

CHARACTERISTIC FREE DESCRIPTION OF SEMI-INVARIANTS OF 2×2 MATRICES

M. DOMOKOS

ABSTRACT. A minimal homogeneous generating system of the algebra of semi-invariants of tuples of two-by-two matrices over an infinite field of characteristic two or over the ring of integers is given. In an alternative interpretation this yields a minimal system of homogeneous generators for the vector invariants of the special orthogonal group of degree four over a field of characteristic two or over the ring of integers. An irredundant separating system of semi-invariants of tuples two-by-two matrices is also determined, it turns out to be independent of the characteristic.

1. INTRODUCTION

For positive integers n, m denote by $M := (\mathbb{F}^{n \times n})^m$ the space of m -tuples of $n \times n$ matrices over an infinite field \mathbb{F} . The group $SL_n \times SL_n$ (the direct product of two copies of the special linear group over \mathbb{F}) acts on this space as follows:

$$(g, h) \cdot (A_1, \dots, A_m) := (gA_1h^{-1}, \dots, gA_mh^{-1})$$

for $g, h \in SL_n, A_1, \dots, A_m \in \mathbb{F}^{n \times n}$. Write $R = \mathcal{O}(M)^{SL_n \times SL_n}$ for the corresponding *algebra of polynomial invariants*; that is, R consists of the polynomial functions on M that are constant along the $SL_n \times SL_n$ -orbits. We call R the *algebra of semi-invariants of m -tuples of $n \times n$ matrices* (and sometimes we shall denote it by $R_{\mathbb{F}}$, when the indication of the base field seems desirable). Interest in this algebra was raised recently by connections to algebraic complexity theory, see for example [18], [21], [22]. Another motivation comes from representation theory of quivers: semi-invariants of tuples of matrices are special instances of semi-invariants associated to representation spaces of quivers, which are used to construct moduli spaces parametrizing quiver representations, see [25].

\mathbb{F} -vector space spanning sets of R were given independently by Derksen and Weyman [7], Domokos and Zubkov [14], and in characteristic zero by Schofield and Van den Bergh [30] (these papers deal with the more general setup of semi-invariants of quiver representations). To deduce a finite \mathbb{F} -algebra generating set of R one needs an explicit degree bound for the generators. Good degree bounds were given recently by Derksen and Makam [4], [5]. These results imply that the \mathbb{Z} -form $R_{\mathbb{Z}}$ of R (see Section 5) is generated as a ring by an explicitly given finite set of elements (see Theorem 5.4), moreover, generators of $R_{\mathbb{Z}}$ yield generators in $R_{\mathbb{F}}$ by base change (see Proposition 5.1). This raises the question of finding an explicit minimal homogeneous system of generators of the ring $R_{\mathbb{Z}}$ (as an optimal characteristic free description of the generators of $R_{\mathbb{F}}$). In the present paper we answer the special case $n = 2$ of this question.

2010 *Mathematics Subject Classification*. Primary: 13A50; Secondary: 14L30, 15A72, 16R30.

This research was partially supported by National Research, Development and Innovation Office, NK-FIH K 119934.

In fact an explicit minimal homogeneous generating system of $R_{\mathbb{F}}$ is known in very few cases only. In the special case $n = 2$ and $\mathbb{F} = \mathbb{C}$, a minimal homogeneous generating system of $R_{\mathbb{C}}$ was determined by Domokos [9]. The generators have degree 2 and 4. (As a byproduct of our calculations here we get a new proof of this statement, see Theorem 4.3.) It was pointed out by Domokos and Drensky [10] that the result remains valid for any infinite field \mathbb{F} with $\text{char}(\mathbb{F}) \neq 2$ thanks to the characteristic free description of vector invariants of the special orthogonal group due to De Concini and Procesi [2]. Apart from that a minimal homogeneous generating system of $R_{\mathbb{F}}$ is known only when $n = m = 3$ by [8, Theorem 4.3] for $\text{char}(\mathbb{F}) = 0$ (see also [28, Proposition 11.49]) and by [11, Theorem 3] for arbitrary infinite \mathbb{F} or for $R_{\mathbb{Z}}$.¹

In the present paper we determine a minimal homogeneous generating system of $R_{\mathbb{F}}$ when $n = 2$ and $\text{char}(\mathbb{F}) = 2$ (see Theorem 2.1). Simultaneously we get in Theorem 2.2 a minimal system of \mathbb{Z} -algebra generators in the \mathbb{Z} -form of $\mathcal{O}((\mathbb{Q}^{2 \times 2})^m)^{SL_2 \times SL_2}$. An irredundant separating system of $SL_2 \times SL_2$ -invariants on $(\mathbb{F}^{2 \times 2})^m$ is provided for an algebraically closed base field of arbitrary characteristic in Theorem 6.1.

Additional interest in the calculations of this paper stems from a connection to the open problem of generating vector invariants of the orthogonal group in characteristic two. This is discussed in Section 7, where we deduce that in the 4-dimensional case, the exotic vector invariants of $SO(4, \mathbb{F})$ (with $\text{char}(\mathbb{F}) = 2$) constructed by Domokos and Frenkel [13] together with the well-known quadratic invariants generate the corresponding algebra of invariants.

2. THE MAIN RESULT

Denote by $x_{ijk} \in \mathcal{O}(M)$ the function mapping $(A_1, \dots, A_m) \in M$ to the (i, j) -entry of $A_k \in \mathbb{F}^{n \times n}$. Then $\mathcal{O}(M)$ is the mn^2 -variable polynomial algebra $\mathbb{F}[x_{ijk} \mid 1 \leq i, j \leq n, k = 1, \dots, m]$. Write x_k for the $n \times n$ matrix over $\mathcal{O}(M)$ whose (i, j) -entry is x_{ijk} ($k = 1, \dots, m; 1 \leq i, j \leq n$). So x_1, \dots, x_m (called sometimes *generic matrices*) are elements of the noncommutative ring $\mathcal{O}(M)^{n \times n}$. The algebra $\mathcal{O}(M)$ is graded in the standard way, namely the generators x_{ijk} have degree 1. The subalgebra R is generated by homogeneous elements. Write R_+ for the subspace of R spanned by its homogeneous elements of positive degree (clearly R_+ is an ideal in R and $R/R_+ \cong \mathbb{F}$). By the graded Nakayama lemma some homogeneous elements in R_+ form a minimal homogeneous \mathbb{F} -algebra generating system of R if and only if they constitute an \mathbb{F} -vector space basis in an \mathbb{F} -vector space direct complement of the ideal $(R_+)^2$ in R_+ . A homogeneous semi-invariant $f \in R_+$ is said to be *indecomposable* if f is not contained in $(R_+)^2$ (equivalently, f can not be expressed as a polynomial of semi-invariants of strictly smaller degree).

