Journal of Software for Algebra and Geometry

HeLP: a GAP package for torsion units in integral group rings

ANDREAS BÄCHLE AND LEO MARGOLIS

HeLP: a GAP package for torsion units in integral group rings

ANDREAS BÄCHLE AND LEO MARGOLIS

ABSTRACT: We briefly summarize the background of the HeLP method for
torsion units in group rings and present some functionality of a GAP package
implementing it.

1. THE ZASSENHAUS CONJECTURE AND THE PRIME GRAPH QUESTION. As we consider the integral group ring $\mathbb{Z}G$ of a finite group G, one question that arises naturally is: "What does the unit group $\mathrm{U}(\mathbb{Z}G)$ look like?" For example, what are the *torsion units*, i.e., the units of finite order? Clearly, there are the so-called *trivial units* $\pm g$ for $g \in G$. Already in G. Higman's PhD thesis [1940], it was proved that all the torsion units are of this form, provided G is abelian. As we are not interested in the torsion coming solely from the ring, but rather in the torsion coming from the group-ring interplay, we consider the group of *normalized units* $\mathrm{V}(\mathbb{Z}G)$, i.e., the units mapping to 1 under the augmentation homomorphism

$$\varepsilon : \mathbb{Z}G \to \mathbb{Z} : \sum_{g \in G} u_g g \mapsto \sum_{g \in G} u_g.$$

Then $\mathrm{U}(\mathbb{Z}G) = \pm \mathrm{V}(\mathbb{Z}G)$.

In the noncommutative case, there are in general, of course, more torsion units than the trivial ones, e.g., conjugates of group elements by units of $\mathbb{Q}G$ which end up in $\mathbb{Z}G$ again. H. J. Zassenhaus conjectured more than 40 years ago that these are all the torsion units.

Zassenhaus conjecture (ZC) [1974]. *Let G be a finite group and u a torsion unit in $\mathrm{V}(\mathbb{Z}G)$. Then there exists a unit x in $\mathbb{Q}G$ such that $x^{-1}ux = g$ for some $g \in G$.*

Elements $u, v \in \mathbb{Z}G$ which are conjugate by a unit $x \in \mathbb{Q}G$ are called *rationally conjugate*, denoted by $u \sim_{\mathbb{Q}G} v$. The Zassenhaus conjecture is nowadays one of the

main open questions in the area of integral group rings. A highlight was certainly Weiss' proof of this conjecture for nilpotent groups [Weiss 1991].

As a first step towards the Zassenhaus conjecture, W. Kimmerle formulated a weaker version which has attracted attention.

Prime graph question (PQ) [Kimmerle 2006]. Let G be a finite group and p and q different primes such that $V(\mathbb{Z}G)$ contains an element of order pq. Does G then possess an element of order pq?

Given a group G the prime graph of G is defined to be the graph whose vertices are labeled by primes appearing as orders of elements in G, and two vertices p and q are connected by an edge if and only if G contains an element of order pq. Thus (PQ) asks whether G and $V(\mathbb{Z}G)$ have the same prime graph.

A method to attack these questions, known as the HeLP method, was introduced by Luthar and Passi [1989] and later extended by Hertweck [2007]. The name *HeLP* (*He*rtweck *L*uthar *P*assi) is due to A. Konovalov. The method can be applied algorithmically to a concrete group or, if one has generic characters at hand, a series of groups.

The present note presents a GAP package implementing this method [HeLP package]. The main motivation for this program is to make the algorithm available to researchers working in the field, and to enable readers of papers using the method to check results obtained by the method. We describe the method in Section 2 and discuss several aspects of our implementation in Sections 3 and 4.

2. THE HELP CONSTRAINTS. Let G always be a finite group.

The possible orders of torsion units in $\mathbb{Z}G$ are restricted:

Proposition 2.1. *Let $u \in V(\mathbb{Z}G)$ be a torsion unit.*

(a) *The order of u divides the exponent of G* [Cohn and Livingstone 1965, Corollary 4.1].

