Tuples of polynomials over finite fields with pairwise coprimality conditions

JUAN ARIAS DE REYNA
Department of Mathematical Analysis, Seville University
Seville, Spain
arias@us.es

RANDELL HEYMAN
School of Mathematics and Statistics,
University of New South Wales
Sydney, Australia
randell@unsw.edu.au

July 12, 2017

Abstract

Let q be a prime power. We estimate the number of tuples of degree bounded monic polynomials $(Q_1, \dots, Q_v) \in (\mathbb{F}_q[z])^v$ that satisfy given pairwise coprimality conditions. We show how this generalises from monic polynomials in finite fields to Dedekind domains with a finite norm.

Keywords: relatively prime, coprime, polynomials, finite fields, Dedekind domains

AMS Classification: 11C08

1 Introduction

The question of calculating the number of relatively prime polynomials of fixed degree in finite fields arose in [6, Section 4.6.1, Ex.5]. Further results can be found in [4, 10, 2, 3, 5].

This naturally leads to the concept of tuples of polynomials in finite fields that exhibit pairwise coprimality conditions. This concept is also relevant to polynomial remainder codes used in, amongst other things, error correction (see [11] for an early paper). The density of pairwise coprime polynomials in tuples of finite fields can be inferred from a recent paper [8]. We improve on this result in two ways. Firstly, we contemplate generalised pairwise coprimality conditions. That is, conditions that require some, not necessarily all, of the

pairs of polynomials to be coprime. Secondly, we give an asymptotic counting formula rather than simply a density.

Our results regarding polynomials in finite fields can be applied to the more general setting of ideals in Dedekind domains. We explain this further in Section 2.

Our result is heavily based on [1]; a paper that estimates tuples of pairwise coprime integers of bounded height. We use a graph to represent the required primality conditions as follows. Let $G = (V, E)$ be a graph with v vertices and e edges. The set of vertices, V, will be given by $V = \{1, \dots, v\}$ whilst the set of edges of G, denoted by E, is a subset of the set of pairs of elements of V. That is, $E \subseteq \{\{1,2\},\{1,3\},\dots,\{r,s\},\dots,\{v-1,v\}\}$. We admit isolated vertices (that is, vertices that are not adjacent to any other vertex). An edge is always of the form $\{r,s\}$ with $r \neq s$ and $\{r,s\} = \{s,r\}$. Let

$$X = \{(Q_1, \dots, Q_v) \in (\mathbb{F}_q[z])^v : Q_r \text{ monic}, 1 \leq r \leq v\}.$$

For each real $x > 0$ and any prime power q, we define the set of all tuples that satisfy the primality conditions by

$$Y_G(x) := \{(Q_1, \dots, Q_v) \in X : \deg Q_r \leq x,\ \gcd(Q_r, Q_s) = 1 \text{ if } \{r,s\} \in E\}.$$

We also let $g(x) = |Y_G(x)|$, and denote with d the maximum degree of the vertices of G. All references to polynomials in $\mathbb{F}_q[z]$ will refer to monic polynomials. Finally, let $Q_G(z) = 1 + B_2 z^2 + \cdots + B_v z^v$ be the polynomials associated to the graph G, defined by

$$Q_G(z) = \sum_{F \subset E} (-1)^{|F|} z^{|v(F)|}, \qquad Q_G^+(z) = \sum_{F \subset E} z^{|v(F)|}, \tag{1.1}$$

where $|v(F)|$ is the number of non-isolated vertices of graph F.

Our main result is as follows.

Theorem 1.1. *For a natural number $n > 1$, let $g(n)$ be the cardinality of tuples of monic polynomials $(Q_1, \dots, Q_v)$ in $\mathbb{F}_q[z]$ of degree $\deg(Q_r) \leq n$ satisfying the coprimality conditions given by the graph G whose vertices have degree $\leq d$. Then for any $0 < \varepsilon < \frac{1}{2}$ we have*

$$g(n) = \frac{\rho_{G,q}}{(q-1)^v} q^{nv} \Big(1 + O_{G,q}(n^d q^{-n}) + O_{G,q}(q^{-(1-\varepsilon)n})\Big). \tag{1.2}$$

where

$$\rho_{G,q} = \prod_{\substack{P \in \mathbb{F}_q[z] \\ P \text{ irreducible}}} Q_G(q^{-\deg(P)}). \tag{1.3}$$

The dependence of the constants in the O symbols on G and q may be given

explicitly. Namely,

$$O_{G,q}(n^d q^{-n}) = \frac{\exp(d)2^{2^e}(q-1)v}{\rho_{G,q}} O(n^d q^{-n})$$

and

$$O_{G,q}(q^{-(1-\varepsilon)n}) = \frac{3}{\rho_{G,q}} \Big(\sum_{j=1}^{e} \rho^+_{G'_j,q} \Big) O(q^{-(1-\varepsilon)n}),$$

where the constants in the new O terms are absolute,

$$\rho^+_{G,q} = \prod_P Q^+_G(q^{-\deg(P)}) \tag{1.4}$$

and G'_j is the graph obtained from G by removing the edge j.

We make some comments about $\rho_{G,q}$. Letting $p(n)$ represent the total number of v-tuples of monic polynomials in $\mathbb{F}_q[x]$ of degree less than equal to n, we observe that

$$|p(n)| = \left(\frac{q^n - 1}{q-1} \right)^v.$$

Thus, the density of v-tuple of polynomials in $\mathbb{F}_q[x]$ that are monic and have the coprimality conditions induced by graph G is given by

$$\lim_{n\to\infty} \frac{g(n)}{p(n)} = \rho_{G,q}.$$

The formula for the density, $\rho_{G,q}$, is explicit. In [1, Section 4] we outlined the calculations for the density of 4-tuples of integers with given pairwise coprimality conditions. The calculations to obtain $\rho_{G,q}$ in the case of polynomials in finite fields can be approached in the same way. In fact the calculations to obtain $\rho_{G,q}$ in (1.4) are easier. We can group the polynomials by degree, since each polynomial of a given degree contributes in the identical way in the product formula for $\rho_{G,q}$.

1.1 Notation

$\subset$ is used to indicate subset, including the equality case.

$\mathcal{D}$ is a Dedekind domain with the finite norm property.

$I(\mathcal{D})$ is the set of non-null ideals in $\mathcal{D}$.

$\mathcal{R}(\mathcal{D})$ is the the ring of ideals defined in Section 2.1. Its elements include Z, Z^+ and W.

X, Y are sets of tuples of polynomials.

$|X|$ is the cardinality of the set X.

$G = (V, E)$ is a graph with set of vertices V and edges E.

Q usually runs over non-null ideals in $\mathcal{D}$. In the case $\mathcal{D} = \mathbb{F}_q[z]$, the ring of polynomials with coefficients in the Galois field $\mathbb{F}_q[z]$, these ideals can be identified with monic polynomials.

A, B, R, S and occasionally other variables denote non-null ideals on $\mathcal{D}$.

P are prime ideals in $\mathcal{D}$ or monic irreducible polynomials when $\mathcal{D} = \mathbb{F}_q[z]$.

$\omega(Q)$ denotes the number of distinct primes dividing the ideal Q. Or the number of distinct monic irreducible polynomials dividing the polynomial Q when $\mathcal{D} = F_Q[z]$.

$\mu(Q)$ denotes 0 if the ideal Q is divisible by P^2 (the square of some prime ideal) or $(-1)^{\omega(Q)}$ if Q is squarefree. In the case of monic polynomials we define $\mu(Q)$ analogously.

$\omega(q^n)$ denotes the number of monic polynomials of degree less than or equal to n in $F_q[z]$, (see definition 3.3).

$\mathcal{N}(Q)$ is the norm of the ideal Q, that is, $\mathcal{N}(Q) = |\mathcal{D}/Q|$. If $\mathcal{D} = \mathbb{F}_q[z]$ then $\mathcal{N}(Q)$ is also equal to $q^{\deg Q}$.

r, s are vertices of G, so that $1 \leq r, s \leq v$.

$\{r, s\}$ is a typical edge of the graph G.

d denotes the maximum degree of the vertices of G.

e denotes the number of edges of G.

2 Problem setting

The general setting of our problem refers to a Dedekind domain [9, Chap. 1]. We recall that in a Dedekind domain, $\mathcal{D}$, every nonzero ideal Q has a unique factorization of prime ideals $Q = P_1^{\alpha_1} \cdots P_k^{\alpha_k}$. We also require that each ideal in $\mathcal{D}$ has a finite norm. That is, $\mathcal{N}(Q) := |\mathcal{D}/Q| < \infty$. These Dedekind domains with finite norm property are considered in [9, p. 11]. The norm is multiplicative $\mathcal{N}(Q_1 Q_2) = \mathcal{N}(Q_1)\mathcal{N}(Q_2)$, and for any given positive real number x the number of ideals Q with $\mathcal{N}(Q) \leq x$ is finite.

Our main example is the ring of polynomials with coefficients in a Galois field $\mathcal{D} = \mathbb{F}_q[z]$. But there is also another important case when $\mathcal{D}$ is the ring of integers of a number field.

