Applicable Algebra in Engineering, Communication and Computing manuscript No.
(will be inserted by the editor)

A. Campillo · J. I. Farran · M. J. Pisabarro

Evaluation codes at singular points of algebraic differential equations

Received: date / Revised: date

Abstract We use the special geometry of singular points of algebraic differential equations on the affine plane over finite fields to study the main features and parameters of error correcting codes giving by evaluating functions at sets of singular points. In particular, one gets new methods to construct codes with designed minimum distance.

Keywords evaluation codes · algebraic differential equations · Cayley–Bacharach theorem · designed minimum distance

1 Introduction

Let F be a finite field with q elements, $P_1, \ldots, P_n$ points of the affine plane $\mathcal{A}^2 = F^2$,rational over F (i.e. having coordinates in F), and $m > 0$ an integer. Denote by $F[x,y]_{\leq m}$ the vector space of polynomials in x, y with coefficients in F and degree less or equal than m. Consider the linear evaluation map

$$\mathcal{E} : F[x,y]_{\leq m} \longrightarrow F^n$$

given by

$$f \to (f(P_1), \ldots, f(P_n))$$

This work was partially supported by MCyT BFM2001-2251

A. Campillo
Dpto. Algebra, Geometria y Topologia, Univ. Valladolid, Spain
E-mail: campillo@agt.uva.es

J. I. Farran
Dpto. Matematica Aplicada, Univ. Valladolid, Spain
E-mail: ignfar@eis.uva.es

M. J. Pisabarro
Dpto. Matematicas, Univ. Leon, Spain
E-mail: demmpm@isidoro.unileon.es

Linear error correcting codes, or simply codes along this paper, are exactly the vector subspaces C of F^n for some integer $n > 0$. Elements of F^n, which are called words in the alphabet F, are considered for transmission through noisy channels. Words in C are really those which are transmitted. Received words are not necessarily in C as some errors usually occur during transmission. The code given by the image of $\mathcal{E}$ is called the evaluation code of polynomials of degree at most m at the points $P_1, \ldots, P_n$.

Main parameters associated to a code C are its length $n = n(C)$, its dimension $k = k(C)$ and its minimum distance $d = d(C)$. The value of n is nothing but the length of the considered words. The value of k is the dimension of C as vector space. The integer d is the minimum of the values $d(\mathbf{x}, \mathbf{y})$ where $\mathbf{x}$,$\mathbf{y}$ range over the pairs of different words of C and $d(-,-)$ stands for the Hamming distance, i.e. $d(\mathbf{x}, \mathbf{y})$ is the number of places for which the letters of $\mathbf{x}$ and $\mathbf{y}$ are different. The number of errors which a code can correct in the transmission is the largest integer t satisfying $2t + 1 \leq d$. Thus, coding theory is interested in constructing codes with relatively large value of d/n. Obviously, because of efficiency in the transmission, it is also interested in codes with relatively large value of k/n. One can check the best values of d for fixed q, n and k on the web

`http://www.win.tue.nl/~aeb/voorlincod.html`

Further details can be found in [8].

Algebraic geometry provides a general technique to give suitable codes. It consists in considering a smooth projective variety X over F, an F-rational divisor G, and a set of rational points of X not in the support of G. Then, the code is the image of the evaluation map at the considered points of the functions in the vector space $\mathcal{L}(G)$. For codes of this type, which are called AG codes, estimates for their dimension k are often available from algebraic geometry. However, estimates for the minimum distance d are only available in very few cases. The most relevant of those cases is that of the geometric Goppa codes, i.e. AG codes for which X is a projective curve. In that case, one has the well-known estimates given by

$$k \geq deg(G) + 1 - g$$

$$d \geq n - deg(G)$$

g being the genus of the curve. The estimation of the minimum distance for AG codes on varieties of dimension bigger than one is an open problem. An overview on AG codes can be found in [7].

Evaluation codes, as introduced before, are nothing but the AG codes on the projective plane $\mathcal{P}^2$ taking as divisor mH, H being the infinity line, and the considered affine points P_i as evaluating points. In this case, one obviously has $\mathcal{L}(mH) = k[x, y]_{\leq m}$, and the evaluation map is $\mathcal{E}$. Again, the dimension of evaluation codes is not difficult to compute, however, estimates for the minimum distance are not known for a general set of evaluating points. In particular, it becomes a natural problem to construct evaluation codes with a designed minimum distance.

Notice that we are talking about different kind of evaluation codes: evaluating either polynomials at points of the affine plane or certain rational functions at rational points of an algebraic curve. Evaluation codes can be defined in a more general way, as in [6] or [7]. However, it seems that evaluation codes are not defined fully consistently in the literature.

In this paper, we consider evaluation codes at sets of singular points of an algebraic ordinary differential equation on the plane. The geometry of such sets of singular points has been recently determined in [2] by considering the extension of the differential equation to the projective plane $\mathcal{P}^2$ as an algebraic foliation. Using essentially the approach in [2] and new results, we will show how the minimum distance of those evaluation codes can be estimated for the various values of m, giving rise to the construction of new codes with designed minimum distance.

