Algebra is Half the Battle: Verifying Presentations for Graded Unipotent Chevalley Groups

ITP 2025

Eric Wang

Arohee Bhoja

Cayden Codel

Noah Singer

Eric Wang

Arohee Bhoja

Cayden Codel

Noah Singer

Work done at

Eric Wang

Arohee Bhoja

Cayden Codel

Noah Singer

Work done at

Undergraduates
(Wrote the proofs)

Eric Wang

Arohee Bhoja

Cayden Codel

Noah Singer

Work done at

Undergraduates
(Wrote the proofs)

PhD student
(Knew the maths)

Eric Wang

Arohee Bhoja

Cayden Codel

Noah Singer

Work done at

Undergraduates
(Wrote the proofs)

PhD student
(Automation)

PhD student
(Knew the maths)

Eric Wang

Arohee Bhoja

Cayden Codel

Noah Singer

Work done at

Undergraduates
(Wrote the proofs)

PhD student
(Automation)

PhD student
(Knew the maths)

Eric Wang

Arohee Bhoja

Cayden Codel

Noah Singer

Work done at

Visit for the world's best cinnamon roll [citation needed?]

(Not sponsored)

Undergraduates
(Wrote the proofs)

PhD student
(Automation)

PhD student
(Knew the maths)

Eric Wang

Arohee Bhoja

Cayden Codel

Noah Singer

Algebra is Half the Battle: Verifying Presentations for Graded Unipotent Chevalley Groups

~~Algebra is Half the Battle: Verifying Presentations for Graded Unipotent Chevalley Groups~~

~~Algebra is Half the Battle: Verifying Presentations for Graded Unipotent Chevalley Groups~~

Alternative titles include:

~~Algebra is Half the Battle: Verifying Presentations for Graded Unipotent Chevalley Groups~~

Alternative titles include:

- Some type isomorphisms are better than others $\alpha \mid \beta \mid \alpha + \beta$

~~Algebra is Half the Battle: Verifying Presentations for Graded Unipotent Chevalley Groups~~

Alternative titles include:

- Some type isomorphisms are better than others $\alpha \mid \beta \mid \alpha + \beta$
- Surely there's a macro for that `theorem lin_of_α`

~~Algebra is Half the Battle: Verifying Presentations for Graded Unipotent Chevalley Groups~~

Alternative titles include:

- Some type isomorphisms are better than others $\alpha \mid \beta \mid \alpha + \beta$
- Surely there's a macro for that `theorem lin_of_α`
- Parentheses, begone! $a * (b * c) = (a * b) * c$

~~Algebra is Half the Battle: Verifying Presentations for Graded Unipotent Chevalley Groups~~

Alternative titles include:

- Some type isomorphisms are better than others $\alpha \mid \beta \mid \alpha + \beta$
- Surely there's a macro for that `theorem lin_of_α`
- Parentheses, begone! $a * (b * c) = (a * b) * c$
- Automation in need of automation `lin_id_inv_thms`

Warning!

I know about the math we formalized, but not much about the surrounding research context

What we proved

What we proved

We proved in Lean that three specific groups can be defined using a canonically smaller set of equations than previously known.

What we proved

We proved in Lean that three specific groups can be defined using a canonically smaller set of equations than previously known.

More specifically, we showed that the A_3, B_3-small, and B_3-large graded unipotent Chevalley groups presented by the “weak” Steinberg relations are isomorphic to the groups presented by the “full” Steinberg relations.

What we proved

We proved in Lean that three specific groups can be defined using a canonically smaller set of equations than previously known.

More specifically, we showed that the A_3, B_3-small, and B_3-large graded unipotent Chevalley groups presented by the “weak” Steinberg relations are isomorphic to the groups presented by the “full” Steinberg relations.

Our proof strategy was to show that each full relation could be derived from the weak relations. We derived each relation by solving one or more group rewriting problems.

Why we proved it

Why we proved it

Cornell University

We gratefully acknowledge support from the Simons Foundation, member institutions, and all contributors. Donate

arXiv > math > arXiv:2411.05916

Search... All fields Search

Help | Advanced Search

Mathematics > Group Theory

[Submitted on 8 Nov 2024]

Coboundary expansion inside Chevalley coset complex HDXs

Ryan O'Donnell, Noah G. Singer

Recent major results in property testing~\cite{BLM24,DDL24} and PCPs~\cite{BMV24} were unlocked by moving to high-dimensional expanders (HDXs) constructed from $\widetilde{C}_d$-type buildings, rather than the long-known $\widetilde{A}_d$-type ones. At the same time, these building quotient HDXs are not as easy to understand as the more elementary (and more symmetric/explicit) \emph{coset complex} HDXs constructed by Kaufman--Oppenheim~\cite{KO18} (of A_d-type) and O'Donnell--Pratt~\cite{OP22} (of B_d-, C_d-, D_d-type). Motivated by these considerations, we study the B_3-type generalization of a recent work of Kaufman--Oppenheim~\cite{KO21}, which showed that the A_3-type coset complex HDXs have good 1-coboundary expansion in their links, and thus yield 2-dimensional topological expanders.
The crux of Kaufman--Oppenheim's proof of 1-coboundary expansion was: (1)~identifying a group-theoretic result by Biss and Dasgupta~\cite{BD01} on small presentations for the A_3-unipotent group over~$\mathbb{F}_q$; (2)~``lifting'' it to an analogous result for an A_3-unipotent group over polynomial extensions~$\mathbb{F}_q[x]$.
For our B_3-type generalization, the analogue of~(1) appears to not hold. We manage to circumvent this with a significantly more involved strategy: (1)~getting a computer-assisted proof of vanishing 1-cohomology of B_3-type unipotent groups over~$\mathbb{F}_5$; (2)~developing significant new ``lifting'' technology to deduce the required quantitative 1-cohomology results in B_3-type unipotent groups over $\mathbb{F}_{5^k}[x]$.

Comments:	130 pages
Subjects:	**Group Theory (math.GR)**; Discrete Mathematics (cs.DM)
Cite as:	arXiv:2411.05916 **[math.GR]**
	(or arXiv:2411.05916v1 **[math.GR]** for this version)
	https://doi.org/10.48550/arXiv.2411.05916

Submission history

From: Noah Singer [view email]

[v1] Fri, 8 Nov 2024 19:00:29 UTC (134 KB)

Access Paper:

View PDF
TeX Source
Other Formats
view license

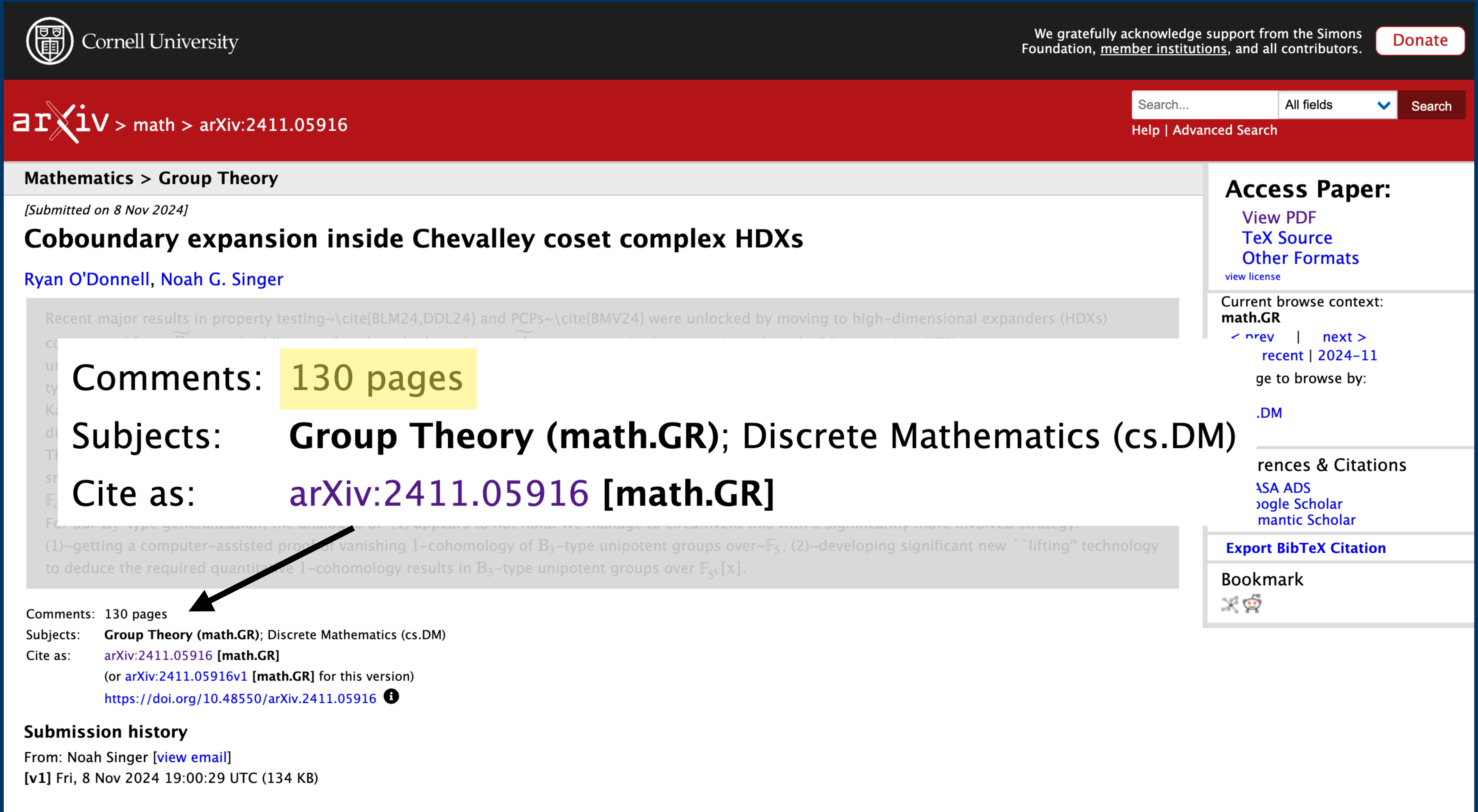
Current browse context:
math.GR
< prev | next >
new | recent | 2024-11
Change to browse by:
cs
cs.DM
math

