Approximate Counting of Contingency Tables Using Markov Chains

A Thesis presented by

Patricia Hersh

to

Mathematics and Computer Science

in partial fulfillment of the honors requirements

for the degree of

Bachelor of Arts

Harvard College

Cambridge, Massachusetts

June 20, 1999

Contents

1 Introduction

This thesis examines the problem of approximating the number of matrices of nonnegative integers with a fixed set of constraints such as fixed row and column sums. The space of such matrices may also be viewed as the set of lattice points in a polytope, and so is related to a widely studied approximation problem in theoretical computer science. In particular, this thesis studies approximate counting of $n \times n$ tables with each row, column and the two main diagonals summing to r, i.e. magic squares. The intent is to apply to this counting problem the technique of approximation by random generation of elements using Markov chains as discussed in [14], and also to obtain exact answers to measure the accuracy of approximation methods. The approach is experimental in that Markov chains were run and the accuracy of results were examined for varied sample sizes and for varied numbers of steps taken to generate each sample item.

The focus is not on the more generally studied problem of bounding how quickly Markov chains converge to a stationary distribution, but instead on algebraic techniques useful in running Markov chains in this problem and perhaps also relevant to other approximation problems. Commutative algebra arises both in choosing a set of basic moves for a Markov chain and in the exact counting problem; combinatorics and homology theory also arise in this counting problem. A key analytic result about Markov chain convergence is cited and used, but its proof is well beyond the scope of this thesis.

Chapter two surveys techniques for choosing basic moves for a Markov chain. First necessary ideas from computational algebraic geometry and commutative algebra are developed including the concept of a Gröbner basis. Next is presented an algorithm due to Sturmfels and Diaconis found in [17] for finding a set of basic moves which was used and made the approximation work in this thesis possible. An alternative approach developed in [8] is also described since it is quite possibly more capable of handling large examples.

Another issue that was intentionally emphasized is testing how well some theoretical ideas work in practice. The third chapter outlines explicitly how results were obtained and presents these results on sampling by Markov chains for 3×3 and 4×4 magic squares. The appendices include a sample Macaulay script to generate a Gröbner basis and a list of the resulting Markov chain basic moves. This is meant to streamline the process for anyone wishing to run similar Markov chains.

Finally, chapter four examines a theorem of Stanley about exact counting of tables with equal row and column sums and how it might generalize to magic squares. If the theorem does generalize, it will provide a reasonable way of counting magic squares and would enable us to test the accuracy of approximations on magic squares even with very large sums for each row, column and the main diagonals. Since the approximation techniques used for magic squares are the same as would be used in the general case of contingency tables with row, column and additional constraints, any results about the accuracy of approximate counting of magic squares should be indicative of the effectiveness of approximation for more general contingency tables. Stanley's proof does not generalize to magic squares as counterexamples were found to an important lemma, but quite possibly the result itself does generalize and much of the argument may also carry over to another proof, and so chapter three surveys Stanley's proof in addition to offering a very basic formula for counting magic squares in the 3×3 case which is used to test very small approximations.

I am grateful to Professor Diaconis for suggesting a problem which so beautifully applies algebra and geometry to a question of interest to statisticians and computer scientists. I would like to thank him also for making me aware of areas of math I had no idea I would find so interesting and for all his advice and encouragement. Thanks also go to Professor Valiant for suggesting last spring I study a topic related to much current research, that of approximation by Markov chains. I also appreciate several discussions with Brad Mann who offered clear and relevant advice while Professor Diaconis was in France, and I especially want to thank Professor Harris for showing how beautiful math could be three years ago and for his encouragement and very thoughtful advice ever since.

1.1 Approximation by Markov Chains

Monte Carlo methods are often used to approximate the size of large sets which would be difficult to count exactly. For example, one method of estimating $\pi/4$ is to randomly choose ordered pairs of numbers (x, y) between 0 and 1 and then measure what fraction of these pairs satisfy the inequality $x^2+y^2 < 1$. A related approximation technique involves randomly generating elements of the set being approximated to see what fraction of these lie in some subset whose size can be more easily estimated since it is smaller. If reasonable bounds on approximations exist, this approach can be used on multiple levels to recur down to a problem that can be solved exactly.

Definition 1.1.1 *A Markov chain is a state space together with a transition matrix in which entry $a_{i,j}$ is the conditional probability of moving from state i to state j at each time interval.*

A key property of a Markov chain is that the probability of moving to a particular state at time $t+1$ is based only on the position at time t, so the past history is entirely irrelevant. Markov chains have proven useful in approximations when random generation of elements is itself a difficult problem. If, for example, one proves that some Markov chain is almost equally likely to be anywhere in the state space after 1000 moves regardless of starting position, then one may generate elements approximately uniformly at random by running a Markov chain and choosing an element for a randomly generated sample once every 1000 steps.

A walk is defined as rapidly mixing if some Markov chain connects the space in such a way that the uniform distribution is closely approximated after a small number of moves. By small we mean there is some polynomial in the log of the size of the state space and in the inverse of the allowable error size which bounds the number of moves from any starting point needed to approximate the uniform distribution within the allowable degree of error. Intuitively, a walk will be rapidly mixing if there are many paths from any state to any other. To prove a walk is rapidly mixing, one would look at the underlying graph constructed by making a node of each state and an edge between states connected by some basic move of our Markov chain. One method of showing a Markov chain is rapidly mixing uses estimates of the second largest eigenvalue of the transition matrix; there is some stationary distribution, which is an eigenvector with eigenvalue 1, and we do not want other distributions to be almost as stable.

The intent in doing approximations is to examine only a tiny fraction of the state space which might be quite large, but for an approximation of what fraction of the whole a subset occupies to be a good estimate, the subset also needs to occupy a significant portion of the entire space.

1.2 Approximate Counting of Magic Squares and Contingency Tables

One problem for which approximation techniques have had some success is the question of approximating the number of tables of nonnegative integers with fixed row and column sums, known as contingency tables. One well-known class of contingency tables are magical squares, i.e. $n \times n$ tables of nonnegative integers with equal row and column sums. More generally, statisticians study $n \times m$ tables of data with fixed row and column sums. General contingency tables may be used to count people with two traits such as hair color and eye color, measuring one in the rows and the other in the columns; generating random tables and approximating the number of tables with specified sums prove useful in measuring whether an apparent corollation between two traits is random coincidence or significant. Diaconis suggested studying magic squares as an example of contingency tables with extra constraints which might also be reasonably easy to count exactly.

Combinatorialists have developed interesting expressions for the number of $n \times m$ tables of nonnegative integers with a particular set of row and column sums, but actual counting quickly grows into an unwieldy task, so work at approximation by Markov chains is a promising alternative. Beautiful exact formulas involving such objects as descent sets, induced representations and double cosets may be found in [6]. Stanley proved the number of $n \times n$ magical squares of sums r is a polynomial of degree $(n-1)^2$ in r, a more useful result for obtaining numerical counts with reasonable efficiency in this special case. Diaconis and Saloffe-Coste very recently showed that Markov chains on the kernel of a class of matrices known as totally unimodular matrices are rapidly mixing; this applies to contingency tables and also magic squares, that is, magical squares with main diagonals also summing to the same value as the rows and columns, so approximation not only appears effective, but provably so.

In the case of contingency tables, one may choose basic moves for a Markov chain by picking two rows and two columns at random and changing the four numbers they specify; in each of the two rows and the two columns one must increase one of the numbers by 1 and decrease the other by 1. For example,

$$\begin{pmatrix} + & - & 0 \\ - & + & 0 \end{pmatrix}$$

may be used as a basic move for 2×3 tables. If a move makes some entry negative, then instead of moving to an illegal table, one sits idle for a step. The set of legal moves changing two rows and two columns not only spans the space of moves preserving row and column sums viewed as the kernel of a matrix specifying the set of constraints, but it also connects the space of legal moves so that any table may be reached from any other without ever needing to leave the space of legal tables.

We study the problem of approximating the number of magic squares, tables with additional constraints that the two diagonals sum to the same number as all the rows and columns. This adds the twist that basic moves for contingency tables no longer connect the space since altering four positions may not alter a diagonal and still preserve its sum. Gröbner bases prove useful in choosing basic moves for magic squares, and other tables with additional constraints so chapter 2 surveys algorithms using commutative algebra and algebraic geometry needed for chapter 3.

2 Algebraic Techniques for Computing Basic Moves

The problem of generating a set of basic moves for a Markov chain on magic squares can be rephrased as a problem of commutative algebra for which a practical algorithm is known and for which implementations can be found in such software packages as Macaulay and Maple. Sturmfels and Diaconis translated the problem of finding basic moves for a random walk to one of computing Gröbner bases to which we may apply a useful algorithm of Buchberger. Section 2.1 introduces the necessary computational algebraic geometry found in [5], and then section 2.2 explains how to use it to find basic moves for a Markov chain outlining ideas of [17]. Since this algorithm may sometimes exceed current memory bounds in actual computation, another less direct approach found in [8] which may be more efficient in large cases is presented in section 2.3 as an alternative.

2.1 Computational Algebraic Geometry and Gröbner Bases

This section serves as an overview of ideas described more thoroughly in [5] which are relevant to later sections.

Definition 2.1.1 *An ideal is a subset I of a ring R such that for any $r \in R$ and $s \in I$, $rs \in I$.*

Definition 2.1.2 *A basis B is a subset of an ideal I contained in a ring R such that every ideal element may be expressed in terms of basis elements, i.e. such that $s \in I$ implies s may be written as a finite sum $\sum_{i=1}^{m} r_i b_i$ with $r_i \in R$ and $b_i \in B$ for all i.*

We will be concerned with constructing finite bases for ideals of polynomial rings, so it is useful to note that for k a field, every ideal in the polynomial ring $k[x_1, \ldots, x_n]$ has a finite basis. This is a well known result called the Hilbert Basis Theorem. A simple proof may be found in [5] Also necessary is a notion of division of a polynomial by an ideal to systematically find a common unique remainder for each class of polynomials which differ from each other by ideal elements, but this will first require some notion of which monomials are "larger" for the concept of decreasing remainders to make sense. An order known as lexicographic order proves convenient in studying contingency tables. First let us order the variables $x_1, \ldots, x_n$ by requiring $x_1 > x_2 > \ldots > x_n$.

Definition 2.1.3 *Lexicographic order is the monomial order such that* $x_1^{\alpha_1} \ldots x_n^{\alpha_n} > x_1^{\beta_1} \ldots x_n^{\beta_n}$ *if* $\alpha_j > \beta_j$*, and* $i < j$ *implies* $\alpha_i = \beta_i$*.*

For example, $x_1^2 x_2^3 x_3$ is a higher order monomial than $x_1^2 x_2 x_3^4$ under this monomial order. Throughout we will use lexicographic order exclusively. Each polynomial in G has a leading monomial or leading term of highest order which we denote by $LT(g)$. Throughout, we will let x^α denote $x_1^{\alpha_1} \ldots x_n^{\alpha_n}$ to simplify notation.

In division of integers, for any $a, b \in \mathbb{Z}$, there exists $q, r \in \mathbb{Z}$ such that $a = bq + r$ for $|r| < b$. This generalizes to division of a polynomial by an ideal. The goal is to express the polynomial as an ideal element plus a remainder which is as small as possible. If a polynomial is in the ideal, there should be a systemative way of discovering that the remainder is 0. For polynomials not in the ideal, we would like to reduce in the same fashion until the remainder can be reduced no further. To design such an algorithm to produce a unique remainder, we first introduce what is known as a Gröbner basis for an ideal.

Definition 2.1.4 *A basis* $\{g_1, \ldots, g_t\}$ *for a polynomial ideal* I *is a Gröbner basis if* $\langle LT(g_1), \ldots, LT(g_t)\rangle = \langle LT(I)\rangle$*.*

This means that the span of the leading terms of the basis is the set of all the leading terms of all elements of the ideal.

Example 2.1.5 *The set* $\{x_1 - x_2, x_1 - x_3\}$ *is not a Gröbner basis for* $\langle x_1 - x_2, x_1 - x_3\rangle$ *with respect to the lexicographic order with* $x_1 > x_2 > x_3$ *since* $(x_1 - x_2) - (x_1 - x_3)$ *is in the ideal, but it has leading term* $-x_2$*, and this is not in* $\langle x_1\rangle$*, the span of the leading terms of the basis elements.*

The point of a Gröbner basis is to allow a division algorithm by making it unnecessary to ever express a polynomial as a smaller remainder plus a sum of two ideal elements with high order leading terms which cancel.

In a Gröbner basis, any nonzero element of the generated ideal can be reduced to one with a smaller order leading term since some combination of Gröbner basis elements has the same leading term as the polynomial being reduced, so subtracting this combination cancels leading terms leaving only smaller order terms as remainder.

This will allow us to pick a basepoint table such as the table with all entries $\frac{r}{d}$ and move from any table to any other with the same sums by reducing each to the same remainder table; the difference between legal tables is a table with sums all 0, and the set of these leval move tables corresponds to an ideal for which we find a Gröbner basis. This will not only show we can move from any table to any other, but also give an upper bound on the maximum distance between any two tables.

An algorithm called Buchberger's algorithm is used to compute a Gröbner basis for the ideal we construct to represent legal moves, i.e. tables with row, column and main diagonal sums 0 by which two tables with equal sums may differ. Let us first define S-polynomials, a key construct for the algorithm.

Definition 2.1.6 *Given two polynomials f and g in an ideal I where x^γ is the least common multiple of the leading terms of f and g, let $S(f,g) = \frac{x^\gamma}{LT(f)} \cdot f - \frac{x^\gamma}{LT(g)} \cdot g$.*

Note that leading terms cancel since both $\frac{x^\gamma}{LT(f)} \cdot f$ and $\frac{x^\gamma}{LT(g)} \cdot g$ have leading term x^γ. The S-polynomials are designed to produce cancellation of leading terms. Buchberger proved that a basis $\langle g_1, \ldots, g_n \rangle$ for an ideal I is a Gröbner basis if and only if whenever $i \neq j$, $LT(S(g_i, g_j)) \in \langle LT(g_1), \ldots, LT(g_n) \rangle$. Buchberger's algorithm simply involves taking an ideal basis $\langle g_1, \ldots, g_n \rangle$ and extending the basis to include any combination $S(g_i, g_j)$ such that $LT(S(g_i, g_j)) \notin \langle LT(g_1), \ldots LT(g_m) \rangle$ where $\langle g_1, \ldots, g_m \rangle$ is the basis built thus far. The following results prove this process terminates to generate a Gröbner basis.

Theorem 2.1.7 *If $x^\delta = x^{\alpha(1)} LT(g_1) = \ldots = x^{\alpha(t)} LT(g_t)$ and $\deg \left(\sum_{i=1}^t c_i x^{\alpha(i)} g_i \right) < \delta$, then $\sum_{i=1}^t c_i x^{\alpha_i} g_i$ can be written as a sum of terms of the form $x^{\delta - \gamma_{j,k}} S(g_j, g_k)$ for $x^{\gamma_{j,k}} = LCM \left(x_1^{LT(g_j)_1} \ldots x_n^{LT(g_j)_n}, x_1^{LT(g_k)_1} \ldots x_n^{LT(g_k)_n} \right)$. Each term $x^{\delta - \gamma_{j,k}} S(g_j, g_k)$ has degree less than δ.*

Proof. We express the original sum $\sum_{i=1}^t c_i x^{\alpha_i} g_i$ more conveniently as a sum of terms of the form $x^{\alpha(i)} g_i - x^{\alpha(i+1)} g_{i+1}$. At the ith stage replace $x^{\alpha(i)} g_i$ in the sum by $x^{\alpha(i)} g_i - x^{\alpha(i+1)} g_{i+1}$, and then at the $(i+1)$st stage add extra terms to cancel the extra $-x^{\alpha(i+1)}g_{i+1}$ introduced at the ith stage. Hence, note that

$$\begin{aligned}
\sum_{i=1}^{t} c_i x^{\alpha(i)} g_i &= \sum_{i=1}^{t-1} c_i \left(x^{\alpha(i)} g_i - x^{\alpha(i+1)} g_{i+1}\right) + \sum_{i=1}^{t-2} c_i \left(x^{\alpha(i+1)} g_{i+1} - x^{\alpha(i+2)} g_{i+2}\right) \\
&\quad + \ldots + \sum_{i=1}^{1} c_i \left(x^{\alpha(i+t-2)} g_{i+t-2} - x^{\alpha(i+t-1)} g_{i+t-1}\right) \\
&\quad + (c_1 + \ldots + c_t) x^{\alpha(t)} g(t) \\
&= \sum_{i=1}^{t-1} (c_1 + \ldots + c_i) \left(x^{\alpha(i)} g_i - x^{\alpha(i+1)} g_{i+1}\right) + (c_1 + \ldots + c_t) x^{\alpha(t)} g_t.
\end{aligned}$$

Let d_i be the coefficient of the leading term of g_i to obtain

$$\begin{aligned}
\sum_{i=1}^{t} c_i x^{\alpha(i)} g_i &= \sum_{i=1}^{t} c_i d_i x^{\alpha_i} \left(\frac{g_i}{d_i}\right) \\
&= \sum_{i=1}^{t} (c_1 d_1 + \ldots + c_i d_i) \left(x^{\alpha(i)} g_i / d_i - x^{\alpha(i+1)} g_{i+1} / d_{i+1}\right) \\
&\quad + (c_1 d_1 + \ldots + c_t d_t) x^{\alpha(t)} g_t / d_t.
\end{aligned}$$

Since $\deg(\sum_{i=1}^{t} c_i x^{\alpha(i)} g_i) < \delta$, note that $(c_1 d_1 + \ldots + c_t d_t) x^{\alpha(t)} g_t / d_t = 0$, so $\sum_{i=1}^{t} c_i x^{\alpha(i)} g_i$ is expressible in terms of differences $\dfrac{x^{\alpha(i)} g_i}{d_i} - \dfrac{x^{\alpha(i+1)} g_{i+1}}{d_{i+1}}$. Since $x^{\alpha(i)} = \dfrac{x^\delta}{LT(g_i)}$ which means $\dfrac{x^{\alpha(i)} g_i}{d_i} = \dfrac{x^\delta g_i}{LT(g_i)} = x^{\delta - \gamma_{i,i+1}} \left(\dfrac{x^{\gamma_{i,i+1}} g_i}{LT(g_i)}\right)$, these differences $\dfrac{x^{\alpha(i)} g_i}{d_i} - \dfrac{x^{\alpha(i+1)} g_{i+1}}{d_{i+1}}$ can be written as $x^{\delta - \gamma_{i,i+1}} S(g_i, g_{i+1})$. Note also that each term $x^{\delta - \gamma_{j,k}} S(g_j, g_k)$ has degree less than δ since $S(g_j, g_k)$ has degree less than $\gamma_{j,k}$ by the definition of $S(g_j, g_k)$. □

Next we show that adding elements of the form $S(g_i, g_j)$ to a basis until each $LT(S(g_i, g_j))$ is in $\langle LT(g_1), \ldots, LT(g_n)\rangle$ yields a Gröbner basis.

