International Journal of Pure and Applied Mathematics

Volume 69 No. 1 2011, 49-55

AG CODES OBTAINED FROM BLOWING-UPS OF THE PLANE AT NON-RATIONAL POINTS

E. Ballico

Department of Mathematics
University of Trento
38 123 Povo (Trento) - Via Sommarive, 14, ITALY
e-mail: ballico@science.unitn.it

Abstract: Here we look at some AG codes over $\mathbb{F}_q$ obtained blowing-up the plane at points on one or two lines, no point being in $\mathbb{P}^2(\mathbb{F}_q)$.

AMS Subject Classification: 14G50, 94B27
Key Words: blowing-up, algebraic geometric code, AG code

*

Fix a prime p and a p-power q. For a balanced introduction of algebraic geometry codes (or AG codes) and how to use rational surfaces to construct them, see the first two sections of [5], whose references list some key papers on this topic (see [6], [7], [12], [17]). Here we consider a related set-up, i.e. we consider rational surfaces, X, defined over $\mathbb{F}_q$ obtained blowing-up points of $\mathbb{P}^2(\overline{\mathbb{F}}_q)$ but for which the blow-down map $\beta : X \to \mathbb{P}^2$ is defined over $\mathbb{F}_q$. We also need to take a line bundle on X defined over $\mathbb{F}_q$. This may be done in the following way. Notice that the Frobenius F_q acts on $\mathbb{P}^2(\overline{\mathbb{F}}_q)$. Fix an integer $b \geq 2$, a set $B \subset \mathbb{P}^2(\overline{\mathbb{F}}_q)$ such that $\sharp(B) = b$, an ordering $P_1, \dots, P_b$ of its points and positive integers $m_1, \dots, m_b$. Since B is finite, there is an integer $e \geq 1$ such that $B \subseteq \mathbb{P}^2(\mathbb{F}_{q^e})$). We say that the datum $(b; B; m_1, \dots, m_b)$ is allowable if $F_q(B) \subset B$ and $m_i = m_j$ for all i, j such that $P_j = F_q(P_j)$, i.e. F_q induces a bijection $\phi_q : B \to B$ and the values of the multiplicities m_i are constant on the orbits of the subgroup Ψ of the permutation group $\mathrm{Aut}(B) \cong S_b$ generated by ϕ_q. Since $F_q(B) = B$, the rational variety X and the birational morphism β is defined over $\mathbb{F}_q$. Set $E_i := \beta^{-1}(P_i)$, $1 \leq i \leq b$. Each E_i is

Received: January 1, 2011

an effective divisor of X defined over $\overline{\mathbb{F}}_q$. More precisely, if the Ψ-orbit of P_i has cardinality e, then E_i is defined over $\mathbb{F}_{q^e}$. We have $\mathrm{Pic}(X)(\overline{\mathbb{F}}_q) \cong \mathbb{Z}^{b+1}$ and we may take $H := \beta^*(\mathcal{O}_{\mathbb{P}^2}(1))$ and E_i, $1 \le i \le b$, as a $\mathbb{Z}$-basis of $\mathrm{Pic}(X)(\overline{\mathbb{F}}_q)$. Since β is defined over $\mathbb{F}_q$, H is defined over $\mathbb{F}_q$. Hence dH is defined over $\mathbb{F}_q$ for any $d \in \mathbb{Z}$. If the datum $(b; B; m_1, \dots, m_b)$ is allowable, then each line bundle $dH - m_1E_1 - \cdots - m_bE_b$ is defined over $\mathbb{F}_q$. Set $R := \mathbb{F}[x, y, z]$ and $\overline{R} := \overline{\mathbb{F}}_q[x, y, z]$. For all integers $m \ge 0$ let R_m (resp. $\overline{R}_m$) be the vector subspace of R (resp. $\overline{R}$) formed by the homogeneous degree m forms. For any $f \in \overline{R}_m \setminus \{0\}$ set $Z(f) := \{P \in \mathbb{P}^2(\mathbb{F}_q) : f(P) = 0\}$. Let $\mathcal{R} = \mathcal{R}(q, m, b, m_1, \dots, m_b, P_1, \dots, P_m)$ denote the $\mathbb{F}_q$-vector space given by the set of all $f \in R_m$ vanishing at each P_i with multiplicity at least m_i. With the notation of [8] this linear system is $H^0(\mathbb{P}^2, \mathcal{I}_{m_1P_1 \cup \cdots \cup m_bP_b}(m))$. The integer $h^0(\mathbb{P}^2, \mathcal{I}_{m_1P_1 \cup \cdots \cup m_bP_b}(m))$ be the vector space dimension of this linear space. If we assume $m \ge m_1 + \cdots + m_b - 1$, then

