**YUFEI ZHAO:** OK. I want to begin by giving some comments regarding the Wikipedia assignment. So I sent out an email about this last night. And so first of all, thank you for your contributions to this assignment, to Wikipedia. It plays a really important role in educating a wider audience what this subject is about because as many of you have experienced, the first time-- if you heard of some term, you have no idea what it is, you put it into Google, and often Wikipedia's entry is one of the top results that come up. And what gets written in there actually plays a fairly influential role in educating a broader audience about what this topic is about.

And so I want to emphasize that this is not simply some homework assignment. It's something that is a real contribution. And it's something that contributes to the dissemination of knowledge. And for that, it is really important to do a good job, to do it right, to do it well, so that next time someone-- maybe even yourselves-- maybe you've forgotten what the subject is about and go back and you want to look it up again and remind yourself. You will have a useful resource to look into.

But also let's say someone wants to find out what is external graph theory about? What is additive combinatorics about? You want them to land on the page that points you to the right type of places, that points you to useful resources, that opens doors so that you can explore further. And some of the contributions, indeed, serve you well in that purpose. It opens doors to many things.

And part of the spirit of this assignment is for you to do your own research, do your own literature search, to learn more about a subject, more than what has been taught in these lectures so that you can write about it on Wikipedia. You can link to more references, you know, show the world what the subject is about.

OK, continuing with our program, so we spent the past few lectures developing tools regarding the structure of set addition so that we can prove Freiman's theorem. So that's been our goal for the past few lectures. And today we'll finally prove Freiman's theorem. But let me first remind you the statement-- so in Freiman's theorem, we would like to show that if you are in a subset-- if you're in the integers, you have a set A that has bounded doubling-- doubling constant, constant k-- then the said must be contained in a small, generalized arithmetic progression, down to dimension and size, only a constant factor larger than a.

We developed various tools the past three lectures building up to your intermediate results. But we also collected this very nice set of tools for proving Freiman's theorem. So let me review some of them, which we'll encounter again today. PlünneckeRuzsa inequality tells you that if you have a set with small doubling, then the further iterated sums are also controlled.

So I want you to think of these parameters as k is a constant, so k to the some power is still a constant, but also I don't really care about polynomial changes in k. So I-- you know, we should ignore polynomial changes in k and view this constant more or less as the original k itself. So if some is-- the a plus a is around the same size as a, then further iterations also do not change the sizes very much.

Ruzsa covering lemma: so this was some statement that if x plus b looks like it could be covered by copies of b, just in terms of their sizes alone, then in fact, x could be covered by a small number of translates of a slightly larger ball. But here B can be any set.

We had a thing called Ruzsa modeling lemma. In particular, a consequence of it is that if a has small doubling, then there exists the prime n that's not too much bigger than the size of a, and a very large proportion-- an eighth of a subset of an eighth of a such that this subset a prime is prime and 8 isomorphic to a subset of z mod n.

So even though you start with a set that's potentially very spread out, provided they have small doubling, I can pick out a pretty large piece of it and model it by something in a fairly small cyclic group. And here the modeling is 8 isomorphic, so it preserves sums up to eight term sums.

We had Bogolyubovs lemma so now we're inside a small cyclic group of a large subset of a small cyclic group. Then Bogolyubovs lemma says that 2a minus 2a contains a large bore set, of large structure within the situated subset. And last time we showed that the geometry of numbers, Minkowskis second term, one can deduce that every bore set of small dimension and small width contains-- of large width contains a proper GAP that's pretty large.

So putting these two together, putting the last two things together, we obtain that if you have a subset of the cyclic group and n is prime-- OK, so here in previous statement n is prime. So n is prime. And a is pretty large. Then 2a minus 2a contains a proper generalized arithmetic progression of dimension at most alpha to the minus 2 and size at least 1 over 40 to the d times n.

So it's just starting from the size of a. 2a minus 2a contains a pretty large GAP. So we're going to put all of these ingredients together and show that you can now contain the original set, a, in a small GAP. So just from knowing that some subset of it, 2a minus 2a, so think 2a prime minus 2a prime, contains this large GAP. We're going to use it to boost it up to a cover.

So now let's prove Freiman's theorem. Using the modeling lemma-- using the modeling lemma-- the corollary of the modeling lemma-- we find that since a plus a is size at most k kind of size of a, there exists some prime n at most 2k to the 16 times a. And so I'm just copying the consequence of this modeling lemma.

So I find a pretty large subset of a such that a prime is prime and 8 isomorphic to a subset of z mod n. Now, applying the final corollary with alpha being the size of this a prime, which is at least the size of a over n, which is at least 1 over 16 to the times k to the power 16, so all constants.

We see that 2a prime minus-- so let me actually-- let me change the letters and call a prime b so I don't have to keep on writing primes. So subset of a is called b. OK, so 2b minus 2b now contains a large GAP. And the GAP has dimension d bounded. So the dimension is bounded by alpha to the minus 2. So it's some constant.

