JOACHIM VON ZUR GATHEN (2011). Counting decomposable multivariate polynomials. *Applicable Algebra in Engineering, Communication and Computing* **22**(3), 165–185.
URL http://dx.doi.org/10.1007/s00200-011-0141-9. Abstract in *Abstracts of the Ninth International Conference on Finite Fields and their Applications*, pages 21–22, Dublin, July 2009, Claude Shannon Institute, http://www.shannoninstitute.ie/fq9/AllFq9Abstracts.pdf.


# COUNTING DECOMPOSABLE MULTIVARIATE POLYNOMIALS

JOACHIM VON ZUR GATHEN

October 25, 2010

**Abstract.** A polynomial $f$ (multivariate over a field) is *decomposable* if $f = g \circ h$ with $g$ univariate of degree at least 2. We determine the dimension (over an algebraically closed field) of the set of decomposables, and an approximation to their number over a finite field. The relative error in our approximations is exponentially decaying in the input size.

**Keywords.** computer algebra, polynomial decomposition, multivariate polynomials, finite fields, combinatorics on polynomials

## 1. Introduction

It is intuitively clear that the decomposable polynomials form a small minority among all polynomials (multivariate over a field). The goal in this work is to give a precise quantitative version of this intuition. Interestingly, we find a special case for bivariate polynomials where the intuition about the "most general decomposable polynomials" is incorrect.

We use the methods from von zur Gathen (2008d), where the corresponding task was solved for reducible, squareful, relatively irreducible, and singular bivariate polynomials; further references are given in that paper, starting with early work of Carlitz ? and Cohan ?. Von zur Gathen, Viola & Ziegler (2010c) extend those results to multivariate polynomials and give further information such as exact formulas and generating functions.

Our question has two facets: in the *geometric* view, we want to determine the dimension of the algebraic set of decomposable polynomials, say over an algebraically closed field. The *combinatorial* task is to approximate the number of decomposables over a finite field, together with a good relative error bound. The goal is to have a bound that is exponentially decreasing in the input size. The choices we make in our calculations are guided by the goal of such bounds in a form which is as simple and universal as possible.

As mentioned above, a special case occurs for bivariate polynomials. Usually, the largest number of decompositions results from maximizing the number of choices for the right component. But for some special degrees—the squares of primes and numbers of RSA type—most bivariate decompositions arise from having a large number of choices for the left component. At three or more variables, all is uniform.

Giesbrecht (1988) was the first to consider a variant of our counting problem. He showed that the decomposable univariate polynomials form an exponentially small fraction of all univariate polynomials. My interest, dating back to the supervision of this thesis, was rekindled by my study of similar counting problems (von zur Gathen 2008d), and during a visit to Pierre Dèbes' group at Lille, where I received a preliminary version of Bodin, Dèbes & Najib (2009). Their results are substantially weaker, as explained after Remark 4.21.

The companion paper von zur Gathen (2008b) deals with decomposable univariate polynomials, and this line of inquiry is continued in von zur Gathen *et al.* (2010b).

## 2. Decompositions

We have a field $F$, a positive integer $r$, and the polynomial ring $R = F[x_1, \ldots, x_r]$. We assume a degree-respecting term order on $R$, so that in particular the *leading term* $\operatorname{lt}(f)$ of an $f \in R$ is defined and $\deg \operatorname{lt}(f) = \deg f$. Throughout this paper, deg denotes the total degree. If $f \neq 0$, the constant coefficient $\operatorname{lc}(f) \in F^\times = F \setminus \{0\}$ of $\operatorname{lt}(f)$ is the *leading coefficient* of $f$. Then $f$ is *monic* if $\operatorname{lc}(f) = 1$. We call $f$ *original* if its graph contains the origin, that is, $f(0, \ldots, 0) = 0$.

The reader might think of the usual degree-lexicographic ordering, where terms of higher degree come before those of lower degree, and terms of the same degree are sorted lexicographically, with $x_1 > x_2 > \cdots > x_r$. For example,

$$f = -3x_1^2x_3 - 2x_2^3 + 4x_4x_5^2 + 5x_1^2 + 8x_1x_2 + 5x_6^2 - 7$$

is written in order, $\operatorname{lc}(f) = -3$ (provided that $-3 \neq 0$), and $f$ is not original (if $-7 \neq 0$).

Definition 2.1. *For $g \in F[t]$ and $h \in R$,*

$$f = g \circ h = g(h) \in R$$

*is their* composition. *If $\deg g \geq 2$ and $\deg h \geq 1$, then $(g, h)$ is a* decomposition *of $f$. A polynomial $f \in R$ is* decomposable *if there exist such $g$ and $h$.*

*Otherwise $f$ is* indecomposable. *The decomposition $(g, h)$. It is* superlinear *if* $\deg h \geq 2$.

There are other notions of decompositions. The present one is called uni-multivariate in von zur Gathen *et al.* (2003). Another one is studied in Faugère & Perret (2008) for cryptanalytic purposes. In the context of univariate polynomials, only superlinear decompositions are traditionally considered.

REMARK 2.2. *Multiplication by a unit or addition of a constant does not change decomposability, since*

$$f = g \circ h \Longleftrightarrow af + b = (ag + b) \circ h$$

*for all $f$, $g$, $h$ as above and $a, b \in F$ with $a \neq 0$. In other words, the set of decomposable polynomials is invariant under this action of $F^\times \times F$ on $R$. There is a unique monic original $f$ in each orbit of this action.*

*Furthermore, for any decomposition $(g, h)$ we can take $a = \mathrm{lc}(h)^{-1} \in F^\times$, $b = -a \cdot h(0, \ldots, 0) \in F$, $g^* = g((t - b)a^{-1}) \in F[t]$, and $h^* = ah + b$. Then $g \circ h = g^* \circ h^*$ and $h^*$ is monic original.*

Lastly, if $f = g \circ h$ and $h$ is monic original, then $\mathrm{lc}(f) = \mathrm{lc}(g)$ and $f(0, \ldots, 0) = g(0)$, so that $f$ is monic original, if and only if $g$ is. If the latter holds, then $(g, h)$ is called monic original and remark.

The following result is shown for $r \geq 2$ in Bodin *et al.* (2009). It is trivially valid for $r = 1$, where

$$f(x_1) = f(t) \circ x_1 \tag{2.3}$$

for any $f \in F[x_1]$. This decomposition is not superlinear.

FACT 2.4. *Any polynomial in $R$ has at most one monic original decomposition with indecomposable right component.*

If we also allowed trivial decompositions $f = g \circ h$ with $\deg g = 1$, then every polynomial would have exactly one monic original decomposition with indecomposable right component.

We fix some notation for the remainder of this paper. For $r \geq 1$ and $n \geq 0$, we write

$$P_{r,n}^{\mathrm{all}} = \{f \in F[x_1, \ldots, x_r] \colon \deg f \leq n\}$$

for the vector space of polynomials of degree at most $n$, of dimension

$$\dim P_{r,n} = b_{r,n} = \binom{r+n}{r}.$$

Furthermore, we consider the subset

$$P_{r,n} = \{f \in P_{r,n}^{\mathrm{all}} \colon f \text{ monic and original of degree } n\}.$$

Over an infinite field, $P_{r,n}^{\mathrm{all}} \smallsetminus P_{r,n-1}^{\mathrm{all}}$ is a Zariski-open subset of $P_{r,n}^{\mathrm{all}}$ and irreducible, taking $P_{r,-1}^{\mathrm{all}} = \{0\}$. Now $P_{r,n}$ is obtained by further imposing one equation on the coefficients and working modulo multiplication by units, so that

$$\dim P_{r,n} = b_{r,n} - 2,$$

with $P_{r,0} = \varnothing$. For any divisor $e$ of $n$, we have the monic original compositions

$$D_{r,n,e} = \{g \circ h \colon g \in P_{1,e}, h \in P_{r,n/e}\} \subseteq P_{r,n}. \tag{2.5}$$

Here $P_{1,e}$ consists of polynomials in $F[t]$ rather than in $F[x_1]$.) The set $D_{r,n}$ of all decomposable polynomials in $P_{r,n}$ satisfies

$$D_{r,n} = \bigcup_{1<e|n} D_{r,n,e}. \tag{2.6}$$

In particular, $D_{r,1} = \varnothing$ for all $r \geq 1$. Over an algebraically closed field, each $D_{r,n,e}$ is the image of a polynomial map from an irreducible variety, hence algebraic and irreducible, and also $D_{r,n}$ is algebraic. The dimension of $D_{r,n}$ is taken to be the maximal dimension of its irreducible components. We also denote as

$$I_{r,n} = P_{r,n} \smallsetminus D_{r,n}$$

the set of indecomposable polynomials. Thus $I_{r,1} = P_{r,1}$ for $r \geq 1$.

Let $D_{r,n}^{\mathrm{all}}$ consist of all decomposable polynomials in $P_{r,n}^{\mathrm{all}}$ of degree $n$. Then $D_{r,n}^{\mathrm{all}}$ is the union of the orbits of $D_{r,n}$ under the action of $F^\times \times F$ described in Remark 2.2. Over an infinite field $F$ we have $\dim D_{r,n}^{\mathrm{all}} = \dim D_{r,n} + 2$. This allows us to concentrate exclusively on $D_{r,n}$ in the remainder of this paper.

In order to have a nontrivial concept also in the univariate case, where (2.3) holds, we introduced in Definition 2.1 the notion of superlinear decompositions $f = g \circ h$ where $\deg h \geq 2$. The set of all these is

$$D_{r,n}^{\mathrm{sl}} = \bigcup_{\substack{e|n \\ 1<e<n}} D_{r,n,e}. \tag{2.7}$$

In particular, $D_{r,n}^{\mathrm{sl}} = \varnothing$ if $n$ is prime. We also let $I_{r,n}^{\mathrm{sl}} = P_{r,n}^{=} \smallsetminus D_{r,n}^{\mathrm{sl}}$. In the present paper, we investigate this notion only for two or more variables. The mote challenging univariate case is treated in von zur Gathen (2008c) and von zur Gathen, Giesbrecht & Ziegler (2010b).

## 3. Dimension of decomposables

In this section, we determine the dimension of the set of decomposable polynomials over an algebraically closed field. This forms the basis for the counting result in the next section.

Throughout the paper, $\ell$ denotes the smallest prime factor of $n \geq 2$. In the following, we have to single out the following special case:

$$r = 2, n/\ell \text{ is prime and } n/\ell \leq 2\ell - 5. \tag{3.1}$$

The smallest examples are $n = \ell^2$ with $\ell \geq 5$, $n = 11 \cdot 13$, and $n = 11 \cdot 17$. In particular, $\ell$ and $n/\ell$ are always at least 5.

THEOREM 3.2. *Let $F$ be an algebraically closed field, $r \geq 1$, $n \geq 2$, let $\ell$ be the smallest prime divisor of $n$, and*

$$m = \begin{cases} n & \text{if (3.1) holds or } r = 1, \\ \ell & \text{otherwise.} \end{cases} \tag{3.3}$$

*Then the following hold.*

*(i) $D_{r,n}$ has dimension*

$$\dim D_{r,n} = \binom{r + n/m}{r} + m - 3.$$

*(ii) If $r \geq 2$, then $I_{r,n}$ contains a dense open subset of $P_{r,n}$, of dimension $\binom{r+n}{r} - 2$.*

*(iii) We assume that $r \geq 2$. Then $D^{\mathrm{sl}}_{r,n} = \varnothing$ if $n$ is prime, and otherwise*

$$\dim D^{\mathrm{sl}}_{r,n} = \binom{r + n/\ell}{r} + \ell - 3.$$

PROOF. The decomposition (2.3) implies that $D_{1,n} = P_{1,n}$, and thus the claim (i) for $r = 1$. We assume $r \geq 2$ in the remainder of the proof.

