The unstable range in Lusztig's conjecture

Geordie Williamson
Max Planck Institute, Bonn.

Darstellungstheorie Schwerpunkttagung,
Bad Honnef, March 2015.

In representation theory there are numerous examples of beautiful combinatorial structure: Weyl character formula, Young tableaux, Littelmann path model, Kazhdan-Lusztig conjecture ...

In representation theory there are numerous examples of beautiful combinatorial structure: Weyl character formula, Young tableaux, Littelmann path model, Kazhdan-Lusztig conjecture ...

But there are also questions which seem fundamentally difficult: Kronecker coefficients, determination of the unitary dual, the character table of $SL_n(\mathbb{F}_q)$, ...

(Perhaps there is rich structure waiting around the corner. At present the difficulties seem to lie quite deep.)

This will be a talk about *modular representation theory*: i.e. the study of representations over some field k (usually $\mathbb{F}_p$ or $\overline{\mathbb{F}}_p$) of positive characteristic p.

Here the same dichotomy is present. One has beautiful structural theorems (Brauer's theory of defect groups, derived equivalence …) and dimension/character conjectures/formulas (LLT conjecture, Lusztig conjecture, James conjecture …).

In dimension and character formulas experience shows that the situation is “chaotic” for very small p (Richard Guy: “There aren't enough small numbers to meet the many demands made of them.”) and uniform for very large p. (Think about a finite rank $\mathbb{Z}$-algebra.)

One hopes that there is some range of “bad” primes, after which the situation becomes uniform (what exactly uniform means might take decades to pin down):

In dimension and character formulas experience shows that the situation is "chaotic" for very small p (Richard Guy: "There aren't enough small numbers to meet the many demands made of them.") and uniform for very large p. (Think about a finite rank $\mathbb{Z}$-algebra.)

One hopes that there is some range of "bad" primes, after which the situation becomes uniform (what exactly uniform means might take decades to pin down):

Examples:

(James conjecture) Modular representations of S_n should be uniform if $p > \sqrt{n}$.

(Lusztig conjecture) Modular representations of $SL_n(\mathbb{F}_{p^m})$ in natural characteristic should be uniform if $p > n$.

Theorem: There exists a constant $c > 1$ such that Lusztig's conjecture on representations of $SL_n(\mathbb{F}_p)$ fails for many primes $p > c^n$ and $n \gg 0$.

Theorem: There exists a constant $c > 1$ such that Lusztig's conjecture on representations of $SL_n(\mathbb{F}_p)$ fails for many primes $p > c^n$ and $n \gg 0$.

Note: Lusztig's conjecture holds for p very large (a highly non-trivial theorem).

Theorem: There exists a constant $c > 1$ such that Lusztig's conjecture on representations of $SL_n(\mathbb{F}_p)$ fails for many primes $p > c^n$ and $n \gg 0$.

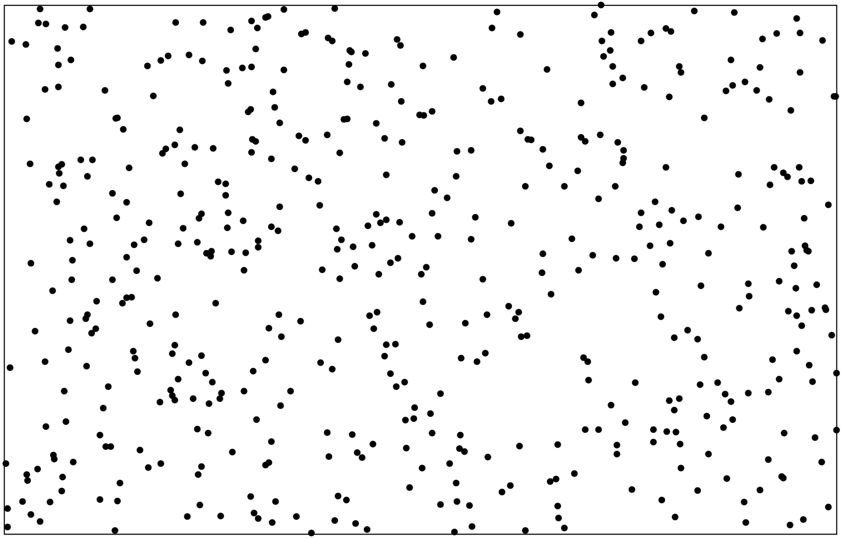
Note: Lusztig's conjecture holds for p very large (a highly non-trivial theorem).