And the size is pretty large. So size is at least 1 over 40 d. If you only care about constants, just remember that everything that depends on k or d is a constant. OK. Because b is Freiman's 8 isomorphic, b is Freiman 8 isomorphic to-- ah, sorry. b is-- a prime is a subset of a and b is the subset of z mod-- b is a subset of z mod n that a prime is 8 isomorphic, too.

So since b is 8 isomorphic to a prime, every GAP in b-- so if you think about what 8 isomorphism preserves, you find that if you look at 2b minus 2b, it must be 2 prime-- 2 isomorphic to 2a prime minus 2a prime. So the point of prime and isomorphism is that we just want to preserve enough additive structure.

Well, we're doing to preserve all the additive structure, but just enough additive structure to do what we need to do. And being able to preserve an arithmetic progression, or in general or generalized arithmetic progression, requires you to preserve Freiman 2 isomorphism. And that's where the a comes in. So I want to analyze 2b minus 2b and I want that to preserve 2 isomorphisms. So initially I want b to preserve 8 isomorphisms.

So 2b minus 2b is Freiman isomorphic to 2a prime minus 2a prime. So the GAP, which we

found earlier in 2B minus 2B is mapped via this Freiman isomorphism to a proper GAP, which we'll call q, now setting aside 2a minus 2a and preserving the same dimension and size. So Freiman isomorphisms are good for preserving these partial additive structures like GAPs. Yes?

**AUDIENCE:** So are we using this smaller structure to be [INAUDIBLE]?

**YUFEI ZHAO:** Correct. So question is, we're using-- so because we have to pass the 2b minus 2b, we want 2b minus 2b to be prime and isomorphic to 2a prime minus 2a prime. So that's why in the proof I want b to be 8 isomorphic to a prime. So you see, so I'm skipping details of this step. But if you read the definition of Freiman's s isomorphism, you see that this implication holds.

**AUDIENCE:** [INAUDIBLE]

**YUFEI ZHAO:** No. 2 isomorphism is a weaker condition. 2 isomorphism just means that you are preserving two y sums. So think about the definition of Freiman 2 isomorphisms. In particular, if two sets are Freiman 2 isomorphic and you have a arithmetic progression in one, then that arithmetic progression is also an arithmetic progression in the other.

So it's just enough additive structure to preserve things like arithmetic progressions and generalized arithmetic progressions. OK. So we found this large GAP in 2a minus 2a. So this is very good. So we wanted to contain a in the GAP. Seems that by now we're doing something slightly in the opposite direction. We find a large GAP within 2a minus 2a.

But something we've seen before, we're going to use this to boost ourselves to a covering of a via the Ruzsa covering lemma. So once you find this large structure, you can now try to take translates of it to cover a. And this is-- if there's any takeaway from the spirit of this proof is this idea. Even though I want to cover the whole set, it's OK. I just find a large structure within it and then I use translaters to cover.

How do we do this? So since q is containing 2a minus 2a, we find that q plus a is containing 3a minus 2a. Therefore, by Plünnecke-Ruzsa-- by Plünnecke-Ruzsa inequality, the size of cube plus a is at most the size of 3a minus 2a, which is, at most, k to the fifth power times the size of a.

And I claim that this final quantity is also not so different from the size of cube, because-- so all of these-- I mean, the point here is, we are doing all of these transformations, passing down to subsets, putting something bigger, putting-- getting to something smaller, but each time we

only loose something that is polynomial in k. We're not losing much more.

I am also only losing a constant factor. There is sometimes a bit more than polynomial, but any case, we're losing only a constant factor at each step. So in particular, since n upper bounds the size of a prime is here where we ended up embedding into z modern, n is larger than a prime, which is at least a constant fraction of a and the size of q is at least 1 over 40 raised d times n.

So we find that this bound-- upper bound earlier on q plus a. We can write it in terms of size of cube where k prime is-- you put all of these numbers together. What it is specifically doesn't matter so much, other than that it is a constant.

d is polynomial in k. So what we have here is something that is exponential, polynomial of k. OK, so now we're in a position to apply the Ruzsa covering lemma. So look at that statement up there. So what is the saying, that a plus q looks like it could be covered by q, just in terms of size. So I should expect to cover a by a small number of translates of q minus q.

So by covering lemma, a is containing some x plus q minus q for some x in a where the size of x is at most k prime. I claim-- so we've covered a by something. q is a GAP. x is a bounded size set, and I claim that this is the type of object that we're happy to have. Just to spell out some details, first note that x is contained in a GAP dimension x or x minus 1 with length 2 in each direction.

So add a new direction for every element of x. It's wasteful, but everything's constant. And recall that the dimension of Q as a GAP is d. So x plus q minus q is contained in a GAP of dimension. OK, so what's the dimension? So when I do q minus q, it's like taking a box and doubling its dimension-- doubling its lengths. I'm not changing the number of dimensions.

