$

where $t = (n/2) - 2$ and $l \in \{0, \ldots, (n/2) - 2\}$. Since the subvariety Z is defined by symmetric equations, we can assume that the λ_i's are ordered so that $\prod_{r<l}(\lambda_r - \lambda_l)\prod_{s>l}(\lambda_l - \lambda_s)$ is positive.

Since $0 \leq k_l \leq n+1$, we should have

$$(-1)^{l+1}\lambda_0 \ldots \widehat{\lambda_l} \ldots \lambda_t \geq 0$$

for any l. If all the λ_i's were positive, k_0 would be negative against the assumptions. If the number of negative λ_i's is odd, k_0 would be negative. If the number of positive λ_i's is even, k_1 would be negative. If all the λ_i's are negative and t is odd, k_0 would be negative. If all the λ_i's are negative and t is even, k_1 would be negative. In any case, there exists a k_i which is negattive, whereas all the k_i's are positive by assumption. □

3 – Birational Models of the Mirror Quintic

It is important to understand whether a given Calabi-Yau is indeed new or birational to an existing one. Let us consider the following families:

	F_t
1	$x_1^5 + x_2^5 + \ldots + x_5^5 - 5tx_1x_2\cdots x_5$
2	$x_1^4x_2 + x_2^4x_3 + x_3^4x_4 + x_4^4x_5 + x_5^4x_1 - 5tx_1x_2\cdots x_5$
3	$x_1^4x_2 + x_2^4x_3 + x_3^4x_4 + x_4^4x_1 + x_5^5 - 5tx_1x_2\cdots x_5$
4	$x_1^4x_2 + x_2^4x_3 + x_3^4x_1 + x_4^5 + x_5^5 - 5tx_1x_2\cdots x_5$
5	$x_1^4x_2 + x_2^4x_3 + x_3^4x_1 + x_4^4x_5 + x_5^4x_4 - 5tx_1x_2\cdots x_5$
6	$x_1^4x_2 + x_2^4x_1 + x_3^5 + x_4^5 + x_5^5 - 5tx_1x_2\cdots x_5$

Each of them can be rewritten in the form

$$F_{A,t} := \sum_{i=1}^{5}\prod_{j=1}^{5} x_j^{a_{ij}} - 5tx_1x_2\cdots x_5,$$

where

$$a_{i1} + a_{i2} + \ldots + a_{i5} = 5, \quad a_{1j} + a_{2j} + \ldots + a_{5j} = 5.$$

If we set

$$z_i := \prod_{j=1}^{5} x_j^{a_{ij}}, \qquad z_1z_2\cdots z_5 = (x_1x_2\cdots x_5)^5,$$

we get the equations (2). This means that there exists a non-constant rational map

$$q_{A,t} : X_{A,t} \longrightarrow X_t/G, \qquad (x_1 : \ldots : x_5) \longmapsto (z_0 : z_1 \ldots : z_5),$$

where $z_0 := x_1x_2\cdots x_5$.

If we show that $q_{A,t}$ is birationally equivalent to a quotient map $X_{A,t} \to X_{A,t}/H_A$ for some group H_A, then Y_t is birational equivalent to $X_{A,t}/H_A$, thereby yielding a birational model of Y_t. In some cases, H_A is the identity group. We have shown that $q_{A,t}$ is birationally equivalent to a quotient map in [2]. To state the theorem, we need to define the group H_A.

Let d be the smallest positive integer such that $B := dA^{-1}$ has integer entries. Set

$$X_{dI,t} := Z(F_{dI,t}) \subset \mathbb{P}^{n-1}, \qquad F_{dI,t} = \sum_{j=1}^{n} y_j^d - nt\left(\prod_{j=1}^{n} y_j\right)^m,$$

$$d = mn.$$

We introduce a map

$$\phi_A : X_{dI,t} \longrightarrow X_{A,t}, \qquad (y_1 : \ldots : y_n) \longmapsto (x_1 : \ldots : x_n),$$

$$x_j = \prod_{k=1}^{n} y_k^{b_{jk}}.$$

For $a = (a_1, \ldots, a_n) \in (\mathbb{Z}/d\mathbb{Z})^n$ define the automorphism g_a on $\mathbb{P}^{n-1}$ in the following way:

$$g_a(y_1 : \ldots : y_n) := (\zeta^{a_1} y_1 : \ldots : \zeta^{a_n} y_n).$$

Set

$$\Gamma_d := \{g_a \,:\, a = (a_1, \ldots, a_n),\ a_1 + \ldots + a_n \equiv 0 \mod n\}/\langle g_{(1,1,\ldots,1)} \rangle.$$

It is an easy exercise to show that

$$\Gamma_d \cong \mathbb{Z}/m\mathbb{Z} \times (\mathbb{Z}/d\mathbb{Z})^{n-2}.$$

Γ_d induces an action on $X_{A,t}$. Indeed, we have:

$$\phi_A(g_a(y)) = (\zeta^{a'_1} x_1 : \ldots : \zeta^{a'_n} x_n),\ a'_j = \sum_{k=1}^{n} a_k b_{jk};$$

so

$$\Gamma_d \longrightarrow Aut(X_{A,t}), \qquad g_a \longmapsto g_{Ba} = g_{a'}. \tag{8}$$

Let Γ_A and H_A be the kernel and the image of the homomorphism (8). Then the following holds ([2])

THEOREM 3.1. *Let A be an $n \times n$ matrix with non-negative integer entries such that the sum of the entries in any row and column is equal to n and such that $X_{A,t}$ is irreducible. Then:*

$\phi_{A,t} : X_{dI,t} \longrightarrow X_{A,t}$, is birational to the quotient map

$$X_{dI,t} \longrightarrow X_{dI,t}/\Gamma_A,$$

$q_{A,t} : X_{A,t} \longrightarrow \overline{M}_t$, is birational to the quotient map

$$X_{A,t} \longrightarrow X_{A,t}/H_A,$$

and thus $q_{A,t} \circ \phi_{A,t} : X_{dI,t} \longrightarrow \overline{M}_t$, is birational to the quotient map

$$X_{dI,t} \longrightarrow X_{dI,t}/\Gamma_d.$$

REMARK 3.2. If we consider the second family

$$S_t := \left\{ x_1^4 x_2 + x_2^4 x_3 + \ldots + x_5^4 x_1 - 5t x_1 x_2 \ldots x_5 = 0 \right\},$$

the Theorem above and direct computation (with MAGMA) yield that S_t/H_t is birational to Y_t, where H_t is isomorphic to $\mathbb{Z}/41\mathbb{Z}$. This answers positively a conjecture posed by Greene, Plesser and Roan [8].

REFERENCES

[1] G. BINI: *Quotients of Hypersurfaces in Weighted Projective Space*, eprint arXiv: 0905.2099 to appear in Adv. in Geom.

[2] G. BINI – B. VAN GEEMEN – L. K. TYLER: *Mirror Quintics, discrete symmetries and Shioda Maps*, e-print arxiv:math/08091791v1, to appear in JAG.

[3] G. BINI – A. GARBAGNATI: *The geometry of the generalized Dwork pencil and its quotients*, in preparation.

[4] W. CHEN – Y. RUAN: *A new cohomology of orbifold*, Comm. Math. Phys. **248** (2004) 1–31.

[5] A. D. COX – S. KATZ: *Mirror Symmetry and algebraic geometry*, Mathematical Surveys and Monographs **68**, A.M.S, Providence, RI, 1999.

[6] C. DORAN – B. GREENE – S. JUDES: *Families of quintic Calabi-Yau 3-folds with discrete symmetries*, Comm. Math. Phys. **280** (2008) 675–725.

[7] B. R. GREENE – M. R. PLESSER: *Duality in Calabi-Yau moduli space*, Nucl. Phys. B **338** (1990) 15–37.

[8] B. R. GREENE – M. R. PLESSER – S. S. ROAN: *New constructions of mirror manifolds: Probing moduli space far from Fermat points*, Essays on Mirror Manifolds, editor S-T Yau, International Press (1992) 408–450.

[9] M. HARRIS – N SHEPHERD-BARRON – R. TAYLOR: *A family of Calabi-Yau varieties and potential automorphy*, available on: http://www.math.harvard.edu /∼rtaylor/.

[10] N. KATZ: *Another look at the Dwork family*, preprint.

[11] H. W. LIN: *On crepant resolution of some hypersurface singularities and a criterion for UFD*, Trans. Amer. Math. Soc. **354**,5, 1861–1868.

[12] B. D. PARK, M. PODDAR: *The Chen-Ruan cohomology ring of mirro quintic*, J. Reine Angew. Math. **578** (2005) 49–77.

[13] O. PRATOUSSEVITCH: *On the link space of a $\mathbb{Q}$-Gorenstein Quasi-Homogeneous surface singularties*, Real and complex singularities, São Carlos Workshop 2004, eds. J.P. Brasselet, M.A. Soares Ruas, Birkhä user, Basel, 2006.

[14] M. REID: *Canonical 3-folds*, Gèomètrie algèbrique d'Angers 1979, ed. A. Beauville, Sijthoff and Noordhoff 1980, Rockville, USA.

[15] J. SEADE: *On the topology of isolated singularities in analytic space*, Birkhäuser, Basel, 2006.

[16] C. SCHOEN: *On the geometry of a special determinantal hypersurface associated to the Mumford-Horrocks vector bundle*, J. Reine Angew. Math. **364** (1986) 85–111.

[17] C. Schoen: *Algebraic cycles on certain desingularized nodal hypersurfaces*, Math. Ann. **270**.

[18] T. Shioda: *An explicit algorithm for computing the Picard number of certain algebraic surfaces*, Amer. J. Math. **108** (1986) 415–432.

[19] T. Yasuda: *Twisted jet, motivic measure and orbifold cohomology*, Compos. Math. **140**, 2 (2004) 396–422.

Lavoro pervenuto alla redazione il 10 marzo 2010
ed accettato per la pubblicazione il 15 marzo 2010.
Bozze licenziate il 20 aprile 2010

Indirizzo dell'Autore:

Gilberto Bini – Dipartimento di Matematica – Università degli Studi di Milano – Via C. Saldini 50 – 20133 Milano – Italy
E-mail: gilberto.bini@unimi.it

Rendiconti di Matematica, Serie VII
Volume 30, Roma (2010), 47-66

Some models of geometries after Hilbert's Grundlagen

CINZIA CERRONI

Dedicated to Professor Marialuisa de Resmini

ABSTRACT: *We investigate the contribution of Max Dehn to the development of non-Archimedean geometries and the contribution of his student Ruth Moufang to the development of non-Desarguesian geometries.*

1 – Introduction

In 1899, David Hilbert published the *Grundlagen der Geometrie*, a book that opened up research in the foundations of geometry. In fact, the Grundlagen took the axiomatic method both as a culmination of geometry and as the beginning of a new phase of research. In that new phase, the links between the postulates were not seen as the cold expression of their logical relations or interdependence, but as the creation of new geometries having equal importance at the research level. In particular, the starting point of research on non-Archimedean geometries was the investigation of the independence of Archimedes'axiom[(1)] from other axioms and the starting point of research on non-desarguesian geometries was the investigation of the independence of Desargues'theorem[(2)] from the axioms of plane geometry.

KEY WORDS AND PHRASES: *David Hilbert – Max Dehn – Roberto Bonola – Ruth Moufang – Non-Desarguesian geometry – Non-Archimedean geometry – Octonions*
A.M.S. CLASSIFICATION: 01A70, 01A60, 51A35, 05B35, 17D05.

(1) As is well known, Archimedes'axiom states that if A and B are two segments, with A smaller than B ($A < B$), then there exists a positive integer n such that n times A is greater than B ($nA > B$).

(2) As is well known, Desargues's theorem states that if two triangles $a_1b_1c_1$, $a_2b_2c_2$ are in perspective from a point V, then the lines containing the opposite edges intersect in three collinear points, d_1, d_2, d_3.

The present paper aims to describe some models of non-Archimedean and non-desarguesian geometries that was born after the *Grundlagen*[3].

2 – Max Dehn and non-archimedean geometries

As is well known, Hilbert devoted Chapter II of his *Grundlagen der Geometrie* to proving the independence and non-contradictoriness of axioms. In particular, he proved the independence of Archimedes' axiom from the other ones. More precisely, he showed that Archimedes' axiom is not a consequence of axioms I (of incidence (connection)), II (of order), III (of parallelism), and IV (of congruence)[4] by exhibiting a geometry where Archimedes'axiom fails to be valid [Hilbert 1899].

On Hilbert's suggestion, Dehn studied the relationship between Legendre's theorems[5] and Archimedes'axiom. This last analysis is agreed with the point of view of Hilbert's Grundlagen. In fact, in the proofs of Legendre's theorems, that we can find in the literature (*i.e.* those of Euclid, those of Saccheri and those of Legendre himself) Archimedes'axiom is used, in a more or less explicit way. In the optic of Hilbert, and consequently of Dehn, it is remarkable to study whether these theorems really depend on this axiom.

Max Dehn was one of Hilbert's most prominent students. He was Born in Hamburg in 1878 and he received his doctorate in Göttingen at age twenty-one, under Hilbert's supervision, with the dissertation *Die Legendre'schen Satze über die Winkelsumme im Dreieck* on the foundations of geometry [Dehn 1900a]. He got his Habilitation in Munich in 1901, with a thesis in which he solved the third of the twenty-three problems Hilbert posed at the International Congress of Mathematicians in Paris in 1900 [Dehn 1900b],[Dehn 1901]; he was the first to solve one of Hilbert's problems. His solution showed that Archimede's axiom was needed to prove that two tetrahedra have the same volume, if they have the same altitudes as well as bases of the same area.

M. Dehn was Privatdozent in Munich from 1901 until 1911 and became Ordinarius in Breslau in 1913. He moved to the University of Frankfurt in 1921 where he lectured until 1935. Moreover, he published several valuable essays on the relationship between Greek philosophy and mathematics. In 1922 the seminar of history of Mathematics was founded, in Frankfurt, and Dehn was the

[3] This work is an elaboration of the two papers [Cerroni 2004], [Cerroni 2007], with some integrations.

[4] Usually, axioms III are on congruence and axioms IV are on parallelism,like in the more recent edition of the Grundlagen.

[5] These theorems are already in [Saccheri 1733], and in Italy they are called Saccheri's theorems. We recall that Legendre's theorems state that:

1. The sum of the angles of a triangle is equal to or less than two right angles.
2. If in a triangle the sum of the angles is equal to two right angles, it is so in every triangle.

driving force of this institution. The seminar on the history of Mathematics was held each semester until 1935. The rule of the seminar was to study the most important mathematical discoveries from all epochs in the original version.

In 1939, since he was a Jew, he emigrated from Germany to Copenhagen and later to Trondheim in Norway, where he took over the post of a vacationing colleague at the Technical University until 1940. Since German soldiers occupied Trondheim, Dehn and his wife, in October of 1941, emigrated to the United States via the trans-Siberian railway (from Moscov the tracks extended some 9,200 km to Vladivostok).

Dehn related their journey in a talk he gave at Idaho Southern not long after his arrival there [Dehn 1941]. According to that narrative, at the frontier between Norway and Sweden their luggage was "*ransacked*" and they were treated "*extremely unkindly and roughly*" by the border guards. They were delayed three weeks in Stockholm, apparently because of an outbreak of plague in Manchukuo and Vladivostok, but actually Dehn thought, for "*obscure political*" reasons. In the end they took the Amur River route and so did not pass through Manchukuo. At last the necessary tickets and travel document were issued, the Dehns were vaccinated and they flew on to Moscow.

During the several days they spent crossing the "*endless Russian plain*", the temperature at times fell low and Dehn developed a life-threatening combination of influenza and pneumonia, for which he was treated in Irkutsk. When the Dehns finally reached Vladivostok, they were forced to remain six more days while waiting for a ship to Kobe. The crossing to Japan proved to be very rough and cramped. He said nothing about the subsequent voyage to san Francisco, where he and his wife arrived on New Year's Day.

In United States, Dehn led a rather itinerant life until he found a position where he felt more or less comfortable. At the beginning Dehn spent one and a half year as a Professor of Mathematics and Philosophy at the State University of Idaho at Pocatello. The next year Dehn worked at the Illinois Institute of Technology in Chicago and after at St John's College in Annapolis, Maryland, where he was specially unhappy. Finally, in 1945 Dehn arrived at the final station in his life. This was Black Mountain College in North Carolina. He stayed there for the last 7 years of his life, leaving only for short periods as a guest lecturer in Madison, Wisconsin. He died in 1952 in Black Mountain, North Carolina [Dawson Jr. 2002], [Gillispie 1970-1990], [Siegel 1965].

M. Dehn, in his dissertation *Die Legendre'schen Sätze über die Winkelsumme im Dreieck*, analysed the relationship between Legendre's theorems and Archimedes' axiom. In particular, he asked:

"*Can one prove Legendre's theorems without an axiom of continuity, i.e. without making use of the Archimedian axiom?*"[(6)] [Dehn 1900a, p. 405].

[(6)] *The original texts in the following are faithfully translated by the author.*

To answer this question, Dehn first showed that Legendre's second theorem is only a consequence of the incidence, order and congruence axioms by proving, in a geometry (named *pseudogeometry*) [Dehn 1900a, pp. 406-411], where such axioms hold and Archimedes' axiom does not hold, the following more general theorem:

> "*If the angle sum of one triangle is less than two right angles then this is true for every triangle.*
> *If the angle sum of one triangle is equal to two right angles then it is so for every triangle.*
> *If the angle sum of one triangle is greater than two right angles then the same holds for every triangle.*" [Dehn 1900a, pp. 430-431].

Note that, the second statement is Legendre's second theorem.

Subsequently, Dehn showed that it is impossible to prove Legendre's first theorem with the incidence, the order, the congruence axioms and without Archimedes' axiom, by constructing a *Non-Legendrian Geometry* in which there are infinitely many lines parallel to a fixed line through a point, Archimede's axiom does not hold and the sum of the inner angles of a triangle is greater than two right-angles and constructing a *Semi-Euclidean Geometry* in which there are infinitely many lines parallel to a fixed line through a point, Archimede's axiom does not hold but the sum of the inner angles of every triangle is still equal to two right angles [Dehn 1900a, pp. 431-438].

2.1 – Hilbert analytic model of non-Archimedean geometry

Hilbert, in Chapter II of his *Grundlagen der Geometrie*, constructed a non-archimedean number system on which he based an analytic geometry. In particular, he considered the set $\Omega(t)$ consisting of the algebraic functions of t obtained from the set of polynomials with rational coefficients in t by the five operations of addition, subtraction, multiplication, division and the operation $\sqrt{1+\omega^2}$, where ω is a function derived from the previous five operations.

The set $\Omega(t)$ is countable and it can be regarded as the set of real- valued functions of a real variable defined at all but a finite number of points. Moreover, if c is a function in $\Omega(t)$, *i.e.* c is an algebraic function of t, it will vanish only on a finitely many values of t. Therefore, c, for positive large values of t, is either always positive or always negative. The usual operations are valid in $\Omega(t)$, and if a and b are two functions in $\Omega(t)$, a will be greater than b ($a > b$) or a less than b ($a < b$) if $a - b$ is always positive or always negative, respectively.

Let n be a positive integer, then n is less than t ($n < t$) since $n - t$ is always negative for large positive values of t. Consider the numbers 1 and t in $\Omega(t)$. Then, every multiple of 1 is always less than t, so $\Omega(t)$ is a non-archimedean number system.

Hilbert constructed an analytic geometry on this number system as follows: (x, y, z), where x, y, $z \in \Omega(t)$, is a point; $ux + vy + wz + r = 0$, where u, v, w, $r \in \Omega(t)$, is a plane; a line is the intersection of two planes [Hilbert 1899, pp. 24-26].

It easy to see that such a geometry is non-archimedean; indeed, on the basis of the above, a line segment the length of which is n times that of the unit segment will never exceed a segment of length t on the same line.

2.2 – The non-Legendrian Geometry

As it is well known, Legendre's first theorem affirms that the sum of the inner angles of a triangle is less or equal than two right-angles. Dehn showed that the Archimede axiom is needed to prove the previous theorem and analyzed the relationships between Archimede's axiom, the number of lines through a point parallel to a fixed line and the sum of inner angles of a triangle [Dehn 1900a, pp. 431-436].

It is known that if the Archimede axiom holds, there exists the following relationships between the hypothesis on the existence and the number of parallel lines through a point and the sum of the inner angles of a triangle: if the sum of the inner angles of a triangle is greater, equal or less than two right-angles then, no line passes through a point parallel to a fixed line, there exists exactly one line through a point parallel to a fixed line, there exist infinite lines through a point parallel to a fixed line, respectively.

Dehn constructed a non-archimedean geometry where through a point there exist infinite parallel lines and where the sum of inner angles of a triangle is greater than two right-angles, therefore as he wrote:

"*For all that is shown the non-validity of Legendre's first theorem and the hypothesis on the sum of the inner angles of a triangle, as Saccheri said, is not related with the hyphotesis on the existence and number of parallel lines through a point*" [Dehn 1900a, p. 432].

Dehn considered the non-archimedean number system introduced by Hilbert, that is the set $\Omega(t)$ of the algebraic functions of t obtained from t with the five operations of addition, subtraction, multiplication, division and the operation $\sqrt{1 + \omega^2}$, where ω is a function obtained by the previous five operations and constructed an analytic geometry over the set $\Omega(t)$ as follows: the points are the pairs (x, y), with x, y in $\Omega(t)$, and the lines have the equations $ux + vy + w = 0$, with u, v, w in $\Omega(t)$ [Dehn 1900a, p. 432]. In the previous geometry all the axioms hold with the exclusion of Archimede's axiom.

Dehn constructed, over this non-archimedean plane, an *elliptic* or *Riemanniann* geometry as follows. He took the conic

$$x^2 + y^2 + 1 = 0,$$

and considered as points and lines of the elliptic geometry, all the points and the lines of the non-archimedean plane together with the line at infinity with its points and, as congruences of the elliptic geometry, the real transformations that fix the conic[(7)]. Then, he considered, as points of the new geometry, the points of the *elliptic* geometry (x, y) satisfyting the following conditions:

$$\frac{-n}{t} < x < \frac{n}{t}$$
$$\frac{-n}{t} < y < \frac{n}{t}$$

where n is an integer, and as a lines, the lines whose points satisfied the previous condition [Dehn 1900a, pp. 433]. Dehn showed that all the axioms are valid except Euclid's axioms and Archimede's axiom and that the sum of the inner angles of a triangle is greater that two right-angles [Dehn 1900a, pp.433-436]. Thus, as he wrote:

"*We have constructed a geometry where axioms* I, II *and* IV *hold, where through one point there exist infinite lines parallel to a fixed line and where the sum of the inner angles of a triangle is greater than two right-angles. The Archimede axiom does not hold. Then it is shown that Legendre's first theorem does not hold without the help of the Archimede axiom. We call the constructed geometry "Non-Legendrian "geometry [...]*" [Dehn 1900a, p. 436].

2.3 – The Semi-Euclidean Geometry

Dehn continued his analysis on the relationship between the sum of inner angles of a triangle and the hypothesis on the existence and the number of parallel lines through a point by constructing another kind of geometry. He considered the above non-archimedean plane and constructed over it a new geometry as follows: the points of the new geometry are the points (x, y) of the non-archimedean plane satisfying the following condition,

$$-n < x < n$$
$$-n < y < n,$$

where n is a positive integer and the lines are the lines of the non-archimedean plane whose points satisfying the condition above [Dehn 1900a, p. 436]. Dehn showed that in this geometry axioms I, II and IV hold and moreover, since the segments and the angles are defined as in the euclidean geometry, Legendre's first theorem is valid:

(7) This construction was done by Klein [Klein 1871].

"*[. . .] Moreover, the theorems of the classic euclidean geometry are valid in the limited zone. The sum of inner angles is equal to two right-angles in every triangles.*" [Dehn 1900a, p. 437].

However, it is easy to see that through a point there exist infinite lines parallel to a fixed line. To show this Dehn considered the line through the points $(t, 0)$ and $(0, 1)$; this is a line of the new geometry, since it passes through the points $(0, 1)$ and $(1, \frac{t-1}{t})$ which are points of the new geometry, but intersects the x axis in a point that is not a point of the new geometry. Then, he considered the line through the points $(-t, 0)$ and $(0, 1)$; this line is a line of the new geometry which intersects the x axis in a point that is not a point of the new geometry. The two previous lines pass through the point $(1, 0)$ and are parallel to the x axis. So, Dehn showed that:

"*This is a non-archimedean geometry in which the parallel axiom is not valid but where the sum of the inner angles of a triangle is equal to two right-angles.*" [Dehn 1900a, p. 438].

Thus, Dehn constructed a geometry where the theorems of the Euclidean geometry hold, but where the parallel axiom does not; Dehn called this geometry *Semi-Euclidean* geometry.

Hilbert was struck by this kind of geometry which he called a *remarkable geometry* so that he constructed, in his lectures on foundations of geometry of 1902, another model of *semi-Euclidean* geometry, inspired by Dehn's result [Hallet and Ulrich 2004].

Dehn summed up the previous results in the following diagram:

The sum of the inner angles of a triangle is:	Lines through a fixed point and parallel to a given line:		
	No parallel lines	One parallel line	Infinite parallel lines
$> 2R$	Elliptic Geometry	(impossible)	Non-Legendre geometry
$= 2R$	(impossible)	Euclidean geometry	Semi-Euclidean geometry
$< 2R$	(impossible)	(impossible)	Hyperbolic geometry

Hilbert also summarized the results in detail in his conclusion to the French and English translations of the *Festschrift* [Hilbert 1899], and from the second

edition of the *Grundlagen*, there are short remarks on Dehn's work at the end of Chapter III.

3 – Italian school and Bonola research on Saccheri's theorem

A pioneer in the study of non-archimedean geometry was Giuseppe Veronese (1854-1917). In the work *Fondamenti di Geometria* [Veronese 1891] he constructed, in abstract manner, a geometry in which he postulated the existence of a segment which is infinitesimal with respect to another, and where the straight line of geometry is not equated with the continuous straight line of Dedekind.

This work brought about many critics and it caused a national and international discussion[(8)] which involved, from the others, Rodolfo Bettazzi (1861-1941), George Cantor (1845-1918), Wilhelm Killing (1847-1923), Tullio Levi Civita (1873-1941), Giuseppe Peano (1858-1932), Arthur Moritz Schönflies (1853, 1928), Otto Stolz (1842-1905), and Giulio Vivanti (1859-1949).

In 1893 there is a turning-point in the discussion; Tullio Levi Civita published the work *Sugli infiniti ed infinitesimi attuali quali elementi analitici* [Levi Civita 1893] in which he constructed from the reals number, in an analitically way, a number system whose numbers (the *monosemii*) are the marks of the infinite and infinitesimal segments of Veronese.

The discussion about the possibility of the existence of infinite and infinitesimal segments ended with the publication of Hilbert's *Grundlagen*, as we have seen in the previous sections and it is possible that the international discussion influenced Hilbert, who knew the work of Veronese and referred to it as *deep work* [Hilbert 1899, p. 48].

Strangely enough, the approach of Veronese, who anticipated from many points of view Hilbert's work, did not eventually produce an Italian school in this kinds of studies[(9)]. So mach so that, R. Bonola was more influenced by the works of M. Dehn than the ones of G. Veronese.

Roberto Bonola was born in 1874 in Bologna and there died prematurely in 1911. He graduated in Mathematics in 1898 under the supervision of F. Enriques, who choose him as his assistant. In 1900 he became a teacher of mathematics in schools for girls, first in Petralia Sottana, then in Pavia, where he spent the best years of his short life. In 1902 he became assistant to the course of Calculus at the University of Pavia and in 1904 he gave lectures on the Foundations of

[(8)] See for examples the works [Bettazzi 1891], [Bettazzi 1892], [Cantor 1895], [Cantor 1897], [Killing 1895-1897], [Killing 1897], [Levi Civita 1893], [Levi Civita 1898],[Peano 1892], [Peano 1892a], [Schönflies 1897], [Schönflies 1897a], [Stolz 1883], [Stolz 1891], [Veronese 1892], [Veronese 1896], [Veronese 1897], [Veronese 1898], [Vivanti 1891], [Vivanti 1891a].

[(9)] For a study in depht of the Italian question see [Avellone et al. 2002] and [Bottazzini 2001].

Geometry. Moreover, from 1904 to 1907, he taught a mathematics course for Chemistry and Natural Science students. In 1909 he obtained the *Libera Docenza* of Projective Geometry and in 1910 he became Ordinary Professor on the Regio Istituto Superiore di Magistero femminile in Rome. He was seriously sick since 1900 and he died while he established in Rome. [Amaldi 1911].

Bonola was among the very few Italians who were deeply interested in Dehn's work. At the time, he was working under the supervision of Enriques on non-Euclidean geometry from an historical point of view [Bonola 1906], which can be considered his main work.

He was thus deeply interested in understanding the role of Archimedes' axiom in the proof of Saccheri's theorem[(10)]. In his work [Bonola 1905], he demonstrated, in a direct way without the use of Archimedes' axiom, Saccheri's theorem on the sum of the inner angles of a triangle:

"*This note aims at giving a direct and elementary proof of the result by Dehn, that is of the proof of Saccheri's theorem, without the use of Archimedes' axiom.*" [Bonola 1905, p. 652].

In fact, Bonola shared his master's (F. Enriques) vision of geometry, *i.e.* as a deeply intuitive discipline. Thus, only a direct proof could really satisfy our intuitive vision:

"*The way followed by Dehn to prove, without Archimedes' axiom, Saccheri's theorem is very elegant and logically complete. Geometrical intuition, however, needed a direct proof, that is a proof without formal systems, constructed over abstract concepts, that only formally satisfies the geometrical properties.*" [Bonola 1905, p. 652].

He started from the research of Father Saccheri [Saccheri 1733] on Euclid's V axiom. He considered the birectangular isosceles quadrilateral ABCD (= 1 right angle and AB=CD), that is now called the Saccheri Quadrilateral and distinguished the three Hypothesis: the one of the right angle, the one of the acute angle and the one of the obtuse angle.

He then demonstrated Saccheri's theorem: "*If one of the three previous Hypotheses is valid in a Saccheri Quadrilateral, this hypothesis is valid in every Saccheri Quadrilateral*" without using Archimedes' axiom and since Saccheri's theorem on the sum of the inner angles of a triangle is a consequence of this theorem, the aim is achieved [Bonola 1905]. To prove Saccheri's theorem, he considered a plane in which the axioms of connection, order, and congruence are satisfied, distinguishing two cases: *the closed line* and *the open line.*

[(10)] Bonola called Saccheri's theorem the second theorem of Legendre.

4 – M. Dehn research program, Moufang planes and their coordinatizating algebra

As we have seen in the previous sections, the foundations of geometry represent a type of mathematical inquiry that highly suited some characteristic features of Dehn's mind. However, he was not primarily interested in finding minimal sets of axioms or in separating the postulates of a given discipline into sets of weaker ones and then proving their independence and completeness. That kind of axiomatic approach is well represented by Moritz Pasch (1843-1930), whose book *Vorlesungen über neuere Geometrie* first appeared in 1882. The second edition of this book appeared in 1926 with a supplementary part by Dehn, entitled *Die Grundlegung der geometrie in historischer Entwicklung* [Dehn 1926]. Whereas Pasch emphasized precision and detail, Dehn focused on insight and ideas. He was interested in finding solid and simple foundations for a theory, in particular for projective geometry:

"*[t]he aim of the foundations of projective geometry, as well as of metric geometry, is to transform the projective relations (collineations) into algebraic relations.*" [Dehn 1926, pp. 213-214].

As this makes clear, Dehn was interested in the relationships between algebra and geometry. In particular, he was deeply impressed by the part of Hilbert's *Grudlagen* in which it is showed that the incidence axioms of (projective) geometry together with a single incidence theorem, namely, Pappus's theorem, are equivalent to the definition of a field, and that the same axioms together with Desargues's theorem define a skew field [Magnus and Maufang 1954], [Magnus 1978-1979].

This kind of approach was to become a real *Research Program* for Dehn and he inspired many students. One of Dehn's students was Ruth Moufang. In a series of difficult papers, she proved that there exists a third theorem of the type of Desargues and Pappus, *the theorem of the complete quadrilateral*.

Ruth Moufang was born in Darmstadt, Germany on 10 January, 1905. Her interest in mathematics was first stimulated at the Realgymnasium in Bad Kreuznach, which she attended from 1921 to 1924. She then studied mathematics at the University of Frankfurt from 1925 until 1930 and she passed the teacher's examination in 1929.

She took her Ph.D. in 1931 under Dehn's supervision with a dissertation on projective geometry. After, she spent a year in Rome with a research fellowship. She lectured from 1932 to 1933 at the University of Königsberg, where she took a course with Emmy Noether, was encouraged in the study of mathematics by Kurt Reidemeister (1893-1971), and met Richard Brauer (1901-1977).

She returned to Frankfurt in 1934 and held a Lehrauftrag there while writing her Habilitationsschrift. On 9 February, 1937, Ruth Moufang became the third woman in Germany to receive the Habilitation in mathematics.

The logical course of events would have been for her to become a Privatdozent, but in March 1937, she received a letter from the Ministry of Education informing her that the policies of the Third Reich required a professor to be a *leader* of students in more than just the academic sphere. Since the student population was mostly male, they did not think it feasible to appoint women professors.

Although they had no objection if she devoted herself solely to research, since there was no permanent position at the university to do only research, she left to work for the Krupps Research Institute in the autumn of 1937 and stayed there until 1946. She was the first German woman with a doctorate to be employed as an industrial mathematician. In this period, she published several papers in theoretical physics, in particular elasticity theory [Moufang 1941-1942], [Moufang 1946-1947], [Moufang 1948].

After the war, the University of Frankfurt was looking for first-rate mathematicians who had not joined any Nazi organization under Hitler. In 1946, Moufang moved there and was given the venia legendi. She served as Privatdozent until her appointment as associate professor in December 1947. In February 1957, she became the first woman in Germany to be appointed full professor and remained at the University of Frankfurt until her retirement in 1970. In the postwar years, she published almost nothing, although she was a successful teacher and had many Ph.D. students. She died in Frankfurt on 26 November, 1977.

