18.821 PROJECT 2: GENERATING MATRICES

ROGERS EPSTEIN, BEN MYERS, AND CONNOR SELL

1. Introduction

Generators and relations prove to be key to understanding many areas of math, most notably group theory. In this paper, we consider the case of dealing with generators and relations in the algebra of complex $n \times n$ matrices, looking at structures that come from these relations as well as how these relations interact with linear independence and what relations are attainable in this algebra.

Let M be the n^2 dimensional space of complex $n \times n$ matrices. Thus, $M \cong \mathbb{C}^{n^2}$. We are interested in calculating values for the following function:

Definition 1. *Given a pair of $n \times n$ matrices (X, Y), we define $d(X, Y) \in \mathbb{N}$ to be the smallest number such that the set of all monomials in X and Y of degree at most $d(X, Y)$ spans M, provided such a value exists.*

If $d(X, Y)$ exists, we say (X, Y) *generates* M. Of course, there are certainly (X, Y) that do not generate M (i.e. the pair of zero matrices, pairs of upper triangular matrices, etc.). We also show the nontrivial result that if $XY = YX$, then (X, Y) cannot generate M. Additionally, we generalize this to show that if X and Y both fix the same subspace of $\mathbb{C}^n$, then (X, Y) does not generate M.

One can also interpret $d(X, Y)$ as the lower bound of the highest degree monomial in any basis of M. For most of the approaches in the paper, we use the fact that a real basis (one such that the linear combinations of basis elements can only use real coefficients) of a real space is also a complex basis of the complexification of that space. This is a well-known result that we will not prove in this paper.

In studying this problem over different values of n, we wish to find functions of n, δ_n and Δ_n, such that $\delta_n \leq d(X, Y) \leq \Delta_n$. Our aim is to make these bounds as tight as possible.

In our research, we claim that the tightest such lower bound is $\delta_n = \lceil \log_2(n^2+1) \rceil - 1$ and the conjecture the tightest upper bound to be $\Delta_n = 2n - 2$. In later sections we give intuition through examples and results of computer simulation in order to reinforce the validity of these functions, as well as give a simple proof that $\Delta_n \leq n^2 - 1$.

Lastly, it will be useful to have a notion for how quickly the dimension of the space spanned by monomials under a given degree grows as we allow larger-degree monomials.

Definition 2. *For a given pair of matrices A, B, let $V_i \subset M$ be the linear space spanned by monomials of degree less than or equal to i in A, B. Then we define $g : \mathbb{Z}^+ \to \mathbb{Z}^+$ as $g(i) = \dim V_i - \dim V_{i-1}$.*

2. Examples

First, we look at some archetypal examples of matrices that display certain patterns. The intuition here is that both whether or not a pair of matrices will generate M and the rate at which it generates M is determined by what relations there are between monomials of the matrices.

First, consider an arbitrary matrix such as the 4×4 matrices below, which are randomly-generated integer matrices with elements between 0 and 100

$$R_1 = \begin{bmatrix} 89 & 91 & 30 & 80 \\ 75 & 20 & 43 & 88 \\ 6 & 74 & 15 & 64 \\ 81 & 21 & 96 & 52 \end{bmatrix}, R_2 = \begin{bmatrix} 77 & 27 & 64 & 57 \\ 79 & 0 & 28 & 19 \\ 67 & 0 & 43 & 7 \\ 5 & 17 & 73 & 89 \end{bmatrix}.$$

.

These in fact generate M with $d(R_1, R_2)$ being minimal. As we will discuss further in Section 4, random matrices usually minimize d, which is to be expected for the following reason. Namely, that given an arbitrary pair of matrices, we don't expect their monomials to have simple relations that reduce the number of distinct, linearly independent elements generated.

More precisely, monomials of two $n \times n$ matrices have "simple relations" between them if (X, Y) is a zero of some degree-n non-trivial two-variable polynomials with non-commuting variables and complex-valued coefficients). Such a relation would show certain monomials are linear combinations of monomials of lesser degree. This is unlikely unless we have some structure in our matrices.

