Scalar q-subresultants and Dickson matrices

Bence Csajbók*

Abstract

Following the ideas of Ore and Li we study q-analogues of scalar subresultants and show how these results can be applied to determine the rank of an $\mathbb{F}_q$-linear transformation f of $\mathbb{F}_{q^n}$. As an application we show how certain minors of the Dickson matrix $D(f)$, associated with f, determine the rank of $D(f)$ and hence the rank of f.

Keywords: Dickson matrix, subresultant, linearized polynomial

1 Introduction

Let $f(x) = \sum_{i=0}^{k} a_i x^i$ and $g(x) = \sum_{i=0}^{l} b_i x^i$, with $a_k b_l \neq 0$, be two univariate polynomials with coefficients in the field $\mathbb{K}$ [1]. In elimination theory, the classical resultant of f and g is

$$\operatorname{Res}(f,g) = (-1)^{kl} b_l^k \prod_{i=1}^{l} f(\xi_i),$$

where $g(x) = b_l \prod_{i=1}^{l}(x-\xi_i)$ with $\xi_1, \xi_2, \ldots, \xi_l \in \overline{\mathbb{K}}$ (where $\overline{\mathbb{K}}$ denotes the algebraic closure of $\mathbb{K}$). For $0 \leqslant m \leqslant \min\{k,l\}$ consider the following

*Supported by the ÚNKP-18-4 New National Excellence Program of the Ministry of Human Capacities and by OTKA Grant No. K 124950.

[1]Note that in many of the cited literature a_0 and b_0 are used to denote the leading coefficients of f and g.

$(k+l-2m) \times (k+l-2m)$ matrix:

$$R_m(f,g) := \begin{pmatrix} a_k & a_{k-1} & a_{k-2} & \dots & a_{k-l+m+1} & \dots & a_{2m-l+2} & a_{2m-l+1} \\ 0 & a_k & a_{k-1} & \dots & a_{k-l+m+2} & \dots & a_{2m-l+3} & a_{2m-l+2} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \dots & 0 & \dots & a_k & \dots & a_{m+1} & a_m \\ b_l & b_{l-1} & b_{l-2} & \dots & \dots & \dots & b_{2m-k+2} & b_{2m-k+1} \\ 0 & b_l & b_{l-1} & \dots & \dots & \dots & b_{2m-k+3} & b_{2m-k+2} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \dots & 0 & b_l & \dots & \dots & b_{m+1} & b_m \end{pmatrix},$$

where coefficients out of range are considered to be 0.

The determinant of $R_m(f,g)$ is also called the m-th *scalar subresultant* of f and g. Note that $|R_0(f,g)| = \mathrm{Res}(f,g)$ and hence $\gcd(f,g) = 1$ if and only if $|R_0(f,g)| \neq 0$. This result has the following well-known generalization in elimination theory. For a proof we cite here the Appendix of [10] and the references therein, since the proof of Theorem 2.1 was motivated by the arguments found there.

Result 1.1. *The degree of* $\gcd(f,g)$ *is* t *if and only if* $|R_0(f,g)| = \ldots = |R_{t-1}(f,g)| = 0$ *and* $|R_t(f,g)| \neq 0$.

The strength of the Result 1.1 is that it provides a way to study the number of common roots of f and g only by means of their coefficients.

Now let $\mathbb{K}$ be a field of characteristic p, and let q be a power of p. A *q-polynomial* over $\mathbb{K}$ with *q-degree* m is a polynomial of the form $f(x) = \sum_{i=0}^{m} a_i x^{q^i}$, with $a_m \neq 0$ and $a_0, a_1, \ldots, a_m \in \mathbb{K}$. When $q = p$ prime, q-analogue of the classical resultant for q-polynomials was already mentioned in [14, Chapter 1, Section 7], however, an explicit formula was not given there. An explicit formula can be found for example in [17, page 59].

The subresultant theory was extended to Ore polynomials (cf. [15]) and hence also to the non-commutative ring of q-polynomials by Li in [11]. Here the non-commutative operation between two q-polynomials is composition, while addition is defined as usual. Note that this ring is a right-Euclidean domain with respect to the q-degree, cf. [14]. When $g = f \circ h$ then we will also say that h is a symbolic right divisor of g. Note that in the paper of Li the word subresultant is used to what is also known as *polynomial subresultant*. In the classical theory the m-th scalar subresultant is the leading coefficient of the m-th polynomial subresultant. See for example [1, Section 2] for a brief summary, where $S_m^{(m)}$ corresponds to what we (and some other authors) call scalar subresultant. For the various notions consult with [9].

Let $\mathbb{K} = \mathbb{F}_{q^n}$ and consider $\mathbb{K}$ as an n-dimensional vector space over $\mathbb{F}_q$. Then there is an isomorphism between the ring of q-polynomials

$$\left\{ \sum_{i=0}^{n-1} a_i x^{q^i} : a_0, \ldots, a_{n-1} \in \mathbb{F}_{q^n} \right\}$$

considered modulo $(x^{q^n} - x)$ and the ring of $\mathbb{F}_q$-linear transformations of $\mathbb{F}_{q^n}$. The set of roots of a q-polynomial form an $\mathbb{F}_q$-subspace and the dimension of this subspace is the dimension of the kernel of the corresponding $\mathbb{F}_q$-linear transformation. Thus $\deg \gcd(f(x), x^{q^n} - x) = q^{n-k}$, where k is the rank of the $\mathbb{F}_q$-linear transformation of $\mathbb{F}_{q^n}$ defined by $f(x)$. When n is clear from the context, then we will say that k is the *rank* of f.

