

**YUFEI ZHAO:** Last time, we started discussing the extremal problem for bipartite graphs. And in particular, we saw the Kovari-Sos-Turan theorem, which tells us that if you forbid your graph from having a complete bipartite graph,  $K_{s,t}$ , then you have this upper bound on the number of edges in your graph. So we gave a proof. It was fairly short, used the double counting argument, and it give you this bound.

And the next question is how tight is this bound? Is there a lower bound that is off by, let's say, at most a constant factor? And that's a major open problem. It's a conjecture that this bound is tight up to constant factors. But that conjecture is known for only a very small number of graphs. And we saw a couple of examples last time.

So last time we saw construction that shows that for  $S$  equals to 2, this bound is tight. So the extremal number for  $k$  through 2 is on the order of  $n$  to the  $3/2$ . So this  $\theta$  means I'm hiding constant factors.

And our construction used this polarity graph, which is essentially the point line incidence graph of a projective plane. And a basic algebraic or geometric fact, if you will, that two lines intersecting at most one point. We also sketched a construction that showed that for  $S$  equals to 3, this bound is also tight. And this construction here involved using spheres, again, in some space over a finite field.

So both these constructions are in some sense algebraic geometric. And you can ask, is there a way to extend these ideas to construct other examples of  $K_{s,t}$  free graphs with the right number of edges using some ingredients from algebraic geometry? And today, I want to show you two different ways of doing that.

So the state of the art, which I mentioned last time, let me remind you what is known about constructions that achieve the right exponent up there. So in a series of two papers by [INAUDIBLE] it is shown that if the constants  $t$  and  $s$ , such that  $t$  is large enough compared to  $s$ , in particular  $t$  is bigger than  $s$  minus 1 factorial, then the extremal number of  $K_{s,t}$ 's is of the order, same order, as given in the upper bound of the Kovari-Sos-Turan theorem. In particular, these range of parameters allows you to do  $(2, 2)$ ,  $(3, 3)$ , which we already know how to do. But the next case is  $4, 7$ . And it is still open how to do  $4, 6$ .

So I want to show you this construction. And I will tell you exactly what the graph is. I'll give you an explicit description of this graph, which is Kst free and has lots of edges. And as I mentioned earlier, it is an algebraic construction. So as before, we start with  $p$  prime. And we will take  $n$  to be a  $p$  raised to the power  $s$ . And let's restrict  $s$  to be integer at least 2. And, of course, that's same as last time, if you have other values of  $n$ , take a prime close to the desired value and then take it from there.

To describe the construction, let me remind you, the norm map, if you have a field extension, in this case, specifically I am looking at the field extension, this  $F_p$  to the  $s$ , I can define a norm map as follows. Sending  $x$  to be the product of all the conjugates, or the Galois conjugates of  $x$ , in this field extension. So explicitly written out is just that expression, which I can clean and collect and write it down like this.

So I wrote that the image of this norm map lies in the base field  $F_p$ . And that is because-- well, one of the many reasons why this is the case, is that if you look at-- so I'll denote this norm map by  $N$ -- if you look at  $N$  of  $x$ , it raised to power  $p$ , leaves this value unchanged. And the base field is the field where it is invariant under power by  $p$ .

So here's the graph, which I'll denote the norm graph with parameters  $p$  and  $s$ . So the norm graph will have as vertices just the elements of this field extension. And the edges will be the set of all pairs of vertices, not equal, of course, such that a norm of their sum equals to 1. So that's the graph. This is an explicit description of what the vertices and what the edges are.

So now, we need to verify a couple of things. One is that this graph has the desired number of edges. It has lots of edges. And two is that this graph is Kst free. So let's do both of those things.

So the first is let's check it has the right number of edges. So that's a relatively easy task. What we need to do is to count for every  $a$  how many choices of  $b$  are there in this field extension such that  $a + b$  has norm exactly 1? And I claim that that number-- well, so here's a basic algebra fact, that the number of elements in this field extension with norm exactly 1 is precisely  $p$  to the  $s$  minus 1 divided by  $p$  to the  $s$ .

And this is because really we're looking in the multiplicative subgroup. So the multiplicative group in this  $F_p$  to the  $s$ . And it has a cyclical-- so there's a generator-- the order of the cyclic group is  $p$  to the  $s$  minus 1. So you're asking, how many elements when raised to this power here ends up at the identity? So that's the answer.

So that's one aspect. And so as a result, every vertex is adjacent to, well, how many vertices? For every given  $a$  I need to solve for  $b$ . And basically, this many solutions, I have to be just slightly careful because I don't want loops in my graph. So I may need to subtract 1. So it's adjacent to at least this number up here minus 1 to account for possible loops, which is pretty large,  $p$  to the  $s$  minus 1, which in other words is  $n$  raised to  $1$  minus  $1$  over  $s$ , that many vertices, and you see that this gives you the right number of edges.

