Discrete Mathematics 90 (1991) 21–40
North-Holland

The decoding of extended Reed–Solomon codes

Arne Dür

Mathematisches Institut, Universität Innsbruck, 6020 Innsbruck, Austria

Received 23 November 1987
Revised 9 May 1989

Abstract

Dür, A., The decoding of extended Reed–Solomon codes, Discrete Mathematics 90 (1991) 21–40.

Cauchy codes are a class of maximum distance separable codes that include Reed–Solomon codes, singly- and doubly-extended Reed–Solomon codes, and reversible BCH over GF(2^m) of length $2^m + 1$. The decoding problem for Cauchy codes is studied by using an analogue of the classical theory of apolarity of binary forms, and Berlekamp's decoding algorithm for Reed–Solomon codes is extended to Cauchy codes. The covering radius of a Cauchy code over GF(q) of length n and minimum distance d is shown to be either $d-2$ or $d-1$, and the exact value is determined unless $n = q + 1$ and $q/2 + 3 < d < q$. If $n = q + 1$ and $d = q$ is even, the covering radius is $q - 1$, and the determination of all cosets with leaders of weight $q - 1$ is equivalent to the determination of all ovals with $q + 2$ points in the projective plane.

1. Introduction

In this paper we study the decoding of Cauchy codes and determine the covering radius for most of these codes. Cauchy codes are a class of maximum distance separable codes which have been introduced in [8] and include generalized Reed–Solomon codes [7] and generalized doubly-extended Reed–Solomon codes [21, 17, 19]. In Section 2 we formulate the decoding problem for Cauchy codes in terms of binary forms. In Section 3 we develop an analogue of the classical theory of apolarity of binary forms [11, ch.XI] which provides the algebraic background for our discussion of the decoding problem. The results of this section are then applied to Cauchy codes in Section 4.

We present a general decoding algorithm for Cauchy codes which decodes up to the packing radius of the code and is based on Berlekamp's decoding algorithm for Reed–Solomon codes. In the literature [21; 3, sec. 9.3], doubly-extended Reed–Solomon codes are decoded by applying Berlekamp's algorithm twice. Our algorithm uses Berlekamp's algorithm only once and, for Reed–Solomon codes,

0012-365X/91/$03.50 © 1991 — Elsevier Science Publishers B.V. (North-Holland)

is similar to the variations of Berlekamp's algorithm proposed in [20] and [4]. Furthermore, our algorithm always produces a candidate for the error locator polynomial of degree less than or equal to the packing radius of the code, and thus avoids one failure mode of Berlekamp's algorithm.

Finally, we prove that the covering radius of a Cauchy code over GF(q) of length n and minimum distance d is either $d-1$ or $d-2$, and we determine the exact value unless $n = q+1$ and $q/2+3 < d < q$. If $n = q+1$ and $d = q$ is even, the covering radius is $d-1$ and the determination of all deep holes of the sphere packing in Hamming space defined by the code is equivalent to the determination of all ovals with $q+2$ points in the projective plane, which is known to be a difficult problem of finite geometry [12, sec. 8.4].

2. Syndromes of Cauchy codes

We first introduce some notation. Let K be a field. Let $K^* = K \setminus \{0\}$ denote the group of nonzero elements of K, let $\bar{K} = K \cup \{\infty\}$ denote the projective line over K, and let $K[X, Y]_\kappa$ denote the vector space of binary forms over K of degree κ. For $P \in K[X, Y]_\kappa$, $P = \sum_{i=0}^{\kappa} a_i X^i Y^{\kappa-i}$, we set $P(z) := P(z, 1)$ if $z \in K$, and $P(z) := P(1, 0)$ if $z = \infty$.

We next recall the definition of a Cauchy code from [8]. Our general reference for coding terminology is [15].

Definition 0. Let $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ where the α_i are distinct elements of $\bar{K}$, let $y = (y_1, y_2, \ldots, y_n)$ where the y_i are elements of K^*, and let $1 \leq k \leq n-1$. Then the Cauchy code $C_k(\alpha, y)$ consists of all vectors

$$(y_1 P(\alpha_1), y_2 P(\alpha_2), \ldots, y_n P(\alpha_n))$$

where P ranges over all elements of $K[X, Y]_{k-1}$. $C_k(\alpha, y)$ is an $[n, k]$-code over K of minimum distance $d = n+1-k$. The subset $L = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ of $\bar{K}$ is called the location set of $C_k(\alpha, y)$.

Example 0. The class of Cauchy codes includes Reed–Solomon codes ($L = K^*$), singly-extended Reed–Solomon codes ($L = K$), doubly-extended Reed–Solomon codes ($L = \bar{K}$), and reversible BCH codes over $K = \mathrm{GF}(2^m)$ of length $2^m + 1$ ($L = \bar{K}$). See [8] and [9] for details.

Now let $C = C_k(\alpha, y)$ be a Cauchy code with location set L. According to [8, Theorem 1], the dual code of C is $C_{n-k}(\alpha, y')$, and a parity check matrix of C is $H = (y_i' P_l(\alpha_i); l = 0, 1, \ldots, \kappa, i = 1, 2, \ldots, n)$ where $y_i' \in K^*$ has been defined in [8, Theorem 1], $P_l = X^l Y^{\kappa - l}$, and $\kappa = d-2$. Then, for $x = (x_1, x_2, \ldots, x_n) \in K^n$, the vector $(s_0, s_1, \dots, s_\kappa) \in K^{\kappa+1}$,

$$s_l = \sum_{i=1}^{n} x_i H_{li} = \sum_{i=1}^{n} x_i y_i' P_l(\alpha_i),$$

is usually called the syndrome of x. It will prove more convenient, however, to use a binary form instead of a vector.

Definition 1. The syndrome of the vector $x \in K^n$ is the binary form

$$S_x = \sum_{l=0}^{\kappa} s_l P_{\kappa-l} = \sum_{i=1}^{n} y_i' x_i \langle \alpha_i \rangle \in K[X, Y]_\kappa$$

where, for $z \in \bar{K}$,

$$\langle z \rangle = \sum_{l=0}^{\kappa} P_{\kappa-l}(z) P_l.$$

E.g.,

$$\langle 0 \rangle = X^\kappa, \qquad \langle 1 \rangle = \sum_{l=0}^{\kappa} X^l Y^{\kappa-l}, \quad \text{and} \quad \langle \infty \rangle = Y^\kappa.$$

Then the decoding problem for Cauchy codes reads as follows.

Problem 1. Given $S \in K[X, Y]_\kappa$, find a representation $S = \sum_{z \in N} \lambda(z) \langle z \rangle$ of minimal length where $N \subset L$ and $\lambda(z) \in K^*$.

3. An analogue of the theory of apolarity of binary forms

In the classical theory of invariants of binary forms with coefficients in the complex numbers, the concept of apolarity can be used to solve the following problem:

Given a binary form $P = \sum_{i=0}^{\kappa} a_i X^i Y^{\kappa-i}$, find the minimum number ν such that P can be written as a sum of ν κth powers of linear forms ("Waring's problem for binary forms").

A first step to the solution of this problem is the following result.

The binary form P is the sum of μ or fewer κth powers of linear forms if and only if there exists a binary form $Q = \sum_{j=0}^{\mu} b_j X^j Y^{\mu-j}$ without repeated roots in $\bar{\mathbb{C}}$ such that the apolar covariant $\{P, Q\}$ vanishes. Written out, $\{P, Q\} = 0$ says that $\sum_{j=0}^{\mu} (-1)^{\mu-j} a_{j+i} b_{\mu-j} / \binom{\kappa}{j+i} = 0$ for $i = 0, 1, \dots, \kappa - \mu$.

See, e.g., [11, p. 213], [14, p. 60], and [13]. In this section, we study an analogue of the theory of apolarity of binary forms where the ground field K is arbitrary and powers of linear forms are replaced by scalar multiples of the geometric series $\langle z \rangle$, $z \in \bar{K}$. If K has characteristic 2 and $\kappa = 2^e - 1$ for some $e \geq 0$, the analogue is very similar to the theory of apolarity because in that case the binomial coefficients $\binom{\kappa}{i}$, $0 \leqslant i \leqslant \kappa$, are all equal to 1 and, for every $z \in \bar{K}$, $\langle z \rangle$ is the power of a linear form.

Definition 2. For binary forms

$$P = \sum_{i=0}^{\kappa} a_i X^i Y^{\kappa-i} \quad \text{and} \quad Q = \sum_{j=0}^{\mu} b_j X^j Y^{\mu-j},$$

the bracket of P and Q is the binary form

$$\{P, Q\} = \sum_{i=0}^{\kappa-\mu} \left(\sum_{j=0}^{\mu} a_{i+j} b_{\mu-j} \right) X^i Y^{\kappa-\mu-i}$$

if $\kappa \geqslant \mu$, and $\{P, Q\} = 0$ if $\kappa < \mu$. The bracket $\{P, Q\}$ can be interpreted as a truncated version of the product PQ.