Result 1.2 (Ore [14, Theorem 2])**.** *The greatest common symbolic right divisor of two q-polynomials is the same as their ordinary greatest common divisor.*

It follows that the q-subresultant theory can be applied to determine $\gcd(f(x), x^{q^n} - x)$ and hence the rank of f. Our contribution to this theory is a direct proof to a q-analogue of Result 1.1 providing sufficient and necessary conditions which ensure that f has rank $n - k$ (cf. Theorem 2.1).

Recall that the Dickson matrix associated with $f(x) = \sum_{i=0}^{n-1} a_i x^{q^i} \in \mathbb{F}_{q^n}[x]$ is

$$D(f) := \begin{pmatrix} a_0 & a_1 & \ldots & a_{n-1} \\ a_{n-1}^q & a_0^q & \ldots & a_{n-2}^q \\ \vdots & \vdots & \vdots & \vdots \\ a_1^{q^{n-1}} & a_2^{q^{n-1}} & \ldots & a_0^{q^{n-1}} \end{pmatrix}.$$

It is well-known that the rank of f equals the rank of $D(f)$, see for example [18, Proposition 4.4] or [13, Proposition 5]. In some recent constructions of maximum scattered subspaces and MRD-codes it was crucial to the determine the rank of certain Dickson matrices (cf. [6, Section 7] and [7, Section 5]). In these papers this was done by considering certain minors of such matrices and excluding the possibility that their determinants vanish at the same time. On the other hand, in [4, Section 3] Dickson matrices were used to prove non-existence results of certain MRD-codes. This was done by proving that, for a certain choice of the parameters, all 6×6 submatrices of a 9×9 Dickson matrix have zero determinant. As an application of Theorem

2.1 we show that it is enough to investigate the nullity of the determinant of at most $k+1$ well-defined minors to decide whether f has rank $n-k$. This result can significantly simplify the above mentioned arguments.

To state here the main result of this paper we introduce the notion $D_m(f)$ to denote the $(n-m)\times(n-m)$ matrix obtained from $D(f)$ after removing its first m columns and last m rows. Our main result is the following.

Theorem 1.3. $\dim_q(\ker f)=\mu$ *if and only if*

$$|D_0(f)| = |D_1(f)| = \ldots = |D_{\mu-1}(f)| = 0 \tag{1}$$

and $|D_\mu(f)| \neq 0$.

Results in a similar direction have been obtained recently in [5] where for each q-polynomial f of q-degree k, k conditions were given, in terms of the coefficients of f, which are satisfied if and only if f has rank $n-k$ (there is a hidden $(k+1)$-th condition here as well, namely the assumption that the coefficient of x^{q^k} in f is non-zero). Independently, in [16] it was proved that the rank of f is $n-m$ if and only if a certain $k\times k$ matrix has rank $k-m$. If $m=k$, then this result gives back the main result of [5].

2 Scalar q-subresultants

Consider $f(x)=\sum_{i=0}^{k} a_i x^{q^i}$ and $g(x)=\sum_{i=0}^{l} b_i x^{q^i}$, two q-polynomials with coefficients in $\overline{\mathbb{F}}_q$ such that $a_k b_l \neq 0$. Put

$$q^\mu = \deg\gcd(f,g).$$

By Result 1.2, μ also equals the q-degree of the symbolic greatest common right divisor of f and g.

For $m \leqslant \min\{k,l\}$ we define the $(k+l-2m)\times(k+l-2m)$ matrix $R_{m,q}(f,g)$ as follows:

$$\begin{pmatrix}
a_k^{q^{l-m-1}} & a_{k-1}^{q^{l-m-1}} & a_{k-2}^{q^{l-m-1}} & \ldots & a_{k+m-l+1}^{q^{l-m-1}} & \ldots & a_{2m-l+2}^{q^{l-m-1}} & a_{2m-l+1}^{q^{l-m-1}} \\
0 & a_k^{q^{l-m-2}} & a_{k-1}^{q^{l-m-2}} & \ldots & a_{k+m-l+2}^{q^{l-m-2}} & \ldots & a_{2m-l+3}^{q^{l-m-2}} & a_{2m-l+2}^{q^{l-m-2}} \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
0 & \ldots & 0 & \ldots & a_k & \ldots & a_{m+1} & a_m \\
b_l^{q^{k-m-1}} & b_{l-1}^{q^{k-m-1}} & b_{l-2}^{q^{k-m-1}} & \ldots & \ldots & \ldots & b_{2m-k+2}^{q^{k-m-1}} & b_{2m-k+1}^{q^{k-m-1}} \\
0 & b_l^{q^{k-m-2}} & b_{l-1}^{q^{k-m-2}} & \ldots & \ldots & \ldots & b_{2m-k+3}^{q^{k-m-2}} & b_{2m-k+2}^{q^{k-m-2}} \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
0 & \ldots & 0 & b_l & \ldots & \ldots & b_{m+1} & b_m
\end{pmatrix}.$$

Note that $R_{m+1,q}(f,g)$ is obtained from $R_{m,q}(f,g)$ by removing its first and last columns, and its first and $(l-m+1)$-th rows.

We state here the q-analogue of Result 1.1.

Theorem 2.1. *The q-degree of* $\gcd(f,g)$ *is* μ *if and only if* $|R_{0,q}(f,g)| = \ldots = |R_{\mu-1,q}(f,g)| = 0$ *and* $|R_{\mu,q}(f,g)| \neq 0$.