So the dimension of q minus q is still d. The dimension of x is, at most, the size of x. All of these things are constants. So we're happy. But to spell it out, the constant here is-- well, k prime is what we wrote up there. So this is a constant.

And the size-- so what is the size of the GAP that contains this guy here? So I'm expanding x to a GAP by adding a new direction for every element of x. And I might expand that size a little bit. But the size of this GAP that contains x is no more than 2 to the power x-- 2 raised to the size of x.

What is the size of GAP q minus q? So q is the GAP of dimension d. And we know that a GAP of dimension d has doubling constant and those 2 to the d-- 2 to the d times the size of q. OK. And because q is contained in qa minus 2a, we find that q is contained in 2a minus 2a. And 2 to the x, well, I know what the site of x is bounded by, it's k prime plus the size of x is-- size of x is, at most, k prime.

And then I have 2 to the d over here, so 2a minus 2a by Plünnecke-Ruzsa is at most k to the 4 times the size of a. OK, you put everything together, we find that this bound here is doubly exponential in the-- it's a polynomial in k. And that's it. This proves Freiman's theory.

Now, to recap-- we went through several steps. So first, using the modeling lemma, we know that if a set a has small doubling, then we can pass a large part of a to a relatively small cyclic group. Going to work inside our cyclic group. Using Bogolyubovs lemma and its geometry of numbers corollary, we find that inside the cyclic group, the corresponding set, which we called b, is such that 2b minus 2b contains a large GAP.

We pass that GAP back to the original set a because we are preserving 8 isomorphisms Freiman 8 isomorphisms in Ruzsa modeling lemma so we can pass to the original set a and find the large GAP in 2a minus 2a. Once we find this large GAP 2a minus 2a, then we're going to use the Ruzsa covering lemma to contain a inside a small number of translates of this GAP.

OK. You put all of these things together and the appropriate bounds coming from Plünnecke-Ruzsa inequalities and you get a final theorem. And this is the proof of Freiman's theorem.

**AUDIENCE:** [INAUDIBLE]

**YUFEI ZHAO:** OK. The question is how do you make it proper? Up until the step with q, it is still proper. So the very last step over here it is-- you might have destroyed properness. So this proof here doesn't give you properness.

So I mentioned at the beginning that in Freiman's theorem, you can obtain properness of the additional arguments. So that I'm not going to show. There's some more work which is related to geometry of numbers.

So for example, you can look up in the textbook by Tao and Vu, and see how to get from a GAP to contain it in a proper GAP, without losing too much in terms of size. So think about it this way-- when do you have something which is not proper? When you have-- and if some linear dependence, you have some integer linear dependence. And in that case, you kind of

lost a dimension.

When you have improperness, you actually go down a dimension. But then you need to salvage the size, make sure that the size doesn't blow up too much. And so there are some arguments to be done there. And we're not going to do it here.

**AUDIENCE:** Well, I guess my [INAUDIBLE] do they change [INAUDIBLE] within the proof, like say [INAUDIBLE] q or whatever? Or do they use the same proof, but later on, say that [INAUDIBLE]?

**YUFEI ZHAO:** OK, good. Yeah, so the question is, to get properness, do I have to modify the proof, or can I use Freiman's theorem as witness of a black box. So my understanding is that I can use the statement as a black box and obtain properness. But if you want to get good bounds, maybe you have to go into the proof, although that, I'm not sure. OK, any more questions?

So this took a while. This was the most involved proof we've done in this course so far, in proving Freiman's theorem. We had to develop a large number of tools. And we came up-- so we eventually arrived at-- it's a beautiful theorem.

So this is a fantastic result that gives you an inverse structure, something-- we know that GAP's have small doubling. And conversely, if something has a small doubling, it has to, in some sense, look like a GAP. So you see that the proof is quite involved and has a lot of beautiful ideas.

In the remainder of today's lecture, I want to present some remarks on additional extensions and generalizations of Freiman's theorem. And while we're not going to do any proofs, there's a lot of deep and beautiful mathematics that are involved in the subject. So I want to take you on a tour through some more things that we can talk about when it comes to Freiman's theorem.

But first, let me mention a few things that I mentioned very quickly when we first introduced Freiman's theorem, namely some remarks on the bounds. So the proof that we just saw gives you a bound, which is basically exponential in the dimension and doubly exponential for the size blow-up. They're all constants, so if you only care about constants, then this is just fine.

But you may ask, are we losing too much here? What is the right type of dependence? So what is the right type of dependence?

So we saw an example. So we saw an example where if you start with A being a highly dissociated set, where there is basically no additive structure within A, then you do need-- so this example shows that you cannot do better than polynomial-- well, actually, than linear in K, in the dimension, and exponential in the size blow-up. So in particular, you do need to blow up the size by some exponential quantity in K.

So here, K is roughly the size of A over 2 in this example. And you can create modifications of the example to keep K constant and A getting larger. But the point is that you cannot do better than this type of dependence simply from that example. And it's conjecture that that is the truth. We're almost there in proving this conjecture, but not quite, although the proof that we just gave is somewhat far, because you lose an exponent in each bound.