$$h^0(\mathbb{P}^2, \mathcal{I}_{m_1P_1 \cup \cdots \cup m_bP_b}(m)) = \binom{m+2}{2} - \sum_{i=1}^{b} \binom{m_i+1}{2}. \tag{1}$$

As shown in [8] the equality (1) may be obtained with weaker assumptions on m, unless B is contained in a line. If B is contained in a line, then $m_1 + \cdots + m_b - 1$ is the minimal positive integer m for which (1) holds. Fix an admissible datum $(b; B; m_1, \dots, m_b)$ and a positive integer m for all i such that (1) holds. For any $S \subseteq \mathbb{P}^2(\mathbb{F}_q) \setminus B \cap \mathbb{P}^2(\mathbb{F}_q)$ we obtain an $\mathbb{F}_q$-linear code $\mathcal{C} = \mathcal{C}(m; b; B; m_1, \dots, m_b; S)$. If the evaluation map at S is injective, i.e. if $h^0(\mathbb{P}^2, \mathcal{I}_{S \cup m_1P_1 \cup \cdots \cup m_bP_b}(m)) = 0$, then $\mathcal{C}$ is an $[n, k, d]$ code with $k := \binom{m+2}{2} - \sum_{i=1}^{b} \binom{m_i+1}{2}$ and $n := \sharp(S)$. Our aim here is to show that taking suitable B not contained in $\mathbb{F}_q$ we may find $[n, k, d]$ codes with d larger than the ones obtained taking $B \subset \mathbb{P}^2(\mathbb{F}_q)$. The main reason is that in this way we handle elements of $\mathcal{R} \setminus \{0\}$ whose zero-locus is a union of lines. Almost always in [5] these configurations are the only ones computing the minimum distance of the code. Avoiding too many lines defined of $\mathbb{F}_q$ also allows us to use several recent results on the number of $\mathbb{F}_q$-points of plane curves (see [9], [10]). When the curve is integral we may also use Hasse-Weil bound for singular curves and related results (see [18], [1], [2], [3], [4], [11]). Of course, the minimum distance depends on S and n. Here we raise the following questions. For any $m, b, m_1, \dots, m_b$ and any $S \subseteq \mathbb{P}^2(\mathbb{F}_q)$. Let $E(S, m, b, m_1, \dots, m_b)$ the set of all $B \subset \mathbb{P}^2(\overline{\mathbb{F}}_q)$ such that $S \cap B = \emptyset$ and $(b; B; m_1, \dots, m_b)$ is allowable. Let $A_1(S, m, b, b_1, \dots, m_b)$ (resp. $E_1(S, m, b_1, \dots, m_b)$ be the maximal (resp. minimal) integer obtained as the minimum distance for some code $\mathcal{C}(m; b; B; m_1, \dots, m_b; S)$ with $B \in (S, m, b, m_1, \dots, m_b)$. Fix a positive integer $s \le q^2 + q + 1$.

Question 1. What are the maximal and the minimal values of the integers $A_1(S, m, b, b_1, \dots, m_b)$ and $E_1(S, m, b_1, \dots, m_b)$ with S admissible and $\sharp(S) = s$?

In the case $S = \mathbb{P}^2$ we would like to consider also B containing some point of $\mathbb{P}^2(\mathbb{F}_q)$. We may do this in the following way. Fix $m, b, m_1, \dots, m_b$. For any allowable datum $(b; B; m_1, \dots, m_b)$ set $S_B := \mathbb{P}^2(\mathbb{F}_q) \setminus B \cap \mathbb{P}^2(\mathbb{F}_q)$.

Question 2. What are the maximal and minimal integers appearing as the minimum distance of some code $\mathcal{C}(m; b; B; m_1, \dots, m_b; S_B)$ for some allowable B with fixed $m, b, m_1, \dots, m_b$ or with fixed $m, b, m_1, \dots, m_b$ and $\sharp(S_B)$?