Lemma 1. *Let P, Q, and R be binary forms. Then $\{P, QR\} = \{\{P, Q\}, R\}$. In particular, $\{P, Q\} = 0$ implies $\{P, QR\} = 0$.*

Proof. Both $\{P, QR\}$ and $\{\{P, Q\}, R\}$ are trilinear in P, Q, and R. For $P = X^i Y^{\kappa-i}$, $Q = X^j Y^{\mu-j}$, and $R = X^l Y^{\nu-l}$, it is easy to check that $\{P, QR\} = \{\{P, Q\}, R\}$. □

Definition 3. Let

$$\mathrm{GL}(2, K) = \left\{ f = \begin{pmatrix} a & b \\ c & d \end{pmatrix}; \det(f) = ad - bc \neq 0 \right\},$$

and let Gal(K) be the Galois group of K over its prime field. Then Gal(K) operates on GL(2, K) by

$$\gamma(f) = \begin{pmatrix} \gamma(a) & \gamma(b) \\ \gamma(c) & \gamma(d) \end{pmatrix}$$

and gives rise to the semidirect product

$$\Gamma L(2, K) = \mathrm{GL}(2, K) \rtimes \mathrm{Gal}(K).$$

$\Gamma L(2, K)$ admits the permutation representation

$$(f, \gamma)(z) = f(\gamma(z)) = \frac{a\gamma(z) + b}{c\gamma(z) + d}, \quad z \in \bar{K},$$

by semilinear fractional transformations on $\bar{K}$. The natural operation of $\Gamma L(2, K)$ on $K[X, Y]_\kappa$ is given by

$$(f, \gamma)P = \gamma(P)(AX + BY, CX + DY)$$

where $f^{-1} = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$ and the binary form $\gamma(P)$ is obtained from P by applying γ to each coefficient. Then $\Gamma L(2, K)$ operates on the dual space $K[X, Y]_\kappa^*$ by

$((f,\gamma)P^*)(P) = \gamma(P^*((f,\gamma)^{-1}P))$ where $P \in K[X, Y]_\kappa$ and $P^* \in K[X, Y]_\kappa^*$. On $K[X, Y]_\kappa$ the bracket is a nondegenerate symmetric bilinear form, hence $K[X, Y]_\kappa \to K[X, Y]_\kappa^*$, $P \to \{P, \cdot\}$, is an isomorphism, and pulling back the operation of $\Gamma L(2, K)$ on $K[X, Y]_\kappa^*$ gives a new operation of $\Gamma L(2, K)$ on $K[X, Y]_\kappa$, which is denoted by $*$ and satisfies

$$\{(f,\gamma) * P, (f,\gamma)Q\} = \gamma(\{P, Q\}) \tag{1}$$

for all $P, Q \in K[X, Y]_\kappa$.

Lemma 2. *Let $(P_l = X^l Y^{\kappa-l}; l = 0, 1, \ldots, \kappa)$ be the standard basis of $K[X, Y]_\kappa$.*

(i) *Let $P = \sum_{l=0}^{\kappa} a_l P_l$ and $(f,\gamma) \in \Gamma L(2, K)$. Then $(f,\gamma) * P = \sum_{l=0}^{\kappa} b_l P_l$ where*

$$b_l = \sum_{j=0}^{\kappa} \gamma(a_j) \sum_{i=0}^{\kappa-j} \binom{\kappa-l}{i}\binom{l}{\kappa-j-i} a^i b^{\kappa-l-i} c^{\kappa-j-i} d^{l+j+i-\kappa} \quad \textit{and} \quad f = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

(ii) *Let $z \in \bar{K}$ and $(f,\gamma) \in \Gamma L(2, K)$. Then*

$$(f,\gamma) * \langle z \rangle = \theta(f, \gamma(z))^\kappa \langle f(\gamma(z)) \rangle$$

where the cocycle θ: $\mathrm{GL}(2, K) \times \bar{K} \to K$ *has been defined in* [8, p. 76].

(iii) *Let $P \in K[X, Y]_\kappa$ and $Q \in K[X, Y]_\mu$ such that $\{P, Q\} = 0$. Then*

$$\{(f,\gamma) * P, (f,\gamma)Q\} = 0 \quad \text{for all } (f,\gamma) \in \Gamma L(2, K).$$

(iv) *Suppose that K has characteristic $p > 0$ and that $\kappa <$* card(K). *Let $P \in K[X, Y]_\kappa$, $P \neq 0$. Then P is semi-invariant with respect to the operation $*$ of $GL(2, K)$ (i.e., $f * P$ is a scalar multiple of P for all $f \in$* GL$(2, K)$) *if and only if $\kappa = 2(p^e - 1)$ for some $e \geq 0$ and P is a scalar multiple of $P_{\kappa/2}$. (For a Cauchy code over* GF(q) *of length n and dimension k we have assumed in Definition 0 that $1 \leq k \leq n-1$, so $0 \leq \kappa = d - 2 \leq n - 2 \leq q - 1$ in that case).*

(v) *Suppose that K has characteristic $p > 0$ and that $\kappa = p^e - 1$ for some $e \geq 0$. Let $P \in K[X, Y]_\kappa$ and $(f,\gamma) \in \Gamma L(2, K)$. Then $(f,\gamma) * P =$* det$(f)^\kappa (f,\gamma)P$.

Proof. (i) $(f,\gamma) * P = \sum_{l=0}^{\kappa} \{(f,\gamma) * P, P_{\kappa-l}\} P_l$ because $\{P_l, P_{\kappa-j}\} = \delta_{l,j}$ for $0 \leq l, j \leq \kappa$. Using Eq. (1) we find that

$$\begin{aligned}\{(f,\gamma) * P, P_{\kappa-l}\} &= \gamma(\{P, (f,\gamma)^{-1} P_{\kappa-l}\}) = \{\gamma(P), f^{-1} P_{\kappa-l}\} \\ &= \sum_{j=0}^{\kappa} \gamma(a_j)\{P_j, f^{-1} P_{\kappa-l}\}.\end{aligned}$$

Multiplying out $f^{-1} P_{\kappa-l} = (aX + bY)^{\kappa-l}(cX + dY)^l$ gives the result.

(ii) As $\{\langle z \rangle, P_l\} = P_l(z)$ for all l, we have $\{\langle z \rangle, Q\} = Q(z)$ for all $Q \in K[X, Y]_\kappa$. Using (i), Eq. (1) and [8, equation (2)], we obtain

$$\begin{aligned}\{(f,\gamma) * \langle z \rangle, Q\} &= \sum_{l=0}^{\kappa} P_{\kappa-l}(\gamma(z))\{f * P_l, Q\} = (f^{-1}Q)(\gamma(z)) \\ &= \theta(f, \gamma(z))^\kappa Q(f(\gamma(z))) = \{\theta(f, \gamma(z))^\kappa \langle f(\gamma(z)) \rangle, Q\}\end{aligned}$$

which implies the result.

(iii) We may assume that $\gamma = id$ and $\kappa \geqslant \mu$. Let $R \in K[X, Y]_{\kappa-\mu}$. By Lemma 1 and Eq. (1), we have

$$\begin{aligned}\{\{f * P, fQ\}, R\} &= \{f * P, (fQ)R\} = \{f * P, f(Q(f^{-1}R))\}\\ &= \{P, Q(f^{-1}R)\} = \{\{P, Q\}, f^{-1}R\} = 0.\end{aligned}$$

Hence $\{f * P, fQ\} = 0$.

(iv) The group GL(2, K) is generated by the subgroups $T = \{(\begin{smallmatrix} a & 0 \\ 0 & d \end{smallmatrix}); a, d \in K^*\}$, $U = \{(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}); b \in K\}$, and the element $w = (\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix})$. Let $P = \sum_{l=0}^{\kappa} a_l P_l$ be a nonzero semi-invariant. From $f * P = \sum_{l=0}^{\kappa} a_l a^{\kappa-l} d^l P_l$ for $f \in T$ and from $\kappa <$ card(K) it follows either that $P = a_i P_i$ for some i, or, if $K = \mathrm{GF}(q)$ and $\kappa = q - 1$, that $P = a_0 P_0 + a_{q-1} P_{q-1}$. In the first case, $w * P_i = (-1)^{\kappa-i} P_{\kappa-i}$ implies that κ is even and $i = \kappa/2$. Furthermore, since $f * P_i = \sum_{l=0}^{i} \binom{\kappa-l}{i} b^{i-l} P_l$ for $f \in U$, we must have $\kappa = 2(p^e - 1)$, $e \geqslant 0$, by Lucas's theorem. In the second case,

$$w * (a_0 P_0 + a_{q-1} P_{q-1}) = a_{q-1} P_0 + a_0 P_{q-1}$$

implies that $a_{q-1} = \pm a_0$. But

$$f * (P_0 \pm P_{q-1}) = P_0 \pm \sum_{l=0}^{q-1} b^{q-1-l} P_l$$

for $f \in U$, so $P_0 \pm P_{q-1}$ cannot be semi-invariant. Conversely, the arguments above prove that $P_{\kappa/2}$ is semi-invariant if $\kappa = 2(p^e - 1)$ for some $e \geqslant 0$.

(v) We first prove that, for $P, Q \in K[X, Y]_\kappa$ and $f \in \mathrm{GL}(2, K)$, $\{fP, fQ\} = \det(f)^{-\kappa}\{P, Q\}$. It suffices to verify this for $P = P_l$ and $Q = P_j$, $0 \leqslant l, j \leqslant \kappa$, and for $f \in T$, $f \in U$, and $f = w$. By a straight-forward computation we find that $\{fP_l, fP_j\} = (ad)^{-\kappa}\,\delta_{l,\kappa-j}$ if $f = (\begin{smallmatrix} a & 0 \\ 0 & d \end{smallmatrix})$, $\{fP_l, fP_j\} = (-b)^{l+j-\kappa}\binom{l+j}{\kappa}$ if $f = (\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix})$, and $\{fP_l, fP_j\} = (-1)^\kappa\,\delta_{l,\kappa-j}$ if $f = w$. Observe that $\{P_l, P_j\} = \delta_{l,\kappa-j}$. As the characteristic of K is p and $\kappa = p^e - 1$ for some $e \geqslant 0$, Lucas's theorem implies that all three expressions are equal to $\det(f)^{-\kappa}\{P_l, P_j\}$. Finally, for $(f, \gamma) \in \Gamma L(2, K)$, we have

$$\begin{aligned}\{(f, \gamma)P, (f, \gamma)Q\} &= \{f\gamma(P), f\gamma(Q)\} = \det(f)^{-\kappa}\{\gamma(P), \gamma(Q)\}\\ &= \det(f)^{-\kappa}\{(f, \gamma) * P, (f, \gamma)Q\}\end{aligned}$$

by Eq. (1), and hence $(f, \gamma)P = \det(f)^{-\kappa}(f, \gamma) * P$. □

Theorem 1. *Let $Q \in K[X, Y]_\mu$, $Q \neq 0$, and let $\kappa \geqslant \mu$. Then the subspace $\{P \in K[X, Y]_\kappa; \{P, Q\} = 0\}$ has dimension μ over K. If Q splits over K in linear factors, i.e. $Q = \lambda \prod_{z \in N} [(X, Y), z]^{m(z)}$ where $\lambda \in K^*$, $N \subset \bar{K}$, $m(z) > 0$, and $[(X, Y), z]$ denotes the linear form $X - zY$ if $z \in K$, and $-Y$ if $z = \infty$, then a basis of this subspace is $(\langle z; j\rangle; z \in N, 0 \leqslant j \leqslant m(z) - 1)$ where*

$$\langle z; j\rangle := \sum_{i=j}^{\kappa} \binom{i}{j} z^{i-j} X^{\kappa-i} Y^i \text{ if } z \in K, \quad \text{and} \quad \langle z; j\rangle := X^j Y^{\kappa-j} \text{ if } z = \infty.$$

(Note that $\langle z; 0\rangle = \langle z\rangle$ for all $z \in \bar{K}$).