So this is a graph with lots of edges. So that part wasn't so hard. The next part, it's much trickier, which is we want to check that this graph has no  $K_{s,t}$ 's. So previously in our algebraic construction, we used some geometric facts, such as no two lines intersect in more than one point to show that there's no  $K_{2,2}$  in the polarity graph. So there's going to be something like that here.

So the claim is that this construction, this norm graph, is  $K_{s,t}$  free. So it's not quite the bound I claimed. So it's a little bit weaker. But it is in the spirit of what I am claiming, namely that for  $t$  large enough, this graph is  $K_{s,t}$  free. So for  $t$  a large enough comes constant here will show  $s$  factorial plus 1.

And as a result, it would follow that the extremal number  $\text{ex}(n, K_{s,t})$  is at least  $1/2$  minus little  $1$  of the constant-- I don't already worry about that much, but it's on the order of  $n$  to the  $2$  minus  $1$  over  $s$ . OK, everyone with me? So we need to verify this graph here has no  $K_{s,t}$ . Yes, question?

**AUDIENCE:** Should that  $t$  be an  $s$ ?

**YUFEI ZHAO:** Yes, that should be an  $s$ . Thank you. Any more questions?

**AUDIENCE:** Should that be  $s$  minus 1 factorial?

**YUFEI ZHAO:** So we will show later on a better result using  $s$  minus 1 factorial, but for now I'll show you the slightly weaker result, which is still in the same spirit. Yep.

**AUDIENCE:** Is the stronger result using the same graph?

**YUFEI ZHAO:** We'll change to a different graph. For the stronger result, we will change to a different graph.

OK, so now let's show that this graph here is  $K_{s,t}$  free. And for that claim, we need to invoke an algebraic fact, which let me write down now. So suppose we have a field  $f$ . Any field will work

with a finite field. Any field is fine. And I have a bunch of elements from the field, such that a sub  $i_j$  is different from a sub  $r_j$  for all  $i$  not the same as  $r$ .

Then the system of equations-- and I'll write down the system. So  $x_1$  minus  $a_{1,1}$ ,  $x_2$  minus  $a_{1,2}$ , and so on.  $x_s$  minus  $a_{1,s}$  equals to  $b_1$ . That's the first equation.

Second equation,  $x_1$  minus  $a_{2,1}$ ,  $x_2$  minus  $a_{2,2}$ ,  $\dots$ ,  $x_s$  minus  $a_{2,s}$  equals to  $b_2$ . The system has at most  $s!$  solutions, where I'm working inside this field.

So that's the claim. So let me just give you some intuition for this claim. Suppose the right side vector is 0, all zeroes. Then I claim that this is trivial.

So what is the saying? I need to select  $x_1$  to be one of the  $a$ 's from the first row and  $x_2$  be one of the  $a$ 's from the second row, and so on. But each column of  $a$  is distinct. So that's the hypothesis. You have all the  $a$ 's in the first column are distinct. So no two of the  $x$ 's can-- so I need to set one of the  $x_i$ 's to be one of the  $a$ 's from the first row. But you see that you cannot set  $x_1$  to be  $a_{1,1}$ , and  $x_1$  to be  $a_{s,1}$  at the same time. So the solution just counts permutations, which is exactly  $s!$ .

So this algebraic fact plays a key role in the proof of the theorem that the lower bound that we're stating up there, if you look at the paper, they give a proof of this result. And it's not a long proof. But it uses some commutative algebra and algebraic geometry. And usually in a class, if the instructor doesn't present the proof, it's for one of several reasons.

Maybe the proof is too short. It doesn't need to be presented. Maybe it's too long or too difficult. Maybe it's not instructive to the class. And the last reason, which is the case here, is that I don't actually understand the proof. As in I can follow it line by line, but I don't understand why it is true.

And if one of you wants to come up with a different proof or try to explain to me how this seemingly elementary algebraic fact is proved, I would appreciate it. For small values of  $x$ , you can check it by hand. So  $x$  equals to 2, you're solving a system of two quadratic equations. And that you can check by hand. And three maybe you can do it with some work. But even with 4 it's not so clear how to do it.

And also, one of the geometric intuition is that if  $b$  is  $\neq 0$ , then you have exactly  $s$  factorial solutions. And the geometric intuition is somehow that if you move  $b$  around, then the fiber, the sides of the fiber, the number of solutions  $x$  can only go down. It can not go up. And this corresponds to some algebraic geometry phenomenon. And that's all I will say about this algebraic fact, which we'll now use as a black box.

Great. So now we have that as our algebraic input, let us show that a norm graph is  $K_{s+1}$  free. It's actually not so hard once you assume that theorem up there. So let's show that a norm graph is  $K_{s+1}$  free.

Well, what does it mean to have a  $K_{s+1}$ ? It means that if you have distinct vertices, which then correspond to elements,  $s$  elements,  $y_1$  through  $y_s$ , of this field, then the common neighbors of these elements correspond to solutions of this system of equations where I set all of these values to be 1.

