Contemporary Mathematics

On the characterization of a semi-multiplicative analogue of planar functions over finite fields

A. Muratović-Ribić, A. Pott, D. Thomson and Q. Wang

Abstract. In this paper, we present a characterization of a semi-multiplicative analogue of planar functions over finite fields. When the field is a prime field, these functions are equivalent to a variant of a doubly-periodic Costas array and so we call these functions Costas. We prove an equivalent conjecture of Golomb and Moreno that any Costas polynomial over a prime field is a monomial. Moreover, we give a class of Costas polynomials over extension fields and conjecture that this class represents all Costas polynomials. This conjecture is equivalent to the conjecture that there are no non-Desarguesian planes of a given type with prime power order.

1. Introduction

A *Costas array* of order n is a $n \times n$ permutation array (with exactly one dot in every row and column and blanks elsewhere) such that every vector connecting two dots are distinct. The Costas property ensures that the array has ideal auto-correlation, which makes Costas arrays highly desired for use in RADAR and SONAR communications.

Suppose f is a permutation defining a Costas array of order n. Let (w, h) be a vector joining any two dots in the array, then $h = f(x + w) - f(x)$ for some $x = 0, 1, \ldots, n - 1 - w$. In this paper, we study properties of arrays generated by functions f with finite domain or codomain (or both). More generally, let G_1 and G_2 be finite Abelian groups (written additively) and let $f\colon G_1 \to G_2$. The map $\Delta_{f,d}(x) = f(x + d) - f(x)$ is the *difference map* of f with parameter d. Since the map $\Delta_{f,0}$ is trivial, we consider only difference maps where d is the non-identity element of G_1.

Difference maps are related to *difference sets* and functions whose difference maps have special properties have applications in many areas such as symmetric-key cryptography and projective geometry. If $G_1 = G_2 = \mathbb{F}_q$ and $\Delta_{f,d}$ is a *permutation polynomial* for all $d \in G_1 \setminus \{0\}$ (that is, the difference maps are all injective), then f is a *planar function*. It is easy to see that planar permutations cannot exist and planar functions never exist over groups of even order, although there has been recent work on a new sort of function which is "planar" in the geometric sense over characteristic 2 [**23**].

In Section 2, we further investigate periodicity properties of Costas arrays, which provides the background and motivation for studying Costas polynomials over finite fields. In Section 3, we present a proof of a conjecture of Golomb and Moreno [**9**], which characterizes Costas polynomials over finite fields of prime order. Our proof is based on the equivalence of direct-product difference sets to projective planes of a certain type. Section 4 deals with Costas polynomials over finite extension fields. We show that certain types of Costas polynomials are closed under composition and conjecture that this class provides all known Costas polynomials. This conjecture is equivalent to the non-existence of non-Desarguesian planes of a certain type.

2. Periodicity properties of Costas arrays

Let $\mathbb{Z}_{\geq 0}$ denote the non-negative integers and $\mathbb{Z}_m$ the ring of integers modulo a positive integer m. We view a Costas array as a map $f\colon \mathbb{Z}_{\geq 0} \to \mathbb{Z}_{\geq 0}$ by placing $f(x) = y$ whenever there is a dot in the (x, y) position, $0 \leq x \leq n-1$. Moreover, since the x-coordinate is understood, we consider only the sequence of images of f: if $f(i) = y_i$ for any i, the sequence is given by $(y_0, y_1, \ldots, y_{n-1})$.

If a sequence has the property that

$$y_{i+k} - y_i = y_{j+k} - y_j \text{ implies } i = j \text{ or } k = 0 \text{ for all } i, j, k \text{ such that } 0 \leq i + k, j + k \leq n - 1,$$

then the sequence is a *Costas sequence*. A common tool to determine if a given sequence is Costas is the *difference triangle*. Suppose $\mathbf{y} = (y_0, y_1, \ldots, y_{n-1})$ is a given sequence. For $1 \leq k \leq n-1$, the k-th row of the difference triangle of $\mathbf{y}$ is the sequence $y_{i+k} - y_i$, where $0 \leq i \leq n-k-1$. Thus, $\mathbf{y}$ is a Costas sequence if every row in the difference triangle has distinct entries. The *difference square* can be found by computing the difference $y_{i+k} - y_i$, where $0 \leq i \leq n-1$ and the indices are taken modulo n.

When considering periodicity properties of Costas sequences, it is natural to consider the following scenarios.

