J. Korean Math. Soc. **0** (0), No. 0, pp. 1–0
https://doi.org/10.4134/JKMS.j170684
pISSN: 0304-9914 / eISSN: 2234-3008

FIXED DIVISOR OF A MULTIVARIATE POLYNOMIAL AND GENERALIZED FACTORIALS IN SEVERAL VARIABLES

Krishnan Rajkumar, Arikatla Satyanarayana Reddy, and Devendra Prasad Semwal

Abstract. We define new generalized factorials in several variables over an arbitrary subset $\underline{S} \subseteq R^n$, where R is a Dedekind domain and n is a positive integer. We then study the properties of the fixed divisor $d(\underline{S}, f)$ of a multivariate polynomial $f \in R[x_1, x_2, \ldots, x_n]$. We generalize the results of Polya, Bhargava, Gunji & McQuillan and strengthen that of Evrard, all of which relate the fixed divisor to generalized factorials of $\underline{S}$. We also express $d(\underline{S}, f)$ in terms of the images $f(\underline{a})$ of finitely many elements $\underline{a} \in R^n$, generalizing a result of Hensel, and in terms of the coefficients of f under explicit bases.

1. Introduction

Let R be a Dedekind domain, n a positive integer and $\underline{S} \subseteq R^n$ be an arbitrary subset. Let $f \in R[x_1, x_2, \ldots, x_n] = R[\underline{x}]$ be a polynomial in n variables. The fixed divisor of f over $\underline{S}$, denoted $d(\underline{S}, f)$, is defined as the ideal in R generated by the values of f on $\underline{S}$.

The study of $d(\underline{S}, f)$ appears to have been initiated by Hensel [15] (see [11] also) in 1896 where he proved the following.

Theorem 1.1. *Let $f \in \mathbb{Z}[\underline{x}]$ be a polynomial with degree m_i in x_i for $i = 1, 2, \ldots, n$. Then $d(\mathbb{Z}^n, f)$ equals the g.c.d. of the values $f(r_1, r_2, \ldots, r_n)$, where each r_i ranges over $m_i + 1$ consecutive integers.*

In case when R is a Dedekind domain with finite norm property, Polya [17] (see [16] also) explicitly constructed a sequence of ideals A_k for each integer k, which served as a bound for the fixed divisor of a univariate polynomial. He proved:

Received October 27, 2017; Revised February 7, 2018; Accepted March 5, 2018.
2010 *Mathematics Subject Classification.* Primary 13F20, 11Rxx.
Key words and phrases. fixed divisor, generalized factorial, Dedekind domain.
We thank Prof. Paul-Jean Cahen for his suggestions which helped us to improve this paper. We also thank the referee for a careful reading of the manuscript and giving several suggestions to correct misprints and improve readability.

Theorem 1.2. *Let R be a Dedekind domain with finite norm property, $I \subseteq R$ be a proper ideal and $k \geq 2$. Then I is the fixed divisor of some primitive polynomial of degree k in $R[x]$ over R if and only if I divides A_k.*

When $\underline{S} = R = \mathbb{Z}$, $A_k = k!$ is the upper bound. Later Cahen [6] relaxed the condition of finite norm property in the above theorem.

Gunji and McQuilllan [13], [14] extended Theorem 1.2 in two different aspects. For the one variable case and R any number field, they generalized the result of Polya when $\underline{S}$ is the coset of any ideal. In the multivariate case for $R = \mathbb{Z}$, they considered the case when $\underline{S}$ is the Cartesian product of arithmetical progressions and proved the following.

Theorem 1.3. *Let $A_i = \{sa_i + b_i\}_{s \in \mathbb{Z}}$ be an arithmetic progression with $a_i, b_i \in \mathbb{Z}$ for $i = 1, 2, \ldots, n$. Let $\underline{A} = A_1 \times A_2 \times \cdots \times A_n$ and $d \in \mathbb{Z}$ be any integer. Then there exists a primitive polynomial $f \in \mathbb{Z}[\underline{x}]$ in n variables with degree m_i in each variable x_i such that $d(\underline{A}, f) = (d)$ if and only if d divides $\prod_{i=1}^{n} m_i! a_i^{m_i}$.*

In the case of one variable, the complete generalization of Theorem 1.2 for a general subset $S \subseteq R$ was given by Bhargava [4] (also see [3] and [5]) by introducing the notion of generalized factorial $k!_S$ to replace A_k of Theorem 1.2. For an excellent exposition of the history and various definitions of $k!_S$ see Cahen and Chabert [9] (also see [3], [5], [18]). Bhargava also obtained a formula for $d(S, f)$ in terms of the coefficients of f.

The case of a multivariate polynomial for general $\underline{S}$ was addressed by Evrard [12] by generalizing Bhargava's factorial in several variables. In order to define this factorial, we need the notion of the ring of integer valued polynomials on $\underline{S}$.

Let K be the field of fractions of R. Then for $\underline{S} \subseteq R^n$, the ring of integer valued polynomials on $\underline{S}$ is defined as

$$\mathrm{Int}(\underline{S}, R) = \{f \in K[\underline{x}] : f(\underline{S}) \subseteq R\}.$$

These rings have been extensively studied in the last few decades. Cahen and Chabert [7] is a good reference for this. We also need the following notation

$$\mathrm{Int}_k(\underline{S}, R) = \{f \in \mathrm{Int}(\underline{S}, R) : \text{ total degree of } f \leq k\}.$$

The generalized multivariable factorial is defined as follows.

Definition. For each $k \in \mathbb{N}$ and $\underline{S} \subseteq R^n$, the generalized factorial of index k is defined by

$$k!_{\underline{S}} = \{a \in R : a \,\mathrm{Int}_k(\underline{S}, R) \subseteq R[\underline{x}]\}.$$

There are several properties of $k!_{\underline{S}}$ that make it a good generalization of Bhargava's factorial to several variables. These properties will be discussed in Section 2. Using this factorial Evrard [12] proved the following generalization of Theorem 1.2.

Theorem 1.4. *Let f be a primitive polynomial of total degree k in n variables and $\underline{S} \subseteq R^n$. Then $d(\underline{S}, f)$ divides $k!_{\underline{S}}$ and this is sharp.*

The sharpness of the statement denotes (and will denote in next sections) the existence of a polynomial f satisfying the conditions of the theorem such that $d(\underline{S}, f) = k!_{\underline{S}}$. This sharpness was obtained by using the notion of ν-ordering in $\underline{S}$ (originally due to Bhargava [5]). This notion also proved to be very useful in the computation of $k!_{\underline{S}}$ ([12, Proposition 26]) and in testing for membership of a polynomial in $\mathrm{Int}_k(\underline{S}, R)$([12, Corollary 17]).

Observe that Theorems 1.1 and 1.3 consider the notion of partial degrees for a multivariate polynomial as compared to Theorem 1.4 which considers the notion of total degree. In this paper we take into account *both* these notions of degree and obtain a new generalization of Bhargava's factorial in several variables. This factorial denoted $\Gamma_{\mathbf{m},k}(\underline{S})$ is indexed by two parameters $\mathbf{m} \in \mathbb{W}^n$, $k \in \mathbb{W}$ and reduces to $k!_{\underline{S}}$ in special cases. Here (and throughout this paper) $\mathbb{W}$ denotes the set of non-negative integers.

We use this factorial to get a generalization of Polya's result (Theorem 1.2) which is sharper than Theorem 1.4. For $\underline{S}$ not contained in an algebraic subset of K^n, we define an analogue of ν-ordering which is helpful in the computation of $\Gamma_{\mathbf{m},k}(\underline{S})$ and also improves the criteria for membership in $\mathrm{Int}(\underline{S}, R)$ in some cases.

We also obtain a generalization of Hensel's result (Theorem 1.1) for such $\underline{S}$, in which we show that $d(\underline{S}, f)$ is the g.c.d. of finitely many values of f (at explicitly constructed elements). To our knowledge, excepting the case of a univariate polynomial over a discrete valuation ring (DVR) in [4], this is the first time that this question has been addressed in the general case. Finally we show that at most two values of f are sufficient to determine $d(\underline{S}, f)$!