But I can write I exactly what these guys are because I have this form, that representation there for the norm map, so I can write it out. And now remember this fact that when you are in characteristic  $p$ ,  $x + y$  raised to the power  $p$ , is the same as  $x^p + y^p$  and characteristic  $p$ . So I can expand the remaining parenthesis like that. So I want the first line to equal to 1, and so on. And each of the lines has that equal to 1.

How many solutions in  $x$  does this system of equations have? So even if I treat each of  $x$  and  $x$  to the  $p$  and so on as separate variables, that theorem appear tells me that there are at most  $s$  factorial solutions in  $x$ . Satisfies all the hypotheses of that theorem up there. Therefore, the graph is  $K_{s+1}$  free. You do not have more than  $s+1$  different values of  $x$  satisfying this system of equations. And that's the proof that this norm graph is  $K_{s+1}$  free. Yes, question?

**AUDIENCE:** Why can't powers of like [INAUDIBLE]

**YUFEI ZHAO:** Sorry, can you repeat the question?

**AUDIENCE:** Why cannot the powers of the  $y$ 's be the same?

**YUFEI ZHAO:** The question is why cannot the powers of the  $p$ 's be the same? So you are asking, down the second column, let's say, why are all these  $y$ 's different? Because you're working inside a field. And raising to a  $p$  in this field is a bijection. So think about the order of the cyclic group. It has co-prime to  $p$ . But great question. Anything else?

OK, so this gives you a construction that gives you  $K_{st}$  free for  $t$  bigger than  $s$  plus  $s$  factorial. Now, let me show you how to improve this construction to do a little bit better, to get  $s$  minus 1 factorial. And the idea is to take a variant of this norm graph, which we'll call the projective norm graph. And the projective norm graph will define it for  $s$  at least 3 is rather similar. But there's a twist.

I have as the vertex set, not just the field extension-- OK, so now I take field extension, but one level less. And I take a second coordinate, which consists of non-zero elements from  $F_p$ . The edges are formed by putting an edge between these two elements, if and only if, the norm of the sum of the first coordinates equals to the product of the second coordinates.

So now, you can run through a similar calculation that tells you the number of edges. So first of all, the number of vertices is  $p$  to the  $s$  minus 1 times  $p$  minus 1, so basically the same as  $p$  to  $s$ . And additionally, every vertex has degree exactly  $p$  raised to  $s$  minus 1 minus 1. And the reason is that if I tell you the values of  $x$  little  $x$  and big  $y$ , which cannot equal minus  $x$ , or else you will never form an edge, then they together uniquely determine little  $y$ . So for every value of big  $X$  and little  $x$ , I just need to run through all the values of big  $Y$  other than minus  $x$ .

So the number of edges then equals to  $1/2$  times the number of vertices times the degree of every vertex, which, as before, is the claimed asymptotic. And the remaining thing to show is that this projective norm graph is  $K_{st}$  free. So it's  $K_{s, s-1}$  factorial plus 1 free. It's a similar calculation as the one before, but we need to take into account the small variant in the construction.

So suppose we fix  $s$  vertices, labeled by this big  $Y$ 's, little  $y$ 's. And now we need to solve for uppercase  $X$ , lowercase  $x$  in this system of equations, so asking how many different pairs, big  $X$ , little  $x$ , can appear as a solution to this system of equations? Well, first of all, if some pairs of the first coordinates, big  $I$  is equal to big  $J$ , then if you have a solution, then that forces little  $y$  to be the same as little  $j$ . And so the  $y$ 's wouldn't have been distinct to begin with. So this is not possible. So all the big  $Y$ 's are distinct.

Well, now, let's divide these equations by the final equation. And we get that the  $i$ -th equation becomes like that, which you can rewrite by dividing by the coordinate of the norm of big  $Y_i$  minus big  $Y_s$ . This is non-zero because we just showed that all the big  $Y$ 's are distinct. If you divide by this norm here and rearrange appropriately, we find that the equations become like

this.

So after doing some rearranging-- so this is the equation the set of new questions that we get. And you see that if you use new variables,  $x$  prime, do a substitution, this being  $x$  prime, then it has basically the same form as the one that we just saw with a different set of constants. And in particular from what we just saw, we see that you cannot have more than  $s$  minus 1 factorial solutions in  $x$ . Now, they're  $s$  minus 1 equations. And the field extension working as the  $x$  minus 1 field extension.

So we saved an equation by using this projectivization. And that's it. So this shows you the claim of constructing a  $K_{s,t}$  free graph for  $t$  bigger than  $s$  minus 1 factorial, which has the desired number of edges. Yes, question?

**AUDIENCE:** Why do you have the if some capital  $Y$  equals capital  $IJ$ ?

**YUFEI ZHAO:** OK, so the question is why do I say this part? So I'm maybe skipping a sentence. I'm saying, if there is a solution to this system of equations  $x$ , if these vertices have a common neighbor, then if you have some  $x$  satisfying this system of equations, then having two different big  $Y$ 's being the same forces you to have the two smaller  $y$ 's being the same.

**AUDIENCE:** OK.

**YUFEI ZHAO:** Right. And then the  $Y$ 's will have been distinct. So for them to have some common neighbors, you better have these big  $Y$ 's being distinct. Any more questions? Great.