(i) Each $D_{r,n,e}$ is an algebraic set, and we have

$$\dim \mathrm{D}_{r,n,e} \leq \dim P_{1,e} + \dim P_{r,n/e} = b_{r,n/e} + e - 3. \tag{3.4}$$

We let $E = \{e \in \mathbb{N} \colon 1 < e \mid n\}$ be the index set in (2.6). When $n$ is prime, then $e = n = \ell$ is the only element of $E$, and the upper bound $\dim D_{r,n} \leq r + n - 2$

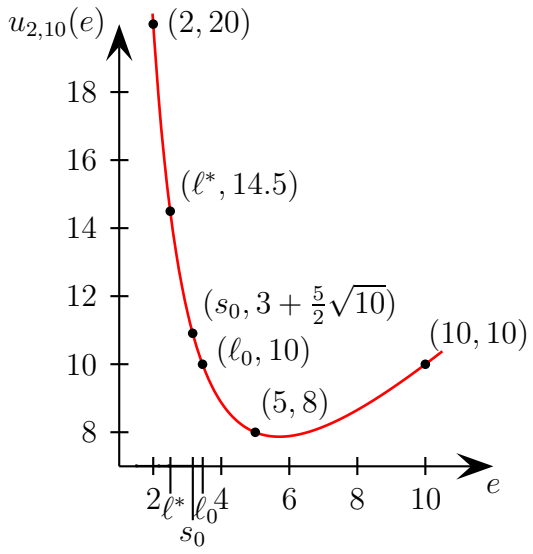


Figure 3.1: An example of $u_{r,n}$, for $r = 2$ and $n = 10$, with $\ell = 2$, $\ell^* = \frac{5}{2}$, $s_0 = \sqrt{10} \approx 3.16$, and $\ell_0 = 1 + \sqrt{6} \approx 3.45$.

in (i) follows. We may now assume that $n$ is composite. We consider the right hand side in (3.4) as the function

$$u_{r,n}(e) = b_{r,n/e} + e - 3 \tag{3.5}$$

of a real variable $e$ on the interval $[1, n]$. See Figure 3.1 for an example. We claim that

$$u_{r,n}(m) = \max_{e \in E} u_{r,n}(e). \tag{3.6}$$

The upper bound in (i) follows from this. The second derivative

$$\frac{\partial^2 u_{r,n}}{\partial e^2}(e) = \frac{n}{e^3 \cdot r!} \sum_{1 \le i \le r} \left( \frac{n}{e} \sum_{\substack{1 \le j \le r \\ j \ne i}} \prod_{\substack{1 \le k \le r \\ k \ne i,j}} (k + \frac{n}{e}) + 2 \prod_{\substack{1 \le j \le r \\ j \ne i}} (j + \frac{n}{e}) \right)$$

is positive on $[1, n]$, so that $u_{r,n}$ is convex. In particular, $u_{r,n}$ takes its maximum on the interval $[\ell, n]$ at one of the two endpoints.

For (3.6), we start with the case $r \ge 3$ and claim that $u_{r,n}(\ell) \ge u_{r,n}(n)$. Setting $s_0 = \sqrt{n}$, we have

$$u_{r,n}(s_0) - u_{r,n}(n) = \binom{r + s_0}{r} + s_0 - r - 1 - s_0^2.$$

Now we replace $s_0$ by a real variable $s$, and set

$$v_r(s) = \binom{r+s}{r} + s - r - 1 - s^2.$$

Then

$$v_r(2) = \frac{r^2 + r - 4}{2} > 0, \tag{3.7}$$

since $r \geq 2$. Furthermore, we have

$$\frac{\partial v_r}{\partial s}(s) = \frac{1}{r!} \sum_{1 \leq i \leq r} \prod_{\substack{1 \leq j \leq r \\ j \neq i}} (j + s) + 1 - 2s.$$

Expanding the product, we find that the coefficient in the sum of the linear term in $s$ equals

$$\sum_{1 \leq i \leq r} \sum_{\substack{1 \leq j \leq r \\ j \neq i}} \prod_{\substack{1 \leq k \leq r \\ k \neq i,j}} k = r! \sum_{\substack{1 \leq i,j \leq r \\ j \neq i}} \frac{1}{i \cdot j} \geq r! \cdot 2 \cdot \left(\frac{1}{1 \cdot 2} + \frac{1}{1 \cdot 3} + \frac{1}{2 \cdot 3}\right) = 2 \cdot r!,$$

since $r \geq 3$. Thus

$$\frac{\partial v_r}{\partial s}(s) \geq 0,$$

and together with (3.7) this implies $v_r(s) > 0$ for all $s \geq 2$. Since $n$ is composite, we have $2 \leq \ell \leq \sqrt{n} = s_0 < n$, and from the above we have

$$u_{r,n}(\ell) \geq u_{r,n}(s_0) \geq u_{r,n}(n).$$

Since $m = \ell$, this shows the claim (3.6) and the upper bound in (i).

For the case $r = 2$, we observe that

$$u_{2,n}(\ell) - u_{2,n}(n) = \frac{(n - \ell)(n + 4\ell - 2\ell^2)}{2\ell^2} \tag{3.8}$$

is nonnegative if and only if $\ell \leq \ell_0$, where $\ell_0 = 1 + \frac{1}{2}\sqrt{2n+4}$ is the positive root of the quadratic factor. Furthermore, we note that

$$u_{2,n}(n) > u_{2,n}(\ell) \iff \ell > \ell_0 \iff n/\ell < 2\ell - 4 \iff n/\ell \leq 2\ell - 5, \tag{3.9}$$

$$\ell_0^2 = n/2 + \sqrt{2n+4} + 2 > n/2.$$

If the conditions in (3.9) hold, there is at most one other prime factor of $n$ besides $\ell$, so that $n/\ell$ is prime and (3.1) holds. (3.6) follows in this case, and also otherwise because of the equivalences in (3.9).

We have now shown one inequality in (i), namely that $\dim D_{r,n} \le u_{r,n}(m)$. For (ii), we claim that $u_{r,n}(m) < u_{r,n}(1) = \dim P_{r,n}$. Since $1 < m \le n$ and $u_{r,n}$ is convex, it is sufficient to show that

$$r + n - 2 = u_{r,n}(n) < u_{r,n}(1) = \binom{r+n}{r} - 2.$$

The inequality is equivalent to

$$r! < (r + n - 1)^{\underline{r-1}},$$

where $a^{\underline{r}} = a \cdot (a-1) \cdots (a-r+1)$ is the falling factorial (or Pochhammer symbol). This is valid for $n = 2$ since $2 < r + 1$, and the right hand side is monotonically increasing in $n$, so that the claim is proven.

It follows that $D_{r,n}$ is contained in a proper closed subset of $P_{r,n}$, and there is a dense open subset consisting of indecomposable polynomials, which is (ii). This fact also holds in each $P_{r,n/e}$. From the uniqueness of monic original decompositions with indecomposable right component (Fact 2.4) ,we conclude that if we restrict $h$ in (2.5) to be in $I_{r,n/e}$, then the map $(g, h) \mapsto g \circ h$ is injective. Thus equality holds in (3.4), and (i) is also proven.

(iii) For superlinear compositions, we have $D^{\mathrm{sl}}_{r,n} = \varnothing$ if $n$ is prime, and now may assume $n$ to be composite. The maximal value allowed for $e$ in (2.7) is $n/\ell$. Thus (iii) follows from (i) when $m < n$. Then $r = 2$, and

$$u_{2,n}(\ell) - u_{2,n}(n/\ell) = \frac{(n - \ell^2)(n + \ell^2 + \ell)}{2\ell^2} \tag{3.10}$$

is always nonnegative, so that

$$\dim D^{\mathrm{sl}}_{2,n} = \dim \mathrm{D}_{2,n,\ell} = u_{2,n}(\ell).$$

Together with the uniqueness of Fact 2.4, this proves (iii) also for $m = n$. □

## 4. Counting decomposables over finite fields

The goal in this section is to approximate the number of multivariate decomposables over a finite field, with a good relative error bound.

Over a finite field $F = \mathbb{F}_q$ with $q$ elements, we have

$$\#P_{r,n} = \frac{q^{b_{r,n}} - q^{b_{r,n-1}}}{q \cdot (q-1)} = q^{b_{r,n}-2} \frac{1 - q^{-b_{r-1,n}}}{1 - q^{-1}}.$$

For the set $D_{r,n}^{\mathrm{all}}$ of all decomposable polynomials of degree $n$, we have

$$\#D_{r,n}^{\mathrm{all}} = q^2(1-q^{-1}) \cdot \#D_{r,n}.$$

The proof of the following estimate of $\#D_{r,n}$ involves several case distinctions which are reflected in the somewhat complicated statement of the theorem. A simplified version is presented in Corollary 4.23 below.

THEOREM 4.1. *Let $F = \mathbb{F}_q$ be a finite field with $q$ elements, $r \geq 2$, $\ell$ the smallest prime divisor of $n \geq 2$, and $m$ as in (3.3). We set*

$$\begin{aligned}
\alpha_{r,n} &= q^{\binom{r+n/m}{r}+m-3} \cdot \frac{1-q^{-\binom{r-1+n/m}{r-1}}}{1-q^{-1}}, \\
c_{r,n,1} &= \ell - 3, \\
c_{r,n,2} &= \ell - 2, \\
c_{r,n,3} &= \binom{r+1}{2} - 2, \\
c_{r,n,4} &= \binom{r-1+n/\ell}{r-1} - 1,
\end{aligned} \tag{4.2}$$

$$\beta_{r,n} = \begin{cases}
0 & \text{if } n \text{ is prime}, \\
\dfrac{2q^{-c_{r,n,1}}(1-q^{-n/\ell-1})}{1-q^{-2}} & \text{if (3.1) holds}, \\
2q^{-c_{r,n,2}} & \text{if } r=2 \text{ and } n/\ell = 2\ell-3 \text{ is prime}, \\
q^{-c_{r,n,3}} & \text{if } n = 4, \\
\dfrac{2q^{-c_{r,n,4}}}{1-q^{-1}} & \text{otherwise}.
\end{cases} \tag{4.3}$$

*Then the following hold.*

*(i)*

$$|\#D_{r,n} - \alpha_{r,n}| \leq \alpha_{r,n} \cdot \beta_{r,n}.$$

*(ii)*

$$\#I_{r,n} \geq \#P_{r,n} - 2\alpha_{r,n}.$$

*(iii) We set*

$$\alpha^{\mathrm{sl}}_{r,n} = \begin{cases} 0 & \text{if } n \text{ is prime,} \\ q^{\binom{2+n/\ell}{2}+\ell-3}(1-q^{-n/\ell-1}) & \text{if (3.1) holds,} \\ \alpha_{r,n} & \text{otherwise,} \end{cases}$$

$$\beta^{\mathrm{sl}}_{r,n} = \begin{cases} q^{-(n+\ell^2+\ell)(n-\ell^2)/2\ell^2} & \text{if (3.1) holds and } n > \ell^2, \\ q^{-(n+\ell-2)/2} & \text{if (3.1) holds and } n = \ell^2, \\ \beta_{r,n} & \text{otherwise.} \end{cases}$$

*Then*

$$\left|\#D^{\mathrm{sl}}_{r,n} - \alpha^{\mathrm{sl}}_{r,n}\right| \le \alpha^{\mathrm{sl}}_{r,n} \cdot \beta^{\mathrm{sl}}_{r,n}. \tag{4.4}$$

*(iv)* $\#I^{\mathrm{sl}}_{r,n} \ge \#P_{r,n} - 2\alpha^{\mathrm{sl}}_{r,n}$.