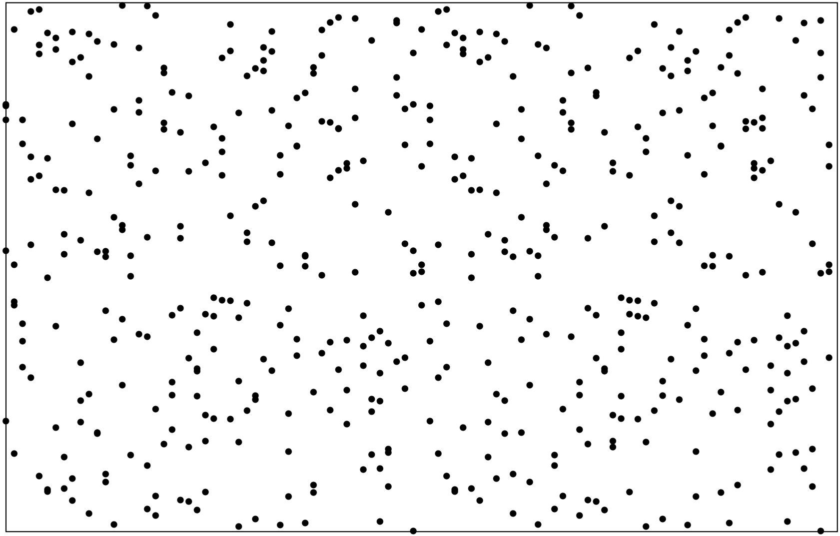
This theorem simply says that the "unstable range" is much larger than we first thought.

It is disconcerting from the structural point of view that there is some interesting number theory behind these results.

A riddle for the end of the talk:

What are similar and different about the following slides?





Fix an algebraic group G over $k := \bar{\mathbb{F}}_p$.

A *rational representation* is a homomorphism $\rho : G \to GL_n$ of algebraic groups (i.e. matrix coefficients are regular functions on G).

Studying rational representations is "harmonic analysis in algebraic geometry".

Example: The standard representation of SL_2 on $V = kx \oplus ky$ (column vectors) is rational.

Example: The standard representation of SL_2 on $V = kx \oplus ky$ (column vectors) is rational.

For any $m \geqslant 0$ we get a representation on the symmetric power $S^m(V)$ (a.k.a homogenous polynomials in x, y of degree m).

Example: The standard representation of SL_2 on $V = kx \oplus ky$ (column vectors) is rational.

For any $m \geqslant 0$ we get a representation on the symmetric power $S^m(V)$ (a.k.a homogenous polynomials in x, y of degree m).

These are not all simple in characteristic p:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot x^p = (ax + cy)^p = a^p x^p + c^p y^p.$$

Hence $L(p) := kx^p \oplus ky^p \subset S^p(V)$ is a submodule.

The wierd and wonderful world of rational representations:

Exercise: (Easy) $S^p(V)/L(p)$ is simple and isomorphic to $L(p-2) := S^{p-2}(V)$. Hence:

$$[S^p(V)] = [L(p)] + [L(p-2)]$$

Moreover, $L(p) \cong V^{(1)}$, where $V^{(1)}$ is V pulled back under the Frobenius map

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} a^p & b^p \\ c^p & d^p \end{pmatrix}$$

The wierd and wonderful world of rational representations:

Exercise: (Easy) $S^p(V)/L(p)$ is simple and isomorphic to $L(p-2) := S^{p-2}(V)$. Hence:

$$[S^p(V)] = [L(p)] + [L(p-2)]$$

Moreover, $L(p) \cong V^{(1)}$, where $V^{(1)}$ is V pulled back under the Frobenius map

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} a^p & b^p \\ c^p & d^p \end{pmatrix}$$

Exercise: (Harder) For any m, $S^{p^m-1}(V)$ is simple and

$$S^{p^m-1}(V) \cong S^{p-1}(V) \otimes S^{p-1}(V)^{(1)} \otimes \cdots \otimes S^{p-1}(V)^{(m-1)}.$$

The wierd and wonderful world of rational representations:

Exercise: (Easy) $S^p(V)/L(p)$ is simple and isomorphic to $L(p-2) := S^{p-2}(V)$. Hence:

$$[S^p(V)] = [L(p)] + [L(p-2)]$$

Moreover, $L(p) \cong V^{(1)}$, where $V^{(1)}$ is V pulled back under the Frobenius map

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} a^p & b^p \\ c^p & d^p \end{pmatrix}$$

Exercise: (Harder) For any m, $S^{p^m-1}(V)$ is simple and

$$S^{p^m-1}(V) \cong S^{p-1}(V) \otimes S^{p-1}(V)^{(1)} \otimes \cdots \otimes S^{p-1}(V)^{(m-1)}.$$

(Crazy from the perspective of char 0 representation theory!)

Assume that G is reductive. Then G may be obtained by reduction modulo p from an algebraic group ("Chevalley scheme") over $\mathbb{Z}$.

Similarly, one may start with a simple highest weight representation over $\mathbb{C}$ and "reduce it modulo p" to get a highest weight representation $\Delta(\lambda)$ of G.

For SL_2: $\Delta(m) = S^m(V)^*$.

Assume that G is reductive. Then G may be obtained by reduction modulo p from an algebraic group ("Chevalley scheme") over $\mathbb{Z}$.

Similarly, one may start with a simple highest weight representation over $\mathbb{C}$ and "reduce it modulo p" to get a highest weight representation $\Delta(\lambda)$ of G.

For SL_2: $\Delta(m) = S^m(V)^*$.

Theorem (Chevalley): $\Delta(\lambda)$ has a unique simple quotient $L(\lambda)$. The $L(\lambda)$ are pairwise non-isomorphic and exhaust all simple G-modules.