The following table gives the results for these example cases. The degree refers to the the highest degree of monomials we allow, and the dimension is the dimension of the space spanned by monomials of the given degree or lower. Recall that $g(k)$, defined in the introduction, is simply the growth in the dimension of this spanned space at step k.

Growth for R_1 and R_2		
Degree	Dimension	g
1	3	2
2	7	4
3	15	8
4	16	1

We see very rapid growth, in fact exponential growth in the dimension (that is, $g(k) = 2^k$) as we increase the allowed degree of monomials. This means that as long as possible before exhausting M, the set of formally distinct monomials is linearly independent (since the total number of formally distinct monomials with non-commuting variables is easily seen to be 2^k). We can think about this in terms of relations between arbitrary pairs of matrices: most pairs will not have simple relations between them at all until necessary due to the limited size of M.

Setting aside arbitrarily-chosen examples, we consider a typical case where our matrices are chosen to have more structure. Let

$$A_4 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

.

In general, we can discuss A_n, the matrix with a 1 in the upper left corner of the matrix and zeros elsewhere.

For A_4, and in general for A_n, we have $A_n^k = A_n$. This gives us a simple relation that clearly decreases the number of linearly independent monomials of a given degree. One important effect of this is that it increases $d(A_n, \cdot)$ relative to $d(R, \cdot)$ where R is a matrix of the same size with little to no structure.

In this example, if we pair A_4 with the randomly generated matrix

$$R_3 = \begin{bmatrix} 81 & 61 & 3 & 80 \\ 48 & 22 & 24 & 88 \\ 16 & 20 & 39 & 20 \\ 64 & 75 & 15 & 2 \end{bmatrix}$$

we attain the following growth pattern.

Growth for A_4 and R_3		
Degree	Dimension	g
1	3	2
2	6	3
3	10	4
4	13	3
5	15	2
6	16	1

We see that the relations significantly slowed the growth rate of the dimension of the space spanned by monomials compared with the two randomly generated matrices.

3. Commuting Matrices and Other Non-Generators

Perhaps the simplest example of a non-commuting pair of matrices is a pair of diagonal matrices. Since all products and sums of diagonal matrices remain diagonal, such a pair can only generate diagonal matrices, not the entire space M. This is a special case of a more general result about commuting matrices.

Theorem 1. *Let X, Y be commuting, $n \times n$ matrices. Then X and Y do not generate M.*

Proof. In the appendix (Section 7), we give a well-known proof that if two matrices commute, then they are simultaneously (upper) triangularizable. That is, we can choose a basis under which A, B are both upper triangular. Choosing this basis, it's clear that A, B cannot generate M since the products and sums of upper triangular

matrices are upper triangular and therefore all linear combinations of monomials must have only zeros below the diagonal. The space spanned therefore cannot include M. □

Indeed, a yet more general result also holds. Namely, even if X and Y do not commute, then we can say that X and Y will not generate M if X and Y both fix some subspace $U \subset \mathbb{C}^n$.

Theorem 2. *Let X, Y be $n \times n$ matrices. Suppose there is a non-trivial subspace $U \subset \mathbb{C}^n$ such that both X and Y preserve U; that is, $X(U) \subset U$ and $Y(U) \subset U$. Then X, Y do not generate M.*

Proof. We show first that products and sums of matrices preserving U also preserve U. Since both X and Y preserve U, it's clear that

$$(XY)(U) \subset X(U) \subset U,$$

and similarly for other products, implying all products of X and Y preserve U.