There is a refinement of the final step in the argument, so let me comment on that. So we can refine the final step or the final steps in the proof to get polynomial bounds. And to get a polynomial bounds, which is much more in the right ballpark compared to what we got.

And the idea is basically over here, we used the Ruzsa covering lemma. So we started with that Q up there. So up until this point, you should think of this step as everything coming from Bogolyubov and its corollary. So that stays the same.

And now the question is starting with our Q, what would you use? How would you use this Q to try to cover it? Well, what we do, we apply Ruzsa covering lemma. Remember how the proof of Ruzsa covering lemma goes.

You take a maximal set of translates, disjoint translates. And if you blow everything up a factor 2, then you've got a cover. But it turns out to be somewhat wasteful. And you see, there was a lot of waste in going from x to 2 to the x.

So you could do that step more slowly. So starting with Q, cover now some, not all of A. So cover parts of A by translates of 2 minus Q, say. So we do Ruzsa covering lemma, you don't cover the whole thing, but nibble away, cover a little bit, and then look at the thing that you get, which is that Q will become some new thing, let's say Q1. And now cover more by Q1 minus Q1.

So apparently, if you do the covering step more slowly, you can obtain better bounds. And that's enough to save you this exponent, to go down to polynomial-type bounds for Freiman's theorem. So I'm not giving details, but this is roughly the idea. So you can modify the final step

to obtain this bound.

The best bound so far is due to Tom Sanders, who proved Freiman's theorem for bounds on dimension that's like K times poly log K, and the size blowup to be E to the K times poly log K. So in other words, other than this polylogarithmic factor, it's basically the right answer. And so this proof is much more sophisticated.

So it goes much more in depth into analyzing the structure of set addition. So Sanders has a very nice survey article called "The structure of Set Addition" that analyzes some of the modern techniques that are used to prove these types of results.

There is one more issue, which I want to discuss at length in the second half of this lecture, which is that you might be very unhappy with this exponential blowup, because if you think about what happens in these examples-- I mean, not the examples, but if you think about what happens, like the spirit of what we're trying to say, Freiman's theorem is some kind of an inverse theorem. And to go forward, you're trying to say that if you have a GAP of dimension d, then the size blowup is like 2 to the d.

So we want to say some structure applies small doubling, and Freiman's theorem tells the reverse, that you have small doubling, then you obtain this structure. And seems like you are losing. Getting from here to here, there is a polynomial type of loss, whereas going from here to here, it seems that we're incurring some exponential type of loss.

And it'll be nice to have some kind of inverse theorem that also preserves these relationships qualitatively. So that may not make sense in this moment, but we'll get back to it later this lecture. Point is, there's more, much more to be said about the bounds here, even though right now it looks as if they're very close to each other.

One more thing that I want to expand on is, we've stated and proved Freiman's theorem in the integers. And you might ask, what about in other groups? We also proved Freiman's theorem in F2 to the m, or more generally, groups of bounded exponent or bounded portion, so abelian groups of bounded exponent.

For general abelian groups, so Freiman's theorem in general abelian groups, you might ask what happens here? And in some sense what is even the statement of the theorem? So we want something which combines, somehow, two different types of behavior.

On one hand, you have z, which is what we just did. And here the model structures are GAP's.

And on the other hand, we have, which we also proved, things like F2 to the m, where the model structures are subgroups.

And there's a sense in which these are not the GAP's and subgroups. They have some similar properties, but they're not really like each other. So now if I give you a general group, which might be some combination of infinite torsion or very large torsion elements versus very small torsion elements-- so for example, take a Cartesian product of these groups.

Is there a Freiman's theorem? And what does such a theorem look like? What are the structures? What are the subsets of bounded doubling?

So that's kind of the thing we want to think about. So it turns out for Freiman's theorem in general abelian groups-- so there is a theorem. So this theorem was proved by Green and Ruzsa.

So following a very similar type of proof framework, although the individual steps, in particular the modeling lemma needs to be modified. And let me tell you what the statement is. So the common generalization of GAP's and subgroups is something called a "co-set progression."

So a co-set progression is a subset which is a direct sum of the form P plus H, where P is a proper GAP. So the definition of GAP works just fine in every abelian group. You start with the initial point, a few directions, and you look at a grid expansion of those directions.

P is a proper GAP, and H is a subgroup. And here, the direct sum refers to the fact that every-- so if P plus H equals to P prime plus H prime for some P and P prime in the set P, and H and H prime in the set H, then P equals to P prime and H equals to H prime. So every element in here is written in a unique way as some P plus some H. So that's what I mean by "direct sum."

For such an object, so such a co-set progression, I call its dimension to be the dimension of the GAP, P. And its size in this case, actually, is just the size of the set, which is also the size of P times the size of H. So the theorem is that if A is a subset of an arbitrary abelian group and it has bounded doubling, then A is contained in a co-set progression of bounded dimension and size, bounded blowup of the size of A.

