HAL
archives-ouvertes.fr

Incidence structures from the blown-up plane and LDPC codes

Alain Couvreur

▶ To cite this version:

Alain Couvreur. Incidence structures from the blown-up plane and LDPC codes. IEEE Transactions on Information Theory, Institute of Electrical and Electronics Engineers, 2011, 57 (7), pp.4401 - 4416. <10.1109/TIT.2011.2146490>. <inria-00540023v2>

HAL Id: inria-00540023
https://hal.inria.fr/inria-00540023v2

Submitted on 24 Jan 2011

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

INCIDENCE STRUCTURES FROM THE BLOWN–UP PLANE AND LDPC CODES

ALAIN COUVREUR

Abstract. In this article, new regular incidence structures are presented. They arise from sets of conics in the affine plane blown–up at its rational points. The LDPC codes given by these incidence matrices are studied. These sparse incidence matrices turn out to be redundant, which means that their number of rows exceeds their rank. Such a feature is absent from random LDPC codes and is in general interesting for the efficiency of iterative decoding. The performance of some codes under iterative decoding is tested. Some of them turn out to perform better than regular Gallager codes having similar rate and row weight.

Keywords: Incidence structures, LDPC codes, algebraic geometry, finite geometry, conics, linear systems of curves, blowing up.

Introduction

LDPC codes were first discovered by Gallager in [2] in the beginning of the sixties. They regained popularity in the mid-nineties and became a fascinating and highly dynamic research area providing numerous applications. The main reason of this success is that, thanks to iterative decoding, these codes perform very close to the theoretical Shannon limit. For instance, see [13].

Constructions. In the literature, one can distinguish two general approaches to construct LDPC codes. The first one is based on random constructions (for instance see [11]). The second one is based on combinatorial and algebraic methods involving finite fields, block designs, incidence structures and so on. The present article focuses on the second approach.

A well–known construction of LDPC codes from incidence structures is due to Kou, Lin and Fossorier in [8] who proposed to use the points-lines incidence in affine and projective spaces. Kou et al's approach motivated several other works about the study of LDPC codes arising from incidence structures. Among them (and the list is far from being exhaustive), other codes from points and lines incidence structures in affine or projective spaces are studied in [6] and [17]. Codes from partial and semi-partial geometries are considered in [5] and [9]. Several other well–known incidence structures have also been used to produce good LDPC codes, among them: generalised quadrangles [7], generalised polygons [10], unital designs [4], incidence structures from Hermitian curves [12], oval designs [16], flats [15] and so on.

Redundant matrices. An interesting property of LDPC codes from incidence structures is that they are frequently defined by parity–check matrices whose number of rows exceeds their rank. Such matrices are said to be *redundant*. Even if it has no influence on the code, a redundant matrix may improve the efficiency of the iterative decoding.

This work was partially supported by the French ANR Defis program under contract ANR-08-EMER-003 (COCQ project).

It is worth noting that sparse matrices obtained by random constructions are generically full rank. Of course, it is always possible to add new rows by linear combinations. However, a linear combination of a large number of rows is in general non-sparse. On the other hand, adding linear combinations of a small number of rows does not improve the performance of iterative decoding.

In the case of the codes described in the above-cited references, the parity–check matrix is highly redundant and no row is a linear combination of a small number of other rows. This is particularly interesting for iterative decoding.

New incidence structures. In this article, we introduce new incidence structures obtained from the incidence relations between points and strict transforms of conics on the affine plane blown–up at all of its rational points. Three incidence structures are presented corresponding to three different sets of conics. These three incidence structures are regular (each point is incident to a constant number of blocks and each block is incident to a constant number of points) and any two points of them have at most one block in common. Moreover, the girth of their incidence graph is proved to be either 6 or 8.

LDPC Codes. Using these incidence structures, we construct **binary** LDPC codes and study their parameters. A formula giving their minimum distance is proved and their dimension is discussed. Two conjectures are stated on the dimensions of some of these codes. Using the computer algebra software Magma, the actual dimension of some codes is computed. The information rates of these codes turn out to be close to $1/2$ and their parity–check matrices are highly redundant since they are almost square and hence contain twice more parity checks than necessary. Finally, simulations of these codes on the Gaussian channel are done and some codes turn out to perform better than regular Gallager codes having the same rates and row weight.

Outline of the article. The aims of the article are described in Section 1. Some necessary background in algebraic geometry (namely, blow–ups and linear systems of curves) are recalled in Section 2. Section 3 is devoted to plane conics. Some well-known basic results on conics are recalled and some lemmas used in what follows are proved. The context and some conventions are stated in Section 4. In Section 5, three sets of conics are introduced and studied. These three sets are the respective first stones of the constructions of the three new incidence structures presented in the following sections. In Section 6, we introduce the surface $\mathbf{B}$ obtained by blowing up all the rational points of the affine plane. We derive three interesting sets of curves on this surface arising from the three sets of conics introduced in the previous section. This yields three new incidence structures defined in Section 7. They are proved to be regular. Explicit formulas for the number of points per block and the number of blocks incident to a point are given. The girth of the incidence graph of these structures is computed and proved to be either 6 or 8. Moreover, the number of minimal cycles is estimated. In Section 8, the LDPC codes from these incidence structures are studied. Some computer aided calculations to get the exact information rate of such codes are presented. Finally, simulations on the Additive White Gaussian Noise channel are presented at the end of the article.

Notations and terminology. In this article, lots of notations and terminologies are introduced and maintained throughout the paper. To help the reader, an index of notations and terminologies is given in Appendix C.

1. Aims of the present article

The aim of the article is to construct binary LDPC codes which could be efficiently decoded by iterative algorithms. To seek good candidates, we are looking for binary matrices which

(1) are sparse;
(2) have a Tanner graph with few small cycles and in particular no cycles of length 4;
(3) are highly redundant, i.e. whose number of rows exceeds the rank.

In order to construct such matrices, we seek incidence structures having some particular properties. First recall the definition of incidence structure.

Definition 1.1 (Incidence structure)**.** An incidence structure $\mathcal{I} := (\mathcal{P}, \mathcal{B}, \mathcal{R})$ consists in three finite nonempty sets. A set of points $\mathcal{P}$, a set of blocks $\mathcal{B}$ and a set of relations $\mathcal{R} \subseteq \mathcal{P} \times \mathcal{B}$ called *incidence relations*. A point $P \in \mathcal{P}$ and a block $B \in \mathcal{B}$ are said to be incident if and only if $(P, B) \in \mathcal{R}$.

An incidence relation can be described by an incidence matrix M, which is a $\sharp\mathcal{P} \times \sharp\mathcal{B}$ binary matrix such that

$$M_{i,j} = \begin{cases} 1 & \text{if } (P_i, B_j) \in \mathcal{R} \\ 0 & \text{otherwise} \end{cases}.$$

Thus, if we want to use incidence structures to construct codes satisfying the above conditions (1), (2), (3), we have to look for incidence structures

(1) have few incidence relations, i.e. $\sharp\mathcal{R} \ll \sharp\mathcal{P} \times \sharp\mathcal{B}$;
(2) have few small cycles in their incidence graph, in particular no cycles of length 4 (which means no pairs of points P, Q being both incident with at least two distinct blocks);
(3) whose number of blocks exceeds the rank of the incidence matrix with entries in $\mathbf{F}_2$.

2. Some algebraic–geometric tools

The aim of this section is to give the minimal background in algebraic geometry to read this article. Hopefully, the contents of this section are enough to understand what follows. Most of the proofs are omitted since the presented results are well–known. We refer the readers to [1] and [14] for more details.

Most of the results stated in the present section hold for arbitrary fields. However, we chose to state the definitions and the results in the context of the article. Thus, from now on, $\mathbf{F}_q$ denotes some finite field and $\overline{\mathbf{F}}_q$ its algebraic closure.

2.1. Points, curves, tangent lines and intersections.

2.1.1. *Affine and projective planes.* We denote respectively by $\mathbf{A}^2$ and $\mathbf{P}^2$ the affine and projective plane over $\mathbf{F}_q$. Given a system of homogeneous coordinates (X, Y, Z) on $\mathbf{P}^2$, the projective plane can be obtained as a union of three copies of $\mathbf{A}^2$ corresponding to the subsets $\{X \neq 0\}$, $\{Y \neq 0\}$ and $\{Z \neq 0\}$. Such subsets are called *affine charts* of $\mathbf{P}^2$.

2.1.2. *Points.* A *geometric point* of $\mathbf{A}^2$ (resp. $\mathbf{P}^2$) is a point whose coordinates are in $\overline{\mathbf{F}}_q$. An $\mathbf{F}_q$*–rational point* (or a *rational point*, when no confusion is possible) is a point whose coordinates are in $\mathbf{F}_q$.

2.1.3. *Curves.*

Definition 2.1 (Curve)**.** A *plane affine curve* C defined over $\mathbf{F}_q$ (resp. a *plane projective curve* defined over $\mathbf{F}_q$) is the vanishing locus in $\mathbf{A}^2$ (resp. $\mathbf{P}^2$) of a squarefree polynomial $f(x,y) \in \mathbf{F}_q[x,y]$ (resp. a squarefree homogeneous polynomial $f \in \mathbf{F}_q[X,Y,Z]$). Equivalently, it is the set of geometric points $P \in \mathbf{A}^2$ (resp $\mathbf{P}^2$) with coordinates (a,b) (resp. $(a:b:c)$) such that $f(a,b)=0$ (resp. $f(a,b,c)=0$). The polynomial f is a *defining polynomial* of the curve. The degree of C is defined as $\deg(C) := deg(f)$.

Remark 2.2. A defining polynomial of a curve over $\mathbf{F}_q$ is unique up to multiplication by a nonzero element of $\mathbf{F}_q$. In what follows we authorise ourselves to say "the defining polynomial of C" even if it is a misuse of language.

Definition 2.3 (Reducible and irreducible curves)**.** A curve C is said to be *irreducible* if its defining polynomial is irreducible. Else it is said to be *reducible*.

Definition 2.4 (Smooth and singular points)**.** Let C be an affine curve, f be its defining polynomial and P be a geometric point of C. The curve is said to be *singular* at P if the partial derivatives $\frac{\partial f}{\partial x}$ and $\frac{\partial f}{\partial y}$ vanish at P. Else, the curve C is said to be *smooth* at P. A curve is said to be *singular* if it is singular at at least one geometric point. Else it is said to be *smooth*.

Remark 2.5. The notion of being smooth or singular at a point P is extended to projective curves by reasoning on an affine chart of $\mathbf{P}^2$ containing P.

Definition 2.6 (Projective closure)**.** Let C be a plane affine curve defined by the squarefree polynomial $f \in \mathbf{F}_q[x,y]$. Let $f^\sharp$ be the unique homogeneous polynomial in $\mathbf{F}_q[X,Y,Z]$ such that $f^\sharp(x,y,1) = f(x,y)$ and $\deg(f^\sharp) = \deg(f)$. The projective curve of equation $f^\sharp = 0$ is called the projective closure of C. It is obtained by adding to C some *points at infinity* (see Definition 4.1 further).

2.1.4. *Tangent lines.*

Definition 2.7 (Tangent line)**.** Let C be a plane affine curve. Let P be a geometric point of C and L be a line of $\mathbf{A}^2$ containing P. The line L is said to be a *tangent* to C at P if

$$a\frac{\partial f}{\partial x}(P) + b\frac{\partial f}{\partial y}(P) = 0$$

for all director vectors (a,b) of L.

Remark 2.8. As in Remark 2.5, the notion of tangent line can be extent to projective curves by considering affine charts.

Proposition 2.9. *A plane curve is smooth at a point P if and only if it has a unique tangent line at this point. A plane curve C is singular at P if and only if any line containing P is a tangent to C at P.*

2.1.5. *Intersection multiplicity.* The notion of intersection multiplicity is pretty easy to feel but heavy to define properly. Therefore, we do not state its definition for which we refer the reader to [1] Chapter 3 §3. However, let us give some basic properties of this mathematical function which are enough for what follows.

If P is a geometric point of $\mathbf{A}^2$ (resp. $\mathbf{P}^2$) and C, D are two curves which have no common irreducible component (i.e. their defining polynomials are prime to each other), then one can define a nonnegative integer denoted by $m_P(C,D)$ and called the *intersection multiplicity* of C and D at P which satisfies the following properties.

(1) $m_P(C,D) = 0$ if and only if one of the curves C, D does not contain P;
(2) $m_P(C,D) = 1$ if and only if both curves contain P, are smooth at it and have distinct tangent lines at this point;
(3) else, $m_P(C,D) \geq 2$.

In particular, a curve has always intersection multiplicity > 1 at P with one of its tangent lines at this point.

To conclude this subsection let us recall the well–known Bézout's Theorem.

Theorem 2.10 (Bézout's Theorem)**.** *Let C, D be two plane projective curves having no common irreducible components. Then the set of geometric points of intersection of C and D is finite and*

$$\sum_{P \in C \cap D} m_P(C,D) = \deg(C).\deg(D).$$

2.2. **Blow–up of a surface at a point.** Blowing up a point of a surface is a classical operation in algebraic geometry. It is often used to "desingularise" a curve embedded in a surface or to "regularise" a non regular map at a point. In this section, we briefly present the notion of blow–up and summarise its most useful properties for the following sections. We refer the reader to [1] Chapter 7 or [14] Chapter II.4 for further details.

Definition 2.11 (Blow–up of a surface at one point)**.** Let S be an algebraic surface and P be a smooth point of S. The blow–up of S at P is a surface $\widetilde{S}$ together with a surjective map $\pi : \widetilde{S} \to S$ satisfying the following properties.

(i) The set $\pi^{-1}(\{P\})$ of pre-images of P by π is a curve E isomorphic to the projective line and called the *exceptional divisor*.
(ii) The restriction $\pi : \widetilde{S} \setminus E \to S \setminus \{P\}$ is an isomorphism of varieties.

Proposition 2.12. *The blow–up of a surface at a point is unique up to isomorphism.*

Example 2.13 (Blow–up of the affine plane). Consider the affine plane $\mathbf{A}^2$ with coordinates (x, y) and let P be the origin. Then, the blow–up of $\mathbf{A}^2$ at P is the surface

$$\widetilde{\mathbf{A}}^2 := \{(x, y, (u : v)) \in \mathbf{A}^2 \times \mathbf{P}^1 \mid xu = yv\}.$$

together with the projection map

$$\pi : \left\{ \begin{array}{ccc} \widetilde{\mathbf{A}}^2 & \to & \mathbf{A}^2 \\ (x, y, (u : v)) & \mapsto & (x, y) \end{array} \right. .$$

One sees easily that the set of pre-images of the origin is isomorphic to $\mathbf{P}^1$ and that any point of $\mathbf{A}^2 \setminus \{P\}$ has a unique pre-image by π.