Theorem 2.1.8 *A basis $g_1, \ldots, g_n$ is a Gröbner basis if and only if $S(g_i, g_j) \in \langle LT(g_1), \ldots, LT(g_n)\rangle$ for all i and j.*

Proof. If G is a Gröbner basis, then the leading term of any nonzero polynomial, and in particular the leading term of $S(g_i, g_j)$, may be written in terms of the leading terms of basis elements since any positive remainder may be reduced to a lower order one by subtracting some combination of elements of G to cancel the leading term.

To show the converse, we prove that any $f \in I$ may be written as a sum $\sum_{i=1}^{n} h_i g_i$ with $\max(\deg(h_i g_i)) = \deg(f)$. Certainly $\deg(f) \leq \max_i \deg(h_i g_i)$. Consider the expression for f as a sum $\sum_{i=1}^{n} h_i g_i$ minimizing the maximum degree δ. Suppose $\delta > \deg(f)$. Then f may be split into a sum of monomials of degree δ together with a sum of all remaining monomials of lower degree. Now the first sum fits the conditions of theorem 2.1.7 and so is expressible as $\sum_{i,j} x^{\delta-\gamma_{i,j}} S(g_i, g_j)$, a sum with maximum degree less than δ, and the second sum is defined to have maximum degree less than δ, so the overall maximum degree is less than δ, a contradiction. Hence f can be expressed in terms of $h_i g_i$ of degree at most $\deg(f)$, so $LT(f) = \sum_{i=1}^{n} LT(h_i g_i) \cdot s_i$ for $s_i = 1$ if $\deg(LT(h_i g_i)) = \deg(f)$ and $s_i = 0$ for $\deg(LT(h_i g_i)) < \deg(f)$. This means $\langle LT(f_1), \ldots, LT(f_n)\rangle = \langle LT(I)\rangle$, so G is a Gröbner basis. □

The process of extending a basis $g_1, \ldots, g_n$ by adjoining $S(g_i, g_j)$ until every $LT(S(g_i, g_j)) \in \langle LT(g_1), \ldots, LT(g_n)\rangle$ terminates, so we can use it to find a Gröbner basis.

Theorem 2.1.9 *The process of adding $S(f_i, f_j)$ to a basis $(f_1, \ldots, f_m)$ until every $LT(S(g_i, g_j))$ is expressible in terms of the $LT(f_i)$ terminates after a finite number of steps.*

PROOF. Clearly at each stage we are generating elements of our ideal by construction since we are taking combinations of elements of the ideal. The ideal $\langle LT(g_1) \ldots LT(g_m)\rangle$ is enlarged each time we add a new basis element $S(g_i, g_j)$ to G, so by the ascending chain condition on $k[x_1, \ldots, x_n]$, that is, the condition that any sequence of ideals each contained in the next must stabilize, the process of adjoining basis elements $S(g_i, g_j)$ terminates. Note that the ascending chain condition holds for polynomial rings by the Hilbert basis theorem which shows that every ideal of a polynomial ring has a finite basis. □

A Gröbner basis with respect to lexicographic order proves useful later because any element of our ideal which only involves some of the lower order variables will be expressible in terms of Gröbner basis elements which also only use these variables. It sometimes proves easier to find a basis for a polynomial ideal in $k[x_1, \ldots, x_n]$ by finding one for a larger, more easily defined ideal in $k[x_1, \ldots, x_n, y_1, \ldots, y_m]$ using more variables, constructing from this a Gröbner basis giving the extra variables higher order than the ones we are interested in preserving, and then using the elimination theorem, theorem 2.1.10 to find a Gröbner basis for the subset involving only the original variables.

Theorem 2.1.10 *If G is a Gröbner basis of I in $k[x_1, \ldots, x_n]$ with respect to lexicographic order with $x_1 > \ldots > x_n$, then $G \cap k[x_j, \ldots, x_n]$ is a Gröbner basis for $I \cap k[x_j, \ldots, x_n]$.*

PROOF. $G \cap k[x_j, \ldots, x_n] \subseteq I \cap k[x_j, \ldots, x_n]$, so we must show $G \cap k[x_j, \ldots, x_n]$ spans $I \cap K[x_j, \ldots x_n]$ and that for $g_k, g_l \in k[x_j, \ldots, x_n]$, $S(g_k, g_l)$ yields remainder 0 upon division by $G \cap k[x_j, \ldots, x_n]$. Every $f \in I$ may be written as a sum of $a_i g_i$ with $\deg(g_i) \leq \deg(f)$ for all i, so if $f \in I \cap k[x_j, \ldots, x_n]$, then each such g_i is in $k[x_j, \ldots, x_n]$, so $G \cap k[x_j, \ldots, x_n]$ spans $I \cap k[x_j, \ldots, x_n]$. Likewise, for $g_k, g_l \in G \cap k[x_j, \ldots, x_n]$, $S(g_k, g_l) \in I \cap k[x_j, \ldots, x_n]$, so $S(g_k, g_l)$ is expressible in terms of elements of $G \cap k[x_j, \ldots, x_n]$, and so $S(g_k, g_l)$ has remainder 0. $\square$

2.2 Using Gröbner Bases to Find a Set of Basic Moves for a Markov Chain

This section outlines results of Diaconis and Sturmfels found in [17]. Let X be a finite set and T a map from X to $\mathbb{Z}^d$. The set X can be viewed as the $n \cdot m$ variables representing the positions in $n \times m$ tables of nonnegative integers, and d as the number of constraints forced on the tables. Elements of X are actually tables with all zeroes except in one position, but it serves equally well to think of them as the actual positions. For our purposes, the map T takes an element $x \in X$ to the d-tuple which is 0 in the coordinates representing equations in which x plays no role and is 1 in the coordinates representing equations including one copy of x. For example, if the first constraint were $x_{1,1} + x_{1,2} + x_{1,3} = 5$ then T would take $x_{1,1}, x_{1,2}$ and $x_{1,3}$ to d-tuples beginning with a 1 but the other variables $x_{i,j}$ to d-tuples beginning with a 0.

A linear combination $\sum_{i,j} c_{i,j} \cdot x_{i,j}$ of elements of X will be in the kernel of T if and only if the move adding $c_{i,j}$ to position $x_{i,j}$ of a contingency table for each i and j preserves all our specified constraints. We want a simple set of basic moves that will allow us to move from any one legal table to any other in such a way that after each basic move we still possess a legal table. The reason a basis for the kernel of the matrix of constraints does not suffice is that the basis needs to be a $\mathbb{Z}$-basis, and although every legal move is a linear combination of basis elements of the kernel, it might be impossible to move from one legal table to another without somehow along the way allowing a table entry to be negative, i.e. temporarily leaving the space of legal tables.

Example 2.2.1 *In the linear algebra sense of a basis,*

$$\begin{pmatrix} + & - & 0 \\ - & + & 0 \end{pmatrix} \quad \textit{and} \quad \begin{pmatrix} 0 & + & - \\ 0 & - & + \end{pmatrix}$$

span the space of moves preserving row and column sums, but then to move from

$$\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \quad \textit{to} \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

requires an intermediate step to

$$\begin{pmatrix} 1 & -1 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

which is not a legal table.

These difficulties may be overcome by finding a Gröbner basis for an ideal including all tables with sums 0. Let g be a function from X to $\mathbb{N}$ which corresponds to the table with value $g(x)$ at position x for $x \in X$, and let $T(g) = \Sigma_{x \in X} g(x)T(x) = \Sigma_{x \in X}$ (value at position x in table) $\cdot$ (vector which is 1 in coordinates whose equations involve x and 0 elsewhere) $= (r_1, r_2, \ldots, r_n, c_1, \ldots, c_m, d_1, d_2)$. Legal moves correspond to tables g with $T(g) = 0$, i.e. they are tables which can be added without changing any of the sums to be preserved. We extend to the algebra $k[X]$ of polynomials whose variables are elements of X and associate to each function g on X a monomial $X^g = \prod_{x \in X} x^{g(x)}$ in the ring $k[X]$ of polynomials in the variables $x_{i,j}$. Since T is a map only on X, it must be extended to a map ϕ_T from $k[X]$; if T sends x to $(i_1, i_2, \ldots, i_d) \in \mathbb{Z}^d$, then let ϕ_T send x to $y_1^{i_1} \ldots y_d^{i_d}$. This means

$$\phi_T(X^g) \quad = \quad \sum_{x \in X} y_1^{g(x)T(x)_1} \ldots y_d^{g(x)T(x)_d}$$

$$= y_1^{\Sigma g(x)T(x)_1} \dots y_d^{\Sigma g(x)T(x)^d}$$
$$= y_1^{T(g)_1} \dots y_d^{T(g)_d}.$$

In the language of algebraic geometry, $\ker(\phi_T)$ is a toric ideal we denote by I_T.

Lemma 2.2.2 *The toric ideal I_T is generated by the monomial differences $X^{f^+} - X^{f^-}$ for functions f with $\sum_{x\in X} f(x)T(x) = 0$.*

PROOF. Let $I' = \langle\{X^{f^+} - X^{f^-} \mid \sum_{x\in X} f(x)T(x) = 0\}\rangle$. If $\sum_{x\in X} f(x)T(x) = 0$, then $\sum_{x\in X} f^+(x)T(x) = \sum_{x\in X} f^-(x)T(x)$, so $\phi_T(X^{f^+}) = \phi_T(X^{f^-})$ which means $I' \subset I_T$. Suppose there exists p such that $p \in I_T$ but $p \notin I'$, and hence I_T/I' is nontrivial. There exists some nonzero polynomial $p \in I_T/I'$ which is not a monomial since ϕ_T applied to a monomial never yields 0. In fact, since $k[X]$ is a polynomial ring and ϕ_T sends monomials to monomials, p must involve a pair of monomials with images that sum to 0 under the action of Φ_T. Choose such a p of minimal degree and let x^β be the leading term of p, then there is some term x^α of p such that $\phi_T(x^\beta) = \phi_T(x^\alpha)$. Rewrite $x^\beta - x^\alpha$ as $x^\gamma(x^{\beta'} - x^{\alpha'})$ for $\gamma_i = \min(\alpha'_i, \beta'_i)$ so that $x^{\beta'}$ and $x^{\alpha'}$ have no common factors. Since p is of minimal degree in I_T/I', $x^{\beta'} - x^{\alpha'} \in I'$, so we can subtract $x^\gamma(x^{\beta'} - x^{\alpha'})$ from p to obtain an equivalent element of I_T/I' of smaller degree, a contradiction to p being of minimal degree. This implies I_T/I' is empty so $I_T = I'$. □

Theorem 2.2.3 *A set of functions $f_1, \dots, f_n$ preserves a set of table constraints and connects the space of legal tables if and only if the monomial differences $\{X^{f_i^+} - X^{f_i^-}\}$ generate I_T.*

PROOF. The condition $\sum_{x\in X} f_i(x)T(x) = 0$ is equivalent to $\{X^{f_i^+} - X^{f_i^-}\} \subseteq I_T$ by the definition of T. Now we must show that $f_1, \dots, f_n$ connect the space if and only if the set $\{X^{f_i^+} - X^{f_i^-}\}$ generates the toric ideal I_T. Lemma 2.2.2 implies that $\{X^{f_i^+} - X^{f_i^-}\}$ generates I_T if it generates the set of $X^{f^+} - X^{f^-}$ such that $\sum_{x\in X} f(x)T(x) = 0$. Suppose $f_1, \dots, f_n$ connect two tables which differ by $f^+ - f^-$, so $f^+ - f^-$ may be written as $\sum_{j=1}^{A} \epsilon_j f_{i_j}$. The proof is by induction, so first note that if $f^+ - f^- = \epsilon_j f_{i_j}$ for some j and $\epsilon = 1$, then $f^+ = f_{i_j}^+$ and $f^- = f_{i_j}^-$ so that $X^{f^+} - X^{f^-} = X^{f_{i_j}^+} - X^{f_{i_j}^-}$ which is in the ideal, and for $\epsilon = -1$ simply switch $f_{i_j}^+$ and $f_{i_j}^-$. Assume for $m < A$ that $f^+ - f^- = \sum_{j=1}^m \epsilon_j f_{i_j}$ implies $X^{f^+} - X^{f^-} \in \langle\{X^{f_i^+} - X^{f_i^-}\}\rangle$. Note that if $f^+ - f^-$ can be written as $\sum_{j=1}^A \epsilon_j f_{i_j}$ then $f^- + \epsilon_1 f_{i_1}$ and f^- differ by a sum of fewer than A of the f_i and so $X^{f^- + \epsilon_1 f_{i_1}} - X^{f^-}$ is in the ideal. Likewise, $X^{f^+} - X^{f^- + \epsilon_1 f_{i_1}} \in \langle\{X^{f_i^+} - X^{f_i^-}\}\rangle$ since $f^+ - (f^- + \epsilon_1 f_{i_1}) = \sum_{j=2}^A \epsilon_j f_{i_j}$. Hence, $X^{f^+} - X^{f^-}$ is a sum of ideal elements and so is itself in the ideal.

Assume every $X^g - X^{g'} \in I_T$ is in $\langle\{X^{f_i^+} - X^{f_i^-}\}\rangle$ and therefore can be written as $\sum_{j=1}^A X^{h_r}(X^{f_{i_r}^+} - X^{f_{i_r}^-})$. If A is 1 then $g = h_r + f_{i_1}^+$ and $g' = h_r + f_{i_1}^-$, so $g - g' = f_i$, so g is connected to g' completing the base case of the induction. Suppose $X^g - X^{g'} = \sum_{r=1}^j X^{h_r}(X^{f_{i_r}^+} - X^{f_{i_r}^-})$ for $j \leq A-1$ implies g is connected to g'. We will show inductively this is true also for $j = A$ by eliminating one term from the sum to obtain an intermediate legal table, i.e. taking a step from g toward g' without leaving the space of legal tables. There is some k such that $X^{g'} = X^{h_k} X^{f_{i_k}^-}$ as $X^{g'}$ must appear as a term in the sum $\sum_{r=1}^j X^{h_r}(X^{f_{i_r}^+} - X^{f_{i_r}^-})$, so $g' - f_{i_k}^- = h_k$. This is nonnegative since X^{h_k} is the multiple of $X^{f_{i_k}^-}$ taken in expressing $X^g - X^{g'}$ as a linear combination of basis elements; since $g' + f_{i_k} = g' + f_{i_k}^+ - f_{i_k}^- = h_k + f_{i_k}^+$ which is nonnegative, note also that $g' + f_{i_k}$ is nonnegative. Subtracting $X^{h_k}(X^{f_{i_k}^+} - X^{f_{i_k}^-})$ from the sum $\sum_{r=1}^A X^{h_r}(X^{f_{i_r}^+} - X^{f_{i_r}^-})$ which equals $X^g - X^{g'}$, yields a sum of only $A - 1$ terms, but $(X^g - X^{g'}) - X^{h_k}(X^{f_{i_k}^+} - X^{f_{i_k}^-}) = X^g - X^{g' + f_{i_k}}$, and $g' + f_{i_k}$ is nonnegative, so the induction is complete. $\square$

This reduces the problem of finding basic moves connecting a space to that of finding a Gröbner basis for a toric ideal, and this follows directly from theorem 2.1.10, the elimination theorem, since $\langle\{x_{i,j} - Y^{T_{i,j}}\}\rangle \cap k[X] = I_T$, so if G is a Gröbner basis for $\langle\{x_{i,j} - Y^{T_{i,j}}\}\rangle$, then $G \cap k[X]$ is a Gröbner basis for $\langle\{x_{i,j} - Y^{T_{i,j}}\}\rangle \cap k[X]$.

