COEFFICIENTS OF GAUSSIAN POLYNOMIALS MODULO N

DYLAN PENTLAND

1. Research experience

I have always been interested in numbers and patterns, although I was not seriously interested in mathematics until I was in middle school. During that time period, I discovered that there was more to math than just carrying out calculations or solving equations. I had a particularly engaging math class in 7th and 8th grade and I remember one problem about an 8x8 chessboard with the opposing corners removed. Suppose you want to tile this chessboard with dominoes – even though there are an even number of squares left, this tiling is actually impossible. I was astonished by how simple the proof was: every domino covers both a black and a white tile. Thus, if you want to cover a subset of the board with dominoes it must have equal numbers of black and white tiles. When you remove opposite corners, this is no longer the case.

This type of thinking opened my eyes to how powerful mathematics can be. Sometimes, a simple insight can turn a seemingly impossible problem into an easy one. Different areas of mathematics are full of amazing insights just like the chessboard problem, and when these ideas are combined they allow you to solve problems that seemed unreachable before.

As I entered high school I became interested in learning about different areas of mathematics but I was also interested in the research process. It was one thing to read about mathematics, but what was inventing it like?

Eventually, this path led me to the MIT PRIMES program where I was paired up with a graduate student to work on a project in combinatorics. The problem I worked on was a conjecture by Prof. Richard Stanley about q-binomial coefficients, and generalization of binomial coefficients. Fortunately, we did not have to spend much time on background material since I had already read [Sta12] the previous year and I was able to jump into

the project. My mentor had me read through some related papers concerning the topic so that I got a good sense of the area and which directions people were interested in exploring. One of the motivations for the project came from the Kronecker coefficients $g_{\mu\nu}^{\lambda}$ (see [Man15]), so I also read some material on the representation theory of S_n.

Initially, most of my attempts at resolving the conjecture were misguided and I did not make much progress. I decided to focus on edge cases where I could work out some explicit formulas for the coefficients and study the residues modulo N, hoping that I could make some progress there that would help with the larger problem. I found it extremely helpful to use Sage to create programs which would output the residues I was interested in. This dramatically sped up the process of catching errors, and also allowed me to spot interesting patterns that hinted at the path to a proof of the conjecture. My work on edge cases eventually proved useful, since the main technique of my proof was to use the edge case to inductively build up a certain periodic decomposition of the residues. Once this was done, I had a powerful theorem describing the exact structure of the residues which made proving many of my earlier conjectures (and the main conjecture) much easier.

2. Project details

2.1. **What are q-binomial coefficients?** My project was in 'enumerative combinatorics', which has to do with finding ways to enumerate or count the number of objects in sets or sequences of sets.

The exact problem I was working on involved coefficients of a type of polynomial called a q-binomial coefficient, denoted by $\begin{bmatrix} n \\ k \end{bmatrix}_q$. The name and notation is not a coincidence – these polynomials are intended to generalize binomial coefficients in the sense that when the polynomial $\begin{bmatrix} n \\ k \end{bmatrix}_q$ is evaluated at $q = 1$ we obtain the binomial coefficient $\binom{n}{k} = \frac{n!}{k!(n-k)!}$. We can define these by the rational expression

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \frac{[n]!}{[n-k]![k]!},$$

where $[n]! = \prod_{i=1}^{n} (1-q^i)/(1-q)$. Note here that $(1-q^i)/(1-q) = 1 + q + \ldots q^{i-1}$, so at $q = 1$ we obtain i – this makes is clear that evaluating $\begin{bmatrix} n \\ k \end{bmatrix}_q$ at 1 returns $\binom{n}{k}$. These polynomials in the fraction cancel nicely when simplified, and we are left with

a polynomial in q of degree $k(n-k)$. These types of generalizations are known as q-analogues in combinatorics.

One useful perspective to see why these are a good generalization of binomial coefficients has to do with finite fields. The is also the origin of the convention to use q as the variable instead of x. Informally, a field is set of objects with two operations $+, \times$ which behave similarly to the same operations on $\mathbb{Q}$. One of the most important properties is the existence of multiplicative inverses for nonzero elements. Here, 'zero' refers to the element e so that $a + e = a$ for all a, which is provably unique.