The organization of this paper is as follows. In Section 2 we will define $\Gamma_{\mathbf{m},k}(\underline{S})$, establish many of its properties and also discuss the advantages of these factorials in this section and the next. In Section 4 we consider the case when $\underline{S}$ is a Cartesian product and obtain a formula for $d(\underline{S}, f)$ in terms of coefficients of f. We shall also compute and compare the various factorials in this case. In Section 5 we determine $d(\underline{S}, f)$ by finitely many values of f.

2. New generalized factorials in several variables

We start this section by recalling some of the properties of the factorial function which play an important role in various applications. See Chabert [8] for more information regarding these applications as well as generalizations of these properties in other contexts.

Property A. For all $k, l \in \mathbb{N}$, $k!l!$ divides $(k+l)!$.
Property B. For every sequence $x_0, x_1, \ldots, x_n$ of $n+1$ integers, the product $\prod_{0 \le i < j \le n} (x_j - x_i)$ is divisible by $1!2! \cdots n!$.
Property C. For every primitive polynomial $f \in \mathbb{Z}[x]$ of degree n, $d(\mathbb{Z}, f)$ divides $n!$.
Property D. For every integer-valued polynomial $g \in \mathbb{Q}[x]$ of degree n, $n!g \in \mathbb{Z}[x]$.

Note that property C is Polya's result (Theorem 1.2) in the case $R = \mathbb{Z}$. As mentioned in Section 1, $k!_{\underline{S}}$ satisfies generalizations of each of these properties. We introduce a new generalized factorial which also satisfies all of the above properties in the general setting and coincides with $k!_{\underline{S}}$ in special cases.

The new generalized factorial can be defined by starting from any of Properties B, C or D. For instance, the starting point for Bhargava [5] is a generalization of Property B while Evrard [12] starts with that of Property D. Each of these definitions has its advantages and all turn out to be equivalent. In this section we will follow the latter approach as the exposition becomes very concise. We note that almost all of the results and proofs in [12] carry over to this setting (with appropriate restrictions on the degree of the polynomials involved). However, for the sake of completeness we include the alternative proofs.

Let us fix the notation for the rest of the paper. Let $\mathbf{i} \in \mathbb{W}^n$ denote the n-tuple $(i_1, i_2, \ldots, i_n)$, with $\mathbf{0} = (0, 0, \ldots, 0)$. Let $\mathbf{i} \leq \mathbf{j}$ denote the condition that $i_k \leq j_k$ for each component $k = 1, 2, \ldots, n$. The degree of the multivariate polynomial f, denoted by $\deg(f)$, is defined as the n-tuple $\mathbf{m} = (m_1, m_2, \ldots, m_n)$ where m_i is the partial degree of f in x_i. Note that this definition is different from the total degree of the polynomial, denoted by $\mathrm{tdeg}(f)$ for the remainder of this paper. We call f of type $(\mathbf{m}, k)$ if $\deg(f) = \mathbf{m}$ and $\mathrm{tdeg}(f) = k$.

For any $\mathbf{m} \in \mathbb{W}^n$ and $k \in \mathbb{W}$, define

$$\mathrm{Int}_{\mathbf{m},k}(\underline{S}, R) = \{f \in \mathrm{Int}(\underline{S}, R) : \deg(f) \leq \mathbf{m},\ \mathrm{tdeg}(f) \leq k\}.$$

Similarly, we can also define $\mathrm{Int}_{\mathbf{m}}(\underline{S}, R)$ as above without any condition on total degree. Thus we always have $\mathrm{Int}_{\mathbf{m},k}(\underline{S}, R) = \mathrm{Int}_k(\underline{S}, R) \cap \mathrm{Int}_{\mathbf{m}}(\underline{S}, R)$.

Definition. For $\mathbf{m} \in \mathbb{W}^n, k \in \mathbb{W}$, and $\underline{S} \subseteq R^n$, the generalized factorial of index k with respect to $\mathbf{m}$ is defined by

$$\Gamma_{\mathbf{m},k}(\underline{S}) = \{a \in R : a\, \mathrm{Int}_{\mathbf{m},k}(\underline{S}, R) \subseteq R[\underline{x}]\}.$$

It follows that $\Gamma_{\mathbf{m},k}(\underline{S})$ always divides $k!_{\underline{S}}$. For fixed k and varying $\mathbf{m}$, the factorials $\Gamma_{\mathbf{m},k}(\underline{S})$ will be identical to $k!_{\underline{S}}$ when each $m_i \geq c$ for some constant $c = c(k, \underline{S})$ (for example, $c = k$ will do). A similar phenomenon occurs if we fix $\mathbf{m}$ and vary k.

We now arrive at the central result of this section which is a strengthening of Theorem 1.4 and is the generalization of Polya's result in this setting.

Theorem 2.1 (**Generalized Property C**). *Let f be a primitive polynomial of type $(\mathbf{m}, k)$. Then $d(\underline{S}, f)$ divides $\Gamma_{\mathbf{m},k}(\underline{S})$ and this is sharp.*

Proof. From [7] (Prop. XI.1.9) on localization with respect to any nonzero prime ideal $\mathcal{P}$ of R, we have

$$(\mathrm{Int}_{\mathbf{m},k}(\underline{S}, R))_{\mathcal{P}} = \mathrm{Int}_{\mathbf{m},k}(\underline{S}, R_{\mathcal{P}}).$$

Thus the localization of $\Gamma_{\mathbf{m},k}(\underline{S})$ at $\mathcal{P}$ is same as $\Gamma_{\mathbf{m},k}(\underline{S})$ in $R_{\mathcal{P}}$. Hence, it suffices to prove the theorem in the case of a DVR V with valuation ν and uniformizing parameter π (i.e., $\nu(\pi) = 1$).

Let $\Gamma_{\mathbf{m},k}(\underline{S}) = (\pi^s)$ for some $s \in \mathbb{W}$. Recall that for any polynomial $f \in K[\underline{x}]$ with coefficients $a_0, a_1, \ldots, a_n$, $\nu(f)$ is defined as $\inf_{0\leq i\leq n} \nu(a_i)$. Note that $\mathrm{Int}_{\mathbf{m},k}(\underline{S}, V)$ is a V-module finitely generated by polynomials $f_1, f_2, \ldots, f_r$ say (Prop. 3.1 also gives a V-basis). By the definition of $\Gamma_{\mathbf{m},k}(\underline{S})$ these polynomials have to satisfy the condition

$$-\nu(f_j) \leq \nu(\Gamma_{\mathbf{m},k}(\underline{S})) = s \ \forall\ 0 \leq j \leq r,$$

and there must exist some f_i such that $-\nu(f_i) = s$, if not, then $\nu(\Gamma_{\mathbf{m},k}(\underline{S}))$ will have valuation strictly less than s. It is clear that the polynomial $\pi^s f_i \in V[\underline{x}]$ gives us sharpness.

For a given primitive polynomial $f \in V[\underline{x}]$ of type $(\mathbf{m}, k)$ with $\nu(d(\underline{S}, f)) = t$, $\frac{f}{\pi^t}$ belongs to $\mathrm{Int}_{\mathbf{m},k}(\underline{S}, V)$ and hence is a combination of $f_1, f_2, \ldots, f_r$. Consequently, $-\nu(\frac{f}{\pi^t})$ cannot exceed s. Since $\nu(f) = 0$ we get $t \leq s$ completing the proof. □

The following example suggests that the factorial defined by us gives a better bound for fixed divisor than that of [4] and [12] in some cases.

Example 2.2. If f is a primitive polynomial of type $((2,2),3)$, we have the following bounds (refer Equations (5) and (10) for their computations) for $d(\mathbb{Z}\times 2\mathbb{Z}, f)$:

(1) Theorem 1.4 gives $3!_{\mathbb{Z}\times 2\mathbb{Z}} = 2^3 3!$.
(2) Corollary 4.4 (or Theorem 1.3) gives $2!_{\mathbb{Z}} 2!_{2\mathbb{Z}} = 2! 2^2 2!$.
(3) Proposition 4.1 gives $\Gamma_{(2,2),3}(\mathbb{Z}\times 2\mathbb{Z}) = 2^2 2!$.