We prove this result directly by following the proof of the classical Result 1.1. Theorem 2.1 will easily follow from Proposition 2.3.

Proposition 2.2. *Recall* $q^\mu = \deg\gcd(f,g)$ *and let* $m \leqslant \mu$. *Let* $c(x) = \sum_{i=0}^{k-m} c_i x^{q^i}$ *and* $d(x) = \sum_{i=0}^{l-m} d_i x^{q^i}$ *be q-polynomials over* $\overline{\mathbb{F}_q}$ *with* $c_{k-m} = a_k^{q^{l-m}}$, $d_{l-m} = b_l^{q^{k-m}}$, *and their other coefficients are considered as unknowns. Then the set of solutions for these coefficients such that*

$$d \circ f - c \circ g = 0 \tag{2}$$

form a $(\mu - m)$*-dimensional affine* $\overline{\mathbb{F}_q}$*-space.*

Proof. First assume that f and g have only simple roots.

Let r be the greatest common monic symbolic right divisor of f and g and suppose that (2) holds for some c and d. Then $f = f_1 \circ r$ and $g = g_1 \circ r$ and (2) yields $d \circ f_1 = c \circ g_1$, thus d is zero on $f_1(\ker g_1)$ (in this proof the kernel is always taken over $\overline{\mathbb{F}_q}$) and c is zero on $g_1(\ker f_1)$. Since the greatest common symbolic right divisor of f_1 and g_1 is the identity map, it follows that $\gcd(f_1, g_1) = x$ and hence $\ker f_1 \cap \ker g_1 = \{0\}$. Thus $\dim_q f_1(\ker g_1) = \dim_q \ker g_1 = l - \mu$ and similarly $\dim_q g_1(\ker f_1) = k - \mu$. It follows that the unique q-polynomial d_1 of q-degree $l-\mu$ and with leading coefficient $b_l^{q^{k-\mu}}$ which vanishes on $f_1(\ker g_1)$ is a divisor of d. By Result 1.2 $\gcd(d, d_1) = d_1$ is also a symbolic right divisor of d, i.e. $d = d_2 \circ d_1$, for some monic d_2 with q-degree $(\mu - m)$. Similarly, the unique q-polynomial c_1 of q-degree $k - \mu$ and with leading coefficient $a_k^{q^{l-\mu}}$ which vanishes on $g_1(\ker f_1)$ is a symbolic right divisor of c, i.e. $c = c_2 \circ c_1$, for some monic c_2 with q-degree $(\mu - m)$.

Note that

$$d_1 \circ f_1 - c_1 \circ g_1$$

has q-degree $k + l - 2\mu - 1$ (the coefficient of $x^{q^{k+l-2\mu}}$ vanishes because of the assumptions on the leading coefficients of c and d) and it vanishes on $\ker f_1 \oplus \ker g_1$. Thus it is the zero polynomial.

Then

$$c_2 \circ c_1 \circ g_1 = c \circ g_1 = d \circ f_1 = d_2 \circ d_1 \circ f_1 = d_2 \circ c_1 \circ g_1$$

and hence $c_2 = d_2$. On the other hand, if $c_2 = d_2$, then we clearly have a solution since (2) becomes $d_2 \circ (d_1 \circ f_1 - c_1 \circ g_1) \circ r$ with the zero polynomial in the middle.

Since we can choose the first $(\mu - m)$ coefficients of $d_2(x) = \sum_{i=0}^{\mu-m} \hat{d}_i x^{q^i}$ arbitrarily, the assertion follows. More precisely, if $d_1(x) = \sum_{j=0}^{\mu-m} \bar{d}_j x^{q^j}$ with $\bar{d}_{l-\mu} = b_l^{q^{k-\mu}}$ and with coefficients out of range defined as 0, then $d(x)$ is of the form

$$\sum_{i=0}^{k-m} \sum_{j=0}^{i} \hat{d}_{i-j} \bar{d}_j^{\,q^{i-j}} x^{q^i},$$

with $\hat{d}_k \in \overline{\mathbb{F}_q}$ for $0 \leqslant k \leqslant \mu - m - 1$, $\hat{d}_{\mu-m} = 1$ and $\hat{d}_l = 0$ for $l > \mu - m$. These polynomials form a $(\mu - m)$-dimensional affine $\overline{\mathbb{F}_q}$-space and as we have seen, any such $d(x)$ uniquely defines a $c(x)$ for which (2) holds.

Now consider the case when f and g may have multiple roots. Let $f = x^{q^{k_1}} \circ \tilde{f}$ and $g = x^{q^{l_1}} \circ \tilde{g}$ where $\tilde{f}$ and $\tilde{g}$ have only simple roots. W.l.o.g. assume $l_1 \leqslant k_1$. We want to find the dimension of the solutions of

$$d \circ x^{q^{k_1}} \circ \tilde{f} = c \circ x^{q^{l_1}} \circ \tilde{g},$$

under the given assumptions on the degrees and leading coefficients of c and d. Clearly, the multiplicities of the roots of the left hand side and the right hand side have to coincide and hence $c = c' \circ x^{q^{k_1 - l_1}}$. Let $\tilde{d}$ and $\tilde{c}'$ denote the q-polynomials whose coefficients are the q^{-k_1}-th roots of the coefficients of d and c, respectively. Then the solutions of the previous system correspond to the solutions of

$$x^{q^{k_1}} \circ \tilde{d} \circ \tilde{f} = x^{q^{k_1}} \circ \tilde{c}' \circ \tilde{g}$$