The condition that $\{X^{f_i^+} - X^{f_i^-}\}$ connects I_T is equivalent to $\{X^{f_i^+} - X^{f_i^-}\}$ being a Gröbner basis for I_T. Given the standard definition of a Gröbner basis, we can reduce an ideal element to elements with smaller and smaller leading terms without having to introduce higher order terms and thus keeping exponents nonnegative at each step, so given any two ideal elements, we can find sequences of functions reducing these to 0 also yielding equal sums as in the condition that the f_i connect the space. The converse is the same argument reversed.

Buchberger's algorithm will yield a Gröbner basis, and we remove superfluous elements to obtain from this a reduced Gröbner basis. The result is a minimal basis such that the leading terms of the basis elements span the ideal generated by the leading terms of the original set. From this, we use the elimination theorem to obtain a Gröbner basis for $I \cap k[X]$. The reduced Gröbner basis is very nice in that it not only connects the space, but the paths between our functions, i.e. tables, will be of minimal length. These serve as basic moves for Markov chains.

Corollary 2.2.4 *A generating set for the space of legal moves between contingency tables is* $\{x_{ij} - Y^{T_{ij}}\}$.

PROOF. Simply note that $x_1^{\alpha_1} \dots x_n^{\alpha_n} - x_1^{\beta_1} \dots x_n^{\beta_n} = r_1^{\alpha_1} c_1^{\alpha_1} \dots r_n^{\alpha_n} c_n^{\alpha_n} - r_1^{\beta_1} \dots c_n^{\beta_n}$ in $k[X,Y]/\{x_{i,j} - Y^{T_{i,j}}\}$ and this equals 0 if and only if $\Phi(X^\alpha) = \Phi(X^\beta)$. □

Example 2.2.5 *The kernel of the space of legal moves on* 3×3 *tables with row and column constraints is generated by* $\{x_{11}-r_1c_1d_1, x_{12}-r_1c_2, x_{13}-r_1c_3d_2, x_{21}-r_2c_1, x_{22}-r_2c_2d_1d_2, x_{23}-r_2c_3, x_{31} - r_3c_1d_2, x_{32} - r_3c_2, x_{33} - r_3c_3d_1\}$. *Hence, the* r_i *represent row constraints, the* c_i *represent column constraints and the* d_i *diagonal constraints.*

2.3 Computing Gröbner Bases Without Introducing Extra Variables

DiBiase and Urbanke introduce another algorithm in [8] for computing a Gröbner basis for the kernel of a homomorphism, but by avoiding introducing extra variables to represent constraints, this algorithm may handle larger examples. Gröbner basis computations grow exponentially in work required as the number of variables increases, so minimizing variables is an important concern.

The method relies on a few observations we will prove following [8] after outlining the algorithm to compute a Gröbner basis for the kernel of a map π between polynomials in $k[x_1, \dots, x_n]$ and polynomials in $k[y_1, \dots, y_m]$. The polynomials in $k[x_1, \dots, x_n]$ represent tables while those in $k[y_1, \ldots, y_m]$ denote constraints. Let Φ map elements of $\mathbb{Z}^n$ to monomial differences by sending $(\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}^n$ to $x_1^{\alpha_1^+} \ldots x_n^{\alpha_n^+} - x_1^{\alpha_1^-} \ldots x_n^{\alpha_n^-}$ where $(\alpha_1, \ldots, \alpha_n) = (\alpha_1^+, \ldots, \alpha_n^+) - (\alpha_1^-, \ldots, \alpha_n^-)$ for $\alpha_i^+ = \max(\alpha_i, 0)$ and $\alpha_i^- = \max(0, -\alpha_i)$. The map π induces a map π_* from exponents of monomials in $k[X]$ to exponents of monomials in $k[Y]$ by letting $\pi_*(\alpha_1, \ldots, \alpha_n) = \log(\pi(x_1^{\alpha_1} \ldots x_n^{\alpha_n})) = (\beta_1 \ldots \beta_m)$ for $\pi(x_1^{\alpha_1} \ldots x_n^{\alpha_n}) = y_1^{\beta_1} \ldots y_m^{\beta_m}$.

Theorem 2.3.1 $\ker(\pi) = \langle \Phi(\mathit{ker}(\pi_*)) \rangle$.

Proof. This is a restatement of lemma 2.2.2 from the previous section. □

The approach of [8] hence seeks a Gröbner basis for $\langle \Phi(\ker(\pi_*)) \rangle$ since the result is also a Gröbner basis for $\ker(\pi)$. The first step is to find a $\mathbb{Z}$-basis K for $\ker(\pi_*)$ and apply Φ to it; this alone is not a basis for $\langle \Phi(\ker(\pi_*)) \rangle$ since $\langle \Phi(K) \rangle$ often does not equal $\langle \Phi(\mathrm{span}(K)) \rangle$ for a finite set K, but the set $\Phi(K)$ can be modified into a basis in a later step. If A is the matrix representation for π_* with respect to the natural choice of basis, the next step is to find a matrix U such that $AU = B$, the first $n - m$ columns of B are 0 and the last m columns form an m by m upper triangular submatrix of integer entries; the initial columns of U form a $\mathbb{Z}$-basis for $\ker(A)$ as is proved quite simply in [4]. U is obtained by converting A to B by elementary row operations and echoing the operations applied to the identity just as one would find the inverse of a matrix in Gaussian elimation.

The following pseudocode generates U. We modify the algorithm published in [4] and given below slightly to make sure we do not assume elements which could be 0 are nonzero. Before starting, reorder the rows so that the bottom row has nonzero entry in final position if possible, and before each step reorder remaining columns to make pivot nonzero if possible.

$k := n$ (pivot on last column)

for $i = m$ to 1 (i denotes row)

  for $j = n - 1$ to 1 (j denotes column)

    $d :=\gcd(a_{i,j}, a_{i,k})$ (will divide by d later to make entries smaller)

    $(x, y) :=$ sol'n to eq'n $a_{i,j} \cdot x + a_{i,k} \cdot y = d$ (use Euclid's algorithm, found in [4])

    column $j := \frac{a_{i,j}}{d}$col $k - \frac{a_{i,k}}{d}$col j (puts 0 at $a_{i,j}$ and integers in column j)

    column $k := x\cdot$old col $j + y\cdot$ old col k (puts d in position $a_{i,k}$)

$k := j$ (move pivot to column with only 0's below it)

do same column operations to U which is initialized to ID matrix

output columns of U corresponding to 0 columns of A as $\mathbb{Z}$-basis for $\ker(\pi_*)$.

The $\mathbb{Z}$-basis for $\ker(\pi_*)$ formed in the initial columns of U can be thought of as the rows of a new matrix. In algorithm 2.3.2 elementary row operations will yield a new $\mathbb{Z}$-basis for $\ker(\pi_*)$ such that each column of this new matrix is strictly nonnegative or strictly nonpositive. This corresponds to every basis element belonging to the same quadrant.

Algorithm 2.3.2 *First note that* 0 *is both nonnegative and nonpositive, so we need only be concerned with columns with some nonzero entries. The first row is made to have 0's only in columns which are strictly 0 by adding enough copies of some other row i with nonzero entry $a_{i,j}$ to make $a_{1,j}$ nonzero also; enough copies are chosen so that no first row entry already made nonzero becomes 0. Once the first row has 0 entries only in columns of all 0's, we may add such a large multiple of the first row to every row that every column has only entries of the same sign as in that position in the first row.*

The next step requires the notion of a reduced Gröbner basis.

Definition 2.3.3 *A reduced Gröbner basis is a Gröbner basis in which no element may be reduced by any other*

Theorem 2.3.7 will show that if $K \in \mathbb{N}^{r\times n}$, then $\langle\Phi(K)\rangle = \langle\Phi(\mathrm{span}(K))\rangle$ which means if the $\mathbb{Z}$-basis for $\ker(\pi_*)$ were an $\mathbb{N}$-basis, then the set $\langle\Phi(\mathrm{basis}(\ker(\pi_*)))\rangle$ already formed would equal $\langle\Phi(\ker(\pi_*))\rangle$ which is what we seek. We construct from the matrix with each column strictly nonnegative or strictly nonpositive a matrix in $\mathbb{N}^{r\times n}$ by multiplying nonpositive columns by -1, find a reduced Gröbner basis for the resulting matrix and then construct from this a reduced Gröbner basis for the original matrix.

We iterate the process of converting a column in the $\mathbb{N}$-matrix back to its original form by multiplying by -1 and deriving from the reduced Gröbner basis associated to the old matrix a reduced Gröbner basis associated to the matrix with this new nonpositive column.

Theorem 2.3.9 shows that if T_j is the action which multiplies column j by -1, then applying T_j to the elements of a reduced Gröbner basis for span(K) by acting on the associated row vectors yields a basis for span(T_jK). Buchberger's algorithm [5] will convert this to a reduced Gröbner basis so the process of acting by each needed T_j may be iterated until all nonpositive columns of A have been restored to nonpositive.

We now verify the assertions needed in this method. To preserve notation from [8], let m_p be the monomial that can be factored out of the monomial difference associated to p by Φ. Let u_p denote $\log(p^+) - \log(p^-)$ for p the difference of monomials $p^+ - p^-$ and let u_p^+ and u_p^- denote $\log p^+$ and $\log p^-$ respectively.

Lemma 2.3.4 *For $p = m_p\Phi(u_p)$ and $q = m_q\Phi(u_q)$ there is some monomial $m_{p,q} \in k[x_1, \ldots, x_n]$ such that $\frac{LCM(p^-,q^+)}{p^-}p + \frac{LCM(p^-,q^+)}{q^+}q = m_{p,q}\Phi(u_p + u_q)$.*

Proof. Note that

$$\begin{aligned}
\frac{LCM(p^-,q^+)}{p^-}p + \frac{LCM(p^-,q^+)}{q^+}q &= \frac{LCM(p^-,q^+)}{p^-}\left(p^+ - p^-\right) \\
&\quad + \frac{LCM(p^-,q^+)}{q^+}\left(q^+ - q^-\right) \\
&= \frac{LCM(p^-,q^+)}{p^-}p^+ - (LCM(p^-,q^+))\left(\frac{p^-}{p^-}\right) \\
&\quad + (LCM(p^-,q^+))\left(\frac{q^+}{q^+}\right) - \frac{LCM(p^-,q^+)}{q^+}q^- \\
&= \frac{LCM(p^-,q^+)}{p^-}p^+ - \frac{LCM(p^-,q^+)}{q^+}q^- \\
&= (LCM(p^-,q^+))\left(\frac{p^+}{p^-} - \frac{q^-}{q^+}\right) \\
&= (LCM(p^-,q^+))(x^{u_p^+ - u_p^-} - x^{u_q^- - u_q^+}).
\end{aligned}$$

Let $m_0 = LCM(p^-,q^+)$ and let $m_1 = m_0 \cdot x^{u_p^+ - u_p^- - (u_p + u_q)^+}$, so m_1 is a monomial in $k[x_1, \ldots, x_n]$. Note that $(u_p + u_q)^+ - (u_p + u_q)^- = (u_p^+ - u_p^-) + (u_q^+ - u_q^-)$, and hence observe that

$$(LCM(p^-,q^+))(x^{u_p^+ - u_p^-} - x^{u_q^- - u_q^+}) = m_0\left(x^{u_p^+ - u_p^-} - x^{-(u_q^+ - u_q^-)}\right)$$

$$
\begin{aligned}
&= \left(m_0 x^{u_p^+ - u_p^- - (u_p+u_q)^+}\right) \\
&\quad \cdot \left(x^{(u_p+u_q)^+} - x^{-u_p^+ + u_p^- + (u_p+u_q)^+ - (u_q^+ - u_q^-)}\right) \\
&= m_1 \left(x^{(u_p+u_q)^+} - x^{-(u_p^+ - u_p^-) + (u_p+u_q)^+ - (u_q^+ - u_q^-)}\right) \\
&= m_1 \left(x^{(u_p+u_q)^+} - x^{(u_p+u_q)^-}\right)
\end{aligned}
$$

Since $x^{(u_p+u_q)^+} - x^{(u_p+u_q)^-} = \Phi(u_p+u_q)$, note that $\frac{LCM(p^-,q^+)}{p^-}p + \frac{LCM(p^-,q^+)}{q^+}q = m_1\Phi(u_p+u_q)$. It remains to be shown that $\log(m_1) \in \mathbb{N}^n$. Recall $m_1 = LCM(p^-, q^+)x^{u_p^+ - u_p^- - (u_p+u_q)^+}$. Note that $\log(m_1)$ grows as m_p and m_q grow, so showing $\log(m_1) \in \mathbb{N}^n$ for $m_p = m_q = 1$ and applying induction suffices.

The following identities may be understood by thinking about what happens for each variable x_i which can also be thought of as a vector coordinate. Note, for instance, that $LCM(u_p^-, u_q^+) = u_p^- + (u_q^+ - u_p^-)^+$ because the right side is u_q^+ for coordinates in which $u_p^- < u_q^+$ and elsewhere $(u_q^+ - u_p^-)^+$ is 0 which makes $LCM(u_p^-, u_q^+) = u_p^-$. Hence,

$$
\begin{aligned}
\log(m_1) &= LCM(u_p^-, u_q^+) + (u_p^+ - u_p^- - (u_p+u_q)^+) \\
&= u_p^- + (u_q^+ - u_p^-)^+ + u_p^+ - u_p^- - (u_p+u_q)^+ \\
&= (u_q^+ - u_p^-)^+ + u_p^+ - (u_p+u_q)^+ \\
&= u_p^+ + (u_q^+ - u_p^-)^+ - (u_p+u_q)^+.
\end{aligned}
$$

Also note that $(u_p + u_q)^+ = (u_p^+ - u_q^-)^+ + (u_q^+ - u_p^-)^+$ since both sides equal $u_p + u_q$ in coordinates where u_p and u_q are both positive, both equal $u_p - u_q$ in coordinates where $u_p > 0$ and $u_q < 0$, both equal $u_q - u_p$ in coordinates where $u_p < 0$ and $u_q > 0$, and otherwise both are 0. Substituting $-(u_p^+ - u_q^-)^+$ for $(u_q^+ - u_p^-)^+ - (u_p+u_q)^+$ implies $\log(m_1) = u_p^+ - (u_p^+ - u_q^-)^+$, but $(u_p^+ - u_q^-)^+ \le u_p^+$ coordinatewise, and so $\log(m_1) \in \mathbb{N}^n$. □

Definition 2.3.5 *The support of a function is the subset of the domain which is not sent to 0.*

Corollary 2.3.6 *If $p = \Phi(u_p)$ and $q = \Phi(u_q)$ for $u_p, u_q \in \mathbb{Z}^n$ and if u_p^+ and u_q^- have disjoint support, then $\Phi(u_p + u_q)$ can be expressed in terms of $\Phi(u_p)$ and $\Phi(u_q)$.*

PROOF. By lemma 2.3.4, $x^z\Phi(u_p+u_q) = \frac{LCM(p^-,q^+)}{p^-}p + \frac{LCM(p^-,q^+)}{q^+}q$ for some $z \in \mathbb{N}^n$, and since $p = \Phi(u_p)$ and $q = \Phi(u_q)$, we need only show that $x^z = 1$. Recall that $z = u_p^+ - u_p^- + LCM\left((u_p^- + log(m_p)), (u_q^+ + log(m_q))\right) - (u_p+u_q)^+$, but $m_p = m_q = 1$ since $p = \Phi(u_p)$ and $q = \Phi(u_q)$, so $z = u_p^+ - (u_p^+ - u_q^-)^+$ by the same argument as in the proof of lemma 2.3.4 when we assumed $m_p = m_q = 1$. Since support(u_p^+) and support(u_q^-) are disjoint, u_q^- only contributes to terms of $u_p^+ - u_q^-$ not involving u_p^+, and then it contributes negative values, so $(u_p^+ - u_q^-)^+ = u_p^+$. Hence, $z = u_p^+ - u_p^+ = 0$, so $\Phi(u_p+u_q) = \frac{LCM(p^-,q^+)}{p^-}p + \frac{LCM(p^-,q^+)}{q^+}q = \frac{LCM(p^-,q^+)}{p^-}\Phi(u_p) + \frac{LCM(p^-,q^+)}{q^+}\Phi(u_q)$. □

Theorem 2.3.7 *If $K \in \mathbb{N}^{r\times n}$, then $\langle\Phi(K)\rangle = \langle\Phi(span(K))\rangle$.*

PROOF. Clearly $\langle\Phi(K)\rangle \subseteq \langle\Phi(\text{span}(K))\rangle$ since $K \subseteq \text{span}(K)$. Suppose $v \in \langle\Phi(\text{span}(K))\rangle$. This means v may be written as a sum of terms of the form $\Phi(\sum_{v_i\in K} a_i v_i)$ each of which is contained in $\langle\Phi(v_1),\ldots,\Phi(v_n)\rangle$ by corollary 2.3.6; the disjoint support condition of corollary 2.3.6 is satisfied since the term u_q^- is always 0 for vectors in $\mathbb{N}^n$. Hence, v is a sum of elements of $\langle\Phi(K)\rangle$, i.e. $v \in \langle\Phi(K)\rangle$. This means $\langle\Phi(\text{span}(K))\rangle \subseteq \langle\Phi(K)\rangle$, and so $\langle\Phi(K)\rangle = \langle\Phi(\text{span}(K))\rangle$. □

Theorem 2.3.8 *Let K be a $\mathbb{Z}$-basis. If G is a reduced Gröbner basis for $\langle\Phi(span(K))\rangle$, then $G \subseteq \Phi(span(K))$.*

PROOF. Every $g \in G$ may be written as a difference of monomials by lemma 2.3.4 since each g is an S-polynomial, the object defined for Buchberger's algorithm in section 2.1 and also the linear combination equal to $m_{p,q}\Phi(u_p+u_q)$ in lemma 2.3.4. If we may factor some nontrivial monomial $m_{p,q}$ out of this difference, then $g = m_{p,q}q$ for some q of lower order than g. Since $q \in \langle\Phi(U)\rangle$, a multiple of some element g' of G other than g can be subtracted from q to reduce it, so likewise g can be reduced by $m_{p,q}g'$, and this contradicts the assumption that G is reduced. □

Recall that T_j sends a matrix A in $\mathbb{Z}^{r\times n}$ to the matrix where the jth column of A is multiplied by -1. For a polynomial $p = \Phi(u)$, let $T_j(p) = \Phi(T_j u)$.

