Torsion units in integral group rings of sporadic simple groups

National University of Ireland, Galway

Alexander Konovalov

School of Computer Science
and
Centre for Interdisciplinary Research in Computational Algebra
University of St Andrews

November 22, 2007

Outline

Our notation

G – finite group

$\mathbb{Z}G$ – its integral group ring

$$\mathbb{Z}G = \left\{ \sum_{g \in G} \lambda_g g \;\middle|\; \lambda_g \in \mathbb{Z} \right\}$$

$U(\mathbb{Z}G)$ – group of units of $\mathbb{Z}G$

Normalized unit group of $\mathbb{Z}G$

$$V(\mathbb{Z}G) = \{ \sum \alpha_g g \mid \sum \alpha_g = 1 \} \subseteq U(\mathbb{Z}G)$$

Studying torsion units

General question

Which torsion units can appear in $\mathbb{Z}G$?

If G is abelian, then the set of torsion units is $\pm G$.

Problem

Describe torsion units of $U(\mathbb{Z}G)$ when G is not-abelian

Conjectures by Zassenhaus

In 1974 Hans Zassenhaus formulated the following conjectures:

ZC-1

Every torsion unit $u \in V(\mathbb{Z}G)$ is conjugate within the rational group algebra $\mathbb{Q}G$ to an element of G

ZC-2

Every subgroup $H \subseteq V(\mathbb{Z}G)$ such that $|H| = |G|$ is conjugate to G within the rational group algebra $\mathbb{Q}G$

ZC-3

Every finite subgroup $H \subseteq V(\mathbb{Z}G)$ is conjugate to a subgroup of G within the rational group algebra $\mathbb{Q}G$

Conjectures by Zassenhaus

Current state

- Obviously, ZC-3 implies ZC-2 and ZC-1
- Variety of counterexamples to ZC-2:
  - of order 2880 – Roggenkamp & Scott, 1988
  - of orders 2880 and 6720 – Klingler, 1991
  - of order 1140 (metabelian) – Hertweck, 2002
  - Hertweck, 2003 – of orders:
    - 180 (metabelian)
    - 360 (supersolvable)
    - 72600 (Frobenius)
  - of order 96 (three groups) – Blanchard, 2001 (also verified using GAP 3.4.4 that these are counterexamples of minimal possible order)
- ZC-1 is still open!!!

The 1st Zassenhaus conjecture

ZC-1 holds for:

- nilpotent groups (ZC-3)
- a number of semidirect products under various conditions
- Frobenius groups of order $p^m q^n$
- groups of order $p^2 q$

The ZC-1 conjecture appeared to be very hard, and raised several weakened variations.

IP-C conjecture

One of the variations states that that if $V(\mathbb{Z}G)$ contains a torsion unit u of order k, then the group G contains an element of order k:

Conjecture (Isomorphism of cyclic subgroups)

(IP-C) *Every finite cyclic subgroup $H \subseteq V(\mathbb{Z}G)$ is isomorphic to a subgroup of the group G.*

Another variation is related with the notion of the *prime graph* of the group.

Prime graph of a group

Definition

$\pi(G)$ – *prime graph* of a finite group G:

- vertices labelled by primes dividing $|G|$
- edge $pq \Leftrightarrow G$ has an element of order pq

Example

Mathieu group M_{11} has elements of orders 2, 3, 4, 5, 6, 8 and 11.
Its prime graph has the following form: 

Conjecture by Kimmerle

Conjecture (Kimmerle, 2005)

(KC) *If G is a finite group, then*

$$\pi(G) = \pi(V(\mathbb{Z}G))$$

It is easy to see that ZC-1 $\Rightarrow$ IP-C $\Rightarrow$ KC

In the section 4 of the same paper W. Kimmerle jontly with C. Höfert proved that KC holds for finite Frobenius and solvable groups and indicated that for non-solvable groups the known methods admit so far only results for few cases.

Research program

Verifying KC for sporadic simple groups

- Jointly with Victor Bovdi, we started the program of verifying KC for sporadic simple groups.
- We consider this problem in IP-C and ZC-1 context, so we do not restrict ourselves in orders of elements, since we are interested in any new information about possible torsion units.
- We are limited by the fact that we can not use that known techniques which are based on the normal structure of the group.
- However, there is a method developed by I. S. Luthar and I. B. S. Passi (1989), and later extended by M. Hertweck (2006), and it works in our situation.