and hence to those of

$$\tilde{d} \circ \tilde{f} = \tilde{c}' \circ \tilde{g},$$

where the q-degree of $\tilde{d}$ is $(l - l_1) - (m - l_1)$ and the q-degree of $\tilde{c}'$ is $(k - k_1) - (m - l_1)$. The roots of the q-polynomials $\tilde{f}$ and $\tilde{g}$ are simple, thus we can apply the first part of this proof for these polynomials. The leading coefficients of $\tilde{d}$ and $\tilde{c}'$ are $b_l^{q^{k-m-k_1}}$ and $a_k^{q^{l-m-k_1}}$, respectively; the leading coefficients of $\tilde{f}$ and $\tilde{g}$ are $a_k^{q^{-k_1}}$ and $b_l^{q^{-l_1}}$, respectively. Since $b_l^{q^{k-m-k_1}} = b_l^{q^{-l_1} \deg \tilde{c}'}$ and $a_k^{q^{l-m-k_1}} = a_k^{q^{-k_1} \deg \tilde{d}}$, the conditions on the leading coefficients also hold. Note that the q-degree of $\gcd(\tilde{f}, \tilde{g})$ is $\mu - l_1$. Then the dimension of the solutions of this system is $(\mu - l_1) - (m - l_1) = \mu - m$.

□

Proposition 2.3. *Suppose $m \leqslant \mu$. Then the nullity of the matrix $R_{m,q}(f,g)$ is $\mu - m$.*

Proof. Let f, g, c, d be defined as before, then

$$d \circ f - c \circ g = \sum_{i=0}^{l-m} d_i \sum_{j=0}^{k} a_j^{q^i} x^{q^{j+i}} - \sum_{i=0}^{k-m} c_i \sum_{j=0}^{l} b_j^{q^i} x^{q^{j+i}} =$$

$$\sum_{i=0}^{k+l-m} \left(\sum_{j=0}^{i} d_{i-j} a_j^{q^{i-j}} - c_{i-j} b_j^{q^{i-j}} \right) x^{q^i}.$$

The q-degree of $r := \gcd(f,g)$ is $\mu \geqslant m$ and $r \mid d \circ f - c \circ g$, thus d and c form a solution to $d \circ f - c \circ g = 0$ if and only if the q-degree of $d \circ f - c \circ g$ is less than m. In another words, we only have to concentrate on the coefficients of terms with q-degree $i \in \{m, m+1, \ldots, k+l-m\}$ in $d \circ f - c \circ g$.

Note that the coefficient of q^{k+l-m} is $d_{l-m} a_k^{q^{l-m}} - c_{k-m} b_l^{q^{k-m}}$ (coefficients out of range are considered to be 0), which is 0 because of our assumptions on c and d. Now let

$$\mathbf{v} = (d_{l-m-1}, d_{l-m-2}, \ldots, d_0, -c_{k-m-1}, -c_{k-m-2}, \ldots, -c_0)$$

and

$$\mathbf{b} = (b_l^{q^{k-m}} a_{k-1}^{q^{l-m}} - a_k^{q^{l-m}} b_{l-1}^{q^{k-m}}, \ldots, b_l^{q^{k-m}} a_{2m-l}^{q^{l-m}} - a_k^{q^{l-m}} b_{2m-k}^{q^{k-m}}).$$

We claim that

$$\mathbf{v} R_{m,q}(f,g) = -\mathbf{b} \tag{3}$$

holds if and only if

$$\sum_{j=0}^{i} d_{i-j} a_j^{q^{i-j}} - c_{i-j} b_j^{q^{i-j}} = 0 \tag{4}$$

for all $m \leqslant i \leqslant k+l-m-1$. To see this we show that the $(k+l-2m-t)$-th coordinates in the vectors at the left and right hand side of (3) coincide if and only if (4) holds with $i = m+t$. Indeed, in

$$\sum_{j=0}^{m+t} d_{m+t-j} a_j^{q^{m+t-j}} - c_{m+t-j} b_j^{q^{m+t-j}} \tag{5}$$

$d_{m+t-j} \neq 0$ only if $j \in \{m+t, m+t-1, \ldots, 2m+t-l\}$ and $c_{m+t-j} \neq 0$ only if $j \in \{m+t, m+t-1, \ldots, 2m+t-k\}$. Thus, after changing indices in the summation, (5) equals

$$\sum_{j=0}^{l-m} d_{l-m-j} a_{2m+t-l+j}^{q^{l-m-j}} - \sum_{j=0}^{k-m} c_{k-m-j} b_{2m+t-k+j}^{q^{k-m-j}}. \tag{6}$$

Since $d_{l-m} = b_l^{q^{k-m}}$ and $c_{k-m} = a_k^{q^{l-m}}$, the $(k+l-2m-t)$-th coordinates on the left and right hand side of (3) coincide if and only if

$$\sum_{j=0}^{l-m-1} d_{l-m-1-j} a_{2m-l+1+t+j}^{q^{l-m-1-j}} - \sum_{s=0}^{k-m-1} c_{k-m-1-s} b_{2m-k+1+t+j}^{q^{k-m-1-s}} =$$

$$d_{l-m} a_{2m-l+t}^{q^{l-m}} - c_{k-m} b_{2m-k+t}^{q^{k-m}},$$

and this happens if and only if (6) equals zero.