References & Citations
NASA ADS
Google Scholar
Semantic Scholar

Export BibTeX Citation

Bookmark

Why we proved it


Cornell University

We gratefully acknowledge support from the Simons Foundation, member institutions, and all contributors.

Donate

arXiv > math > arXiv:2411.05916

Search... All fields Search

Help | Advanced Search

Mathematics > Group Theory

[Submitted on 8 Nov 2024]

Coboundary expansion inside Chevalley coset complex HDXs

Ryan O'Donnell, Noah G. Singer

Recent major results in property testing~\cite{BLM24,DDL24} and PCPs~\cite{BMV24} were unlocked by moving to high-dimensional expanders (HDXs)

(1)~getting a computer-assisted proof of vanishing 1-cohomology of B_3-type unipotent groups over~$\mathbb{F}_5$; (2)~developing significant new ``lifting'' technology to deduce the required quantitative 1-cohomology results in B_3-type unipotent groups over $\mathbb{F}_{5^k}[x]$.

Comments: 130 pages

Subjects: **Group Theory (math.GR)**; Discrete Mathematics (cs.DM)

Cite as: arXiv:2411.05916 **[math.GR]**

Comments: 130 pages

Subjects: **Group Theory (math.GR)**; Discrete Mathematics (cs.DM)

Cite as: arXiv:2411.05916 **[math.GR]**

(or arXiv:2411.05916v1 **[math.GR]** for this version)

https://doi.org/10.48550/arXiv.2411.05916

Submission history

From: Noah Singer [view email]

[v1] Fri, 8 Nov 2024 19:00:29 UTC (134 KB)

Access Paper:

View PDF

TeX Source

Other Formats

view license

Current browse context:

math.GR

< prev | next >

recent | 2024-11

ge to browse by:

.DM

rences & Citations

ASA ADS

oogle Scholar

mantic Scholar

Export BibTeX Citation

Bookmark

Why we proved it

Why we proved it

- To verify a result involving hundreds of calculations

Why we proved it

- To verify a result involving hundreds of calculations
  - Constants, negative signs, delicate computations

Why we proved it

- To verify a result involving hundreds of calculations
  - Constants, negative signs, delicate computations
  - Noah: “What if I made a mistake somewhere?”

Why we proved it

- To verify a result involving hundreds of calculations
  - Constants, negative signs, delicate computations
  - Noah: “What if I made a mistake somewhere?”
- To lay the groundwork for similar verifications

Why we proved it

- To verify a result involving hundreds of calculations
    - Constants, negative signs, delicate computations
    - Noah: “What if I made a mistake somewhere?”
- To lay the groundwork for similar verifications
    - Lots of future work left!

Why work on this problem?

Why work on this problem?

- To construct higher-dimensional expanders

Why work on this problem?

- To construct higher-dimensional expanders

Higher-dimensional expanders

(Specifically, topological expanders)

Why work on this problem?

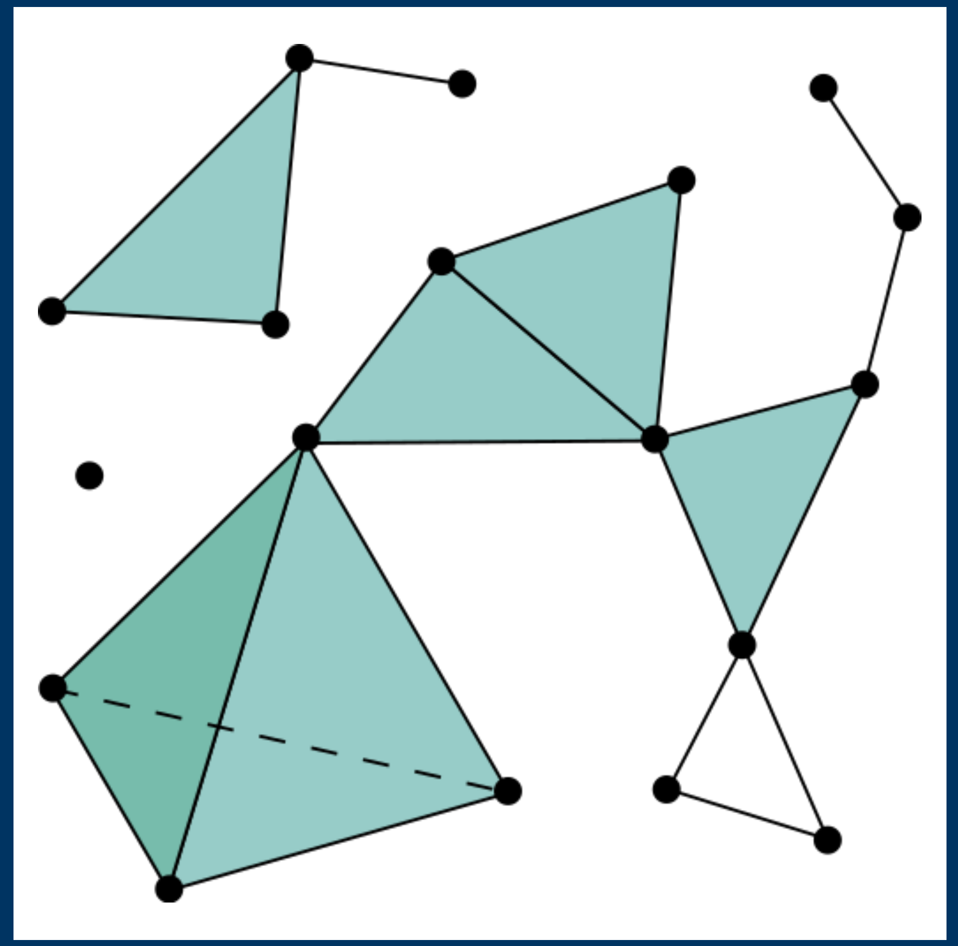
- To construct higher-dimensional expanders

Higher-dimensional expanders

(Specifically, topological expanders)

↑

Simplicial complexes



Why work on this problem?

