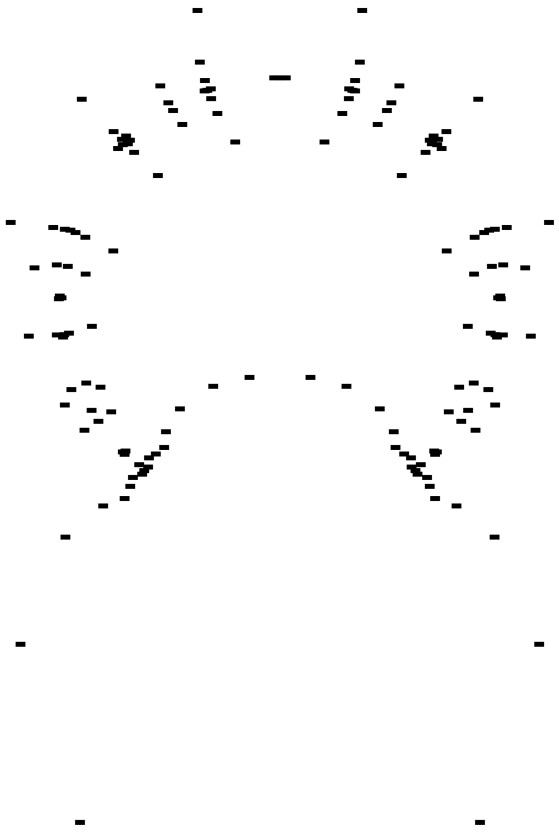
Invariant Theory and Graphs

A computational approach

Magnus Rahbek Hansen



M.Sc. in Mathematics

Supervised by Henrik Holm
Co-supervised by Søren Eilers

Department of Mathematical Sciences
University of Copenhagen, Denmark

December, 2023

Я согласен, что дважды два четыре — превосходная вещь; но если уже всё хвалить, то и дважды два пять — премилая иногда вещица

—Фёдор Достоевский, *Записки из подполья*

Abstract

In this thesis, we provide an exposition of the invariant theory of finite groups, with a focus on algorithms and the Hilbert series. We apply the built-up theory to the algebra of invariants of multigraphs, as well as s-graphs, which are graphs weighted in $\{0, 1, ..., s\}$. Utilizing computer exploration on the invariant algebra of s-graphs, we derive a formula for the Hilbert series of any permutation group acting on a special discrete variety, $V|_s$. We conjecture that this formula can be generalized to any finite group. Furthermore, we present a version of King's algorithm for computing a (minimal) generating set for the algebra of invariants on simple graphs. We conjecture the correctness of this algorithm and its potential generalization to any finite group acting on $V|_s$. Finally, we recreate Thiery's disproof of Pouzet's conjecture, from [Thi00].

This page intentionally left blank.

Contents

0 Introduction

Invariant theory is the study of group actions on algebraic varieties, by considering their effect on functions. In the classic sense, this means looking at group actions on the algebra, $\mathbb{C}[V]$, where usually $V = \mathbb{C}^n$. In particular, we want to describe the set of elements (i.e. polynomials) in $\mathbb{C}[V]$, which stay invariant under the action, $g \cdot f(\mathbf{x}) = f(g \cdot \mathbf{x})$. Within the past 50 years, this subject has enjoyed a resurgence of interest, with applications in fields spanning as far as the cohomology of finite groups, coding theory, material science, and even computer vision. One particular application of invariant theory is that of graph theory, which will be the focus of this thesis.

Outline. The thesis is split into four main sections.

1. *Preliminaries:* This section is mainly a collection of combinatorial results and procedures, used throughout section 3 and 4. The most important result being Pòlya's enumeration theorem.

2. *Invariant Theory of Finite Group:* A concise exposition of the theory of invariants of finite groups. This includes old, as well as new, results, with a focus on computability, bounds and the Hilbert series. The main results of this section is Hilbert's finiteness theorem, Molien's formula, and King's algorithm.

3. *Invariant Theory on Graphs:* We apply the results and algorithm of Section 2 to the example of the invariant algebra of graphs. We primarily follow [Thi00], however, we expand upon his work. In particular, we look at the algebras, $\mathcal{I}^n|_s$, of invariants of graphs weighted in $\{0, 1, ..., s\}$. This led us to a new formula for the Hilbert series of $\mathbb{C}[V|_s]^G$, where G is a permutation group, and $V|_s$ is a special finite variety. Furthermore, we conjecture to have found a variation of King's algorithm, which explicitly computes a (perhaps minimal) generating set of $\mathcal{I}^n|_s$.

4. *Reconstructability:* We investigate an algebraic generalization of Ulam's conjecture for multigraphs, known as Pouzet's conjecture. The main goal of this section is to recreate Thiery's ([Thi00]) disprove Pouzet's conjecture.

The focus throughout the thesis is computability, and the interplay between invariant theory and its algorithms, along with combinatorics and computer exploration. We have implemented most of the algorithms we come across in the computer algebra system, `SAGEMATH`, and make heavy use of these implementations to aid us in our investigations of graphs, through the lens of invariant theory. For instance, the disproof of Pouzet's conjecture relies heavily on computations from these implementations, and is a great example of how these tools can be utilized.

New improvements and conjectures. Throughout the thesis we give a few new improvements to known results, as well as a few conjectures, most of which is

contained in Section 3. Generally, in the Section 3, we expanded the theory from that of simple- and multigraphs, to that of graphs weighted in $\{0, 1, ..., s\}$.

We will now briefly expand on the results mentioned in item 3, of the outline above. Firstly, we define the discrete finite variety,

$$V|_s = \{\textstyle\sum_{i=0}^{\binom{n}{2}} g_i \mathbf{e_i} \mid g_i \in \{0, 1, 2, ..., s\}\},$$

of s-graph (graphs with weights in $\{0, 1, ..., s\}$), and we denote by $S_n^{(2)}$ the representation of the symmetric group S_n acting on two-sets, $\sigma\{i, j\} = \{\sigma i, \sigma j\}$. Then the algebra, $\mathcal{I}^n|_s := \mathbb{C}[V|_s]^{S_n^{(2)}}$, is the algebra of invariants on s-graphs. In particular, the polynomials in $\mathcal{I}^n|_s$ separate s-graph isomorphism classes. We find that the Hilbert series, $H(\mathcal{I}^n|_s, z)$, enumerates the number of s-graphs, and from this, we find the formulas,

$$i) \quad H(\mathcal{I}^n|_s, z) = \frac{1}{n!} \sum_{\lambda} |C_\lambda| \prod_i \left(\sum_{k=0}^{s} z^{k \cdot i} \right)^{\overline{\lambda}_i}$$

$$ii) \quad H(\mathcal{I}^n|_s, z) = \frac{1}{n!} \sum_{M \in S_n^{(2)}} \frac{\det(\mathrm{id}_n - z^{s+1} M)}{\det(\mathrm{id}_n - zM)}$$

which led us to the following generalization: For any permutation group G we have

$$H(\mathbb{C}[V|_s], z) = \frac{1}{|G|} \sum_{M \in G} \frac{\det(\mathrm{id} - z^{s+1} M)}{\det(\mathrm{id} - zM)}.$$

Perhaps this formula is true for any finite group G; however, due to time constraints, we could not test this proposal. (See Remark 3.5, Question 3.1 for these results).

We also wish to compute a (minimal) generating set for $\mathcal{I}^n|_1$, but since the author know of no algorithm which finds invariants over $\mathbb{C}[V|_s]$, the only way to compute these invariants was to compute a minimal generating set of $\mathcal{I}^n$, and take the quotient map of these. However, we found that the set attained by this process was not, in general, minimal. Miraculously, however, through trial and error, we came up with a variation of King's algorithm, Algorithm 4, which seems to produce a (perhaps minimal) generating sets for $\mathcal{I}^n|_1$. This was tested on $n = 4$ and $n = 5$. Both of which yielded the same sets, found by hand. We conjecture the algorithm is correct and that it can be altered to work for $\mathcal{I}^n|_s$. Moreover, we conjecture (if the correctness conjecture is true) that it will work for any finite group.

Prerequisites. It is assumed that the reader is familiar with commutative algebra, basic algebraic geometry, along with Gröbner bases and basic representation theory. Any standard textbook on these subjects should suffice. Furthermore, some homological algebra is used when we discuss the Gorenstein property. However, this is a small part of the thesis, and is in not needed for the understanding of the rest.

Acknowledgements. I would like to extend my deep gratitude to my supervisors, Henrik Holm and Søren Eilers. Through means of great supervision and tasty breakfasts, have they made the writing process of this thesis thoroughly enjoyable and thereby effectively painless!

1 Preliminaries

This section serves to provide the necessary background theory, to be used throughout this thesis, and also serves to introduce the notation and definitions used.

1.1 Graded algebras and Hilbert series

Graded algebras and their Hilbert series play a fundamental role in this thesis. We will now briefly walk through the basic definitions, and a condition which plays a vital role later on. Many more properties of these structures will be shown in later sections.

Definition 1.1. An algebra, A, over a field, K, is said to be $\mathbb{N}$-*graded* if we can decompose A as $A = \bigoplus_{d=0}^{\infty} A_d$, into a direct sum of vector spaces, A_d, such that $A_d A_r \subseteq A_{d+r}$.

We call the summand, A_d, the *homogeneous component* of degree d, the elements of which are said to be *homogeneous* of degree d.

We say that the graded algebra, A, is *connected* if $A_0 = K$.

Unless stated otherwise, we will simply refer to connected $\mathbb{N}$-graded algebras as graded algebras.

Definition 1.2. The *Hilbert series*, $H(A, z)$, of a graded algebra, A, is the power series given by

$$H(A, z) := \sum_{d=0}^{\infty} \dim(A_d) z^d.$$

Of course, one can extend this definition to any algebra, with some given decomposition into direct sums of finite-dimensional vector spaces. Later on, we will be considering the Hilbert series of a so-called *semi-graded* algebra.

The following allows us to give a bound on the dimensions of the homogeneous components. The condition may seem weak, but it turns out to be rather powerful, and is crucial in disproving Pouzet's conjecture.

Condition 1.1. *Let $H = \{h_1, ..., h_k\}$ be a finite homogeneous generating set for the connected $\mathbb{N}$-graded algebra, A, with respective degrees $D = \{d_1, ..., d_k\}$. Then $H(A, z)$ is dominated by (i.e. term-wise bounded by) the power series,*

$$F(D, z) := \prod_{d \in D} \frac{1}{1 - z^d} = \sum_{i=0}^{\infty} f_i z^i.$$

I.e. we have $\dim(A_i) \leq f_i$ for all i.

Proof sketch due to [Thi00]. As vector spaces, the homogeneous component, A_d, is generated by all products $h_1^{l_1} \cdots h_k^{l_k}$ with $l_1 d_1 + \cdots + l_k d_k = d$. One sees that these products are counted by the power series of $F(D, z)$. □

1.2 Pólya's Enumeration Theorem

Later in this thesis, we will want to count the number of unlabelled graphs under some set of restrictions. This may seem like a daunting task, but thanks to the remarkable enumeration theorem of Pólya, doing so becomes quite doable!

In this section, we present the necessary background to state, but not prove, the theorem. The exposition closely follows that of Harary and Palmer in [HP73].

Let A be a finite group acting by permutation on a finite set, $X = \{1, 2, ..., n\}$. With this action, each permutation $\alpha \in A$ can be written uniquely as a product of disjoint cycles. Denote by $\lambda_i(\alpha)$ the number of cycles in α of length i.

Definition 1.3. With the setup above, the *cycle index*, $Z(A)$, of A is defined as the polynomial, in the variables $s_1, s_2, ..., s_n$, given by

$$Z(A) = \frac{1}{|A|} \sum_{\alpha \in A} \prod_{i=1}^{n} s_i^{\lambda_i(\alpha)}.$$

In case we want to explicitly display the variables s_k, we write $Z(A; s_1, s_2, ..., s_n)$, and we may exchange the s_k's with an expression if we wish.

Example 1.1 ([HP73])**.** Using Notation 3.1 and denoting by C_λ the conjugacy class tied to the partition, λ, the cycle index of the symmetric group, S_n, is given by

$$Z(S_n) = \frac{1}{n!} \sum_{\lambda} |C_\lambda| \prod_{i=1}^{n} s_i^{\lambda_i},$$

where we sum over all partitions, λ, of n.

Let A be as before, and let B be a finite group acting by permutation on some countable set, Y, of at least two elements. We define the *power group*, denoted by B^A, to be the group consisting of all ordered pairs, denoted $(\alpha; \beta)$, with $\alpha \in A$, $\beta \in B$. Its defining action is on the collection, Y^X, of functions from X to Y, by

$$((\alpha; \beta)f)(x) := \beta f(\alpha x),$$

for all $x \in X$, and $(\alpha; \beta) \in B^A$.

We now take $B = E$, with E being the identity group on Y, and consider the power group E^A acting on Y^X. We call a function $w : Y \to \mathbb{N}$ with finite fibers (i.e., $|w^{-1}(k)| < \infty$, for all k) a *weight function*, and we say that a $y \in Y$ for which $w(y) = k$, has weight k. We then define the number of *figures* by

$$c_k = |w^{-1}(k)|$$

for all $k \in \mathbb{N}$. Furthermore, we define the *figure counting series* as the power series,

$$c(z) = \sum_{k=0}^{\infty} c_k z^k,$$

which enumerates the elements of Y, by weight.

We define the *weight of a function*, $f \in Y^X$ by

$$w(f) = \sum_{x \in X} w(f(x)),$$

and find that it is constant over any orbit in E^A. Hence, it is well-defined to define the *weight*, $w(F)$, *of an orbit*, F, of E^A to be the weight of an arbitrary $f \in F$. Since we demanded that $|w^{-1}(k)| < \infty$, there are only a finite number of orbits for any given weight, k, so we define $C_k < \infty$ to be the number of orbits of weight k. We define the *function counting series* to be given by

$$C(z) = \sum_{k=0}^{\infty} C_k z^k.$$

Finally, we write $Z(A, c(z)) := Z(A; c(z), c(z^2), c(z^3), ...)$ and may state Pólya's Enumeration Theorem.

Theorem 1.1 (Pólya's Enumeration Theorem)**.** *The function counting series, $C(z)$, is determined by substituting for each variable, s_k in $Z(A)$, the figure counting series, $c(z^k)$. That is, we have*

$$C(z) = Z(A, c(z)).$$

Proof. Omitted. For a proof see [HP73, p.43]. □

This theorem can be generalized to n variables. For this, we again consider the power group E^A acting on Y^X, but now consider the n-variable weight function, $w : Y \to \mathbb{N}^n$, with finite fibers. Using component-wise addition, everything is defined as before, and now the figure counting series and function counting series are power series over all monomials, $z_1^{k_1} \cdots z_n^{k_n}$. Denote by $Z(A, c(z_1, ..., z_n))$ the polynomial obtained by replacing s_k in $Z(A)$ by $c(z_1^k, ..., z_n^k)$. Then the multivariable Pólya's Enumeration Theorem is stated as follows.

Theorem 1.2 (Multivariable Pólya's Enumeration Theorem)**.** *The function counting series, $C(z_1, ..., z_n)$, is obtained by substituting for each variable, s_k, in $Z(A)$, the figure counting series. That is we have*

$$C(z_1, ..., z_n) = Z(A, c(z_1, ..., z_n)).$$

The following identity if well-known.

Proposition 1.1. *The following identity holds*

$$\sum_{n=1}^{\infty} Z(S_n, c(z_1, ..., z_k)) = \exp\left(\sum_{n=1}^{\infty} \frac{c(z_1^n, ..., z_k^n)}{n}\right).$$

Proof sketch. Expand the left side using the definition and Example 1.1, and expand the right side using the Taylor series for the exponential. Compare the coefficients to find that they are, in fact, the same. □

1.3 The Euler transformation of generating functions

In this thesis, we will come across many sequences, some of which we wish to transform. One such transformation is the (inverse) Euler transformation. Here, we give a basic rundown of its definition, interpretations, and computations. We take inspiration from [HP73], [Sta78], and [Cam89].

Throughout this section, let a_n and b_n be two infinite sequences with generating functions $A(x)$ and $B(x)$.

Definition 1.4. We say that $\{b_n\}$ is the *Euler transform* of $\{a_n\}$ if they are related by the equality

$$1 + \sum_{n=1}^{\infty} b_n x^n = \prod_{n=1}^{\infty} \frac{1}{(1-x^n)^{a_n}}.$$

Conversely, we say $\{a_n\}$ is the *inverse Euler transform* of $\{b_n\}$.

An equivalent definition can be given in terms of their generating functions. Due to the lack of proofs in the literature, we present our own proof.

Proposition 1.2. *Let $\{b_n\}$ be the Euler transformation of $\{a_n\}$ with generating functions $B(x)$, respectively $A(x)$. Then the two generating functions are related by*

$$1 + B(x) = \exp\left(\sum_{k=1}^{\infty} \frac{A(x^k)}{k}\right)$$

Proof. Clearly we need only show $\prod_{n=1}^{\infty} \frac{1}{(1-x^n)^{a_n}} = \exp(\sum_{k=1}^{\infty} \frac{A(x^k)}{k})$. We see that

$$\begin{aligned}
\log\left(\prod_{n=1}^{\infty} \frac{1}{(1-x^n)^{a_n}}\right) &= \sum_{n=1}^{\infty} -a_n \log(1-x^n) \\
&= \sum_{n=1}^{\infty} a_n \sum_{k=1}^{\infty} \frac{x^{nk}}{k} \\
&= \sum_{k=1}^{\infty} \frac{\sum_{n=1}^{\infty} a_n x^{nk}}{k} \\
&= \sum_{k=1}^{\infty} \frac{A(x^k)}{k}
\end{aligned}$$

where we used the Taylor expansion, $-\log(1-x) = \sum_{k=1}^{\infty} \frac{x^k}{k}$, and allowed an interchange of sums, since we don't care about convergence. Taking the exponential of both sides finishes the proof. □

Sequences related as above have many interesting interpretations, one of which comes from the following theorem.

Theorem 1.3. *Let A be a connected $\mathbb{N}$-graded K-algebra, generated by the nonzero homogeneous elements, $y_1, ..., y_n$, of positive degree, $d_1, ..., d_n$. Then the y_i's are algebraically independent over k if and only if*

$$H(A,z) = 1 + \sum_{i=1}^{\infty} \dim(A_i) z^i = \prod_{i=1}^{n} \frac{1}{1-z^{d_i}} = \prod_{i=1}^{\infty} \frac{1}{(1-z^i)^{e_i}}$$

where e_i counts the number of elements of $\{y_1, ..., y_n\}$, who is of degree i.

Proof. Omitted. See Theorem 3.5 of [Sta78] for a proof. □

Thus, since A in the above is connected, we clearly see that the dimension of the homogeneous components, $\dim(A_i)$, is the Euler transformation of the number of algebraically independent homogeneous generators of degree d of A.

Computing the Euler transform of a sequence is just a trivial matter of evaluating the power series of the rational function, given on the right-hand side of Definition 1.4.[1] However, we also wish to compute the inverse Euler transform of a given sequence. To do this, we follow the recipe of [HP73]. Firstly, we need the following result, which, again because of the lack of proofs in the literature, we give our own proof.

Proposition 1.3. *If $\sum_{n=0}^{\infty} b_n x^n = \exp(\sum_{n=1}^{\infty} a_n x^n)$ then for $n \geq 1$ we have*

$$n a_n = n b_n - \sum_{k=1}^{n-1} k a_k b_{n-k}.$$

Proof. Take the derivative on both sides of $\sum_{n=0}^{\infty} b_n x^n = \exp(\sum_{n=1}^{\infty} a_n x^n)$ to get, by the chain rule, that

$$\begin{aligned}
\sum_{n=1}^{\infty} n b_n x^{n-1} &= \left(\sum_{n=1}^{\infty} n a_n x^{n-1} \right) \exp\left(\sum_{n=1}^{\infty} a_n x^n \right) \\
&= \left(\sum_{n=1}^{\infty} n a_n x^{n-1} \right) \left(\sum_{n=0}^{\infty} b_n x^n \right) \\
&= \left(\sum_{n=1}^{\infty} n a_n x^{n-1} \right) \left(1 + \sum_{n=1}^{\infty} b_n x^n \right) \\
&= \sum_{n=1}^{\infty} n a_n x^{n-1} + \left(\sum_{n=1}^{\infty} n a_n x^{n-1} \right) \left(\sum_{n=1}^{\infty} b_n x^n \right)
\end{aligned}$$

Multiplying through by x and using the Cauchy product formula, we get

$$\sum_{n=1}^{\infty} n b_n x^n = \sum_{n=1}^{\infty} n a_n x^n + \sum_{n=1}^{\infty} \left(\sum_{k=1}^{n-1} k a_k b_{n-k} \right) x^n$$

and by comparing coefficients the desired formula is derived. □

[1] There is a more sophisticated way, which speeds up the computation time. We implemented, without proof, this faster way. (See Listing 1).

Given two sequences, as in Definition 1.4, and using the form from Proposition 1.2, we may compute the inverse Euler transform of $B(x)$ as follows:

First set

$$\sum_{n=1}^{\infty} c_n x^n = \log(1 + B(x)),$$

and take $\exp(-)$ on both sides. Using Proposition 1.3, we then get

$$nc_n = nb_n - \sum_{k=1}^{n-1} kc_k b_{n-k},$$

which allows us to compute c_n from $b_1, ..., b_n$ and $c_1, ..., c_{n-1}$. (Note $c_1 = b_1$).