Thus the dimension of the kernel of the $\overline{\mathbb{F}_q}$-linear transformation of $\overline{\mathbb{F}_q}^{k+l-2m}$ defined by $\mathbf{x} \mapsto \mathbf{x} R_{m,q}(f,g)$ is the same as the dimension of the set of solutions of (2) and this finishes the proof. $\square$

Corollary 2.4. *Let f be a q-polynomial over $\mathbb{F}_{q^n}$ and put $g(x) = x^{q^n} - x$. Then $\dim_q(\ker f) = \mu$ if and only if*

$$|R_{0,q}(f,g)| = |R_{1,q}(f,g)| = \ldots = |R_{\mu-1,q}(f,g)| = 0 \tag{7}$$

and $|R_{\mu,q}(f,g)| \neq 0$.

As an illustration, the $(n+k) \times (n+k)$ matrix $R_{0,q}(f,g)$ in the particular case when $g(x) = x^{q^n} - x$ and $f(x) = \sum_{i=0}^{k} a_i x^{q^i}$ has the following form:

$$\begin{pmatrix}
a_k^{q^{n-1}} & a_{k-1}^{q^{n-1}} & \ldots & a_0^{q^{n-1}} & 0 & \ldots & 0 & 0 & \ldots & 0 \\
0 & a_k^{q^{n-2}} & \ldots & a_1^{q^{n-2}} & a_0^{q^{n-2}} & \ldots & 0 & 0 & \ldots & 0 \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
0 & 0 & \ldots & 0 & 0 & \ldots & a_k & a_{k-1} & \ldots & a_0 \\
1 & 0 & \ldots & 0 & 0 & \ldots & 0 & -1 & \ldots & 0 \\
0 & 1 & \ldots & 0 & 0 & \ldots & 0 & 0 & \ldots & 0 \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
0 & 0 & \ldots & 0 & 0 & \ldots & 0 & 0 & \ldots & -1
\end{pmatrix}.$$

The matrix $R_{m,q}(f,g)$ can be obtained from $R_{0,q}(f,g)$ by removing its first and last m columns and its first m rows together with the $(n+1)$-th, $(n+2)$-th, ..., $(n+m)$-th rows.

Let $\tilde{f}(x) = \sum_{i=0}^{k-1} a_i x^{q^i}$ and $g(x) = x^{q^n} - x$. If we substitute $a_k = 0$ in $R_{m,q}(f,g)$, then its determinant equals either $|R_{m,q}(\tilde{f},g)|$ or $-|R_{m,q}(\tilde{f},g)|$. This argument can be iterated and hence one can use Corollary 2.4 even if the q-degree of f is not known, by considering the $(2n-1-2m)\times(2n-1-2m)$ m-th scalar q-subresultants of $\sum_{i=0}^{n-1} a_i x^{q^i}$ and $g(x)$.

3 A connection with Dickson matrices

In this section we prove Theorem 1.3 but before that we need some preparation.

Result 3.1 (Schur's determinant identity, [3]). *Consider the square matrix*

$$M := \begin{pmatrix} X & Y \\ Z & W \end{pmatrix},$$

where W is also square and invertible. Then $\det(M) = \det(W)\det(X - YW^{-1}Z)$.

Corollary 3.2. *Consider the square matrices*

$$M := \begin{pmatrix} A & B & C \\ I_l & O & -I_l \end{pmatrix},$$

$$N := \begin{pmatrix} B & A+C \end{pmatrix},$$

where A and C are $k \times l$ matrices, B is $k \times (k-l)$, I_l denotes the $l \times l$ identity matrix and O is the $l \times (k-l)$ zero matrix. Then $\det(M) = (-1)^{l(k-l+1)} \det(N)$.

Proof. Result 3.1 with $X = \begin{pmatrix} A & B \end{pmatrix}$, $Y = C$, $Z = \begin{pmatrix} I_l & O \end{pmatrix}$ and $W = -I_l$ gives

$$\det(M) = \det(-I_l)\det\left(\begin{pmatrix} A & B \end{pmatrix} + C\begin{pmatrix} I_l & O \end{pmatrix}\right) = (-1)^l \det\begin{pmatrix} A+C & B \end{pmatrix}.$$

The result follows since N can be obtained from $\begin{pmatrix} A+C & B \end{pmatrix}$ by $l(k-l)$ column changes. □

Let us introduce the abbreviation

$$R_m(f) := R_{m,q}(f,g),$$

where $g(x) = x^{q^n} - x$ and $f(x) = \sum_{i=0}^{n-1} a_i x^{q^i}$ for some $a_i \in \mathbb{F}_{q^n}$.

Lemma 3.3. $|D_m(f)| = |R_m(f)|$.

Proof. Note that $D_{n-1}(f) = R_{n-1}(f) = (a_{n-1})$, so we may assume $m < n-1$. Let T_k denote the $k \times k$ anti-diagonal matrix whose non-zero entries equal to one and let I_k denote the $k \times k$ identity matrix. By O we will always denote a zero matrix whose dimension will be clear from the context. We distinguish two cases.

If $m \geqslant (n-1)/2$, then $2n-1-2m \leqslant n$ and hence $R_m(f)$ has the form:

$$\begin{pmatrix} A & B \\ I_{n-1-m} & O \end{pmatrix},$$

where $B = T_{n-m} D_m(f) T_{n-m}$. We have

$$\left|\begin{pmatrix} A & B \\ I_{n-1-m} & O \end{pmatrix}\right| = (-1)^{(n-m-1)(n-m)} \left|\begin{pmatrix} B & A \\ O & I_{n-1-m} \end{pmatrix}\right|,$$

and hence by Result 3.1

$$|R_m(f)| = |B| = |D_m(f)|.$$

If $m < (n-1)/2$, then first consider the last m rows of $R_m(f)$: for $k \in \{0, 1, \ldots, m-1\}$ the $(2n-2m-1-k)$-th row of $R_m(f)$ contains only one non-zero entry, namely, a 1 at position $n-1-m-k$. Then it is easy to see by row expansion applied to the last m rows that:

$$(-1)^{(n-1)m} |R_m(f)| = \left|\begin{pmatrix} A & B & C \\ I_{n-2m-1} & O & -I_{n-2m-1} \end{pmatrix}\right|,$$

where A and C are $(n-m) \times (n-2m-1)$ matrices and

$$\begin{pmatrix} B & A + C \end{pmatrix} = T_{n-m} D_m(f) T_{n-m}.$$

According to Corollary 3.2,

$$(-1)^{(n-1)m} |R_m(f)| = (-1)^{(n-2m-1)(m+2)} |T_{n-m} D_m(f) T_{n-m}|,$$

which proves the assertion.

