Research Statement

Christopher O’Neill

My research lies in the intersection of commutative algebra, discrete optimization, and semigroup theory, using methods from algebraic and enumerative combinatorics. The primary objects of study are combinatorial invariants arising in discrete geometry, with connections to computation, algorithms, and the development and use of software in mathematical research.

Research overview. Affine semigroups (finitely generated, additive subsemigroups of \( \mathbb{Z}^d_{\geq 0} \)) have played an increasingly important role in semigroup theory in recent years, due in large part to their effective use in algebraic and geometric settings involving combinatorics, in addition to semigroup theory itself. Indeed, many landmark results in semigroup theory center around exhibiting extremal behavior, and the setting of affine semigroups is broad enough to encompass a large variety of such behavior [ACHP07, CK15, OPe17a]. At the same time, affine semigroups benefit from algorithms and implementations for explicit computation, which have been instrumental in their study [DGM17, Gar15]. As such, affine semigroups provide a wealth of explicit examples, and obtaining a more thorough understanding of their structure has implications on the general setting.

Non-negative integer solutions to linear equations, which are central to discrete optimization and have a multitude of applications across nearly every discipline [EFRS06, Lee08, LLS08], are intimately tied to affine semigroups. One of the central themes in semigroup theory are expressions of semigroup elements as sums of generators, called factorizations, and for an affine semigroup \( S = \langle \alpha_1, \ldots, \alpha_k \rangle \subset \mathbb{Z}^d_{\geq 0} \), the factorizations of a given element \( \alpha \in S \) coincide with non-negative integer solutions to a system of linear equations. More specifically, the set of factorizations of \( \alpha \), given by

\[
Z_S(\alpha) = \{(x_1, \ldots, x_k) \in \mathbb{Z}^k_{\geq 0} : \alpha = x_1 \alpha_1 + \cdots + x_k \alpha_k \},
\]

is precisely the set of non-negative integer solutions to the equation \( Ax = \alpha \), where the matrix \( A \in \mathbb{Z}^{d \times k} \) has columns \( \alpha_1, \ldots, \alpha_k \). This correspondence goes both ways; in any setting involving non-negative integer solutions to a linear system \( Ax = \alpha \), an affine semigroup structure is present, and this viewpoint has proven fruitful on countless occasions.

Additionally, affine semigroups arise in commutative algebra in the presence of gradings, which assign to each monomial \( x^a \) in the polynomial ring \( R = \mathbb{k}[x_1, \ldots, x_k] \) with coefficient field \( \mathbb{k} \) an element of the semigroup \( S \) as its graded degree [MS05, Sta96]. The simplest example is the “standard grading” where \( S = \mathbb{Z}_{\geq 0} \) and the graded degree of each monomial is its total degree. Under minimal assumptions, the algebraic structure of \( R \) is then determined (up to finite dimensional linear transformations) by the additive semigroup structure of \( S \), and many quantities of interest in commutative algebra and algebraic geometry can be expressed in terms of \( S \), resulting in combinatorial formulas [Hoc77] and algorithms for explicit computation [BS98, HM05]. Additionally, relations between affine semigroup generators correspond to toric ideal generators, the simultaneous solutions of which arise in countless applications [DS98].

The special case of numerical semigroups (additive subsemigroups of \( \mathbb{Z}_{\geq 0} \)) also plays a unique role in additive combinatorics. Numerical semigroups are central to the Frobenius coin-exchange problem, which ask for the largest non-negative integer value that cannot be evenly changed using a collection of relatively prime coin values \( n_1, \ldots, n_k \) [All05, BR07]. In this context, each coin value represents an irreducible element of the numerical semigroup \( S = \langle n_1, \ldots, n_k \rangle \subset \mathbb{Z}_{\geq 0} \), and factorizations of an element \( m \in S \) correspond to distinct ways of making change for \( m \).
Combinatorially flavored invariants, which assign a value to each semigroup element based on its factorizations, play a major role in the study of affine semigroups in each of the aforementioned areas, as they provide a concrete measure of the quantity and distribution of factorizations within a given semigroup. For example, one could choose the optimal value of some quantity (e.g. a linear functional) defined on the level of factorizations. This task arises frequently in linear programming when searching for an optimal non-negative integer solution of a linear system [PS82]. Invariants from combinatorial commutative algebra are often closely connected to affine semigroup structure as well. For instance, minimal relations between semigroup generators can be used to characterize the Betti numbers of certain graded polynomial modules [BPS98].

My general research goals are to

1. examine the asymptotic behavior of combinatorial structures arising in affine semigroups,
2. develop and implement more efficient algorithms for computing with affine semigroups in popular open-source software packages [DGM17], and
3. characterize expected invariant behavior for randomly sampled semigroups.