In this note we collect a few results in the cases in which B is contained in a line defined over $\mathbb{F}_q$ and we cal x the equation of this line. See also Propositions 2 and 3 when B is contained in 2 lines not defined over $\mathbb{F}_q$.

Theorem 1. *Assume $q > m = b \geq 2$, $m_i = 1$ for all i, $B \subset \{x = 0\}$ and $B \cap \mathbb{P}^2(\mathbb{F}_q) = \emptyset$. For any S the code $\mathcal{C}$ contains all forms xh with $h \in R_{b-1}$.*

(a) If $S = \mathbb{P}^2(\mathbb{F}_q)$, then $\mathcal{C}$ is an $[n, k, d]$ code with $n = q^2 + q + 1$, $k = (b^2 + b + 3)/2$ and $d = n - bq - 1$. Every codeword with Hamming weight at least $n - (b - 1)q$ is induced by $f \in \mathcal{R}$ with $f/x \in R_{m-1}$.

(b) If $S = \mathbb{P}^2 \setminus \{x = 0\}$, then $\mathcal{C}$ is an $[n, k, d]$ code with $n = q^2$, $k = (b^2 + b + 3)/2$ and $n - (b - 1)q - 1 \leq d \leq n - (b - 1)q$.

Proof. Fix any $f \in \mathcal{R} \setminus \{0\}$ and set $C := \{f = 0\}$. Since $\sharp(C \cap \{x = 0\}) = b = \deg(C)$ and $B \cap \mathbb{P}^2(\mathbb{F}_q) = \emptyset$, we have $C \cap \{x = 0\} \cap \mathbb{P}^2(\mathbb{F}_q) = \emptyset$. Since $\{x = 0\}$ is defined over $\mathbb{F}_q$ and any two lines defined over $\mathbb{F}_q$ contain a point of $\mathbb{P}^2(\mathbb{F}_q)$, we get that C contains no line defined over $\mathbb{F}_q$, unless $\{x = 0\}$ is one of these lines. First assume that $\{x = 0\}$ is a component of C and call C' the union of the other components. C' is a curve of degree $\leq b - 1$ and defined over $\mathbb{F}_q$. Thus $\sharp(C'(\mathbb{F}_q)) \leq (b-1)q + 1$ and equality holds if and only if C' is a union of $b - 1$ lines defined over $\mathbb{F}_q$ (see [17], Remark 2 at p. 242). Since $\{x = 0\}$ meets each of these lines, we get $\sharp(C(\mathbb{F}_q)) \leq bq + 1$ and equality holds if and only if $P \in \{x = 0\}$ and C is a union of b distinct lines through P, all of them defined over $\mathbb{F}_q$. In this case we have $\sharp(C(\mathbb{F}_q) \cap (\mathbb{P}^2(\mathbb{F}_q) \setminus \{x = 0\}) = (b - 1)q$.

Now assume that $\{x = 0\}$ is not a component of C. Hence no component of C is a line defined over $\mathbb{F}_q$. Since $q > b$, we have $(q, d) \neq (2, 2)$. Thus we may use an upper bound for the cardinality of the sets $C(\mathbb{F}_q)$ for a degree b plane curve defined over $\mathbb{F}_q$, but containing no line defined over $\mathbb{F}_q$ (see [9], [10]). We get $\sharp(C(\mathbb{F}_q)) \leq (b - 1)q + 1$. □

Remark 1. As a comparison in Thorem 1, but with $B \subset \{x = 0\} \cap \mathbb{P}^2(\mathbb{F}_q)$ and $S = \mathbb{P}^2 \setminus (\{x = 0\} \cup \{y = 0\} \cup \{z = 0\})$ (i.e. S much smaller than in case

(b)) the minimum distance is $(q-1)^2-b(q-1)+c(b-c) = n-b(q-1)+c(b-c)$, where $c := \sharp(B \cap (\{y=0\} \cup \{z=0\})$ (see [5], Theorem 4.2.5). Notice that $0 \le c \le 2$. The distance is reached by $f \in \mathcal{R} \setminus \{0\}$ such that $\{f=0\}$ is a union of b lines through a point of $\{y=0\} \cup \{z=0\}$ (use [5], Corollary 4.2.2, and the analysis of the possible configurations of $\mathbb{F}_q$-lines for each case of $c \in \{0,1,2\}$).