□

Lemma 3.3 immediately yields Theorem 1.3.

For some s with $\gcd(s, n) = 1$ put $\sigma := q^s$. The set of σ-polynomials over $\mathbb{F}_{q^n}$ is isomorphic to the skew-polynomial ring $\mathbb{F}_{q^n}[t, \sigma]$ where $t\alpha = \alpha^\sigma t$ for all $\alpha \in \mathbb{F}_{q^n}$. Analogies for some of the results of Section 2 should hold in these non-commutative polynomial rings as well. Next we show a generalization of Theorem 1.3 for σ-polynomials.

Consider the σ-polynomial $f(x) := \sum_{i=0}^{n-1} a_i x^{\sigma^i} \in \mathbb{F}_{q^n}[x]$, which is also a q-polynomial. As before, by $\ker f$ we will denote $\gcd(f(x), x^{q^n} - x)$ and similarly to $D(f)$ we define

$$D_\sigma(f) := \begin{pmatrix} a_0 & a_1 & \dots & a_{n-1} \\ a_{n-1}^\sigma & a_0^\sigma & \dots & a_{n-2}^\sigma \\ \vdots & \vdots & \vdots & \vdots \\ a_1^{\sigma^{n-1}} & a_2^{\sigma^{n-1}} & \dots & a_0^{\sigma^{n-1}} \end{pmatrix}.$$

We will denote by $D_{m,\sigma}(f)$ the $(n-m) \times (n-m)$ matrix obtained from $D_\sigma(f)$ after removing its first m columns and last m rows. Because of the applications it might be useful to have conditions on other minors of $D_\sigma(f)$. In the next corollary we show some results also in this direction.

Corollary 3.4. *If $f(x) = \sum_{i=0}^{n-1} a_i x^{\sigma^i} \in \mathbb{F}_{q^n}[x]$ with $\gcd(s,n) = 1$, then $\dim_q(\ker f) = \mu$ if and only if*

$$|D_{0,\sigma}(f)| = |D_{1,\sigma}(f)| = \ldots = |D_{\mu-1,\sigma}(f)| = 0 \tag{8}$$

and $|D_{\mu,\sigma}(f)| \neq 0$.

Index the rows and columns of $D_\sigma(f)$ from 0 to $n-1$. For $0 \leqslant m \leqslant \dim_q(\ker f)$ if $J, K \subseteq \{0, 1, \ldots, n-1\}$ are two sets of m consecutive integers modulo n then let $M_{J,K}(f)$ denote the $(n-m) \times (n-m)$ matrix obtained from $D_\sigma(f)$ after removing its rows and columns with indices in J and K, respectively. Then

$$|M_{J,K}(f)| = 0 \Leftrightarrow |D_{m,\sigma}(f)| = 0.$$

Proof. Consider f as a q-polynomial with $\dim_q(\ker f) = \mu$. This happens if and only if $D(f)$ has rank μ. Recall that rows and columns of $D(f)$ are indexed from 0 to $n-1$ and let P denote the permutation matrix for which the i-th row of PA is the si-th row of A (considered modulo n). Then $PAP^{-1} = D_\sigma(f)$ and hence the rank of $D_\sigma(f)$ is the same as the rank of $D(f)$ (cf. also [8, Remark 2.3]). Note that $D_\sigma(f)$ is the Dickson matrix of a σ-polynomial considered as an $\mathbb{F}_\sigma$-linear transformation of $\mathbb{F}_{\sigma^n}$ with kernel a μ-dimensional $\mathbb{F}_\sigma$-subspace of $\mathbb{F}_{\sigma^n}$. By Theorem 1.3 this happens if and only if the conditions on $|D_{m,\sigma}(f)|$ holds for $0 \leqslant m \leqslant \mu$.

For the second part take $0 \leqslant m \leqslant \dim_q(\ker f)$. Note that for any σ-polynomial $g(x) = \sum_{i=0}^{n-1} b_i x^{\sigma^i} \in \mathbb{F}_{q^n}[x]$ and for any non-negative integer t the rank of $g(x)$ is the same as

1. the rank of $g(x)^{\sigma^t}$ considered modulo $x^{q^n} - x$,
2. the rank of $\hat{g}(x) := \sum_{i=0}^{n-1} b_{n-i}^{\sigma^i} x^{\sigma^i}$ (since $D_\sigma(g)^T = D_\sigma(\hat{g})$, where by ^{T} we denote matrix transposition).