Proof. Let $Q=\sum_{j=0}^{\mu} b_jX^jY^{\mu-j}$. For $P=\sum_{l=0}^{\kappa} a_lX^lY^{\kappa-l}$, $\{P, Q\}=0$ if and only if $\sum_{l=i}^{\mu+i} b_{\mu+i-l}a_l=0$, $i=0, 1, \ldots, \kappa-\mu$. Since the rank of this system of linear equations is $\kappa+1-\mu$, the subspace ${}^{\perp}Q=\{P\in K[X, Y]_{\kappa}; \{P, Q\}=0\}$ has dimension μ. In particular, if $Q=Y^{\mu}$, then $\{P, Y^{\mu}\}=\sum_{i=0}^{\kappa-\mu} a_{i+\mu}X^iY^{\kappa-\mu-i}$, and a basis of ${}^{\perp}Q$ is $(X^jY^{\kappa-j}; j=0, 1, \ldots, \mu-1)$. If $Q=(X-zY)^{\mu}$ where $z\in K$, then a basis of ${}^{\perp}Q$ is $(f*X^jY^{\kappa-j}; j=0, 1, \ldots, \mu-1)$ where $f=\left(\begin{smallmatrix} z & 1\\ 1 & 0\end{smallmatrix}\right)$. To see this, recall that, by Lemma 2(iii), $\{P, Y^{\mu}\}=0$ implies $\{f*P, Q\}=\{f*P, fY^{\mu}\}=0$. Using Lemma 2(i), we find that

$$f*X^jY^{\kappa-j}=\sum_{i=j}^{\kappa}\binom{i}{j}z^{i-j}X^{\kappa-i}Y^i.$$

In general, if $Q=\lambda\prod_{z\in N}[(X, Y), z]^{m(z)}$, then, by Lemma 1, $\{\langle z;j\rangle, Q\}=0$, and the result follows from Lemma 3. □

Lemma 3. *Let $N\subset\bar{K}$ and $m\in\mathbb{N}^N$ such that $\sum_{z\in N} m(z)\leq\kappa+1$ (Here $\mathbb{N}$ denotes the set of positive integers). Then the binary forms $\langle z;j\rangle$, $z\in N$, $0\leq j\leq m(z)-1$, are linearly independent in $K[X, Y]_{\kappa}$.*

Proof. We may assume that $\sum_{z\in N} m(z)=\kappa+1$. For $0\leq j\leq m(z)-1$, we have

$$\langle z;j\rangle=\sum_{i=j}^{\kappa}\binom{i}{j}z^{i-j}P_{\kappa-i}$$

if $z\in K$, and $\langle z;j\rangle=P_j$ if $z=\infty$. Thus the matrix of coefficients with respect to the standard basis $(P_l; l=0, 1, \ldots, \kappa)$ is a degenerate form of the Vandermonde matrix and hence nonsingular (compare, e.g., [1, pp. 123–126]). □

Lemma 4. *Let $P\in K[X, Y]_{\kappa}$, $Q\in K[X, Y]_{\mu}$, and $R\in K[X, Y]_{\nu}$ such that $\mu+\nu\leq\kappa+1$ and $\{P, Q\}=\{P, R\}=0$. Then $\{P, \gcd(Q, R)\}=0$.*

Proof. We may assume that K is a splitting field for Q and R. Let

$$Q=\lambda'\prod_{z\in N'}[(X, Y), z]^{m'(z)} \quad\text{and}\quad R=\lambda''\prod_{w\in N''}[(X, Y), w]^{m''(w)}.$$

By Lemma 3, a basis of ${}^{\perp}Q\cap{}^{\perp}R$ is $(\langle z;j\rangle; z\in N, 0\leq j\leq m(z)-1)$ where $N=N'\cap N''$ and $m(z)=\min(m'(z), m''(z))$. As

$$\gcd(Q, R)=\prod_{z\in N}[(X, Y), z]^{m(z)},$$

we conclude that $\{P, \gcd(Q, R)\}=0$. □

Definition 4. Let κ be even. For $P=\sum_{i=0}^{\kappa} a_iX^iY^{\kappa-i}$, we define

$$c(P)=\det(a_{i+j}; 0\leq i, j\leq\kappa/2)$$

(In classical invariant theory, this determinant is called the catalecticant).

Theorem 2. *Let $P \in K[X, Y]_\kappa$ and $t = \lfloor(\kappa+1)/2\rfloor$ (Here $\lfloor a \rfloor$ denotes the greatest integer less than or equal to a).*

(i) *If κ is odd or if κ is even and $c(P) = 0$, there exists a nonzero form $R \in K[X, Y]_\nu$ with $\{P, R\} = 0$ and $\nu \leq t$ such that every form $Q \in K[X, Y]_\mu$ with $\{P, Q\} = 0$ and $\mu \leq \kappa + 1 - \nu$ is a multiple of R. The binary form R is unique up to scalar multiples, and ν is the minimum degree of a nonzero binary form Q over K with $\{P, Q\} = 0$.*

(ii) *If κ is even and $c(P) \neq 0$, the minimum degree of a nonzero binary form Q over K with $\{P, Q\} = 0$ is $t + 1$, and the subspace $\{Q \in K[X, Y]_{t+1}; \{P, Q\} = 0\}$ has dimension 2.*

Proof. Let $P = \sum_{l=0}^{\kappa} a_l X^l Y^{\kappa - l}$. For $\mu \leq \kappa$, these exists a nonzero form Q of degree μ with $\{P, Q\} = 0$ if and only if the matrix $(a_{i+j}; 0 \leq i \leq \kappa - \mu, 0 \leq j \leq \mu)$ has rank at most μ. Hence, in case (i), there always exists a nonzero form Q of degree t with $\{P, Q\} = 0$, and Lemma 4 implies the result. In case (ii), the matrix $(a_{i+j}; 0 \leq i \leq t-1, 0 \leq j \leq t+1)$ has rank t because $c(P) \neq 0$. □

Let F be the algebraic closure of K, and let $\mathrm{Gal}(F/K)$ be the Galois group of F over K. Then a modification of Problem 1 is the following problem.

Problem 2. Given $S \in K[X, Y]_\kappa$, find a representation

$$S = \sum_{z \in N} \sum_{j=0}^{m(z)-1} \lambda(z, j)\langle z; j\rangle \quad \text{where } N \subset \bar{F},\ m \in \mathbb{N}^N,$$

$$\lambda(z, j) \in F, \qquad \lambda(z, m(z) - 1) \neq 0, \quad \text{and} \quad \sum_{z \in N} m(z) \leq \kappa + 1,$$

such that $\sum_{z \in N} m(z)$ is minimal.

In the sequel we call $\sum_{z \in N} m(z)$ the 'length' of the representation although some $\lambda(z, j)$ may be zero. The representation is called $\mathrm{Gal}(F/K)$-invariant if $\mathrm{Gal}(F/K)$ permutes the terms of the sum. By Lemma 3, every solution of Problem 1 of length $\leq \lfloor \kappa/2 \rfloor + 1$ also is a solution of Problem 2.

Corollary 1. *Let $t = \lfloor(\kappa+1)/2\rfloor$.*

(i) *If κ is odd or if κ is even and $c(S) = 0$, Problem 2 has a unique solution. This representation is* $\mathrm{Gal}(F/K)$*-invariant. Its length is at most t and is equal to the minimal degree of a nonzero binary form Q over K with $\{S, Q\} = 0$.*

(ii) *If κ is even and $c(S) \neq 0$, Problem 2 has several* $\mathrm{Gal}(F/K)$*-invariant solutions. These representations have length $t + 1$.*

Proof. Apply Theorem 1 and Theorem 2 for the field F and use Galois descent to prove the existence of $\mathrm{Gal}(F/K)$-invariant solutions. □

In Theorem 3 we shall describe an algorithm that computes a Gal(F/K)-invariant solution of Problem 2. As a preparation, we next show how a Gal(F/K)-invariant representation can be specified by two binary forms over K.