So as I mentioned, it is an open problem to determine whether what is the extremal number for  $K_{4,4}$ ,  $K_{4,5}$ ,  $K_{4,6}$ . And you may ask, well, we have this nice construction-- it maybe somewhat mysterious because of that, but explicit. And you can write this graph down. And you can ask is this graph  $K_{4,6}$  free? So do we gain one extra number for free, maybe because we didn't analyze things properly?

And it turns out that's not the case. So there was a very recent paper just released last month showing that this graph here for  $s$  equals to 4 actually does contain some  $K_{4,6}$ 's. So if you want to prove a corresponding lower bound for  $K_{4,6}$ , you better come up with a different construction. And that's I think an interesting direction to explore. Any questions? Yes.

**AUDIENCE:** Do we know of any similar results about this construction not working for larger  $s$ ?

**YUFEI ZHAO:** The question is, do we know any similar result of about does this graph contain  $K_{s,t}$  for other values of  $s$  and  $t$  less than the claimed threshold? It is unclear. So the paper that was uploaded, it doesn't address the issue of  $s$  bigger than 4. Yeah.

**AUDIENCE:** Why  $F_p$  to the power  $s$ ?

**YUFEI ZHAO:** So question is why  $F_p$  to the power of  $s$ ? So let's go back to the norm graph construction. So where do we use  $F_p$  to the power of  $s$ ? Well, certainly we needed it to have the right edge count. So that comes up in the edge count. And also in the norm expression, you have the correct number of factors. So I encourage you to try for if you use a smaller or bigger value of  $s$ , you either don't get something which is  $K_{s,t}$  free or you have the wrong number of edges. Any more questions?

So later, I will show you a different construction of  $K_{s,t}$  free graphs, again, for  $t$  large compared to  $s$  that will not do as well as this one. But it is a genuinely different construction. And it uses the idea of randomized algebraic construction, which is something that actually was only developed a few years ago. It's a very recent development. And it's quite nice. So it combines some of the things we've talked about with constructing using random graphs to construct  $H$  free graphs on one hand, and on the other hand, some of the algebraic ideas. In particular, we're not going to use that theorem up there, but we'll use some other algebraic geometry fact. OK, so let's take a quick break.

So what I want to discuss now is a relatively new idea called a randomized algebraic construction, which combines some ideas from both the randomized construction and also the algebraic construction that we just saw. So this idea is due to Boris Bukh just a few years ago. And the goal is to give an alternative construction of a  $K_{s,t}$  free graph with lots of edges provided that as before,  $t$  is much larger compared to  $s$ .

So this band here will not be as good as the one that we just saw. And I will even tell you what it is. But it's some constant. So for every  $s$  there is some  $t$ , such that this construction works.

As before, we working inside some finite field geometry. So let's start with  $a$ , a prime power. You can think of prime if you like. It doesn't make so much difference. So we're working inside a finite field. And let's assume  $s$  is fixed and at least 4.

Let me write down some parameters. Don't worry about them for now. Just think of them as sufficiently large constants. So  $d$  is this quantity here. So we'll come back to it later when it

comes up.

OK, so what's the idea? When we looked at the randomized construction, we took a random graph. We took an Erdos Renyi graph. Every edge appeared independently. And saw that it has lots of edges, if you choose  $p$  property and not so many copies of  $h$ . So you can remove all the copies of  $h$  to get a graph with lots of edges that is  $h$  free.

What we're going to do now is instead of taking the edges randomly, we're going to take a random polynomial.  $F$  will be a random polynomial chosen uniformly among all polynomials with-- so I wrote uppercase  $Y$  and uppercase  $X$  and  $Y$ . Actually,  $X$  and  $Y$ , they're not single variants. They are-- so each of them is a vector of  $s$  variables. So in other words,  $x_1$  through  $x_s$  are the variables in the polynomial. And then  $y_1$  through  $y_s$ . So it's a  $2s$  variable polynomial.

So among all polynomials with degree, at most  $d$ --  $d$  being the number up here-- in each of  $x$  and  $y$  sets of variables. So you look at it as  $xs$  variables, each monomial has their exponents sum to our most  $d$ , and likewise with each monomial for the  $y$  variables. So this is the random object. It's a random polynomial in  $2s$  variables. And the degree is bounded. So you only have a finite number of possibilities, and I choose one of them uniformly at random.

And now, what's my graph? We're going to construct a bipartite graph  $G$ . The bipartiteness, it's not so crucial. But it'll make our life somewhat easier. So it's a bipartite graph. So it has two vertex parts, which I will label left and right,  $L$  and  $R$ . And they are both the  $s$  dimensional vector space over  $F$ .

And we'll put an edge between two vertices, if and only if that polynomial up there  $f$  evaluates to 0 on these values. That's the graph. So I give you a random polynomial  $f$ . And then you put in edges according to when  $f$  vanishes. So  $f$ , if you view the bipartite graph as a subset of  $F^s \times F^s$ , then this is the zero set. The edge set is the zero set.