Suppose $J = \{j, j+1, \dots, j+m-1\}$ and $K = \{k, k+1, \dots, k+m-1\}$ considered modulo n. Then $f_1(x) := f(x)^{\sigma^{n-k-m}}$ modulo $x^{q^n} - x$ has the same rank as $f(x)$ and $|M_{J,K'}(f_1)| = |M_{J,K}(f)|^{\sigma^{n-k-m}}$ where $K' = \{n-m, m+1, \dots, n-1\}$. Then $\hat{f}_1(x)$ has the same rank as $f_1(x)$ and $|M_{K',J}(\hat{f}_1)| = |M_{J,K'}(f_1)|$. Finally, $f_2(x) := \hat{f}_1(x)^{\sigma^{n-j}}$ modulo $x^{q^n} - x$ has the same rank as $\hat{f}_1(x)$ and $|M_{K',J'}(f_2)| = |M_{K',J}(\hat{f}_1)|^{\sigma^{n-j}}$ where $J' = \{0, 1, \dots, m-1\}$. By definition $M_{K',J'}(f_2) = D_{m,\sigma}(f_2)$, and hence

$$|D_{m,\sigma}(f_2)| = 0 \Leftrightarrow |M_{K',J}(\hat{f}_1)| = 0 \Leftrightarrow |M_{J,K'}(f_1)| = 0 \Leftrightarrow |M_{J,K}(f)| = 0.$$

Recall $0 \leqslant m \leqslant \dim_q(\ker f)$. Since f_2 and f has the same rank, it follows from the first part of the assertion that $|D_{m,\sigma}(f_2)| = 0 \Leftrightarrow |D_{m,\sigma}(f)| = 0$ and this finishes the proof. □

3.1 Applications

A q-polynomial $f(x) \in \mathbb{F}_{q^n}[x]$ is called *scattered* if $\{f(x)/x \colon x \in \mathbb{F}_{q^n} \setminus \{0\}\}$ (the *set of directions determined by the graph of* f) has maximum size, that is $(q^n-1)/(q-1)$. Put $U_f = \{(x, f(x)) \colon x \in \mathbb{F}_{q^n}\}$, which is an n-dimensional $\mathbb{F}_q$-subspace of $\mathbb{F}_{q^n}^2$. The *linear set* of $\mathrm{PG}(1, q^n)$ defined by f is the set of projective points $L_f := \{\langle (x, f(x)) \rangle_{q^n} \colon x \in \mathbb{F}_{q^n} \setminus \{0\}\}$. The *weight* of a point $\langle (a,b) \rangle_{\mathbb{F}_{q^n}} \in \mathrm{PG}(1, q^n)$ w.r.t. the $\mathbb{F}_q$-subspace U_f is $\dim_q \langle (a,b) \rangle_{\mathbb{F}_{q^n}} \cap U_f$. The polynomial f is scattered if and only if the points of L_f have weight 1. In this case L_f and U_f are called *maximum scattered*. This happens if and only if the $\mathbb{F}_q$-linear transformations of $\mathbb{F}_{q^n}$ in the $\mathbb{F}_{q^n}$-subspace $M := \langle x, f(x) \rangle_{\mathbb{F}_{q^n}}$ have rank at least $n-1$. Equivalently, M is equivalent to an $\mathbb{F}_{q^n}$-linear maximum rank distance (MRD for short) code of $\mathbb{F}_q^{n \times n}$ with minimum distance $n-1$. For more details about these objects and the relations among them we refer to [16, Section 13.3.6] and the references therein.

Corollary 3.5. *Consider the q-polynomial* $f(x) = \sum_{i=0}^{n-1} a_i x^{q^i} \in \mathbb{F}_{q^n}[x]$ *and with* y *as a variable consider the matrix*

$$H := \begin{pmatrix} y & a_1 & \dots & a_{n-1} \\ a_{n-1}^q & y^q & \dots & a_{n-2}^q \\ \vdots & \vdots & \vdots & \vdots \\ a_1^{q^{n-1}} & a_2^{q^{n-1}} & \dots & y^{q^{n-1}} \end{pmatrix}.$$

The determinant of the $(n-m) \times (n-m)$ matrix obtained from H after removing its first m columns and last m rows is a polynomial $H_m(y) \in \mathbb{F}_{q^n}[y]$. Then the following holds:

1. *The roots of $H_0(y)$ are in $\mathbb{F}_{q^n}$,*
2. *the number of points of weight μ of L_f w.r.t. U_f is the same as the number of common roots of $H_0(y), H_1(y), \dots, H_{\mu-1}(y)$ which are not roots of $H_\mu(y)$,*
3. *in particular $f(x)$ is scattered if and only if $H_0(y)$ and $H_1(y)$ have no common roots.*

Proof. Let y_0 be a root of $H_0(y)$. Note that Lemma 3.3 does not require the coefficients of f to be in $\mathbb{F}_{q^n}$, thus also for $y_0 \in \overline{\mathbb{F}}_q$ we have $0 = H_0(y_0) = |R_{0,q}(y_0 x + \sum_{i=1}^{n-1} a_i x^{q^i}, x^{q^n} - x)|$ and hence by Theorem 2.1 there exists $x_0 \in \mathbb{F}_{q^n} \backslash \{0\}$ such that $y_0 = -\sum_{i=1}^{n-1} a_i x_0^{q^i - 1}$. Here the right-hand side is in $\mathbb{F}_{q^n}$ and hence $y_0 \in \mathbb{F}_{q^n}$.

By Theorem 1.3 $H_0(y_0) = H_1(y_0) = \ldots = H_{\mu-1}(y_0) = 0$ and $H_\mu(y_0) \neq 0$ hold if and only if the q-polynomial $(y_0 - a_0)x + f(x) \in \mathbb{F}_{q^n}[x]$ has nullity μ, equivalently, the point $\langle (1, a_0 - y_0) \rangle_{q^n}$ has weight μ.