For any graph $G = (V, E)$ we seek an estimate of the cardinality of the set

$$G_{\mathcal{D}}(x) = \{(Q_1, \ldots, Q_v) \in I(\mathcal{D})^v : \mathcal{N}(Q_r) \leq x, \gcd(Q_r, Q_s) = 1 \text{ if } \{r, s\} \in E\}.$$

2.1 The ring of ideals

As a tool in our reasoning we consider formal sums of the type

$$\sum_{Q\in I(\mathcal{D})} \frac{n(Q)}{Q},$$

where the coefficients $n(Q)$ are real (or complex) numbers. We define two operations, sum and product, by the rules

$$\Big(\sum_{Q\in I(\mathcal{D})} \frac{n(Q)}{Q}\Big) + \Big(\sum_{Q\in I(\mathcal{D})} \frac{m(Q)}{Q}\Big) = \Big(\sum_{Q\in I(\mathcal{D})} \frac{n(Q)+m(Q)}{Q}\Big)$$

and

$$\Big(\sum_{Q\in I(\mathcal{D})} \frac{n(Q)}{Q}\Big)\Big(\sum_{Q\in I(\mathcal{D})} \frac{m(Q)}{Q}\Big) = \sum_{Q\in I(\mathcal{D})} \frac{1}{Q}\Big(\sum_{BC=Q} n(B)m(C)\Big).$$

Since there is only a finite set of pairs of ideals with $BC = Q$ the product is well defined. It is clear that this makes the set of these sums, $\mathcal{R}(\mathcal{D})$, a ring.

A particular element of this ring is Z is given by

$$Z = \sum_{Q} \frac{1}{Q}.$$

The unique factorization of ideals in a Dedekind ring gives us

$$Z = \sum_{Q} \frac{1}{Q} = \prod_{P}\Big(1 + \frac{1}{P} + \frac{1}{P^2} + \cdots\Big).$$

Here P runs through the prime ideals. To give a meaning to the infinite product we may consider simply the product topology in $\mathbb{R}^{I(\mathcal{D})}$ of the discrete topology in $\mathbb{R}$.

We will write

$$\Big(\sum_{Q\in I(\mathcal{D})} \frac{n(Q)}{Q}\Big) \lhd \Big(\sum_{Q\in I(\mathcal{D})} \frac{m(Q)}{Q}\Big) \tag{2.1}$$

to denote that for any ideal Q we have $n(Q) \le m(Q)$.

Observe that for any $\sigma > 0$ we obtain from (2.1) that, when the series converge,

$$\Big(\sum_{Q\in I(\mathcal{D})} \frac{n(Q)}{\mathcal{N}(Q)^\sigma}\Big) \le \Big(\sum_{Q\in I(\mathcal{D})} \frac{m(Q)}{\mathcal{N}(Q)^\sigma}\Big).$$

We will use the notation

$$\mathcal{N}^\sigma\Big(\sum_{Q\in I(\mathcal{D})} \frac{n(Q)}{Q}\Big)$$

to denote

$$\Big(\sum_{Q\in I(\mathcal{D})}\frac{n(Q)}{\mathcal{N}(Q)^\sigma}\Big).$$

In particular $\mathcal{N}^\sigma(Z)$ is the Dedekind zeta function in the case of a number field. Notice that $\mathcal{N}^\sigma(XY)=\mathcal{N}^\sigma(X)\mathcal{N}^\sigma(Y)$ for any X, $Y\in\mathcal{R}(\mathcal{D})$.

2.2 The particular case of polynomials in finite fields

Our reasoning depends heavily on the function $f(x)$ that counts the number of ideals of $\mathcal{D}$ having norm $\leq x$. This function behaves very differently in the case of polynomials and for the integers of a number field. So that in spite of our arguments being general we consider here only the case of $\mathcal{D}=\mathbb{F}_q[z]$.

Therefore for us $\mathcal{D}=\mathbb{F}_q[z]$ and in this case each non-null ideal is generated by a unique monic polynomial. Therefore we speak of ideals or monic polynomials indistinctly and use the letter Q to denote them. The norm of a ideal Q depends only on the degree of the corresponding polynomial. Specifically, $\mathcal{N}(Q)=q^r$ if $\deg(Q)=r$. Therefore instead of consider tuples of polynomials with $\mathcal{N}(Q)\leq x$ we will consider tuples of polynomials of degree $\deg(Q)\leq n$.

In the rest of the paper we have fixed a graph $G=(V,E)$, a natural number n and a Dedekind ring $\mathcal{D}=\mathbb{F}_q[z]$ where q is a fixed prime power. With these elements we construct a general set of tuples

$$X=X(n)=\{(Q_1,\ldots,Q_v)\in\mathbb{F}_q[z]^v\colon\ \deg(Q_r)\leq n, 1\leq r\leq v\},\tag{2.2}$$

and a set of tuples satisfying the coprimality conditions

$$Y=Y_G(n)=\{(Q_1,\ldots,Q_v)\in X\colon\ \gcd(Q_r,Q_s)=1 \text{ for any edge } \{r,s\}\in E\}\tag{2.3}$$

We are interested in $g(n)=|Y_G(n)|$.

3 Exact formula for the number of tuples satisfying the coprimality conditions

We give here a general formula to compute $g(x)$ in the case where $\mathcal{D}=\mathbb{F}_q[z]$. We begin with two definitions.

Definition 3.1. *Given the graph $G=(V,E)$, an* edge labeling *is a tuple $(Q_1,\ldots,Q_e)$ of non-null ideals in $\mathcal{D}$, associating an ideal Q_a to each edge $a\in E$. Analogously we consider* vertex labelings. *These are associations $(Q_1,\ldots,Q_v)$ of an ideal Q_j for each vertex $j\in V$.*

Frequently (see, for example, the proof of Lemma 4.3) we start with an edge labeling $(N_1,\ldots,N_e)$ and associate to it a vertex labeling $(M_1,\ldots,M_v)$ in the following way.

Definition 3.2. *Given an edge labeling* $(N_1, \dots, N_e)$ the associated vertex labeling $(M_1, \dots, M_v)$ *is defined by*

$$M_r = \operatorname{lcm}\{N_a : \text{ the edge } a = \{r, s\} \text{ joins the vertex } r \text{ with any other one } s\}, \tag{3.1}$$

where $\operatorname{lcm}(\emptyset) = 1$.

We introduce some notation for the number of monic polynomials of degree m or less.

Definition 3.3. *Let*

$$w(q^m) = \begin{cases} 0 & m < 0, \\ \frac{q^{m+1}-1}{q-1} & m \geq 0. \end{cases}$$

Any time we use the notations N_a and M_j we assume that $(M_1, \dots, M_v)$ is the associated vertex labelling to the edge labeling $(N_1, \dots, N_e)$.

The general formula for $g(x)$ will be an application of the Principle of inclusion-exclusion.

Theorem 3.4 (Principle of inclusion-exclusion)**.** *Let* X *be a finite set and let* Y_j *be subsets of* X *for* $1 \leq j \leq n$. *Then*

$$\Big| X \smallsetminus \bigcup_{j=1}^{n} Y_j \Big| = \sum_{J \subset \{1,2,\dots,n\}} (-1)^{|J|} |Y_J|,$$

where $Y_J = X$ *for* $J = \emptyset$ *and* $Y_J = \bigcap_{j \in J} Y_j$ *for* $J \neq \emptyset$.

Lemma 3.5. *Consider the graph* $G = (V, E)$ *and the natural number* n.

Then $g(n)$, *the number of tuples of polynomials* $(Q_1, \dots, Q_v)$ *of degree* $\leq n$ *satisfying the coprimality conditions imposed by* G, *is given by the expression*

$$g(n) = \sum_{\substack{(N_1,\dots,N_e) \\ \deg(N_e) \leq n}} \mu(N_1) \cdots \mu(N_e) \prod_{r=1}^{v} w(q^n / q^{\deg(M_r)}). \tag{3.2}$$

Proof. We have a graph $G = (V, E)$ as described in Section 2. We start with the set of all tuples of polynomials X defined in (2.2) We want to define subsets Y_j of X so that the difference

$$X \smallsetminus \bigcup_{j=1}^{n} Y_j$$

is the set Y defined in (2.3), so that $g(n) = |Y|$.

If an element $(Q_1, \dots, Q_v) \in X$ is not in Y there is an edge $e = \{r, s\}$ in G such that $\gcd(Q_r, Q_s) \neq 1$. Then there is an irreducible monic polynomial P such that $P \mid Q_r$ and $P \mid Q_s$. Obviously this polynomial P will be of degree less than or equal to n.

Therefore we define a set $Y_{(P,e)}$ for any irreducible polynomial P of degree $\leq n$ and any edge $e = \{r, s\}$ of G by

$$Y_{(P,e)} = \{(Q_1, \ldots, Q_v) \in X : P \mid Q_r \text{ and } P \mid Q_s\}.$$

With these definitions it is clear that

$$Y = X \setminus \bigcup_{P,e} Y_{(P,e)}.$$

To apply the principle of inclusion-exclusion we consider the intersection

$$Y_J = \bigcap_{j=1}^{m} Y_{(P_j,e_j)}, \qquad J = \{(P_1, e_1), \ldots, (P_m, e_m)\}$$

of a finite set of subsets $Y_{(P,e)}$.