(b) *If G is solvable, then the order of u coincides with the order of an element of G* [Hertweck 2008, Theorem].

Definition 2.2. Let $u = \sum_{g \in G} u_g g \in \mathbb{Z}G$, $x \in G$ and denote by x^G its conjugacy class. Then

$$\varepsilon_x(u) = \sum_{g \in x^G} u_g$$

is called the *partial augmentation of u with respect to x* (or, rather, the conjugacy class of x).

The following proposition by Marciniak, Ritter, Sehgal and Weiss connects (ZC) to partial augmentations.

Proposition 2.3 [Marciniak et al. 1987, Theorem 2.5]. *Let $u \in V(\mathbb{Z}G)$ be a torsion unit of order k. Then u is rationally conjugate to a group element if and only if $\varepsilon_x(u^d) \geq 0$ for all divisors d of k and all $x \in G$.*

Certain partial augmentations vanish a priori:

Proposition 2.4. *Let $u \in V(\mathbb{Z}G)$ be a torsion unit and $x \in G$.*

(a) *If $o(u) \neq 1$, then $\varepsilon_1(u) = 0$ (Berman and Higman; see [Sehgal 1993, Proposition 1.4]).*

(b) *If $o(x) \nmid o(u)$, then $\varepsilon_x(u) = 0$ [Hertweck 2007, Theorem 2.3].*

Let ψ be a character of the group G. A representation afforded by ψ can be extended linearly to a representation of $\mathbb{Q}G$ and then restricted to a representation D of the group of units $U(\mathbb{Q}G)$. We will denote its character also by ψ. Now consider for a torsion unit $u \in V(\mathbb{Z}G)$ of order k, a linear character $\chi : C_k \simeq \langle u \rangle \to \mathbb{C}$ given by $\chi(u) = \zeta^\ell$, with $\zeta \in \mathbb{C}^\times$ a primitive k-th root of unity, $\ell \in \mathbb{Z}$. Then we have that the multiplicity of ζ^ℓ as an eigenvalue of $D(u)$ is given by

$$\langle \chi, \psi \rangle_{\langle u \rangle} \in \mathbb{Z}_{\geq 0},$$

where $\langle -, - \rangle_{\langle u \rangle}$ denotes the inner product on the class functions of $C_k \simeq \langle u \rangle$. Working out an explicit formula for this, one obtains part (a) of the following proposition.

Proposition 2.5. *Let G be a finite group and $u \in V(\mathbb{Z}G)$ a torsion unit of order k. Let $\zeta \in \mathbb{C}^\times$ be a primitive k-th root of unity, $\ell \in \mathbb{Z}$.*

(a) *[Luthar and Passi 1989, Theorem 1] Let χ be an ordinary character of G and let D be a representation afforded by χ. Then the multiplicity of ζ^ℓ as an eigenvalue of $D(u)$ is given by*

$$\mu_\ell(u, \chi) = \frac{1}{k} \sum_{d \mid k} \mathrm{Tr}_{\mathbb{Q}(\zeta^d)/\mathbb{Q}}(\chi(u^d)\zeta^{-d\ell}). \tag{1}$$

(b) *[Hertweck 2007, Section 4] Let p be a prime not dividing k, and $\zeta \mapsto \bar{\zeta}$ be a fixed isomorphism between the group of k-th roots of unity in characteristic 0 and those in characteristic p. Let φ be a p-Brauer character of G and P be a representation afforded by φ. Then the multiplicity of $\bar{\zeta}^\ell$ as an eigenvalue of $P(u)$ is given by*

$$\mu_\ell(u, \varphi) = \frac{1}{k} \sum_{d \mid k} \mathrm{Tr}_{\mathbb{Q}(\zeta^d)/\mathbb{Q}}(\varphi(u^d)\zeta^{-d\ell}). \tag{2}$$