Hence the polynomial $\frac{f}{2^4}$ cannot be integer valued since 2^4 exceeds $\Gamma_{(2,2),3}(\mathbb{Z}\times 2\mathbb{Z})$. We refer to the discussion after Corollary 4.5 for a detailed comparison of these bounds.

A multivariate polynomial of total degree k can be of different types and hence there are different bounds for its fixed divisor over any subset. For example, when $k = 3$, a polynomial in two variables is one of the following types

$$\{((3,0),3),((3,1),3),((3,2),3),((3,3),3),((2,1),3),$$
$$((2,2),3),((2,3),3),((1,2),3),((1,3),3),((0,3),3)\}.$$

Further taking $\underline{S} = \mathbb{Z}\times 2\mathbb{Z}$, by Proposition 4.1 we have the following bounds for fixed divisor

degree	(3,0)	(3,1)	(3,2)	(3,3)	(2,1)
bound	6	12	24	48	4
degree	(2,2)	(2,3)	(1,2)	(1,3)	(0,3)
bound	8	48	8	48	48

The generalized factorials also satisfy the following property.

Proposition 2.3 (Generalized Property A). *For all* $\mathbf{m}, \mathbf{m}' \in \mathbb{W}^n, k, k' \in \mathbb{W}$, $\Gamma_{\mathbf{m},k}(\underline{S}) \cdot \Gamma_{\mathbf{n},k'}(\underline{S})$ *divides* $\Gamma_{\mathbf{m}+\mathbf{n},k+k'}(\underline{S})$.

The proof follows by verifying the fact

$$\mathrm{Int}_{\mathbf{m},k}(\underline{S},R)\cdot\mathrm{Int}_{\mathbf{m}',k'}(\underline{S},R)\subseteq\mathrm{Int}_{\mathbf{m}+\mathbf{m}',k+k'}(\underline{S},R).$$

3. $\nu_{\mathbf{m}}$-orderings and generalized factorials

Now we shall introduce the concept of a $\nu_{\mathbf{m}}$-ordering of $\underline{S}$ which will help in establishing generalizations of Properties B and C with certain restrictions on $\underline{S}$. We will also obtain the local construction of $\Gamma_{\mathbf{m},k}(\underline{S})$ using these $\nu_{\mathbf{m}}$-orderings. In this section we restrict to the case when $R=V$ where V is a DVR with valuation ν.

Let $K_{\mathbf{m}}[\underline{x}]$ be the vector subspace of $K[\underline{x}]$ containing polynomials of degree at most $\mathbf{m}$. Take the unitary monomial basis of $K_{\mathbf{m}}[\underline{x}]$ and place a total order on it which is compatible with the total degree. Denote the cardinality of this basis by $l_{\mathbf{m}}$. Thus the monomials are arranged in a sequence $(p_j)_{0\le j<l_{\mathbf{m}}}$ with $p_0=1$ and $\mathrm{tdeg}(p_i)\le\mathrm{tdeg}(p_j)$ if $i<j$. For future reference, we also denote by $l_{\mathbf{m},k}$, the cardinality of the monomial basis of $K_{\mathbf{m},k}[\underline{x}]$, where $K_{\mathbf{m},k}[\underline{x}]$ is the set of polynomials of $K_{\mathbf{m}}[\underline{x}]$ of total degree at most k. Note that $l_{\mathbf{m},k}\le\binom{n+k}{k}$. For any sequence of elements $\underline{a}_0,\underline{a}_1,\ldots,\underline{a}_r$ in V^n with $r<l_{\mathbf{m}}$, define

$$\Delta_{\mathbf{m}}(\underline{a}_0,\underline{a}_1,\underline{a}_2,\ldots,\underline{a}_r)=\det(p_j(\underline{a}_i))_{0\le i,j\le r}. \tag{1}$$

Definition. Let $\underline{S}\subseteq V^n$, a sequence of elements $\{\underline{a}_i\}_{0\le i<l_{\mathbf{m}}}$ of $\underline{S}$ is said to be a $\nu_{\mathbf{m}}$-*ordering* of $\underline{S}$ if, for every $1\le r<l_{\mathbf{m}}$,

$$\nu(\Delta_{\mathbf{m}}(\underline{a}_0,\underline{a}_1,\ldots,\underline{a}_r))=\inf_{\underline{a}\in\underline{S}}\nu(\Delta_{\mathbf{m}}(\underline{a}_0,\ldots,\underline{a}_{r-1},\underline{a})).$$

The ordering defined above is the analogue of the ν-ordering of [12] mentioned in the introduction. All the important properties of these orderings occur only in the case that $\underline{S}$ is not contained in any algebraic subset of K^n. In other words, $I(\underline{S})=\{f\in K[\underline{x}]:f(\underline{S})=0\}$ is trivial. This condition is a natural one to impose on $\underline{S}$ as $I(\underline{S})\neq\{0\}$ implies that $\Gamma_{\mathbf{m},k}(\underline{S})=\{0\}$ for large enough values of m_i and k. *Hence we will assume the condition $I(\underline{S})=\{0\}$ for the rest of this paper.*

We note that for any $\nu_{\mathbf{m}}$-ordering $\{\underline{a}_i\}$ of $\underline{S}$, we have $\Delta_{\mathbf{m}}(\underline{a}_0,\underline{a}_1,\ldots,\underline{a}_r)\neq0$ for all $1\le r<l_{\mathbf{m}}$. This is because the vanishing of any of these would automatically give us a non-zero polynomial $\Delta_{\mathbf{m}}(\underline{a}_0,\underline{a}_1,\ldots,\underline{a}_t,\underline{x})$ which would belong to $I(\underline{S})$ contradicting our assumption on $\underline{S}$.

Hence we can define the associated sequence of polynomials as follows.

Definition. With all notations as above we define

$$F_{\mathbf{m},r}(\underline{x})=\frac{\Delta_{\mathbf{m}}(\underline{a}_0,\underline{a}_1,\ldots,\underline{a}_{r-1},\underline{x})}{\Delta_{\mathbf{m}}(\underline{a}_0,\underline{a}_1,\ldots,\underline{a}_r)}$$

for $1\le r<l_{\mathbf{m}}$ and $F_{\mathbf{0},0}(\underline{x})=1$.

The following result gives a criterion for membership in $\mathrm{Int}_{\mathbf{m},k}(\underline{S},V)$.

Proposition 3.1. *Given* $\mathbf{m} \in \mathbb{W}^n, k \in \mathbb{W}$ *and* $\underline{S} \subseteq V^n$*, let* $\{\underline{a}_i\}$ *be a* $\nu_{\mathbf{m}}$*-ordering of* $\underline{S}$*. Then, the associated polynomials* $\{F_{\mathbf{m},r}\}_{0\leq r<l_{\mathbf{m},k}}$ *form a* V*-basis for the* V*-module* $\mathrm{Int}_{\mathbf{m},k}(\underline{S}, V)$*. Hence, given* $f \in K[\underline{x}]$ *of type* $(\mathbf{m}, k)$*, we have the following*

$$f \in \mathrm{Int}_{\mathbf{m},k}(\underline{S}, V) \Leftrightarrow f(\underline{a}_r) \in V \text{ for } 0 \leq r < l_{\mathbf{m},k}.$$

Proof. First note that $\{F_{\mathbf{m},r}\}_{0\leq r<l_{\mathbf{m},k}}$ is a subset of $\mathrm{Int}_{\mathbf{m},k}(\underline{S}, V)$ by the definition of $\nu_{\mathbf{m}}$-ordering. These polynomials also form a basis of $K_{\mathbf{m},k}[\underline{x}]$. Their expansion in terms of $\{p_r\}$ gives a lower-triangular matrix with the diagonal consisting of the non-zero entries

$$\frac{\Delta_{\mathbf{m}}(\underline{a}_0, \underline{a}_1, \underline{a}_2, \ldots, \underline{a}_{r-1})}{\Delta_{\mathbf{m}}(\underline{a}_0, \underline{a}_1, \underline{a}_2, \ldots, \underline{a}_r)}.$$

Hence any $g \in \mathrm{Int}_{\mathbf{m},k}(\underline{S}, V)$ can be expressed as $g(\underline{x}) = \sum_r c_r F_{\mathbf{m},r}(\underline{x})$ where $c_r \in K$.