4.1 – Moufang planes

Moufang's works from 1931 and 1937[(11)], marked the starting point of a new mathematical specialty in the algebraic analysis of projective planes that drew upon a mixture of geometry and algebra. She studied what are known today as *Moufang planes* and *Moufang loops*. Her studies became part of the foundations of geometry and were inspired by Max Dehn's work.

Her dissertation of 1931 inaugurated the systematic study of non-Desarguesian planes. In her first works, written between 1931 and 1932 and suggested by M. Dehn, she studied problems about *incidence theorems* in a projective plane. In particular, she investigated, in general, when one incidence configuration follows from another and examined what the consequences of this are on the introduction of coordinates:

"*[t]he following study which has arisen from a suggestion of Herr Dehn, is at the foundations of a very general problem in projective planes: let there be two incidence configurations, the problem is to decide whether or not, under*

[(11)] See [Moufang 1931], [Moufang 1931a], [Moufang 1932], [Moufang 1932a], [Moufang 1933], [Moufang 1933a], [Moufang 1934], [Moufang 1937].

the axioms of order and incidence, one follows from the other." [Moufang 1931, p. 536].

In her main work, *Alternative Körper und der Satz von Vollstadingen Vierseit* (D_9) [Moufang 1933a], she constructed the non-Desarguesian planes coordinatizited by an alternative division ring[(12)] (of characteristic $\neq 2$), that now are named *Moufang planes*, exhibiting a delicate interplay between geometry and algebra.

Of particular interest here, however, is how Moufang hit upon the idea of relating alternative division rings to the geometric construction of Moufang planes. As noted, Moufang's early work concerned the problem of considering the relationship between various *theorems on configurations* in a projective plane. In the paper *Die Schnittpunktsätze des projektiven speziellen Fünfecknetzes in ihrer Abhängigkeit voneinander* [Moufang 1932], proposed by Max Dehn, she investigated some special cases of Desargues's theorem, analyzing whether from one of these configurations the other ones follow and whether they are equivalent to the complete quadrilateral theorem.

In particular, she considered a special case of Desargues's theorem, which she called D_9. Here, the triangles $1'2'3'$ and 123 are in perspective with respect to the point a, one side of each triangle goes through one vertex of the other, two vertices of one of the perspective triangles lie on two sides of the other one.

At this point in her argument, Moufang followed Hilbert's method. As she explained,

"*[w]e now investigate, as in Hilbert's Grundlagen der Geometrie (Chapter V, 7th Edition), to what extent the calculus of a skew field (which obtains in the presence of Desargues's theorem) obtains under the configuration* D_9". [Moufang 1932, p. 766].

Therefore, she introduced the operations of addition and multiplication, as in the *Grundlagen*, by using D_9 and obtained the following rules:

$$(*) \qquad \begin{aligned} \alpha+\beta &= \beta+\alpha \\ (\alpha+\beta)+\gamma &= \alpha+(\beta+\gamma) \\ \alpha(\beta+\gamma) &= \alpha\beta+\alpha\gamma \\ (\beta+\gamma)\alpha &= \beta\alpha+\gamma\alpha \end{aligned}$$

if $\alpha \neq 0$, then there exists α^{-1}, such that $\alpha^{-1}\alpha = 1 = \alpha\alpha^{-1}$, and $\alpha^{-1}(\alpha\beta) = \beta = (\beta\alpha)\alpha^{-1}$. [Moufang 1932, pp. 767-771].

[(12)] Recall that an alternative division ring is a triple $(A, +, \cdot)$, where $(A, +)$ is an Abelian group and where $(A, \cdot)$ is a quasigroup with identity (loop), in which the distributive laws and the *alternative laws* are satisfied: $\forall a, b \in, A\ a(ab) = (aa)b$, $a(ba) = (ab)a$, $(ba)a = b(aa)$. The multiplication is thus, in general, non-associative.

Thus, she showed that, in general, the multiplication is non associative.

In [Moufang 1932], she did not recognize the equivalence between a structure with properties (*) and an alternative division ring. She also neither constructed planes coordinatized by such a structure nor showed that D_9 is weaker than Desargues's theorem. In fact, her paper was completely geometric and ended with the following question: can Desargues's theorem follow from the configuration D_9? She conjectured an answer in the negative.

After completing this work, Moufang went, to Königsberg in 1932, where she was influenced by both Reidemeister and Brauer. Her stay there was decisive for her growth as an algebraist and for her subsequent research.

In fact, her main work, *Alternative Korper und der Satz von Vollstadingen Vierseit* (D_9) [Moufang 1933a] was written while she was in Königsberg. There, she thanked Brauer explicitly "*for the hint that, according to the introduction of the paper of Herr Zorn*", the number system she had constructed was a "*generalization of Cayley's number system, as presented in* 133*, Dickson's Algebren und ihre Zahlentheorie* (*p.* 264)", namely, a Cayley-Dickson system [Moufang 1933a, p. 222].

This paper is more algebraic than the others, she exhibited a delicate interplay between geometry and algebra. Her approach was systematic and followed Hilbert's method:

"*Hilbert had shown that a subset of his axioms for plane geometry (essentially the incidence axioms) together with the incidence theorem of Desargues allows for the introduction of coordinates on a straight line that are elements of a skew field.*

He proceeded as follows: he had defined the operations of addition and multiplication and their inverses, using the incidence theorems. So, Desargues's theorem and the incidence axioms are sufficient to prove the calculus rules except for the commutative rule of multiplication. Conversely, he had constructed a geometry in which Desargues's theorem is valid, by using the elements of a skew field.

We investigate in the same way, by using a particular case of Desargues's theorem, which is equivalent to the theorem of the complete quadrilateral (we call this theorem D_9*).*" [Moufang 1933a, p. 207].

Therefore, she first considered a plane coordinatized by a structure that satisfies (*) and proved, following Hilbert's method, that it is a projective plane and that the configuration D_9 is valid [Moufang 1933a, p. 211-215]. She also established the equivalence of D_9 and an alternative division ring in a purely algebraic way [Moufang 1933a, pp. 216-219], by showing that a structure that satisfies (*) satisfies the *alternative rules*, and conversely. She closed, as Hilbert did, by exhibiting a non-Desarguesian number system and by constructing what are now called *Moufang planes.*

Thus, whereas Hilbert had shown that Desargues's theorem together with the incidence axioms of planes allows one to introduce coordinates in a projective

plane which are elements of a skew field, and conversely, Moufang proved that the configuration D_9 (or, equivalently, the complete quadrilateral theorem) holds in a projective plane if and only if it can be coordinatized by an alternative division ring (of characteristic $\neq 2$). The non-Desarguesian Moufang planes are of this type.

While Moufang planes are not the first examples of non-Desarguian planes, they are very important since they gave rise to the systematic study of such planes. Ruth Moufang recognized the connections between the geometric properties of planes and the algebraic properties of the coordinatizing structure. In 1943, Marshall Hall introduced a general way to coordinatize every projective plane by planary ternary rings and provided a classification that exploited the relationship between the algebraic and geometric properties [Hall 1943]. Moufang's results and techniques thus led in a crucial way to a *modern* method of classification of algebraic and geometric structures.

4.2 – The Alternative division ring

The general structure of alternative division ring was risen with the discovery of the Octonions, who are an example of such structure. Here, we sketch their history. The Octonions were discovered in 1843 by John Thomas Graves (1806-1870), who called them octaves. He was an Irish jurist, a mathematician and he was a friend of W.R. Hamilton. He is credited both with inspiring Hamilton to discover the Quaternions [Baez 2001].

The Octonions were discovered independently by Arthur Cayley (1821-1895) who published the first paper on them in 1845 [Cayley 1845]. Subsequently, in 1847 Cayley showed that they are not associative [Cayley 1847] and in 1881 he found their moltiplicative table [Cayley 1881]. Therefore, they are sometimes referred to as Cayley numbers or the Cayley algebra.

In 1912, after 31 years, Leonard Eugene Dickson (1874-1954) showed that the Octonions are a division ring [Dickson 1912] and in 1914 he found a new description of the Octonions as an ordered pairs of quaternions, with multiplication and conjugation defined exactly as for the quaternions [Dickson 1914]. This description is called Cayley-Dickson construction.

Max Zorn first introduced abstract alternative division rings in his paper, *Theorie der alternativen Ringe* [Zorn 1930], after he has noted that Cayley numbers satisfies the "Alternative laws"; he credited with Emil Artin (1898-1962) some results. Zorn also showed that a finite alternative division ring is a skew field. It followed that a finite Moufang plane is Desarguesian.

R. Moufang also opened up new avenues in the field of abstract algebra. In the work [Moufang 1934], she studied the multiplicative structure of alternative division rings, constructing the objects now called *Moufang loops*. The main theorem in this area was then showed by L.A. Skornjakov [Stornjakov 1950,

pp. 74-84] and Richard Bruck and Erwin Kleinfeld [Bruk and Kleinfeld 1951, p. 887], namely, that any alternative division ring of characteristic $\neq 2$ is either associative or a Cayley-Dickson algebra over its center.

The intrinsic link between the Moufang planes and the Octonions was further confirmed by studies of Ernst Pasqual Jordan (1902-1980). In 1949, he showed that the idempotent elements of the exceptional algebra $h_3(\mathcal{O})$[(13)] are a Moufang plane [Jordan 1949].

In the first half of '900 was found a link between the Octonions and the theory of Lie algebras. Between 1887 and 1890 Wilhelm Killing classified the simple Lie algebras and he recognized the five exceptional algebras, and then the corresponding five exceptional Lie groups: G_2, F_4, E_6, E_7, E_8. The Octonions intervened in this context, because, it is possible to describe four of these exceptional groups through to them.

In 1914, Elie Cartan (1869-1951) showed that the group of automorphisms of the Octonions is G_2 [Cartan 1914]. In 1950, Armand Borel (1923-2003) observed that F_4 is the group of isometries of the Moufang plane [Borel 1950]. In the same year Claude Chevalley (1909-1984) and Richard Schafer (1918 -) showed that F_4 is the automorphism group of the exceptional Jordan algebra $h_3(\mathcal{O})$ and they described E_6 as the group of linear transformations of $h_3(\mathcal{O})$ that preserves the determinant [Chevalley and Schafer 1950]. Finally, in 1954 Hans Freudenthal (1905-1990) described the group E_7 as the automorphisms group of a 56-dimensional structure of Octonions [Freudenthal 1954].

5 – Conclusions

It follows from the previous considerations that the approach of Hilbert was at least partially realized by his students, in particular by Max Dehn. Dehn's approach was "modern", and he was interested, moreover, precisely in the mutual interrelation between algebraic structure and geometric relations. This point of view marked the starting point of a "new mathematics", one whose principal author was Ruth Moufang. In her works, she embraced Dehn's "modern" approach as well as ideas on "structural" algebra that were increasingly defining a school of algebraic research around Emmy Noether.

We may, also, note that Veronese's pioneering work did not give rise to a real mathematical school, but to a lasting debate on the subject of non-Archimedean geometry also within Italian geometers. Infact, what it is happened in German and in America did not happen in Italy. Before Hilbert, the contributions of the Italian geometrical school, with Riccardo De Paolis (1854-1892), Federico Enriques (1871-1946), Gino Fano (1871-1952), Giuseppe Peano (1858-1932), Mario

(13) Which is the algebra of Hermitian matrices over Octonions with product $ab = \frac{1}{2}(ab + ba)$.

Pieri (1860-1913), Corrado Segre (1863-1924) and Giuseppe Veronese (1854-1917) to the Foundantions of Projective Geometry were considerable.

After Hilbert, the foundations of geometry in Italy were totally replaced by the works of the German and the American schools. One of the reasons was that the Italian school considered the foundations as the end of a process of building a geometric theory [Avellone et al. 2002] contrary to the Grundlagen that inspired a new phase of geometry researches, as we have seen.

Furthermore, we find interesting to analyze the "case" of the Octonions. In fact their history shows how an abstract theory can find unexpected applications long after its introduction. It seemed that the role of the Octonions in Mathematics was simply to be an example of non-associative structure and even within the same Cayley after their introduction, forgot to them for about 30 years. As we have seen, it was due to arrive in the first half of the twentieth century to find their first important applications both the projective geometry and the theory of Lie.

Surprisingly, in the eighties it was assumed a link between the Octonions and the String theory. The physicists have found that in the spaces of dimensions 3, 4, 6 and 10 each spinor can be represented as a pair of elements of the same algebra. This is satisfied only if the space has dimension 2 plus the dimensions of a normed division algebra. So that, from the dimensions 1, 2, 4, 8 are obtained just 3, 4, 6 and 10. Therefore, the String theories candidate to be defined are, respectively, the Real, the Complex, the Quaternionic and the Octonionic and it seems that the most authoritative to be a model of physical reality is just that Octonionic.

This assumption made them return the focus of scientific research today and made them the protagonists of many books both informative and technical as [Stewart 2008], [Conway and Smith 2003].

REFERENCES

[Amaldi 1911] U. Amaldi: *R. Bonola, Bollettino Mathesis*, 3, 1911, pp.145–152.

[Avellone et al. 2002] M. Avellone – A. Brigaglia – C. Zappulla: *The Foundations of Projective Geometry in Italy from De Paolis to Pieri*, Arch. Hist. Exact Sci., **56** (2002) pp. 363–425.

[Baez 2001] J. C. Baez: *The Octonions*, Bulletin of the American Mathematical Society **39**,2 (2001) pp. 145–205.

[Bettazzi 1891] R. Bettazzi: *Osservazioni sopra l'articolo del Dr. G. Vivanti Sull'infinitesimo attuale*, Rivista di Matematica, **1** (1891) pp. 174–182.

[Bettazzi 1892] R. Bettazzi: *Sull'infinitesimo attuale*, Rivista di Matematica, **2** (1892) pp. 38–41.

[Bonola 1905] R. Bonola: *I teoremi del Padre Girolamo Saccheri sulla somma degli angoli di un triangolo e le ricerche di M. Dehn*, Rendiconti dell'Istituto Lombardo, serie II, **28** (1905) pp. 651-662.

[Bonola 1906] R. Bonola: *Geometria Non-Euclidea*, N. Zanichelli, Bologna, 1906.

[Borel 1950] A. Borel: *Le plan projectif des octaves et les sphéres commes espaces homogènes*, Compt. Rend. Acad. Sci., **230** (1950) pp. 1378–1380.

[Bottazzini 2001] U. Bottazzini: *I geometri italiani e il problema dei fondamenti (1889-1899)*, Boll. Unione Mat. Ital. Sez.A Mat. Soc. Cult., **4**, 8 (2001) pp. 281–329.

[Bruck, Kleinfeld 1951] R. H. Bruck – E. Kleinfeld: *The structure of alternative division rings*, Proc. Amer. Math. Soc., **2** (1951) pp. 878–890.

[Cantor 1895] G. Cantor: *Beiträge zur Begründung der transfiniten Mengenlehre, I*, Math. Ann., **46** (1895) pp. 481–512.

[Cantor 1897] G. Cantor: *Beiträge zur Begründung der transfiniten Mengenlehre, II*, Math. Ann., **49** (1897) pp. 207–246.

[Cayley 1845] A. Cayley: *On Jacobi's elliptic functions, in reply to the Rev. B. Bronwin; and on quaternions*, Philosophical Magazine, **26**, 172 (1845) pp. 208–211.

[Cayley 1847] A. Cayley: *Note on System of Imaginaries*, Philosophical Magazine, **30** (1847) pp. 257–258.

[Cayley 1881] A. Cayley: *On the 8-square Imaginaries*, American Journal of Mathematics, IV (1881) pp. 293–296.

[Cartan 1914] E. Cartan: *Les groupes reels simples finis et continues*, Ann. Sci. École Norm. Sup., **31** (1914) pp. 255–262.

[Chevalley, Schafer 1950] C. Chevalley – R. D. Schafer: *The exceptional simple Lie algebras F_4 and E_6*, Proc. Nat. Acad. Sci.U.S.A., **36** (1950) pp. 137–141.

[Cerroni 2004] C. Cerroni: *Non-Desarguian geometries and the foundations of geometry from David Hilbert to Ruth Moufang*, Historia Mathematica, **31** (2004) pp. 320–336.

[Cerroni 2007] C. Cerroni: *The contributions of Hilbert and Dehn to non-Archimedean geometries and their impact on the italian school*, Revue d'Histoire des Mathèmatiques, **13**, 2 (2007) pp. 273–313.

[Conway, Smith 2003] J. H. Conway – D. A. Smith: *On Quaternions and Octonions: Their Geometry, Arithmetic, and Symmetry*, A K Peters, 2003.

[Dawson Jr. 2002] Jr. J. W. Dawson – M. Dehn – K. Gödel – the Trans-Siberian escape Route: *Notices of the AMS*, **49**, 9, pp.1068–1075.

[Dehn 1900a] M. Dehn: *Die Legendreschen Sätze über die Winkelsumme im Dreieck*, Math. Ann., **53** (1900) pp. 404–439.

[Dehn 1900b] M. Dehn: *Über raumgleiche Polyeder*, Göttinger Nachrichten, 1900, pp. 345–354.

[Dehn 1901] M. Dehn: *Über den Rauminhalt*, Math. Ann., **55** (1901) pp. 465–478.

[Dehn 1926] M. Dehn – M. Pasch: *Vorlesungen über neuere Geometrie*, Julius Springer, 2nd edition, 1926.

[Dehn 1941] M. Dehn: *Untitled account of trans-Siberian emigration*, 8 page typescript, Dehn papers, Archive of American Mathematics, University of Texas at Austin, 1941.

[Dickson 1912] L. E. Dickson: *Linear Algebras*, Trans. Amer. Math. Soc., **13** (1912) pp. 59–73.

[Dickson 1914] L. E. Dickson: *Linear Algebras*, Cambridge, 1914.

[Freudenthal 1954] H. Freudenthal: *Beziehungen der e_7 und e_8 zur Oktavenebene I,II*, Indag. Math., **16** (1954) pp. 218–230; 363–368.

[Gillispie 1970-1990] C. G. Gillipsie: *Dictionary of Scientific Biography*, Charles Scribner's Sons, 1970-1990; 16 vols. and 2 supps.

[Hall 1943] M. Hall: *Projective planes*, Trans. Amer. Math. Soc., **54** (1943) pp. 229–277.

[Hallet, Ulrich 2004] M. Hallet – M. Ulrich: *David Hilbert's Lectures on the Foundations of Geometry*, 1891-1902, David Hilbert's Foundational Lectures, vol. 1, Berlin: Springer, 2004.

[Hilbert 1899] D. Hilbert: *Grundlagen der Geometrie*, Festschrift zur Feier der Enthüllung des Gauss-Weber Denkmals in Goettingen. Herausgegeben von dem Fest-Comitee. Auflage 1. Teubner, Berlin, 1899; fr. tr. L. Laugel, Les principes fondamentaux de la géométrie. Festschrift publiée à l'occasion des fêtes pour l'inauguration du monument Gauss-Weber à Göttingen, Annales scientifiques de l'école normale supérieure, (3^e série) 17, 1900, pp. 103–209; eng. tr E.J. Townsend, The Foundations of Geometry, Chicago: The Open Court Publishing Company, 1902.

[Jordan 1949] P. Jordan: *Über eine nicht-desarguessche ebene projektive Geometrie*, Abh. Math. Sem. Hamburg, **16** (1949) pp. 74–76.

[Killing 1895-1897] W. Killing: *Bemerkungen über Veronese's Transfiniten Zahlen*, Index Lectionun, Münster Universität, 1895-96

[Killing 1897] W. Killing: *Über Transfinite Zahlen*, Math. Ann., **48** (1897) pp. 425– 432.

[Klein 1871] F. Klein: *Über die sogenannte Nicht-Euklidische Geometrie*, Math. Ann., **4** (1871) pp. 573–625.

[Levi Civita 1893] T. Levi Civita: *Sugli infiniti ed infinitesimi attuali quali elementi analitici*, Atti dell'Istituto Veneto, **7** (1893) pp. 1765–1815.

[Levi Civita 1898] T. Levi Civita: *Sui numeri transfiniti*, Atti della Reale Accademia dei Lincei, Classe di scienze Fisiche matematiche e naturali, Rendiconti, Roma, Serie V, **7** (1898) pp. 91–96.

[Magnus, Moufang 1954] W. Magnus – R. Moufang: *Max Dehn zum Gedächtnis*, Math. Ann., **127** (1954) pp. 215–227.

[Magnus 1978-1979] W. Magnus – M. Dehn: *Math. Intelligencer*, **1** (1978/79) pp. 132–143.

[Peano 1892] G. Peano: *Recenzione al volume di G. Veronese*, Fondamenti di Geometria a più dimensioni e a più specie di unità rettilinee, ecc., Rivista di Matematica, **2** (1892) pp. 143–144.

[Moufang 1931] R. Moufang: *Zur Struktur der projectiven Geometrie der Ebene*, Math. Ann., **105** (1931) pp. 536–601.

[Moufang 1931a] R. Moufang: *Die Einführung der idealen Elemente in die ebene Geometrie mit Hilfe des Satzes von vollständigen Viersiet*, Math. Ann., **105** (1931) pp. 759–778.

[Moufang 1932] R. Moufang: *Die Schnittpunktsätze des projektiven speziellen Fünfecknetzes in ihrer Abhängigkei voneinander*, Math. Ann., **106** (1932) pp. 755–795.

[Moufang 1932a] R. Moufang: *Ein Satz über die Schnittpunktsätze des allgeimeinen Fünfecknetzes*, Math. Ann., **107** (1932) pp. 124–139.

[Moufang 1933] R. Moufang: *Die Desarguesschen Sätze von Rang* 10, Math. Ann., **108** (1933) pp. 296–310.

[Moufang 1933a] R. Moufang: *Alternative Körper und der Satz von Vollstadingen Vierseit (D_9)*, Abh. Math. Sem. Hamburg, **9** (1933) pp. 207–222.

[Moufang 1934] R. Moufang: *Zur Strucktur von Alternativkörpern*, Math. Ann., **110** (1934) pp. 416–430.

[Moufang 1937] R. Moufang: *Einige Untersuchungen über geordenete Schiefkörper*, J. Reine Angew. Math., **76** (1937) pp. 203–223.

[Moufang 1941-1942] R. Moufang: *Das plastische Verhalten von Rohren unter statischem Innendruck bei Verformungen*, Ingen. Arch., **12** (1941) pp. 265–283, Zentralblatt, **26** (1942) p.279.

[Moufang 1946-1947] R. Moufang: *Volumentreue Verzerrungen bei endlichen Formänderungen*, Ber. Math. Tagung Tubingen, 1946, pp. 109–110; Zentralblatt, **28** (1947) p. 82.

[Moufang 1948] R. Moufang: *Strenge Berechnung der Eigenspannungen, die in plastisch aufgeweiteten Hohlzylindern nach der Entlastung zurückbleiben*, Z. Angew. Math. Mech., **28** (1948) pp. 33–42; Zentralblatt, **29** (1948) p. 329.

[Peano 1892a] G. Peano: *Dimostrazione dell'impossibilità di segmenti infinitesimi costanti*, Rivista di Matematica, **2** (1892) pp. 58–62.

[Saccheri 1733] G. Saccheri: *Euclides ab omni naevo vindicatus sive conatus geometricus quo stabiliuntur prima ipsa universale geometriae principia*, Milano, Paolo Antonio Montano, 1773.

[Schönflies 1897] A. M. Schönflies: *Transfinite Zahlen, das Axiom des Ar-*

chimedes un die projective Geometrie, Jahresbericht der Deutschen Mathematiker Vereinigung, **5** (1897) pp. 75–81.

[Schönflies 1897a] A. M. Schönflies: *Sur les nombres transfinis de Mr. Veronese*, Rendiconti dell'Accademia Nazionale dei Lincei,**6**, 5 (1897) pp. 362–368.

[Siegel 1965] C. L.Siegel: *Zur Geschichte des Frankfurter mathematischen Seminars*, Victorio Klostermann, 1965.

[Skornjakov 1950] L. A. Skornjakov: *Alternativekörper*, Ukrainian Math. J., **2**, 1 (1950) pp. 70–85.

[Stewart 2008] I. Stewart: *L'eleganza della verità. Storia della Simmetria*, Einaudi, 2008.

[Stolz 1883] O. Stolz: *Zur Geometrie der Alten, insbesondere über ein Axiom des Archimedes*, Math. Ann., **22** (1883) pp. 504–519.

[Stolz 1891] O. Stolz: *Ueber das Axiom des Archimedes*, Math. Ann., **39** (1891) pp. 107–112.

[Veronese 1891] G. Veronese: *Fondamenti di geometria a più dimensioni e a più specie di unità rettilinee esposti in forma elementare*, Lezioni per la Scuola di magistero in Matematica, Tipografia del Seminario, 1891.

[Veronese 1892] G. Veronese: *Osservazioni sopra una dimostrazione contro il segmento infinitesimo attuale*, Rendiconti del Circolo Matematico di Palermo, **6** (1892) pp. 73–76.

[Veronese 1896] G. Veronese: *Intorno ad alcune osservazioni sui segmenti infiniti o infinitesimi attuali*, Math. Ann., **47** (1896) pp. 423–432.

[Veronese 1897] G. Veronese: *Sul postulato della continuità*, Rendiconti della Reale Accademia dei Lincei, **5** (1897) pp. 161–167.

[Veronese 1898] G. Veronese: *Segmenti e numeri transfiniti*, Rendiconti della Reale Accademia dei Lincei **5** (1898) pp. 79–87.

[Vivanti 1891] G. Vivanti: *Sull'infinitesimo attuale*, Rivista di matematica, **1** (1891) pp. 135–153.

[Vivanti 1891a] G. Vivanti: *Ancora sull'infinitesimo attuale*, Rivista di matematica, **1** (1891) pp. 248–255

[Zorn 1930] M. Zorn: *Theorie der alternativen Ringe*, Abh. Math. Sem. Univ. Hamburg, **8** (1930) pp. 123–147.

Lavoro pervenuto alla redazione il 10 marzo 2010
ed accettato per la pubblicazione il 15 marzo 2010.
Bozze licenziate il 20 aprile 2010

Indirizzo dell'Autore:

Cinzia Cerroni– Dip. di Mat. ed Appl. – Università di Palermo – via Archirafi 34 – I-90123 Palermo – Italy
E-mail: cerroni@math.unipa.it

Rendiconti di Matematica, Serie VII
Volume 30, Roma (2010), 67-76

Some recent results in finite geometry and coding theory arising from the Gale transform

ANTONIO COSSIDENTE – ANGELO SONNINO

Dedicated to Professor Marialuisa de Resmini

Abstract: *The Gale transform is an involution on sets of points in a projective space. It plays a crucial role in several different subjects, such as algebraic geometry, optimization, coding theory, and so on. We give a brief survey—from a finite geometry point of view—on the algebraic and geometrical implications of the Gale transform with emphasis on its applications to coding theory, and describe some recent results.*

1 – Introduction

The Gale transform of a set $\mathcal{T}$ consisting of γ labelled points of a projective space $\mathrm{PG}(r,q)$ is an involution which maps $\mathcal{T}$ into a set $\mathcal{T}'$ consisting of γ labelled points of $\mathrm{PG}(s,q)$, defined up to automprphisms of $\mathrm{PG}(s,q)$, with $\gamma = r+s+2$.

The simplest way to define the Gale transform of a set of points is in terms of projective coordinates. Choose homogeneous coordinates in such a way that the coordinates of the points of $\mathcal{T}$ are the rows of the matrix

$$\begin{pmatrix} I_{r+1} \\ A \end{pmatrix},$$

where I_n denotes the $n \times n$ identity matrix and A is an $(s+1) \times (r+1)$ matrix. Then, the Gale transform of $\mathcal{T}$ is the set $\mathcal{T}'$ consisting of the points of $\mathrm{PG}(s,q)$

Key Words and Phrases: *Gale transform – Linear code – Mathieu group – Cap*
A.M.S. Classification: 51E20, 94B27.

whose homogeneous coordinates are the rows of the matrix

$$\begin{pmatrix} {}^{\tau}A \\ I_{s+1} \end{pmatrix},$$

where ${}^{\tau}A$ is the transpose matrix of A.

Although from the definition itself one may doubt whether the Gale transform has any geometry at all in the classical projective sense, the research work carried out over more than two centuries by some of the most important mathematicians is there to show that it is not true.

The first historical occurrency of a result related to the Gale transform is the following theorem which appeared in Pascal's "Essay Pour Les Coniques", see [24].

THEOREM 1.1. (*Pascal,* 1640) *The vertices of two triangles which are circumscribed around the same conic lie on another conic.*

Basically, the six points involved in Theorem 1.1 consitute a set of points which is the Gale transform of itself. At an early stage, finding sets of points which are the Gale transform of themselves represented the main goal of mathematicians dealing with the Gale transform. After Pascal, sets that are the Gale transform of themselves appeared in the work of Hesse [17, 18], von Staudt [26], Weddle [27], Zeuthen [29], Dobriner [11], Sturm [25], Rosanes [22, 23], Castelnuovo (who called two sets of points that are the Gale transform of one another "gruppi associati di punti") [3], and many others.

However, it was Coble—whose work had remarkable applications to theta functions and Jacobians of curves, see [4, 5, 6, 7]—the first who studied the Gale transform in a more general setting, starting off with the following alternative definition formulated in terms of matrices over a field.

Let $\mathbb{K}$ be a field and r, s two integers not less than 1. *Set $\gamma = r + s + 2$. Consider a subset Γ of a projective spaces of dimension r and a subset Γ' of a projective space of dimension s. Further, let Γ and Γ' be represented by a $\gamma \times (r+1)$ matrix G and a $\gamma \times (s+1)$ matrix G' respectively. Then Γ' is said to be the Gale transform of Γ if there is a nonsingular diagonal $\gamma \times \gamma$ matrix D such that ${}^{T}GDG = 0$.*

Whitney [28] and Gale [14] developed similar ideas in the affine case. Later on, Goppa—see [15] and [16] for instance—studied the Gale transform from a coding theory point of view. It is well known that in coding theory the Gale transform is the passage from a code to its dual; Goppa proved that a code defined by the set of $\mathrm{GF}(q)$-rational points on a certain algebraic curve is dual to another code of similar nature.

What we have seen so far is just a quick outline of the rich history of the Gale transform, which has implications in many other branches of modern

mathematics such as optimization, group theory, linear spaces, scheme theory, and so on. A full historical treatise on the development of the Gale transform over more than 150 years is well beyond the scope of these notes. For a more detailed historical account on the Gale transform the interested reader is referred to [12] and the references therein.

2 – Preliminary results

The first crucial result concerning the Gale transform of sets of points in finite projective spaces is stated in the following theorem.

THEOREM 2.1. *The Gale transform of the projective line* $\mathrm{PG}(1,q)$*, with* $q \geq 4$*, is a normal rational curve of* $\mathrm{PG}(q-2,q)$*.*

The result of Theorem 2.1 was already known to Goppa, as it is related with the so-called Goppa duality among the error correcting codes bearing his name [15, 16]. In [8] there is an alternative proof of this result which is based only on the properties of finite fields.

A natural generalisation of Theorem 2.1 in the finite case, if q is large enough, is the following result.

COROLLARY 2.2. *If* ℓ *is a line in some projective space* $\mathrm{PG}(r,q)$ *and* $\mathcal{T} \subseteq \ell$*, with* $|\mathcal{T}| = r+s+2$*, then the Gale transform* $\mathcal{T}'$ *of* $\mathcal{T}$ *is contained in the unique normal rational curve of* $\mathrm{PG}(s,q)$ *containing the fundamental frame.*

The proof of Corollary 2.2 is based on the fact that the Gale transform of any subset of points on a line in a projective space $\mathrm{PG}(r,q)$ of higher dimension is independent of the embedding of the line in the space. This can be clarified by means of a simple example obtained with the aid of MAGMA [2].

In the projective plane $\mathrm{PG}(2,4)$, where (X_1,X_2,X_3) are projective homogeneous coordinates, consider without loss of generality the line $\ell : X_3 = 0$ whose point set is $\{(1,0,0),(0,1,0),(1,\omega,0),(1,\omega^2,0),(1,1,0)\}$, with ω a primitive element of $\mathrm{GF}(4)$. With respect to the Gale transform, the essential part of ℓ is the subset $\{1,\omega,0),(1,\omega^2,0),(1,1,0)\}$ which—after truncation at the second coordinate—gives rise to the points $(1,1,1)$ and $(1,\omega,\omega^2)$. By adding the fundamental points of $\mathrm{PG}(2,4)$ we get a conic of $\mathrm{PG}(2,4)$.

Similarly, for $q=5$ it can be observed that a line of $\mathrm{PG}(2,5)$ is mapped by the Gale transform onto a twisted cubic of $\mathrm{PG}(3,5)$.

The following result is an important consequence of [19, Theorem 27.5.4].

PROPOSITION 2.3. *The Gale transform of a* k*-cap in a projective space* $\mathrm{PG}(r,q)$*,* $k \geq r+4$*, is a* k*-cap in* $\mathrm{PG}(k-r-2,q)$*.*

What we have seen so far can be summarized in the following fundamental result, see [8].

THEOREM 2.4. *Let $\mathcal{T}$ be any set consisting of k of points in* $\mathrm{PG}(r,q)$, $r \geq 2$ *and $k \geq r+4$. Then the Gale transform $\mathcal{T}'$ of $\mathcal{T}$ is a k-cap in* $\mathrm{PG}(k-r-2,q)$.

Sometimes it is convenient to have some control over the automorphism groups associated to the geometrical objects obtained in some peculiar way. With this respect, the Gale transform has an interesting behaviour, as it is shown by the following result [8].

PROPOSITION 2.5. *Let $\mathcal{K}$ be a k-cap in* $\mathrm{PG}(r,q)$ *and $\mathcal{K}'$ its Gale transform. Then $\mathcal{K}$ and $\mathcal{K}'$ have isomorphic collineation groups.*

3 – Self-associated sets

A set of points which is the Gale transform of itself is called a self-associated set. Actually, at an early stage the study of the Gale transform was mainly devoted to finding self-associated sets of points with some prescribed properties, see [12] for details and historical information. Some more recent results concerning self-associated sets from an algebraic geometry point of view can be found in [13].

Unlike the classical case, in finite geometry self-associated sets are somehow rare, due to the great number of constrains that the condition of being self-associate imposes over sets of points in a finite projective space. What follows provides a typical example of such results.