Thus, we have that

$$\sum_{n=1}^{\infty} c_n x^n = \log(1 + B(x)) = \sum_{n=1}^{\infty} \frac{A(x^k)}{k}$$

and, by comparing the coefficients, we get

$$nc_n = \sum_{d|n} da_d,$$

where a_d is the coefficient of x^d in $A(x)$. Using the Möbius inversion formula on this, we may express a_n as a sum of c_i's,

$$a_n = \sum_{d|n} \frac{\mu(d)}{d} c_{n/d},$$

where μ is the Möbius function. We summarize this into the following procedure.

Procedure 1.1. Given a sequence, $\{b_n\}$, we may compute its inverse Euler transformation, $\{a_n\}$, using the intermediary sequence, $\{c_n\}$, and the two equalities,

$$nc_n = nb_n - \sum_{k=1}^{n-1} kc_k b_{n-k},$$

$$a_n = \sum_{d|n} \frac{\mu(d)}{d} c_{n/d},$$

where μ is the Möbius function.

We have implemented this procedure into `SAGEMATH`. See Listing 2.

The above procedure generalises to any number of variables, but we will only be using the two variable version. This formulation of the procedure is due to [HP73].

Procedure 1.2. If we have two generating functions, $A(x,y) = \sum a_{n,m}x^n y^m$ and $B(x,y) = \sum b_{n,m}x^n y^m$, related by

$$1 + B(x,y) = \exp\left(\sum_{k=1}^{\infty} \frac{A(x^k, y^k)}{k}\right),$$

then we may compute $A(x,y)$ from $B(x,y)$ by using the intermediary series, $C(x,y) = \sum c_{n,m}x^n y^m$, and the two equalities,

$$nc_n(y) = nb_n(y) - \sum_{k=1}^{n-1} kc_k(y)b_{n-k}(y),$$

$$a_{n,m} = \sum_{d \mid \gcd(n,m)} \frac{\mu(d)}{d} b_{n/d,m/d},$$

where $s_n(y) = \sum_{m=1}^{\infty} s_{n,m}y^m$, for $s \in \{a,b,c\}$.

While being a little more hairy to implement, it is very analogous to the one-variable version. See Listing 3 for our implementation.

Remark 1.1. Working backwards in the proof of Proposition 1.2, but with two variables, we see that the relation in Procedure 1.2 is the same as the relation,

$$1 + \sum_{n,m} b_{n,m}x^n y^m = \prod_{n,m} \frac{1}{(1 - x^n y^m)^{a_{n,m}}}.$$

The interpretation of this is not entirely clear. Perhaps it to be related to the multigradings of algebras, in much the same way as for one variable?

2 Invariant Theory of Finite Groups

The theory of invariants is a very old field of mathematics, dating back to the 1840s with the works of Cayley and Boole. Later on, Hilbert entered the scene and proved many great results, with Hilbert's finiteness theorem being the magnum opus, and effectively putting a lid on invariant theory for a long time. However, within the past 50 years, there has been a resurgence of the field from the perspective of computation, as well as many new results in the so-called *modular case*.

In this section, we present some important results in invariant theory, both old and new, which we will put into practice in Section 3. This exposition is based in large parts on [DK15] and [PS08]. Most of the results we present are proved in full generality in [DK15]; however, we simplify these proofs to the finite case.

Throughout this section, let V be an n-dimensional vector space over $\mathbb{C}$ with a fixed basis $\mathbf{e}_1, ..., \mathbf{e}_n$. Moreover, throughout this thesis, we let $R = \mathbb{C}[V] = \mathbb{C}[x_1, ..., x_n]$ be the graded algebra of polynomials over $\mathbb{C}$ in n variables, and let $G \subseteq \mathrm{GL}(V)$ be some finite matrix group. We see that, G, acts naturally on R by

$$(Mf)(\mathbf{x}) = f(M\mathbf{x})$$

for all $f \in R$ and $M \in G$.

We are interested in the polynomials, f, for which $Mf = f$ for all $M \in G$. We call such a polynomial a *G-invariant*, or simply an *invariant*, if there is no ambiguity of the group, G. The collection of all such invariants,

$$R^G := \{f \in R \mid Mf = f \text{ for all } M \in G\},$$

is called the *invariant algebra* of G. It is clear that $R^G \subseteq R$ is a subalgebra.

The main goal of invariant theory is to describe R^G. However, this turns out to be a daunting task, and so one may start small and ask whether or not R^G is finitely generated: That is, does there exist $f_1, ..., f_m \in R^G$ such that $R^G = \mathbb{C}[f_1, ..., f_m]$? This was positively answered by Hilbert in 1890 with *Hilbert's finiteness theorem*. We will see a proof of this fact in the subsequent subsection.

With Hilbert's finiteness theorem in mind, we follow up with three questions related to the generators, $f_1, ..., f_m$:

- How do we (efficiently) find the generators $f_1, ..., f_m$?
- What is the algebraic relation among the generators?
- Give an (efficient) algorithm to write any $g \in R^G$ in terms of $f_1, ..., f_m$. That is, construct a polynomial, p, such that $g = p(f_1, ..., f_m)$.

These three problems are often referred to as the *fundamental problems of invariant theory*.

Example 2.1 (Symmetric group)**.** The most classical and fundamental example is that of the invariant algebra of the symmetric group, S_n, acting by permutation of the variables, x_i. This algebra is quite well understood. Indeed, the generators of R^{S_n} turn out to be exactly the elementary symmetric polynomials:

$$\sigma_k = \sum_{1 \leq j_1 < \cdots < j_k \leq n} x_{j_1} \cdots x_{j_k}.$$

And there is no algebraic relation between them. That is, the polynomials are algebraically independent.

This result is called the *fundamental theorem of symmetric polynomials*.

Remark 2.1. It is easily seen that R^G consists of the polynomials that are constant on all G-orbits in $\mathbb{C}^n$. This suggests an interpretation of R^G in terms of algebraic geometry. Indeed, in the case of finite groups, all orbits of G acting on $V = \mathbb{C}^n$ are certainly finite and are thus closed in $\mathbb{C}^n$. Hence one has that $\mathbb{C}^n/G$ is an algebraic variety, with coordinate ring $\mathbb{C}[V]^G$. The problem of finding a set of generators, $f_1, ..., f_m$, is then really a matter of finding an embedding $\mathbb{C}^n/G \hookrightarrow \mathbb{C}^m$. See [PS08] for a deeper discussion of this interpretation.

2.1 The Reynolds operator and Hilbert's finiteness theorem

We'll now move on to proving Hilbert's finiteness theorem. To do this, we need an operator called the *Reynolds operator*. It plays a fundamental role in the proof. In fact, it is in general a very useful operator and will make appearances throughout this thesis.

Definition 2.1. Let $G \subseteq \mathrm{GL}(\mathbb{C}^n)$ be a finite group, acting on $R = \mathbb{C}[x_1, ..., x_n]$. A *Reynolds operator* is a G-invariant linear map $\mathcal{R} : R \to R^G$ such that if $f \in R^G$ then $\mathcal{R}(f) = f$.

In the case of finite groups, we can construct the Reynolds operator explicitly:

$$\mathcal{R}(f) = \frac{1}{|G|} \sum_{M \in G} Mf.$$

Indeed, the three defining properties hold: $\mathcal{R}$ is clearly linear. It is G-invariant, since right multiplication by $N \in G$, (i.e. $M \mapsto NM$) is a permutation of G, so we have that

$$\mathcal{R}(N \cdot f) = \frac{1}{|G|} \sum_{M \in G} MN \cdot f = \frac{1}{|G|} \sum_{M' \in G} M' \cdot f = \mathcal{R}(f).$$

Finally, if $f \in R^G$ then

$$\mathcal{R}(f) = \frac{1}{|G|} \sum_{M \in G} M \cdot f = \frac{1}{|G|} \sum_{M \in G} f = \frac{1}{|G|} |G| f = f.$$

We say that a subspace $W \subseteq V$ is *G-stable* if $Mw \in W$ for all $M \in G$ and all $w \in W$. Then, $\mathcal{R}$ has the following two properties:

Proposition 2.1. *It holds for the Reynolds operator $\mathcal{R} : R \to R^G$ that*

i) *$\mathcal{R}$ is a R^G-module homomorphism.*

ii) *If a subspace, $W \subseteq R$, is G-stable, then $\mathcal{R}(W) = W^G$.*

The first property means that $\mathcal{R}(fg) = f\mathcal{R}(g)$ if $f \in R^G$ and $g \in R$. This is called the *Reynolds identity*.

Proof. i) From the properties already shown, it suffice to prove that $\mathcal{R}(fg) = f\mathcal{R}(g)$ for all $f \in R^G$ and $g \in R$. However, this is immediate from the simple computation:

$$\mathcal{R}(fg) = \frac{1}{|G|}\sum_{M\in G} M \cdot (fg) = \frac{1}{|G|}\sum_{M\in G}(M \cdot f)(M \cdot g) = \frac{1}{|G|}\sum_{M\in G} fM \cdot g = f\mathcal{R}(g)$$

ii) Take any $f \in W$. By assumption $Mf \in W$ for all f, thus $\mathcal{R}(f)$ is a finite linear combination of elements of W. But $\mathcal{R}(f)$ is also invariant so $\mathcal{R}(f) \in R^G \cap W = W^G$. □

Example 2.2. Since $M \in G$ is necessarily invertible (G is a group), we have that every entry of $M\mathbf{x}$ is a non-zero linear combination of the x_i's. Thus, if $f \in R$ is homogeneous of degree d, then clearly we have that $f(M\mathbf{x})$ will again be homogeneous of degree d. So we see that $R_d \subseteq R$ is a G-stable subspace, and we have $\mathcal{R}(R_d) = R_d^G$.

A map, $\varphi : X \to Y$, between two sets, which are both acted upon by G, is called *G-equivariant* if $\varphi(Mx) = M\varphi(x)$ for all $x \in X$ and $M \in G$.

Proposition 2.2. *Let $\mathbb{C}[V_1]$ and $\mathbb{C}[V_2]$ be two coordinate rings. If $\varphi : \mathbb{C}[V_1] \twoheadrightarrow \mathbb{C}[V_2]$ is a surjective G-equivariant linear map, then $\varphi(\mathbb{C}[V_1]^G) = \mathbb{C}[V_2]^G$.*

Proof. Since φ is G-equivariant, we have that $\ker(\varphi)$ is clearly G-stable, and so, by Maschke's theorem, there exist a G-stable complement, W, to $\ker(\varphi)$ so that $\mathbb{C}[V_1] \cong \ker(\varphi) \oplus W$. Thus $\varphi|_W : W \to \mathbb{C}[V_2]$ is an isomorphism of representations of G, and it follows that $\varphi(\mathbb{C}[V_1]) = \varphi|_W(W^G) = \mathbb{C}[V_2]^G$. □

We now prove the most important result of invariant theory.

Theorem 2.1 (Hilbert's finiteness theorem)**.** *The subalgebra R^G is finitely generated as an algebra over $\mathbb{C}$.*

Proof. Let $I \subseteq R$ be the ideal generated by all homogeneous invariant polynomials of positive degree. Since R is Noetherian (Hilbert's basis theorem), we have that $I = \langle f_1, ..., f_n\rangle$ is finitely generated with $f_i \in R^G$. We will show that $R^G = \mathbb{C}[f_1, ..., f_n]$.

Clearly, $\mathbb{C}[f_1, ..., f_n] \subseteq R^G$, so it suffices to take $h \in R^G$, homogeneous of degree d, and show $h \in \mathbb{C}[f_1, ..., f_n]$. We show this by induction on d:

For $d = 0$ we have $h \in \mathbb{C} \subseteq \mathbb{C}[f_1, ..., f_n]$.

For $d > 0$, we may decompose h as

$$h = \sum_{i=1}^{n} g_i f_i,$$

with $g_i \in R$ being homogeneous of degree $d - \deg(f_i) < d$, since h itself is homogeneous and f_i is of positive degree. Applying the Reynolds operator to both sides of this decomposition, and applying the Reynolds identity we get that

$$h = \mathcal{R}(h) = \mathcal{R}\left(\sum_{i=1}^{n} g_i f_i\right) = \sum_{i=1}^{n} \mathcal{R}(g_i) f_i.$$

By Example 2.2 we have that $\mathcal{R}(R_d) = R_d^G$. It follows that $\deg(\mathcal{R}(g_i)) = \deg(g_i) = d - \deg(f_i) < d$, and so by the induction hypothesis $\mathcal{R}(g_i) \in \mathbb{C}[f_1, ..., f_n]$, for all i. Thus we have $h \in \mathbb{C}[f_1, ..., f_n]$, as desired. □

Remark 2.2. In the proof above, we only use the finiteness assumption when we use the Reynolds operator. In fact, the proof above works for any group, which admits a Reynolds operator. These groups are called reductive. For a version of the above statements in full generality, see [DK15, Chapter 2].

Noether refined Hilbert's theorem for finite groups in 1916 with the following theorem. We define the *degree* of a group $G \subseteq \mathrm{GL}(V)$ to be $m = \dim(V)$.

Theorem 2.2 (Nother's degree bound)**.** *The invariant ring, R^G, of a finite group, G, has an algebra basis consisting of at most $\binom{m+|G|}{m}$ invariants of degree at most $|G|$.*

This bound is optimal in the sense that there exists groups $G \subseteq \mathrm{GL}(\mathbb{C}^m)$ such that *all* algebra bases for R^G contain at least $\binom{m+|G|-1}{m-1}$ invariants of degree $|G|$. (See [PS08, Proposition 2.1.5]). However, in almost all cases of interest, these bounds horribly loose.

The optimal bound on the degree of a generating set of invariants plays a larger role, and so we will denote it by $\beta(R^G)$. That is,

$$\beta(R^G) := \inf\{\ n \mid R^G \text{ is generated by } \bigoplus_{d=0}^{n} R_d^G\ \} \in \mathbb{N} \cup \infty.$$

It's an interesting and important problem to find a good bound, D, on $\beta(R^G) \leq D$. In fact, good bounds have great algorithmic implications on the construction of the invariants. Indeed, the bound often plays the role of a stopping condition for many algorithms in invariant theory. For example, Algorithm 1 uses it as a stopping condition. See [DK15] for more such algorithms.

Finally, we conclude this section with a small proposition regarding the algebraic relations of invariants.

Proposition 2.3. *Let m be the degree of a finite matrix group G. Then the invariant algebra R^G has Krull dimension m. This is equivalent to the existence of a set of m algebraically independent invariants. This set will be maximal with respect to cardinality.*

Proof. Let t be an indeterminate. Define a family of polynomials in $R[t]$ by $F_i := \prod_{M\in G}(Mx_i - t)$ for each $i \in \{1, 2, ..., m\}$. We have that $F_i \in R^G[t]$ since it is invariant under the action of G on the x_i's and thus its coefficients are also invariant.

By construction $t = x_i$ is a root of F_i, since $\mathrm{id} \in G$. Hence per definition every x_i is algebraically dependent on a certain invariants. It follows that R^G and R have the same Krull dimension. Since R is a polynomial ring, the Krull dimension of $R = \mathbb{C}[V]$ equals the number of indeterminates, which equals the dimension of V, which by definition is the degree of $G \subseteq \mathrm{GL}(V)$. □

2.2 Molien's formula

Since $R = \oplus_{d=0}^{\infty} R_d$ is a connected graded algebra by degree, it is clear that $R^G = \oplus_{d=0}^{\infty} R_d^G$ inherits this grading by degree.

The Hilbert series contains a lot of important information about the invariant ring; however, as it is defined, it is quite difficult to compute. Luckily, Molien's formula gives us a tangible way of computing Hilbert series for any finite group:

Theorem 2.3 (Molien's Formula)**.** *Let V be a $\mathbb{C}$-vector space and let G be a finite group realised as its matrix group in* $\mathrm{GL}(n)$*. Then*

$$H(\mathbb{C}[V]^G, z) = \frac{1}{|G|}\sum_{M\in G}\frac{1}{\det_V(\mathrm{id}_n - zM)},$$

where id_n *is the $n \times n$ identity matrix.*

Before we prove this, we need a small representation theoretic lemma.

Lemma 2.1. *Let G be finite matrix group and let*

$$V^G := \{v \in \mathbb{C}^n \mid Mv = v \text{ for all } M \in G\}$$

denote the invariant subspace. Then $\dim(V^G) = \frac{1}{|G|}\sum_{M\in G}\mathrm{tr}(M)$.

Proof. Consider the average, $A = \frac{1}{|G|}\sum_{M\in G} M$.[2] Since clearly $Av = v$ for $v \in V^G$ and since $A^2v = Av$ (since M acts by permutation on G), we have that A is a projection onto V^G. This implies that A has only 1 and 0 as possible eigenvalues, and it follows that A must have rank equal to the multiplicity of it's 1-eigenvalue. Hence, $\dim(V^G) = \mathrm{rank}(A) = \mathrm{tr}(A) = \frac{1}{|G|}\sum_{M\in G}\mathrm{tr}(M)$. □

[2] In the case of Theorem 2.3, this A turns out to just be the Reynolds operator.

Proof of Theorem 2.3. Recall that the graded part, $\mathbb{C}[V]_d$, is an $\binom{n+d-1}{d}$-dimensional vector space, with monomials of degree d as a basis. Let M_d denote the corresponding matrix of the induced action of M on $\mathbb{C}[V]_d$. The invariant subspace of $\mathbb{C}[V]_d$ with respect to the induced group, $G_d = \{M_d \mid M \in G\}$, will clearly coincide with $\mathbb{C}[V]_d^G$. So we want to find trace of M_d, since then we can use Lemma 2.1.

Identify $\mathbb{C}^n$ with $\mathbb{C}[V]_1$, within which we denote by $v_{M,1}, ..., v_{M,n} \in \mathbb{C}[V]_1$ the eigenvectors of $M = M_1$. Let $\lambda_{M,1}, ..., \lambda_{M,n}$ denote the corresponding eigenvalues. By construction, the eigenvectors of M_d will then be all combinations, $v_{M,1}^{d_1} \cdots v_{M,2}^{d_2}$, such that $d_1 + \cdots + d_n = d$. The corresponding eigenvalues will be $\lambda_{M,1}^{d_1} \cdots \lambda_{M,n}^{d_n}$. Thus we find that

$$\operatorname{tr}(M_d) = \sum_{d_1+\cdots+d_n=d} \lambda_{M,1}^{d_1} \cdots \lambda_{M,n}^{d_n},$$

and by Lemma 2.1 we get

$$\dim(\mathbb{C}[V]_d^G) = \frac{1}{|G|} \sum_{M\in G} \sum_{d_1+\cdots+d_n=d} \lambda_{M,1}^{d_1} \cdots \lambda_{M,n}^{d_n}.$$

Using the closed form of the geometric series, we obtain our result:

$$\begin{aligned}
H(\mathbb{C}[V]^G, z) &= \sum_{d=0}^{\infty} \dim(\mathbb{C}[V]_d^G) z^d \\
&= \sum_{d=0}^{\infty} \left(\frac{1}{|G|} \sum_{M\in G} \sum_{d_1+\cdots+d_n=d} \lambda_{M,1}^{d_1} \cdots \lambda_{M,n}^{d_n} \right) z^d \\
&= \frac{1}{|G|} \sum_{M\in G} \sum_{(d_1,\ldots,d_n)\in\mathbb{N}^n} \lambda_{M,1}^{d_1} \cdots \lambda_{M,n}^{d_n} z^{d_1+\cdots+d_n} \\
&= \frac{1}{|G|} \sum_{M\in G} \frac{1}{(1-\lambda_{M,1}z)\cdots(1-\lambda_{M,n}z)} \\
&= \frac{1}{|G|} \sum_{M\in G} \frac{1}{\det(\mathrm{id}_n - zM)}
\end{aligned}$$

□

Recall from character theory that two members of the same conjugacy class will yield the same character, and thus have the same trace. We therefore see, from the last list of equalities in the proof of Theorem 2.3, that the summands depend only on the conjugacy class. The following corollary follows.

Corollary 2.1. *Let $\mathcal{C}(G)$ denote the set of conjugacy classes of G and M_C denote an arbitrary element of $C \in \mathcal{C}(G)$. Then*

$$H(\mathbb{C}[V]^G, z) = \frac{1}{|G|} \sum_{C\in\mathcal{C}(G)} |C| \frac{1}{\det(\mathrm{id}_n - zM_C)}.$$

Remark 2.3. Molien's formula can be generalized to work with any vector space, over any field, K, whose characteristic doesn't divide $|G|$.

Furthermore there exist a way to extend Molien's formula to the case where $\text{char}(K) = p$ divides $|G|$, but p^2 does *not* divide $|G|$. In general, however, there exists no version of Molien's formula for the modular case. ([DK15, Chapter 2.7]).

2.3 Homogeneous systems of parameters

It turns out that the invariant algebra, R^G, can be decomposed in a special manner, called the Hironaka decomposition. This decomposition is very useful and can aid us in many tasks. For example, it may help us determine better bounds, and many algorithms for constructing a generating set for R^G are based on it.

Let A be a connected graded $\mathbb{C}$-algebra with Krull dimension m. A subset, $\{\theta_1, ..., \theta_m\}$, of homogeneous elements of A of positive degree is called a *homogeneous system of parameters* (h.s.o.p.) if A is finitely generated, as a module over $\mathbb{C}[\theta_1, ..., \theta_m] \subseteq A$. Note that $\theta_1, ..., \theta_m$ can always be chosen to be algebraically independent.

Noether's normalization lemma implies that an h.s.o.p. for A always exists.

The following theorem is purely commutative algebra, and so we will not prove it here, but a proof can be found in [PS08].