Theorem 2.3.9 *Let K be a set of r vectors in $\mathbb{Z}^n$ and choose U such that $U \subseteq span(K)$ such that U is finite and $\langle \Phi(U) \rangle = \langle \Phi(spanK) \rangle$. If G is a reduced Gröbner basis for $\langle \Phi(U) \rangle$ with respect to lexicographic order with $x_j > x_i$ for all $i \neq j$, then $\langle T_j(G) \rangle = \langle \Phi(span(T_j K)) \rangle$.*

Proof. If $g \in G$, then there exists $u \in \text{span}(K)$ such that $g = \Phi(u)$ by theorem 2.3.8, so $T_j g = \Phi(T_j u)$. Hence $g \in G$ implies $T_j g \in \Phi(\text{span}(T_j K))$ so $\langle T_j G \rangle \subseteq \langle \Phi(\text{span}(T_j K)) \rangle$.

Now assume $v \in \langle \Phi(U) \rangle$. Express v as $x_j^{\alpha_j} m_1 - p_1$ for m_1 and p_1 monomials in $[x_1, \ldots, x_{j-1}, x_{j+1}, \ldots, x_n]$; this is possible since $v = \Phi(u)$ for some $u \in U$, so it is a binomial with at most one term involving x_j. Likewise, there is some $g \in G$ which will reduce v as G is a Gröbner basis for $\langle \Phi(U) \rangle$ and since $g \in \Phi(U)$, g can also be written as $x_j^{\beta_j} m_2 - p_2$ for some m_2, p_2 monomials in $[x_1, \ldots k, x_{j-1}, x_{j+1}, \ldots, x_n]$ with $\beta_j \leq \alpha_j$ and m_2 dividing m_1. Note that $T_j v = m_1 - x_j^{\alpha_j} p_1$ and $T_j g = m_2 - x_j^{\beta_j} p_2$, so

$$\begin{aligned} T_j v &= m_1 - x_j^{\alpha_j} p_1 \\ &= \left(m_2 - x_j^{\beta_j} p_2\right)\left(\frac{m_1}{m_2}\right) + x_j^{\beta_j} p_2 \left(\frac{m_1}{m_2}\right) - x_j^{\alpha_j} p_1 \\ &= T_j g \cdot \frac{m_1}{m_2} + x_j^{\beta_j}\left(\left(\frac{m_1}{m_2}\right) p_2 - p_1 x_j^{\alpha_j - \beta_j}\right). \end{aligned}$$

Since $T_j g \in \langle T_j G \rangle$, if $\left(\frac{m_1}{m_2}\right) p_2 - p_1 x_j^{\alpha_j - \beta_j}$ is in $\langle T_j G \rangle$, then $T_j v \in \langle T_j G \rangle$. Since $\left(\frac{m_1}{m_2}\right) p_2 - p_1 x_j^{\alpha_j - \beta_j}$ is a lower order term than $T_j v$, induction implies every $T_j v$ is in $\langle T_j G \rangle$. Since $T_j v$ is an arbitrary element of $T_j \langle \Phi(U) \rangle$, and this equals $\langle \Phi(\text{span}(T_j(K)) \rangle$, $\langle \Phi(\text{span}(T_j K)) \rangle \subseteq \langle T_j G \rangle$ as desired.

$\square$

3 Computational Results

This section details how Markov chains were run and what results were obtained. Section 3.1 together with the first appendix discuss how to go about computing Gröbner bases used in Markov chains and when it is reasonable to do so. Section 3.2 describes the random number generator used since this can have a significant impact on results of Markov chains. We outline in section 3.3 how to compute expected deviation for different sample sizes to help in the analysis of results obtained and in choosing sample size. Section 3.4 gives a very brief description of the results most relevant to determining how fast our Markov chains should converge to the uniform distribution with respect to the diameter of the underlying connectivity graph; we also provide a bound on this diameter used to decide how many steps to run a Markov chain to generate each element of random sample. Pseudocode is provided in section 3.5 for running Markov chains and testing how many elements in a resulting sample belong to a subset to approximate what fraction of a larger space it occupies. Finally, section 3.6 lists results of Markov chain runs and compares these to some of the exact values being approximated.

3.1 Using Macaulay to Find a Set of Basic Moves

We use Macaulay to find a Gröbner basis corresponding to basic moves for a Markov chain. Maple and other software packages include the necessary functions, but Macaulay seems much faster and better able to handle large computations. Gröbner basis computations in general, and specifically using Macaulay, are very sensitive to the number of variables and the degrees of the polynomials involved, so it is important to take care to minimize these. One must input an initial basis for an ideal and from this a Gröbner basis, or standard basis, is computed. Macaulay requires polynomials in this initial basis to be homogeneous which adds to the rate at which the degree of the polynomials grow; for example, if $x_{1,1} - r_1c_1d_1$ were a basis element, then the variable $x_{1,1}$ would be given weight 3 and thereby increase the degree of all polynomials involving $x_{1,1}$.

In entering the ideal defined in terms of 25 variables for the 16 table positions, 4 row constraints, 3 column constraints and 2 main diagonal constraints, the computation just satisfied memory bounds of Macaulay. It computed a basis consisting of polynomials of degree at most 4, but because polynomials must be made homogeneous and because it must do further testing to be sure a Gröbner basis is complete, Macaulay in this case tests polynomials of degree up to 17, and the software package only allows polynomials of degree up to 20 when dealing with 25 variables. Simply including the redundant column constraint makes the computation too large since Macaulay has an internal bound related to the product of the number of variables and the maximum polynomial degree being tested. Some slight optimizations are discussed in [2], but probably more useful is a second technique discussed in 2.3 for computing Gröbner bases without introducing constraint variables; this should make larger examples feasible to compute.

A script instructing Macaulay to find a Gröbner basis for 4×4 magic squares may be found in the first appendix together with an explanation of the commands used. Located in the second appendix is the resulting basis of size 51 for the case where all 16 positions are free to move.

3.2 Choosing a Random Number Generator

Knuth suggests a random number generator for producing a long sequence of random bits quickly in [9]. This is especially useful in Markov chain simulation for deciding whether to choose a basic move or its negation.

This random number generator is based on a few facts about finite fields. If $\pi(x)$ is an irreducible polynomial in $\mathbb{Z}_p[x]$, then $(\mathbb{Z}_p[x])_{\pi(x)}$ is a finite field of size $p^{\deg(\pi(x))}$ with some element ξ of order $p^{\deg(\pi(x))} - 1$ generating the multiplicative group $(\mathbb{Z}_p[x])^*_{\pi(x)}$. If $p = 2$, then $x^{35} + x^2 + 1$ is irreducible, and for example every polynomial in $(\mathbb{Z}_2[x])_{x^{35}+x^2+1}$ can be represented by a string of 35 bits. Multiplication within the field of a polynomial in ξ by ξ corresponds to a leftshift followed by replacing any ξ^{35} term by $\xi^2 + 1$, i.e. adding mod 2 the lead bit with the new bits in positions 0 and 2. Since ξ is primitive, all $2^{35} - 1$ possible nonzero sequences are generated before repetition occurs, and so taking the lead bit at each step as a stream of random numbers yields quite good results assuming the sample size is much smaller than 2^{35} bits.

This random number generator alone will not suffice for choosing which basic move to use at each step of a Markov chain run since more than single bits are required to choose from as many as 51 basis elements and Knuth warns against concatenating bits to generate larger random numbers, so a C random number generator is used instead. It is not so important that this be an excellent random number generator as long as there is a reasonable chance of choosing each possible basic move. It is much more important that the decision of whether to take a move or its negation be very random, and so for this we use the random number generator described above and found in [9].

3.3 Computing Sample Size

Suppose a random sample is taken from a set A to approximate what fraction lies in a subset B. If $\dfrac{|B|}{|A|} = p$, then the binomial distribution measures the distribution of approximations to p since the likelihood that exactly k out of n things chosen in a sample will lie in B is clearly $\binom{n}{k} p^k (1-p)^{n-k}$. According to [12], the normal distribution may reasonably be used to approximate the binomial distribution for $np > 5$ and $n(1-p) > 5$, and this is easily satisfied in studying tables with row, column and main diagonal sums r by choosing n large enough since p and $1-p$ certainly never need to be smaller than $\frac{1}{r}$.

Let Z be a new random variable of normal probability distribution with mean 0 and variance 1, i.e. $N(0,1)$. Multiply this by the expected variance σ for the binomial distribution to achieve a nomal distribution approximation to the variance of a binomial random variable X from its mean p. Note that $\dfrac{X}{n} \approx p + \dfrac{\sigma Z}{n}$. Taking logs after factoring out a p on the right side yields

$$\log\left(\frac{X}{n}\right) \approx \log(p) + \log\left(1 + \frac{1}{p}\left(\frac{\sigma Z}{n}\right)\right).$$

Since $\log(1+\epsilon)$ is very close to ϵ for small ϵ, approximate $\log\left(\frac{X}{n}\right) - \log(p)$ by $\dfrac{1}{p}\left(\dfrac{\sigma Z}{n}\right)$. Hence,

$$\begin{aligned}
P\left(1-\epsilon < \frac{X/n}{p} < 1+\epsilon\right) &= P(\log(1-\epsilon) < \log(X/n) - \log(p) < \log(1+\epsilon)) \\
&\approx P(-\epsilon < \log(X/n) - \log(p) < \epsilon) \\
&\approx P\left(-\epsilon < \frac{1}{p}\left(\frac{\sigma Z}{n}\right) < \epsilon\right)
\end{aligned}$$

$$= \quad P\left(-\frac{(pn)\epsilon}{\sigma} < Z < \frac{(pn)\epsilon}{\sigma}\right).$$

We require $\frac{(pn)\epsilon}{\sigma}$ be 3 because then a chart in [12] analyzing $N(0,1)$ claims Z will lie in the acceptable range with probability 0.9944. Choose either a sample size n to be used and solve for ϵ, a bound on the expected error range, or choose an ϵ to see what sample size that degree of assured accuracy will require. Recall that for the binomial distribution $\sigma = \sqrt{np(1-p)}$, so the equations to be solved are

$$n = \frac{9(1-p)}{p\epsilon^2} \quad \text{and} \quad \epsilon = \sqrt{\frac{9(1-p)}{pn}}.$$

For example, when we later use samples of size 1000 to approximate p which is actually 0.6, note that $\epsilon = 0.077$, so there is a very high probability of not deviating from 0.6 by more than 0.077 if the Markov chain runs long enough for the sample collected to be from very nearly the uniform distribution.In our Markov chain run, the deviance was only 0.013.

3.4 Deciding How Many Steps are Needed to Generate Each Sample Element

Diaconis and Saloffe-Coste very recently showed in [7] that Markov chain runs on the kernel of totally unimodular matrices converge to a stationary distribution at a rate proportional to the square of the diameter of the underlying connectivity graph.

Definition 3.4.1 *A matrix is totally unimodular if the entries are all* 0 *or* ± 1 *and if the rows can be partitioned into two subsets* R_1 *and* R_2 *such that the sum of the rows in* R_1 *subtracted from the sum of the rows in* R_2 *is a row with entries all either* 0 *or* ± 1.

Note that contingency tables fit this model since they form the kernel of a matrix of constraints with rows which may be partitioned into two groups, those representing row constraints and those representing column constraints, and each column of this constraint matrix has a single 1 in each of the two groups since exactly one row constraint and one column constraint involves each table entry. To see this, note for example that the matrix of constraints for 3×3 tables is

$$\begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix},$$

where this is applied to a vector $(x_{1,1}, x_{1,2}, \ldots, x_{3,3})$.

Likewise, the problem of magic squares also fits this category since if one of the additional constraints is placed in one set of rows and the other constraint in the other collection of rows, the difference of the two sets will be the difference of these two rows each with entries of only 0 or 1, and so the new differences have absolute value at most 1.

Example 3.4.2 *The constraint matrix for* 3×3 *magic squares is*

$$\begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \end{pmatrix},$$

Hence, it would suffice to bound the diameter of the underlying graph for magic squares, except that the basic moves chosen for Markov chains run in this paper are not exactly the same as those very recently found and used for totally unimodular matrices in [7]. Nevertheless, it seems likely that the square of the diameter would be a reasonable bound for Markov chain convergence for the Gröbner basis moves too.

Theorem 3.4.3 *The diameter of the space of* $n \times n$ *magic squares with sums* r *is at most* $2r\left((n-1)^2 - (n-2)\right)$.

PROOF. Any two magic squares with the same row, column and main diagonal sums differ by an element of an ideal I where I is the kernel of the map sending tables of integers to monomial differences in $k[y_1, \ldots, y_{2n+1}]$ with $y_1, \ldots, y_{2n+1}$ representing the $2n+1$ table constraints. In particular, if

$$\begin{pmatrix} \alpha_{1,1} & \alpha_{1,2} & \ldots & \alpha_{1,n} \\ \ldots & \ldots & \ldots & \ldots \\ \alpha_{n,1} & \alpha_{n,2} & \ldots & \alpha_{n,n} \end{pmatrix}$$

can be written as a difference of matrices with nonnegative entries $\alpha^+_{i,j}$ and $\alpha^-_{i,j}$ respectively, then the map sends the matrix in α to $x_{1,1}^{\alpha^+_{1,1}} \cdots x_{n,n}^{\alpha^+_{n,n}} - x_{1,1}^{\alpha^-_{1,1}} \cdots x_{n,n}^{\alpha^-_{n,n}}$. Hence, reducing a monomial in $k[y_1, \ldots, y_m]$ by elements of a Gröbner basis for I corresponds to starting with a legal table and applying basic moves to it. It suffices then to show any two monomials differing by an element of I may both be reduced to the same unique remainder in $r(n-1)^2 - r(n-2)$ steps.