Now suppose that $n = 2$, and let us construct some semi-invariants. Clearly the determinant $\det(x_k)$ is a semi-invariant for $k = 1, \dots, m$, and we also have its linearization; that is, for $1 \leq k, l \leq m$ define $\langle x_k | x_l \rangle$ by the equality

$$\det(zx_k + wx_l) = z^2 \det(x_k) + zw \langle x_k | x_l \rangle + w^2 \det(x_l) \in \mathcal{O}(M)[z, w]$$

(where z, w are additional commuting variables). That is,

$$\langle x_k | x_l \rangle = x_{11k}x_{22l} + x_{11l}x_{22k} - x_{12k}x_{21l} - x_{12l}x_{21k}.$$

¹After publication of the present work came to my attention that this account is not complete, see Section 8 at the end of the paper.

For $\alpha \in (\mathbb{N}_0^{q \times q})^m$ set

$$t^\alpha := \prod_{r,s,k} t_{rsk}^{\alpha_{rsk}} \in \mathcal{O}(N) \subset \mathcal{O}(M \times N).$$

An element $f \in \mathcal{O}(M, N)$ can be viewed as a polynomial over $\mathcal{O}(M)$ with variables t_{rsk} , and denote by $\text{Coef}(t^\alpha, f) \in \mathcal{O}(M)$ the coefficient of t^α in f :

$$f = \sum_{\alpha \in (\mathbb{N}_0^{q \times q})^m} \text{Coef}(t^\alpha, f) t^\alpha.$$

A well known construction of semi-invariants is based on the multiplicativity of the determinant:

Lemma 3.1. *For any $u \in (\mathcal{O}(N)^{q \times q})^m$ and $\alpha \in (\mathbb{N}_0^{q \times q})^m$ we have that $\text{Coef}(t^\alpha, \det(x \otimes u))$ belongs to R .*

Proof. For $g \in SL_n$ write $\text{diag}(g, \dots, g)$ for the element of SL_{qn} obtained by glueing q copies of g along the diagonal. Given $(g, h) \in SL_n \times SL_n$ we have the matrix equality

$$\text{diag}(g^{-1}, \dots, g^{-1}) \cdot x \otimes u \cdot \text{diag}(h, \dots, h) = \sum_{k=1}^m (g^{-1} x_k h) \otimes u.$$

Take determinants, and use the multiplicativity of the determinant to conclude that

$$\det(x \otimes u) = \det\left(\sum_{k=1}^m (g^{-1} x_k h) \otimes u\right).$$

The latter equality shows that the coefficients of $\det(x \otimes u)$ (viewed as a polynomial in the t_{rsk} with coefficients in $\mathcal{O}(M)$) are $SL_n \times SL_n$ -invariant. \square

Our starting point is the following result of Derksen and Weyman [7], Domokos and Zubkov [14], and (in characteristic zero) of Schofield and Van den Bergh [30]; in positive characteristic this result was obtained using the theory of modules with good filtration (see [16] and the references there):

Theorem 3.2. *Let \mathbb{F} be an infinite field. Then the degree of a non-zero homogeneous element in R_+ is a multiple of n , and for $q = 1, 2, \dots$, the degree nq homogeneous component of the algebra R of matrix semi-invariants is spanned as an \mathbb{F} -vector space by*

$$(3) \quad \{\text{Coef}(t^\alpha, \det(x \otimes t)) \mid \alpha \in (\mathbb{N}_0^{n \times n})^m \text{ with } \sum_{r,s,k} \alpha_{rsk} = nq\}.$$

4. THE MAIN REDUCTIONS

In this section we turn to the case $n = 2$, write M for $(\mathbb{F}^{2 \times 2})^m$ and R for $\mathcal{O}(M)^{SL_2 \times SL_2}$.

Lemma 4.1. *Take $q \geq 2$ and $\alpha \in (\mathbb{N}_0^{q \times q})^m$ such that $\text{Coef}(t^\alpha, \det(x \otimes t))$ is indecomposable in R . Then the following hold:*

- (i) *For all $r, s \in \{1, \dots, q\}$ we have $\sum_{k=1}^m \alpha_{rsk} \in \{0, 1\}$.*
- (ii) *The semi-invariant $\text{Coef}(t^\alpha, \det(x \otimes t))$ up to sign agrees with $\xi(x_{k_1}, \dots, x_{k_{2q}})$, where k_1, \dots, k_{2q} are elements of $\{1, \dots, m\}$.*

Proof. (i) When we expand the determinant of $x \otimes t$, each of the $(2q)!$ terms contains at most two entries from each 2×2 block of $x \otimes t$. Since $\text{Coef}(t^\alpha, \det(x \otimes t)) \neq 0$, it follows that for all $r, s \in \{1, \dots, q\}$ we have $\sum_{k=1}^m \alpha_{rsk} \leq 2$. Suppose contrary to our statement (i) that $\sum_{k=1}^m \alpha_{rsk} = 2$ for some r, s . By symmetry we may assume that $r = s = 1$. Laplace expansion of the determinant of $x \otimes t$ along the first two rows shows that

$$\text{Coef}(t^\alpha, \det(x \otimes t)) = \text{Coef}\left(\prod_{k=1}^m t_{11k}^{\alpha_{11k}}, \det\left(\sum_{k=1}^m t_{11k} x_k\right)\right) \cdot \text{Coef}\left(\prod_{r,s=2}^q \prod_{k=1}^m t_{rsk}^{\alpha_{rsk}}, \det(x \otimes u)\right),$$

where $u \in (\mathcal{O}(N)^{(q-1) \times (q-1)})^m$ is obtained from $t = (t_1, \dots, t_m)$ by removing the first row and column of each component $t_k \in \mathcal{O}(N)^{q \times q}$. The two factors on the right hand side above both belong to R_+ by Lemma 3.1. Since $\text{Coef}(t^\alpha, \det(x \otimes t))$ is indecomposable, this is a contradiction. Thus $\sum_{k=1}^m \alpha_{rsk} \leq 1$ for all r, s .