Theorem 2.4. *Let A be a connected graded $\mathbb{C}$-algebra with an h.s.o.p, $\theta_1, ..., \theta_n$. Then the following two are equivalent:*

i) *There exists a finite set of homogeneous elements $\eta_1, ..., \eta_t \in A$ such that*

$$A = \bigoplus_{i=1}^{t} \eta_i \mathbb{C}[\theta_1, ..., \theta_m]. \tag{2.1}$$

I.e. A is a finitely generated free *module over $\mathbb{C}[\theta_1, ..., \theta_m]$.*

ii) *A is a finitely generated* free *module over $\mathbb{C}[\phi_1, ..., \phi_m]$ for every h.s.o.p., $\phi_1, ..., \phi_m$.*

Definition 2.2. A connected graded algebra which satisfies (i), and thus also (ii), of Theorem 2.4 is said to be a *Cohen-Macaulay* algebra. We call the decomposition, in Eq. (2.1), the *Hironaka decomposition* of A.

Furthermore, if $A = R^G$ is an invariant algebra, then we call $\theta_1, ..., \theta_m$ the *primary invariants*, and $\eta_1, ..., \eta_t$ the *secondary invariants*. Together they clearly form a generating set for R^G.

A lot of algorithms for computing invariants depend on the Hironaka decomposition: They often first compute the primary invariants, and thereafter compute the secondary invariants. (See [DK15] for examples).

Furthermore, the Hilbert series of a Cohen-Macaulay algebra and the Hironaka decomposition are closely intertwined, as seen in the following corollary shows. A proof of the fact can be found in [Sta78].

Corollary 2.2. *Let A be a Cohen-Macaulay algebra with Krull dimension m. Set $d_1 = \deg(\theta_i)$ and $e_i = \deg(\eta_i)$, then*

$$H(A,z) = \frac{\sum_{i=1}^{t} z^{e_i}}{\prod_{i=1}^{m}(1-z^{d_i})}.$$

Remark 2.4. From this corollary, one can estimate a degree bounds. For instance, if one already knows a good set of primary invariants, then one can multiply through by the denominator to get that

$$\prod_{i=1}^{m}(1-z^{d_i})H(A,z) = \sum_{i=1}^{t} z^{e_i}.$$

From this one can read off the highest degree, e_t, meaning $\beta(A) \leq \max(e_t, d_m)$. Furthermore, the number of secondary invariants of degree i is the the coefficient of z^{e_i} in the polynomial above.

Finally, for invariant algebras, R^G, of Krull dimension m, one can see by Laurent expanding $H(R^G, z)$ that we have

$$t = \frac{d_1 ... d_m}{|G|} \quad \text{and} \quad rt + 2(e_1 + \cdots + e_t) = t(d_1 + \cdots + d_m - m),$$

where r is the number of pseudo-reflections. (An element $M \in \mathcal{I}^n$ is called a *pseudo-reflection* if it has precisely one eigenvalue not equal to 1). From this, one can determine t, the number of secondary invariants. (See [Sta79] for a proof).

We now find ourselves at another critical theorem of modern invariant theory. The theorem says that any invariant algebra of a finite group is Cohen-Macaulay![3] Although being so critical, it was allegedly folk lore for a long time, until properly proven in a 1971 paper by Hochster and Eagon.

Theorem 2.5. *Let $R = \mathbb{C}[x_1, ..., x_m]$ and $G \subseteq \mathrm{GL}(\mathbb{C}^n)$ be a finite matrix group. Then R^G is Cohen–Macaulay.*

Proof. Recall the polynomials F_i from the proof of Proposition 2.3. They are monic polynomials with coefficients in R^G and with x_i a root. Hence, R is finitely generated as an R^G-module. Furthermore, we may decompose $R = R^G \oplus U$ as R^G-modules, with $U = \{\ f \in R \mid \mathcal{R}(f) = 0\ \}$.

Noether's normalization lemma implies that R^G has an h.s.o.p., say $\theta_1, ..., \theta_m$. So we have that R is finite over R^G, which is finite over $\mathbb{C}[\theta_1, ..., \theta_m]$, which means

[3] In fact, the result works in a more general setting: If G is a linearly reductive group, then $K[V]^G$ is Cohen-Macaulay. This is called the Hochster-Roberts Theorem. (See. [DK15])

that R is also finite over $\mathbb{C}[\theta_1, ..., \theta_m]$. Since R is clearly Cohen-Macaulay (e.g. take the h.s.o.p. $\{x_1, ..., x_m\}$) it follows from Theorem 2.4, that R is a finitely generated *free* $\mathbb{C}[\theta_1, ..., \theta_m]$-module.

Hence, by modding out by $\langle \theta_1, ..., \theta_m \rangle$ of $R = R^G \oplus U$, we get that

$$R/\langle \theta_1, .., \theta_m \rangle = R^G/\langle \theta_1, ..., \theta_m \rangle \oplus U/(\theta_1 U, ..., \theta_m U)$$

is a finite dimensional vector space. We can thus choose a $\mathbb{C}$-basis of homogeneous polynomials, $\overline{\eta}_1, ..., \overline{\eta}_t, \overline{\eta}_{t+1}, ..., \overline{\eta}_s$ for $R/\langle \theta_1, .., \theta_m \rangle$, such that $\overline{\eta}_1, ..., \overline{\eta}_t$ is a basis for $R^G/\langle \theta_1, .., \theta_m \rangle$ and $\overline{\eta}_{t+1}, ..., \overline{\eta}_s$ is a basis for $U/(\theta_1 U, .., \theta_m U)$.

We may now lift $\overline{\eta}_1, ..., \overline{\eta}_t$ resp. $\overline{\eta}_{t+1}, ..., \overline{\eta}_s$ to elements $\eta_1, ..., \eta_t \in R^G$ resp. $\eta_{t+1}, ..., \eta_s \in U$. By Theorem 2.4, we have that $R = \bigoplus_{i=1}^{s} \eta_i \mathbb{C}[\theta_1, ..., \theta_m]$, which by our decomposition, $R = R^G \oplus U$, gives the desired Hironaka decomposition of R^G,

$$R^G = \bigoplus_{i=1}^{t} \eta_i \mathbb{C}[\theta_1, ..., \theta_m],$$

which, by definition, shows that R^G is Cohen-Macaulay. □

2.3.1 The Gorenstein property

An even stronger property, than the Cohen-Macaulay property, that *some* invariant rings admit is the Gorenstein property. The following are one of the many equivalent definitions of the Gorenstein property.

Definition 2.3. A commutative local Noetherian ring, R, is said to be a *Gorenstein local ring* if it has finite injective dimension as an R-module. A general commutative Noetherian ring is said to be *Gorenstein* if it is a Gorenstein local ring for every localization at a prime ideal.

Remark 2.5 ([DK15])**.** Let $R = \mathbb{C}[V]$, G finite and let $A \subseteq R^G$ be a subalgebra generated by a set of primary invariants. We have that $\mathrm{Hom}(R^G, A)$ is a R^G-module with $(f \cdot \varphi)(g) := \varphi(f \cdot g)$ for $f, g \in R^G$ and $\varphi \in \mathrm{Hom}(R^G, A)$. Then R^G is Gorenstein if $\mathrm{Hom}(R^G, A)$ is free of rank one, as an R^G-module. This is independent of the choice of A.

In particular, Gorenstein implies Cohen-Macaulay, meaning it's a strictly stronger property.

This next remarkable theorem, due to [Sta78], is not strictly within the field of invariant theory, but since it assumes Cohen-Macaulay, it is very well suited for invariant theory. The complete proof is rather very long, so we'll only be given a sketch of the "only if" part, which is arguably the most interesting part.

Theorem 2.6. *Let A be connected graded Cohen-Macaulay algebra. Assume further that A is an integral domain with Krull dimension m. Then A is a Gorenstein algebra if and only if there exists some $r \in \mathbb{Z}$ such that $H(A, \frac{1}{z}) = (-1)^m z^{m+r} H(A, z)$.*

Proof sketch of the "only if" part of theorem 4.4 in [Sta78]. Since A is finitely generated it has, say, s generators. Let then $P = \mathbb{C}[y_1, ..., y_s]$ be a polynomial ring over $\mathbb{C}$ in s independent variables.

Because A is Cohen-Macaulay we may consider the canonical module, K_A, of A (i.e. $K_A = \mathrm{Ext}_P^{s-m}(A, P)$). The proof is then based on the fact that A is Gorenstein if and only if $K_A \cong A$.

To show this isomorphism one first shows that K_A can be graded, as an A-module, in such a way that $H(K_A, z) = (-1)^m z^q H(K_A, \frac{1}{z})$, for some $q \in \mathbb{Z}$. (This is the hard part).

Because the above, along with the assumptions of the theorem, we may 'shift' the grading of K_A in such a way that the 0-degree elements form a vector space over K of dimension one. Furthermore, since A is an integral domain, we have that K_A is isomorphic to an ideal of A. Identifying K_A with this ideal, we see from the above that $H(K_A, z) = H(A, z)$, and since A is an integral domain, we have that $\dim(xA_d) = \dim(A_d) = H(A, z)_d = H(K_A, z)_d$, for any $0 \neq x \in K_A$ of degree 0. But $K_A \subseteq A$ is an ideal and $x \in K_A$ so $xA_d \subseteq K_{A,d}$, and since $\dim(xA_d) = H(K_A, z)_d = \dim(K_{A,d})$, we have $xA_d \cong K_{A,d}$. It then follows that $A \cong xA \cong K_A$. □

Being Gorenstein comes with a lot of homological properties (see [Hap91]), which we didn't have time to explore with our example of graphs in Section 3. However, we do think it would be fruitful to explore what can be inferred about graphs, by applying the above theorem and focusing on the homological properties, which arise from its Gorenstein property.

2.4 Minimal generating sets and King's algorithm

Given some set of primary invariants, the set of secondary invariants are minimal module-generators. However, the union of the two need not be minimal algebra generators, as defined below.

Definition 2.4. Let $\mathcal{B}$ be a set of elements of a connected graded algebra, A. We call $\mathcal{B}$ a minimal system of generators if A is generated by $\mathcal{B}$, but *no* strict subset of $\mathcal{B}$ generates A, as an algebra.

Similarly to vector spaces, where bases are not unique but the number of basis elements is, we see that minimal generating sets for graded algebras are not unique, but the number of elements as well as the degrees *are* unique. In fact, the two notions are closely related as the proof of the following shows.

Proposition 2.4. *Let* $\{a_1, ..., a_k\}$ *and* $\{b_1, ..., b_l\}$ *be two homogeneous minimal generating sets for a connected graded algebra,* A *over* $\mathbb{C}$*, sorted in increasing order by degree. Then* $k = l$ *and* $\deg(a_i) = \deg(b_i)$ *for all* i*. Hence* $\beta(A) = \deg(a_k)$.

Proof sketch. Let $A_+ \subseteq A$ denote the ideal in A of consisting of elements of positive degree. A homogeneous set $\mathcal{B}$ generates A as an algebra if and only if the same set generates $A_+ \subseteq A$ as an ideal. Furthermore, by Nakayama's lemma (the graded version) we have that $\mathcal{B}$ generates A_+ as an ideal if and only if they generate A_+/A_+^2 as a vector space over $\mathbb{C}$. Thus $\{a_1, ..., a_k\} \subseteq \mathcal{B}$ can be chosen to be a basis of the vector space A_+/A_+^2, and their lift to A will then be a minimal generating set. □

There is no known general shortcut for knowing the size of the minimal generating set, nor how many of each degree there are. Thus, the only real way to know these numbers is to compute a minimal generating set.

2.4.1 King's algorithm

A relatively new way of computing a minimal generating set for a finite group was introduced by King in 2007 ([Kin13]) with what is now called King's algorithm. It is a remarkably simple algorithm that directly computes the minimal generating set, avoiding primary and secondary invariants. Here we give the slightly altered version and proof, both due to [DK15]. King's algorithm is also noteworthy in that it essentially avoids the use of Gröbner bases; however, in our experience with the examples from Section 3, we found that using d-truncated Gröbner bases is faster.

Let M_d denote the set of monomials of degree d, let $\mathrm{LM}(f)$ denote the leading monomial of f, and let $\mathrm{NF}_{\mathcal{G}}(f)$ denote the normal form of f, with respect to the set of polynomials, $\mathcal{G}$. (See [DK15, Algorithm 1.1.6] for an algorithm). We also denote by $\mathrm{spol}(f, g)$ the s-polynomial of f, g. (See [DK15, Section 1.1.4]). Finally, a subset, $\mathcal{G} \subseteq I$, of an ideal is called a *d-truncated Gröbner basis* if every monomial of $L(I) := \{\mathrm{LM}(f) \mid f \in I\}$ of degree $\leq d$ is contained in $L(\mathcal{G})$.

Algorithm 1: King's algorithm

input : Finite group, G, and an upper bound, D, on $\beta(\mathbb{C}[V]^G)$
output: Minimal generating set, S, of $\mathbb{C}[V]^G$, where $V = \mathbb{C}^m$

```
S ← ∅
G ← ∅
for d from 1 to D do
    G ← d-truncated Gröbner basis of ⟨S⟩
    M ← {m ∈ M_d | ∄g ∈ G such that LM(g) divides m}
    if M = ∅ then break;
    for t ∈ M do
        f ← R(t)
        if g ← NF_G(f) ≠ 0 then
            Add f to S
            Add g to G
return S
```

Proof of correctness. Denote by $\mathbb{C}[V]^G_{<d}$ the subalgebra generated by all invariants of degree $< d$. The proof is by induction on d, and since the base case is clear, we need only show that after the d'th iteration, we have that $\mathbb{C}[V]^G_{<d} \subseteq \mathbb{C}[S]$. So let S be the set we get at the end of the $(d-1)$'th iteration, and assume $\mathbb{C}[V]^G_{<d-1} \subseteq \mathbb{C}[S]$.

Let $f \in \mathbb{C}[V]^G_d$. By definition of the normal form, we have $f - \mathrm{NF}_{\mathcal{G}}(f) \in \langle \mathcal{G} \rangle \subseteq \langle S \rangle$, so we may write $f - \mathrm{NF}_{\mathcal{G}}(f) = \sum_{i=1}^r g_i f_i$, with homogeneous $f_i \in S$ and homogeneous $g_i \in \mathbb{C}[V]$ of degree $d - \deg(f_i) < d$. By applying the Reynolds operator, $\mathcal{R}$, on equality, we get that

$$f - \mathcal{R}(\mathrm{NF}_{\mathcal{G}}(f)) = \sum_{i=1}^{r} \mathcal{R}(g_i) f_i \in \mathbb{C}[S]. \tag{2.2}$$

Notice that by construction $\mathrm{NF}_{\mathcal{G}}(f)$ lies in the K-span of $\langle M \rangle$. Thus, $\mathcal{R}(\mathrm{NF}_{\mathcal{G}}(f))$ lies in the K-span of $\langle \mathcal{R}(M) \rangle$, and so we can conclude that

$$\mathbb{C}[V]^G_d \subseteq \mathbb{C}[S] + \mathrm{span}(\langle \mathcal{R}(M) \rangle). \tag{2.3}$$

It remains to prove that the algebra generated by S, after the for-loop of line 7, contains $\mathcal{R}(M)$. Assume some number of iterations have passed and let $f_1, ..., f_m$, respectively $g_1, ..., g_m$, be the invariants which have been added to S, respectively be the normal forms of the f_i's added to $\mathcal{G}$. Denote $S' = S \cup \{f_1, ..., f_m\}$ and $\mathcal{G}' = \mathcal{G} \cup \{g_1, ..., g_m\}$ these new sets. We notice that $\mathcal{G}'$ remains a d-truncated Gröbner basis since no s-polynomial of degree $\leq d$ can arise from $g_1, ..., g_m$ and $\mathcal{G}$. Thus, the classic membership test will work with $\mathcal{G}'$, i.e. $\mathrm{NF}_{\mathcal{G}'}(\mathcal{R}(t)) = 0$ if and only if $\mathcal{R}(t) \in \langle S' \rangle$, which, by Eq. (2.2) and the argument below Eq. (2.2), means that $\mathcal{R}(t) \in \mathbb{C}[S']$. Therefore, by the end of the for-loop, we must have $\mathcal{R}(M) \subseteq \mathbb{C}[S']$, and, since we only added elements whenever it made the algebra larger, the set S' must be minimal. Finally, since $\mathcal{G}$ remained a d-truncated Gröbner basis, when we pass to iteration $d+1$, step 4 will yield the correct result.

In the case that $M = \emptyset$ we have from Eq. (2.3) that $\mathbb{C}[V]^G_{<d} \subseteq \mathbb{C}[S]$. Furthermore, $M = \emptyset$ implies that every monomial of degree d is divisible by the leading monomials of some $g \in \mathcal{G}$. But this is clearly also true clearly for every monomial of degree $> d$, and so $M = \emptyset$ for all subsequent iterations. Thus if $M = \emptyset$, we must conclude that $\mathbb{C}[S] = \mathbb{C}[V]^G$, and we may terminate the process. □

Because line 4 in the algorithm can be replaced with the line,

$$\mathcal{G} \leftarrow \mathcal{G} \cup \{\mathrm{NF}_{\mathcal{G}}(h) \mid h = \mathrm{spol}(f, g), \forall f, g \in \mathcal{G} \text{ with } \deg(h) = d\},$$

the algorithm is sometimes called 'essentially Gröbner free'. However we found the algorithm, as presented above, to be much faster.

There are a few ways to further optimize King's algorithm, however we will not implement them here. See [DK15, Chapter 3.8].

In most cases King's algorithm outperforms all other algorithms for computing algebra generators, for arbitrary finite invariant algebras. So not only is King's algorithm simple and gives a *minimal* set, it's also generally the most effective known method!

King's algorithm has already been implemented many places, such as in `SINGULAR` and `MAGMA`, however we still implement our own version in `SAGEMATH`. See Appendix A, Listing 5.

2.5 Permutation groups

Permutation groups are particularly well-behaved, as we will see in this section. First and most importantly, we have a 'canonical' choice for primary invariants, when G is a permutation group. Indeed, the following shows that it is quite natural to study R^G as an R^{S_m}-module. A proof of the fact can be found in [DK15, Chapter 3.10].

Theorem 2.7. *Let $R = \mathbb{C}[x_1, ..., x_m]$ and $G \subseteq S_m$ be a permutation group. Then the elementary symmetric polynomials, $\sigma_1, ..., \sigma_m$, as defined in Example 2.1, is a choice of primary invariants of R^G.*

We may combine this fact with Remark 2.4 to get the following bounds.

Corollary 2.3. *Let $R = \mathbb{C}[x_1, ..., x_m]$ and $G \subseteq S_m$ be a permutation group. Then R^G is a free module of rank $t = \frac{m!}{|G|}$ over R^{S_m}. Furthermore, the number and degree of the secondary invariants can be found by observing the polynomial,*

$$\sum_{i=1}^{t} z^{\deg(\eta_i)} = H(R^G, z) \prod_{i=1}^{n} (1 - z^i),$$

with η_i denoting the secondary polynomials.

Remark 2.6. In fact, in [Gö95], Göbel managed to show that when G is a permutation group of degree m, we have that $\beta(R^G) \leq \binom{m}{2}$.

All these results may seem very helpful, since there are clever algorithms that compute the secondary invariants, when the primary invariants are given. However, it is seldom the case that the choice of the elementary symmetric polynomials yield a minimal generating set. In fact, for group of high degree, it will yield uncomputably large sets. For example, the algebra, $\mathcal{I}^5$, from Section 3.1 has a minimal generating set of size 56, i.e. 46 secondary invariants ([Thi00]). However, with the choice above we would have a whopping $\frac{\binom{10}{2}!}{5!} = 30\,240$ secondary invariants! Even worse, $\mathcal{I}^6$ is conjectured to have a minimal generating set consisting of 552 secondary invariants, while the above would give us $\frac{\binom{6}{2}!}{6!} = 1\,816\,214\,400$ secondary invariants.

Moreover, in his article, [Bor15], Borie used the elementary symmetric polynomials as primary invariants to create an effective algorithm for computing these secondary invariants. Incredibly, he managed to compute all 30 240 secondary invariants of $\mathcal{I}^{5[4]}$ in a couple of minutes, whereas he claims it would take `MAGMA` and `SINGULAR` over 24 hours to do the same. However, as stated above, because he uses a 'bad' set of primary invariants, the algorithm won't scale well to $\mathcal{I}^6$ or higher since we would either run out of memory or even storage.

But what *is* helpful is that the Hilbert series becomes very computable, in the case of Permutation groups!

2.5.1 Hilbert Series of permutation groups

We will, in this subsection, give an easy to compute formula for the Hilbert series of R^G, when G is a permutation group. This formula plays a crucial role in Section 3.

We start with a helpful lemma.

Lemma 2.2. *Let M be the permutation matrix corresponding to a permutation σ. Then we have that*

$$\det(\mathrm{id}_n - zM) = \prod_k (1 - z^k)^{l_k},$$

where l_k denotes the number of k-cycles in the cycle decomposition of σ.

Proof. First note that we may rearrange and decompose $M = \oplus_i P_{k_i}$, where P_{k_i} corresponds to a k-cycle, for some k. I.e. P_{k_i} is the $k \times k$-matrix with 1 in the super diagonal and in the bottom-left and 0 otherwise. Thus

$$\mathrm{id}_k - zP_{k_i} = \begin{pmatrix} 1 & -z & & \\ & 1 & -z & \\ & & \ddots & \\ -z & & & 1 \end{pmatrix},$$

and one easily sees that $\det(P_{k_i} - z\mathrm{id}_k) = 1 - z^k$, from which it follows that

$$\det(\mathrm{id}_n - zM) = \det(\oplus_i(\mathrm{id}_k - zP_{k_i})) = \prod_i \det(\mathrm{id}_k - zP_{k_i}) = \prod_k (1 - z^k)^{l_k},$$

where in the last equality we combined all cycles of equal length. □

Since permutations of the same conjugacy class have the same cycle-type we may combine the above lemma with Theorem 2.3 to get the following, quite explicit, formula.