Proposition 1. *Assume $q > m > b \ge 2$, $m_i = 1$ for all i, $B \subset \{x=0\}$ and $B \cap \mathbb{P}^2(\mathbb{F}_q) = \emptyset$.*

(a) For any S the code $\mathcal{C}$ contains all forms xh with $h \in R_{m-1}$.

(b) If $S = \mathbb{P}^2(\mathbb{F}_q)$, then $\mathcal{C}$ is an $[n,k,d]$ code with $n = q^2+q+1$, $k = \binom{m+2}{2} - m$ and $d = n - mq - 1$. Every codeword with minimum Hamming weight is induced by $f \in R_m$ divisible by x.

(c) If $S = \mathbb{P}^2 \setminus \{x=0\}$, then $\mathcal{C}$ is an $[n,k,d]$ code with $n = q^2$, $k = \binom{m+2}{2} - m$ and $n-(m-1)q-2 \le d \le n-(m-1)q-1$.

Proof. The values of n and k are obvious. Fix any $f \in \mathcal{R} \setminus \{0\}$ and set $C := \{f=0\}$. First assume that x divides f. Thus $C = \{x=0\} \cup C'$ with C' a degree $m-1$ plane curve defined over $\mathbb{F}_q$. Varying f we obtain as C' all plane curves of degree $m-1$ defined over $\mathbb{F}_q$. Hence $\sharp(C(\mathbb{F}_q)) \le mq+1$ and equality holds if and only if C is a union of m distinct lines defined over $\mathbb{F}_q$, one of them being the line $\{x=0\}$ (see [17], Remark 2 at p. 242). Thus part (b) is proved by the quoted result of Serre (see [17]). The example with m distinct lines defined over $\mathbb{F}_q$, one of them being the line $\{x=0\}$, also gives the inequality $d \le n-(m-1)q-1$ in part (c). Now we check the other inequality for d in part (c). Hence we may assume that C has not the line $\{x=0\}$ as one of its components. Write $C = C_1 \cup C_2$ with C_1 union of the lines defined over $\mathbb{F}_q$ and contained in C. Set $e := \deg(C_1)$. Since $B \cap \mathbb{P}^2(\mathbb{F}_q) = \emptyset$, we have $0 \le e \le m-b$. We have $\sharp(C_1(\mathbb{F}_q)) \le eq+1$ (see [17]) if $e > 0$ and $\sharp(C_1(\mathbb{F}_q)) = 0$ if $e = 0$. Since $q > m$, we have $\sharp(C_2(\mathbb{F}_q)) \le (m-e)q+1$. Hence $d \ge n-(m-1)q-2$. □

Proposition 2. *Fix an even integer $b \ge 2$ and take $m_i = 1$ for all i and $m := b/2$. Assume $q > b$. Fix a line $L_1 \subset \mathbb{P}^2$ defined over $\mathbb{F}_{q^2}$, but not defined over $\mathbb{F}_q$ and let $L_2 \subset \mathbb{P}^2$ the conjugate line for the Frobenius F_q of $\mathbb{P}^{2*}$. Thus L_2 is defined over $\mathbb{F}_{q^2}$, but not over $\mathbb{F}_q$, $L_1 \cap L_2$ is a single point, P, and $P \in \mathbb{P}^2(\mathbb{F}_q)$. Fix $B_1 \subset L_1(\mathbb{F}_{q^2}) \setminus \{P\}$ such that $\sharp(B_1) = b/2$ and let $B_2 \subset L_2(\mathbb{F}_{q^2}) \setminus \{P\}$ the conjugate of B_1 for the Frobenius F_q of $\mathbb{P}^2$. Set $B := B_1 \cup B_2$ and $S := \mathbb{P}^2(\mathbb{F}_q)$. Then the associated code $\mathcal{C}$ is an $[n,k,d]$ code with $n = q^2+q+1$, $k = (b^2+b+3)/2$ and $d \ge n-bq-1$. There is at most one codeword of $\mathcal{C}$ whose Hamming distance x, is at most $n-(b-1)q-2$. There*

is such codeword with Hamming distance x for some code associated to one B_1 if and only if there is a union $T \subset \mathbb{P}^2$ of b lines defined over $\mathbb{F}_q$ and such that $\sharp(T(\mathbb{F}_q)) = n - x$.