DEFINITION 2.1.
(1) *Consider a function $f\colon \mathbb{Z}_{\geq 0} \to \mathbb{Z}_m$; that is, the values of the sequence (hence, the entries of the difference triangle) are taken modulo a positive integer m. The resulting sequence is* range-periodic. *If the rows of the difference triangle with entries modulo m are distinct, the sequence is* range-periodic Costas.
(2) *Consider a function $f\colon \mathbb{Z}_n \to \mathbb{Z}$; that is, the inputs of the sequence are taken modulo a positive integer n. The resulting sequence is* domain-periodic. *If the rows of the difference square have distinct entries, the sequence is* domain-periodic Costas.
(3) *A sequence which is domain periodic Costas modulo m and range-periodic Costas modulo $m+1$ is a* circular *Costas sequence.*

EXAMPLE 1. *Consider the sequence* $\{3,2,6,4,5,1\}$. *The corresponding* 6×6 *array is*

(1)

3	2	6	4	5	1
					○
	○				
○					
			○		
				○	
		○			

.

Rather than attempt to construct all of the vectors, we construct the difference triangle of the array.

As integers:

3	2	6	4	5	1
	1	−4	2	−1	4
		−3	−2	1	3
			−1	−3	5
				−2	1
					2

Since the entries in each row are distinct, the sequence is Costas.

Modulo 7*:*

3	2	6	4	5	1
	1	3	2	6	4
		4	5	1	3
			6	4	5
				5	1
					2

Since the entries in each row are distinct modulo 7*, the sequence is range-periodic Costas.*

To determine domain-periodicity, we consider instead the difference square.

As integers:

3	2	6	4	5	1
−2	1	−4	2	−1	4
2	−1	−3	−2	1	3
1	3	−5	−1	−3	5
3	2	−1	−3	−2	1
−1	4	−2	1	−4	2

Since the entries in each row are distinct, the sequence is domain-periodic Costas modulo 6*.*

Modulo 7*:*

3	2	6	4	5	1
5	1	3	2	6	4
2	6	4	5	1	3
1	3	2	6	4	5
3	2	6	4	5	1
6	4	5	1	3	2

Since the entries in each row are distinct, the sequence is circular (with $m=6$*).*

A circular Costas sequence can be realized as a Costas array augmented with a blank row at the top or bottom. The extra row arises from the additional element in the codomain. The augmented array from Example 1 becomes

(2)

3	2	6	4	5	1
					○
	○				
○					
			○		
				○	
		○			

,

and since all the rows of the difference square (mod 7) have distinct entries, the array has the circular Costas property. Moreover, it can be shown, see for example [**15**], that it is impossible to have a square Costas array which is both domain- and range-periodic modulo the same value. Thus, (2) is, in some sense, an example of the smallest type of array of width 6 containing all non-trivial displacement vectors.

The sequence given in Example 1 is derived by one of the main constructions of Costas arrays, known as the *exponential Welch construction*.

THEOREM 2.2. *Let p be a prime and let α be a primitive element of $\mathbb{F}_p$; that is, α generates the multiplicative group $\mathbb{F}_p^*$. Define the map $f(x) = \alpha^x$, for $x = 0, 1, \ldots, p-2$. The resulting sequence of values $(y_0, y_1, \ldots, y_{p-2})$ is Costas; moreover, $\alpha^e(y_0, y_1, \ldots, y_{p-2})$ is the cyclic shift of the values of the sequence right by e positions and the resulting sequence is still Costas.*

The exponential Welch construction yields a sequence that is domain-periodic modulo $p-1$, since $\alpha^{p-1} = 1$, and range-periodic modulo p, since the entries are elements of $\mathbb{F}_p$. Hence, exponential Welch sequences are circular Costas. In [**9**] the authors conjectured that the exponential Welch construction of Theorem 2.2 yields the only circular Costas sequences.

CONJECTURE 2.3. [**9**] *A sequence is circular Costas if and only if it is exponential Welch.*

As far as we know, this conjecture is considered to be unsolved. Indeed, in private correspondence with the authors of [**9**], they indicated that they were not previously aware of a solution to this problem. Several steps towards this conjecture were previously known. It is easy to show that $m+1$ is odd, while it was shown in [**8**] that $m+1$ is necessarily prime.