Proof. The proof of (i) and (ii) proceeds in three stages: an upper bound on decomposables, a lower bound on indecomposables, and a lower bound on decomposables. Each stage depends on the previous one. The art here is to find bounds that are reasonably aesy to use on the one hand, and strong enough on the other hand so that the lower bound from the third stage essentially matches the upper bound.

According to (4.3), we have to distinguish five cases:

| $i$ | condition for case $i$ | $m$ | $c_{r,n,i}$ |
|---|---|---|---|
| 0 | $n$ prime | $n$ | |
| 1 | $r=2$, $n/\ell \le 2\ell-5$ prime | $n$ | $\ell-3$ |
| 2 | $r=2$, $n/\ell = 2\ell-3$ prime | $\ell$ | $\ell-2$ |
| 3 | $n=4$ | $\ell$ | $\binom{r+1}{2}-2$ |
| 4 | otherwise | $\ell$ | $\binom{r-1+n/\ell}{r-1}-1$ |

In the first stage, for a divisor $e$ of $n$, we have

$$\#D_{r,n,e} \le \#P_{1,e} \cdot \#P_{r,n/e} = q^{b_{r,n/e}+e-3} \cdot \frac{1-q^{-b_{r-1,n/e}}}{1-q^{-1}},$$

and thus with $u_{r,n}$ from (3.5)

$$\#D_{r,n} \le \sum_{1<e|n} \#\,\mathrm{D}_{r,n,e} \le \sum_{1<e|n} q^{u_{r,n}(e)} \cdot \frac{1-q^{-b_{r-1,n/e}}}{1-q^{-1}}. \tag{4.5}$$

We write $u$ for $u_{r,n}$ and $c_i$ for $c_{r,n,i}$, and recall $E = \{e \in \mathbb{N}\colon 1 < e \mid n\}$.

If $n$ is prime, then $E = \{n\}$, $m = \ell = n$ (see (3.3)), and each right hand component $h$ in a decomposition is linear, hence indecomposable. It follows from Fact 2.4 that the map $(g, h) \mapsto g \circ h$ is injective, $D_{r,n} = \operatorname{im} \gamma_{r,n,n}$, and $\#D_{r,n} = \alpha_{r,n}$. All claims follow in this case. We may now assume that $n$ is composite.

In the first stage, we use the following blanket assumptions and notations:

$$r \geq 2, a = n/\ell \geq \sqrt{n} \geq \ell \geq 2, a^2 \geq n \geq 2\ell \geq \ell + 2. \tag{4.6}$$

We first explain our general strategy for the upper bound

$$\#D_{r,n} \leq \alpha_{r,n}(1 + \beta_{r,n}) \tag{4.7}$$

in (i). From (3.6) we know that the maximal value of $u$ occurs at $e = m$. By the convexity of $u$, each value is assumed at most twice, and we can majorize the sum in (4.5) by twice a geometric sum. However, this would provide an unsatisfactory error estimate, and we want to show that the difference between $u(m)$ and the other values $u(e)$ with $e \in E$ is sufficently large. We abbreviate

$$w = \frac{1 - q^{-b_{r-1,n/\ell}}}{1 - q^{-b_{r-1,n/m}}},$$

define $\delta$, $\mu$, and $\beta$ in (4.8), and claim that for any $c$ the following implication holds:

$$\left.\begin{array}{rcl} c \leq \delta & = & \min_{e \in E \smallsetminus \{m\}}(u(m) - u(e)) \\ \mu & = & \min\{\#E - 1, \frac{2}{1-q^{-1}}\} \\ \beta & = & \mu w q^{-c} \end{array}\right\} \Rightarrow \#D_{r,n} \leq \alpha_{r,n}(1 + \beta). \tag{4.8}$$

In our four cases, $c$ will be instantiated by $c_1$, $c_2$, $c_3$, and $c_4$. We note that $\mu \leq 4$. In order to prove the claim, we note that

$$u(e) - u(m) \leq -c$$

for all $e \in E \smallsetminus \{m\}$. Since $b_{r-1,k}$ is monotonically increasing in $k$ and $n/e \leq n/\ell$, we have

$$1 - q^{-b_{r-1,n/e}} \leq 1 - q^{-b_{r-1,n/\ell}}$$

for all $e \in E$. Using this estimate for all $e \neq m$ and the fact that the convex function $u$ takes any of its values at most twice, we find that

$$\begin{aligned} q^{-u(m)} \sum_{e \in E} q^{u(e)}(1 - q^{-b_{r-1,n/e}}) &< (1 + 2w \sum_{i \leq -c} q^i) \cdot (1 - q^{-b_{r-1,n/m}}) \\ &= (1 + \frac{2wq^{-c}}{1 - q^{-1}}) \cdot (1 - q^{-b_{r-1,n/m}}). \end{aligned}$$

Also, since $E \smallsetminus \{m\}$ has $\#E - 1$ elements, we find

$$q^{-u(m)} \sum_{e \in E} q^{u(e)} (1 - q^{-b_{r-1,n/e}}) \le (1 + (\#E - 1) w q^{-c}) \cdot (1 - q^{-b_{r-1,n/m}}).$$

Using (4.5) we conclude that

$$\#D_{r,n} \le q^{u(m)} \cdot \frac{1 - q^{-b_{r-1,n/m}}}{1 - q^{-1}} \cdot (1 + \mu w q^{-c}) = \alpha_{r,n}(1 + \beta), \tag{4.9}$$

as claimed. It then remains to see that $\beta \le \beta_{r,n}$.

We now turn to our four cases. In case 1, (3.1) holds, $E = \{\ell, n/\ell, n\}$, $r = 2$, $\ell \ge 5$, $m = n$, and

$$w = \frac{1 - q^{-n/\ell - 1}}{1 - q^{-2}}.$$

Now (3.10) says that

$$u(\ell) - u(n/\ell) = \frac{(n - \ell^2)(n + \ell^2 + \ell)}{2\ell^2} \ge 0,$$

so that $u(e) \le u(\ell)$ for all $e \in E \smallsetminus \{m\} = \{\ell, n/\ell\}$, and by (3.8)

$$\delta = u(n) - u(\ell) = \frac{1}{2}(\frac{n}{\ell} - 1)(2\ell - 4 - \frac{n}{\ell}) > 0.$$

The two right hand factors are positive integers. If the second one equals 1, then

$$\delta = \frac{1}{2}(2\ell - 5 - 1) = \ell - 3 = c_1.$$

Otherwise, $\delta \ge n/\ell - 1 \ge \ell - 1 > \ell - 3 = c_1$. Thus the assumptions in (4.8) hold with $c = c_1$, and since $\#E \le 3$, we have $\mu \le 2$ and $\beta \le 2wq^{-c} = \beta_{r,n}$. This shows (4.7) in case 1.

In case 2, we have $E = \{\ell, 2\ell - 3, n\}, m = \ell$, and

$$\begin{aligned} u(\ell) - u(n) &= \ell - 2, \\ u(\ell) - u(2\ell - 3) &= \frac{1}{2}(\ell - 3)(3\ell - 2). \end{aligned}$$

The minimum of these two values is $\ell - 2$ when $\ell \ge 5$. Then $\delta = \ell - 2 = c_2$, and furthermore $\mu = 2$ and $w = 1$. This implies (4.7) in case 2, when $\ell \ge 5$. For $\ell = 3$, we have $n = 9$, $E = \{3, 9\}$, $u(3) = 10$, $u(9) = 9$, $\delta = 1 = \ell - 2 = c_2$, $\mu = 1$, and $w = 1$. Thus $\beta = q^{-c_2} < \beta_{r,n}$, and (4.7) again holds.

In case 3, we have $E = \{2, 4\}$, $\ell = m = 2$, $w = \mu = 1$,

$$\delta = u(2) - u(4) = \binom{r+1}{2} - 2 = c_3 \geq 1,$$

and (4.7) holds.

In case 4, we have $m = \ell < n$, and introduce $\ell^* = n\ell/(n-\ell) \in \mathbb{Q}$. Thus $\ell^*$ is an integer only when $n$ is 4 or 6. We first claim that

$$u(n) \leq u(\ell^*). \tag{4.10}$$

We start with the subcase $r \geq 3$ and have to show that

$$\binom{r+a-1}{r} + \frac{n}{a-1} - 3 = u(\ell^*) \geq u(n) = r + n - 2. \tag{4.11}$$

We first treat the subcase $a \geq 5$. Then $a^3 \geq 3a^2 + 4a + 12$, so that the first inequality in

$$\begin{aligned} \frac{1}{a-1}\binom{r+a-2}{a-2} &= \frac{1}{r+a-1}\binom{r+a-1}{r} \\ &\geq 1 + \frac{a^2}{r+a-1} \geq 1 + \frac{n}{r+a-1} \end{aligned} \tag{4.12}$$

is valid for $r = 3$, and for all $r \geq 3$ since the left hand side is monotonically increasing and the right hand side decreasing in $r$. Using (4.6), this yields (4.11).

In the remaining subcase $r \geq 3$ and $a \leq 4$, we have $n \in \{4, 6, 8, 9\}$. Case 3 covers $n = 4$. The inequality between the outer terms in (4.12) holds for the following values of $(r, n)$: $(4, 6)$, $(3, 8)$, and $(4, 9)$, and by monotonicity for these values of $n$ and any larger $r$. One checks (4.11) for $(3, 6)$ and $(3, 9)$.

We next have the subcase $r = 2$ and $a \geq 3$. Then

$$\begin{aligned} u(n) - u(\ell^*) &= \frac{a-2}{2a-2} \cdot (2n - a^2 - 2a + 3), \\ u(n) > u(\ell^*) &\iff 2a\ell = 2n > a^2 + 2a - 3 \\ &\iff 2\ell > a + 2 - \frac{3}{a} \iff 2\ell \geq a + 2 \iff 2\ell - 2 \geq a. \end{aligned} \tag{4.13}$$

By assumption, (3.1) does not hold, and if (4.13) is positive, then $2\ell - 4 \leq a \leq 2\ell - 2$ follows. If $a$ is even, then $\ell = 2$, and one finds that $n = 4$, which is case

3. So the only remaining possibility is $a = 2\ell - 3$. Since each prime divisor of $a$ is at least $\ell$, $a$ is prime. But this is case 2, and therefore (4.10) holds.

For the remaining possibility $a = 2$, we find $\ell = 2$ and $n = 4$, which has been dealt with. We conclude that (4.10) always holds in case 4.