Evaluation of this expansion at $\underline{x} = \underline{a}_r$ for each r gives us the matrix equation

$$(g(\underline{a}_r))_{0\leq r<l_{\mathbf{m},k}} = U \cdot (c_r)_{0\leq r<l_{\mathbf{m},k}},$$

where U is an upper-triangular matrix with entries in V and unit diagonal. Hence U is unimodular and has an inverse with entries in V, leading to the conclusion that $c_r \in V$ for all r. This establishes that $\{F_{\mathbf{m},r}\}_{0\leq r<l_{\mathbf{m},k}}$ is a V-module basis for $\mathrm{Int}_{\mathbf{m},k}(\underline{S}, V)$.

The second statement follows by observing that we only need $g(\underline{a}_r) \in V$ in the above proof. □

Now we come to the next advantage of our approach over that of [12]. Given a polynomial of type $(\mathbf{m}, k)$, it needs to be evaluated at $l_{\mathbf{m},k}$ points in order to check for it being an integer-valued, which in general, may be much smaller than the corresponding number $\binom{n+k}{k}$ if one considers only total degree ([12, Cor. 17]).

Example 3.2. Consider the polynomial

$$f(x, y) = 1 - \frac{53y}{30} + \frac{xy}{2} + \frac{12y^2}{5} - \frac{xy^2}{2} - \frac{19y^3}{30} \text{ and } \underline{S} = \mathbb{Z}_5 \times \mathbb{Z}_5.$$

If we will keep only total degree in mind ([12, Cor. 17]) then corresponding to the monomial ordering $1, x, y, x^2, xy, y^2, x^3, x^2y, xy^2, y^3$ we must check values of f on first $\binom{3+2}{2}$ terms of ν-ordering. The terms of ν-ordering are - $(0,0), (1,0), (0,1), (2,0), (1,1), (0,2), (3,0), (2,1), (1,2)$ and $(0,3)$ with corresponding f values $1, 1, 1, 1, 1, 2, 1, 1, 1$ and $\frac{1}{5}$ respectively. The last value implies that this polynomial does not map $\underline{S}$ back to $\mathbb{Z}_5$.

Now $\deg(f) = (1,3)$ and the monomial sequence is $1, x, y, xy, y^2, xy^2, y^3$. Thus it is sufficient to check first $l_{(1,3),3} = 7$ terms of $\nu_{(1,3)}$-ordering. The values of f corresponding to $\nu_{(1,3)}$-ordering $(0,0), (1,0), (0,1), (1,1), (0,2), (1,2)$ and $(0,3)$ are $1, 1, 1, 1, 2, 1$ and $\frac{1}{5}$ respectively. Again the last value implies that polynomial doesn't maps $\underline{S}$ back to $\mathbb{Z}_5$.

Now we give the local construction of the new factorials. For that we define the following minor

$$\Delta_{\mathbf{m}}(s;\underline{a}_0,\underline{a}_1,\underline{a}_2,\ldots,\underline{a}_{r-1}) = \det(p_j(\underline{a}_i))_{0\le i<r, 0\le j\le r, j\neq s}$$

for $r < l_{\mathbf{m}}$ and $0 \le s \le r$.

Given the basis of $\mathrm{Int}_{\mathbf{m},k}(\underline{S},V)$ as in Proposition 3.1, the next corollary follows from the same argument as in Theorem 2.1.

Corollary 3.3. *Given* $\mathbf{m}, k, \underline{S}, V, \nu$ *and* $\{\underline{a}_i\}$ *as in Prop. 3.1, we have*

$$\nu(\Gamma_{\mathbf{m},k}(\underline{S})) = \max_{\substack{0\le r<l_{\mathbf{m},k}\\ 0\le s\le r}} \nu\left(\frac{\Delta_{\mathbf{m}}(\underline{a}_0,\underline{a}_1,\ldots,\underline{a}_r)}{\Delta_{\mathbf{m}}(s;\underline{a}_0,\underline{a}_1,\ldots,\underline{a}_{r-1})}\right). \tag{2}$$

Note that this result implies that the right side of Equation (2) is independent of the particular choice of $\nu_{\mathbf{m}}$-ordering. Conversely Equation (2) can be used as a definition of the new factorial, provided we establish this independence by other means. One way to do that would be to first establish that the generalization of Property B holds for the new factorials, which is the last result of this section. Here we interpret property B as follows: the product $\prod_{i<j}(x_i - x_j)$ is the Vandermonde determinant $\det(f_j(x_i))$ where $f_j(x)$ is the monomial x^j; the product of factorials $0!1!\cdots n!$ is the particular value of this determinant for the choice $x_i = i$ which plays the role of the ν - ordering for a valuation ν coming from any prime ideal of $\mathbb{Z}$.

Proposition 3.4 (**Generalized Property B**). *Given* $\mathbf{m}, \underline{S}, V, \nu$ *and* $\{\underline{a}_i\}$ *as in Prop. 3.1, we have for* $r < l_{\mathbf{m}}$

$$\nu(\Delta_{\mathbf{m}}(\underline{a}_0,\underline{a}_1,\ldots,\underline{a}_r)) = \min_{\underline{x}_0,\underline{x}_1,\cdots,\underline{x}_r\in\underline{S}} \nu(\Delta_{\mathbf{m}}(\underline{x}_0,\underline{x}_1,\ldots,\underline{x}_r)).$$

Proof. Let $r \le l_{\mathbf{m}}$ be fixed then we know $(p_j)_{0\le j\le r}$ generates the same vector space over K as $(F_{\mathbf{m},i})_{0\le i\le r}$ generates. Denote the change of basis matrix by M then we have

$$\det(p_j(\underline{a}_i)) = \det(M)\det(F_{\mathbf{m},j}(\underline{a}_i)). \tag{3}$$

Let $\underline{x}_0,\underline{x}_1,\ldots,\underline{x}_r$ be an arbitrary sequence of elements of $\underline{S}$ then

$$\det(p_j(\underline{x}_i)) = \det(M)\det(F_{\mathbf{m},j}(\underline{x}_i)). \tag{4}$$

By substracting Equation (3) from Equation (4) after taking valuation we get

$$\nu(\det(p_j(\underline{x}_i))) - \nu(\det(p_j(\underline{a}_i))) = \nu(\det(F_{\mathbf{m},j}(\underline{x}_i))) - \nu(\det(F_{\mathbf{m},j}(\underline{a}_i))).$$

Since $(F_{\mathbf{m},j})_{j\ge 0}$ are integer valued and $\det(F_{\mathbf{m},j}(\underline{a}_i)) = 1$, $\nu(\det(p_j(\underline{x}_i))) \ge \nu(\det(p_j(\underline{a}_i)))$ completing the proof. □

It follows from this result that the sequence $\nu_{\mathbf{m}}(\Delta(\underline{a}_0,\underline{a}_1,\ldots,\underline{a}_r))$ is independent of the choice of the particular $\nu_{\mathbf{m}}$-ordering.

4. Fixed divisor in the case of Cartesian product of sets

This section is devoted to the case when $\underline{S} = S_1 \times S_2 \times \cdots \times S_n$ where each $S_i \subseteq R$. We start this section by fixing few notations. For any n-tuple $(i_1, i_2, \ldots, i_n) = \mathbf{i}$, its sum of components will be denoted by $|\mathbf{i}|$ and $\mathbf{i}!_{\underline{S}}$ will denote $i_1!_{S_1} \cdots i_n!_{S_n}$.