In Section 1, fundamental tools from combinatorial commutative algebra are introduced, several specific invariants of interest in discrete optimization are defined, and projects concerning their asymptotic behavior are stated. Section 2 contains several projects involving parametrized families of semigroups, including recently studied “shifted” numerical semigroups, and software implementations are discussed. Finally, Section 3 begins with a discussion of “random semigroups” and a novel approach to a longstanding conjecture in the numerical semigroups literature is introduced.

Undergraduate research. Suitably chosen research problems in non-unique factorization theory are ideal for undergraduate projects, as they offer a high probability of producing publishable output by undergraduates while remaining accessible to students wishing to experience mathematical research. While significant contributions to open problems in commutative algebra often require extensive background in the subject, factorization theory can place algebraic objects in combinatorial settings, making them more concrete to work with explicitly. In fact, several of the motivating results presented below are products of undergraduate research projects I have coadvised, either in the REU setting [BOP14a, BOP14b, CCMMP14, CGP14, HKMOP14, KOP15, OPTW15, CGHORWW17] or independently [BOP14a, BOP14b, HO17a, GOW17], as well as software packages [HO17b, KOS17, DGM17].

Many of the problems presented below are excellent starting places for undergraduate research projects. As an example, initial investigations for Projects 1 and 2 will involve utilizing mathematics software packages to examine invariant values, providing a natural starting place for students to acquire familiarity and build intuition. Additionally, improvements on the computation in Table 1 are ideal for a computer science student interested in computational mathematics, and Project 3 will also benefit from computation in their early stages.

1. Invariants and discrete optimization

Throughout this section, several invariants appearing in both the factorization theory literature and the discrete geometry literature are introduced. Several of my results characterizing their eventual behavior over affine semigroups are formally stated, and subsequent work is proposed.

1.1. Quasipolynomials and Hilbert’s theorem. The length of a factorization \( f \) of a semigroup element \( m \in S \) is the number of generators in \( f \); \( L(m) \) denotes the set of factorization lengths of \( m \) (its length set). Many invariants of interest in semigroup theory are derived from factorization lengths, the simplest and most natural of which are maximum and minimum factorization length, which assign to each semigroup element the values \( M(m) = \max L(m) \) and \( m(m) = \min L(m) \), respectively. Maximum and minimum factorization length also arise in integer programming problems, where factorizations in a given affine semigroup coincide with integer solutions to a set of
linear equations [CGLR06, DeL05, DDK13]. In this setting, a semigroup element’s factorizations that achieve the maximum (resp. minimum) factorization length are precisely those solutions with maximal (resp. minimal) $\ell_1$-norm.

Recent joint work with Barron and Pelayo has uncovered explicit characterizations in the special case of numerical semigroups for the eventual behavior of maximum and minimum factorization length invariants [BOP14a]. In particular, the maximum factorization length invariant over any numerical semigroup $S = \langle n_1, \ldots, n_k \rangle$ satisfies

$$M(m) = \frac{1}{n_1} m + a_0(m)$$

for all $m > n_1 n_k$, where $a_0$ is some $n_1$-periodic function depending on $S$. The above function is an example of a \textit{quasipolynomial}, that is, a polynomial with periodic coefficients.

This characterization relies on the fact that numerical semigroups (i) possess only finitely many irreducible elements and (ii) can be totally ordered. Recently, I have successfully generalized this result from numerical semigroups to affine semigroups, using techniques from combinatorial commutative algebra [One15]. As affine semigroups need not possess a total ordering, these extensions are stated using an appropriate multivariate quasipolynomial analog.

**Definition 1.1.** A function $f : \mathbb{Z}_{\geq 0}^d \to \mathbb{R}$ is \textit{eventually quasipolynomial} if (i) $f$ restricts to a polynomial on each of finitely many cones (that is, sets of the form

$$C(\beta; \alpha_1, \ldots, \alpha_r) = \beta + \alpha_1 \mathbb{Z}_{\geq 0} + \cdots + \alpha_r \mathbb{Z}_{\geq 0}$$

for $\beta$ and linearly independent $\alpha_1, \ldots, \alpha_r \in \mathbb{Z}_{\geq 0}$, and (ii) the union of these cones equals $\mathbb{Z}_{\geq 0}^d$.

Hilbert’s theorem, a cornerstone of commutative algebra, states that the Hilbert function of any finitely generated, positively multigraded module is eventually quasipolynomial [Sta96, Fie00]. Hilbert’s theorem is often applied to problems in enumerative combinatorics by constructing a graded module whose Hilbert function coincides with a counting function of interest [Ehr62, Mac71, DLM00]. For example, constructions of this type yield an alternative proof that the number of proper $k$-colorings of a finite undirected graph $G$ is a polynomial in $k$ whose degree is the number of vertices of $G$ [Sta12].

My recent work characterizes the eventual behavior of maximum and minimum factorization length for any affine semigroup by applying Hilbert’s theorem in precisely this manner [One15]. More specifically, given an affine semigroup $S \subset \mathbb{Z}_{\geq 0}^d$, a family of multigraded modules is constructed whose Hilbert functions determine the maximum factorization length of each element of $S$. Applying Hilbert’s theorem to the modules in this family yields a description of the factorization invariant in terms of multivariate eventually quasipolynomial functions. When $S$ is a numerical semigroup (that is, when $d = 1$), this specializes to a known result for each invariant.