The singular locus of a foliation is considered reduced, although technically it is could also be possible to consider infinitely near points. However, even in the easiest case of points on a bamboo or fat points, estimating the minimum distance of such evaluation codes, in the way it is given in this paper, is not possible.

Recently, results on the knowledge of the geometry of the singular locus were extended to the case of algebraic (ordinary) differential equations on arbitrary algebraic varieties [3]. Thus, one can expect that the estimation of parameters for AG codes defined over more general varieties and given by evaluation on singularities of differential equations can be studied. This is to be done in the future.

2 Conditions imposed by systems of points: Cohomology tools

Let V_k be the vector space of homogeneous polynomials in $F[X, Y, Z]$ of degree k, F being a finite field with q elements. Consider a system of distinct points $P_1, \ldots, P_n$ in $\mathbf{P^2}$ which are rational over F. Set $W_k(P_1, \ldots, P_n) = \{f \in V_k \mid f(P_i) = 0, \quad i = 1, \ldots, n\}$, which is a vector subspace since the equations $f(P_i) = 0$ impose linear conditions on V_k. Denote by $s_k(P_1, \ldots, P_n)$ number of linearly dependent conditions among these $f(P_i) = 0$ defining $W_k(P_1, \ldots, P_n)$. Then one obviously has

$$dim\, W_k(P_1, \ldots, P_n) - s_k(P_1, \ldots, P_n) = dim\, V_k - n$$

what is known in algebraic geometry as the Riemann–Roch equality.

If H_1, H_2 are hypersurfaces of respective degrees d_1, d_2, which intersect in $d = d_1 \cdot d_2$ different F-rational points $P_1, \ldots, P_d$, then Cayley–Bacharach theorem provides us with a formula which becomes useful to compute values of s_k for subsystems of points the above set. Thus, for $n < d_1 d_2$ Cayley–Bacharach states that

$$dim\, W_{k'}(P_{n+1}, \ldots, P_d) - dim\, W_{k'}(P_1, \ldots, P_d) = s_k(P_1, \ldots, P_n)$$

where $k' = d_1 + d_2 - 3 - k$, provided $0 \leq k \leq d_1 + d_2 - 3$.

In general, one needs in practice to consider general systems of points, which are nothing but F-rational zero-dimensional subschemes of $\mathbf{P^2}$, given by the data of an ideal sheaf $\mathcal{I} \subset \mathcal{O}_{\mathbf{P^2}}$ such that $\ell(\mathcal{I}) = \ell(\mathcal{O}_{\mathbf{P^2}}/\mathcal{I})$ is finite. In fact, for the given data $\mathcal{I}$, the subscheme $Z(\mathcal{I})$ is what we will call a system of $\ell(\mathcal{I})$ points. For the system of points $Z = Z(\mathcal{I})$ also one can define $W_k(Z)$ and $s_k(Z)$ in an obvious way.

If $\mathcal{I} \supset \mathcal{I}_\Gamma$, where $\mathcal{I}_\Gamma = (F_1, F_2)$ is the ideal of the proper complete intersection Γ of two curves of degrees d_1, d_2, given respectively by the equations F_1, F_2, then the complement $Z' = Z(\mathcal{I}')$ of $Z = Z(\mathcal{I})$ in Γ is given by $\mathcal{I}' = \mathrm{Ann}_{\mathcal{O}_{\mathbf{P^2}}}(\mathcal{I}/\mathcal{I}_\Gamma)$. Thus, Riemann–Roch and Cayley–Bacharach equalities are written respectively as

$$\begin{array}{l} dim\, W_k(Z) - s_k(Z) = dim\, V_k - \ell(\mathcal{I}) \\ dim\, W_{k'}(Z') - dim\, W_{k'}(\Gamma) = s_k(Z), \quad \textit{where} \;\; k' = d_1 + d_2 - 3 - k \end{array}$$

Now we will introduce some cohomological tools, since they are not only a standard notation (see [4]) but they will become useful for the computations along the rest of this paper. In fact, notice that one has that $H^0(\mathcal{I}(k)) = W_k(Z)$, $h^0(\mathcal{I}(k)) = dim\, W_k(Z)$ and $h^1(\mathcal{I}(k)) = s_k(Z)$, i.e. the considered integers $dim\, W_k(Z)$ and $s_k(Z)$ are nothing but the respective dimensions of the order 0 and 1 cohomologies of the twisted sheaf $\mathcal{I}(k)$.

Now, the statements given in Riemann–Roch and Cayley–Bacharach theorems can be rewritten as the following propositions.