[4] Actually, in the paper, Borie claims he is computing invariants of $\mathcal{I}^5$. However, when we computed the Hilbert series of the permutation group that he used, it did *not* match that of $\mathcal{I}^5$, meaning he can't have computed the invariants of $\mathcal{I}^5$. Nevertheless, the effectiveness of the algorithm still stands.

Corollary 2.4. *Let $G \subset S_n$ be a permutation group, let $\mathcal{C}(G)$ denote the set of conjugacy classes of G, and let σ_C be an arbitrary element of $C \in \mathcal{C}(G)$. Then*

$$H(R^G, z) = \frac{1}{|G|} \sum_{C \in \mathcal{C}(G)} |C| \frac{1}{\prod_i (1 - z^i)^{\lambda_i(\sigma_C)}}$$

where $\lambda_i(\sigma_C)$ denotes the number of i-cycles of $\sigma_C \in C$.

Furthermore, we noticed the following connection to Section 1.2, which we haven't seen noted anywhere else, even though it's quite a quirky connection.

Remark 2.7. For a permutation group, G, we have that

$$H(R^G, z) = Z(G, \tfrac{1}{1-z}).$$

This follows from immediately from Corollary 2.4 and the definition of $Z(G)$.

3 Invariant Theory on Graphs

With all the relevant background theory built up, we now move to a peculiar application of invariant theory, namely graphs. This section mainly follows Nicolas Thiery's exposition of the topic ([Thi00]), but we expand upon certain parts, using inspiration from other sources, which will be mentioned along the way.

We consider an undirected finite graph, $g = (V, E)$, with vertex set, V, and edge set, E. We will label each vertex with a number, so that $V = \{1, 2, ..., n\}$, and the edges by *2-sets*, so that $E = \{\ \{i, j\} \mid i, j \in V\ \}$. We call such a graph a *labelled* graph. If we assign to each edge, $\{i, j\}$, of a graph, g, a weight, $w_g(\{i, j\}) \in K$ over some field, K, then we call the graph a labelled K-*weighted* graph.

Given a vertex set, V, we may consider the K-vector space with basis vectors, $\mathbf{e}_{\{i,j\}}$, indexed by the edges, $\{i, j\} \subseteq V$. We denote this vector space by $\mathbb{G}_n$. It is clear that $\mathbb{G}_n$ and the set of all labelled K-weighted graphs are in bijection. Thus each point in $\mathbb{G}_n$ corresponds to a K-weighted graph. Furthermore $\mathbb{G}_n$ has dimension $m := \binom{n}{2}$, since there are m possible edges.

Recall the symmetric group, S_n, and let it act on our vertex set $V = \{1, 2, ..., n\}$. This is the classical representation of S_n. However, S_n also acts on our edge set, E, by $\sigma \cdot \{i, j\} = \{\sigma \cdot i, \sigma \cdot j\}$, with $\sigma \in S_n$. This gives us a representation of S_n in $S_{\binom{n}{2}}$, and we denote this representation by $S_n^{(2)}$. Clearly, $S_n^{(2)}$ is a permutation group of degree $\binom{n}{2}$ and size $n!$. $S_n^{(2)}$ also acts naturally on $\mathbb{G}_n$, by its induced action on the basis vectors, $\sigma \cdot \mathbf{e}_{\{i,j\}} = \mathbf{e}_{\{\sigma \cdot i, \sigma \cdot j\}}$.

Two K-weighted graphs, $g = (V, E)$ and $g' = (V', E')$, are said to be isomorphic if there exists some $\sigma \in S_n^{(2)}$ such that $\sigma \cdot g = \sigma \cdot \sum_E w\mathbf{e}_{\{i,j\}} = \sum_E w\mathbf{e}_{\{\sigma \cdot i, \sigma \cdot j\}} = g'$, i.e. if they are in the same $S_n^{(2)}$-orbit. If $w \in \{0, 1\}$ then g and g' are simple graphs and the definition of graph isomorphism coincides with the usual definition. We call an isomorphism class of a labelled K-weighted graph, an *unlabelled* K-weighted graphs.

We now let $K = \mathbb{C}$ and consider the coordinate ring,

$$\mathbb{C}[\mathbb{G}_n] = \mathbb{C}[\ x_{\{i,j\}} \mid \{i, j\} \in E\ ],$$

where evaluation $f(g)$, of a polynomial $f \in \mathbb{C}[\mathbb{G}_n]$ on a $\mathbb{C}$-weighted graph $g \in \mathbb{G}_n$, is given by mapping $x_{\{i,j\}}$ to $w_g(\{i, j\})$. Naturally, $S_n^{(2)}$ acts on $\mathbb{C}[\mathbb{G}_n]$, defined by $\sigma \cdot x_{\{i,j\}} = x_{\{\sigma \cdot i, \sigma \cdot j\}}$, i.e. acts by permutation of the indeterminates.

We are, of course, now interested in the invariant ring, $\mathcal{I}^n := \mathbb{C}[\mathbb{G}_n]^{S_n^{(2)}}$, since it holds a lot of information about the orbits of $S_n^{(2)}$ on $\mathbb{G}_n$, and thus also about the isomorphism classes of $\mathbb{C}$-weighted graphs (i.e. unlabelled graphs). For example, if the invariants $f_1, ..., f_n \in \mathcal{I}^n$ generate $\mathcal{I}^n$, then they necessarily separate the orbits, meaning that $g \cong g'$ if and only if $f_i(g) = f_i(g')$ for all i.

All this leads into the following naïve algorithm to check graph isomorphism, based on invariant theory:

Algorithm 2: Check graph isomorphism

input : Graphs g and g'

output: Boolean value of `True` if $g \cong g'$ and `False` otherwise

```
Compute a generating set f_1, ..., f_r of I^n
if f_i(g) = f_i(g') for all i = 1, ..., r then
    return True
else
    return False
```

The problem of finding an efficient algorithm[5] which checks if two given graphs are isomorphic is called the graph isomorphism problem. In fact, it is still not known if this is an NP-hard problem, meaning we have yet to find (or know if there exists) a polynomial time algorithm to check if two graphs are isomorphic.

In our case, if Algorithm 3 were to be a polynomial time algorithm, then, first of all, the maximal degree and the number of terms of the f_i need to be bounded by a polynomial function. Secondly, the number of generators, r, must also be bounded by some polynomial function, with respect to the number of vertices, n. Finally, we must be able to compute $\mathcal{I}^n$ in polynomial time.

By Remark 2.6, we know that $\beta(\mathcal{I}^n) \leq \binom{\binom{n}{2}}{2}$, which is polynomial! However, there can be up to $n!$ terms in a polynomial, but we're uncertain if they can be avoided. For the second concern, it seems that even for minimal invariant sets, the number, r, increases exponentially (see [Thi00]). The final concern is even worse since the computation of $\mathcal{I}^n$ proves to be exceedingly difficult, with only $\mathcal{I}^n$ having ever only been computed for $n \leq 5$.

But even so, as study of $\mathcal{I}^n$ can still be fruitful as we can extract a lot of information about graphs from this ring, such as enumeration of number of graphs and even be used to prove that certain classes of graphs are reconstructable. Furthermore, for the invariant algebra of simple graphs, which we will encounter later on, it is still not entirely known to which extend these concerns transfer.

3.1 The invariant ring $\mathcal{I}^n$

We will now delve deeper into the structure of $\mathcal{I}^n$ as defined above.

Our first observation is that labelled multigraphs (i.e. a graph weighted in $\mathbb{N}$), g, may be uniquely encoded as the monomial,

$$\mathbf{x}^g := \prod_{\{i,j\} \subseteq \{1,2,\ldots,n\}} x_{\{i,j\}}^{w_g(\{i,j\})}.$$

And it is clear that the set of such monomials corresponds one-to-one to the set of all *labelled* multigraphs.

[5] By efficient algorithm, we mean an algorithm that runs in polynomial time.

From this we can construct an obvious invariant by summing over all the elements in the orbit of g:

$$\mathbf{x}^{g^{\circledast}} := \sum_{h \in S_n^{(2)} \cdot g} \mathbf{x}^h. \tag{3.1}$$

We call $\mathbf{x}^{g^{\circledast}}$ the *exponential* of g. Since it is the sum of the isomorphism class of a given graph, it follows that the set of all exponentials correspond one-to-one to the set of *unlabelled* multigraphs! In fact, the exponential of a graph is just to the Reynolds operator, $\mathcal{R}$, up to a factor of the size of the automorphism group of g, $|\mathrm{Aut}(g)|$, that is, $\mathbf{x}^{g^{\circledast}} = |\mathrm{Aut}(g)|\mathcal{R}(\mathbf{x}^g)$. Since exponentiation is the Reynolds operator up to a scalar, we see that it is a projection to the invariant set. This leads to the first easy theorem.

Theorem 3.1. *Labelled graphs form a basis of $\mathbb{C}[\mathbb{G}_n]$ and unlabelled graphs form a basis of $\mathcal{I}^n$, as vector spaces. Furthermore, $\dim(\mathbb{C}[\mathbb{G}_n]_d)$ (resp. $\dim(\mathcal{I}^n_d)$) count the number of labelled (resp. unlabelled) multigraphs which use exactly d edges.*

Proof. We have that the set of monomials form a basis for $\mathbb{C}[\mathbb{G}_n]$, and we saw above that the set of such monomials correspond one-to-one to the set of labelled graphs on n vertices. It follows from Example 2.2 that $\mathcal{R}(\mathbb{C}[\mathbb{G}_n]_d) = \mathcal{I}^n_d$ and because $\mathcal{R}$ is linear it maps a basis to a basis. Thus the first claim follows from the fact that exponentiation is $\mathcal{R}$ up to a scalar.

The second claim follows from the fact that the monomials $\mathbf{x}^g$, with

$$\sum_{\{i,j\} \subseteq \{1,2,\ldots,n\}} w_g(\{i,j\}) = d,$$

form a basis for $\mathbb{C}[\mathbb{G}_n]_d$ and so $\mathbf{x}^{g^{\circledast}}$ is a basis for $\mathcal{I}^n_d$. □

For large n, the computation of the exponential can be quite exhaustive. However, it has a lot of interesting properties. One such property is its ability to count subgraphs.

Proposition 3.1. *Let g and h be simple graphs on n vertices. Then the evaluation $\mathbf{x}^{g^{\circledast}}(h)$ counts the number of subgraphs of h which are isomorphic to g. We denote the number, $\mathbf{x}^{g^{\circledast}}(h)$, by $s(g,h)$.*

Proof. We have $\mathbf{x}^g = \prod_{e \text{ edge in } g} x_e$ and so $\mathbf{x}^g(h)$ is 1 if g is a subgraph of h and 0 otherwise. Since $\mathbf{x}^{g^{\circledast}}$ is the sum over the isomorphism class of g of such products it follows that $\mathbf{x}^{g^{\circledast}}(h)$ counts the number elements in the orbit of g which is a subgraph of h. This is exactly the number of subgraphs of h which are isomorphic to g. □

For example, if g has only one edge, then $s(g,h)$ counts the number of edges in h. If g is a closed loop visiting all vertices exactly once then $s(g,h)$ is the number of Hamiltonian cycles of h.

3.1.1 The Hilbert series of $\mathcal{I}^n$ and group generators of $S_n^{(2)}$

Since $S_n^{(2)}$ is a permutation group we can use the results of Section 2.5.1 to compute the Hilbert series of $\mathcal{I}^n$. By Theorem 3.1, this doubles as a generating series for the number of unlabelled multigraphs.

We first introduce some notation.

Notation 3.1. For a partition, λ of n, we write λ_i for the number of factors i contributes to the partition. For example, for $n = 5$, and $\lambda = 1+1+1+2$, we have $\lambda_1 = 3$, $\lambda_2 = 1$, $\lambda_3 = 0$, and so on. The partition λ induces a partition $\overline{\lambda}$ of $\binom{n}{2}$ over $S_n^{(2)}$, which we call the *induced partition*. That is, $\overline{\lambda}$ is given by the cycle type of the induced permutation, $\overline{\sigma} \in S_n^{(2)}$, of any $\sigma \in C_\lambda$, with C_λ being the conjugacy class tied to the partition λ.

The following technical lemma gives us an explicit way to compute $\overline{\lambda}$ from a given λ.

Lemma 3.1. *Let $\sigma \in S_n$ and let $\overline{\sigma} \in S_n^{(2)}$. Then every cyclic factor of $\overline{\sigma}$ arise in one of the following ways:*

i) *If k odd, then each k-cycle contributes exactly $\frac{k-1}{2}$ k-cycles to $\overline{\sigma}$.*

ii) *If k even, then each k-cycle contributes one $\frac{k}{2}$-cycle and $\frac{k-2}{2}$ k-cycles to $\overline{\sigma}$.*

iii) *Every pair, k-cycle and l-cycle, of cyclic factors of σ contribute* $\gcd(i,j)$ *factors of* $\mathrm{lcm}(i,j)$*-cycles to $\overline{\sigma}$.*

The following proof is due to [Ker91].

Proof. i) Let k be odd. By symmetry, we may assume the k-cycle that we consider is $(1\ 2\ ...\ k)$. Choose any $0 \leq l \leq \frac{k-1}{2}$. Then $\overline{\sigma}$ will contain the k-cycle,

$$(\{1, l+1\}\ \{2, l+2\}\ ...\ \{k-l, k\}\ \{1, k-l+1\}\ \{2, k-l+2\}\ ...\ \{l, k\}).$$

These cycles are pairwise disjoint for differing l. These are all the cycles arising from $(1\ 2\ ...\ k)$ that there are since k is odd, so

$$(\{1, l+1\}\ \{2, l+2\}\ ...) = (\{1, k-l+1\}\ \{2, k-l+2\}\ ...).$$

ii) Let $k = 2m$ be even. By symmetry, we may assume the k-cycle that we consider is $(1\ 2\ ...\ 2m)$. Choose $0 \leq l \leq m$. Then $\overline{\sigma}$ will contain the k-cycle,

$$(\{1, l\}\ \{2, l+1\}\ ...\ \{k-l+1, k\}\ \{1, k-l+2\}\ \{2, k-l+3\}\ ...\ \{l-1, k\}).$$

Furthermore $\overline{\sigma}$ will contain the $\frac{k}{2}$-cycle,

$$(\{1, m+1\}\ \{2, m+2\}\ ...\ \{m, 2m\}).$$

iii) By symmetry, we may assume the pair we consider are $(1\ ...\ k)(k+1\ ...\ k+m)$. Then $\overline{\sigma}$ will contain the product of disjoint cycles,

$$(\{1, k+l\}\ \{2, k+l+1\}\ ...)(\{1, k+l+1\}\ \{2, k+l+2\}\}\ ...)...,$$

each factor being a $\text{lcm}(k,m)$-cycle and thus there being a total of $\gcd(k,m)$ of them.

□

Remark 3.1. The proof of Lemma 3.1 is stronger than the actual lemma, since it gives a recipe to construct $\overline{\sigma}$. This fact can be used to construct generators for $S_n^{(2)}$. Indeed, since S_n is famously generated by $(1\ 2)$ and $(1\ 2\ \cdots\ n)$, we need only follow the above proof twice to the get generators $\overline{(1\ 2)}$ and $\overline{(1\ 2\ \cdots\ n)}$ of $S_n^{(2)}$.

This leads us to the next 'algorithm' which gives us generators for $S_n^{(2)}$. This algorithm is our own idea, design and work, however it is quite likely that this has already been created before.

In the following algorithm we let S_n be the symmetric group acting on $\{1, 2, ..., n\}$ and let $m = \binom{n}{2}$. We label the two-sets $\{i, j\}$ with respect to the lexicographic order.[6] Note also that we put commas in the cycles for readability.

Algorithm 3: Construct generators of $S_n^{(2)}$

input : $n \geq 3$

output: Elements, g_1 and g_2, generating $S_n^{(2)}$

$g_1 \leftarrow (2,n)(3,n+1)(4,n+2)\cdots(n-1,n)$

$g_2 \leftarrow ()$

if n is even **then**

  for $i \in \{1, ..., \frac{n-2}{2}\}$ **do**

    $g_2 \leftarrow g_2(i, i+(n-1), i+(n-1)+(n-2), \cdots, i+(n-1)+\cdots+(n-i), (n-i)+(n-1), (n-i)+(n-1)+(n-2), \cdots, (n-i)+(n-1)+\cdots+i)$

  $g_2 \leftarrow g_2({}^n\!/_2, {}^n\!/_2+(n-1), \cdots, {}^n\!/_2+(n-1)+\cdots+(n-{}^n\!/_2)$

if n is odd **then**

  for $i \in \{1, ..., \frac{n-1}{2}\}$ **do**

    $g_2 \leftarrow g_2(i, i+(n-1), i+(n-1)+(n-2), \cdots, i+(n-1)+\cdots+(n-i), (n-i)+(n-1), (n-i)+(n-1)+(n-2), \cdots, (n-i)+(n-1)+\cdots+i)$

return g_1, g_2

Proof of correctness. We first consider $g_1 = \overline{(1,2)}$. Clearly $\{a,b\}$ is fixed if $a = 1$ and $b = 2$ or if $b > a > 2$. The elements which not fixed are the sets, $\{1,a\}$, with $3 \leq a \leq n$, which are labelled by $2, 3, ..., n-1$. Since $(1,2)$ maps $\{1,a\}$ to $\{2,a\}$,

[6] E.g. if $n = 4$ we label $\{1,2\}$ by 1, $\{1,3\}$ by 2, $\{1,4\}$ by 3, $\{2,3\}$ by 4, $\{2,4\}$ by 5, and $\{3,4\}$ by 6.

which in terms of the labelling means that it maps $a-1$ to $n-1+a-1$. From this follows g_1.

Next, we consider $g_2 = \overline{(1,2,...,n)}$. Note that in terms of our labelling we have that $\{1,2\}$ is labelled by 1, $\{2,3\}$ by n, $\{3,4\}$ by $n+(n-1)$, $\{4,5\}$ by $n+(n-1)+(n-2)$, and so on. So in general, if $\{a,b\}$, with $a<b<n$, is labelled by i, then $\{a+1,b+1\}$ is labelled by $i+(n-a)$. The only other case is $\{a,b\}$, with $a<b=n$, which is mapped by $(1,2,...,n)$ to $\{1,a+1\}$ which is labelled by a. From this along with the proof of Lemma 3.1 follows g_2. □

We have implemented the above procedure in SAGEMATH, and the implementation itself is in our opinion a tiny bit more legible than the above. See Appendix A, Listing 8.

This algorithm allows us to explicitly construct $S_n^{(2)}$ as a permutation group in SAGEMATH. Because of SAGEMATH's many feature, this opens the door to many of the pre-built methods of permutation groups, that SAGEMATH has. For example, SAGEMATH allows us to compute the subgroups and homology/cohomology groups of permutation groups.[7] It even allows us to compute the Hilbert series, however the following is much more efficient.[8] Moreover, the explicit construction allows us to use King's algorithm on $\mathcal{I}^n$!

Since the conjugacy classes of S_n are indexed by the partitions of n, we can combine Lemma 2.2 with Corollary 2.4 to get a very explicit formula for the Hilbert series of $\mathcal{I}^n$.

Formula 3.1. *Let C_λ be the conjugacy class corresponding to the partition, λ of n, and let $\overline{\lambda}$ denote the induced partition over $S_n^{(2)}$. Then the Hilbert series of $\mathcal{I}^n$ is given by*

$$H(\mathcal{I}^n, z) = \frac{1}{n!}\sum_{\lambda} |C_\lambda| \frac{1}{\prod_i (1-z^i)^{\overline{\lambda}_i}},$$

where we sum over all partitions λ of n.

Using this corollary with Lemma 3.1, we implement an algorithm for computing $H(\mathcal{I}^n, z)$ in SAGEMATH. The source code can found in Appendix A, Listing 11.

Remark 3.2. From Remark 2.7 and from the theorem of [HP73, p.88], one again find, through different means, that $\dim(\mathbb{C}[V_n]_d^G)$ counts the number of multigraphs on n vertices with exactly d edges.

[7] See doc.sagemath.org/html/en/reference/groups/sage/groups/perm_gps/permgroup.html for the full documentation on support SAGEMATH has on permutation groups.

[8] Indeed, it takes several hours to for the SAGEMATH built-in function to compute the Hilbert series of $\mathcal{I}^9$, while our own custom implementation below only takes us a couple of seconds. (We remark this this is *not* due to the fact that SAGEMATH computes the entire group as it only takes ∼1.2 seconds to compute $S_9^{(2)}$).

3.1.2 Computing invariants of $\mathcal{I}^n$ explicitly

Using Algorithm 3 to get generators of $S_n^{(2)}$. We can construct the group as a permutation group object by plugging the generators into the `SAGEMATH` function, `PermutationGroup`. We then plug this group into our implementation, Listing 5, of King's algorithm (Algorithm 1) to compute a minimal invariant set of $\mathcal{I}^n$.