We have

$$\ell^2 + 2\ell < 2n$$

for all $n \neq 4$, since this follows from $n \geq \ell^2$ when $\ell \geq 3$, and also for $\ell = 2$. This implies that

$$\ell^* - \ell = \frac{\ell}{n/\ell - 1} < 2.$$

For any $e \in E \smallsetminus \{\ell\}$, we have $\ell < e \leq n$ and $n/e < n/\ell$. These values are both integers, so that

$$\frac{n}{e} \leq \frac{n}{\ell} - 1 = \frac{n}{\ell^*}.$$

Thus $\ell^* \leq e \leq n$ for all $e \in E \smallsetminus \{\ell\}$. By (4.10) and the convexity of $u$, the maximal value of $u(e)$ for these $e$ is at most $\max\{u(\ell^*), u(n)\} = u(\ell^*)$. In (4.8) we have

$$\begin{aligned}\delta \geq u(\ell) - u(\ell^*) &= \binom{r + n/\ell}{r} - \binom{r - 1 + n/\ell}{r} + \ell - \ell^* \\ &= \binom{r - 1 + n/\ell}{r - 1} + \ell - \ell^* > c_4 + 1 - 2 = c_4 - 1.\end{aligned}$$

Since $\delta$ and $c_4$ are integers, we also have $\delta \geq c_4$. Furthermore, we have $w = 1$ and $\mu \leq 2(1 - q^{-1})^{-1}$, so that $\beta \leq \beta_{r,n}$. Then the assumptions in (4.8) hold with $c = c_4$, and (4.7) follows.

In the next stage, we derive the lower bound in (ii) on the number $\#I_{r,n}$ of indecomposable polynomials. The previous results yield

$$\#P_{r,n} - \#I_{r,n} = \#D_{r,n} \leq \alpha_{r,n}(1 + \beta_{r,n}).$$

The claim in (ii) is that the last expression is at most $2\alpha_{r,n}$, that is, $\beta_{r,n} \leq 1$. Again, we distinguish according to our four cases.

For case 1, we have $\ell \geq 5$ and $(1 - q^{-2})^{-1} \leq 4/3$, and thus $\beta_{r,n} < \frac{8}{3} q^{-\ell+3} \leq \frac{8}{3} \cdot 2^{-2} < 1$.

In case 2, we have $\ell \geq 3$ and

$$\beta_{r,n} = 2q^{-\ell+2} \leq q^{-\ell+3} \leq 1.$$

In case 3, we have $c_3 = \binom{r+1}{2} - 2 \geq 1 > 0$ and $\beta_{r,4} = q^{-c_3} < 1$.

In case 4, we have $\beta_{r,n} \leq 4q^{-c_4} \leq q^{2-c_4}$, so that it is sufficient to show that $c_4 \geq 2$. We have $r, a \geq 2$ and

$$c_4 + 1 = \binom{r-1+a}{r-1} \geq \binom{r+1}{r-1} = \frac{r \cdot (r+1)}{2} \geq 3.$$

This concludes the proof of (ii).

In the last stage, we estimate the number of decomposable polynomials from below. The idea is obvious: we take the largest type of decomposable polynomials, as identified above, and then use only indecomposable polynomials as right components, so that the uniqueness property of Fact 2.4 applies. We have

$$\begin{aligned}\#D_{r,n} &\geq \#D_{r,n,m} \geq \#(P_{1,m} \times I^0_{r,n/m}) \geq q^{m-1}(\#P_{r,n/m} - 2\alpha_{r,n/m}) \\ &= q^{b_{r,n/m}+m-3}(1 - \frac{2\alpha_{r,n/m}}{\#P_{r,n/m}})\frac{1-q^{-b_{r-1,n/m}}}{1-q^{-1}} = \alpha_{r,n} \cdot (1 - \frac{2\alpha_{r,n/m}}{\#P_{r,n/m}}).\end{aligned}$$

In the cases 2 and 3, $n/m$ is prime, $\beta_{r,n/m} = 0$, and we could replace the factor 2 in the last expression by 1; however, we do not need this in the following. In order to prove the lower bound $\#D_{r,n} \geq \alpha_{r,n}(1 - \beta_{r,n})$ in (i), we proceed according to our four cases. In case 1, we have $r = 2$, (3.1) holds, $m = n$, $I_{r,1} = P_{r,1}$, and

$$\#D_{r,n} \geq \#D_{r,n,n} = \#(P_{1,n} \times P_{2,1}) = q^n(1 + q^{-1}) = \alpha_{r,n}. \tag{4.14}$$

For the remaining three cases, we have $m = \ell$ and claim that

$$\frac{2\alpha_{r,n/\ell}}{\#P_{r,n/\ell}} \leq \beta_{r,n}, \tag{4.15}$$

from which the lower bound follows:

$$\#D_{r,n} \geq \alpha_{r,n} \cdot (1 - \frac{2\alpha_{r,n/\ell}}{\#P_{r,n/\ell}}) \geq \alpha_{r,n} \cdot (1 - \beta_{r,n}).$$

We denote by $m^*$ the quantity defined in (3.3) for the argument $a = n/\ell$ instead of $n$ (and hence using the smallest prime divisor of $n/\ell$ instead of $\ell$), and set $d = a/m^* = n/\ell m^*$. Thus $m^*$ is either $a$ or its smallest prime divisor, $a = m^*d \geq 2d \geq 2$, and

$$\frac{2\alpha_{r,a}}{\#P_{r,a}} = \frac{2q^{-c^*}(1 - q^{-b_{r-1,d}})}{1 - q^{-b_{r-1,a}}} \leq 2q^{-c^*}, \tag{4.16}$$

with

$$c^* = \binom{r+a}{r} - \binom{r+d}{r} - m^* + 1.$$

It is therefore sufficient for (4.15) to show

$$2q^{-c^*} \le \beta_{r,n}. \tag{4.17}$$

In case 2, $m^* = a = n/\ell = 2\ell - 3$ is prime, and

$$\begin{aligned} c^* &= (2\ell-1)(\ell-2) > \ell - 2, \\ 2q^{-c^*} &< 2q^{-(\ell-2)} = \beta_{2,n}, \end{aligned}$$

and (4.17) is satisfied.

In case 3, we have $n = 4$, $\ell = 2$, $a = m^* = 2$, $d = 1$, $c^* = \binom{r+1}{2} - 1$, and thus

$$2q^{-c^*} \le q \cdot q^{-\binom{r+1}{2}+1} = \beta_{r,4}.$$

In case 4, we have

$$\beta_{r,n} = \frac{2q^{-c_4}}{1-q^{-1}} > 2q^{-c_4},$$

and it is sufficient for (4.17) to show that

$$c^* \ge c_4, \tag{4.18}$$

which in turn amounts to showing that

$$\binom{r-1+a}{r} = \binom{r+a}{r} - \binom{r-1+a}{r-1} \ge \binom{r+d}{r} + m^* - 2, \tag{4.19}$$

using Pascal's identity. We prove this by induction on $r \ge 2$. For $r = 2$, we use $a = m^* d \ge m^* \ge 2$. Thus

$$a^2 + a - (\frac{a}{m^*})^2 - 3\frac{a}{m^*} = \frac{a}{(m^*)^2}\big(a((m^*)^2 - 1) + (m^*)^2 - 3m^*\big) \ge 2m^* - 2,$$

since the inequality holds for $a = m^*$ and the middle term is monotonically increasing in $a$ for $m^* \ge 2$. It follows that

$$a^2 + a \ge (\frac{a}{m^*})^2 + 3\frac{a}{m^*} + 2m^* - 2,$$

which implies (4.19) for $r = 2$.

For the induction step, we have $a-1 \geq a/2 \geq a/m^* = d$, and

$$\binom{r+a-1}{r} - \binom{r+d}{r} \geq \binom{r-1+a-1}{r-1} - \binom{r-1+d}{r-1} \geq m^* - 2,$$

again by Pascal.

This finishes the proof of (i), and it remains to prove (iii) and (iv). We may assume $n$ to be composite. Since $D^{\mathrm{sl}}_{r,n} \subseteq D_{r,n} = D^{\mathrm{sl}}_{r,n} \cup \operatorname{im} \gamma_{r,n,n}$, the upper bound on $\#D_{r,n}$ in (i) also holds for $\#D^{\mathrm{sl}}_{r,n}$, and the lower bound does unless $m = n$. Thus (iii) and (iv) follow unless (3.1) holds, which we now assume.

Since $n/\ell \geq \ell$, we have $1 - q^{-n/\ell-1} \geq 1 - q^{-\ell-1}$. Using (3.10), we find

$$\begin{aligned}
\#D^{\mathrm{sl}}_{2,n} &\leq \#(P_{1,\ell} \times P_{2,n/\ell}) + \#(P_{1,n/\ell} \times P_{2,\ell}) \\
&= \alpha^{\mathrm{sl}}_{2,n}(1 + q^{-(n+\ell^2+\ell)(n-\ell^2)/2\ell^2} \frac{1-q^{-\ell-1}}{1-q^{-n/\ell-1}}) \leq \alpha^{\mathrm{sl}}_{2,n}(1+\beta^{\mathrm{sl}}_{2,n}), \\
\#D^{\mathrm{sl}}_{2,n} &\geq \#(P_{1,\ell} \times I^0_{2,n/\ell}) \\
&\geq \#P_{1,\ell} \cdot (\#P_{2,n/\ell} - 2\alpha_{2,n/\ell}) \cdot \frac{\#P_{2,n/\ell}}{\#P_{2,n/\ell}} \\
&= \alpha^{\mathrm{sl}}_{2,n}(1 - 2q^{-(n+2\ell)(n-\ell)/2\ell^2} \frac{1-q^{-2}}{1-q^{-n/\ell-1}}) \\
&\geq \alpha^{\mathrm{sl}}_{2,n}(1 - q^{-(n+2\ell)(n-\ell)/2\ell^2+1}) \\
&> \alpha^{\mathrm{sl}}_{2,n}(1-\beta^{\mathrm{sl}}_{2,n}).
\end{aligned}$$

If $n = \ell^2$, then $D^{\mathrm{sl}}_{2,n} = D_{2,n,\ell}$ and

$$\begin{aligned}
&\#D^{\mathrm{sl}}_{2,n} \leq \#(P_{1,\ell} \times P_{2,\ell}) = \alpha^{\mathrm{sl}}_{2,n}, \\
&\#D^{\mathrm{sl}}_{2,n} \geq \#(P_{1,\ell} \times I^0_{2,\ell}) \geq \alpha^{\mathrm{sl}}_{2,n}(1 - \beta^{\mathrm{sl}}_{2,n} \frac{1-q^{-2}}{1-q^{-\ell-1}}) \geq \alpha^{\mathrm{sl}}_{2,n}(1-\beta^{\mathrm{sl}}_{2,n}). \qquad \square
\end{aligned}$$

When $r \geq 2$ and $n = \ell$ is prime, then $\#D_{r,n} = \alpha_{r,n}$ and

$$\begin{aligned}
\#I_{r,n} &= \#P_{r,n} - \alpha_{r,n} \\
&= q^{\binom{r+n}{r}-2} \frac{1-q^{-\binom{r-1+n}{r-1}}}{1-q^{-1}} - q^{r+n-2} \frac{1-q^{-r}}{1-q^{-1}}.
\end{aligned} \tag{4.20}$$

Remark 4.21. *In the simple case where $n$ has exactly two prime factors and $r \geq 2$, it is easy to determine $\#D_{r,n}$ exactly. For $n = \ell^2$,*

$$D_{r,n} = \{g \circ h \colon g \in P_{1,\ell}, h \in I_{r,\ell}\} \cup D_{r,n,n}$$

*is a disjoint union. We have*

$$\#D_{r,n} = \begin{cases} \alpha_{r,n} + q^{(n+\ell-4)/2}\frac{1-q^{-\ell-1}}{1-q^{-1}} - \alpha_{r,n}\cdot q^{-(\ell-1)^2} & \text{if } r=2 \text{ and } \ell \geq 5, \\ \alpha_{r,n} + q^{n+r-2}(1-q^{-r})(1-q^{2\ell-n-1}) & \text{otherwise.} \end{cases}$$