Technique

The Luthar-Passi method

- Produces constraints imposed on coefficients of torsion units in $V(\mathbb{Z}G)$ and (in the ideal situation) eliminates all unwanted cases.
- First was used to prove that ZC-1 holds for A_5 (Luthar & Passi, 1989) and S_5 (Luthar & Trama, 1991).
- Suits computational purposes well, because:
  - it uses the character table of the group without constructing the group itself, and without explicit computations in integral group rings.
  - it can use the character table library (both ordinary and Brauer character tables) of the computational algebra system GAP.
  - it can be parallelized to speed up computation.

Partial augmentations

Notations

$C_1, \ldots, C_n$ – conjugacy classes of G

$u = \sum \alpha_g g$ – torsion unit of $\mathbb{Z}G$

$\nu_i = \nu_i(u) = \varepsilon_{C_i}(u)$ – partial augmentation of u, corresponding to the conjugacy class C_i :

$$\nu_i(u) = \sum_{g \in C_i} \alpha_g$$

Main goal

Let u be a torsion unit of $V(\mathbb{Z}G)$ of order k. We will prove that **(ZC-1)** holds for u, if u satisfies the following theorem:

Theorem (Marciniak–Ritter–Sehgal–Weiss, 1987; Luthar–Passi, 1989)

Let u be a torsion unit of $V(\mathbb{Z}G)$ of order k. Then u is conjugate in $\mathbb{Q}G$ to an element $g \in G$ $\Leftrightarrow$ for each d dividing k there is precisely one conjugacy class C with partial augmentation $\varepsilon_C(u^d) \neq 0$.

Order limit

The upper bound for orders of torsion units is given by the following theorem:

Theorem (Cohn–Livingstone, 1965)

Let u be a torsion unit in $V(\mathbb{Z}G)$.
Then the order of u divides the exponent of G.

How shall we begin?

Example:

- Let M_{11} be the 1^{st} simple Mathieu group.
- Then $exp(M_{11}) = 1320 = 2^3 \cdot 3 \cdot 5 \cdot 11$.
- M_{11} has elements of orders 2, 3, 4, 5, 6, 8 and 11.
- Above the group, it is enough to start with considering elements of $V(\mathbb{Z}G)$ of orders 10, 12, 15, 22, 33 and 55, because if u will be a unit of another possible order, then there is $t \in \mathbb{N}$ such that u^t has an order from this list.
- Later this list can be extended: for example, if we can not prove that there are no elements of order 12 in $V(\mathbb{Z}G)$, then we need to consider elements of order 24, etc.

First restrictions

From the Berman–Higman Theorem (1955) we obtain that:

- $\nu_1 = 0$
- $\nu_2 + \nu_3 + \cdots + \nu_m = 1$
- for non-simple groups it helps that $\nu_i = 0$, if $|C_i| = 1$

Example

If $G = M_{11}$, for an arbitrary unit of $V(\mathbb{Z}G)$ we have

$$\nu_{2a} + \nu_{3a} + \nu_{4a} + \nu_{5a} + \nu_{6a} + \nu_{8a} + \nu_{8b} + \nu_{11a} + \nu_{11b} = 1$$

Further eliminations

One of the earlier results in this direction was the following theorem:

Theorem (Marciniak-Ritter-Sehgal-Weiss, 1987; Luthar-Passi, 1989)

Let u be a torsion unit of $V(\mathbb{Z}G)$. Let C be a conjugacy class of G. If p is a prime dividing the order of a representative of C but not the order of u then the partial augmentation $\varepsilon_C(u) = 0$.

Example

If $G = M_{11}$, for units of order 2 we have:

$$\nu_{3a} = \nu_{5a} = \nu_{6a} = \nu_{11a} = \nu_{11b} = 0$$

$$\nu_{2a} + \nu_{4a} + \nu_{8a} + \nu_{8b} = 1$$

Improved restrictions

Recently M. Hertweck obtained stronger result:

Theorem (Hertweck, 2005–2006)

Let G be a finite group and let u be a torsion unit in $V(\mathbb{Z}G)$. If x is an element of G whose p-part, for some prime p, has order strictly greater than the order of the p-part of u, then $\varepsilon_x(u) = 0$.

Example

If $G = M_{11}$, we have:

- for a unit of order 2 $\quad \nu_{4a} = \nu_{8a} = \nu_{8b} = 0$, so $\nu_{2a} = 1$ is the only one non-zero partial augmentation, and ZC-1 holds for order 2.
- for a unit of order 10 $\quad \nu_{4a} = \nu_{8a} = \nu_{8b} = 0, \quad$ so $\quad \nu_{2a} + \nu_{5a} = 1.$ This is not enough for ZC-1 yet.