A tuple $(Q_1, \ldots, Q_v) \in X$ is in the intersection Y_J if and only if $P_j \mid Q_{r_j}$ and $P_j \mid Q_{s_j}$ for any of the edges $e_j = \{r_j, s_j\}$. For any edge e let $N_e = \operatorname{lcm}\{P\colon (P, e) \in J\}$ with $N_e = 1$ if the set $\{P\colon (P, e) \in J\}$ is empty. In this way, given J, we have associated a monic polynomial to any edge in E. With this notation it is obvious that a tuple $(Q_1, \ldots, Q_v) \in X$ is in the intersection Y_J if and only if $N_e \mid Q_r$ and $N_e \mid Q_s$ for any edge $e = \{r, s\} \in E$. Notice that the polynomials N_e associated in this way to a given J are squarefree, because they are the least common multiple of a set of irreducible polynomials. We note that J determines the monic squarefree polynomials $N_1, \ldots, N_e$; one for each edge in E whose factors are all of degree less than or equal n. Conversely, the monic squarefree polynomials $N_1, \ldots, N_e$, one for each edge in e whose factors are all of degree less than or equal n, determines J.

Looking at it in another way the polynomial Q_r associated to a given vertex r needs to be divisible by $N_{e_1}, \ldots, N_{e_\ell}$ if e_j are the edges joining the vertex r with some other (it maybe none, $\ell = 0$ when the vertex is isolated). The condition on Q_r is equivalent to $M_r \mid Q_r$, where $M_r = \operatorname{lcm}(N_{e_1}, \ldots, N_{e_\ell})$ (taking $\operatorname{lcm}(\emptyset) = 1$, in the case where there is no condition on Q_r). Thus, associated to the given finite set J of pairs (P, e) we have associated a tuple of polynomials $(M_1, \ldots, M_v)$ such that

$$Y_J = \bigcap_{j=1}^{m} Y_{(P_j,e_j)} = \{(Q_1, \ldots, Q_v) \in X\colon M_r \mid Q_r, 1 \leq r \leq v\}.$$

Notice that the polynomials M_r associated in this way to a given J are squarefree because they are the least common multiple of a set of squarefree polynomials.

The tuple of monic polynomials $(Q_1, \ldots, Q_v)$ is in Y_J if each component Q_r satisfies two conditions. Firstly, $\deg(Q_r) \leq n$ for Q_r to be in X, and secondly $M_r \mid Q_r$ for Q_r to be in Y_J. These conditions will be satisfied by any product $M_r A$ of M_r with any monic polynomial A such that $\deg(M_r) + \deg(A) \leq n$. Therefore if $\deg(M_r) > n$, there is no possible Q_r. When $\deg(M_r) \leq n$ let

$m = n - \deg(M_r)$. Then A can be any monic polynomial of degree $\leq m$. The number of possible polynomials A, and therefore the number of possible Q_r, are

$$1 + q + q^2 + \cdots + q^m = \frac{q^{m+1} - 1}{q - 1}.$$

With these notation the cardinality of Y_J can be computed as

$$|Y_J| = \prod_{r=1}^{v} w(q^n / q^{\deg(M_r)}),$$

where the w function is as shown in Definition 3.3. We now compute $|J|$. This is the total number of prime factor across all the N_j. As mentioned before N_j is squarefree, so

$$(-1)^{|J|} = (-1)^{\sum_{j=1}^{e} \omega(N_j)} = \mu(N_1) \cdots \mu(N_e).$$

Therefore the Principle of inclusion-exclusion yields

$$g(n) = |Y| = \sum_{N_1} \cdots \sum_{N_e} \mu(N_1) \cdots \mu(N_e) \prod_{r=1}^{v} w(q^n / q^{\deg(M_r)}),$$

where the summations are over all monic squarefree polynomials N_j with irreducible factors of degree $\leq n$. We notice that if some N_j have an irreducible factor of degree $> n$, then some M_r will have a degree $> n$ and the corresponding sum will then be zero because the factor $w(q^n / q^{\deg(M_r)})$ will equal zero. Also, if some N_j is not squarefree the factor $\mu(N_j) = 0$.

Therefore the sum with the restricted conditions on N_j will be the same as the sum extended on all polynomials. In fact we may restrict the summation to the N_j of degree $\leq n$, because otherwise there is a factor $w(q^n / q^{\deg(M_r)}) = 0$ in the corresponding term. This proves equation (3.2). □

4 Main part of the asymptotic formula

We now establish the asymptotic formula in the main theorem. We begin by establishing the main term and the error term of $g(n)$. The main part of $w(q^m)$ is $u(q^m) := \frac{q^{m+1}}{q-1}$. We define the error term $v(q^m)$ as the difference, so that for any integer m we have

$$w(q^m) = u(q^m) + v(q^m). \tag{4.1}$$

We will need the following properties of $u(q^m)$ and $v(q^m)$:

Lemma 4.1. *(a) For all integers $m \in \mathbb{Z}$ we have $|v(q^m)| \leq 1$.*

(b) For all integers $m \in \mathbb{Z}$ we have $|w(q^m)| \leq u(q^m)$.

Proof. For $m < 0$ we have $w(q^m) = 0$ and therefore $u(q^m) = \frac{q^{m+1}}{q-1} = -v(q^m)$. Since $m + 1 \le 0$, we have $|v(q^m)| = \frac{q^{m+1}}{q-1} \le \frac{1}{q-1} \le 1$. Also, in the case $m < 0$ we have $|w(q^m)| = 0 \le u(q^m)$.

For $m \ge 0$ we have $w(q^m) = \frac{q^{m+1}-1}{q-1}$, $u(q^m) = \frac{q^{m+1}}{q-1}$ and therefore $v(q^m) = -\frac{1}{q-1}$. So that $|v(q^m)| = \frac{1}{q-1} \le 1$. On the other hand $|w(q^m)| = w(q^m) = \frac{q^{m+1}-1}{q-1} < u(q^m)$. □

To separate the main part in the sum (3.2) we will use the following simple lemma, easily proved by induction.

Lemma 4.2. *Let $w_r = u_r + v_r$ for $1 \le r \le R$ be elements of any ring, then*

$$\prod_{r=1}^{R} w_r = \prod_{r=1}^{R} u_r + \sum_{s=1}^{R}\Big(v_s \cdot \prod_{j=1}^{s-1} u_j \cdot \prod_{j=s+1}^{R} w_j\Big), \tag{4.2}$$

where the empty products are equal to 1.

We can now establish the following.

Lemma 4.3. *The number $g(n)$, of tuples $(Q_1, \dots, Q_v)$ with $\deg(Q_a) \le n$ satisfying the conditions of coprimality given by the graph G, is given by*

$$g(n) = \Big(\frac{q^n}{q-1}\Big)^v \sum_{\substack{(N_1,\dots,N_e)\\ \deg(N_a)\le n}} \frac{\mu(N_1)\cdots\mu(N_e)}{q^{m_1}\cdots q^{m_v}} + \sum_{k=1}^{v} R_k, \tag{4.3}$$

where $m_r = \deg(M_r)$.

The error terms R_k are bounded by

$$|R_k| \le \Big(\frac{q^n}{q-1}\Big)^{v-1} \sum_{\substack{(N_1,\dots,N_e)\\ \deg(N_a)\le n}} \frac{|\mu(N_1)\cdots\mu(N_e)|}{q^{m_1}\cdots\widehat{q^{m_k}}\cdots q^{m_v}}, \tag{4.4}$$

where $\widehat{q^{m_k}}$ indicates that this factor is omitted.

Proof. Applying Lemma 4.2 to the exact expression of $g(n)$ in (3.2) and using

the decomposition $w(q^m) = u(q^m) + v(q^m)$ we obtain, with $m_r := \deg M_r$,

$$\begin{aligned}
g(n) = &\sum_{\substack{(N_1,\dots,N_e)\\ \deg(N_a)\le n}} \mu(N_1)\cdots\mu(N_e)\prod_{r=1}^{v} u\Big(\frac{q^n}{q^{m_r}}\Big)\\
&+\sum_{\substack{(N_1,\dots,N_e)\\ \deg(N_a)\le n}} \mu(N_1)\cdots\mu(N_e)v\Big(\frac{q^n}{q^{m_1}}\Big)\prod_{r=2}^{v} w\Big(\frac{q^n}{q^{m_r}}\Big)\\
&+\sum_{\substack{(N_1,\dots,N_e)\\ \deg(N_a)\le n}} \mu(N_1)\cdots\mu(N_e)u\Big(\frac{q^n}{q^{m_1}}\Big)v\Big(\frac{q^n}{q^{m_2}}\Big)\prod_{r=3}^{v} w\Big(\frac{q^n}{q^{m_r}}\Big)\\
&\cdots\\
&+\sum_{\substack{(N_1,\dots,N_e)\\ \deg(N_a)\le n}} \mu(N_1)\cdots\mu(N_e)u\Big(\frac{q^n}{q^{m_1}}\Big)\cdots v\Big(\frac{q^n}{q^{m_{v-1}}}\Big)w\Big(\frac{q^n}{q^{m_v}}\Big)\\
&+\sum_{\substack{(N_1,\dots,N_e)\\ \deg(N_a)\le n}} \mu(N_1)\cdots\mu(N_e)u\Big(\frac{q^n}{q^{m_1}}\Big)\cdots u\Big(\frac{q^n}{q^{m_{v-1}}}\Big)v\Big(\frac{q^n}{q^{m_v}}\Big)\\
&=\sum_{\substack{(N_1,\dots,N_e)\\ \deg(N_a)\le n}} \mu(N_1)\cdots\mu(N_e)\prod_{r=1}^{v} u\Big(\frac{q^n}{q^{m_r}}\Big)+\sum_{k=1}^{v} R_k, \qquad (4.5)
\end{aligned}$$

where for $1 \le k \le v$,

$$\begin{aligned}
R_k = &\sum_{\substack{(N_1,\dots,N_e)\\ \deg(N_a)\le n}} \mu(N_1)\cdots\mu(N_e)\cdot\\
&u\Big(\frac{q^n}{q^{m_1}}\Big)\cdots u\Big(\frac{q^n}{q^{m_{k-1}}}\Big)v\Big(\frac{q^n}{q^{m_k}}\Big)w\Big(\frac{q^n}{q^{m_{k+1}}}\Big)\cdots w\Big(\frac{q^n}{q^{m_v}}\Big).
\end{aligned}$$