Also for sums of matrices preserving U, we have that since U is a subspace,

$$(X + Y)(U) \subset X(U) + Y(U) \subset U.$$

Thus it follows that all linear combinations of monomials preserve U. However, since not all matrices in M preserve U, we conclude that X, Y do not generate M. □

4. Most Efficient Generators

Theorem 3. *If a pair (X, Y) generates M, then $d(X, Y) \geq \lceil \log_2(n^2 + 1) \rceil - 1$. We conjecture that this function is our desired δ_n.*

Proof. Note that there are exactly 2^d monomials of degree d, since there are 2 choices for the ith multiplicand (namely X and Y). This formula also holds for $d = 0$, as we are given the identity matrix. So, there are $\sum_{i=0}^{d} 2^i = 2^{d+1} - 1$ possible products to be obtained. Since M has dimension n^2, we require n^2 linearly independent monomials, so $2^{d+1} - 1 \geq n^2$. Also knowing that $d \in \mathbb{N}$, we can rearrange this inequality to get the one above. □

As mentioned in Section 2, in order to investigate when and how efficiently a matrix pair (X, Y) would generate M, we wrote a Python program that would generate "random" matrices according to certain parameters. These matrices were then multiplied to create monomials of degree up to n^2 in order to calculate the smallest monomial degree d needed to create a basis of M. In addition to seeing the distribution of attainable d, we want to see if the trivial lower bound achieved above is attainable as well, and thus show that this bound is δ_n.

These matrices were generated as follows: first, a positive integral upper bound u was specified along with the desired n. Then, each entry of the matrix was selected uniformly at random from the set $\{z \in \mathbb{Z} \mid 0 \leq z < u\}$. So, there were u^{n^2} possible matrices that could have been generated in any such trial.

Intuitively, smaller u would make it more "difficult" for the generated (X, Y) pair to generate M. This intuition comes from knowing that an $n \times n$ matrix with rank less than n will preserve proper subspaces of an n dimensional space, and thus not generate

M as shown in the last section. We tested this methodology again over several (u, n) pairs, generating $1,000$ or more matrix pairs in each case. The results support this way of thinking:

Proportion of Random Matrices that Generate M			
u	n = 2	n = 3	n = 4
2	39.8%	58.7%	78.8%
5	87.3%	98.4%	$\sim 100\%$
10	96.6%	99.9%	$\sim 100\%$

Importantly, "almost-generating" pairs (X, Y) form a basis of M using at most the degree that matches that trivial bound. It is apparent that if a pair (X, Y) generates M, but not within the trivial degree, then X and Y have some structure to them. So, we claim:

Conjecture 1. *δ_n is precisely equal to $\lceil \log_2(n^2 + 1) \rceil - 1$.*

Additionally, while "most" random matrices seem to generate M, "most" of these matrices generate M as efficiently as possible. Intuitively, this means that "most" choices for (X, Y) yield a generating pair that has no nontrivial (e.g. not $0X = 0$) relation of degree at most δ_n with at most n^2 monomials. In other words:

Conjecture 2. *The space of (X, Y) such that $d(X, Y) \neq \delta_n$ has measure 0.*

5. Least Efficient Generators

Next, we investigate the least efficient X and Y that generate a basis for M. More precisely, we want to maximize $d(X, Y)$. In other words, we want to know the largest degree d such that there exist matrices X, Y that generate M, but require monomials of degree at least d to do so.

We haven't proven that this is the highest degree possible, but we can present X and Y such that degree $d = 2n - 2$ is required. Consider the $n \times n$ matrices

$$X = \begin{bmatrix} 1 & & & \\ & & & \\ & & & \\ & & & \end{bmatrix}, \quad Y = \begin{bmatrix} & 1 & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \\ 1 & & & & \end{bmatrix}$$

X is the matrix with a 1 in the upper left corner, X_{11} the only nonzero entry. Y is a permutation matrix, with ones along the diagonal directly above the main diagonal, and a single one in the bottom left corner. This type of matrix is also known as a shift matrix.

We'll first show that X and Y generate a basis for M using monomials of degree at most $2n - 2$, and then that monomials of degree $2n - 2$ are required for such a basis.

Now in constructing the monomials of our basis, note that multiplication of a matrix on the left by Y shifts each of the rows up one, with the top row becoming the bottom row. Similarly, multiplying a matrix on the right by Y shifts each of the columns right one, with the rightmost column becoming the leftmost column. Thus we can repeatedly

multiply X on the left and right by Y to move the single nonzero entry to any given position in the matrix. To be precise, let the matrix with a single nonzero element in its ith row and jth column, with the nonzero element equal to 1, be denoted E_{ij}. Then we can generate E_{ij} as the monomial $Y^{n+1-i}XY^{j-1}$, with $n+1-i$ and $j-1$ taken modulo n.