This proposition is the linchpin of the HeLP method. Let $u \in V(\mathbb{Z}G)$ be again a torsion unit of order k. For an ordinary character χ we have $\chi(u) = \sum_{x^G} \varepsilon_x(u)\chi(x)$. By [Hertweck 2007, Theorem 3.2], an analogous statement holds for p-Brauer

characters and p-regular units u, where the sum is taken only over the conjugacy classes of p-regular elements in G (an element is called *p-regular* if its order is not divisible by p). Assume for an ordinary or a Brauer character ψ in characteristic $p \nmid k$ one knows inductively the character values of $\psi(u^d)$. Then the following condition on the $\varepsilon_x(u)$ holds for every ℓ:

$$\sum_{x^G} \frac{\mathrm{Tr}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\psi(x)\zeta^{-\ell})}{k} \varepsilon_x(u) + a_\ell(u, \psi) \in \mathbb{Z}_{\geq 0}, \tag{3}$$

where the $a_\ell(u, \psi) = \frac{1}{k} \sum_{1 \neq d \mid k} \mathrm{Tr}_{\mathbb{Q}(\zeta^d)/\mathbb{Q}}(\psi(u^d)\zeta^{-d\ell})$ are assumed to be "known". By Proposition 2.4 it is enough to take the sum (3) over classes of elements having an order dividing k.

Remarks 2.6.

- By [Hales et al. 1990, Corollary 2.3], the partial augmentations are bounded and thus solving the inequalities is a finite problem. These bounds are, however, encoded in the ordinary character table, so they will not add new information to the algorithm.

- It is intrinsic in the formula that the μ_ℓ's sum up to the degree of the character.

3. THE EXTENDED WAGNER TEST. The program uses also a criterion proved in a special form by Roland Wagner in his Diplomarbeit [1995]. Proposition 3.1, the more general case, is recorded in [Bovdi and Hertweck 2008, Remark 6] and follows from [Sehgal 1993, Lemma 7.1], which is well known. For the sake of completeness, we include a proof since no short complete proof seems to be available in the literature. We write $g \sim h$ if g and h are conjugate in a group G.

Proposition 3.1. *Let G be a finite group, $s \in G$ and $u \in \mathrm{V}(\mathbb{Z}G)$. Let p be a prime and j a nonnegative integer. Then*

$$\sum_{x^G, \ x^{p^j} \sim s} \varepsilon_x(u) \equiv \varepsilon_s(u^{p^j}) \mod p.$$

Proof. Let $u = \sum_{g \in G} u_g g \in \mathrm{V}(\mathbb{Z}G)$, set $q = p^j$ and $v = u^q$. By definition,

$$\varepsilon_s(v) = \sum_{\substack{(g_1, \ldots, g_q) \in G^q \\ g_1 \cdots g_q \sim s}} \prod_{j=1}^{q} u_{g_j}. \tag{4}$$

The set over which the sum is taken can be decomposed into $\mathcal{M} = \{(g, \ldots, g) \in G^q : g^q \sim s\}$ and $\mathcal{N} = \{(g_1, \ldots, g_q) \in G^q : g_1 \cdots g_q \sim s \text{ and there exists } r, r' : g_r \neq g_{r'}\}$.

The cyclic group $C_q = \langle t \rangle$ of order q acts on the set $\mathcal{N}$ by letting the generator t shift the entries of a tuple to the left, i.e.,

$$(g_1, g_2, g_3, \ldots, g_q) \cdot t = (g_2, g_3, \ldots, g_q, g_1).$$

Note that all orbits have length p^i with $i \geq 1$. For elements in the same orbit, the same integer is summed up in (4). Hence using Fermat's little theorem we have

$$\varepsilon_s(v) = \sum_{(g,\ldots,g)\in\mathcal{M}} u_g^q + \sum_{(g_1,\ldots,g_q)\in\mathcal{N}} \prod_{j=1}^{q} u_{g_j}$$

$$\equiv \sum_{(g,\ldots,g)\in\mathcal{M}} u_g^q \equiv \sum_{(g,\ldots,g)\in\mathcal{M}} u_g \equiv \sum_{x^G,\; x^{p^j}\sim s} \varepsilon_x(u) \mod p. \qquad \square$$

By induction and the Berman–Higman result (Proposition 2.4 (a)), Wagner obtained the following. For units of prime power order the result also follows from [Cohn and Livingstone 1965, Theorem 4.1].