Assume that G is reductive. Then G may be obtained by reduction modulo p from an algebraic group ("Chevalley scheme") over $\mathbb{Z}$.

Similarly, one may start with a simple highest weight representation over $\mathbb{C}$ and "reduce it modulo p" to get a highest weight representation $\Delta(\lambda)$ of G.

For SL_2: $\Delta(m) = S^m(V)^*$.

Theorem (Chevalley): $\Delta(\lambda)$ has a unique simple quotient $L(\lambda)$. The $L(\lambda)$ are pairwise non-isomorphic and exhaust all simple G-modules.

Hence one has a classification by highest weight just as in characteristic zero. However the simple modules are usually much smaller than in characteristic zero. (The definition of $L(\lambda)$ as a head is not explicit.)

Explicit constructions of $L(\lambda)$ are a distant dream (except for SL_2).

Explicit constructions of $L(\lambda)$ are a distant dream (except for SL_2).

Instead we try to write the unknown in terms of the "known":

$$[L(\lambda)] = \sum a_{\mu\lambda}[\Delta(\mu)].$$

Explicit constructions of $L(\lambda)$ are a distant dream (except for SL_2).

Instead we try to write the unknown in terms of the "known":

$$[L(\lambda)] = \sum a_{\mu\lambda}[\Delta(\mu)].$$

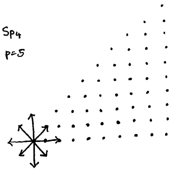
As "reductions modulo p", the $[\Delta(\mu)]$ have the same formal characters as their characteristic zero cousins (Weyl's character formula). One can see the above equality as an identity of formal characters.

$\boxed{SL_2,\ p=5}$

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	Dimension
L(0)	1	·	·	·	·	·	·	·	·	·	·	·	·	·	·	1
L(1)	·	1	·	·	·	·	·	·	·	·	·	·	·	·	·	2
L(2)	·	·	1	·	·	·	·	·	·	·	·	·	·	·	·	3
L(3)	·	·	·	1	·	·	·	·	·	·	·	·	·	·	·	4
L(4)	·	·	·	·	1	·	·	·	·	·	·	·	·	·	·	5
L(5)	·	·	·	-1	·	1	·	·	·	·	·	·	·	·	·	2
L(6)	·	·	-1	·	·	·	1	·	·	·	·	·	·	·	·	4
L(7)	·	-1	·	·	·	·	·	1	·	·	·	·	·	·	·	6
L(8)	-1	·	·	·	·	·	·	·	1	·	·	·	·	·	·	8
L(9)	·	·	·	·	·	·	·	·	·	1	·	·	·	·	·	10
L(10)	1	·	·	·	·	·	·	·	-1	·	1	·	·	·	·	~~4~~ 3
L(11)	·	2	·	·	·	·	·	-1	·	·	·	1	·	·	·	~~5~~ 6