Note that at each step, we start with a monomial to be reduced, and since the Gröbner basis constructed consists only of differences of monomials, each reduction of a monomial yields a new monomial in which the highest order variable that needed to be reduced now has smaller exponent. In choosing the Gröbner basis, we ordered the variables $x_{i_1,j_1} < x_{i_2,j_2}$ if $i_1 < i_2$, or $i_1 = i_2$ and $j_1 < j_2$. Each of $(n-1)^2$ variables needs to be reduced in turn as these determine the other variable values, and the diameter is bounded by the sum of the amounts by which these variable are reduced. The $(n-1)^2$ positions to be reduced start with values no larger than r, and the sum of the end values is at least $r(n-2)$ since the last row and column which include variables not to be reduced have sum r. This means the sum of the magnitudes of all the reductions is at most $r(n-1)^2 - r(n-2)$, but since two tables must be reduced to the same remainder, the diameter is at most twice this. □

3.5 Simulating Markov Chains

A C program corresponding to the following pseudocode chooses from a set of basic moves to generate random tables, and approximates what fraction of these have a certain value in the first position. The same program together with the maximum subset of the Gröbner basis involving variables $x_{i,j}, \ldots, x_{n,n}$ will generate tables with fixed entries either $x_{1,1}, \ldots, x_{i,j-1}$

for $j \neq 1$ or $x_{1,1}, \ldots, x_{i+1,j}$ otherwise. This new basis is used for approximating what fraction of the tables have a specific value in position $x_{i,j}$ once earlier positions are fixed. Following is the main loop of the random walk program.

```
while (walkcount < TOTALSTEPS)
    {
    while (needtable)
        {
        needtable := FALSE /* assume at start new table will be legal */
        coinflip := getrand() /* random number generator taken from [9] */
        i := lrand48() mod  BASISSIZE /* choose random basis element */
        for count = 0 to TABLESIZE - 1
            {
            if (coinflip = HEAD)
              newtable[count]:=table[count]+basis[i] [count] /* do move */
            else newtable[count]:=table[count]-basis[i] [count] /* undo move */
            if (newtable[count] < 0)
              needtable := TRUE /* if negative entry then new table invalid */
            }
        walkcount := walkcount + 1 /*Increment number of tables visited. */
        if ((walkcount mod RANSTEP = 0) and (needtable = TRUE))
            if table[TESTPOSITION] = TESTVALUE
              incount:=incount + 1 /* test whether table lies in subset */
            else outcount:=outcount + 1 /* while sitting idle one step */
    }
    for  count = 0 to TABLESIZE - 1
        table[count]:=newtable[count]
    if  (walkcount mod RANSTEP = 0)
      if table[TESTPOSITION] = TESTVALUE /* test whether table lies in subset */
        incount:=incount + 1 /* after moving to new position */
      else outcount:=outcount + 1
```

In choosing which subset of the space of remaining tables to measure in the 4×4 case with sums 5, we fix more and more entries to values in the matrix

$$\begin{pmatrix} 2 & 1 & 1 & 1 \\ 1 & 1 & 1 & 2 \\ 1 & 2 & 1 & 1 \\ 1 & 1 & 2 & 1 \end{pmatrix}$$

since these seem likely to occupy nearly as large a fraction of the space as possible and approximations of larger subsets tend to be more accurate.

Hence, we approximate first what fraction of tables with sums 5 have a 2 in position $x_{1,1}$, and then what fraction of these also have a 1 in position $x_{1,2}$ and so on. In the case with sums 20, the table of all 5's serves as a good reference table from which to choose subsets since it is in some sense near the middle of the space of legal tables.

3.6 Numerical Results

We test the quality of Markov chain approximations in which we use the square of the diameter bound given in 3.4 or some multiple of it as the number of steps to take before assuming one is in any position with equal probability. Hence, if this bound is s, then once every s steps of the Markov chain we choose an element for a random sample.

We begin with an example with know exact ratio. Simple calculation shows that the number of 3×3 tables with row, column and main diagonal sums 6 is 13 and that 5 of these have a 2 in the upper left corner, so $\frac{5}{13} = 0.38461$ is the exact ratio of tables with a 2 in the upper left corner to all magic squares of sums 5.

The following table shows results of a random walk in which an item was chosen for the sample once every 1300 steps.

Tables with $x_{1,1} = 2$	Sample Size	Fraction	Deviance	Allowable Deviance
197	500	0.3940	0.0094	0.1697
398	1000	0.3980	0.0134	0.1200
1929	5000	0.3858	0.0012	0.0537
3865	10000	0.3865	0.0019	0.0379

The choice of 1300 steps is made because the diameter of the underlying graph is bounded above by $2r((n-1)^2 - (n-2)) = 36 \approx \sqrt{1300}$. as r in this case is 6 and d is 4.

The next table shows results of a random walk in which an item was chosen for the sample once every 5200 steps since there is an unknown constant involved in the growth rate, so we try four times the square of the diameter steps between sample elements.

Tables with $x_{1,1} = 2$	Sample Size	Fraction	Deviance	Allowable Deviance
188	500	0.3760	0.0086	0.1697
382	1000	0.3820	0.0026	0.1200
1946	5000	0.3892	0.0046	0.0537
3837	10000	0.3837	0.0009	0.0379

Now we test more thoroughly the affect of changing number of steps in another simple case. The next table shows results of a random walk in which an item was chosen for the sample once every 325 steps. The diameter bound is 18, so 325 is chosen as approximately the square of the diameter and used in the next run. The ratio being approximated in this case is actually 0.6.

Tables with $x_{1,1} = 2$	Sample Size	Fraction	Deviance	Allowable Deviance
155	250	0.6200	0.0200	0.1550
305	500	0.6100	0.0100	0.1096
616	1000	0.6160	0.0160	0.0775
3033	5000	0.6066	0.0066	0.0347
6043	10000	0.6043	0.0043	0.0245
15102	25000	0.6041	0.0041	0.0155

Trying a short Markov chain run, 50 steps per sample item, results are much better than expected.

Tables with $x_{1,1} = 2$	Sample Size	Fraction	Deviance	Allowable Deviance
149	250	0.5960	0.0040	0.1550
305	500	0.5980	0.0020	0.1096
595	1000	0.5950	0.0050	0.0775
3033	5000	0.6014	0.0014	0.0347
6043	10000	0.5994	0.0006	0.0245
15102	25000	0.5998	0.0002	0.0155

Using 1800 steps per sample item yields good approximations as well though surprisingly not as good as with 50 steps between sample items.

Tables with $x_{1,1} = 2$	Sample Size	Fraction	Deviance	Allowable Deviance
138	250	0.5520	0.0480	0.1550
292	500	0.5840	0.0160	0.1096
606	1000	0.6060	0.0060	0.0775
2966	5000	0.5932	0.0068	0.0347
6025	10000	0.6025	0.0025	0.0245
15026	25000	0.6010	0.0010	0.0155

Next we approximate in several stages to estimate the number of 4×4 tables with sums 5. Running 5000 steps between sample elements since the diameter bound is 70, we generate samples of size 4000 at each stage with the following results. Note that in this example the individual, actual values of p are unknown, so we use the estimates obtained for p to roughly approximate the allowable deviance.

Position Tested	Value	Tables with Value	Fraction	Allowable Deviance
$x_{1,1}$	2	770	0.1925	0.0971
$x_{1,2}$	1	1382	0.3455	0.0653
$x_{1,3}$	1	1576	0.3940	0.0588
$x_{2,1}$	1	1533	0.3833	0.0602
$x_{2,2}$	1	1785	0.4463	0.0528
$x_{2,3}$	1	1187	0.2968	0.0730

Since there are 3 tables satisfying all these conditions, multiplication of ratios gives an overall approximation of 2256 tables. A simple counting program reveals that the exact number of tables is 1904, so the ratio of this approximation to the actual value is 1.185. This is clearly better than the combined allowable deviances necessitate for high certainty.

Trying the same example, but with only 2500 steps per element of sample generated yields the following approximate ratios.

Position Tested	Value	Tables with Value	Fraction
$x_{1,1}$	2	767	0.1918
$x_{1,2}$	1	1356	0.3390
$x_{1,3}$	1	1605	0.4013
$x_{2,1}$	1	1503	0.3758
$x_{2,2}$	1	1827	0.4568
$x_{2,3}$	1	1152	0.2880

The corresponding estimate of 2327 tables is 1.222 times the actual number.

Again using 2500 steps between sample items, but with a much larger sample of size

40,000, the results are somewhat better.

Position Tested	Value	Tables with Value	Fraction
$x_{1,1}$	2	7943	0.1986
$x_{1,2}$	1	13616	0.3404
$x_{1,3}$	1	15428	0.3857
$x_{2,1}$	1	15220	0.3805
$x_{2,2}$	1	18210	0.4553
$x_{2,3}$	1	11991	0.2998

The estimate is 2215 tables which gives an improved ratio of 1.164.

In approximating the number of tables with sums 20 using a sample of size 1000 and taking 80,000 steps to generate each element of random sample as the diameter bound in this case is 280, the following estimates were obtained.

Position Tested	Value	Tables with Value	Fraction	Allowable Deviance
$x_{1,1}$	5	82	0.082	0.318
$x_{1,2}$	5	102	0.102	0.282
$x_{1,3}$	5	105	0.105	0.277
$x_{2,1}$	5	97	0.097	0.290
$x_{2,2}$	5	142	0.142	0.234
$x_{2,3}$	5	132	0.132	0.244

Since there are 121 tables in the subset with all the above values, this gives an approximation of 75 million magic squares with sums all equal to 20. Eric Rains conjectures the existence of a piecewise polynomial counting the number of magic squares which if correct would imply there are actually only about 5 million such magic squares and so the approximation is not very good. He tested this conjecture for $-12 \leq 0 \leq 8$ and so overdetermines the coefficients making the conjecture seem quite plausible.

Conjecture 3.6.1 *The number of* 4×4 *magic squares is*

$$f(r) = \begin{cases} \frac{(r+2)^3(r^4+8r^3+29r^2+52r+60)}{480}, & r \text{ even,} \\ \frac{(r+1)(r+2)(r+3)(r^2+6r+13)(r^2+2r+5)}{480}, & r \text{ odd.} \end{cases}$$

For $r > 0$, $(-1)^7 f(-r)$ *equals the number of such tables with only nonzero entries.*

The maximum allowable deviance estimate suggests a random sampling should yield approximations no more than 4 times the actual value for this size sample, and that would allow estimates of at most 20 million. Some error may arise when we use the sample fractions as approximations to p values in computing this allowable deviance, where perhaps these estimates do not yield exactly ϵ. Nevertheless, this estimate demonstrates that more work needs to be done in understanding this, that perhaps 80,000 steps is not enough to be in a random position in the space of tables, or maybe a better random number generator is needed.

For reference, the actual number of magic squares with sums up to 10 are listed in the next table. These were computed by a simple C program without any special optimization.

0	1	2	3	4	5	6	7	8	9	10
1	8	48	200	675	1904	4736	10,608	21,925	42,328	77,328

None of the included approximations ran for more than a few hours though perhaps the last example suggests obtaining good approximations when row and column sums are greater would be slow. There are, however, techniques for increasing the rate at which random walks converge such as scaling steps by larger constants, and this should help a great deal in larger examples.

4 An Approach to Obtaining Exact Answers for Testing Accuracy of Approximations

In section 4.1 we obtain a formula for counting 3×3 magic squares with sums r which allows us to measure the accuracy of simple approximations. Diaconis suggested also trying to generalize to magic squares a result of Stanley that the number of $n \times n$ magical squares of row and column sums r is a polynomial H_n in r of degree $(n-1)^2$ such that $H_n(r) = H_n(-n-r)$. The intent was to compute exact answers in small cases to determine the coefficients of the polynomial for a particular n and to use this to enumerate tables with larger sums. Restricting attention to magic squares eases the problem of exact counting and consequently gauging accuracy though approximations should work comparably on more general tables with extra constraints. Diaconis suggested perhaps this theorem would generalize to a result about magical squares with additional constraints $\sum_{i=1}^{n} a_{i,i} = \sum_{i=1}^{n} a_{i,n-i+1} = r$, but the key lemma of Stanley's proof is not true for magic squares. Section 4.2 surveys this proof explaining where it fails for magic squares. The theorem itself may actually generalize though not by the same argument.

Stanley views the space of tables with equal row and column sums as the intersection of finitely many half spaces comprising what is known as a convex polyhedral cone, and he uses the theory of linear homogeneous diophantine equations to count the lattice points in its interior. This theory is developed in Stanley's book, Enumerative Combinatorics, and we present much of it in section 4.2.

4.1 Enumerating 3×3 Magic Squares

Lemma 4.1.1 *If a 3×3 magic square has row, column and main diagonal sums s, then s is a multiple of 3.*

Proof. Denote the center entry of such a magic square by c and each sum by s. The sum of the two diagonals and the middle row is $3s$, but subtracting the three copies of the center entry from this sum yields the sum of the left and right columns, so $3s - 3c = 2s$ which implies $s = 3c$. Since c is an integer, s is a multiple of 3. □

Proposition 4.1.2 *There are $r^2+(r+1)^2$ magic squares with row, column and main diagonal sums $3r$.*

PROOF. We express the number of 3×3 magic squares with sums $3r$ in terms of the number of 3×3 magic squares with sums $3(r-1)$ and use induction. First note that there is one table of sum $3 \cdot 0$ and $1 = 0^2 + 1^2$. Assume there are $(r-1)^2 + r^2$ tables with sums $3(r-1)$. Obtain a bijection between the tables of sums $3(r-1)$ with nonnegative entries and the tables of sums $3r$ with strictly positive entries by simply adding the magic square of all 1's to each table of sums $3(r-1)$.

Next we show that there are $4r$ tables of sum $3r$ with some 0 entries. Note that the only legal basic moves are

$$\begin{pmatrix} 0 & + & - \\ - & 0 & + \\ + & - & 0 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} - & + & 0 \\ + & 0 & - \\ 0 & - & + \end{pmatrix},$$

and these connect the space of legal tables. This can be verified by observation or using Macaulay. Each move involves a sum of these two types of basic moves or their negations. Let m_1 and m_2 denote the number of respective basic moves of each type taken in moving from

$$\begin{pmatrix} r & r & r \\ r & r & r \\ r & r & r \end{pmatrix}$$

to another table. To make some entry 0 requires $|m_1| + |m_2| = r$ as this forces entry a_{12}, a_{21}, a_{23} or a_{32} to be 0. Since there are $4r$ solutions to $|m_1| + |m_2| = r$ in integers, we obtain $4r$ legal tables of sums $3r$ with some 0 entries. Since $(r-1)^2 + r^2 + 4r = r^2 + (r+1)^2$, the induction is complete. $\square$

4.2 Stanley's Theorem on Expressing the Number of Magical Squares as a Polynomial

First we present the key lemma that every magical square may be expressed as a sum of permutation matrices and show examples where both this and the weaker result Stanley requires fail when diagonal constraints are introduced and magic squares are studied. Hence, the picture is substantially more complicated by diagonal constraints. Stanley's proof found in [16] for magical squares is then divided into two sections, the first of which shows the number of $n \times n$ magical squares with row and column sums r is a polynomial in r and the second of which relates $H_n(r)$ to $H_n(-n-r)$ making it easier to obtain the polynomial by reducing the number of places it needs to be evaluated to be determined.

4.2.1 An Underlying Lemma which does not Generalize to Magic Squares

The $n \times n$ magical squares, also known as integer stochastic matrices, are solutions of the set of equations $\sum_{k=1}^{n} \alpha_{i,k} = \sum_{k=1}^{n} \alpha_{k,j}$ for $1 \leq i, j \leq n$. These equations specify that every row sum equals every column sum. From this, we use n^2 variables of the form $x_{i,j}$ to represent our n^2 positions and denote the magic square

$$\begin{pmatrix} \alpha_{1,1} & \alpha_{2,1} & \dots & \alpha_{n,1} \\ \dots & \dots & \dots & \dots \\ \alpha_{1,n} & \alpha_{2,n} & \dots & \alpha_{n,n} \end{pmatrix}$$

by $x_{1,1}^{\alpha_{1,1}} x_{1,2}^{\alpha_{1,2}} \dots x_{n,n}^{\alpha_{n,n}}$ which is sometimes written simply as x^{α}. Let E be the space of all magic squares, and for $\alpha = (\alpha_{1,1}, \alpha_{1,2}, \dots \alpha_{n,n})$ let $E(x)$ denote $\sum_{\alpha \in E} x_{1,1}^{\alpha_{1,1}} x_{1,2}^{\alpha_{1,2}} \dots x_{n,n}^{\alpha_{n,n}}$.

Lemma 4.2.1 *The coefficient of λ^r in $E(\underbrace{\lambda, \dots, \lambda}_{n}, 1, \dots, 1)$ counts the number of magical squares of sums r.*

PROOF. Substituting λ for $x_{1,1}, \dots, x_{1,n}$, and for $i > 1$ substituting 1 for $x_{i,j}$, then each magic square with $\alpha_{11} + \dots + \alpha_{1n} = r$, i.e. each magic square with sums r, contributes one copy of λ^r to the sum. Hence the coefficient of λ^r in $E(\underbrace{\lambda, \dots, \lambda}_{n}, 1, \dots, 1)$ is the number of magical squares with sums r. □

This allows us to first study $E(x)$ and then gain information about specific coefficients of $E(\underbrace{\lambda, \ldots, \lambda}_{n}, 1, \ldots, 1)$ to count the magical squares with sums r.