Definition 5. Let $S \in K[X, Y]_\kappa$ have the Gal(F/K)-invariant representation

$$S = \sum_{z\in N} \sum_{j=0}^{m(z)-1} \lambda(z, j)\langle z; j\rangle \quad \text{where } N \subset \bar{F},\ m \in \mathbb{N}^N,$$

$$\lambda(z, j) \in F, \qquad \lambda(z, m(z) - 1) \neq 0, \quad \text{and} \quad \sum_{z\in N} m(z) \leq \kappa + 1.$$

Let $v = \sum_{z\in N} m(z)$ be the length of this representation. We define the locator form $\Lambda \in K[X, Y]_v$ and the evaluator form $\Omega \in K[X, Y]_{v-1}$ by

$$\Lambda = \prod_{z\in N} \Lambda_z \quad \text{and} \quad \Omega = \sum_{z\in N} \Omega_z \Lambda/\Lambda_z$$

where

$$\Lambda_z = (X - zY)^{m(z)} \quad \text{and} \quad \Omega_z = \sum_{j=0}^{m(z)-1} \lambda(z, j) Y^j (X - zY)^{m(z)-1-j}$$

if $z \in F$, or $\Lambda_z = Y^{m(\infty)}$ and $\Omega_z = \sum_{j=0}^{m(\infty)-1} \lambda(\infty, j) X^j Y^{m(\infty)-1-j}$ if $z = \infty$ (For the empty representation $S = 0$, we set $\Lambda = 1$ and $\Omega = 0$).

Lemma 5. (i) *The representation* $S = \sum_{z\in N} \sum_{j=0}^{m(z)-1} \lambda(z, j)\langle z; j\rangle$ *can be recovered from its locator form* Λ *and its evaluator form* Ω *by the following recursion*: *For* $z \in N$,

$$\lambda(z, m(z) - 1) = \Omega(z)/\Delta^{(m(z))}|_z \Lambda,$$

and, for $j = 1, 2, \ldots, m(z) - 1$,

$$\lambda(z, m(z) - 1 - j)$$
$$= (\Delta^{(j)}|_z \Omega - \sum_{i=1}^{j} \lambda(z, m(z) - 1 - j + i)\Delta^{(i+m(z))}|_z \Lambda)/\Delta^{(m(z))}|_z \Lambda.$$

Here $\Delta^{(j)}|_z P$ *denotes the hyperderivative of order* j *of the binary form* P *evaluated at* $z \in \bar{K}$ *which is defined by* $\Delta^{(j)}|_z P := (\Delta_X^{(j)} P)(z)$ *if* $z \in K$, *and* $\Delta^{(j)}|_z P := (\Delta_Y^{(j)} P)(\infty)$ *if* $z = \infty$, *where* $\Delta_X^{(j)}$ *and* $\Delta_Y^{(j)}$ *denote the partial hyperderivatives of order* j *with respect to* X *or* Y [18, p. 27].

(ii) *If* $N \subset F$, $S(1, Y)\Lambda(1, Y) \equiv \Omega(1, Y) \bmod Y^{\kappa+1}$.

(iii) *Suppose that* $\infty \in N$. *Let*

$$\tilde{N} = N \setminus \{\infty\}, \qquad \mu = m(\infty), \qquad \tilde{\Lambda} = \Lambda/\Lambda_\infty \in K[X, Y]_{v-\mu},$$

and

$$\tilde{\Omega} = \sum_{z\in \tilde{N}} \Omega_z \tilde{\Lambda}/\Lambda_z \in K[X, Y]_{v-\mu-1}.$$

Then

$$\Omega = Y^{\mu}\tilde{\Omega} + \Omega_{\infty}\tilde{\Lambda}$$

and

$$S(1, Y)\tilde{\Lambda}(1, Y) \equiv \tilde{\Omega}(1, Y) + Y^{\kappa-\mu+1}\Omega_{\infty}(1, Y)\tilde{\Lambda}(1, Y) \bmod Y^{\kappa+1}.$$

Proof. For $z \in \bar{F}$, let $K_z = \Lambda/\Lambda_z$. Applying $\Delta^{(j)}|_z$ to $\Omega = \sum_{w \in N} \Omega_w K_w$ gives

$$\Delta^{(j)}|_z\, \Omega = \Delta^{(j)}|_z\, \Omega_z K_z = \sum_{i=0}^{j} (\Delta^{(i)}|_z\, K_z)\lambda(z, m(z) - 1 - j + i).$$

Solving for $\lambda(z, m(z) - 1 - j)$ and observing that $\Delta^{(i)}|_z\, K_z = \Delta^{(i+m(z))}|_z\, \Lambda$ yields (i).

For $z \in N$, let $S_z = \sum_{j=0}^{m(z)-1} \lambda(z, j)\langle z; j\rangle$. The formal power series identity

$$\sum_{i=j}^{\infty} \binom{i}{j} z^{i-j} Y^{i} = Y^{j}(1 - zY)^{-1-j}$$

implies that

$$\langle z; j\rangle(1, Y) \equiv Y^{j}(1 - zY)^{-1-j} \bmod Y^{\kappa+1}.$$

Consequently,

$$S_z(1, Y)(1 - zY)^{m(z)} \equiv \Omega_z(1, Y) \bmod Y^{\kappa+1}$$

and

$$S_z(1, Y)\Lambda(1, Y) \equiv \Omega_z(1, Y)K_z(1, Y) \bmod Y^{\kappa+1}.$$

Summing up over $z \in N$ proves (ii). Let

$$S_{\infty} = \sum_{j=0}^{m(\infty)-1} \lambda(\infty, j)\langle \infty; j\rangle.$$

Then

$$S_{\infty}(1, Y) = Y^{\kappa-m(\infty)+1}\Omega_{\infty}(1, Y),$$

and hence

$$S_{\infty}(1, Y)\tilde{\Lambda}(1, Y) \equiv Y^{\kappa-m(\infty)+1}\Omega_{\infty}(1, Y)\tilde{\Lambda}(1, Y) \bmod Y^{\kappa+1}.$$

By (ii),

$$\sum_{z \in \bar{N}} S_z(1, Y)\tilde{\Lambda}(1, Y) \equiv \tilde{\Omega}(1, Y) \bmod Y^{\kappa+1}.$$

Adding these congruences gives (iii). □

Theorem 3. *Let* $S \in K[X, Y]_{\kappa}$, $S = \sum_{i=0}^{\kappa} s_{\kappa-i} X^{i} Y^{\kappa-i}$, *and let* $t = \lfloor(\kappa + 1)/2\rfloor$. *Then the following algorithm computes the locator form* Λ *and the evaluator form* Ω *of a* $\mathrm{Gal}(F/K)$*-invariant solution of Problem* 2.

```
1. Initialize $B(Y) \leftarrow 1$, $D(Y) \leftarrow -1$, $\nu \leftarrow 0$, $\Lambda(Y) \leftarrow 1$, and $\Omega(Y) \leftarrow 0$.
2. Set $r \leftarrow 0$.
3. Set $\delta \leftarrow \sum_{i=0}^{\nu} \Lambda_i s_{r-i}$.
```

```
4. If $\delta = 0$ go to 9.
5. If $r - v \geq t$ go to 13.
6. Set $T(Y) \leftarrow \Lambda(Y) - \delta Y B(Y)$ and $V(Y) \leftarrow \Omega(Y) - \delta D(Y)$.
7. If $2v \leq r$ set $B(Y) \leftarrow \delta^{-1}\Lambda(Y)$, $D(Y) \leftarrow \delta^{-1} Y \Omega(Y)$,
   $v \leftarrow r + 1 - v$, $\Lambda(Y) \leftarrow T(Y)$, $\Omega(Y) \leftarrow V(Y)$, and go to 10.
8. Set $\Lambda(Y) \leftarrow T(Y)$ and $\Omega(Y) \leftarrow V(Y)$.
9. Set $B(Y) \leftarrow YB(Y)$ and $D(Y) \leftarrow YD(Y)$.
10. Set $r \leftarrow r + 1$.
11. If $r \leq \kappa$ go to 3.
12. Stop.
13. Set $j \leftarrow r$, $\mu \leftarrow \kappa + 1 - j$, and $\Omega(Y) \leftarrow Y^{\mu}\Omega(Y) + \delta\Lambda(Y)$.
14. If $r \geq \kappa$ go to 18.
15. Set $r \leftarrow r + 1$.
16. Set $\delta \leftarrow \sum_{i=0}^{v} \Lambda_i s_{r-i}$ and $\Omega(Y) \leftarrow \Omega(Y) + (\delta - \Omega_{r-j}) Y^{r-j} \Lambda(Y)$.
17. Go to 14.
18. Set $v \leftarrow v + \mu$ and $\Lambda(Y) \leftarrow Y^{\mu}\Lambda(Y)$.
19. Stop.
```

In the algorithm, $\Lambda(Y) = \sum_{i \geq 0} \Lambda_i Y^i$ *and* $\Omega(Y) = \sum_{i \geq 0} \Omega_i Y^i$ *are polynomials in the variable* Y, *and* v *is a natural number,* $B(Y)$, $D(Y)$, $T(Y)$, *and* $V(Y)$ *are auxiliary polynomials, and* r *counts the iterations. When the algorithm stops,* $\Lambda(X, Y) = X^v \Lambda(Y/X)$ *and* $\Omega(X, Y) = X^{v-1}\Omega(Y/X)$.

Remark 1. The core of this algorithm is Berlekamp's algorithm [2, p. 180] for the decoding of Reed–Solomon codes which consists of the Steps 1–4 and 6–12. Our notation is close to that in [5].

Example 1. Let $\kappa = 5$ and $S = X^5 + X^4Y + X^3Y^2 + X^2Y^3$. Then $t = 3$, and the algorithm of Theorem 3 proceeds as follows.

r	δ	$T(Y)$	$V(Y)$	$B(Y)$	$D(Y)$	v	$\Lambda(Y)$	$\Omega(Y)$
				1	-1	0	1	0
0	1	$1-Y$	1	1	0	1	$1-Y$	1
1	0			Y	0			
2	0			Y^2	0			
3	0			Y^3	0			
4	-1	$j=4$, $\mu=2$						Y^2+Y-1
5	0					3	Y^2-Y^3	$2Y^2-1.$

Hence $\Lambda(X, Y) = (X - Y)Y^2$ and $\Omega(X, Y) = 2Y^2 - X^2$. Applying Lemma 5(i) with $N = \{1, \infty\}$, $m(1) = 1$, and $m(\infty) = 2$, we obtain $\lambda(1, 0) = 1$, $\lambda(\infty, 1) = -1$, and $\lambda(\infty, 0) = -1$, which agrees with $S = \langle 1; 0 \rangle - \langle \infty; 0 \rangle - \langle \infty; 1 \rangle$.