Proposition 1 (Riemann–Roch theorem)
For any system of points $Z = Z(\mathcal{I})$ and any integer $k \geq 0$ one has

$$h^0(\mathcal{I}(k)) - h^1(\mathcal{I}(k)) = \frac{(k+1)(k+2)}{2} - \ell(\mathcal{I})$$

Proposition 2 (Cayley–Bacharach theorem)
If $Z = Z(\mathcal{I})$ is a subscheme of the proper complete intersection $\Gamma = Z(\mathcal{I}_\Gamma)$ of two curves os degrees d_1, d_2, and $Z' = Z(\mathcal{I}')$ is the complement of Z in Γ, then for $0 \leq k \leq d_1 + d_2 - 3$ one has

$$h^0(\mathcal{I}'(k')) - h^0(\mathcal{I}_\Gamma(k')) = h^1(\mathcal{I}(k))$$

where $k' = d_1 + d_2 - 3 - k$.

The proof of Riemann–Roch theorem is elementary, and that of Cayley–Bacharach theorem can be found in [4] (Satz CB7).

3 The singular locus of algebraic foliations on the projective plane

In this section we will consider algebraic foliations on $\mathbf{P^2} \equiv \mathbf{P^2}_{\mathbf{F}}$, defined over finite field F. Since F is a perfect field, such foliations can be seen as objects over $\mathbf{P^2} \equiv \mathbf{P^2}_{\overline{\mathbf{F}}}$, $\overline{F}$ being an algebraic closure of F, which are invariant under the elements of the Galois group $\mathcal{G}al(\overline{F}/F)$, and hence there is no need of assuming the geometrical context and, therefore, one can describe and study foliations by means of rational over F objets and properties related to them.

The concept of algebraic foliation is introduced in various equivalent ways, so that the reader can find something one is familiar with. If it results confusing for, one can just think that such a foliation can be described as a kind of vector field on the projective plane, namely as an objet given by the data of a vector field over a nonempty open set. This description could be the most helpful for intuition, whereas, for instance, the ideal sheaf description could be more useful for proofs and computations.

Let F be a finite field with q elements, and $X : Y : Z$ homogeneous coordinates on the projective plane $\mathbf{P^2}$ over F. A foliation $\mathcal{F}$ of degree $r \geq 0$ on $\mathbf{P^2}$ is given by a differential form $\Omega = AdX + BdY + CdZ$ (determined up to a multiplicative constant in F^*) where A, B, C are homogeneous polynomials in $F[X, Y, Z]$ of degree $r+1$ without non constant common factor and satisfying the Euler condition $XA+YB+ZC = 0$. On the affine chart $\mathcal{A}^2$ given by $Z \neq 0$, the foliation is given by the differential form $\omega = a(x, y)dx+b(x, y)dy$, where $a(x, y) = A(x, y, 1)$ and $b(x, y) = B(x, y, 1)$, or equivalently by the vector field $\delta = b(x, y)\partial_x - a(x, y)\partial_y$, or even by the first order differential equation $b(x, y)y' + a(x, y) = 0$. In fact, the foliations becomes the same data as either the differential form ω, either the vector field δ, or the associated differential equation. In other words, if for instance δ is given, then what one actually has is a vector field and the foliation can be seen as nothing but a certain object that extends δ to $\mathbf{P^2}$ in a way that is useful for both algebraic and geometric purposes.

In the same way, the foliation can be regarded as a certain kind of extension to $\mathbf{P^2}$ of an algebraic differential equation on the affine plane $\mathcal{A}^2$. In geometric terms, such an extension is carried out by means of the rational map Φ from $\mathbf{P^2}$ to its dual projective plane which takes each point q to the projective line through q which has the direction of the vector giving locally the foliation at q. Such a map, which is called polarity in [2] (section 1) is given by the linear net of (prime) divisors whose equations are in the vector space V generated by the forms A, B, C. Thus, divisors in the net are nothing but pullbacks of hyperplanes in the dual space, so they correspond one to one with points in the plane, in such a way that each such divisor is called the polar with respect to $\mathcal{F}$ of the corresponding point (the pole of the polar) in the plane. Using elementary algebraic geometry, one can have a complete background on foliations in terms of Φ.

The singular scheme of $\mathcal{F}$ is defined to be the zero dimensional closed subscheme of $\mathbf{P^2}$ given by the indeterminacy ideal $\mathcal{I}$ of the polarity map Φ, i.e. the ideal $\mathcal{I} = (A, B, C)$. Locally, on each affine chart, $\mathcal{I}$ is generated by the coefficients of the form ω, or those of the vector field δ defining the foliation (for instance, on the affine chart $\mathcal{A}^2$, $\mathcal{I}$ is nothing but the ideal (a, b) of the polynomial ring). In particular, $\mathcal{I}$ is a local complete intersection. Finally, if for an ideal sheaf $\mathcal{J}$ of $\mathcal{O}_{\mathbf{P^2}}$ with zero dimensional support, $\ell(\mathcal{J})$ stands for the colength of $\mathcal{J}$ at $\mathcal{O}_{\mathbf{P^2}}$, then for the ideal of the singular scheme of the foliation one has

$$\ell(\mathcal{I}) = r^2 + r + 1$$

(See [2], proposition 1.1, for the details).