Since $u(q^m) = \frac{q^m}{q-1}$ the main term can be written as

$$\begin{aligned}
&\sum_{\substack{(N_1,\dots,N_e)\\ \deg(N_a)\le n}} \mu(N_1)\cdots\mu(N_e)\prod_{r=1}^{v} u\Big(\frac{q^n}{q^{m_r}}\Big)\\
&\qquad = \Big(\frac{q^n}{q-1}\Big)^v \sum_{\substack{(N_1,\dots,N_e)\\ \deg(N_a)\le n}} \frac{\mu(N_1)\cdots\mu(N_e)}{q^{m_1+\cdots+m_v}}
\end{aligned}$$

On the other hand, thanks to Lemma 4.1, the error term can be bounded by

$$|R_k| \le \sum_{\substack{(N_1,\dots,N_e)\\ \deg(N_a)\le n}} |\mu(N_1)\cdots\mu(N_e)| \prod_{\substack{1\le r\le v\\ r\ne k}} \Big|u\Big(\frac{q^n}{q^{m_r}}\Big)\Big|$$

The factor k is missing because $|v(q^m)| \leq 1$. Therefore we obtain

$$|R_k| \leq \Big(\frac{q^n}{q-1}\Big)^{v-1} \sum_{\substack{(N_1,\dots,N_e)\\ \deg(N_a)\leq n}} \frac{|\mu(N_1)\cdots\mu(N_e)|}{q^{m_1}\cdots\widehat{q^{m_k}}\cdots q^{m_v}},$$

which completes the proof. □

5 The coefficient of the main term

We consider now the coefficient

$$\sum_{\substack{(N_1,\dots,N_e)\\ \deg(N_a)\leq n}} \frac{\mu(N_1)\cdots\mu(N_e)}{q^{m_1}\cdots q^{m_v}}$$

of our first expression (4.3) for $g(n)$. It is clear that the number of terms added increases with n. We will see that the sum has a limit when $n \to \infty$. We require some results regarding certain multiplicative functions.

5.1 Multiplicative functions in Dedekind domains

In this section we assume, given a Dedekind domain $\mathcal{D}$ with the finite norm property, that $I(\mathcal{D})$ is the set of non-null ideals in $\mathcal{D}$ and $\mathcal{R}(\mathcal{D})$ is the ring of ideals defined in Section 2.1. Also $G = (V, E)$ is a given finite graph as in Section 2.

Definition 5.1. *A function $f\colon I(\mathcal{D}) \to \mathbb{C}$ defined on the set of non-null ideals, is* multiplicative *if for any relatively prime pair of ideals Q, R we have $f(QR) = f(Q)f(R)$.*

One important example is the Möbius function $\mu(Q) = (-1)^{\omega(Q)}$ when Q is the product of $\omega(Q)$ different primes ideals, and $\mu(Q) = 0$ if there is a prime P with $P^2 \mid Q$. An ideal Q with $|\mu(Q)| = 1$ is called *squarefree*. It is well known that

Lemma 5.2 (Euler product)**.** *Let $f\colon I(\mathcal{D}) \to \mathbb{C}$ be a multiplicative function. We have the identity*

$$\sum_Q \frac{f(Q)}{Q} = \prod_P \Big(1 + \frac{f(P)}{P} + \frac{f(P^2)}{P^2} + \cdots\Big). \tag{5.1}$$

We recall that we are considering in $\mathcal{R}(\mathcal{D})$ the product topology of $\mathbb{C}^{I(\mathcal{D})}$ giving to $\mathbb{C}$ the discrete topology. The important thing for us is that this implies the equality

$$\sum_Q \frac{f(Q)}{\mathcal{N}(Q)} = \prod_P \Big(1 + \frac{f(P)}{\mathcal{N}(P)} + \frac{f(P^2)}{\mathcal{N}(P)^2} + \cdots\Big), \tag{5.2}$$

when one of the two sides of the equation converges absolutely.

5.2 Multiplicative functions associated to a graph

Lemma 5.3. *Let $f\colon I(\mathcal{D}) \to \mathbb{C}$ be a multiplicative function, G a graph and r a vertex in G. Then the two functions $g_{G,f}$ and $g^r_{G,f}\colon I(\mathcal{D}) \to \mathbb{C}$, defined by*

$$g_{G,f}(Q) = \sum_{\substack{(N_1,\dots,N_e)\\ M_1\cdots M_v = Q}} f(N_1)\cdots f(N_e) \tag{5.3}$$

and (5.4)

$$g^r_{G,f}(Q) = \sum_{\substack{(N_1,\dots,N_e)\\ M_1\cdots \widehat{M_r}\cdots M_v = Q}} f(N_1)\cdots f(N_e), \tag{5.5}$$

are multiplicative.

Proof. Consider the second function (the other is analogous and simpler). First we show that the sum defining $g^r_{G,f}(Q)$ is finite. Let $(N_1,\dots,N_e)$ be an edge labeling such that $M_1\cdots\widehat{M_r}\cdots M_v = Q$. Any edge a contains a vertex $s \neq r$, therefore $N_a \mid M_s$ and therefore $N_a \mid Q$. Therefore the sum can be restricted to edge labelings formed with divisors of Q. These are of finite number. Therefore the two functions are well defined.

Consider now an edge labelling $(N_1,\dots,N_e)$ such that $M_1\cdots\widehat{M_r}\cdots M_v = Q_1Q_2$ with $\gcd(Q_1,Q_2)=1$. By the previous reasoning we have $N_a \mid Q_1Q_2$ for any edge a. Therefore we can find another two edge labelings $(N_{1,1},\dots,N_{1,e})$ and $(N_{2,1},\dots,N_{2,e})$ such that $N_{1,a} \mid Q_1$, $N_{2,a} \mid Q_2$ and $N_{1,a}N_{2,a} = N_a$, for any edge a. It is easy to see that in this case (with $\gcd(Q_1,Q_2)=1$) we have $M_s = M_{1,s}M_{2,s}$ for any vertex s, and

$$M_{1,1}\cdots\widehat{M_{1,r}}\cdots M_{1,v} = Q_1, \quad M_{2,1}\cdots\widehat{M_{2,r}}\cdots M_{2,v} = Q_2.$$

Analogously if we start with two edge labelings $(N_{i,1},\dots,N_{i,e})$ for $i=1,\,2$, satisfying the above relations, the edge labeling formed with $N_a = N_{1,a}N_{2,1}$ will satisfy $M_1\cdots\widehat{M_r}\cdots M_v = Q_1Q_2$. Notice also that since $\gcd(N_{1,a},N_{2,a})=1$ we have $f(N_a) = f(N_{1,a})f(N_{2,a})$.

Therefore

$$g^r_{G,f}(Q_1Q_2) = \sum_{\substack{(N_1,\dots,N_e)\\ M_1\cdots\widehat{M_r}\cdots M_v = Q}} f(N_1)\cdots f(N_e) =$$

$$\sum_{\substack{(N_{1,1},\dots,N_{1,e})\\ M_{1,1}\cdots\widehat{M_{1,r}}\cdots M_{1,v}=Q_1}} f(N_{1,1})\cdots f(N_{1,e}) \sum_{\substack{(N_{2,1},\dots,N_{2,e})\\ M_{1,1}\cdots\widehat{M_{2,r}}\cdots M_{2,v}=Q_2}} f(N_{2,1})\cdots f(N_{2,e}).$$

In other words $g^r_{G,f}(Q_1Q_2) = g^r_{G,f}(Q_1)g^r_{G,f}(Q_2)$. □

We will need to consider the case of the multiplicative functions $f = \mu$ or

$f = |\mu|$. Therefore we define

$$f_G(Q) := \sum_{\substack{(N_1,\dots,N_e)\\ M_1\cdots M_v = Q}} \mu(N_1)\cdots\mu(N_e),$$

$$f_G^+(Q) := \sum_{\substack{(N_1,\dots,N_e)\\ M_1\cdots M_v = Q}} |\mu(N_1)\cdots\mu(N_e)|$$

$$g_{G,r}(Q) := \sum_{\substack{(N_1,\dots,N_e)\\ M_1\cdots \widehat{M_r}\cdots M_v = Q}} \mu(N_1)\cdots\mu(N_e),$$

$$g_{G,r}^+(Q) := \sum_{\substack{(N_1,\dots,N_e)\\ M_1\cdots \widehat{M_r}\cdots M_v = Q}} |\mu(N_1)\cdots\mu(N_e)|$$

By Lemma 5.3 these four functions are multiplicative so that their values are determined by their values in powers P^n of prime ideals P. It is very easy to see that these values $f_G(P^n)$, $f_G^+(P^n)$, $g_G(P^n)$, $g_G^+(P^n)$ are rational integers independent of the special Dedekind domain, because the divisors of P^n are 1, P, P^2, …, P^n in any Dedekind domain.