Proof. The parameter n of $\mathcal{C}$ is obvious. The value of parameter k for $\mathcal{C}$ is true if and only if $h^1(\mathcal{I}_B(b/2)) = 0$. Since $\sharp(B_2) = b/2 \leq b/2 + 1$, we have $h^1(L_2, \mathcal{I}_{B_2}(b/2)) = 0$. Notice that B_1 is the complement of $B \cap L_2$ inside B. Hence we have the so-called Castelnuovo's exact sequence

$$0 \to \mathcal{I}_{B_1}(t-1) \to \mathcal{I}_B(t) \to \mathcal{I}_{B_2,L_2}(t) \to 0 \tag{2}$$

Since $\sharp(B_1) = b/2 - 1$, we have $h^1(\mathbb{P}^2, \mathcal{I}_{B_1}(b/2-1)) = 0$. Hence the case $t = b/2$ of the long cohomology exact sequence of (2) gives $h^1(\mathbb{P}^2, \mathcal{I}_B(b/2)) = 0$, proving the value k of $\mathcal{C}$.

Take $f \in \mathcal{R} \setminus \{0\}$ computing d, i.e. such that $\sharp(Z(f))$ is maximal and set $C := \{f = 0\}$. First assume that C contains no line defined over $\mathbb{F}_q$. Since $(q, b) \neq (4, 4)$, we have $\sharp(Z(f)) \leq (b-1)q+1$ (see [10]). Now assume $C = C_1 \cup C_2$ with C_1 unions of all lines defined over $\mathbb{F}_q$ and contained in C. Set $e := \deg(C_1)$. Thus $\deg(C_2) \leq b - e$. First assume $e < b$. Since C is defined over $\mathbb{F}_q$, we have $e \leq b - 2$. We have $\sharp(C_1(\mathbb{F}_q)) \leq eq + 1$ (see [17], Remark 2 at p. 242) and $\sharp(C_1(\mathbb{F}_q)) \leq (b - e - 1)q + 1$ (see [10]). Hence $\sharp(C(\mathbb{F}_q)) \leq (b-1)q + 2$. Now assume $e = b$, i.e. assume that C is a union of b distinct lines defined over $\mathbb{F}_q$. Let T be an arbitrary union of $b/2$ distinct lines defined over $\mathbb{F}_q$ such that $P \notin T$. Set $A_i := T \cap L_i$. Then $\sharp(A_i) = b/2$, $A_i \subset L_i(\mathbb{F}_{q^2}) \setminus \{P\}$ and A_2 is the conjugate of A_1 for the Frobenius of $\mathbb{P}^2$. Notice that T is uniquely determined by $A_1 \cup A_2$, because for each $O \in A_1$ exactly one of the lines of T is the line spanned by O and its conjugate point $O' \in A_2$. This observation proves the last two sentences of the proposition. □

Proposition 3. *Fix an even integer b and assume $q > m > b/2$ and $m_i = 1$ for all i. Fix a line $L_1 \subset \mathbb{P}^2$ defined over $\mathbb{F}_{q^2}$, but not defined over $\mathbb{F}_q$ and let $L_2 \subset \mathbb{P}^2$ the conjugate line for the Frobenius F_q of $\mathbb{P}^{2*}$. Thus L_2 is defined over $\mathbb{F}_{q^2}$, but not over $\mathbb{F}_q$, $L_1 \cap L_2$ is a single point, P, and $P \in \mathbb{P}^2(\mathbb{F}_q)$. Fix $B_1 \subset L_1(\mathbb{F}_{q^2}) \setminus \{P\}$ such that $\sharp(B_1) = b/2$ and let $B_2 \subset L_2(\mathbb{F}_{q^2}) \setminus \{P\}$ the conjugate of B_1 for the Frobenius F_q of $\mathbb{P}^2$. Set $B := B_1 \cup B_2$ and $S := \mathbb{P}^2(\mathbb{F}_q)$. Then the associated code $\mathcal{C}$ is an $[n, k, d]$ code with $n = q^2 + q + 1$, $k = \binom{m+2}{2} - b$ and $d \geq n - mq - 1$. There is B_1 with $d = n - mq - 1$; in this case all the codewords with minimal Hamming weight are unions of m distinct lines defined over $\mathbb{F}_q$ and passing through the same point.*