The main component of the method

Theorem (Luthar-Passi, 1989; modular case - Hertweck, 2005)

Let either $p = 0$ or p is a prime divisor of $|G|$. Suppose that $u \in V(\mathbb{Z}G)$ has finite order k and assume k and p are coprime in case $p \neq 0$.

If z is a complex primitive k-th root of unity and χ is either a classical character or a p-Brauer character of G, then for every integer l the number

$$\mu_l(u, \chi, p) = \frac{1}{k} \sum_{d|k} Tr_{\mathbb{Q}(z^d)/\mathbb{Q}}\{\chi(u^d) z^{-dl}\}$$

is a non-negative integer.

How to compute $\mu_l(u,\chi)$

Let u be a unit of order k, and $\nu_1, \dots \nu_n$ be its partial augmentations not known to be zero. We need to express

$$\mu_l(u,\chi) = \frac{1}{k}\sum_{d|k} Tr_{\mathbb{Q}(z^d)/\mathbb{Q}}\{\chi(u^d)z^{-dl}\} \geq 0$$

in the form

$$\mu_l(u,\chi) = x_1\nu_1 + \dots + x_n\nu_n + b \geq 0$$

First we will separate cases of $d = 1$ and $d > 1$:

$$\mu_l(u,\chi) = \frac{1}{k}\Big(Tr_{\mathbb{Q}(z)/\mathbb{Q}}\{\chi(u)z^{-l}\} + \sum_{d|k, d\neq 1} Tr_{\mathbb{Q}(z^d)/\mathbb{Q}}\{\chi(u^d)z^{-dl}\}\Big)$$

How to compute $\mu_l(u, \chi)$

To compute the first summand

$$Tr_{\mathbb{Q}(z)/\mathbb{Q}}\{\chi(u)z^{-l}\}$$

note that for any character χ of G of degree n, we have that

$$\chi(u) = \sum_{i=2}^{m} \nu_i \, \chi(h_i),$$

where h_i is a representative of the conjugacy class C_i. This gives us the linear combination $x_1\nu_1 + \cdots + x_n\nu_n$, and since all trace values must exists, we might obtain that some more $\nu_i = 0$, if the character values will not belong to $\mathbb{Q}(z)$

How to compute $\mu_l(u, \chi)$

To get the coefficient b of the inequality, we compute the 2^{nd} summand

$$\sum_{d|k, d\neq 1} Tr_{\mathbb{Q}(z^d)/\mathbb{Q}}\{\chi(u^d)z^{-dl}\}, \quad \text{using that} \quad \chi(u^d) = \sum_{i=2}^{\widetilde{m}} \widetilde{\nu}_i \, \chi(h_i),$$

and substitute various cases corresponding to (already known) admissible partial augmentations for elements of order k/d.

If ZC already holds for elements of order k/d, we need to consider for such substitution only various cases determined by conjugacy classes of elements or order k/d.

Such substitution of solutions coming from previous steps is one of the novelties of our approach.

M_{11}: Order 10 revisited

Example

Let $G = M_{11}$, and let u be a unit of order 10 in $V(\mathbb{Z}G)$. Then

$$\nu_{2a} + \nu_{5a} = 1.$$

Using the Brauer character table modulo 3, we obtain the system of inequalities

$$\mu_5(u, \chi_4) = \tfrac{1}{10}(-8\nu_{2a} + 8) \geq 0$$

$$\mu_0(u, \chi_4) = \tfrac{1}{10}(8\nu_{2a} + 12) \geq 0$$

$$\mu_2(u, \chi_2) = \tfrac{1}{10}(-\nu_{2a} + 6) \geq 0$$

which has no integral solutions such that all $\mu_i(u, \chi_j) \in \mathbb{Z}$.

Additional filter

If the order of the torsion unit is a power of prime, we may use additional condition:

Theorem (Cohn–Livingstone, 1965)

Let p be a prime, and let u be a torsion unit of $V(\mathbb{Z}G)$ of order p^n. Then for $m \neq n$ the sum of all partial augmentations of u with respect to conjugacy classes of elements of order p^m is divisible by p.

For M_{11}, this helps to eliminate some cases for units of order 4.