In [1], using slightly different notation, we considered two polynomials associated to a graph G. Namely,

$$Q_G(z) = \sum_{F\subset E} (-1)^{|F|} z^{|v(F)|}, \quad Q_G^+(z) = \sum_{F\subset E} z^{|v(F)|}, \tag{5.6}$$

where $v(F) = \cup_{\{r,s\}\in\mathbb{F}}\{r,s\}$; the set of all vertices adjacent to edges contained in F. We proved

Lemma 5.4. *For any graph G and prime P the value $f_G(P^k)$ (respectively of $f_G^+(P^k)$) is equal to the coefficient of z^k in the polynomial $Q_G(z)$, (respectively in the polynomial $Q_G^+(z)$).*

In particular we have $f_G(P) = f_G^+(P) = 0$.

To study the two functions $g_{G,r}$ and $g_{G,r}^+$ we introduce two other polynomials,

$$Q_{G,r}(z) = \sum_{F\subset E} (-1)^{|F|} z^{|v(F)\smallsetminus\{r\}|}, \quad Q_{G,r}^+(z) = \sum_{F\subset E} z^{|v(F)\smallsetminus\{r\}|}. \tag{5.7}$$

Lemma 5.5. *Let G be a graph and r one of its vertices. For any prime P the value $g_{G,r}(P^k)$ (respectively $g_{G,r}^+(P^k)$) is equal to the coefficient of z^k in the polynomial $Q_{G,r}(z)$ (respectively in the polynomial $Q_{G,r}^+(z)$).*

In particular we have $g_{G,r}^+(P) = -g_{G,r}(P) = d_r$, where d_r is the degree of the vertex r and $g_{G,r}^+(P^m) = -g_{G,r}(P^m) = 0$ for $m \geq v$.

Proof. Consider, for example, the case of $g_{G,r}(P^k)$. By definition

$$g_{G,r}(P^k) := \sum_{\substack{(N_1,\dots,N_e)\\ M_1\cdots \widehat{M_r}\cdots M_v = P^k}} \mu(N_1)\cdots\mu(N_e).$$

Any edge labeling $(N_1, \ldots, N_e)$ giving a non-null term satisfies $N_j \mid P^k$ for $1 \leq j \leq e$. Therefore for each j we have $N_j = 1$ or $N_j = P$. In this way each non-null term is associated bijectively to a subset $F \subset E$: the set of j for which $N_j = P$. In this case $\mu(N_1) \cdots \mu(N_e) = (-1)^{|F|}$. The elements of the corresponding vertex labelling $(M_1, \ldots M_v)$ satisfies also $M_s = 1$ or $M_s = P$. Precisely $M_s = P$ if $s \in v(F)$. Since $M_1 \cdots \widehat{M_r} \cdots M_v = P^k$ we have $k = |v(F) \smallsetminus \{r\}|$. It follows that $g_{G,r}(P^k)$ is the coefficient of the polynomial $Q_{G,r}(z)$.

We have $|v(F) \smallsetminus \{r\}| = 1$ just in the case F consists only of an edge $e = \{r, s\}$ with an extreme equal to r. There are precisely d_r such edges. Therefore the term of first degree in $Q^+_{G,r}(z)$ is d_r. In the case of $Q_{G,r}(z)$ these same terms appear with a factor $(-1)^{|F|} = -1$.

Finally notice that $|v(F) \smallsetminus \{r\}| \leq v - 1$. Therefore this is the maximum degree of any term of the polynomials $Q_{G,r}(z)$ and $Q^+_{G,r}(z)$. □

5.3 A particular multiplicative function

We define a function that we will use later in the bound of the error terms in our approximation to $g(n)$.

Definition 5.6. *Let $G = (V, E)$ be a graph that has two vertices $r \neq s$ with r, $s \in V$, that are not joined by an edge. That is, $\{r, s\} \notin E$ We define a function $f_{r,s} \colon I(\mathcal{D}) \to \mathcal{R}(\mathcal{D})$ from the ideals to the ring of ideals by*

$$f_{r,s}(Q) = \sum_{\substack{(N_1,\ldots,N_e) \\ N_j \mid Q}} \frac{|\mu(N_1) \cdots \mu(N_e)|}{M_1 \cdots \widehat{M_r} \cdots \widehat{M_s} \cdots M_v}. \tag{5.8}$$

We sum on all edge labeling formed with divisors of Q and we omit the two factors M_r and M_s corresponding to the vertices of the pair $\{r, s\}$.

Lemma 5.7. *The function $f_{r,s}(Q)$ is multiplicative. That is,* $\gcd(Q_1, Q_2) = 1$ *implies $f_{r,s}(Q_1 Q_2) = f_{r,s}(Q_1) f_{r,s}(Q_2)$.*

Proof. If we assume $\gcd(Q_1, Q_2) = 1$, then any edge labeling $(N_1, \ldots, N_e)$ with $N_j \mid Q_1 Q_2$ can be obtained in a unique way from two edge labelings $(N_{1,1}, \ldots, N_{1,e})$ and $(N_{2,1}, \ldots, N_{2,e})$ with $N_{i,j} \mid Q_i$ by the equations $N_j = N_{1,j} N_{2,j}$. The corresponding vertex labeling then satisfies $M_j = M_{1,j} M_{2,j}$, and the result follows. □

Lemma 5.8. *Let $Q_{r,s}(z)$ be the polynomial*

$$Q_{r,s}(z) = \sum_{F \subset E} z^{|v(F) \smallsetminus \{r,s\}|}. \tag{5.9}$$

For any natural number m and prime ideal P we have

$$f_{r,s}(P^m) = f_{r,s}(P) = Q_{r,s}\Big(\frac{1}{P}\Big). \tag{5.10}$$

Proof. In the definition of $f_{r,s}(P^m)$ we have to sum for each edge labeling $(N_1, \dots, N_e)$ of G, where $N_j \mid P^m$. Each term of the sum has a coefficient $|\mu(N_1)\cdots\mu(N_e)|$. Therefore we have only to consider the term with $N_j = 1$ or $N_j = P$. Any such labeling is determined by the set $F = \{j \colon 1 \le j \le e, N_j = P\}$. Therefore each non-null term corresponds to a subset $F \subset E$. It is clear that for this labeling the corresponding vertex labeling $(M_1, \dots, M_v)$ will have $M_t = 1$ or $M_t = P$. Precisely the set $v(F) = \cup_{\{t_1,t_2\}\in F}\{t_1, t_2\}$ coincides with the set of vertices t with $M_t = P$. Therefore the corresponding term is equal to $1/P^{|v(F)\smallsetminus\{r,s\}|}$.

After this reasoning it is clear that we have (5.10). □

We will also need the following.

Lemma 5.9. *We have*

$$f_{r,s}(P) = 1 + \frac{a_1}{P} + \cdots + \frac{a_{v-2}}{P^{v-2}}, \tag{5.11}$$

where the sum of all coefficients $1 + a_1 + \cdots + a_{v-2} = 2^e$.

Proof. The sum of the coefficients is the number of non-null terms in the sum (5.9). Therefore $1 + a_1 + \cdots + a_{v-2} = 2^e$. □

5.4 Formula for the coefficient of the main term

We are now able to quantify the coefficient of the main term.

Lemma 5.10. *For any given finite graph* $G = (V, E)$*, the series*

$$\sum_{(N_1,\dots,N_e)} \frac{\mu(N_1)\cdots\mu(N_e)}{q^{m_1}\cdots q^{m_v}} = \prod_P Q_G(q^{-\deg(P)}), \tag{5.12}$$

where the sum extends to all possible edge labelings, and $m_r = \deg(M_r)$ *converges absolutely.*

Proof. First notice that $q^{m_r} = \mathcal{N}(M_r)$, therefore our sum is the norm of the member of the ring of ideals

$$Z = \sum_{(N_1,\dots,N_e)} \frac{\mu(N_1)\cdots\mu(N_e)}{M_1\cdots M_v}. \tag{5.13}$$

Since we want to show absolute convergence we consider instead

$$Z^+ = \sum_{(N_1,\dots,N_e)} \frac{|\mu(N_1)\cdots\mu(N_e)|}{M_1\cdots M_v}. \tag{5.14}$$

In this sum when we take the norm each element is positive, therefore for the convergence we may reorder terms. We do so by joining the terms for which

$M_1 \cdots M_v = Q$ a given ideal. For each Q we are associating a finite number of terms of the sum (see proof of Lemma 5.3). We obtain

$$Z^+ = \sum_Q \frac{1}{Q}\Big(\sum_{\substack{(N_1,\dots,N_e)\\ M_1\cdots M_v = Q}} |\mu(N_1)\cdots\mu(N_e)|\Big) = \sum_Q \frac{f_G^+(Q)}{Q}.$$

By Lemma 5.2 (Euler product) we have

$$Z^+ = \prod_P \Big(1 + \frac{f_G^+(P)}{P} + \frac{f_G^+(P^2)}{P^2} + \cdots\Big).$$

By Lemma 5.4 we have also $f_G^+(P) = 0$.