*The first case corresponds to (3.1). We set*

$$\beta'_{r,n} = \begin{cases} q^{-(\ell-1)(\ell-4)/2}\dfrac{1-q^{-\ell-1}}{1-q^{-2}} - q^{-(\ell-1)^2} & \text{if } r=2 \text{ and } \ell \geq 5, \\ q^{-\binom{r+n/\ell}{r}+n+r+1-\ell}\dfrac{(1-q^{-r})(1-q^{2\ell-n-1})}{1-q^{-\binom{r-1+n/\ell}{r-1}}} & \text{otherwise.} \end{cases}$$

*Then*

$$\#D_{r,n} = \alpha_{r,n}(1+\beta'_{r,n}).$$

*This value is exact, in contrast to the estimates of Theorem 4.1, and* $\beta'_{r,n}$ *is often much smaller than* $\beta_{r,n}$*. The drawback is that the values are more complicated, and an attempt to generalize this approach to more than two prime factors of* $n$ *does not seem to lead to manageable results.*

*If* $n > \ell^2$ *and* $n/\ell$ *is prime, then one finds similarly that*

$$\begin{aligned} \#D_{r,n} = {} & q^{b_{r,n/\ell}+\ell-1}(1-q^{-b_{r-1,n/\ell}}) + q^{b_{r,\ell}+n/\ell-1}(1-q^{b_{r-1,\ell}}) \\ & + q^{n+r}(1-q^{-r})(1-2q^{\ell+n/\ell-n-1}). \end{aligned}$$

*Here it is not even transparent which of the summands is the dominating one. However, using the case distinction of (3.1), one again obtains a quantity* $\beta'_{r,n}$*, so that* $\#D_{r,n} = \alpha_{r,n}(1+\beta'_{r,n})$*. The previous remarks apply to this solution as well.*

Table 4.1 compares the exact results with the approximations of Theorem 4.1 for $r = 2$ variables and degree $n \leq 6$ and $n \in \{25, 26\}$. We have $\ell = m$ in all of these cases, except for $n = 25$.

For all $r$ and $n$ where $\beta'_{r,n}$ is defined, we have $\beta'_{r,n} \leq \beta_{r,n}$. For $n = 4$ or 6 in Table 4.1, we have

$$\begin{aligned} \beta_{2,4} &= \beta'_{2,4} + q^{-2}\frac{1+2q^{-1}}{1+q^{-1}+q^{-2}}, \\ \beta_{2,6} &= \beta'_{2,6} + q^{-4}\frac{2+5q^{-1}+3q^{-2}-2q^{-3}}{1-q^{-4}}, \\ \beta_{2,25} &= \beta'_{2,25} - 2q^{-16}. \end{aligned}$$

| $n$ | $\#D_{2,n}$ | $\alpha_{2,n}$ | $\beta'_{2,n}$ | $\beta_{2,n}$ |
|---|---|---|---|---|
| 2 | $q^2+q$ | $q^2+q$ | $0$ | $0$ |
| 3 | $q^3+q^2$ | $q^3+q^2$ | $0$ | $0$ |
| 4 | $q^5+2q^4+q^3-q^2$ | $q^5+q^4+q^3$ | $q^{-1}\dfrac{1-q^2}{1+q^{-1}+q^{-2}}$ | $q^{-1}$ |
| 5 | $q^5+q^4$ | $q^5+q^4$ | $0$ | $0$ |
| 6 | $q^9+q^8+q^7+3q^6$ $+2q^5-q^4-2q^3$ | $q^9+q^8+q^7+q^6$ | $q^{-3}\dfrac{2+2q^{-1}-q^{-2}-2q^{-3}}{1+q^{-1}+q^{-2}+q^{-3}}$ | $\dfrac{2q^{-3}}{1-q^{-1}}$ |
| 25 | $q^{25}+q^{24}+2q^{23}+2q^{22}$ $+2q^{21}+2q^{20}+2q^{19}$ $+2q^{18}-2q^9-2q^{-8}$ | $q^{25}+q^{24}$ | $2q^{-2}+2q^{-4}$ $+2q^{-6}-2q^{-16}$ | $2q^{-2}+2q^{-4}$ $+2q^{-6}$ |
| 26 | $q^{104}\frac{1-q^{-14}}{1-q^{-1}}+q^{26}+q^{25}$ $+q^{16}+q^{15}-q^{14}-2q^{13}$ | $q^{104}\dfrac{1-q^{-14}}{1-q^{-1}}$ | $q^{-78}(1+q^{-1}+q^{-10}$ $+q^{-11}-q^{-12}-2q^{-13})\cdot\dfrac{1-q^{-1}}{1-q^{-14}}$ | $\dfrac{2q^{-13}}{1-q^{-1}}$ |

Table 4.1: Exact values and bounds for $r=2$ and seven values of $n$.

The differences are small, but $\beta_{2,26}\approx 2q^{-13}$ and $\beta'_{2,26}\approx q^{-78}$ differ by many orders of magnitude.

Bodin *et al.* (2009) obtain results similar to those of Remark 4.21. They also show that $\#I_{r,n}/\#P^{=}_{r,n}\to 1$ as $n\to\infty$ (see Theorem 4.1(ii)). Their methods do not lead to a unified formula as in Theorem 4.1(i), and the error bounds are weaker than the present ones by factors of $O(n)$ or $O(q)$. They did not discover the special case (3.1), where the result is different from the generic one.

If $u_{2,n}(e)=u_{2,n}(e')$ never happened for distinct divisors $e$, $e'\ge 2$ of $n$, we could save a factor of 2 in $\beta_{2,n}$. However, if we take two arbitrary positive integers $k\ge 2$ and $m$, set $e=2km^2+2m^2+3m$, $e'=ke$, and $n=2mke$, then $e<e'$ and $u_{2,n}(e)=u_{2,n}(e')$. The smallest such choice gives $n=36$, $e=9$, $e'=18$.

We can unify cases 2 and 4 in (4.3), and the other cases fit in trivially. We set

$$\begin{aligned} c_{r,n,5} &= \frac{1}{2}\binom{r-1+n/\ell}{r-1}-1, \\ \beta^*_{r,n} &= \frac{2q^{-c_{r,n,5}}}{1-q^{-1}}. \end{aligned} \tag{4.22}$$

COROLLARY 4.23. *Let $D_{r,n}$ be the set of decomposable polynomials of degree $n \geq 2$ in $r \geq 2$ variables over $\mathbb{F}_q$, and $\alpha_{r,n}$ and $\beta^*_{r,n}$ as in (4.2) and (4.22), respectively. Then*

$$|\#D_{r,n} - \alpha_{r,n}| \leq \alpha_{r,n} \cdot \beta^*_{r,n}.$$

PROOF. It is sufficient to show that $\beta_{r,n} \leq \beta^*_{r,n}$ in all cases. This is an easy calculation. □

Introducing the second largest nontrivial divisor of $n$ as an additional parameter would sharpen some of the bounds in Theorem 4.1 and simplify the proof. However, the resulting estimates woould be harder to use, and some effort was spent on avoiding this sparameter.

How close is our relative error estimate $\beta_{r,n}$ to being exponentially decaying in the input size? In the "general" Case 4 of (4.3), $\beta_{r,n}$ is about $q^{-c_4}$ with $c_4$ approximately $b_{r-1,n/\ell} = \binom{r-1+n/\ell}{r-1}$. Definitions (4.22) and Corollary 4.23 relate also the special cases to this.

The (usual) dense representation of a polynomial in $r$ variables and of degree at most $n$ requires $b_{r,n} = \binom{r+n}{r}$ monomials, each of them equipped with a coefficient from $\mathbb{F}_q$, using about $\log_2 q$ bits. Thus the total input size is about $\log_2 q \cdot b_{r,n}$ bits. Now $\log_2 q \cdot b_{r,n/\ell}$ differs from $\log_2 \beta_{r,n}$ by a factor of $1 + \frac{n}{r\ell}$. Furthermore, $n$ and $n/\ell$ are polynomially related, since $n > n/\ell \geq \sqrt{n}$. Up to these polynomial differences (in the exponent), $\beta_{r,n}$ is exponentially decaying in the input size. Furthermore $\beta_{r,n}$ is exponentially decaying in any of the parameters $r$, $n$ and $\log_2 q$, when the other two are fixed.

We compare our results to those of von zur Gathen (2008d) on the number $\#R_n$ of reducible and $\#E_n$ of relatively irreducible (irreducible and not absolutely irreducible) bivariate polynomials. Ignoring factors close to 1 and special cases like (3.1), we have for composite $n$

$$\begin{aligned}
\#R_n &\approx q^{\binom{n+2}{2}-n+1} \\
\#E_n &\approx q^{\binom{n+2}{2}-\frac{n^2(\ell-1)}{2\ell}} \\
\#D_{2,n} &\approx q^{\binom{n/\ell+2}{2}+\ell-1}.
\end{aligned}$$

The first exponent is always greater than the third one, and for the second and third ones we have

$$\binom{n+2}{2} - \frac{n^2(\ell-1)}{2\ell} - \binom{n/\ell+2}{2} - \ell + 1 = \frac{(\ell-1)(n^2+3n\ell-2\ell^2)}{2\ell^2} > 0.$$

In other words, there are many more reducible or relatively irreducible bivariate polynomials than decomposable ones, as one would expect.

Open Question 4.24. *Can one (im)prove Theorem 4.1 with higher-level methods, hopefully avoiding some of the case distinctions?*

## 5. Acknowledgements

I appreciate the interesting discussions with Arnaud Bodin, Pierre Dèbes, and Salah Najib about the topic, and in particular the challenges that the preliminary version of Bodin *et al.* (2009) posed.

A first version of this paper is in von zur Gathen (2008b). The work was supported by the B-IT Foundation and the Land Nordrhein-Westfalen.

## References

Arnaud Bodin, Pierre Dèbes & Salah Najib (2009). Indecomposable polynomials and their spectrum. *Acta Arithmetica* **139(1)**, 79–100.

Jean-Charles Faugère & Ludovic Perret (2008). High Order Derivatives and Decomposition of Multivariate Polynomials. In *Extended Abstracts of the Second Workshop on Mathematical Cryptology WmC 08*, Álvar Ibeas & Jaime Gutiérrez, editors, 90–93. URL `http://grupos.unican.es/amac/wmc-2008/`.

Joachim von zur Gathen (2008a). Correction to "Counting reducible and singular bivariate polynomials".

Joachim von zur Gathen (2008b). Counting decomposable multivariate polynomials. *Preprint,* 21 pages. URL `http://arxiv.org/abs/0811.4726`.

Joachim von zur Gathen (2008c). Counting decomposable univariate polynomials. *Preprint,* 92 pages. URL `http://arxiv.org/abs/0901.0054`. Extended abstract see von zur Gathen (2009). For a correction see von zur Gathen (2008a).

Joachim von zur Gathen (2008d). Counting reducible and singular bivariate polynomials. *Finite Fields and Their Applications* **14**(4), 944–978. URL `http://dx.doi.org/10.1016/j.ffa.2008.05.005`. Extended abstract in *Proceedings of the 2007 International Symposium on Symbolic and Algebraic Computation ISSAC2007,* Waterloo, Ontario, Canada (2007), 369-376.