Note that the set of such E_{ij} over all i and j is trivially a basis of M. We can construct these matrices with $Y^{n+1-i}XY^{j-1}$ as described above. The highest degree of any of these monomials is $2n-1$, when both $n+1-i$ and $j-1$ modulo n are equal to $n-1$, so that $i=2$ and $j=n$. But since we can express the shift matrix $Y^{n-2} = \sum_{k=1}^{n} E_{k,k-2 \pmod n}$, we can substitute I_n as a basis element instead of $Y^{n-1}XY^{n-1}$, and it has degree $n-2$ rather than $2n-1$. All other elements have degree at most $2n-2$, so we've given a basis generated by X and Y with degree at most $2n-2$.

Now we just need to show that any basis generated by X and Y requires an element of degree at least $2n-2$. Intuitively, we can't remove the monomials of degree $2n-2$ using the same method that we did to remove the monomial of degree $2n-1$, because there are two of them, and their corresponding nonzero entries occur in the same shift matrix. So we can remove one of them, but not the other.

Note that X is idempotent, or in other words, $X^2 = X$. Thus any monomial with two consecutive X's in its expansion is equal to a monomial of smaller degree. Furthermore, note that Y is a permutation matrix of a permutation of order n, so $Y^n = I_n$. So likewise, any monomial with Y^n in its expression is equal to a monomial of smaller degree.

Now suppose we have a monomial with at least two X's in its expansion. In order for it not to be equal to a monomial of smaller degree, there must be at least 1 but at most $n-1$ Y's between the X's. But note that XY^j is the matrix $E_{1,j+1}$, with the single nonzero element in the top row and $(j+1)$th column. If $j+1 \not\equiv 1 \pmod n$, then $XY^jX = 0$, since the column of the only nonzero entry in XY^j is not the row of the only nonzero entry in X. But $j+1 \equiv 1$ exactly when $j \equiv 0 \pmod n$. We assumed $1 \leq j \leq n-1$, so this can't happen. Thus, $XY^jX = 0$. So no matter what else is in this monomial, we're multiplying it by 0, so our monomial is equal to the zero matrix.

Thus we can't have X occur more than once in a monomial expansion or else either our monomial is 0 or equal to a monomial of lower degree. So what remains are the monomials in which it occurs once or not at all. Our remaining matrices are of the form Y^iXY^j or just Y^k. We already noted that $Y^iXY^j = E_{n+1-i,j+1}$, a matrix with a single nonzero element. Monomials of the form Y^k are powers of the shift matrix Y, so they are shift matrices as well.

Assuming the exponents of Y are less than n, we have n^2+n matrices remaining. We can split these into n sets of $n+1$ matrices, with each set S_k containing a single shift matrix Y^k and the E_{ij} with its nonzero entry in the same position as one of the 1's in Y^k. Note that for given k, these are the entries (i,j) such that $j-i \equiv k \pmod n$. In particular, for each set, the sum of the matrices of the form E_{ij} is the matrix of the form Y^k, so no set is linearly independent. We can remove the matrix of highest degree from each set, then, without removing any elements from its span. Then we can put the remaining n matrices from each set back together to get a basis for M.

Note in particular that $Y^{n-2}XY^{n-1} = E_{3,n}$ and $Y^{n-1}XY^{n-2} = E_{2,n-1}$ are in the same set S_{n-3} since $n-3 = (n-1)-2$.

Now, suppose we have a basis for M consisting of monomials of X and Y of degree less than $2n-2$. No basis elements can be zero, so if we repeatedly replace each monomial equal to a monomial of lower degree with the lower-degree monomial, until the monomial has no equal monomial of lower degree, we'll have a basis consisting of monomials of the form Y^k or Y^iXY^j.