To study $E(x)$, we discuss a more general theory of solutions of systems of equations of the form $\sum_{i=1}^{m} a_i \alpha_i = 0$ for fixed a_i where in our case we have n^2 equations for the n^2 choices of $1 \leq i, j \leq n$ such that $\sum_{k=1}^{n} \alpha_{k,i} - \sum_{l=1}^{n} \alpha_{j,l} = 0$. We obtain a solution region in n^2 dimensional space with coordinates representing our n^2 table entries. This region includes the origin and any linear combination of solutions since these are still magical squares, but since all coordinates must be nonnegative, the solution region does not include any lines and hence comprises what is known as a pointed, convex polyhedral cone. The lattice points of this region correspond to the tables of nonnegative integers, so our problem is one of counting lattice points.

Stanley looks for a set of vectors whose convex hull is the space of all tables satisfying the constraints. A vector α belongs to the set of completely fundamental vectors $CF(E)$ for a fixed convex polyhedral cone E if $n\alpha = \beta + \beta'$ for $\beta, \beta' \in E$ implies β and β' are multiples of α. In the case of magical squares, he proves that the permutation matrices comprise $CF(E)$. Unfortunately, the completely fundamental elements of our space with added diagonal constraints are not so simply described; not every magic square with main diagonal sums equal to its row and column sums has some multiple of itself which can be decomposed into a sum of permutation matrices with a single 1 on each diagonal. For example,

$$\begin{pmatrix} 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 2 & 0 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 2 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 2 \\ 0 & 2 & 0 & 0 & 1 \\ 0 & 0 & 3 & 0 & 0 \end{pmatrix}$$

are completely fundamental elements once diagonal constraints are introduced.

No multiple of these can be broken into a sum of other elements of E, so they are in $CF(E)$. Nevertheless, we survey Stanley's proof for magical squares beginning by proving that for magical squares, $CF(E)$ consists of permutations. We first need a few tools from graph theory.

Definition 4.2.2 *A bipartite graph is a collection of edges E and vertices V which can be partitioned into V_1 and V_2 such that if $v_i, v_j \in V_1$ or $v_i, v_j \in V_2$, then $(v_i, v_j) \notin E$.*

Definition 4.2.3 *A perfect matching of a bipartite graph is a collection of edges such that each vertex in the graph is adjacent to exactly one edge in the collection.*

A perfect matching is a bijective correspondence between vertices of V_1 and V_2 where there is an edge between any vertex of V_1 and its counterpart in V_2. We will use the following well known result of graph theory about perfect matchings which is known as Hall's Theorem.

Theorem 4.2.4 *Any bipartite graph in which every $A \subseteq V_1$ is connected to at least $|A|$ vertices in V_2 has a perfect matching.*

PROOF. May be found in [3] $\square$

Theorem 4.2.5 *The set of completely fundamental elements are the permutation matrices.*

PROOF. First construct a bipartite graph from a magical square by creating a vertex in V_1 for each row and a vertex in V_2 for each column. If entry i, j of the magical square has value $a_{i,j}$, then place $a_{i,j}$ edges between $v_i \in V_1$ and $v_j \in V_2$. The result is a graph where every vertex has degree equal to the sum of every row and every column, and $|V_1| = |V_2|$. This graph satisfies the condition of Hall's Theorem, so we may remove a perfect matching, i.e. subtract a permutation from the magical square and are left with another graph satisfying Hall's condition. Hence, we may inductively decompose the magical square into permutations.

This implies only permutations may be in $CF(E)$, but clearly all permutations are in $CF(E)$. $\square$

4.2.2 Obtaining a Polynomial $H_n(r)$

We will use the resulting fact that for π a completely fundamental element, i.e. a permutation matrix, $1 - x^\pi = 1 - \lambda$ when we set x_{1j} to λ and $x_{i,j}$ to 1 for $i > 1$ in looking at $E(\underbrace{\lambda, \ldots, \lambda}_{n}, 1, \ldots, 1)$ since only one element of each column of π is nonzero so $\prod x_{i,j}^{\alpha_{i,j}}|_{(\lambda,\ldots,\lambda,1,\ldots,1)} = \lambda$.

Stanley's approach is to triangulate the solution region, prove results about pieces of the triangulation which are simpler to study and use these to obtain general results. This relation of regions will depend on Möbius function theory.

Definition 4.2.6 *An n-simplex is the convex hull of n points in space.*

Lemma 4.2.7 *A pointed convex polyhedral cone can be triangulated in such a way that the edges of the triangulation are the edges of the cone.*

Proof. If the dimension is 1 or 2, the cone cannot have more edges than the dimension, so the region is simplicial. Assume any cone can be triangulated with k extreme rays. If we add another ray, we can triangulate the new cone by taking the convex hull of each of the original simplices with our new ray to form new nonintersecting simplices which cover the cone, hence a new triangulation, and so by induction we can triangulate any cone with the edges of the cone equal to the edges of the triangulation. □

Let E_σ be the region $E \cap \sigma$ for $\sigma \in \Gamma$.

Proposition 4.2.8 *If Γ is a triangulation of E, then $CF(E) = \cup_{\sigma\in\Gamma} CF(E_\sigma)$.*

Proof. Any element $\alpha \in E$ on an extreme ray must be a multiple of some element of $CF(E)$ since otherwise some multiple of it could be written as $\alpha_1 + \alpha_2$ for $\alpha_1, \alpha_2 \in CF(E)$, but either α_1 or α_2 would not lie in our region unless both were along the same ray as α. Hence, $\{\beta \in E | \beta$ lies on an extreme ray, but $\beta \neq n\beta'$ for any $\beta' \in CF(E)$ and $n > 1\} \subseteq CF(E)$. The extreme rays of Γ are exactly the extreme rays of E according to lemma 4.2.7, so for $\sigma \in \Gamma$, $CF(E_\sigma) \subseteq \{\beta \in E | \beta$ lies on an extreme ray, but $\beta \neq n\beta'$ for any $\beta \in CF(E)$ and

$n > 1\} \subseteq CF(E)$ and so $CF(E_\sigma) \subseteq CF(E)$ which means the union is contained in $CF(E)$. The reverse inclusion follows from 4.2.7. $\square$

We next develop background about partially ordered sets, the Mobius function and generating functions to prove $E(\underbrace{\lambda, \ldots, \lambda}_{n}, 1, \ldots 1)$ is a rational function of degree < 0 with denominator $(1-\lambda)^t$ for some integer t.

Definition 4.2.9 *A poset, or partially ordered set, is a set X together with a relation $\leq$ satisfying the following properties.*

1. *For $x \in X$, $x \leq x$.*
2. *For $x, y \in X$, if $x \leq y$ and $y \leq x$, then $x = y$.*
3. *For $x, y, z \in X$, if $x \leq y$ and $y \leq z$, then $x \leq z$.*

As the term partially ordered set implies, not all elements are comparable, but the preceding properties give us the notion of chains of terms which can be compared. A poset may be pictured as a directed graph with no cycles in which a vertex is smaller than all its ancestors and larger than its descendents.

Definition 4.2.10 *A chain is a totally ordered subset of a poset.*

We will be concerned with posets of simplices. One simplex is contained in another if the set of vertices specifying the former is a subset of the vertices specifying the latter. Clearly, most simplices are not comparable. Conversely, from a poset we may construct a simplicial complex by creating a vertex for each element of the poset and an i-face for every i-chain so that the dimension of a face equals the length of the chain defining it.

Definition 4.2.11 *The Möbius function μ for a poset is defined by the following rules.*

1. $\mu(x, x) = 1$
2. $\mu(x, y) = -\sum_{x \leq z < y} \mu(x, z)$ *for $x < y$.*

Example 4.2.12 *If x is the point v_0 and y is the tetrahedron v_0, v_1, v_2, v_3, then $\mu(x, y) = 1-$number of edges including v_0+number of triangles including v_0, and this is -1 since $\sum_{keven} \binom{n}{k} - \sum_{kodd} \binom{n}{k} = (1-1)^n = 0$.*

A property of the Möbius function that we use next is the Möbius inversion formula proven in [16] which states that $g(x) = \sum_{y \leq x} f(y)$ if and only if $f(x) = \sum_{y \leq x} g(y)\mu(y, x)$.

Define $\overline{E}$ to be the subspace of E including only tables with strictly positive entries. More generally, let $\overline{E}_\sigma$ be the region within E_σ which excludes the boundary, i.e. $\overline{E}_\sigma = \{u \in E_\sigma : u \notin E_\tau \text{ for all } \tau \subset \sigma\}$.

We prove relations between generating functions for the regions $E, \overline{E}, E_\sigma$, and $\overline{E}_\sigma$. Studying E and $\overline{E}$ together and then relating them to each other will later yield the formula $H_n(-n-r) = \pm H_n(r)$.

Lemma 4.2.13 *The generating functions $E(x), \overline{E}(x), E_\sigma(x)$ and $\overline{E}_\sigma(x)$ satisfy the following equations.*

$$E(x) = -\sum_{\sigma \in \Gamma} \mu(\sigma, \hat{1}) E_\sigma(x).$$
$$\overline{E}(x) = \sum_{\sigma \in \Gamma} \overline{E}_\sigma(x).$$

Proof. By definition, $E(x) = \sum_{\alpha \in E} x^\alpha$, and for Γ a triangulation of E with $\sigma \in \Gamma$, $E_\sigma(x) = \sum_{\alpha \in E_\sigma} x^\alpha$. $E_\sigma(x) = \sum_{\tau \leq \sigma} \overline{E}_\tau(x)$, so by Mobius inversion

$$\overline{E}_{\hat{1}}(x) = \sum_{\sigma \leq \hat{1}} E_\sigma(x)\mu(\sigma, \hat{1}).$$

Since $\overline{E}_{\hat{1}}$ is the subset of E in no smaller simplex, and this is empty, $\overline{E}_{\hat{1}}(x) = 0$, so $\sum_{\sigma \leq \hat{1}} E_\sigma(x)\mu(\sigma, \hat{1}) = 0$. This implies $E_{\hat{1}}(x)\mu(\hat{1}, \hat{1}) + \sum_{\sigma < \hat{1}} E_\sigma(x)\mu(\sigma, \hat{1}) = 0$, so

$$-\sum_{\sigma < \hat{1}} \mu(\sigma, \hat{1}) E_\sigma(x) = \mu(\hat{1}, \hat{1}) E_{\hat{1}}(x) = E_{\hat{1}}(x) = E(x)$$

as desired. Also note that $\overline{E}_\sigma(x) \cap \overline{E}_\tau(x) = \emptyset$ for $\sigma, \tau \in \Gamma$ which means $\overline{E} = \cup_{\sigma \in \Gamma} \overline{E}_\sigma$, so $\overline{E}(x) = \sum_{\sigma \in \overline{\Gamma}} \overline{E}_\sigma(x)$. □

In examining regions of a lattice in proposition 4.2.14 and theorem 4.2.15, let $\{\alpha_i\}$ be a set of generators for the region such that $\gamma \in E$ implies there exists $n > 0$ and $a_1, \ldots, a_t \in \mathbb{Z}$ such that $\gamma = a_1\alpha_1 + \ldots + a_t\alpha_t$. Let R_E be the subregion of remainders, i.e. linear combinations of the α_i with coefficients all less than 1 whose sum is some $\gamma \in E$. Let $\overline{R_E}$ denote the related region with positive coefficients no larger than 1.

Proposition 4.2.14 *The generating functions* $E(x) = \sum_{\alpha \in E} x^\alpha$ *and* $\overline{E}(x) = \sum_{\alpha \in \overline{E}} x^\alpha$ *can be expressed as*

$$E(x) = \left(\sum_{\beta \in R_E} x^\beta \right) \prod_{i=1}^{t} (1 - x^{\alpha_i})^{-1}$$

and

$$\overline{E}(x) = \left(\sum_{\beta \in \overline{R}_E} x^\beta \right) \prod_{i=1}^{t} (1 - x^{\alpha_i})^{-1}.$$

PROOF. By the division algorithm, every $\gamma \in E$ can be written uniquely as $\beta + \sum_{i=1}^{t} a_i \alpha_i$ with $a_i \in \mathbb{Z}$ for all i and $\beta \in R_E$ is the remainder term. Likewise any $\gamma \in \overline{E}$ can be written uniquely as $\overline{\beta} + \sum_{i=1}^{t} a_i \alpha_i$ for $\overline{\beta} \in \overline{R}_E$ and each $a_i \in \mathbb{Z}$. This implies

$$E(x) = \left(\sum_{\beta \in R_E} x^\beta \right) \prod_{i=1}^{t} (1 - x^{\alpha_i})^{-1}$$

since each $x^\gamma \in E$ can be written uniquely as a monomial in

$$\left(\sum_{\beta \in R_E} x^\beta \right) \prod_{i=1}^{t} (1 + x^{\alpha_i} + x^{2\alpha_i} + \ldots)$$

and likewise,

$$\overline{E}(x) = \left(\sum_{\beta \in \overline{R}_E} x^\beta \right) \prod_{i=1}^{t} (1 - x^{\alpha_i})^{-1}.$$

$\square$

These expressions for $E(x)$ and $\overline{E}(x)$ are used to prove $E(\underbrace{\lambda, \ldots, \lambda}_{n}, 1, \ldots, 1)$ and $\overline{E}(\underbrace{\lambda, \ldots, \lambda}_{n}, 1, \ldots, 1)$ have denominator a power of $1 - \lambda$.

Theorem 4.2.15 *Let* $a_1, \ldots, a_m$ *be any collection of integers such that* $r \in \mathbb{N}$ *implies the number of solutions* $(\alpha_1, \alpha_2, \ldots, \alpha_m) \in E$ *to the equation* $a_1\alpha_1 + \ldots + a_m\alpha_m = r$ *is finite. Let* $g(r)$ *be the number of solutions and let* $G(\lambda) = \sum_{r \geq 0} g(r)\lambda^r$*. For* E *nonempty, the degree of the generating function* G *is negative.*

PROOF. Since $E(x)$ is expressible as a sum of terms $E_\sigma(x)$ by lemma 4.2.13, it suffices to show that the degree of $E_\sigma(\lambda^{a_1}, \ldots, \lambda^{a_m})$ is negative for $\sigma \in \Gamma$. By proposition 4.2.14,

$$E_\sigma(x) = \left(\sum_{\beta \in R_{E_\sigma}} x^\beta \right) \prod_{i=1}^{t} (1 - x^{\alpha_i})^{-1},$$

so this implies

$$E_\sigma(\lambda^{a_1},\ldots,\lambda^{a_m}) = \left(\sum_{\beta\in R_{E_\sigma}} (\lambda^{\beta_1})^{a_1}\ldots(\lambda^{\beta_m})^{a_m}\right)\prod_{i=1}^{t}(1-\lambda^{\alpha_i a_i})^{-1}.$$

Since each β may be written as $\sum_{i=1}^t \beta_i\alpha_i$ for some $\beta_i < 1$ with $\sum_{i=1}^t \beta_i a_i \le \sum_{i=1}^t \alpha_i a_i$, the degree of each term is negative. □

Lemma 4.2.16 *If $(\alpha_1,\ldots,\alpha_n) = 1$, then $1 - x^\alpha$ is irreducible.*

PROOF. If $a \in k$ for k a field and a not a pth power in k, then by a theorem in [10], $x^n - a$ is irreduible in $k[x]$. Let k be $k[x_1,\ldots,x_{n-1},\frac{1}{x_1},\ldots,\frac{1}{x_{n-1}}]$, then $1 - x^\pi$ can be rewritten as $\left(\frac{1}{x_1^{\alpha_1}\ldots x_{n-1}^{\alpha_{n-1}}} - x_n^{\alpha_n}\right)x_1^{\alpha_1}\ldots x_{n-1}^{\alpha_{n-1}}$, but $\frac{1}{x_1^{\alpha_1}\ldots x_{n-1}^{\alpha_{n-1}}}$ is not a pth power, so $\frac{1}{x_1^{\alpha_1}\ldots x_{n-1}^{\alpha_{n-1}}} - x_n^{\alpha_n}$ does not factor over $k[x_1,\ldots,x_{n-1},\frac{1}{x_1},\ldots,\frac{1}{x_{n-1}}]$ which implies $1-x^\pi$ does not factor in the smaller ring $k[x_1,\ldots,x_{n-1}]$, so $1 - x^\pi$ is irreducible. □

Theorem 4.2.17 *The generating functions $E(x)$ and $\overline{E}(x)$ are rational functions with denominator $\prod_{\alpha\in CF(E)}(1-x^\alpha)$ when written in lowest terms.*

PROOF. Theorem 4.2.13 gives an expression for $E(x)$ as $-\sum_{\sigma\in\Gamma}\mu(\sigma,1)E_\sigma(x)$ and for $\overline{E}(x)$ as $-\sum_{\sigma\in\overline{\Gamma}}\overline{E}_\sigma(x)$, so it suffices to note by 4.2.14 that $E_\sigma(x)$ and $\overline{E}_\sigma(x)$ have denominators $\prod_{\alpha\in CF(E_\sigma)}(1-x^\alpha)$ and $\prod_{\alpha\in CF(\overline{E}_\sigma)}(1-x^\alpha)$ respectively for each σ and to observe by 4.2.8 that $\cup_{\sigma\in\Gamma}CF(E_\sigma) = CF(E)$ for $\sigma\in\Gamma$, so the denominators $D(x)$ for the expression for $E(x)$ and $\overline{D}(x)$ for $\overline{E}(x)$ will be of the form $\prod_{\alpha\in CF(E)}(1-x^\alpha)$ as desired. If the expressions for $E(x)$ and $\overline{E}(x)$ with denominators $D(x)$ and $\overline{D}(x)$ are not in lowest terms, then some prime $P(x)$ divides $D(x)$, and in particular divides some term $1-x^\alpha$. Since $1-x^\alpha$ is irreducible by lemma 4.2.16, $P(x) = 1-x^\alpha$, so $E(x)$ may be reduced to $N'(x)/\prod_{\beta\neq\alpha}(1-x^\beta)$ for some $N'(x)$, but the left sum includes $x^{n\alpha}$ for every α while the right side may have only finitely many such terms since α is in $CF(E)$, so multiples of it are not expressible in terms of other elements of $CF(E)$; only finitely many $x^{n\alpha}$ may be found on the right side as increasing $n\alpha$ require greater and greater contribution from terms of the finite polynomial $N'(x)$ to obtain points further and further from the convex hull of $CF(E)-\{\alpha\}$. This yields a contradiction, and similar argument shows $\overline{E}(x)$ is as desired. □

Recall now that $CF(E)$ consists of permutations, so $E(\underbrace{\lambda,\ldots,\lambda}_{n},1,\ldots,1)$ has denominator some power of $1-\lambda$.