Taking norms we have

$$\mathcal{N}(Z^+) = \prod_P \Big(1 + \frac{f_G^+(P^2)}{q^{2\deg(P)}} + \frac{f_G^+(P^3)}{q^{3\deg(P)}} + \cdots\Big).$$

The number of monic irreducible polynomials of degree n is $\le q^n$ (see Lemma 6.1). The sum of the coefficients of $Q_G^+(z)$ is a constant $C = Q_G^+(1)$. Therefore

$$\mathcal{N}^+(Z) \le \prod_{n=0}^{\infty} \Big(1 + \frac{C}{q^{2n}}\Big)^{q^n}$$

It is clear that this is finite because taking logarithms yields

$$\sum_{n=0}^{\infty} q^n \log\Big(1 + \frac{C}{q^{2n}}\Big) \le C \sum_{n=0}^{\infty} \frac{1}{q^n} = C\frac{q}{q-1} < \infty$$

By similar reasoning we obtain

$$Z = \sum_Q \frac{1}{Q}\Big(\sum_{\substack{(N_1,\dots,N_e)\\ M_1\cdots M_v = Q}} \mu(N_1)\cdots\mu(N_e)\Big) = \sum_Q \frac{f_G(Q)}{Q}.$$

By Lemma 5.2 (Euler product) we have

$$Z = \prod_P \Big(1 + \frac{f_G(P)}{P} + \frac{f_G(P^2)}{P^2} + \cdots\Big).$$

Taking norms

$$\mathcal{N}(Z) = \sum_{(N_1,\dots,N_e)} \frac{\mu(N_1)\cdots\mu(N_e)}{q^{m_1}\cdots q^{m_v}} = \prod_P Q_G(q^{-\deg(P)}),$$

where the sum extends to all monic irreducible polynomials P in $\mathbb{F}_q[z]$. □

Let $\rho_{G,q}$ be the sum in (5.12). We have now established an interim result; expressing $g(n)$ as a fully developed main term and a number of error terms as follows.

Lemma 5.11. *The number $g(n)$, of tuples $(Q_1, \dots, Q_v)$ with $\deg(Q_a) \le n$ satisfying the conditions of coprimality given by the graph G, is*

$$g(n) = \rho_{G,q}\Big(\frac{q^n}{q-1}\Big)^v - T + \sum_{k=1}^{v} R_k \tag{5.15}$$

where

$$T = \Big(\frac{q^n}{q-1}\Big)^v \sum_{\substack{(N_1,\dots,N_e)\\ some\ \deg(N_a)>n}} \frac{\mu(N_1)\cdots\mu(N_e)}{q^{m_1}\cdots q^{m_v}}, \tag{5.16}$$

and R_k satisfies the bound in (4.4).

6 Bound on the error terms

In this Section we obtain bounds on the terms T and R_k in (5.15) and (5.16).

6.1 Bound on R_k

Let $r_q(n)$ be the number of monic irreducible polynomials in $\mathbb{F}_q[z]$ of degree n. It is well known that (see, for example, [7, Th. 3.25, p.84])

$$r_q(n) = \frac{1}{n}\sum_{d|n} \mu\left(n/d\right) q^d. \tag{6.1}$$

We will need the following lemma.

Lemma 6.1. *The number $r_q(n)$ of irreducible polynomials of degree $= n$ in $\mathbb{F}_q[z]$ is bounded by $r_q(n) \le \frac{1}{n}q^n$.*

Proof. By (6.1) we have to prove that $\sum_{d|n} \mu(n/d)q^d \le q^n$. If $n = 1$ or $n = p$ is a prime number, this is trivial. When n is composite let p be the least prime number dividing n. The divisors of n in decreasing order are

$$n, \quad n/p, \quad d_3, \quad d_4, \dots$$

Therefore we have

$$\begin{aligned}\sum_{d|n} \mu\left(n/d\right) q^d &= q^n - q^{n/p} + \sum_{k\ge 3} \mu(n/d_k) q^{d_k} \\ &\le q^n - q^{n/p} + \sum_{d=1}^{n/p-1} q^d = q^n - q^{n/p} + \frac{q^{n/p}-1}{q-1} < q^n.\end{aligned}$$

□

We now state and prove a bound on R_k.

Lemma 6.2. *Let d be the maximum degree of a vertex in the graph G. The error terms R_k are bounded by*

$$\Big|\sum_{k=1}^{v} R_k\Big| \le \exp(d) 2^{2^e} v n^d \Big(\frac{q^n}{q-1}\Big)^{v-1}. \tag{6.2}$$

Proof. The proof is similar to the proof of Lemma 5.10. We consider the element of the ring of ideals

$$W = \sum_{\substack{(N_1,\dots,N_e)\\ \deg(N_a)\le n}} \frac{|\mu(N_1)\cdots\mu(N_e)|}{M_1\cdots\widehat{M_k}\cdots M_v},$$

whose norm is equal to the sum appearing in (4.4). That is,

$$\mathcal{N}(W) = \sum_{\substack{(N_1,\dots,N_e)\\ \deg(N_a)\le n}} \frac{|\mu(N_1)\cdots\mu(N_e)|}{q^{m_1}\cdots\widehat{q^{m_k}}\cdots q^{m_v}}.$$

The primes P that divide the ideals $M_1\cdots\widehat{M_k}\cdots M_v$ appearing in the denominators of W divide some of the N_a. Therefore $\deg(P)\le n$. It follows that

$$W \lhd \sum_Q{}^{*} \frac{1}{Q}\Big(\sum_{M_1\cdots\widehat{M_k}\cdots M_v = Q} |\mu(N_1)\cdots\mu(N_e)|\Big),$$

where the $*$ in the sum indicates that we restrict the sum to monic polynomials all of whose prime factors have degree $\le n$. This is not an equality because there may be some edge labelings $(N_1,\dots,N_e)$ that satisfy $M_1\cdots\widehat{M_k}\cdots M_v = Q$ that are not contained in W because of the restriction on the degrees.

Noticing the definition of $g^+_{G,k}(Q)$ we have

$$\sum_Q{}^{*} \frac{1}{Q}\Big(\sum_{M_1\cdots\widehat{M_k}\cdots M_v = Q} |\mu(N_1)\cdots\mu(N_e)|\Big) = \sum_Q{}^{*} \frac{g^+_{G,k}(Q)}{Q}.$$

Reasoning as in the Euler product proof we obtain

$$W \lhd \prod_{\deg(P)\le n} \Big(1 + \frac{g^+_{G,k}(P)}{P} + \frac{g^+_{G,k}(P^2)}{P^2} + \cdots\Big).$$

By Lemma 5.5 we have $g^+_{G,k}(P) = d_k$, the degree of the vertex k in G. And $g^+_{G,k}(P^m) = 0$ for $m \ge v$. Let $C = Q^+_{G,k}(1) \le 2^e$ be the sum of $g^+_{G,k}(P^m)$ for $0 \le m \le v$. Taking norms in the above relation $\lhd$, yields

$$\mathcal{N}(W) \le \prod_{m=1}^{n} \Big(1 + \frac{d_k}{q^m} + \frac{C}{q^{2m}}\Big)^{r(m)},$$

where $r(m)$ is the number of monic irreducible polynomials of degree m.

From Lemma 6.1 we have $r(m) \le \frac{1}{m}q^m$, and so

$$\begin{aligned}\log \mathcal{N}(W) &\le \sum_{m=1}^{n} \frac{q^m}{m} \log\Big(1 + \frac{d_k}{q^m} + \frac{C}{q^{2m}}\Big) \le \sum_{m=1}^{n} \frac{q^m}{m}\Big(\frac{d_k}{q^m} + \frac{C}{q^{2m}}\Big) \\ &= d_k \sum_{m=1}^{n} \frac{1}{m} + \sum_{m=1}^{n} \frac{2^e}{mq^m} \le (1 + \log n)d_k + 2^e \log 2.\end{aligned}$$

Using the bound on $\mathcal{N}(W)$ in (4.4) yields

$$|R_k| \le 2^{2^e} (\exp(1)n)^{d_k} \Big(\frac{q^n}{q-1}\Big)^{v-1}.$$

This proves our lemma. □

6.2 Bound on the error term T

To bound the error term T we require the following lemma.

Lemma 6.3. *For any squarefree polynomial $Q \in \mathbb{F}_q[z]$ of degree $n > 1$ we have*

$$\omega(Q) \le 4\frac{n}{\log n} \log q. \tag{6.3}$$

Proof. Let $x = \frac{1}{2}\frac{\log n}{\log q}$. We may assume $x \ge 1$, for otherwise

$$\omega(Q) \le n \le \frac{n}{x} = 2\frac{n}{\log n} \log q < 4\frac{n}{\log n} \log q.$$

So we assume $x \ge 1$. Since Q is squarefree we have $Q = Q_1Q_2$ where Q_1 is the product of irreducible polynomials $P \mid Q$ with degree $\le x$ and Q_2 is the product of irreducible polynomials $P \mid Q$ with degree $> x$.