(ii) Consider the set of pairs $P := \{(r, s) \mid \sum_{k=1}^m \alpha_{rsk} = 1\}$. Each of the $(2q)!$ terms of the expansion of the determinant of the matrix $x \otimes t$ contains exactly two factors from the first two rows (respectively columns), two factors from the second two rows (respectively columns), etc. Taking into account (i), we get that for each $r = 1, \dots, q$ we have $|P \cap \{(r, 1), (r, 2), \dots, (r, q)\}| = 2$, and for each $s = 1, \dots, q$ we have $|P \cap \{(1, s), (2, s), \dots, (q, s)\}| = 2$. A theorem of König [26] (asserting that a regular bipartite graph has a perfect matching) implies that there exist permutations σ, π of the set $\{1, 2, \dots, q\}$ such that $\sigma(r) \neq \pi(r)$ for each $r = 1, \dots, q$, and $P = \{(r, \sigma(r)), (r, \pi(r)) \mid r = 1, \dots, q\}$. By symmetry (or simultaneously renumbering the rows of the matrix components of t) we may assume that σ is the identity permutation, and so π is fix point free. We claim that π is in fact a q -cycle. Suppose to the contrary that π preserves a proper non-empty subset of $\{1, \dots, q\}$. Again after a possible simultaneous renumbering of both the rows and columns of the matrix components of t we may assume that π preserves the subset $\{1, \dots, d\}$ (and then necessarily π preserves the complement $\{d+1, \dots, q\}$). This means that each component $\alpha_k \in \mathbb{N}_0^{q \times q}$ of $\alpha \in (\mathbb{N}_0^{q \times q})^m$ is block diagonal, so $\alpha_k = \text{diag}(\beta_k, \gamma_k)$, where $\beta_k \in \mathbb{N}_0^{d \times d}$ and $\gamma_k \in \mathbb{N}_0^{(q-d) \times (q-d)}$. Set $u = (u_1, \dots, u_m)$, where u_k is the left upper $d \times d$ block of t_k , and set $v = (v_1, \dots, v_m)$, where v_k is the complementary block to u_k in t_k . The Laplace expansion of the determinant of $x \otimes t$ along the first $2d$ rows shows that

$$\text{Coef}(t^\alpha, \det(x \otimes t)) = \text{Coef}(t^\beta, \det(x \otimes u)) \cdot \text{Coef}(t^\gamma, \det(x \otimes v)),$$

where $\beta = (\beta_1, \dots, \beta_m) \in (\mathbb{N}_0^{d \times d})^m$ and $\gamma = (\gamma_1, \dots, \gamma_m) \in (\mathbb{N}_0^{(q-d) \times (q-d)})^m$. Both factors on the right hand side above belong to R_+ by Lemma 3.1, so this is a contradiction. This proves our claim that π is a q -cycle. Moreover, after a possible simultaneous renumbering of both the rows and columns of all components of t we may assume that π is the q -cycle $(1, 2, \dots, q)$. Thus there exist unique elements $k_1, \dots, k_{2q} \in \{1, \dots, m\}$ such that

$$\alpha_{rsk} = \begin{cases} 1 & \text{for } (r, s, k) \in \{(r, r, k_r) \mid r = 1, \dots, q\} \\ 1 & \text{for } (r, s, k) \in \{(r, r+1, k_{q+r}) \mid r = 1, \dots, q-1\} \\ 1 & \text{for } (r, s, k) = (q, 1, k_{2q}) \\ 0 & \text{otherwise.} \end{cases}$$

For this α we have $\text{Coef}(t^\alpha, \det(x \otimes t)) = \xi(x_{k_1}, \dots, x_{k_{2q}})$. Since in the process of reducing to this special α we had to renumber rows and columns of the components of t , the original semi-invariant we started with agrees with this latter up to sign. \square

In view of statement (i), it is sufficient to prove (ii) in the special case when $k_1 = k_{q+1}$. The multihomogeneous component of (4) of multidegree $(2, \underbrace{1, \dots, 1}_{q-1}, 0, \underbrace{1, \dots, 1}_{q-1}, 0, \dots, 0)$

gives

$$\xi_q(x_1, x_2, \dots, x_q, x_1, x_{q+2}, x_{q+3}, \dots, x_{2q}) \equiv 0,$$

from which the desired statement follows by making the substitution $x_d \mapsto x_{k_d}$, $d = 1, \dots, 2q$. □

Proof of Theorem 2.1. Combining Theorem 3.2, Lemma 4.1, and Lemma 4.2 we get that the homogeneous semi-invariants in the statement of Theorem 2.1 indeed generate the \mathbb{F} -algebra R . To prove minimality of this generating system, note that each of the given generators are multihomogeneous with respect to the \mathbb{N}_0^m -grading of R mentioned in the proof of Lemma 4.2. Therefore it is sufficient to show that each generator is indecomposable. This is obvious for $\det(x_k)$ and $\langle x_l | x_r \rangle$ since they have minimal possible total degree. Indecomposability of $\xi(x_{k_1}, \dots, x_{k_{2q}})$ for $1 \leq k_1 < \dots < k_{2q} \leq m$ and $\text{char}(\mathbb{F}) = 2$ was proved by Domokos and Frenkel [12, Proposition 2.5]. □

We finish this section by pointing out that Theorem 3.2, Lemma 4.1 and Lemma 4.2 allow an alternative deduction of the zero characteristic case of the following known minimal generating system of $\mathcal{O}((\mathbb{F}^{2 \times 2})^m)^{SL_2 \times SL_2}$:

Theorem 4.3. *For an infinite field \mathbb{F} of characteristic different from 2,*

$$(5) \quad \{ \det(x_k), \langle x_l | x_r \rangle, \xi(x_{k_1}, x_{k_2}, x_{k_3}, x_{k_4}) \mid k = 1, \dots, m; 1 \leq l < r \leq m; 1 \leq k_1 < \dots < k_4 \leq m \}.$$

is a minimal homogeneous generating system of $\mathcal{O}((\mathbb{F}^{2 \times 2})^m)^{SL_2 \times SL_2}$.

Proof. As explained in the introduction, this is known by [2], [9], [10]. We give a new argument for the case $\text{char}(\mathbb{F}) = 0$.

Combining Theorem 3.2, Lemma 4.1, and Lemma 4.2 we get that the semi-invariants (2) generate the \mathbb{F} -algebra R . Therefore to prove that (5) is already a generating system of R , it is sufficient to show that $\xi(x_1, \dots, x_{2q})$ is decomposable in R for each $q > 2$.