In [2] (theorem 3.2, case $t = 0$) it is shown that $H^0(\mathcal{I}(r + 1)) = V$ and that, if $r \geq 2$, one has that the singular scheme (as subscheme of the plane) uniquely determines $\mathcal{F}$. Moreover, a given zero dimensional locally complete intersection subscheme $Z(\mathcal{I})$ with $\ell(\mathcal{I}) = r^2 + r + 1$, $r \geq 2$ is the singular scheme of a foliation if and only if the following two conditions are satisfied:

1. $h^0(\mathcal{I}(r + 1) \geq 3$.

2. For each j, $1 \leq j \leq r-1$, and each ideal $\mathcal{J}$ with $\mathcal{I} \subset \mathcal{J}$ and such that $\ell(\mathcal{J}) = (r-j)(r+j+1)$, one has $h^0(\mathcal{J}(r-j)) = 0$.

In other words, one can say that the "system of points" $Z = Z(\mathcal{I})$ is the singular scheme of a degree r foliation on $\mathbf{P^2}$ if and only if there are at least three independent divisors of degree $r+1$ passing through the points of Z and for each j, $1 \leq j \leq r-1$, there are no subset of $(r-j)(r+j+1)$ points of Z lying on a divisor of degree $r-j$.

In fact, one can prove a finer result than the above mentioned one and concerning with nonexistence of fixed degree divisors passing through points of Z. Since this result is new and also will provide better bounds for the parameters of the codes considered in the next sections, we will prove it here.

Theorem 1 *Let $\mathcal{F}$ be a foliation of degree $r \geq 1$ on $\mathbf{P^2}$ and $Z = Z(\mathcal{I})$ its singular scheme. Then one has:*

1. *For any j, $1 \leq j \leq r-2$ and each ideal $\mathcal{J}$ with $\mathcal{I} \subset \mathcal{J}$ and such that $\ell(\mathcal{J}) = (r+1)(r-j)$, one has $h^0(\mathcal{J}(r-j)) = 0$.*
2. *For each ideal $\mathcal{J}$ with $\mathcal{I} \subset \mathcal{J}$ and such that $\ell(\mathcal{J}) = (r+2)$, one has $h^0(\mathcal{J}(1)) = 0$.*
3. *For each ideal $\mathcal{J}$ with $\mathcal{I} \subset \mathcal{J}$ and such that $\ell(\mathcal{J}) = (r+1)$ one has either $h^0(\mathcal{J}(1)) = 0$ or $Z(\mathcal{J})$ lies on an invariant line for $\mathcal{F}$.*

Proof Assume that C is a divisor of degree $r-j$ given by a nonzero element of $H^0(\mathcal{J}(r-j))$, where $Z(\mathcal{J})$ is a subscheme of $Z(\mathcal{I})$ such that $\ell(\mathcal{J}) = (r+1)(r-j)$. Then take a (non necessarily rational over F) geometric point p of $\mathrm{Supp}(C)$ not in $Z(\mathcal{I})$. Then the elements of the net of polars passing through p form a pencil which is either free of base curves or it has an invariant line L as base curve (in this case the pencil consists exactly of the polars of the points of L).

First, assume that C is reduced irreducible. Then the curve C and a generic polar P of the pencil intersect properly except if $C = L$ is an invariant line. If C is not an invariant line, then Bezout theorem implies that $(r+1)(r-j)$ is the maximum number of points (counted properly) lying on the intersection of C and P (i.e. the intersection zero dimensional scheme of both curves has colength equal to $(r+1)(r-j)$). Since p is in $C \cap P$, one has $(r+1)(r-j)+1$ points, namely those in $Z(\mathcal{J})$ together with P, lying on the intersection of C and P. This is a contradiction, and hence such curves C cannot exist. If, otherwise, $C = L$ is an invariant line, then by applying the same argument to the intersection of L and a generic polar of the net, one would find that at most $r+1$ points of $Z(\mathcal{I})$ lie on L.

Now, assume that C is non reduced or non irreducible. Then the same argument works when C has no invariant line as a component. If C has invariant lines as components, then applying above arguments to the components of C one gets the conclusion that C can not exist as well. This is obvious if some of the components is not an invariant line. If C consists of only invariant lines as components, then the intersection of two of them will be a singular point of $\mathcal{F}$ and, therefore, at most $2r+1 < 2(r+1)$ points of $Z(\mathcal{I})$ can lie on the union of both lines. If C has only a multiple component which is an invariant line L, then L can meet a generic polar of the net at most at $r+1$ singular points, so that C can not contain $(r+1)(r-j)$ points of $Z(\mathcal{I})$, $r-j$ being the degree of C.