- A conic $\mathcal{C}$ in $\mathrm{PG}(2,q)$ is self-associated if and only if $q=5$. In fact, $\gamma = |\mathcal{C}| = q+1$ and from $\gamma = r+s+2$, $r=s=2$ it follows $q=5$.
- In $\mathrm{PG}(r,q)$ no self-associated set is the complement of a hyperplane if q is odd. Indeed, if π is a hyperplane of $\mathrm{PG}(r,q)$, then $\gamma = q^r = 2(r+1)$, and this equality cannot hold unless q is even.
- The complement of a plane in $\mathrm{PG}(3,q)$ is self-associated if and only if $q=2$. Indeed, if π is a plane in $\mathrm{PG}(3,q)$, then $\gamma = |\mathrm{PG}(3,q)\backslash\pi| = q^3$ implies $q^3 = 8$, and hence $q=2$.
- The complement of a hyperplane in $\mathrm{PG}(r,2)$ is a self-associated set if and only if $r=3$. Indeed, let π be a hyperplane of $\mathrm{PG}(r,2)$. Then, $\gamma = |\mathrm{PG}(r,2) \setminus \pi| = 2^r$. If $r=s$ then $2^{r-1} = r+1$, which implies $r=3$.

What we have just seen can be summarised as follows, see [8].

LEMMA 3.1. *The only finite projective space containing a self-associated set which is the complement of a hyperplane is* $\mathrm{PG}(3,2)$.

4 – The Gale transform of an elliptic quadric in PG(3, 3) and the Mathieu groups

In this section we show an interesting connection among the group of an elliptic quadric of PG(3, 3) and the Mathieu groups M_{11}, M_{12} obtained by means of the Gale transform.

Let $\mathcal{E}$ be the elliptic quadric of PG(3, 3) whose points are

$$\begin{aligned} P_1 &= (1,0,0,0), & P_2 &= (0,1,0,0), & P_3 &= (0,0,1,0), \\ P_4 &= (0,0,0,1), & P_5 &= (1,1,1,0), & P_6 &= (1,0,2,1), \\ P_7 &= (1,2,1,2), & P_8 &= (1,1,2,2), & P_9 &= (1,2,0,1), \\ P_{10} &= (0,1,1,1). \end{aligned}$$

Their coordinate vectors are the rows of the matrix

$$\begin{pmatrix} I_4 \\ A \end{pmatrix}.$$

The matrix associated to the Gale transform $\mathcal{E}'$ of $\mathcal{E}$ is

$$\begin{pmatrix} {}^{\tau}A \\ I_6 \end{pmatrix},$$

where

$${}^{\tau}A = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 2 & 1 & 2 & 1 \\ 1 & 2 & 1 & 2 & 0 & 1 \\ 0 & 1 & 2 & 2 & 1 & 1 \end{pmatrix}.$$

The rows of ${}^{\tau}A$ generate a vector space $V_1 = V(4, 3)$.

Let $V = V(10, 3)$ be a 10-dimensional vector space over $\mathbb{F}_3$ equipped with the standard scalar product. Then, the orthogonal complement of V_1 in V is $V_1^{\perp} = V(6, 3) = V_2$.

The 10-caps in PG(5, 3) whose points can be arranged to produce the rows of a 10×6 matrix whose columns span a vector space like the above V_2 are called dual 10-caps of $\mathcal{E}$.

Consider the (unique up to isomorphisms) Steiner System $\mathcal{S} = S(3, 4, 10)$

whose points are the points of $\mathcal{E}'$ and blocks are as follows:

$$\begin{array}{lll}
\{P_4,P_5,P_7,P_9\}, & \{P_1,P_2,P_3,P_9\}, & \{P_6,P_8,P_9,P_{10}\},\\
\{P_3,P_6,P_7,P_9\}, & \{P_3,P_5,P_9,P_{10}\}, & \{P_2,P_5,P_6,P_7\},\\
\{P_2,P_7,P_9,P_{10}\}, & \{P_4,P_5,P_6,P_{10}\}, & \{P_2,P_4,P_6,P_9\},\\
\{P_1,P_2,P_4,P_7\}, & \{P_1,P_2,P_5,P_{10}\}, & \{P_3,P_4,P_8,P_9\},\\
\{P_2,P_3,P_6,P_{10}\}, & \{P_1,P_5,P_6,P_9\}, & \{P_3,P_5,P_6,P_8\},\\
\{P_4,P_6,P_7,P_8\}, & \{P_5,P_7,P_8,P_{10}\}, & \{P_1,P_6,P_7,P_{10}\},\\
\{P_3,P_4,P_7,P_{10}\}, & \{P_1,P_4,P_5,P_8\}, & \{P_2,P_4,P_8,P_{10}\},\\
\{P_1,P_2,P_6,P_8\}, & \{P_1,P_4,P_9,P_{10}\}, & \{P_1,P_7,P_8,P_9\},\\
\{P_2,P_3,P_7,P_8\}, & \{P_2,P_5,P_8,P_9\}, & \{P_1,P_3,P_8,P_{10}\},\\
\{P_2,P_3,P_4,P_5\}, & \{P_1,P_3,P_5,P_7\}, & \{P_1,P_3,P_4,P_6\}.
\end{array}$$

- $\mathcal{E}'$ and $\mathcal{E}$ admit the same automorphism group $G = \mathrm{PGO}^-(4,q)$ which acts transitively on the plane sections of $\mathcal{E}$.
- $\mathcal{S}$ is the so-called Witt design W_{10};
- The isomorphism group of $\mathcal{S}$ is denoted by M_{10} and is isomorphic to a proper subgroup of $\mathrm{PGL}(2,9)$ containing $\mathrm{PSL}(2,9)$.
- G in its 6-dimensional representation is reducible; it fixes a line ℓ which is splitted into two orbits:

$$\ell_1 = \{(1,1,0,2,2,2),(1,2,2,0,1,2)\};$$
$$\ell_2 = \{(1,0,1,1,0,2),(0,1,2,1,2,0)\}.$$

  Fix the orbit ℓ_1 and let $\mathcal{E}_1 = \mathcal{E}' \cup \{(1,1,0,2,2,2)\}$. Then, $\mathcal{E}_1$ turns out to be the set of points of the unique Steiner system $S(4,5,11)$ admitting M_{11} as its automorphism group. The cap code associated to $\mathcal{E}_1$ is the well known ternary Golay code, which is a perfect $[11,6,5]_3$ code, see [8, 20 ,21].

Further, let $\mathcal{E}_2 = \mathcal{E}_1 \cup \{(1,2,2,0,1,2)\}$. Then, $\mathcal{E}_2$ turns out to be the set of points of the unique Steiner system $S(5,6,12)$ admitting M_{12} as its automorphism group, see [8, 21]. We obtained the following result.

LEMMA 4.1. *The Gale transform of an elliptic quadric of* $\mathrm{PG}(3,3)$ *can be extended in* $\mathrm{PG}(5,3)$ *to obtain the extended ternary Golay code.*

Note that the above procedure can also be applied starting off with the points of the affine plane $\mathrm{AG}(2,3)$ obtained by removing from $\mathrm{PG}(2,3)$ the line of equation $X_1 + X_2 + X_3 = 0$—in place of the points of $\mathcal{E}$—to obtain a cap admitting M_{12} as its automorphism group.

REMARK 4.2. *A similar construction can be performed starting off with an hyperbolic quadric in* $\mathrm{PG}(3,3)$ *instead. In this case we end up with a* 16*-cap in* $\mathrm{PG}(11,3)$ *which is the join of four normal rational curves. Furthermore, this* 16*-cap admits an automorphism group which is isomorphic to the group* $\mathrm{PGL}(2,3) \times \mathrm{PGL}(2,3)$ *of the initial hyperbolic quadric.*

5 – Extending scalars

In connection with what we have seen in the previous section, it is also interesting to note the following constructions based on the action of the groups M_{11} and M_{12}.

5.1 – A $[110,5,90]_9$-linear code [9]

Start off with a Singer cyclic subgroup $\mathcal{S}$ of $\mathrm{PSL}(5,3)$. The group S admits a subgroup of order 11 partitioning $\mathrm{PG}(4,3)$ into 11-caps. Let $\mathcal{K}$ be one of these caps. Then, $\mathcal{K}$ is the smallest complete cap in $\mathrm{PG}(4,3)$, and it is preserved setwise by the Mathieu group M_{11}, see [20]. As we mentioned before, the cap code associated to $\mathcal{K}$ is the well known ternary Golay code.

Embed $\Sigma = \mathrm{PG}(4,3)$ in $\mathrm{PG}(4,9)$ as a canonical Baer subgeometry, and look at the orbits of M_{11} on $\mathrm{PG}(4,9) \setminus \Sigma$; it turns out that M_{11} has five orbits in $\mathrm{PG}(4,9)$ of lengths 110, 220, 990, 1980 and 3960.

Recall that $\mathcal{K}$ has 55 secants; let r be an arbitrary GF(9)-extended secant to $\mathcal{K}$. The stabilizer H of r in M_{11} is the group

$$M_9 \rtimes C_2 \simeq (E_9 \times Q_8) \rtimes C_2$$

of order 144.

Now let $\mathcal{O}$ be the orbit of size 110 in $\mathrm{PG}(4,9) \setminus \Sigma$. The group H has four orbits on r: three of them have length 2, while the fourth one has length 4. Two of the orbits of length 2 yield the line $r \cap \Sigma$. Varying r among the secants to $\mathcal{K}$, the other orbit of length 2 gives rise to the orbit $\mathcal{O}$ we mentioned before. Actually, $\mathcal{O}$ is a complete 110-cap of $\mathrm{PG}(4,9)$.

The 110-cap $\mathcal{O}$ yields a $[110,5,90]_9$-linear code C with weight distribution

$$2^{55},\ 8^{1980},\ 11^{1320},\ 14^{2970},\ 17^{990},\ 20^{66}.$$

A code with the same parameters can be found in [1]. However, in the cited paper the authors do not mention its automorphism group. The main advantage of our approach relies on the fact that it is possible to keep track of the automorphism group throughout the construction procedure, and codes with large automorphism groups are of some interest in their own right.

5.2 – A $[132, 6, 96]_9$-linear code

The extended ternary Golay code is a $[12, 6, 6]_3$ linear code obtained by adding a zero-sum check digit to the $[11, 6, 5]_3$ code. The automorphism group of the extended ternary Golay code is $C_2 \times M_{12}$. Such a code can be realized geometrically in terms of a 12-cap $\mathcal{C}$ in PG$(5, 3)$, see [10].

Embed $\Pi = \mathrm{PG}(5, 3)$ in PG$(5, 9)$ as a canonical Baer subgeometry and look at the orbits of $G = M_{12}$ on $\mathrm{PG}(5, 9) \setminus \Pi$. With the aid of MAGMA [2] we checked that G has one orbit $\mathcal{O}$ of size 132 which is a cap.

The number of secants to $\mathcal{C}$ is 66. Let r be an arbitrary $\mathbb{F}_9$-extended secant to $\mathcal{C}$. The stabiliser H of r in G is the group

$$M_{10} \rtimes C_2 \simeq A_6 \times E_4$$

of order 1440. The group H has 4 orbits on r of lenghts 2, 2, 2 and 4.

Two orbits of length 2 form the the line $r \cap \Pi$. Varying r among the secants to $\mathcal{C}$, the remaining orbit of size 2 gives rise to the cap $\mathcal{O}$. Therefore, Coxeter's 12-cap gives rise to our cap $\mathcal{O}$. We checked with MAGMA [2] that the cap-code arising from $\mathcal{O}$ is a $[132, 6, 96]_9$ linear code.

REFERENCES

[1] J. Bierbrauer – T. A. Gulliver: *New linear codes over* $\mathbf{F}_9$, Australas. J. Combin. **21** (2000) pp. 131–140.

[2] W. Bosma – J. J. Cannon – C. Playoust: *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24**,3-4 (1997) pp. 235–265.

[3] G. Castelnuovo: *Su certi gruppi associati di punti*, Rend. Circ. Mat. Palermo **3** (1889) pp. 179–192.

[4] A. B. Coble: *Point sets and allied Cremona groups. I*, Trans. Amer. Math. Soc. **16**, 2 (1915) pp. 155–198.

[5] A. B. Coble: *Point sets and allied Cremona groups. II*, Trans. Amer. Math. Soc. **17**, 3 (1916) pp. 345–385.

[6] A. B. Coble: *Point sets and allied Cremona groups. III*, Trans. Amer. Math. Soc. **18**, 3 (1917) pp. 331–372.

[7] A. B. Coble: *Associated sets of points*, Trans. Amer. Math. Soc. **24**, 1 (1922) pp. 1–20.

[8] A. Cossidente – A. Sonnino: *Finite geometry and the Gale transform*, To appear on Discrete Math., doi:10.1016/j.disc.2009.08.019.

[9] A. Cossidente – A. Sonnino: *A geometric construction of a* $[110, 5, 90]_9$*-linear code admitting the Mathieu group* M_{11}, IEEE Trans. Inform. Theory **54**, 11 (2008) pp. 5251–5252.

[10] H. S. M. Coxeter: *Twelve points in* PG(5, 3) *with* 95040 *self-transformations*, Proc. Roy. Soc. London. Ser. A **247** (1958) pp. 279–293.

[11] H. Dobriner: *Über das Räumliche Achteck welches die Schnittpunkte dreier Oberflächen zweiter Ordnung bilden*, Acta Math. **12** (1889) pp. 339–361.

[12] D. Eisenbud – S. Popescu: *The projective geometry of the Gale transform*, J. Algebra **230**, 1 (2000), pp. 127–173.

[13] F. Flamini: *Towards an inductive construction of self-associated sets of points*, Matematiche (Catania) **53** (1998), no. suppl., pp. 33–41 (1999), Pragmatic 1997 (Catania).

[14] D. Gale: *Neighboring vertices on a convex polyhedron*, Linear inequalities and related system, Annals of Mathematics Studies, Princeton University Press, Princeton, N.J., **38** (1956) pp. 255–263.

[15] V. D. Goppa: *A new class of linear correcting codes*, Problemy Peredači Informacii **6**, 3 (1970) pp. 24–30.

[16] V. D. Goppa: *Codes and information*, Uspekhi Mat. Nauk **39**, 1(235) (1984) pp. 77–120.

[17] L. O. Hesse: *De curvis et superficiebus secundi ordinis*, J. Reine Angew. Math. **20** (1840) pp. 285–308.

[18] L. O. Hesse: *Über die lineare Cconstruction des achten Schnittpunktes dreier Oberflächen zewiter Ordnung, wenn sieben Schnittpunkte derselben gegeben sind*, J. Reine Angew. Math. **26** (1840) pp. 147–154.

[19] J. W. P. Hirschfeld – J. A. Thas: *General Galois geometries*, Oxford Mathematical Monographs, The Clarendon Press Oxford University Press, New York, 1991.

[20] G. Pellegrino: *Sulle proprietà della* 11*-calotta completa di* $S_{4,3}$ *e su un B.I.B.-disegno ad essa collegato*, Boll. Un. Mat. Ital. **7**, 4 (1973) pp. 463–470.

[21] G. Pellegrino: *Su una interpretazione geometrica dei gruppi* M_{11} *ed* M_{12} *di Mathieu e su alcuni* $t-(v, k, \lambda)$*-disegni-deducibili da una* $(12)^4_{5,3}$ *calotta completa*, Atti Sem. Mat. Fis. Univ. Modena **23**, 1 (1974) pp. 103–117 (1975).

[22] J. Rosanes: *Über linear abhängige Punktsysteme*, J. Reine Angew. Math. **88** (1880) pp. 241–272.

[23] J. Rosanes: *Zur Theorie der reciproken Verwandshaften*, J. Reine Angew. Math. **90** (1881) pp. 303–321.

[24] D. J. Struik (ed.): *A source book in mathematics, 1200–1800*, Princeton Paperbacks, Princeton University Press, Princeton, NJ, 1986, Reprint of the 1969 edition.

[25] R. Sturm: *Über Collineation und Correlation*, Math. Ann. **12** (1877) pp. 254–368.

[26] G. K. C. von Staudt: *Beiträge zur Geometrie der Lage*, vol. 3, Verlag von Bauer und Raspe (Julius Merz), Nürnberg, 1860.

[27] T. Weddle: *On the theorems in space analogous to those of Pascal and Brianchon in a plane*, Cambridge and Dublin Math. J. **5** (1852) pp. 58–69.

[28] H. Whitney: *Some combinatorial properties of complexes*, Proc. Nat. Acad. Sci. U. S. A. **26** (1940) pp. 143–148.

[29] H. G. Zeuthen: *Note sur les huit points d'intersection de trois surfaces du second ordre*, Acta Math. **12** (1889) pp. 362–366.

Lavoro pervenuto alla redazione il 10 marzo 2010
ed accettato per la pubblicazione il 15 marzo 2010.
Bozze licenziate il 20 aprile 2010

Indirizzo degli Autori:

Antonio Cossidente – Dipartimento di Matematica e Informatica – Università della Basilicata – Campus Macchia Romana – Viale dell'Ateneo Lucano, 10 – 85100 Potenza, Italy
E-mail: antonio.cossidente@unibas.it

Angelo Sonnino – Dipartimento di Matematica e Informatica – Università della Basilicata – Campus Macchia Romana – Viale dell'Ateneo Lucano, 10 – 85100 Potenza, Italy
E-mail: angelo.sonnino@unibas.it

Rendiconti di Matematica, Serie VII
Volume 30, Roma (2010), 77-88

Curves of genus 3

J.W.P. HIRSCHFELD

Dedicated to Marialuisa de Resmini on her retirement

Abstract: *Any curve of genus 3 can be represented as a plane quartic curve. The question of the maximum number of points on such a curve over a finite field is discussed.*

1 – Questions about curves

(i) What is meant by the 'number of points' on a curve?
(ii) What is the number of points on a curve that can occur, given some parameters such as
q, the size of the field,
g, the genus of the curve,
n, the degree of a plane curve?
(iii) What is the maximum number of points?
(iv) Find curves with certain parameters.
(v) Classify the curves with a set of these parameters.

One such problem is to find the number of rational points over $\mathbf{F}_q$ on a non-singular plane quartic curve, that is, a curve of genus 3.

This article surveys this problem and its background. For contrast, curves of genus 1 and 2 are also considered.

Key Words and Phrases: *Cubic surface – Quartic curve*
A.M.S. Classification: 11G25, 51E20.

2 – Cubic surfaces

Let $\mathcal{V} = \mathbf{v}(F_1, \ldots, F_r)$ be the variety given by the zeros of the homogeneous polynomials $F_1, \ldots, F_r$.

THEOREM 2.1. *A non-singular surface $\mathcal{F}^3$ of degree three over a field K has at most 27 lines and over the algebraic closure $\overline{K}$ exactly 27 lines.*

THEOREM 2.2. *Over $\mathbf{F}_q$, there exists an $\mathcal{F}^3$ with 27 lines if $q \neq 2, 3, 5$. Equivalently, in $\mathrm{PG}(2, \mathrm{q})$, there exists a 6-arc not on a conic if $q \neq 2, 3, 5$.*

THEOREM 2.3.
(i) *The group G_{27} of automorphisms of the 27 lines is isomorphic to*

$$\mathrm{P\Gamma U}(4,4) \cong \mathrm{PGO}_-(6,2) \cong \mathrm{PGSp}(4,3) \cong \mathrm{PGO}(5,3),$$

and has order $51,840 = 72 \times 6!$.
(ii) *The simple group G'_{27} of index two in G_{27} is isomorphic to $\mathrm{PGU}(4,4)$, and has order $25,920 = 36 \times 6!$.*

2.1 – From 27 to 28

THEOREM 2.4. *For a point P not on a line of $\mathcal{F}^3$, the intersection $\mathcal{C}^6$ of $\mathcal{F}^3$ and the polar quadric $\mathcal{Q}^2$ of $\mathcal{F}^3$ at P has a double point at P; it projects from P to a non-singular plane quartic when K has characteristic other than two.*

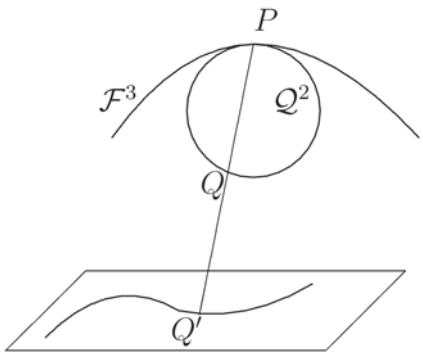


Figure 1
$\mathcal{F}^3 \cap \mathcal{Q}^2 = \mathcal{C}^6 \overset{P}{\to} \mathcal{C}^4$

PROOF. Let $P = (1, 0, 0, 0)$ and $\pi = \mathbf{v}(X_0)$. Then

$$\begin{aligned}
\mathcal{F}^3 &= \mathbf{v}(X_0^2 f_1(X_1, X_2, X_3) + X_0 f_2(X_1, X_2, X_3) + f_3(X_1, X_2, X_3)),\\
\mathcal{Q}^2 &= \mathbf{v}(2X_0 f_1(X_1, X_2, X_3) + f_1(X_1, X_2, X_3)),\\
\mathcal{C}^6 &= \mathbf{v}(X_0^2 f_1 + X_0 f_2 + f_3,\ 2X_0 f_1 + f_2)\\
\mathcal{C}^4 &= \mathbf{v}(f_2^2 - 4f_1 f_3, X_0)
\end{aligned}$$

For q even, $\mathcal{C}^4 = \mathcal{C}^2 \cup \mathcal{C}^2$, a repeated conic. For q odd, $\mathcal{F}^3$ is non-singular if and only if $\mathcal{C}^4$ is non-singular. □

THEOREM 2.5. *For q odd, $q \geq 9$, there exists a non-singular $\mathcal{C}^4$ with 28 bitangents if and only if there exists $\mathcal{F}^3$ with 27 lines and P not on the lines.*

EXAMPLE 2.6. For $q = 9$, let

$$\begin{aligned}
F &= X_0^4 + X_1^4 + X_2^4\\
&= X_0\bar{X}_0 + X_1\bar{X}_1 + X_2\bar{X}_2,
\end{aligned}$$

where $t \mapsto t^3 = \bar{t}$ is the involutory automorphism of $\mathbf{F_9}$. So $\mathcal{F} = \mathbf{v}(F)$ is a Hermitian curve with $q\sqrt{q}+1 = 28$ rational points, all of which are undulations; that is, the tangents have 4-point contact and so are bitangents.

2.2 – Number of points

THEOREM 2.7.

(i) *The number of rational points on a non-singular cubic surface $\mathcal{F}^3$ over $\mathbf{F}_q$ is $|\mathcal{F}^3(\mathbf{F}_q)| = q^2 + 7q + 1$.*

(ii)
   (a) *The 27 lines of $\mathcal{F}^3$ lie on 45 tritangent planes of which e meet $\mathcal{F}^3$ in three concurrent lines.*
   (b) *The number of rational points on the lines is $N_0 = 27(q-4) + e$.*

PROOF.

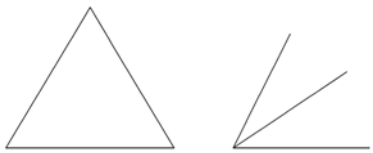
(i) In the correspondence between $\mathcal{F}^3$ and the plane, each line in one half of a double-six corresponds to a point.

(ii) (b) A triangle contains $3q$ points, whereas a triad of concurrent lines contains $3q+1$ points. As each line meets 10 others, a count of points on just one of the 27 lines plus those on more than one line gives the following:

$$N_0 = 27(q + 1 - 10) + 27 \times 10/2 + e.$$

□

$q^2 + q - 5 + 6(q+1)$



$45 - e$ $\qquad$ e

2.3 – Full $\mathcal{F}^3$

DEFINITION 2.8. A cubic surface defined over K is *full* if its lines contain all its rational points.

THEOREM 2.8.

(i) *There exists a full* $\mathcal{F}^3$ *for*

$$q = 4,\ 7,\ 8,\ 9,\ 11,\ 13,\ 16\,.$$

(ii) *Canonical forms for the full surfaces are as follows*:

$$\mathcal{E} = \mathbf{v}(X_0^3 + X_1^3 + X_2^3 + X_3^3), \quad q = 4, 7, 13, 16;$$
$$\mathcal{D} = \mathbf{v}\left(X_0^3 + X_1^3 + X_2^3 + X_3^3 + X_4^3, \sum X_i\right), \quad q = 4, 11, 16;$$
$$\mathcal{D} = \mathbf{v}\left(\sum X_i X_j X_k,\ \sum X_i\right), \quad q = 9;$$
$$\mathcal{C} = \mathbf{v}(X_0 X_1 (X_0 + X_1) + X_2 X_3 (X_0 + X_2 + X_3)), \quad q = 8.$$

(iii) *For* $q = 4, 7, 8$, *every* $\mathcal{F}^3$ *is full.*

(iv) *For* $q > 16$, *no* $\mathcal{F}^3$ *is full.*

2.4 – Number of lines and bitangents

THEOREM 2.10. *For a cubic surface* $\mathcal{F}_3$ *and the corresponding* $\mathcal{C}_4$ *over* $\mathbf{F}_q$, *let* n *be the number of possible lines on* $\mathcal{F}_3$ *and* b *the number of possible bitangents on* $\mathcal{C}_4$.

(i) *For* q *odd*,

$$n = 27,\ 15,\ 9,\ 7,\ 5,\ 3,\ 2,\ 1,\ 0;$$
$$b = 28,\ 16,\ 10,\ 8,\ 6,\ 4,\ 3,\ 2,\ 1,\ 0.$$

(ii) *For* $q = 2$,

$$n = 15,\ 9,\ 5,\ 3,\ 2,\ 1,\ 0.$$

QUESTION 2.11. What are the possible numbers of lines on a non-singular cubic over $\mathbf{F}_{2^h}$?

THEOREM 2.12. *For q even, the possible numbers of bitangents of a non-singular plane quartic are* 7, 3, 1, 0. *In the case of* 7 *bitangents they form a* $\mathrm{PG}(2,2)$.

EXAMPLE 2.13. (The Klein curve for $q = 8$)

$$\mathcal{F} = \mathbf{v}(X^3Y + Y^3Z + Z^3X).$$

The 24 rational points are all inflexions. There are 7 bitangents

$$\mathbf{v}(c^3X + cY + Z), \quad c \in \mathbf{F}_8 \backslash \{\mathbf{0}\},$$

forming a $\mathrm{PG}(2,2)$.

THEOREM 2.14. *For an algebraically closed field of characteristic two, the possible configurations of bitangents are the following* :

(1) 7 *lines forming a* $\mathrm{PG}(2,2)$;
(2) 4 *lines with* 3 *concurrent*;
(3) 1 *line*;
(4) *a pencil plus a line*;
(5) *a pencil with one special line.*

3 – The number of points on a non-singular curve

For a curve $\mathcal{F}$ defined over $\mathbf{F}_q$ with N_i the number of points of $\mathcal{F}$ rational over $\mathbf{F}_{q^i}$, the *zeta function* is

$$\zeta_q(T) = \exp(1 + N_1T + N_2T^2/2 + N_3T^3/3 + \cdots).$$

THEOREM 3.1. (*Hasse–Weil*)

$$\zeta_q(T) = \exp\left(\sum N_iT^i/i\right) = \frac{f(T)}{(1-T)(1-qT)},$$

with $f \in \mathbf{Z}[T]$, $\quad \deg f = 2g$.

COROLLARY 3.2.
(i) $N_1 \leq q + 1 + 2g\sqrt{q}$.
(ii) *When* $g = 1$,

$$\zeta_q(T) = \frac{1 + c_1 T + qT^2}{(1-T)(1-qT)}.$$

THEOREM 3.3. (*Serre*) $N_1 \leq q + 1 + g\lfloor 2\sqrt{q} \rfloor$.

NOTATION 3.4. $N_q(g) = \max N_1$, taken over all non-singular curves $\mathcal{C}$ of genus g over $\mathbf{F}_q$.

EXAMPLE 3.5. For the Klein curve with $q = 2$,

$$F = X^3Y + Y^3Z + Z^3X,$$
$$N_1 = 3, \quad N_2 - N_1 = 2, \quad N_3 - N_1 = 21,$$
$$f(T) = 1 + 5T^3 + 8T^6.$$

A special case of an important theorem gives other bounds.

THEOREM 3.6. (*Stöhr–Voloch*) *For a plane curve of degree* n *with not all points inflexions and* $p \neq 2$,

$$N_1 \leq \frac{1}{2} n(n + q - 1).$$

The case that $q = 7, n = 4, g = 3$ gives

$$N_7(3) \leq 20 < 23 = 7 + 1 + 3\lfloor 2 \times \sqrt{7} \rfloor$$

In fact, $N_7(3) = 20$.

4 – Curves of genus 1

A curve of genus 1, or elliptic curve, can be regarded as a plane non-singular cubic. Plane cubics may be classified up to isomorphism or projective equivalence.

THEOREM 4.1. *Up to isomorphism, a curve* $\mathcal{F} = \mathbf{v}(F)$ *of genus* 1 *over* $\mathbf{F}_q$, *with* $q = p^h$, *has at least one point of inflexion and the following canonical forms.*

(i) *When* $p \neq 2, 3$,

$$F = Y^2Z + X^3 + cXZ^2 + dZ^3,$$

where $4c^3 + 27d^2 \neq 0$.

(ii) *When* $p = 3$,

(a)

$$F = Y^2Z + X^3 + bX^2Z + dZ^3,$$

where $bd \neq 0$;

(b)

$$F' = Y^2Z + X^3 + cXZ^2 + dZ^3,$$

where $c \neq 0$.

(iii) *When* $p = 2$,

(a)

$$F = Y^2Z + XYZ + X^3 + bX^2Z + dZ^3,$$

where $b = 0$ *or a fixed element of trace* 1, *and* $c \neq 0$;

(b)

$$F' = Y^2Z + YZ^2 + eX^3 + cXZ^2 + dZ^3,$$

where $e = 1$ *when* $(q-1, 3) = 1$ *and* $e = 1, \alpha, \alpha^2$ *when* $(q-1, 3) = 1$, *with* α *a primitive element of* $\mathbf{F}_q$; *also,* $d = 0$ *or a particular element of trace* 1.

Canonical forms up to a projectivity exist for cubics with no inflexions; see [7, Chapter 11]. For example, over $\mathbf{F_7}$, let

$$F = X^3 + 2Y^3 + 3Z^3.$$

The corresponding curve $\mathcal{F}$ has no inflexion.

THEOREM 4.2. *Let* N_1 *be the number of rational points of an elliptic curve over* $\mathbf{F}_q$.

(i)

$$q + 1 - 2\sqrt{q} \leq N_1 \leq q + 1 + 2\sqrt{q}.$$

(ii) *The precise number* $N_1 = q + 1 - t$, *with* $|\, t \,| \leq 2\sqrt{q}$, *of points that can occur is given in Table 1.*

TABLE 1: VALUES OF t

	t	p	h
(1)	$t \not\equiv 0 \pmod{p}$		
(2)	$t = 0$		odd
(3)	$t = 0$	$p \not\equiv 1 \pmod 4$	even
(4)	$t = \pm\sqrt{q}$	$p \not\equiv 1 \pmod 3$	even
(5)	$t = \pm 2\sqrt{q}$		even
(6)	$t = \pm\sqrt{2q}$	$p = 2$	odd
(7)	$t = \pm\sqrt{3q}$	$p = 3$	odd

THEOREM 4.3. *If A_q and P_q are the numbers of distinct elliptic curves up to isomorphism and projective equivalence, then*

$$A_q = 2q + 3 + \left(\frac{-4}{q}\right) + 2\left(\frac{-3}{q}\right);$$
$$P_q = 3q + 2 + \left(\frac{-4}{q}\right) + \left(\frac{-3}{q}\right)^2 + 3\left(\frac{-3}{q}\right).$$

Here the bracketed numbers are Legendre and Legendre–Jacobi symbols taking the values $-1, 0, 1$.

The prime power $q = p^h$ is *exceptional* if h is odd, $h \geq 3$, and p divides $\lfloor 2\sqrt{q} \rfloor$.

THEOREM 4.4. *The actual upper bounds for elliptic curves over $\mathbf{F}_q$ are as follows:*

$$N_q(1) = \begin{cases} q + \lfloor 2\sqrt{q} \rfloor, & \text{if } q \text{ is exceptional} \\ q + 1 + \lfloor 2\sqrt{q} \rfloor, & \text{if } q \text{ is non-exceptional;} \end{cases}$$

COROLLARY 4.5. *The number N_1 takes every value between $q + 1 - \lfloor 2\sqrt{q} \rfloor$ and $q + 1 + \lfloor 2\sqrt{q} \rfloor$ if and only if*

(a) $q = p$;
(b) $q = p^2$ *with* $p = 2$ *or* $p = 3$ *or* $p \equiv 11 \pmod{12}$.

4.1 – Unsolved problem

Let $m_3(2,q)$ be the maximum size of a point set $\mathcal{K}$ in $\mathrm{PG}(2,q)$ such that at most three points of $\mathcal{K}$ lie on a line. Show that

$$m_3(2,q) > N_q(1) \quad \text{for } q \neq 4.$$

This is true for $q \leq 13$ as in Table 2.

TABLE 2: VALUES OF $m_3(2,q)$

q	2	3	4	5	7	8	9	11	13
$m_3(2,q)$	7	9	9	11	15	15	17	21	23
$N_q(1)$	5	7	9	10	13	14	16	18	21

5 – Curves of genus 2

THEOREM 5.1. *For a curve of genus* 2 *over* $\mathbf{F}_q$ *with* q *square,*

$$\begin{aligned} &N_q(2) = q + 1 + 4\sqrt{q}, \quad \text{if } q \neq 4, 9; \\ &N_4(2) = 10; \\ &N_9(2) = 20. \end{aligned}$$

The prime power $q = p^h$ is *special* if (a) or (b) holds:

(a) p divides $\lfloor 2\sqrt{q} \rfloor$;
(b) there exists m such that $q = m^2 + 1$ or $q = m^2 + m + 1$ or $q = m^2 + m + 2$.