Example 3.1. The algebra $\mathcal{I}^4$ has a minimal generating set consisting of

$$
\begin{aligned}
f_1 &= \tfrac{1}{6}(x_1 + x_2 + x_3 + x_4 + x_5 + x_6)\\
f_2 &= \tfrac{1}{6}(x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_5^2 + x_6^2)\\
f_3 &= \tfrac{1}{6}(x_1^3 + x_2^3 + x_3^3 + x_4^3 + x_5^3 + x_6^3)\\
f_4 &= \tfrac{1}{6}(x_1^4 + x_2^4 + x_3^4 + x_4^4 + x_5^4 + x_6^4)\\
f_5 &= \tfrac{1}{6}(x_1^5 + x_2^5 + x_3^5 + x_4^5 + x_5^5 + x_6^5)\\
f_6 &= \tfrac{1}{3}(x_1x_6 + x_2x_5 + x_3x_4)\\
f_7 &= \tfrac{1}{24}(x_1^2x_2 + x_1^2x_3 + x_2^2x_1 + x_2^2x_3 + x_3^2x_1 + x_3^2x_2 + x_1^2x_4 + x_1^2x_5\\
&\quad + x_5^2x_1 + x_4^2x_5 + x_5^2x_1 + x_5^2x_4 + x_2^2x_4 + x_2^2x_6 + x_4^2x_2 + x_4^2x_6\\
&\quad + x_6^2x_2 + x_6^2x_4 + x_3^2x_5 + x_3^2x_6 + x_5^2x_3 + x_5^2x_6 + x_6^2x_3 + x_6^2x_5)\\
f_8 &= \tfrac{1}{24}(x_1^3x_2 + x_1^3x_3 + x_2^3x_1 + x_2^3x_3 + x_3^3x_1 + x_3^3x_2 + x_1^3x_4 + x_1^3x_5\\
&\quad + x_5^3x_1 + x_4^3x_5 + x_5^3x_1 + x_5^3x_4 + x_2^3x_4 + x_2^3x_6 + x_4^3x_2 + x_4^3x_6\\
&\quad + x_6^3x_2 + x_6^3x_4 + x_3^3x_5 + x_3^3x_6 + x_5^3x_3 + x_5^3x_6 + x_6^3x_3 + x_6^3x_5)\\
f_9 &= \tfrac{1}{4}(x_1x_2x_3 + x_1x_4x_5 + x_2x_4x_6 + x_3x_5x_6)
\end{aligned}
$$

The computation of this set takes us around 0.37 seconds to compute on our `Intel(R) Core(TM) i5-6600K CPU @ 3.50GHz` processor. This is quite good and proves the power of King's algorithm, since our implementation is very naïve with little to no optimizations.

However, the big challenge is to compute $\mathcal{I}^5$, which is a significantly more intense computation. In [Thi00], Thiery and Kemper managed to compute this set, using a permutation group specific algorithm and ad hoc methods. Here we recompute it, using King's algorithm.

Example 3.2. The algebra $\mathcal{I}^5$ has a minimal generating set consisting of 56 polynomials of degree at most 9. It's degree vector is $[1, 2, 4, 7, 10, 13, 13, 4, 2]$, where index d is the number of invariants of degree d.

The full list of the invariants, in a `SAGEMATH`-friendly format, can be found on our website at `www.maraha.dk/invariants_of_I5.txt` and also in latex format at `www.maraha.dk/invariants_of_I5_latex.txt`.

The bottleneck of the procedure is the computation of the truncated Gröbner basis, but with the proper strategy (Macaulay2:F4), we still managed to compute the invariants of $\mathcal{I}^5$ in 8 hours and 12 minutes on the same hardware as the previous

example.[9] By decomposing the generators of $S_n^{(2)}$, and using MAGMAs strategy of computing Gröbner bases, King ([Kin13]) managed to compute $\mathcal{I}^n$ in only 37.5 seconds!

3.1.3 When is $\mathcal{I}^n$ Gorenstein?

Recall the necessary and sufficient condition for an algebra to be Gorenstein, seen in Theorem 2.6. We're interested in whether or not $\mathcal{I}^n$ satisfies the conditions, and since we already know how to compute $H(\mathcal{I}^n, z)$, we can also easily compute $H(\mathcal{I}^n, \frac{1}{z})$, and thus construct a while loop which attempts to find an r satisfying Theorem 2.6. Doing this for all $2 \leq n \leq 20$, we find that when n is even it is Gorenstein, with $r = 0$, and when n is odd the loop does not seem to terminate. See Listing 10 for how we executed the test.

Thus, from this experimentation we formulate and prove the following theorem, which is a satisfactory answer to our question.

Theorem 3.2. *If n is even then $\mathcal{I}^n$ satisfies Theorem 2.6 with $r = 0$. If n is odd then $\mathcal{I}^n$ never satisfies Theorem 2.6. Thus, $\mathcal{I}^n$ is Gorenstein if and only if n is even.*

Proof. Let $d = \binom{n}{2}$ be the Krull dimension of $\mathcal{I}^n$, and let $M_{\overline{\lambda}}$ be an arbitrary element of $C_{\overline{\lambda}}$. Then using Theorem 2.6 on Formula 3.1 we find that

$$\begin{aligned}
H(\mathcal{I}^n, \tfrac{1}{z}) &= \frac{1}{n!}\sum_{\lambda} |C_\lambda| \frac{1}{\prod_i (1-\frac{1}{z^i})^{\overline{\lambda}_i}} \\
&= \frac{1}{n!}\sum_{\lambda} |C_\lambda| \frac{1}{\prod_i (\frac{1-z^i}{-z^i})^{\overline{\lambda}_i}} \\
&= \frac{1}{n!}\sum_{\lambda} |C_\lambda| \frac{\prod_i (-z^i)^{\overline{\lambda}_i}}{\prod_i (1-z^i)^{\overline{\lambda}_i}} \\
&= \frac{1}{n!}\sum_{\lambda} |C_\lambda| \frac{(-1)^d (-1)^{\sum_i \overline{\lambda}_i} z^{\sum_i i\overline{\lambda}_i}}{\prod_i (1-z^i)^{\overline{\lambda}_i}} \\
&= (-1)^d z^d \frac{1}{n!}\sum_{\lambda} |C_\lambda| \frac{\operatorname{sign}(M_{\overline{\lambda}})}{\prod_i (1-z^i)^{\overline{\lambda}_i}},
\end{aligned}$$

where we used that $\sum_i i\overline{\lambda}_i = \binom{n}{2} = d$ and $(-1)^{\sum_i \overline{\lambda}_i} = \operatorname{sign}(M_{\overline{\lambda}})$.

Hence, for the equality above to hold, we must have $\operatorname{sign}(M_{\overline{\lambda}}) = 1$, for all λ. Since we may decompose into transpositions, and a transposition, T_λ, of 2 vertices becomes a transposition, $T_{\overline{\lambda}}$, of $n-2$ pairs of edges, we have that $\operatorname{sign}(M_{\overline{\lambda}}) = 1$, if n is even and $\operatorname{sign}(M_{\overline{\lambda}}) = \operatorname{sign}(M_\lambda)$, if n is odd. The result thus follows. □

[9] We also attempted to compute a minimal invariants set of $\mathcal{I}^5$ using SINGULAR's built in implementation of King's algorithm, however it got stuck computing the Gröbner basis at degree 8 and after 100 hours of computing, we killed the process. This shows how important which strategy one uses is.

Remark 3.3. From the proof above, we also saw that $\det(M_{\overline{\lambda}}) = \text{sign}(M_{\overline{\lambda}}) = 1$, which means that $S_n^{(2)}$ is a subgroup of the special linear group, $\text{SL}(V)$.

Remark 3.4. If n is even then $\mathcal{I}^n$ contains no pseudo-reflections. This fact follows immediately from the above, together with [Sta78, theorem 5.5]

The proof above it our own, however all of this (and more) was already known from [Thi00] where Watanabe's theorem was used.

3.2 The restricted invariant ring $\mathcal{I}^n|_s$

While multigraphs are interesting in their own right, the stars of graph theory are of course simple graphs. In this section we investigate the invariant ring of, what we call, *s-graphs*; graphs where we allow a maximum of s edges between two vertices. In particular, for $s = 1$ we obtain simple graphs, and for $s = \infty$ we recover $\mathcal{I}^n$ from the previous section. While everything in this section is already known for $s = 1$ and $s = \infty$, we haven't seen it presented in the generality which we present it here.

Fix n, the number of vertices on our graph. Let $m = \binom{n}{2}$ denote the number of possible edges and set $V = \mathbb{C}^m = \mathbb{G}_n$ a vector space. Using the same set-up as in the beginning of Section 3, we now restrict the functions w_g to only take on values in $\{0, 1, 2, ..., s\}$, such that there is a bijection between such functions and s-graphs.

Denote by $V|_s$ the set of all s-graphs, i.e.

$$V|_s = \{\textstyle\sum_{i=0}^m g_i \mathbf{e_i} \mid g_i \in \{0, 1, 2, ..., s\}\} \subset V, \tag{3.2}$$

which is clearly an affine variety and it's coordinate ring is given by

$$\mathbb{C}[V|_s] \cong \mathbb{C}[x_1, ..., x_m]/I|_s \tag{3.3}$$

where

$$I|_s := I(V|_s) = \Big\langle \prod_{k=0}^{s}(x_1 - k), \prod_{k=0}^{s}(x_2 - k), ..., \prod_{k=0}^{s}(x_m - k) \Big\rangle. \tag{3.4}$$

Notice that we have that, as vector spaces, $\mathbb{C}[V|_s] \cong \mathbb{C}^{(s+1)^m}$, with basis consisting of all monomials, $x_1^{\ell_1} x_2^{\ell_2} \cdots x_m^{\ell_m}$, with $0 \leq \ell_m \leq s$. This is reflected in the fact that there are exactly $(s + 1)^m$ labelled s-graphs on n vertices.

This next theorem is a generalisation of a theorem of [Bed15].

Theorem 3.3. *Let $I|_s$ be as above. Then*

i) $\mathbb{C}[V|_s] \cong \mathbb{C}[x_1, ..., x_m]/I|_s$

ii) $\mathcal{I}^n|_s := \mathbb{C}[V|_s]^{S_n^{(2)}} \cong \mathcal{I}^n/(I|_s \cap \mathcal{I}^n)$

Proof. i) This is just Eq. (3.3).

ii) Let $\pi : \mathbb{C}[V] \to \mathbb{C}[V|_s]$ be the map given by

$$\pi(x_i^{s+1}) = x_i^{s+1} - \prod_{k=0}^{s}(x_i - k) \quad \text{for all } 1 \leq i \leq m,$$

and $\pi(x_i^\ell) = x_i^\ell$ if $\ell \leq s$. This is clearly surjective with kernel equal to $I|_s$.

Hence, it will suffice to show that π is $S_n^{(2)}$-equivariant, since then by Proposition 2.2 the invariants of $\mathbb{C}[V]$ then will be mapped surjectively to the invariants of $\mathbb{C}[V|_s]$ under π, the image of which is clearly $\mathcal{I}^n/(I|_s \cap \mathcal{I}^n)$.

Without loss of generality, we need only consider monomials. Pick any $\sigma \in S_n^{(2)}$ and any monomial $x_1^{\ell_1}x_2^{\ell_2}\cdots x_m^{\ell_m}$. The result is clear for $\ell_i < s+1$, so assume $\ell_i = s+1$.

$$\begin{aligned}
\pi(\sigma(x_1^{s+1}x_2^{s+1}\cdots x_m^{s+1})) &= \pi(x_{\sigma(1)}^{s+1}x_{\sigma(2)}^{s+1}\cdots x_{\sigma(m)}^{s+1}) \\
&= \left(x_{\sigma(1)}^{s+1} - \prod_{k=0}^{s}(x_{\sigma(1)} - k)\right)\cdots\left(x_{\sigma(m)}^{s+1} - \prod_{k=0}^{s}(x_{\sigma(m)} - k)\right) \\
&= \sigma\left(\left(x_1^{s+1} - \prod_{k=0}^{s}(x_1 - k)\right)\cdots\left(x_m^{s+1} - \prod_{k=0}^{s}(x_m - k)\right)\right) \\
&= \sigma(\pi(x_1^{s+1}x_2^{s+1}\cdots x_m^{s+1}))
\end{aligned}$$

□

The proof for (ii) will work for any $I|_s = \langle p(x_1), ..., p(x_k)\rangle$, with $p \in \mathbb{C}[t]$ being any monic polynomial of degree $s+1$. In fact, most (if not all) of the following results appear to work for any such ideal (perhaps with the exception of $m(t) = t^{s+1}$).

3.2.1 Hilbert Series of $\mathcal{I}^n|_s$

While $\mathcal{I}^n|_s$ is no longer graded, it is still a connected *semi-graded*, meaning we have

i) Decomposition into vector spaces, $\mathcal{I}^n|_s = \bigoplus_{d\geq 0}\mathcal{I}_d^n|_s$.

ii) For every $r, d \geq 0$ we have $\mathcal{I}_d^n|_s\mathcal{I}_r^n|_s \subseteq \mathcal{I}_0^n|_s \oplus \cdots \oplus \mathcal{I}_{r+d}^n|_s$.

iii) $\mathcal{I}_0^n|_s = \mathbb{C}$.

So, one may still ask about the nature of the Hilbert series.

Of course since V is no longer a $\mathbb{C}$-vector space we cannot use Molien's formula. Luckily, the next two theorems tell us what the Hilbert series encodes, and how we we can effectively compute that which it encodes. Thus, by combining the two theorems we find a nice concise description of the Hilbert series. For $s = 1$, this description was the main theorem of [Bed15], however our proof is much shorter when given the following lemma and theorem, the first of which is proved (for $s = 1$) in their paper and the second is stated.

Lemma 3.2. *The dimension of the d-graded part,* $\dim(\mathcal{I}^n_d|_s)$*, equals the number of s-graphs on n vertices with exactly d edges.*

Proof. The proof is analogous to that of Theorem 3.1. Indeed, as before, a labelled s-graph, g, which uses exactly d edges, can be encoded as the monomial,

$$\mathbf{x}^g := \prod_{\{i,j\}\subseteq\{1,2,\ldots,n\}} x_1^{w_g(\{i,j\})},$$

with $\sum_{\{i,j\}\subseteq\{1,2,\ldots,n\}} w_g(\{i,j\}) = d$ and $w_g(\{i,j\}) \leq s$.

Clearly, $\mathbb{C}[V|_s]_d$ has basis of all monomials whose exponent sums to d, and so we find a clear one-to-one correspondence between such monomials and s-graphs which use exactly d edges. Since $\mathcal{R}(\mathbf{x}^g)$ is a scaled sum of the elements of the isomorphism class of g, we have, as before, that $\mathcal{R}$ maps a labelled graph to its corresponding unlabelled graph.

Thus, $\mathcal{R}$ maps the basis for $\mathbb{C}[V|_s]_d$, which, as noted, consists of all labelled s-graphs, encoded as monomials, which use exactly d edges, to a basis of $\mathbb{C}[V|_s]_d^{S_n^{(2)}} = \mathcal{I}^n_d|_s$, which, as remarked above, will consist of the set unlabelled s-graphs, which use exactly d edges. □

Although being quite an easy generalization we haven't seen Lemma 3.2 above written and proved in any literature we've come by. Only versions for $s = 1$ or $s = \infty$ have we seen being noted (e.g. in [Bed15]).

Note that the this result implies that $\mathcal{I}^n_d|_s = 0$ for $d > s\binom{n}{2}$, since an s-graph can hold at most $s\binom{n}{2}$ edges.

The second theorem was given in [HP73, p.84]. But, as before, we generalize it from simple graphs to the context of s-graphs.

Theorem 3.4. *The polynomial* $g_n(z)$ *which enumerates the number of s-graphs is given by*

$$g_n(z) = \frac{1}{n!}\sum_{\lambda} |C_\lambda| \prod_i \left(\sum_{k=0}^{s} z^{k\cdot i}\right)^{\overline{\lambda}_i}$$

where we sum over all partitions, λ*, of n, and* $\overline{\lambda}$ *denotes the induced partition over* $S_n^{(2)}$*. I.e. the coefficient of* z^d *counts the number of s-graphs on n vertices which use exactly d edges.*

Proof. Recall the notation and definitions of Section 1.2. We will first show that

$$g_n(z) = Z(S_n^{(2)}, \textstyle\sum_{k=0}^{s} z^k), \tag{3.5}$$

and then show that

$$Z(S_n^{(2)}) = \frac{1}{n!}\sum_{\lambda} |C_\lambda| \prod_i s_{2i+1}^{i\lambda_{2i+1}} \prod_i (s_i s_{2i}^{i-1})^{\lambda_{2i}} \prod_{r<t} s_{\mathrm{lcm}(r,t)}^{\gcd(r,t)\lambda_r\lambda_t}, \tag{3.6}$$

since then the result will follow from Lemma 3.1 using the Notation 3.1.

Let $X = \{1, 2, ..., n\}$ and $X^{(2)} = \{\ \{i, j\} \mid i, j \in X\}$. Define the weight function w on $Y = \{0, 1, 2, ..., s\}$ by setting $w(k) = k$, for all $k \in Y$, so that $c(z) = \sum_{k=0}^{s} z^k$. Remark that any s-graph, g, can be encoded as a function, $f_g : X^{(2)} \to Y$, and that any two isomorphic graphs g and g' will have $w(f_g) = w(f_{g'})$, since they will by definition be in the same orbit of $E^{S_n^{(2)}}$. Remark also that the weight of an orbit of $E^{S_n^{(2)}}$ is simply the number of lines of the graph, corresponding to that orbit. Thus, since C_k counts the number of orbits of weight k, Eq. (3.5) then follows from Pólya's Enumeration Theorem.

It remains to derive Eq. (3.6). Since $S_n^{(2)}$ is induced from S_n it follows by definition of the cycle index that $Z(S_n)$ gives rise to $Z(S_n^{(2)})$ by the exchange $s_1^{\lambda_1} s_2^{\lambda_2} \cdots s_n^{\lambda_n} \to s_1^{\overline{\lambda}_1} s_2^{\overline{\lambda}_2} \cdots s_n^{\overline{\lambda}_n}$ as described in Lemma 3.1. Writing $s_i^{\overline{\lambda}_i}$ in terms of $s_i^{\lambda_i}$ and using Example 1.1 we get Eq. (3.6). □

Corollary 3.1. *We get the following two descriptions of the Hilbert series of $\mathcal{I}^n|_s$:*

$$i)\quad H(\mathcal{I}^n|_s, z) = \frac{1}{n!} \sum_{\lambda} |C_\lambda| \prod_i \left(\sum_{k=0}^{s} z^{k \cdot i} \right)^{\overline{\lambda}_i}$$

$$ii)\quad H(\mathcal{I}^n|_s, z) = \frac{1}{n!} \sum_{M \in S_n^{(2)}} \frac{\det(\mathrm{id}_n - z^{s+1} M)}{\det(\mathrm{id}_n - zM)}$$

Proof. We have

$$\begin{aligned} H(\mathcal{I}^n|_s, z) &= \frac{1}{n!} \sum_{\lambda} |C_\lambda| \prod_i \left(\sum_{k=0}^{s} z^{k \cdot i} \right)^{\overline{\lambda}_i} \\ &= \frac{1}{n!} \sum_{\lambda} |C_\lambda| \prod_i \left(\frac{1 - z^{(s+1) \cdot i}}{1 - z^i} \right)^{\overline{\lambda}_i} \\ &= \frac{1}{n!} \sum_{\lambda} |C_\lambda| \frac{\prod_i (1 - z^{(s+1) \cdot i})^{\overline{\lambda}_i}}{\prod_i (1 - z^i)^{\overline{\lambda}_i}} \\ &= \frac{1}{n!} \sum_{M \in S_n^{(2)}} \frac{\det(\mathrm{id}_n - z^{s+1} M)}{\det(\mathrm{id}_n - zM)} \end{aligned}$$

where the first equality follows from combining Lemma 3.2 and Theorem 3.4 and the last equality follows from Lemma 2.2. □

In particular, for $s = 1$, we get the following formula for the Hilbert series in the case of simple graphs, which was the main theorem of [Bed15]:

$$H(\mathcal{I}^n|_1, z) = \frac{1}{n!} \sum_{M \in S_n^{(2)}} \frac{\det(\mathrm{id}_n - z^2 M)}{\det(\mathrm{id}_n - zM)}.$$

Furthermore, if we take the limit $s \to \infty$ we recover the formula we found for the Hilbert series of $\mathcal{I}^n (= \mathcal{I}^n|_\infty)$, since we have

$$\begin{aligned} H(\mathcal{I}^n|_\infty, z) &= \frac{1}{n!} \sum_\lambda |C_\lambda| \prod_i \left(\sum_{k=0}^{\infty} z^{k \cdot i} \right)^{\overline{\lambda}_i} \\ &= \frac{1}{n!} \sum_\lambda |C_\lambda| \prod_i \left(\frac{1}{1 - z^i} \right)^{\overline{\lambda}_i} \\ &= \frac{1}{n!} \sum_\lambda |C_\lambda| \frac{1}{\prod_i (1 - z^i)^{\overline{\lambda}_i}} = H(\mathcal{I}^n, z), \end{aligned}$$

where we used the closed form of the geometric series in the second equality.

We saw in Remark 2.7 how the cycle index was related to Hilbert Series via $\frac{1}{1-z}$ for any permutation group. This fact seems to generalise:

Remark 3.5. Combining the definitions of the figure counting series, function counting series, Pólya's Enumeration Theorem and the proof of Theorem 3.4 we see that all our argumentation above works for a general permutation group G. Thus we have that

$$H(\mathbb{C}[V|_s]^G, z) = Z(G, \textstyle\sum_{k=0}^{s} z^k),$$

with $V|_s$ defined as in Eq. (3.2).

Furthermore, by definition of $Z(G)$, and because cycle types are constant within conjugacy classes, this also implies that Corollary 3.1 generalises to

$$\begin{aligned} H(\mathbb{C}[V|_s]^G, z) &= \frac{1}{|G|} \sum_{C \in \mathcal{C}} |C| \prod_i \left(\sum_{k=0}^{s} k^{k \cdot i} \right)^{\lambda_i(\sigma_C)} \\ &= \frac{1}{|G|} \sum_{M \in G} \frac{\det(\mathrm{id} - z^{s+1} M)}{\det(\mathrm{id} - zM)}, \end{aligned}$$

for *any* permutation group, G.

This result is as far as we know entirely new. However, we think that we may go even further. Indeed, the second description of the Hilbert series above does not immediately 'depend on' Lemma 2.2, so we have a hunch that this description may be true for any finite group:

Question 3.1. *Is it true that, for any finite group, G, we have*

$$H(\mathbb{C}[V|_s]^G, z) = \frac{1}{|G|} \sum_{M \in G} \frac{\det(\mathrm{id} - z^{s+1} M)}{\det(\mathrm{id} - zM)} \ ?$$

Due to time constraints, and the sheer difficulty in constructing examples, we have not tested this formula for any non-permutation groups.