Suppose to the contrary that $\xi(x_1, \dots, x_{2q}) \notin (R_+)^2$. We may assume that $m = 2q$. Denote by T the subspace of R spanned by the elements having multidegree $(\underbrace{1, \dots, 1}_{2q})$.

The symmetric group $\Sigma_{2q} = \text{Sym}\{1, \dots, 2q\}$ acts linearly on R via \mathbb{F} -algebra automorphisms, namely a permutation π sends x_{ijk} to $x_{ij\pi^{-1}(k)}$. Obviously both T and R_+^2 are Σ_{2q} -invariant subspaces in R . By Lemma 4.2 (i) we have that the image of $\xi(x_1, \dots, x_{2q})$ in $T / ((R_+)^2 \cap T)$ spans a one-dimensional Σ_{2q} -invariant subspace on which Σ_{2q} acts via its sign representation. In particular, the Σ_{2q} -module T has the sign representation as a direct summand. This is a contradiction. Indeed, $e := \frac{1}{(2q)!} \sum_{\pi \in \Sigma_{2q}} \text{sign}(\pi) \pi$ is the primitive central idempotent in the group algebra $\mathbb{F}\Sigma_{2q}$ corresponding to the sign representation, and $e \cdot T = \{0\}$ when $2q > 4$.

To see minimality of this homogeneous generating system, note that the given generators are multihomogeneous with distinct multidegrees, so it is sufficient to show that each of them is indecomposable. The quadratic generators have minimal possible degree in R_+ , therefore they are indecomposable. The degree four generators are not contained in the subalgebra of R generated by the quadratic generators. Indeed, suppose to the contrary

that $\xi(x_1, x_2, x_3, x_4)$ is contained in the subalgebra generated by the quadratic generators. Since the quadratic generators take the same value on (A_1, A_2, A_3, A_4) and the transposed 4-tuple $(A_1^T, A_2^T, A_3^T, A_4^T)$, the same holds then for $\xi(x_1, x_2, x_3, x_4)$. However, this is not the case, as one can easily check. \square

5. \mathbb{Z} -ALGEBRA GENERATORS

The algebra $\mathcal{O}((\mathbb{Q}^{n \times n})^m)$ contains the subring $\mathcal{O}_{\mathbb{Z}} := \mathbb{Z}[x_{ijk} \mid 1 \leq i, j \leq n, k = 1, \dots, m]$, and $R_{\mathbb{Q}} := \mathcal{O}((\mathbb{Q}^{n \times n})^m)^{SL_n \times SL_n}$ contains the subring

$$R_{\mathbb{Z}} := \mathcal{O}_{\mathbb{Z}} \cap R_{\mathbb{Q}}.$$

For an infinite field \mathbb{F} identify $\mathcal{O}_{\mathbb{F}} := \mathcal{O}((\mathbb{F}^{n \times n})^m)$ with $\mathbb{F} \otimes \mathcal{O}_{\mathbb{Z}}$ in the obvious way (here and later the symbol \otimes stands for tensor product of \mathbb{Z} -modules), and denote by

$$\iota_{\mathbb{F}} : \mathcal{O}_{\mathbb{Z}} \rightarrow \mathcal{O}_{\mathbb{F}} \text{ the map } h \mapsto 1 \otimes h.$$

Since $R_{\mathbb{Z}}$ can be interpreted as a ring of invariants of the affine group scheme $SL_n \times SL_n$ over \mathbb{Z} , we have

$$\iota_{\mathbb{F}}(R_{\mathbb{Z}}) \subseteq R_{\mathbb{F}}$$

(see the book of Jantzen [23, I.2.10] for the relevant material on invariants of group schemes). Even more, we have the following:

Proposition 5.1. *Let \mathbb{F} be an infinite field.*

- (i) *The algebra $R_{\mathbb{F}}$ is spanned as an \mathbb{F} -vector space by $\iota_{\mathbb{F}}(R_{\mathbb{Z}})$.*
- (ii) *Any system of generators of the ring $R_{\mathbb{Z}}$ is mapped to an \mathbb{F} -algebra generating system of $R_{\mathbb{F}}$.*

Proof. For $\mathbb{F} = \mathbb{Q}$ the elements in (3) belong to $R_{\mathbb{Z}}$, and Theorem 3.2 asserts that for an arbitrary infinite field \mathbb{F} their images span $R_{\mathbb{F}}$ as an \mathbb{F} -vector space. So (i) holds, and it implies (ii). \square

The polynomial rings $\mathcal{O}_{\mathbb{Z}}, \mathcal{O}_{\mathbb{F}}$ are graded in the standard way (the variables x_{ijk} have degree 1), and the subrings $R_{\mathbb{Z}}, R_{\mathbb{F}}$ are generated by homogeneous elements. Below for a graded ring A we shall write $A^{(d)}$ for the degree d homogeneous component of A .

Lemma 5.2. *Suppose that S is a graded \mathbb{Z} -submodule of $R_{\mathbb{Z}}$ such that $\iota_{\mathbb{F}}(S)$ spans $R_{\mathbb{F}}$ for any infinite field \mathbb{F} . Then $S = R_{\mathbb{Z}}$.*

Proof. Note that the factor \mathbb{Z} -module $\mathcal{O}_{\mathbb{Z}}/R_{\mathbb{Z}}$ is torsion-free. Indeed, if $kh \in R_{\mathbb{Z}}$ for some positive integer k and $h \in \mathcal{O}_{\mathbb{Z}}$, then $h \in \mathcal{O}_{\mathbb{Z}} \cap \mathbb{Q}R_{\mathbb{Z}} = \mathcal{O}_{\mathbb{Z}} \cap R_{\mathbb{Q}} = R_{\mathbb{Z}}$. It follows that for any non-negative integer d , $\mathcal{O}_{\mathbb{Z}}^{(d)}/R_{\mathbb{Z}}^{(d)}$ is a finitely generated free \mathbb{Z} -module. Therefore $R_{\mathbb{Z}}^{(d)}$ is a \mathbb{Z} -module direct summand in $\mathcal{O}_{\mathbb{Z}}^{(d)}$, hence the embedding $R_{\mathbb{Z}} \hookrightarrow \mathcal{O}_{\mathbb{Z}}$ induces an isomorphism

$$(6) \quad \mathbb{F} \otimes R_{\mathbb{Z}} \xrightarrow{\cong} \mathbb{F} \iota_{\mathbb{F}}(R_{\mathbb{Z}}) \subseteq \mathbb{F} \otimes \mathcal{O}_{\mathbb{Z}} = \mathcal{O}_{\mathbb{F}}.$$