THEOREM 5.2. *If* q *is a non-square, with* $\{2\sqrt{q}\} = 2\sqrt{q} - \lfloor 2\sqrt{q} \rfloor$,

$$\begin{aligned} &N_q(2) = q + 1 + 2\lfloor 2\sqrt{q} \rfloor, && \text{if } q \text{ is not special;} \\ &N_q(2) = q + 2\lfloor 2\sqrt{q} \rfloor, && \text{if } q \text{ is special and } \{2\sqrt{q}\} > \frac{1}{2}(\sqrt{5} - 1); \\ &N_q(2) = q - 1 + 2\lfloor 2\sqrt{q} \rfloor, && \text{if } q \text{ is special and } \{2\sqrt{q}\} < \frac{1}{2}(\sqrt{5} - 1). \end{aligned}$$

6 – Curves of genus 3

From Section 3, there is the following result.

THEOREM 6.1.

(i) $N_q(3) \le q + 1 + 3\lfloor 2\sqrt{q} \rfloor = S_3$.

(ii) $N_q(3) \le \begin{cases} 28, & q = 9 \\ 2(q+3), & q \text{ odd, } q \ne 9 \\ 2(q+4), & q \text{ even} \end{cases} = V_3$.

THEOREM 6.2. (*Lauter*) *For a curve of genus* 3,

$$\left.\begin{array}{ll} N_1 \le q - 1 + 3\lfloor 2\sqrt{q} \rfloor & \text{if } q = m^2 + 1; \\ N_1 \le q - 1 + 3\lfloor 2\sqrt{q} \rfloor & \text{if } q = m^2 + 2 \text{ with } m \ge 2; \\ N_1 \le q - 2 + 3\lfloor 2\sqrt{q} \rfloor & \text{if } q = m^2 + m + 1; \\ N_1 \le q - 2 + 3\lfloor 2\sqrt{q} \rfloor & \text{if } q = m^2 + m + 3 \text{ with } m \ge 3. \end{array}\right\} = L_3$$

THEOREM 6.3. *For a curve of genus* 3, *if* $N_1 > 2q + 6$ *then one of the following holds*:

(i) $N_1 = 28$, $q = 9$ *and* $\mathcal{C}$ *is the Hermitian curve*;
(ii) $N_1 = 24$, $q = 8$ *and* $\mathcal{C}$ *is the Klein curve.*

Table 3 summarises the results for small q.

TABLE 3: NUMBER OF POINTS ON CURVES OF GENUS 3

q	2	3	4	5	7	8	9	11	13	16	17	19	23	25	27
$N_q(3)$	7	10	14	16	20	24	28	28	32	38	40	44	48	56	56
S_3	9	13	17	18	23	24	28	30	35	41	42	44	51	56	58
V_3	10	12	16	16	20	24	28	28	32	40	40	44	52	56	60
L_3	7	10		16	20			28	32		40		48		56

THEOREM 6.4. (*Ibukiyama*) *For* $q = p^{4m+2}$,

$$N_q(3) = q + 1 + 6\sqrt{q}.$$

THEOREM 6.5.

(i) *When $q < 100$, there is equality $N_q(3) = S_3$ if and only if*

$$q \in \{8, 9, 19, 25, 29, 41, 47, 49, 53, 61, 64, 67, 71, 79, 81, 89, 97\}.$$

(ii) *When $q \leq 27$, there is equality $N_q(3) = V_3$ if and only if*

$$q \in \{5, 7, 11, 13, 17, 19, 25\}.$$

REFERENCES

[1] A. D. CAMPBELL: *Plane quartic curves in the Galois fields of order* 2^n, Tôhoku Math. J. **37** (1933) pp. 88–93.

[2] L. R. A. CASSE: *Concerning bitangents of irreducible plane quartic curves over* $GF(2^h)$, Teorie Combinatorie, vol. II, Accad. Naz. dei Lincei, Rome, 1976, (Rome, 1973), pp. 381–387.

[3] M. J. DE RESMINI: *Sulle quartiche piane sopra un campo di caratteristica due*, Ricerche Mat. **19** (1970) pp. 133–160.

[4] L. E. DICKSON: *Classification of quartic curves*, modulo 2, Messenger of Mathematics, **44** (1915), pp. 189–192.

[5] L. E. DICKSON: *Geometrical and invariantive theory of quartic curves*, modulo 2, Amer. J. Math., **37** (1915) pp. 337–354.

[6] L. E. DICKSON: *Quartic curves*, modulo 2, Trans. Amer. Math. Soc., **16** (1915) pp. 111–120.

[7] J. W. P. HIRSCHFELD: *Projective Geometries over Finite Fields*, second edition, Oxford University Press, Oxford, 1998, xiv p. 555.

[8] J. W. P. HIRSCHFELD: *Finite Projective Spaces of Three Dimensions*, Oxford University Press, Oxford, 1985, x p. 316.

[9] J. W. P. HIRSCHFELD – G. KORCHMÁROS – F. TORRES: *Algebraic Curves over a Finite Field*, Princeton University Press, Princeton, 2008, xxii p. 696.

[10] T. IBUKIYAMA: *On rational points of curves of genus 3 over finite fields*, Tohoku Math. J., **45** pp. 311–329.

[11] R. H. JEURISSEN – C. H. VAN OS – J. H. STEENBRINK: *The configuration of the bitangents of the Klein curve*, Discrete Math., **132** (1994) pp. 83–96.

[12] K. LAUTER: *The maximum or minimum number of rational points on genus three curves over finite fields*, Compositio Math., **134** (2002) pp. 87–111 (Appendix by J.-P. Serre).

[13] B. SEGRE: *Arithmetical Questions on Algebraic Varieties*, The Athlone Press, University of London, London, 1951, p. 55

[14] J. Top: *Curves of genus 3 over small finite fields*, Indag. Math., **14** pp. 275–283.

Lavoro pervenuto alla redazione il 10 marzo 2010
ed accettato per la pubblicazione il 15 marzo 2010.
Bozze licenziate il 20 aprile 2010

Indirizzo dell'Autore:

J. W. P. Hirschfeld – Department of Mathematics – University of Sussex – Brighton BN1 9RF United Kingdom
Email: jwph@sussex.ac.uk – http://www.maths.sussex.ac.uk/Staff/JWPH/

Rendiconti di Matematica, Serie VII
Volume 30, Roma (2010), 89-109

Deformations of algebraic subvarieties

DONATELLA IACONO

Dedicated to Professor Marialuisa de Resmini

ABSTRACT: *In this paper, we use (bi)semicosimplicial language to study the classical problem of infinitesimal deformations of a closed subscheme in a fixed smooth variety, defined over an algebraically closed field of characteristic 0. In particular, we give an explicit description of the differential graded Lie algebra controlling this problem.*

– Introduction

In the last fifty years, deformation theory has played an important role in algebraic and complex geometry. The main goal is the classification of families of geometric objects in such a way that the classifying space (the so called moduli space) is a reasonable geometric space. In particular, each point of our moduli space corresponds to one geometric object (class of isomorphism). The study of small deformations of the complex structures of complex manifolds started with the works of K. Kodaira and D.C. Spencer [KoSp58] and M. Kuranishi [Ku71]. Then, A. Grothendieck [Gr59], M. Schlessinger [Schl68] and M. Artin [Ar76] formalized this theory translating it into a functorial language. The idea is that, with a infinitesimal deformations of a geometric object, we can associate a deformation functor of Artin rings $F : \mathbf{Art} \to \mathbf{Set}$. For example, we can study the functor Def_X of infinitesimal deformations of a variety X or the functor Hilb^Z_X of infinitesimal deformations of a subvariety Z in a fixed variety X. The fundamental fact is that, using these functors, we are able to study the formal neighborhood of the points in the moduli space. In particular, we can

KEY WORDS AND PHRASES: *Differential graded Lie algebras – Functors of Artin rings*
A.M.S. CLASSIFICATION: 13D10, 14D15.

determine the tangent space or analyze the obstructions (smoothness) problem [Ma07, Ia07, IM09].

A modern approach to the study of deformation functors, associated with geometric objects, is via differential graded Lie algebras or, in general, via L_∞-algebras. At this stage, we can think about these structures as a generalization of differential graded vector spaces in which we also have a bracket, plus some compatibility conditions between the differential and the bracket. Once we have a differential graded Lie algebra L, we can define the associated deformation functor $\mathrm{Def}_L : \mathbf{Art} \to \mathbf{Set}$, using the solutions of the Maurer-Cartan equation up to gauge equivalence.

The guiding principle is the idea due, at least, to P. Deligne, V. Drinfeld, D. Quillen and M. Kontsevich [Kon03] that "in characteristic zero every deformation problem is controlled by a differential graded Lie algebra". In other words, if F is the deformation functor associated with a geometric problem, then there exists a differential graded Lie algebra L (up to quasi-isomorphism) such that $\mathrm{Def}_L \cong F$. We point out that it is easier to study a deformation functor associated with a differential graded Lie algebra but, in general, it is not an easy task to find the right differential graded Lie algebra (up to quasi-isomorphism) associated with the problem [Kon94]. A first example, in which the associated differential graded Lie algebra is well understood, is the case of deformations of complex manifolds. If X is a complex compact manifold, then the infinitesimal deformations of X are controlled by its Kodaira-Spencer algebra KS_X, see [GM90, Ma04b, Ma09] and [Ia06, Theorem II.7.3]. We recall that $KS_X = \oplus_i \Gamma(X, \mathcal{A}_X^{0,i}(\Theta_X))$, where $\mathcal{A}_X^{0,i}(\Theta_X)$ is the sheaf of the $(0,i)$-forms on X, with values in the holomorphic tangent bundle Θ_X.

In general, if we work over an algebraically closed field of characteristic zero, different from the complex numbers, then we can not use the Kodaira-Spencer algebra.

A strategy to solve this problem and "produce"differential graded Lie algebras, is via semicosimplicial objects [Hin97, Pr03, FMM08, FIM09]. Actually, the fundamental idea goes back to K. Kodaira and D.C. Spencer:"a deformation of X is regarded as the gluing of the same polydisks via different identifications"[Kod86, pag. 182]. In other words, a deformation of a geometric object consists in deforming the object locally and then glue back together these local deformations. Then, from the algebraic point of view, we have to find the algebraic objects that control locally the deformations and then glue them together. Thus, we can think at a semicosimplcial object as a sequence of objects, that controls locally the deformations, and a sequence of maps, that controls the gluing. For example, let X be a smooth projective variety, over an algebraically closed field $\mathbb{K}$ of characteristic 0, with tangent sheaf Θ_X. Given an affine open cover $\mathcal{U} = \{U_i\}$ of X, we can define the Čech semicosimplicial Lie algebra $\Theta_X(\mathcal{U})$, *i.e.*, we have a sequence of Lie algebras $\{\mathfrak{g}_k = \prod_{i_0<\cdots<i_k} \Theta_X(U_{i_0\cdots i_k})\}$ and a "lot"of maps among them, that are the

restrictions to open subsets. In particular, $\mathfrak{g}_0 = \prod_i \Theta_X(U_i)$ and each $\Theta_X(U_i)$ controls the infinitesimal deformations of U_i; moreover, the maps controls the gluing of deformations, see [FMM08] and [IM09, Section 5].

In general, we will have a semicosimplicial differential graded Lie algebra, $\mathfrak{g}^\Delta = \{\mathfrak{g}_k\}_k$, with $\mathfrak{g}_0$ that controls the deformations of each open of the cover, as in the case of deformations of varieties or of coherent sheaves [FIM09, FIM].

Next, once we have a semicosimplicial differential graded Lie algebra $\mathfrak{g}^\Delta$, we need to find out just one differential graded Lie algebra. Following [NaA87, FMM08], there is a canonical way to define a differential graded Lie algebra $\mathrm{Tot}_{TW}(\mathfrak{g}^\Delta)$, using the Thom-Whitney construction. In conclusion, given a geometric deformation problem, if we are able to associate with it a semicosimplicial differential graded Lie algebra, then we can find out just one differential graded Lie algebra controlling our problem.

Inspired by these ideas, in this paper we use semicosimplicial language to study infinitesimal deformations of closed subschemes. More precisely, let X be a smooth variety, defined over an algebraically closed field $\mathbb{K}$ of characteristic 0, and $Z \subset X$ a closed subscheme. Denote by Hilb_X^Z the functor of infinitesimal deformations of Z in X and by Hilb'^Z_X the subfunctor of locally trivial infinitesimal deformations. We recall that $\mathrm{Hilb}_X^Z = \mathrm{Hilb}'^Z_X$, whenever Z is smooth. For $\mathbb{K} = \mathbb{C}$ and Z smooth, the analysis of this problem via differential graded Lie algebra is due to M. Manetti [Ma07]. Here, we extend his work to all algebraically closed fields $\mathbb{K}$ of characteristic 0, using semicosimplicial language; more precisely, it is convenient to use bisemicosimplial Lie algebras. Indeed, let Θ_X be the tangent sheaf of X and $\Theta_X(-\log Z)$ the sheaf of tangent vectors to X which are tangent to Z. Denote by $\chi : \Theta_X(-\log Z) \hookrightarrow \Theta_X$ the inclusion of sheaves of Lie algebras. We can associate with $\Theta_X(-\log Z)$ and Θ_X the Čech semicosimplicial Lie algebra $\Theta_X(-\log Z)(\mathcal{U})$ and $\Theta_X(\mathcal{U})$, respectively; and so we can consider the bisemicosimplicial Lie algebra $\chi^\blacktriangle : \Theta_X(-\log Z)(\mathcal{U}) \to \Theta_X(\mathcal{U})$. Once again, using the Thom-Whitney construction, we can define a differential graded Lie algebra $\mathrm{Tot}^\blacktriangle_{TW}(\chi^\blacktriangle)$. This algebra controls the deformations of the closed subscheme Z; more precisely, we prove the following theorem.

Theorem (A). *Let X be a smooth variety, defined over an algebraically closed field $\mathbb{K}$ of characteristic 0, and $Z \subset X$ a closed subscheme. Then, there exists an isomorphism of functors $\mathrm{Def}_{\mathrm{Tot}^\blacktriangle_{TW}(\chi^\blacktriangle)} \cong \mathrm{Hilb}'^Z_X$. In particular, if $Z \subset X$ is smooth, then $\mathrm{Def}_{\mathrm{Tot}^\blacktriangle_{TW}(\chi^\blacktriangle)} \cong \mathrm{Hilb}_X^Z$.*

In a forthcoming paper, we will use this theorem to study the obstruction to deformations of Z in X, via the semiregularity map.

The paper goes as follows: the first section is intended for the nonexpert reader and is devoted to recall the basic notions of differential graded Lie algebras and their role in deformation theory.

In Section 2, we introduce semicosimplicial objects and total constructions. In particular, we review semicosimplicial differential graded Lie algebras, the corresponding Thom-Whitney DGLA and the associated deformation functors.
Sections 3 is devoted to bisemicosimplicial objects and, again, to the total constructions and the associated deformation functors. In particular, we describe the bisemicosimplicial Lie algebra $\chi^{\blacktriangle} : \Theta_X(-\log Z)(\mathcal{U}) \to \Theta_X(\mathcal{U})$, associated with the inclusion $\chi : \Theta_X(-\log Z) \hookrightarrow \Theta_X$.
In Section 4, we go back to geometric applications and we prove Theorem A.

NOTATION. Throughout the paper, we work over an algebraically closed field $\mathbb{K}$ of characteristic zero. All vector spaces, linear maps, tensor products etc. are intended over $\mathbb{K}$. We denote by **Set** the category of sets (in a fixed universe) and by **Art** the category of local Artinian $\mathbb{K}$-algebras (with residue field $\mathbb{K}$). If A is an object in **Art**, then $\mathfrak{m}_A$ denotes its maximal ideal.

1 – Review of differential graded Lie algebras

A differential graded vector space is a pair (V, d), where $V = \oplus_{i\in\mathbb{Z}} V^i$ is a $\mathbb{Z}$-graded vector space and d is a differential of degree $+1$, *i.e.*, $d : V^i \to V^{i+1}$ and $d \circ d = 0$. For every integer n, we define a new differential graded vector space $V[n]$, by setting

$$V[n]^i = V^{n+i} \qquad \text{and} \qquad d_{V[n]} = (-1)^n d_V.$$

DEFINITION 1.1. *A differential graded Lie algebra (DGLA for short) is a triple $(L, [\,,\,], d)$, where $(L = \oplus_{i\in\mathbb{Z}} L^i, d)$ is a differential graded vector space and $[\,,\,] : L \times L \to L$ is a bilinear map of degree zero, called bracket, satisfying the following conditions:*

(1) (*graded skewsymmetry*) $[a, b] = -(-1)^{\deg(a)\deg(b)}[b, a]$;
(2) (*graded Jacobi identity*) $[a, [b, c]] = [[a, b], c] + (-1)^{\deg(a)\deg(b)}[b, [a, c]]$;
(3) (*graded Leibniz rule*) $d[a, b] = [da, b] + (-1)^{\deg(a)}[a, db]$.

EXAMPLE 1.2. If $L = \oplus L^i$ is a DGLA, then L^0 is a Lie algebra in the usual sense; vice-versa, every Lie algebra is a differential graded Lie algebra concentrated in degree 0 (and differential zero).

EXAMPLE 1.3. If L is a DGLA and B is a commutative $\mathbb{K}$-algebra, then $L \otimes B$ has a natural structure of DGLA, given by

$$[l \otimes a, m \otimes b] = [l, m] \otimes ab;$$

$$d(l \otimes a) = dl \otimes a.$$

A morphism of differential graded Lie algebras $\phi\colon L \to M$ is a linear map that preserves degrees and commutes with brackets and differentials. A quasi-isomorphism of DGLAs is a morphism that induces an isomorphism in cohomology. Two DGLAs L and M are said to be quasi-isomorphic if they are equivalent under the equivalence relation generated by: $L \sim M$ if there exists a quasi-isomorphism $\phi : L \to M$.

1.1 – Deformation functor associated with a DGLA

DEFINITION 1.4. *Let L be a DGLA; then, the Maurer-Cartan functor associated with L is the functor*

$$MC_L : \mathbf{Art} \to \mathbf{Set},$$

$$MC_L(A) = \left\{ x \in L^1 \otimes m_A \mid dx + \frac{1}{2}[x,x] = 0 \right\}.$$

Note that in the previous equation we use the DGLA structure on $L \otimes m_A$ induced by the one on L (see Example 1.3).

DEFINITION 1.5. *Two elements x and $y \in L^1 \otimes m_A$ are gauge equivalent if there exists $a \in L^0 \otimes m_A$ such that*

$$y = e^a * x := x + \sum_{n \geq 0} \frac{[a,-]^n}{(n+1)!}([a,x] - da).$$

The operator $*$ is called the gauge action of the group $\exp(L^0 \otimes m_A)$ on $L \otimes m_A$; indeed, $e^a * e^b * x = e^{a \bullet b} * x$, where $\bullet$ is the Baker-Campbell-Hausdorff product in the nilpotent DGLA $L \otimes m_A$, *i.e.*, $a \bullet b = a + b + \frac{1}{2}[a,b] + \frac{1}{12}[a,[a,b]] - \frac{1}{12}[b,[b,a]] + \cdots$.

DEFINITION 1.6. *The deformation functor associated with a differential graded Lie algebra L is:*

$$\mathrm{Def}_L : \mathbf{Art} \to \mathbf{Set},$$

$$\mathrm{Def}_L(A) = \frac{\mathrm{MC}_L(A)}{\text{gauge}} = \frac{\{x \in L^1 \otimes \mathfrak{m}_A \mid dx + \frac{1}{2}[x,x] = 0\}}{\exp(L^0 \otimes \mathfrak{m}_A)}.$$

REMARK 1.7. Every morphism of DGLAs induces a natural transformation of the associated deformation functors. If L and M are quasi-isomorphic DGLAs, then the associated functor Def_L and Def_M are isomorphic [SS79, GM88, GM90], [Ma99, Corollary 3.2], or [Ma04b, Corollary 5.52].

2 – Semicosimplicial objects

Let Δ_{mon} be the category whose objects are the finite ordinal sets $[n] = \{0, 1, \dots, n\}$, $n = 0, 1, \dots$, and whose morphisms are order-preserving injective maps among them. Every morphism in Δ_{mon}, different from the identity, is a finite composition of coface morphisms:

$$\partial_k \colon [i-1] \to [i], \qquad \partial_k(p) = \begin{cases} p & \text{if } p < k \\ p+1 & \text{if } k \leq p \end{cases}, \qquad k = 0, \dots, i.$$

The relations about compositions of them are generated by

$$\partial_l \partial_k = \partial_{k+1} \partial_l \,, \qquad \text{for every } l \leq k.$$

DEFINITION 2.1. *According to* $[EZ50, We94]$*, a semicosimplicial object in a category* $\mathbf{C}$ *is a covariant functor* $A^\Delta \colon \Delta_{\mathrm{mon}} \to \mathbf{C}$*. Equivalently, a semicosimplicial object* A^Δ *is a diagram in* $\mathbf{C}$*:*

$$A_0 \rightrightarrows A_1 \;\substack{\rightarrow\\ \rightarrow\\ \rightarrow}\; A_2 \;\substack{\rightarrow\\ \rightarrow\\ \rightarrow\\ \rightarrow}\; \cdots \,,$$

where each A_i *is in* $\mathbf{C}$*, and, for each* $i > 0$*, there are* $i+1$ *morphisms*

$$\partial_k \colon A_{i-1} \to A_i, \qquad k = 0, \dots, i,$$

such that $\partial_l \partial_k = \partial_{k+1} \partial_l$*, for any* $l \leq k$*.*

EXAMPLE 2.2. Let $\chi : L \to M$ be a morphism in a category $\mathbf{C}$. Then, we can consider it as a semicosimplicial object in $\mathbf{C}$, by extension with zero, *i.e.*,

$$\chi^\Delta : \quad L \rightrightarrows M \;\substack{\rightarrow\\ \rightarrow}\; 0 \cdots, \quad \partial_0 = \chi, \quad \partial_1 = 0,$$

EXAMPLE 2.3. Let X be a smooth variety, defined over an algebraically closed field of characteristic 0. Let $\mathcal{U} = \{U_i\}$ be an affine open cover and $\mathcal{F}$ a sheaf of Lie algebras on X. Then, we can define the Čech semicosimplicial Lie algebra $\mathcal{F}(\mathcal{U})$ as the semicosimplicial Lie algebra

$$\mathcal{F}(\mathcal{U}) : \quad \prod_i \mathcal{F}(U_i) \rightrightarrows \prod_{i<j} \mathcal{F}(U_{ij}) \;\substack{\rightarrow\\ \rightarrow\\ \rightarrow}\; \prod_{i<j<k} \mathcal{F}(U_{ijk}) \;\substack{\rightarrow\\ \rightarrow\\ \rightarrow\\ \rightarrow}\; \cdots \,,$$

where the coface maps ∂_h: $\prod_{i_0<\cdots<i_{k-1}} \mathcal{F}(U_{i_0\cdots i_{k-1}}) \to \prod_{i_0<\cdots<i_k} \mathcal{F}(U_{i_0\cdots i_k})$ are given by

$$\partial_h(x)_{i_0\dots i_k} = x_{i_0\dots\widehat{i_h}\dots i_k\,|U_{i_0\cdots i_k}}, \qquad \text{for } h = 0,\dots,k.$$

2.1 – The total construction

Given a semicosimplicial differential graded vector space

$$V^\Delta : V_0 \rightrightarrows V_1 \;\substack{\rightarrow\\ \rightarrow\\ \rightarrow}\; V_2 \;\substack{\rightarrow\\ \rightarrow\\ \rightarrow\\ \rightarrow}\; \cdots,$$

the graded vector space $\bigoplus_{n\geq 0} V_n[-n]$ has two differentials, *i.e.*,

$$d = \sum_n (-1)^n d_n, \qquad \text{where} \quad d_n \text{ is the differential of } V_n,$$

and

$$\partial = \sum_i (-1)^i \partial_i, \qquad \text{where} \quad \partial_i \text{ are the coface maps.}$$

More explicitly, if $v \in V_n^i$, then the degree of v is $i+n$ and

$$d(v) = (-1)^n d_n(v) \in V_n^{i+1},\ \partial(v) = \partial_0(v) - \partial_1(v) + \cdots + (-1)^{n+1}\partial_{n+1}(v) \in V_{n+1}^i.$$

Since $d\partial + \partial d = 0$, we define $\mathrm{Tot}(V^\Delta)$ as the graded vector space $\bigoplus_{n\geq 0} V_n[-n]$, endowed with the differential $D = d + \partial$.

Remark 2.4. In Example 2.3, the total complex $\mathrm{Tot}(\mathcal{F}(\mathcal{U}))$, associated with the Čech semicosimplicial Lie algebra $\mathcal{F}(\mathcal{U})$, is nothing else that the Čech complex $\check{C}(\mathcal{U},\mathcal{F})$ of the sheaf $\mathcal{F}$.

There is also another way to associate with a semicosimplicial differential graded vector space V^Δ a differential graded vector space. Namely, let $(A_{PL})_n$ be the differential graded commutative algebra of polynomial differential forms on the standard n-simplex $\{(t_0,\dots,t_n) \in \mathbb{K}^{n+1} \mid \sum t_i = 1\}$ [FHT01]:

$$(A_{PL})_n = \frac{\mathbb{K}[t_0,\dots,t_n,dt_0,\dots,dt_n]}{(1-\sum t_i, \sum dt_i)}.$$

For every n, m the tensor product $V_n \otimes (A_{PL})_m$ is a differential graded vector space and then also $\prod_n V_n \otimes (A_{PL})_n$ is a differential graded vector space. Denote by

$$\delta^k\colon (A_{PL})_n \to (A_{PL})_{n-1}, \quad \delta^k(t_i) = \begin{cases} t_i & \text{if } 0 \leq i < k \\ 0 & \text{if } i = k \\ t_{i-1} & \text{if } k < i \end{cases}, \qquad k = 0,\dots,n,$$

the face maps, for every $0 \leq k \leq n$; then, there are well-defined morphisms of differential graded vector spaces

$$Id \otimes \delta^k \colon V_n \otimes (A_{PL})_n \to V_n \otimes (A_{PL})_{n-1},$$
$$\partial_k \otimes Id \colon V_{n-1} \otimes (A_{PL})_{n-1} \to V_n \otimes (A_{PL})_{n-1}.$$

The Thom-Whitney differential graded vector space $\mathrm{Tot}_{TW}(V^\Delta)$ of V^Δ is the differential graded subvector space of $\prod_n V_n \otimes (A_{PL})_n$, whose elements are the sequences $(x_n)_{n\in\mathbb{N}}$ satisfying the equations

$$(Id \otimes \delta^k)x_n = (\partial_k \otimes Id)x_{n-1}, \quad \text{for every } \ 0 \leq k \leq n.$$

LEMMA 2.5. *The differential graded vector spaces* $\mathrm{Tot}(V^\Delta)$ *and* $\mathrm{Tot}_{TW}(V^\Delta)$ *are quasi-isomorphic.*

PROOF. See [Whi57, Dup76, Dup 78, NaA87, Get04, FMM08, CG08] for explicit description of the quasi-isomorphism. □

Let

$$\mathfrak{g}^\Delta : \quad \mathfrak{g}_0 \rightrightarrows \mathfrak{g}_1 \;\substack{\rightarrow\\ \rightarrow\\ \rightarrow}\; \mathfrak{g}_2 \;\substack{\rightarrow\\ \rightarrow\\ \rightarrow\\ \rightarrow}\; \cdots,$$

be a semicosimplicial differential graded Lie algebra. Since, every DGLA is, in particular, a differential graded vector space, we can consider the associated total complex $\mathrm{Tot}(\mathfrak{g}^\Delta)$. Even if all $\mathfrak{g}_i$ are DGLAs, there is no natural DGLA structure on $\mathrm{Tot}(\mathfrak{g}^\Delta)$ [FiMa07, IM09]

EXAMPLE 2.6. Let $\chi : L \to M$ be a morphism of DGLAs, then, following Example 2.2, we can associate with it a semicosimplicial DGLA. Its total complex $\mathrm{Tot}(\chi^\Delta)$ is nothing else than the (suspension of the) mapping cone complex associated with χ. Even in this simple case, it is not possible to define a canonical DGLA structure on $\mathrm{Tot}(\chi^\Delta)$, such that the projection $\mathrm{Tot}(\chi^\Delta) \to L$ is a morphism of DGLAs [IM09, Example 3.1].

However, in the case of semicosimplicial DGLAs, we can apply the Thom-Whitney construction to g^Δ: it turns out that $\mathrm{Tot}_{TW}(\mathfrak{g}^\Delta)$ has a structure of DGLA [NaA87, FMM08] .

REMARK 2.7. Using the homotopy transfer, the DGLA structure of $\mathrm{Tot}_{TW}(\mathfrak{g}^\Delta)$ induces an L_∞-algebra structure $\widetilde{\mathrm{Tot}}(\mathfrak{g}^\Delta)$ on the differential graded vector space $\mathrm{Tot}(\mathfrak{g}^\Delta)$, such that $\widetilde{\mathrm{Tot}}(\mathfrak{g}^\Delta)$ and $\mathrm{Tot}_{TW}(\mathfrak{g}^\Delta)$ are quasi-isomorphic; see [FiMa07, FMM08] or [IM09, Corollary 3.3].

2.2 – Deformation functor associated with semicosimplicial DGLAs

Let $\mathfrak{g}^\Delta$ be a semicosimplicial DGLA. Applying the Thom-Whitney construction of the previous section, we can consider the DGLA $\mathrm{Tot}_{TW}(\mathfrak{g}^\Delta)$ and so the associated deformation functor $\mathrm{Def}_{\mathrm{Tot}_{TW}(\mathfrak{g}^\Delta)}$. Beyond this way, there is another natural, and more geometric, way to define a deformation functor associated with $\mathfrak{g}^\Delta$, see [Pr03, Definitions 1.4 and 1.6], [FMM08, Section 3] or [FIM09, Definition 2.1 and 2.2].

More precisely, if $\mathfrak{g}^\Delta$ is a semicosimplicial DGLA, we can define the functor

$$Z^1_{\mathrm{sc}}(\exp \mathfrak{g}^\Delta)\colon \mathbf{Art} \to \mathbf{Set},$$

such that, for all $A \in \mathbf{Art}$, $Z^1_{\mathrm{sc}}(\exp \mathfrak{g}^\Delta)(A)$ is the set of the pairs $(l, m) \in (\mathfrak{g}^1_0 \otimes \mathfrak{m}_A) \oplus (\mathfrak{g}^0_1 \otimes \mathfrak{m}_A)$, satisfying the following conditions:

(1) $dl + \frac{1}{2}[l, l] = 0$;
(2) $\partial_1 l = e^m * \partial_0 l$;
(3) $\partial_0 m \bullet -\partial_1 m \bullet \partial_2 m = dn + [\partial_2\partial_0 l, n]$, for some $n \in \mathfrak{g}_2^{-1} \otimes \mathfrak{m}_A$.

Moreover, we define the functor

$$H^1_{\mathrm{sc}}(\exp \mathfrak{g}^\Delta)\colon \mathbf{Art} \to \mathbf{Set},$$

such that

$$H^1_{\mathrm{sc}}(\exp \mathfrak{g}^\Delta)(A) = \frac{Z^1_{\mathrm{sc}}(\exp \mathfrak{g}^\Delta)(A)}{\sim},$$

where (l_0, m_0) and $(l_1, m_1) \in Z^1_{\mathrm{sc}}(\exp \mathfrak{g}^\Delta)(A)$ are equivalent under the relation $\sim$ if and only if there exist elements $a \in \mathfrak{g}^0_0 \otimes \mathfrak{m}_A$ and $b \in \mathfrak{g}_1^{-1} \otimes \mathfrak{m}_A$, such that

(1) $e^a * l_0 = l_1$;
(2) $-m_0 \bullet -\partial_1 a \bullet m_1 \bullet \partial_0 a = db + [\partial_0 l_0, b]$.

Example 2.8. Let L be a differential graded Lie algebra, then it can be considered as a semicosimplicial DGLA $\mathfrak{L}^\Delta$ by zero extension, *i.e.*, $\mathfrak{L}^\Delta_0 = L$ and $\mathfrak{L}^\Delta_i = 0$, for all $i > 0$. In this case, the above functors $Z^1_{\mathrm{sc}}(\exp \mathfrak{L}^\Delta)$ and $H^1_{\mathrm{sc}}(\exp \mathfrak{L}^\Delta)$ reduce to MC_L and Def_L, respectively.

Example 2.9. If $\chi : L \to M$ is a morphism of DGLAs, then we can consider it as a simple case of semicosimplicial DGLA χ^Δ, extending χ by zero (see Example 2.2).

In this case, the functors $Z^1_{\mathrm{sc}}(\exp \chi^\Delta)$ and $H^1_{\mathrm{sc}}(\exp \chi^\Delta)$ coincide with the functors MC_χ and Def_χ defined in [Ma07, Section 2]. More precisely, we have

$$\mathrm{Def}_\chi(A) = \frac{\mathrm{MC}_\chi(A)}{\exp(L^0 \otimes \mathfrak{m}_A) \times \exp(dM^{-1} \otimes \mathfrak{m}_A)},$$

where

$$\mathrm{MC}_\chi(A)=\left\{(x,e^a)\in(L^1\otimes\mathfrak{m}_A)\times\exp(M^0\otimes\mathfrak{m}_A)\,|\,dx+\frac{1}{2}[x,x]=0,\ e^a*\chi(x)=0\right\},$$

and the gauge action of $\exp(L^0\otimes\mathfrak{m}_A)\times\exp(dM^{-1}\otimes\mathfrak{m}_A)$ is given by the formula

$$(e^l,e^{dm})*(x,e^a)=(e^l*x,e^{dm}e^ae^{-\chi(l)})=(e^l*x,e^{dm\bullet a\bullet-\chi(l)}).$$

In particular, if $\chi:L\to M$ is an injective morphism of DGLAs, then for every $A\in\mathbf{Art}$, we have

$$\mathrm{MC}_\chi(A)=\left\{e^a\in\exp(M^0\otimes\mathfrak{m}_A)\mid\ e^{-a}*0\in L^1\otimes\mathfrak{m}_A\right\}.$$

Under this identification, the gauge action becomes

$$\exp(L^0\otimes\mathfrak{m}_A)\times\mathrm{MC}_\chi(A)\to\mathrm{MC}_\chi(A),\qquad(e^m,e^a)\mapsto e^ae^{-m},$$

and then

$$\mathrm{Def}_\chi(A)=\frac{\mathrm{MC}_\chi(A)}{\exp(L^0\otimes\mathfrak{m}_A).}$$

Example 2.10. If all $\mathfrak{g}_i=0$, for all $i>1$, then the functors $Z^1_{\mathrm{sc}}(\exp\mathfrak{g}^\Delta)$ and $H^1_{\mathrm{sc}}(\exp\mathfrak{g}^\Delta)$ reduce to the functors $\mathrm{MC}_{(\partial_0,\partial_1)}$ and $\mathrm{Def}_{(\partial_0,\partial_1)}$, respectively, associated with the pair of morphisms of DGLAs $\partial_0,\partial_1:\mathfrak{g}_0\to\mathfrak{g}_1$, introduced in [Ia08].