We now view any circular Costas sequence $(y_0, y_1, \ldots, y_{p-2})$ as a map from $\mathbb{F}_p^* \to \mathbb{F}_p$, with p an odd prime. Construct the function g by placing $g(\alpha^i) = y_i$, where α is a primitive element of $\mathbb{F}_p$. Since y_i is a Costas sequence, the set of values $y_{i+k} - y_i$ are distinct for all $i, k \neq 0$, hence $g(\alpha^{i+k}) - g(\alpha^i) = g(\alpha^i\alpha^k) - g(\alpha^i)$ permutes the elements of $\mathbb{F}_p^*$. By defining $g(0)$, g can be described as a polynomial of degree at most $p-1$ modulo $x^p - x$, by Lagrange interpolation. If $g(0) = 0$, then g is a permutation of $\mathbb{F}_p$. Moreover, labeling $\alpha^k = d$ gives that $g(xd) - g(x)$ is a permutation polynomial of $\mathbb{F}_p$. If the sequence is exponential Welch, then $y_i = \beta^i$ for some primitive element β. Thus $y_i = \alpha^{is}$, where $\beta = \alpha^s$ with $\gcd(s, p-1) = 1$. Polynomials defining circular Costas sequences yield semi-multiplicative analogues of planar function, where the domain is the multiplicative group of a finite field and the codomain is the corresponding additive group. Due to their importance throughout this work, we give a special name to functions which satisfy the circular Costas property.

DEFINITION 2.4. *Suppose $f \in \mathbb{F}_q[x]$ such that $f(0) = 0$ and $f(xd) - f(x)$ is a permutation for all $d \in \mathbb{F}_q$, $d \neq 1$. Then f is a* Costas polynomial.

While we have defined Costas polynomials over any finite field, we emphasize that they are equivalent to circular Costas sequences only over prime fields. In view of the preceding discussion, in the next section we prove an equivalent conjecture, also due to [**9**], on Costas polynomials over prime fields.

In the next section we restrict our attention to prime fields and prove Conjecture 2.3.

3. Costas polynomials and direct product difference sets

In this section, we present a proof of Conjecture 2.3 in the following equivalent form.

CONJECTURE 3.1. *If $f \in \mathbb{F}_p[x]$ be a monic Costas polynomial, then $f(x) = x^s$ for some integer s satisfying* $\gcd(s, p-1) = 1$.

The key to our proof is a connection between Costas polynomials and the following well-studied object.

DEFINITION 3.2. *Let G be a finite group, $|G| = n^2 - n$ and let $G = H \times E$, where $|E| = n = |H| + 1$, E is written additively and H is written multiplicatively.. A subset R of G with the property that the non-identity quotients of R consist of every element of $G \setminus \{(H,0),(1,E)\}$ exactly once and no element of $(H,0)$ or $(1,E)$ appears as a quotient is a* direct product difference set.

Two direct product difference sets R_1 and R_2 are *equivalent* if there is a pair $(a,b) \in H \times E$ and a group automorphism $\psi \in \mathrm{Aut}(H \times E)$, say $\psi = (\psi_H, \psi_E)$, such that $R_2 = (a,b) \cdot \psi(R_1)$.

Let n be a positive integer and let E and H be groups such that $|E| = n = |H| + 1$. Obviously, any injective function $f\colon H \to E$ with the property

(3) $xy^{-1} = x'y'^{-1} \neq 1$ and $f(x) - f(y) = f(x') - f(y')$ implies $x = x'$ and $y = y'$

yields a direct product difference set $R = \{(x, f(x))\colon x \in H\} \subseteq H \times E$ and, conversely, a direct product difference set in $H \times E$ gives rise to a function satisfying (3). This is true since E and H are finite groups, and (3) says that every element in $H \times E$ has at most one "difference representation" with elements from R. The function f is said to be *associated* to R, and we denote such a direct product difference set R_f.