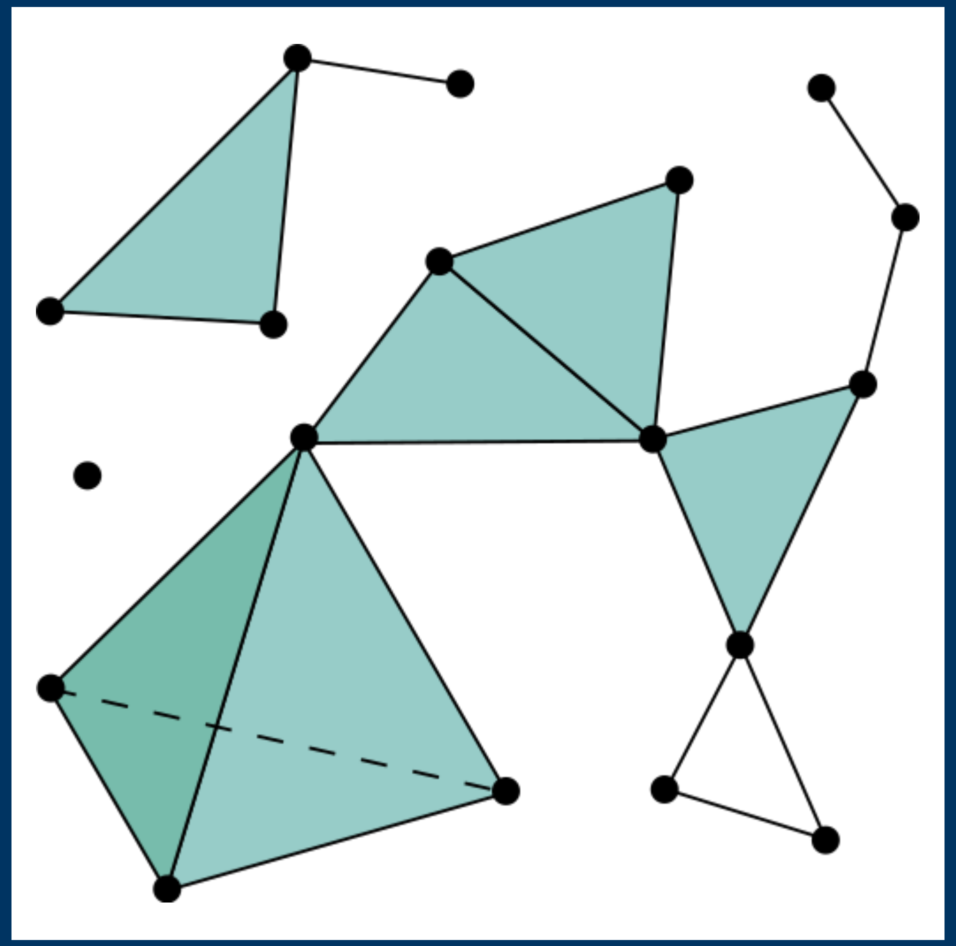
- To construct higher-dimensional expanders

Higher-dimensional expanders

(Specifically, topological expanders)

Simplicial complexes

Quotients of Bruhat-Tits buildings



Why work on this problem?

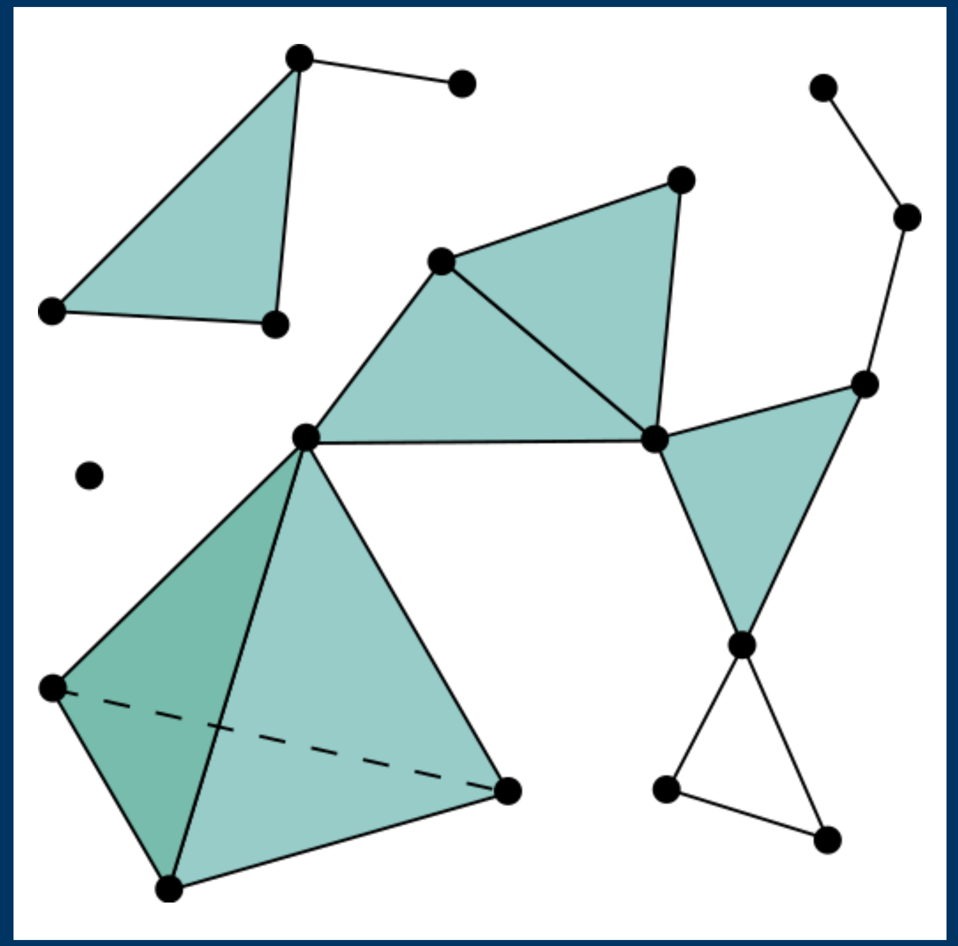
- To construct higher-dimensional expanders

Higher-dimensional expanders
(Specifically, topological expanders)

Simplicial complexes

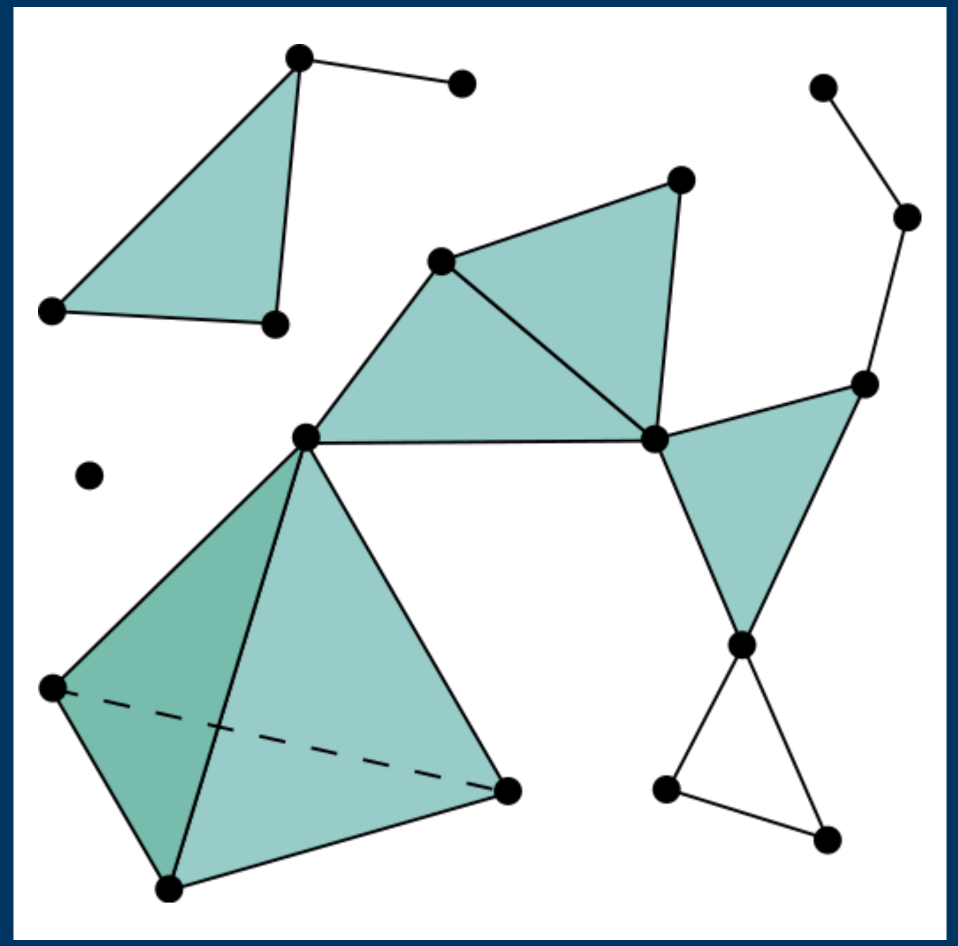
Quotients of Bruhat-Tits buildings

Coset complexes



Why work on this problem?