The above collection of facts shows that $h^0(\mathcal{J}(r-j)) = 0$ if either $1 \leq j \leq r-2$ and $\ell(\mathcal{J}) = (r+1)(r-j)$, or $j = r-1$ and $Z(\mathcal{J})$ lies on an invariant projective line for $\mathcal{F}$, and that $h^0(\mathcal{J}(1)) = 0$ if $\ell(\mathcal{J}) = (r+2)$. This proves the theorem.

□

Remark 1 From above theorem one can deduce a better characterization of singular subschemes of foliations. In fact, one has that $Z = Z(\mathcal{I})$ is the singular locus of a foliation in $\mathbf{P^2}$ with degree $r \geq 2$ if and only if

1. there are at least 3 independent divisors of degree $r+1$ passing through the points of Z,
2. for each $1 \leq j \leq r-2$ there is no subset with $(r-j)(r+1)$ points of Z lying on a divisor of degree $r-j$, and
3. there is no subset of $r+2$ points of Z lying on a (projective) line.

4 Evaluation codes at singularities of differential equations

Keeping notations as in the above section, consider a foliation $\mathcal{F}$ of degree $r \geq 2$ on the projective plane $\mathbf{P^2}$ over the finite field F with q elements. From now on, we will assume that the singularities of $\mathcal{F}$ are reduced and rational over F, i.e. that the support of $Z(\mathcal{I})$ consists of r^2+r+1 different points of $\mathbf{P^2}$ and that all of them are rational over F. This strong assumption implies, in fact, that $r \leq q$, as the number of rational points of the projective plane is given by q^2+q+1.

Denote by $P_1, ..., P_n$ the points in $Z(\mathcal{I}) \cap \mathcal{A}^2$ and by l the cardinality of $Z(\mathcal{I}) \cap H$, H being the infinite line given by $Z = 0$. One obviously has

$$r^2 + r + 1 = n + l$$

Let m be an integer, $1 \leq m \leq 2r-2$, and denote by $E_m = E_m(\mathcal{F}, H)$ the AG code given by evaluation of the functions of $\mathcal{L}(mH) = F[x,y]_{\leq m}$ at the rational points $P_1, ..., P_n$. In other words E_m is the image of the linear map

$$\mathcal{E} : F[x,y]_{\leq m} \longrightarrow F^n$$

given by

$$f \rightarrow (f(P_1), ..., f(P_n))$$

Next, we will show how the knowledge of the geometry of the singular scheme of $\mathcal{F}$ provides exact formulas for the dimension of the codes E_m and accurate bounds for their minimum distance. In this section, we will compute the dimensions $k(E_m)$. Notice that the length n of those codes is given by $n = r^2+r+1-l \geq r^2$, the last inequality coming from the fact that $l \leq r+1$ which follows from Theorem 1.

Along the rest of the paper, for every non negative integer s, N_s will stand for the number of monomials of degree s in three variables, i.e. $N_s = (s+1)(s+2)/2$.

Theorem 2 *With assumptions and notations as above, one has*

$$k(E_m) = N_m,$$

for $1 \leq m \leq r-1$,

$$k(E_m) = N_m - (m-r)(m-r+2) - max(0, l+m+1-2r)$$

for $r \leq m \leq 2r-2$.

Proof If $1 \leq m \leq r-1$, we claim that the evaluation map $\mathcal{E}$ is injective. In fact, if otherwise, one would have a curve C of degree m passing through $n \geq r^2$ points of $Z = Z(\mathcal{I})$, which contradicts Theorem 1 (notice that $r \geq 2$). Thus, the claim implies that $k(E_m) = N_m$.

If $r \leq m \leq 2r-2$, denote by $\mathcal{J}$ the ideal of the set of points $P_1, ..., P_n$ and by $\mathcal{J}'$ the ideal of the points in $Z(\mathcal{I}) \cap H$. Since $Ker(\mathcal{E}) = H^0(\mathcal{J}(m))$, one has

$$k(E_m) = N_m - h^0(\mathcal{J}(m)) = n - h^1(\mathcal{J}(m)),$$

the last equality being derived from Riemann–Roch theorem. Now, from Cayley–Bacharach theorem (see [4]), applied to complements of the complete intersection of two generic polars of the net, together with theorem 1, one has

$$h^1(\mathcal{J}(m)) = h^0(\mathcal{J}''(2r-m-1)) = h^0(\mathcal{J}'(2r-m-2))$$

where $\mathcal{J}''$ is the ideal of the residual of $Z(\mathcal{J})$ in the complement of the two generic polars. The last equality follows from the fact that $Z(\mathcal{J}'') = Z(\mathcal{J}') \cup Z^*$ where Z^* is a set of r points lying on a line, taking into account that $2r-m-1 < r$. Now, again from Riemann–Roch, one deduces that

$$h^0(\mathcal{J}'(2r-m-2)) = h^1(\mathcal{J}'(2r-m-2)) + N_{2r-m-2} - l$$

Finally, since the points in $Z(\mathcal{J}')$ are distinct points of a line, one has that

$$h^1(\mathcal{J}'(2r-m-2)) = 0$$

if $l \leq 2r-m-1$, and

$$h^1(\mathcal{J}'(2r-m-2)) = l - (2r-m-1)$$

if $l > 2r-m-1$. Taking the above equalities all together, one gets the equality

$$\begin{aligned} k(E_m) &= n + l - N_{2r-m-2} - max(0, l+m+1-2r) = \\ &= N_m - (m-r)(m-r+2) - max(0, l+m+1-2r) \end{aligned}$$

in the statement of the theorem.