LEMMA 3.3. *Let q be a prime power and let $G = \mathbb{F}_q^* \times \mathbb{F}_q$. A polynomial $f \in \mathbb{F}_q[x]$ is a Costas polynomial if and only if $R_f = \{(x, f(x))\colon x \in \mathbb{F}_q^*\}$ is a direct product difference set of G.*

PROOF. Let R be a direct product difference set of G. From the definition, any $x \in \mathbb{F}_q^*$ occurs exactly once as the first coordinate of a pair of R. Now construct a map $f\colon \mathbb{F}_q^* \to \mathbb{F}_q$ by setting $y = f(x)$ whenever $(x,y) \in R := R_f$. The "quotient" of (x,y) and (x',y') from G is $(x/x', y - y')$. The subgroup $1 \times E = \{(1,y)\colon y \in \mathbb{F}_q\}$ is avoided by distinct x, x', so suppose $x/x' = d^{-1} \neq 1$. To avoid $H \times 0 = \{(x,0)\colon x \in \mathbb{F}_q^*\}$, the difference $y - y' = f(x) - f(x') = f(x) - f(xd) \neq 0$ for any $d \neq 1$; that is, $f(xd) - f(x)$ is an injection for all $d \neq 1$. Moreover, if $x/x' = d^{-1} \neq 1$, then since R_f is a direct product difference set, $f(x) - f(xd)$ must map to every element of $\mathbb{F}_q$ except for 0. By defining $f(0) = 0$, we get that any direct product difference set of $G = \mathbb{F}_q^* \times \mathbb{F}_q$ yields a Costas polynomial. The reverse conclusion is immediate. □

We now prove Conjecture 3.1. Our proof is based on the characterization of desarguesian planes which can be described by direct product difference sets. We rely on several results from [**21**, Section 5.3] concerning projective planes with quasiregular collineation groups.

THEOREM 3.4. *If $f \in \mathbb{F}_p[x]$ be a monic Costas polynomial, then $f(x) = x^s$ for some integer s satisfying $(s, p-1) = 1$.*

PROOF. Suppose f is a Costas polynomial. By Lemma 3.3, the set $R_f = \{(x, f(x)) \colon x \in \mathbb{F}_p^*\}$ is a direct product difference set in $G = \mathbb{F}_p^* \times \mathbb{F}_p$. By [**21**, Proposition 5.3.1], G must act as a quasiregular collineation group on a certain type of projective plane of order p, and [**21**, Corollary 5.3.6] then shows that this plane is Desarguesian. Thus, by [**21**, Theorem 5.3.4], and by the definition of equivalence of direct product difference sets, f must act as an automorphism of the multiplicative group of $\mathbb{F}_p$. Hence, $f(x) = x^s$ with $\gcd(s, p-1) = 1$. □

4. Costas polynomials in extension fields

In the previous section, we considered Costas polynomials over prime fields due to their connections to Costas arrays. For a general function $f \colon \mathbb{F}_q \to \mathbb{F}_q$, with q a non-trivial power of p, there is no obvious way to construct Costas arrays from the images of f since the codomain is not cyclic. It is easy to see that monomial permutation polynomials over any finite field define Costas polynomials, so a natural question is whether these define all Costas polynomials.

Let $q = p^e$ with $e \geq 1$ and let $L(x) = \sum_{i=0}^{e-1} a_i x^{p^i}$ be a *linearized polynomial*. Linearized polynomials define linear operators over finite fields and as a corollary define permutations if and only if they have a trivial kernel. Suppose that L is a linearized permutation polynomial and let $d \in \mathbb{F}_q^*, d \neq 1$. Then $L(xd) - L(x) = L(x(d-1)) = L(x) \circ ((d-1)x)$, which is a composition of permutations and hence a permutation. Thus, linearized permutation polynomials also define Costas polynomials. More generally, we have the following result.

THEOREM 4.1. *Let f be a linearized permutation polynomial (hence f is a linearized Costas polynomial) and let g be any Costas polynomial, then $f \circ g$ is also Costas.*

PROOF. Since g is a Costas polynomial, the set $R_g = \{(x, g(x)) \colon x \in \mathbb{F}_q^*\} \subseteq \mathbb{F}_q^* \times \mathbb{F}_q$ is a direct product difference set. If R' is direct product difference set which is equivalent to R_g, then $R' = (a, b) \cdot \psi(R_g)$, where $(a, b) \in \mathbb{F}_q^* \times \mathbb{F}_q$ and $\psi = (\psi_{(\mathbb{F}_q^*)}, \psi_{(\mathbb{F}_q)})$ is an automorphism of $\mathbb{F}_q^* \times \mathbb{F}_q$. Thus, $\psi_{(\mathbb{F}_q)}$ can be realized as a linearized permutation polynomial f. Finally, if $(a, b) = (1, 0)$ and $\psi_{(\mathbb{F}_q^*)} = \mathrm{id}_{(\mathbb{F}_q^*)}$, then $R' = \{(x, (f \circ g)(x)) \colon x \in \mathbb{F}_q^*\}$ and $f \circ g$ is Costas. □

We use Theorem 4.1, along with the known fact that permutation monomials are Costas, in order to generalize the monomial construction of Costas polynomials in prime fields to a larger class of Costas polynomials over extension fields.