- To construct higher-dimensional expanders



Higher-dimensional expanders

(Specifically, topological expanders)

↑

Simplicial complexes

↗ ↖

Quotients of Bruhat-Tits buildings

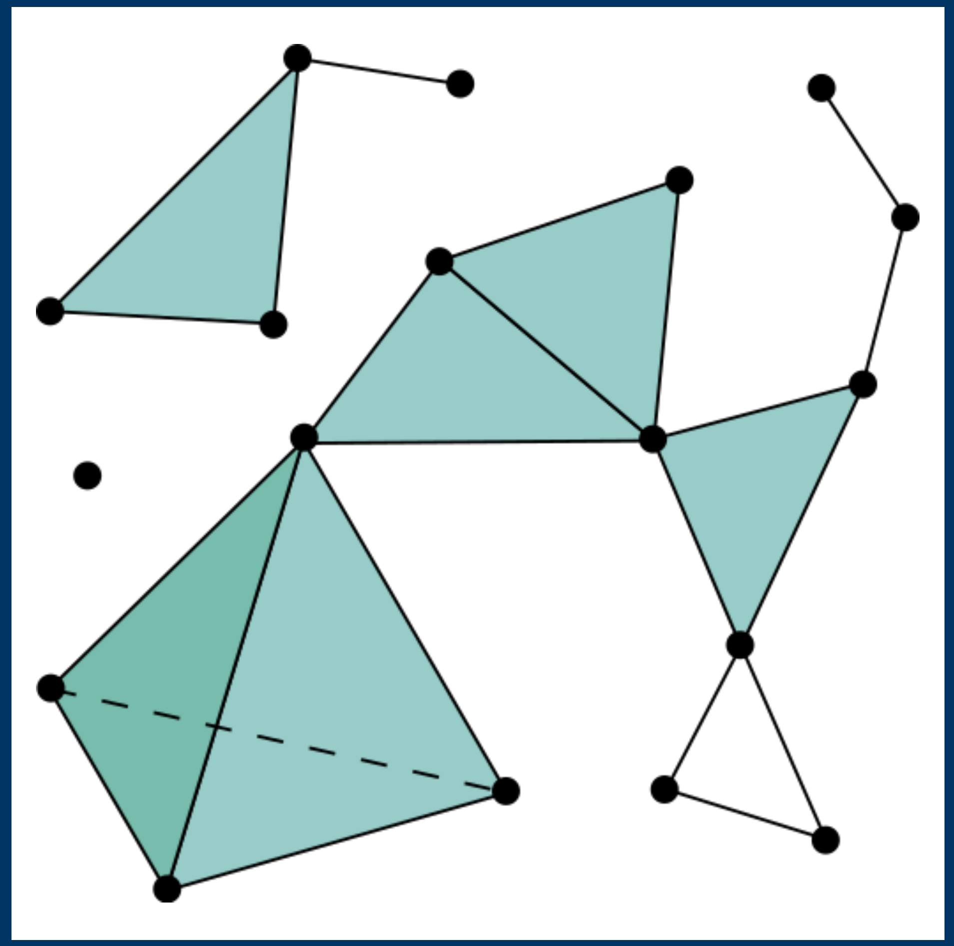
Coset complexes

↑

Chevalley groups
defined by a good set of Steinberg relations

Why work on this problem?

- To construct higher-dimensional expanders



Higher-dimensional expanders
(Specifically, topological expanders)

↑

Simplicial complexes

↗ ↖

Quotients of Bruhat-Tits buildings

Coset complexes

↑

Chevalley groups
defined by a good set of Steinberg relations

We formalized this part

Why work on this problem?

- To construct higher-dimensional expanders

Why work on this problem?

- To construct higher-dimensional expanders
  - Useful for (quantum) error correction, local property testing, and higher-dimensional geometry

Why work on this problem?

- To construct higher-dimensional expanders
  - Useful for (quantum) error correction, local property testing, and higher-dimensional geometry
- To do basic research in group theory

Chevalley groups

Chevalley groups

- Similar to Lie groups

Chevalley groups

- Similar to Lie groups
- Defined on square matrices containing field elements

Chevalley groups

- Similar to Lie groups
- Defined on square matrices containing field elements
- Express nice symmetries and geometric properties

Chevalley groups

Chevalley groups

- Fact: every Chevalley (and Lie) group can be generated from a set of generators comprising vectors and field elements.

Chevalley groups

- Fact: every Chevalley (and Lie) group can be generated from a set of generators comprising vectors and field elements.
- Group multiplication on the generators corresponds closely to geometric properties of the vectors.

Chevalley groups

- Fact: every Chevalley (and Lie) group can be generated from a set of generators comprising vectors and field elements.
- Group multiplication on the generators corresponds closely to geometric properties of the vectors.
- In our paper, these generators are either pairs or triples:

$$\{\zeta, t\} \qquad \{\zeta, i, t\}$$

Chevalley groups

- Fact: every Chevalley (and Lie) group can be generated from a set of generators comprising vectors and field elements.
- Group multiplication on the generators corresponds closely to geometric properties of the vectors.
- In our paper, these generators are either pairs or triples:

$$\{\zeta,\ t\} \qquad \{\zeta,\ i,\ t\}$$

Root (vector)

Chevalley groups

- Fact: every Chevalley (and Lie) group can be generated from a set of generators comprising vectors and field elements.
- Group multiplication on the generators corresponds closely to geometric properties of the vectors.
- In our paper, these generators are either pairs or triples:

$\{\zeta, t\}$ $\{\zeta, i, t\}$

Root (vector) Field element in $\mathbb{F}_q$

Chevalley groups

- Fact: every Chevalley (and Lie) group can be generated from a set of generators comprising vectors and field elements.
- Group multiplication on the generators corresponds closely to geometric properties of the vectors.
- In our paper, these generators are either pairs or triples:

$$\{\zeta,\ t\} \qquad\qquad \{\zeta,\ i,\ t\}$$

Degree

Root (vector) Field element in $\mathbb{F}_q$

Chevalley groups

- Fact: every Chevalley (and Lie) group can be generated from a set of generators comprising vectors and field elements.
- Group multiplication on the generators corresponds closely to geometric properties of the vectors.
- In our paper, these generators are either pairs or triples:

$\{\zeta, t\}$ $\{\zeta, i, t\}$

Degree

Root (vector) Field element in $\mathbb{F}_q$

```
structure GradedChevalleyGenerator
    (Φ : Type TΦ) [PositiveRootSystem Φ]
    (R : Type TR) [Ring R]
where
  ζ : Φ -- root
  i : ℕ -- degree
  hi : i ≤ height ζ
  t : R -- field coefficient
```

Chevalley groups

Chevalley groups

- These generators have nice properties:

Chevalley groups

- These generators have nice properties:
  - Linearity: $\{\zeta, i, t\} \cdot \{\zeta, i, u\} = \{\zeta, i, t + u\}$

Chevalley groups

- These generators have nice properties:
  - Linearity: $\{\zeta, i, t\} \cdot \{\zeta, i, u\} = \{\zeta, i, t + u\}$
  - Identity: $\{\zeta, i, 0\} = 1$

Chevalley groups

- These generators have nice properties:
  - Linearity: $\{\zeta, i, t\} \cdot \{\zeta, i, u\} = \{\zeta, i, t+u\}$
  - Identity: $\{\zeta, i, 0\} = 1$
  - Inverse: $\{\zeta, i, t\}^{-1} = \{\zeta, i, -t\}$

Chevalley groups

- These generators have nice properties:
  - Linearity: $\{\zeta, i, t\} \cdot \{\zeta, i, u\} = \{\zeta, i, t + u\}$
  - Identity: $\{\zeta, i, 0\} = 1$
  - Inverse: $\{\zeta, i, t\}^{-1} = \{\zeta, i, -t\}$
  - Commutator: For any pair of roots ζ and η, the commutator is a product of generators of the following form, for Chevalley constants a, b, and $C^{a,b}_{\zeta,\eta} \in [-3,3]$:

$$[\{\zeta, i, t\}, \{\eta, j, u\}] = \Pi \ \{a\zeta + b\eta, ai + bj, C^{a,b}_{\zeta,\eta} t^a u^b\}$$

Chevalley groups

- These generators have nice properties:
  - Linearity: $\{\zeta, i, t\} \cdot \{\zeta, i, u\} = \{\zeta, i, t+u\}$
  - Identity: $\{\zeta, i, 0\} = 1$
  - Inverse: $\{\zeta, i, t\}^{-1} = \{\zeta, i, -t\}$
  - Commutator: For any pair of roots ζ and η, the commutator is a product of generators of the following form, for Chevalley constants a, b, and $C^{a,b}_{\zeta,\eta} \in [-3,3]$:

$$[\{\zeta, i, t\}, \{\eta, j, u\}] = \Pi \ \{a\zeta + b\eta, ai + bj, C^{a,b}_{\zeta,\eta} t^a u^b\}$$