□

5 Estimates for the minimum distance for evaluation codes at singularities of differential equations

In this section we will prove the main result in the paper, providing estimates which can be seen as accurate ones for the evaluation codes E_m considered in the above section. This result is stated in the next theorem.

Theorem 3 *Keeping notations and assumptions as in the above section, one has*

$$d(E_1) \geq r^2 - l$$
$$d(E_m) \geq (r+1)(r-m) - l + 2$$

for $2 \leq m \leq r-1$,

$$d(E_m) \geq 2r - m - l$$

for $r \leq m \leq 2r-2$ *if* $l < 2r - m - 1$,

$$d(E_m) \geq 2r - m - 1$$

for $r \leq m \leq 2r-2$ *if* $l \geq 2r - m - 1$.

Proof If $w(\mathbf{c}) = d(\mathbf{c}, \mathbf{0})$ denotes the weight of a codeword $\mathbf{c}$, notice that, since the code is linear, the minimum distance is equal to the minimum of the values of $w(\mathbf{c})$ for $\mathbf{c}$ ranging over the non zero codewords in E_m.

First, assume $1 \leq m \leq r-1$. If $w = w(\mathbf{c})$ for a nonzero codeword $\mathbf{c}$, then there is a divisor C of degree m passing through $n-w$ points of $Z(\mathcal{J})$. From Theorem 1, it follows that one would have $n - w < (r+1)m$ if $m \geq 2$ and $n - w \leq (r+1)$ if $m = 1$. Hence, one derives the estimates $d(E_1) \geq r^2 - l$ and $d(E_m) \geq (r+1)(r-m) - l + 2$ for $2 \leq m \leq r$.

Now, assume $r \leq m \leq 2r-2$. Then, one can proceed as follows: if one finds a positive integer d such that for every ideal $\mathcal{K}$ with $\mathcal{J} \subset \mathcal{K}$ and $\ell(\mathcal{K}) = n - d + 1$ one has $h^0(\mathcal{K}(m)) = h^0(\mathcal{J}(m))$, then one has $d(E_m) \geq d$. In fact, the proof of the above statement follows from the fact that if each time that a divisor of degree m passes through $n-d+1$ points of $Z(\mathcal{J})$ then one knows that it also passes through all $P_i's$, then the weights of all nonzero codewords are at least equal to d.

Now, using Riemann–Roch and Cayley–Bacharach theorems exactly as in the proof of Theorem 2, above statement can be translated into one which involves residual schemes (actually, residual sets of points). Thus, one can proceed also as follows: if one finds a positive integer d such that for every ideal $\mathcal{K}'$ with $\mathcal{I} \subset \mathcal{K}' \subset \mathcal{J}'$ and $\ell(\mathcal{K}') = d-1+l$ one has $h^1(\mathcal{J}'(2r-m-2)) = h^1(\mathcal{K}'(2r-m-2))$, then one has $d(E_m) \geq d$. In order to handle this statement, there are two possibilities. If $l \geq 2r-m-1$, then the divisors of degree $2r-m-2$ containing $Z(\mathcal{J}')$ should contain the line H itself and, therefore, the condition in the statement means that the points in $Z(Ann(\mathcal{J}'/\mathcal{K}'))$ should impose independent conditions to divisors of degree $2r-m-3$. This is always guaranteed for values of d with $d-1 \leq 2r-m-3+1$, i.e. for values of d with $d \leq 2r-m-1$. If $l < 2r-m-1$, then one has $h^1(\mathcal{J}'(2r-m-2)) = 0$, therefore, the condition in the statement is nothing but $h^1(\mathcal{K}'(2r-m-2)) = 0$ which can be guaranteed if one has $d-1+l \leq 2r-m-2+1$, i.e. if one has $d \leq 2r-m-l$. This completes the proof of the theorem.

□

Remark 2 From the proof of the previous theorem one could obtain, for particular cases, better conclusions for the bounds of the codes. For example, take $m = 2r - 4$ with $r \geq 4$ and $l < 2r - m - 1 = 3$ (i.e. $r = 0, 1, 2$). If one assumes that there exists no line passing through three of these $r^2 + r + 1$ points, then for all $\mathcal{K}' \supseteq \mathcal{J}'$ with $\ell(\mathcal{K}') = 5$ one has $h^1(\mathcal{K}'(2)) = 0$ (here $2r-m-2 = 2$). Thus, the condition for d in Theorem 3 works with $5 = d-1+l$ and hence $d \geq 6 - l$. In this case $n = r^2 + r + 1 - l$, and by Theorem 2 one has $k = r^2 + r - 5$, and thus these codes satisfy $k + d = n$.