Example 3.3. Using Remark 3.5 on the usual representation of S_n, one finds that

$$H(\mathbb{C}[V|_s]^{S_n}, q) = \begin{bmatrix} s+n \\ n \end{bmatrix}$$

where $\begin{bmatrix} s+n \\ n \end{bmatrix}$ is the q-binomial coefficients, defined by:

$$\begin{bmatrix} s+n \\ n \end{bmatrix} = \frac{\prod_{k=1}^{s+n}(1-q^k)}{\prod_{k=1}^{n}(1-q^k)\prod_{k=1}^{s}(1-q^k)}.$$

It is well known that the coefficient of q^r of a q-binomial coefficients is the number of partitions of r with n or fewer parts each less than or equal to s.

Example 3.4. Let A_3 be usual representation of the alternating group of degree 3. It is well known that the coefficient of z^n of $H(\mathbb{C}[x,y,z]^{A_3}, z)$ is the number of solutions to $x+y+z=0 \pmod n$ with $0 \le x \le y \le z < n$.[10]

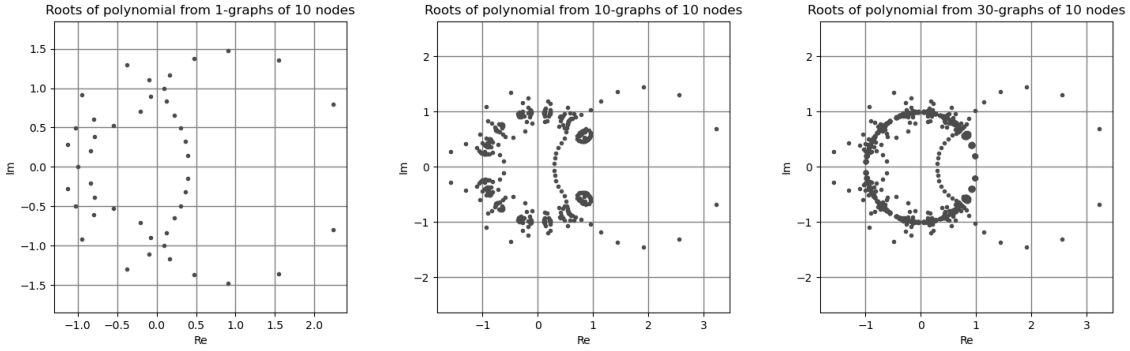
It then appears that the coefficient of z^n of $H(\mathbb{C}[V|_s]^{A_3}, z)$ is the number of solutions to $x+y+z=0 \pmod n$ with $0 \le x \le y \le z < \min\{n, s+1\}$. We have yet to prove this, but we have found that the coefficient of z^n for $n > 3s$ is 0, and is equal to the corresponding coefficient of $H(\mathbb{C}[\mathbb{C}^3]^{A_3}, z)$ when $n \le s$. This aligns with what we would expect.

Loosely speaking, it seems that if $H(\mathbb{C}[V]^G, z)$ enumerates some class of objects, where the component members have some unbounded weight (e.g. the size of each part of partition, or the weight of the edges in a multi-graph), then $H(\mathbb{C}[V|_s]^G, z)$ enumerates the same class of objects, but with the weights now bounded by s.

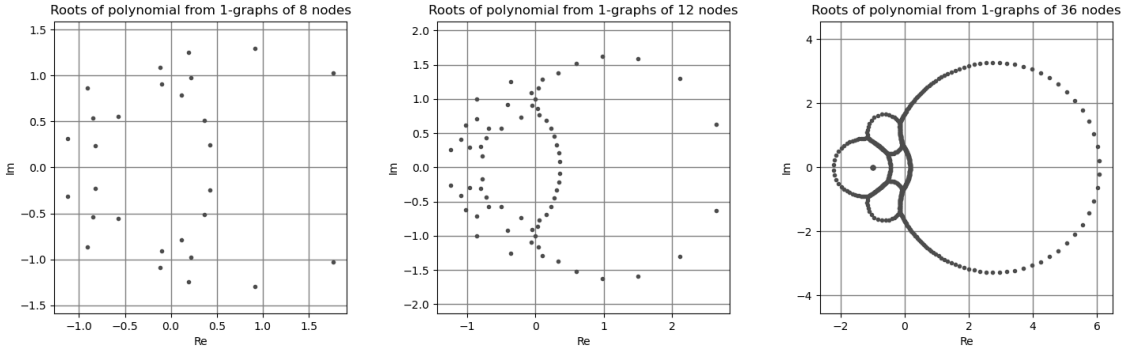
[10] See A007997 in The On-Line Encyclopedia of Integer Sequences (OEIS).

3.2.2 Roots of $H(\mathcal{I}^n|_s, z)$

For a breath of fresh air, we now shoehorn in some curious plots for the visually inclined, even though we haven't deduced much about this oddity. You see, the Hilbert series, $H(\mathcal{I}^n|_s, z)$, are just polynomials with positive integer coefficients, and so we may compute and plot the roots of them. This yielded a quite peculiar pattern, which looks to converge towards some fractal-like pattern as $s \to \infty$. For example if we fix $n = 10$ and vary s we get the following series of images:



If we fix $s = 1$ and vary n, we get another series of images, which also seems to converge to some shape. However, as n increases, the size of the shape grows:



We have put animated versions of these, for differing n and s, on our website.

- For n fixed, see: `www.maraha.dk/fixed_n.html`
- For s fixed, see: `www.maraha.dk/fixed_s.html`

Some remarks are in order about $H(\mathcal{I}^n|_s, z) = a_t z^t + \cdots + a_1 z + a_0$, which partly explain the symmetries.

- Since the coefficients are real, the conjugate of a root is also a root. Hence roots are mirrored over the real axis.
- Since we have $a_i = a_{t-i}$ we have that if z is a root then $\frac{1}{z}$ is also a root. Hence the roots are 'mirrored' over the unit circle.

So we see that it suffice to consider only the roots in the upper unit semi-circle.

3.2.3 Computing invariants of $\mathcal{I}^n|_1$ explicitly

The space of graphs weighted in $\{1, 2, ..., s\}$ inject into $\mathbb{C}$-weighted graphs, and so if we have a generating set of invariants, $f_1, ..., f_k$, of $\mathbb{C}$-weighted graphs, then the image, $\pi(f_i), ..., \pi(f_k)$, of the f_i's clearly generate the invariant algebra of $\mathcal{I}^n|_s$, where $\pi : \mathbb{C}[V] \to \mathbb{C}[V|_s]$ is the quotient map. (This also clear from the proof of Theorem 3.3). Of course, this set of invariants may be much smaller, since it may happen that $\pi(f_i) = \pi(f_j)$. However, we found that the image of a generating set need *not* necessarily be minimal, even if $f_1, ..., f_k$ is minimal, as the following example will show.

For ease of notation we will henceforth denote $\pi(f)$ by $\bar{f}$.

Example 3.5. Recall the minimal generating set of $\mathcal{I}^4$ from Example 3.1. We see that for $s = 1$ we have that $\bar{x_i}^p = \bar{x_i}$, and so $\mathcal{I}^n|_1$ will be generated by the four invariants, $\bar{f_1}, \bar{f_6}, \bar{f_7}, \bar{f_9}$, since $\bar{f_1} = \bar{f_2} = \bar{f_3} = \bar{f_4} = \bar{f_5}$ and $\bar{f_7} = \bar{f_8}$.

However, $\bar{f_6}$ is superfluous since we can write it as a combination of the others,

$$\bar{f_6} = 6\bar{f_1}^2 - \bar{f_1} - 4\bar{f_7}.$$

Note that, this relation was found through sheer trial and error.

We believe the set $\{\bar{f_1}, \bar{f_7}, \bar{f_9}\}$ to be minimal.

Example 3.6. We may do the same as in Example 3.5, but for $\mathcal{I}^5$. If we map the minimal generating set, which we found in Example 3.2, through π (with $s = 1$ as before), we get the following generating set for $\mathcal{I}^5|_1$.

$$\begin{aligned}
\bar{f}_1 &= \tfrac{1}{10}(x_0 + x_1 + x_2 + x_3 + x_4 + x_5 + x_6 + x_7 + x_8 + x_9)\\
\bar{f}_2 &= \tfrac{1}{30}(x_0x_1 + x_0x_2 + x_1x_2 + x_0x_3 + x_1x_3 + x_2x_3 + x_0x_4 + x_1x_4 + x_0x_5 + x_2x_5 + x_4x_5 +\\
&\quad x_0x_6 + x_3x_6 + x_4x_6 + x_5x_6 + x_1x_7 + x_2x_7 + x_4x_7 + x_5x_7 + x_1x_8 + x_3x_8 + x_4x_8 +\\
&\quad x_6x_8 + x_7x_8 + x_2x_9 + x_3x_9 + x_5x_9 + x_6x_9 + x_7x_9 + x_8x_9)\\
\bar{f}_3 &= \tfrac{1}{60}(x_0x_2x_4 + x_1x_2x_4 + x_0x_3x_4 + x_1x_3x_4 + x_0x_1x_5 + x_1x_2x_5 + x_0x_3x_5 + x_2x_3x_5 + x_1x_4x_5 +\\
&\quad x_2x_4x_5 + x_0x_1x_6 + x_0x_2x_6 + x_1x_3x_6 + x_2x_3x_6 + x_1x_4x_6 + x_3x_4x_6 + x_2x_5x_6 + x_3x_5x_6 +\\
&\quad x_0x_1x_7 + x_0x_2x_7 + x_1x_3x_7 + x_2x_3x_7 + x_0x_4x_7 + x_2x_4x_7 + x_0x_5x_7 + x_1x_5x_7 + x_4x_6x_7 +\\
&\quad x_5x_6x_7 + x_0x_1x_8 + x_1x_2x_8 + x_0x_3x_8 + x_2x_3x_8 + x_0x_4x_8 + x_3x_4x_8 + x_4x_5x_8 + x_0x_6x_8 +\\
&\quad x_1x_6x_8 + x_5x_6x_8 + x_2x_7x_8 + x_3x_7x_8 + x_5x_7x_8 + x_6x_7x_8 + x_0x_2x_9 + x_1x_2x_9 + x_0x_3x_9 +\\
&\quad x_1x_3x_9 + x_0x_5x_9 + x_3x_5x_9 + x_4x_5x_9 + x_0x_6x_9 + x_2x_6x_9 + x_4x_6x_9 + x_1x_7x_9 + x_3x_7x_9 +\\
&\quad x_4x_7x_9 + x_6x_7x_9 + x_1x_8x_9 + x_2x_8x_9 + x_4x_8x_9 + x_5x_8x_9)\\
\bar{f}_4 &= \tfrac{1}{10}(x_0x_1x_4 + x_0x_2x_5 + x_0x_3x_6 + x_1x_2x_7 + x_4x_5x_7 +\\
&\quad x_1x_3x_8 + x_4x_6x_8 + x_2x_3x_9 + x_5x_6x_9 + x_7x_8x_9)\\
\bar{f}_5 &= \tfrac{1}{20}(x_0x_1x_2 + x_0x_1x_3 + x_0x_2x_3 + x_1x_2x_3 + x_0x_4x_5 + x_0x_4x_6 + x_0x_5x_6 + x_4x_5x_6 +\\
&\quad x_1x_4x_7 + x_2x_5x_7 + x_1x_4x_8 + x_3x_6x_8 + x_1x_7x_8 + x_4x_7x_8 + x_2x_5x_9 + x_3x_6x_9 +\\
&\quad x_2x_7x_9 + x_5x_7x_9 + x_3x_8x_9 + x_6x_8x_9)\\
\bar{f}_6 &= \tfrac{1}{60}(x_0x_1x_2x_4 + x_0x_1x_3x_4 + x_0x_1x_2x_5 + x_0x_2x_3x_5 + x_0x_1x_4x_5 + x_0x_2x_4x_5 + x_0x_1x_3x_6 +\\
&\quad x_0x_2x_3x_6 + x_0x_1x_4x_6 + x_0x_3x_4x_6 + x_0x_2x_5x_6 + x_0x_3x_5x_6 + x_0x_1x_2x_7 + x_1x_2x_3x_7 +\\
&\quad x_0x_1x_4x_7 + x_1x_2x_4x_7 + x_0x_2x_5x_7 + x_1x_2x_5x_7 + x_0x_4x_5x_7 + x_1x_4x_5x_7 + x_2x_4x_5x_7 +\\
&\quad x_4x_5x_6x_7 + x_0x_1x_3x_8 + x_1x_2x_3x_8 + x_0x_1x_4x_8 + x_1x_3x_4x_8 + x_0x_3x_6x_8 + x_1x_3x_6x_8 +\\
&\quad x_0x_4x_6x_8 + x_1x_4x_6x_8 + x_3x_4x_6x_8 + x_4x_5x_6x_8 + x_1x_2x_7x_8 + x_1x_3x_7x_8 + x_4x_5x_7x_8 +\\
&\quad x_4x_6x_7x_8 + x_0x_2x_3x_9 + x_1x_2x_3x_9 + x_0x_2x_5x_9 + x_2x_3x_5x_9 + x_0x_3x_6x_9 + x_2x_3x_6x_9 +\\
&\quad x_0x_5x_6x_9 + x_2x_5x_6x_9 + x_3x_5x_6x_9 + x_4x_5x_6x_9 + x_1x_2x_7x_9 + x_2x_3x_7x_9 + x_4x_5x_7x_9 +\\
&\quad x_5x_6x_7x_9 + x_1x_3x_8x_9 + x_2x_3x_8x_9 + x_4x_6x_8x_9 + x_5x_6x_8x_9 + x_1x_7x_8x_9 + x_2x_7x_8x_9 +\\
&\quad x_3x_7x_8x_9 + x_4x_7x_8x_9 + x_5x_7x_8x_9 + x_6x_7x_8x_9).
\end{aligned}$$

As before, this is not minimal! Indeed, $\bar{f}_3$ is superfluous, since we have the relation, which, as before, we found through sheer trial and error,

$$\bar{f}_3 = \frac{1}{18}(-50\bar{f}_1{}^3 + 15\bar{f}_1{}^2 + 90\bar{f}_1\bar{f}_2 - \bar{f}_1 - 18\bar{f}_2 - 6\bar{f}_4 - 12\bar{f}_5).$$

We believe that $\{\bar{f}_1, \bar{f}_2, \bar{f}_4, \bar{f}_5, \bar{f}_6\}$ is a minimal generating set for $\mathcal{I}^5|_1$, however, we have not proved this, nor does it seem trivial to prove.

Since $\mathcal{I}^n|_1$ only uses square-free monomials, we thought that King's algorithm may be specialized to produce invariants of this family of invariant algebras. Through some naive experimentation of altering King's algorithm, we found the following algorithm. This algorithm executes all the same procedures, but does so in the quotient ring. The only exception is the construction of M, where we need to lift to the polynomial ring to check division. Let us first introduce some notation.

For $f \in \mathbb{C}[V]$ we denote by $\bar{f}$ the image of the quotient map $\pi : \mathbb{C}[V] \to \mathbb{C}[V]/I|_1$. We denote by $\text{lift}(\bar{f})$ the natural lift from $\mathbb{C}[V]/I|_1$ to $\mathbb{C}[V]$. Note that, f is equal to $\text{lift}(\bar{f})$ if and only if every term of f is square-free in the x_i's. Finally, we denote by $\overline{M}_d$ the *square-free* monomials of degree d in $\mathbb{C}[V]$.

Algorithm 4: King's algorithm for simple graphs

input : Permutation group, $S_n^{(2)}$, and upper bound, D, on $\beta(\mathcal{I}^n|_1)$
output: A minimal generating set, S, of $\mathcal{I}^n|_1$

$S \leftarrow \emptyset$
$\mathcal{G} \leftarrow \emptyset$
for d **from** 1 **to** D **do**
  $\mathcal{G} \leftarrow d$-truncated Gröbner basis of $\langle S \rangle$ (over $\mathbb{C}[\mathbb{G}_n]/I|_s$)
  $M \leftarrow \{m \in \overline{M}_d \mid \nexists g \in \mathcal{G}$ such that $\text{LM}(\text{lift}(g))$ divides $m\}$
  if $M = \emptyset$ **then break**;
  for $t \in M$ **do**
    $f \leftarrow \mathcal{R}(t)$
    if $\bar{g} \leftarrow \text{NF}_{\mathcal{G}}(\bar{f}) \neq 0$ **then** `// Normal form taken over` $\mathbb{C}[V]/I|_1$
      Add $\bar{f}$ to S
      Add $\bar{g}$ to $\mathcal{G}$
return S

Conjecture 3.1. *Algorithm 4 is correct.*

We have no idea how to prove this, given the authors limited knowledge on the area of Gröbner bases in quotient rings. However, we have implemented this algorithm (Listing 12), and it yields the same generating sets for $n = 4$ and $n = 5$ as the generating sets we found in Example 3.5 and Example 3.6. Of course, we are not entirely confident, that the sets of those examples actually are minimal.

We have absolutely no idea why this works or if this is simply just a fluke. But we find it miraculous that it yields the same two results, that we found by hand. Assuming Conjecture 3.1 is true, we can now compute the invariants of $\mathcal{I}^6|_1$. A computation never done before! The full list of the invariants computed can be found on our website at `www.maraha.dk/Invariants_I6s1.txt`.[11] We also computed $\mathcal{I}^7|_1$ up to and including degree 5; see `www.maraha.dk/Invariants_I7s1.txt`.

Perhaps Algorithm 4 can be generalized to $s > 1$. However testing this would require the exhaustive recomputations of Example 3.5 and Example 3.6 for $s > 1$.

Furthermore, since we made no changes to King's algorithm, which were specific to $S_n^{(2)}$, to arrive at Algorithm 4, we believe that, if Conjecture 3.1 is true, then the following conjecture is true, as well.

Conjecture 3.2. *Algorithm 4 works for any finite group G.*

[11] The degree vector of this set is $[1, 1, 3, 3, 3, 11]$.

We tested this extended conjecture, by using the algorithm on the symmetric group, S_n, for $1 \leq n \leq 9$. For all such n, it returns only the polynomial, $\frac{1}{n}(x_1 + x_2 + \cdots + x_n)$, which is correct, since the set, $\{\frac{1}{n}(x_1 + \cdots + x_n), ..., \frac{1}{n}(x_1^n + \cdots + x_n^n)\}$, is a minimal generating set, and the image of this set under the quotient map is clearly just $\frac{1}{n}(x_1 + x_2 + \cdots + x_n)$.

3.3 Number of minimal generators

Let $\mathcal{I}^n_{<d}$ be the subalgebra of $\mathcal{I}^n$ generated by all invariants of degree $< d$, and set $s_0(\mathcal{I}^n) := 0$ and $s_d(\mathcal{I}^n) = \dim \mathcal{I}^n_d - \dim(\mathcal{I}^n_{<d})_d$. Then the series,

$$s(\mathcal{I}^n, z) := \sum_{d=0}^{\infty} s_d(\mathcal{I}^n) z^d,$$

has degree $\beta(\mathcal{I}^n)$, and the coefficients, $s_d(\mathcal{I}^n)$, count the number of invariants of degree d in a minimal generating set. Algorithmically these two pieces of information would have great implications, since they would serve as a stopping point and an indicator for when to jump to the next iteration.

Because the d'th entry in the inverse Euler transformation of a sequence, $\{a_k\}_k$, only depends on $a_1, ..., a_d$, and due to Theorem 1.3, we came up with the following conjecture.

Conjecture 3.3. *Let $\{a^n_d\}_d$ be the sequence of coefficients of $H(\mathcal{I}^n, z)$ and $\{b^n_d\}_d$ be its inverse Euler transformation. Then*

$$s_d(\mathcal{I}^n) = b^n_d$$

for all $d \leq n + 2$.

We test the conjecture on $\mathcal{I}^n$, for $3 \leq n \leq 7$, and verify that the conjecture holds in this range. The values of s_d for $n = 6$ and $n = 7$ are borrowed from [Thi00].

$d =$	1	2	3	4	5	6	7	8	9	10	11	12
$s_d(\mathcal{I}^3)$	1	1	1	0	0	0	0	0	0	0	0	0
$\{b^3_d\}_d$	1	1	1	0	0	0	0	0	0	0	0	0
$s_d(\mathcal{I}^4)$	1	2	3	2	1	0	0	0	0	0	0	0
$\{b^4_d\}_d$	1	2	3	2	1	0	-1	-2	-1	-1	1	1
$s_d(\mathcal{I}^5)$	1	2	4	7	10	13	13	4	2	0	0	0
$\{b^5_d\}_d$	1	2	4	7	10	13	13	2	-22	-76	-147	-221
$s_d(\mathcal{I}^6)$	1	2	5	10	21	41	74	121	162	??	??	??
$\{b^6_d\}_d$	1	2	5	10	21	41	74	121	162	90	-317	-1601
$s_d(\mathcal{I}^7)$	1	2	5	11	28	72	172	414	??	??	??	??
$\{b^7_d\}_d$	1	2	5	11	28	72	172	414	946	1950	3496	4570

Table 1: Comparing $s_d(\mathcal{I}^n)$ with the inverse Euler transformation of $H(\mathcal{I}^n, z)$

Furthermore, we found that it also seemingly works for $\mathcal{I}^n|_1$ as well. However, in this case the bound in d is a bit smaller.

Conjecture 3.4. *Let $\{a_d^n\}_d$ be the sequence of the coefficients of $H(\mathcal{I}^n|_1, z)$ and $\{b_d^n\}_d$ be its inverse Euler transformation. Then*

$$s_d(\mathcal{I}^n|_1) = b_d^n$$

for all $d \leq n-1$.