COROLLARY 4.2. *Let $q = p^e$ with $e \geq 1$ and let $f \in \mathbb{F}_q[x]$. The polynomial $f = \sum_{i=0}^{e-1} a_i x^{sp^i}$ is a Costas polynomial if $\sum_{i=0}^{e-1} a_i x^{p^i}$ is a permutation polynomial and $\gcd(s, q-1) = 1$.*

Although we have presented classes of Costas polynomials, the problem of characterizing Costas polynomials is still open when $\mathbb{F}_q$ is a non-trivial extension field. We have seen that a Costas polynomial over a finite field is precisely the construction required to form a direct product difference set $R_f = \{(x, f(x)) \subseteq \mathbb{F}_q^* \times \mathbb{F}_q\}$. The existence of such a direct product difference set implies that $\mathbb{F}_q^* \times \mathbb{F}_q$ acts on a certain type of projective plane of order q. A natural question is to

ask if there are other groups admitting a direct product difference set. However, the prime power conjecture for projective planes acted upon by a quasiregular collineation group was established by Jungnickel and de Resmini.

THEOREM 4.3. [**12**] *Let G be an Abelian collineation group of order $n(n-1)$ of a projective plane of order n. Then n must be a power of a prime p and the p-part of G is elementary Abelian.*

Since direct product difference sets, and hence Costas maps, cannot exist for non-prime power values of n, we restrict our attention to $G = H \times (\mathbb{F}_q, +)$, and in particular $H = \mathbb{F}_q^*$. Moreover, Corollar 4.2 and results in [**12**] motivate our final conjecture.

CONJECTURE 4.4. *All Costas polynomials over $\mathbb{F}_q$ are of the form given in Corollary 4.2.*

We note that we can construct direct product difference sets algebraically through these Costas polynomials obtained in Corollary 4.2. Costas polynomials can also be used to define complete mappings. Complete mappings were introduced in [**17**] by Mann to study the problem of constructing orthogonal Latin squares. Complete mappings of $\mathbb{F}_q$ are permutations $f \in \mathbb{F}_q[x]$ such that $f(x) + x$ is also a permutation of $\mathbb{F}_q$. Motivated by an earlier study of non-simple Bol loops of order pr, with $p > r$ both odd primes which can be characterized by pairs of complete mappings of $\mathbb{F}_p$ [**18**], these complete mappings of $\mathbb{F}_q$ were studied by Niederreiter and Robinson in [**19**]. This raises the problem of finding interesting classes of complete mappings of finite fields.

PROPOSITION 4.5. *Let $f \in \mathbb{F}_q[x]$ be a Costas polynomial, then $f(df^{-1}(x)) - x$ is a complete mapping for all $d \in \mathbb{F}_q \setminus \{0, 1\}$.*

PROOF. Let $g(x) = f(df^{-1}(x)) - x$ and re-label $f^{-1}(x) = y$. It is clear that $g(x) + x$ is a permutation. Moreover, $g(x) = f(dy) - f(y)$ is a permutation for all $d \in \mathbb{F}_q \setminus \{0, 1\}$. □

We conclude the article with a note on how Costas polynomials are related to a modular (doubly-periodic) version of the n-queens problem, which is the place n non-attacking queens on an $n \times n$ board. A survey on the n-queens problem can be found [**1**]. Contrary to the Costas case, it can be shown, for example in [**1**, Page 16], that the exponential-Welch construction does not yield a solution to the modular p-queens problem. More generally, h is a solution to the modular n-queens problem if and only if both h and $-h$ are complete mappings (mod n).

Extrapolating the n-queens problem over finite fields, it would be interesting to find some ds such that $f(df^{-1}(x)) - 2x$ is also a permutation. If we can find such d's, then both $f(df^{-1}(x)) - x$ and $-(f(df^{-1}(x)) - x)$ are complete mappings and solve an $\mathbb{F}_q$ analogue of the n-queens problem.

Acknowledgement. We would like to thank an anonymous referee for their insightful suggestions which greatly improved the delivery of these results.