And here, these constants D and K are universal. They do not depend on the group. So there are some specific numbers, functions you can write down. They do not depend on the group.

So this theorem gives you the characterization of subsets in general abelian groups that have

small doubling. Any questions? Yes?

**AUDIENCE:** [INAUDIBLE]

**YUFEI ZHAO:** That's a good question. So I think you could go into their paper and see that you can get polynomial type bounds. And I think Sander's results also work for this type of setting to give you these type of bounds. But I-- yes, so you should look into Sanders' paper, and he will explain. I think in Sanders' paper he walks in general abelian groups.

The next question I want to address is-- well, what do you think is the next question? Non-abelian groups, so Freiman's theorem in non-abelian groups, or rather the Freiman problem in non-abelian groups. So here's a basic question-- if I give you a non-abelian group, what subsets have bounded doubling?

Of course, the examples from abelian groups also work in non-abelian groups, where you have subgroups, you have generalized arithmetical progressions. But are there genuinely new examples of sets in non-abelian groups that have bounded doubling? So think about that, and let's take a quick break.

Can you think of examples in non-abelian groups that have small doubling, that do not come from the examples that we have seen before? So let me show you one construction. And this is that important construction for non-abelian groups. So it has a name. It's called a discrete Heisenberg group, which is the matrix group consisting of matrices that look like what I've written.

So you have integer entries above the diagonal, 1 on the diagonal, and 0 below the diagonal. So let's do some elementary matrix multiplication to see how group multiplication in this group works. So if I have two such matrices, I multiply them together.

And then you see that the diagonal is preserved, of course. But this entry over here is simply addition. So this entry here is just addition.

This entry over here is also addition. And the top right entry is a bit more complicated. It's some addition, but there's an additional twist.

So this is how matrix multiplication works in this group. I mean, this is how matrix multiplication works, but in terms of elements of this group, that's what happens. So you see it's kind of like an abelian group, but there's an extra twist, so it's almost abelian, so the first step you can

take away from abelian.

And there's a way to quantify this notion. It's called "nilpotency." And we'll get to that in a second. But in particular, if you set S to be the following generators-- so if you take S to be these four elements, and you ask what does the r-th power of S look like, so I look at all the elements which can be written by r or at most r elements from S, what do these elements look like?

What do you think? So if you look at elements in here, how large can this entry, the 1, comma, 2 entry be? r. So each time you do addition, so it's at most r.

So let me be a bit rough here, and say it's big O of r. And likewise, the 2, 1, 2, 3, entry is also big O of r. What about the top right entry over here?

So it grows like r squared, because there is an extra multiplication term. So you can be much more precise about the growth rate of these individual entries. But very roughly, it looks like this ball over here.

So the size of S, the r-th ball of S, is roughly, it's on the order of 4th power of r. So in particular, the doubling constant, if r is reasonably large, is what? What happens when we go from r to 2r? The size increases by a factor of around 16.

So that's an example of a set in a non-abelian group with bounded doubling, which is genuinely different from the examples we have seen so far. So that's non-abelian. Yeah.

**AUDIENCE:** [INAUDIBLE]

**YUFEI ZHAO:** The question is, is the size-- we've shown the size is-- I'm not being very precise here, but you can do upper bound and lower bound. So size turns out to be the order of r to the 4. So you want to show that there are actually enough elements over here that you can fill in, but I'll leave that to you. Can you build other examples like this one? Yeah.

**AUDIENCE:** How do we know that this isn't similar to a co-set, the direct sum [INAUDIBLE]?

**YUFEI ZHAO:** Question is, how do we know this isn't like a co-set sum or a co-set progression? For one thing, this is not abelian. S, if you multiply entries of S in different orders, you get different elements. So already in that way, it's different from the examples that we have seen before. But no, you're right. So maybe we can write this a semi-direct product in terms of things we

have seen before. And it is, in some sense, a semi-direct product, but it's a very special kind of semi-direct product.

From that example, you can build bigger examples, of course with more entries in the matrix. But more generally, these things are what are known as "nilpotent groups." So that's an example of a nilpotent group. And to remind you, the definition of a nilpotent group is a group where the lower central series eventually terminates.

In particular, inside that if you look at-- so this is the commutator of G, so look at all the elements that we recognize x, y, x inverse, y inverse-- the set of elements that can be written this way. So that's a subgroup. And if I repeat this operation enough times, I eventually would get just the identity.

And you could trade on that group. If you do the commutator, so essentially you get rid of abelian-ness and you move up the whole diagonal, you create a commutator, you'd get rid of these-- all these two entries. So you get z alone. If you do it one more time, you zero out that entry.

And so more generally, all of these nilpotent groups have this phenomenon, have the polynomial growth phenomenon. So if you take a set of generators and look at a ball, and look at the volume of the ball, how does the volume of the ball grow with the radius? It grows like a polynomial.