Definition 2.14 (Strict transform of a curve)**.** Let S be a smooth surface and P be a point of S. Let $\pi : \widetilde{S} \to S$ be the blow–up of S at P and denote by E the corresponding exceptional divisor. Let C be a curve embedded in S and containing P. The decomposition into irreducible components of the algebraic set $\pi^{-1}(C)$ is of the form $\pi^{-1}(C) = E \cup \widetilde{C}$, where $\widetilde{C}$ does not contain E. The curve $\widetilde{C}$ is called the *strict transform* of C by π.

If C does not contain P, its strict transform is defined as $\widetilde{C} := \pi^{-1}(C)$.

Remark 2.15. The above definition extends naturally to a map obtained by the composition of a finite number of blow–ups.

In the proposition below, we summarise most of the properties of blow–ups needed in what follows.

Proposition 2.16. *Let $\pi : \widetilde{S} \to S$ be the blow–up of a surface S at a smooth point P. Denote by E the exceptional divisor.*

(i) There is a one-to-one correspondence between tangent lines to S at P and points of the exceptional divisor. In particular, given a tangent line L to S at P, there exists a unique point $Q \in E$ such that for all curve $C \subset S$ smooth at P and tangent to L at this point, the strict transform $\widetilde{C}$ meets E at Q and only at this point.

(ii) If two curves C, D meet at P, are smooth at it but have no common tangent line at P, then their strict transforms do not meet in a neighbourhood of the exceptional divisor.

(iii) If two curves C, D meet at P, are smooth at it and have a common tangent L (i.e. their intersection multiplicity at P is greater than or equal to 2), then, their strict transforms meet at the point $Q \in E$ corresponding to L. Moreover,

$$m_P(C, D) > m_Q(\widetilde{C}, \widetilde{D}) \geq 1,$$

where $m_P(.,.)$ denotes the intersection multiplicity at P.

We conclude this sub-section with the following lemma.

Lemma 2.17. *In the context of Proposition 2.16, if $C \subset S$ is a curve which is smooth at P or avoids P, then $\widetilde{C}$ is isomorphic to C. In particular, C and $\widetilde{C}$ have the same number of rational points.*

2.3. **Linear automorphisms of the projective plane.** Some proofs in this article involve the action of the group $\mathbf{PGL}(3, \mathbf{F}_q)$ of linear automorphisms of $\mathbf{P}^2$. It is well–known that this group acts simply transitively on 4–tuples of rational points of $\mathbf{P}^2$ such that no 3 of them are collinear. More generally we have the following lemma.

Lemma 2.18. *The group $\mathbf{PGL}(3, \mathbf{F}_q)$ acts transitively on 4–tuples of the form:*

(1) $(P, \overline{P}, P_3, P_4)$ where P_3, P_4 are rational points and $P, \overline{P}$ are non rational points conjugated under the action of the Frobenius and no 3 of these points are collinear;

(2) (P_1, P_2, L_1, L_2), where P_1, P_2 are rational points and L_1, L_2 are lines defined over $\mathbf{F}_q$ such that $P_1 \in L_1$, $P_2 \in L_2$, $P_1 \notin L_2$ and $P_2 \notin L_1$;

(3) (P_1, P_2, P_3, L) such that P_1, P_2, P_3 are non-collinear rational points and L is a line defined over $\mathbf{F}_q$ containing P_3 and avoiding P_1, P_2;

(4) $(P, \overline{P}, P_3, L)$ where P_3 is a rational point and $P, \overline{P}$ are conjugated under the action of the Frobenius map, the three points are non collinear and L is a line defined over $\mathbf{F}_q$ containing P_3 and avoiding $P, \overline{P}$.

In case (1), the action is also free.

The proof of Lemma 2.18 is given in Appendix A.

2.4. **Linear Systems of plane projective curves.** Linear systems of curves is a central object in this article. Let us recall their definition and some of their properties. For reference, see [1] Chapter 5 §2.

Definition 2.19 (Linear System of curves)**.** A linear system Γ of curves in the affine (resp. projective) plane is a set of (possibly non-reduced) curves linearly parametrised by some projective space $\mathbf{P}^n$. That is, there exists a family of linearly independent polynomials $F_0, \ldots, F_s \in \mathbf{F}_q[x, y]$ (resp. linearly independent homogeneous polynomials in $\mathbf{F}_q[x, y, z]$ of the same degree), such that for each element $C \in \Gamma$, there exists a unique point $P = (p_0 : \ldots : p_s) \in \mathbf{P}^s$ such that $p_0F_0 + \cdots + p_sF_s = 0$ is an equation of C.

Remark 2.20 (Non-reduced curves). In §2.1.3, a curve is defined as the vanishing locus of a squarefree polynomial. In the above definition, some elements of the linear set of polynomials may have square factors. The good formalism to take care of this difficulty is that of Grothendieck's schemes (see for instance [3] Chapter II). However, this theory requires a huge background which is useless for what follows.

In the present article, the linear systems are always linear systems of curves of degree 2. The only degenerate cases are polynomial of the form $l(x,y)^2$, where l has degree 1. In this case, the corresponding "curve" C is called the *double line* supported by L (where L is the line of equation $l(x,y)=0$). The points of C are those of L. In addition, C is singular at all of its points and any line containing a point $P \in C$ is tangent to C at P. Considering $l(x,y)^2$ as the defining polynomial of C, this property is actually coherent with Definition 2.7 and Proposition 2.9.

Definition 2.21. In the context of Definition 2.19, if $P=(p_0:\ldots:p_s)$ is a geometric point of $\mathbf{P}^s$, the curve of equation $p_0F_0+\cdots+p_sF_s=0$ is called a *geometric element* of Γ. If P is a rational point of $\mathbf{P}^s$, then this curve is said to be a *rational element* of Γ. The rational elements of Γ are the curves of Γ which are defined over $\mathbf{F}_q$.

Definition 2.22. The dimension of a linear system is the dimension of its projective space of parameters.

The example of the linear system of conics is studied in the following section.

3. The linear system of plane conics

This section is devoted to the linear system of plane projective conics and the properties of some of its subsystems. The family of polynomials $X^2, Y^2, Z^2, XY, XZ, YZ$ generates a linear system of dimension 5 on $\mathbf{P}^2$ called the *linear system of plane conics*. Its elements are classified in the following proposition.

Proposition 3.1 (Classification of plane projective conics)**.** *An element of the linear system of conics can be*

(1) either a smooth irreducible curve, in this situation, it has $q+1$ rational points;
(2) or a union of two lines defined over $\mathbf{F}_q$;
(3) or a union of two lines defined over $\mathbf{F}_{q^2}$ and conjugated under the Frobenius map;
(4) or a "doubled" line defined over $\mathbf{F}_q$ (see Remark 2.20).

The two following lemmas are frequently useful in what follows. To state them, the following notation is convenient.

Notation 3.2. Let P, Q be two points of the affine (resp. projective) plane. We denote by (PQ) the unique affine (resp. projective) line joining P to Q.

Lemma 3.3. *Let P_1, P_2, P_3 be three non-collinear geometric points of $\mathbf{P}^2$. Let L be a line containing P_3 and avoiding P_1 and P_2. The linear system $\Lambda_1(P_1,P_2,P_3,L)$ of conics containing P_1, P_2, P_3 and tangent to L at P_3 has dimension 1. Moreover its only singular geometric elements are $C:=(P_1P_2)\cup L$ and $C':=(P_1P_3)\cup(P_2P_3)$.*

Remark 3.4. In the above statement, the curve $C':=(P_1P_3)\cup(P_2P_3)$ is singular at P_3. Therefore, from Proposition 2.9, any line containing P_3 is tangent to C' at P_3.

Proof of Lemma 3.3. Applying a suitable automorphism in $\mathbf{PGL}(3,\overline{\mathbf{F}}_q)$ (use Lemma 2.18 (3) replacing $\mathbf{PGL}(3,\mathbf{F}_q)$ by $\mathbf{PGL}(3,\overline{\mathbf{F}}_q)$), one can assume that P_1, P_2, P_3 have respective coordinates $(1:0:0)$, $(0:1:0)$, $(0:0:1)$ and the line L has equation $Y=X$. Take an equation $aX^2+bXY+cY^2+dXZ+eYZ+fZ^2=0$ of a conic.

The vanishing conditions at P_1, P_2, P_3 yield respectively $a = 0, c = 0$ and $f = 0$. The tangency condition entails $d = e$. Thus, the resulting linear system is parametrised by $\mathbf{P}^1$ and generated by the polynomials XY and $XZ + YZ$.

Now, let D be a singular element of $\Lambda_1(P_1, P_2, P_3, L)$. From Proposition 3.1, D is a union of two lines. We conclude by noticing that the only pairs of lines satisfying the conditions of the linear system are $(P_1P_2) \cup L$ and $(P_1P_3) \cup (P_2P_3)$. □

Lemma 3.5. *Let P_1, P_2 be two geometric points of $\mathbf{P}^2$. Let L_1, L_2 be two lines such that $L_1 \ni P_1$, $L_2 \ni P_2$, $P_1 \notin L_2$ and $P_2 \notin L_1$. Then the linear system $\Lambda_2(P_1, P_2, L_1, L_2)$ of conics containing P_1, P_2 and being respectively tangent to L_1, L_2 at these points has dimension 1. Moreover its only singular geometric elements are $L_1 \cup L_2$ and the doubled line supported by (P_1P_2) (see Remark 2.20).*

Proof. It is almost the same approach as that of the proof of Lemma 3.3 □

Remark 3.6. In Lemmas 3.3 and 3.5, the linear systems have exactly $q - 1$ smooth $\mathbf{F}_q$–rational elements.

4. Context, notations and terminology

In what follows, the cardinal q of the base field $\mathbf{F}_q$ is assumed to be greater than or equal to 4. The characteristic of the base field may be odd. We fix a system of coordinates (x, y) for $\mathbf{A}^2$ and a system of homogeneous coordinates $(X : Y : Z)$ on $\mathbf{P}^2$. Moreover, we identify $\mathbf{A}^2$ as an affine chart of $\mathbf{P}^2$ by the map $(x, y) \mapsto (x : y : 1)$.

Caution. In this whole article, we deal with error correcting codes and with algebraic geometry over finite fields. It is worth noting that, although the geometric objects we deal with are defined over finite fields $\mathbf{F}_q$ with $q \geq 4$ and possibly odd, all the codes we construct are **binary** codes (i.e. defined over $\mathbf{F}_2$).

Notation 4.1. The line $\{Z = 0\}$, is called "the line at infinity" and denoted by L_∞. We fix an element $\alpha \in \mathbf{F}_{q^2} \setminus \mathbf{F}_q$ and denote respectively by P_∞, Q_∞, R_∞ and $\overline{R}_\infty$ the points of respective coordinates:

$$\begin{array}{lcllcl} P_\infty & := & (0:1:0) & \qquad Q_\infty & := & (1:0:0) \\ R_\infty & := & (\alpha:1:0) & \qquad \overline{R}_\infty & := & (\alpha^q:1:0). \end{array}$$

The points R_∞ and $\overline{R}_\infty$ are non rational but conjugated under the Frobenius action.

Definition 4.2 (Vertical and horizontal lines)**.** We call vertical (resp. horizontal) lines the affine lines having an equation of the form $x = a$ (resp. $y = a$), where $a \in \mathbf{F}_q$. Equivalently, vertical (resp. horizontal) lines are affine lines whose projective closure contain the point P_∞ (resp. Q_∞).

We keep Notation 3.2: given two points P, Q we denote by (PQ) the line joining these points. Moreover, we introduce the following notation.

Notation 4.3. Let C be a plane curve and P be a smooth point of it, we denote by T_PC the tangent line of C at P.

5. Incidence structures of conics of the affine plane

In the present section, we introduce the sets of conics $\mathcal{C}_1(q), \mathcal{C}_2(q)$ and $\mathcal{C}_3(q)$ which are further used to construct the block set of the incidence structures introduced in §5.5.

5.1. **The problem of small cycles.** As said in §1, one of our objectives is to construct incidence structures in which two points are both incident with at most one block. If one considers a set of points of the affine or projective plane together with a set of conics, the corresponding incidence structure does in general not satisfy such expectations. Indeed, from Bézout's Theorem (2.10), two projective conics with no common irreducible components may meet at up to 4 distinct points.

Therefore, in order to construct a "good" incidence structure from conics, i.e. a set of points and a set of blocks such that two points have at most one block in common, we use two ideas.

(1) First, we consider particular sets of affine conics such that the projective closures of any two of them intersect twice at infinity. Such curves meet at most twice in the affine plane. This is the point of the present section.
(2) Second, we blow–up the rational points of the affine plane and consider the strict transforms of conics on this blown–up plane. From Proposition 2.16 these strict transforms meet less frequently and provide an incidence structure which turns out satisfy our expectations. This is the point of Section 6.

5.2. **Three sets of affine conics.** We describe three sets of affine conics respectively denoted by $\mathcal{C}_1(q), \mathcal{C}_2(q)$ and $\mathcal{C}_3(q)$. They are constructed from 3–dimensional linear system of conics having prescribed points or tangents at infinity.

Definition 5.1 (The set $\mathcal{C}_1(q)$)**.** Let Γ_1 be the linear system of conics containing P_∞ and tangent to L_∞ at P_∞ (see Notation 4.1). We define the set $\mathcal{C}_1(q)$ to be the set affine conics defined over $\mathbf{F}_q$ whose projective closure is a smooth element of Γ_1. In affine geometry over the reals, such conics would be a family of parabolas.

Definition 5.2 (The set $\mathcal{C}_2(q)$)**.** Let Γ_2 be the linear system of projective conics containing the points P_∞ and Q_∞ (see Notation 4.1). We define the set $\mathcal{C}_2(q)$ to be the set of affine conics defined over $\mathbf{F}_q$ whose projective closure is a smooth element of Γ_2. In affine geometry over the reals, such conics would be a family of hyperbolas.

Definition 5.3 (The set $\mathcal{C}_3(q)$)**.** Let Γ_3 be the linear system of projective conics containing the pair $(R_\infty, \overline{R}_\infty)$ (see Notation 4.1). We define $\mathcal{C}_3(q)$ to be the set of affine conics defined over $\mathbf{F}_q$ whose projective closure is a smooth element of Γ_3. In affine geometry over the reals, such conics would be a family of ellipses.