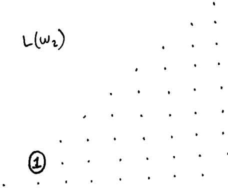
Sp_4

$p=5$

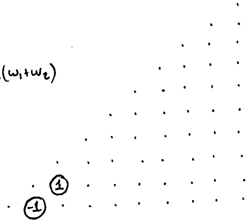


$L(0)$

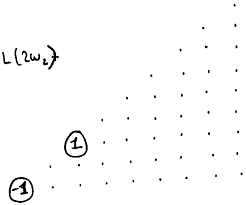
$L(\omega_2)$



$L(\omega_1+\omega_2)$

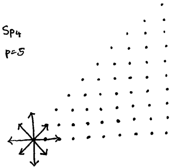


$L(2\omega_2)$

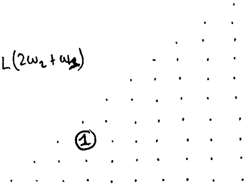


Sp_4

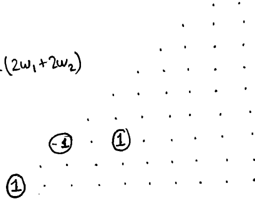
$p=5$



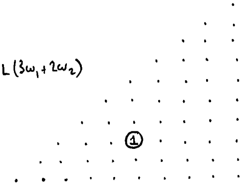
$L(2\omega_2+\omega_1)$



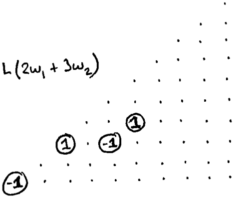
$L(2\omega_1+2\omega_2)$



$L(3\omega_1+2\omega_2)$



$L(2\omega_1+3\omega_2)$

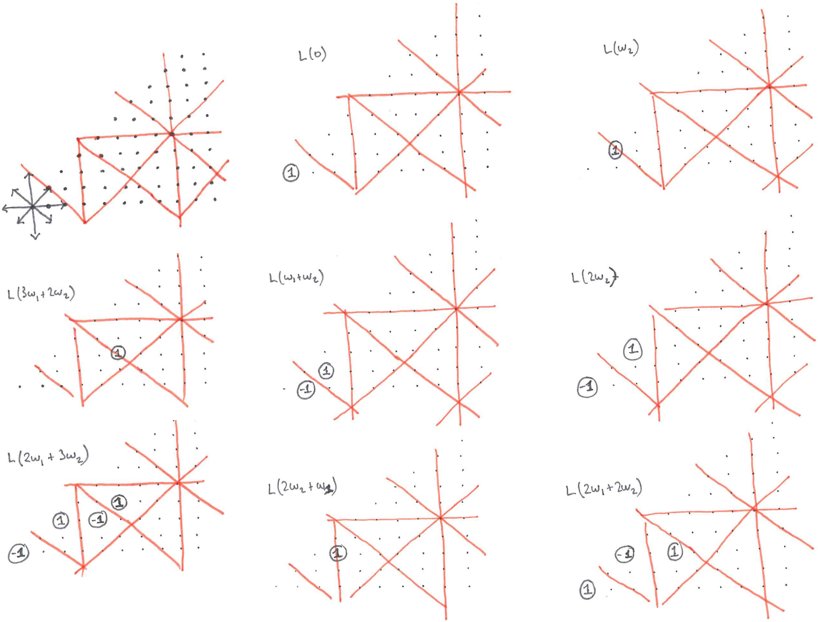


Verma noticed that behind all of this lurks the dot action of an affine Weyl group, where translations are dilated by p.

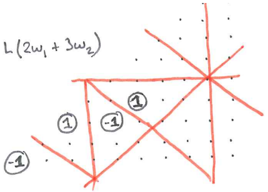
We denote this p-dilated dot action $\lambda \mapsto x \cdot_p \lambda$.

SL_2, $p=5$

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	Dimension
L(0)	1															1
L(1)		1														2
L(2)			1													3
L(3)				1												4
L(4)					1											5
L(5)				-1		1										2
L(6)			-1				1									4
L(7)		-1						1								6
L(8)	-1								1							8
L(9)										1						10
L(10)	1								-1		1					3
L(11)		1						-1				1				6
L(12)			1				-1						1			9
L(13)				1		-1								1		12
L(14)															1	15

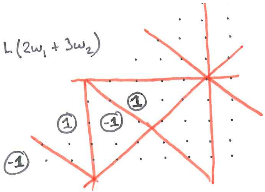


L(0)
L(ω₂)
L(3ω₁+2ω₂)
L(ω₁+ω₂)
L(2ω₂)
L(2ω₁+3ω₂)
L(2ω₂+ω₁)
L(2ω₁+2ω₂)



Lusztig's character formula (1979): If $x \cdot 0$ is "restricted" (all digits in fundamental weights less than p) then

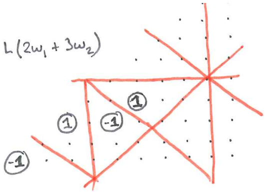
$$[L(x \cdot_p 0)] = \sum_y (-1)^{\ell(y)-\ell(x)} P_{w_0 y, w_0 x}(1)[\Delta(y \cdot_p 0)].$$



Lusztig's character formula (1979): If $x \cdot 0$ is "restricted" (all digits in fundamental weights less than p) then

$$[L(x \cdot_p 0)] = \sum_y (-1)^{\ell(y)-\ell(x)} P_{w_0 y, w_0 x}(1)[\Delta(y \cdot_p 0)].$$

The $P_{x,y}$ are Kazhdan-Lusztig polynomials associated to the affine Weyl group. (Tricky, combinatorial, but "easy" if you or your computer has enough memory.)



Lusztig's character formula (1979): If $x \cdot 0$ is "restricted" (all digits in fundamental weights less than p) then

$$[L(x \cdot_p 0)] = \sum_y (-1)^{\ell(y)-\ell(x)} P_{w_0 y, w_0 x}(1)[\Delta(y \cdot_p 0)].$$

The $P_{x,y}$ are Kazhdan-Lusztig polynomials associated to the affine Weyl group. (Tricky, combinatorial, but "easy" if you or your computer has enough memory.)

This formula is enough to determin all characters (Steinberg tensor product theorem, Jantzen's translation principle).

Lusztig's character formula (1979): If $x \cdot 0$ is restricted then

$$(LCF) \qquad [L(x \cdot_p 0)] = \sum_y (-1)^{\ell(y)-\ell(x)} P_{w_0 y, w_0 x}(1) [\Delta(y \cdot_p 0)].$$

Lusztig's character formula (1979): If $x \cdot 0$ is restricted then

$$(LCF) \qquad [L(x \cdot_p 0)] = \sum_y (-1)^{\ell(y)-\ell(x)} P_{w_0 y, w_0 x}(1)[\Delta(y \cdot_p 0)].$$

Lusztig's formulation required $p \geqslant 2h - 2$ where h is the Coxeter number of G (e.g. n for SL_n). It was later realized (by Kato and others) that $p \geqslant h$ looks reasonable.