**Theorem 1.2** ([One15]). The max and min factorization length functions $M, m : S \to \mathbb{Z}_{\geq 0}$ are eventually quasilinear for any affine semigroup $S \subset \mathbb{Z}_{\geq 0}^d$. Moreover, if $S = \langle n_1, \ldots, n_k \rangle \subset \mathbb{Z}_{\geq 0}$ is a numerical semigroup, then

$$M(m) = \frac{1}{n_1} m + a_0(m) \quad \text{and} \quad m(m) = \frac{1}{n_k} m + b_0(m)$$

for $m \geq n_k - 1 n_k$, where $a_0$ and $b_0$ are $n_1$-periodic and $n_k$-periodic functions, respectively.

Theorem 1.2 states that the function $M : S \to \mathbb{Z}_{\geq 0}$ over any affine semigroup $S$ coincides with an eventual quasipolynomial in which the degree of each polynomial restriction is at most 1. If $S = \langle n_1, \ldots, n_k \rangle$ is a numerical semigroup, then more can be said. In particular, the polynomial restrictions occur on $n_1$ 1-dimensional cones, each generated by $n_1$, whose union has finite complement in $S$. The restriction of $M$ to each 1-dimensional cone is linear, and the leading coefficient of each linear restriction is $\frac{1}{n_1}$. The remaining cones are all 0-dimensional, one for each element of $S$ outside of the 1-dimensional cones.
Theorem 1.2 is part of a larger collection of my results from semigroup theory. Several purely semigroup-theoretic invariants, including delta sets \([BCKR06]\), \(\omega\)-primality \([OPe14]\), and catenary degree \([BGG11]\), extract highly specialized information about the semigroup’s factorization structure, and each has been recently shown to be eventually periodic or quasilinear for any numerical semigroup \(S\) \([CHK09, OPe13, CCMMP14, OPe15]\). My work in \([One15]\) simultaneously generalizes these results to affine semigroups using Hilbert’s theorem in the same manner as Theorem 1.2, resulting in a definitive link between combinatorial commutative algebra and the invariants of interest in semigroup theory, as well as a new framework through which semigroup theorists can examine these invariants for semigroups with finitely many generators. This illustrates a crucial benefit of using Hilbert’s theorem: bringing new tools to the table in adjacent areas.

1.2. Norm-optimizing factorizations. Theorem 1.2 implies that the extremal \(\ell_1\)-norms of the factorizations of sufficiently large affine semigroup elements \(m \in S\) are parametrized by the extremal \(\ell_1\)-norms of their divisors. Moreover, the proof of Theorem 1.2 for numerical semigroups characterizes which factorizations achieve such values, yielding an explicit parametrization ideal for use in discrete optimization problems.

The \(\ell_1\)-norm is a special case of a more general class of norms given by linear functionals. In particular, given a weight vector \(w \in \mathbb{Z}^k \geq 1\), consider the norm \(\| (a_1, \ldots, a_k) \|_w = w_1a_1 + \cdots + w_ka_k\), which clearly specializes to the standard \(\ell_1\)-norm when \(w = (1, \ldots, 1)\). Results in discrete geometry involving the \(\ell_1\)-norm often hold for more general linear functionals, and preliminary computations for several numerical semigroups indicate that Theorem 1.2 is no exception.

Project 1. Prove the following statement.

Given \(S \subset \mathbb{Z}^d_{\geq 0}\) affine and \(w \in \mathbb{Z}^k_{\geq 1}\), the function sending semigroup elements to the \(\max\) (resp. \(\min\)) \(\| \cdot \|_w\)-value of their factorizations is eventually quasilinear. Additionally, express the period and leading coefficient in terms of generators in the case when \(S\) is a numerical semigroup, and give a lower bound on the start of periodicity.

The eventually quasipolynomial behavior described in Theorem 1.2 is not limited to linear norms. One such example is the \(\ell_0\)-norm, which returns the number of nonzero entries in the input vector. A factorization of an affine semigroup element with small 0-norm can be seen as a “sparse solution” to the underlying linear equations. For real solutions, the 0-norm minimization problem has applications in signal processing via compressed sensing, where a linear programming relaxation provides a guaranteed approximation \([CERT06, CT05]\), and random matrices, where upper and lower bounds are known \([BDE09, CT05]\). In our setting of integer solutions, the 0-norm arises in the study of error-correcting codes, where it coincides with Hamming distance, and 0-norm minimization arises as the nearest codeword problem \([APY09, Mic14, Var97]\). Additionally, the 0-norm minimization problem arises in the context of finding guarantees for bin-packing problems via the Gilmore-Gomory formulation \([GG61, KK82]\).