And so let me define that. So given G, a finitely generated group, so generated by set S, we say that G has polynomial growth if the size S to the r grows like at most a polynomial in r. It's worth noting that this definition is really a definition about G. It does not depend on the choice of generators.

You can have different choices, generators for the group. But if it has polynomial growth with respect to one set of generators, then it's the same. It also has polynomial growth with regards to every other set.

So we've seen an example of groups with polynomial growth. Abelian groups have polynomial growth. So if you think of polynomial growth, think lattice or z to the m. So if you take a ball growing, so it has size growing like r to the dimension. But nilpotent groups is another example of groups with polynomial growth.

And these are, intuitively at least for now, related to bounded doubling. If it's polynomial

growth, then it has bounded doubling. So is there a classification of groups with bounded-- with polynomial growth?

So if I tell you a group-- so an infinite group always, because otherwise if finite, then it maxes out already at some point. So I give you an infinite group. I tell you it has polynomial growth.

What can you tell me about this group? Is there some characterization that's an inverse of what we've seen so far? And the answer is yes.

And this is a famous and deep result of Gromov. So Gromov's theorem on groups of polynomial growth from the '80s. Gromov showed that a finitely generated group has polynomial growth if and only if it's virtually nilpotent, where "virtually" is an adverb in group theory where you have some property like "abelian," or "solvable," or whatever.

So virtually P means that there exists a finite index subgroup with property P. So "virtually nilpotent" means there is a finite index subgroup that is nilpotent. So it completely characterizes groups of polynomial growth. So basically, all the examples we've seen so far are representative, so up to changing by a finite index subgroup, which as you would expect, shouldn't change the growth nature by so much.

There are some analogies to be made here with, for example in geometry, you ask in Euclidean space, how fast is the ball of radius r growing? In dimension d, it grows like r to the d. What about in the hyperbolic space?

Does anyone know how fast, in a hyperbolic space, a ball of radius r grows? It's exponential in the radius. So for non-negatively curved spaces, the balls grow polynomially. But for something that's negatively curvatured, in particular the hyperbolic space, the ball growth might be exponential.

You have a similar phenomenon happening here. The opposite of polynomial growth is, well, super polynomial growth, but one specific example is that of a free group, where there are no relations between the generators. In that case, the balls, they grow like exponentially. So the balls grow exponentially in the radius.

Gromov's theorem is a deep theorem. And its original proof used some very hard tools coming from geometry. And Gromov developed a notion of convergence of metric spaces, somewhat akin to our discussion of graph limits. So starting with discrete objects, he looked at some

convergence to some continuous objects, and then used some very deep results from the classification of locally compact groups to derive this result over here.

So this proof has been quite influential, and is related to something called "Hilbert's fifth problem, which concerns characterizations of Lie groups. So all of these are inverse-type problems. I tell you some structure has some property. Describe that structure.

What does this all have to do with Freiman's theorem? Already you see some relation. So there seems, at least intuitively, some relationship between groups of polynomial growth versus subsets of bounded doubling. One implies the other, although not in the converse.

And they are indeed related. And this comes out of some very recent work. I should also mention that Gromov's theorem has been made simplified by Kleiner, who gave an important simplification, a more elementary proof of Gromov's theorem.

So let's talk about the non-abelian version of Freiman's theorem. We would like some result that says that is it true that every set, most every set of-- so previously, we had small doubling. You want to have some similar notion, although it may not be exactly small doubling, but let me not be very precise and to say, "small doubling."

In literature, these things are sometimes also known as "approximate groups." So if you look this up, you will get to the relevant literature on the subject. Most every set of small doubling in some non-abelian group behaves like one of these known examples, something which is some combination of subgroups and nilpotent balls.

So these combinations are sometimes known as "co-set nilprogressions." So this was something that was only explored in the past 10 years or so in a series of very difficult works. Previously, it had been known, and still was being investigated for various special classes of matrix groups or special classes of groups like solvable groups and whatnot, that are more explicit or easier to handle or closer to the abelian analog.

There was important work of Hrushovski, which was published about 10 years ago, who showed using model theory techniques, so using methods from logic, that a weak version of Freiman's theorem is true for non-abelian groups. And later on, Breuillard, Green, and Tao building on Hrushovskis work-- so this actually came quite a bit later, even though the journal publication dates are the same year-- so they were able to build on Hrushovski's work, and greatly expanding on it, and going back to some of the older techniques coming from Hilbert's

fifth problem, and as a result, proved an inverse structure theorem that gave some kind of answer to this question of non-abelian Freiman. So we now do have some theorem which is like Freiman's theorem for abelian groups that says in a non-abelian group, if you have something that resembles small doubling, then the set must, in some sense, look like a combination of subgroups and nilpotent balls. But let me not be precise at all.

The methods here build on Hrushovski. And Hrushovski used model theory, which is kind of-- it's something where-- in particular, one feature of all of these proofs is that they give no bounds. Similar to what we've seen earlier in the course, in proofs that involved compactness, what happens here is that the arguments use ultra filters.