Proof of Theorem 3. We first recall a result on Berlekamp's algorithm which consists of the steps 1–4 and 6–12. Let $0 \leq r \leq \kappa$, and let $S^{(r)} = \sum_{i=0}^{r} s_i X^{r-i} Y^i \in$

$K[X, Y]_r$, so that, in particular, $S^{(\kappa)} = S$. In the rth iteration, Berlekamp's algorithm computes the minimal number $\nu(r)$ and a polynomial $\Lambda^{(r)}(Y) = \sum_{i=0}^{\nu(r)} \Lambda_i^{(r)} Y^i$ with $\Lambda_0^{(r)} = 1$ such that, for $i = \nu(r), \nu(r)+1, \ldots, r$, $s_i = -\sum_{j=1}^{\nu(r)} \Lambda_j^{(r)} s_{i-j}$. Stated in terms of binary forms, this say that the form $\Lambda^{(r)}(X, Y) = X^{\nu(r)} \Lambda^{(r)}(Y/X) \in K[X, Y]_{\nu(r)}$ has minimal degree among the binary forms Q with $\{S^{(r)}, Q\} = 0$ and $Q(\infty) = 1$. Clearly $\nu(0) \leqslant \nu(1) \leqslant \cdots \leqslant \nu(\kappa)$. From $\{S^{(r-1)}, \Lambda^{(r-1)}\} = 0$ it follows that $\{S^{(r)}, \Lambda^{(r-1)}\} = \delta^{(r)} Y^{r-\nu(r-1)}$ where $\delta^{(r)} = \sum_{j=0}^{\nu(r-1)} \Lambda_j^{(r-1)} s_{r-j}$ is known as the rth discrepancy and, for completeness, $S^{(-1)} = 0$, $\nu(-1) = 0$, and $\Lambda^{(-1)} = 1$.

Now let ν be the minimum degree of a nonzero binary form Q over K with $\{S, Q\} = 0$. We next prove that our algorithm yields a nonzero form $\Lambda \in K[X, Y]_\nu$ with $\{S, \Lambda\} = 0$. For this we distinguish two cases.

In the first case, we assume that, for $r = 0, \ldots, \kappa$, $\delta^{(r)} = 0$ or $r - \nu(r-1) < t$. Then our algorithm runs as Berlekamp's algorithm. Suppose that there exists a nonzero form $R \in K[X, Y]_\nu$ with $\{S, R\} = 0$ and $R(\infty) = 0$. Let $R = Y^\mu \tilde{R}$ where $\mu > 0$ and $\tilde{R}(\infty) \neq 0$. Then, by Lemma 1,

$$0 = \{S, R\} = \{S^{(\kappa)}, Y^\mu \tilde{R}\} = \{\{S^{(\kappa)}, Y^\mu\}, \tilde{R}\} = \{S^{(\kappa-\mu)}, \tilde{R}\},$$

and hence $\nu(\kappa - \mu) \leqslant \nu - \mu$. Let $r = \kappa + 1 - \mu$. Then, by Theorem 2, $r - \nu(r-1) \geqslant \kappa + 1 - \nu \geqslant t$, and, by assumption, $\delta^{(r)} = 0$. Since

$$\{S, Y^{\mu-1}\Lambda^{(\kappa-\mu)}\} = \{\{S, Y^{\mu-1}\}, \Lambda^{(\kappa-\mu)}\} = \{S^{(r)}, \Lambda^{(r-1)}\} = \delta^{(r)} Y^{r-\nu(r-1)} = 0$$

and

$$\mu - 1 + \nu(\kappa - \mu) < \nu,$$

we have a contradiction. It follows that in the first case every nonzero form $R \in K[X, Y]_\nu$, with $\{S, R\} = 0$ satisfies $R(\infty) \neq 0$, and we conclude that $\nu = \nu(\kappa)$ and $\Lambda = \Lambda^{(\kappa)}$.

In the second case, we assume that $\delta^{(r)} \neq 0$ and $r - \nu(r-1) \geqslant t$ for some r, $0 \leqslant r \leqslant \kappa$. Let j be the least possible such r, and let $\mu = \kappa + 1 - j$. Then our algorithm leaves Berlekamp's algorithm at the jth iteration and yields the form $Y^\mu \Lambda^{(j-1)}$ of degree $\nu(j-1) + \mu$. Suppose that $\nu < \nu(j-1) + \mu$. Then there exists a nonzero form $R \in K[X, Y]_\nu$ with $\{S, R\} = 0$. By assumption, $\nu(j-1) + \mu \leqslant \kappa + 1 - t$, hence $\nu + \nu(j-1) + \mu \leqslant \kappa + 1$, and we can apply Lemma 4 to obtain $\{S, \gcd(R, Y^\mu \Lambda^{(j-1)})\} = 0$. Since

$$\{S, Y^{\mu-1}\Lambda^{(j-1)}\} = \{S^{(j)}, \Lambda^{(j-1)}\} = \delta^{(j)} Y^{j-\nu(j-1)} \neq 0$$

by assumption, we have $R = Y^\mu \tilde{R}$ where $\tilde{R}$ has degree $\nu - \mu < \nu(j-1)$. Let $D = \gcd(\tilde{R}, \Lambda^{(j-1)})$. Then D has degree less than $\nu(j-1)$, $D(\infty) \neq 0$, and $\{S^{(j-1)}, D\} = \{S, Y^\mu D\} = 0$ which is impossible. We conclude that in the second case $\nu = \nu(j-1) + \mu$ and $\Lambda = Y^\mu \Lambda^{(j-1)}$ where $\mu = \kappa + 1 - j$.

Summing up, we have shown that our algorithm yields a nonzero form $\Lambda \in K[X, Y]_\nu$ with $\{S, \Lambda\} = 0$. Let N be the vanishing set of Λ in $\bar{F}$, and, for

$z \in N$, let $m(z)$ be the multiplicity of the root z. Then $\sum_{z \in N} m(z) = \nu \leqslant \kappa + 1$, and, by Theorem 1, there exists a unique representation $S = \sum_{z \in N} \sum_{j=0}^{m(z)-1} \lambda(z, j)\langle z; j\rangle$ where $\lambda(z, j) \in F$. Clearly this representation is Gal(F/K)-invariant, and, for $z \in N$, $\lambda(z, m(z)-1) \neq 0$. We next prove that our algorithm computes the evaluator form $\Omega \in K[X, Y]_{\nu-1}$ of this representation. We distinguish two cases in the same way as before.

In the first case, we have seen that $\Lambda = \Lambda^{(\kappa)}$ and $N \subset F$. Hence, by Lemma 5(ii), $S(1, Y)\Lambda(1, Y) \equiv \Omega(1, Y) \bmod Y^{\kappa+1}$. Now recall that Berlekamp's algorithm computes, for $r = 0, 1, \ldots, \kappa$, a polynomial $\Omega^{(r)}(Y) = \sum_{i=0}^{\nu(r)-1} \Omega_i^{(r)} Y^i$ such that $S^{(r)}(1, Y)\Lambda^{(r)}(Y) \equiv \Omega^{(r)}(Y) \bmod Y^{r+1}$. Comparing both congruences, we conclude that $\Omega(1, Y) = \Omega^{(\kappa)}(Y)$ and $\Omega(X, Y) = X^{\nu-1}\Omega^{(\kappa)}(Y/X)$.

In the second case, we have seen that $\Lambda = Y^{\mu}\Lambda^{(j-1)}$ where $\mu = \kappa + 1 - j > 0$ and $\Lambda^{(j-1)}(\infty) = 1$. Applying Lemma 5(iii) with $m(\infty) = \mu$, we obtain

$$S(1, Y)\tilde{\Lambda}(1, Y) \equiv \tilde{\Omega}(1, Y) + Y^j\Omega_\infty(1, Y)\tilde{\Lambda}(1, Y) \bmod Y^{\kappa+1}. \tag{2}$$

Clearly $\tilde{\Lambda} = \Lambda^{(j-1)}$. Berlekamp's algorithm has computed, for $r = 0, 1, \ldots, j-1$, polynomials $\Omega^{(r)}(Y)$ such that $S^{(r)}(1, Y)\Lambda^{(r)}(Y) \equiv \Omega^{(r)}(Y) \bmod Y^{r+1}$. Since

$$\tilde{\Omega}(1, Y) \equiv S(1, Y)\tilde{\Lambda}(1, Y) \equiv S^{(j-1)}(1, Y)\Lambda^{(j-1)}(Y) \equiv \Omega^{(j-1)}(Y) \bmod Y^j,$$

we find that $\tilde{\Omega}(1, Y) = \Omega^{(j-1)}(Y)$. In step 13–17 our algorithm computes, for $r = j, j+1, \ldots, \kappa$, polynomials $\Omega^{(r)}(Y) = \sum_{i=0}^{\nu-1} \Omega_i^{(r)} Y^i$ by the recursion

$$\Omega^{(j)}(Y) = Y^{\mu}\Omega^{(j-1)}(Y) + \delta^{(j)}\Lambda^{(j-1)}(Y),$$

and, for $r = j+1, j+2, \ldots, \kappa$,

$$\Omega^{(r)}(Y) = \Omega^{(r-1)}(Y) + (\delta^{(r)} - \Omega_{r-j}^{(r-1)})Y^{r-j}\Lambda^{(j-1)}(Y)$$

where $\delta^{(r)} = \sum_{i=0}^{\nu(j-1)} \Lambda_i^{(j-1)} s_{r-i}$. Then the polynomials $\Psi^{(r)}(Y) = \Omega^{(r)}(Y) - Y^{\mu}\Omega^{(j-1)}(Y)$, $j \leqslant r \leqslant \kappa$, satisfy the recursion $\Psi^{(j)}(Y) = \delta^{(j)}\Lambda^{(j-1)}(Y)$ and, for $r = j+1, j+2, \ldots, \kappa$,

$$\Psi^{(r)}(Y) = \Psi^{(r-1)}(Y) + (\delta^{(r)} - \Psi_{r-j}^{(r-1)})Y^{r-j}\Lambda^{(j-1)}(Y).$$