Recent joint work with Aliev, De Loera, and Oertel \([ADOO17]\) proves that the \(\ell_0\)-norm has eventually quasiconstant minimum over any affine semigroup \(S\). Analogous to Theorem 1.2, this result specializes when \(S\) is a numerical semigroups.

Theorem 1.3 \([ADOO17]\). For any affine semigroup \(S \subset \mathbb{Z}^d_{\geq 0}\), the function \(m_0 : S \rightarrow \mathbb{Z}_{\geq 0}\) sending each element \(m \in S\) to the minimum 0-norm of its factorizations is eventually quasiconstant. Moreover, if \(S = \langle n_1, \ldots, n_k \rangle \subset \mathbb{Z}_{\geq 0}\) is a numerical semigroup, then \(m_0\) is eventually periodic with period \(\text{lcm}(n_1, \ldots, n_k)\).

The maximum and minimum values of other norms, such as the \(\ell_r\)-norms for \(r \in \mathbb{Z}_{\geq 1}\), are also important in discrete optimization \([DHK12, DHK13]\), and characterizing the eventual behavior of their maximum and minimum values over affine semigroup factorizations would have further impacts in this setting. Since the formula for the \(\ell_r\)-norm of a factorization concludes by taking an
r-th root, it is unlikely to be eventually quasipolynomial (or even admit a polynomial rate of growth for large semigroup elements). It is equivalent to characterize which factorizations admit maximal or minimal \((\ell_{r})^{r}\)-norm, and this quantity has a better chance of being eventually quasipolynomial since it, unlike the \(\ell_{1}\)-norm, is a polynomial in the coordinates of the input factorization.

Preliminary computations for large elements in several specific numerical semigroups indicates that \((\ell_{2})^{2}\)-norm values may be eventually quasiquadratic with period equal to the sum of the squares of the generators, providing evidence of a positive answer to Project 2 when \(r = 2\). On the other hand, \((\ell_{3})^{3}\)-norm values in the same semigroups either do not begin quasipolynomial behavior until significantly larger elements, or (more likely) are not eventually quasipolynomial.

**Project 2.** Given \(S \subset \mathbb{Z}_{\geq 0}^{k}\) affine, determine for which \(r \in [2, \infty)\) the function sending semigroup elements to the max (resp. min) \((\ell_{r})^{r}\)-value of their factorizations is eventually quasipolynomial. Specialize any answers in the affirmative to the special case where \(S\) is a numerical semigroup.

2. **Parametrized families of semigroups**

In this section, we consider families of semigroups indexed by a parameter \(n\) whose computational complexity is unexpectedly low, resulting in collections of “large” semigroups requiring less computation time than more general semigroups of comparable size.

2.1. **Parametric numerical semigroups.** Consider the family of numerical semigroups \(M_{n} = \langle n, n + r_{1}, \ldots, n + r_{k} \rangle\) obtained by “shifting” a base semigroup \(S = \langle r_{1} < \cdots < r_{k} \rangle\) by some shift parameter \(n\) (choosing \(n\) as the first generator of \(M_{n}\) ensures that every numerical semigroup falls into exactly one shifted family). Recent joint work with Pelayo [OPe17b] gives explicit formulas for the Frobenius number and genus (i.e. the number of gaps) of \(M_{n}\) when \(n > r_{k}^{2}\). Unlike previously mentioned results (e.g., Theorem 1.2), which described how invariant values change element-by-element, our results investigate how a semigroup’s properties change as the generators vary by a shift parameter. As with the aforementioned element-wise investigations of invariant values, our semigroup-wise analysis reveals eventual quasipolynomial behavior, this time with respect to the shift parameter \(n\).

Our main result characterizes the Apéry set of \(M_{n}\) for large \(n\) in terms of the Apéry set of the semigroup \(S = \langle r_{1}, \ldots, r_{k} \rangle\) at the base of the shifted family. Apéry sets are non-minimal generating sets that concisely encapsulate much of the underlying semigroup structure, and many properties of interest can be recovered directly and efficiently from the Apéry set [Gar15], making it a “one stop shop” for computation. We utilize these connections to derive quasipolynomial formulas for the Frobenius number and genus of \(M_{n}\) in terms of the base semigroup \(S\) for sufficiently large \(n\).

The results described above are a special case of the “parametric Frobenius problem”, which asks whether for fixed eventually positive polynomial functions \(f_{1}, \ldots, f_{k} : \mathbb{Z}_{\geq 0} \to \mathbb{Z}\), the Frobenius number of the numerical semigroup \(\langle f_{1}(n), \ldots, f_{k}(n) \rangle\) is eventually quasipolynomial in the parameter \(n\). Originally posed by Roune and Woods [RW15], this problem was answered in the affirmative by Shen [She17], with no further restrictions on \(f_{1}, \ldots, f_{k}\), using Ehrhart’s Theorem [Ehr62]. However, our approach in the special case of shifted numerical semigroups (i.e. when each \(f_{i}\) is linear with unit slope) has several advantages over the general approach. While Shen’s general approach does not yield precise control over the degree or coefficients of the eventual quasipolynomial, nor a bound on the start of quasipolynomial behavior, our approach yields precise control over each.