The polynomial Q_1 is a divisor of R_1, the product of all irreducibles of degree $\le x$. That is,

$$R_1 = \prod_{k \le x} \prod_{\deg(P)=k} P.$$

We have

$$\omega(R_1) = \sum_{k \le x} r_q(k) \quad \text{and} \quad \deg(R_1) = \sum_{k \le x} k r_q(k).$$

All irreducible factors of Q_2 have degree $> x$. Therefore

$$x\omega(Q_2) < \deg(Q_2) = n - \deg(Q_1).$$

Therefore

$$\omega(Q) = \omega(Q_1) + \omega(Q_2) \le \omega(R_1) + \frac{n - \deg(Q_1)}{x} \le \frac{n}{x} + \sum_{k \le x} r_q(k),$$

where $r_q(n)$ is the number of monic irreducible polynomials in $\mathbb{F}_q[z]$ of degree n. By Lemma 6.1 we have $r_q(k) \le \frac{1}{k}q^k$, so that for $x \ge 1$ we obtain

$$\sum_{k\le x} r_q(k) = \sum_{k\le x} \frac{1}{k} q^k \le q^x(1+\log x).$$

Since $x = \frac{1}{2}\frac{\log n}{\log q}$

$$\begin{aligned}\omega(Q) &\le 2\frac{n}{\log n}\log q + (1+\log x)\exp\Big(\frac{1}{2}\frac{\log n}{\log q}\log q\Big)\\ &= 2\frac{n}{\log n}\log q + n^{\frac{1}{2}}\Big(1+\log\Big(\frac{1}{2}\frac{\log n}{\log q}\Big)\Big) \le 4\frac{n}{\log n}\log q.\end{aligned}$$

Note that

$$n^{\frac{1}{2}}\Big(1+\log\Big(\frac{1}{2}\frac{\log n}{\log q}\Big)\Big) \le n^{\frac{1}{2}}\Big(1+\log\Big(\frac{1}{2}\frac{\log n}{\log 2}\Big)\Big),$$

and

$$\frac{n}{\log n}\log 2 \le 2\frac{n}{\log n}\log q.$$

So it will suffice to show that

$$n^{\frac{1}{2}}\Big(1+\log\Big(\frac{1}{2}\frac{\log n}{\log 2}\Big)\Big) \le 2\frac{n}{\log n}\log 2.$$

This is equivalent to

$$y(1+\log y) \le 2^y, \qquad \text{for} \quad y = \frac{1}{2}\frac{\log n}{\log 2} \ge x \ge 1,$$

which is easily shown to be true. □

We now prove the following bound on T.

Lemma 6.4. *Given any $0 < \varepsilon < \frac{1}{2}$ the term T defined in* (5.16) *is bounded by*

$$|T| \le 3\sum_{j=1}^{e} \rho^{+}_{G'_j,q}\Big(\frac{q^n}{q-1}\Big)^v q^{-(1-\varepsilon)n}, \qquad n > n_0, \tag{6.4}$$

where G'_j is the graph obtained from G after removing the edge e_j, and n_0 depends on ε and the number of vertices in the graph G.

Proof. By the definition (5.16) of T we have

$$\begin{aligned}|T| &\le \Big(\frac{q^n}{q-1}\Big)^v \sum_{\substack{(N_1,\dots,N_e)\\ \text{some } \deg(N_a)>n}} \frac{|\mu(N_1)\cdots\mu(N_e)|}{q^{m_1}\cdots q^{m_v}}\\ &\le \Big(\frac{q^n}{q-1}\Big)^v \sum_{a=1}^{e} \sum_{\substack{(N_1,\dots,N_e)\\ \deg(N_a)>n}} \frac{|\mu(N_1)\cdots\mu(N_e)|}{q^{m_1}\cdots q^{m_v}}.\end{aligned}$$

This is only an inequality because some edge labelings $(N_1, \dots, N_e)$ may have more than one N_a of degree $> n$. We have to bound each of the e sums. They are all equivalent, in fact the index of the edges is arbitrary. Therefore we only bound the one with $\deg(N_1) > n$. This simplifies our notations a little.

Therefore we bound the sum

$$S := \sum_{\substack{(N_1,\dots,N_e)\\ \deg(N_1)>n}} \frac{|\mu(N_1)\cdots\mu(N_e)|}{q^{m_1}\cdots q^{m_v}},$$

and the corresponding element of the ring of ideals

$$W := \sum_{\substack{(N_1,\dots,N_e)\\ \deg(N_1)>n}} \frac{|\mu(N_1)\cdots\mu(N_e)|}{M_1\cdots M_v},$$

with $\mathcal{N}(W) = S$.

The edge $e_1 = \{r, s\}$ plays a special role in W. We treat this edge differently from the others. Let $(N_1, \dots, N_e)$ be an edge labeling with $\deg(N_1) > n$ and squarefree N_a so that the corresponding term in W is not null. By definition of the associated labeling (Definition 3.2),

$$M_r = \operatorname{lcm}(N_1, N_{\alpha_1}, \dots, N_{\alpha_k}), \quad M_s = \operatorname{lcm}(N_1, N_{\beta_1}, \dots, N_{\beta_\ell}),$$

where we may have $k = 0$ or $\ell = 0$.

For any other edge $2 \le j \le e$ we define $D_j = \gcd(N_1, N_j)$ and then

$$N_j = D_j N'_j, \quad D_j \mid N_1. \tag{6.5}$$

Since we assume that N_j is squarefree we have $\gcd(N_1, N'_j) = 1$. It is clear that

$$\begin{aligned} M_r &= \operatorname{lcm}(N_1, D_{\alpha_1}N'_{\alpha_1}, \dots, D_{\alpha_k}N'_{\alpha_k}) = N_1 \operatorname{lcm}(N'_{\alpha_1}, \dots, N'_{\alpha_k}),\\ M_s &= N_1 \operatorname{lcm}(N'_{\beta_1}, \dots, N'_{\beta_\ell}). \end{aligned}$$

For any other vertex $t \neq r$ and $t \neq s$ we have

$$\begin{aligned} M_t &= \operatorname{lcm}(N_{t_1}, \dots, N_{t_m}) = \operatorname{lcm}(D_{t_1}N'_{t_1}, \dots, D_{t_m}N'_{t_m})\\ &= \operatorname{lcm}(D_{t_1}, \dots, D_{t_m}) \operatorname{lcm}(N'_{t_1}, \dots, N'_{t_m}), \end{aligned}$$

where m will depend on t.

It follows that the given term of W satisfies

$$\begin{aligned} \frac{|\mu(N_1)\cdots\mu(N_e)|}{M_1\cdots M_v} \lhd \frac{\mu(N_1)}{N_1^2} &\frac{|\mu(N_2)\cdots\mu(N_e)|}{\operatorname{lcm}(N'_{\alpha_1}, \dots, N'_{\alpha_k}) \operatorname{lcm}(N'_{\beta_1}, \dots, N'_{\beta_l})}\\ &\cdot \prod_{\substack{1\le t\le v\\ t\neq r,\ t\neq s}} \frac{1}{\operatorname{lcm}(D_{t_1}, \dots, D_{t_m}) \operatorname{lcm}(N'_{t_1}, \dots, N'_{t_m})}. \end{aligned}$$

This is true even if the N_j are not squarefree because in this case both members are equal to 0.

We have

$$|\mu(N_2)\cdots\mu(N_e)| = |\mu(D_2N_2')\cdots\mu(D_eN_e')| \\ \leq |\mu(D_2)\cdots\mu(D_e)| \times |\mu(N_2')\cdots\mu(N_e')|.$$

It follows that

$$\frac{|\mu(N_1)\cdots\mu(N_e)|}{M_1\cdots M_v} \lhd \frac{|\mu(N_1)|}{N_1^2}|\mu(D_2)\cdots\mu(D_e)| \prod_{\substack{1\leq t\leq v\\ t\neq r,\ t\neq s}} \frac{1}{\operatorname{lcm}(D_{t_1},\ldots,D_{t_m})} \\ \cdot \frac{|\mu(N_2')\cdots\mu(N_e')|}{\operatorname{lcm}(N_{\alpha_1}',\ldots,N_{\alpha_k}')\operatorname{lcm}(N_{\beta_1}',\ldots,N_{\beta_l}')} \prod_{\substack{1\leq t\leq v\\ t\neq r,\ t\neq s}} \frac{1}{\operatorname{lcm}(N_{t_1}',\ldots,N_{t_m}')}$$

Consider the graph $G'=(V,E')$ obtained from G by removing the edge $e_1=\{r,s\}$. Then $(N_2',\ldots,N_e')$ is an edge labeling for G' and $M_t'=\operatorname{lcm}(N_{t_1}',\ldots,N_{t_m}')$ for any vertex $t\notin\{r,s\}$ of G', while $M_r'=\operatorname{lcm}(N_{\alpha_1}',\ldots,N_{\alpha_k}')$ and $M_s'=\operatorname{lcm}(N_{\beta_1}',\ldots,N_{\beta_l}')$. The above relation can be written as

$$\frac{|\mu(N_1)\cdots\mu(N_e)|}{M_1\cdots M_v} \lhd \frac{|\mu(N_1)|}{N_1^2}|\mu(D_2)\cdots\mu(D_e)| \prod_{\substack{1\leq t\leq v\\ t\neq r,\ t\neq s}} \frac{1}{\operatorname{lcm}(D_{t_1},\ldots,D_{t_m})}\cdot \\ \cdot \frac{|\mu(N_2')\cdots\mu(N_e')|}{M_1'\cdots M_v'}.$$