Results for the Mathieu group M_{11}

Theorem (Victor Bovdi, A.K., 2006)

$G = M_{11}$, u – torsion unit of $V(\mathbb{Z}G)$ of order $|u|$

- $|u| \neq 12 \Rightarrow$ *G has an element of order $|u|$*
- $|u| \in \{2, 3, 5, 11\} \Rightarrow$ *u is rationally conjugate to some $g \in G$*
- $|u| = 4 \Rightarrow (\nu_{2a}, \nu_{4a}) \in \{(0, 1), (2, -1)\}$
- $|u| = 6 \Rightarrow (\nu_{2a}, \nu_{3a}, \nu_{6a}) \in$
  $\{(-2, 3, 0), (0, 0, 1), (0, 3, -2), (2, -3, 2), (2, 0, -1)\}$
- $|u| = 8 \Rightarrow (\nu_{4a}, \nu_{8a}, \nu_{8b}) \in \{(0, 0, 1), (0, 1, 0), (2, -1, 0), (2, 0, -1)\}$
- $|u| = 12 \Rightarrow$ *no units such that their partial augmentations are not in the set* $(\nu_{2a}, \nu_{4a}, \nu_{6a}) \in \{(-1, 1, 1), (1, 1, -1)\}$

Results for the Janko group J_1

Theorem (Victor Bovdi, Eric Jespers, A.K., 2006)

$G = J_1$, u – torsion unit of $V(\mathbb{Z}G)$ of order $|u|$

- *No elements of order 14, 21, 22, 33, 35, 38, 55, 57, 77, 95, 133 and 209 in $V(\mathbb{Z}G)$. Equivalently, $|u| \neq 30 \Rightarrow$ G has an element of order $|u|$*
- $|u| \in \{2, 3, 7, 11, 19\} \Rightarrow$ *u is rationally conjugate to some $g \in G$*
- $|u| = 5 \Rightarrow (\nu_{5a}, \nu_{5b}) \in \{(-1, 2), (0, 1), (1, 0), (2, -1)\}$
- $|u| = 6$ *: six cases for* $(\nu_{2a}, \nu_{3a}, \nu_{6a})$
- $|u| = 10$ *: 12 cases for* $(\nu_{5a}, \nu_{5b}, \nu_{10a}, \nu_{10b})$
- $|u| = 15 \Rightarrow (\nu_{5a}, \nu_{5b}, \nu_{15a}, \nu_{15b}) \in$
  $\{(-1, 1, 0, 1), (0, 0, 0, 1), (0, 0, 1, 0), (1, -1, 1, 0)\}$
- $|u| = 30 \Rightarrow$ *no units such that their partial augmentations are not from one of the six cases for* $(\nu_{2a}, \nu_{4a}, \nu_{6a})$

Results for the Mathieu group M_{22}

Theorem (Victor Bovdi, Steve Linton, A.K., 2007)

$G = M_{22}$, u – torsion unit of $V(\mathbb{Z}G)$ of order $|u|$

- *No elements of order 10, 14, 15, 21, 22, 33, 35, 55, 77 in $V(\mathbb{Z}G)$. Equivalently, $|u| \notin \{12, 24\} \Rightarrow$ G has an element of order $|u|$*
- $|u| \in \{2, 3, 5\} \Rightarrow$ *u is rationally conjugate to some $g \in G$*
- $|u| = 4$ *: 34 cases for* $(\nu_{2a}, \nu_{4a}, \nu_{4b})$
- $|u| = 6$ *: 15 cases for* $(\nu_{2a}, \nu_{3a}, \nu_{6a})$
- $|u| = 7$ *: 4 cases for* (ν_{7a}, ν_{7b})
- $|u| = 11$ *: 10 cases for* (ν_{11a}, ν_{11b})
- $|u| = 8$ *: 76 cases for* $(\nu_{2a}, \nu_{4a}, \nu_{4b}, \nu_{8a})$
- $|u| = 12$ *: 1166 cases for* $(\nu_{2a}, \nu_{3a}, \nu_{4a}, \nu_{4b}, \nu_{6a})$

Kimmerle's conjecture

We (VB & AK) proved that KC holds for:

- Mathieu simple groups:
  - M_{11}
  - M_{12} (jointly with S. Siciliano)
  - M_{22} (jointly with S. Linton)
  - M_{23}
  - M_{24}
- Janko simple groups (jointly with E. Jespers):
  - J_1
  - J_2
  - J_3
- Higman-Sims simple group *HS*
- McLaughlin simple group *McL*
- Rudvalis simple group *Ru*
- Suzuki simple group *Suz* (jointly with E.N. Marcos)

Overview of results

Information about possible orders of torsion units and their partial augmentations (italic denotes data obtained using computer)