Another advantage of our approach over Shen’s pertains to computation. While Apéry sets of numerical semigroups (and many of the invariants derived from them) are generally more difficult to compute when the minimal generators are large, our results give a way to more efficiently perform these computations by instead computing them for the numerical semigroup \(S\), which has both smaller and fewer generators than \(M_{n}\). In fact, one surprising artifact of our algorithm, which is currently implemented in the popular GAP package numericalsgps [DGM17], is that the
computation of the Apéry set of $\mathcal{M}_n$ for $n > r_k^2$ is often significantly faster than for $\mathcal{M}_n$ with $n \leq r_k^2$, even though the former has larger generators. In contrast, computing the Ehrhart polynomials arising in Shen’s general proof has significantly higher complexity [DDK13].

The success of our specialized approach motivates the following project.

**Project 3.** Given positive polynomial functions $f_1, \ldots, f_k : \mathbb{Z}_{\geq 0} \to \mathbb{Z}_{\geq 1}$, express the Apéry set of the numerical semigroup $(f_1(n), \ldots, f_k(n))$ for large $n$ in terms of the base semigroup $(f_1(0), \ldots, f_k(0))$.

When first stating their general conjecture, Roune and Woods proved that the Frobenius number is eventually quasipolynomial in both of these cases. Their proof was direct (i.e. uses no heavy machinery like Ehrhart’s theorem) and yielded a formula for the quasipolynomial degree, although not in such a way as to recover information about the underlying Apéry set. Preliminary computations also indicate that a formula similar in spirit to that for shifted numerical semigroups holds in both of these cases.

### 2.2. Minimal relations in shifted semigroups.

The family of shifted numerical semigroups $\mathcal{M}_n = \langle n, n + r_1, \ldots, n + r_k \rangle$ is also found in a conjecture of Herzog and Srinivasan, which stated that the Betti numbers of the defining toric ideal of $\mathcal{M}_n$ are eventually periodic in $n$. Their conjecture was proved in several special cases [GSS13, JS13] using semigroup-theoretic arguments, and then in general by Vu [Vu14] using techniques from combinatorial commutative algebra.

A recent REU project coadvised with Pelayo and Wissmam [CGHORWW17] proved the same result using *minimal presentations*, which combinatorially encapsulate the minimal relations between semigroup generators. More concretely, a minimal presentation of an affine semigroup $\mathcal{S}$ is a minimal collection of pairs of factorizations, called *trades*, that can connect any two factorizations of each element of $\mathcal{S}$. For example, a minimal presentation of the numerical semigroup $\mathcal{S} = \langle 6, 9, 20 \rangle$ consists of the two relations: $\langle (3, 0, 0), (0, 2, 0) \rangle$, which trades 3 copies of 6 for 2 copies of 9, and $\langle (10, 0, 0), (0, 0, 3) \rangle$, a minimal trade between 6’s and 20’s. Any two factorizations in $\mathcal{S}$ can be connected by applying each of these trades an appropriate number of times.

Minimal presentations arise in the study of toric ideals, where they correspond to minimal generating sets for kernels of monomial maps [CLO15], algebraic statistics, where they correspond to Markov bases used for independence sampling [AHT12, DS98], and discrete optimization, where they provide explicit algorithms for certain optimization problems [DHK13]. Additionally, many arithmetic invariants of interest in combinatorial commutative algebra (e.g. Betti numbers and minimal syzygies [MS05, Sta96]) and semigroup theory (e.g. catenary degree [BGG11]) can be easily recovered (both theoretically and computationally) from a minimal presentation, making them a particularly useful tool in computational algebra [Gar15]. The software package 4ti2 [4TI2] computes minimal presentations as one of its primary functionalities, and is internally linked to both the algebraic geometry software Macaulay2 [M2] and the GAP package numericalsgps [DGM17] as the preferred method of doing so.

Theorem 2.1 describes how minimal presentations of $\mathcal{M}_n$ vary with large $n$. More specifically, we give an explicit bijection between the minimal presentations of $\mathcal{M}_n$ and those of $\mathcal{M}_{n+r_k}$ when $n > r_k^2$. As a consequence, we derive eventually quasipolynomial relationships for several of the aforementioned arithmetic quantities, more directly than would be possible from statements in [Vu14]. In particular, much of the theory we develop would have been necessary for specialized proofs of these consequences, and such specialization would obscure the underlying connections. This is in part because our approach is purely combinatorial; shedding the dependence on commutative algebra better isolates the core structural changes that occur once $n$ is large enough.