References

[1] J. Bell and B. Stevens, A survey of known results and research areas for n-queens, *Discrete Mathematics* **309** (2009) 1–31.

[2] R. S. Coulter, The classification of planar monomials over fields of prime square order, *Proceedings of the American Mathematical Society* **134** (2006), 3373–3378.

[3] P. Dembowski and F. Piper, Quasiregular collineation groups of finite projective planes, *Mathematische Zeitschrift* **99** (1967), 53–75.
[4] K. Drakakis, R. Gow and L. O'Carroll, On the symmetry of Welch- and Golomb-constructed Costas arrays, *Discrete Mathematics* **309**, (2009) 2559–2563.
[5] T. Etzion, S. W. Golomb and H. Taylor, Tuscan-K squares, *Advances in Applied Mathematics* **10** (1989), 164–174.
[6] D. Gluck, Affine planes and permutation polynomials, *Coding Theory and Design Theory, part II (Design Theory)*, The IMA Volumes in Mathematics and its Applications, Springer-Verlag **21** (1990), 99-100.
[7] S. Golomb, Algebraic constructions for Costas arrays, *Journal of Combinatorial Theory, Series A* **37** (1984), 13–21.
[8] S. W. Golomb, T. Etzion and H. Taylor, Polygonal path constructions for Tuscan-k squares, *Ars Combinatoria* **30** (1990), 97–140.
[9] S. Golomb and O. Moreno, On periodicity properties of Costas arrays and a conjecture on permutation polynomials. *IEEE Transactions on Information Theory* **42** (1996), 2252–2253.
[10] Y. Hiramine, A conjecture of affine planes of prime order, *Journal of Combinatorial Theory Series A* **52** (1989), 44–50.
[11] N. L. Johnson, Projective planes of order p that admit collineation groups of order p^2, *Journal of Geometry* **30** (1987), 49–68.
[12] D. Jungnickel and M. J. de Resmini, Another case of the prime power conjecture for finite projective planes, *Advances in Geometry* **2** (2002), 215–218.
[13] C. W. H. Lam, The search for a finite projective plane of order 10, *American Mathematical Monthly* **98**, 305–318.
[14] R. Lidl and H. Niederreiter, Finite Fields (2nd ed.), Cambridge University Press, Cambridge UK, (1997).
[15] J. Jedwab and J. Wodlinger, Costas arrays I. Toroidal vectors, *preprint* (2013).
[16] J. B. Kelly, A characteristic property of quadratic residues, *Proceedings of the American Mathematical Society* **5** (1954), 38–46.
[17] H. B. Mann, The construction of orthogonal latin squares, *Annals of Mathematical Statistics* **13** (1942), 418–423.
[18] H. Niederreiter and K. H. Robinson, Bol loops of order pq, *Mathematical Proceedings of the Cambridge Philosophical Society* **89** (1981), 241–256
[19] H. Niederreiter and K. H. Robinson, Complete mappings of finite fields, *Journal of Australian Mathematical Society (Series A)* **33** (1982), 197–212.
[20] D. Panario, A. Sakzad, B. Stevens and Q. Wang, Two new measures for permutations: ambiguity and deficiency, *IEEE Transactions on Information Theory* **57**, (2011) 7648–7657.
[21] A. Pott, Chapter 5: Projective planes with quasiregular collineation groups, Finite Geometry and Character Theory, Springer, Berlin, 1995.
[22] D. Roy, Confirmation of the non-existence of a projective plane of order 10, MSc thesis, Carleton University (2011), 226 pages.
[23] K.-U. Schmidt and Y. Zhou, Planar functions over fields of characteristic two, *Journal of Algebraic Combinatorics*, to appear (2014).

(Amela Muratović-Ribić) University of Sarajevo, Department of Mathematics, Zmaja od Bosne 33-35, 71000 Sarajevo, Bosnia and Herzegovina, amela@pmf.unsa.ba

(Alexander Pott) Otto-von-Guericke-Universität, Fakultät für Mathematik, Institut für Algebra und Geometrie, Postfach 4120, 39016 Magdeburg, Germany, alexander.pott@ovgu.de

(David Thomson) School of Mathematics and Statistics, Carleton University, Ottawa, ON K1S 5B6, Canada, dthomson@math.carleton.ca

(Qiang Wang) School of Mathematics and Statistics, Carleton University, Ottawa, ON K1S 5B6, Canada, wang@math.carleton.ca