On the other hand, taking $m = 2r - 5$ for $r \geq 5$ and $l \geq 2r - m - 1 = 4$ (i.e. $4 \leq l \leq r + 1$), if one assumes now that there exists no line passing through three of the $r^2 + r + 1 - l$ singular affine points, then $h^1(\mathcal{K}^*(2)) = 0$ for all $\mathcal{K}^* \supseteq \mathcal{J}$ with $\ell(\mathcal{K}^*) = 5$ (here $2r - m - 3 = 2$ and $\mathcal{K}^* = Ann(\mathcal{K}'/\mathcal{J}')$. In this case, the equality $d-1 = 5$ shows that $d = 6$ is a lower bound for the minimum distance. Now $n = r^2+r+1-l$ and by Theorem 2, $k = r^2+r-5+l$ and $d = 6$, and again $k + d = n$.

In both cases, the bound for d is better than the one given by Theorem 3 ($4 - l$ in the fist case and 4 in the second one), and it follows from the idea of the proof, not from the statement of the theorem itself. In this way, the additional assumption that there are not three points on the same line improves the bound for the minimum distance. This assumption seems to be feasible for q large with respect to r.

From the results of this paper one easily can prove the following result, concerning the number $k + d$.

Theorem 4

(I) For $r \leq m \leq 2r - 2$, write $u = 2r - 2 - m$ for some $u \in [0, r - 2]$. Then $k + d \geq n + 1 - g$ where

$$g := \begin{cases} u(u+1)/2 \text{ if } l \leq u \\ u(u-1)/2 \text{ if } l > u \end{cases}$$

In fact, there are similar bounds for d and k, namely
- *$d \geq u + l + 2$ (resp. $d \geq u + 1$) if $l \leq u$ (resp. $l > u$).*
- *$k \geq r^2 + r - u(u + 3)/2$ (resp. $d \geq r^2 + r - l - (u - 1)(u + 2)/2$) if $l \leq u$ (resp. $l > u$).*

(II) For $1 \leq m \leq r - 1$, write $u = r - m$ for some $u \in [1, r - 1]$. Then $k + d \geq n + 1 - g$ where

$$g := \begin{cases} \dfrac{1}{2r(r-1)} - \dfrac{1}{2u(u-1)} & \textit{if } u < r - 1 \\ r - 2 & \textit{if } u = r - 1 \end{cases}$$

In fact, $k = 1/2(m + 1 - u)(m + 2 - u)$ and $d \geq (r + 1)u - l + 2$ (resp. $d \geq (r+1)u-l+1 = (r+1)(r-1)-l+1$) if $u < r-1$ (resp. $u = r-1$).

This last result shows certain analogies with the case of AG codes, concerning the estimates of the parameters of those codes in terms of the genus of the curve, namely the so-called Goppa estimates (see [7], theorems 2.65 and 2.69, and section 2.9).

6 Some remarks and examples

Results in Theorem 3 are used to search for codes with preassigned minimum distance. This is one of the applications of that class of codes. In a certain sense, this class can be seen as an alternative to the class of evaluation codes at points of a complete intersection treated in [6]. In that paper, polynomials are evaluated in the points of a complete intersection which are in an affine open set of a general projective l-space. Instead, we evaluate at the singular locus of a foliation, which is a part of special complete intersections (those given by two generic polars, which are nothing but appropiated associated curves which theoretically exist but which need not to be fixed a priori), so that what is left to be a complete intersection is a set o r points in a line, which are not necessarily rational over the base field (and needs not to be explicitly considered). This special situation allows us to obtain special results for slightly different sets of points. Finally, notice that although for the sake of simplicity we consider evaluation on sets of singular points of foliations on the affine plane, one could also evaluate on sets of singular points on arbitrary open sets of the projective plane (as done [6]) without essential differences.

The characterization of the subschemes which are singular schemes of foliation given in [2] has in its statement the weakest possible hypothesis on postulation of the points. Further characterizations can be obtained by making those hypothesis stronger. Thus, one can state a similar characterization in terms of such conditions in Theorem 1. This fact can be applied to improving bounds on the parameters of evaluation codes, since stronger conditions on postulation provide better estimates for the minimum distance. Thus, for instance, if $2 \leq m \leq r-1$, Theorem 3 provides the bound $d(E_m) \geq (r+1)(r-m)-l+2$ which is better than the bound $d(E_m) \geq (r-m)^2+(r-m)+1-l$ deduced from the characterization statement in [2].