Furthermore, for $j \leqslant r \leqslant \kappa$,

$$S^{(r)}(1, Y)\tilde{\Lambda}(1, Y) \equiv \tilde{\Omega}(1, Y) + Y^j\Psi^{(r)}(Y) \bmod Y^{r+1},$$

which we prove by induction. For $r = j$,

$$S^{(j)}(1, Y)\tilde{\Lambda}(1, Y) \equiv \tilde{\Omega}(1, Y) + Y^j\Psi^{(j)}(Y) \bmod Y^{j+1}$$

because

$$S^{(j-1)}(1, Y)\Lambda^{(j-1)}(1, Y) \equiv \Omega^{(j-1)}(1, Y) \bmod Y^j.$$

If

$$S^{(r-1)}(1, Y)\tilde{\Lambda}(1, Y) \equiv \tilde{\Omega}(1, Y) + Y^j\Psi^{(r-1)}(Y) \bmod Y^r,$$

then

$$\begin{aligned} S^{(r)}(1, Y)\tilde{\Lambda}(1, Y) \equiv \tilde{\Omega}(1, Y) &+ Y^j\Psi^{(r-1)}(Y) \\ &+ (\delta^{(r)} - \Psi_{r-j}^{(r-1)})Y^r\tilde{\Lambda}(1, Y) \bmod Y^{r+1} \end{aligned}$$

because $\tilde{\Lambda}(1, 0) = 1$. Applying the recursion formula for $\Psi^{(r)}(Y)$ completes the proof by induction. For $r = \kappa$, the congruence above reads

$$S(1, Y)\tilde{\Lambda}(1, Y) \equiv \tilde{\Omega}(1, Y) + Y^j \Psi^{(\kappa)}(Y) \bmod Y^{\kappa+1}.$$

Comparing this congruence with (2), we find that

$$\Psi^{(\kappa)}(Y) \equiv \Omega_\infty(1, Y)\tilde{\Lambda}(1, Y) \bmod Y^\mu.$$

As $\tilde{\Lambda}(1, Y)$ is invertible mod Y^μ and $\Psi^{(\kappa)}(Y)$ is a multiple of $\tilde{\Lambda}(1, Y)$ of degree $\leqslant \mu - 1 + \nu - \mu$, it follows that $\Psi^{(\kappa)}(Y) = \Omega_\infty(1, Y)\tilde{\Lambda}(1, Y)$. By Lemma 5(iii), we conclude that

$$\Omega(1, Y) = Y^\mu \tilde{\Omega}(1, Y) + \Omega_\infty(1, Y)\tilde{\Lambda}(1, Y) = \Omega^{(\kappa)}(Y)$$

and

$$\Omega(X, Y) = X^{\nu-1}\Omega^{(\kappa)}(Y/X). \qquad \square$$

4. Decoding and covering radius of Cauchy codes

We now apply the results of the previous section to the decoding problem for Cauchy codes (Problem 1). Let $C = C_k(\alpha, y)$ be a Cauchy code over K of minimum distance d, and let $L = \{\alpha_1, \alpha_2, \ldots, \alpha_n\} \subset \bar{K}$ be the location set of C. In Section 2 we have defined the syndrome of a vector $x \in K^n$ as the binary form $S_x = \sum_{i=1}^n y_i' x_i \langle \alpha_i \rangle \in K[X, Y]_\kappa$ where $\kappa = d - 2$. In coding theory, $S_x(1, Y)$ is called the syndrome polynomial of x. The following corollary characterizes the Hamming distance between the vector x and the nearest codeword in terms of the bracket $\{,\}$.

Corollary 2. *Let $S \in K[X, Y]_\kappa$. Then the weight of a coset leader with syndrome S is equal to the minimal degree of a nonzero form $Q \in K[X, Y]_\mu$ such that $\{S, Q\} = 0$ and Q has μ distinct roots in L. We denote this number by $\rho_L(S)$. Clearly $0 \leqslant \rho_L(S) \leqslant d - 1$.* $\square$

The packing radius of the code C is the greatest integer radius such that the spheres around the codewords are disjoint, and is equal to $t = \lfloor (d-1)/2 \rfloor$. The following theorem extends Berlekamp's decoding algorithm for Reed–Solomon codes to general Cauchy codes, e.g. doubly-extended Reed–Solomon codes.

Theorem 4. *Suppose that the minimum distance d is odd. Given $S \in K[X, Y]_\kappa$, $S = \sum_{i=0}^\kappa s_i X^{\kappa - i} Y^i$, the following algorithm, called the extended Berlekamp algorithm, computes the uniquely determined solution of Problem 1 if $\rho_L(S) \leqslant t$, and announces a decoding failure if $\rho_L(S) > t$.*

```
1. Initialize $B(Y) \leftarrow 1$, $D(Y) \leftarrow -1$, $\nu \leftarrow 0$, $\Lambda(Y) \leftarrow 1$, $\Omega(Y) \leftarrow 1$,
   $N \leftarrow \emptyset$, and $r \leftarrow 0$.
2. Set $\delta \leftarrow \sum_{i=0}^{\nu} \Lambda_i s_{r-i}$.
3. If $\delta = 0$ go to 10.
```

```
4. If $r - v < t$ go to 7.
5. If $\infty \notin L$ or $r < \kappa$ announce a decoding failure and stop.
6. Set $N \leftarrow N \cup \{\infty\}$, $\lambda(\infty) \leftarrow \delta$, and go to 13.
7. Set $T(Y) \leftarrow \Lambda(Y) - \delta Y B(Y)$ and $V(Y) \leftarrow \Omega(Y) - \delta D(Y)$.
8. If $2v \leqslant r$ set $B(Y) \leftarrow \delta^{-1}\Lambda(Y)$, $D(Y) \leftarrow \delta^{-1}Y\Omega(Y)$, $v \leftarrow r + 1 - v$, $\Lambda(Y) \leftarrow T(Y)$, $\Omega(Y) \leftarrow V(Y)$, and go to 11.
9. Set $\Lambda(Y) \leftarrow T(Y)$ and $\Omega(Y) \leftarrow V(Y)$.
10. Set $B(Y) \leftarrow YB(Y)$ and $D(Y) \leftarrow YD(Y)$.
11. Set $r \leftarrow r + 1$.
12. If $r \leqslant \kappa$ go to 2.
13. Let $\Lambda^*(Y) = \sum_{i=0}^{v} \Lambda_i Y^{v-i}$ and $\Omega^*(Y) = \sum_{i=0}^{v-1} \Omega_i Y^{v-1-i}$.
14. Determine the zeros of $\Lambda^*$ in $L \cap K$.
15. If there are less than $v$ zeros in $L \cap K$, announce a decoding failure and stop.
16. Set $N \leftarrow N \cup \{$zeros of $\Lambda^*$ in $L \cap K\}$ and, for each zero $z$ of $\Lambda^*$ in $L \cap K$, $\lambda(z) \leftarrow \Omega^*(z)/(d\Lambda^*/dY)(z)$.
17. Output $N$ and $\lambda(z)$, $z \in N$.
```

Remark 2. In coding theory [2–3, 5, 10], $\Lambda(Y) = \sum_{i=0}^{v} \Lambda_i Y^i$ and $\Omega(Y) = \sum_{i=0}^{v-1} \Omega_i Y^i$ are called the error locator polynomial and the error evaluator polynomial, respectively. The above algorithm extends Berlekamp's algorithm by the steps 4–6 which involve no extra computations, and avoids that failure mode of Berlekamp's algorithm where the shift register length v exceeds the packing radius t. If $L = K^*$, the above algorithm is similar to the variations of Berlekamp's algorithm proposed in [20] and [4].

Proof of Theorem 4. By Theorem 3, it suffices to show that $\lambda(\infty) = \delta^{(\kappa)}$ if ∞ is a root of $\Lambda(X, Y)$ of multiplicity 1. By Lemma 5(i) and (iii), we have $\lambda(\infty) = \lambda(\infty, 0) = \Omega(1, 0) = \Omega_\infty(1, 0) = \delta^{(\kappa)}$. □

The Berlekamp–Massey decoding algorithm for Reed–Solomon codes differs from the Berlekamp algorithm by using the recursive extension of the error spectrum instead of the computation of the error evaluator polynomial. The following corollary shows how to extend the Berlekamp–Massey algorithm to doubly-extended Reed–Solomon codes.

Corollary 3. *Let C be a doubly-extended Reed–Solomon code of minimum distance $d = 2t + 1$. For the frequency domain encoder in* [3, sec. 8.4], *a frequency domain decoder is given as follows* (*in the notation of* [3]):

Let $(v_-, v_0, v_1, \ldots, v_{q-2}, v_+)$ be the received vector.