Just like in random graphs, with the construction with random graphs, we'll need to show a couple of things. One is that has lots of edges, which will not be hard to show. And second, that it will have typically a small number of copies of  $K_{s,t}$ . And that will have some ingredients which are similar to the random graphs case we saw before, but it will have some new ideas coming from algebraic geometry.

First, let's show that this graph has lots of edges. And that's a simple calculation, because for every pair of points of vertices, I claim that the probability-- so here  $f$  is the random object-- the

probability that  $f$  evaluates to 0 on this pair is exactly  $q^{-1}$ . So exactly  $1/q$ ,  $1$  over the size of the field. So this is not too hard.

And the reason is that the distribution of  $f$  is identical to if you are an extra random constant on  $f$ , chosen uniformly at random. So I took a random polynomial. I shifted by a random constant. It's still uniformly random polynomial, according to that distribution.

But now, you see that this, whatever  $f$  evaluated to, if I shift by a random constant, you will end up with a uniform distribution. So it tells you that that guy up there is uniform distribution on every fixed point  $u, v$ . So in particular, it hits 0 with probability exactly  $1/q$ .

And as a result, the number of edges of  $g$  in the expectation is exactly  $n^2/q$ , where  $n$  is the number of vertices. So  $n$  is actually not the number of vertices, but the size of each vertex part, namely  $q^{1/s}$ . So you see that it gives you the right number of edges, so  $n^{2-1/s}$ . So we have the right number of edges.

And now, we want to show that this graph here typically does not have too many copies of  $K_s$ 's. It might have some copies of  $K_s$ 's. Somehow that is unavoidable. Just as in the random case, you do have some copies of  $K_s$ 's. But if they are not too many copies, I can remove them and obtain a  $K_s$  free graph.

OK, so what is the intuition? How does it compare to the case when you have a genuine Erdos-Renyi random graph? Well, what is the expected number of common neighbors? So if you fix some  $u$  with let's say on the left side with exactly  $s$  vertices, I want to understand, how many common neighbors does  $u$  have? But because the common neighbors, if he has too many common neighbors, then that's a  $K_s$ .

It is not hard to calculate the expectation of this quantity, both in the random graph case as well as in this case. And you can calculate if you pretend every edge occurs independently, the expected number of common neighbors is exactly  $n^{1-s}$ . So there are  $s$  elements of  $u$ , which is exactly 1. And you know that for a binomial distribution with expectation 1 and a large number of variables, the distribution is approximately Poissonian.

Ah, but that's in the case when it's independently distributed, which is the case in the case of GMP. But it turns out for the algebraic setting we're doing here, things don't behave independently. It's not that you're doing coin flops for every possible edge. We're doing some randomized algebraic construction.

And for algebraic geometry reasons, you will see that the distribution is very much not like Poissonian. It will turn out that either the number of common neighbors is bounded or it is very large. And that means that we can show using some Markov inequality that the probability that it is very large is quite small. So typically, it will not have many common neighbors? And that's the intuition, and so let's work out this intuition. Any questions so far?

So how do we do this calculation? So first, let's start with something that's actually fairly elementary. So suppose you have some parameters,  $r$  and  $s$ . So I think of  $r$  and  $s$ -- so I have some parameters  $r$  and  $s$ . And think of them as constants. Have some restrictions, but don't worry too much about them.

Suppose I have two bounded subsets of the finite field, where you have size  $s$  and  $v$  has size  $r$ . Then the claim is that the probability that  $f$  vanishes on the Cartesian product of  $u$  and  $v$ . OK, so what do you expect it to be? So I have  $s \cdot r$  elements, and I want  $f$ , this random polynomial, to vanish on the entire product.

Well, if  $s$ , its value behaved independently for every point, you should expect that the probability is exactly  $q$  to the power minus  $s \cdot r$ . And it turns out that is the case. So this is true. This is an exact statement.

OK, so why is this true? So this is in some sense a generalization of this claim over here. And you have to do a little bit more work. But it's not too difficult.

So let's first consider this lemma in a somewhat simpler case, where all the first coordinates of  $x$  are distinct-- of  $u$  are distinct. And all the first coordinates of  $v$  are distinct. Suppose  $u$  and  $v$  have that form. So I write down the list of points for  $u$  and first coordinates are all distinct.

What I want to do is to give you a random shift, to do a uniform random shift. And I will shift it by a polynomial  $g$ , which is a bivariate polynomial. So these are not vectors. They are just single variables. And I look at all possible sum of monomials, where the degree in  $i$  is less than  $s$ , and the degree in  $j$  is less than  $r$ . And these  $a$ 's are chosen uniformly independently at random from the ground field  $\mathbb{F}_q$ .

And as before, we see that  $f$  and  $f$  plus  $g$  have the same distribution, the same probability distribution. And so all it remains to show that is whatever  $f$  comes out to be, if I tack on this extra random  $g$ , it creates a uniform distribution on the values on the entire  $u$  cross  $v$ . But, actually, see, I have  $sr$  choices exactly for these coefficients. And I have  $sr$  values that I'm

trying to control. So really it's a counting problem.