While the most obvious examples, like $\mathbb{Q}$, are infinite, there are also many examples of finite fields. These must have q elements where $q = p^e$ is a prime power, and are denoted $\mathbb{F}_q$. We can take the vector space $\mathbb{F}_q^n$ (constructed in the same way as $\mathbb{R}^n$, using a direct sum) and consider k-dimensional subspaces. Since $\mathbb{F}_q^n$ has finitely many elements, this means that there are a finite number of such subspaces. In fact, when these are counted there are precisely $\begin{bmatrix} n \\ k \end{bmatrix}_q$ such subspaces of dimension k. The q-binomial coefficients count subspaces while regular binomial coefficients will count subsets, creating a parallel between the two objects.

The q-binomial coefficients routinely appear in generating function identities, particularly often in those related to $\mathbb{F}_q$. A technical explanation is given by the theory of binomial posets, which attempts to explain why certain types of generating functions like exponential generating functions are useful while others are not. A poset is a collection of objects with a 'partial order' $\leq$. This works very similarly to $\leq$ on $\mathbb{Z}$, except there is no guarantee that we can compare any two objects. A binomial poset is just a specific type of poset with some restrictions on the objects and partial order. In particular, the existence of the binomial poset $\mathbb{B}(q)$ as in [Sta12] §3.18 explains why generating functions of the form

$$F(x) = \sum_{n \geq 0} f(n) \frac{x^n}{[n]!}$$

are natural and can be of use in combinatorics. For this poset, the objects are finite dimensional subspaces of $\mathbb{F}_q^\infty$, and the partial order is given by natural inclusions.

In [Sta12], Stanley constructs an algebra isomorphism ϕ taking $f \in R(\mathbb{B}(q)) \mapsto \sum_{n \geq 0} f(n) \frac{x^n}{B(n)}$, where $B(n) = [n]!$. Here, $R(\mathbb{B}(q))$ is the reduced incidence algebra, which

consists of functions on intervals of $\mathbb{B}(q)$ which depend only on the length of the interval. What this means is that we can translate between generating functions $\sum_{n\geq 0} f(n)\frac{x^n}{B(n)}$ and certain functions $f(n)$ on the poset, where n is the length of some interval.

The relevance of $\begin{bmatrix} n \\ k \end{bmatrix}_q$ is that it is used in convolution within the reduced incidence algebra $R(\mathbb{B}(q))$, a subalgebra of the regular incidence algebra $I(\mathbb{B}(q))$ taken over $\mathbb{C}$. These algebras both consist of functions from intervals in the poset to $\mathbb{C}$.

In the restricted incidence algebra, there is an operation $*$ called convolution which combines functions f, g in $R(\mathbb{B}(q))$ to obtain a new function $f*g \in R(\mathbb{B}(q))$. Importantly, the convolution $f * g$ of functions in the restricted incidence algebra introduces the q-binomial coefficient in its calculation. Implicit in the statement that ϕ is an isomorphism of algebras is the statement $\phi(f * g) = \phi(f)\phi(g)$, which shows that when we multiply these generating functions we involve the q-binomial coefficient. As a result, the q-binomial coefficient will make a natural appearance whenever a generating function of the form $\sum_{n\geq 0} f(n)\frac{x^n}{[n]!}$ is used. It also explains why we might use this type of generating function, since the isomorphism tells us that multiplication of generating functions of this type inherits the structure of convolution in $R(\mathbb{B}(q))$. This is a good sign the generating function will be useful, especially for functions related to $\mathbb{F}_q$, since convolution in the incidence algebra generally lends itself to combinatorial interpretation. Once we can represent a function in the incidence algebra as a convolution of other functions, we immediately have a generating function identity.

2.2. **The project.** In my project, I studied a function which counted the number of residues of each type the coefficients of $\begin{bmatrix} n \\ k \end{bmatrix}_q$ have modulo N. This function, $f_{k,R}(n)$ is defined as

$$f_{k,R}(n) = \#\left\{ i : [q^i] \begin{bmatrix} n \\ k \end{bmatrix}_q \equiv R \pmod{N} \right\}$$

for some fixed $N \in \mathbb{N}$. Richard Stanley had made the following conjecture about the function:

Conjecture 2.1. *The function $f_{k,R}(n)$ is quasipolynomial for each $N \in \mathbb{N}$.*

Here, quasipolynomial means that we can determine nonzero functions periodic functions $c_i(n)$ of integer period Q such that

$$f_{k,R}(n) = c_d(n)n^d + c_{d-1}(n)n^{d-1} \ldots + c_0(n)$$

for some integer d. We the call $f_{k,R}$ quasipolynomial of degree d.