Joachim von zur Gathen (2009). The Number of Decomposable Univariate Polynomials. In *Proceedings of the 2009 International Symposium on Symbolic and Algebraic Computation ISSAC2009,* Seoul, Korea, John P. May, editor, 359–366. ISBN 978-1-60558-609-0.

Joachim von zur Gathen, Mark Giesbrecht & Konstantin Ziegler (2010a). Composition collisions and projective polynomials – Statement of results. In *Proceedings of the 2010 International Symposium on Symbolic and Algebraic Computation ISSAC2010,* Munich, Germany, Stephen Watt, editor, 123–130. ACM Press. Preprint available at `http://arxiv.org/abs/1005.1087`.

Joachim von zur Gathen, Mark W. Giesbrecht & Konstantin Ziegler (2010b). Composition collisions and projective polynomials. URL `http://arxiv.org/abs/1005.1087`. Extended abstract see von zur Gathen *et al.* (2010a).

Joachim von zur Gathen, Jaime Gutierrez & Rosario Rubio (2003). Multivariate polynomial decomposition. *Applicable Algebra in Engineering, Communication and Computing* **14**, 11–31. URL `http://dx.doi.org/10.1007/s00200-003-0122-8`. Extended abstract in *Proceedings of the Second Workshop on Computer Algebra in Scientific Computing, CASC '99,* München, Germany (1999), 463-478.

Joachim von zur Gathen, Alfredo Viola & Konstantin Ziegler (2010c). Counting Reducible, Powerful, and Relatively Irreducible Multivariate Polynomials over Finite Fields (Extended Abstract). In *Proceedings of LATIN 2010,* Oaxaca, Mexico, Alejandro López-Ortiz, editor, volume 6034 of *Lecture Notes in Computer Science*, 243–254. Springer-Verlag, Berlin, Heidelberg. ISBN 978-3-642-12199-9. ISSN 0302-9743 (Print) 1611-3349 (Online). URL `http://dx.doi.org/10.1007/978-3-642-12200-2_23`.

Mark William Giesbrecht (1988). Complexity Results on the Functional Decomposition of Polynomials. Technical Report 209/88, University of Toronto, Department of Computer Science, Toronto, Ontario, Canada. Available as `http://arxiv.org/abs/1004.5433`.

## 6. Appendix: Some calculations

Section 3

$$u_{r,n} = \binom{r+\frac{n}{e}}{r} + e - 1 = \frac{(r+\frac{n}{e})^{\underline{r}}}{r!} + e - 1 = \frac{1}{r!}\prod_{1\le i\le r}(i+\frac{n}{e}) + e - 1,$$

$$u'_{r,n} = 1 + \frac{1}{r!}\sum_{1\le i\le r}\prod_{\substack{1\le j\le r\\ j\neq i}}(j+\frac{n}{e})\cdot\frac{-n}{e^2},$$

$$u''_{r,n} = \frac{1}{r!}\sum_{1\le i\le r}\Big(\sum_{\substack{1\le j\le r\\ j\neq i}}\prod_{\substack{1\le k\le r\\ k\neq i,j}}(k+\frac{n}{e})\cdot(\frac{-n}{e^2})^2 + \prod_{\substack{1\le j<r\\ j\neq i}}(j+\frac{n}{e})\cdot\frac{2n}{e^3}\Big)$$

$$v_r(2) = \binom{r+2}{r} + 2 - 1 - (r+4) = \frac{1}{2}(r^2+3r+2-2r-6)$$
$$= \frac{1}{2}(r^2+r-4).$$

$$u_{2,n}(\ell) - u_{2,n}(n) = \binom{2+n/\ell}{2} + \ell - 3 - (3+n-3)$$
$$= \frac{(n+2\ell)(n+\ell)}{2\ell^2} + \ell - n - 3$$
$$= \frac{n^2+3n\ell+2\ell^2+2\ell^3-2n\ell^2-6\ell^2}{2\ell^2}$$
$$= \frac{n^2+3n\ell-4\ell^2-2n\ell^2+2\ell^3}{2\ell^2}$$
$$= \frac{(n-\ell)(n+4\ell-2\ell^2)}{2\ell^2},$$

$$n + 4\ell_0 - 2\ell_0^2 = n + 4 + 2\sqrt{2n+4} - 2(1+\sqrt{2n+4} + (2n+4)/4) = 0.$$

$$\ell > \ell_0 \Longleftrightarrow n + 4\ell - 2\ell^2 < 0 \Longleftrightarrow n/\ell < 2\ell - 4,$$
$$\frac{(r+2)^{\underline{r}}}{(r+1)!} = \frac{(r+2)\cdots 4\cdot 3}{(r+1)!} = \frac{r+2}{2} > 1,$$

$$\begin{aligned}
u_{2,n}(\ell) - u_{2,n}(n/\ell) &= \binom{2+\frac{n}{\ell}}{2} + \ell - 3 - (\binom{2+\ell}{2} + \frac{n}{\ell} - 3) \\
&= \frac{1}{2\ell^2}((n+2\ell)(n+\ell) + 2\ell^3 - 2n\ell - \ell^2(\ell+2)(\ell+1)) \\
&= \frac{1}{2\ell^2}(n^2 + 3n\ell + 2\ell^2 + 2\ell^3 - 2n\ell - \ell^4 - 3\ell^3 - 2\ell^2) \\
&= \frac{1}{2\ell^2}(n^2 + n\ell - \ell^3 - \ell^4) \\
&= \frac{1}{2\ell^2}(n-\ell^2)(n+\ell+\ell^2).
\end{aligned}$$

Section 4
Theorem 4.1, Case 1, (3.1) holds:

$$\begin{aligned}
u(n) - u(\ell) &= \binom{2+1}{2} + n - 1 - (\binom{2+n/\ell}{2} + \ell - 1) \\
&= \frac{1}{2}(-(\frac{n}{\ell}+2)(\frac{n}{\ell}+1) + 2n - 2\ell + 6) \\
&= \frac{1}{2}(-(\frac{n}{\ell})^2 - \frac{3n}{\ell} + 2n - 2\ell + 4) \\
&= \frac{1}{2}(\frac{n}{\ell} - 1)(2\ell - 4 - \frac{n}{\ell}).
\end{aligned}$$

Case 2: substitute $n/\ell = 2\ell - 3$ into previous equation:

$$\begin{aligned}
u(\ell) - u(n) &= -\frac{1}{2}(2\ell - 4)(-1) \\
&= \ell - 2,
\end{aligned}$$

$$\begin{aligned}
u(n) - u(2\ell-3) &= \binom{2+1}{2} + n - 1 - (\binom{2+\ell}{2} + 2\ell - 3 - 1) \\
&= \frac{1}{2}(-(\ell+2)(\ell+1) + 2\ell(2\ell-3) - 4\ell + 12) \\
&= \frac{1}{2}(-\ell^2 - 3\ell - 2 + 4\ell^2 - 6\ell - 4\ell + 12) \\
&= \frac{1}{2}(3\ell^2 - 13\ell + 10) \\
&= \frac{1}{2}(3\ell - 10)(\ell - 1).
\end{aligned}$$

Theorem 4.1, Case 3, $n = 4$

$$\begin{aligned} u(2) - u(4) &= \binom{r+2}{r} + 2 - 1 - (\binom{r+1}{r} + 4 - 1) \\ &= \binom{r+1}{r-1} - 2, \\ \#D_{r,4} &\le q^{u(2)}(1 - q^{-b_{r-1,2}}) + q^{u(4)}(1 - q^{-b_{r-1,1}}) \\ &\le \alpha_{r,4}(1 - q^{-u(2)+u(4)}). \end{aligned}$$

Theorem 4.1(i), Case 4:

$$\begin{aligned} \ell_0 \in \mathbb{Z} &\Rightarrow n - \ell \mid n\ell \Rightarrow \frac{n}{\ell} - 1 \mid n \\ &\Rightarrow \frac{n}{\ell} \cdot (\frac{n}{\ell} - 1) \mid n \Rightarrow \frac{n^2}{\ell^2} - \frac{n}{\ell} = \frac{n}{\ell}(\frac{n}{\ell} - 1) \le n \\ &\Rightarrow n \le \ell(\ell+1) \Rightarrow n = \ell^2 \text{ or } n = \ell(\ell+1). \end{aligned}$$

If $n = \ell^2$, then $\ell - 1 \mid \ell^2$, hence $\ell = 2$. If $n = \ell(\ell+1)$ and $\ell \neq 2$, then $\ell + 1$ is not prime, hence has a prime factor less than $\ell$.

$$\begin{aligned} &6(a+2)(\frac{1}{3+a-1}\binom{3+a-1}{3} - (1 + \frac{a^2}{3+a-1})) \\ &= (a+2)(a+1)a - 6(a+2) - 6a^2 \\ &= a^3 + 3a^2 + 2a - 6a - 12 - 6a^2 \\ &= a^3 - 3a^2 - 4a - 12 \ge 0, \end{aligned}$$

$$\begin{aligned} &(r+a-1)\binom{r+a-2}{a-2} - (a-1)\binom{r+a-1}{r} \\ &= (r+a-1)\frac{(r+a-2)!}{(a-2)!r!} - (a-1)\frac{(r+a-1)!}{r!(a-1)!} = 0. \end{aligned}$$

$(r, n) = (4, 6); a = 3$ :

$$\frac{1}{2}\binom{5}{1} = \frac{5}{2} > 2 = 1 + \frac{6}{6},$$

$(r,n) = (3,8), a = 4$ :

$$\frac{1}{3}\binom{5}{2} = \frac{10}{3} > \frac{14}{6} = 1 + \frac{8}{6},$$

$(r,n) = (4,9), a = 3$ :

$$\frac{1}{2}\binom{5}{1} = \frac{5}{2} = 1 + \frac{9}{6}.$$

$(r,n) = (3,6), a = 3$ :

$$\binom{5}{3} + \frac{6}{2} - 1 = 12 > 9 = 3 + 6,$$

$(r,n) = (3,9), a = 3$ :

$$\binom{5}{3} + \frac{9}{2} - 1 = \frac{27}{2} > 12 = 3 + 9.$$

$r = 2$ :

$$\begin{aligned} u(n) - u(\ell_0) &= n + 2 - \binom{a+1}{2} - \frac{n}{a-1} + 1 \\ &= \frac{1}{2a-2}(2an - 2n + 4a - 4 - a^3 + a - 2n + 2a - 2) \\ &= \frac{1}{2a-2}(2an - 4n + 7a - 6 - a^3), \end{aligned}$$

$$\begin{aligned} (a-2)(2n - a^2 - 2a + 3) &= 2an - a^3 - 2a^2 + 3a - 4n + 2a^2 + 4a - 6 \\ &= 2an - a^3 + 7a - 4n - 6. \end{aligned}$$

$$\ell_0 - \ell = \frac{n - (\frac{n}{\ell} - 1)\ell}{\frac{n}{\ell} - 1} = \frac{\ell}{\frac{n}{\ell} - 1},$$

Theorem 4.1, lower bound in (i), case 0, $n$ prime:

$$\begin{aligned} \#(P^{=}_{1,n} \times P^{0}_{r,1}) &= q^{n+1}(1 - q^{-1}) \cdot q^{r+1-2}\frac{1 - q^{-r}}{1 - q^{-1}} \\ &= q^{r+n}(1 - q^{-r}) = \alpha_{r,n}. \end{aligned}$$