Proof. The value k of the code is computed as in the proof of Proposition 2 taking $t := m$ in (2). First assume that C contains no line defined over $\mathbb{F}_q$. Since $(q, m) \neq (4, 4)$, we have $\sharp(Z(f)) \leq (m-1)q+1$ (see [10]). The assertions on the minimum distance are proven as in Proposition 2. □

Acknowledgments

The author was partially supported by MIUR and GNSAGA of INdAM (Italy).

References

[1] Y. Aubry, M. Perret, A Weil Theorem for singular curves, In: *Arithmetic, Geometry and Coding Theory*, Luminy, 1993, de Gruyter, Berlin (1996), 1-7.

[2] Y. Aubry, M. Perret, Coverings of singular curves over finite fields, *Manuscripta Math.*, **88**, No. 4 (1995), 467-478.

[3] Y. Aubry, M. Perret, On the characteristic polynomials of the Frobenius endomorphism for projective curves over finite fields, *Finite Fields Appl.*, **10**, No. 3 (2004), 412-431.

[4] E. Bach, Weil bounds for singular curves, *Appl. Algebra Engrg. Comm. Comput.*, **7**, No. 4 (1996), 289-298.

[5] J.A. Davis, Algebraic geometric codes on anticanonical surfaces, *J. Pure Appl. Algebra*, **215**, No. 4 (2011), 496-510.

[6] J.P. Hansen, Toric surfaces and error-correcting codes, In: *Coding Theory, Cryptography and Related Areas*, Guanajuato, Springer, Berlin (1998), 132-142.

[7] J.P. Hansen, Toric variety, Hirzebruch surfaces and error-correcting codes, *Appl. Algebra Engrg. Comm. Comput.*, **13**, No. 4 (2002), 293-300.

[8] B. Harbourne, The geometry of rational surfaces and Hilbert functions of points in the plane, In: *Proceedings of the 1984 Vancouver Conference in Algebraic Geometry*, Providence, RI;' In: *CMS Conf. Proc.*, **6**, Amer. Math. Society (1986), 95-111.

[9] M. Homma, S.J. Kim, Around Sziklai's conjecture on the number of points of a plane curve over a finite field, *Finite Fields Appl.*, **15**, No. 4 (2009), 468-474.

[10] M. Homma, S.J. Kim, Sziklai's conjecture on the number of points of a plane curve over a finite field III, *Finite Fields Appl.*, **16**, No. 5 (2010), 315-319.

[11] D.B. Leep, C.C. Yeomans, The number of points on a singular curve over a finite field, *Arch. Math.*, Basel, **63**, No. 5 (1994), 420-426.

[12] J. Little, H. Schenck, Toric surfaces and Minkowski sums, *SIAM J. Discrete Math.*, **20**, No. 4 (2006), 999-1014.

[13] Y. Rodier, A. Sboui, Highest numbers of points of hypersurfaces over finite fields and generalized Reed-Muller codes, *Finite Fields Appl.*, **14**, No. 3 (2008), 816-822.

[14] A. Sboui, Second highest number of points of hypersurfaces in ${\mathbb{F}_q}^n$, *Finite Fields Appl.*, **13**, No. 3 (2007), 444-449.

[15] A. Sboui, Special numbers of rational points on hypersurfaces in the n-dimensional projective space over a finite field, *Discrete Math.*, **309**, No. 16 (2009), 5048-5059.

[16] J.-P. Serre, Lettre à M. Tsfasman du 24 juillet 1989, In: *Journées Arithmétiques de Luminy*, 17–21 juillet 1989; *Astérisque*, 198–199–200 (1991), 240-242.

[17] H.K. Schenk, Linear systems on a special rational surface, *Math. Res. Lett.*, **11**, No-s: 5, 6 (2004), 697-713.

[18] O.-K. Stöhr, J.F. Voloch, Weierstrass points and curves over finite fields, *Proc. London Math. Soc.*, 3, **52**, No. 1 (1986), 1-19.

56