Now tensor with \mathbb{F} the short exact sequence

$$0 \rightarrow S^{(d)} \rightarrow R_{\mathbb{Z}}^{(d)} \rightarrow R_{\mathbb{Z}}^{(d)}/S^{(d)} \rightarrow 0$$

to get the exact sequence

$$(7) \quad \mathbb{F} \otimes S^{(d)} \xrightarrow{\varphi} \mathbb{F} \otimes R_{\mathbb{Z}}^{(d)} \rightarrow \mathbb{F} \otimes R_{\mathbb{Z}}^{(d)}/S^{(d)} \rightarrow 0.$$

The image of φ above is $\mathbb{F}_{\mathbb{F}}(S^{(d)}) = R_{\mathbb{F}}^{(d)}$ by assumption, which by Proposition 5.1 (i) and by (6) is $R_{\mathbb{F}}^{(d)} = \mathbb{F}_{\mathbb{F}}(R_{\mathbb{Z}}^{(d)}) = \mathbb{F} \otimes R_{\mathbb{Z}}^{(d)}$. So φ is surjective, and thus the exactness of (7) means that $R_{\mathbb{Z}}^{(d)} \otimes R_{\mathbb{Z}}^{(d)} / S^{(d)} = 0$. This holds for any infinite field \mathbb{F} .

Now $R_{\mathbb{Z}}^{(d)} / S^{(d)}$ is a finitely generated \mathbb{Z} -module. The equality $\mathbb{Q} \otimes R_{\mathbb{Z}}^{(d)} / S^{(d)} = 0$ implies that $R_{\mathbb{Z}}^{(d)} / S^{(d)}$ is a torsion \mathbb{Z} -module, hence it is a finite abelian group. We claim that it is zero. Assume on the contrary that it is non-zero, and let p be a prime divisor of its order. Then for any field \mathbb{F} whose characteristic is p , we have $\mathbb{F} \otimes R_{\mathbb{Z}}^{(d)} / S^{(d)} \neq 0$, a contradiction. So we have $R_{\mathbb{Z}}^{(d)} / S^{(d)} = 0$ holds for all $d \in \mathbb{N}_0$. This means that $S = R_{\mathbb{Z}}$. □

Remark 5.3. A similar argument was used by Donkin [15, Page 399] to get generators in the \mathbb{Z} -form of the algebra of simultaneous conjugation invariants of m -tuples of $n \times n$ matrices.

As a special case of a general result of Seshadri [31] one gets that the ring $R_{\mathbb{Z}}$ is finitely generated. An explicit finite generating system is given below:

Theorem 5.4. *The ring $R_{\mathbb{Z}}$ is generated by the elements in (3) with $q = 1, 2, \dots, mn^3$, where $\mathbb{F} = \mathbb{Q}$.*

Proof. Denote by S the subring of $R_{\mathbb{Z}}$ generated by the elements in (3) with $q = 1, 2, \dots, mn^3$, where $\mathbb{F} = \mathbb{Q}$. For any infinite field \mathbb{F} , $\mathbb{F}_{\mathbb{F}}(S)$ is a subalgebra of $R_{\mathbb{F}}$. By Theorem 3.2 it contains the homogeneous components of $R_{\mathbb{F}}$ of degree at most mn^4 . Derksen and Makam [5] proved that these components generate the \mathbb{F} -algebra $R_{\mathbb{F}}$. Thus we have $\mathbb{F}_{\mathbb{F}}(S) = R_{\mathbb{F}}$ for any infinite field \mathbb{F} . Consequently, by Lemma 5.2 we conclude $S = R_{\mathbb{Z}}$. □

Remark 5.5. Similar arguments together with the results of [5], [7], [14] yield finite generating systems of the \mathbb{Z} -forms of rings of semi-invariants on spaces of quiver representations. We omit the details.

Next we return to the special case $n = 2$:

Proof of Theorem 2.2. Denote by S the subring of $\mathbb{Z}[x_{ijk} \mid 1 \leq i, j \leq 2, k = 1, \dots, m]$ generated by the elements (2). The conditions of Lemma 5.2 hold for S by Theorem 3.2, Lemma 4.1 and Lemma 4.2, hence by Lemma 5.2 we get that $S = R_{\mathbb{Z}}$.

Minimality of this generating system follows from the minimality statement in Theorem 2.1 (which follows from [12]) and Proposition 5.1 (ii). □

6. MINIMAL SYSTEM OF SEPARATING INVARIANTS

In this section we assume that the base field \mathbb{F} is algebraically closed. Following Derksen and Kemper [3], a subset S of $R = \mathcal{O}(M)^{SL_n \times SL_n}$ is called *separating* if for any $A, B \in M$, if there exists an $f \in R$ with $f(A) \neq f(B)$, then there exists an $h \in S$ with $h(A) \neq h(B)$.

Theorem 6.1. *Let \mathbb{F} be an algebraically closed field of arbitrary characteristic.*

(i) *The following is a separating system of $\mathcal{O}((\mathbb{F}^{2 \times 2})^m)^{SL_2 \times SL_2}$:*

$$\mathcal{S}_m := \{ \det(x_k), \langle x_l | x_r \rangle, \xi(x_{k_1}, x_{k_2}, x_{k_3}, x_{k_4}) \mid k = 1, \dots, m; 1 \leq l < r \leq m; 1 \leq k_1 < \dots < k_4 \leq m \}.$$

(ii) *The above separating system is irredundant.*

Proof of Theorem 6.1 (i). In the special case $m = 4$, \mathcal{S}_4 is even a generating system by Theorem 2.1 and Theorem 4.3. Since $\dim_{\mathbb{F}}(\mathbb{F}^{2 \times 2}) = 4$, a general result of Draisma, Kemper and Wehlau [17] or Grosshans [20, Theorem 7] implies that the polarizations of a separating system in $\mathcal{O}((\mathbb{F}^{2 \times 2})^4)$ constitute a separating system in $\mathcal{O}((\mathbb{F}^{2 \times 2})^m)$ for an arbitrary m . Now for $m \geq 4$ the polarizations of the subset \mathcal{S}_4 are contained in the subalgebra generated by \mathcal{S}_m . \square

In order to prove Theorem 6.1 (ii) it is helpful to recall a connection between the ring of matrix semi-invariants and another ring of invariants. Namely the group SL_n acts on $(\mathbb{F}^{n \times n})^m$ by simultaneous conjugation: for $g \in SL_n$ and (A_1, \dots, A_m) we set

$$g \cdot (A_1, \dots, A_m) = (gA_1g^{-1}, \dots, gA_mg^{-1}).$$

For $m \geq 2$ consider the embedding

$$\sigma : \mathcal{O}((\mathbb{F}^{n \times n})^{m-1}) \rightarrow \mathcal{O}((\mathbb{F}^{n \times n})^m), \quad (A_1, \dots, A_{m-1}) \mapsto (A_1, \dots, A_{m-1}, I)$$

where I stands for the $n \times n$ identity matrix.