As far as I know, these constants don't follow any pattern, and are hard-coded in our formalization

Chevalley groups

- These generators have nice properties:
  - Linearity: $\{\zeta, i, t\} \cdot \{\zeta, i, u\} = \{\zeta, i, t+u\}$
  - Identity: $\{\zeta, i, 0\} = 1$
  - Inverse: $\{\zeta, i, t\}^{-1} = \{\zeta, i, -t\}$
  - Commutator: For any pair of roots ζ and η, the commutator is a product of generators of the following form, for Chevalley constants a, b, and $C_{\zeta,\eta}^{a,b} \in [-3,3]$:

$$[\{\zeta, i, t\}, \{\eta, j, u\}] = \prod \{a\zeta + b\eta, ai + bj, C_{\zeta,\eta}^{a,b} t^a u^b\}$$

These are (some of the) Steinberg relations

As far as I know, these constants don't follow any pattern, and are hard-coded in our formalization

Presentations (not the academic kind)

Presentations (not the academic kind)

We specify these Chevalley groups with a presentation:

Presentations (not the academic kind)

We specify these Chevalley groups with a presentation:

- Roughly, a presentation is a string rewriting system on a set of generator symbols S, modulo a set of relations R

Presentations (not the academic kind)

We specify these Chevalley groups with a presentation:

- Roughly, a presentation is a string rewriting system on a set of generator symbols S, modulo a set of relations R
- The identity element is the empty string ϵ

Presentations (not the academic kind)

We specify these Chevalley groups with a presentation:

- Roughly, a presentation is a string rewriting system on a set of generator symbols S, modulo a set of relations R

- The identity element is the empty string ϵ

- Examples:

Presentations (not the academic kind)

We specify these Chevalley groups with a presentation:

- Roughly, a presentation is a string rewriting system on a set of generator symbols S, modulo a set of relations R

- The identity element is the empty string ϵ

- Examples:

  - $\langle \{x\} \mid \{x^n\} \rangle \cong (\mathbb{Z}, +)$

Presentations (not the academic kind)

We specify these Chevalley groups with a presentation:

- Roughly, a presentation is a string rewriting system on a set of generator symbols S, modulo a set of relations R
- The identity element is the empty string ϵ
- Examples:
  - $\langle \{x\} \mid \{x^n\} \rangle \cong (\mathbb{Z}, +)$
  - $\langle \{x, y\} \mid \{xyx^{-1}y^{-1}\} \rangle \cong (\mathbb{Z} \times \mathbb{Z}, +)$

Presentations (not the academic kind)

We specify these Chevalley groups with a presentation:

- Roughly, a presentation is a string rewriting system on a set of generator symbols S, modulo a set of relations R
- The identity element is the empty string ϵ
- Examples:
  - $\langle \{x\} \mid \{x^n\} \rangle \cong (\mathbb{Z}, +)$
  - $\langle \{x, y\} \mid \{xyx^{-1}y^{-1}\} \rangle \cong (\mathbb{Z} \times \mathbb{Z}, +)$

Presentations give a succinct way of specifying groups

Presentations (not the academic kind)

We specify these Chevalley groups with a presentation:

- Roughly, a presentation is a string rewriting system on a set of generator symbols S, modulo a set of relations R
- The identity element is the empty string ϵ
- Examples:
  - $\langle \{x\} \mid \{x^n\} \rangle \cong (\mathbb{Z}, +)$
  - $\langle \{x, y\} \mid \{xyx^{-1}y^{-1}\} \rangle \cong (\mathbb{Z} \times \mathbb{Z}, +)$

Equivalently, G is the free group on S modulo the normal closure of R in S

Presentations give a succinct way of specifying groups

An example calculation

An example calculation

Assume the weak Steinberg relations. Then we want to show the full relation

$$\{\beta + \psi + \omega, i, t\}\{\beta + \psi + \omega, i, u\} = \{\beta + \psi + \omega, i, t + u\}$$

An example calculation

Assume the weak Steinberg relations. Then we want to show the full relation

$$\{\beta+\psi+\omega, i, t\}\{\beta+\psi+\omega, i, u\} = \{\beta+\psi+\omega, i, t+u\}$$

Proof. Decompose i arbitrarily into $i = i_1 + i_2$. Then

An example calculation

Assume the weak Steinberg relations. Then we want to show the full relation

$$\{\beta+\psi+\omega, i, t\}\{\beta+\psi+\omega, i, u\} = \{\beta+\psi+\omega, i, t+u\}$$

Proof. Decompose i arbitrarily into $i = i_1 + i_2$. Then

$\{\beta+\psi+\omega, i, t\}\{\beta+\psi+\omega, i, u\}$

An example calculation

Assume the weak Steinberg relations. Then we want to show the full relation

$$\{\beta+\psi+\omega, i, t\}\{\beta+\psi+\omega, i, u\} = \{\beta+\psi+\omega, i, t+u\}$$

Proof. Decompose i arbitrarily into $i = i_1 + i_2$. Then

$$\underline{\{\beta+\psi+\omega, i, t\}}\{\beta+\psi+\omega, i, u\}$$

$$= \underline{\{\beta, i_1, t\}\{\psi+\omega, i_2, 1\}\{\beta, i_1, -t\}\{\psi+\omega, i_2, -1\}}\{\beta+\omega+\psi, i, u\}$$

An example calculation

Assume the weak Steinberg relations. Then we want to show the full relation

$$\{\beta+\psi+\omega, i, t\}\{\beta+\psi+\omega, i, u\} = \{\beta+\psi+\omega, i, t+u\}$$

Proof. Decompose i arbitrarily into $i = i_1 + i_2$. Then

$$\{\beta+\psi+\omega, i, t\}\{\beta+\psi+\omega, i, u\}$$

$$= \{\beta, i_1, t\}\{\psi+\omega, i_2, 1\}\{\beta, i_1, -t\}\{\psi+\omega, i_2, -1\}\underline{\{\beta+\omega+\psi, i, u\}}$$

$$= \{\beta, i_1, t\}\underline{\{\beta+\omega+\psi, i, u\}}\{\psi+\omega, i_2, 1\}\{\beta, i_1, -t\}\{\psi+\omega, i_2, -1\}$$

An example calculation

Assume the weak Steinberg relations. Then we want to show the full relation

$$\{\beta+\psi+\omega, i, t\}\{\beta+\psi+\omega, i, u\} = \{\beta+\psi+\omega, i, t+u\}$$

Proof. Decompose i arbitrarily into $i = i_1 + i_2$. Then

$$\{\beta+\psi+\omega, i, t\}\{\beta+\psi+\omega, i, u\}$$

$$= \{\beta, i_1, t\}\{\psi+\omega, i_2, 1\}\{\beta, i_1, -t\}\{\psi+\omega, i_2, -1\}\{\beta+\omega+\psi, i, u\}$$

$$= \{\beta, i_1, t\}\underline{\{\beta+\omega+\psi, i, u\}}\{\psi+\omega, i_2, 1\}\{\beta, i_1, -t\}\{\psi+\omega, i_2, -1\}$$

$$= \{\beta, i_1, t\}\underline{\{\beta, i_1, u\}\{\psi+\omega, i_2, 1\}\{\beta, i_1, -u\}\{\psi+\omega, i_2, -1\}}\{\psi+\omega, i_2, 1\}\{\beta, i_1, -t\}\{\psi+\omega, i_2, -1\}$$

An example calculation

Assume the weak Steinberg relations. Then we want to show the full relation

$$\{\beta+\psi+\omega, i, t\}\{\beta+\psi+\omega, i, u\} = \{\beta+\psi+\omega, i, t+u\}$$

Proof. Decompose i arbitrarily into $i = i_1 + i_2$. Then

$$\{\beta+\psi+\omega, i, t\}\{\beta+\psi+\omega, i, u\}$$

$$= \{\beta, i_1, t\}\{\psi+\omega, i_2, 1\}\{\beta, i_1, -t\}\{\psi+\omega, i_2, -1\}\{\beta+\omega+\psi, i, u\}$$

$$= \{\beta, i_1, t\}\{\beta+\omega+\psi, i, u\}\{\psi+\omega, i_2, 1\}\{\beta, i_1, -t\}\{\psi+\omega, i_2, -1\}$$

$$= \underline{\{\beta, i_1, t\}\{\beta, i_1, u\}}\{\psi+\omega, i_2, 1\}\{\beta, i_1, -u\}\underline{\{\psi+\omega, i_2, -1\}\{\psi+\omega, i_2, 1\}}\{\beta, i_1, -t\}\{\psi+\omega, i_2, -1\}$$

$$= \underline{\{\beta, i_1, t+u\}}\{\psi+\omega, i_2, 1\}\{\beta, i_1, -u\}\underline{\{\psi+\omega, i_2, 0\}}\{\beta, i_1, -t\}\{\psi+\omega, i_2, -1\}$$