Hence theorem 4.2.15 shows that the degree of $E(\underbrace{\lambda,\ldots,\lambda}_{n},1,\ldots,1)$ is less than 0. Theorem 4.2.17 implies that $E(x)$ is rational with denominator $\prod_{\alpha\in CF(E)}(1-x^{\alpha})$ and so $E(\lambda^{a_1},\ldots,\lambda^{a_n})$ has denominator $(1-\lambda)^t$ for some t since $x^{\pi}|_{(\lambda,\ldots,\lambda,1,\ldots,1)}=\lambda$ for π a permutation. These facts together with 4.2.19 will imply that $H_n(r)$ is a polynomial. First we show the following from which 4.2.19 quickly follows.

Theorem 4.2.18 *Let $\alpha_1,\ldots,\alpha_d$ be complex numbers. The following conditions on generating functions are equivalent.*
1. $\sum_{n\geq 0} f(n)x^n=\frac{P(x)}{Q(x)}$ for $Q(x)=1+\alpha_1 x+\ldots+\alpha_d x^d$ with $P(x)$ of degree no more than $d-1$.
2. For all $n\geq 0$, $f(n+d)+\alpha_1 f(n+d-1)+\ldots+\alpha_d f(n)=0$.
3. For all $n\geq 0$, $f(n)=\sum_{i=1}^{k}P_i(n)\gamma_i^n$, for $\prod_{i=1}^{k}(1-\gamma_i x)^{d_i}=1+\alpha_1 x+\ldots+\alpha_d x^d$, $\gamma_i\neq\gamma_j$ for $i\neq j$ and $P_i(n)$ a polynomial of degree less than d_i.
4. $\sum_{n\geq 0} f(n)x^n=\sum_{i=1}^{k}G_i(x)(1-\gamma_i x)^{-d_i}$ for some $G_i(x)$ of degree less than d_i, where $1+\alpha_1 x+\ldots+\alpha_d x^d=\prod_{i=1}^{k}(1-\gamma_i x)^{d_i}$ for distinct γ_i.

PROOF. We show that the four vector spaces consisting of functions with these four properties have the same dimension and then show inclusions to prove that the properties are equivalent by showing that the vector spaces are the same. These vector spaces all have dimension d since the first is determined by the d coefficients of $P(x)$, the second by d consecutive values of f and the last two vector spaces by the d coefficients of the set of $P_i(n)$.

If $\sum_{n\geq 0} f(n)x^n=\frac{P(x)}{Q(x)}$, then $\sum_{n\geq 0} f(n)Q(x)x^n=P(x)$, so equating coefficients of x^{n+d} implies

$$f(n)\alpha_d+f(n+1)\alpha_{d-1}+\ldots+f(n+d)=0$$

as the degree of $P(x)$ is less than $n+d$, so $V_1\subseteq V_2$. By equality of dimensions, $V_1=V_2$. If

$$\sum_{n\geq 0} f(n)x^n=\sum_{i=1}^{k}G_i(x)(1-\gamma_i x)^{-d_i},$$

then the right sum may be written as

$$\sum_{i=1}^{k} \frac{G_i(x)\prod_{j\neq i}(1-\gamma_j x)^{d_j}}{\prod_{j=1}^{k}(1-\gamma_i x)^{d_i}} = \sum_{i=1}^{k} \frac{G_i(x)\prod_{j\neq i}(1-\gamma_j x)^{d_j}}{Q(x)},$$

but for V_4 we assume $d_j <$ degree of $G_i(x)$, so the numerator has degree less than d which implies $V_4 \subseteq V_1$. This implies $V_1 = V_4$. Now $\sum_{i=1}^{k} \frac{G_i(x)}{(1-\gamma_i x)^{d_i}}$ is a sum of terms of the form $x^j(-\gamma_i x)^n \binom{-d_i}{n}$ which equals $\pm x^{n+j}\gamma_i^n \binom{d_i+n-1}{n}$. Replacing $n+j$ by n implies

$$\begin{aligned} x^n \gamma_i^{n-j} \binom{d_i+n-1-j}{n-j} &= x^n \gamma_i^n \gamma_i^{-j} \binom{d_i+n-1-j}{d_i-1} \\ &= x^n \gamma_i^n \gamma_i^{-j} \binom{(d_i-1)+(n-j)}{d_i-1}, \end{aligned}$$

so the coefficient of x^n is a polynomial in n of degree $d_i - 1$, so $V_1 \subseteq V_3$ which means $V_1 = V_3$. Hence, $V_1 = V_2 = V_3 = V_4$. □

Corollary 4.2.19 *If $\sum_{n\geq 0} f(n)x^n = \frac{P(x)}{(1-x)^{d+1}}$ for P a polynomial of degree $\leq d$, then $f(n)$ is a polynomial of degree at most d.*

PROOF. If $Q(x) = (1-x)^{d+1}$, then condition 1 of theorem 4.2.18 is satisfied. This implies condition 3 is also satisfied, so $f(n) = \sum_{i=1}^{k} P_i(n)\gamma_i^n$ where each $P_i(n)$ has degree at most d, so $f(n)$ is a polynomial of degree at most d. □

Theorem 4.2.20 *The number of $n \times n$ magical squares is a polynomial in r of degree $(n-1)^2$.*

PROOF. Since $E(x)$ is rational of negative degree with denominator some power of $1-x$, and $E(\lambda^{a_1}, \ldots, \lambda^{a_m})$ has coefficients $H_n(\lambda)$, $H_n(r)$ is a polynomial.

Now we show it has degree $(n-1)^2$ by showing it grows with respect to r faster than any smaller degree polynomial and slower than any larger degree polynomial. First note that once the first $n-1$ positions in each row and column are chosen, the constraints specify the rest of the entries, so we have at most $r+1$ choices of value in each of $(n-1)^2$ table positions for at most $(r+1)^{(n-1)^2}$ possible tables, a polynomial in r of degree $(n-1)^2$. We need only fill in these $(n-1)^2$ positions subject to the constraints that the row and column sums be bounded above by r and the total of all $(n-1)^2$ entries be at least $(n-2)\cdot r$, so the entries in the last row and column are not forced to be negative. If we choose each entry between $\frac{n-2}{(n-1)^2}r$ and $\frac{n-1}{(n-1)^2}r$, then we find $\left(\frac{r}{(n-1)^2}\right)^{(n-1)^2}$ possible legal tables, and this grows faster than any polynomial in r of degree less than $(n-1)^2$. □

4.2.3 Relating $H_n(r)$ to $H_n(-n-r)$ to Compute $H_n(r)$ More Easily

Finally, we relate $E(X)$ to $\overline{E}(x)$ to show $H_n(r) = \pm H_n(-n-r)$, but proving 4.2.26 will require some algebraic topology, though it is not necessary to understand the proof to use the result, so the argument is only sketched.

Definition 4.2.21 *The Euler characteristic $\chi(K)$ of a simplicial complex K of dimension m is the alternating sum of the number of q-simplices, i.e. $\sum_{q=0}^{m}(-1)^q \dim(C_q(K,\mathbb{Z}))$ where C_q is the space of linear combinations of q-simplices of K with coefficients in $\mathbb{Z}$.*

For our purposes, $\dim(C_q(K,\mathbb{Z}))$ which we denote by f_q counts q-chains in the poset $P(K)$ corresponding to q-faces of the simplicial complex K. Treat $\emptyset$ as the unique (-1)-face, so that f_{-1} is to be interpreted as 1.

Definition 4.2.22 *The reduced Euler characteristic $\tilde{\chi}(K)$ equals $\sum_{q=-1}^{m}(-1)^q f_q$.*

Note that $\tilde{\chi}(K) = \chi(K) - 1$ in general. Now let $\mu_{\hat{P}}(\hat{0},\hat{1})$ be the Möbius function applied to P with minimal and maximal elements $\hat{0}$ and $\hat{1}$ adjoined. Let $\Delta(P)$ be the simplicial complex associated to P by sending q-chains to q-faces and for the next theorem let c_i be the number of i-chains including $\hat{0}$ and $\hat{1}$.

Theorem 4.2.23 $\mu_{\hat{P}}(\hat{0},\hat{1}) = \tilde{\chi}(\Delta(P))$.

Proof. The Möbius function can be defined as the inverse of the function ζ where

$$\zeta(x,y) = \begin{cases} 1 & \text{for } x \leq y \\ 0 & \text{otherwise} \end{cases}$$

so $(\zeta - 1)(x, y) = 1$ if $x < y$ and $(\zeta - 1)^q(x, y)$ counts the number of q-chains. This ζ is described further in [16] Note that

$$\begin{aligned}
\mu_{\hat{P}}(\hat{0}, \hat{1}) &= \zeta_{\hat{P}}^{-1}(0,1) \\
&= (1 + (\zeta_{\hat{P}} - 1))^{-1}(0,1) \\
&= \delta(\hat{0}, \hat{1}) - (\zeta_{\hat{P}} - 1)(0,1) + (\zeta_{\hat{P}} - 1)^2(0,1) - \ldots \\
&= c_0 - c_1 + c_2 - \ldots \pm c_{m+2} \\
&= 0 - f_{-1} + f_0 - f_1 + \ldots \pm f_m \\
&= \tilde{\chi}(\Delta(P)).
\end{aligned}$$

□

By definition $\tilde{\chi}(K) = \sum_{q=-1}^{m}(-1)^q$ rank $\tilde{C}_q$ where $\tilde{C}_q$ is the group of possible linear combinations of q-simplices, but this will imply $\tilde{\chi}(K) = \sum_{q=-1}^{m}(-1)^q$ rank $\tilde{H}_q$ where $\tilde{H}_q$ is the qth reduced homology group of the simplicial complex. Homology is a measure of the degree to which a sequence of maps δ fails to be exact, i.e. the amount $\ker(\delta_q)$ differs from $\mathrm{im}(\delta_{q+1})$. Let δ_q be a map from C_{q+1} to C_q sending $\langle p_0, \ldots, p_q\rangle$ to $\sum_{i=0}^{q}(-1)^i\langle p_0, \ldots, p_{i-1}, p_{i+1} \ldots p_q\rangle$; note that $\delta_{q-1}\delta_q = 0$. Denote $\ker(\delta_q)$ by Z_q and $\mathrm{image}(\delta_{q+1})$ by B_{q+1}, and then define $\tilde{H}_q$ to be Z_q/B_{q+1}. A simple and elegant proof that the reduced Euler characteristic is the alternating sum of the dimensions of the $\tilde{H}_q$ may be found in [13].

The advantage of this expression is that $\tilde{H}$ is invariant under choice of triangulation as is shown in [13]. In particular, reduced homology is preserved in moving to what is known as a barycentric subdivision for a simplicial complex.

Definition 4.2.24 *The barycentric subdivision of a simplicial complex K is a new simplicial complex which adds an additional point for each simplex of the original complex; each new vertex is positioned at the average of the vertices of the simplex specifying it, and edges are added connecting it to each vertex belonging to the boundary of its simplex.*

From the poset associated to a simplicial complex, a new simplicial complex may be constructed in which each element of the poset becomes a vertex and each q-face corresponds to a q-chain. The result is clearly the barycentric subdivision of the original simplicial complex. Computing $\mu(x, y)$ for corollary 4.2.26 corresponds to finding the reduced Euler characteristic of what is known as the link of F where F is a maximal set $\{x_1, \ldots, x_r, x, y, y_1, \ldots, y_s\}$ such that $x_1 < \ldots < x$ and $y < \ldots < y_s$.

Definition 4.2.25 *The link of a simplex s is the union of all simplices in K which are disjoint from s, but whose vertices together with those of s define simplices in K.*

Corollary 4.2.26 follows directly from the fact that the reduced homology of link(F) is simply that of either a ball or a sphere depending on whether F is in the boundary of K or not; the reduced homology of a sphere or a ball may easily be computed using a Mayer-Vietorus argument. Both this method and a discussion of the link may be found in [11].

Corollary 4.2.26 *If Γ is a triangulation and Γ' is the corresponding poset of inclusions which is graded of rank d, then*

$$\mu(\sigma, \tau) = \begin{cases} (-1)^{dim(\tau)-dim(\sigma)} & \textit{if } \sigma \leq \tau < 1 \\ (-1)^{d-dim(\sigma)+1} & \textit{for } \tau = 1 \textit{ and } \sigma \textit{ not in the boundary of } \Gamma \\ 0 & \textit{for } \tau = 1 \textit{ and } \sigma \textit{ in the boundary of } \Gamma \end{cases}$$

PROOF. Note that $\mu(\sigma, \tau)$ can be translated via the above discussion to the reduced Euler characteristic of the link of a simplex in a simplicial complex, and this is an alternating sum of reduced homology groups which in this case are equivalent to the reduced homology groups of either a sphere or a ball depending whether σ is in the boundary of the complex or not. An argument using a Mayer-Vietorus long exact sequence will show that the reduced homology groups of a sphere are all 0 except in dimension m where the reduced homology group is $\mathbb{Z}$and the reduced homology groups of a ball are all 0, so the result follows. $\square$

Lemma 4.2.27 $\overline{E}_\sigma(x) = (-1)^{\dim(\sigma)} E_\sigma(\frac{1}{x})$.

PROOF. Let d =dim(σ). By 4.2.14,

$$E_\sigma\left(\frac{1}{x}\right) = \left(\sum_{\beta \in R_E} x^{-\beta}\right) \prod_{i=1}^{t} (1 - x^{-\alpha_i})^{-1},$$

but $\sum_{\beta\in R_E} x^{-\beta} = (-1)^d \sum_{\beta\in R_E} x^{\alpha-\beta}$ since each $x^{-\beta}$ term corresponds to some $x^{\alpha-\beta}$ term, but with -1 applied to each of the d coordinates. Hence, $E_\sigma\left(\frac{1}{x}\right) = (-1)^d \left(\sum_{\beta\in R_E} x^{\alpha-\beta}\right)\prod_{i=1}^t(1-x^{-\alpha_i})^{-1} = (-1)^d\left(\sum_{\beta\in \overline{R}_E} x^{\beta}\right)\prod_{i=1}^t(1-x^{-\alpha_i})^{-1} = (-1)^d\overline{E}_\sigma(x) = (-1)^{\dim(\sigma)}\overline{E}_\sigma(x)$. □

Theorem 4.2.28 *If d is the dimension of the region containing E, then $\overline{E}(x) = (-1)^d E\left(\frac{1}{x}\right)$.*

PROOF. By 4.2.17, $E\left(\frac{1}{x}\right) = -\sum_{\sigma\in\Gamma}\mu(\sigma,1)E_\sigma\left(\frac{1}{x}\right)$, but then 4.2.26 implies

$$E\left(\frac{1}{x}\right) = -\sum_{\sigma\in\Gamma}(-1)^{d-dim\sigma+1}E_\sigma\left(\frac{1}{x}\right).$$

From this, 4.2.27 implies

$$\sum_{\sigma\in\Gamma}(-1)^{d-dim\sigma}E_\sigma\left(\frac{1}{x}\right) = \sum_{\sigma\in\overline{\Gamma}}\left((-1)^{d-dim\sigma}/(-1)^{dim\sigma}\right)\overline{E}_\sigma(x),$$

so

$$E\left(\frac{1}{x}\right) = \sum_{\sigma\in\overline{\Gamma}}(-1)^d\overline{E}_\sigma(x) = (-1)^d\sum_{\sigma\in\overline{\Gamma}}\overline{E}_\sigma(x).$$

Lemma 4.2.13 then expresses $(-1)^d\sum_{\sigma\in\Gamma}\overline{E}_\sigma(x)$ as $(-1)^d\overline{E}(x)$ as desired. □

Corollary 4.2.29 *The following are equivalent.*

1. $E\left(\frac{1}{x}\right) = (-1)^d x^\gamma E(x)$.