Proposition 4.1. *In the case when $\underline{S} = S_1 \times S_2 \times \cdots \times S_n$, we have*

$$\Gamma_{\mathbf{m},k}(\underline{S}) = \operatorname*{lcm}_{\substack{\mathbf{0} \le \mathbf{i} \le \mathbf{m} \\ |\mathbf{i}| \le k}} \mathbf{i}!_{\underline{S}}. \tag{5}$$

Proof. It suffices to prove in the case when R is a DVR. Let $S \subseteq V$ be a non-empty subset of the DVR V and $\{a_i\}_{i \ge 0}$ be some ν-ordering of S. Define

$$\binom{x}{r}_S = \frac{(x-a_0)(x-a_1)\ldots(x-a_{r-1})}{(a_r-a_0)(a_r-a_1)\ldots(a_r-a_{r-1})}.$$

The denominator is clearly $r!_S$. In our setting $\underline{S} = S_1 \times S_2 \times \cdots \times S_n$ with some choice of ν-ordering for S_j's we can define analogously for $\mathbf{i} \in \mathbb{W}^n$

$$\binom{\underline{x}}{\mathbf{i}}_{\underline{S}} = \binom{x_1}{i_1}_{S_1} \binom{x_2}{i_2}_{S_2} \cdots \binom{x_n}{i_n}_{S_n}. \tag{6}$$

These polynomials form a V-module basis for $\mathrm{Int}_{\mathbf{m},k}(\underline{S}, V)$ provided we consider only those $\mathbf{i}$'s having the properties $\mathbf{i} \le \mathbf{m}$ and $|\mathbf{i}| \le k$ simultaneously as in Proposition 3.1. As we pointed out in the proof of Theorem 2.1, $\nu(\Gamma_{\mathbf{m},k}(\underline{S}))$ will be the maximum of the valuations of the denominators of this basis, i.e.,

$$\nu(\Gamma_{\mathbf{m},k}(\underline{S})) = \max_{\substack{\mathbf{0} \le \mathbf{i} \le \mathbf{m} \\ |\mathbf{i}| \le k}} \nu(\mathbf{i}!_{\underline{S}}).$$

□

For any subset $T \subseteq R$ and any ideal I with prime factorization $I = \prod_{i=1}^{r} P_i^{e_i}$, define an *$I$-ordering* of T to be a sequence $\{a_j\}_{j=0}^{\infty}$ in R which is congruent modulo $P_i^{e_i+1}$ to a P_i-ordering of T for each $i = 1, 2, \ldots, r$. This type of sequence was also constructed by Bhargava (see [3, Sec. 3]) in case of quotient of Dedekind domain.

Now, for our setting of $\underline{S} = S_1 \times S_2 \times \cdots \times S_n$ and I any fixed ideal, let $\{a_{i,j}\}_{i=0}^{\infty}$ be an I-ordering of S_j for each $j = 1, 2, \ldots, n$. Given $\mathbf{i} = (i_1, i_2, \ldots, i_n) \in \mathbb{W}^n$, let $a_{\mathbf{i}} = (a_{i_1,1}, a_{i_2,2}, \ldots, a_{i_n,n})$ and the associated polynomial $B_{\mathbf{i}}(\underline{x}) = \prod_{j=1}^{n} \prod_{k=0}^{i_j-1} (x_j - a_{k,j})$. For a given prime ideal P and ideal J of R, $w_P(J)$ will denote the highest power of P dividing J. With these notations the following lemma is straightforward.

Lemma 4.2. *For all $\mathbf{i} \in \mathbb{W}^n$ such that $\Gamma_{\mathbf{i},|\mathbf{i}|}(\underline{S})$ divides I we have*

(i) *For all $\mathbf{k} \in \mathbb{W}^n$ such that some component $k_j < i_j$, $B_{\mathbf{i}}(a_{\mathbf{k}}) = 0$;*
(ii) *For all prime P dividing I and $\underline{s} \in \underline{S}$, $w_P(\Gamma_{\mathbf{i},|\mathbf{i}|}(\underline{S})) = w_P(B_{\mathbf{i}}(a_{\mathbf{i}}))$ and $w_P(B_{\mathbf{i}}(a_{\mathbf{i}})) \mid w_P(B_{\mathbf{i}}(\underline{s}))$.*

Let $\{p_j\}_{j\geq 0}$ be the monomials in $K_{\mathbf{m}}[\underline{x}]$ ordered in a sequence compatible with total degree (see the paragraph before Equation 1). Given $f \in R[\underline{x}]$ of type $(\mathbf{m}, k)$, we have

$$f(\underline{x}) = \sum_{j=0}^{l_{\mathbf{m},k}-1} c_j p_j(\underline{x}),$$

where all coefficients $c_j \in R$. We denote the degree of the last monomial in the above expression by $\mathbf{k}$. We now take $I = \operatorname{lcm}(d(\underline{S}, f), \Gamma_{\mathbf{m},k}(\underline{S})) = \prod_{i=1}^{r} P_i^{e_i}$ and construct $a_{\mathbf{i}} = (a_{i_1,1}, a_{i_2,2}, \ldots, a_{i_n,n})$ as described above. It can be seen that f also has the following representation

$$f(\underline{x}) = \sum_{\substack{\mathbf{0}\leq \mathbf{i}\leq \mathbf{m} \\ |\mathbf{i}|\leq k}} b(\mathbf{i}) B_{\mathbf{i}}(\underline{x}). \tag{7}$$

We write this expression in such a way that it ends with $B_{\mathbf{k}}(\underline{x})$. Now we present the main theorem of this section which can be viewed as a generalization of Theorem 1.2 in this setting.

Theorem 4.3. *Let f be a primitive polynomial of type $(\mathbf{m}, k)$ and $b(\mathbf{i})$ be as in (7). Then*

$$d(\underline{S}, f) = (b(\mathbf{0})\Gamma_{\mathbf{0},0}(\underline{S}), \ldots, b(\mathbf{i})\Gamma_{\mathbf{i},|\mathbf{i}|}(\underline{S}), \ldots, b(\mathbf{k})\Gamma_{\mathbf{k},|\mathbf{k}|}(\underline{S})). \tag{8}$$

Consequently, $d(\underline{S}, f)$ divides $\Gamma_{\mathbf{m},k}(\underline{S})$ and this is sharp. Conversely, for each I dividing $\Gamma_{\mathbf{m},k}(\underline{S})$ there exists a primitive polynomial f of type $(\mathbf{m}, k)$ with $d(\underline{S}, f) = I$.

Proof. Let P_j be any prime ideal dividing $d(\underline{S}, f)$ and $P_j^e = w_{P_j}(d(\underline{S}, f))$. Then, by construction $f(a_{\mathbf{i}}) \equiv f(\underline{s})$ modulo $P_j^{e_j+1}$ for some $\underline{s} \in \underline{S}$ and hence P_j^e divides $f(a_{\mathbf{i}})$. We claim that P_j^e divides $b(\mathbf{i})\Gamma_{\mathbf{i},|\mathbf{i}|}(\underline{S})$ and establish it by induction on $|\mathbf{i}|$ as follows.

The base case is clear from the observation that $f(a_{\mathbf{0}}) = b(\mathbf{0})\Gamma_{\mathbf{0},0}(\underline{S})$. Let induction hypothesis be true for all $\mathbf{i}$ for which $|\mathbf{i}| \leq r$. Let $\mathbf{j}$ be an arbitrary index such that $|\mathbf{j}| = r + 1$. Consider the expansion (7) of $f(a_{\mathbf{j}})$. By Lemma 4.2(i), the sum is over the indices $\mathbf{i} \leq \mathbf{j}$. All of these indices, excluding $\mathbf{j}$, have sum of components less than or equal to r. Hence by Lemma 4.2(ii) and the induction hypothesis, we get the desired result that P_j^e divides $b(\mathbf{j})\Gamma_{\mathbf{j},|\mathbf{j}|}(\underline{S})$. This establishes the claim. Consequently P_j^e and hence $d(\underline{S}, f)$ divides $(b(\mathbf{0})\Gamma_{\mathbf{0},|\mathbf{0}|}(\underline{S}), \ldots, b(\mathbf{i})\Gamma_{\mathbf{i},|\mathbf{i}|}(\underline{S}), \ldots, b(\mathbf{k})\Gamma_{\mathbf{k},|\mathbf{k}|}(\underline{S}))$.