(i) *Compute the Fourier transform $(V_0, V_1, \ldots, V_{q-2})$ of $(v_0, v_1, \ldots, v_{q-2})$.*

(ii) *Compute the syndrome $(s_0, s_1, \ldots, s_{2t-1})$ by $s_0 = V_{j_0} - v_-$, $s_j = V_{j+j_0}$ for $j = 1, 2, \ldots, 2t - 2$, and $s_{2t-1} = V_{j_0+2t-1} - v_+$.*

(iii) *Apply the extended Berlekamp–Massey algorithm defined below*:

```
1. Initialize $B(Y) \leftarrow 1$, $v \leftarrow 0$, $\Lambda(Y) \leftarrow 1$, and $r \leftarrow 0$.
2. Set $\delta \leftarrow \sum_{i=0}^{v} \Lambda_i s_{r-i}$.
3. If $\delta = 0$ go to 10.
4. If $r - v < t$ go to 7.
5. If $r < 2t - 1$ announce a decoding failure and stop.
6. Set $s_{2t-1} \leftarrow s_{2t-1} - \delta$, $r \leftarrow r + 1$, and go to 13.
7. Set $T(Y) \leftarrow \Lambda(Y) - \delta Y B(Y)$.
8. If $2v \leqslant r$ set $B(Y) \leftarrow \delta^{-1}\Lambda(Y)$, $v \leftarrow r + 1 - v$, $\Lambda(Y) \leftarrow T(Y)$, and go to 11.
9. Set $\Lambda(Y) \leftarrow T(Y)$.
10. Set $B(Y) \leftarrow YB(Y)$.
11. Set $r \leftarrow r + 1$.
12. If $r < 2t$ go to 2.
13. Compute $s_{2t}, s_{2t+1}, \dots, s_{q-1}$ by the iteration $s_r = -\sum_{i=1}^{v} \Lambda_i s_{r-i}$.
14. If $\Lambda_v \neq 0$ go to 17.
15. If $\Lambda_{v-1} = 0$ announce a decoding failure and stop.
16. Set $s_0 \leftarrow s_{q-1}$ and $v \leftarrow v - 1$.
17. Compute $s_q, s_{q+1}, \dots, s_{q-1+v}$ by the iteration $s_r = -\sum_{i=1}^{v} \Lambda_i s_{r-i}$. If $s_r \neq s_{r-q+1}$ for some $r$, announce a decoding failure and stop.
18. Output the estimated information symbols $C_j = V_j - s_{j-j_0}$ for $j = 2t - 1 + j_0, \dots, q - 1 + j_0$, where the subscripts are to be read modulo $q - 1$.
```

Remark 3. The above algorithm extends the Berlekamp–Massey algorithm by the steps 4–6, always yields a shift register length v not greater than t, and is simpler than the algorithm in [3, sec. 9.3].

All the decoding algorithms discussed so far decode only up to the packing radius of the Cauchy code and announce a decoding failure outside. The covering radius of the code is the least integer radius such that the spheres around the codewords cover the whole space, and specifies the maximum number of errors that a complete decoder has to correct. For a Cauchy code, the covering radius is equal to the greatest possible length of a solution of Problem 1, and hence equal to the maximum value of $\rho_L(S)$ for arbitrary $S \in K[X, Y]_\kappa$. We denote this value by ρ_L.

Theorem 5. *If L is a proper subset of $\bar{K}$, then $\rho_L = d - 1$.*

Proof. By [6, Proposition 2], the covering radius of a maximum distance separable code is less than its minimum distance, which proves $\rho_L \leqslant d - 1$. Since L is properly contained in $\bar{K}$, it can be mapped into K by some linear fractional transformation. By [8, Theorem 4], we may, therefore, assume that $L \subset K$. But if $L \subset K$, then $C_k(\alpha, y)$ is contained in $C_{k+1}(\alpha, y)$, and, by the Supercode Lemma [6, Proposition 1], $\rho_L \geqslant d - 1$. □

In case that $L = \bar{K}$, the determination of the covering radius is more difficult, and we shall not give a complete answer. To state our results we introduce the following notation.

Definition 6. Let $K = \mathrm{GF}(q)$ and $2 \leqslant d \leqslant q + 1$. Let $\kappa = d - 2$, $n = q + 1$, and $k = n + 1 - d$, so that $1 \leqslant k \leqslant n - 1$. Then all Cauchy codes $C_k(\alpha, y)$ over K with location set $L = \{\alpha_1, \alpha_2, \ldots, \alpha_n\} = \bar{K}$ are equivalent and have the same covering radius which we denote by $\rho(d, q)$.

Proposition 1. *Let D_κ be the set of all nonzero binary forms over K of degree κ that have κ distinct roots in $\bar{K}$. Then $d - 2 \leqslant \rho(d, q) \leqslant d - 1$, and $\rho(d, q) = d - 2$ if and only if D_κ intersects every linear hyperplane in $K[X, Y]_\kappa$.*

Proof. We only have to show that $\rho(d, q) \geqslant d - 2$. By Theorem 5, there exists a form $R \in K[X, Y]_{\kappa-1}$ with $\rho_K(R) = \kappa$. As $P \rightarrow \{P, Y\}$ maps $K[X, Y]_\kappa$ onto $K[X, Y]_{\kappa-1}$, there exists a form $S \in K[X, Y]_\kappa$ such that $R = \{S, Y\}$. Then $\rho_{\bar{K}}(S) \geqslant \kappa$ which we prove indirectly. Suppose that there exists a form $Q \in D_{\kappa-1}$ with $\{S, Q\} = 0$. By Lemma 1, $\{R, Q\} = \{\{S, Y\}, Q\} = \{S, YQ\} = \{\{S, Q\}, Y\} = 0$. Since $\rho_K(R) = \kappa$, it follows that $Q = Y\tilde{Q}$ where $\tilde{Q} \in D_{\kappa-2}$ and $\tilde{Q}(\infty) \neq 0$. But then $\{R, \tilde{Q}\} = \{\{S, Y\}, \tilde{Q}\} = \{S, Q\} = 0$ contradicting $\rho_K(R) = \kappa$. □

Theorem 6. *The numbers $\rho(d, q)$, $2 \leqslant d \leqslant q + 1$, form an ascending sequence*

$$\rho(2, q) \leqslant \rho(3, q) \leqslant \cdots \leqslant \rho(q, q) \leqslant \rho(q + 1, q).$$

Particular values are $\rho(2, q) = 1$, $\rho(3, q) = 1$, $\rho(4, q) = 3$ if q is even, $\rho(4, q) = 2$ if q is odd, $\rho(5, q) = 3$, $\rho(6, q) = 4$, $\rho(7, q) = 5$, $\rho(q, q) = q - 1$ if q is even, $\rho(q, q) = q - 2$ if q is odd, and $\rho(q + 1, q) = q - 1$.

Proof. By Proposition 1, $d - 2 \leqslant \rho(d, q) \leqslant d - 1 \leqslant \rho(d + 1, q) \leqslant d$. Clearly $\rho(2, q) = 1$ because $D_0 = K^*$, and $\rho(3, q) = 1$ because $D_1 = \{Q \in K[X, Y]_1; Q \neq 0\}$. If $d = 4$ and q is even, the discriminant variety $KY^2 + KX^2$ is a linear hyperplane having empty intersection with D_2, and hence $\rho(4, q) = 3$. Now let $d = 4$ and q be odd. Let $S = s_0X^2 + s_1XY + s_2Y^2$ be nonzero. Then $\{S, (X - (s_1/s_0)Y)Y\} = 0$ if $s_0 \neq 0$, $\{S, X((s_1/s_2)X - Y)\} = 0$ if $s_2 \neq 0$, and $\{S, (X - Y)(X + Y)\} = 0$ if $s_0 = s_2 = 0$. We conclude that $\rho(4, q) = 2$ if q is odd. The results on $\rho(d, q)$ for $d = 5, 6, 7$, and $d = q$ are consequences of the subsequent Proposition 2 and Theorem 7. Finally, the repetition code $K(1, 1, \ldots, 1)$ over $K = \mathrm{GF}(q)$ of length $q + 1$ has, by the pidgeonhole principle, covering radius $\rho(q + 1, q) = q - 1$. □

Proposition 2. *If $5 \leqslant d \leqslant q/2 + 3$, then $\rho(d, q) = d - 2$.*

Proof. On $\bar{K}$ coordinates are given by the map $\varphi=(\varphi_1,\varphi_2):\bar{K}\to K^2$, $\varphi(z)=(z,1)$ if $z\in K$, and $\varphi(\infty)=(1,0)$. For a polynomial $V(X_1,Y_1;X_2,Y_2;\cdots;X_\kappa,Y_\kappa)$ over K and for elements $z_1,z_2,\ldots,z_\kappa\in\bar{K}$, we define $V(z_1,z_2,\ldots,z_\kappa)=V(\varphi(z_1),\varphi(z_2),\ldots,\varphi(z_\kappa))$. For example, let $e_l^{(\kappa)}(X_1,X_2,\ldots,X_\kappa)$ be the elementary symmetric polynomial in the variables $X_1,X_2,\ldots,X_\kappa$ of degree l, $0\leq l\leq\kappa$, and define a new polynomial in the variables $X_1,Y_1,X_2,Y_2,\ldots,X_\kappa,Y_\kappa$ by

$$\begin{aligned}E_l^{(\kappa)}&=E_l^{(\kappa)}(X_1,Y_1;X_2,Y_2;\cdots;X_\kappa,Y_\kappa)\\&=Y_1Y_2\cdots Y_\kappa e_l^{(\kappa)}(X_1/Y_1,X_2/Y_2,\cdots,X_\kappa/Y_\kappa).\end{aligned}$$

Then

$$\prod_{i=1}^{\kappa}[(X,Y),z_i]=\sum_{l=0}^{\kappa}(-1)^lE_l^{(\kappa)}(z_1,z_2,\ldots,z_\kappa)X^{\kappa-l}Y^l$$

and, for $1\leq l\leq\kappa-1$,

$$\begin{aligned}E_l^{(\kappa)}(z_1,z_2,\ldots,z_\kappa)=E_{l-1}^{(\kappa-1)}&(z_1,z_2,\ldots,z_{\kappa-1})\varphi_1(z_\kappa)\\&+E_l^{(\kappa-1)}(z_1,z_2,\ldots,z_{\kappa-1})\varphi_2(z_\kappa).\end{aligned}$$