Since all of the monomials have degree less than $2n-2$, neither $Y^{n-2}XY^{n-1}$ nor $Y^{n-1}XY^{n-2}$ can be in this basis. But then there are at most $n-1$ basis elements from S_{n-3}, and at least $n(n-1)+1$ basis elements from the other $n-1$ sets. Thus, by the pigeonhole principle, the basis must contain at least $n+1$ elements from some S_k. But this is impossible, since the $n+1$ elements in any given S_k are not linearly independent. Thus, our basis for M of monomials of degree less than $2n-2$ cannot exist.

Note that this argument holds for any n. So for matrices of any size, there must always exist X and Y that require a monomial of degree at least $2n-2$ to generate a basis for M. This is a lower bound, then, for how inefficient we can choose X and Y to be. Next, we'll prove an upper bound for this case.

5.1. **Proving Upper Bounds.** Although we've been unable to prove the $2n-2$ bound, we've made some progress towards a proof. To begin, we give a full proof that n^2-1 is an upper bound.

Theorem 4. *Given two $n \times n$ matrices X, Y generating M,*

$$d(X,Y) \leq n^2 - 1$$

Proof. To prove this upper bound, we'll look at the smallest values g can take stepwise. Suppose $g(k) = 0$ for some k. Then we'll show $g(k+1) = 0$.

Since $g(k) = 0$, any monomial α of degree k can be written as a linear combination $\alpha = \sum_i \beta_i$, where β_i are monomials of degree $k-1$ or less. Thus, $X\alpha, \alpha X, Y\alpha$, and αY can each be written as X or Y multiplied by a sum of monomials of degree $k-1$. This can be seen as follows: if $\alpha = \sum_i \beta_i$, then

$$X\alpha = X\sum_i \beta_i = \sum_i X\beta_i,$$

where $X\beta_i$ is a monomial of degree k or less. If indeed $X\beta_i$ is of degree k, then we can write it as a different linear combination $X\beta_i = \sum_j \gamma_j$, where γ_j is of degree $k-1$ or less.

Thus, since any monomial α' of degree $k+1$ can be written as $X\alpha, \alpha X, Y\alpha$, or αY for some α of degree k, we've shown that $g(k) = 0 \implies g(k+1) = 0$.

Thus, the slowest case imaginable becomes that where $g(k) = 1$ for all k as long as possible, since the dimension of this span must increase for each increase in k until it includes all of M. Recalling that $\dim M = n^2$ and that we have the identity matrix initially, we conclude that $d(X,Y) \leq n^2 - 1$, as desired. □

We think there is a stronger bound than this one. In fact, we have yet to discover any X and Y requiring degree more than $2n-2$. If we accept the following conjectures,

we can prove the sharp upper bound of $2n-2$. These conjectures are consistent with empirical data; we tested 10000 3×3 and 2×2 matrices with entries 0 or 1, and they held every time.

Conjecture 3. *If $g(k) > g(k+1)$, then $g(k+1) > g(k+2)$.*

Conjecture 4. *For all k with $g(k) > 0$, $g(k) \neq g(k+1)$.*

Intuitively, we can try to make each $g(k)$ as small as possible for each k to maximize the highest nonzero value of k. By Conjecture 4, each time we increment k, $g(k)$ must increase or decrease, but by Conjecture 3, whenever $g(k)$ decreases, it must continue to decrease until it reaches 0. Thus $g(k)$ monotonically increases until it reaches a single peak, and then monotonically decreases back to 0.

To maximize $d(X, Y)$, then, we increase $g(k)$ from 0 as slowly as possible, and then decrease it back down to 0 as slowly as possible. Since $g(k)$ must be an integer, this means increasing or decreasing $g(k)$ by 1. Thus, our sequence of values of $g(k)$ looks like this for some peak value r, in the best case:

$$1, 2, 3, \ldots, r-1, r, r-1, \ldots, 3, 2, 1$$

Note that since we start with $g(0)$, the last 1 must be $g(2r-2)$. Furthermore, we can find the total number of basis elements to be r^2. But we know that a basis of M must have exactly n^2 elements, so since n and r are both positive, $n = r$. Thus, $g(2n-2) = 1$, and we have $d(X, Y) = 2n-2$.