Recall that D_j are divisors of N_1. The above implies that

$$W \lhd W_1W_2,$$

where we define

$$W_1 = \sum_{\deg(N_1)>n} \frac{|\mu(N_1)|}{N_1^2} \sum_{\substack{(D_2,\ldots,D_e)\\ D_j|N_1}} |\mu(D_2)\cdots\mu(D_e)| \prod_{\substack{1\leq t\leq v\\ t\neq r,\ t\neq s}} \frac{1}{\operatorname{lcm}(D_{t_1},\ldots,D_{t_m})},$$

$$W_2 = \sum_{(N_2',\ldots,N_e')} \frac{|\mu(N_2')\cdots\mu(N_e')|}{M_1'\cdots M_v'}.$$

From the data of N_1, $(D_2,\ldots,D_e)$ and $(N_2',\ldots,N_e')$ we reconstruct uniquely the edge labeling $(N_1,\ldots,N_e)$ by the equations (6.5). Lemma 5.10 applied to the graph G' gives us that $\mathcal{N}(W_2)=\rho^+_{G',q}$ is a finite constant.

Therefore we need to bound the norm $\mathcal{N}(W_1)$ because $W\lhd W_1W_2$ implies

$$\mathcal{N}(W)\leq \mathcal{N}(W_1)\mathcal{N}(W_2).$$

Let G' be the graph G with the edge $\{r,s\}$ removed. Then $(D_2,\dots,D_e)$ is a edge labeling of G' and $\operatorname{lcm}(D_{t_1},\dots,D_{t_m})$ are the polynomials of the corresponding vertex labeling. Therefore, with the notations of Definition 5.6, we have

$$W_1 = \sum_{\deg(N)>n} \frac{|\mu(N)|}{N^2} f_{r,s}(N),$$

where $f_{r,s}$ is the function associated to the graph G' and the pair of vertices, not forming an edge in G', $\{r,s\}$. By Lemma 5.9, for each irreducible polynomial P, the norm of $f_{r,s}(P)$ is less than or equal 2^{e-1} because $e-1$ is the number of edges of the graph G'. Hence if N is squarefree with $\omega(N)$ irreducible factors, we have $\mathcal{N}(f_{rs}(N)) \le 2^{e\,\omega(N)}$. It follows that the norm of W_1 is less than or equal to

$$\mathcal{N}\left(\sum_{\deg(N)>n} \frac{\mu(N)}{N^2} 2^{e\,\omega(N)}\right).$$

It will now suffice to calculate a suitable upper bound on this norm.

In fact we will show the following.

Lemma 6.5. *Given $0<\varepsilon<1/2$ and a natural number a there is an $n_0 = n_0(\varepsilon,a)$ such that*

$$\mathcal{N}\Big(\sum_{\deg(Q)>n} \frac{|\mu(Q)|2^{a\omega(Q)}}{Q^2}\Big) \le 3q^{-(1-\varepsilon)n}, \qquad n \ge n_0. \tag{6.6}$$

Proof. Joining the terms with $\deg(Q)=m$ and applying (6.3), the norm $\mathcal{N}$ in (6.6) is bounded by

$$\mathcal{N} \le \sum_{m=n+1}^{\infty} q^m \frac{1}{q^{2m}} \exp\Big(a(\log 2) 4 \frac{m}{\log m}\log q\Big).$$

Taking $n_0 = n_0(\varepsilon,a)$ we will have

$$4\frac{a\log 2}{\log m} < \varepsilon, \qquad \text{for } m \ge n_0.$$

Therefore we have for $n \ge n_0$,

$$\mathcal{N} \le \sum_{m=n+1}^{\infty} \frac{1}{q^m} q^{\varepsilon m} = \frac{1}{q^{(1-\varepsilon)n}} \frac{1}{q^{1-\varepsilon}-1}.$$

Since $q \ge 2$ and $\varepsilon < 1/2$, the term $\frac{1}{q^{1-\varepsilon}-1} \le \frac{1}{2^{1/2}-1} < 3$ is bounded by an absolute constant. Thus,

$$\mathcal{N}\Big(\sum_{\deg(Q)>n} \frac{|\mu(Q)|2^{a\omega(Q)}}{Q^2}\Big) \le 3q^{-(1-\varepsilon)n},$$

which concludes the proof of Lemma 6.5. □

This concludes the proof of the upper bound on T. □

7 Proof of the main theorem

We can now prove the main theorem.

Proof. In (5.15) we obtained

$$g(n) = \frac{\rho_{G,q}}{(q-1)^v} q^{nv} - T + \sum_{k=1}^{v} R_k.$$

In (6.2) we showed that we have

$$\Big|\sum_{k=1}^{v} R_k\Big| \le \exp(d) 2^{2^e} v n^d \left(\frac{q^n}{q-1}\right)^{v-1},$$

where d is the maximum degree of the vertices of G. And in (6.4) we have shown that given $0 < \varepsilon < \frac{1}{2}$ we have for $n \ge n_0(\varepsilon, e)$

$$|T| \le 3 \sum_{j=1}^{e} \rho^+_{G'_j,q} \Big(\frac{q^n}{q-1}\Big)^v q^{-(1-\varepsilon)n}.$$

Hence

$$g(n) = \frac{\rho_{G,q}}{(q-1)^v} q^{nv} \Big(1 - \frac{(q-1)^v}{q^{nv}\rho_{G,q}} T + \frac{(q-1)^v}{q^{nv}\rho_{G,q}} \sum_{k=1}^{v} R_k\Big).$$

Since

$$\Big|\frac{(q-1)^v}{q^{nv}\rho_{G,q}} T\Big| \le \frac{3}{\rho_{G,q}} \Big(\sum_{j=1}^{e} \rho^+_{G'_j,q}\Big) q^{-(1-\varepsilon)n}, \qquad n \ge n_0(\varepsilon, e)$$

and

$$\Big|\frac{(q-1)^v}{q^{nv}\rho_{G,q}} \sum_{k=1}^{v} R_k\Big| \le \frac{\exp(d) 2^{2^e} (q-1) v}{\rho_{G,q}} n^d q^{-n},$$

we obtain

$$g(n) = \frac{\rho_{G,q}}{(q-1)^v} q^{nv} L,$$

where

$$L = 1 + \frac{\exp(d) 2^{2^e} (q-1) v}{\rho_{G,q}} O(n^d q^{-n}) + \frac{3}{\rho_{G,q}} \Big(\sum_{j=1}^{e} \rho^+_{G'_j,q}\Big) O(q^{-(1-\varepsilon)n}),$$

and the constants in the O symbols are absolute in both cases.

We can also write this in the simplified form

$$g(n) = \frac{\rho_{G,q}}{(q-1)^v} q^{nv} \Big(1 + O_{G,q}(n^d q^{-n}) + O_{G,q}(q^{-(1-\varepsilon)n})\Big).$$

□

8 Acknowledgment

The authors thanks Igor Shparlinski for pointing out that [1] could be adapted for tuples of monic polynomials in finite fields.

References

[1] J. Arias de Reyna and R. Heyman, 'Counting tuples restricted by pairwise coprimality conditions', J. Integer Seq., **18** (2015), 15.10.4.

[2] M. García-Armas, S. R. Ghorpade and S. Ram, 'Relatively prime polynomials and nonsingular Hankel matrices over finite fields', J. Combin. Theory Ser. A, **118** (2011), 819–828.

[3] A. T. Benjamin and C. D. Bennett, 'The probability of relatively prime polynomials', Math. Mag., **80** (2007), 196–202.

[4] S. Corteel, C. D. Savage, H. S. Wilf and D. Zeilberger, 'A pentagonal number sieve', J. Combin. Theory Ser. A, **82** (1998), 186–192.

[5] X. Hou and G. L. Mullen, 'Number of irreducible polynomials and pairs of relatively prime polynomials in several variables over finite fields', Finite Fields Appl. **15** (2009), 304–331.

[6] D. E. Knuth, *The Art of computer programming, Vol 2. Seminumerical algorithms (3rd Edition)*, Addison Wesley, Boston, 1998.

[7] R. Lidl and H. Niederreiter, *Finite fields*, Addison-Wesley 1983.

[8] G. Micheli and R. Schnyder, 'On the density of coprime m-tuples over holomorphy rings', Preprint, 2017, available from arXiv/1411.6876 [math.NT]].

[9] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, Springer, 3$^{\text{rd}}$ Ed., 2004.

[10] A. Reifegerste, 'On an involution concerning pairs of polynomials over $\mathbb{F}_2$', J. Combin. theory Ser. A, **90** (2000), 216–220.

[11] J. J. Stone, 'Multiple-burst error correction with the Chinese remainder theorem', J. Soc. Indust. Appl. Math., **11** (1963), 74–81.