The last part follows from the fact that f is scattered if and only if L_f does not have points of weight larger than 1. $\square$

In [2] Part 3. of Corollary 3.5 is used to derive sufficient and necessary conditions for $f(x) = bx^q + x^{q^4} \in \mathbb{F}_{q^6}[x]$ to be a scattered polynomial and to prove [6, Conjecture 7.5] regarding the number of scattered polynomials of this form.

In [4] the authors study MRD-codes with maximum idealisers, or equivalently, the problem of finding sets of distinct integers $\{t_0, t_1, \dots, t_k\}$ such that every $\mathbb{F}_q$-linear transformation of $\mathbb{F}_{q^n}$ in the $\mathbb{F}_{q^n}$-subspace $\langle x^{q^{t_0}}, x^{q^{t_1}}, \dots, x^{q^{t_k}} \rangle_{\mathbb{F}_{q^n}}$ has rank at least $n-k$. In [4, Corollary 3.6] it is stated that in $M := \langle x, x^q, x^{q^2}, x^{q^4} \rangle_{\mathbb{F}_{q^9}}$ one can find an $\mathbb{F}_q$-linear transformation of $\mathbb{F}_{q^9}$ with rank at most 5 and hence the set of integers $\{0, 1, 2, 4\}$ does not satisfy the above mentioned condition. In [4] this was proved by calculating sixteen 6×6 submatrices of $D(f)$, where $f(x) = -x + (1 + c^{-q})x^q + cx^{q^2} - x^{q^4}$ and $c \in \mathbb{F}_{q^9}$ satisfies certain conditions, and by proving that each of them has zero determinant. According to Theorem 1.3 the same result follows also by calculating only $|D_0(f)|$, $|D_1(f)|$, $|D_2(f)|$, $|D_3(f)|$ and by proving that all of them are zero.

Acknowledgement

The author is thankful to Tamás Héger from whom he learned Result 1.1 and its proof, which was adapted to prove Theorem 2.1.

References

[1] C. D'Andrea, T. Krick, A. Szanto: Multivariate subresultants in roots, J. Algebra 302 (2006), 16–36.

[2] D. Bartoli, B. Csajbók, M. Montanucci: On a conjecture about maximum scattered subspaces of $\mathbb{F}_{q^6} \times \mathbb{F}_{q^6}$, manuscript.

[3] R.A. Brualdi, H. Schneider: Determinantal identities: Gauss, Schur, Cauchy, Sylvester, Kronecker, Jacobi, Binet, Laplace, Muir, and Cayley. Linear Algebra Appl. 52/53 (1983), 769–791.

[4] B. Csajbók, G. Marino, O. Polverino, Y. Zhou:. Maximum rank-distance codes with maximum left and right idealisers. Submitted manuscipt. https://arxiv.org/abs/1807.08774

[5] B. Csajbók, G. Marino, O. Polverino, F. Zullo: A characterization of linearized polynomials with maximum kernel. Finite Fields Appl. 56 (2019), 109–130.

[6] B. Csajbók, G. Marino, O. Polverino, C. Zanella: A new family of MRD-codes. Linear Algebra Appl. 548 (2018), 203–220.

[7] B. Csajbók, G. Marino, F. Zullo: New maximum scattered linear sets of the projective line, Finite Fields Appl. 54 (2018), 133–150.

[8] B. Csajbók, A. Siciliano: Puncturing maximum rank distance codes, J. Algebraic Combin. 49 (2019), 507-534.

[9] J. von zur Gathen, T. Lucking: Subresultants revisited, Theoretical Computer Science 297 (2003), 199–239.

[10] T. Héger: Some graph theoretic aspects of finite geometries, PhD Thesis, Eötvös Loránd University (2013) Available online at `http://web.cs.elte.hu/~hetamas/publ/HTdiss-e.pdf`

[11] Z. Li: A Subresultant Theory for Ore Polynomials with Applications, in: Proceedings of the 1998 International Symposium on Symbolic and Algebraic Computation, pages 132–139, ACM Press, 1998.

[12] G. McGuire, J. Sheekey: A Characterization of the number of roots of linearized and projective polynomials in the field of coefficients. Finite Fields Appl. 57 (2019), 68–91.

[13] G. Menichetti: Roots of affine polynomials, in: Combinatorics '84, Ann. Discrete Math. 30 (1986), 303–310.

[14] O. Ore: On a special class of polynomials, Trans. Amer. Math. Soc. 35(3) (1933), 559–584.

[15] O. Ore: Theory of Non-Commutative Polynomials, Annals of Mathematics, Second Series, Vol 34., No. 3 (Jul. 1933), pp. 480–508.

[16] J. Sheekey: MRD Codes: Constructions and Connections, in: Combinatorics and Finite Fields: Difference Sets, Polynomials, Pseudorandomness and Applications Ed. by Schmidt, Kai-Uwe and Winterhof, Arne, Series: Radon Series on Computational and Applied Mathematics 23, De Gruyter 2019.

[17] D.S. Thakur: Function field arithmetic, World Scientific Publishing, River Edge, NJ, 2004.

[18] B. Wu, Z. Liu: Linearized polynomials over finite fields revisited, Finite Fields Appl. 22 (2013), 79–100.

Bence Csajbók
MTA–ELTE Geometric and Algebraic Combinatorics Research Group
ELTE Eötvös Loránd University, Budapest, Hungary
Department of Geometry
1117 Budapest, Pázmány P. stny. 1/C, Hungary
csajbokb@cs.elte.hu