**Theorem 2.1** ([CGHORWW17]). There is a map sending each relation between generators of $\mathcal{M}_n$ to a relation between generators of $\mathcal{M}_{n+r_k}$ that, for $n > r_k^2$, bijects minimal presentations onto minimal presentations.
Aside from providing an alternative proof to Herzog and Srinivasan’s conjecture, Theorem 2.1 yields a significantly faster algorithm for computing minimal presentations of “sufficiently shifted” numerical semigroups. Minimal presentations are also used frequently in computer software package implementations, since many quantities of interest can then be quickly computed [Gar15]. Most existing algorithms to compute a minimal presentation of a given numerical semigroup use Gröbner basis techniques, which become computationally infeasible as the number and size of the generators grow large [CLO15]. Theorem 2.1 yields a method of reducing this complexity in certain cases. In particular, if the generators of a numerical semigroup \( M = \langle n_1, \ldots, n_k \rangle \) satisfy \( n_1 > (n_k - n_1)^2 + (n_k - n_1) \), then a minimal presentation for \( M \) can be computed by first computing a minimal presentation for \( M' = \langle n_1 - R, \ldots, n_k - R \rangle \), where \( R \) is some appropriately chosen multiple of \( n_k - n_1 \), and then successively applies the bijection in Theorem 2.1 until a minimal presentation for \( M \) is obtained. In cases where the generators of \( M' \) are significantly smaller than those of \( M \), the resulting computation is much faster than directly computing a minimal presentation for \( M \). Our bound of \( n > r_k^2 \), while not tight, is lower than that appearing in [Vu14], which is crucial for effective use in the software implementation, which can be found in the GAP package \texttt{numericalsgps} [DGM17].

Project 4 proposes a generalization of Theorem 2.1 concerning an intentionally redundant list of relations called a Graver basis. Unlike minimal presentations, which simply ensure that any two factorizations of a semigroup element \( m \in M \) can be connected by a sequence of relations, the Graver basis contains sufficiently many additional relations to ensure a path between any two factorizations may be constructed using a greedy algorithm. This allows many computations (such as linear optimization) to run in significantly fewer steps, but comes at a cost: Graver bases are usually far too large to compute explicitly, as their size grows doubly exponentially as the number and magnitude of generators of \( M \) grows [Stu96].

In view of the size limitations of Graver bases, there is significant interest in finding families of semigroups with polynomial Graver complexity. One example of such a family is comprised of a block diagonal matrix with \( n \) identical blocks \( B \) and a block row matrix with \( n \) identical blocks \( A \). For fixed matrices \( A \) and \( B \), the size of the Graver basis of \( F_n \) is a polynomial in \( n \) [DHOW08].

Aside from a handful of generalizations [HKW10], \( n \)-fold products are the only known families of affine semigroups with polynomial Graver complexity.

Quite surprisingly, preliminary computations indicate that families of shifted numerical semigroups also have polynomial Graver complexity. More specifically, for sufficiently large \( n \), each relation in the Graver basis of the numerical semigroup \( M_n = \langle n, n + r_1, \ldots, n + r_k \rangle \) seems to be determined by a relation in the Graver basis for \( M_{n-(r_j-r_i)} \) for some \( i < j \), in a manner reminiscent of how each relation in a minimal presentation for \( M_n \) can be recovered from a relation in a minimal presentation for \( M_{n-r_k} \). In addition to implying polynomial Graver complexity in \( n \), proving the claim in Project 4 result would yield an inductive algorithm to compute the Graver basis of \( M_n \).

Project 4. Prove the following statement:

For fixed \( r_1, \ldots, r_k \), the number of elements in the Graver basis of the numerical semigroup \( M_n = \langle n, n + r_1, \ldots, n + r_k \rangle \) is eventually quasipolynomial in \( n \).

3. Random numerical semigroups

There is a long history of using randomness and probability to study algebraic objects. One of the earliest examples concerns the expected number of real roots of a polynomial with randomly chosen coefficients [LO38]. The study of random matrices has also spanned the better part of the last century, resulting in beautiful universality theorems [Tao12] and highly efficient randomized algorithms [RK04, DF94]. More recently, properties of random Betti tables [EEL15] were obtained
using Boij-Söderberg theory [BS08], chordal networks were paired with probabilistic algorithms to yield significant performance improvements for fundamental algebraic geometry computations [CP17], and there has been a surge in the study of random algebraic objects using tools that have proven successful in studying random combinatorial objects (e.g. graphs [ER59] and simplicial complexes [Kah14]).

There are several reasons for examining the “average behavior” of algebraic objects produced in this fashion. For one, in many cases, the worst-case behavior happens only a small fraction of the time, allowing for randomized or approximate algorithms to be particularly effective. A classical example is Gaussian elimination, which is provably numerically unstable in general [OW82] but is quite stable in practice [TS90]. Additionally, probabilistic arguments can demonstrate the existence of objects with extremal properties when concrete examples are too large or infrequent to construct explicitly. As an example, random flag complexes were recently used to construct families of objects with extremal properties when concrete examples are too large or infrequent to construct explicitly [Kah14].