And it suffices to show a bijection, namely that for every possible vector of values, there exists a choice of coefficients, as above, such that  $g$  evaluates to the prescribed values with the given coefficients. And that uniformity will follow just because you have the exact if you just do a counting.

And the one-dimensional version of this claim, so let's think about what that is. So if I have, let's say, three points on the line and a degree 2 polynomial, what I am saying is that if you give me the values you want on these three points, I can produce for you a unique polynomial that evaluates to the prescribed values on these three points. And that you should all know as Lagrange interpolation. So it tells you exactly how to do that. And that works for many reasons. One of them is that the random indeterminate is invertible.

Here, we have multi-variables. So let's do Lagrange interpolation twice, once for each variable. So we'll apply Lagrange interpolation twice. So the first time, we'll see that for all values of  $u$ , there exists a single variate polynomial in the  $y$  variable with degree at most  $r$  minus 1 that evaluates to the correct values on the fixed little  $u$ . So do it for one variable at a time. For fixed  $u$ , do Lagrange interpolation on the  $y$  variable.

And now, once we have those things there, viewing the  $g$  that we want to find as a polynomial whose coefficients are polynomials in the  $x$  variables, but is itself is a polynomial in the  $y$  variable, we find that again using Lagrange interpolation, there exists these values for these coefficients here, such that each coefficient of if you plug in the first entry into little  $u$  agrees with the coefficients of the  $g$  that we just found. And that should be the case for every little  $u$ .

So once you find these polynomials and now you have a bonafide polynomial in  $g$ . And that's the claim above. So using Lagrange interpolation twice, once for each variable. So this is-- if you're confused, just think about it. There is nothing deep here.

So that finishes the claim in the case when the first coordinates are all distinct. So we use that fact crucially in doing this Lagrange interpolation. Now, for general  $u$  and  $v$ , where we don't have this assumption of having distinct first coordinates, well, let's make them to have distinct first coordinates by considering a random linear transformation, so using a probabilistic method.

So we suffice as to find invertible linear maps,  $p$  and  $s$ , on this vector space, such that  $TU$  and

SV have the above properties. So let me show you how to do it for  $u$ . So I need to find you a invertible linear transformation  $t$ .

Well, it's just the first coordinate that matters. So it suffices to find just a linear map corresponding to the first coordinate that is injective of  $u$ . Whatever linear map you have, even if it's zero, that's fine, I can extend it to the remaining coordinates. Actually, if it's zero, then it's not going to be injective of  $u$ . So it better not be zero.

OK, well, let's find this map randomly. So pick  $t$  uniform via random among all linear maps. And I want to understand what is the probability of collision, bad event, if two elements of  $u$  end up getting mapped to the same point. Well, that's not too hard. So for every distinct pair of points in  $f_q$  to the  $s$  the probability that they collide, think about why this is true. It's exactly  $1$  over  $q$ . If  $x$  and  $x$  prime, they're differing at least one coordinate, then even just along that coordinate, I can make them distinct.

So this is the case for every pair. So now by union bound, the probability that  $t_1$  is injective on  $u$  is at least  $1$  minus the size if  $u$  choose  $2$  times  $1$  over  $q$ . And that's why we chose  $q$  to be large enough. So  $q$  is at least  $r$  squared,  $s$  So this number here is positive. So such a  $t$  exists. And so we can transform this  $u$  and  $v$ , two configurations where the first coordinates are all distinct, and then run the argument as before. OK, great.

So what we've shown so far is that if you look at these  $K_{s,r}$  structures, they appear with probability exactly-- well, with expectation exactly what you might expect as in independent random case. But what we really want to understand is the distribution of the number of common neighbors. In particular, we want to upper bound the probability that there are too many common neighbors. We want to understand some kind of tail probabilities.

And to do that, one way to do tail probabilities is to consider moments. Yes, question?

**AUDIENCE:** [INAUDIBLE]

**YUFEI ZHAO:** Sorry, can you repeat the question?

**AUDIENCE:** How do you have the equality right before the lemma?

**YUFEI ZHAO:** Question, how do I have the equality right before the lemma? So there, I'm actually saying for the Erdos-Renyi random graph case-- that's the case-- in Erdos-Renyi random graph, each edge, if you have the same edge probability, is  $1$  over  $q$ . And then that's the number of

common neighbors you would expect. So that's a heuristic for the Erdos-Renyi random graph case.

OK, so now let's try to understand the distribution of the number of common neighbors. So let's fix a  $u$  subset of  $F_p$  to the  $s$  with exactly  $s$  elements. And I want to understand how many common neighbors it has. So let's consider the number of common neighbors of  $u$  and the  $d$ -th moment of this random variable. So this is a common way to do upper tail bounds.

And one way to analyze such moments is to decompose this count as a sum of indicator random variables. So let me write  $I$  of  $v$  to be the quantity which is 1 if  $f$  of  $uv$  is 0 for all with  $ou$  and big  $U$ . In the words, it's a common neighbor. It's 1 if  $v$  is a common neighbor for  $u$ , and 0 otherwise.