Lusztig's character formula (1979): If $x \cdot 0$ is restricted then

$$(LCF) \qquad [L(x \cdot_p 0)] = \sum_y (-1)^{\ell(y)-\ell(x)} P_{w_0 y, w_0 x}(1)[\Delta(y \cdot_p 0)].$$

Lusztig's formulation required $p \geqslant 2h - 2$ where h is the Coxeter number of G (e.g. n for SL_n). It was later realized (by Kato and others) that $p \geqslant h$ looks reasonable.

There is also a version for quantum groups at roots of unity where the necessary but annoying assumptions ($p \geqslant h$, $x \cdot 0$ restricted) magically disappear.

A potted history:

1. It was shown in the early 90s that LCF holds for $p \gg 0$ by combined work of Kazhdan-Lusztig, Kashiwara-Tanisaki, Lusztig, Andersen-Jantzen-Soergel.

A potted history:

1. It was shown in the early 90s that LCF holds for $p \gg 0$ by combined work of Kazhdan-Lusztig, Kashiwara-Tanisaki, Lusztig, Andersen-Jantzen-Soergel. Hence, though complicated, it seems that the LCF is *necessarily* complicated.

A potted history:

1. It was shown in the early 90s that LCF holds for $p \gg 0$ by combined work of Kazhdan-Lusztig, Kashiwara-Tanisaki, Lusztig, Andersen-Jantzen-Soergel. Hence, though complicated, it seems that the LCF is *necessarily* complicated.
2. Another proof (for $p \gg 0$) was given by Bezrukavnikov and coauthors in the mid 2000s.

A potted history:

1. It was shown in the early 90s that LCF holds for $p \gg 0$ by combined work of Kazhdan-Lusztig, Kashiwara-Tanisaki, Lusztig, Andersen-Jantzen-Soergel. Hence, though complicated, it seems that the LCF is *necessarily* complicated.
2. Another proof (for $p \gg 0$) was given by Bezrukavnikov and coauthors in the mid 2000s.
3. Fiebig (2008) gave another approach. From his method he could deduce an explicit enormous bound above which the LCF holds.

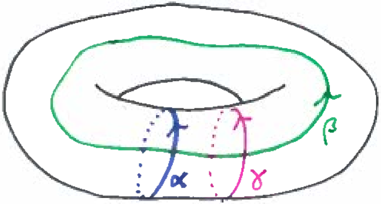
Soergel (2000): "The goal of this article is to forward [Lusztig's conjecture] to the topologists or geometers."

Soergel (2000): “The goal of this article is to forward [Lusztig’s conjecture] to the topologists or geometers.”

After much translation (parts of) Lusztig’s conjecture (and much of highest weight representation theory) can be formulated in terms of “intersection forms”.

Canonical example: $T = S^1 \times S^1$.

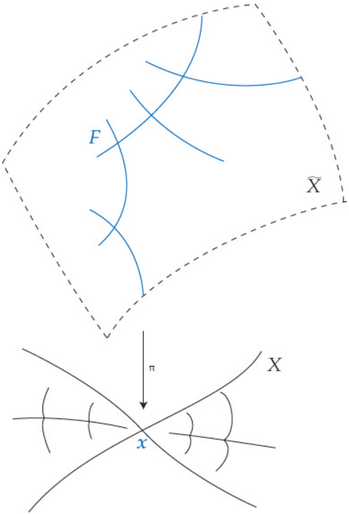
$$H_1(T) = \mathbb{Z}[\alpha] \oplus \mathbb{Z}[\beta]$$



$\langle \alpha, \alpha \rangle = 0 \qquad (\alpha \sim \gamma)$

$\langle \beta, \beta \rangle = 0$

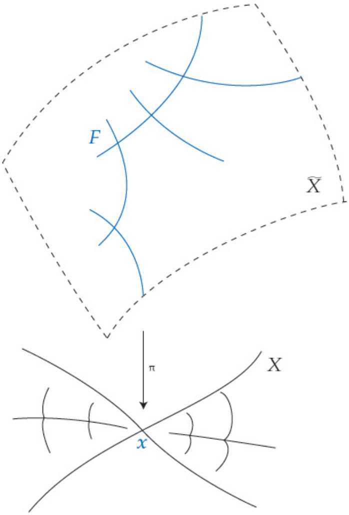
$\langle \alpha, \beta \rangle = \pm 1$ (depending on orientation)



$\widetilde{X}$ is smooth.

π is a resolution of singularities.

X (usually singular), normal.

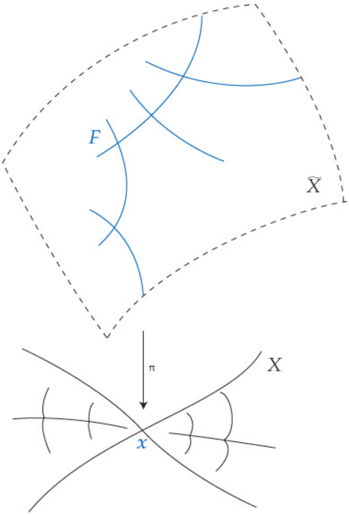


After fixing a point $x \in X$ we can consider the fibre

$$F := \pi^{-1}(x).$$

F is connected.
If $F \subset \widetilde{X}$ half-dimensional (of real dimension d) we have a "refined intersection form"

$$H_d(F) \times H_d(F) \to H_0(\widetilde{X}) = \mathbb{Z}.$$



After fixing a point $x \in X$ we can consider the fibre

$$F := \pi^{-1}(x).$$

F is connected.
If $F \subset \widetilde{X}$ half-dimensional (of real dimension d) we have a "refined intersection form"

$$H_d(F) \times H_d(F) \to H_0(\widetilde{X}) = \mathbb{Z}.$$

$H_d(F)$ has a basis $[F_i]$ consisting of fundamental classes of irreducible components of maximal dimension.