Remark 5.4. Even if the set of curves $\mathcal{C}_3(q)$ depends on the choice of α, given two choices α, α' of elements of $\mathbf{F}_{q^2} \setminus \mathbf{F}_q$, Lemma 2.18 (1) asserts the existence of $\sigma \in \mathbf{PGL}(3, \mathbf{F}_q)$ sending $\{(\alpha : 1 : 0), (\alpha^q : 1 : 0)\}$ onto $\{(\alpha' : 1 : 0), (\alpha'^q : 1 : 0)\}$. Thus, $\mathcal{C}_3(q)$ is unique up to isomorphism and changing the choice of α does not change the isomorphism class of the incidence structure or that of the LDPC code.

Remark 5.5. In the linear systems Γ_1, Γ_2 and Γ_3, one finds some reducible conics obtained by the union of the line at infinity together with any other line. The trace of such curves in $\mathbf{A}^2$ is a line and hence a smooth irreducible curve but is not an affine conic. Such elements are not elements of the sets $\mathcal{C}_1(q), \mathcal{C}_2(q)$ or $\mathcal{C}_3(q)$.

5.3. **Explicit equations.** The following Lemmas give an explicit descriptions of the elements of $\mathcal{C}_1(q), \mathcal{C}_2(q)$ and $\mathcal{C}_3(q)$.

Proposition 5.6 (Equation of an element of $\mathcal{C}_1(q)$)**.** *An affine curve is in $\mathcal{C}_1(q)$ if and only if it has an equation of the form*

$$y = ax^2 + bx + c, \quad \textit{with} \quad a \in \mathbf{F}_q \setminus \{0\} \textit{ and } b, c \in \mathbf{F}_q.$$

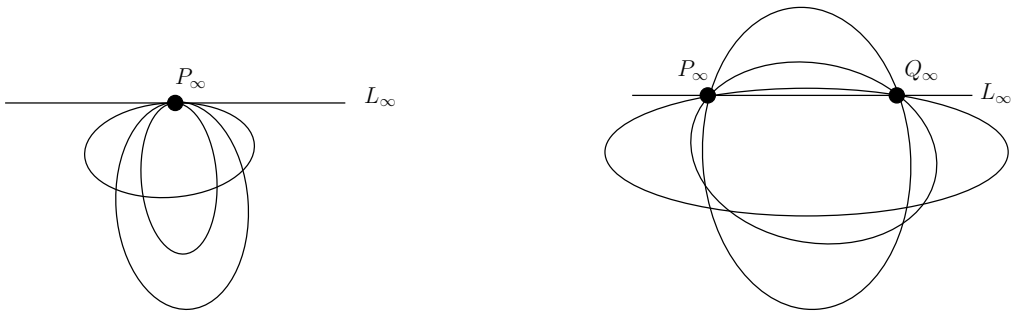

FIGURE 1. The linear systems Γ_1 (on the left) and Γ_2 (on the right)

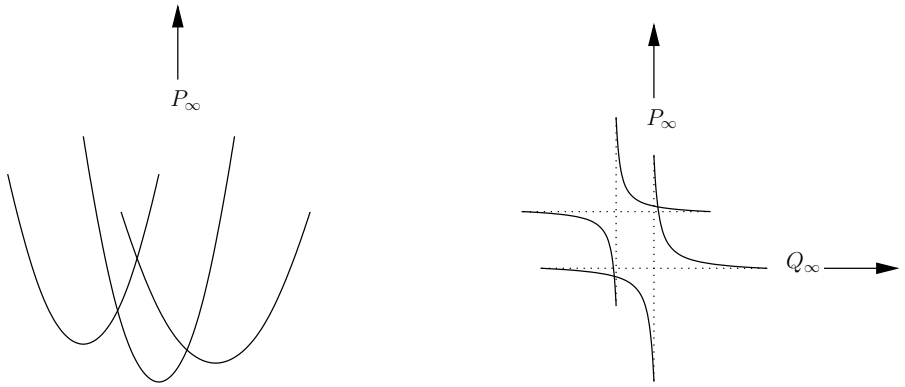

FIGURE 2. The sets $\mathcal{C}_1(q)$ (on the left) and $\mathcal{C}_2(q)$ (on the right)

Proof. Let $C \in \mathcal{C}_1(q)$, let $\overline{C}$ be its projective closure and $F(X,Y,Z) = \lambda_1 X^2 + \lambda_2 XY + \lambda_3 XZ + \lambda_4 Y^2 + \lambda_5 YZ + \lambda_6 Z^2$ be a defining polynomial of $\overline{C}$. The condition $P_\infty = (0:1:0) \in \overline{C}$ entails $\lambda_4 = 0$. For the tangency condition, consider the affine chart $\{Y \neq 0\}$. In this chart, we get a non homogeneous equation $g(x,z) = \lambda_1 x^2 + \lambda_2 x + \lambda_3 xz + \lambda_5 z + \lambda_6 z^2 = 0$. The point P_∞ has coordinates $(0,0)$ in this chart. From Definition 2.7, being tangent at P_∞ to L_∞ (which has equation $z = 0$ in this chart), means that $\frac{\partial g}{\partial x}(0,0) = 0$ and hence $\lambda_2 = 0$. In addition, if λ_5 was zero, then $\frac{\partial g}{\partial z}$ would also vanish at P_∞ and $\overline{C}$ would be singular. Thus, $\lambda_5 \neq 0$ and can be set to -1 without loss of generality

In the affine chart $\{Z \neq 0\}$, the conic has an affine equation of the form $f(x,y) = \lambda_1 x^2 + \lambda_3 x + \lambda_6 - y = 0$. Moreover, λ_1 must be nonzero or the corresponding affine curve would be a line and not a conic. There remains to show that under these conditions $\overline{C}$ is always smooth. It is obviously smooth at P_∞ (that was the reason why we set $\lambda_5 \neq 0$). It is also smooth in the affine chart $\{Z \neq 0\}$ since the partial derivative $\frac{\partial f}{\partial y} \equiv 1$ and hence never vanishes in this chart. □

Proposition 5.7 (Equation of an element of $\mathcal{C}_2(q)$)**.** *An affine curve is in $\mathcal{C}_2(q)$ if and only if it has an equation of the form*

$$xy = ax + by + c, \quad \textit{with} \quad (a,b,c) \in \mathbf{F}_q^3 \textit{ and } c \neq -ab.$$

Proof of Proposition 5.7. Let $C \in \mathcal{C}_2(q)$ and $\overline{C}$ and $F(X,Y,Z)$ be as in the proof of Proposition 5.6. The conditions at P_∞ and $Q_\infty \in \overline{C}$ entail respectively $\lambda_4 = 0$ and $\lambda_1 = 0$. This yields an affine equation for C of the form $f(x,y) = \lambda_2 xy + \lambda_3 x + \lambda_5 y + \lambda_6 = 0$. Since C is a conic and not a line, $\lambda_2 \neq 0$ and can bet set to -1 without loss

of generality. Then $\frac{\partial f}{\partial x} = \lambda_3 - y$ and $\frac{\partial f}{\partial y} = \lambda_5 - x$. Thus, C is singular if and only if the point (λ_5, λ_3) is in C. One checks easily that this situation happens if and only if $\lambda_6 = -\lambda_3\lambda_5$. Therefore if $\lambda_6 \neq -\lambda_3\lambda_5$ then C is smooth. There remains to check that $\overline{C}$ is also smooth at P_∞ and Q_∞. Since $\overline{C}$ has degree 2 and meets L_∞ at P_∞ and Q_∞, from Bézout's Theorem, the intersection multiplicities $m_{P_\infty}(\overline{C}, L_\infty)$ and $m_{Q_\infty}(\overline{C}, L_\infty)$ are both equal to 1 and hence $\overline{C}$ cannot be singular at these points (see §2.1.5). □

The equation of the elements of $\mathcal{C}_3(q)$ depend on the choice of α. From Remark 5.4, there is no loss of generality to consider an arbitrary choice of α, which is what we do in the two following lemmas.

Proposition 5.8 (Equation of an element of $\mathcal{C}_3(q)$ in odd characteristic)**.** *Assume that q is odd. Let β be a non-square element of $\mathbf{F}_q \setminus \{0\}$ and $\alpha \in \mathbf{F}_{q^2} \setminus \mathbf{F}_q$ such that $\alpha^2 = \beta$. For this choice of α, an affine curve is in $\mathcal{C}_3(q)$ if and only if it has an equation of the form*

$$x^2 - \beta y^2 = ax + by + c, \quad \textit{with} \quad c \neq \frac{b^2}{4\beta} - \frac{a^2}{4}.$$

Proof. Let $C \in \mathcal{C}_3(q)$ and $\overline{C}$ and $F(X, Y, Z)$ be as in the proof of Proposition 5.6. The vanishing conditions at R_∞ and $\overline{R}_\infty \in \overline{C}$ entail $\lambda_1\alpha^2 + \lambda_2\alpha + \lambda_4 = 0$. Since $T^2 - \beta$ is the minimal polynomial of α, we have $\lambda_2 = 0$ and $\lambda_4 = -\beta\lambda_1$. If $\lambda_1 = 0$, then C would have an affine equation of the form $\lambda_3 x + \lambda_5 y + \lambda_6 = 0$ and hence would not be a conic. Therefore, λ_1 is nonzero and can be set to -1 without loss of generality. As in the proof of Lemma 5.7, an argument based on Bézout's Theorem asserts that on these conditions $\overline{C}$ is smooth at R_∞ and $\overline{R}_\infty$. There remains to find under which additional conditions it is smooth in the affine chart $\{Z \neq 0\}$. In this chart, the curve has an equation of the form $f(x, y) = \lambda_3 x + \lambda_5 y + \lambda_6 - (x^2 - \beta y^2)$. A computation of the partial derivatives of f entails that C is singular if and only if $f(\frac{\lambda_3}{2}, -\frac{\lambda_5}{2\beta}) = 0$. This leads to the assertion that C is smooth provided $\frac{\lambda_3^2}{4} - \frac{\lambda_5^2}{4\beta} + \lambda_6 \neq 0$. □

Proposition 5.9 (Equation of an element of $\mathcal{C}_3(q)$ in even characteristic)**.** *Assume that q is even. Let β be an element of $\mathbf{F}_q \setminus \{0\}$ such that $\mathrm{Tr}_{\mathbf{F}_{q^2}/\mathbf{F}_q}(\beta) \neq 0$ and $\alpha \in \mathbf{F}_{q^2} \setminus \mathbf{F}_q$ such that $\alpha^2 + \alpha + \beta = 0$. For this choice of α, an affine curve is in $\mathcal{C}_3(q)$ if and only if it has an equation of the form*

$$x^2 + xy + \beta y^2 = ax + by + c, \quad \textit{with} \quad c \neq a^2 + b^2 + ab.$$

Proof. The proof is similar as that of Proposition 5.8, the conditions R_∞ and $\overline{R}_\infty$ entail $\lambda_1 = \lambda_2$ and $\lambda_3 = \beta\lambda_1$. Moreover, $\lambda_1 \neq 0$ and can be set to 1 without loss of generality. Using Bézout's Theorem, one asserts that $\overline{C}$ is smooth at the points at infinity.

In the affine chart $\{Z \neq 0\}$, the curve C has an equation of the form $f(x, y) = \lambda_3 x + \lambda_5 y + \lambda_6 + (x^2 + x + \beta y^2)$ and computations on the partial derivatives entail that this curve is smooth provided $\lambda_3^2 + \lambda_5^2 + \lambda_3\lambda_5 + \lambda_6 \neq 0$. □

5.4. **Counting number of elements.**

Proposition 5.10 (Cardinal of the $\mathcal{C}_i(q)$'s)**.** *The sets $\mathcal{C}_1(q), \mathcal{C}_2(q)$ and $\mathcal{C}_3(q)$ have $q^3 - q^2$ elements.*

Proof. It is a straightforward consequence of Lemmas 5.6 to 5.9. □

Proposition 5.11 (Number of points of an element of $\mathcal{C}_i(q)$)**.** *Any element of $\mathcal{C}_1(q)$ (resp. $\mathcal{C}_2(q)$, resp. $\mathcal{C}_3(q)$) has exactly q (resp. $q-1$, resp $q+1$) rational points in $\mathbf{A}^2$.*

Proof. By definition, for all $C \in \mathcal{C}_1(q)$ (resp. $\mathcal{C}_2(q), \mathcal{C}_3(q)$) the projective closure $\overline{C}$ is smooth. Thus, from Proposition 3.1 (1), $\overline{C}$ has $q+1$ rational points. Moreover, it has one (resp. two, resp. zero) prescribed rational point at infinity, this yields the result. □

5.5. **Incidence relations.**

Lemma 5.12 (Incidence structures given by the $\mathcal{C}_i(q)$'s)**.** *Let C, D be a pair of distinct elements of $\mathcal{C}_1(q)$ (resp. of $\mathcal{C}_2(q)$, resp. of $\mathcal{C}_3(q)$). Then, these two curves meet at 0 or 1 or 2 rational points of $\mathbf{A}^2$. Moreover, if they have a common tangent at a rational point P of $\mathbf{A}^2$, then they do not meet at another point of $\mathbf{A}^2$.*

Proof. By definition, any two conics of $\mathcal{C}_1(q)$ (resp. $\mathcal{C}_2(q)$, resp. $\mathcal{C}_3(q)$) meet at least twice (counted with multiplicities) at infinity. This claim together with Bézout's Theorem yield the result. □

5.6. **Affine automorphisms.** To conclude the present section, we focus on automorphisms of $\mathbf{A}^2$ preserving $\mathcal{C}_1(q)$ (resp. $\mathcal{C}_2(q)$, resp. $\mathcal{C}_3(q)$). Basically they are the projective automorphisms preserving the pair (P_∞, L_∞) (resp. (P_∞, Q_∞), resp. $R_\infty, \overline{R}_\infty$). We have the following lemma.

Lemma 5.13. *The group of automorphisms of $\mathbf{A}^2$ preserving $\mathcal{C}_1(q)$ (resp. $\mathcal{C}_2(q)$, resp. $\mathcal{C}_3(q)$) acts transitively on the pairs (P, L) such that P is a rational point of $\mathbf{A}^2$ and L is a non vertical line containing P (resp. a neither vertical nor horizontal line containing P, resp. a line containing P).*

Proof. It is a consequence of Lemma 2.18. □

6. The blown–up plane

As said in Lemma 5.12, two conics of $\mathcal{C}_i(q)$ may meet at two distinct points, therefore the incidence structure given by the rational points of $\mathbf{A}^2$ together with the elements of $\mathcal{C}_1(q)$ (resp. $C_2, \mathcal{C}_3(q)$) does not satisfies the conditions expected in §1. This is the reason why, we introduce the surface $\mathbf{B}$.