Cases 2,3 and 4:

$$\frac{2\alpha_{r,a}}{\#P^{=}_{r,a}} = \frac{2q^{\binom{r+a/m*}{r}+m*-1}(1-q^{-\binom{r-1+a/m*}{r-1}})}{q^{\binom{r+a}{r}}(1-q^{-\binom{r-1+a}{r-1}})}.$$

Case 2: $m* = a = 2\ell - 3$, $d = 1$,

$$\begin{aligned} c* &= \binom{2+2\ell-3}{2} - \binom{2+1}{2} - (2\ell-3) + 1 \\ &= \frac{1}{2}(2\ell-1)(2\ell-2) - 2\ell + 1 = (2\ell-1)(\ell-2). \end{aligned}$$

$$\begin{aligned} \frac{2\alpha_{2,2\ell-3}}{\#P^{=}_{2,2\ell-3}} &= \frac{2q^{-(2\ell-1)(\ell-2)}(1-q^{-2})}{1-q^{-2\ell+4}} \\ &\leq 2q^{-(2\ell-1)(\ell-2)} < 2q^{-(\ell-2)} = \beta_{2,n}. \end{aligned}$$

Case 3:

$$\begin{aligned} c^* &= \binom{r+2}{r} - \binom{r+1}{r} - 2 + 1 \\ &= \frac{(r+2)(r+1)}{2} - (r+1) - 1 = \frac{r(r+1)}{2} - 1. \end{aligned}$$

Case 4:

$$\begin{aligned} 6 \cdot (\binom{3-1+a}{3} - (2a^2 - 4a)) &= (a+2)(a+1)a - 12a^2 + 24a \\ &= a^3 + 3a^2 + 2a - 12a^2 + 24a \\ &= a^3 - 9a^2 + 26a \geq 0 \end{aligned}$$

Theorem 4.1(i), lower bound, case 4 with $r = 2$:

$$\begin{aligned} &2(\binom{a+2}{2} - (\binom{a+1}{1} + \binom{d+2}{2} + a - 2)) \\ &= (a+2)(a+1) - 2a - 2 - (d+2)(d+1) - 2a + 4 \\ &= a^2 - a - d^2 - 3d + 2 \geq 0. \end{aligned}$$

Cases covered: $r = 2$; $a > r \geq 3$; $d = 1$; $r \geq a$ and $d \geq 2$.

Case $r \ge a$, $d \ge 2$:

$$\begin{aligned} 3d < 4d - 1 \Rightarrow 1 &< \frac{4}{3} - \frac{1}{3d}, \\ 4 \cdot 6^4 = 5184 &< 7203 = 3 \cdot 7^4, \\ 4/3 = 1 + 3^{-1} &\le (4/3 - 1/6)^4 = (7/6)^4. \end{aligned}$$

$$\begin{aligned} r^2 &\ge 3r, \\ (r + n/\ell)(r - 1 + n/\ell) &= r^2 + 2rn/\ell + n^2/\ell^2 - r - n/\ell \\ &= 2r + n + (2r - 1)n/\ell. \end{aligned}$$

Lower bound on $D$, Case 3, $r = 3$, $a \ge r + 1$

$$\begin{aligned} &a^2 - 9a + 26 \ge 0, \\ &a^2 + 3a + 2 \ge 12a - 24, \\ &\frac{a(a^2 + 3a + 2)}{6} = a\binom{2 + a}{3} \ge 2a^2 - 4a = a(2a - 4). \\ &1 \ge \frac{2a(a - 2)}{\binom{r-1+a}{r}} = \frac{2a(a - 2) \cdot r!}{(r - 1 + a)\underline{r}} = \frac{2(a - 2) \cdot r}{\binom{r-1+a}{r-1}}, \\ &a \ge r + 1 \ge r + \frac{2r(a - 2)}{\binom{r-1+a}{r-1}}, \\ &\frac{\binom{r+a}{r}}{2\binom{r-1+a}{r-1}} = \frac{r + a}{2r} = \frac{1}{2} + \frac{a}{2r} \ge \frac{1}{2} + \frac{1}{2} + \frac{a - 2}{\binom{r-1+a}{r-1}}. \end{aligned}$$

Factor in $\beta_{r,n,1}$:

$$\begin{aligned} &a = n/\ell \ge 1, \\ &\frac{4}{3} \le \frac{1}{1 - q^{-2}} \le w = \frac{1 - q^{-a-1}}{1 - q^{-2}} \le \frac{1 - q^{-8}}{1 - q^{-2}} = 1 + q^{-2} + q^{-4} + q^{-6} \\ &\quad \le 1 + 2^{-2} + 2^{-4} + 2^{-6} = 1 + \frac{21}{64}. \end{aligned}$$

Theorem 4.1(i):

$$\begin{aligned}
u(n) - u(\ell^*) &= \binom{2+1}{2} + n - 1 - \left(\binom{2+\frac{n}{\ell^*}}{2} + \ell^* - 1\right) \\
&= 3 + n - \binom{2+a-1}{2} - \frac{n\ell}{n-\ell} \\
&= 3 + n - \frac{(a+1)\cdot a}{2} - \frac{n}{a-1} \\
&= \frac{1}{2a-2} \cdot ((3+n)(2a-2) - (a^2-1)\cdot a - 2n) \\
&= \frac{1}{2a-2}(6a - 6 + 2an - 2n - a^3 + a - 2n) \\
&= \frac{1}{2a-2}(2an - 4n + 7a - a^3 - 6) \\
&= \frac{a-2}{2a-2}(2n - a^2 + 2a - 3)
\end{aligned}$$

Theorem 4.1(iii), $r = 2$, (3.1) holds, $n > \ell^2$

$$\begin{aligned}
1 - q^{-\ell-1} &< 1 - q^{-n/\ell-1}, \\
2\ell^2 \cdot (&\frac{(\ell+2)(\ell+1)}{2} + \frac{n}{\ell} - 1 - (\frac{(\frac{n}{\ell}+2)(\frac{n}{\ell}+1)}{2} + \ell - 1)) \\
&= \ell^4 + 3\ell^3 + 2\ell^2 + 2n\ell - (n^2 + 3n\ell + 2\ell^2) - 2\ell^3 \\
&= -n^2 - n\ell + \ell^4 + \ell^3 = -(n-\ell^2)(n+\ell^2+\ell) \\
\#D_{2,n}^{s\ell} &\le q^{\binom{\ell+1}{1}-2} \cdot q^{\binom{2+n/\ell}{2}-2} \cdot \frac{1 - q^{-\binom{1+n/\ell}{1}}}{1-q^{-1}} \\
&\quad + q^{\binom{n/\ell+1}{1}-2} \cdot q^{\binom{2+\ell}{2}-2} \cdot \frac{1 - q^{-\binom{1+\ell}{1}}}{1-q^{-1}} \\
&= q^{(n/\ell+2)(n/\ell+1)/2+\ell-3} \frac{1 - q^{-1-n/\ell}}{1-q^{-1}} \\
&\quad + q^{(\ell+2)(\ell+1)/2+n/\ell-3} \frac{1 - q^{-1-\ell}}{1-q^{-1}} \\
&= \alpha_{2,n}^{s\ell}(1 + q^{-(n-\ell^2)(n+\ell^2+\ell)/2\ell^2} \cdot \frac{1 - q^{-\ell-1}}{1 - q^{-n/\ell-1}}),
\end{aligned}$$

$m = n$,

$$\begin{aligned}\alpha_{2,n/\ell} &= q^{\binom{2+1}{2}+\frac{n}{\ell}-1}(1-q^{-\binom{1+1}{1}}) \\ &= q^{n/\ell+2}(1-q^{-2}),\end{aligned}$$

$$\begin{aligned}\binom{n/\ell+2}{2} - \frac{n}{\ell} - 2 &= \frac{1}{2}((\frac{n}{\ell})^2 + \frac{3n}{\ell} + 2 - \frac{2n}{\ell} - 4) \\ &= \frac{1}{2}((\frac{n}{\ell})^2 + \frac{n}{\ell} - 2) = \frac{1}{2}(\frac{n}{\ell}+2)(\frac{n}{\ell}-1),\end{aligned}$$

$$\begin{aligned}\#D^{s\ell}_{2,n} &\geq \#P_{1,\ell}\cdot(\#P_{2,n/\ell} - \alpha_{2,n/\ell}) \\ &= q^{\ell-1}\cdot(q^{\binom{n/\ell+2}{2}-2}\frac{1-q^{-n/\ell-1}}{1-q^{-1}} - q^{n/\ell}\frac{1-q^{-2}}{1-q^{-1}}) \\ &= q^{\binom{n/\ell+2}{2}+\ell-3}\frac{1-q^{-n/\ell-1}}{1-q^{-1}}(1-q^{n/\ell+2-\binom{n/\ell+2}{2}}\frac{1-q^{-2}}{1-q^{-n/\ell-1}}) \\ &= \alpha^{\mathrm{sl}}_{2,n}(1-q^{-(n+2\ell)(n-\ell)/2\ell^2}\frac{1-q^{-2}}{1-q^{-n/\ell-1}}) \\ &\geq \alpha^{\mathrm{sl}}_{2,n}(1-q^{-(n+2\ell)(n-\ell)/2\ell^2}) \\ &> \alpha^{\mathrm{sl}}_{2,n}(1-q^{-(n+\ell^2+\ell)(n-\ell^2)/2\ell^2+1}) \\ &= \alpha^{\mathrm{sl}}_{2,n}(1-\beta^{\mathrm{sl}}_{2,n}),\end{aligned}$$

$(n+2\ell)(n-\ell) = n^2+n\ell-2\ell^2 > n^2+n\ell-\ell^4-\ell^3 = (n+\ell^2+\ell)(n-\ell^2)$.

$n=\ell^2$:

$$\#(P_{1,\ell}\times P_{2,\ell}) = q^{\ell+1}(1-q^{-1})\cdot q^{\binom{2+\ell}{2}-2}\frac{1-q^{-\ell-1}}{1-q^{-1}} = \alpha^{\mathrm{sl}}_{2,n},$$

$$\begin{aligned}\#(P_{1,\ell}\times I_{2,\ell}) &\geq \#P_{1,\ell}\cdot(\#P_{2,\ell}-\alpha_{2,\ell}) \\ &= \alpha^{s\ell}_{2,n}(1-\frac{\alpha_{2,\ell}}{\#P_{2,\ell}}) \\ &= \alpha^{s\ell}_{2,n}(1-q^{\ell-b_{2,\ell}+2}\frac{1-q^{-1}}{1-q^{-\ell-1}}) > \alpha^{s\ell}_{2,n}(1-q^{-b_{\ell,2}+\ell+2}) \\ &= \alpha_{2,n}(1-q^{-(\ell+2)(\ell-1)/2}) \\ &= \alpha_{2,n}(1-\beta^{s\ell}_{2,n}).\end{aligned}$$