So there are these constructions from mathematical logic. And like compactness, they give no bounds. So it remains an open problem to prove Freiman's theorem for non-abelian groups with some concrete bounds. Question.

**AUDIENCE:** [INAUDIBLE] nilpotent ball?

**YUFEI ZHAO:** What is nilpotent ball? I don't want to give a precise definition, but roughly speaking, it's balls that come out of those types of constructions. So you take a nilpotent subgroup. You take a nilpotent group. You look at an image of a nilpotent group into your group, and then look at the image of that ball, so something that looks like one of the previous constructions. So that's all I want to say about non-abelian extensions of Freiman's theorem. Any questions?

**AUDIENCE:** Would you say one more time what you mean by "approximate group?"

**YUFEI ZHAO:** So what I mean by-- you can look in the papers and see the precise definitions, but roughly speaking, it's that if you have-- there are different kinds of definitions and most of them are equivalent. But one version is that you have a set A such that A is coverable by K translates of A, so it's a bit more than just the size information, but it's actually related to size information. So we've already seen in this course how many of these different notions can go back and forth from one to the other, covering to size, and whatnot.

The final thing I want to discuss today is one of the most central open problems in additive combinatorics going back to the abelian version. So this is known as the "polynomial Freiman-Ruzsa conjecture." So we would like some kind of a Freiman theorem that preserves the constants up to polynomial changes without losing an exponent.

Now, from earlier discussions, I showed you that the bounds that we almost proved is close to

the truth. You do need some kind of exponential loss in the blowup size of the GAP. But it turns out those kind of examples are slightly misleading. So let's look at the examples of the constructions again.

So if A-- so just for simplicity in exposition, I'm going to stick with F2 to the n, at least initially. So if A is an independent set of size n, then K, being the doubling constant of A, is roughly like n over 2. And yet the subgroup that contains A has size 2 to the something on the order of K times A. So you necessarily incur an exponential loss over here.

Now, you might complain that the size of A here is basically K. But of course, I can blow up this example by considering what happens if you take each element here, and blow it up into an entire subspace. So the e's are the coordinate vectors. So now I'm sitting inside F2 to the m plus n. And that gives me this set.

The doubling constant is still the same as before. And yet, we see that the subgroup generated by A still has this exponential blowup in this constant, exponential in the doubling constant. But now you see in this example here, even though the subgroup generated by A can be much larger than A, so everything's still constant, so much larger in terms of as a function of the doubling constant, A has a very large structure. So A contains a very large subspace. By "subspace," I mean affine subspace.

And the subspace here is comparable to the size of A itself. So you might wonder, if you don't care about containing A inside a single subspace, can you do much better in terms of bounds? And that's the content of the polynomial Freiman-Ruzsa conjecture.

The PFR conjecture for F2 to the m says that if you have a subset of F2 to the m and A plus A is size at most K times the size of A, then there exists a subspace V of size at most A such that V contains a large proportion of A. And the large here-- we only lose something that is polynomial in these doubling constants. So that's the case.

It's over here. So instead of containing A inside an entire subspace, I just want to contain a large fraction of A in a subspace. And the conjecture is that I do not need to incur exponential losses in the constants.

**AUDIENCE:** So V is an affine subspace?

**YUFEI ZHAO:** V is-- question is, V is an affine subspace. You can think of V as an affine subspace. You can

think of V as a subspace. It doesn't actually matter in this formulation.

There's an equivalent formulation which you might like better, where you might complain, initially, PFR is initially-- Freiman's theorem is about covering A. And now we've only covered a part of A. But of course, we saw from earlier arguments, you can use Ruzsa's covering lemma to go from covering a part of A to covering all of A.

Indeed, it this the case that this formulation is equivalent to the formulation that if A is in F to the n and A plus A size at most K times A, then there exists some subspace V with the size of V no larger than the size of A, such that A can be covered by polynomial in K many co-sets of V. We see that here. Here A has doubling constant K, which is around the same as n. And even though I cannot contain A by a single subspace of roughly the same size, I can use K different translates to cover A. Any questions?

So I want to leave it to you as an exercise to prove that these two versions are equivalent to each other. It's not too hard. It's something if I had more time, I would show you. It uses Ruzsa covering lemma to prove this equivalence.

The nice thing about the-- so the polynomial Freiman-Ruzsa conjecture, PFR conjecture, is considered a central conjecture in additive combinatorics, because it has many equivalent formulations and relates to many problems that are central to the subject. So we would like some kind of an inverse theorem that gives you these polynomial bounds. And I'll mention a couple of these equivalent formulations.