Example 2.11. If each $\mathfrak{g}_i$ is concentrated in degree zero, *i.e.*, $\mathfrak{g}^\Delta$ is a semicosimplicial Lie algebra, then the functors $Z^1_{\mathrm{sc}}(\exp\mathfrak{g}^\Delta)$ and $H^1_{\mathrm{sc}}(\exp\mathfrak{g}^\Delta)$ reduce to the one defined in [FMM08, Section 3]. More explicitly, in this case, we have

$$Z^1_{sc}(\exp\mathfrak{g}^\Delta)(A)=\{x\in\mathfrak{g}_1\otimes\mathfrak{m}_A\mid e^{\partial_0x}e^{-\partial_1x}e^{\partial_2x}=1\},$$

and $x\sim y$ if and only if there exists $a\in\mathfrak{g}_0\otimes\mathfrak{m}_A$, such that $e^{-\partial_1a}e^xe^{\partial_0a}=e^y$.

Therefore, given a semicosimplicial DGLA $\mathfrak{g}^\Delta$, we can define two deformations functor, $\mathrm{Def}_{\mathrm{Tot}_{TW}(\mathfrak{g}^\Delta)}$ and $H^1_{\mathrm{sc}}(\exp\mathfrak{g}^\Delta)$. The relation between these functors is given by the following theorem.

Theorem 2.12. *Let $\mathfrak{g}^\Delta$ be a semicosimplicial DGLA such that $H^k(\mathfrak{g}_i)=0$, for all i and for all $k<0$. Then, there exists a natural isomorphism of deformation functors*

$$\mathrm{Def}_{\mathrm{Tot}_{TW}(\mathfrak{g}^\Delta)}\simeq H^1_{\mathrm{sc}}(\exp\mathfrak{g}^\Delta).$$

PROOF. In the case of semicosimplicial Lie algebra, this theorem was proved in [FMM08, Theorem 6.8]. For the general case, see [FIMM09, Theorem 7.6]. □

3 – Bisemicosimplicial objects

In this section, we generalize the notion of semicosimplicial objects, defining bisemicosimplicial objects.

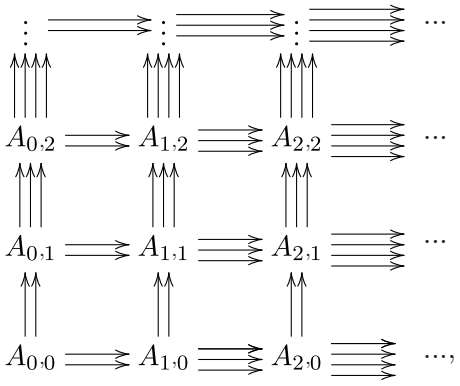
DEFINITION 3.1. *According to [GJ99, Chapter IV], a bisemicosimplicial object $A^{\blacktriangle}$ in a category $\mathbf{C}$ is a covariant functor $A^{\blacktriangle}\colon \Delta_{\mathrm{mon}} \times \Delta_{\mathrm{mon}} \to \mathbf{C}$; equivalently, a bisemicosimplicial object in $\mathbf{C}$ is a semicosimplicial object in the category of semicosimplicial object in $\mathbf{C}$. More explicitly, it consists of objects $A_{i,j}$, for all $i, j \geq 0$, and morphisms $\partial_k^{V_i}$ and $\partial_s^{H_j}$ in $\mathbf{C}$, for each $i, j > 0$, such that*

$$\partial_k^{V_i}\colon A_{i,j-1} \to A_{i,j}, \qquad k = 0, \dots, j,$$
$$\partial_s^{H_j}\colon A_{i-1,j} \to A_{i,j}, \qquad s = 0, \dots, i,$$

and the following compatibility conditions are satisfied

$$\begin{aligned}
\partial_l^{V_i} \circ \partial_k^{V_i} &= \partial_{k+1}^{V_i} \circ \partial_l^{V_i}, && \forall l \leq k,\\
\partial_s^{H_j} \circ \partial_t^{H_j} &= \partial_{t+1}^{H_j} \circ \partial_s^{H_j}, && \forall s \leq t,\\
\partial_s^{H_{j+1}} \circ \partial_k^{V_i} &= \partial_k^{V_{i+1}} \circ \partial_s^{H_j}, && \forall s \leq i+1,\ k \leq j+1.
\end{aligned}$$

We shall say that the object $A_{i,j}$ has bidegree (i, j) or precisely horizontal degree i and vertical degree j, and that $\partial_\bullet^{H_j}$ and $\partial_\bullet^{V_i}$ are horizontal (height j) and vertical (column i) morphisms, respectively. In particular, for all fixed j, $(A_{\bullet,j}, \partial_\bullet^{H_j})$ is a (horizontal) semicosimplicial object in $\mathbf{C}$; analogously, for all fixed i, $(A_{i,\bullet}, \partial_\bullet^{V_i})$ is a (vertical) semicosimplicial object in $\mathbf{C}$. To sum up, a bisemicosimplicial object $A^{\blacktriangle}$ looks like a diagram



where each line and each column is a semicosimplicial object and each square commutes in a simplicial sense, *i.e.*, for all s, k, i and j, the following diagram commutes

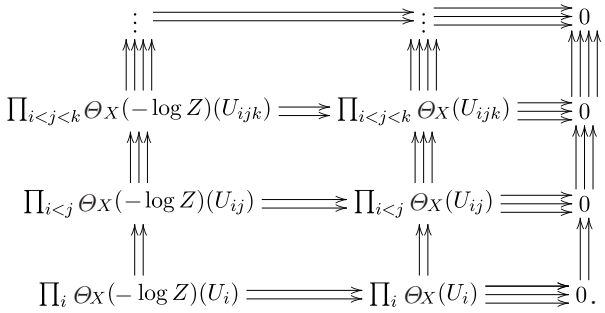
$$\begin{array}{ccc} A_{i,j+1} & \xrightarrow[\partial_s^{H_{j+1}}]{} & A_{i+1,j+1} \\ \partial_k^{V_i} \uparrow & & \uparrow \partial_k^{V_{i+1}} \\ A_{i,j} & \xrightarrow[\partial_s^{H_j}]{} & A_{i+1,j} \end{array}$$

EXAMPLE 3.2. Every semicosimplicial object in a category $\mathbf{C}$ can be considered as a bisemicosimplcial object concentrated in zero (vertical or horizontal) degree.

Bisemicosimplicial objects naturally arise in simple situation. Indeed, let $\mathcal{F}$ and $\mathcal{G}$ be sheaves on a variety X, with value in a category $\mathbf{C}$. Fix an affine open cover $\mathcal{U} = \{U_i\}$. Then, as in Example 2.3, we denote by $\mathcal{F}(\mathcal{U})$ and $\mathcal{G}(\mathcal{U})$ the associated Čech semicosimplicial objects in $\mathbf{C}$. Next, let $\varphi : \mathcal{F} \to \mathcal{G}$ be a morphism of sheaves. Since φ commutes with restrictions of every open subsets, it induces a morphism $\varphi^{\Delta} : \mathcal{F}(\mathcal{U}) \to \mathcal{G}(\mathcal{U})$ of semicosimplcial objects. Finally, as in Example 2.2, we can consider the semicosimplicial extension of φ^{Δ} (by zero) to get a bisemicosimplcial object $\varphi^{\blacktriangle} : \mathcal{F}(\mathcal{U}) \to \mathcal{G}(\mathcal{U})$ in $\mathbf{C}$. This construction is commutative, *i.e.*, we can firstly extend φ (by zero) to get a semcosimplicial sheaf of object in $\mathbf{C}$, and then apply the Čech semicosimplicial construction to all sheaves.

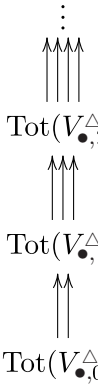
EXAMPLE 3.3. Let X be a smooth variety, defined over an algebraically closed field of characteristic 0, and $\mathcal{U} = \{U_i\}$ be an affine open cover. Let $Z \subset X$ be a closed subscheme of X. We denote by $\Theta_X(-\log Z)$ the sheaf of germs of tangent vectors to X which are tangent to Z [Se06, Section 3.4.4]. We recall that, if $\mathcal{I} \subset \mathcal{O}_X$ is the ideal sheaf of Z in X, then $\Theta(-\log Z) = \{f \in Der(\mathcal{O}_X, \mathcal{O}_X) \mid f(\mathcal{I}) \subset \mathcal{I}\}$. Let $\chi : \Theta_X(-\log Z) \hookrightarrow \Theta_X$ be the inclusion of sheaves of Lie algebras. Then, we can associate with $\Theta_X(-\log Z)$ and Θ_X the Čech semicosimplicial Lie algebra $\Theta_X(-\log Z)(\mathcal{U})$ and $\Theta_X(\mathcal{U})$, respectively. Finally, extending the morphism χ by zero, we get a a bisemicosimplicial Lie algebra $\chi^{\blacktriangle} : \Theta_X(-\log Z)(\mathcal{U}) \to \Theta_X(\mathcal{U})$.

More explicitly, we have the following diagram



3.1 – The total construction

Let $V^{\blacktriangle} = (V^*_{n,m}, d_{n,m})_{n,m}$ be a bisemicosimplicial differential graded vector space; in particular, we recall that each line and each column is a semicosimplicial differential graded vector space. Then, as in Section 2.1, with each horizontal semicosimplicial differential graded vector space $(V^{\Delta}_{\bullet,m}, \partial^{H_m}_{\bullet})$, we can associate the total complex $\mathrm{Tot}(V^{\Delta}_{\bullet,m})$. We recall that $\mathrm{Tot}(V^{\Delta}_{\bullet,m}) = \bigoplus_{n\geq 0} V^*_{n,m}[-n]$ and its differential is $D_m = \sum_n (-1)^n d_{n,m} + \sum_j (-1)^j \partial^{H_m}_j$. In this way, we construct a semicosimplicial differential graded vector space $\mathrm{Tot}^{H,\Delta}(V^{\blacktriangle})$



In particular, we can still apply the total construction to $\mathrm{Tot}^{H,\Delta}(V^{\blacktriangle})$ to obtain the differential graded vector space $\mathrm{Tot}(\mathrm{Tot}^{H,\Delta}(V^{\blacktriangle}))$. More explicitly, $\mathrm{Tot}(\mathrm{Tot}^{H,\Delta}(V^{\blacktriangle})) = \bigoplus_m \mathrm{Tot}(V^{\Delta}_{\bullet,m})[-m] = \bigoplus_{n,m} V^*_{n,m}[-n-m]$ and the differential is $D = \sum_m (-1)^m D_m + \sum_k (-1)^k \partial^{V_\bullet}_k = \sum_{m,n} (-1)^{m+n} d_{n,m} + \sum_{j,m} (-1)^{j+m} \partial^{H_m}_j + \sum_k (-1)^k \partial^{V_\bullet}_k$.

Analogously, given $V^{\blacktriangle} = (V^*_{n,m}, d_{n,m})_{n,m}$, we can firstly focus our attention on each vertical semicosimplicial differential graded vector space $(V^{\Delta}_{n,\bullet}, \partial^{V_n}_{\bullet})$. As before, we can associate with each column its total complex, to get a semicosimplicial differential graded vector space $\mathrm{Tot}^{V,\Delta}(V^{\blacktriangle})$

$$\mathrm{Tot}(V^{\Delta}_{0,\bullet}) \rightrightarrows \mathrm{Tot}(V^{\Delta}_{1,\bullet}) \;\substack{\rightarrow\\ \rightarrow\\ \rightarrow}\; \mathrm{Tot}(V^{\Delta}_{2,\bullet}) \;\substack{\rightarrow\\ \rightarrow\\ \rightarrow\\ \rightarrow}\; \cdots,$$

In this case, $\mathrm{Tot}(V^{\Delta}_{n,\bullet}) = \bigoplus_m V^*_{n,m}[-m]$ and its differential is given by $D'_n = \sum_m (-1)^m d_{n,m} + \sum_j (-1)^j \partial^{V_n}_j$. Then, applying again the total construction to $\mathrm{Tot}^{V,\Delta}(V^{\blacktriangle})$, we get the differential graded vector space $\mathrm{Tot}(\mathrm{Tot}^{V,\Delta}(V^{\blacktriangle}))$. In this case, we have $\mathrm{Tot}(\mathrm{Tot}^{V,\Delta}(V^{\blacktriangle})) = \bigoplus_n \mathrm{Tot}(V^{\Delta}_{n,\bullet})[-n] = \bigoplus_{n,m} V^*_{n,m}[-n-m]$ and the differential is $D' = \sum_n (-1)^n D'_n + \sum_k (-1)^k \partial^{H_\bullet}_k = \sum_{m,n} (-1)^{n+m} d_{n,m} + \sum_{j,n} (-1)^{j+n} \partial^{V_n}_j + \sum_k (-1)^k \partial^{H_\bullet}_k$.

Moreover, we can also consider the total complex $(\mathrm{Tot}^{\blacktriangle}(V^{\blacktriangle}), D)$ associated with the triple complex $(V^*_{n,m}, d_{n,m}, \partial^V, \partial^H)$. More explicitly, $\mathrm{Tot}^{\blacktriangle}(V^{\blacktriangle})^i = \bigoplus_{n,m} V_{n,m}[-n-m]^{i-n-m}$ and the differential is given by $D = d + \partial_1 + \partial_2$, where $d = \sum_{m,n} (-1)^{m+n} d_{n,m}$, $\partial_1 = \sum_{j,m} (-1)^{j+m} \partial^{H_m}_j$ and $\partial_2 = \sum_k (-1)^k \partial^{V_\bullet}_k$.

LEMMA 3.4. *Let $V^{\blacktriangle} = (V^*_{n,m}, d_{n,m})_{n,m}$ be a bisemicosimplicial differential graded vector space. Then, the associated differential graded vector spaces $(\mathrm{Tot}^{\blacktriangle}(V^{\blacktriangle}), D)$, $\mathrm{Tot}(\mathrm{Tot}^{H,\Delta}(V^{\blacktriangle}))$ and $\mathrm{Tot}(\mathrm{Tot}^{V,\Delta}(V^{\blacktriangle}))$ are quasi isomorphic.*

PROOF. It follows from a standard computation, using spectral sequence. □

As in the previous section, we can also apply the Thom-Whitney construction instead of the total complex construction. Also in this case, we get two differential graded vector spaces $\mathrm{Tot}_{TW}(\mathrm{Tot}^{H,\Delta}_{TW})$ and $\mathrm{Tot}_{TW}(\mathrm{Tot}^{V,\Delta}_{TW})$ depending, a priori, on the order of the construction. There is also a more direct way, based on the Thom-Whitney construction, to associate a differential graded vector space with a bisemicosimplicial differential graded vector space.

DEFINITION 3.5. *Let $V^{\blacktriangle} = (V_{n,m})$ be a bisemicosimplicial DGLA. The Thom-Whitney DGLA $\mathrm{Tot}^{\blacktriangle}_{TW}(V^{\blacktriangle})$ is defined as the sub-differential graded vector space of $\prod_{n,m} V_{n,m} \otimes (A_{PL})_n \otimes (A_{PL})_m$, whose elements are sequences $(x_{n,m})_{n,m}$ satisfying the relations:*

$$(\partial^{H_m}_k \otimes Id \otimes Id) x_{n,m} = (Id \otimes \delta^k \otimes Id) x_{n+1,m}, \quad \textit{for every } 0 \le k \le n,$$

and

$$(\partial^{V_n}_k \otimes Id \otimes Id) x_{n,m} = (Id \otimes Id \otimes \delta^k) x_{n,m+1}, \quad \textit{for every } 0 \le k \le m.$$

More explicitly, we are considering sequence of elements $(x_{n,m})_{n,m} = x_{n,m} \otimes \alpha_n \otimes \beta_m \in V_{n,m} \otimes (A_{PL})_n \otimes (A_{PL})_m$ *such that*

$$\partial_k^{H_m} x_{n,m} \otimes \alpha_n \otimes \beta_m = x_{n+1,m} \otimes \delta^k \alpha_{n+1} \otimes \beta_m$$

and

$$\partial_k^{V_n} x_{n,m} \otimes \alpha_n \otimes \beta_m = x_{n,m+1} \otimes \alpha_n \otimes \delta^k \beta_{m+1}.$$

LEMMA 3.6. *Let* $V^{\blacktriangle} = (V_{n,m})$ *be a bisemicosimplicial differential graded vector space; then, the Thom-Withney construction does not depend on the order, i.e.,* $\mathrm{Tot}_{TW}(\mathrm{Tot}_{TW}^{H,\Delta}) \cong \mathrm{Tot}_{TW}(\mathrm{Tot}_{TW}^{V,\Delta}) \cong \mathrm{Tot}_{TW}^{\blacktriangle}(V^{\blacktriangle})$

PROOF. It follows from the explicit description of the Thom-Withney construction. □

If $\mathfrak{g}^{\blacktriangle}$ is a bisemicosimplicial DGLAs, then, as in the semicosimplicial case, the differential graded vector space $\mathrm{Tot}_{TW}^{\blacktriangle}(\mathfrak{g}^{\blacktriangle})$ inherits a structure of DGLA.

REMARK 3.7. As for the semicosimplicial case, the differential graded vector spaces $\mathrm{Tot}_{TW}^{\blacktriangle}(\mathfrak{g}^{\blacktriangle})$ and $\mathrm{Tot}^{\blacktriangle}(\mathfrak{g}^{\blacktriangle})$ are quasi-isomorphic. In a forthcoming paper, we will use the DGLA structure of $\mathrm{Tot}_{TW}^{\blacktriangle}(\mathfrak{g}^{\blacktriangle})$ and the homotopy transfer to define a canonical L_∞-algebra structure $\widetilde{\mathrm{Tot}}^{\blacktriangle}(\mathfrak{g}^{\blacktriangle})$ on $\mathrm{Tot}^{\blacktriangle}(\mathfrak{g}^{\blacktriangle})$, such that $\widetilde{\mathrm{Tot}}^{\blacktriangle}(\mathfrak{g}^{\blacktriangle})$ and $\mathrm{Tot}_{TW}^{\blacktriangle}(\mathfrak{g}^{\blacktriangle})$ are quasi-isomorphic L_∞-algebra.

3.2 – Deformation functors associated with a bisemicosimplicial DGLA

In this section, we will describe how we can associate a deformation functor with a bisemicosimplicial DGLA. In Section 2.2, we introduced the deformation functor $H^1_{\mathrm{sc}}(\exp \mathfrak{g}^{\Delta})$ associated with a semicosimplicial DGLA $\mathfrak{g}^{\Delta}$. Moreover, Theorem 2.12 states that $H^1_{\mathrm{sc}}(\exp \mathfrak{g}^{\Delta}) \simeq \mathrm{Def}_{\mathrm{Tot}_{TW}(\mathfrak{g}^{\Delta})}$, whenever $H^k(\mathfrak{g}_i) = 0$, for all i and for all $k < 0$.

Next, let $\mathfrak{g}^{\blacktriangle}$ be a bisemicosimplicial DGLA. In the previous section, we associate with $\mathfrak{g}^{\blacktriangle}$, the semicosimplicial DGLA $\mathrm{Tot}_{TW}^{H,\Delta}$ and $\mathrm{Tot}_{TW}^{V,\Delta}$. Therefore, we can naturally associate with $\mathfrak{g}^{\blacktriangle}$ the two deformations functors $H^1_{\mathrm{sc}}(\exp \mathrm{Tot}_{TW}^{H,\Delta})$ and $H^1_{\mathrm{sc}}(\exp \mathrm{Tot}_{TW}^{V,\Delta})$. Moreover, we associate with $\mathfrak{g}^{\blacktriangle}$ the Thom-Whitney DGLA $\mathrm{Tot}_{TW}^{\blacktriangle}(\mathfrak{g}^{\blacktriangle})$ and its deformation functor $\mathrm{Def}_{\mathrm{Tot}_{TW}^{\blacktriangle}(\mathfrak{g}^{\blacktriangle})}$. The following theorem explains the relation between all these functors.

THOREM 3.8. *Let* $\mathfrak{g}^{\blacktriangle}$ *be a bisemicosimplicial DGLA such that* $H^k(\mathfrak{g}_{i,j}) = 0$ *for all* i, j *and* $k < 0$. *Then, there exist natural isomorphisms of deformation functors*

$$H^1_{\mathrm{sc}}(\exp \mathrm{Tot}_{TW}^{H,\Delta}) \cong \mathrm{Def}_{\mathrm{Tot}_{TW}(\mathrm{Tot}_{TW}^{H,\Delta}(V^{\blacktriangle}))} \cong$$

$$\cong \mathrm{Def}_{\mathrm{Tot}_{TW}^{\blacktriangle}(\mathfrak{g}^{\blacktriangle})} \cong \mathrm{Def}_{\mathrm{Tot}_{TW}(\mathrm{Tot}_{TW}^{V,\Delta}(\mathfrak{g}^{\blacktriangle}))} \cong H^1_{\mathrm{sc}}(\exp \mathrm{Tot}_{TW}^{V,\Delta}).$$

PROOF. The cohomological constraint of the hypothesis implies that $H^k(\mathrm{Tot}^{H,\Delta}_{TW}(\mathfrak{g}^{\blacktriangle})_m) = H^k(\mathrm{Tot}^{V,\Delta}_{TW}(\mathfrak{g}^{\blacktriangle})_n) = 0$, for all n, m and for all $k < 0$. Therefore, the first and last isomorphisms follow from Theorem 2.12. The remaining isomorphisms follow from Lemma 3.6. □

EXAMPLE 3.9. (Example 3.3 revisited) Let X be a smooth variety, $Z \subset X$ a closed subscheme and $\mathcal{U} = \{U_i\}_i$ an affine open cover of X. Denote by $\chi : \Theta_X(-\log Z) \hookrightarrow \Theta_X$ the inclusion of sheaves of Lie algebras. Following Example 3.3, we have the bisemicosimplicial Lie algebra $\chi^{\blacktriangle} : \Theta_X(-\log Z)(\mathcal{U}) \to \Theta_X(\mathcal{U})$ and so we can consider the associated DGLA $\mathrm{Tot}^{\blacktriangle}_{TW}(\chi^{\blacktriangle})$. Moreover, as in the the previous construction, we can associate with χ two semicosimplicial DGLAs. he easiest way is to consider the induced morphism of DGLA $\chi_{TW} : \mathrm{Tot}_{TW}(\Theta_X(-\log Z)(\mathcal{U})) \to \mathrm{Tot}_{TW}(\Theta_X(\mathcal{U}))$, and view it as a semicosimplcial DGLA by zero extension (see Example 2.2), *i.e.*,

$$\chi^{\Delta}_{TW} : \quad \mathrm{Tot}_{TW}(\Theta_X(-\log Z)(\mathcal{U})) \underset{\chi_{TW}}{\overset{0}{\rightrightarrows}} \mathrm{Tot}_{TW}(\Theta_X(\mathcal{U})) \rightrightarrows 0 \cdots .$$

Analogously, if we apply the Thom-Whitney construction firstly on the rows, then we get the semicosimplcial DGLA T^{Δ}

$$\begin{array}{c} \vdots \\ \uparrow\uparrow\uparrow\uparrow \\ T_2 = \mathrm{Tot}_{TW}(\prod_{i<j<k} \Theta_X(-\log Z)(U_{ijk}) \to \prod_{i<j<k} \Theta_X(U_{ijk})) \\ \uparrow\uparrow\uparrow \\ T_1 = \mathrm{Tot}_{TW}(\prod_{i<j} \Theta_X(-\log Z)(U_{ij}) \to \prod_{i<j} \Theta_X(U_{ij})) \\ \uparrow\uparrow \\ T_0 = \mathrm{Tot}_{TW}(\prod_{i} \Theta_X(-\log Z)(U_{i}) \to \prod_{i} \Theta_X(-\log Z)(U_{i})). \end{array}$$

In this second case, the vertical maps are the restrictions to open subsets (see Example 2.3). The previous Theorem 3.8 implies that there exist isomorphisms of deformation functors

$$\mathrm{Def}_{\chi_{TW}} \cong \mathrm{Def}_{\mathrm{Tot}^{\blacktriangle}_{TW}(\chi^{\blacktriangle})} \cong H^1_{\mathrm{sc}}(\exp T^{\Delta}).$$

We recall that the functor $\mathrm{Def}_{\chi_{TW}}$ is isomorphic to $H^1_{\mathrm{sc}}(\exp \chi^{\Delta}_{TW})$ (see Example 2.9). More explicitly, since χ is injective, for all $A \in \mathbf{Art}$, the set $\mathrm{Def}_{\chi_{TW}}(A)$ is given by

$$\mathrm{Def}_{\chi_{TW}}(A) = \frac{\mathrm{MC}_{\chi_{TW}}(A)}{\sim},$$

where

$$\mathrm{MC}_{\chi_{TW}}(A) = \{a \in \mathrm{Tot}_{TW}(\Theta_X(\mathcal{U}))^0 \otimes \mathfrak{m}_A) |$$
$$e^{-a} * 0 \in \mathrm{Tot}_{TW}(\Theta_X(-\log Z)(\mathcal{U}))^1 \otimes \mathfrak{m}_A\},$$

and $e^a \sim e^{a'}$ if and only if there exist $b \in \mathrm{Tot}_{TW}(\Theta_X(-\log Z)(\mathcal{U}))^0 \otimes \mathfrak{m}_A$, such that $e^{a'} = e^a e^{-b}$.

4 – Application: Deformations of subvarieties in a fixed smooth variety

Let X be a smooth variety, defined over an algebraically closed field $\mathbb{K}$ of characteristic 0, and $Z \subset X$ a closed subscheme of X. We recall the definition of infinitesimal deformations of Z in X fixed, full details can be found in [Se06].

Definition 4.1. *Let $A \in \mathbf{Art}$. An infinitesimal deformation of Z in X over* $\mathrm{Spec}(A)$ *is a cartisian diagram*

$$\begin{array}{ccc} Z & \xrightarrow{i} & Z_A \subset X \times \mathrm{Spec}(A) \\ \downarrow & & \downarrow \pi \\ \mathrm{Spec}(\mathbb{K}) & \xrightarrow{a} & \mathrm{Spec}(A), \end{array}$$

where π is a flat map induced by the projection from $X \times \mathrm{Spec}(A)$ to $\mathrm{Spec}(A)$. *The associated infinitesimal deformation functor is*

$$\mathrm{Hilb}_X^Z : \mathbf{Art} \to \mathbf{Set},$$

such that

$$\mathrm{Hilb}_X^Z(A) = \{\textit{infinitesimal deformations of } Z \textit{ in } X \textit{ over } \mathrm{Spec}(A)\}.$$

Moreover, we can define the sub-functor

$$\mathrm{Hilb}'^Z_X : \mathbf{Art} \to \mathbf{Set},$$

where

$\mathrm{Hilb}'^Z_X(A)$ =\{locally trivial infinitesimal deformations of Z in X over $\mathrm{Spec}(A)$\}.

We recall that, an infinitesimal deformation Z_A of Z in X over $\mathrm{Spec}(A)$ is called locally trivial if, for every point $z \in Z$, there exists an open neighbourhood $U_z \subset Z$ such that

$$\begin{array}{ccc} U_z & \xrightarrow{\ i\ } & Z_{A|U_z} \\ \big| & & \big| \\ \mathrm{Spec}(\mathbb{K}) & \xrightarrow{\ a\ } & \mathrm{Spec}(A), \end{array}$$

is a trivial deformation of U_z. Whenever $Z \subset X$ is smooth, then every deformation of Z in X is locally trivial and so $\mathrm{Hilb}^Z_X = \mathrm{Hilb}'^Z_X$.

Next, following Examples 3.3 and 3.9, denote by $\chi : \Theta_X(-\log Z) \hookrightarrow \Theta_X$, the inclusion of sheaves of Lie algebras, and by $\chi^{\blacktriangle} : \Theta_X(-\log Z)(\mathcal{U}) \to \Theta_X(\mathcal{U})$, the associated bisemicosimplicial Lie algebra.

THEOREM 4.2. *Let X be a smooth variety, defined over an algebraically closed field $\mathbb{K}$ of characteristic 0, and $Z \subset X$ a closed subscheme. Then, there exists an isomorphism of functors* $\mathrm{Def}_{\mathrm{Tot}^{\blacktriangle}_{TW}(\chi^{\blacktriangle})} \cong \mathrm{Hilb}'^Z_X$. *In particular, if $Z \subset X$ is smooth, then* $\mathrm{Def}_{\mathrm{Tot}^{\blacktriangle}_{TW}(\chi^{\blacktriangle})} \cong \mathrm{Hilb}^Z_X$.

PROOF. For $\mathbb{K} = \mathbb{C}$ and Z smooth, this theorem was already proved in [Ma07, Theorem 5.2]ManettiSemireg, without the use of semicosimplicial language.

Let $\mathcal{U} = \{U_i\}_{i\in I}$ be an affine open cover of X and $\mathcal{V} = \{V_i = U_i \cap Z\}_{i\in I}$ the induced one on Z. Let Z_A be a locally trivial deformation of Z in X over $\mathrm{Spec}(A)$. Then, Z_A is obtained by gluing the trivial deformations $V_i \otimes A$ in $U_i \otimes A$ along the double intersections $V_{ij} \otimes A$, such that the induced deformation of X is trivial. Therefore, it is determined by a sequence $\{\theta_{ij}\}_{i<j}$ of automorphisms of the sheaves of A-algebras

$$\begin{array}{ccccc} & & \mathcal{O}_Z(V_{ij}) & & \\ & \nearrow & & \nwarrow & \\ \mathcal{O}_Z(V_{ij}) \otimes A & & \xrightarrow[\simeq]{\theta_{ij}} & & \mathcal{O}_Z(V_{ij}) \otimes A \\ & \nwarrow & & \nearrow & \\ & & A, & & \end{array}$$

satisfying the cocycle condition

$$\theta_{jk}\theta_{ik}^{-1}\theta_{ij} = \mathrm{Id}_{\mathcal{O}_Z(V_{ijk})\otimes A}, \qquad \forall\ i<j<k \in I, \tag{1}$$

and such that there exist automorphisms α_i of $\mathcal{O}_X(U_i) \otimes A$ satisfying

$$\theta_{ij} = {\alpha_i}^{-1}\alpha_j, \qquad \forall i<j. \tag{2}$$

Note that Equation (2) implies (1). Since we are in characteristic zero, we can take the logarithms and write $\theta_{ij} = e^{d_{ij}}$, for some $d_{ij} \in \Theta_X(-\log Z)(U_{ij}) \otimes \mathfrak{m}_A$, and $\alpha_i = e^{a_i}$, with $a_i \in \Theta_X(U_i) \otimes \mathfrak{m}_A$.

Therefore, a locally trivial deformation of Z in X over $\mathrm{Spec}(A)$ is equivalent to the datum of a sequence $\{a_i\}_i \in \prod_i \Theta_X(U_i) \otimes \mathfrak{m}_A$, such that

$$e^{-a_i} e^{a_j} \in \exp(\Theta_X(-\log Z)(U_{ij}) \otimes \mathfrak{m}_A), \qquad \forall\, i < j \in I.$$

As regards the equivalence relation, let Z_A and Z'_A be two deformations of Z in X over $\mathrm{Spec}(A)$. Denote by $\theta_{ij} = e^{d_{ij}} = e^{-a_i} e^{a_j}$ and $\theta'_{ij} = e^{d'_{ij}} = e^{-a'_i} e^{a'_j}$ the data associated with Z_A and Z'_A, respectively. The deformations Z_A and Z'_A are isomorphic if, for every i, there exists an automorphism β_i of $\mathcal{O}_Z(V_i) \otimes A$, such that $\theta_{ij} = {\beta_i}^{-1} \theta'_{ij} \beta_j$, for every $i < j$, and satisfying the compatibility relation $\alpha'_i \beta_i = \alpha_i$. Taking again logarithms, an isomorphism between Z_A and Z'_A is equivalent to the existence of a sequence $\{b_i\}_i \in \prod_i \Theta_X(-\log Z)(U_i) \otimes \mathfrak{m}_A$, such that $e^{a_i} = e^{a'_i} e^{b_i}$.

Next, from the DGLA point of view, we showed in Example 3.9, that $\mathrm{Def}_{\mathrm{Tot}^{\blacktriangle}_{TW}(\chi^{\blacktriangle})} \cong H^1_{\mathrm{sc}}(\exp \chi^{\blacktriangle}) \cong \mathrm{Def}_{\chi_{TW}}$. Therefore, it is enough to prove that ${\mathrm{Hilb}'}^Z_X \cong \mathrm{Def}_{\chi_{TW}}$, with $\chi_{TW} : \mathrm{Tot}_{TW}(\Theta_X(-\log Z)(\mathcal{U})) \hookrightarrow \mathrm{Tot}_{TW}(\Theta_X(\mathcal{U}))$; and it follows from the explicit description of $\mathrm{Def}_{\chi_{TW}}$. Indeed, $\mathrm{MC}_{\chi_{TW}}(A)$ is the set of all $a \in \mathrm{Tot}_{TW}(\Theta_X(\mathcal{U}))^0 \otimes \mathfrak{m}_A$, such that $e^{-a} * 0 \in \mathrm{Tot}_{TW}(\Theta_X(-\log Z)(\mathcal{U}))^1 \otimes \mathfrak{m}_A$, *i.e.*, $a = \{a_i\}_i \in \prod_i \Theta_X(U_i) \otimes \mathfrak{m}_A$, such that $e^{-a_i} e^{a_j} \in \exp(\Theta_X(-\log Z)(U_{ij}) \otimes \mathfrak{m}_A)$. Moreover, $a \sim a'$ if and only is there exist $b \in \mathrm{Tot}_{TW}(\Theta_X(-\log Z)(\mathcal{U}))^0 \otimes \mathfrak{m}_A$, such that $e^{a'} = e^a e^{-b}$, *i.e.*, $b = \{b_i\}_i \in \prod_i \Theta_X(-\log Z)(U_i) \otimes \mathfrak{m}_A$ such that $e^{a_i} = e^{a'_i} e^{b_i}$. □

Remark 4.3. In a forthcoming paper, we will use this theorem to study the obstructions to the deformations of Z in X, via the semiregularity map.