After these preparations, we now prove that, for every $S\in K[X,Y]_\kappa$, there exists a form $Q\in D_\kappa$ with $\{S,Q\}=0$. We may assume that $S\neq0$. Let $S=\sum_{i=0}^{\kappa}(-1)^ia_iX^iY^{\kappa-i}$, and let $Q=\prod_{i=1}^{\kappa}[(X,Y),z_i]$ where $z_1,z_2,\ldots,z_\kappa$ are distinct elements of $\bar{K}$. Then

$$\begin{aligned}\{S,Q\}&=\sum_{l=0}^{\kappa}a_lE_l^{(\kappa)}(z_1,\ldots,z_\kappa)\\&=A(z_1,\ldots,z_{\kappa-1})\varphi_1(z_\kappa)+B(z_1,\ldots,z_{\kappa-1})\varphi_2(z_\kappa)\end{aligned}$$

where

$$A(z_1,\ldots,z_{\kappa-1})=\sum_{l=1}^{\kappa}a_lE_{l-1}^{(\kappa-1)}(z_1,\ldots,z_{\kappa-1})$$

and

$$B(z_1,\ldots,z_{\kappa-1})=\sum_{l=0}^{\kappa-1}a_lE_l^{(\kappa-1)}(z_1,\ldots,z_{\kappa-1}).$$

Consequently, the existence of a form $Q\in D_\kappa$ with $\{S,Q\}=0$ follows from the existence of distinct elements $z_1,z_2,\ldots,z_{\kappa-1}\in\bar{K}$ such that, for $m=1,2,\ldots,\kappa-1$,

$$A(z_1,\ldots,z_{\kappa-1})\varphi_1(z_m)+B(z_1,\ldots,z_{\kappa-1})\varphi_2(z_m)\neq0.$$

To that end, we consider the polynomial

$$\begin{aligned}W&=W(X_1,Y_1;X_2,Y_2;\cdots;X_{\kappa-1},Y_{\kappa-1})\\&=\prod_{i>j}(X_iY_j-X_jY_i)\prod_{m=1}^{\kappa-1}\left(\sum_{l=0}^{\kappa}a_lE_l^{(\kappa)}(X_1,Y_1;\cdots;X_{\kappa-1},Y_{\kappa-1};X_m,Y_m)\right)\end{aligned}$$

which, for each m, is partially homogeneous in X_m and Y_m of degree $\leqslant 2\kappa - 2$. As

$$\sum_{l=0}^{\kappa} a_l E_l^{(\kappa)}(X_1, Y_1; \cdots; X_{\kappa-1}, Y_{\kappa-1}; X_{\kappa-1}, Y_{\kappa-1})$$
$$= \Big(\sum_{l=0}^{\kappa-2} a_{l+2} E_l^{(\kappa-2)}\Big) X_{\kappa-1}^2 + 2\Big(\sum_{l=0}^{\kappa-2} a_{l+1} E_l^{(\kappa-2)}\Big) X_{\kappa-1} Y_{\kappa-1}$$
$$+ \Big(\sum_{l=0}^{\kappa-2} a_l E_l^{(\kappa-2)}\Big) Y_{\kappa-1}^2$$

is not identically zero for $\kappa \geqslant 3$, the polynomial W is not identically zero. Since $2\kappa - 2 < q + 1$ by hypothesis, there exist elements $z_1, z_2, \ldots, z_{\kappa-1} \in \bar{K}$ such that $W(z_1, z_2, \ldots, z_{\kappa-1}) \neq 0$. □

Theorem 7. *Let* $S \in K[X, Y]_{q-2}$ *where* $K = \mathrm{GF}(q)$. *Then* $\rho_{\bar{K}}(S) = q - 1$ *if and only if the set*

$$\{K(zS(z), zS(1), S(1)); z \in K\} \cup \{K(1, 0, 0), K(0, 1, 0)\}$$

is an oval in the projective plane $\mathrm{PG}(2, q)$. *Hence* $\rho(q, q) = q - 1$ *if* q *is even, and* $\rho(q, q) = q - 2$ *if* q *is odd.*

Remark 4. If q is odd, there exist no ovals with $q + 2$ points in PG(2, q). If q is even, every oval in PG(2, q) consists of $q + 2$ points and can be brought into the form of Theorem 7 by a projective transformation (compare [12, p. 163]). Therefore, the determination of all syndromes $S \in K[X, Y]_{q-2}$ with $\rho_{\bar{K}}(S) = q - 1$ is equivalent to the determination of all ovals in PG(2, q), q even. In addition to the regular ovals that arise from conics, there also exist irregular ovals for $q = 16$, 32, and $q \geqslant 128$. According to [16, p. 278], it is unlikely that the determination of all ovals in PG(2, q), q even, will be completed in the near future. For small values of q, we refer to [12, p. 174 and p. 413].

Proof of Theorem 7. Let $S = \sum_{i=0}^{\kappa} s_i X^{\kappa-i} Y^i$ where $\kappa = q - 2$. Then $\rho_{\bar{K}}(S) = q - 1$ if and only if, for all $Q \in D_\kappa$, $\{S, Q\} \neq 0$. If $Q = \prod_{z \in N}(X - zY)$ where $N = K - \{a, b\}$ and $a, b \in K$, then

$$Q = (a - b)^{-1} \sum_{j=0}^{\kappa} (a^{j+1} - b^{j+1}) X^{\kappa-j} Y^j$$

and

$$\{S, Q\} = (a - b)^{-1}(aS(a) - bS(b)).$$

If $Q = \prod_{z \in N}[(X, Y), z]$ where $N = \bar{K} - \{a, b, c\}$ and $a, b, c \in K$, then

$$Q = (b - c)^{-1}(c - a)^{-1}(a - b)^{-1}$$
$$\times \sum_{i=0}^{\kappa} ((b - c)a^{i+1} + (c - a)b^{i+1} + (a - b)c^{i+1}) X^{\kappa-i} Y^i$$

and

$$\{S, Q\} = (b-c)^{-1}(c-a)^{-1}(a-b)^{-1}((b-c)aS(a)+(c-a)bS(b)$$
$$+(a-b)cS(c)).$$

Consequently, $\rho_K(S) = q-1$ if and only if, for all distinct elements $a, b, c \in K$, both $aS(a) \neq bS(b)$ and $(b-c)aS(a)+(c-a)bS(b)+(a-b)cS(c) \neq 0$. But this is precisely the condition for the set $\{K(zS(z), zS(1), S(1)); z \in K\} \cup \{K(1, 0, 0)$ $K(0, 1, 0)\}$ to be an oval in PG$(2, q)$ [12, p. 174]. □

Remark 5. It remains an open problem to determine $\rho(d, q)$ if $q/2+3<d<q$.

References

[1] I.S. Beresin and N.P. Shidkow, Numerische Methoden 1 (Deutscher Verlag der Wissenschaften, Berlin, 1970).

[2] E.R. Berlekamp, Algebraic Coding Theory (McGraw-Hill, New York, 1968).

[3] R.E. Blahut, Theory and Practice of Error Control Codes (Addison-Wesley, Reading, MA, 1983).

[4] C.L. Chen, High-spped decoding of BCH codes, IEEE Trans. Info. Theory 27 (1981) 254–256.

[5] G.C. Clark and J.B. Cain, Error-Correcting Coding for Digital Communications (Plenum, New York, 1981).

[6] G.D. Cohen, M.G. Karpovsky, H.F. Mattson Jr and J.R. Schatz, Covering radius—survey and recent results, IEEE Trans. Info. Theory 31 (1985) 328–343.

[7] P. Delsarte, On subfield subcodes of modified Reed–Solomon codes, IEEE Trans. Info. Theory 21 (1975) 575–576.

[8] A. Dür, The automorphism groups of Reed–Solomon codes, J. Combin. Theory Ser. A 44 (1987) 69–82.

[9] A. Dür, On linear MDS codes of length $q+1$ over GF(q) for even q, J. Combin. Theory Ser. A 49 (1988) 172–174.

[10] G.D. Forney Jr, On decoding BCH codes, IEEE Trans. Info. Theory 11 (1965) 549–557.

[11] J.H. Grace and A. Young, The Algebra of Invariants (Cambridge Univ. Press, Cambridge, 1903).

[12] J.W.P. Hirschfeld, Projective Geometries over Finite Fields (Clarendon Press, Oxford, 1979).

[13] J.P.S. Kung, Gundelfinger's theorem on binary forms, Studies in Appl. Math. 75 (1986) 163–170.

[14] J.P.S. Kung and G.-C. Rota, The invariant theory of binary forms, Bull. Amer. Math. Soc. (N.S.) 10 (1983) 27–85.

[15] F.J. MacWilliams and N.J.A. Sloane, The Theory of Error-Correcting Codes (North-Holland, Amsterdam, 1981).

[16] S.E. Payne and J.A. Thas, Finite Generalized Quadrangles (Pitman, London, 1984).

[17] R.M. Roth and G. Seroussi, On generator matrices of MDS codes, IEEE Trans. Info. Theory 31 (1985) 826–830.

[18] W.M. Schmidt, Equations over Finite Fields, Lecture Notes in Mathematics 536 (Springer, Berlin, 1976).

[19] G. Seroussi and R.M. Roth, On MDS extensions of generalized Reed–Solomon codes, IEEE Trans. Info. Theory 32 (1986) 349–354.

[20] K.K. Tzeng, C.R.P. Hartmann and R.T. Chien, Some notes on iterative decoding, Proc. Ninth Allerton Conf. on Circuit and Systems Theory (1971) 689–695.

[22] J.K. Wolf, Adding two information symbols to certain nonbinary BCH codes and some applications, Bell Syst. Tech. J. 48 (1969) 2405–2424.