The maximum value of r for a foliation satisfying the assumption imposed on Section 3 is $r=q$. In fact such a foliation of degree q exists and it is unique. It is a foliation having as singular scheme the reduced set of all rational points of the projective space. In analytic terms, this foliation is given by the differential form

$$\begin{aligned} \Omega = {} & YZ(Y^{q-1}-Z^{q-1})dX+ \\ & +ZX(Z^{q-1}-X^{q-1})dY+ \\ & +XY(X^{q-1}-Y^{q-1})dZ \end{aligned}$$

Thus, among the family of evaluation codes at the singularities of a differential equation one finds the Reed-Muller codes, one of the few cases of AG codes for which the minimum distance has been determined exactly. Looking to Reed-Muller codes, one realizes that the bound for the minimum distance in Theorem 3 is sharp for all the values $r \leq m \leq 2r-2$. In general, improvements of the bounds for the minimum distance could be obtained by using the procedure in the proof of Theorem 3 and remark 1.

For concrete parameters one can find some appropriate foliations giving good codes. For instance, we show a simple example for $q=3$ and $r=2$, with $q-1$ points at infinity (i.e. $n=5$ and $l=2$). Consider the points in the affine chart $z = 1$ given by

$$P_1 = (0,0),\ P_2 = (1,1),\ P_3 = (1,2),$$
$$P_4 = (2,1),\ P_5 = (2,2)$$

and the points at infinity $Q_1 = (1:0:0)$ and $Q_2 = (0:1:0)$. The forms for the corresponding foliation is given by

$$\begin{aligned} A &= x(z^2 - y^2) \\ B &= y(x^2 - z^2) \\ C &= z(y^2 - x^2) \end{aligned}$$

Notice that they satisfy the Euler equation and they have no common factor. Taking $m = 1$ one obtains a code with parameters $n = 5$, $k = 3$ and $d = 2$.

In the same way, for $q = 3$ and $r = 2$ but now with just one point at infinity (i.e. $n = 6$ and $l = 1$), we consider the affine points ($z = 1$) given by

$$P_1 = (0,0),\ P_2 = (0,2),\ P_3 = (1,1),$$
$$P_4 = (1,2),\ P_5 = (2,1),\ P_6 = (2,2)$$

and the point $Q = (0:1:0)$ at infinity. Now the possible forms for the foliations are given by

$$\begin{aligned} A &= (y+z)(yz - x^2) \\ B &= x(x^2 - z^2) \\ C &= x(x^2 - y^2) \end{aligned}$$

If $m = 1$ one gets a code with parameters $n = 6$, $k = 3$ and $d = 3$, which is easily checked to be optimum, in the sense that any other code with the same parameters n and k over the finite field with q elements cannot have a larger minimum distance (one can check it by using the Main Conjecture MDS, on *maximum distance separable* codes, see [8]).

As a final remark, note that although the searching of good codes constructed in this way is based on some deep results about foliations, the practical construction is quite elementary once you choose the suitable foliation and fix the numbers q, r, l and m. In fact, the points are computed in terms of Groebner bases from the equations of the forms, and afterwards all we have to do is evaluating monomials at points in the affine plane. The computer algebra system SINGULAR [5] is a very efficient tool to perform computations. Moreover, you do not even need the foliation, but just need to know that a certain set of points is the set of singular affine points of such a foliation, and this can be done from [2] (corollary 4.10) in geometric terms, just by checking whether curves of some degrees pass through a certain number of points or not.

References

1. A. Campillo, J. Olivares: *"Assigned conditions and geometry of foliations on the projective plane"*. Advanced Studies in Pure Mathematics, Math. Soc. Japan 29, pp. 97-113 (2000).
2. A. Campillo, J. Olivares: *"Polarity with respect to a foliation and Cayley–Bacharach theorems"*. J. Reine Angew Math. 534, pp. 95-118 (2001).

3. A. Campillo, J. Olivares: *"On sections with isolated singularities of twisted bundles and applications to foliations by curves"*. Math. Res. Letters 10, 5-6, pp. 651-658 (2003).
4. D. Eisenbud, M. Green, J. Harris: *"Cayley–Bacharach theorems and conjectures"*. Bull.Amer.Math.Soc. 33, 3, pp. 295-324 (1996).
5. G.-M. Greuel, G. Pfister and H. Schönemann: "SINGULAR *2.0: A computer algebra system for polynomial computations"*. Centre for Computer Algebra, University of Kaiserslautern (2001). Available via `http://www.singular.uni-kl.de/`.
6. J. Hansen: *"Linkage and codes on complete intersections"*. Applicable Algebra in Engineering, Communication and Computing 14, 3, pp. 175-185 (2003).
7. T. Hoholdt, J.H. Van Lint, R. Pellikaan: *"Algebraic geometric of codes"*. In Handbook of coding theory, Vol. I, pp. 871-961, Elsevier, North-Holland, Amsterdam (1998).
8. F.J. MacWilliams, N. Sloane: *"The theory of error-correcting codes"*. North Holland Mathematical Library, Vol.16, North Holland Publ.Co., Amsterdam (1977).