Acknowledgements

I gratefully acknowledge the Max Planck Institute of Bonn, where this note was carried out, for financial support and warm hospitality. I wish to thank Marco Manetti for many useful discussions, advices and suggestions. This paper is dedicated to Marialuisa J. de Resmini: I am indebted with her as she guides my first steps into the world of research.

REFERENCES

[Ar76] M. Artin: *Deformations of Singularities*, Tata Institute of Foundamental Research, Bombay, (1976).

[CG08] X. Z. Cheng – E. Getzler: *Homotopy commutative algebraic structures*, J. Pure Appl. Algebra, **212** (2008) pp. 2535–2542; `arXiv:math.AT/0610912`.

[Dup76] J. L. Dupont: *Simplicial de Rham cohomology and characteristic classes of flat bundles*, Topology, **15**, (1976) pp. 233–245.

[Dup78] J. L. Dupont: *Curvature and characteristic classes*, Lecture Notes in Mathematics, **640**, Springer-Verlag, New York Berlin, (1978).

[EZ50] S. Eilenberg – J. A. Zilber: *Semi-simplicial complexes and singular homology*, Ann. of Math., (2), **51** (1950) pp. 499–513.

[FHT01] Y. Félix – S. Halperin – J. Thomas: *Rational homotopy theory*, Graduate texts in mathematics, **205**, Springer-Verlag, New York Berlin, (2001).

[FIM09] D. Fiorenza – D. Iacono – E. Martinengo: *Differential graded Lie algebras controlling infinitesimal deformations of coherent sheaves*, Preprint `arXiv: 0904.1301v3`.

[FIM] D. Fiorenza – D. Iacono – E. Martinengo: *Infinitesimal deformations of singular varieties*, (in preparation).

[FiMa07] D. Fiorenza – M. Manetti: *L_∞ structures on mapping cones*, Algebra Number Theory, **1** (2007) pp. 301–330; `arXiv:math.QA/0601312`.

[FMM08] D. Fiorenza – M. Manetti – E. Martinengo: *Semicosimplicial DGLAs in deformation theory*, Preprint `arXiv:0803.0399v1`.

[Get04] E. Getzler: *Lie theory for nilpotent L_∞-algebras*, Ann. of Math., (1), **170** (2009) pp. 271–301; `arXiv:math/0404003v4`.

[GJ99] P. G. Goerss – J. F. Jardine: *Simplicial homotopy theory*, Progress in Mathematics **174**; Birkaüser-Verlag; Basel-Boston-Berlin, (1999).

[GM88] W. M. Goldman – J. J. Millson: *The deformation theory of representations of fundamental groups of compact kähler manifolds*, Publ. Math. I.H.E.S., **67** (1988) pp. 43–96.

[GM90] W. M. Goldman – J. J. Millson: *The homotopy invariance of the Kuranishi space*, Illinois J. Math., **34** (1990) pp. 337–367.

[Gr59] A. Grothendieck: *Technique de Descente et théorèmes d'existence en géométrie algébrique. II. Le théorèmes d'existence en théorie formelle des modules*, Séminaire Bourbaki, t. 12, Exp. no. **195** (1959-1960).

[Hin97] V. Hinich: *Descent of Deligne groupoids,*, Internat. Math. Res. Notices, **5** (1997) pp. 223–239.

[Ia06] D. Iacono: *Differential Graded Lie Algebras and Deformations of Holomorphic Maps*, Phd Thesis, (2006) `arXiv:math.AG/0701091`.

[Ia07] D. Iacono: *A semiregularity map annihilating obstructions to deforming holomorphic maps*, Cand. Math. Bull (to appear) `arXiv:0707.2454`.

[Ia08] D. Iacono: *L_∞-algebras and deformations of holomorphic maps.*, Int. Math. Res. Not. **8** (2008) p. 36 `arXiv:0705.4532`.

[IM09] D. Iacono – M. Manetti: *An algebraic proof of Bogomolov-Tian-Todorov theorem*, accepted by Proceedings of the Workshop "Algebraic and Geometric Deformation Spaces"; `arXiv:0902.0732`.

[Kod86] K. Kodaira: *Complex manifold and deformation of complex structures*, Grundlehren der mathematischen Wissenschaften, **283**, Springer-Verlag, New York, Berlin (1986).

[KoSp58] K. Kodaira – D. C. Spencer: *On Deformations of Complex Analytic Structures, II*, Ann. of Math., (2), **67** (1958) pp. 403–466.

[Kon94] M. Kontsevich: *Topics in algebra-deformation theory*, unpublished notes on a course given at the University of Berkley, (1994).

[Kon03] M. Kontsevich: *Deformation quantization of Poisson manifolds, I.*, Letters in Mathematical Physics, **66** (2003) pp. 157–216 arXiv:q-alg/9709040.

[Ku71] M. Kuranishi: *Deformations of compact complex manifolds*, Séminaire de Mathematiques Supérieures, No. **39** (Été 1969), Les Presses de l'Université de Montreal, Montreal, (1971).

[Ma99] M. Manetti: *Deformation theory via differential graded Lie algebras,*, Seminari di Geometria Algebrica 1998-1999, Scuola Normale Superiore, (1999); arXiv: math.AG/0507284.

[Ma04b] M. Manetti: *Lectures on deformations of complex manifolds.*, Rend. Mat. Appl., (7), **24** (2004) pp. 1–183; arXiv:math.AG/0507286.

[Ma07] M. Manetti: *Lie description of higher obstructions to deforming submanifolds*, Ann. Sc. Norm. Super. Pisa Cl. Sci., **6** (2007) pp. 631-659; arXiv: math.AG/0507287.

[Ma09] M. Manetti: *Differential graded Lie algebras and formal deformation theory*, Algebraic Geometry: Seattle 2005. Proc. Sympos. Pure Math., **80** (2009) pp. 785–810.

[NaA87] V. Navarro Aznar: *Sur la théorie de Hodge-Deligne*, Invent. Math., **90** (1987) pp. 11–76.

[Pr03] J. P. Pridham: *Deformations via Simplicial Deformation Complexes*, Preprint arXiv:math/0311168v6.

[Schl68] M. Schlessinger: *Functors of Artin rings,*, Trans. Amer. Math. Soc., **130** (1968) pp. 208–222.

[SS79] M. Schlessinger, J. Stasheff: *Deformation Theory and Rational Homotopy Type*, Preprint (1979).

[Se06] E. Sernesi: *Deformations of Algebraic Schemes*, Grundlehren der mathematischen Wissenschaften, Springer-Verlag, New York Berlin, **334** (2006).

[We94] C. A. Weibel: *An introduction to homological algebra*, Cambridge Studies in Advanced Mathematics, Cambridge Univesity Press, Cambridge, **38** (1994).

[Whi57] H. Whitney: *Geometric integration theory*, Princeton University Press, Princeton, N. J., (1957).

Lavoro pervenuto alla redazione il 10 marzo 2010
ed accettato per la pubblicazione il 15 marzo 2010.
Bozze licenziate il 20 aprile 2010

Indirizzo dell'Autore:

Donatella Iacono – Max-Planck Institut für Mathematik –Vivatsgasse 7, D 53111 – Bonn – Germany
Email: iacono@mpim-bonn.mpg.de

Rendiconti di Matematica, Serie VII
Volume 30, Roma (2010), 111-120

Characterizing Geometric Designs

To Marialuisa J. de Resmini on the occasion of her retirement

DIETER JUNGNICKEL

Abstract: *We conjecture that the classical geometric 2-designs $PG_d(n,q)$, where $2 \leq d \leq n-1$, are characterized among all designs with the same parameters as those having line size $q+1$. The conjecture is known to hold for the case $d = n-1$ (the Dembowski-Wagner theorem) and also for $d = 2$ (a recent result established by Tonchev and the present author). Here we extend this result to the cases $d = 3$ and $d = 4$. The general case remains open and seems to be difficult.*

1 – Introduction

In this note, we are concerned with the problem of characterizing the classical geometric designs $PG_d(n,q)$, where d is in the range $2 \leq d \leq n-2$, among all designs with the same parameters. For the convenience of the reader, we first recall basic facts about these designs. Let Π denote $PG(n,q)$, the n-dimensional projective space over the field $GF(q)$ with q elements. Then the points and d-spaces of Π form a 2-(v,k,λ) design $\mathcal{D} = PG_d(n,q)$ with parameters

$$v = \begin{bmatrix} n+1 \\ 1 \end{bmatrix}_q = (q^{n+1}-1)/(q-1),$$

$$k = \begin{bmatrix} d+1 \\ 1 \end{bmatrix}_q = (q^{d+1}-1)/(q-1),$$

$$r = \begin{bmatrix} n \\ d \end{bmatrix}_q, \lambda = \begin{bmatrix} n-1 \\ d-1 \end{bmatrix}_q \text{ and } b = \begin{bmatrix} n+1 \\ d+1 \end{bmatrix}_q,$$

Key Words and Phrases: *Projective spce – Block Designs*
A.M.S. Classification: 51E20, 05B05.

where $\begin{bmatrix} n \\ i \end{bmatrix}_q$ denotes the number of i-dimensional subspaces of an n-dimensional vector space over $GF(q)$. These so-called Gaussian coefficients are given explicitly as

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

Furthermore, the lines of the design $\mathcal{D}$ are just the lines of Π; in particular, all lines of $\mathcal{D}$ have cardinality $q+1$.[(1)] All these facts are well-known.

The classical designs are far from being characterized by their parameters. This is well-known for the case $d = n-1$: the number of symmetric 2-designs with the parameters of a classical point-hyperplane design $PG_{n-1}(n,q)$ grows exponentially, and a similar result also holds for affine 2-designs with the parameters of a classical point-hyperplane design $AG_{n-1}(n,q)$. These results were originally established by the author [5] in 1984, whose bounds were subsequently improved in several papers [7, 8, 9]. In a recent paper, the author and Tonchev established the corresponding result for the number of 2-designs with the parameters of $PG_d(n,q)$, where d is in the range $2 \le d \le n-2$.

This naturally poses the problem of characterizing the classical geometric designs $PG_d(n,q)$ among all designs with the same parameters. Again, the case $d = n-1$ has been settled for a long time: Dembowski and Wagner obtained several elegant characterizations in a celebrated paper [2] which appeared in 1960; see also [1] for a proof. One of their results characterizes the designs $PG_{n-1}(n,q)$ by their line size, namely $q+1$, and an analogous result was recently established by Tonchev and the present author [6] for the case $d = 2$.

In contrast, not that much is known for the cases $3 \le d \le n-2$. The only result I am aware of is due to Lefèvre-Percsy [10], who proved that a smooth[(2)] design with the parameters of $PG_d(n,q)$, where $d \ge 2$ and $q \ge 4$, but q not necessarily a prime power, is classical if and only if all lines have size at least $q+1$.

Unfortunately, Lefèvre-Percsy's hypothesis that the design should be smooth is a very severe restriction; moreover, the assumption $q \ge 4$ seems somewhat unnatural. Therefore the problem of finding a nicer characterization remains open. In this direction, I offer the following

---

(1) Recall that the *line* determined by two points of a design is defined as the intersection of all blocks containing these two points. See [1] for background on designs, and [3, 4] for background on finite projective spaces.

(2) Recall that the *plane* determined by three non-collinear points of a design is defined as the intersection of all blocks containing the three given points. In general, planes may be properly contained in other planes. This undesirable phenomenon is excluded if one requires the design to be *smooth*, that is, if one assumes that any three non-collinear points are contained in a constant number of blocks, which is then usually denoted by ϱ. See [1] for details.

CONJECTURE 1.1. A design with the parameters of $PG_d(n,q)$, where $2 \leq d \leq n-1$ and where $q \geq 2$ is not necessarily a prime power, is classical (so that q is actually a prime power) if and only if all lines have size $q+1$.

As mentioned before, this conjecture is already known to hold for the case $d = n-1$ (the Dembowski-Wagner theorem) and also for $d = 2$ (by the recent result of [6]). In the present note, I will establish the validity of Conjecture 1.1 for the cases $d = 3$ and $d = 4$. For the convenience of the reader, I shall also repeat the simple proof for the case $d = 2$ as a warm-up. It will become apparent that the problem gets more and more involved as d grows, so that a general proof will most likely require some major new idea. Even the next open case $d = 5$ seems to be rather challenging.

My proofs will repeatedly appeal to a simple, but extremely useful result concerning subspaces of linear spaces. Recall that a *linear space* Σ is just a pairwise balanced design with joining number $\lambda = 1$; therefore one speaks of *lines* instead of *blocks* in this context. A *subspace* of Σ is a subset S of the point set with the property that each line intersecting S in at least two points is entirely contained in S; thus the lines of Σ induce a linear space on S. The result alluded to gives bounds on the cardinality of a proper subspace, see [1, I.8.4]. As we shall only require the case where Σ has constant line size k (so that Σ is actually a 2-design), we merely state this special case:

LEMMA 1.2. *Let S be a proper subspace of a $2-(v,k,1)$-design Σ. Then the cardinality of S satisfies the bound $|S| \leq (v-1)/(k-1)$.*

Finally, the subspace *spanned* by a subset U of the point set of a linear space Σ is, of course, just the smallest subspace S of Σ containing U.

2 – The cases $d = 2$ and $d = 3$

We begin by recalling the case $d = 2$ from [6]:

THEOREM 2.1. *Let $\mathcal{D}'$ be a 2-design with the same parameters as the classical design $\mathcal{D} = PG_2(n,q)$, where $n \geq 3$ and where $q \geq 2$ is not necessarily a prime power. Then $\mathcal{D}'$ is isomorphic to the classical design if and only if all lines of $\mathcal{D}'$ have size $q+1$.*

PROOF. The condition that all lines have size $q+1$ is trivially necessary. Thus assume that this condition is satisfied. Note that all blocks of $\mathcal{D}'$ have cardinality $k = q^2+q+1$ in this case. Consider an arbitrary block B. Any two points of B define a unique line of $\mathcal{D}'$ which, by our hypothesis, has size $q+1$. Thus the lines of B induce a $(q^2+q+1, q+1, 1)$-design on B, and hence every block of $\mathcal{D}'$ carries the structure of a projective plane of order q.

We next claim that an arbitrary line ℓ of $\mathcal{D}'$ and an arbitrary point $p \notin \ell$ determine a unique block of $\mathcal{D}'$; in other words, the blocks of $\mathcal{D}'$ containing ℓ partition the points not in ℓ. Note first that no two such blocks can intersect outside ℓ, since each block is a projective plane and since a line of a plane together with a point outside spans the entire plane. Now it suffices to count: there are $q^n + ... + q^2$ points outside ℓ and there are $q^{n-2} + \ldots + q + 1$ blocks containing ℓ, each of which has q^2 points not in ℓ.

It is now easily seen that the points and lines of $\mathcal{D}'$ satisfy the Veblen-Young axioms and therefore define a projective space Π; see, for instance, [1, Section XII.1]. In view of the parameters of $\mathcal{D}'$, we have $\Pi \cong PG(n, q)$, and thus $\mathcal{D}' \cong \mathcal{D}$. □

As we shall see, the case $d = 3$ is already more involved:

THEOREM 2.2. *Let $\mathcal{D}'$ be a 2-design with the same parameters as the classical design $\mathcal{D} = PG_3(n, q)$, where $n \geq 4$ and where $q \geq 2$ is not necessarily a prime power. Then $\mathcal{D}'$ is isomorphic to the classical design if and only if all lines of $\mathcal{D}'$ have size $q + 1$.*

PROOF. The condition that all lines have size $q + 1$ is trivially necessary. Thus assume that this condition is satisfied. Note that all blocks of $\mathcal{D}'$ have cardinality $k = q^3 + q^2 + q + 1$ in this case. Consider an arbitrary block B. Any two points of B define a unique line of $\mathcal{D}'$ which, by our hypothesis, has size $q+1$. Thus the lines of B induce a linear space Σ_B with constant line size $q+1$ on B. We want to show that an arbitrary line ℓ of $\mathcal{D}'$ and an arbitrary point $p \notin \ell$ again span a projective plane of order q, as in the case $d = 2$; this will require more work than before.

Step 1. Let ℓ be a line, B a block through ℓ, and $p \notin \ell$ a point of B. Then the subspace S of Σ_B spanned by p and ℓ is either a projective plane of order q or equal to B. In the latter case, B is the only block containing ℓ and p.

As each of the $q + 1$ points p' of ℓ determines together with p a line pp' of size $q+1$, it is clear that S has at least $q(q+1)+1$ points; in case of equality, S is obviously a projective plane of order q. But by Lemma 1.2, a proper subspace of Σ_B contains at most

$$\frac{v-1}{k-1} = \frac{q^3+q^2+q}{q} = q^2+q+1$$

points, and therefore either S is a proper subspace of cardinality $q^2 + q + 1$ of Σ_B, or $S = B$. As any two blocks intersect in a proper subspace (of either of these blocks), the assertion follows.

Step 2. Let ℓ be a line and $p \notin \ell$ a point of $\mathcal{D}'$. Then there are exactly

$$\varrho = q^{n-3} + \ldots + q + 1$$

blocks of $\mathcal{D}'$ containing both p and ℓ.[3]

We first fix the line ℓ and determine the average number of blocks containing ℓ and a point $p \notin \ell$. Now ℓ is on

$$\lambda = \frac{(q^{n-1}-1)(q^{n-2}-1)}{(q^2-1)(q-1)}$$

blocks, each of which contains q^3+q^2 further points. As there are altogether $q^n+q^{n-1}+\ldots+q^2$ points not in ℓ, a short computation shows that the desired average number is precisely the quantity ϱ defined in the assertion. Hence it suffices to check that ϱ is also an upper bound for the number ϱ_p of blocks containing ℓ and some given point $p \notin \ell$. Obviously, we may assume $\varrho_p \geq 2$ for this purpose. Then the ϱ_p blocks through p and ℓ intersect in a common subspace S of cardinality q^2+q+1, by Step 1. Moreover, no two of these blocks can share a point not in S, by Lemma 1.2. As there are exactly $q^n+\ldots+q^4+q^3$ points $p' \notin S$, we obtain indeed

$$\varrho_p \leq \frac{q^n+\ldots+q^4+q^3}{q^3} = \varrho.$$

Step 3. Let Σ denote the linear space induced by the lines of $\mathcal{D}'$. Then the subspace spanned by any three non-collinear points of $\mathcal{D}'$ is a projective plane of order q.

This follows immediately by combining Steps 1 and 2.

Step 4. The linear space Σ is isomorphic to $PG_1(n,q)$.

Using Step 3, one easily checks that the points and lines of $\mathcal{D}'$ satisfy the Veblen-Young axioms and therefore define a projective space Π; see, for instance, [1, section XII.1]. In view of the parameters of $\mathcal{D}'$, we have $\Sigma \cong PG_1(n,q)$.

Step 5. $\mathcal{D}'$ is isomorphic to $PG_3(n,q)$.

After Step 4, it still remains to show that the blocks of $\mathcal{D}'$ are actually the 3-subspaces of Π. Let us first note that the subspaces of cardinality q^2+q+1 of Σ are just the planes of Π. This is clear, as any given line ℓ and any point $p \notin \ell$ determine the same projective plane of order q in both structures, namely the union of the $q+1$ lines pp' where p' runs over the points of ℓ; see Step 3. By Step 2 and by the counting argument used there, any given plane S is in exactly ϱ blocks, which give rise to a partition of the points not in S. Hence S and any such point p determine a unique block, namely the union of the q^2+q+1 lines pp' where p' runs over the points of S. But this is also the point set of the 3-subspace of Π determined by S and p. □

[3] This will establish that $\mathcal{D}'$ is smooth, and hence we could then, for $q \geq 4$, appeal to the result of [10]. Of course, this would leave the cases $q=2$ and $q=3$ unresolved.

3 – The case $d = 4$

We now settle the case $d = 4$ of Conjecture 1.1 , using similar arguments as for the case $d = 3$; as already mentioned, this turns out to be quite involved.

THEOREM 3.1. *Let $\mathcal{D}'$ be a 2-design with the same parameters as the classical design $\mathcal{D} = PG_4(n, q)$, where $n \geq 5$ and where $q \geq 2$ is not necessarily a prime power. Then $\mathcal{D}'$ is isomorphic to the classical design if and only if all lines of $\mathcal{D}'$ have size $q + 1$.*

PROOF. The condition that all lines have size $q + 1$ is trivially necessary. Thus assume that this condition is satisfied. Note that all blocks of $\mathcal{D}'$ have cardinality $k = q^4 + q^3 + q^2 + q + 1$ in this case. Consider an arbitrary block B. Any two points of B define a unique line of $\mathcal{D}'$ which, by our hypothesis, has size $q+1$. Thus the lines of B induce a linear space Σ_B with constant line size $q+1$ on B. Again, we need to show that an arbitrary line ℓ of $\mathcal{D}'$ and an arbitrary point $p \notin \ell$ span a projective plane of order q, as in the cases $d = 2$ and $d = 3$; this will require considerably more work than before.

As before, let Σ denote the linear space induced by the lines of $\mathcal{D}'$ on the point set V of $\mathcal{D}'$. For any subset X of V, we shall denote the subspace of Σ spanned by X as $S(X)$. For any line ℓ and any point $p \notin \ell$, we put $S(p, \ell) := S(\{p\} \cup \ell)$ and write $\varrho(p, L)$ for the number of blocks containing both p and ℓ, and hence all of $S(p, \ell)$. As in the proof of Theorem 2.2, one easily obtains

Step 1. $S(p, \ell) \geq q^2 + q + 1$ for each line ℓ and each point $p \notin \ell$.

But now we get a further possibility for the precise structure of $S(p, \ell)$:

Step 2. Let ℓ be a line, B a block through ℓ, and $p \notin \ell$ a point of B. Then $S(p, \ell)$ is either a projective plane of order q, or a proper maximal subspace of Σ_B, or equal to B. In the latter case, B is the only block containing both ℓ and p.

To see this, note that a proper subspace of Σ_B contains at most q^3+q^2+q+1 points, by Lemma 1.2. If $S(p, \ell)$ is not a projective plane of order q, it has at least $q^2 + q + 2$ points, by Step 1.[(4)] Using Lemma 1.2 again, any subspace properly containg S then has to have cardinality at least $q^3 + q^2 + 2q + 1$, and hence has to be equal to B.

Step 3. Let ℓ be a line. Then the average number of blocks containing ℓ and a point $p \notin \ell$ is given by

$$\varrho = \frac{(q^{n-2} - 1)(q^{n-3} - 1)}{(q^2 - 1)(q - 1)}.$$

[(4)] Actually it would be easy to obtain a stronger bound, namely $2q^2 + 2q + 2$, but the weak version given above will already suffice. However, it seems not possible to obtain a precise cardinality for this – as we shall see, anyway entirely hypothetical – case.

The line ℓ is on

$$\lambda = \frac{(q^{n-1}-1)(q^{n-2}-1)(q^{n-3}-1)}{(q^3-1)(q^2-1)(q-1)}$$

blocks, each of which contains $q^4+q^3+q^2$ further points. As there are altogether $q^n+q^{n-1}+\ldots+q^2$ points not in ℓ, we get

$$\varrho = \frac{(q^{n-1}-1)(q^{n-2}-1)(q^{n-3}-1)q^2(q^2+q+1)}{(q^3-1)(q^2-1)(q-1)q^2(q^{n-2}+\ldots+q+1)},$$

and a short computation gives the desired result for ϱ.

Step 4. Let ℓ be a line, and p a point not on ℓ. Then $S(p,\ell)$ is a projective plane of order q, provided that $\varrho(p,\ell) \geq q^{n-4}+\ldots+q^2+q+2$.

Assume otherwise. Then Step 2 shows that $S := S(p,\ell)$ is a proper maximal subspace of Σ_B for every block B containing both p and ℓ, so that any two distinct blocks B and B' containing both p and ℓ intersect precisely in S. Moreover, as we have seen in the proof of Step 2,

$$q^2+q+2 \leq |S(p,\ell)| \leq q^3+q^2+q+1.$$

Hence there are at most $q^n+\ldots+q^4+q^3-1$ points not in S, and each of these points is on at most one block containing S. Also, each such block contains at least q^4 such points. Hence we get

$$\varrho(p,\ell) \leq \frac{q^n+\ldots+q^4+q^3-1}{q^4} < q^{n-4}+\ldots+q^2+q+2,$$

contradicting the hypothesis.

Step 5. Let ℓ be a line, p a point not on ℓ, and assume that $S := S(p,\ell)$ is a projective plane of order q. Given any point $p' \notin S$, let us put $S' = S'(p') := S(\ell \cup \{p,p'\})$. Then either S' is contained in at most one block, or $|S'| = q^3+q^2+q+1$. Moreover, there are at most $\tau := q^{n-3}+\ldots+q+1$ subspaces of cardinality q^3+q^2+q+1 containing S, and equality holds if and only if S and any point $p' \notin S$ always span a subspace of cardinality q^3+q^2+q+1.

Note that S is a proper subspace of S', and therefore, by Lemma 1.2, $|S'| \geq q^3+q^2+q+1$. If S' is contained in two distinct blocks, it is a proper subspace of both of them, and another application of Lemma 1.2 gives the desired equality. Now the second assertion is easily seen, as there are exactly $q^n+\ldots+q^4+q^3$ choices for p'.

Step 6. Let S' be any subspace of Σ of cardinality q^3+q^2+q+1. Then there are at most $\sigma := q^{n-4}+\ldots+q+1$ blocks containing S', and equality holds if and only if all such blocks give rise to a partition of the set V' of all points of Σ not contained in S'.

We may assume that there are two distinct blocks containing S', so that S' is a proper maximal subspace of every block containing it. Then no two such blocks can intersect in a point of V'. Hence we indeed get at most

$$\frac{q^n+\ldots+q^5+q^4}{q^4} = \sigma$$

blocks through S', and clearly equality holds iff these blocks partition V'.

Step 7. Let ℓ be a line, p a point not on ℓ, and assume $\varrho(p,\ell) \geq \varrho$. Then $S := S(p,\ell)$ is a projective plane of order q, and one actually has $\varrho(p,\ell) = \varrho$. Moreover, there are exactly τ subspaces S' of cardinality q^3+q^2+q+1 containing S, each of which lies in precisely σ blocks, and the blocks containing a given S' give rise to a partition of the set of points of Σ not contained in S'.

By Step 4, S is a projective plane of order q. Let us write $\varrho(p,\ell) = \varrho+\epsilon$, where $\epsilon \geq 0$, and let us denote the cardinality of the set X of all points $p' \notin S$ which are on at most one block B containing S by x. We now count the number f of all flags (p',B) with $p' \notin S \subset B$ in two ways. As each block B through S contains exactly q^4+q^3 points $p' \notin S$, we get

$$(1)\quad f = (\varrho+\epsilon)(q^4+q^3) = (q^{n-3}+\ldots+q+1)(q^{n-4}+\ldots+q+1)q^3+\epsilon(q^4+q^3).$$

On the other hand, counting via the points $p' \notin S$ first, we also obtain

$$(2)\qquad f \leq x+(q^n+\ldots+q^4+q^3-x)\sigma,$$

as each point in X is on at most one block B containing S, whereas each of the $q^n+\ldots+q^4+q^3-x$ points $p' \notin S \cup X$ determines a subspace $S' = S'(p')$ of cardinality q^3+q^2+q+1 by Step 5, which is then on at most σ blocks B through S by Step 6. Therefore

$$(q^{n-4}+\ldots+q+1)((q^n+\ldots+q^4+q^3)-(q^n+\ldots+q^4+q^3-x)) \leq x-\epsilon(q^4+q^3) \leq x,$$

forcing $x = \epsilon = 0$. Thus indeed $\varrho(p,\ell) = \varrho$, and we have also proved that each point $p' \notin S$ is on at least two blocks B through S. Now Step 5 shows that there are exactly τ subspaces of cardinality q^3+q^2+q+1 containing S, and that these subspaces give rise to a partition of the set of all points $p' \notin S$. As $\epsilon = 0$, equation (1) above becomes

$$f = (q^n+\ldots+q^4+q^3)\sigma,$$

and therefore (using $x = 0$) the inequality (2) has to hold with equality, which is only possible if each of the subspaces $S' = S'(p')$ of cardinality $q^3 + q^2 + q + 1$ determined by the points not in S is actually on exactly σ blocks B containing S. Now the final assertion follows from Step 6.

Step 8. Let Σ denote the linear space induced by the lines of $\mathcal{D}'$. Then the subspace spanned by any three non-collinear points of $\mathcal{D}'$ is a projective plane of order q. Moreover, any four non-planar points determine a subspace of cardinality $q^3 + q^2 + q + 1$.

By Step 3, the average number of blocks containing three non-collinear points is ϱ. By Step 7, this is also an upper bound for the number of blocks containing any three given non-collinear points, and hence any three such points always lie in exactly ϱ common blocks. Hence the conclusions of Step 7 hold for any three non-collinear points, and then an appeal to Step 5 establishes also the second assertion.

Step 9. The linear space Σ is isomorphic to $PG_1(n, q)$.

Using the first assertion of Step 8, one easily checks that the points and lines of $\mathcal{D}'$ satisfy the Veblen-Young axioms and therefore define a projective space Π; see, for instance, [1, Section XII.1]. In view of the parameters of $\mathcal{D}'$, we have $\Sigma \cong PG_1(n, q)$.

Step 10. $\mathcal{D}'$ is isomorphic to $PG_4(n, q)$.

It still remains to show that the blocks of $\mathcal{D}'$ are actually the 4-subspaces of Π. Again, we first note that the subspaces of cardinality $q^2 + q + 1$ of Σ are simply the planes of Π; this follows as in the proof of Theorem 2.2.

By Step 8, any given plane S together with any point $p' \notin S$ determines a unique subspace S' of cardinality $q^3 + q^2 + q + 1$, which has to be the union of the $q^2 + q + 1$ lines $p's$ where s runs over the points of S. But this is also the point set of the 3-subspace of Π determined by S and p'. Therefore the subspaces of cardinality $q^3 + q^2 + q + 1$ of Σ are precisely the 3-spaces of Π.

Finally, by Steps 6 and 7, the blocks containing any given 3-subspace S' partition the points not in S'. Hence S' and any such point p'' determine a unique block of $\mathcal{D}'$, namely the union of the $q^3 + q^2 + q + 1$ lines $s'p''$ where s' runs over the points of S'. But this is also the point set of the 4-subspace of Π determined by S' and p''. □

4 – Conclusion

We have seen that the correct line size $q + 1$ characterizes any design with the parameters of $PG_d(n, q)$ as this classical geometric design, provided that $d \in \{2, 3, 4, n-1\}$. These results provide considerable evidence for the validity of

Conjecture 1.1 . The key step in our proofs was establishing that any three non-collinear points always determine a projective plane of order q, or, in other words, that the given design is smooth (which was a hypothesis in the characterization result of Lefèvre-Percsy [10]). Unfortunately, this key step becomes more and more involved as the dimension d grows, the reason being that the number of a priori possibilities for the subspace spanned by a line ℓ and a point p not in this line grows with d. For the first open case, namely $d = 5$, we would for the first time have to consider the possibility that $S(p, \ell)$ is neither a projective plane of order q, nor a proper maximal subspace of a block B, nor B itself, but some proper, non-maximal subspace of Σ_B. This suggests that even this case will be a lot more complex than the case $d = 4$, which was already rather involved. Thus, settling Conjecture 1.1 in general seems a challenging problem which will most likely require some additional ideas.

REFERENCES

[1] T. Beth – D. Jungnickel – H. Lenz: *Design Theory (2nd edition)*, Cambridge University Press (1999).

[2] P. Dembowski – A. Wagner: *Some characterizations of finite projective spaces*, Arch. Math., **11** (1960) pp. 465–469.

[3] J. W. P. Hirschfeld: *Projective Geometries over Finite Fields (2nd edition)*, Oxford University Press (1998).

[4] J. W. P. Hirschfeld: *Finite Projective Spaces of Three Dimensions*, Oxford University Press (1985).

[5] D. Jungnickel: *The number of designs with classical parameters grows exponentially*, Geom. Dedicata, **16** (1984) pp. 167–178.

[6] D. Jungnickel – V. D. Tonchev: *The Number of Designs with Geometric Parameters Grows Exponentially*, Des. Codes Cryptogr., to appear.

[7] W. M. Kantor: *Automorphisms and isomorphisms of symmetric and affine designs*, J. Algebraic Combin., **3** (1994) pp. 307–338.

[8] C. Lam – S. Lam – V. D. Tonchev: *Bounds on the number of affine, symmetric, and Hadamard designs and matrices*, J. Combin. Theory Ser. A, **92** (2000) pp. 186–196.

[9] C. Lam – V. D. Tonchev: *A new bound on the number of designs with classical affine parameters.*, Des. Codes Cryptogr., **27** (2002) pp. 111–117.

[10] C. Lefèvre-Percsy: *Characterizations of designs constructed from affine and projective spaces.*, European J. Comb., **1** (1980) pp. 347–352.