An example calculation

Assume the weak Steinberg relations. Then we want to show the full relation

$$\{\beta+\psi+\omega, i, t\}\{\beta+\psi+\omega, i, u\} = \{\beta+\psi+\omega, i, t+u\}$$

Proof. Decompose i arbitrarily into $i = i_1 + i_2$. Then

$$\begin{aligned}
&\{\beta+\psi+\omega, i, t\}\{\beta+\psi+\omega, i, u\} \\
&= \{\beta, i_1, t\}\{\psi+\omega, i_2, 1\}\{\beta, i_1, -t\}\{\psi+\omega, i_2, -1\}\{\beta+\omega+\psi, i, u\} \\
&= \{\beta, i_1, t\}\{\beta+\omega+\psi, i, u\}\{\psi+\omega, i_2, 1\}\{\beta, i_1, -t\}\{\psi+\omega, i_2, -1\} \\
&= \{\beta, i_1, t\}\{\beta, i_1, u\}\{\psi+\omega, i_2, 1\}\{\beta, i_1, -u\}\{\psi+\omega, i_2, -1\}\{\psi+\omega, i_2, 1\}\{\beta, i_1, -t\}\{\psi+\omega, i_2, -1\} \\
&= \{\beta, i_1, t+u\}\{\psi+\omega, i_2, 1\}\underline{\{\beta, i_1, -u\}}\{\psi+\omega, i_2, 0\}\underline{\{\beta, i_1, -t\}}\{\psi+\omega, i_2, -1\} \\
&= \{\beta, i_1, t+u\}\{\psi+\omega, i_2, 1\}\underline{\{\beta, i_1, -(t+u)\}}\{\psi+\omega, i_2, -1\}
\end{aligned}$$

An example calculation

Assume the weak Steinberg relations. Then we want to show the full relation

$$\{\beta+\psi+\omega, i, t\}\{\beta+\psi+\omega, i, u\} = \{\beta+\psi+\omega, i, t+u\}$$

Proof. Decompose i arbitrarily into $i = i_1 + i_2$. Then

$$\begin{aligned}
&\{\beta+\psi+\omega, i, t\}\{\beta+\psi+\omega, i, u\} \\
&= \{\beta, i_1, t\}\{\psi+\omega, i_2, 1\}\{\beta, i_1, -t\}\{\psi+\omega, i_2, -1\}\{\beta+\omega+\psi, i, u\} \\
&= \{\beta, i_1, t\}\{\beta+\omega+\psi, i, u\}\{\psi+\omega, i_2, 1\}\{\beta, i_1, -t\}\{\psi+\omega, i_2, -1\} \\
&= \{\beta, i_1, t\}\{\beta, i_1, u\}\{\psi+\omega, i_2, 1\}\{\beta, i_1, -u\}\{\psi+\omega, i_2, -1\}\{\psi+\omega, i_2, 1\}\{\beta, i_1, -t\}\{\psi+\omega, i_2, -1\} \\
&= \{\beta, i_1, t+u\}\{\psi+\omega, i_2, 1\}\{\beta, i_1, -u\}\{\psi+\omega, i_2, 0\}\{\beta, i_1, -t\}\{\psi+\omega, i_2, -1\} \\
&= \{\beta, i_1, t+u\}\{\psi+\omega, i_2, 1\}\{\beta, i_1, -(t+u)\}\{\psi+\omega, i_2, -1\} \\
&= \{\beta+\psi+\omega, i_1+i_2, t+u\}
\end{aligned}$$

An example calculation

Assume the weak Steinberg relations. Then we want to show the full relation

$$\{\beta+\psi+\omega, i, t\}\{\beta+\psi+\omega, i, u\} = \{\beta+\psi+\omega, i, t+u\}$$

Proof. Decompose i arbitrarily into $i = i_1 + i_2$. Then

$$
\begin{aligned}
&\{\beta+\psi+\omega, i, t\}\{\beta+\psi+\omega, i, u\} \\
&= \{\beta, i_1, t\}\{\psi+\omega, i_2, 1\}\{\beta, i_1, -t\}\{\psi+\omega, i_2, -1\}\{\beta+\omega+\psi, i, u\} \\
&= \{\beta, i_1, t\}\{\beta+\omega+\psi, i, u\}\{\psi+\omega, i_2, 1\}\{\beta, i_1, -t\}\{\psi+\omega, i_2, -1\} \\
&= \{\beta, i_1, t\}\{\beta, i_1, u\}\{\psi+\omega, i_2, 1\}\{\beta, i_1, -u\}\{\psi+\omega, i_2, -1\}\{\psi+\omega, i_2, 1\}\{\beta, i_1, -t\}\{\psi+\omega, i_2, -1\} \\
&= \{\beta, i_1, t+u\}\{\psi+\omega, i_2, 1\}\{\beta, i_1, -u\}\{\psi+\omega, i_2, 0\}\{\beta, i_1, -t\}\{\psi+\omega, i_2, -1\} \\
&= \{\beta, i_1, t+u\}\{\psi+\omega, i_2, 1\}\{\beta, i_1, -(t+u)\}\{\psi+\omega, i_2, -1\} \\
&= \{\beta+\psi+\omega, \underline{i_1+i_2}, t+u\} \\
&= \{\beta+\psi+\omega, \underline{i}, t+u\}
\end{aligned}
$$

An example calculation

Assume the weak Steinberg relations. Then we want to show the full relation

$$\{\beta+\psi+\omega, i, t\}\{\beta+\psi+\omega, i, u\} = \{\beta+\psi+\omega, i, t+u\}$$

Proof. Decompose i arbitrarily into $i = i_1 + i_2$. Then …

```
@[simp, chev_simps]
theorem lin_of_βψω : ∀ (i : N) (t u : F),
    {βψω, i, t} * {βψω, i, u} = {βψω, i, t + u} := by
  intro i hi t u
  rcases decompose i with ⟨i₁, i₂⟩    -- i = i₁ + i₂
  grw [ expr_βψω_as_β_ψω_β_ψω,                          -- Line 1
        expr_βψω_ψω_as_ψω_βψω, expr_βψω_β_as_β_βψω,     -- Line 2
        expr_βψω_ψω_as_ψω_βψω,                          -- Line 3
        mul_one u, expr_βψω_as_β_ψω_β_ψω,               -- Line 5
        mul_one (t + u), expr_βψω_as_β_ψω_β_ψω ]        -- Line 6
```

An example calculation

Assume the weak Steinberg relations. Then we want to show the full relation

$$\{\beta+\psi+\omega, i, t\}\{\beta+\psi+\omega, i, u\} = \{\beta+\psi+\omega, i, t+u\}$$

Proof. Decompose i arbitrarily into $i = i_1 + i_2$. Then …

```
@[simp, chev_simps]
theorem lin_of_βψω : lin_of_root((weakB3SmallGraded F).project, βψω) :=
by
  intro i hi t u
  rcases decompose 1 2 i hi with ⟨i₁, i₂, rfl, hi₁, hi₂⟩
  rw [←mul_one t, expr_βψω_as_β_ψω_β_ψω Fchar hi₁ hi₂]
  grw [←expr_βψω_ψω_as_ψω_βψω Fchar, ←expr_βψω_β_as_β_βψω Fchar,
  ←expr_βψω_ψω_as_ψω_βψω Fchar]
  rw [←mul_one u]
  grw [expr_βψω_as_β_ψω_β_ψω Fchar hi₁ hi₂]
  rw [←mul_one (t + u)]
  grw [expr_βψω_as_β_ψω_β_ψω Fchar hi₁ hi₂]
  ring_nf
```