Proposition 6.2. [8, Proposition 4.1] *The comorphism $\sigma^* : \mathcal{O}((\mathbb{F}^{n \times n})^m) \rightarrow \mathcal{O}((\mathbb{F}^{n \times n})^{m-1})$ of σ maps $\mathcal{O}(M)^{SL_n \times SL_n}$ surjectively onto the algebra $\mathcal{O}((\mathbb{F}^{n \times n})^{m-1})^{SL_n}$ of simultaneous conjugation invariants of matrices.*

This statement has the following immediate corollary (cf. [6, Proposition 3.2]):

Corollary 6.3. *Any separating system of $SL_n \times SL_n$ -invariants on $(\mathbb{F}^{n \times n})^m$ is mapped by σ^* to a separating system of simultaneous conjugation SL_n -invariants on $(\mathbb{F}^{n \times n})^{m-1}$.*

Proof. Let $S \subset \mathcal{O}(M)^{SL_n \times SL_n}$ be a separating system. Suppose that for $A = (A_1, \dots, A_{m-1}) \in (\mathbb{F}^{n \times n})^{m-1}$ and $B = (B_1, \dots, B_{m-1}) \in (\mathbb{F}^{n \times n})^{m-1}$ there exists an $f \in \mathcal{O}((\mathbb{F}^{n \times n})^{m-1})^{SL_n}$ with $f(A) \neq f(B)$. By Proposition 6.2 there exists a $b \in \mathcal{O}(M)^{SL_n \times SL_n}$ with $\sigma^*(b) = f$. Then we have $b(\sigma(A)) \neq b(\sigma(B))$, therefore there exists an $h \in S$ with $h(\sigma(A)) \neq h(\sigma(B))$. Now $\sigma^*(h) \in \sigma^*(S)$ separates A and B . \square

For sake of completeness we recall that for a representation of a reductive group, two points can be separated by polynomial invariants if and only if the unique Zariski closed orbits in their orbit closures are different, see for example [19, Theorem A]. Therefore Corollary 6.3 follows from the following geometric refinement of Proposition 6.2. The group SL_n acts faithfully on $SL_n \times SL_n$ via $a \cdot (g, h) := (ga^{-1}, ha^{-1})$, hence we can form the associated fibre bundle $(SL_n \times SL_n) \times_{SL_n} (\mathbb{F}^{n \times n})^{m-1}$ (see for example [1, Lemma 5.16] for the properties of associated fibre bundles needed below).

Proposition 6.4. (*special case of [14, Lemma 3.1]*) *Set*

$$M_0 := \{(A_1, \dots, A_m) \in (\mathbb{F}^{n \times n})^m \mid \det(A_m) = 1\}.$$

The map

$$SL_n \times SL_n \times (\mathbb{F}^{n \times n})^{m-1} \longrightarrow M_0, \quad (g, h, A_1, \dots, A_{m-1}) \mapsto (gA_1h^{-1}, \dots, gA_{m-1}h^{-1}, gh^{-1})$$

is SL_n -invariant, and factors through an isomorphism

$$(SL_n \times SL_n) \times_{SL_n} (\mathbb{F}^{n \times n})^{m-1} \xrightarrow{\cong} M_0.$$

In particular, the map σ induces a bijection between SL_n -invariant subvarieties in $(\mathbb{F}^{n \times n})^{m-1}$ and $SL_n \times SL_n$ -invariant subvarieties in M_0 . This bijection respects inclusions and Zariski

closures, so restricts to a bijection between Zariski closed SL_n -orbits in $(\mathbb{F}^{n \times n})^{m-1}$ and Zariski closed $SL_n \times SL_n$ -orbits in M_0 .

Remark 6.5. In a recent preprint Derksen and Makam [6] gave an algorithm that decides whether the $SL_n \times SL_n$ -orbit closures of $A, B \in M$ intersect.

We need the following observation of I. Kaygorodov, A. Lopatin and Y. Popov [24, Lemma 3.1]:

Lemma 6.6. *The following is an irredundant separating system of conjugation SL_2 -invariants on $(\mathbb{F}^{2 \times 2})^3$:*

$$\mathrm{tr}(x_k), \det(x_k), k = 1, 2, 3; \mathrm{tr}(x_l x_r), 1 \leq l < r \leq 3; \mathrm{tr}(x_1 x_2 x_3).$$

Note that we have

$$(8) \quad \langle x_l | x_r \rangle = \mathrm{tr}(x_l) \mathrm{tr}(x_r) - \mathrm{tr}(x_l x_r).$$

Proof of Theorem 6.1 (ii). Assume to the contrary that omitting an element h from \mathcal{S}_m we still have a separating system. Now h depends only on at most 4 matrix components. By symmetry we may assume that h does not depend x_5, \dots, x_m , so $h \in \mathcal{S}_4$. Identify $(\mathbb{F}^{2 \times 2})^4$ with the subspace of $(\mathbb{F}^{2 \times 2})^m$ consisting of the tuples whose last $m - 4$ matrix components are zero. Since all elements in $\mathcal{S}_m \setminus \mathcal{S}_4$ vanish identically on the subspace $(\mathbb{F}^{2 \times 2})^4$ in $(\mathbb{F}^{2 \times 2})^m$, we conclude that $\mathcal{S}_4 \setminus \{h\}$ is a separating system in $\mathcal{O}((\mathbb{F}^{2 \times 2})^4)$.