Lavoro pervenuto alla redazione il 10 marzo 2010
ed accettato per la pubblicazione il 15 marzo 2010.
Bozze licenziate il 20 aprile 2010

Indirizzo dell'Autore:

Dieter Jungnickel – Lehrstuhl für Diskrete Mathematik, Optimierung und Operations Research – Universität Augsburg – D–86135 Augsburg – Germany
E-mail: jungnickel@math.uni-augsburg.de

Rendiconti di Matematica, Serie VII
Volume 30, Roma (2010), 121-144

Combinatorial methods for determining subgroup structures of finite groups

CAFER CALISKAN – S. S. MAGLIVERAS –L. C. YU

Dedicated to Prof. Marialuisa J. de Resmini

ABSTRACT: *In this paper we discuss methods that might be employed in determining the subgroup structure of a finite group G. These methods have a particularly combinatorial flavor connected with graphs, designs and the combinatorial nature of presentations of groups. In particular, the methods are illustrated for the case of the simple group $U_3(5) = PSU_3(5^2)$ whose maximal subgroups are determined up to conjugacy.*

1 – Introduction

This paper is devoted to a discussion of some methods that might be employed in determining the subgroup structure of a finite group G. The methods have a strong combinatorial flavor and are illustrated here for the case of the simple group $U_3(5) = PSU_3(5^2)$ whose maximal subgroups are determined up to conjugacy. This example possesses a measure of difficulty suitable for exemplifying these methods. The reader is assumed to be acquainted with the elements of the theory of finite groups, including finite permutation groups as for example discussed in [8], [12], [19], [20], [22]. He is also assumed to have knowledge of the rudiments of the theory of strongly regular graphs and association schemes as

KEY WORDS AND PHRASES: *Finite groups – Subgroup structure – Combinatorial methods*
A.M.S. CLASSIFICATION: 20E32, 20E28, 05E30.

discussed in [2], [3], [9], [10], [11]. Finally, the reader should have some knowledge of the beautiful Frobenius theory of ordinary characters [6], [7], [13], [16].

2 – The controlling viewpoint

The question of whether a list of subgroups is complete for a given group G can most effectively be dealt with if anticipated. Since the minimal normal subgroups of a group are characteristically simple, every subgroup M of a finite group G normalizes some subgroup of the form $A^r = A\times A\times\cdots\times A$ with A simple. This suggests that a systematic approach to determining the subgroups structure of G could consist of determining, up to conjugacy, all characteristically simple subgroups of G and subsequently determining their normalizers. The above observation allows us to "control" the process of determining the subgroups of G, and affords a way of verifying completeness.

We usually advance with the above procedure in two stages: First, we obtain the class Λ of *local* subgroups of G, *i.e.* the normalizers of the elementary abelian subgroups of G. Subsequently, we determine the class Ξ of normalizers of the non-soluble characteristically simple groups in G. The maximal subgroups of G must clearly occur in $\Xi\cup\Lambda$. Of course, we often have that $\Xi\cap\Lambda\neq\emptyset$.

3 – Matrices belonging to subgroups

Let G be a finite group acting transitively on a set Ω, and let Γ be the graph induced on Ω by a non-trivial, self-paired orbital of G on $\Omega\times\Omega$ [9], [21], [22]. Since the orbital is self-paired and non-trivial the graph is undirected and irreflexive. If $x\in\Omega$ and r is a non-negative integer, the *circle of radius* r about x is defined to be the set

$$S_r(x)=\{y\in\Omega\ :\ d(x,y)=r\}$$

where d is the usual distance function in the graph Γ.

If $\{\Delta_1,\dots,\Delta_\ell\}$ is a partition of Ω we denote by $[\Delta_1,\Delta_2,\dots,\Delta_\ell]$ the collection of all subgroups of G fixing each of the Δ_i setwise. Furthermore, if $k_1,\dots,k_\ell$ are positive integers such that

$$\sum_{i=1}^{\ell}k_i=|\Omega|,$$

we denote by $[k_1,k_2,\dots,k_\ell]$ the collection of all subgroups of G which have orbits of lengths $k_1,k_2,\dots,k_\ell$.

If $H\leq G$, and H has orbits $\Delta_1,\dots,\Delta_\ell$ on Ω, for $x\in\Delta_i$ we put $a_H(i,j)=|S_1(x)\cap\Delta_j|$. We call the matrix $A_H=(a_H(i,j))$ *the matrix belonging to the subgroup* H.

Let $M = (m_{i,j})$ be an $n \times n$ matrix with non-negative integral entries and constant row sums. The *domain* of M, $\mathcal{D}(M)$ is defined to be the collection of all partitions $P = \{\Delta_i\}_{i=1}^{k}$ of $\Omega = \{1, 2, \ldots, n\}$ for which $x, y \in \Delta_i$ implies that

$$\sum_{q \in \Delta_j} m_{x,q} = \sum_{q \in \Delta_j} m_{y,q} = \overline{m_{i,j}}$$

for each pair of indices i, j, $1 \leq i, j \leq k$. We set $M(P) = \overline{(m_{i,j})}$.

If $N = M(P)$ for some $P \in \mathcal{D}(M)$ we say that N *covers* M and write $M \leq N$. We note that if $M \leq N$ then N is a $k \times k$ matrix with non-negative entries, constant row sums, and $k \leq n$. We write $\int M$ for the collection of all covers of M and call $\int M$ *the cover* of M. We omit the proof of the following easy consequence:

PROPOSITION 3.1. *If H, K are subgroups of G and $H \leq K$, then $A_H \leq A_K$.*

Thus, the mapping $H \to A_H$ is an isotone function from the lattice of subgroups of G to the partially ordered set of all covers of the adjacency matrix of Γ.

The connection of the above concept with the concepts developed by D.G. Higman [10], [11], and also by Kramer and Mesner [14], [15], is apparent. The authors wish to emphasize the utility of the concept in investigations involving the determination of subgroup structures. We give below a hint of the way in which the matrices A_H are used and use the method more extensively in the $U_3(5)$ example.

When the adjacency matrix A of the graph Γ is given, one can calculate $\int A$. If H is any subgroup of G which is intransitive on Ω, then it corresponds to a cover of A. In particular, the covers determine which partitions of Ω are stabilized by intransitive subgroups of G. To obtain a focusing effect, and ignore duplication due to conjugacy, we may select a certain cyclic subgroup H of G, determine its matrix A_H and calculate $\int A_H$. This process is especially useful when we are seeking the non-soluble simple subgroups of G which contain H or a partial normalizer of H. Usually, only very few such covers exist, and these point to partitions whose stabilizers are the desired simple subgroups. If one knows the number of orbits of a sought subgroup, or even better, the vector of orbit lengths, the number of partitions of the given type corresponding to covers of A_H is even smaller. Sometimes, other small subgroups can be used in place of cyclic groups. For example, minimal simple groups which are known to be contained in G and whose orbit structure on Ω as well as corresponding matrices are easy to obtain.

The method can be used to determine whether some intransitive subgroup H of known matrix A_H is contained in any intransitive subgroup K, thus contributing to questions of maximality of a given subgroup.

The method is, of course, useful for the study of intransitive subgroups of G, however, its effectiveness is limited to relatively small $|\Omega|$. Transitive subgroups can be handled if one considers simultaneously several transitive permutation representations of G.

4 – Two-generator subgroups

Interest in two-generator subgroups becomes justified in view of the fact that there is evidence to support a conjecture that every finite non-abelian simple group is a 2-generator group. Even if the conjecture is false, all known simple groups except possibly for a few sporadic ones, are known to be 2-generator groups. For example, all $PSL_2(q)$ can be generated by two elements, one of which is an involution [1]. If $q \neq 9$, furthermore, $PSL_2(q)$ can be generated by two elements, one of order 2 and one of order 3. It is convenient to use the following notation: the conjugacy classes of G are denoted by $K_1 = \{1\}$, $K_2, \dots, K_c$.

If x is an element of G then $C(x) = C_G(x)$ denotes the centralizer of x in G. Furthermore σ_x denotes the order of $C(x)$. If $G|\Omega$ is a group action, the *meta-rank*, $\rho(G|\Omega)$, is defined to be the number of G-orbits on Ω. We write:

$$(4.1) \quad [K_i \times K_j \to K_k] \;=\; \{(a,b) \in K_i \times K_j \mid ab \in K_k\}, i,j,k \in \{1,\dots,c\}$$

We denote $|\,[K_i \times K_j \to K_k]\,|$ by $|K_i \times K_j \to K_k|$.

$$(4.2) \qquad \langle K_i \times K_j \to K_k \rangle \;=\; \{\langle a,b\rangle \mid (a,b) \in [K_i \times K_j \to K_k]\,\}$$

Here, $\langle a,b\rangle$ denotes the subgroup of G generated by a and b.

$$(4.3) \qquad \sigma_i \;=\; |C_G(x)|, \quad x \in K_i\,;$$

For $x_1, x_2, \dots, x_\ell \in G$,

$$(4.4) \qquad \sigma_{x_1,\dots,x_\ell} \;=\; |\bigcap_{i=1}^{\ell} C_G(x_i)| = |C_G\langle x_1,\dots,x_\ell\rangle|$$

The structure constants of the center of the group algebra are denoted by $a_{i,j,k}$; thus,

$$(4.5) \qquad K_iK_j \;=\; \sum_{k=1}^{c} a_{i,j,k}K_k \quad i,j \in \{1,\dots,c\}\,;\ \text{also,}$$

$$(4.6) \qquad a_{i,j,k} \;=\; \frac{|G|}{\sigma_i\sigma_j} \sum_{t=1}^{c} \frac{\chi_t(i)\chi_t(j)\overline{\chi_t(k)}}{\chi_t(1)}$$

where $\chi_t(i)$ is the value of the irreducible ordinary character χ_t of G on the elements of the class K_i.

We also introduce the symmetric rational constants:

$$\beta_{i,j,k} \;=\; \frac{a_{i,j,k}}{\sigma_k}\,, \quad i,j,k \in \{1,\ldots,c\}. \tag{4.7}$$

Consider the action of G on $K_i \times K_j$ by conjugation and define the mapping

$$\begin{aligned} \phi :\; & K_i \times K_j \to G \\ \phi : (x,y) \quad & \mapsto xy\,, \end{aligned}$$

then, $(x',y') \in (x,y)^G$ implies that $\phi(x',y')$ is conjugate to $\phi(x,y)$ in G. Furthermore, if z is G-conjugate to $xy \in K_i \times K_j$, then there exists $(x',y') \in (x,y)^G$ such that $\phi(x',y') = z$. Hence, ϕ is a surjection onto a union of classes of G and $[K_i \times K_j \to K_k]$ is a union of G-orbits of $K_i \times K_j$. We have that:

$$|(x,y)^G| \;=\; [G : C(x) \cap C(y)] = \frac{|G|}{\sigma_{x,y}},$$

furthermore,

$$|(x,y)^G \cap \phi^{-1}(xy)| \;=\; [C(xy) \;:\; C(x) \cap C(y)] \;=\; \frac{\sigma_{xy}}{\sigma_{x,y}}\,, \tag{4.8}$$

an invariant of the orbit $(x,y)^G$. Given a fixed element $z \in K_k$, $a_{i,j,k} \;=\; |\phi^{-1}(z)|$. If the G-orbits $\Omega_1, \Omega_2, \ldots, \Omega_m$ of $K_i \times K_j$ and no others are carried by ϕ into K_k, choose $(x_i, y_i) \in \Omega_i$ such that $\phi(x_i, y_i) \;=\; x_i y_i \;=\; z$, we get:

$$a_{i,j,k} = \sum_{i=1}^{m} |\Omega_i \cap \phi^{-1}(z)| = \sum_{i=1}^{m} \sigma_z / \sigma_{x_i,y_i}$$

hence,

$$\beta_{i,j,k} = \sum_{i=1}^{m} \frac{1}{\sigma_{x_i,y_i}}. \tag{4.9}$$

Since $\sigma_{x_i,y_i} = \sigma_{x_i,y_i,x_iy_i}$, we obtain:

$$\sigma_{x_i,y_i} | gcd(\sigma_i, \sigma_j, \sigma_{x_iy_i}) \tag{4.10}$$

If the induced characters $\theta_i = 1_{C(x)} \uparrow^G$, $\theta_j = 1_{C(y)} \uparrow^G$, $(x,y) \in K_i \times K_j$ are known, then

$$\rho(G|\, K_i \times K_j\,) = (\theta_i, \theta_j), \tag{4.11}$$

and conditions (4.9), (4.10) and (4.11) are usually sufficient to determine the number of orbits of G on $[K_i \times K_j \to K_k]$ for each $k \in \{1, \dots, c\}$.

Now, if $(x', y') = (x, y)^g$, then $\langle x', y' \rangle = \langle x, y \rangle^g$. Hence, if we are interested in $\{\langle x, y \rangle \mid (x, y) \in K_i \times K_j\}$ up to conjugacy, it suffices to consider one pair from each G-orbit of $K_i \times K_j$. We must, however, observe that it is possible for (x, y), (x', y') to belong to different G-orbits yet $\langle x, y \rangle$ to be G-conjugate to $\langle x', y' \rangle$. Thus,

$$\rho(G|\,\langle K_i \times K_j \to K_k \rangle\,) \leq \rho(G|\,[K_i \times K_j \to K_k]\,)\,. \tag{4.12}$$

To determine what orbit fusion is induced when we pass from the group action $G|\,[K_i \times K_j \to K_k]$ to the group action $G|\,\langle K_i \times K_j \to K_k \rangle$, in addition to standard group action conditions we use a certain combinatorial technique which roughly speaking, involves counting the number of ways in which a fixed two-generator subgroup is generated by pairs of elements of $K_i \times K_j$. More specifically, we introduce mappings of the sort

$$\begin{aligned} f &: [K_i \times K_j \to K_k] \to \langle K_i \times K_j \to K_k \rangle \\ f &: (x, y) \to \langle x, y \rangle \end{aligned}$$

and determine the uniform sizes of preimages $f^{-1}(\langle x, y \rangle)$. The $U_3(5)$ example involves several applications of the above ideas.

5 – Compound Characters

Let G be a finite group whose irreducible ordinary characters are $1_G, \chi_2, \chi_3, \dots, \chi_c$. If $x \in G$, $H \leq G$, then we write $g_x = |[x]|$, and $h_x = |[x] \cap H|$, where $[x] = x^G$ is the G-conjugacy class containing x.

If θ and ψ are two ordinary characters of G, we denote by (θ, ψ) their inner product in the algebra of class functions of G. If ϕ is an ordinary character of G, then $\phi = \sum_{i=1}^{c} a_i \chi_i$, with $a_i \in \mathbb{Z}^+ = \{0, 1, 2, \dots\}$. Since the collection $\{\chi_i\}_{i=1}^{c}$ forms an orthonormal basis for the algebra of class functions of G, we have that $a_i = (\phi, \chi_i)$.

If $H \leq G$, then the character θ of the transitive permutation representation

$$\begin{aligned} \pi : G &\to \mathcal{S}_m \; m = [G \;:\; H] \\ g &\to \pi(g) = \begin{pmatrix} Hx \\ Hxg \end{pmatrix} \end{aligned}$$

is the induced character $1_H \uparrow^G$ of the principle character of H to G [7], [16].

It is immediate that the following necessary conditions are satisfied by θ :

(i) $(\theta, 1_G) = 1$

(ii) $\theta(x) \in \mathbb{Z}^+$, for each $x \in G$

(iii) $(\theta, \chi_i) \leq \chi_i(1) \ = \ n_i$

(iv) $\theta(x^k) \geq \theta(x)$, for $x \in G$, $k \in \mathbb{Z}^+$

(v) $\theta(1) = [G \ : \ H]$, hence $\theta(1)$ divides $|G|$

(vi) $\theta(x) = \theta(1) \cdot (h_x/g_x)$ and therefore $\theta(1)$ divides $\theta(x) \cdot g_x$.

(vii) $(\theta, \chi_i) \ = \ (\theta, \overline{\chi_i})$, where $\overline{\chi_i}$ is the complex conjugate character of χ_i.

By a *compound character* of G we mean here any character of G satisfying conditions (i) to (vii). Thus, the character of every transitive permutation representation of G is a compound character but there may exist compound characters which are not the characters of any transitive permutation representation of G and therefore which correspond to no subgroup H of G.

In investigating the subgroup structure of a group G whose character table is known the following question arises: "*Are there any subgroups of G of index δ?* " More generally, if it is known that G possesses a subgroup H with associated compound character θ, what are the compound characters ϕ corresponding to subgroups K of G subject to $H \leq K \leq G$? If such an intermediate subgroup exists, then

$$\theta = 1_H \uparrow^G = 1_H \uparrow^K \uparrow^G, \quad \text{and } (1_H \uparrow^K, 1_K) = 1$$

imply that:

$$\text{(viii)} \qquad (\theta, \chi_i) \geq (\phi, \chi_i), \ i \in \{1, \ldots, c\}.$$

i.e. the multiplicities of the irreducible characters of G in θ are greater than or equal to those in ϕ. Thus, there is an order inverting homomorphism from the lattice of subgroups of G into the cone $(\mathbb{Z}^+)^c$, each subgroup mapping onto a vector of multiplicities $\overline{a} = (a_1, \ldots, a_c)$ of the associated compound character. The authors, and undoubtedly others, have algorithms which answer the above question by investigating all partitions of δ :

$$\delta = 1 + \sum a_i \chi_i(1) \quad \text{for each } \delta \mid |H|, \ |H| \mid \delta,$$

and testing that the corresponding character

$$\theta = [1] + \sum a_i \chi_i$$

satisfies (i) to (viii). Such programs can be made quite efficient if the algorithms incorporate knowledge of special numerical conditions in the given character table.

6 – The Maximal Subgroups of $U_3(5)$

In this section we illustrate the methods discussed on the simple group $U_3(5)$. We obtain the following result :

THEOREM 6.1. *There are eight conjugacy classes of maximal subgroups of $U_3(5)$ as follows : a) Local: $C_G(z) \cong \langle z \rangle \setminus \mathcal{S}_5$, z is an involution in G; for $Q \in Syl_5(G)$, $N_G(Q) = N_G\langle 5_1 \rangle \cong Q \setminus \mathbb{Z}_8$. b) Non-local : Three conjugacy classes of self normalizing A_7's ; Three conjugacy classes of M_{10}'s each normalizing a subgroup of G isomorphic to A_6. The classes of A_7's and the classes of M_{10}'s are distinguished by the G-class of elements of order five they contain.*

LOCAL ANALYSIS

6.1 – Local 2-Subgroups

There is one conjugacy class of involutions in G, and the Sylow-2 subgroup of G is quasidihedral. Thus, the only possible elementary abelian 2-groups of order greater than 2 that can occur in G are Klein four groups $V_4 \cong C_2 \times C_2$.

LEMMA 6.1. *There is exactly one conjugacy class of V_4's in G.*

PROOF. $a_{2,2,2} \neq 0$ implies that there exist V_4's in G. $|C_G(z)| = 240$, $[G : C_G(z)] = 525$, and from the fusion map $C_G(z) \to G$ we compute the character of the action $G|K_2$ as

$$\theta_{525} = 1_{C(z)} \uparrow^G = [1] + [28]_1 + [28]_2 + [28]_3 + [84] + [105] + [125] + [126].$$

Hence, $\rho(G|K_2 \times K_2) = (\theta_{525}, \theta_{525}) = 8$. Computation of the $a_{2,2,k}$ (See Table 1) shows that the 8 orbits of $G|K_2 \times K_2$ are already differentiated by the class in which k lies. *i.e.* There are precisely 8 $a_{2,2,k} \neq 0$ for k lying in 8 distinct conjugacy classes, and consequently the orbits are $[K_2 \times K_2 \to K_j]$ for those j for which $a_{2,2,j} \neq 0$. Thus $[K_2 \times K_2 \to K_2]$ is a G-orbit, and there exists one conjugacy class of V_4's. ∎

TABLE 1

k	:	1	2	4	8_1	8_2	3	6	5_1	5_2	5_3	5_4	10	7_+	7_-
$a_{2,2,k}$	:	525	20	4	0	0	18	6	0	5	5	5	0	0	0
$\langle 2,2,k\rangle$	:	$\langle z\rangle$	V_4	D_4	-	-	$\mathcal{S}_3$	D_6	-	D_{5_2}	D_{5_3}	D_{5_4}	-	-	-
$\lvert\langle 2,2,k\rangle\rvert$	:	2	4	8	-	-	6	12	-	10	10	10	-	-	-

Let z be an involution of G. It is easy to verify that $C_G(z)$ acts primitively on fix(z) with kernel $\langle z\rangle$. Thus $C_G(z) \cong \langle z\rangle \setminus \mathcal{S}_5$.

PROPOSITION 6.1. *$C_G(z)$, $|z| = 2$, is maximal in G.*

PROOF. From the proof of Lemma 6.1

$$\theta_{525} = 1_{C(z)} \uparrow^G = [1] + [28]_1 + [28]_2 + [28]_3 + [84] + [105] + [125] + [126].$$

Suppose $C(z)$ is not maximal, then there exists $H \leq G$ such that $C(z) \lneq H \lneq G$ and $[G : H] \mid 3 \cdot 5^2 \cdot 7$. By considering compound characters of degrees $\delta \mid 3 \cdot 5^2 \cdot 7$, we rule out all but one case, namely the case $[G : H] = 175$. In this case H would be a group of order $720 = 2^4 \cdot 3^2 \cdot 5$, $[G : H] = 175$, and $\theta_{175} = 1_H \uparrow^G = [1] + [125] + [21] + [28]_i$ for $i \in \{1, 2, 3\}$. We note that character [21] does not appear in $1_{C(z)} \uparrow^G$, a contradiction to 5.(viii). Hence $C(z)$ is maximal. □

6.1.1 – $C_G(V_4)$, $N_G(V_4)$

$a_{2,2,2} = 20$ implies that $\beta_{2,2,2} = 20/240 = 1/12$; but the number of orbits of G on $[K_2 \times K_2 \to K_2]$ is 1. Therefore $\beta_{2,2,2} = \frac{1}{|C(V_4)|} \Rightarrow |C(V_4)| = 12$. $N(V_4)/C(V_4) \lesssim AutV_4 \cong GL_2(2) \cong \mathcal{S}_3 \Rightarrow |N(V_4)|$ divides $6 \cdot 12 = 72$. Consider an A_7 inside G, and represent A_7 in its canonical representation. Let $V_4 = [1, (12)(34), (13)(24), (14)(23)] \leq A_7$, then $C_{A_7}(V_4) = V_4 \times \langle\sigma\rangle$ where $\sigma = (567)$. Therefore $C_G(V_4) = C_{A_7}(V_4) \cong V_4 \times \mathbb{Z}_3$. The elements $\rho = (23)(56)$, $z = (234)$ normalize V_4 in A_7; thus $\langle V_4, \sigma, \rho, z\rangle \subseteq N_{A_7}(V_4) \subseteq N_G(V_4)$. But $|\langle V_4, \sigma, \rho, z\rangle| = 72$ implies that $|N_G(V_4)| = 72$ and $N_G(V_4) = N_{A_7}(V_4)$. Therefore, $N_G(V_4) \leq A_7$, *i.e.* $N_G(V_4)$ is not maximal. It follows from the above that the structure of $N(V_4)$ is $(V_4 \times \mathbb{Z}_3) \setminus \mathcal{S}_3$; in fact, since $\langle\rho, z\rangle \leq N(V_4)$, $\langle\rho, z\rangle \cong \mathcal{S}_3$ and $\langle\rho, z\rangle \cap \langle V_4, \sigma\rangle = 1$, the extension splits.

6.2 – Local 3-groups

Clearly, there is one conjugacy class of $\mathbb{Z}_3$'s and one class of $\mathbb{Z}_3 \times \mathbb{Z}_3$'s in G. We will now investigate the structures of $C_G(\mathbb{Z}_3)$, $N_G(\mathbb{Z}_3)$, $C_G(\mathbb{Z}_3 \times \mathbb{Z}_3)$, $N_G(\mathbb{Z}_3 \times \mathbb{Z}_3)$.

LEMMA 6.2. *Let $\sigma \in G$, $|\sigma| = 3$, then $C_G(\sigma) \cong \mathbb{Z}_3 \times A_4$.*

PROOF. Take $\sigma \in 3 \cdot 1^4$ in A_7, then $C_{A_7}(\sigma) = \mathbb{Z}_3 \times A_4 \leq A_7$, but $|C_G(\sigma)| = 36$, therefore $C_G(\sigma) \cong \mathbb{Z}_3 \times A_4$. □

REMARK 6.1 Since $C_G(\mathbb{Z}_3 \times \mathbb{Z}_3) \subseteq C_G(\mathbb{Z}_3) \cong \mathbb{Z}_3 \times A_4 \leq A_7$, neither of $C_G(\mathbb{Z}_3)$, $C_G((\mathbb{Z}_3 \times \mathbb{Z}_3))$ are maximal. Since there is exactly one conjugacy class of elts of order 3, $|N_G(\mathbb{Z}_3)| = 2|C_G(\mathbb{Z}_3)|$, hence $|N_G(\mathbb{Z}_3)| = 2^3 \cdot 3^2$ and $N_G(\mathbb{Z}_3) \cong C_G(\mathbb{Z}_3) \setminus \mathbb{Z}_2$.

LEMMA 6.3. *If $\sigma = (123)(4)(5)(6)(7) \in A_7 \leq G$, then $N_G\langle\sigma\rangle = N_{A_7}\langle\sigma\rangle$.*

PROOF. $C_{A_7}(\sigma) = \langle\sigma\rangle \times A_4$ with A_4 on $\{4, 5, 6, 7\}$; furthermore, $\nu = (23)(45)$ normalizes $\langle\sigma\rangle = \{1, \sigma, \sigma^2\}$. Hence, $\langle C_{A_7}(\sigma), \nu\rangle \subseteq N_{A_7}(\sigma)$, but $|\langle C_{A_7}(\sigma), \nu\rangle| = 72$; therefore, $N_G(\langle\sigma\rangle) = N_{A_7}(\langle\sigma\rangle) = \langle C_{A_7}(\sigma), \nu\rangle \leq A_7$. □

COROLLARY 6.1. *$N_G(\mathbb{Z}_3)$ is not maximal in G.*

LEMMA 6.4. *The Sylow-3 subgroups in G are self-centralizing in G.*

PROOF. $C_G(\mathbb{Z}_3 \times \mathbb{Z}_3) \subseteq C_G(\mathbb{Z}_3) = C_{A_7}(3 \cdot 1^4) \cong \mathbb{Z}_3 \times A_4$. It suffices to find $C_{C_3 \times A_4}(\mathbb{Z}_3 \times \mathbb{Z}_3)$. But easily, $C_{\mathbb{Z}_3 \times A_4}(\mathbb{Z}_3 \times \mathbb{Z}_3) = \mathbb{Z}_3 \times \mathbb{Z}_3$. □

In 6.9 we prove that there exists a subgroup S of G with $S \cong M_{10}$, M_{10} the Mathieu group on 10 letters. M_{10} is transitive on the 10 letters and the order of the stabilizer of a point, M_{10_x}, is 72. Let $H = M_{10_x}$; the values of the induced character $1_H \uparrow^{M_{10}}$ on the conjugacy classes yield that there will be exactly 8 elements of order 3 in H and 63 elements of 2-power orders 2^a. Therefore, if $T \in Syl_3(G)$, $|N_G(T)| \geq 72$. Now,

$$N_G(\mathbb{Z}_3 \times \mathbb{Z}_3)/C_G(\mathbb{Z}_3 \times \mathbb{Z}_3) \stackrel{\sim}{\leq} Aut(\mathbb{Z}_3 \times \mathbb{Z}_3)$$

implies that

$$|N_G(\mathbb{Z}_3 \times \mathbb{Z}_3)| \textit{ divides } 9 \cdot |GL_2(3)| = 3^3 \cdot 2^4.$$

Therefore, $|N| = 72$ or $2 \cdot 72$. But by Sylow's Theorem, $2 \cdot 72$ is ruled out. Hence, $|N| = 72$, and

$$N_G(\mathbb{Z}_3 \times \mathbb{Z}_3) = N_{M_{10}}(\mathbb{Z}_3 \times \mathbb{Z}_3) \leq M_{10}.$$

COROLLARY 6.2. *$N_G(\mathbb{Z}_3 \times \mathbb{Z}_3)$ is not maximal in G.*

6.3 – Local 5-groups

Since $Q \in Syl_5(G)$ is non-abelian of order 5^3 and contain no elements of order 25, Q must have the presentation:

$$Q = \langle \alpha, \beta, \gamma \mid \alpha^5 = \beta^5 = \gamma^5 = 1,\ \alpha^\gamma = \alpha,\ \beta^\gamma = \beta,\ [\alpha, \beta] = \gamma \rangle.$$

The elements of Q can be written in the form $\alpha^k \beta^l \gamma^m$; $k, l, m \in \mathbb{Z}_5$, and $\mathbb{Z}(Q) = \langle \gamma \rangle$. Since $\alpha^\beta = \alpha^4 \gamma$, $\beta^\alpha = \beta \gamma^4$, the conjugacy class in Q of a non-central element x is the coset $\langle \gamma \rangle x$. Thus Q contains 24 non-central classes each of size 5.

LEMMA 6.5. *The central element γ must belong to 5_1 and Q consists of exactly*

1. *the identity*
2. *4 elements of type 5_1*
3. *40 elements of each of types 5_2, 5_3, 5_4.*

PROOF. $Q \trianglelefteq N_G(Q)$, $\theta_{126} = 1_{N_G(Q)} \uparrow^G = [1] + [125]$ and $\theta_{126}(5_2) = \theta_{126}(5_3) = \theta_{126}(5_4)$, $|C_G(5_i)| = 25$, $i = 1, 2, 3, 4$ imply that Q contains exactly 40 elements of each 5_i, $i \in \{1, 2, 3, 4\}$. □

From the character table of G follows that $|C_G(\gamma)| = 2 \cdot 5^3$. But $\langle \gamma \rangle$ is a characteristic subgroup of Q which implies that $N_G(Q) \leq N_G(Y)$. Therefore $|N_G(Q)| \mid 4 \cdot |C_G(Y)| = 2^3 \cdot 5^3$. By Sylow's Theorem, it follows that $|N_G(Q)| = 2^3 \cdot 5^3$. By [18], $N_G(Q) \cong Q \setminus \mathbb{Z}_8$ and every element of order 5 is conjugate to its powers. Thus there are exactly four conjugacy classes of $\mathbb{Z}_5$'s in G, namely $\langle 5_1 \rangle$, $\langle 5_2 \rangle$, $\langle 5_3 \rangle$, $\langle 5_4 \rangle$.

The structure and maximality of $N\langle 5_1 \rangle$.

Since $|\sigma| = 5 \Rightarrow \sigma \sim \sigma^k$, $k = 1, 2, 3, 4$, we have that $|N\langle 5_i \rangle| = 4 \cdot |C\langle 5_i \rangle|$. Hence $|N\langle 5_1 \rangle| = 1000$; $|N\langle 5_i \rangle| = 100$ if $i \in \{2, 3, 4\}$. Hence, $N(Q) = N\langle 5_1 \rangle \cong Q \setminus \mathbb{Z}_8$.

PROPOSITION 6.2. *$N\langle 5_1 \rangle$ is maximal in G.*

PROOF. $[G : N\langle 5_1 \rangle] = \frac{126000}{1000} = 126$. The character of the transitive permutation representation of G on the right cosets of $N_G\langle 5_1 \rangle$ is $\theta_{126} = 1_{N\langle 5_1 \rangle} \uparrow^G = [1] + [125]$; therefore, the representation is doubly-transitive, hence it is primitive and consequently, the stabilizer of a point, namely $N\langle 5_1 \rangle$ is maximal. □

LEMMA 6.6. *$i \in \{2,3,4\} \Rightarrow \langle 5_1, 5_i\rangle$ contains exactly*

1. *the identity*
2. *4 elements of type 5_1*
3. *20 elements from class 5_i.*

PROOF. Let $\gamma \in 5_1$ and $\sigma \in 5_i$, $i \neq 1$, such that $\sigma^\gamma = \sigma$. Also let $Q \in Syl_5(G)$ such that $\langle \gamma, \sigma\rangle \leq Q$. Then $y \in \langle\gamma\rangle x \Rightarrow y$ is Q-conjugate to $x \Rightarrow y$ is G-conjugate to x. But also, $x \sim x^k$ for any $k \not\equiv 0$ (*mod* 5). □

PROPOSITION 6.3. *$N\langle 5_i\rangle \leq \langle 5_1\rangle$ if $i \in \{1,2,3,4\}$. Consequently, for $i \neq 1$ $N\langle 5_i\rangle$ are not maximal.*

PROOF. Obvious for $i = 1$. Consider now the case where $i > 1$. If $\sigma \in N\langle 5_i\rangle$, then σ normalizes $C(5_i) = \langle 5_1, 5_i\rangle$. Let $\gamma \in 5_1 \cap C(5_i)$, then by Lemma 6.6 $\gamma^\sigma \in \langle\gamma\rangle \Rightarrow \langle\gamma\rangle^\sigma = \langle\sigma\rangle$, *i.e.* σ normalizes $\langle 5_1\rangle$. Therefore $N\langle 5_i\rangle \leq N\langle 5_1\rangle$. □

COROLLARY 6.3. *$N\langle 5_1, 5_i\rangle \leq N\langle 5_1\rangle$, $i \neq 1$.*

PROOF. Let $\sigma \in N\langle 5_1, 5_i\rangle$ and let $\sigma \in 5_1 \cap \langle 5_1, 5_i\rangle$, then $\gamma^\sigma \in 5_1 \cap \langle 5_1, 5_i\rangle$, therefore by Lemma 6.6, $\langle\gamma\rangle^\sigma = \langle\gamma\rangle$. □

Thus, we have the following :

PROPOSITION 6.4. *There is exactly one up to conjugacy 5-local maximal subgroup of G; it is $N\langle 5_1\rangle = N(Q)$ of order 1000.*

6.4 – Local 7-groups

It is immediate that $N_G(\mathbb{Z}_7) \cong \mathbb{Z}_7^3$. Furthermore, since $N_{A_7}(\mathbb{Z}_7) \cong \mathbb{Z}_7^3$, we have that $N_G(\mathbb{Z}_7) \leq A_7$ and consequently $N_G(\mathbb{Z}_7)$ is not maximal.

6.5 – Non-local Subgroups

PROPOSITION 6.5. *If $H \leq G$, H non-abelian simple group, then H is isomorphic to one of the following: A_5, $PSL_2(7)$, A_6, A_7.*

PROOF. No simple groups not occurring in L.E.Dickson's list are found in the Higman-Sims group [18]. Hence, since $G \leq HS$, the only possible simple groups contained in G must occur in Dickson's list. By consideration of order, the possible non-abelian simple groups are: A_5, A_6, A_7, $PSL_2(7)$, $PSL_2(8)$. However $PSL_2(8) \not\leq HS$, therefore, $PSL_2(8) \not\leq G$. □

REMARK 6.2. Each of above indeed occurs in G. To see this we note that $A_7 \overset{\sim}{\leq} G$ and therefore A_6, A_5, $PSL_2(7)$ which are contained in A_7 are subgroups of G. There remains to determine the number of conjugacy classes of each of the above, and their normalizers.