In the realm of numerical semigroups, the Frobenius function $F(S)$ of a “typical” numerical semigroup $S$ was explored by Arnol’d [Arn99] and Bourgain and Sinai [BS07]. More specifically, these papers considered random numerical semigroups $S$ obtained by selecting a generating set uniformly at random from the set

$$\{a \in \mathbb{Z}_{\geq 1}^k : \gcd(a) = 1 \text{ and } \max\{a_1, \ldots, a_k\} \leq M\}$$

of $k$-tuples with coordinates at most $M$, and characterized, among other things, the expected value of the Frobenius number $F(S)$. Further results in this direction can also be found in [AHH11].

### 3.1. The Erdős-Rényi type model

In recent joint work with De Loera and Wilbourne [DOW17] examines a different model for sampling random numerical semigroups. Under our model, dubbed the ER-type model for its resemblance to the Erdős-Rényi model for random graphs [ER59], a random numerical semigroup $S$ is generated according to the following procedure:

1. fix an upper bound $M \in \mathbb{Z}_{\geq 1}$ and a probability $p \in [0, 1]$;
2. initialize a set of generators $G = \{0\}$ for $S$;
3. independently choose with probability $p$ whether to include each $n \leq M$ in $G$.

ER-type models have been used to generate random graphs, simplicial complexes [Kah14], and monomial ideals [DPSSW17]. Often in these areas, the probability $p = p(M)$ is viewed as a function of $M$, and asymptotic characterizations of expected behavior as $M \to \infty$ are stated in terms of threshold functions, which delineate substantial changes. For example, if a random graph $G$ with $n$ vertices is chosen by including each edge with probability $p$ (the ER-type model for graphs), then as $n \to \infty$, the probability $G$ is connected approaches $1$ if $p = p(n) \gg \log(n)/n$ and approaches $0$ if $p(n) \ll \log(n)/n$ [ER59]. We say $\log(n)/n$ is the threshold function for connectedness.

Our main result for random numerical semigroups selected under the ER-type model identifies threshold functions for cofiniteness in $\mathbb{Z}_{\geq 0}$ and finiteness of the expected number of minimal generators $e(S)$, expected number of gaps $g(S)$, and expected Frobenius number $F(S)$ as $M \to \infty$. When each of these quantities remains finite as $M \to \infty$, we give bounds in terms of $p$.

**Theorem 3.1** ([DOW17]). Let $S$ be a random numerical semigroup sampled using the ER-type model with upper bound $M$ and probability $p$.

1. If $p(M) \ll 1/M$ as $M \to \infty$, then $S = \{0\}$ asymptotically almost surely (a.a.s.);
2. If $1/M \ll p(M)$ and $p(M) \to 0$ as $M \to \infty$, then $S$ has finite complement in $\mathbb{Z}_{\geq 0}$ a.a.s. and
   $$\lim_{M \to \infty} \mathbb{E}[e(S)] = \lim_{M \to \infty} \mathbb{E}[g(S)] = \lim_{M \to \infty} \mathbb{E}[F(S)] = \infty.$$
3. If $p(M) \gg 0$ as $M \to \infty$, then
   $$\lim_{M \to \infty} \mathbb{E}[e(S)], \lim_{M \to \infty} \mathbb{E}[g(S)], \lim_{M \to \infty} \mathbb{E}[F(S)] < \infty.$$
Experiments

<table>
<thead>
<tr>
<th>$p$</th>
<th>Lower bound</th>
<th>Experiments</th>
<th>Upper bound</th>
<th>Exact</th>
</tr>
</thead>
<tbody>
<tr>
<td>$M = 25000$</td>
<td>$M = 50000$</td>
<td>$M = 90$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0.25</td>
<td>2.21</td>
<td>3.3663</td>
<td>3.3761</td>
<td>3.75</td>
</tr>
<tr>
<td>0.1</td>
<td>2.64</td>
<td>4.6236</td>
<td>4.6402</td>
<td>19.9</td>
</tr>
<tr>
<td>0.01</td>
<td>2.96</td>
<td>9.7906</td>
<td>9.776</td>
<td>199.9</td>
</tr>
</tbody>
</table>

Table 1. Comparison of asymptotic bounds on the expected number of minimal generators in Theorem 3.1 with experimental evidence.