In the other direction $(b(\mathbf{0})\Gamma_{\mathbf{0},|\mathbf{0}|}(\underline{S}), \ldots, b(\mathbf{i})\Gamma_{\mathbf{i},|\mathbf{i}|}(\underline{S}), \ldots, b(\mathbf{k})\Gamma_{\mathbf{k},|\mathbf{k}|}(\underline{S}))$ divides $f(\underline{s})$ for all $\underline{s} \in \underline{S}$ (by Lemma 4.2(ii)) and hence divides $d(\underline{S}, f)$ too. This establishes (8).

Note that $(b(\mathbf{0}), \ldots, b(\mathbf{k})) = (c(\mathbf{0}), \ldots, c(\mathbf{k}))$ due to the unimodularity of the matrix which transforms one set of coefficients to the other. So, when f is primitive and P divides $d(\underline{S}, f)$, there exists $\mathbf{i}$ such that P does not divide $b(\mathbf{i})$. Then $w_P(d(\underline{S}, f))$ divides $\Gamma_{\mathbf{i},|\mathbf{i}|}(\underline{S})$. Since $\mathbf{i} \leq \mathbf{m}$ and $|\mathbf{i}| \leq k$, $\Gamma_{\mathbf{i},|\mathbf{i}|}(\underline{S})$

must divide $\Gamma_{\mathbf{m},k}(\underline{S})$, which gives the desired result. For every ideal I dividing $\Gamma_{\mathbf{m},k}(\underline{S})$ selection of $b(\mathbf{i})$'s suitably will give us a primitive polynomial f such that $d(\underline{S}, f) = I$. This proves sharpness also. □

Relaxing the condition of total degree k in Theorem 4.3 and using Proposition 4.1 we get

Corollary 4.4 (Bhargava [4])**.** *Let $f \in R[\underline{x}]$ be a primitive polynomial of degree $\mathbf{m}$ and $b(\mathbf{i})$ be as in* (7) *(with appropriate restrictions on $\mathbf{i}$). Then*

$$d(\underline{S}, f) = (b(\mathbf{0})\mathbf{0}!_{\underline{S}}, \ldots, b(\mathbf{i})\mathbf{i}!_{\underline{S}}, \ldots, b(\mathbf{m})\mathbf{m}!_{\underline{S}}). \tag{9}$$

Hence $d(\underline{S}, f)$ divides $\mathbf{m}!_{\underline{S}}$ and this is sharp. Conversely, for each I dividing $\mathbf{m}!_{\underline{S}}$ there exists a primitive polynomial f of degree $\mathbf{m}$ with $d(\underline{S}, f) = I$.

The following corollary shows the behaviour of the fixed divisor of a multivariate separable polynomial. Its proof follows by induction on the number of variables and by Theorem 4.3.

Corollary 4.5. *Let $f_i(x_i) \in R[x_i]$ for $1 \leq i \leq k$. Then*

$$d(S_1 \times S_2 \ldots \times S_k, f_1 f_2 \ldots f_k) = d(S_1, f_1) d(S_2, f_2) \cdots d(S_k, f_k).$$

We close this section by comparing various bounds of fixed divisor. Recall (see [12, Example 3]) that the generalized factorial $k!_{\underline{S}}$ when $\underline{S}$ is a Cartesian product is given by

$$k!_{\underline{S}} = \operatorname*{lcm}_{|\mathbf{i}|=k} \mathbf{i}!_{\underline{S}}. \tag{10}$$

For a given primitive polynomial f of type $(\mathbf{m}, k)$, Corollary 4.4 and Theorem 1.4 give different bounds on the fixed divisor, viz. $\mathbf{m}!_{\underline{S}}$ and $k!_{\underline{S}}$ respectively and these are not comparable in general. Depending upon the values of $\mathbf{m}$, k and the nature of the subsets S_i, any one result might be stronger than the other.

For example, let $\underline{S} = \mathbb{Z} \times \mathbb{Z}$ and f be a polynomial with integer coefficients with degree $(5, 5)$. If the total degree is 10 (for e.g., $f(x, y) = x^5 y^5$), then Theorem 4.3 asserts that its fixed divisor will divide 5!5! whereas Theorem 1.4 asserts that it will divide 10!. In this case the former is stronger than the latter. On the other hand, if the total degree of the polynomial f is 5 (for e.g., $f(x, y) = x^5 + y^5$), then Theorem 4.3 still says that its fixed divisor will divide 5!5! whereas Theorem 1.4 says that it will divide 5!. In this case the latter is stronger.

Now we note that our factorial always gives a stronger result. If $f(x, y) = x^5 y^5$, then $d(\underline{S}, f)$ divides $\Gamma_{(5,5),10}(\underline{S}) = 5!5!$ and if $f(x, y) = x^5 + y^5$, then $d(\underline{S}, f)$ divides $\Gamma_{(5,5),5}(\underline{S}) = 5!$. Thus in both the cases we get a better bound and this is not a coincidence! $\Gamma_{\mathbf{m},k}(\underline{S})$ always divides $k!_{\underline{S}}$ and $\mathbf{m}!_{\underline{S}}$ but need not to be equal to their g.c.d. as Example 2.2 suggests.

5. Formula for fixed divisor in the general case

In this section we look for various formulae for $d(\underline{S}, f)$ when $\underline{S}$ is an arbitrary subset of R^n such that $I(\underline{S}) = \{0\}$ and R is a Dedekind domain with field of fractions K. We start with few notations; $f(\underline{x})$ will denote a primitive polynomial of type $(\mathbf{m}, k)$ and $\mathbb{P} = \{P_1, P_2, \ldots, P_r\}$ will denote the set of all prime ideals of R which appear in the prime factorization of $\Gamma_{\mathbf{m},k}(\underline{S})$. For each prime ideal $P_i \in \mathbb{P}$, the localization R_{P_i} is a DVR with valuation ν_i, say. For $j = 1, 2, \ldots, r$, let $\{\underline{a}_{i,j}\}_{i=0}^{l_{\mathbf{m},k}-1}$ be a $\nu_{\mathbf{m},j}$-ordering (i.e., $\nu_{\mathbf{m}}$-ordering corresponding to ν_j) of $\underline{S}$ and $e_j = \nu_j\left(\Delta_{\mathbf{m}}(\underline{a}_{0,j}, \underline{a}_{1,j}, \ldots, \underline{a}_{l_{\mathbf{m},k}-1,j})\right)$. Now consider a sequence $\{\underline{a}_i\}_{i=0}^{l_{\mathbf{m},k}-1}$ in R^n which satisfies the congruences

$$\underline{a}_i \equiv \underline{a}_{i,j} \bmod P_j^{e_j+1}. \tag{11}$$

Here $\underline{x} \equiv \underline{y} \bmod I$ denotes $x_i \equiv y_i \bmod I$ for all the components $1 \le i \le n$. We will define the polynomials $B_0(\underline{x}) = 1$ and $B_j(\underline{x}) = \Delta_{\mathbf{m}}(\underline{a}_0, \underline{a}_1, \ldots, \underline{a}_{j-1}, \underline{x})$ for $1 \le j < l_{\mathbf{m},k}$. The following lemmas are easy to prove and hence we omit the proofs.