Remark 4.21, $n = \ell^2$,

$$\begin{aligned}
\#I_{r,\ell} &= \#P_{r,\ell} - \alpha_{r,\ell} = q^{b_{r,\ell}-2}\frac{1-q^{-b_{r-1,\ell}}}{1-q^{-1}} - q^{\binom{r+1}{r}+\ell-3}\frac{1-q^{-\binom{r-1+1}{r-1}}}{1-q^{-1}} \\
&= q^{b_{r,\ell}-2}\frac{1-q^{-b_{r-1,\ell}}}{1-q^{-1}} - q^{r+\ell-2}\frac{1-q^{-r}}{1-q^{-1}}, \\
\#D_{r,n} &= \#P_{1,\ell}\cdot\#I_{r,\ell} + \#P_{1,n}\cdot\#P_{r,1} \\
&= q^{\ell+1-2}\ \frac{1-q^{-1}}{1-q^{-1}}\cdot\big(q^{b_{r,\ell}-2}\frac{1-q^{-b_{r-1,\ell}}}{1-q^{-1}} - q^{r+\ell-2}\ \frac{1-q^{-r}}{1-q^{-1}}\big) \\
&\quad + q^{n+1-2}\ \frac{1-q^{-1}}{1-q^{-1}}\cdot q^{r+1-2}\frac{1-q^{-r}}{1-q^{-1}} \\
&= q^{b_{r,\ell}+\ell-3}\ \frac{1-q^{-b_{r-1,\ell}}}{1-q^{-1}} + q^{r+n-2}\ \frac{(1-q^{-r})(1-q^{2\ell-n-1})}{1-q^{-1}}.
\end{aligned}$$

If $m = \ell(= n/\ell)$:

$$\begin{aligned}
\alpha_{r,n} &= q^{b_{r,\ell}+\ell-3}\ \frac{1-q^{-b_{r-1,\ell}}}{1-q^{-1}} \\
\beta'_{r,n} &= q^{-b_{r,\ell}+r+n-\ell+1}\frac{(1-q^{-r})(1-q^{2\ell-n-1})}{1-q^{-b_{r-1,\ell}}}, \\
\#D_{r,n} &= \alpha_{r,n}(1+\beta'_{r,n}).
\end{aligned}$$

$n = \ell^2$, $m = n$, $r = 2$, $\ell \geq 5$:

$$\begin{aligned}
\alpha_{r,n} &= q^{3+n-3}\ \frac{1-q^{-2}}{1-q^{-1}} = q^n + q^{n-1}, \\
\#D_{r,n} &= q^{\ell-1+b_{2,\ell}-2}\ \frac{1-q^{-\ell-1}}{1-q^{-1}} + \alpha_{r,n}(1-q^{2\ell-n-1}) \\
&= \alpha_{r,n}(1+\beta'_{r,n}), \\
\binom{\ell+2}{2} + \ell - 3 &= \frac{1}{2}(\ell^2+3\ell+2+2\ell-6) = \frac{1}{2}(\ell^2+5\ell-4), \\
\ell + \binom{\ell+2}{2} - 3 - n &= \frac{1}{2}(\ell^2+5\ell-4-2\ell^2) \\
&= \frac{1}{2}(-\ell^2+5\ell-4) = \frac{-1}{2}(\ell-1)(\ell-4), \\
\beta'_{r,n} &= q^{-(\ell-1)(\ell-4)/2}\ \frac{1-q^{-\ell-1}}{1-q^{-2}} - q^{-(\ell-1)^2}.
\end{aligned}$$

Remark 4.21, $n = \ell \cdot n/\ell$, $n/\ell \neq \ell$ prime.

$$\begin{aligned}
\#D_{r,n} &= \#P_{1,\ell} \cdot \#I_{r,n/\ell} + \#P_{1,n/\ell} \cdot \#I_{r,\ell} + \#P_{1,n} \cdot \#P_{r,1} \\
&= q^{\ell-1} \cdot \big(q^{b_{r,n/\ell}-2}\ \frac{1-q^{-b_{r-1,n/\ell}}}{1-q^{-1}} - q^{r+n/\ell-2}\ \frac{1-q^{-r}}{1-q^{-1}}\big) \\
&\quad + q^{n/\ell-1} \cdot \big(q^{b_{r,\ell}-2}\ \frac{1-q^{-b_{r-1,\ell}}}{1-q^{-1}} - q^{r+\ell-2}\ \frac{1-q^{-r}}{1-q^{-1}}\big) \\
&\quad + q^{n-1} \cdot q^{r-1}\ \frac{1-q^{-r}}{1-q^{-1}} \\
&= \frac{1}{1-q^{-1}} \cdot \Big(q^{b_{r,n/\ell}+\ell-3}(1-q^{-b_{r-1,n/\ell}}) + q^{b_{r,\ell}+n/\ell-3}(1-q^{-b_{r-1,\ell}}) \\
&\quad + q^{n+r-2}(1-q^{-r})(1-2q^{-(\ell-1)(n/\ell-1)})\Big).
\end{aligned}$$

If $m = \ell$:

$$\begin{aligned}
\alpha_{r,n} &= q^{b_{r,n/\ell}+\ell-3}\ \frac{1-q^{-b_{r-1,n/\ell}}}{1-q^{-1}} \\
\#D_{r,n} &= \alpha_{r,n} + q^{b_{r,\ell}+n/\ell-3}\ \frac{1-q^{-b_{r-1,\ell}}}{1-q^{-1}} \\
&\quad + q^{n+r-2}\ \frac{(1-q^{-r})(1-2q^{-(\ell-1)(n/\ell-1)})}{1-q^{-1}} \\
&= \alpha_{r,n}(1+\beta'_{r,n}) \\
\beta'_{r,n} &= \frac{1}{1-q^{-b_{r-1,n/\ell}}}(q^{b_{r,\ell}-b_{r,n/\ell}+n/\ell-\ell}(1-q^{-b_{r-1,\ell}}) \\
&\quad + q^{-b_{r,n/\ell}+n+r-\ell+1}(1-q^{-r})(1-2q^{-(\ell-1)(n/\ell-1)})).
\end{aligned}$$

If $m = n$: $r = 2$

$$
\begin{aligned}
\alpha_{r,n} &= q^n + q^{n-1}, \\
b_{r,n/\ell} + \ell - 3 &= \frac{1}{2}(\frac{n}{\ell} + 2)(\frac{n}{\ell} + 1) + \ell - 3 = \frac{1}{2\ell^2}(n^2 + 3n\ell + 2\ell^3 - 4\ell^2) \\
\#D_{r,n} &= \alpha_{2,n}(1 - 2q^{-(\ell-1)(n/\ell-1)}) \\
&\quad + q^{(n^2+3n\ell+2\ell^3-4\ell^2)/2\ell^2} \frac{1 - q^{-n/\ell-1}}{1 - q^{-1}} \\
&\quad + q^{(2n+\ell^3+3\ell^2-4\ell)/2\ell} \frac{1 - q^{-\ell-1}}{1 - q^{-1}} \\
&= \alpha_{r,n}(1 + \beta'_{r,n}), \\
\beta'_{r,n} &= q^{(-2n\ell^2+n^2+3n\ell+2\ell^3-4\ell^2)/2\ell^2} \ \frac{1 - q^{-n/\ell-1}}{1 - q^{-2}} \\
&\quad + q^{(-2n\ell+2n+\ell^3+3\ell^2-4\ell)/2\ell} \frac{1 - q^{-\ell-1}}{1 - q^{-2}} \\
&\quad - 2q^{-(\ell-1)(\ell-4)} \\
&= q^{-(2\ell^2-n-4\ell)(n-\ell)/2\ell^2} \frac{1 - q^{-n/\ell-1}}{1 - q^{-2}} \\
&\quad + q^{-(2n-\ell^2-4\ell)(\ell-1)/2\ell} \frac{1 - q^{-\ell-1}}{1 - q^{-1}} \\
&\quad - 2^{-(\ell-1)(\ell-4)}.
\end{aligned}
$$

Table 4.1 shows that the factor $1 - q^{-b_{r-1,n/m}}$ in $\alpha_{r,n}$ corresponds to terms of lower order than those in the error term $\beta_{r,n}$. Can we drop the factor ? The statement and proof of Theorem 4.1 can be modified to work in most cases, but not in Case 1, where $r = 2$ and $m = n$. The factor is $1 - q^{-2}$ in this case and cannot be bounded by $1 - \beta$, where $\beta$ decreases with $n$ or $\ell$. This affects other cases as well, since in the "inductive step" of (4.16), $(r, a)$ might be in Case 1.

Corollary 4.23:

Case 1: (3.1) holds,

$$\begin{aligned} q^{-1} + q^{-n/\ell-1} &\le 1 + q^{-n/\ell}, \\ (1-q^{-1})(1-q^{-n/\ell-1}) = 1 - q^{-1} - q^{-n/\ell-1} + q^{-n/\ell-2} &< 1 - q^{-2}, \\ \frac{1}{2}(n/\ell+1) - 1 \le \frac{1}{2}(2\ell-5+1) - 1 &= \ell - 2 - 1 = \ell - 3, \\ \beta_{2,n} = \frac{2q^{-\ell+3}(1-q^{-n/\ell-1})}{1-q^{-2}} &\le \frac{2q^{-\frac{1}{2}(n/\ell+1)+1}}{1-q^{-1}} = \beta^*_{2,n}. \end{aligned}$$

Case 2: $r = 2$ and $n/\ell = 2\ell - 3$ is prime,

$$\begin{aligned} \frac{1}{2}(n/\ell+1) - 1 &= \ell - 1 - 1 = \ell - 2, \\ \beta_{2,n} = 2q^{-\ell+2} &\le \frac{2q^{-\frac{1}{2}(n/\ell+1)+1}}{1-q^{-1}} = \beta^*_{2,n}. \end{aligned}$$

Case 3: $r \ge 2$ and $n = 4$

$$\begin{aligned} \frac{1}{2}\binom{r+1}{2} - 1 = \frac{1}{4}(r^2+r-4) &< \frac{1}{2}(r^2+r-4) = \binom{r+1}{2} - 2, \\ \beta_{r,4} = q^{-\binom{r+1}{2}+2} &< \frac{2q^{-\frac{1}{2}\binom{r+1}{2}+1}}{1-q^{-1}} = \beta^*_{r,4}. \end{aligned}$$

$$\begin{aligned} &\binom{n+2}{2} - n + 1 - \left(\binom{n/\ell+2}{2} + \ell - 1\right) \\ &= \frac{1}{2}(n^2+n+4 - \frac{1}{\ell^2}(n^2+3\ell n+2\ell^2(\ell-1))) \\ &= \frac{1}{2\ell^2}(n^2\ell^2 + n\ell^2 + 4\ell^2 - n^2 - 3\ell n - 2\ell^2 - 2\ell^3 + 2\ell^2) \\ &= \frac{1}{2\ell^2}(n^2(\ell^2-1)) + n\ell(\ell-3) + 4\ell^2 - 2\ell^3) \\ &\ge \frac{1}{2\ell^2}(\ell^4(\ell^2-1) + \ell^3(\ell-3) + 4\ell^2 - 2\ell^3) \\ &= \frac{1}{2\ell^2}(\ell^6 - 5\ell^3 + 4\ell^2) \\ &= \frac{1}{2}(\ell^4 - 5\ell + 4) > 0. \end{aligned}$$

$$\begin{aligned}
&\binom{n+2}{2} - \frac{n^2(\ell-1)}{2\ell} - \binom{n/\ell+2}{2} - \ell + 1 \\
&= \frac{1}{2\ell^2}(n^2\ell^2 + 3n\ell^2 + 2\ell^2 - n^2\ell^2 + n^2\ell - n^2 - 3n\ell - 2\ell^2 - 2\ell^2(\ell-1)) \\
&= \frac{1}{2\ell^2}(n^2(\ell-1) + 3n\ell(\ell-1) - 2\ell^2(\ell-1)) \\
&= \frac{\ell-1}{2\ell^2}(n^2 + 3n\ell - 2\ell^2).
\end{aligned}$$

Joachim von zur Gathen
B-IT
Universität Bonn
D-53113 Bonn
gathen@bit.uni-bonn.de
http://cosec.bit.uni-bonn.de/