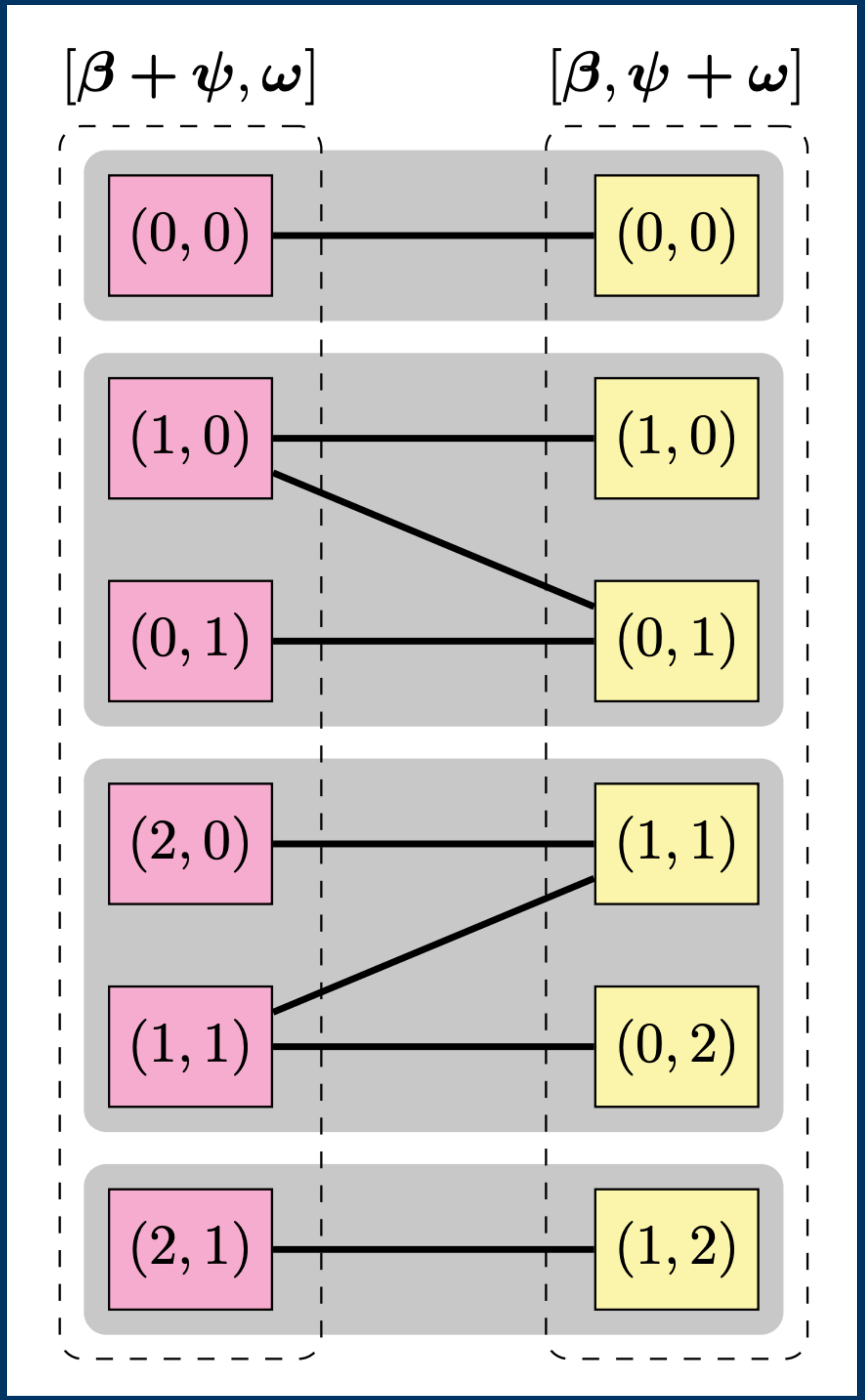
Our proof strategy

Our proof strategy

Almost all of the proofs in our formalization look like that calculation.

Our proof strategy

Almost all of the proofs in our formalization look like that calculation.



Our proof strategy

Almost all of the proofs in our formalization look like that calculation.

Our proof strategy

Almost all of the proofs in our formalization look like that calculation.

Sometimes it's worse:

```
theorem expand_βψω_as_commutator_of_βψ_ω :
  forall_ij_tu 2 1, ⸨βψω, i + j, 2 * t * u⸩ = ⁅⸨βψ, i, t⸩, ⸨ω, j, u⸩⁆ := by
  intro i j hi hj t u
  match i, j with
  | 0, 0 => rw [expr_βψω_as_comm_of_βψ_ω_00 Fchar]
  | 0, 1 => rw [expr_βψω_as_comm_of_βψ_ω_01 Fchar]
  | 1, 0 => rw [expr_βψω_as_comm_of_βψ_ω_10 Fchar]
  | 1, 1 => rw [expr_βψω_as_comm_of_βψ_ω_11 Fchar]
  | 2, 0 => rw [expr_βψω_as_comm_of_βψ_ω_20 Fchar]
  | 2, 1 => rw [expr_βψω_as_comm_of_βψ_ω_21 Fchar]
```

Our proof strategy

Almost all of the proofs in our formalization look like that calculation.

Sometimes it's worse:

Sometimes it's better (i.e. we get proofs for free):

```
-- height 2 (reflection of height 1)
declare_B3Small_reflected_thm F b3small_valid βψω β ψω const 1 heights 2 1 1 to 1 0 1
declare_B3Small_reflected_thm F b3small_valid βψω β ψω const 1 heights 2 0 2 to 1 1 0
declare_B3Small_reflected_thm F b3small_valid βψω βψ ω const 2 heights 2 2 0 to 1 0 1
declare_B3Small_reflected_thm F b3small_valid βψω βψ ω const 2 heights 2 1 1 to 1 1 0
declare_B3Small_reflected_thm F b3small_valid βψω β ψω const 1 heights 3 1 2 to 0 0 0
declare_B3Small_reflected_thm F b3small_valid βψω βψ ω const 2 heights 3 2 1 to 0 0 0
```

Design decision: defining roots

Design decision: defining roots

In this paper, we work with root systems

$$\alpha := e_2 - e_3 \qquad \psi := e_3$$

Design decision: defining roots

In this paper, we work with root systems

$$\alpha := e_2 - e_3 \qquad \psi := e_3$$

$$B_3\text{small} := \{\beta, \psi, \omega, \beta + \omega, \omega + \psi, \beta + \omega + \psi, \beta + 2\psi\}$$

Design decision: defining roots

In this paper, we work with root systems

$$\alpha := e_2 - e_3 \qquad \psi := e_3$$

In Lean, we manually defined the roots

$$B_3\text{small} := \{\beta, \psi, \omega, \beta + \omega, \omega + \psi, \beta + \omega + \psi, \beta + 2\psi\}$$

Design decision: defining roots

In this paper, we work with root systems

$$\alpha := e_2 - e_3 \qquad \psi := e_3$$

In Lean, we manually defined the roots

$$B_3\text{small} := \{\beta, \psi, \omega, \beta + \omega, \omega + \psi, \beta + \omega + \psi, \beta + 2\psi\}$$

```
inductive B3SmallPosRoot
  | β | ψ | ω | βψ | ψω | β2ψ | βψω
```

Design decision: defining roots

In this paper, we work with root systems

In Lean, we manually defined the roots

$$\alpha := e_2 - e_3 \qquad \psi := e_3$$

$$B_3\text{small} := \{\beta, \psi, \omega, \beta + \omega, \omega + \psi, \beta + \omega + \psi, \beta + 2\psi\}$$

```
inductive B3SmallPosRoot
  | β | ψ | ω | βψ | ψω | β2ψ | βψω
```

```
def height : B3SmallPosRoot → Nat
  | β | ψ | ω => 1
  | βψ | ψω => 2
  | βψω | β2ψ => 3
```

Design decision: defining roots

In this paper, we work with root systems

$$\alpha := e_2 - e_3 \qquad \psi := e_3$$

In Lean, we manually defined the roots

Advantage: never wrong; disadvantage: loses the “vector” properties

$$B_3\text{small} := \{\beta, \psi, \omega, \beta + \omega, \omega + \psi, \beta + \omega + \psi, \beta + 2\psi\}$$

```
inductive B3SmallPosRoot
  | β | ψ | ω | βψ | ψω | β2ψ | βψω
```

```
def height : B3SmallPosRoot → Nat
  | β | ψ | ω => 1
  | βψ | ψω => 2
  | βψω | β2ψ => 3
```

Design decision: defining roots

In this paper, we work with root systems

$\alpha := e_2 - e_3 \qquad \psi := e_3$

In Lean, we manually defined the roots

Advantage: never wrong; disadvantage: loses the “vector” properties

$$B_3\text{small} := \{\beta, \psi, \omega, \beta + \omega, \omega + \psi, \beta + \omega + \psi, \beta + 2\psi\}$$

```
inductive B3SmallPosRoot
  | β | ψ | ω | βψ | ψω | β2ψ | βψω
```

```
def height : B3SmallPosRoot → Nat
  | β | ψ | ω => 1
  | βψ | ψω => 2
  | βψω | β2ψ => 3
```

Some type isomorphisms are better than others

Design decision: macros

Design decision: macros

Many proofs were the exact same, differing only by the root.