Suppose first that $h = \xi(x_1, x_2, x_3, x_4)$. Denote by $\sigma : (\mathbb{F}^{2 \times 2})^3 \mapsto (\mathbb{F}^{2 \times 2})^4$ the embedding $(A_1, A_2, A_3) \mapsto (A_1, A_2, A_3, I)$ (where I is the 2×2 identity matrix). Then (8) shows that $\sigma^*(\mathcal{S}_4 \setminus \{h\})$ is contained in the subalgebra of $\mathcal{O}((\mathbb{F}^{2 \times 2})^3)$ generated by the elements of degree at most two in the separating system given in Lemma 6.6. Therefore by Lemma 6.6, $\sigma^*(\mathcal{S}_4 \setminus \{h\})$ is not a separating system on $(\mathbb{F}^{2 \times 2})^3$ with respect to the conjugation action of SL_2 , contrary to Corollary 6.3.

If h does not depend on all the four matrix components, say h does not depend on x_4 , then we get that a proper subset of $\{\det(x_1), \det(x_2), \langle x_1 | x_2 \rangle\}$ is a separating system on $(\mathbb{F}^{2 \times 2})^2$ with respect to the action of $SL_2 \times SL_2$. This is obviously a contradiction. \square

The main result of [24] can be obtained as a consequence of Theorem 6.1 (i) and Lemma 6.6:

Corollary 6.7. *(Kaygorodov, Lopatin and Popov [24, Theorem 1.1]) For an algebraically closed field \mathbb{F} of arbitrary characteristic and a positive integer m , the set*

$$\{\mathrm{tr}(x_k), \det(x_k), \mathrm{tr}(x_l x_r), \mathrm{tr}(x_{k_1} x_{k_2} x_{k_3}) \mid k = 1, 2, 3; 1 \leq l < r \leq m; 1 \leq k_1 < k_2 < k_3 \leq m\}$$

is an irredundant separating system of SL_2 -invariants on $(\mathbb{F}^{2 \times 2})^m$.

Proof. We have the equality

$$(9) \quad \xi(x_1, x_2, x_3, I) = \mathrm{tr}(x_1 x_2 x_3) - \mathrm{tr}(x_1 x_2) \mathrm{tr}(x_3).$$

Indeed, consider (1) in the special case $q = 2$, and substitute x_4 by the 2×2 identity matrix I :

$$\left| \begin{array}{cc} z_1 x_1 & w_1 x_3 \\ w_2 I & z_2 x_2 \end{array} \right| = \left| \begin{array}{cc} 0 & w_1 x_3 - z_1 w_2^{-1} z_2 x_1 x_2 \\ w_2 I & z_2 x_2 \end{array} \right| = |w_1 w_2 x_3 - z_1 z_2 x_1 x_2|.$$

Now (8) gives (9), which implies by Theorem 6.1 (i) and Corollary 6.3 (applied for $m + 1$ instead of m) that the set in our statement is indeed a separating system. Its irredundancy is an immediate consequence of Lemma 6.6. \square

Remark 6.8. We note that similarly to the proof of Theorem 5.4, using Lemma 5.2 one gets from the results of [15] and [5] that the \mathbb{Z} -form $\mathbb{Z}[x_{ijk} \mid 1 \leq i, j \leq n, k = 1, \dots, m] \cap \mathcal{O}((\mathbb{Q}^{n \times n})^m)^{SL_n}$ of the \mathbb{Q} -algebra of simultaneous conjugation invariants of matrices is generated by coefficients of the characteristic polynomials of monomials in the generic matrices x_1, \dots, x_m , that have total degree at most $(m + 1)n^4$.

7. VECTOR INVARIANTS OF THE SPECIAL ORTHOGONAL GROUP

Up to base change there is only one non-singular quadratic form on $\mathbb{F}^4 = \mathbb{F}^{2 \times 2}$, namely the form $A \mapsto \det(A)$ ($A \in \mathbb{F}^{2 \times 2}$). The *orthogonal group* $O(4, \mathbb{F})$ therefore can be defined as the subgroup of $GL(\mathbb{F}^{2 \times 2})$ consisting of the linear transformations that preserve the determinant. The connected component of the identity in $O(4, \mathbb{F})$ is an index two subgroup, called the *special orthogonal group* $SO(4, \mathbb{F})$, and it is well known that $SO(4, \mathbb{F}) = \rho(SL_2 \times SL_2)$, where $\rho: SL_2 \times SL_2 \rightarrow GL(\mathbb{F}^{2 \times 2})$ is the representation of $SL_2 \times SL_2$ on $\mathbb{F}^{2 \times 2}$ given by $(g, h) \cdot A := gAh^{-1}$. So the representation of $SL_2 \times SL_2$ on $(\mathbb{F}^{2 \times 2})^m$ can be thought of as the sum of m copies of the defining representation of $SO(4, \mathbb{F})$, and the algebra $R = \mathcal{O}(M)^{SL_2 \times SL_2} = \mathcal{O}((\mathbb{F}^{2 \times 2})^m)^{SO(4, \mathbb{F})}$ is the so-called *algebra of vector invariants of the special orthogonal group of degree 4*.

Generators of the algebra $\mathcal{O}((\mathbb{F}^n)^m)^{SO(n, \mathbb{F})}$ have a uniform description in characteristic zero, and this is one of the theorems usually referred to as the First Fundamental Theorem of Invariant Theory, see [32]. The result extends verbatim (but with essentially different proof) for odd positive characteristic by [2]. However, in the case $\text{char}(\mathbb{F}) = 2$, for all even m an indecomposable multilinear $SO(n, \mathbb{F})$ -invariant on $(\mathbb{F}^n)^m$ was constructed in [13, Theorem 7]. This led Procesi [29, page 551] to write that "in this case the invariant theory has to be deeply modified". In particular, the following question is open:

Question 7.1. *Do the invariants constructed in [13] together with the quadratic invariants generate $\mathcal{O}((\mathbb{F}^n)^m)^{SO(n, \mathbb{F})}$ when $\text{char}(\mathbb{F}) = 2$?*

Now as an immediate consequence of Theorem 2.1 we get that the answer to Question 7.1 is affirmative in the special case $n = 4$:

Corollary 7.2. *Let \mathbb{F} be an algebraically closed field of characteristic 2. The elements given in [13, Theorem 7] together with the usual quadratic invariants constitute a minimal generating system of the algebra of vector invariants of the special orthogonal group $SO(4, \mathbb{F})$ on $(\mathbb{F}^4)^m$.*

Moreover, formally the same elements as in Corollary 7.2 generate the appropriate \mathbb{Z} -form of $\mathcal{O}((\mathbb{C}^4)^m)^{SO(4, \mathbb{C})}$ by an argument similar to the proof of Theorem 2.2.