Definition 6.1 (The surface $\mathbf{B}$)**.** Let $P_1, \dots, P_{q^2}$ be the rational points of the affine plane. The surface $\mathbf{B}$ is the surface obtained from $\mathbf{A}^2$ by blowing up all the points $P_1, \dots, P_{q^2}$. The corresponding exceptional divisors are denoted by $E_{P_1}, \dots, E_{P_{q^2}}$ and we denote by $\mathcal{E}$ the set $\mathcal{E} := \{E_{P_1}, \dots, E_{P_{q^2}}\}$.

Remark 6.2. Two distinct exceptional divisors on $\mathbf{B}$ are disjoint.

The rational points of $\mathbf{B}$ can be interpreted in terms of *flags*. This is the purpose of the following definition.

Definition 6.3 (Flags)**.** We call a *flag* on $\mathbf{A}^2$ a pair (P, L), where P is a rational point of $\mathbf{A}^2$, L is a line defined over $\mathbf{F}_q$ and $P \in L$.

Definition 6.4 (Incidence flag/curve)**.** A plane curve C and a flag (P, L) are said to be *incident* if $P \in C$ and L is a tangent to C at P.

Lemma 6.5. *The rational points of $\mathbf{B}$ are in one-to-one correspondence with the flags of $\mathbf{A}^2$. In particular, $\mathbf{B}$ has $q^2(q+1)$ rational points.*

Proof. It is a straightforward consequence of Proposition 2.16 (i). □

The following theorem summaries most of the basic elements needed in the study of the further described incidence structures.

Theorem 6.6. *Let (P, L) be a flag in the affine plane, then*

(i) (P, L) is incident with $q-1$ elements of $\mathcal{C}_1(q)$ if L is not a vertical (see Definition 4.2), else it is tangent to none of them;
(ii) (P, L) is incident with $q-1$ elements of $\mathcal{C}_2(q)$ if L is neither vertical nor horizontal (see Definition 4.2), else it is tangent to none of them;
(iii) (P, L) is always incident with $q-1$ elements of $\mathcal{C}_3(q)$.

Proof. Step 1. First suppose that L is vertical, i.e. equal to (PP_∞) (see Notation 3.2) and assume that there exists $C \in \mathcal{C}_1(q)$ which is tangent to $L = (PP_\infty)$ at P. Let $\overline{C}$ be the projective closure of C. By definition, $\overline{C}$ contains P_∞. Then, $m_P(\overline{C}, L) \geq 2$ and $m_{P_\infty}(\overline{C}, L) \geq 1$, which contradicts Bézout's Theorem since $\deg(\overline{C}).\deg(L) = 2$.

Step 2. Suppose that L is non-vertical. Then, the set of conics containing P_∞ and P and which are respectively tangent to L_∞ and L at these points is the linear system $\Lambda_2(P, P_\infty, L, L_\infty)$ (see Lemma 3.5 and Remark 3.6). It has dimension 1, thus has $q+1$ elements defined over $\mathbf{F}_q$ and from Lemma 3.5, they are all smooth but two of them.

One proves (ii) and (iii), by the very same manner using Lemma 3.3 instead of 3.5. □

7. The new incidence structures

In this section we describe three incidence structures obtained from the surface $\mathbf{B}$ and the $\mathcal{C}_i(q)$'s.

7.1. **Description.**

Definition 7.1. The sets $\widetilde{\mathcal{C}_1}(q), \widetilde{\mathcal{C}_2}(q)$ and $\widetilde{\mathcal{C}_3}(q)$ are the respective sets of strict transforms of the elements of $\mathcal{C}_1(q), \mathcal{C}_2(q)$ and $\mathcal{C}_3(q)$ on $\mathbf{B}$.

Recall that $\mathcal{E}$ denotes the set of all exceptional divisors on $\mathbf{B}$.

Definition 7.2 (Incidence structure $\mathcal{I}_1(q)$)**.** We denote by $\mathcal{I}_1(q)$ the incidence structure whose set of points $\mathcal{P}_1(q)$ is the set of rational points of $\mathbf{B}$ corresponding to the flags (P, L) of $\mathbf{A}^2$ such that L is not a vertical and whose set of blocks $\mathcal{B}_1(q)$ is $\widetilde{\mathcal{C}_1}(q) \cup \mathcal{E}$.

Definition 7.3 (Incidence structure $\mathcal{I}_2(q)$)**.** We denote by $\mathcal{I}_2(q)$ the incidence structure whose set of points $\mathcal{P}_2(q)$ is the set of rational points of $\mathbf{B}$ corresponding to the flags (P, L) of $\mathbf{A}^2$ such that L is neither vertical nor horizontal and whose set of blocks $\mathcal{B}_2(q)$ is $\widetilde{\mathcal{C}_2}(q) \cup \mathcal{E}$.

Definition 7.4 (Incidence structure $\mathcal{I}_3(q)$)**.** We denote by $\mathcal{I}_3(q)$ the incidence structure whose set of points $\mathcal{P}_3(q)$ is the set of all rational points of $\mathbf{B}$ and whose set of blocks $\mathcal{B}_3(q)$ is $\widetilde{\mathcal{C}_3}(q) \cup \mathcal{E}$.

Remark 7.5 (Why adding the exceptional divisors?). In the above-described incidence structures, one can wonder why we chose to add the exceptional divisors in the block sets. Actually the incidence structures would have been regular without these blocks. However, by adding a negligible number of blocks (q^2 additional blocks in a set containing already $q^3 - q^2$ blocks), one gets codes with a twice larger minimum distance, see Remark 8.6.

7.2. **Basic properties of the incidence structures.**

Notation 7.6. (1) In what follows, any element of $\mathcal{E}$, (i.e. any exceptional divisor on $\mathbf{B}$) is denoted by E_P, where P is the corresponding blown–up point (i.e. the image of E_P by the canonical map $\mathbf{B} \to \mathbf{A}^2$).

(2) Using Lemma 6.5, any rational point of $\mathbf{B}$ is represented as a flag (P, L) on $\mathbf{A}^2$. We allow ourselves the notation "$(P, L) \in \mathbf{B}$". In particular, we have $(P, L) \in E_P$.
(3) From now on, an element of $\widetilde{\mathcal{C}}_i(q)$ is denoted by $\widetilde{C}$, where C is the affine conic whose strict transform is $\widetilde{C}$.

Theorem 7.7. *The incidence structures $\mathcal{I}_1(q), \mathcal{I}_2(q)$ and $\mathcal{I}_3(q)$ satisfy*

(i) $\sharp\mathcal{B}_1(q) = q^3$ *and* $\sharp\mathcal{P}_1(q) = q^3$ *;*
(ii) $\sharp\mathcal{B}_2(q) = q^3$ *and* $\sharp\mathcal{P}_2(q) = q^2(q-1)$*;*
(iii) $\sharp\mathcal{B}_3(q) = q^3$ *and* $\sharp\mathcal{P}_3(q) = q^2(q+1)$*.*
(iv) any point of $\mathcal{I}_1(q)$ (resp. $\mathcal{I}_2(q)$, resp. $\mathcal{I}_3(q)$) is incident with exactly q blocks;
(v) any block of $\mathcal{B}_1(q)$ (resp. $\mathcal{B}_2(q)$, resp. $\mathcal{B}_3(q)$) is incident with exactly q (resp. $q-1$, resp. $q+1$) points.
(vi) any two distinct points of $\mathcal{I}_1(q)$ (resp. $\mathcal{I}_2(q)$, resp. $\mathcal{I}_3(q)$) are incident with at most 1 common block.

Proof. From Proposition 5.10, the sets $\mathcal{C}_1(q), \mathcal{C}_2(q), \mathcal{C}_3(q)$ and hence the sets $\widetilde{\mathcal{C}}_1(q), \widetilde{\mathcal{C}}_2(q)$, $\widetilde{\mathcal{C}}_3(q)$ have cardinal $q^3 - q^2$. Since $\mathcal{E}$ has cardinal q^2, this proves that the block sets $\mathcal{B}_i(q)'s$ have cardinal q^3. From Lemma 6.5, the surface $\mathbf{B}$ has $q^2(q+1)$ rational points. To construct $\mathcal{P}_1(q)$ (resp. $\mathcal{P}_2(q)$) we remove 1 (resp. 2) rational point(s) per exceptional divisor, corresponding to the vertical direction (resp. vertical and horizontal directions). Consequently, these sets have respectively q^3 and $q^2(q-1)$ elements. To construct $\mathcal{P}_3(q)$ we take all the rational points of $\mathbf{B}$, thus this set has cardinal $q^2(q+1)$. This proves (i), (ii) and (iii).

A point of $\mathcal{I}_1(q)$ (resp. $\mathcal{I}_2(q)$, resp. $\mathcal{I}_3(q)$) corresponds to a flag (P, L) of $\mathbf{A}^2$ such that L is a non-vertical line (resp. is a neither vertical nor horizontal line, resp. is a line) of $\mathbf{A}^2$. From Theorem 6.6(i) (resp. (ii), resp. (iii)), such a flag is incident with exactly $q-1$ conics of $\mathcal{C}_i(q)$ and hence the corresponding point of $\mathbf{B}$ is in $q-1$ elements of $\widetilde{\mathcal{C}}_i(q)$. In addition, this point also lies in the exceptional divisor E_P. Therefore, the point $(P, L) \in \mathbf{B}$ is incident with q blocks in $\mathcal{B}_1(q)$ (resp. $\mathcal{B}_2(q)$, resp. $\mathcal{B}_3(q)$). This proves (iv).

The number of points incident to a block of the form $\widetilde{\mathcal{C}}_i(q)$ is a straightforward consequence of Proposition 5.11 together with Lemma 2.17. For the blocks in $\mathcal{E}$, first recall that an exceptional divisor is isomorphic to a projective line and hence has $q+1$ rational points. Moreover, to construct $\mathcal{P}_1(q)$ (resp. $\mathcal{P}_2(q)$) we take all the flags but those of the form (P, L) where L is vertical (resp. either vertical or horizontal). Thus, we remove 1 (resp. 2) rational point to each exceptional divisor. Consequently, any block in $\mathcal{B}_1(q)$ (resp. $\mathcal{B}_2(q)$, resp. $\mathcal{B}_3(q)$) from $\mathcal{E}$ is incident with q (resp. $q-1$, resp. $q+1$) points in $\mathcal{P}_1(q)$ (resp. $\mathcal{P}_2(q)$, resp. $\mathcal{P}_3(q)$). This proves (v).

Let $i \in \{1, 2, 3\}$. Let $(P, L), (P', L')$ be two distinct points of $\mathcal{P}_i(q)$. First, assume that they both lie in the same exceptional divisor E_P of $\mathbf{B}$, i.e. $P = P'$. Then, E_P is the only block containing both of them. Indeed, no other exceptional divisor contains them from Remark 6.2. Moreover, by definition, elements of $\mathcal{C}_i(q)$ are smooth. Therefore, from Proposition 2.16 (i), a curve $\widetilde{C} \in \widetilde{\mathcal{C}}_i(q)$ meets E at at most one point and hence cannot contain both points (P, L) and (P, L'). Now, suppose that the points $(P, L), (P', L')$ lie in distinct exceptional divisors (i.e. $P \neq P'$). Then, there is at most one element of $\widetilde{\mathcal{C}}_i(q)$ containing both of them. Indeed, assume that there exists two distinct such curves $\widetilde{C}, \widetilde{D} \subset \widetilde{\mathcal{C}}_i(q)$ both containing the points (P, L) and (P', L'). Then, from Proposition 2.16 (iii), the curves C, D both contain the points P, P' and meet with multiplicity

≥ 2 at both them. Therefore, these curves meet at 4 points of $\mathbf{A}^2$ counted with their multiplicities, which contradicts Lemma 5.12. This proves (vi). □

7.3. **Girths.**

Theorem 7.8 (Girth of the incidence graph)**.** *Let $\gamma(i,q)$ be the girth of the incidence graph of the incidence structure $\mathcal{I}_i(q)$. We have*

$$\gamma(1,q) = \begin{cases} 6 & if \quad q \quad even \\ 8 & if \quad q \quad odd \end{cases}$$

$$\gamma(2,q) = \begin{cases} 8 & if \quad q \quad even \\ 6 & if \quad q \quad odd \end{cases}$$

$$\gamma(3,q) = \begin{cases} 8 & if \quad q \quad even \\ 6 & if \quad q \quad odd \end{cases} .$$

Remark 7.9. The incidence graph of an incidence structure is a bipartite graph. Therefore, its cycles have even length. Thus, the girth of such graphs is even.

To prove Theorem 7.8, we need Lemma 7.11, Lemma 7.12, Proposition 7.13 and Lemma 7.16.

Definition 7.10 ($(C3)$ configurations)**.** A triple $\{C_a, C_b, C_c\}$ of distinct plane affine conics is said to be a $(C3)$ configuration if

(i) any two of the conics meet at only one point in $\mathbf{A}^2$ and are tangent at this point;
(ii) in $\mathbf{A}^2$ we have $C_a \cap C_b \cap C_c = \emptyset$.

See Figure 3 for an illustration.

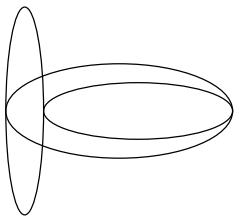

FIGURE 3. A triple of conics in $(C3)$ configuration

Lemma 7.11 (The geometric structure of 6–cycles)**.** *The incidence graph of $\mathcal{I}_1(q)$ (resp. $\mathcal{I}_2(q), \mathcal{I}_3(q)$) has cycles of length 6 if and only if three elements of $\mathcal{C}_1(q)$ (resp. $\mathcal{C}_2(q), \mathcal{C}_3(q)$) are in $(C3)$ configuration.*

Proof. Obviously, a triple of conics in $(C3)$ configuration yields a cycle of length 6 in the incidence graph.