As before, we compute for $3 \leq n \leq 7$, and verify that the conjecture agrees with the values found in Section 3.2.3, assuming the Conjecture 3.1 is true.

$d =$	1	2	3	4	5	6	7	8	9	10	11	12
$s_d(\mathcal{I}^3\|_1)$	1	0	0	0	0	0	0	0	0	0	0	0
$\{b_d^3\}_d$	1	0	0	0	0	0	0	0	0	0	0	0
$s_d(\mathcal{I}^4\|_1)$	1	1	1	0	0	0	0	0	0	0	0	0
$\{b_d^4\}_d$	1	1	1	-2	-2	0	0	0	0	0	0	0
$s_d(\mathcal{I}^5\|_1)$	1	1	2	1	0	0	0	0	0	0	0	0
$\{b_d^5\}_d$	1	1	2	1	-2	-5	-4	1	11	0	0	0
$s_d(\mathcal{I}^6\|_1)$	1	1	3	3	3	11	0	0	0	0	0	0
$\{b_d^6\}_d$	1	1	3	3	3	-4	-12	-21	-13	18	72	106
$s_d(\mathcal{I}^7\|_1)$	1	1	3	4	8	??	??	??	??	??	??	??
$\{b_d^7\}_d$	1	1	3	4	8	9	1	-22	-59	-114	-122	-7

Table 2: Comparing $s_d(\mathcal{I}^n|_1)$ with the inverse Euler transformation of $H(\mathcal{I}^n|_1, z)$

Of course, the values of s_d are merely conjectures themselves, but since the two conjectures agree on the values, it seems to add to our confidence that both Conjecture 3.3 and Conjecture 3.1 are true.

4 Reconstructability

Given a (simple or multi-edged) graph, g, on n vertices, we may consider the graph, $g_{\setminus v}$, on $n-1$ vertices, which is induced by removing vertex, $v \in V$, and all incident edges. We call $g_{\setminus v}$ the v-vertex-deleted subgraph of g. The multiset[12], $\mathrm{deck}(g)$, of all isomorphism classes of all vertex-deleted subgraphs, is called the *deck* of g. If two graphs have the same deck they are said to be *hypomorphic*.

A famous long standing conjecture, due to Kelly and Ulam, is *Ulam's conjecture* (also known as the *graph reconstruction conjecture*).

Conjecture 4.1 (Ulam's conjecture)**.** *Let g and g' be simple graphs on $n \geq 3$ vertices. Then g and g' are isomorphic if and only if they are hypomorphic.*

Of course, the 'only if' part is trivial, however the 'if' part has yet to be proven.

We say that g is *reconstructable* if whenever it is hypomorphic to another graph, g', then g and g' are isomorphic.

Of course, everything above can be generalized to graphs with values in some given set, E. We are interested in the case where $E = \mathbb{N}$ (i.e. multigraphs), in which case Pouzet's conjecture emerges as a closely related conjecture to Ulam's conjecture. We will see that Pouzet's conjecture is stated in purely algebraic terms, and if true would imply both Ulam's conjecture and Ulam's conjecture for multigraphs! In this section we will follow the work of Thiery ([Thi00]) which, sadly, disproves Pouzet's conjecture. The disproof follows from considering a special series and using Condition 1.1.

4.1 Reconstructability of multigraphs

For the rest of Section 4, when we write graph we mean multigraph, unless stated otherwise. However, many of the following results hold for graphs with weights in any set. (See [Thi00]).

Recall that we can evaluate polynomials $f \in \mathbb{C}[\mathbb{G}_n]$ on $\mathbb{C}$-weighted graphs.

Definition 4.1. A polynomial is called *reconstructable* if its value is constant on hypomorphism classes. I.e. if g and g' are hypomorphic then $f(g) = f(g')$.

Recall $\mathcal{I}^n$ from Section 3, and recall how two graphs g and g' are isomorphic if and only if they evaluate to the same on all invariants in $\mathcal{I}^n$ (or just some generating set of $\mathcal{I}^n$). It turns out problem of graph reconstructability and polynomial reconstructability, of those of $\mathcal{I}^n$, is the same problem.

Proposition 4.1. *All $\mathbb{N}$-weighted graphs on n vertices are reconstructable if and only if all invariants $f \in \mathcal{I}^n$ are reconstructable.*

[12] Recall multisets are just sets which allow repetitions.

Proof. Assume that all graphs are reconstructable. Then two hypomorphic graphs, g and g', are isomorphic and so $f(g) = f(g')$ for all $f \in \mathcal{I}^n$. Thus all $f \in \mathcal{I}^n$ are reconstructable.

Assume that all $f \in \mathcal{I}^n$ are reconstructable. Let g and g' be hypomorphic. By assumption, $f(g) = f(g')$ for all $f \in \mathcal{I}^n$. But since $\mathcal{I}^n$ separates isomorphism classes, it follows that g and g' are isomorphic. □

Recall the exponential of a graph (Eq. (3.1)) and its properties.

Proposition 4.2. *Let g be a graph on n vertices with at least one isolated vertex. Then $\mathbf{x}^{g^{\circledast}}$ is reconstructable.*

Proof. For ease of notation, we set $f := \mathbf{x}^{g^{\circledast}}$ and denote the isolated vertex by v.

Let h be some multigraph, then we may write

$$f(h) = \sum_{g' \in S_n^{(2)} \cdot g} \mathbf{x}^{g'}(h) = \frac{1}{|\mathrm{Aut}(g)|} \sum_{\sigma \in S_n^{(2)}} \mathbf{x}^{\sigma g}(h) = \frac{1}{|\mathrm{Aut}(g)|} \sum_{j \in V} \sum_{\sigma, \sigma(v)=j} \mathbf{x}^{\sigma g}(h),$$

and we let $f_j(h) := \sum_{\sigma,\sigma(v)=j} \mathbf{x}^{\sigma g}(h)$. Because v is isolated, and because we sum over σ such that $\sigma(v) = j$, we see that f_j will contains no variables of the form $x_{\{k,j\}}$, and so $f_j(h) = f_j(h_{\setminus j})$. We now let h and h' be two hypomorphic graphs with n vertices. Since they're hypomorphic, there exists some $\sigma \in S_n^{(2)}$ such that $h_{\setminus j} \cong h'_{\setminus \sigma j}$. Since f is an invariant, we have that $f(h') = f(\sigma h')$, and so we may reduce to the case where $\sigma = \mathrm{id}$, so that $h_{\setminus j} \cong h'_{\setminus j}$.

By construction, f_j is invariant under permutations which fix j, and so we get

$$f_j(h) = f_j(h_{\setminus j}) = f_j(h'_{\setminus j}) = f_j(h'),$$

from which we see that

$$f(h) = \frac{1}{\mathrm{Aut}(g)} \sum_{j \in V} f_j(h) = \frac{1}{\mathrm{Aut}(g)} \sum_{j \in V} f_j(h') = f(h'),$$

meaning f is reconstructable. □

This gives rise to the the main definition of this section.

Definition 4.2. We call a polynomial, $f \in \mathcal{I}^n$, *algebraically reconstructable* if can be expressed as a product or sum of polynomials of the form $\mathbf{x}^{g^{\circledast}}$, with g being a graph on n vertices with at least one isolated vertex.

Furthermore, a graph g is called *algebraically reconstructable* if $\mathbf{x}^{g^{\circledast}}$ is algebraically reconstructable as a polynomial.

We will later see that algebraically reconstructable is a *strictly* stronger property than normal reconstructability. In fact, the first step of showing this follows immediately from Proposition 4.2:

Corollary 4.1. *An algebraically reconstructable polynomial is reconstructable.*

Proof. Since sums and products of reconstructable polynomials are clearly reconstructable, the fact follows immediately from Definition 4.2 and Proposition 4.2. □

The polynomials of $\mathcal{I}^n$ separates isomorphism classes of graphs. This next theorem shows that the algebra of algebraically reconstructable polynomials, $\mathfrak{R}^n$, separates hypomorphism classes.

Theorem 4.1. *Two graphs are hypomorphic if and only if they evaluate to the same value on all algebraically reconstructable polynomials.*

Proof. Assume g and g' are hypomorphic. By definition, they evaluate to the same value on all reconstructable polynomials, and so by Corollary 4.1 also on all algebraically reconstructable polynomials.

Let us show the converse. Let $\{f_0, ..., f_k\} \subseteq \mathcal{I}^{n-1}$ be a finite generating set for $\mathcal{I}^{n-1}$. We introduce an extra variable, λ, and set $F = f_0 + \lambda f_1 + \cdots + \lambda^k f_k \in \mathbb{C}[\mathbb{G}_{n-1}, \lambda]$. Clearly, g and g' are isomorphic if and only if $F(g) = F(g') \in \mathbb{C}[\lambda]$.

Fix some vertex $v \in \{1, ..., n\}$. With an appropriate relabelling of the vertices, we may lift $F \in \mathbb{C}[\mathbb{G}_{n-1}, \lambda]$ to a polynomial $F_v \in \mathbb{C}[\mathbb{G}_n, \lambda]$ such that $F_v(g) = F(g_{\backslash v})$ for any graph, g.

Notice, for $\ell \in \mathbb{N}$, we may write $F_v^\ell = c_{v,0} + c_{v,1}\lambda + \cdots + c_{v,d}\lambda^d$ with $c_{v,i}$ a polynomial in the variables $x_{\{i,j\}}$ with no variables of the form $x_{\{v,i\}}$ appearing, since otherwise $F_v(g) \neq F(g_{\backslash v})$. We now define

$$s_\ell := \sum_{v=1}^{n} F_v^\ell = \left(\sum_{v=1}^{n} c_{v,0}\right) + \left(\sum_{v=1}^{n} c_{v,1}\right)\lambda + \cdots + \left(\sum_{v=1}^{n} c_{v,d}\right)\lambda^d$$

where each coefficient, $\sum_{v=1}^{n} c_{v,i}$, is an algebraically reconstructable invariant, since the summands, $c_{v,i}$, do not contain variables of the form $x_{\{v,i\}}$. (v is still isolated).

Let g and g' be two graphs which evaluate to the same value on all algebraically reconstructable polynomials. By construction $s_\ell(g') = s_\ell(g) \in \mathbb{C}[\lambda]$, which spelled out means that

$$\sum_{v=1}^{n} F_v(g)^\ell = s_\ell(g) = s_\ell(g') = \sum_{v=1}^{n} F_v(g')^\ell.$$

It then follows from the basic properties of symmetric functions, that there exists $\sigma \in S_n^{(2)}$ such that $F(g_{\backslash v}) = F_v(g) = F_{\sigma v}(g') = F(g'_{\backslash \sigma v})$ for all v. But we saw that this means that $g_{\backslash v} \cong g'_{\backslash \sigma v}$ for all v. Hence they must have the same deck and so are hypomorphic. □

This led Pouzet to formalizing the following conjecture.

Conjecture 4.2 (Pouzet's conjecture)**.** *Every invariant $f \in \mathcal{I}^n$ is algebraically reconstructable. In other words, the algebra, $\mathfrak{R}^n$, generated by all algebraically reconstructable invariants equals $\mathcal{I}^n$.*

By Theorem 4.1, and since $\mathcal{I}^n$ separate isomorphism classes of graphs, we find that if Pouzet's conjecture were true, it would imply that the multigraph version of Ulam's conjecture was true, and in particular that Ulam's conjecture was true. However, if false it would not imply anything, since Corollary 4.1 is not an 'if and only if'.

Before we move on the the disproof of Pouzet's conjecture, we show the following proposition, which is not necessary for the disproof, but which allows us to show, using algebra, that certain classes of graphs are reconstructable.

Proposition 4.3. *Let g be a multigraph such that $\mathbf{x}^{g^{\circledast}}$ is reconstructable. Then g is reconstructable.*

We will only prove this fact for simple graphs. The proof for the multigraph version is principally the same, but a lot more technical. See [Thi00] for this proof.

Proof. Let g be a simple graph, and let g' be a graph hypomorphic to g. Clearly, g' must also be simple and must have the same number of edges. Thus we may evoke Proposition 3.1 to get that $\mathbf{x}^{g^{\circledast}}(g')$ counts the number of subgraphs of g' isomorphic to g. Since $\mathbf{x}^{g^{\circledast}}$ is reconstructable, we get that $s(g, g') = \mathbf{x}^{g^{\circledast}}(g') = \mathbf{x}^{g^{\circledast}}(g) = s(g, g) > 0$. Hence, g' must have some subgraph which is isomorphic to g, but, since both g and g' have the same number of edges, this subgraph must be g' itself. □

To summarize we have the following for a multigraph, g,

$$g \text{ algebraically reconstructable} \Rightarrow \mathbf{x}^{g^{\circledast}} \text{ reconstructable} \Rightarrow g \text{ reconstructable.} \quad (4.1)$$

We will later see that there exists an example of a non-algebraically reconstructable simple graph which is reconstructable. Thus, the converse of at least one of the above implication is not true.

4.1.1 Disproof of Pouzet's conjecture

We now give a non-constructive disproof of Pouzet's conjecture, using theoretical and computational means.

Definition 4.3. A graph which has at most one non-trivial connected component is called a *quasi-connected* graph.

Lemma 4.1. *The subalgebra of algebraically reconstructable invariants on n vertices, $\mathfrak{R}^n \subseteq \mathcal{I}^n$, is generated by quasi-connected multigraphs whose non-trivial connected component uses $< n$ vertices. We denote this set by $C^{<n}$.*

Proof. By definition $\mathfrak{R}^n$ is generated by all invariants, $\mathbf{x}^{g^{\circledast}}$, where g has an isolated vertex. So if we let g have an isolated vertex, then we wish to show that $\mathbf{x}^{g^{\circledast}}$ is a

product or sum of elements of $C^{<n}$. Clearly, if g has only one non-trivial connected component then $g \in C^{<n}$, and so we're done. Thus without loss of generality we may assume g has an isolated vertex and exactly two non-trivial connected components, since if it has more than two, we may apply the this result recursively. Let g_1, g_2 denote the two connected components on $n_1, n_2 > 0$ vertices such that $n_1 + n_2 = n - 1$.

Consider g_1, g_2 on n vertices, by adding isolated points. Then $g_1, g_2 \in C^{<n}$. Taking the product, $\mathbf{x}^{g_1\circledast}\mathbf{x}^{g_2\circledast}$, will yield a sum of the exponentials of the super-positions of g_1 and g_2. The summands will fall into one of two cases. In the first case, the summand has two disjoint connected components and one isolated vertex and must therefore be isomorphic to g. In the second case, the summand has one connected component and two, or more, isolated vertices, and is thus quasi-connected. Isolating the summands which are isomorphic to g therefore gives us that $\mathbf{x}^{g\circledast} = \mathbf{x}^{g_1\circledast}\mathbf{x}^{g_2\circledast} - \sum_h \mathbf{x}^{h\circledast}$, where h is a super-position of g_1 and g_2, and is quasi-connected. □

Remark 4.1. By an analogous argument, as that of the proof above, one can also show that every non-connected graph is algebraically reconstructable, and thus also reconstructable.

Lemma 4.2. *Let $C_d^{<n}$ denote the number of quasi-connected multigraphs with d edges, and whose connected component uses $< n$ vertices. Let $\{f_d^n\}_d$ be the Euler transformation of $\{C_d^{<n}\}_d$. Then:*

i) *The dimension of $\mathfrak{R}_d^n$ is bounded by f_d^n.*

ii) *The number of algebraically reconstructable multigraphs with n vertices and d edges is bounded by f_d^n.*

iii) *If f_d^n is strictly less than the total number of multigraphs on n vertices and d edges, denoted by m_d^n, then there are at least $m_d^n - f_d^n$ non-algebraically reconstructable multigraphs on n vertices and d edges.*

Proof. By Lemma 4.1, the set $\mathcal{C}^{<n} := \{\mathbf{x}^{g\circledast} \mid g \in C^{<n}\}$ is a homogenous generating set for $\mathfrak{R}^n$. Thus, it follows from Condition 1.1 that we have that $H(\mathfrak{R}^n, z)$ is dominated by

$$\prod_{g\in\mathcal{C}^{<n}} \frac{1}{1 - z^{\deg(g)}} = \prod_{d=1}^{\infty} \frac{1}{(1-z^d)^{C_d^{<n}}} = \sum_{d=0}^{\infty} f_d^n z^d, \tag{4.2}$$

from which (i) follows.

Clearly, (ii) and (iii) follow immediately. □

Remark 4.2. It turns out that f_d^n counts the number of multigraphs with d edges, no isolated vertices, and whose connected components uses $< n$ vertices.

By this Lemma 4.2 we see that to disprove Pouzet's conjecture, we need only compute f_d^n and m_d^n and compare their sizes. To do this, we first need a graph theoretic result.

Proposition 4.4. *Let*

$$m(x,y) = \sum_{n\geq 1, d\geq 0} m_d^n x^n y^d \quad \textit{and} \quad c(x,y) = \sum_{n\geq 1, d\geq 0} c_d^n x^n y^d$$

be the two two-variable power series, enumerating the number of multigraphs on n vertices with d edges, and the number of connected multigraphs on n vertices with d edges, respectfully.

Then $m(x,y)$ and $c(x,y)$ are related by

$$1 + m(x,y) = \exp\left(\sum_{k=1}^{\infty} \frac{c(x^k, y^k)}{k}\right).$$

Proof. By the multivariable Pólya enumeration theorem, we have that $Z(S_m, c(x,y))$ is the generating function for the number of graphs with exactly m connected components. Thus, the sum over all m must yield the generating function for the total number of graphs. That is, we have that

$$1 + m(x,y) = \sum_{m=1}^{\infty} Z(S_m, c(x,y)),$$

and result follows from Proposition 1.1. □

Theorem 4.2. *There is a multigraph on 11 vertices, using 18 edges, which is not algebraically reconstructable. Thus, Pouzet's conjecture is false.*

Proof. By Lemma 4.2 we need only compute f_{18}^{11} and m_{18}^{11} and check that $f_{18}^{11} < m_{18}^{11}$.

Let $m(x,y)$ and $c(x,y)$ be as in Proposition 4.4. We first wish to use Proposition 4.4 and Procedure 1.2 to compute c_d^n from m_d^n, which are known, from Theorem 3.1 to be the coefficients of $H(\mathcal{I}^n, z)$. This we know how to compute from Section 3.1.1.

Fix n. It is then clear that the homogeneous component of degree d of $C^{<n}$, is given by $C_d^{<n} = \sum_{k<n} c_d^k$. And so we may compute the sequence, $\{C_d^{<n}\}_d$, and take its Euler transformation to get the sequence, $\{f_d^n\}_d$.

We implement all of this in `SAGEMATH`, and the code can be found in Appendix A, Listing 13. Setting $n = 11$, we find that $m_{18}^{11} - f_{18}^{11} = 47\,473\,612$, meaning that there are at least 47 473 612, out of a total of 1 457 002 920 graphs on 11 vertices with 18 edges, for which Pouzet's conjecture fails. □

While we can't be sure there isn't some counter example to Pouzet's conjecture for less than 11 vertices, the above theorem shows at least 3.25% of all graphs, on 11 vertices and 18 edges, are not algebraically reconstructable.

We expand on this result by checking for $n > 11$. Thiery managed to compute up to $n = 18$, but as computers have gotten faster, we can check for even higher n:

Corollary 4.2. *Pouzet's conjecture fails for* $n \in \{11, 12, ..., 35\}$.

Proof. Using the exact same set-up, we compute f_d^n and m_d^n for various n and $0 \leq d \leq 150$. We find that, for all $n \in \{11, 12, ..., 35\}$, there is some $0 \leq d \leq 150$ for which $f_d^n < m_d^n$. □

For these larger n, we there can be certain d's, for which this ratio shoots up, past 90%. In fact, it looks as if it converges towards 100%, for some d and $n \to \infty$. Because of this, and because of the previous corollary, we're very confident in the following conjecture.

Conjecture 4.3. *Pouzet's conjecture fails for all* $n \geq 11$.

4.2 Reconstructability of s-graphs

Notice that every definition and result of Section 4.1 will work for s-graphs and the algebras $\mathcal{I}^n|_s$, with analogous proof. This disproof was also done by Thiery in [Thi00], but only for $s = 1$.

Moreover, we have the following lemma, which partly connects the two algebras.

Lemma 4.3. *An s-graph, which is algebraically reconstructable in $\mathcal{I}^n$, is also algebraically reconstructable in $\mathcal{I}^n|_s$.*

Proof. Let $\mathbf{x}^{s\circledast} \in \mathcal{I}^n|_s$ be the exponential of some s-graph. By assumption, there is some polynomial, p, such that $\mathbf{x}^{s\circledast} = p(\mathbf{x}^{g_1\circledast}, ..., \mathbf{x}^{g_k\circledast})$, where g_i are s-graphs with at least one isolated vertex. Then we have

$$\pi(\mathbf{x}^{s\circledast}) = \pi(p(\mathbf{x}^{g_1\circledast}, ..., \mathbf{x}^{g_k\circledast})) = p(\pi(\mathbf{x}^{g_1\circledast}), ..., \pi(\mathbf{x}^{g_k\circledast})),$$

where $\pi : \mathcal{I}^n \to \mathcal{I}^n|_s$ is the quotient map. □

We now recreate the disproof of the previous section in the algebras $\mathcal{I}^n|_s$. In the new context, Lemma 4.1 and Lemma 4.2 reads as follows.