Any sequence of $g(k)$ values that has $g(2n-1) > 0$ and satisfies the conjectures must then correspond to a basis of more than n^2 elements, which is impossible.

6. Extensions

This is an interesting problem that can be approached in a number of ways. While it is difficult to immediately say if and how efficient a pair (X, Y) will generate M, more computer simulations might give more insights into the correct structures between X and Y to analyze.

For such an approach, it should be noted that the available rank functions in Python are merely estimations, which is why in this paper we limited our experiments to $n \leq 7$. Larger n resulted in Python returning incorrect values of the span of a given basis of $n^2 \times 1$ vectors.

It might also be interesting to try this problem not just in $\mathbb{C}$ or the related field of $\mathbb{R}$, but in general fields. An interesting place to start would be running these experiments in $\mathbb{Z}/p\mathbb{Z}$ for a given prime p. Since such structure would yield more relations between X and Y, it is conceivable that there is a larger upper bound on d as a function of p and n compared to the $\mathbb{C}$ case for the same n. However, while it is true that the lower bound δ_n still holds, it may no longer be strict in $\mathbb{Z}/p\mathbb{Z}$.

For a composite $m \in \mathbb{Z}$, one could also try this problem in $\mathbb{Z}/m\mathbb{Z}$, since this process does not require inverting any numbers or matrices. Generating pairs in this system will likely require more structure than the previous cases, since factors of m alone cannot generate $\mathbb{Z}/m\mathbb{Z}$.

7. Appendix

We include a well-known proof that commuting matrices are simultaneously triangularizable.

Theorem 5. *Let A, B be a pair of commuting $n \times n$ matrices with complex entries. Then there exists a basis under which both A and B are upper triangular.*

Proof. First we show that A and B have a common eigenvalue, then we show the rest inductively.

Since $\mathbb{C}$ is algebraically closed, we can find an eigenvalue-eigenvector pair (w, λ) for B. So $Bw = \lambda w$. Then

$$\begin{aligned} A(Bw) &= B(Aw) \\ \lambda Aw &= B(Aw) \end{aligned}$$

Thus, A leaves the eigenspace $E_{B,\lambda}$ invariant. In particular, we can restrict A to $E_{B,\lambda}$, and A will again, since $\mathbb{C}$ is algebraically closed, have an eigenvector. Let this common eigenvector be denoted v.

Thus, if we begin with v and add elements to form a basis $v, w_1, w_2, \ldots, w_{n-1}$, then A and B are of the following form

$$A = \left[\begin{array}{c|c} \lambda & * \\ \hline 0 & A' \end{array}\right]$$
$$B = \left[\begin{array}{c|c} \lambda & * \\ \hline 0 & B' \end{array}\right].$$

Now since

$$\left[\begin{array}{c|c} \lambda^2 & * \\ \hline 0 & A'B' \end{array}\right] = AB = BA = \left[\begin{array}{c|c} \lambda^2 & * \\ \hline 0 & B'A' \end{array}\right],$$

we conclude that $A'B' = B'A'$. So we can continue this process on lower dimensions. A simple inductive argument on the dimension n of the matrices will suffice. (Note that the $n = 2$ case gives a very easy base case.) □

8. Who Did What

Ben started writing the code, but Rogers developed most of it over break. Then, everyone had the chance to experiment with different starting (X, Y) in order to see what possible d's could be achieved, although Connor worked more on rigorously proving the bounds that Rogers and Ben found experimentally.

In terms of sections, Ben was the primary contributor of the "Examples", "Commuting Matrices and Other Non-Generators", and the brief Appendix; he also helped a bit with the subsection "Proving Upper Bounds." Connor wrote most of the "Least Efficient Generators" section. Rogers helped with the introduction, and wrote the "Most Efficient Generators" and "Extension" sections.