All 3 quantities whose asymptotic behavior is characterized in Theorem 3.1 depend closely on the probability $A_n(p)$ that an integer $n$ is not lie in the semigroup generated by the chosen elements less than $n$. For instance $A_{15}(p) = (1-p)^7(1+4p+2p^2)$ is the probability that 15 cannot be written as a sum of the integers 1, ..., 14 each chosen with probability $p$. Surprisingly, the form of $A_{15}(p)$ is no coincidence; factoring out $(1-p)^{\lfloor n/2 \rfloor}$ from $A_n(p)$ yields a polynomial in $p$ with non-negative integer coefficients given by the $h$-vector of a simplicial complex $\Delta_n$, that is,

$$A_n(p) = (1-p)^{\lfloor n/2 \rfloor}(h_{n,0} + h_{n,1}p + \cdots).$$

A cornerstone of algebraic combinatorics, the $h$-vector of a simplicial complex $\Delta$ is a finite integer sequence determined by the numbers $f_i$ of $i$-dimensional faces of $\Delta$, and arises naturally in the study of squarefree monomial ideals [Sta96] and posets [KO96]. More specifically, the $h$-vector gives the coefficients of the numerator of the Hilbert series of the Stanley-Riesner ring $k[\Delta]$ of $\Delta$. If $\Delta$ is sufficiently nice (e.g. shellable, Cohen-Macaulay, or partitionable), then the $h$-vector entries are non-negative integers counting certain facets of $\Delta$.

The facets of the simplicial complex $\Delta_n$, whose $h$-vector entries appear in the polynomial $A_n(p)$, are in bijection with those numerical semigroups that are maximal (w.r.t. containment) among numerical semigroups with Frobenius number $n$ (called irreducible numerical semigroups [GR09]). The complex $\Delta_n$ turns out to be shellable, which implies that the $h$-vector entries (and thus the coefficients arising in $A_n(p)$) each count facets of $\Delta_n$ with certain properties. In the end, the coefficient $h_{n,i}$ counts the number of irreducible numerical semigroups $S$ with $F(S) = n$ and precisely $i$ minimal generators less than $n/2$. Though several posets whose elements are numerical semigroups have been studied elsewhere in the literature [RGGJ04], none examine the simplicial complex $\Delta_n$ specifically.

As a consequence of the above discussion, the asymptotic behaviors of $E[e(S)]$, $E[g(S)]$ and $E[F(S)]$ as $M \to \infty$ are controlled via combinatorial bounds on the $h$-vector of the shellable simplicial complex $\Delta_n$. Consequently, parts (b) and (c) of Theorem 3.1 are obtained, as well as upper and lower bounds in terms of $p$ when each expectation is finite. Table 1 compares the bounds resulting from the proof of Theorem 3.1 with experimental evidence (100,000 samples), and the last column gives the exact expected value for $M = 90$ using polynomials computed with the algorithm [RGGJ04] implemented in the popular GAP package `numericalsgps` [DGM17].

### 3.2. The probabilistic method and Wilf’s conjecture

Wilf’s conjecture [Wil78] is one of the most famous open problems in the numerical semigroups literature. Equality has been shown to hold for $M = \langle n_1, n_2 \rangle$ and $M = \langle m, m + 1, \ldots, 2m - 1 \rangle$, which have respectively the smallest and largest possible number of minimal generators for a numerical semigroup. Aside from a small number of isolated examples, the inequality appears to be strict in all other cases, but despite substantial effort, the conjecture remains open in general.

**Conjecture 3.2** (Wilf). Any numerical semigroup $M = \langle n_1, \ldots, n_k \rangle$ satisfies

$$F(M) + 1 \leq k(F(M) - g(M)),$$

where $F(M)$ is the Frobenius number of $M$ and $g(M)$ is the number of gaps of $M$. 
First popularized by Erdős [Erd64], the probabilistic method in combinatorics is a method of proving objects with a certain property exist without explicitly producing an example. Often, such proofs involve selecting an object at random and proving that the probability it has the desired property is positive [AS16].

The probabilistic method is particularly effective if the objects in question are too large to easily construct but abundant enough to occur frequently. The quintessential example is Erdős proof [Erd63] that the Ramsey numbers $R(r, r)$ grow exponentially in $r$, which he accomplished by proving that any complete graph with at least $(1.1)^r$ vertices has an edge 2-coloring with no monochromatic $r$-vertex subgraphs. Rather than explicitly construct such a coloring, he proved that the probability of a randomly chosen edge coloring having this property is positive. To this day, no concrete examples of such a coloring have been found, despite the fact that his proof demonstrates “most” colorings satisfy this property.

Wilf’s conjecture is precisely the kind of problem the probabilistic method is designed for. Indeed, every numerical semigroup $M$ with $g(M) \leq 60$ has been shown to satisfy Wilf’s conjecture via exhaustive computation [Bra08], so if a counterexample exists, it is not “small”. Additionally, many of the special classes of semigroups for which Wilf’s conjecture has been proven satisfy some inequality that makes the proof easier (for instance, a lower bound on $k$ [Sam12] or an upper bound on $F(M)$ [DM06]), resulting in a form of “selection bias” favoring classes of semigroups that are more likely to satisfy the conjecture. The probabilistic method provides a way to systematically avoid such bias by considering all numerical semigroups at once, partitioning them based on certain conditions, and ensuring that some collection failing to satisfy Wilf’s conjecture is nonempty.

**Project 5.** Use the probabilistic method to prove a counterexample to Wilf’s conjecture exists.
References


RESEARCH STATEMENT