Here is an equivalent formulation which is rather attractive, where instead of considering subsets, we're going to formulate something that has to do with approximate homomorphisms. So the statement still conjecture is that if F is a function from a Boolean space to another Boolean space is such that F is approximately a homomorphism in the sense that the set of possible errors-- so if it's actually a homomorphism, then this quantity is always equal to 0-- but it's approximately a homomorphism in the sense that the set of such errors is bounded by K in size, the conclusion, the conjecture claims that then there exists an actual homomorphism, an actual linear map G, such that F is very close to G, as in that the set of possible discrepancies between F and G is bounded, where you only lose at most a polynomial in K.

So if you are an approximate homomorphism in this sense, then you are actually very close to an actual linear map. Now, it is not too hard to prove a much quantitatively weaker version of

this statement. So I claim that it is trivial to show upper bound of at most 2 to the K over here. So think about that.

So if I give you an F, I can just think about what the values of F are on the basis, and extend it to a linear map. Then this set is necessarily a span of that set, so has size at most 2 to the K. But it's open to show you only have to lose a polynomial in K.

There is also a version of the polynomial Freiman-Ruzsa conjecture which is related to things we've discussed earlier regarding Szemeredi's theorem. And in fact, the polynomial Freiman-Ruzsa conjecture kind of came back into popularity partly because of Gowers' proof of Szemeredi's theorem that used many of these tools. So let me state it here.

So we've seen some statement like this in an earlier lecture, but not very precisely or not precisely in this form. And I won't define for you all the notation here, but hopefully, you get a rough sense of what it's about. So we want some kind of an inverse statement for what's known as a "quadratic uniformity norm," "quadratic Gowers' uniformity norm."

So recall back to our discussion of the proof of Roth's theorem, the Fourier analytic proof of Roth's theorem. We want to say that-- but now think about not three APs, but four APs. So we want to know if you have a function F on the Boolean cube, and this function is 1 bounded, and-- I'm going to write down some notation, which we are not going to define-- but the Gowers' u3 norm is at least some delta. So this is something which is related to 4 AP counts. So in particular, if this number is small, then you have a counting lemma for four-term arithmetic progressions.

If this is true, then there exists a quadratic polynomial q in n variables over F2 such that your function F correlates with this quadratic exponential in q. And the correlation here is something where you only lose a polynomial in the parameters. So previously, I quoted something where you lose something that's only a constant in delta, and that is true. That is known.

But we believe, so it's conjecture, that you only lose a polynomial in these parameters. So this type of statement-- remember, in our proof of Roth's theorem, something like this came up. So something like this came up as a crucial step in the proof of Roth's theorem. If you have something where you look at counting lemma, and you exhibit something like this, then you can exhibit a large Fourier character. And in higher order Fourier analysis, something like this corresponds to having a large Fourier transform.

It turns out that all of these formulations of polynomial Freiman-Ruzsa conjecture are equivalent to each other. And they're all equivalent in a very quantitative sense, so up to polynomial changes in the bounds. So in particular, if you can prove some bound for some version, then that automatically leads to bounds for the other versions. The proof of equivalences is not trivial, but it's also not too complicated. It takes some work, but it's not too complicated.

The best bounds for the polynomial Freiman-Ruzsa conjecture, and hence for all of these versions, is again due to Tom Sanders. And he proved a version of PFR with quasi-polynomial bounds, where by "quasi-polynomial bounds," I mean, for instance over here, instead of K. He proved it for something which is like e to the poly log K, so like K to the log K, but K to the poly log K. So it's almost polynomial, but not quite there.

And it's considered a central open problem to better understand the polynomial Freiman-Ruzsa conjecture. And we believe that this is something that could lead to a lot of important new tools and techniques that are relevant to the rest of additive combinatorics. Yeah.

**AUDIENCE:** Using the fact that all of these are equivalent, is it possible to get a proof of Freiman's theorem using the bound of 2 to the K to be approximate [INAUDIBLE]?

**YUFEI ZHAO:** OK, so the question is, we know that that up there has 2 to the K, so you're asking can you use this 2 to the K to get some bound for polynomial, for something like this? And the answer is yes. So you can use that proof to go through some proofs and get here.

I don't remember how this equivalence goes, but remember that the proof of Freiman's theorem for F2 to the n wasn't so hard. So we didn't use very many tools. Unfortunately, I don't have time to tell you the formulations of polynomial Freiman-Ruzsa conjecture over the integers, and also over arbitrary abelian groups. But there are formulations over the integers, and that's one that people care just as much about. And there are also different equivalent versions, but things are a bit nicer in the Boolean case. Yeah.

**AUDIENCE:** You said [INAUDIBLE]?

**YUFEI ZHAO:** I'm sorry, can you repeat the question?

**AUDIENCE:** [INAUDIBLE]. Yeah, what does that mean?

**YUFEI ZHAO:** Are you asking what does this mean?

**AUDIENCE:** Yeah.

**YUFEI ZHAO:** So this is what's called a "Gowers' uniformity norm." So something I encourage you to look up. In fact, there is an unassigned problem in the problem set that's related to the Gowers' uniformity norm before you U2, which just relates to Fourier analysis. But U3 is related to 4 AP's and quadratic Fourier analysis.