Conversely, assume there is a cycle of length 6 in the incidence graph of $\mathcal{I}_i(q)$. Then, there are three blocks $B_a, B_b, B_c \in \mathcal{B}_i(q)$ together with three points $(P_{bc}, L_{bc}), (P_{ac}, L_{ac}), (P_{ab}, L_{ab}) \in \mathcal{P}_i(q)$ such that (P_{bc}, L_{bc}) (resp. (P_{ac}, L_{ac}), resp. (P_{ab}, L_{ab})) is incident with B_b and B_c (resp. B_a and B_c, resp. B_a and B_b). From Remark 6.2, two exceptional divisors (blocks in $\mathcal{E}$) have no common point in $\mathcal{P}_i(q)$. Therefore, at least two of the B_i's, say B_a, B_b are not in $\mathcal{E}$ and hence are of the form $\widetilde{C}_a, \widetilde{C}_b$ with $C_a, C_b \in \mathcal{C}_i(q)$. Let us prove that B_c cannot be an exceptional divisor. If it was, since points (P_{bc}, L_{bc}) and (P_{ac}, L_{ac}) are both incident with B_c, we would have $P_{bc} = P_{ac}$. In addition, since

$B_a = \widetilde{C}_a$ and $B_b = \widetilde{C}_b$ are both incident with (P_{ab}, L_{ab}), from Proposition 2.16 (iii), the plane curves C_a and C_b meet at least "twice" at P_{ab} (i.e. have a common tangent line L_{ab} at this point). They also meet at $P_{bc} = P_{ac}$, which contradicts Lemma 5.12.

Therefore, B_a, B_b, B_c are curves of the form $\widetilde{C}_a, \widetilde{C}_b$ and $\widetilde{C}_c$ and C_a, C_b (resp. C_a, C_c, resp. C_b, C_c) meet "twice" at P_{ab} (resp. P_{ac}, resp. P_{bc}) i.e. have a common tangent line L_{ab} (resp L_{ac}, resp. L_{bc}) at this point. This means that the affine conics C_a, C_b, C_c are in $(C3)$ configuration. □

Lemma 7.12 (Criterion for the non-existence of $(C3)$ configurations)**.** *Let $i \in \{1, 2, 3\}$. Let (P, L) be an element of $\mathcal{P}_i(q)$ (i.e. a flag such that L is a non-vertical line, resp. a neither vertical nor horizontal line, resp. a line). If for all $C \in \mathcal{C}_i(q)$ such that $P \notin C$, there exists at most one conic $D \in \mathcal{C}_i(q)$ incident with (P, L) and such that C, D are incident with a common flag $(P', L') \in \mathcal{P}_i(q)$, then no three elements of $\mathcal{C}_i(q)$ are in $(C3)$ configuration.*

Proof. Assume that there exists a triple $C_a, C_b, C_c \in \mathcal{C}_i(q)$ of conics in $(C3)$ configuration. Let (P_{ab}, L_{ab}) be the flag such that $P \in C_a \cap C_b$ and $L_{ab} = T_{P_{ab}} C_a = T_{P_{ab}} C_b$. Applying a suitable automorphism of the plane (see Lemma 5.13), one can assume that $(P_{ab}, L_{ab}) = (P, L)$. By definition of $(C3)$ configurations, $P \notin C_c$ and there are two distinct curves (namely C_a and C_b) incident with (P, L) and having a common flag with C_c. This contradicts the assumption of the statement. □

Proposition 7.13. *Let (P, L) be a flag in $\mathcal{P}_i(q)$ and C be an element of $\mathcal{C}_i(q)$ such that $P \notin C$. Denote by $\kappa_i(q, P, L, C)$ the maximum number of elements $C' \in C_i(q)$ such that C' is incident with (P, L) and C, C' are incident with a common flag $(P', L') \in \mathcal{P}_i(q)$.*

If q is even,	$\kappa_1(q, P, L, C) = q - 2$	$\kappa_2(q, P, L, C) = 1$	$\kappa_3(q, P, L, C) = 1$
If q is odd,	$\kappa_1(q, P, L, C) = 1$	$\kappa_2(q, P, L, C) \leq 2$	$\kappa_3(q, P, L, C) \leq 4$.

Remark 7.14. From Lemma 7.12, if $\kappa(q, P, L, C) \leq 1$ for all P, L, C such that $P \notin C$, then no 3 elements of $\mathcal{C}_i(q)$ are in $(C3)$ configuration. From Lemma 7.11, such a condition also entails that the incidence graph of $\mathcal{I}_i(q)$ has no cycles of length 6.

Proof of Proposition 7.13. Step 1. For $i = 1$. From Lemma 5.13, without loss of generality, one can choose (P, L) such that $P = (0, 0)$ and $L = \{y = 0\}$. A curve $C \in \mathcal{C}_1(q)$ avoiding P has an equation of the form (see Proposition 5.6):

$$(C): \quad y = ax^2 + bx + c, \text{ with } a \neq 0 \text{ and } c \neq 0.$$

A curve $C_t \in \mathcal{C}_1(q)$ incident with (P, L) has an equation of the form

$$(C_t): \quad y = tx^2, \text{ where } t \neq 0.$$

A point P of intersection of C and C_t has coordinates satisfying both equations. Thus, its x–coordinate satisfies

$$(a - t)x^2 + bx + c = 0 \tag{1}$$

The curves C and C_t have a common tangent at P if they meet with multiplicity 2 at this point. It happens if equation (1) has a double root.

- **If q is even** then (1) has a double root if and only if $a \neq t$ and $b = 0$. Therefore, if $b = 0$, then C shares a common flag with any curve C_t, with $t \neq 0$ and $t \neq a$. Else it does not share a common flag with any of the C_t. This yields $\kappa_1(q, P, L, C) = q - 2$.
- **If q is odd** then (1) has a double root if and only if $a \neq t$ and its discriminant vanishes. Since $c \neq 0$, it discriminant $\Delta(t) = b^2 - 4(a - t)c$ is a polynomial of degree 1 in t which vanishes for one value of t. This entails $\kappa_1(q, P, L, C) = 1$.

Step 2. For $i = 2$. We choose (P, L) with $P = (0, 0)$ and $L = \{y = x\}$. A curve $C \in \mathcal{C}_2(q)$ avoiding P has an equation of the form (see Proposition 5.7):

$$(C) : xy = ax + by + c \quad \text{where } c \neq ab \text{ and } c \neq 0.$$

A curve $C_t \in \mathcal{C}_2(q)$ incident with (P, L) has an equation of the form

$$(C_t) : \quad xy = t(x + y) \quad \text{where } t \neq 0.$$

Notice that no point of C_t has its x–coordinate equal to t. Thus, from now on one can assume that $x \neq t$. The equation of C_t can then be re-written as $y = \frac{xt}{x-t}$. Using this substitution in the equation of C, a quick computation gives

$$(t - a)x^2 + (t(a - b) - c)x + ct = 0 \tag{2}$$

- **If q is even** then (2) has a double root if and only if $a \neq t$ and $t(a + b) + c = 0$. It happens for one value of t if $a \neq b$ and does not happens if $a = b$. This yields $\kappa_2(q, P, L, C) = 1$.
- **If q is odd** then (2) has a double root if and only if $a \neq t$ and if its discriminant vanishes. Its discriminant $\Delta(t) = (t(a - b) - c)^2 - 4ct(t - a)$ is a polynomial of degree ≤ 2 in t and hence vanishes for at most 2 values of t. This yields $\kappa_2(q, P, L, C) \leq 2$.

Step 3.a. For $i = 3$ and q even. We choose (P, L) as in Step 1. Using the same notations as in the previous steps we get

$$(C) : \quad x^2 + xy + \beta y^2 = ax + by + c, \quad \text{where, } c \neq 0 \text{ and } c \neq a^2 + b^2 + ab.$$

and

$$(C_t) : \quad x^2 + xy + \beta y^2 = tx, \quad \text{where } t \neq 0.$$

If $a = t$ and $b = 0$, then the polynomial system has no solution since $c \neq 0$. Else if $a = t$ and $b \neq 0$, then after substitution we see that C_t is tangent to C at some point if and only if the polynomial $b^2x^2 + b(c + bt)x + \beta c^2$ has a double root. It happens only if $c = bt$.

If $a \neq t$, then after substitutions, one sees that C_t meets C at a point of $\mathbf{A}^2$ with multiplicity 2 if and only if the polynomial

$$(b^2 + (b + \beta(a + t))(a + t))y^2 + (a + t)(c + bt)y + c^2 + ct(a + t)$$

has a double root. Since $a \neq t$, it happens only if $c = bt$.

Finally C_t and C meet with multiplicity 2 if and only if $c = bt$. Since $c \neq 0$, this is possible for one value of t when $b \neq 0$. This yields $\kappa_3(q, P, L, C) = 1$.

Step 3.b. For $i = 3$ and q odd. We choose (P, L) as in Step 1, and get

$$(C) : \quad x^2 - \beta y^2 = ax + by + c, \text{ with } c \neq 0 \text{ and } c \neq \frac{b^2}{4\beta} - \frac{a^2}{4},$$

and

$$(C_t) : \quad x^2 - \beta y^2 = tx \quad \text{where } t \neq 0.$$

The coordinates of a point at the intersection of C_c and C_t satisfy $(a - t)x + by + c = 0$ which can be rewritten as $x = \frac{c}{a-t} - \frac{by}{a-t}$. Substituting this relation in the equation of C_t and after a quick computation, we get

$$(b^2 - \beta^2)y^2 + (tb(a - t) - 2bc)y + c^2 - c(a - t) = 0$$

The discriminant of this polynomial has degree ≤ 4 in t. Thus, $\kappa_3(q, P, L, C) \leq 4$. □

Remark 7.15. In the above proof, Step 1 for q even entails that for a fixed flag (P, L), there are exactly $(q-1)^2$ curves $C \in \mathcal{C}_1(q)$ avoiding P and for which there exists curves $C_t \in \mathcal{C}_1(q)$ incident with (P, L) and tangent to C at some point $P \in \mathbf{A}^2$. Moreover, for such a curve C there are exactly $q-2$ curves C_t tangent to C at some $P \in \mathbf{A}^2$.

Lemma 7.16 (The structure of 8–cycles)**.** *Given a 4–tuple of blocks of $\mathcal{B}_i(q)$ yielding a cycle of length 8 in the incidence graph of $\mathcal{I}_i(q)$, the corresponding curves satisfy one of the following configuration.*

(i) Two of the blocks are exceptional divisors E_P and E_Q, with $P, Q \in \mathbf{A}^2(\mathbf{F}_q)$ and the two other ones are curves $\widetilde{C}, \widetilde{D} \in \widetilde{\mathcal{C}}_i(q)$ such that the corresponding affine plane conics C, D both contain P and Q.

(ii) One of the blocks is an exceptional divisor E_P and the three other ones are curves $\widetilde{C}_1, \widetilde{C}_2$ and $\widetilde{C}_3$ such that $C_1, C_2 \ni P$ and C_3 is incident with a common flag $(P_{13}, L_{13}) \in \mathcal{P}_i(q)$ with C_1 and to another common one $(P_{23}, L_{23}) \in \mathcal{P}_i(q)$ with C_2.

(iii) None of the blocks are exceptional divisors, they are curves $\widetilde{C}_1, \dots, \widetilde{C}_4$. Moreover, there are 4 flags $(P_{13}, L_{13}), (P_{14}, L_{14}), (P_{23}, L_{23}), (P_{24}, L_{24}) \in \mathcal{P}_i(q)$ such that the P_{ij}'s are distinct and C_i, C_j are both incident with (P_{ij}, L_{ij}).

These three possible configurations are represented in figure 4.

Proof. Since two distinct exceptional divisors on $\mathbf{B}$ have no common point (see Remark 6.2), a 4–tuple of blocks yielding an 8–cycle involves at most two exceptional divisors. The remaining curves are strict transforms of conics in $\mathcal{C}_i(q)$. Verifications are left to the reader that these conics should satisfy these conditions. □

Now, using Lemmas 7.11, 7.12, 7.16 and Proposition 7.13, we can proceed to the proof of Theorem 7.8.

Proof of Theorem 7.8. Step 1. Theorem 7.7 (vi) entails the non-existence of cycles of length 4 in the incidence graph. From Remark 7.9, the girth is even and hence $\gamma(i, q) \geq 6$ for all pairs (i, q).

Step 2. Cycles of length 8 always exist in the incidence graph: obviously, the case (i) of Lemma 7.16 always happens. Thus, $\gamma(i, q) \leq 8$ for all i and all q.

Step 3. Proposition 7.13 together with Remark 7.14 entail that the incidence graph of $\mathcal{I}_i(q)$ has no 6–cycles if q odd and $i = 1$ and if q even and $i = 2$ or 3. Therefore, in these situations, $\gamma(i, q) = 8$.

Step 4. For the remaining situations, the girth of the incidence graph is actually 6. To prove it, we explicit triples of elements of $\mathcal{C}_i$ which are in $(C3)$ configuration. In these three examples, the curves are denoted by C_a, C_b, C_c and the flags by $(P_{ab}, L_{ab}), (P_{ac}, L_{ac})$ and (P_{bc}, L_{bc}). Verifications are left to the reader.