6.6 – The set $[K_2 \times K_3 \to K_7]$

From $|K_2 \times K_3| = \frac{|G|}{240} \cdot \frac{|G|}{36} = 2^2 \cdot 3 \cdot 5^5 \cdot 7^2$, $|K_2 \times K_3 \to K_{7_+}| = a_{2,3,7_+} \cdot \frac{|G|}{7} = 3 \cdot |G|$, $|K_2 \times K_3 \to K_{7_-}| = 3 \cdot |G|$, $a_{2,3,7_+}|_{L_2(7)} = 7$, $|K_2 \times K_3 \to K_{7_+}|_{L_2(7)}| = 168$, we have:

$$\#L_2(7)'s = \frac{|K_2 \times K_3 \to K_7|}{2 \cdot 168} = 2250.$$

Let Ω be the set of all $L_2(7)$'s in G and consider the group action $G|\Omega$ by conjugation. The length of an orbit, say L^G, $L \in \Omega$, is $|L^G| = [G : G_L]$ where $G_L = N_G(L)$. Hence, if there are k orbits with representatives L_i, $i = 1, 2, \ldots, k$, we have

$$\sum_{i=1}^{k} [G : G_{L_i}] = 2 \cdot 3^2 \cdot 5^3.$$

Therefore, $2^4 \cdot 3^2 \cdot 5^3 \cdot 7 \cdot \sum_{i=1}^{k} \frac{1}{|N_G(L_i)|} = 2 \cdot 3^2 \cdot 5^3 \Rightarrow 2^3 \cdot 7 \cdot \sum_{i=1}^{k} \frac{1}{|N(L_i)|} = 1$. Now since $L \in \Omega$ implies that $C_G(L) = 1$, if we write $|\frac{N(L_i)}{L_i}| = \ell_i$ we have:

$$\frac{1}{168} \sum_{i=1}^{k} \frac{1}{\ell_i} = \frac{1}{2^3 \cdot 7}.$$

Hence, in particular $\sum_{i=1}^{k} \frac{1}{\ell_i} = 3$ and $k \geq 3$. Consider the group action $G|[K_2 \times K_3 \to K_{7_+}]$ by conjugation. We have the following:

LEMMA 6.7. *The number of G orbits on $[K_2 \times K_3 \to K_{7_+}]$ is three.*

PROOF. Since $g.c.d(\sigma_2, \sigma_3, \sigma_7) = 1$, $\rho(G|[K_2 \times K_3 \to K_{7_+}]) = \beta_{2,3,7_+} = \frac{a_{2,3,7_+}}{7} = \frac{21}{7} = 3$. □

Every $\langle x, y\rangle$ such that $|x| = 2$, $|y| = 3$, $|xy| = 7$ can be thought of as a $(2, 3, 7_+)$; for either $xy \in 7_+$ in which case $(x, y) \in [K_2 \times K_3 \to K_{7_+}]$ or else $xy \in 7_-$ in which case $y^{-1}x^{-1} \in 7_+$ and $\langle x, y\rangle = \langle x^{-1}, y^{-1}\rangle \in (2, 3, 7_+)$.

If (x, y), $(x', y') \in [K_2 \times K_3 \to K_{7_+}]$ and (x, y) is G-conjugate to (x', y'), then clearly $\langle x, y\rangle$ is G-conjugate to (x', y'). Therefore, if $\Omega = \{H \leq G \mid H \cong L_2(7)\}$, then $\rho(G|\Omega) \leq \rho(G|[K_2 \times K_3 \to K_{7_+}]) = 3$.

COROLLARY 6.4. *$k = 3$, $\ell_i = 1$ for $i \in \{1, 2, 3\}$. i.e. each $PSL_2(7)$ in G is self-normalizing.*

6.7 – The conjugacy classes of A_5's in G

If $H \cong A_5$, then $H \in (2, 3, 4)$. Since $\beta_{2,3,5_1} = 0$, $\beta_{2,3,5_i} = 1$ for $i \in \{2, 3, 4\}$ and $gcd(\sigma_2, \sigma_3, \sigma_{5_i}) = 1$ for $i > 1$ it follows that there are exactly 3 conjugacy classes of A_5's in G one for each 5_i, $i > 1$. Consider $A_{5_i} = \langle x, y\rangle$, $(x, y) \in [K_2 \times K_3 \to K_{5_i}]$. $C(A_{5_i}) = C(x) \cap C(y) \cap C(xy) = 1$, implies that each A_5 is centralized by 1. $N(A_5)/C(A_5) \overset{\sim}{\leq} AutA_5 \cong \mathcal{S}_5$. Therefore, $|N(A_5)| \mid 5!$, hence $N(A_5) \cong A_5$ or $\mathcal{S}_5$.

Consider $[K_2 \times K_3 \to K_{5_i}]$ for a fixed $i \in \{2, 3, 4\}$. Then, $|K_2 \times K_3 \to K_{5_i}| = a_{2,3,5_i} \cdot \frac{|G|}{25} = |G|$. Consider the mapping $\Phi : [K_2 \times K_3 \to K_{5_i}] \to \Lambda_i$, $i \in \{2, 3, 4\}$, where Λ_i is the conjugacy class of A_5's of type $(2, 3, 5_i)$, defined by $\Phi(x, y) = \langle x, y\rangle$. Then $H \in \Lambda_i \Rightarrow |\Phi^{-1}(H)| = |K_2 \times K_3 \to K_5|_{|_{A_5}}$.
Hence, $|\Lambda_i| = \frac{2^4 \cdot 3^2 \cdot 5^3 \cdot 7}{3 \cdot 4 \cdot 2 \cdot 5} = 2 \cdot 3 \cdot 5^2 \cdot 7$.

On the other hand

$$|\Lambda_i| = [G : N_G(H)],\ H \in \Lambda_i.$$

Hence, $\frac{2^4 \cdot 3^2 \cdot 5^3 \cdot 7}{2^2 \cdot 3 \cdot 5} \sum_{i=1}^{3} \frac{1}{n_i} = 2 \cdot 3^2 \cdot 5^2 \cdot 7 = |\Lambda_2| + |\Lambda_3| + |\Lambda_4|$.

Hence, $\sum_{i=1}^{3} \frac{1}{n_i} = \frac{3}{2}$, and consequently, each $n_i = 2$. Thus, there is a unique up to conjugacy A_{5_i} for each $i \in \{2, 3, 4\}$ and each of these A_5's are contained in a corresponding $\mathcal{S}_5$. We will show later that none of the above $\mathcal{S}_5$'s is maximal in G.

6.8 – Groups containing $\mathbb{Z}_7^3$

It is well known that the full automorphism group of the Hoffman-Singleton graph on 50 verices is a split extension of our group $G = U_3(5)$ by a group of order 2 [17] [4]. In [17] the Higman-Sims graph of 100 vertices is viewed as the union of two Hoffman-Singleton graphs with appropriate interconnections between the two subgraphs on 50 vertices. In particular $U_3(5)$ acts intransitively

on the 100 vertices of the Higman-Sims graph, and transitively, of rank 3, on each of the two Hoffman-Singleton subgraphs of the Higman-Sims graph. In what follows we consider the transitive, rank-3 action of G on the 50 vertices Ω of the Hoffman-Singleton graph. In view of the discussion in Section 5, the character of the action $G|\Omega$ must be of the form $\chi = [1] + [21] + [28]_i$ for some $i \in \{1, 2, 3\}$.

Suppose a subgroup H of G contains $\mathbb{Z}_7^3$ then

$$A_H \geq A_{\mathbb{Z}_7^3} = \begin{pmatrix} 0 & 7 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 3 \\ 0 & 1 & 0 & 0 & 0 & 6 \\ 0 & 1 & 0 & 0 & 3 & 3 \\ 0 & 1 & 0 & 3 & 0 & 3 \\ 0 & 1 & 2 & 1 & 1 & 2 \end{pmatrix}$$

Suppose $H \leq G$, $[G : H] = 50$, then $1_H \uparrow^G = [1] + [21] + [28]_j$, $j \in \{1, 2, 3\} \Rightarrow$ $\#[\text{Orbits of } H \text{ on } \Omega] = (1_H \uparrow^G, \chi) = 3$ or 2.

LEMMA 6.8. *If $H \cong A_7$, $H \leq G$, then $H \in [1, 7, 42] \cup [15, 35]$.*

PROOF. $[G : H] = 50$. Via consideration of the possible compound characters of degree 50, we see as above that H has 2 or 3 orbits on the canonical set of 50 points. If there are 2 orbits then it easily follows that $A_7 \in [15, 35]$ by consideration of the possible transitive representations of A_7 on ≤ 50 points. Otherwise if A_7 has 3 orbits, the least orbit is of length $\leq [\frac{50}{3}] = 16$, hence of length $1, 7$ *or* 15. If the least orbit has length $= 1$ then $49 = k + \ell$, and A_7 acts transitively on k (as well as ℓ) points, therefore $k = 7$, $\ell = 42$. If the least orbit has length > 1 then by considering the possible transitive representations of A_7 we see that no assignment to k and ℓ is possible. Hence the least orbit must be of length 1. Clearly there is an $A_7 \in [1, 7, 42]$, since G_α in the canonical representation of G on 50 points is isomorphic to A_7. Since G is transitive on 50 points all A_7's with orbit structure $[1, 7, 42]$ are conjugate. □

Now we will show that there are two other conjugacy classes of A_7's in G, which in the standard representation $G|\Omega$ have orbit types $[15, 35]$.

LEMMA 6.9. *If*

$$\begin{aligned} \sigma = &(1)(2\ 11\ 6\ 5\ 26\ 16\ 21)(3\ 39\ 31\ 30\ 36\ 50\ 41) \\ &(4\ 29\ 32\ 33\ 17\ 46\ 9)(7\ 14\ 43\ 25\ 34\ 19\ 47) \\ &(8\ 20\ 28\ 40\ 24\ 27\ 13)(10\ 49\ 42\ 23\ 22\ 35\ 48) \\ &(12\ 44\ 37\ 15\ 45\ 18\ 38) \in G \end{aligned}$$

and cycles of σ are labelled $PABCDEFK$, then $\mathbb{Z}_7^3 = N_G\langle\sigma\rangle \in [P, A, CFK, B, E, D] : [1, 7, 21, 7, 7, 7]$, and any cover of $\mathbb{Z}_7^3$ with two orbits has orbit type $[PED, ABCFK]$ or $[PBD, ACEFK]$.

PROOF. This follows immediately by the discussion of section 3 and $A_{\mathbb{Z}_7^3}$. □

COROLLARY 6.5. *If $H \cong A_7$, $H \leq G$ and H has two orbits on Ω, then $H \in [PED, ABCFK] \cup [PBD, ACEFK]$ and consequently there can be at most 3 conjugacy classes of A_7's in G.*

DEFINITION 6.1. *Let $\Delta_1 = PED \subseteq \Omega$ and $\Delta_2 = PBD \subseteq \Omega$, then we call a subset $\Gamma \subseteq \Omega$ a decapentad of type 1 if and only if $\Gamma^g = \Delta_1$ for some $g \in G$, or a decapentad of type 2 if and only if $\Gamma^g = \Delta_2$ for some $g \in G$. Computation shows there are precisely 50 decapentads of each type.*

Let $\Lambda_i = \Delta_i^G$. Then G acts transitively on Λ_1, Λ_2 and $|G_{(\Delta_i)}| = \frac{|G|}{50} = \frac{7!}{2}$. Hence each $G_{(\Delta_1)}$, $G_{(\Delta_2)}$ are subgroups of G of order $\frac{7!}{2}$ and $G_{(\Delta_1)}$ is not G-conjugate to $G_{(\Delta_2)}$ since $\Delta_2 \notin \Lambda_i$.

PROPOSITION 6.6. $G_{(\Delta_1)} \cong G_{(\Delta_2)} \cong A_7$.

PROOF. $G_{(\Delta_1)}$ has a representation on the 15 points of Δ_1. Since $G_{(\Delta_1)}$ has at most 3 orbits on Ω and since by consideration of $A_{\mathbb{Z}_7^3}$, $\underline{PED}$ or PED are the only possible orbit structures, $G_{(\Delta_1)}$ is transitive on Δ_1. $H = G_{(\Delta_1)}$ acts primitively on Δ_1, for if $H_\alpha \lneq K \leq H$, then K would have orbit type $[8, 7]$ or $[15]$ on Δ_1. But $K \supseteq \mathbb{Z}_7^3$, since $H_\alpha \supseteq \mathbb{Z}_7^3$, hence $[8, 7]$ is not possible. Therefore, K would be transitive on Δ_1, and consequently $|K| = |K_\alpha| \cdot 15$. But clearly $K_\alpha = H_\alpha$ and therefore $K = H$.

It is known however [5] that the only primitive group on 15 points of order $\frac{7!}{2}$ is a group isomorphic to A_7. Therefore, $G_{(\Delta_1)} \cong A_7$. Similarly $G_{(\Delta_2)} \cong A_7$. □

COROLLARY 6.6. *There are at least three conjugacy classes of A_7's namely $A_{7_1} \cong G_\alpha$, $A_{7_2} \cong G_{(\Delta_1)}$, $A_{7_3} \cong G_{(\Delta_2)}$. Hence there are exactly 3 conjugacy classes of A_7's in G.*

The standard representation is $G|\{\text{right cosets of } A_{7_1}\}$. Since $\chi = [1]+[21]+[28]_i$ for some i, and since $\#[orb] = 3$, without loss of generality we take:

$$\chi = \chi_1 = 1_{A_{7_1}} \uparrow^G = 1 + [21] + [28]_1.$$

Since A_{7_2}, A_{7_3} have 2 orbits on Ω, without loss of generality

$$1_{A_{7_2}} \uparrow^G = 1 + [21] + [28]_2$$
$$\text{and}$$
$$1_{A_{7_3}} \uparrow^G = 1 + [21] + [28]_3.$$

Therefore, the elements of order 5 in A_{7_2} or A_{7_3} come from $5_3 \cup 5_2$. Clearly, there is a 3 way symmetry of the above argument relating the representation of G on the cosets of A_7's to the 3 types of A_7's. Therefore each induced character involves each $[28]_i$ exclusively. Hence, $5_2 \in A_{7_1}$, $5_3 \in A_{7_2}$, $5_4 \in A_{7_3}$.

Now we investigate the normalizer $N_G(A_{5_i}) \cong \mathcal{S}_5$. Since each A_{5_i} is contained in an appropriate A_{7_i} and the normalizer in A_{7_i} of A_{5_i} is isomorphic to $\mathcal{S}_5$, $N_G(A_{5_i}) \leq A_{7_i}$, and therefore $N_G(A_{5_i})$ are not maximal in G. Of course $N_G(A_7) = A_{7_i}$ are maximal since there are no permutation characters for G of degree less than 50.

6.9 – The A_6's and their normalizers

Suppose $H \leq G$, $H \cong PGL_2(9)$, then $[G : H] = 175$. Therefore, $\chi = 1_H \uparrow^G = 1 + [125] + [21] + [28]_i \;\; i \in \{1,2,3\} \Rightarrow \;\chi(2) = 1+5+5+4+15$. But $\chi(2)$ should be $\sigma_G(2)(\frac{1}{\sigma_H(2_1)} + \frac{1}{\sigma_H(2_2)}) = 240(\frac{1}{16} + \frac{1}{20}) = 27$, a contradiction. Hence no subgroup of G is isomorphic to $PGL_2(9)$.

Suppose next that there exists $H \leq G$, $H \cong \mathcal{S}_6$. Then $\chi(2) = 240(\frac{1}{48} + \frac{1}{16} + \frac{1}{48}) = 25$, a contradiction; therefore $\mathcal{S}_6 \not\leq G$.

Hence if $A_6 \lhd H \lneq G$, then $H \cong M_{10}$. Consider $\Omega = [K_2 \times K_4 \rightarrow K_{5_i}]$ $i \in \{2,3,4\}$ fixed. $|\Omega| = 75 \cdot |K_{5_i}| = 2^4 \cdot 3^3 \cdot 5^3 \cdot 7$ (Since $a_{2,4,5_i} = 75$). Let $S \subseteq \Omega$ be defined by:

$$(x,y) \in S \text{if and only if } \langle x,y\rangle \cong \mathcal{S}_5$$

$$S \neq \emptyset, \text{ since there exists } H \leq G,\; H \cong \mathcal{S}_5 \in (2,4,5_i).$$

There exists a mapping Φ from S into the collection of all subgroups of G, namely

$$\Phi : (x,y) \rightarrow \langle x,y\rangle.$$

We have

$$|\Phi(S)| = \#[of\ S_5\ with\ a\ 5_i] = [G : \mathcal{S}_5] = 2 \cdot 3 \cdot 5^2 \cdot 7$$

any $H \in \Phi(S)$ is generated in 120 ways as $\langle x, y\rangle$ $|x| = 2$, $|y| = 4$, $|xy| = 5$, $x, y \in H$.

Therefore, $|S| = 120 \cdot |\Phi(S)| = 2^4 \cdot 3^2 \cdot 5^3 \cdot 7$.

Therefore, $T = \Omega \setminus S$ has $2^5 \cdot 3^2 \cdot 5^3 \cdot 7$ elements.

Now consider an A_6 with a 5_i in it. (Such exists since $A_6 \leq A_7$) If $N(A_6) = A_6$, then

$$\#[A_6's\ conjugate\ to\ this\ A_6] = [G : A_6] = 350.$$

But each A_6 is generated as a $(2, 4, 5_i)$ in $2^5 \cdot 3^2 \cdot 5$ ways. Therefore, there would be $350 \cdot 2^5 \cdot 3^2 \cdot 5$ ordered pairs in Ω yielding A_6's. But $350 \cdot 2^5 \cdot 3^2 \cdot 5 > |T| = 2^5 \cdot 3^2 \cdot 5^3 \cdot 7$ a contradiction. Hence, $N(A_6) \cong M_{10}$ and then

$$|T| = 175 \cdot 2^5 \cdot 3^2 \cdot 5.$$

COROLLARY 6.7. *There are exactly* 3 *conjugacy classes of* A_6*'s one for each* $5_2, 5_3, 5_4$*, each normalized by an* M_{10}*.*

– **Appendix**

Generators of $PSU_3(5^2)$:

x :
$(3,17,7)(4,46,38)(5,11,21)(6,26,16)(8,36,32)(9,28,19)$
$(10,13,33)(14,47,15)(18,43,49)(20,44,23)(24,25,39)$
$(29,50,37)(30,35,41)(31,45,40)(34,42,48)$
y :
$(1,3,5,2,4)(6,28,20,12,24)(7,29,16,13,25)(8,30,17,14,21)$
$(9,26,18,15,22)(10,27,19,11,23)(36,37,38,39,40)$
$(41,45,44,43,42)(46,49,47,50,48)$

Character Table of $PSU_3(5^2)$:

x	1	2	4	8_1	8_2	3	6	5_1	5_2	5_3	5_4	10	7_1	7_2
σ_x	$\|G\|$	240	8	8	8	36	12	250	25	25	25	10	7	7
κ_x	1	525	15750	15750	15750	3500	10500	504	5040	5040	5040	12600	18000	18000
χ_1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
χ_2	20	−4	0	0	0	2	2	−5	0	0	0	1	−1	−1
χ_3	28	4	0	0	0	1	1	3	3	−2	−2	−1	0	0
χ_4	28	4	0	0	0	1	1	3	−2	−2	3	−1	0	0
χ_5	28	4	0	0	0	1	1	3	−2	3	−2	−1	0	0
χ_6	21	5	1	−1	−1	3	−1	−4	1	1	1	0	0	0
χ_7	84	−4	0	0	0	3	−1	9	−1	−1	−1	1	0	0
χ_8	126	6	−2	0	0	0	0	1	1	1	1	1	0	0
χ_9	105	1	1	−1	−1	−3	1	5	0	0	0	1	0	0
χ_{10}	144	0	0	0	0	0	0	−6	−1	−1	−1	0	γ	δ
χ_{11}	144	0	0	0	0	0	0	−6	−1	−1	−1	0	δ	γ
χ_{12}	125	5	1	1	1	−1	−1	0	0	0	0	0	−1	−1
χ_{13}	126	−6	0	α	β	0	0	1	1	1	1	-1	0	0
χ_{14}	126	−6	0	β	α	0	0	1	1	1	1	−1	0	0

Hoffman-Singleton Graph

1/	2	5	6	11	16	21	26	26/	1	28	29	34	36	45	49
2/	1	3	7	12	17	22	27	27/	2	29	30	35	37	41	50
3/	2	4	8	13	18	23	28	28/	3	26	30	31	38	42	46
4/	3	5	9	14	19	24	29	29	4	26	27	32	39	43	47
5/	1	4	10	15	20	25	30	30/	5	27	28	33	40	44	48
6/	1	8	9	31	37	43	48	31/	6	12	20	24	28	32	35
7/	2	9	10	32	38	44	49	32/	7	13	16	25	29	31	33
8/	3	6	10	33	39	45	50	33/	8	14	17	21	30	32	34
9/	4	6	7	34	40	41	46	34/	9	15	18	22	26	33	35
10/	5	7	8	35	36	42	47	35/	10	11	19	23	27	31	34
11/	1	13	14	35	39	44	46	36/	10	13	17	24	26	37	40
12/	2	14	15	31	40	45	47	37/	6	14	18	25	27	36	38
13/	3	11	15	32	36	41	48	38/	7	15	19	21	28	37	39
14/	4	11	12	33	37	42	49	39/	8	11	20	22	29	38	40
15/	5	12	13	34	38	43	50	40/	9	12	16	23	30	36	39
16/	1	18	19	32	40	42	50	41/	9	13	20	21	27	42	45
17/	2	19	20	33	36	43	46	42/	10	14	16	22	28	41	43
18/	3	16	20	34	37	44	47	43/	6	17	23	29	15	42	44
19/	4	16	17	35	38	45	48	44/	7	11	18	24	30	43	45
20/	5	17	18	31	39	41	49	45/	8	12	19	25	26	41	44
21/	1	23	24	33	38	41	47	46/	9	11	17	25	28	47	50
22/	2	24	25	34	39	42	48	47/	10	12	18	21	29	46	48
23/	3	25	21	35	40	43	49	48/	6	13	19	30	47	49	22
24/	4	21	22	31	36	44	50	49/	7	14	20	23	26	48	50
25/	5	22	23	32	37	45	46	50/	8	15	16	24	27	46	49

Λ_1															
1	1	7	8	13	14	19	20	24	25	27	28	34	40	43	47
2	2	8	9	14	15	20	16	25	21	28	29	35	36	44	48
3	3	9	10	15	11	16	17	21	22	29	30	31	37	45	49
4	4	10	6	11	12	17	18	22	23	30	26	32	38	41	50
5	5	6	7	12	13	18	19	23	24	26	27	33	39	42	46
6	11	20	4	43	45	28	21	34	2	40	32	48	50	37	10
7	6	28	29	25	18	40	2	19	11	24	33	10	41	15	49
8	5	40	32	34	38	24	11	47	6	27	17	49	3	45	42
9	16	27	17	47	44	13	5	14	26	8	9	23	31	38	22
10	21	13	46	7	37	8	26	43	16	20	4	22	30	12	35
11	39	4	49	45	6	21	46	2	35	32	36	30	15	18	42
12	31	29	42	18	5	2	9	11	48	33	50	36	45	38	23
13	36	33	22	12	16	6	29	5	49	46	3	41	38	44	35
14	50	17	35	44	21	5	32	26	42	9	39	3	12	37	48
15	41	46	48	37	2	26	33	16	23	4	31	39	44	15	10
16	17	22	21	16	45	29	37	49	10	3	11	9	15	30	31
17	46	35	2	21	18	32	15	42	49	39	6	4	45	36	30
18	13	17	1	45	42	30	23	31	4	37	34	50	47	39	7
19	14	18	2	41	43	26	24	32	5	38	35	46	48	40	8
20	15	19	3	42	44	27	25	33	1	39	31	47	49	36	9
21	7	29	30	21	19	36	3	20	12	25	34	6	42	11	50
22	10	27	28	24	17	39	1	18	15	23	32	9	45	14	48
23	1	36	33	35	39	25	12	48	7	28	18	50	4	41	43
24	2	37	34	31	40	21	13	49	8	29	19	46	5	42	44
25	3	38	35	32	36	22	14	50	9	30	20	47	1	43	45
26	7	33	29	19	36	12	22	18	6	41	28	23	16	50	5
27	8	34	30	20	37	13	23	19	7	42	29	24	17	46	1
28	9	35	26	16	38	14	24	20	8	43	30	25	18	47	2
29	10	31	27	17	39	15	25	16	9	44	26	21	19	48	3
30	27	18	25	13	28	1	12	10	43	39	9	49	19	48	3
31	28	19	21	14	29	2	13	6	44	40	10	50	20	25	34
32	29	20	22	15	30	3	14	7	45	36	6	46	16	21	35
33	30	16	23	11	26	4	15	8	41	37	7	47	17	22	31
34	17	47	28	45	14	27	7	5	24	13	16	6	39	23	34
35	18	48	29	41	15	28	8	1	25	14	17	7	40	20	35
36	19	49	30	42	11	29	9	2	21	15	18	8	36	25	31
37	24	7	11	40	6	19	3	27	25	42	26	47	15	33	20
38	25	8	12	36	7	20	4	28	21	43	27	48	11	34	16
39	33	18	26	2	4	50	10	48	38	41	43	31	40	25	11
40	34	19	27	3	5	46	6	49	39	42	44	32	36	21	12
41	35	20	28	4	1	47	7	50	40	43	45	33	37	22	13
42	39	5	31	19	9	47	26	2	44	13	37	50	42	33	23
43	40	1	32	20	10	48	27	3	45	14	38	46	43	34	24
44	30	2	50	45	47	23	36	20	34	32	11	38	4	42	6
45	26	3	46	41	48	24	37	16	35	33	12	39	5	43	7
46	27	4	47	42	49	25	38	17	31	34	13	40	1	44	8
47	28	5	48	43	50	21	39	18	32	35	14	36	2	45	9
48	34	2	24	11	5	49	28	8	47	37	19	41	32	40	43
49	31	4	21	13	2	46	30	10	49	39	16	43	34	37	45
50	32	5	22	14	3	47	26	6	50	40	17	44	35	38	41

Λ_2															
1	1	3	7	14	19	25	30	31	34	36	39	41	43	47	50
2	2	4	8	15	20	21	26	32	35	37	40	42	44	48	46
3	3	5	9	11	16	22	27	33	31	38	36	43	45	49	47
4	4	1	10	12	17	23	28	34	32	39	37	44	41	50	48
5	5	2	6	13	18	24	29	35	33	40	38	45	42	46	49
6	11	29	20	45	28	2	16	33	48	15	24	23	37	10	9
7	6	32	28	18	40	11	21	17	10	45	27	22	15	49	4
8	26	17	24	12	27	5	11	9	42	38	8	48	18	23	32
9	16	46	27	44	13	26	6	4	23	12	20	10	38	22	33
10	21	9	13	37	8	16	5	29	22	44	28	49	12	35	17
11	39	26	4	6	21	35	13	17	30	12	50	25	18	42	7
12	31	16	29	5	2	48	8	46	36	44	41	34	38	23	14
13	30	21	32	26	11	10	20	9	50	37	3	19	12	22	43
14	36	2	33	16	6	49	28	4	41	15	39	47	44	35	25
15	50	11	17	21	5	42	40	29	3	45	31	7	37	48	34
16	41	6	46	2	26	23	24	32	39	18	30	14	15	10	19
17	29	1	49	44	46	22	40	19	33	31	15	37	3	41	10
18	32	1	42	37	9	35	24	47	17	30	45	15	39	3	49
19	33	1	23	15	4	48	27	7	46	36	18	45	31	39	42
20	17	1	22	45	29	10	13	14	9	50	38	18	30	31	23
21	46	1	35	18	32	49	8	43	4	41	12	38	36	30	22
22	9	1	48	38	33	42	20	25	29	3	44	12	50	36	35
23	12	30	16	41	29	3	17	34	49	11	25	24	38	6	10
24	14	27	18	43	26	5	19	31	46	13	22	21	40	8	7
25	15	28	19	44	27	1	20	32	47	14	23	22	36	9	8
26	40	5	50	41	7	22	47	3	31	33	37	26	11	19	43
27	36	1	46	42	8	23	48	4	32	34	38	27	12	20	44
28	37	2	47	43	9	24	49	5	33	35	39	28	13	16	45
29	38	3	48	44	10	25	50	1	34	31	40	29	14	17	41
30	32	30	43	19	1	3	10	12	49	34	46	37	41	39	24
31	33	26	44	20	2	4	6	13	50	35	47	38	42	40	25
32	34	27	45	16	3	5	7	14	46	31	48	39	43	36	21
33	35	28	41	17	4	1	8	15	47	32	49	40	44	37	22
34	40	32	21	11	20	10	28	4	48	50	2	45	37	43	34
35	46	18	31	45	22	1	33	27	43	10	40	4	13	38	49
36	47	19	32	41	23	2	34	28	44	6	36	5	14	39	50
37	48	20	33	42	24	3	35	29	45	7	37	1	15	40	46
38	49	16	34	43	25	4	31	30	41	8	38	2	11	36	47
39	8	46	1	18	23	36	22	30	29	15	19	41	7	31	14
40	43	38	11	3	25	16	27	33	26	12	48	9	10	24	20
41	25	12	6	39	34	21	13	17	16	44	10	4	49	27	28
42	19	37	26	30	47	11	20	9	2	15	42	32	23	8	24
43	47	15	16	36	7	6	28	4	11	45	23	33	22	20	27
44	7	45	21	50	14	5	40	29	6	18	22	17	35	28	13
45	43	33	50	11	7	41	31	40	37	19	47	26	22	5	3
46	25	17	41	6	14	3	30	24	15	47	7	16	35	26	39
47	19	9	39	26	25	31	50	13	18	14	43	2	10	21	30
48	42	8	24	13	9	30	1	12	18	35	17	29	38	25	49
49	22	28	13	20	29	50	1	37	12	10	9	33	44	19	23
50	1	50	17	48	31	34	44	10	14	40	38	41	29	3	25

Acknowledgement

The second author wishes to express his thanks to the Institute for Experimental Mathematics, University of Essen, Germany, and to the Centre for Applied Cryptographic Research, University of Waterloo, Canada, whose hospitality he enjoyed while carrying out parts of this work. Thanks also to L. Babai and E. Luks for many helpful comments.
Research supported in part by National Science Foundation grant CCR- 9610138.

REFERENCES

[1] A. A. Albert – J. Thompson: *Two-element generation of the projective unimodular group*, Illinois J. Math., **3** (1959) pp. 421–439.

[2] E. Bannai – T. Ito: *Algebraic Combinatorics I - Association schemes*, Benjamin/Cummings Publishing Co., London, 1984.

[3] N. Biggs: *Algebraic graph theory*, Cambridge University Press, Cambridge, 1974.

[4] A. E. Brower – J. H. van Lint: *Strongly regular graphs and partial geometries, in: Enumeration and Design*, Proc. Silver Jubilee Conf. on Combinatorics, Waterloo, 1982, D.M. Jackson & S.A. Vanstone (eds.) Academic Press, Toronto (1984) pp. 85–122.

[5] C. J. Colbourn – J. H. Dinitz: *Handbook of Combinatorial Designs*, Chapman & Hall/CRC, Boca Raton, 2007.

[6] C. W. Curtis – I. Reiner: *Methods of Representation Theory with Applications to Finite Groups and Orders*, John Wiley & Sons, New York, 1981.

[7] W. Feit: *Characters of Finite groups*, W. A. Benjamin, Inc., New York, 1967.

[8] D. Gorenstein: *Finite groups*, Harper & Row, New York, 1968.

[9] M. D. Hestenes – D. G. Higman: *Rank* 3 *Groups and Strongly Regular Graphs*, Computers in Algebra and Number Theory, SIAM-AMS Proceeding, **4** (1971) pp. 141–159.

[10] D. G. Higman: *Intersection Matrices for Finite Permutation Groups*, J. Algebra, **6** (1967) pp. 22–42.

[11] D. G. Higman: *Coherent Configurations*, Oxford University Lecture Notes, **4** (1971) pp. 141-159.

[12] B. Huppert: *Endliche Gruppen*, Springer, 1967.

[13] I. M. Isaacs: *Character Theory of Finite Groups*, Academic Press, 1976.

[14] E. S. Kramer – D. M. Mesner: *t-designs on hypergraphs*, Discrete Math., **15** (1976) pp. 263–296.

[15] E. S. Kramer – S. S. Magliveras – D. M. Mesner: *t-designs from the large Mathieu groups*, Discrete Math., **36** (1981) pp. 171–189.

[16] D. E. Littlewood: *The Theory of group characters*, 2nd edition, Clarendon Press, Oxford, 1958.

[17] S. S. Magliveras: *The Subgroup Structure of the Higman-Sims Simple Group*, Ph.D. Dissertation, University of Birmingahm, England (1970), pp. 1–141.

[18] S. S. Magliveras: *The Subgroup Structure of the Higman-Sims Simple Group*, Bulletin of the AMS 77, **4** (1971) pp. 535–539.

[19] M. Hall Jr.: *The theory of groups*, Macmillan, New York, 1959.

[20] D. S. Passman: *Permutation Groups*, W.A. Benjamin, Inc., New York, 1968.

[21] C. C. Sims: *Graphs and Finite Permutation Groups*, Math. Z., **95** (1967) pp. 76–86.

[22] H. Wielandt: *Finite Permutation Groups*, Academic Press, 1964.

Lavoro pervenuto alla redazione il 10 marzo 2010
ed accettato per la pubblicazione il 15 marzo 2010.
Bozze licenziate il 20 aprile 2010

Indirizzo degli Autori:

Cafer Caliskan – Department of Mathematical Sciences – Florida Atlantic University
E-mail: ccaliska@fau.edu

Spyros S. Magliveras – Department of Mathematical Sciences – Florida Atlantic University
Email: spyros@fau.edu

Lucille C. Yu – Sabre Holdings
E-mail: flo_lucille@yahoo.com