A simple motivation for studying this function comes the regular structure of binomial coefficients modulo N. Modulo some prime p, this is precisely described by Lucas's theorem. Earlier, we saw that when $q = 1$ we have $\begin{bmatrix} n \\ k \end{bmatrix}_q = \binom{n}{k}$, so in particular

$$\sum_{0 \le i \le \deg \begin{bmatrix} n \\ k \end{bmatrix}_q} [q^i] \begin{bmatrix} n \\ k \end{bmatrix}_q = \binom{n}{k}.$$

Taking both sides modulo N, the fact that the sum of the coefficients is so structured suggests that the individual residues of the coefficients should also have some structure. The function $f_{k,R}(n)$ attempts to capture some of this structure.

It turns out that this conjecture that $f_{k,R}(n)$ is quasipolynomial is true, and I was able to prove the following main theorem in [Pen17]:

Theorem 2.2. *The function $f_{k,R}(n)$ is quasipolynomial of degree one.*

This is fortunate, because it means that all of the complexity of $f_{k,R}(n)$ will come from the quasiperiod Q. Unfortunately, the proven lower bound for Q grows fairly fast. When $N = p^e$, the asympototic for this lower bound $\pi_{p^e}(k)$ is fairly simple:

$$\log_p(\pi_{p^e}(k)) \sim \log_p \log_p(k) + \frac{\psi(k)}{\ln p},$$

where is it currently known $|\psi(k) - k| \le C\frac{k}{\ln k}$ for k sufficiently large and $C \approx 0.006$. Assuming the Riemann hypothesis, we have $\psi(k) = k + O(k^{\frac{1}{2}+\epsilon})$ for any $\epsilon > 0$.

The simplicity of $f_{k,R}(n)$ also makes studying the functions $c_i(n)$ easier, because we only need to focus on c_0 and c_1. We can equivalently consider $f_{k,R}(n)$ as a set of Q linear functions operating separately on each residue class of $n \pmod Q$. In this context, the constant terms are easily obtained from the first Q values of $f_{k,R}(n)$ and the only interesting object is the slopes. While much more difficult to actually calculate explicitly, I was able to prove a theorem showing that the slopes will repeat themselves several

times over different residue classes in many cases – in this sense, the slopes have a smaller minimal period than the constant terms do, and so this theorem greatly lowers the number of values of $f_{k,R}(n)$ you need to compute to completely determine the function.

The main method I used to prove this claim was to create a decomposition of the coefficients and prove a stronger main theorem which implies Theorem 2.2. First, divide the coefficients in $\begin{bmatrix} n \\ k \end{bmatrix}_q$ into different sections:

Definition 2.3. The ith *section* of the q-binomial coefficient $\begin{bmatrix} n+k \\ k \end{bmatrix}_q$ is the sequence of coefficients denoted by S_i with jth term given by

$$p^{(i)}_{\leq k}(j) = [q^{in+j}] \begin{bmatrix} n+k \\ k \end{bmatrix}_q \pmod N$$

where $j \in \mathbb{Z}/n\mathbb{Z}$. As a special case, S_0 is just a concatenation of copies of $\mathcal{S}$.

The origin of the notation $p^{(i)}_{\leq k}(j)$ comes from partition functions, since the function $p_{\leq k}$ counting partitions with at most k parts is involved in the edge case S_0. To join the sections together, the notation '$\oplus$' was used.

Definition 2.4. Let $X = (x_0, \ldots, x_{|X|-1})$ and $Y = (y_0, \ldots, y_{|Y|-1})$ be finite sequences. The concatenation operator $\oplus$ is defined as $X \oplus Y = (x_0, x_1, \ldots x_{|X|-1}, y_0, y_1, \ldots y_{|Y|-1})$.