Step 4.1. A triple of elements of $\mathcal{C}_1(q)$ with q even in $(C3)$ configuration. Let q be even. By assumption, $q \geq 4$ (see §4). Then, there exists $\eta \in \mathbf{F}_q$ such that $\eta \neq 0$ and $\eta \neq 1$. A $(C3)$ configuration is given by

$$\begin{array}{lllll} (C_a): & y = x^2 & & P_{ab} = (0,0) & L_{ab}: \ y = 0 \\ (C_b): & y = \eta x^2 & ; & P_{ac} = (\eta^{-1/2}, \eta^{-1}) \ ; & L_{ac}: \ y = \eta^{-1} \\ (C_c): & y = (\eta+1)x^2 + 1 & & P_{bc} = (1, \eta) & L_{bc}: \ y = \eta. \end{array}$$

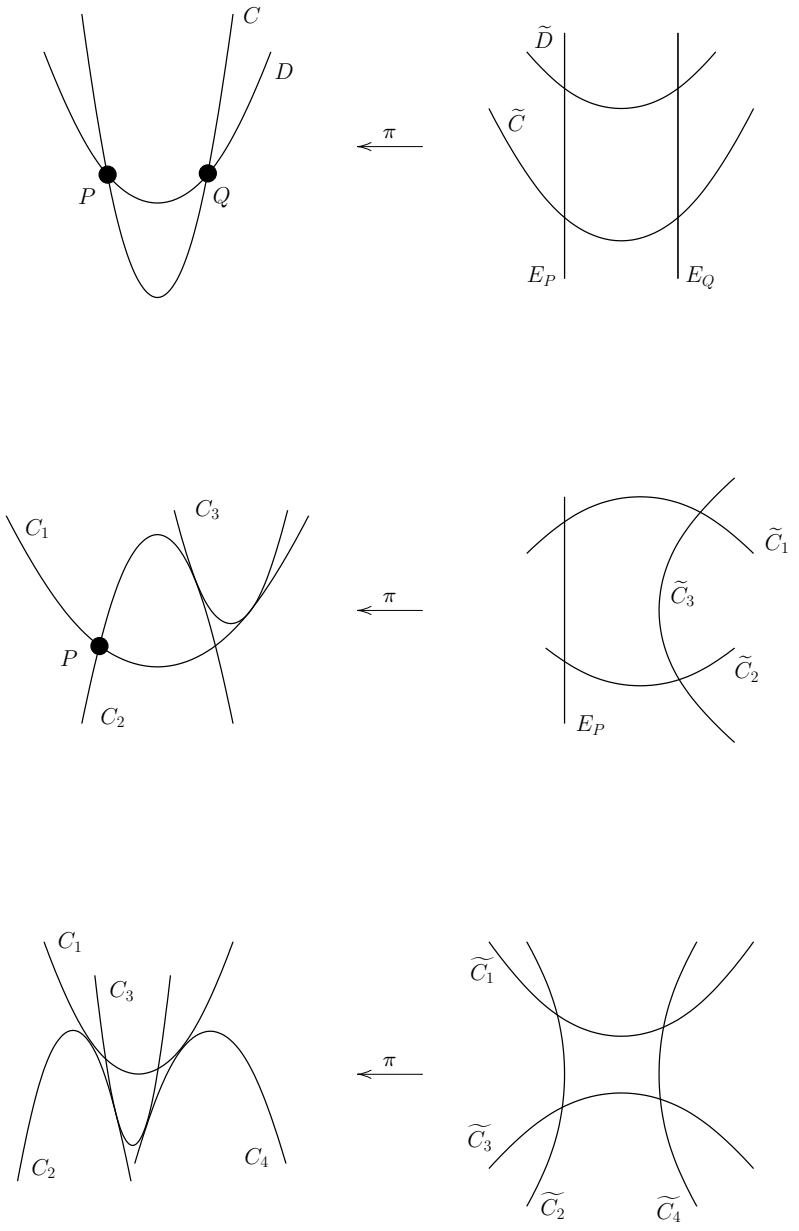

FIGURE 4. The three possible configurations of curves yielding 8–cycles. Left hand pictures represent the curves in $\mathbf{A}^2$ and right hand ones the corresponding curves in $\mathbf{B}$ (π denotes the Blow–up map).

Step 4.2. A triple of elements of $\mathcal{C}_2(q)$ with q odd in $(C3)$ configuration.

$$\begin{array}{lllllllllll} (C_a): & xy & = & x+y & & P_{ab} & = & (0,0) & & L_{ab}: & y & = & -x \\ (C_b): & xy & = & -x-y\ ; & & P_{ac} & = & (2,2) & ; & L_{ac}: & y & = & -x+4 \\ (C_c): & xy & = & 4 & & P_{bc} & = & (-2,-2) & & L_{bc}: & y & = & -x-4. \end{array}$$

Step 4.3. A triple of elements of $\mathcal{C}_3(q)$ with q odd in $(C3)$ configuration.

$$\begin{array}{llllllllllll} (C_a): & x^2-\beta y^2 & = & x & & P_{ab} & = & (0,0) & & L_{ab}: & y & = & 0 \\ (C_b): & x^2-\beta y^2 & = & -x\ ; & & P_{ac} & = & (1,0) & ; & L_{ac}: & y & = & 1 \\ (C_c): & x^2-\beta y^2 & = & 1, & & P_{bc} & = & (-1,0) & & L_{bc}: & y & = & -1. \end{array}$$

□

7.4. **Number of small cycles.** In the previous sub-section it is proved that the incidence graph of $\mathcal{I}_i(q)$ has either girth 6 or girth 8. In both cases we compute or bound above the number of cycles of minimum length.

Theorem 7.17 (Number of cycles of length 6)**.** *For incidence structures $\mathcal{I}_i(q)$ whose incidence graph has girth 6, let $N_6(i,q)$ be the number of 6–cycles. We have*

$$N_6(i,q) \left\{ \begin{array}{lll} = & q^3(q-1)^3(q-2)/6 & \text{if } i=1 \text{ and } q \text{ is even} \\ \leq & q^2(q-1)(q^3-q^2-q)/3 & \text{if } i=2 \text{ and } q \text{ is odd} \\ \leq & 2q^4(q+1)(q-2) & \text{if } i=3 \text{ and } q \text{ is odd} \end{array} \right. .$$

In particular we always have $N_6(i,q)=\mathcal{O}(q^6)$.

Proof. From Lemma 7.11, the number of 6–cycles equals the number of non-ordered triples of conics in $(C3)$ configuration. For that, we compute the number of **ordered** such triples and divide this number by 6.

Step 1. For $\mathcal{C}_1(q)$, with q even. We choose a flag (P,L) and look for the number of ordered triples C_a, C_b, C_c in $(C3)$ configuration and such that C_a, C_b are both incident with (P,L).

Remark 7.15 entails that there are $(q-1)^2$ choices for C_c for which one can find C_a, C_b both incident with (P,L) and such that C_a, C_b, C_c are in $(C3)$ configuration. We have:

- $(q-1)^2$ choices for C_c;
- $(q-1)$ choices for C_a;
- $(q-2)$ choices for C_b.

Since we also have $\sharp\mathcal{I}_1(q)=q^3$ choices for (P,L), this yields $q^3(q-1)^3(q-2)$ ordered triples of conics in $(C3)$ configuration. Thus, there are $q^3(q-1)^3(q-2)/6$ non-ordered triples.

Step 2. For $\mathcal{C}_2(q)$ with q odd. As in the previous step, we choose a flag (P,L) and look for triples C_a, C_b, C_c in $(C3)$ configuration such that C_a, C_b are both incident with (P,L). We choose an arbitrary curve $C_c \in \mathcal{C}_2(q)$ avoiding P. Without loss of generality, one can assume that $P=(0,0)$ and hence C_c has an equation of the form $xy=ax+by+c$ with $c\neq ab$ and $c\neq 0$. This yields q^3-q^2-q possible choices for C_c. Moreover, from Proposition 7.13, there are at most 2 curves in $\mathcal{C}_2(q)$ which are incident with (P,L) and have a common flag with C_c. Thus, we have

- $\sharp\mathcal{P}_2(q) = q^2(q-1)$ choices for (P,L);
- q^3-q^2-q choices for C_c;
- at most 2 choices for C_a;
- at most 1 choice for C_b.

This yields at most $2q^2(q-1)(q^2-q^2-q)$ ordered triples and hence at most $q^2(q-1)(q^3-q^2-q)/3$ non-ordered triples.

Step 3. For $\mathcal{C}_3(q)$ with q odd. The approach is almost the same as that of the previous step. Choose (P,L) and C_c avoiding P. Without loss of generality, one can assume that $P=(0,0)$ and C_c has an equation of the form $x^2-\beta y^2=ax+by+c$ with $c\neq 0$ and

$c \neq \frac{b^2}{4\beta} - \frac{a^2}{4}$. Since β is a non-square in $\mathbf{F}_q$, the expression $\frac{b^2}{4\beta} - \frac{a^2}{4}$ is nonzero of all (a, b). This entails that there are exactly $q^2(q-2)$ possible choices for C_c.

As previously, one applies Proposition 7.13. We have

- $\sharp\mathcal{P}_3(q) = q^2(q+1)$ choices for (P, L);
- $q^2(q-2)$ choices for C_c;
- at most 4 choices for C_a;
- at most 3 choices for C_b.

This yields at most $12q^4(q+1)(q-2)$ ordered triples and hence at most $2q^4(q+1)(q-2)$ non-ordered triples. □

To conclude the present section we state a result on the number of 8–cycles. Such a result can be obtained by counting the number of configurations describes in Lemma 7.16. By counting one can obtain upper bounds on the number of these cycles. However the obtained formulas are pretty rough. We thus chose to give only the asymptotic behaviour of this number of 8–cycles. Notice that the following theorem holds for even when the incidence graph has girth 6.

Theorem 7.18 (Number of cycles of length 8)**.** *The number $N_8(i, q)$ of 8–cycles of $\mathcal{I}_i(q)$ satisfies*

$$N_8(i, q) = \mathcal{O}(q^8).$$

Proof. We have to count the number of configurations described in Lemma 7.16 (see also Figure 4).

Configurations (i). There are q^2 rational points in $\mathbf{A}^2$. Thus, there are $\mathcal{O}(q^4)$ choices for P, Q. There are $\mathcal{O}(q)$ conics in $\mathcal{C}_i(q)$ containing P and Q. This yields $\mathcal{O}(q^2)$ choices for C, D. Finally, we have $\mathcal{O}(q^6)$ configurations (i).

Configurations (ii). There are $\mathcal{O}(q^3)$ choices for P and $\mathcal{O}(q^3)$ choices for C_3 (basically, "almost all" elements of $\mathcal{C}_i(q)$ avoid P). Thus, we have $\mathcal{O}(q^6)$ choices for the pair (P, C_3). Choose two lines L_1, L_2 containing P ($\mathcal{O}(q^2)$ choices), from Proposition 7.13 there is at most 1 element in $\mathcal{C}_i(q)$ incident with (P, L_1) (resp. (P, L_2)) and sharing a common flag with C_3. Thus, we have $\mathcal{O}(q^2)$ choices for C_1, C_2 and hence $\mathcal{O}(q^8)$ configurations (ii).

Configurations (iii). We have $\mathcal{O}(q^6)$ choices for C_1, C_3. Choose two points P, Q of C_1 ($\mathcal{O}(q^2)$ choices). From Proposition 7.13, there is at most one curve in $\mathcal{C}_i(q)$ which is incident with $(P, T_P C_1)$ (resp. $(Q, T_Q C_1)$). Thus there are $\mathcal{O}(q^8)$ configurations (iii). □

8. LDPC codes from the incidence structures

In this section, we construct and study LDPC codes from the previously defined incidence structures. Recall that, even if the incidence structures are constructed using geometry over an arbitrary finite field, the LDPC codes we construct are **binary**.

Codes are defined in §8.1. The weights and minimum distance of these codes are studied in §8.2. The dimension of such codes is discussed in §8.3.

8.1. **The codes.**

Definition 8.1. Let $i \in \{1, 2, 3\}$. The code $C(i, q)$ is the null space of the incidence matrix of $\mathcal{I}_i(q)$ having coefficients in $\mathbf{F}_2$.

Theorem 8.2. *The codes $C(1, q)$ (resp. $C(2, q)$, resp. $C(3, q)$) have a parity–check matrix of size $q^3 \times q^3$ (resp. $q^3 \times q^2(q-1)$ resp. $q^3 \times q^2(q+1)$). Moreover, these matrices are sparse and regular: each row has weight q (resp. $q-1$, resp. $q+1$) and each column has weight q.*

Proof. It is a straightforward consequence of Theorem 7.7. □

As a straightforward consequence of this Theorem, we obtain the length of these codes.

Corollary 8.3 (Length of $C(i,q)$)**.** *The length $n(i,q)$ of the code $C(i,q)$ is*

$$n(i,q) = \begin{cases} q^3 & \text{if } i=1; \\ q^2(q-1) & \text{if } i=2; \\ q^2(q+1) & \text{if } i=3. \end{cases}$$

8.2. **Weights and minimum distances.**

Lemma 8.4. *For all pair (i,q), the codewords of $C(i,q)$ have even weight.*

Proof. Consider the incidence matrix $H(i,q)$ of $\mathcal{I}_i(q)$. A row of this matrix, is a parity check given by some block in $\mathcal{B}_i(q)$. Consider the q^2 rows corresponding to the exceptional divisors. Any two of these rows have disjoint supports (Remark 6.2) and their sum is the vector $(1,\dots,1)$. It is an elementary exercise to prove that in a code whose parity–check matrix has a set of rows satisfying this property, the codewords always have even weight. □

Theorem 8.5 (Minimum distance of $C(i,q)$)**.** *The minimum distance d of $C(i,q)$ is*

$$d = 2q.$$

Caution. In what follows, we deal with codewords of $C(i,q)$. Since we deal with binary codes (even if they arise from geometries over odd characteristic fields), a codeword of $C(i,q)$ can be regarded as a set of flags $\{(P_1,L_1),\dots,(P_s,L_s)\}$ in $\mathcal{P}_i(q)$ such that the number of such flags incident with any block in $\mathcal{B}_i(q)$ is even. From now on, we frequently use the representation of codewords as sets of flags in $\mathcal{P}_i(q)$. Therefore, we allow ourselves to write $(P,L) \in c$ when c is a codeword in $C(i,q)$ and its coordinate corresponding to (P,L) equals 1.

Proof of $d \geq 2q$. Let $c \in C(i,q)$ be a nonzero codeword. Let $(P,L) \in \mathcal{P}_i(q)$ be a flag such that $(P,L) \in c$ (regarding c as a subset of $\mathcal{P}_i(q)$, see Caution above). Because of the block corresponding to the exceptional divisor E_P above P, there is another line L' such that $(P,L') \in \mathcal{P}_i(q)$ and $(P,L') \in c$.

Let $C_1,\dots,C_{q-1}$ (resp. $C'_1,\dots,C'_{q-1}$) be the conics in $\mathcal{C}_i(q)$ which are incident with (P,L) (resp. (P,L')). An example is represented in Figure 5

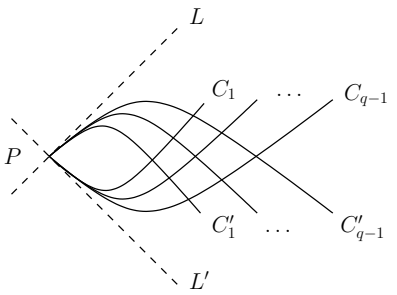

FIGURE 5. The curves $C_1,\dots,C_{q-1}$ and $C'_1,\dots,C'_{q-1}$

Using Lemma 5.12, one sees that any two of these $2q-2$ curves cannot share a common flag distinct from (P,L) or (P,L'). Indeed, two curves of the form C_i, C_j (resp. C'_i, C'_j)

have a common flag (P, L) (resp. (P, L')) and therefore do not meet at another point in $\mathbf{A}^2$. Two curves C_i, C'_j meet with multiplicity 1 at P and hence cannot meet with multiplicity > 1 at another point of $\mathbf{A}^2$.