2. $\alpha\in E$ *if and only if* $\alpha+\gamma\in\overline{E}$.

PROOF. By 4.2.28, $E\left(\frac{1}{x}\right) = (-1^d)\overline{E}(x)$, so condition 1 implies $(-1)^d\overline{E}(x) = (-1)^d x^\gamma E(x)$ which in turn yields $\overline{E}(x) = x^\gamma E(x)$. Hence, the coefficients of x^α in $E(x)$ correspond to coefficients of $x^{\gamma+\beta}$ in $\overline{E}(x)$, so $\alpha\in E$ if and only if $\alpha+\gamma\in\overline{E}$. To show condition 2 implies condition 1, simply reverse all the implications. □

Proposition 4.2.30 *If f satisfies $\alpha_0 f(n+d)+\alpha_1 f(n+d-1)+\ldots+\alpha_d f(n) = 0$ for all $n\in\mathbb{Z}$ and for some complex set of α_i then $\sum_{n\geq 0} f(-n)x^n = -E\left(\frac{1}{x}\right)$.*

PROOF. Let $Q(x) = \sum_{i=0}^{d} \alpha_i x^i$, then note that $Q(x)\sum_{n\in\mathbb{Z}} f(-n)x^n = 0$ since the coefficient of x^n is $f(-n)+\alpha_1 f(-n-1)+\ldots+\alpha_d f(-n-d)$ which is 0. Since $Q(x)\sum_{n\in\mathbb{Z}} f(-n)x^n = 0$, note that $-Q(x)\sum_{n\leq 0} f(-n)x^n = Q(x)\sum_{n\geq 0} f(-n)x^n$ and hence observe

$$\begin{aligned} -Q(x)E\left(\frac{1}{x}\right) &= -Q(x)\sum_{n\geq 1} f(n)x^{-n} \\ &= -Q(x)\sum_{n\leq 0} f(-n)x^n \\ &= Q(x)\sum_{n\geq 0} f(-n)x^n. \end{aligned}$$

Cancelling $Q(x)$ yields $-E\left(\frac{1}{x}\right) = \sum_{n\geq 0} f(-n)x^n$ as desired. $\square$

Since corollary 4.2.29 implies $E(\frac{1}{\lambda}) = (-1)^d\lambda^n E(\lambda,\ldots,\lambda,1,\ldots,1) = (-1)^d\sum_{r\geq 0}\overline{H}_n(r)\lambda^r$, letting $H_n = f$ and using proposition 4.2.30 yields

$$\begin{aligned} \sum_{r\geq -n} H_n(-n-r)\lambda^{n+r} &= \sum_{r\geq -n} f(-n-r)\lambda^{n+r} \\ &= \sum_{r\geq 0} f(-r)\lambda^r \\ &= -E\left(\frac{1}{\lambda}\right) \\ &= (-1)^{d+1}\sum_{r\geq 0}\overline{H}_n(r)\lambda^r \\ &= (-1)^{d+1}\sum_{r\geq 0} H_n(r-n)\lambda^r \\ &= (-1)^{d+1}\sum_{r\geq -n} H_n(r)\lambda^{n+r}. \end{aligned}$$

Equating coefficients shows that $H_n(-n-r) = (-1)^{d+1}H_n(r) = (-1)^{deg(H_n(r))}H_n(r)$. For example, $H_2(r) = r+1$, and $H_2(2) = 3 = -H_2(-4)$. Now $\overline{H}_n(1) = \ldots = \overline{H}_n(n-1) = 0$ and $\overline{H}_n(r) = H_n(r-n)$, so $H_n(1-n) = \ldots = H_n(n-(1-n)) = 0$, and this implies $H_n(-1) = \ldots = H_n(-(n-1)) = 0$ so this gives several initial values of $H_n(r)$. From Stanley's proof presented above we conclude that $H_n(r)$ is a polynomial in r of degree exactly $(n-1)^2$ such that $H_n(-n-r) = (-1)^{d+1}H_n(r)$.

5 Conclusion

Approximate counting of magic squares by Markov chains yields answers comparable to what would be expected for a random sampling in small cases suggesting perhaps the square of the diameter is a sufficient number of steps to take to very nearly approximate the uniform distribution. However, a Markov chain run on tables with sums 20 gave an approximation which was 15 times the exact count assuming magic squares may be counted by a piecewise polynomial. If the sample were taken from the uniform distribution, the expected error would be not much more than 4 times the exact answer, so quite possibly running a Markov chain for 80,000 steps to generate each element of a random sample is not sufficient. The number of steps needed likely grows at a rate proportional to the square of the diameter of the underlying graph, and this is 80,000, but probably there is some constant factor involved which is larger than 1.

The algorithm of Diaconis and Sturmfels for computing a Gröbner basis was very easy to use and sufficed for the case of 4×4 magic squares, but it would be interesting to try the alternative algorithm of DiBiase and Urbanke to see if it actually handles larger cases well and is more efficient. It also remains to be proven that the number of $n \times n$ magic squares of sums r is a polynomial in r of degree $(n-1)^2$. This is probably true, though Stanley's proof for magical squares does not generalize to magic squares.

The assertion, that results about convergence rates for magic squares should be indicative of behavior on more general tables, deserves more careful examination before being fully accepted since the shapes of the spaces involved might be dramatically different. A more thorough and careful analysis of when samples taken from Markov chains give comparable approximations to those expected by uniform sampling might shed light on the constant factors involved in the number of steps needed for a Markov chain to converge to nearly the uniform distribution. It would be interesting to likewise study the behavior of Markov chains using the basic moves very recently introduced in the work of Diaconis and Saloffe-Coste, in which they show that some multiple of the square of the diameter suffices for achieving very nearly the uniform distribution in Markov chain runs on the kernel of totally unimodular matrices, a class of problems including contingency tables and magic squares. Most importantly, more work needs to be done to determine whether good approximations are actually more efficient than exact counting for larger examples, perhaps using more vigorous Markov chain moves.

A Macaulay Script

Macaulay may be obtained from math.harvard.edu by anonymous ftp. To output a Gröbner basis for the set of legal moves on 4×4 matrices with diagonal constraints, create a file such as one containing the following list of commands, begin Macaulay by typing "Macaulay"and then type filename $>$. The "monitor" command echoes results to the file 4d16.

```
ring R
25
d[1]d[2]r[1]-r[4]c[1]-c[3]x[1,1]-x[4,4]
1:9 3 2 2 2 2 3 3 1 2 3 3 1 3 2 2 2
w
c[3]
setring R
ideal z
16
r[1]c[1]d[1]-x[1,1]
r[1]c[2]-x[1,2]
r[1]c[3]-x[1,3]
r[1]d[2]-x[1,4]
r[2]c[1]-x[2,1]
r[2]c[2]d[1]-x[2,2]
r[2]c[3]d[2]-x[2,3]
r[2]-x[2,4]
r[3]c[1]-x[3,1]
r[3]c[2]d[2]-x[3,2]
r[3]c[3]d[1]-x[3,3]
r[3]-x[3,4]
```

```
r[4]c[1]d[2]-x[4,1]
r[4]c[2]-x[4,2]
r[4]c[3]-x[4,3]
r[4]d[1]-x[4,4]
std z y
putstd y
elim y n
monitor 4d16
putstd n
endmon
```

This creates a polynomial ring R in 25 variables d[1],d[2], r[1]-r[4],c[1]-c[3],x[1,1]-x[4,4]. The next line specifies weights for the variables chosen to make ideal elements homogeneous polynomials, i.e. polynomials with each term of the same degree. 1:9 means the first nine variables are assigned weight 1. Eventually, all variables up to c[3] will be eliminated, hence its listing before setring R. There are 16 ideal generators given from which a standard basis, i.e. a Gröbner basis, y is created. This file may easily be modified to other cases, but this computation approaches the limits of Macaulay's allowed memory. To obtain a partial basis for computations which are too large, begin file with "set autocalc 1", followed by "set autodegree x" for x the maximal degree polynomial to be found in any polynomial in the partial basis.

B Gröbner Basis

The following forms a Gröbner basis for $\langle x_{i,i} - r_i c_i d_1, x_{i,n-i+1} - r_i c_{n-i+1} d_2, x_{i,j} - r_i c_j$ for $j \neq i$ and $i + j \neq n + 1\rangle$.

$x_{3,3}x_{3,4}x_{4,1}x_{4,2} - x_{3,1}x_{3,2}x_{4,3}x_{4,4}$

$x_{2,4}x_{3,3}x_{4,2} - x_{2,2}x_{3,4}x_{4,3}$

$x_{2,4}x_{3,3}x_{4,1} - x_{2,3}x_{3,1}x_{4,4}$

$x_{2,4}x_{3,1} - x_{2,1}x_{3,4}$

$x_{2,4}^2x_{3,2}x_{3,3} - x_{2,2}x_{2,3}x_{3,4}^2$

$x_{2,3}x_{3,4}x_{4,2} - x_{2,4}x_{3,2}x_{4,3}$

$x_{2,3}x_{3,3}x_{4,2}^2 - x_{2,2}x_{3,2}x_{4,3}^2$

$x_{2,3}x_{3,1}x_{4,2} - x_{2,1}x_{3,2}x_{4,3}$

$x_{2,2}x_{3,4}x_{4,1} - x_{2,1}x_{3,2}x_{4,4}$

$x_{2,2}x_{2,4}x_{4,1}x_{4,3} - x_{2,1}x_{2,3}x_{4,2}x_{4,4}$

$x_{2,2}x_{2,3}x_{3,1}^2 - x_{2,1}^2x_{3,2}x_{3,3}$

$x_{2,1}x_{3,3}x_{4,2} - x_{2,2}x_{3,1}x_{4,3}$

$x_{2,1}x_{3,3}x_{3,4}x_{4,1} - x_{2,3}x_{3,1}^2x_{4,4}$

$x_{2,1}x_{2,4}x_{3,2}x_{3,3} - x_{2,2}x_{2,3}x_{3,1}x_{3,4}$

$x_{1,4}x_{3,3}x_{4,2} - x_{1,3}x_{3,2}x_{4,4}$

$x_{1,4}x_{2,4}x_{3,3}x_{4,3} - x_{1,3}x_{2,3}x_{3,4}x_{4,4}$

$x_{1,4}x_{2,2}x_{4,3} - x_{1,2}x_{2,3}x_{4,4}$

$x_{1,4}x_{2,2}x_{3,4}x_{4,2} - x_{1,2}x_{2,4}x_{3,2}x_{4,4}$

$x_{1,4}x_{2,2}x_{3,3}x_{4,1} - x_{1,1}x_{2,3}x_{3,2}x_{4,4}$

$x_{1,4}x_{2,2}x_{3,1} - x_{1,1}x_{2,4}x_{3,2}$

$x_{1,4}x_{2,1}x_{3,3} - x_{1,1}x_{2,3}x_{3,4}$

$x_{1,3}x_{4,2} - x_{1,2}x_{4,3}$

$x_{1,3}x_{3,4}x_{4,1} - x_{1,4}x_{3,1}x_{4,3}$

$x_{1,3}x_{2,4}x_{4,1} - x_{1,4}x_{2,1}x_{4,3}$

$x_{1,3}x_{2,4}x_{3,2} - x_{1,2}x_{2,3}x_{3,4}$

$x_{1,3}x_{2,2}x_{4,1} - x_{1,1}x_{2,3}x_{4,2}$

$x_{1,3}x_{2,2}x_{3,1} - x_{1,2}x_{2,1}x_{3,3}$

$x_{1,3}x_{2,1}x_{3,3}x_{4,1} - x_{1,1}x_{2,3}x_{3,1}x_{4,3}$

$x_{1,3}x_{1,4}x_{2,1}x_{2,2} - x_{1,1}x_{1,2}x_{2,3}x_{2,4}$

$x_{1,3}^2x_{2,2}x_{3,2} - x_{1,2}^2x_{2,3}x_{3,3}$

$x_{1,2}x_{3,4}x_{4,1} - x_{1,4}x_{3,1}x_{4,2}$

$x_{1,2}x_{3,3}x_{4,1} - x_{1,1}x_{3,2}x_{4,3}$

$x_{1,2}x_{2,4}x_{4,1} - x_{1,4}x_{2,1}x_{4,2}$

$x_{1,2}x_{2,4}x_{3,3} - x_{1,3}x_{2,2}x_{3,4}$

$x_{1,2}x_{2,3}x_{3,3}x_{4,2} - x_{1,3}x_{2,2}x_{3,2}x_{4,3}$

$x_{1,2}x_{2,3}x_{3,1} - x_{1,3}x_{2,1}x_{3,2}$

$x_{1,2}x_{2,2}x_{3,1}x_{4,1} - x_{1,1}x_{2,1}x_{3,2}x_{4,2}$

$x_{1,2}x_{1,4}x_{3,3}x_{4,3} - x_{1,3}^2x_{3,2}x_{4,4}$

$x_{1,2}x_{1,4}x_{3,1}x_{3,3} - x_{1,1}x_{1,3}x_{3,2}x_{3,4}$

$x_{1,1}x_{3,4}x_{4,3} - x_{1,3}x_{3,1}x_{4,4}$

$x_{1,1}x_{3,4}x_{4,2} - x_{1,2}x_{3,1}x_{4,4}$

$x_{1,1}x_{3,4}^2x_{4,1} - x_{1,4}x_{3,1}^2x_{4,4}$

$x_{1,1}x_{2,4}x_{4,3} - x_{1,3}x_{2,1}x_{4,4}$

$x_{1,1}x_{2,4}x_{4,2} - x_{1,2}x_{2,1}x_{4,4}$

$x_{1,1}x_{2,4}x_{3,4}x_{4,1} - x_{1,4}x_{2,1}x_{3,1}x_{4,4}$

$x_{1,1}x_{2,4}^2x_{4,1} - x_{1,4}x_{2,1}^2x_{4,4}$

$x_{1,1}x_{2,4}^2x_{3,2} - x_{1,4}x_{2,1}x_{2,2}x_{3,4}$

$x_{1,1}x_{2,3}x_{4,2}^2 - x_{1,2}x_{2,2}x_{4,1}x_{4,3}$

$x_{1,1}x_{1,4}x_{4,3}^2 - x_{1,3}^2x_{4,1}x_{4,4}$

$x_{1,1}x_{1,4}x_{4,2}x_{4,3} - x_{1,2}x_{1,3}x_{4,1}x_{4,4}$

$x_{1,1}x_{1,4}x_{4,2}^2 - x_{1,2}^2x_{4,1}x_{4,4}$

References

[1] M. Artin. *Algebra.* Prentice-Hall, 1991.

[2] T. Becker and V. Weispfenning. *Gröbner Bases.* Springer-Verlag, 1993.

[3] B. Bollobás. *Graph Theory: An Introductory Course.* Springer-Verlag, 1979.

[4] H. Cohen. *A Course in Computational Algebraic Number Theory.* Springer-Verlag, 1991.

[5] J. Little D. Cox and D. O'Shea. *Ideals, Varieties and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra.* Springer-Verlag, 1992.

[6] P. Diaconis and A. Gangolli. Rectangular arrays with fixed margins. *To appear in David Aldous, P. Diaconis, J. Spencer, ed., Proceedings IMA Conference on Monte Carlo and Markov Chains*, 1995.

[7] P. Diaconis and L. Saloffe-Coste. An analysis of rates of convergence of random walks on contingency tables. *Preprint*, 1995.

[8] F. DiBiase and R. Urbanke. An algorithm to calculate the kernel of certain polynomial ring homomorphisms. *Preprint*, 1994.

[9] D. Knuth. *The Art of Computer Programming, Volume 2: Seminumerical Algorithms.* Addison-Wesley Publishing Company, 1969.

[10] S. Lang. *Algebra.* Addison-Wesley Publishing Company, 1993.

[11] J. Munkres. *A Course in Algebraic Topology.* Addison-Wesley Publishing Company, 1984.

[12] J. Rice. *Mathematical Statistics and Data Analysis.* Wadsworth and Brooks, Cole, 1988.

[13] J. Rotman. *An Introduction to Algebraic Topology.* Springer-Verlag, 1988.

[14] A. Sinclair. *Algorithms for Random Generation and Counting: A Markov Chain Approach.* Birkhauser, 1993.

[15] R. Stanley. *Combinatorics and Commutative Algebra.* Birkhauser, 1983.

[16] R. Stanley. *Enumerative Combinatorics.* Wadsworth and Brooks, Cole, 1986.

[17] B. Sturmfels and P. Diaconis. Algebraic algorithms for sampling from conditional distributions. *Preprint*, 1993.