"How do the F_i move in $\widetilde{X}$?"

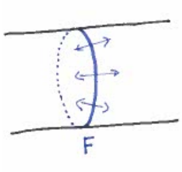
Example ("miracle situation"):

Suppose F is irreducible. Then our intersection form is a 1×1-matrix!

Example ("miracle situation"):

Suppose F is irreducible. Then our intersection form is a 1×1-matrix!

If in addition F is smooth then its self-intersection is



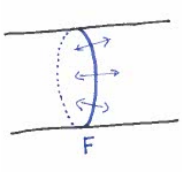
$$\langle [F], [F] \rangle = e$$

where e denotes the Euler class of the normal bundle of $F \subset \widetilde{X}$.

Example ("miracle situation"):

Suppose F is irreducible. Then our intersection form is a 1×1-matrix!

If in addition F is smooth then its self-intersection is



$$\langle [F], [F] \rangle = e$$

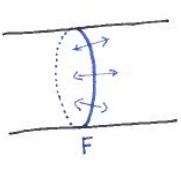
where e denotes the Euler class of the normal bundle of $F \subset \widetilde{X}$.

(One of the few examples where one can compute anything.)

Example ("miracle situation"):

Suppose F is irreducible. Then our intersection form is a 1×1-matrix!

If in addition F is smooth then its self-intersection is



$$\langle [F], [F] \rangle = e$$

where e denotes the Euler class of the normal bundle of $F \subset \widetilde{X}$.

(One of the few examples where one can compute anything.)

E.g. Igelsatz: $S^n \subset TS^n$, $[S^n]^2 = 1 + (-1)^n = \chi(S^n)$.

Forms are everywhere in rep theory and geometry/topology.

In the passage from representation theory to geometry these forms are either:

Forms are everywhere in rep theory and geometry/topology.

In the passage from representation theory to geometry these forms are either:

a) preserved (e.g. Springer correspondence, geometric Satake, Nakajima quiver varieties). This is interesting, but doesn't help computations.

Forms are everywhere in rep theory and geometry/topology.

In the passage from representation theory to geometry these forms are either:

a) preserved (e.g. Springer correspondence, geometric Satake, Nakajima quiver varieties). This is interesting, but doesn't help computations.

b) get much smaller ("we zoom in"). E.g. a contravariant form on a 10^4 dimensional weight space is replaced by 1×1-matrix (e.g. "miracle situation"). This is a computational dream!

Forms are everywhere in rep theory and geometry/topology.

In the passage from representation theory to geometry these forms are either:

a) preserved (e.g. Springer correspondence, geometric Satake, Nakajima quiver varieties). This is interesting, but doesn't help computations.

b) get much smaller ("we zoom in"). E.g. a contravariant form on a 10^4 dimensional weight space is replaced by 1×1-matrix (e.g. "miracle situation"). This is a computational dream!

In Soergel's passage from Lusztig's conjecture to the geometry of the flag variety, we often find ourselves in situation b)!

Notation for the main theorem:

Consider the cohomology of the flag variety of SL_n:

$$H = \mathbb{Z}[x_1, \ldots, x_n]/(e_1, \ldots, e_n)$$

(where e_i denotes the i^{th} elementary symmetric function.)

$$H = \bigoplus \mathbb{Z} X_w$$

where X_w indexed by permutations of n (Schubert basis).

Notation for the main theorem:

Consider the cohomology of the flag variety of SL_n:

$$H = \mathbb{Z}[x_1, \ldots, x_n]/(e_1, \ldots, e_n)$$

(where e_i denotes the i^{th} elementary symmetric function.)

$$H = \bigoplus \mathbb{Z}X_w$$

where X_w indexed by permutations of n (Schubert basis).

On H we consider the operators:

1. $f \mapsto \partial_i(f) := \frac{f - s_i(f)}{x_i - x_{i+1}}$ (a Demazure operator).
2. $f \mapsto x_i f$ for $i \in \{1, n\}$ (mult. by $x_2, \ldots, x_{n-1}$ is *verboten*!)

Consider $C \in \mathbb{Z}$ that may be obtained as a coefficient in the Schubert basis after repeated application of the operators

$$\partial_i \qquad\qquad x_1 \cdot \qquad\qquad x_n \cdot$$

to $1 \in H$. Let N denote the number of times we have multiplied by x_1 or x_n.