G	ZC-1 (fast)	ZC-1 (L–P)	order(#) in G	Omitted orders in G	No orders over $G \Rightarrow$ IP-C $\Rightarrow$ KC	order(#) over G	Omitted orders over G
M_{11}	2, 3, 5	11	4(2), 6(5), 8(4)	—	10, 15, 22, 24, 33, 55	12(2)	—
M_{12}	5	—	2(6), 3(5), 10(2), 11(4)	4, 6, 8	15, 22, 33, 55	—	12, 20, 24, 40
M_{22}	2, 3, 5	—	4(34), 6(15), 7(4), *8(76)*, 11(10)	—	10, 14, 15, 21, 22, 33, 35, 55, 77	*12 (1166)*	24
M_{23}	2, 3, 5	23	4(3), 6(21), 7(4), 8(10), 11(20), 15(6)	14	10, 21, 22, *28*, 33, 35, 46, 55, *56*, 69, 77, 115, 161, 253	—	12, 24
M_{24}	5, 11	23	2(6), 3(6), 7(4), 10(11), *15(34)*, *21(21)*	4, 6, 8, 12, 14	22, 33, 35, 46, 55, 69, 77, 115, 161, 253	—	20, 24, 28, 30, 40, 42, 56, 60, 84, 120, 168
J_1	2, 3, 7, 11	19	5(4), 6(6), 10(12), 15(4)	—	14, 21, 22, 33, 35, 38, 55, 57, 77, 95, 133, 209	*30(6)*	—
J_2	7	15	2(6), 3(3), 4(15), 5(10), 8(18)	6, 10, 12	14, 21, 35	—	20, 24, 30, 40, 60, 120
J_3	2	—	3(10), 4(3), 5(8), 8(15), 17(10), 19(10)	6, 9, 10, 12, 15	34, 38, 51, 57, 85, 95, 323	—	18, 20, 24, 30, 36, 40, 45, 60, 72, 90, 120, 180, 360
HS	3, 7	—	2(6), 5(23), 11(10)	4, 6, 8, 12, 15, 20	14, 21, 22, 33, 35, *55*, 77	—	24, 30, 40, 60, 120
McL	2	—	3(4), 5(6), 7(174), 11(20)	4, 6, 8, 9, 10, 12, 14, 15, 30	21, 22, 33, 35, 55, 77	—	18, 20, 24, 28, 36, 40, 45, 56, 60, 72, 90, 120, 180, 360
Ru	3, 7, 13	—	2(22), 5(8), 29(10)	4, 6, 8, 10, 12, 14, 15, 16, 20, 24, 26	21, 35, 39, 58, 65, 87, 91, 145, 203, 377	—	28, 30, 40, 48, 52, 56, 60, 80, 104, 112, 120, 208, 240
Suz	7, 11	—	2(8), 5(10), 13(18)	4, 6, 8, 9, 10, 12, 14, 15, 18, 20, 21, 24	22, 26, 33, 35, 39, 55, 65, 77, 91, 143	—	28, 30, 36, 40, 42, 45, 56, 60, 63, 72, 84, 90, 120, 126, 168, 180, 252, 360, 504

Technical details

- The program that we are developing is able to compute and analyse constraints imposed on partial augmentations
- It can be used when the number of cases to enumerate is large
- It is implemented in the GAP system
- We intend to make in available in the LAGUNA package
- For cross-checking, it uses two constraint programming solvers:
  - ECLiPSe (http://eclipse.crosscoreop.com, using development version of the GAP package IO)
  - MINION (http://minion.sourceforge.net, using GAP interface by Steve Linton)

  and also our own solver written in GAP.

Further plans

- **To do:** investigate the remaining sporadic simple groups.
- **Parallelizing**: some groups require checking thousands of possible cases, for which we will use software tools developed in the SCIEnce project (http://www.symbolic-computation.org).
- **Wishlist**: to have more Brauer character tables available in the GAP system.
- **Related problems**: Any new constraint on partial augmentations. that will appear in the future, may be tried on our results and hopefully eliminate the remaining unwanted cases to reach ZC-1 or at least IP-C.

References


V. Bovdi and A. Konovalov.
Integral group ring of the first Mathieu simple group.
In *Groups St. Andrews 2005. Vol. I*, volume 339 of *London Math. Soc. Lecture Note Ser.*, pages 237–245. Cambridge Univ. Press, Cambridge, 2007.


V. Bovdi, A. Konovalov, and S. Siciliano.
Integral group ring of the Mathieu simple group M_{12}.
Rend. Circ. Mat. Palermo (2), 56:125–136, 2007.


V. Bovdi, A. Konovalov, and S. Linton.
Torsion units in integral group ring of the Mathieu simple group M_{22}.
LMS J. Comput. Math., 12 pages, to appear, 2007.


V. Bovdi and A. Konovalov.
Integral group ring of the Mathieu simple group M_{23}.
Comm. Algebra, 9 pages, to appear, 2008.


V. Bovdi, E. Jespers, and A. Konovalov.
Torsion units in integral group rings of Janko simple groups.
30 pages, submitted, 2007.