So then the number of common neighbors would simply be the sum of this indicator as  $v$  ranges over the entire vertex set. And I can expand the sum. Then all of these are standard things to do when you're trying to calculate moments.

OK, so I can bring this expectation inside and try to understand what is the expectation of this object inside. Well, if all the  $v$ 's are distinct, then this is simply the expected number of  $K_s$ 's. But the  $v$ 's might not be distinct. So we need to be a little bit careful. But that's not too hard to handle.

So let me write  $M_{sub r}$  to be the number of subjective functions from  $d$  element set to an  $r$  elements set, an  $M$  to be sum of these  $M_{sub r}$ 's for  $r$  up to  $d$ . Then, let's consider how many distinct  $v$  values are there. If there are distinct  $v$  values, then they take on that many possible values. And  $M_r$  for the number of subjections, and for each possible  $r$ , the exact number for the exact value of this expectation is  $q$  to the minus  $rs$ . And that's exactly what we showed.

So this comes from the lemma just now. But we chose-- I mean, look, this is that binomial coefficient. And you have this number here. So they multiply it to at most 1. So we have this number, this quantity there, which I think of as a constant. So this is a constant. So the  $d$ -th moment is bounded.

And one way to get tail bounds once you have the moments is that we can use Markov's inequality. It tells us that the number of common neighbors of  $u$ , the probability that  $u$  has too many common neighbors, more than  $\lambda$  common neighbors. I can rewrite this inequality here by raising both sides to the power  $d$ . And then, using Markov inequality, take expectation.

So all of these are standard techniques for upper tail estimation. You want to understand the upper tails on random variable, understand its moments and use Markov on its moments. But now, we know we have some bound for the  $d$ -th moment, right? Which is  $M$  as we just showed. So there is this bound here.

So far you can run the same argument in the random graphs case. And you wouldn't really do much different. I mean everything is more or less the same what I've said so far, although we had to do a special calculation algebraically that didn't really make sense-- I mean, that you have to show some kind of near independence. Question?

**AUDIENCE:** Is that less than or equal to, right? The Markov inequality.

**YUFEI ZHAO:** Ah, thank you. So this is less than or equal to. Thank you.

But now is where the algebra comes in, so the algebraic geometry nature of this argument comes in. It turns out that this quantity here-- previously, we said, at least heuristically, in the random graphs case, it behaves like a *qua* Poisson random variable. So it's fairly uniform in a Poisson sense.

It turns out because of the algebraic nature of the construction, this random variable behaves nothing like a Poisson. So it turns out it's highly constrained due to reasons using algebraic geometry. And I'll tell you exactly why. So that the number of common neighbors is either very small or very large.

And here is the claim that for every  $s$  and  $d$ , there exists some  $c$ , such that if I have a bunch of polynomials on  $\mathbb{F}_q$  to the  $s$  of degree  $\leq d$ , then if you look at the number of zeros, common zeros, of the  $f$ 's, how many common zeros can you have? It turns out it cannot just be some arbitrary number. So this set has size either bounded at most  $c$ . Or it is at least  $q$  minus something very small.

And I'll explain just a little bit why this is the case, although I will not give a proof. So either somehow you are working in a zero dimensional case, or if this algebraic variety that comes with it has positive dimension, then you should have a lot more points.

And the reason for this dichotomy has to do with how many points are there on the algebraic variety over a finite field? So I will not give a proof, although if you look on the course website for a link to a reference, that does have a proof. But I will tell you what the key algebraic

geometric input is to that claim up here.

And this is an important and famous theorem called a Lang Weil bound. So the Lang Weil bound tells you that if you have an algebraic variety,  $V$ . And for now, it is important in order to say this properly to work in the algebraic closure, so  $\overline{F_q}$  as the algebraic closure, it's the smallest field extension where I can solve all polynomial equations.

Then, the variety cut out by a set of polynomials-- so  $V$  is this variety. So if it is irreducible, it cannot be written as a union of finite number of smaller varieties, irreducible over  $\overline{F_q}$ . And all of these polynomials have degree bounded. Then the question is, if I take these polynomials and I look at how many  $\overline{F_q}$  points does it have? So in other words, now I leave the field. I come back down to Earth, to the base field and ask, what's the number of solutions where the coordinates are in  $F_q$ ?

OK, so how many points do we expect? Well, the simplest example of an algebraic variety is that of a subspace. If you have a  $d$ -dimensional subspace over  $F_q$ , you have  $q^d$  points exactly. So you expect something like  $q^d$  raised to the dimension of the variety.

Now the dimension is actually a somewhat subtle concept. I won't define. But there are many definitions in algebraic geometry.

It turns out it's not always exactly as nice as in the case of linear subspaces. But the Lang Weil bound tells us that is not too far off. You have a deviation that is at most on the order of  $q^{1/2}$  over  $q^d$ , where there are some hidden constants depending on the description of your variety in terms of the degrees of the polynomials with the dimension and the number of polynomials. But the point is that the number of points on this variety is basically should be around the same as the model case, namely that of a subspace.