Consequently, to satisfy all the parity checks, for all i there is at least one flag (P_i, L_i) (resp. P'_i, L'_i) incident with C_i (resp. C'_i), distinct from (P, L) and (P', L') and contained in c. Moreover, the previous claim on the non incidence relations between the C_i's and C'_i's entails that the flags $(P_1, L_1), \ldots, (P_{q-1}, L_{q-1}), (P'_1, L'_1), \ldots, (P'_{q-1}, L'_{q-1})$ are distinct to each other. This yields

$$w(c) \geq \sharp\left\{(P, L), (P, L'), (P_1, L_1), \ldots, (P_{q-1}, L_{q-1}), (P'_1, L'_1), \ldots, (P'_{q-1}, L'_{q-1})\right\} = 2q,$$

where $w(c)$ denotes the Hamming weight of c. □

There remains to prove the existence of codewords of weight $2q$. Their existence and the construction of some of them is given in Appendix B.

Remark 8.6. As noticed in Remark 7.5, if the exceptional divisors were not in the block sets of the incidence structure, then the minimum distance would be only $\geq q$. It can be proved be reproducing the reasoning of the above proof. Using the end of the proof in Appendix B, one can prove that the minimum distance would be actually q in that case.

8.3. **Dimension.** Unfortunately, we did not find formulas giving the dimension of the code $C(i, q)$ as a function of q. The dimension of the $C(i, q)$'s have been computed using Magma for all prime power $q \leq 32$ (see tables 1 to 6 pages 24 to 26). It turns out that the behaviour of these dimensions as a function of q depends on the parity of q. This claim is not surprising, we see for instance in Theorem 7.8, that the girth of their Tanner graph already depends on the parity of q. Therefore the parity of q has important consequences on the incidence structures.

Remark 8.7. It is worth noting that the length of $C(i, q)$ is of the form $q^3 + \mathcal{O}(q^2)$. Therefore, if the dimension of the code for q odd (resp. for q even) is a polynomial in q, then this polynomial has degree at most 3 and leading coefficient between 0 and 1.

Using the tables in §8.5 and Lagrange's interpolation, we get the following conjectures.

Conjecture 1. If q is odd, then

$$\dim C(1, q) = \frac{1}{2}q^3 - q^2 + \frac{3}{2}q - 1 \qquad \dim C(2, q) = \frac{1}{2}q^3 - \frac{5}{2}q^2 + \frac{9}{2}q - \frac{7}{2}.$$

The conjecture is satisfied for all odd prime power $5 \leq q \leq 31$.

A more surprising fact on these dimensions is the following one.

Lemma 8.8. *The dimension of $C(3, q)$ for q odd is not a polynomial in q.*

Proof. From remark 8.7, if the dimension is a polynomial, this polynomial has degree at most 3. Using Table 5 page 25 and interpolating the values for $q = 5, 7, 9, 11$, we obtain the polynomial $\frac{23}{48}q^3 - \frac{15}{16}q^2 - \frac{215}{48}q + \frac{239}{16}$. It is easy to check that this polynomial does not give the other computed values of the dimension. □

Looking at the calculations presented in §8.5, the codes $C(i, q)$ seem have asymptotic information rate $1/2$ when q is odd. This rate seems to be higher when q is even. Since the constructed parity–check matrices are almost square, they are redundant. Mostly, they have about twice more rows than necessary.

8.4. **Cycles of the Tanner graph.** An important criterion for the efficiency of LDPC codes is the girth of their Tanner graph and the number of small cycles. It is proved in Theorem 7.8 that the girth of their Tanner graphs are 6 or 8. Moreover, Theorem 7.17 asserts that if the girth is 6, then the number of small cycles is $\mathcal{O}(q^6)$ and hence $\mathcal{O}(n^2)$, where n denotes the length of the code. Theorem 7.18 asserts that the number of cycles of length 8 is $\mathcal{O}(q^8)$ and hence $\mathcal{O}(n^{8/3})$.

8.5. **Calculations.** We developed MAGMA programs producing the codes $C(i,q)$. These programs are available on `http://www.lix.polytechnique.fr/Labo/Alain.Couvreur/doc_rech/LDPC_codes.tar.gz`. Thanks to them we are able to calculate by computer the dimensions of the $C(i,q)$'s for $q \leq 32$. As seen in §7.3, the parity of q has an important influence on the incidence structure, and hence on the codes. Therefore, we present in distinct tables the cases q even and q odd.

q	Length	Number of Parity checks	Minimum distance	Girth	Dimension	Rate (approx.)
5	125	125	10	8	44	0,35
7	343	343	14	8	132	0,38
9	729	729	18	8	296	0,41
11	1331	1331	22	8	560	0,42
13	2197	2197	26	8	948	0,43
25	15625	15625	50	8	7224	0,46
31	29791	29791	62	8	13980	0,47

TABLE 1. The codes $C(1,q)$ for q odd.

q	Length	Number of Parity checks	Minimum distance	Girth	Dimension	Rate (approx.)
4	64	64	8	6	23	0,36
8	512	512	16	6	259	0,51
16	4096	4096	32	6	2615	0,63
32	32768	32768	64	6	24151	0,74

TABLE 2. The codes $C(1,q)$ for q even.

q	Length	Number of Parity checks	Minimum distance	Girth	Dimension	Rate (approx.)
5	100	125	10	6	19	0,19
7	294	343	14	6	77	0,22
9	648	729	18	6	199	0,31
11	1210	1331	22	6	409	0,34
13	2028	2197	26	6	731	0,36
25	15000	15625	50	6	6359	0,42
31	28830	29791	62	6	12629	0,44

TABLE 3. The codes $C(2,q)$ for q odd.

q	Length	Number of Parity checks	Minimum distance	Girth	Dimension	Rate (approx.)
4	48	64	8	8	11	0,23
8	448	512	16	8	176	0,39
16	3840	4096	32	8	2001	0,52
32	31744	32768	64	8	19594	0,62

TABLE 4. The codes $C(2, q)$ for q even.

q	Length	Number of Parity checks	Minimum distance	Girth	Dimension	Rate (approx.)
5	150	125	10	6	29	0,19
7	392	343	14	6	102	0,26
9	810	729	18	6	248	0,31
11	1452	1331	22	6	490	0,34
13	2366	2197	26	6	852	0,36
17	5202	4913	34	6	2032	0,39
25	16250	15625	50	6	7513	0,46
31	30752	29791	62	6	14431	0,47

TABLE 5. The codes $C(3, q)$ for q odd.

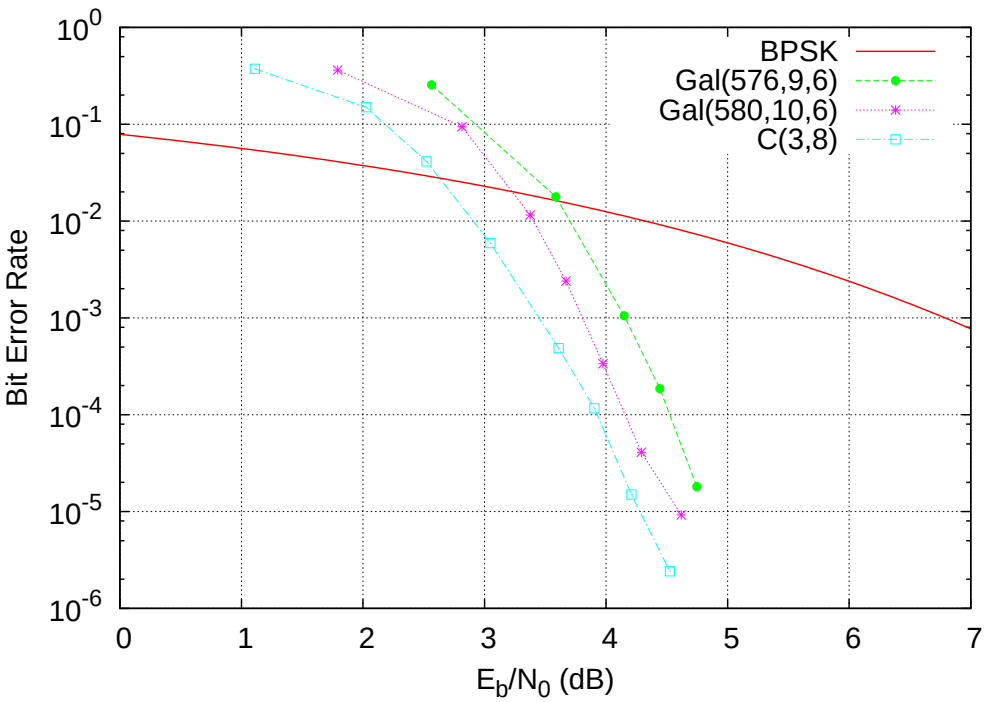

FIGURE 6. Decoding performances of the code $C(3, 8)$ (with parameters $[576, 233]$) and two Gallager codes, with respective row weights 9 and 10 and parameters $[576, 197]$ and $[580, 237]$.

q	Length	Number of Parity checks	Minimum distance	Girth	Dimension	Rate (approx.)
4	80	64	8	8	19	0,24
8	576	512	16	8	223	0,39
16	4352	4096	32	8	2223	0,51
32	33792	32768	64	8	21575	0,64

TABLE 6. The codes $C(3, q)$ for q even.

8.6. **Simulations on the Gaussian Channel.** Using the function `LDPCSimulate` of MAGMA, we have simulated the performances of some codes $C(i, q)$ on the Additive White Gaussian Noise Channel. We compare these results with the performances of regular Gallager codes having nearly the same rate and row weight. These results are presented in Figures 6, 7 and 8. The performances of our codes turn out to beat those of Gallager codes having similar length, rate and row weight.

8.6.1. *Details of the simulations.* All the bit error rates above 10^{-4} have been obtained after between 10^4 and 10^5 random tests. For Bit error rates under 10^{-4}, between 10^6 and 10^7 random tests are done. The number of iterations of the iterative decoding algorithm is set to 50 for the simulations presented in Figure 6 and to 500 for the simulations in Figures 7 and 8.

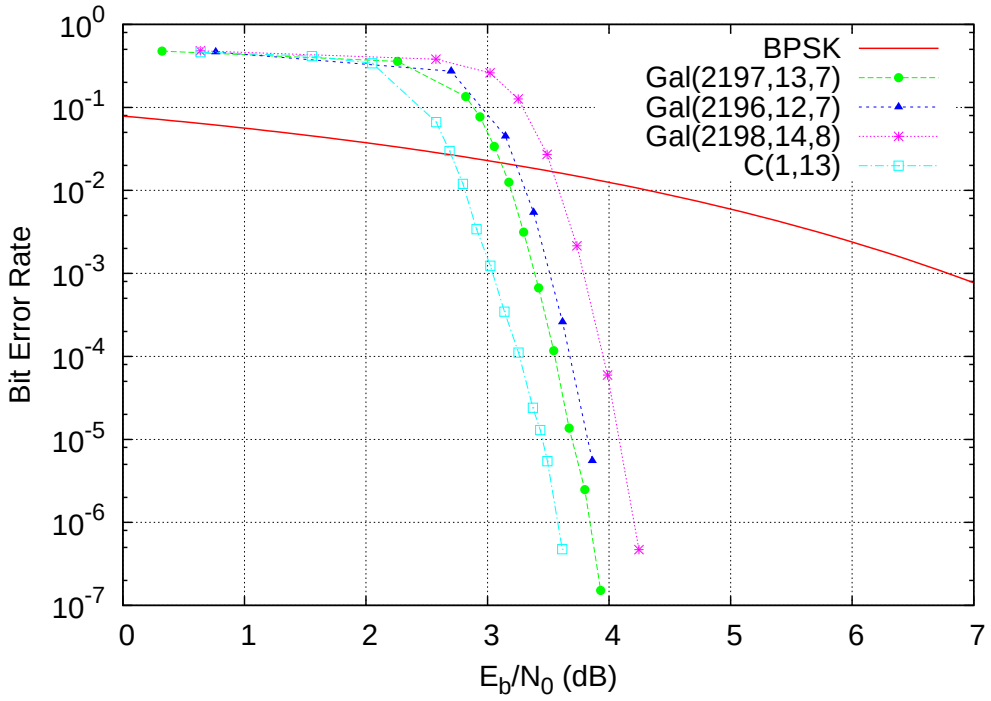

FIGURE 7. Decoding performances of the code $C(1, 13)$ (with parameters $[2197, 948]$) and three Gallager codes, with respective row weights 12, 13 and 14 and parameters $[2196, 921]$, $[2197, 1020]$ and $[2198, 949]$.

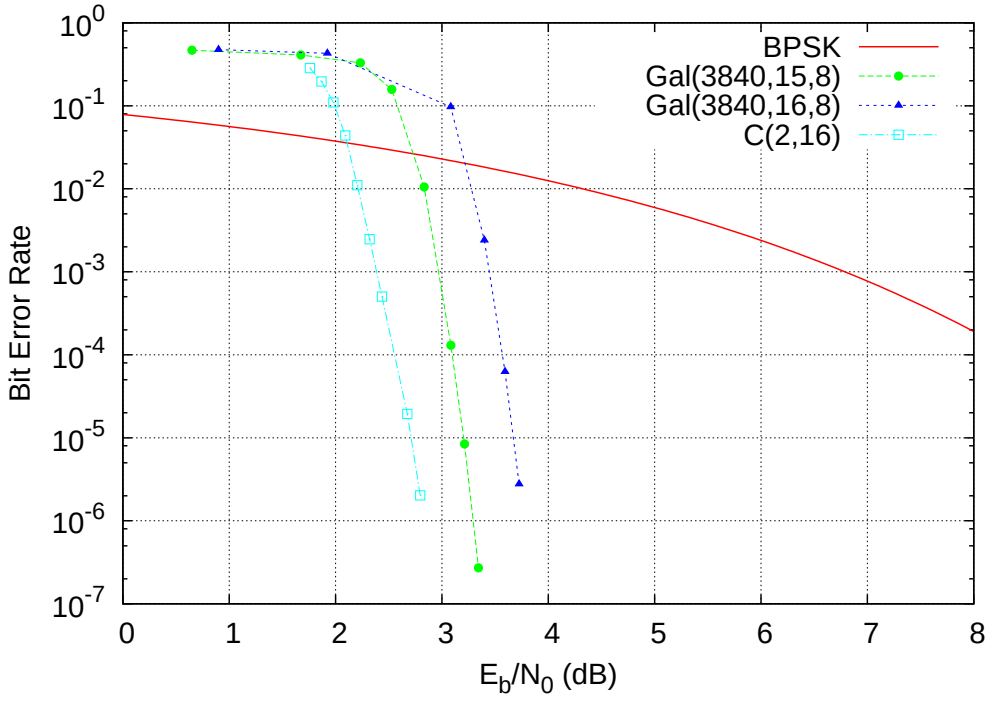

FIGURE 8. Decoding performances of the code $C(2, 16)$ (with parameters $[3840, 2001]$) and two Gallager codes, with respective row weights 15 and 16 and parameters $[3840, 2041]$ and $[3840, 1927]$.