Lemma 5.1. *For $1 \le j < l_{\mathbf{m},k}$, we have*

(i) *For every $P_i \in \mathbb{P}$, and $\underline{s} \in \underline{S}$, $\nu_i(B_j(\underline{a}_j)) \le \nu_i(B_j(\underline{s}))$;*
(ii) *For $0 \le m < j$, $B_j(\underline{a}_m) = 0$.*

Lemma 5.2. *Let $P_i \in \mathbb{P}$ with $P_i^e = w_P(d(\underline{S}, f))$. Then P_i^e divides $f(\underline{a}_j)$ for all $0 \le j < l_{\mathbf{m},k}$.*

Let $\mathbb{T}$ be a finite set of non-zero prime ideals of R. For a given ideal $I \subset R$ define

$$I_{\mathbb{T}} = \prod_{P \in \mathbb{T}} w_P(I).$$

For example, let $R = \mathbb{Z}$ and $\mathbb{T} = \{2\mathbb{Z}, 3\mathbb{Z}\}$ then $2^2 3^2 5^3 7\mathbb{Z}_{\mathbb{T}} = 2^2 3^2 \mathbb{Z}$.

Now, we give a formula for the fixed divisor in general setting.

Proposition 5.3. *Let $f(\underline{x})$ be a primitive polynomial of type $(\mathbf{m}, k)$. Then there exist $b_0, b_1, \ldots, b_{l_{\mathbf{m},k}-1}$ in K such that*

$$d(\underline{S}, f) = (b_0, b_1\Delta_{\mathbf{m}}(\underline{a}_0, \underline{a}_1), \ldots, b_{l_{\mathbf{m},k}-1}\Delta_{\mathbf{m}}(\underline{a}_0, \underline{a}_1, \ldots, \underline{a}_{l_{\mathbf{m},k}-1}))_{\mathbb{P}}. \tag{12}$$

Proof. Clearly, there exist $b_0, b_1, \ldots, b_{l_{\mathbf{m},k}-1}$ in K such that

$$f(\underline{x}) = \sum_{0 \le i < l_{\mathbf{m},k}} b_i B_i(\underline{x}). \tag{13}$$

Let P be a prime dividing $d(\underline{S}, f)$ and $P^e = w_P(d(\underline{S}, f))$. Then by Lemma 5.2, P^e must divide $f(\underline{a}_i)$ for $0 \le i < l_{\mathbf{m},k}$. By substituting $\underline{x} = \underline{a}_i$ in (13) inductively, we see that P^e divides each fractional ideal generated by $b_i\Delta_{\mathbf{m}}(\underline{a}_0, \underline{a}_1, \underline{a}_2, \ldots, \underline{a}_i)$ and so divides the right side of (12).

Conversely, if $P \in \mathbb{P}$ be any ideal such that P^e divides each fractional ideal $b_i \Delta_{\mathbf{m}}(\underline{a}_0, \underline{a}_1, \underline{a}_2, \ldots, \underline{a}_i)$ for $0 \leq i < l_{\mathbf{m},k}$, then P^e divides $f(\underline{s})$ for all $\underline{s} \in \underline{S}$ by (13) and Lemma 5.1. This completes the proof of the theorem. □

Note that the matrix which transforms the coefficients c_i in the usual representation $f(\underline{x}) = \sum_{0 \leq i < l_{\mathbf{m},k}} c_i p_i(\underline{x})$ to the coefficients b_i in (13) can be computed by first expanding $B_i(\underline{x})$ into monomials and then finding the inverse of the appropriate matrix.

The following result is the converse of Theorem 2.1.

Proposition 5.4. *Let I be any divisor of $\Gamma_{\mathbf{m},k}(\underline{S})$. Then there exists a primitive polynomial f of type $(\mathbf{m}, k)$ and degree such that $d(\underline{S}, f) = I$.*

Proof. By Theorem 2.1, there exists a primitive polynomial g of type $(\mathbf{m}, k)$ with $g(\underline{x}) = \sum_{0 \leq i < l_{\mathbf{m},k}} c_i p_i(\underline{x})$ such that $d(\underline{S}, g) = \Gamma_{\mathbf{m},k}(\underline{S})$. Recall that the set of primes dividing $\Gamma_{\mathbf{m},k}(\underline{S})$ is $\mathbb{P} = \{P_1, P_2, \ldots, P_r\}$. Let $\{Q_1, Q_2, \ldots, Q_s\}$ be the set of primes dividing $(c_1, c_2, \ldots, c_{l-1})$. We note that these two sets have no intersection. For, if not, let $Q_i \in \mathbb{P}$, then Q_i divides $g(\underline{s}) \equiv c_0 \bmod Q_i$ for some $\underline{s} \in \underline{S}$. This means that Q_i divides c_0 and g is not primitive, which is a contradiction.

Choose $b \in R$ such that $w_{P_i}(\langle b \rangle) = w_{P_i}(I)$ for all $i = 1, 2, \ldots, r$ and $Q_i \mid b$ for $i = 1, 2, \ldots, s$.

Consider the polynomial $f = b + g$. Clearly, $d(\underline{S}, f) = I$ and f is primitive. □

The following result is the analogue of Hensel's result (Theorem 1.1).

Theorem 5.5. *Let f be a polynomial of type $(\mathbf{m}, k)$ and $\underline{a} \in \underline{S}$ be such that $f(\underline{a}) \neq 0$. Then there exist elements $\underline{a}_1, \ldots, \underline{a}_{l_{\mathbf{m},k}-1}$ in R^n such that $d(\underline{S}, f)$ is given by*

$$d(\underline{S}, f) = (f(\underline{a}), f(\underline{a}_1), \ldots, f(\underline{a}_{l_{\mathbf{m},k}-1})).$$

Proof. Consider the prime factorization $\langle f(\underline{a}) \rangle = \prod_{i=0}^{r} P_i^{e_i}$. Now we construct a sequence $\{\underline{a}_j\}_{0 \leq j < l_{\mathbf{m},k}}$ which is term-wise congruent to a ν_i-ordering of $\underline{S}$ modulo $P_i^{e_i+1}$. For each ν_i-ordering, we put the condition that the first element is $\underline{a}$. Hence, we can assume that $\underline{a}_0 = \underline{a} \in \underline{S}$.

It can be shown, as in Lemma 5.2, that if P^e divides $d(\underline{S}, f)$, then $P = P_i$ for some i and P^e divides $f(\underline{a}_j)$ for every $0 \leq j < l_{\mathbf{m},k}$.

In the other direction, we express $f(\underline{x}) = \sum_{0 \leq j < l_{\mathbf{m},k}} b_j B_j(\underline{x})$ (these B_j are defined as before in terms of a_j). Now if P^e divides $(f(\underline{a}_0), f(\underline{a}_1), \ldots, f(\underline{a}_{l-1}))$, then it must divide $b_j B_j(\underline{a}_j)$ for $0 \leq j < l_{\mathbf{m},k}$ (by induction) and so it must divide $f(\underline{s})$ for all $\underline{s} \in \underline{S}$ (as shown in Lemma 5.1). □

In the case when $\underline{S}$ is a Cartesian product of subsets of R and f a polynomial of degree $\mathbf{m}$, the elements $a_{\mathbf{i}}$ can be constructed as in Section 4 from a $\langle f(\underline{a}_0) \rangle$-ordering in each component, starting with arbitrary $\underline{a}_0 \in \underline{S}$ such that $f(\underline{a}_0) \neq 0$.

Then $d(\underline{S}, f)$ can be shown to be the g.c.d. of the f images of $l_{\mathbf{m},k}$ elements (which is always less than or equal to the bound $(m_1+1)(m_2+1)\cdots(m_n+1)$ given by Theorem 1.1), which might be more useful than Theorem 4.3 in certain situations.

For example, given all assumptions of Theorem 1.1 where $f \in \mathbb{Z}[\underline{x}]$ is a polynomial with degree m_i in x_i for $i = 1, 2, \ldots, n$. Then

$$d(\mathbb{Z}^n, f) = \gcd\{f(r_1, r_2, \ldots, r_n) : 0 \leq r_i \leq m_i\}. \tag{14}$$

Further if $\operatorname{tdeg}(f) = k$ then by Theorem 5.5 we have

$$d(\mathbb{Z}^n, f) = \gcd\{f(r_1, r_2, \ldots, r_n) : 0 \leq r_i \leq m_i, r_1 + r_2 + \cdots + r_n \leq k\}. \tag{15}$$

From Equations (14) and (15), $d(\mathbb{Z}^n, f)$ can be evaluated by finding the g.c.d. of finite number of images of f. Further Equation (15) uses less number of f images than that of Equation (14).