And that brings us some intuition to why this lemma is true. So you have those polynomials up there. So there are some subtle points one needs to verify about your disability, but the punchline is that either you are in the zero-dimensional case, in which case you have something like [INAUDIBLE] theorem, and that tells you that a number of solutions is bounded. Or you're in the positive dimensional case, in which case the Lang Weil term tells you, you must have lots of solutions. And there is no middle ground.

And now, we're ready to finish off Boris Bukh's construction. So we see that applying this lemma up there with this, what should be my polynomials be? I'm going to use my polynomials

of  $u$  of  $y$  to be-- well, I have a random polynomial up there. So I'm trying to find common neighbors. I'm trying to find common solutions.

So these are my polynomial as  $u$  ranges over big  $U$ . So for  $q$  large enough, we find that the number of common neighbors of  $u$ , the probability that it is bigger than  $c$ , where  $c$  is supplied by that lemma, is equal to the probability that a number of common neighbors of  $u$  exceeds  $q$  over 2, where  $q$  over  $w$  is this quantity rounded-- smaller than that quantity up there. So if it has more than  $c$  solutions, that automatically has a lot of solutions.

And now, we can apply the Markov inequality up there, the tail bound on the moments to deduce that this probability is at most  $M$  divided by  $q$  over 2 raised to the power  $d$ . And the moral of it is that we should have a very small number-- I mean, this should occur with very small probability. So let's call  $u$  being a subset of  $v$  bad if  $u$  has  $r$  elements,  $u$  is contained entirely on the left side or the right side of the original bipartition. And most importantly,  $u$  has a lot, namely more than  $c$ , common neighbors in  $j$ .

So how many bad sets do we expect? Basically, a very small number. So the number of bad sets, bad use, is upper bounded by-- well, for each choice of  $s$  elements, the probability that something is bad is this quantity up here, which we chose  $d$  to be a large enough constant depending on  $s$ . If you look at the choice of  $d$  up there, see that this quantity here is quite a bit smaller than the number of vertices.

And now, the last step is the same as our randomized construction using Erdos-Renyi random graphs, where we remove-- well, it's almost the same, but now we remove one vertex from every bad set. And we get some graph  $g$  prime. And we just need to check that  $g$  prime has lots of edges. We know got rid of all the bad sets. So  $g$  prime is now  $K$  sub  $sc$  plus 1 free. We got rid of all possibilities for  $s$  points having more than  $c$  common neighbors.

Now, we just need to check that  $g$  prime has lots of edges. Well, the expected number of edges in  $g$  prime is at least the  $x$ -- what we removed one vertex for every bad  $u$ . And each bad  $u$  carries with it at most  $n$  edges, because there are only  $n$  edge on each side of the bipartition.

And, well, the number of edges of  $g$  has expectations exactly  $n$  squared over  $q$ . And the number of bad  $u$ 's we saw up there is not very large. So in particular, this quantity, the second term is dominated by the first term. And so we obtain the claimed number of edges.

Also, the graph has at most  $2n$  vertices. So we may have gotten got rid of some. But actually,

fewer vertices, the better. At most,  $2n$  vertices, and it is a case of  $s$ -- So it's  $K_{st}$  free for  $t$  large enough.

So this gives you another construction of  $K_{st}$  free graphs. And so today, we saw two different constructions of  $K_{st}$  free graphs for constants  $s$  and  $t$ , but in both cases,  $t$  is substantially larger than  $s$ . But the most important thing is that they both match the Kovari-Sos-Turan bound. So it gives you some evidence that maybe the Kovari-Sos-Turan conjecture, the theorem, is tight up to at most a constant factor, although that is a major open problem.

And it remains a very difficult it seems open problem, but one that is of central importance in extremal graph theory to try to come up perhaps with other constructions that can do better. Maybe they will have some algebraic input. But maybe they will have some input from other ideas. We do not know. Question?

**AUDIENCE:** So is this  $q$  defined? Because I remember  $q$  as a prime power, but it doesn't say there.

**YUFEI ZHAO:** So question is, is  $q$  defined? So just like in the proofs of polarity graphs and what not-- so you have some  $n$ . You rounded down to the nearest prime powers. So  $s$  is a constant. So  $n$  is basically  $q$  to the  $s$ . So take large  $n$ , round it down to the nearest prime power.  $q$  could be a prime, for instance. It could be a prime. It could be a prime power. Think  $q$  to be a prime.

So I'm saying for every  $q$ , there is a construction. And for every  $n$ , you can round down to the nearest  $q$  to the  $s$  and then run this construction. Any more questions?

Great. So next time I will begin by telling you a few more things about why people really like this construction and some conjectures that were solved using this idea and some conjectures that still remain open along the same lines. And we'll also go beyond  $K_{st}$ , so other bipartite graphs and show you how to do upper bounds for those bipartite graphs.