Consider $C \in \mathbb{Z}$ that may be obtained as a coefficient in the Schubert basis after repeated application of the operators

$$\partial_i \qquad x_1 \cdot \qquad x_n \cdot$$

to $1 \in H$. Let N denote the number of times we have multiplied by x_1 or x_n.

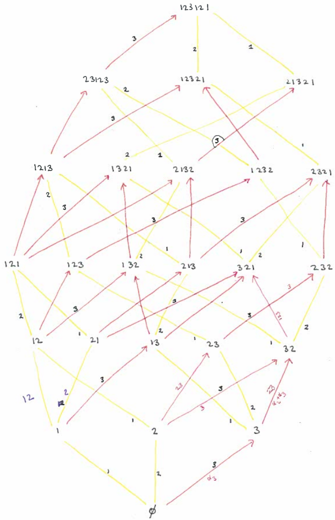
Given the above data ($C +$ the sequence of operators) one can explicitly construct a Schubert variety X and a partial flag variety for SL_{n+N} (don't miss the N) and a (Bott-Samelson) resolution

$$\pi : \widetilde{X} \to X$$

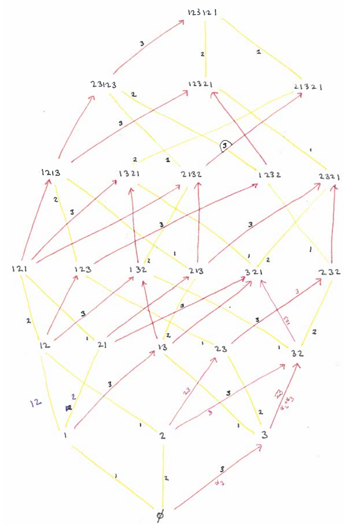
such that π has a smooth irreducible fibre F with self-intersection $\pm C$. (I.e. we get a 1×1-intersection form $(\pm C)$: we are in the "miracle situation".)

The original construction of these counter-examples was algebraic and followed extensive calculations and joint work with Ben Elias ("Soergel calculus": generators and relations for Soergel bimodules) and was based on a formula discovered with Xuhua He.

The above geometric version was discovered later (and was influenced by discussions with Daniel Juteau, Tom Braden and Patrick Polo).

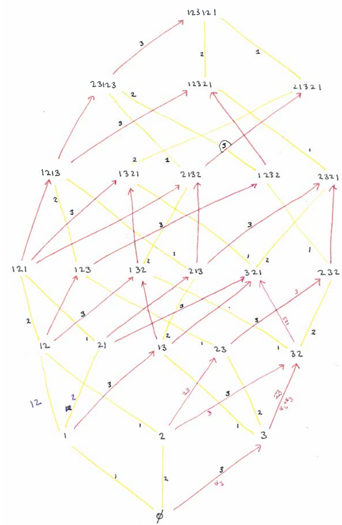


A “discrete dynamical system”:



A "discrete dynamical system":

One has nilpotent operators x_1, x_n (degree 2 $\uparrow$), and nilpotent operators ∂_i (degree 2 $\downarrow$.)



A "discrete dynamical system":

One has nilpotent operators x_1, x_n (degree 2 $\uparrow$), and nilpotent operators ∂_i (degree 2 $\downarrow$.)

Question: How do the prime factors of coefficients grow as we act by these operators?

E.g. if $n = 4$ the operators

$$\begin{aligned} F_1 &: h \mapsto \partial_{23}(x_4^2(\partial_1(x_1 h))) \\ F_2 &: h \mapsto \partial_{21}(x_1^2(\partial_4(x_4 h))) \\ U_1 &: h \mapsto \partial_{21}(x_1^2(\partial_1(x_1 h))) \\ U_2 &: h \mapsto \partial_{23}(x_4^2(\partial_3(x_4 h))) \end{aligned}$$

preserve the submodule

$$\mathbb{Z}x_1 \oplus \mathbb{Z}(x_1 + x_2 + x_3) \subset H$$

and in this (Schubert) basis are given by the matrices:

$$F_1 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \quad F_2 = \begin{pmatrix} 0 & -1 \\ -1 & -1 \end{pmatrix} \quad U_1 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \quad U_2 = \begin{pmatrix} -1 & -1 \\ 0 & -1 \end{pmatrix}$$

The main theorem implies:

Let p be a prime dividing a coefficient or any word of length ℓ in the generators:

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

Then Lusztig's conjecture fails for $SL_{3\ell+5}$ in characteristic p.

E.g.

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n = \begin{pmatrix} f_{n+1} & f_n \\ f_n & f_{n-1} \end{pmatrix}$$

where $f_0 = 0, f_1 = 1, f_2 = 1, f_3 = 2 \dots$ are the Fibonacci numbers / WLAN password. One expects infinitely many Fibonacci numbers to be prime, but this is a conjecture.

Some number theory (which I pretend to understand):

Theorem (with Kontorovich and McNamara): There exists a constant $c \approx 1.39\ldots$ such that for all large L there exists a word γ of length L in the semi-group

$$\left\langle \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle^{+}$$

and a prime $p > c^L$ dividing the top-left entry of γ. Moreover, the number of such primes is (at least) of the order of c^L/L.