It is well known that every ideal in a Dedekind domain is generated by two elements. The following result shows that for $d(\underline{S}, f)$, those elements can be taken from images of f.

Theorem 5.6. *Let $f(\underline{x}) \in R[\underline{x}]$ be a polynomial of type $(\mathbf{m}, k)$. Then for each element $\underline{a} \in \underline{S} \subseteq R^n$ such that $f(\underline{a}) \neq 0$, there exists an element $\underline{b} \in R^n$ such that $d(\underline{S}, f) = (f(\underline{a}), f(\underline{b}))$.*

Proof. Let $\underline{a} \in \underline{S} \subseteq R^n$ such that $f(\underline{a}) \neq 0$ and $\Pi_{i=0}^{r} P_i^{e_i}$ be the prime factorization of $\langle f(\underline{a})\rangle$. For each prime P_i we find an element b_{i,r_i} among first $l_{\mathbf{m},k} - 1$ terms of ν_i-ordering of $\underline{S}$ such that $f(\underline{b}_{i,r_i})$ is divisible by the smallest power of P_i. Now we select $\underline{b}$ which is congruent to $\underline{b}_{i,r_i}$ modulo a sufficiently high power of P_i for all $0 \leq i \leq r$. Then it is easy to check that $d(\underline{S}, f) = (f(\underline{a}), f(\underline{b}))$. □

In general, $d(\underline{S}, f)$ may not be generated by a single $f(a)$ for some $a \in R$. For example, if $f = 5x + 3$, then $d(\mathbb{Z}, f) = \mathbb{Z}$, but one cannot find $m \in \mathbb{Z}$ such that $\langle f(m)\rangle = \mathbb{Z}$.

The following corollary gives a relation connecting $d(\underline{S}, fg)$, $d(\underline{S}, f)$ and $d(\underline{S}, g)$. Its proof follows from Theorem 5.5.

Corollary 5.7. *Let $f(\underline{x})$ and $g(\underline{x})$ be two primitive polynomials of type $(\mathbf{m}_1, k_1)$ and $(\mathbf{m}_2, k_2)$. If $\mathbf{m} = \mathbf{m}_1 + \mathbf{m}_2$ and $k = k_1 + k_2$, then there exist elements $\underline{a}_0, \underline{a}_1, \ldots, \underline{a}_{l_{\mathbf{m},k}-1}$ in R^n such that*

$$d(\underline{S}, fg) = (f(\underline{a}_0)g(\underline{a}_0), f(\underline{a}_1)g(\underline{a}_1), \ldots, f(\underline{a}_{l_{\mathbf{m},k}-1})g(\underline{a}_{l_{\mathbf{m},k}-1})),$$

where

$$d(\underline{S}, f) = (f(\underline{a}_0), f(\underline{a}_1), \ldots, f(\underline{a}_{l_{\mathbf{m},k}-1}))$$

and

$$d(\underline{S}, g) = (g(\underline{a}_0), g(\underline{a}_1), \ldots, g(\underline{a}_{l_{\mathbf{m},k}-1})).$$

The polynomials satisfying $d(\underline{S}, fg) = d(\underline{S}, f)d(\underline{S}, g)$ are closely related to irreducibility in $\operatorname{Int}(\underline{S}, \mathbb{Z})$ where $\underline{S} \subseteq \mathbb{Z}$ (see [10, Theorem 2.8]). Corollary 5.7 may be useful in that direction.

The following result, proved in the case of a DVR in [4], can be derived in the single variable case by Theorem 5.5.

Corollary 5.8. *Let S be a subset of R that admits a simultaneous P-ordering, i.e., a sequence $\{a_i\}$ in S which is a P-ordering of S for all non-zero primes P and $f \in R[x]$ a polynomial of degree k. Then*

$$d(S, f) = (f(a_0), f(a_1), \ldots, f(a_k)).$$

For some examples of subsets with simultaneous P-orderings, see [1], [2] and [5].

To conclude, we would like to remark that Theorems 5.5 and 5.6 have many computational advantages over Theorem 4.3, Proposition 5.3 and Corollary 4.4. Firstly, they do not depend on the evaluation of the factorial of $\underline{S}$ or its prime factorization. In fact, due to the sharpness of Theorems 2.1, 1.4 and Corollary 4.4, it might be possible to use these results to evaluate the factorial in some cases. Second, there is no additional step of computing the coefficients in alternate bases which essentially amounts to inverting matrices with coefficients in R. Finally, there is the additional freedom in the choice of $\underline{a}$ to minimize the number of primes involved in the construction of $\underline{a}_i$.

References

[1] D. Adam, *Simultaneous orderings in function fields*, J. Number Theory **112** (2005), no. 2, 287–297.

[2] D. Adam, J.-L. Chabert, and Y. Fares, *Subsets of $\mathbb{Z}$ with simultaneous orderings*, Integers **10** (2010), A37, 437–451.

[3] M. Bhargava, *P-orderings and polynomial functions on arbitrary subsets of Dedekind rings*, J. Reine Angew. Math. **490** (1997), 101–127.

[4] ———, *Generalized factorials and fixed divisors over subsets of a Dedekind domain*, J. Number Theory **72** (1998), no. 1, 67–75.

[5] ———, *The factorial function and generalizations*, Amer. Math. Monthly **107** (2000), no. 9, 783–799.

[6] P.-J. Cahen, *Polynomes à valeurs entières*, Canad. J. Math. **24** (1972), 747–754.

[7] P.-J. Cahen and J.-L. Chabert, *Integer-Valued Polynomials*, Mathematical Surveys and Monographs, **48**, American Mathematical Society, Providence, RI, 1997.

[8] J.-L. Chabert, *Integer-valued polynomials: looking for regular bases (a survey)*, in Commutative algebra, 83–111, Springer, New York, 2014.

[9] J.-L. Chabert and P.-J. Cahen, *Old problems and new questions around integer-valued polynomials and factorial sequences*, in Multiplicative ideal theory in commutative algebra, 89–108, Springer, New York, 2006.

[10] S. T. Chapman and B. A. McClain, *Irreducible polynomials and full elasticity in rings of integer-valued polynomials*, J. Algebra **293** (2005), no. 2, 595–610.

[11] L. E. Dickson, *History of the Theory of Numbers. Vol. II*, Chelsea Publishing Co., New York, 1966.

[12] S. Evrard, *Bhargava's factorials in several variables*, J. Algebra **372** (2012), 134–148.

[13] H. Gunji and D. L. McQuillan, *On polynomials with integer coefficients*, J. Number Theory **1** (1969), 486–493.

[14] ———, *On a class of ideals in an algebraic number field*, J. Number Theory **2** (1970), 207–222.

[15] K. Hensel, *Ueber den grössten gemeinsamen Theiler aller Zahlen, welche durch eine ganze Function von n Veränderlichen darstellbar sind*, J. Reine Angew. Math. **116** (1896), 350–356.
[16] W. Narkiewicz, *Polynomial Mappings*, Lecture Notes in Mathematics, 1600, Springer-Verlag, Berlin, 1995.
[17] G. Polya, *Uber ganzwertige ganze funktionen*, Rend. Circ. Mat. Palermo **40** (1915), 1–16.
[18] M. Wood, *P-orderings*: *a metric viewpoint and the non-existence of simultaneous orderings*, J. Number Theory **99** (2003), no. 1, 36–56.

Krishnan Rajkumar
School of Computer & Systems Sciences
Jawaharlal Nehru University
Delhi 110067, India
Email address: krishnan@mail.jnu.ac.in

Arikatla Satyanarayana Reddy
Department of Mathematics
Shiv Nadar University
Dadri 201314, India
Email address: satyanarayana.reddy@snu.edu.in

Devendra Prasad Semwal
Department of Mathematics
Shiv Nadar University
Dadri 201314, India
Email address: dp742@snu.edu.in