8. NOTE ADDED AFTER PUBLICATION

Lopatin in [27, Theorems 2.3 and 2.20] determines a minimal system of generators of the algebra of semi-invariants of an arbitrary quiver with a dimension vector taking value 2 at each vertex of the quiver, over an arbitrary infinite base field. In particular, in [27, Lemma 8.6] Lopatin gives an explicit minimal generating system of semi-invariants of quivers having two vertices with dimension vector taking value 2 at both vertices. So

as a special case of Lopatin's result, a minimal generating system of the algebra of semi-invariants of 2×2 matrices was known prior to our Theorem 2.1 also in characteristic 2.

Theorem 2.1 is obtained by different calculations than the corresponding result in [27], and the other topics of the present paper (separating invariants and the connection to the orthogonal group) are not discussed in [27].

REFERENCES

- [1] K. Bongartz, Some geometric aspects of representation theory, *Algebras and Modules I*, CMS Conf. Proc. 23 (1998), 1-27, (I. Reiten, S.O. Smalø, Ø. Solberg, editors).
- [2] C. De Concini and C. Procesi, A characteristic free approach to invariant theory, *Adv. Math.* 21 (1976), 330-354.
- [3] H. Derksen, G. Kemper, *Computational Invariant Theory*, Encyclopaedia of Mathematical Sciences 130, Springer-Verlag, 2002.
- [4] H. Derksen and V. Makam, Polynomial degree bounds for matrix semi-invariants, *Adv. Math.* 310 (2017), 44-63.
- [5] H. Derksen and V. Makam, Generating invariant rings of quivers in arbitrary characteristic, *J. Algebra* 489 (2017), 435-445.
- [6] H. Derksen and V. Makam, Algorithms for orbit closure separation for invariants and semi-invariants of matrices, arXiv:1801.02043
- [7] H. Derksen and J. Weyman, Semi-invariants of quivers and saturation for Littlewood-Richardson coefficients, *J. Amer. Math. Soc.* 13 (2000), 467-479.
- [8] M. Domokos, Relative invariants of 3×3 matrix triples, *Lin. Multilin. Algebra* 47 (2000), 175-190.
- [9] M. Domokos, Poincaré series of semi-invariants of 2×2 matrices, *Lin. Alg. Appl.* 310 (2000), 183-194.
- [10] M. Domokos and V. Drensky, Gröbner bases for the rings of special orthogonal and 2×2 matrix invariants, *J. Algebra* 243 (2001), 706-716.
- [11] M. Domokos and V. Drensky, Defining relation for semi-invariants of three by three matrix triples, *J. Pure Appl. Alg.* 216 (2012), 2098-2105.
- [12] M. Domokos and P. E. Frenkel, On orthogonal invariants in characteristic 2, *J. Algebra* 274 (2004), 662-688.
- [13] M. Domokos and P. E. Frenkel, Mod 2 indecomposable orthogonal invariants, *Adv. Math.* 192 (2005), 209-217.
- [14] M. Domokos and A. N. Zubkov, Semi-invariants of quivers as determinants, *Transformation Groups* 6 (2001), 9-24.
- [15] S. Donkin, Invariants of several matrices, *Inv. Math.* 110 (1992), 389-401.
- [16] S. Donkin, Tilting modules for algebraic groups and finite dimensional algebras, pp. 215-257 in *Handbook of Tilting Theory*, London Math. Soc. Lecture Notes Series 332, ed. L. A. Hügel, D. Happel, H. Krause, Cambridge University Press, 2007.
- [17] J. Draisma, G. Kemper, D. Wehlau, Polarization of separating invariants, *Canad. J. Math.* 60 (2008), 556-571.
- [18] A. Garg, L. Gurvits, R. Oliveira and A. Wigderson, A deterministic polynomial time algorithm for non-commutative rational identity testing, 2016 IEEE 57th Annual Symposium on Foundations of Computer Science (2016), 109-117.
- [19] F. D. Grosshans, *Algebraic Homogeneous Spaces and Invariant Theory*, Lecture Notes in Mathematics 1673, Springer-Verlag, Berlin, 1997.
- [20] F. D. Grosshans, Vector invariants in arbitrary characteristic, *Transform. Groups* 12 (2007), 499-514.
- [21] P. Hrubeš and A. Wigderson, Non-commutative arithmetic circuits with division, ITCS14 Proceedings of the 5th conference on Innovations in theoretical computer science, pp. 49-66, Princeton, NJ, 2014.
- [22] G. Ivanyos, Y. Qiao, K. V. Subrahmanyam, Non-commutative Edmonds' problem and matrix semi-invariants, *Comput. Complex.* (2017), 1-47.

- [23] J. C. Jantzen, Representations of Algebraic Groups, Second edition, Amer. Math. Soc., Providence, Rhode Island, 2003.
- [24] I. Kaygorodov, A. Lopatin and Y. Popov, Separating invariants for 2×2 matrices, Lin. Alg. Appl. 559 (2018), 114-124.
- [25] A. D. King, Moduli of representations of finite dimensional algebras, Quart. J. Math. Oxford (2) 45 (1994), 515-530.
- [26] D. König, Über Graphen und ihre Anwendung auf Determinantentheorie und Mengenlehre, Math. Ann., 77 (1916), 453-465.
- [27] A. Lopatin, Minimal generating set for semi-invariants of quivers of dimension two, Lin. Alg. Appl. 434 (2011), 1920-1944.
- [28] S. Mukai, An Introduction to Invariants and Moduli, Cambridge Univ. Press, 2003.
- [29] C. Procesi, Lie Groups (An Approach through Invariants and Representations), Springer, New York, 2007.
- [30] A. Schofield and M. Van den Bergh, Semi-invariants of quivers for arbitrary dimension vectors, Indag. Mathem., N.S. 12 (2001), 125-138.
- [31] C. S. Seshadri, Geometric reductivity over arbitrary base, Adv. Math. 26 (1977), no. 3, 225-274.
- [32] H. Weyl, The Classical Groups, Second edition, Princeton University Press, Princeton, 1946.

ALFRÉD RÉNYI INSTITUTE OF MATHEMATICS, REÁLTANODA UTCA 13-15, 1053 BUDAPEST, HUNGARY

E-mail address: domokos.matyas@renyi.hu