APPENDIX A. AUTOMORPHISMS OF THE PLANE

Proof of Lemma 2.18 (1). Let $(P, \overline{P}, P_3, P_4)$ and $(Q, \overline{Q}, Q_3, Q_4)$ be two such 4–tuples. Obviously, there exists a unique $\sigma \in \mathbf{PGL}(3, \mathbf{F}_{q^2})$ sending $(P, \overline{P}, P_3, P_4)$ onto $(Q, \overline{Q}, Q_3, Q_4)$. Let us prove that σ is actually defined over $\mathbf{F}_q$, i.e. that $\bar{\sigma} = \sigma$, where $\bar{\sigma}$ denotes the conjugate of σ under the Frobenius action. Since Q_3 is rational, we have $Q_3 = \overline{Q}_3$ and hence $Q_3 = \sigma P_3 = \overline{\sigma P_3} = \bar{\sigma} P_3$. In the same way, we obtain $\bar{\sigma} P_4 = Q_4$. Moreover $\overline{\sigma P} = \overline{Q} = \bar{\sigma}\overline{P}$. By the same manner, we prove that $\bar{\sigma} P = Q$. By uniqueness of σ, we get $\sigma = \bar{\sigma}$ and hence $\sigma \in \mathbf{PGL}(3, \mathbf{F}_q)$. □

Proof of Lemma 2.18 (2). let (P_1, P_2, L_1, L_2) and (Q_1, Q_2, M_1, M_2) be two such 4–tuples. Choose two rational points P_1', P_2' such that $P_1' \in L_1$, $P_2' \in L_2$, $P_1' \notin L_2$ a $P_2' \notin L_1$. Choose two rational points Q_1', Q_2' satisfying the same conditions with respect to the triple (Q_1, Q_2, M_1, M_2). There exists a unique $\sigma \in \mathbf{PGL}(3, \mathbf{F}_q)$ sending (P_1, P_2, P_1', P_2') onto (Q_1, Q_2, Q_1', Q_2'). □

The proofs of Lemma 2.18 (3) and (4) are obtained using the same techniques as in the above proofs.

APPENDIX B. MINIMUM WEIGHT CODEWORDS

In §8.2, it is proved that the codes $C(i, q)$ have minimum distance at least $2q$. In this appendix, we give an explicit construction of some codewords of weight $2q$ which concludes the proof of Theorem 8.5. To construct such codewords, we have to introduce additional mathematical tools.

Lemma B.1. *For all $u \in \mathbf{F}_q^2$, all $P \in \mathbf{A}^2(\mathbf{F}_q)$ and all $a \in \mathbf{F}_q \setminus \{0\}$, the sets $\mathcal{C}_i(q)$ are globally preserved by the translation of vector u and by the homotecy centred at P with ratio a. These affine automorphisms induce therefore automorphisms of $\mathcal{I}_i(q)$.*

Proof. It is sufficient to prove that these automorphisms of $\mathbf{A}^2$ prolongated and regarded as automorphisms of $\mathbf{P}^2$ leave invariant any point at infinity. Since translations and homothecies send a line onto a parallel one, they fix any point at infinity. □

Notation B.2 (Parallel lines)**.** If two lines $L, L' \in \mathbf{A}^2$ are parallel (i.e. they do not meet in $\mathbf{A}^2$) we write $L \sim L'$. Moreover the class of a line L modulo $\sim$ is denoted by $[L]$. The set of such classes is isomorphic to $\mathbf{P}^1$. The class of vertical lines is denoted by $[V]$ and that of horizontal lines by $[H]$.

Proposition B.3. *Let $i \in \{1, 2, 3\}$. Let L_0, L be two lines in $\mathbf{A}^2$ meeting at $P \in \mathbf{A}^2(\mathbf{F}_q)$. If $i = 1$, then L, L_0 are assumed to be non vertical; if $i = 2$, then they are assumed to be neither vertical nor horizontal. Let $C \in \mathcal{C}_i(q)$ be a curve incident with (P, L) and Q be the other point of intersection of C with L_0. Finally, denote by M the line $M := T_Q C$. Then,*

(i) the class $[M]$ modulo $\sim$ (see Notation B.2) depends only on $[L]$ and $[L_0]$ and neither on P, nor on C.

(ii) the map $[L] \mapsto [M]$ is an involution $\psi_{[L_0]}$ of $\mathbf{P}^1 \setminus \{[V], [L_0]\}$ if $i = 1$, of $\mathbf{P}^1 \setminus \{[V], [H], [L_0]\}$ if $i = 2$ and of $\mathbf{P}^1 \setminus \{[L_0]\}$ if $i = 3$.

See figure 9 for an illustration.

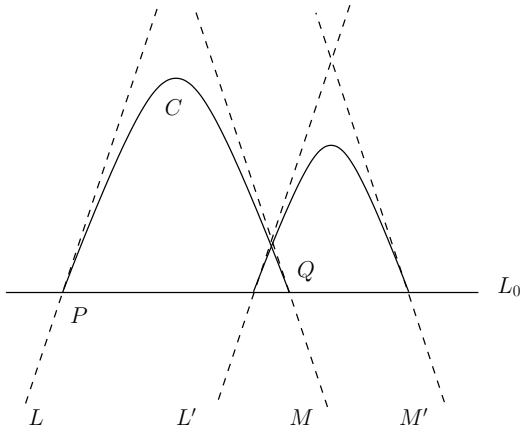

FIGURE 9. The involution $\psi_{[L_0]}$. In this picture, $L \sim L'$ and $\psi_{[L_0]}([L]) = [M] = [M']$.

Proof. First, notice that C is the unique element of $\mathcal{C}_i(q)$ incident with (P, L) and containing Q. Indeed, the existence of two such distinct curves C, D would yield a contradiction with Lemma 5.12, since C, D would meet at least once at Q and twice at P.

Let $C' \in \mathcal{C}_i(q)$ be another curve incident with (P, L) and Q' be the other point of intersection of C' with L_0. By the same way C' is the unique element of $\mathcal{C}_i(q)$ incident with (P, L) and containing Q'. Let h be the homotecy of centre P sending Q on Q'. By uniqueness, h sends C onto C' and $T_{Q'}C' = h(T_Q C) = M$, thus $T_Q C' \sim M$. Therefore $[M]$ does not depend on the choice of C.

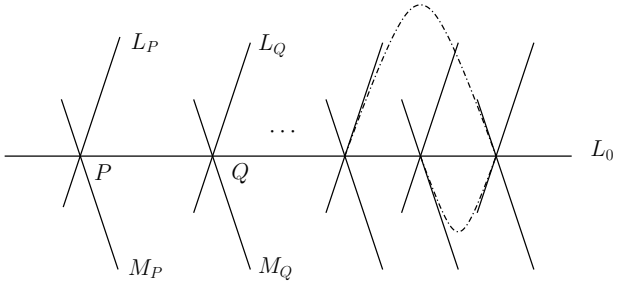

FIGURE 10. The codeword c.

Afterwards, let $P' \in L_0$ be another point and $L' \sim L$ be a line containing P'. Let t be the translation sending P on P', this map sends C onto a curve incident with (P', L'). The curve $t(C)$ meets L_0 at $t(Q)$ and its tangent at this point is parallel to M. This shows that $[M]$ does not depend on P.

Finally, to prove that this correspondence is an involution, it is sufficient to show that $[M]$ is sent onto $[L]$, which is obvious since C is incident with (Q, M), meets L_0 at another point P and has L a tangent at this point, thus $\psi_{[L_0]}([L]) = [M]$. □

Construction of minimum weight codewords. Using Proposition B.3, one can prove the existence of codewords of weight $2q$ in $C(i, q)$ and construct them explicitly. Choose a line L_0 whose class in $\mathbf{P}^1$ is distinct from $[V]$ if $i = 1$ and distinct from $[V], [H]$ if $i = 2$. The involution $\psi_{[L_0]}$ introduced in Proposition B.3 is either constant[1] or permutes at least two distinct classes $[L], [M]$. If it is constant, then choose an arbitrary pair of classes $[L], [M]$, else choose $[L] \neq [M]$ such that $\psi_{[L_0]}([L]) = [M]$. Recall that words in $\mathbf{F}_2^n$ can be represented by sets of flags (see Caution page 22). Consider the word in $\mathbf{F}_2^n$ defined by

$$\begin{aligned} c \;:=\; & \{(P, L_P) : P \in L_0,\ L_P \ni P \text{ and } L_P \sim L\} \cup \\ & \{(P, M_P) : P \in L_0,\ M_P \ni P \text{ and } M_P \sim M\}. \end{aligned}$$

See figure 10 for an illustration.

The line L_0 has q rational points in $\mathbf{A}^2$ and the above word is given by 2 flags per point in L_0. Thus, it has weight $2q$. There remain to show that it is a codeword of $C(i, q)$, which means that any block of $\mathcal{B}_i(q)$ is always incident with an even number of flags in c.

(1) Let E_P be an exceptional divisor. If $P \notin L_0$ then none flag in C is incident with E_P. Else, exactly two of them are, namely (P, L_P) and (P, M_P).
(2) Let $C \in \mathcal{C}_i(q)$, if C is incident with a flag (P, L_P) in c, then C meets L_0 at another point Q. If the involution $\psi_{[L_0]}$ is constant, then $T_Q C \sim L_P$ and hence $T_Q C = L_Q$, else $T_Q C = M_Q$. In both cases, if C is incident with an element of c, then it is always incident with a second one.

This concludes the proof.

[1]One can prove that the involution is constant when $i = 1$ and q is even. In even characteristic, the tangents of a curve of equation $y = ax^2 + bx + c$ are all parallel!

Appendix C. Index of notations and terminologies

$m_P(C,D)$	§2.1.5
The line (PQ)	Nota 3.2
$\Lambda_1(P_1,P_2,P_3,L)$	Lem 3.3
$\Lambda_2(P_1,P_2,L_1,L_2)$	Lem 3.5
$L_\infty,\alpha,P_\infty,Q_\infty,R_\infty,\overline{R}_\infty$	Nota 4.1
Vertical/Horizontal Lines	Def 4.2
$T_P(C)$	Nota 4.3
$\Gamma_1,\Gamma_2,\Gamma_3$	Defs 5.1, 5.2, 5.3
$\mathcal{C}_1(q),\mathcal{C}_2(q),\mathcal{C}_3(q)$	Defs 5.1, 5.2, 5.3
$\mathbf{B}$	Def 6.1
$\mathcal{E}$	Def 6.1
$\widetilde{\mathcal{C}}_i(q)$	Def 7.1
$\mathcal{B}_i(q)$	Defs 7.2, 7.3 and 7.4
$\mathcal{I}_i(q)$	Defs 7.2, 7.3 and 7.4
$\mathcal{P}_i(q)$	Defs 7.2, 7.3 and 7.4
E_P	Nota 7.6
$(C3)$ configuration	Def 7.10
$\kappa_i(q,P,L,C)$	Prop 7.13
$\sim$	Nota B.2
$[L]$	Nota B.2

Acknowledgements

The author expresses a deep gratitude to Daniel Augot and Gilles Zémor for many inspiring discussions. Computations and simulations have been made using Magma.

References

[1] W. Fulton. *Algebraic curves*. Advanced Book Classics. Addison-Wesley Publishing Company Advanced Book Program, Redwood City, CA, 1989. An introduction to algebraic geometry, Notes written with the collaboration of Richard Weiss, Reprint of 1969 original.

[2] R. G. Gallager. Low–density parity–check codes. *IRE Trans.*, IT-8:21–28, 1962.

[3] R. Hartshorne. *Algebraic geometry*, volume 52 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1977.

[4] S. J. Johnson and S. R. Weller. High-rate LDPC codes from unital designs. In *IEEE Globecom*, pages 2036–204, dec 2003.

[5] S. J. Johnson and S. R. Weller. Codes for iterative decoding from partial geometries. *IEEE Transactions on Communications*, 52(2):236–243, feb 2004.

[6] N. Kamiya. High–rate quasi-cyclic low–density parity–check codes derived from finite affine planes. *IEEE Trans. Inform. Theory*, 53(4):1444–1459, 2007.

[7] J.-L. Kim, K. E. Mellinger, and L. Storme. Small weight codewords in LDPC codes defined by (dual) classical generalized quadrangles. *Des. Codes Cryptogr.*, 42(1):73–92, 2007.

[8] Y. Kou, S. Lin, and M. P. C. Fossorier. Low–density parity–check codes based on finite geometries: a rediscovery and new results. *IEEE Trans. Inform. Theory*, 47(7):2711–2736, 2001.

[9] X. Li, C. Zhang, and J. Shen. Regular LDPC codes from semipartial geometries. *Acta Applicandae Mathematicae*, 102:25–35, 2008.

[10] Z. Liu and D. A. Pados. LDPC codes from generalized polygons. *IEEE Trans. Inform. Theory*, 51(11):3890–3898, 2005.

[11] D. J. MacKay and R. M. Neal. Near shannon limit performance of low–density parity–check codes. *Electronics Letters*, 32:1645–1646, 1996.

[12] V. Pepe. LDPC codes from the Hermitian curve. *Des. Codes Cryptogr.*, 42(3):303–315, 2007.

[13] T. J. Richardson, M. A. Shokrollahi, and R. L. Urbanke. Design of capacity–approaching irregular low–density parity–check codes. *IEEE Trans. Inform. Theory*, 47:619–637, 2001.

[14] I. R. Shafarevich. *Basic algebraic geometry. 1.* Springer-Verlag, Berlin, second edition, 1994.
[15] H. Tang, J. Xu, S. Lin, and K. A. S. Abdel-Ghaffar. Codes on finite geometries. *IEEE Trans. Inform. Theory*, 51(2):572–596, 2005.
[16] S. R. Weller and S. J. Johnson. Regular low–density parity–check codes from oval designs. *European Transactions on Telecommunications*, 14(5):399–409, sep 2003.
[17] J. Xu, L. Chen, I. Djurdjevic, S. Lin, and K. Abdel-Ghaffar. Construction of regular and irregular LDPC codes: geometry decomposition and masking. *IEEE Trans. Inform. Theory*, 53(1):121–134, 2007.

INRIA Saclay Île-de-France, Projet TANC – CNRS, LIX UMR 7161, École Polytechnique, 91128 Palaiseau Cedex, France
E-mail address: alain.couvreur@inria.fr