Some number theory (which I pretend to understand):

Theorem (with Kontorovich and McNamara): There exists a constant $c \approx 1.39\ldots$ such that for all large L there exists a word γ of length L in the semi-group

$$\left\langle \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle^+$$

and a prime $p > c^L$ dividing the top-left entry of γ. Moreover, the number of such primes is (at least) of the order of c^L/L.

This theorem is an easy consequence of 2012 deep work of Bourgain and Kontorovich on Zaremba's conjecture. (How random is the map $b \mapsto b^n$ modulo p?)

Some number theory (which I pretend to understand):

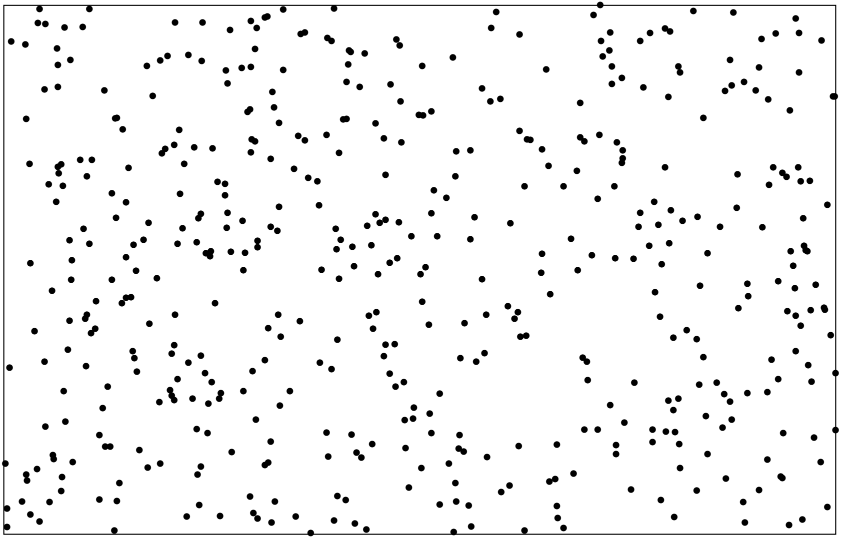
Theorem (with Kontorovich and McNamara): There exists a constant $c \approx 1.39\ldots$ such that for all large L there exists a word γ of length L in the semi-group

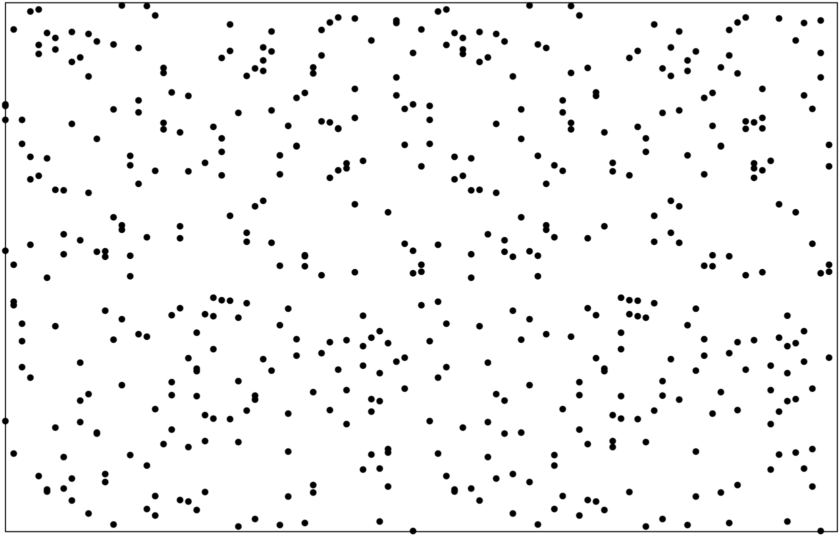
$$\left\langle \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle^{+}$$

and a prime $p > c^L$ dividing the top-left entry of γ. Moreover, the number of such primes is (at least) of the order of c^L/L.

This theorem is an easy consequence of 2012 deep work of Bourgain and Kontorovich on Zaremba's conjecture. (How random is the map $b \mapsto b^n$ modulo p?)

Using the main construction we get the exponential growth of the unstable range in Lusztig's conjecture.





Literature

Slides: `people.mpim-bonn.mpg.de/geordie/talks.html`

Jantzen, *Character formulae from Hermann Weyl to the present*, LMS lecture note series, 2008.

W., *Schubert calculus and torsion*, `arXiv:1309.5055` (new version with appendix with AK and PM available by end of March.)

Soergel, *On the relation between intersection cohomology and representation theory in positive characteristic,* JPAA, 2000.

Fiebig, *Sheaves on affine Schubert varieties, modular representations and Lusztig's conjecture*, JAMS, 2011.

Juteau, Mautner, W., *Parity sheaves*, JAMS, 2014.

Elias, W., *Soergel calculus*, `arXiv:1309.0865`

He, W., *Soergel calculus and Schubert calculus*, `arXiv:1502.04914`