Lemma 4.4. *The subalgebra of algebraically reconstructable s-graphs, $\mathfrak{R}^n|_s \subseteq \mathcal{I}^n|_s$, is generated by quasi-connected s-graphs, whose non-trivial connected component uses $< n$ vertices. We denote this set by $C^{<n}|_s$*

Lemma 4.5. *Let $\{f_d^n|_s\}_d$ be the Euler transformation of $\{C_d^{<n}|_s\}_d$. Then*

i) *The dimension of $\mathfrak{R}_d^n|_s$ is bounded by $f_d^n|_s$.*

ii) *The number of algebraically reconstructable s-graphs with n vertices and d edges is bounded by $f_d^n|_s$.*

iii) *If $f_d^n|_s$ is strictly less than the total number of s-graphs on n vertices and d edges, denoted by $m_d^n|_s$, then there are at least $m_d^n|_s - f_d^n|_s$ non-algebraically reconstructable s-graphs on n vertices and d edges.*

A bit surprisingly, the first counter-example to Pouzet's conjecture changes for differing s, as the proof of the following shows.

Theorem 4.3. *For all $s \in \mathbb{N}$ there exists some s-graph which is not algebraically reconstructable.*

Proof. The proof and code is completely analogous to that of Theorem 4.2, we need only change so that we count the number of s-graphs. However, $H(\mathcal{I}^n|_s, z)$ counts exactly that, and we know how to compute this series from Corollary 3.1.

In regards to the code, we can reuse that of Theorem 4.2 by simply exchanging the function `H(n)` with `Hres(n,s)`. See Listing 14 for the implementation.

Computing this we get that for $s = 1$, the conjecture first fails when $n = 13$ and $d = 17$. For $2 \leq s \leq 5$, the conjecture first fails when $n = 11$ and $d = 17$. And for $6 \leq s \leq 17$ the conjecture first fails when $n = 11$ and $d = 18$.

Finally, for $s, s' \geq 18$ we have $H(\mathcal{I}^{11}|_s, z)_{18} = H(\mathcal{I}^{11}|_{s'}, z)_{18}$ for all $1 \leq d \leq 18$. This is because when $s \geq d$ we have $H(\mathcal{I}^n|_s, z)_d = H(\mathcal{I}^n, z)_d$, so allowing more edges won't change the total number of s-graphs. Since $f^{11}_{18}|_s$ only depends on the values $m^{11}_1|_s, ..., m^{11}_{18}|_s$, we find that $m^{11}_{18}|_s - f^{11}_{18}|_s > 0$ for all $s \geq 18$. □

In particular, we see that there is some simple graph on 13 vertices and 17 edges which is not algebraically reconstructable. However, in [McK22] McKay positively verified the reconstructability conjecture for all graph with at most 13 vertices. Thus, we see that there must exist some simple graph on 13 vertices and 17 edges, which *is not* algebraically reconstructable but *is* reconstructable. This justifies the earlier claim that algebraically reconstructability is a *strictly* stronger property than that of regular reconstructability.

Remark also that the contra positive of Lemma 4.3 implies that this graph is also non-algebraically reconstructable in $\mathcal{I}^n$. Thus, unsurprisingly, the number $m^n_d - f^n_d$ is only a lower bound of the number of non-algebraically reconstructable graphs.

5 Final Remarks and Moving Forward

We have observed how the algorithmic nature of the theory of invariants of finite groups plays well into the combinatorial nature of graphs. We found that the combination of these aspects forms quite an interesting tool for studying graphs, and even paved the way for some contributions back to invariant theory. Indeed, the we saw a few generalizations from their graph-theoretic counterpart, to that of any finite (permutation) group; namely those of Remark 3.5 and Conjecture 3.2, which appear promising if the latter conjecture proves to be true.

However, we also found that many of the computations were intractable, even for small n. In particular, the explicit computation of invariants still has a long way to go, before it can be of much use. Unfortunately, this fact means that we are not exceedingly confident in many of the conjectures made throughout the thesis, as they are based on a very small data set.

Even so, we believe that the application of invariant theory to graphs, holds a lot of potential, and there are still many remaining questions left unanswered.

5.1 Further investigations

Besides the conjectures mentioned throughout the thesis, there are a few more general aspects we deem interesting to investigate, going forward.

Most of the theory and computations of Section 3 and Section 4, can be rewritten for other types of graph with little change. For instance, one could investigate digraphs or hypergraphs by, instead of considering two-sets, $\{i, j\}$, one could, for digraphs use tuples, (i, j), or, for hyper graphs use k-sets, $\{i_1, ..., i_k\}$). The main change would be that of Lemma 3.1.

Furthermore, the representation, $S_n^{(2)}$, can be split into three irreducible components ([Thi00]), and so one can consider the multigraded Hilbert series. This would be particularly interesting, together with the results of Section 1.3 and Remark 1.1.

The nature of the roots of the polynomials, $H(\mathcal{I}^n|_s, z)$, are also a mystery to us, and would be quite interesting to look into, if not just quite aesthetically pleasing. Perhaps analytical tools could be of help?

Finally, it would be interesting to comb through the invariant theory of finite graphs, to see which results (if any) can be generalized to the context of semi-graded rings. This would be very useful in the investigation of the algebras, $\mathcal{I}^n|_s$.

A Source Code

Here we list the code of the implementations, mentioned throughout the thesis. This includes, procedures and algorithms, as well as how these were utilized to disprove Pouzet's conjecture.

We have implemented everything in SAGEMATH, and all of it should be able to be run on a fresh installation, given that the prior functions are defined. Please note that the notation used in the implementations, is not necessarily consistent with the rest of the thesis. Furthermore, we have made no effort in creating a proper documentation (the thesis itself should suffice, for such a project of this scale), and we have made no effort in error handling. Thus, the user may need some knowledge of the theory, before the code can be safely utilized.

Note: In the implementations we work over the field $\mathbb{Q}$. All the theory has been written for $\mathbb{C}$, however since we never actually use that the field is algebraically closed, the theory will work for any field of characteristic 0. In fact, more often than not, it suffice that $\text{char}(K)$ does not divide $|G|$.

Code from section 1

```
def euler_trans(seq):
    # INPUT: seq <- Sequence of integers
    # OUTPUT: A <- The Euler transformation of seq
    C = []
    A = []
    for i in range(1, len(seq)+1):
        s = sum(d*seq[d-1] for d in divisors(i))
        C.append(s)
        s += sum(C[j-1]*A[i-j-1] for j in range(1, i))
        A.append(s/i)
    return A
```

Listing 1: Computing the Euler transformation of sequence, seq.

```
def euler_inv_trans(seq):
    # INPUT: seq <- Sequence of integers
    # OUTPUT: A <- The inverse Euler transformation of seq
    C = []
    A = []
    for i in range(1, len(seq) + 1):
        s = sum(C[j-1]*seq[i-j-1] for j in range(1, i))
        C.append(i*seq[i-1] - s)
        s = sum([moebius(i // d) * C[d - 1] for d in divisors(i)])
        A.append(s/i)
    return A
```

Listing 2: Computing the inverse Euler transformation of sequence, seq.

```
def euler_inv_trans_two_var(mat):
    # INPUT: mat <-- List of sequences of integers
    # OUTPUT: A <-- The two variable inverse euler transformation
    R.<y> = ZZ[]
    # Transform each row into a polynomials in y.
    # We only care about the coefficients up to the given precision
       , why the +O(y^len(mat))
    g = [ add([mat[p][q]*y^(q)+O(y^(len(mat[-1]))) for q in range(
       len(mat[p]))]) for p in range(len(mat)) ]
    b = []
    # Construct intermediary sequence
    for p in range(1, len(g)+1):
        pg = p*g[p-1]
        ps = add([ k*b[k-1]*g[p-k-1] for k in range(1,p) ])
        b.append( (pg-ps)/p )

    # Fill in 0 untill dimensions match
    c = [SR(bi).list() for bi in b]
    for i in range(len(c)):
        while len(c[i]) < len(c[-1]):
            c[i].append(0)
        c[i].pop(0)

    A = []
    for p in range(1, len(c)+1):
        S = []
        for q in range(1, len(c[p-1])+1):
            s = sum([c[(p//r)-1][(q//r)-1]*moebius(r)/r for r in
               divisors(gcd(p,q))])
            S.append(s)
        A.append(S)

    return A
```

Listing 3: **Computing the inverse Euler transformation in two variables of sequence of sequences, `mat`. (The input is more akin to a matrix).**

Code from section 2

```
def RO(G,f):
    # INPUT: G <-- permutation group, f <- polynomial
    # OUTPUT: fr <-- the reynolds operator applied to f
    R = PolynomialRing(QQ, 'x', G.degree())
    fr = 0
    for g in G:
        fr += f(*g(R.gens()))
    return fr/G.cardinality()
```

Listing 4: Evaluation of the Reynolds operator `G` on a polynomial, `f`.

```
def kings_algorithm(G, beta):
    # INPUT: G <-- finite group, beta <-- degree bound of
       invariants (e.g. |G|)
    # OUTPUT: S <-- minimal generating set of R^G
    from sage.rings.polynomial.toy_buchberger import spol
    N = G.degree()
    R = PolynomialRing(QQ,'x',N)
    S, GB = [],[]
    for d in range(1,beta+1):
        print('Computing invariant of degree',d,'...')
        Sd = []
        GB = list(R.ideal(S).groebner_basis(deg_bound=d))
        #GB = GB + [h for f in GB for g in GB if (h := spol(f, g)).
           degree() == d]
        M = []
        for t in WeightedIntegerVectors(d, N*[1]):
            t = R({tuple(t):1})
            if not any((g.lm()).divides(t) for g in GB):
                M.append(t)
        if M == []: break
        for t in M:
            f = RO(G,t)
            g = f.reduce(GB)
            if g != 0:
                Sd.append(f)
                GB.append(g)
        S = S + Sd
        print('Found', len(Sd), 'invariants of degree', d)
        for g in Sd: print(g);print()
        print()
    return S
```

Listing 5: Our implementation of King's algorithm. Note that line 11 could be exchanged by line 12. Be warned! Changing the order of the polynomial ring, `R`, can yield non-minimal sets. (This is likely because the `reduce` method is imported from `SINGULAR` and so does not inherit the order of `R`).

Code from section 3

We found that SAGEMATH implemented partitions in an odd way, so the following helper function translates from SAGEMATH notation to a notation that is more consistent with that of [HP73].

```
def to_HP_notation(p,n):
    # INPUT: p <-- partition of n in Sage-notation
    # OUTPUT: l <-- p in HP notation (l[k] is exponent of s_k+1)
    l = n*[0]
    for k in range(n):
        l[k] = list(p).count(k+1)
    return l
```

Listing 6: **Helper function to translate partition notations.**

```
def to_twoset_cycletype(p,n):
    # INPUT: n <-- integer, p <-- partition of n in HP-notation
    # OUTPUT: l <-- induced partition over S^(2)_n
    if n < 3: l = n*[0]
    else: l = binomial(n,2)*[0]#((n**2 + n)//2)*[0]
    # First contributing factor
    for k in range(n):
        if p[k] == 0: continue
        if k % 2 == 0:
            # This is the odd case
            l[k] += p[k]*(k//2)
        else:
            # This is the even case
            l[(k-1)//2] += p[k]
            l[k] += p[k]*((k-1)//2)

    # Second contributing factor
    for r in range(n):
        if p[r] == 0: continue
        for t in range(r+1):
            if p[t] == 0 or (r == t and p[t] <= 1): continue
            if r == t:
                l[t] += (t+1)*(binomial(p[t],2))
            else:
                l[lcm(r+1,t+1)-1] += gcd(r+1,t+1)*p[r]*p[t]

    return l
```

Listing 7: **Computes the induced partition of $\binom{n}{2}$ over $S_n^{(2)}$. This algorithm is based on Lemma 3.1.**

```
def get_S2n_gens(n):
    # INPUT: n <-- integer > 2
    # OUTPUT: g1,g2 <-- generators of S^(2)_n
    gen1 = [(2+i,n+i) for i in range(n-2)]
    if n%2 == 0:
        gen2 = []
        for i in range(1,(n-2)//2 + 1):
            k = [i + sum(n-r-1 for r in range(l)) for l in range(n-
                i)] + [n-i + sum(n-r-1 for r in range(l)) for l in
                range(i)]
            gen2.append(tuple(k))
        k = [n//2 + sum(n-r-1 for r in range(l)) for l in range(n
            //2)]
        gen2.append(tuple(k))
    else:
        gen2 = []
        for i in range(1,(n-1)//2 + 1):
            k = [i + sum(n-r-1 for r in range(l)) for l in range(n-
                i)] + [n-i + sum(n-r-1 for r in range(l)) for l in
                range(i)]
            gen2.append(tuple(k))
    return (gen1, gen2)
```

Listing 8: Computing two generators, g1,g2, which generate $S_n^{(2)}$. This is the implementation of Algorithm 3.

```
def H(n):
    # INPUT: n <-- positive integer
    # OUTPUT: Q <-- generating function for H(I^n, z)
    P.<z> = ZZ[]
    Q = 0
    for l in Partitions(n):
        T = l.conjugacy_class_size()
        l = to_HP_notation(l,n)
        p = to_twoset_cycletype(l,n)
        for k in range(1, len(p)+1):
            if p[k-1] == 0: continue
            T *= 1/( (1-z^k)^p[k-1] )
        Q += T/factorial(n)
    return Q
```

Listing 9: Computes the generating function for the Hilbert series of $\mathcal{I}^n$, using Formula 3.1 and Lemma 3.1.

```
R.<z> = ZZ[]
limit = 100
for n in range(2,20):
    N = binomial(n,2)
    sign = 1 if N % 2 == 0 else -1
    F = H(n)
    Finv = F(1/z)
    r = 0
    while r <= limit:
        F = sign*z^(N+r)*F
        if F == Finv:
            print(n, r)
            break
        r += 1
    else:
        print(n, "Failed to verify Gorensteiness")
```

Listing 10: Test for $0 \leq r \leq 100$ and $0 \leq n \leq 20$ if $\mathcal{I}^n$ is Gorenstein. If we find r such that $\mathcal{I}^n$ satisfies Theorem 2.6, it will print n and r, and if no $r < 100$ satisfies Theorem 2.6, it will print n and that it failed to verify Gorensteiness.

```
def Hres(n,s):
    # INPUT: n <-- postive integer, s <-- postive integer
    # OUTPUT: Q <-- generating function for H(I^n|_s, z)
    P.<z> = ZZ[]
    Q = 0
    for l in Partitions(n):
        T = l.conjugacy_class_size()
        l = to_HP_notation(l,n)
        p = to_twoset_cycletype(l,n)
        for k in range(1, len(p)+1):
            if p[k-1] == 0: continue
            T *= add([z^(k*i) for i in range(s+1)])^p[k-1]
        Q += T/factorial(n)
    return Q
```

Listing 11: Computes the generating function for the Hilbert series of $\mathcal{I}^n|_s$ using Corollary 3.1 (i).

```
def get_squarefree_monomials(N):
    # INPUT: N <-- Positive integer
    # OUTPUT: L <-- List of all square-free monomials of degree at
       most N
    import itertools
    L = list(itertools.product([0,1],repeat=N))
    return list(L)

def kings_algorithm_simple_graphs(G, beta):
    # INPUT: G <-- S^(2)_n, beta <-- degree bound of invariants
    # OUTPUT: S <-- Conjectured minimal generating set of I^n|_1
    N = G.degree()
    R = PolynomialRing(QQ, 'x', N)
    I = R.ideal([R.gens()[i]^2 - R.gens()[i] for i in range(N)])
    Q = R.quotient(I)
    L = get_squarefree_monomials(N)
    S = []
    GB = []
    for d in range(1,beta+1):
        Sd = []
        GB = list(Q.ideal(S).groebner_basis(deg_bound=d))
        Vd = [v for v in L if sum(v) == d]
        M = []
        for t in Vd:
            t = R({tuple(t):1})
            if not any((g.lift().lm()).divides(t) for g in GB):
                M.append(t)
        if M == []: break
        for t in M:
            f = Q(RO(R,G,t))
            g = f.reduce(GB)
            if g != 0:
                Sd.append(f)
                GB.append(g)
        S = S + Sd
    return [s for s in S]
```

Listing 12: Implementation of Algorithm 4. This is not a proven algorithm, but appears to yield good results for $S_4^{(2)}$ and $S_5^{(2)}$.

Code from section 4

```
prec = 150
R.<z> = PowerSeriesRing(ZZ, prec)
N = 3
while True:
    mat = []
    for n in range(1,N+1):
        HIn = H(n)
        mat.append(R(HIn).list())
    c = EulerInvTransTwoVar(mat)
    CN =[sum([c[k][d] for k in range(N-1)]) for d in range(prec-1)]
    FN = EulerTrans(CN)
    diff = [(mat[N-1][i+1] - FN[i]) for i in range(len(FN))]
    marker = [1 if i > 0 else 0 for i in diff]
    if 1 in marker:
        print('FAIL:', 'n =', N, ', d =', marker.index(1)+1)
    N += 1
```

Listing 13: Procedure to find the first $d \leq 150$ for which Pouzet's conjecture fails for a given n, if Pouzet's fails within the range.

```
s = 1
while True:
    N = 3
    while N < 25:
        mat = []
        for n in range(1,N+1):
            HIn = Hres(n, s)
            mat.append(HIn.list())
        c = EulerInvTransTwoVar(mat)
        CN = [sum([c[k][d] for k in range(N-1)]) for d in range(len
            (c[0]))]
        FN = EulerTrans(CN)
        diff = [(mat[N-1][i+1] - FN[i]) for i in range(len(FN))]
        marker = [1 if i > 0 else 0 for i in diff]
        if 1 in marker:
            print('FAIL:', 's =', s, ', n =', N, ', d =', marker.
                index(1)+1)
            break
        N += 1
    s += 1
```

Listing 14: For all $s \in \mathbb{N}$, the procedure will find the first n and d for which pouzet's conjecture fails, if it fails within the range. Note that, since `Hres` outputs a polynomial, we need not covert to a powerseries, and thus need no precision parameter.

References

[Bed15] Leonid Bedratyuk. "A new formula for the generating function of the numbers of simple graphs". In: *Comptes Rendus de L'Academie Bulgare des Sciences* 69 (Dec. 2015).

[Bor15] Nicolas Borie. "Effective Invariant Theory of Permutation Groups Using Representation Theory". In: *Lecture Notes in Computer Science*. Springer International Publishing, 2015, 58–69. ISBN: 9783319230214. DOI: 10.1007/978-3-319-23021-4_6. URL: http://dx.doi.org/10.1007/978-3-319-23021-4_6.

[Cam89] Peter J. Cameron. "Some sequences of integers". In: *Discrete Mathematics* 75.1 (1989), pp. 89–102. ISSN: 0012-365X. DOI: https://doi.org/10.1016/0012-365X(89)90081-2. URL: https://www.sciencedirect.com/science/article/pii/0012365X89900812.

[DK15] H. Derksen and G. Kemper. *Computational Invariant Theory*. Encyclopaedia of Mathematical Sciences. Springer Berlin Heidelberg, 2015. ISBN: 9783662484227. URL: https://books.google.dk/books?id=U1NECwAAQBAJ.

[Gö95] Manfred Göbel. "Computing Bases for Rings of Permutation-invariant Polynomials". In: *Journal of Symbolic Computation* 19.4 (1995), pp. 285–291. ISSN: 0747-7171. DOI: https://doi.org/10.1006/jsco.1995.1017. URL: https://www.sciencedirect.com/science/article/pii/S0747717185710176.

[Hap91] Dieter Happel. "On Gorenstein Algebras". In: *Representation Theory of Finite Groups and Finite-Dimensional Algebras: Proceedings of the Conference at the University of Bielefeld from May 15–17, 1991, and 7 Survey Articles on Topics of Representation Theory*. Ed. by G. O. Michler and C. M. Ringel. Basel: Birkhäuser Basel, 1991, pp. 389–404. ISBN: 978-3-0348-8658-1. DOI: 10.1007/978-3-0348-8658-1_16. URL: https://doi.org/10.1007/978-3-0348-8658-1_16.

[HP73] F. Harary and E.M. Palmer. *Graphical Enumeration*. Academic Press, 1973. ISBN: 9780123242457. URL: https://books.google.dk/books?id=yqr98zXOalcC.

[Ker91] A. Kerber. *Algebraic Combinatorics Via Finite Group Actions*. B.I. Wissenschaftsverlag, 1991. ISBN: 9783411145218. URL: https://books.google.dk/books?id=Fe7uAAAAMAAJ.

[Kin13] Simon A. King. "Minimal generating sets of non-modular invariant rings of finite groups". In: *Journal of Symbolic Computation* 48 (Jan. 2013), 101–109. ISSN: 0747-7171. DOI: 10.1016/j.jsc.2012.05.002. URL: http://dx.doi.org/10.1016/j.jsc.2012.05.002.

[McK22] Brendan D. McKay. *Reconstruction of small graphs and digraphs*. 2022. arXiv: 2102.01942 [math.CO].

[PS08] P. Paule and B. Sturmfels. *Algorithms in Invariant Theory*. Texts & Monographs in Symbolic Computation. Springer Vienna, 2008. ISBN: 9783211774175. URL: https://books.google.dk/books?id=3lF0cyOHwgQC.

[Sta78] Richard P Stanley. "Hilbert functions of graded algebras". In: *Advances in Mathematics* 28.1 (1978), pp. 57–83. ISSN: 0001-8708. DOI: https://doi.org/10.1016/0001-8708(78)90045-2. URL: https://www.sciencedirect.com/science/article/pii/0001870878900452.

[Sta79] Richard P. Stanley. "Invariants of finite groups and their applications to combinatorics". In: *Bulletin of the American Mathematical Society* 1 (1979), pp. 475–511. URL: https://api.semanticscholar.org/CorpusID:10334677.

[Thi00] Nicolas M. Thiéry. "Algebraic Invariants of Graphs; a Study Based on Computer Exploration". In: *SIGSAM Bull.* 34.3 (2000), 9–20. ISSN: 0163-5824. DOI: 10.1145/377604.377612. URL: https://doi.org/10.1145/377604.377612.