Design decision: macros

Many proofs were the exact same, differing only by the root.

$$\{\zeta, i, t\} \cdot \{\zeta, i, u\} = \{\zeta, i, t + u\}$$

Design decision: macros

Many proofs were the exact same, differing only by the root.

$$\{\zeta, i, t\} \cdot \{\zeta, i, u\} = \{\zeta, i, t + u\}$$

$$[\{\beta, i, t\}, \{\beta + \psi, j, t\}] = 1$$

Design decision: macros

Many proofs were the exact same, differing only by the root.

Solution: use macros to write the theorems for us!

$$\{\zeta, i, t\} \cdot \{\zeta, i, u\} = \{\zeta, i, t + u\}$$

$$[\{\beta, i, t\}, \{\beta + \psi, j, t\}] = 1$$

Design decision: macros

Many proofs were the exact same, differing only by the root.

Solution: use macros to write the theorems for us!

$$\{\zeta, i, t\} \cdot \{\zeta, i, u\} = \{\zeta, i, t + u\}$$

$$[\{\beta, i, t\}, \{\beta + \psi, j, t\}] = 1$$

```
declare_B3Small_lin_id_inv_thms F β
declare_B3Small_lin_id_inv_thms F ψ
declare_B3Small_lin_id_inv_thms F ω
declare_B3Small_lin_id_inv_thms F βψ
declare_B3Small_lin_id_inv_thms F ψω
declare_B3Small_lin_id_inv_thms F β2ψ

declare_B3Small_trivial_span_of_root_pair_thms F β βψ
declare_B3Small_trivial_span_of_root_pair_thms F β β2ψ
declare_B3Small_trivial_span_of_root_pair_thms F ψ β2ψ
declare_B3Small_trivial_span_of_root_pair_thms F βψ β2ψ
declare_B3Small_trivial_span_of_root_pair_thms F β ω
declare_B3Small_trivial_span_of_root_pair_thms F ψ ψω
declare_B3Small_trivial_span_of_root_pair_thms F ω ψω

declare_B3Small_single_span_of_root_pair_thms F ψ ω ψω 2
declare_B3Small_single_span_of_root_pair_thms F ψ βψ β2ψ 2

/-! ### Mixed-degree theorem for specific roots -/

declare_B3Small_mixed_degree_thms F βψ
```

Design decision: macros

Many proofs were the exact same, differing only by the root.

Solution: use macros to write the theorems for us!

$$\{\zeta, i, t\} \cdot \{\zeta, i, u\} = \{\zeta, i, t+u\}$$

$$[\{\beta, i, t\}, \{\beta+\psi, j, t\}] = 1$$

Problem: need to declare the macros for each root system

```
declare_B3Small_lin_id_inv_thms F β
declare_B3Small_lin_id_inv_thms F ψ
declare_B3Small_lin_id_inv_thms F ω
declare_B3Small_lin_id_inv_thms F βψ
declare_B3Small_lin_id_inv_thms F ψω
declare_B3Small_lin_id_inv_thms F β2ψ

declare_B3Small_trivial_span_of_root_pair_thms F β βψ
declare_B3Small_trivial_span_of_root_pair_thms F β β2ψ
declare_B3Small_trivial_span_of_root_pair_thms F ψ β2ψ
declare_B3Small_trivial_span_of_root_pair_thms F βψ β2ψ
declare_B3Small_trivial_span_of_root_pair_thms F β ω
declare_B3Small_trivial_span_of_root_pair_thms F ψ ψω
declare_B3Small_trivial_span_of_root_pair_thms F ω ψω

declare_B3Small_single_span_of_root_pair_thms F ψ ω ψω 2
declare_B3Small_single_span_of_root_pair_thms F ψ βψ β2ψ 2

/-! ### Mixed-degree theorem for specific roots -/

declare_B3Small_mixed_degree_thms F βψ
```

Design decision: macros

Many proofs were the exact same, differing only by the root.

Solution: use macros to write the theorems for us!

$$\{\zeta, i, t\} \cdot \{\zeta, i, u\} = \{\zeta, i, t + u\}$$

$$[\{\beta, i, t\}, \{\beta + \psi, j, t\}] = 1$$

Problem: need to declare the macros for each root system

Solution: a macro to declare macros?

```
declare_B3Small_lin_id_inv_thms F β
declare_B3Small_lin_id_inv_thms F ψ
declare_B3Small_lin_id_inv_thms F ω
declare_B3Small_lin_id_inv_thms F βψ
declare_B3Small_lin_id_inv_thms F ψω
declare_B3Small_lin_id_inv_thms F β2ψ

declare_B3Small_trivial_span_of_root_pair_thms F β βψ
declare_B3Small_trivial_span_of_root_pair_thms F β β2ψ
declare_B3Small_trivial_span_of_root_pair_thms F ψ β2ψ
declare_B3Small_trivial_span_of_root_pair_thms F βψ β2ψ
declare_B3Small_trivial_span_of_root_pair_thms F β ω
declare_B3Small_trivial_span_of_root_pair_thms F ψ ψω
declare_B3Small_trivial_span_of_root_pair_thms F ω ψω

declare_B3Small_single_span_of_root_pair_thms F ψ ω ψω 2
declare_B3Small_single_span_of_root_pair_thms F ψ βψ β2ψ 2

/-! ### Mixed-degree theorem for specific roots -/

declare_B3Small_mixed_degree_thms F βψ
```

Paint point: parentheses

Paint point: parentheses

Problem: commute two terms not in the same set of parentheses

Paint point: parentheses

Problem: commute two terms not in the same set of parentheses

$$a * (b * c) = b * (a * c)$$

Paint point: parentheses

Problem: commute two terms not in the same set of parentheses

Solution: the `grw` tactic and `g_reassoc_of%` (borrowed from category theory)

$$a * (b * c) = b * (a * c)$$

Paint point: parentheses

Problem: commute two terms not in the same set of parentheses

Solution: the `grw` tactic and `g_reassoc_of%` (borrowed from category theory)

Benefit: combine with `chev_simps` for automatic simplification

$$a * (b * c) = b * (a * c)$$

Paint point: parentheses

Problem: commute two terms not in the same set of parentheses

Solution: the `grw` tactic and `g_reassoc_of%` (borrowed from category theory)

Benefit: combine with `chev_simps` for automatic simplification

$$a * (b * c) = b * (a * c)$$

$$\{\beta, i, t\} \cdot \{\beta, i, -t\} \implies \{\beta, i, 0\} \implies 1$$

Other pain points

Other pain points

Presentation relations vs. equations

Other pain points

Presentation relations vs. equations

$$[\{\beta, i, t\}, \{\beta + \psi, j, u\}] = 1$$

$$\Leftrightarrow$$

$$\{\beta, i, t\} \cdot \{\beta + \psi, j, u\} \cdot \{\beta, i, -t\} \cdot \{\beta + \psi, j, -u\} = 1$$

$$\Leftrightarrow$$

$$\{\beta, i, t\} \cdot \{\beta + \psi, j, u\} = \{\beta + \psi, j, u\} \cdot \{\beta, i, t\}$$

Other pain points

Other pain points

Group/field arithmetic often needed massaging to discharge with automation

Other pain points

Group/field arithmetic often needed massaging to discharge with automation

```
have aux₁ : 2 * (u / (2 * t)) = u / t := by ring_nf; field_simp; group
have aux₂ : u / (2 * t) * (u / (2 * t)) = (u * u) / (4 * (t * t)) := by
  ring_nf; simp only [inv_pow, mul_eq_mul_left_iff, inv_inj, mul_eq_zero, ne_eq,
    OfNat.ofNat_ne_zero, not_false_eq_true, pow_eq_zero_iff, inv_eq_zero];
  left
  rw [pow_two, mul_two, two_add_two_eq_four]
```

Thank you for your attention

`https://github.com/singerng/steinberg-formalization`

$\{\zeta,\ t\}$

$\{\zeta,\ i,\ t\}$

Degree

Root (vector)

Field element in $\mathbb{F}_q$

$$\alpha \mid \beta \mid \alpha + \beta$$

theorem lin_of_α

$$a * (b * c) = (a * b) * c$$

lin_id_inv_thms

What we proved

Nonnegative span of a set of
basis vectors

Polynomials with
degrees at most d

Graded unipotent Chevalley groups:
A_3, B_3-small, and B_3-large

We showed through calculation that three specific groups
can be defined by a canonically smaller set of equations
than previously known.

Defined by the presentation on

Steinberg relations