Then, we can make the following further decomposition of S_i that proves useful:

$$\mathsf{S}_i = \mathsf{B}^1_i \oplus \mathsf{B}^2_i \oplus \ldots \oplus \mathsf{B}^l_i \oplus \mathsf{R}_i,$$

where the B^j_i are $\pi'_N(k)$-length subsequences and R_i is the remainder after these $l = \lfloor \frac{n}{\pi'_N(k)} \rfloor$ consecutive subsequences are removed from S_i. Here, $\pi'_N(k)$ is a function giving a quasiperiod of $f_{k,R}$ (which is unfortunately quite complicated – for details, see [Pen17]). Informally, if we regard $\begin{bmatrix} n+k \\ k \end{bmatrix}_q$ as a sequence ordered by the associated exponents of q, we can relate $X = \bigoplus_{i \in [k]} \mathsf{S}_{i-1} \oplus (1)$ to its corresponding q-binomial coefficient. Here, (1) is just a sequence only containing 1. We can index X starting at 0, obtaining

$$\begin{bmatrix} n+k \\ k \end{bmatrix}_q = \sum_{x_i \in X} x_i q^i \pmod N.$$

The benefit of all this is that I was able to prove a stronger theorem:

Theorem 2.5. *Consider the ith section S_i of $\begin{bmatrix} n+k \\ k \end{bmatrix}_q$. Then upon decomposing S_i, we obtain*

$$\mathsf{S}_i = \mathsf{B}_i^1 \oplus \mathsf{B}_i^2 \oplus \ldots \oplus \mathsf{B}_i^l \oplus \mathsf{R}_i,$$

where $l = \lfloor \frac{n}{\pi'_N(k)} \rfloor$. Then $\mathsf{B}_i^1 = \mathsf{B}_i^2 = \ldots = \mathsf{B}_i^l$ and the change $n \mapsto n + \pi'_N(k)$ adds an identical sequence $\mathsf{B}_i^{l+1} = \mathsf{B}_i^0$.

This stronger statement says that the coefficients of $\begin{bmatrix} n \\ k \end{bmatrix}_q$ modulo N form a series of different periodic sequences, and the exact periodic sequences you get only depend on n modulo the quasiperiod $\pi'_N(k)$ when you fix k.

The technique I used to prove this theorem was to study the edge case S_0 using generating functions to show that it had the structure described by Theorem 2.5 (and also some additional structure within B_0^j), and then show that this structure extended inductively by relating S_i to $\mathsf{S}_0, \ldots, \mathsf{S}_{i-1}$ through an overcounting argument.

Once I proved Theorem 2.5, I was able to use it as a powerful tool to obtain many of the important results including the main theorem and some additional results about the structure of S_i and the slopes of the linear functions which composed $f_{k,R}(n)$. The theorem allows for a good understanding of the large-scale patterns of the residues such as periodicity, symmetries, or large patches of zeroes but unfortunately offers no information about the individual residues. I suspect this problem is much more difficult, since it essentially amounts to finding an explicit formula for each residue in $\begin{bmatrix} n \\ k \end{bmatrix}_q$ for small n (due to the periodic nature of the residues). This seems very unlikely given that there is no simple direct formula for the coefficients.

References

[Kwo89a] YH Harris Kwong, *Minimum periods of binomial coefficients modulo m*, Fibonacci Quarterly **27** (1989), 348–351.

[Kwo89b] ———, *Minimum periods of partition-functions modulo m*, Utilitas Mathematica **35** (1989), 3–8.

[Man15] Laurent Manivel, *On the asymptotics of kronecker coefficients*, Journal of Algebraic Combinatorics **42** (2015), no. 4, 999–1025.

[NW87] Albert Nijenhuis and Herbert S Wilf, *Periodicities of partition functions and stirling numbers modulo p*, Journal of Number Theory **25** (1987), no. 3, 308–312.

[Pen17] Dylan Pentland, *Coefficients of gaussian polynomials modulo n*, arXiv preprint arXiv:1801.00188 (2017).

[Sta12] Richard P. Stanley, *Enumerative combinatorics: Volume 1*, 2nd ed., Cambridge University Press, New York, NY, 2012.

[SZ12] Andrew Sills and Doron Zeilberger, *Formulæ for the number of partitions of n into at most m parts (using the quasi-polynomial ansatz)*, Advances in Applied Mathematics **48** (2012), no. 5, 640–645.

[SZ16] Richard P. Stanley and Fabrizio Zanello, *Some asymptotic results on q-binomial coefficients*, Annals of Combinatorics **20** (2016), no. 3, 623–634.