Corollary 3.2 (Wagner). *Let G be a finite group, $u \in \mathrm{V}(\mathbb{Z}G)$, $o(u) = p^j m$ with p a prime and $m \neq 1$. Then*

$$\sum_{x^G,\; o(x)=p^j} \varepsilon_x(u) \equiv 0 \mod p.$$

Example 3.3. Let G be the Mathieu group of degree 11. There exists only one conjugacy class of involutions in G, call it 2a. After applying HeLP (i.e., Proposition 2.5) for a unit u of order 12 in $\mathrm{V}(\mathbb{Z}G)$, one obtains two possible partial augmentations for u. One of these possibilities satisfies $\varepsilon_{2a}(u) = 1$ while the other satisfies $\varepsilon_{2a}(u) = -1$ [Bovdi and Konovalov 2007]. Neither possibility satisfies the constraints of Wagner's result and thus there are no torsion units of order 12 in $\mathrm{V}(\mathbb{Z}G)$ and the order of any torsion unit in $\mathrm{V}(\mathbb{Z}G)$ coincides with the order of an element in G.

4. Implementation.

4A. *Further results.* We used several results in our implementation, which are not consequences of the HeLP method and which we list here. The first one is a direct consequence of the Fong–Swan–Rukolaine theorem [Curtis and Reiner 1981, Theorem 22.1].

Proposition 4.1. *Let G be a p-solvable group and $u \in \mathrm{V}(\mathbb{Z}G)$ a torsion unit of order prime to p. Then the restrictions on the possible partial augmentations of u one can obtain using the p-Brauer table of G are the same as when using the ordinary character table of G.*

To avoid redundant calculations, our implementation also uses the following results instead of solving any inequalities in these situations.

Proposition 4.2. (a) (*ZC*) *holds for nilpotent groups* [Weiss 1991].

(b) (*PQ*) *has an affirmative answer for solvable groups* [Kimmerle 2006].

Remark 4.3. There are other results about (ZC) and (PQ). For example, (ZC) is known for cyclic-by-abelian groups [Caicedo et al. 2013], while (PQ) is known for PSL(2, p) where p denotes a prime [Hertweck 2007]. However, we decided for simplicity only to use the results in Proposition 4.2 in the package.

4B. *Main functions of the HeLP package.* The function HeLP_ZC checks whether (ZC) can be verified using the character tables and Brauer tables available in GAP. For a potential element u of order k whose partial augmentations we want to compute, and p and q different prime divisors of k, we call partial augmentations of u^p and u^q *compatible* if $(u^p)^q$ and $(u^q)^p$ have the same partial augmentations.

Algorithm 1: HeLP_ZC

Input: group or ordinary character table of a group
Output: true or false
if *G nilpotent* **then**
| **return** true (see Proposition 4.2)
end
if *G solvable* **then**
| OrdersToCheck := orders of elements in G (see Proposition 2.1)
else
| OrdersToCheck := divisors of exp G
end
for $k = o(u)$ *in* OrdersToCheck **do**
| **for** *all prime divisors p of $o(u)$ and all possible partial augmentations*
| *of u^p* **do**
| **if** *partial augmentations are compatible* **then**
| Construct and solve the HeLP systems for all relevant
| character tables
| **end**
| **end**
| Apply the Wagner test for order k
| Save the resulting possibilities for partial augmentations of units of
| order k in the global variable HeLP_sol
end
if *only "trivial" partial augmentations are admissible* **then return** true
else return false

The function HeLP_PQ checks whether (PQ) can be verified using the character tables and Brauer tables available in GAP. It works in a similar way to HeLP_ZC but only checks the orders relevant for the prime graph question.

The package contains other functions, such as one that allows the user to check whether units of a given order occur; for further details, see the reference manual.

4C. *Nonstandard characters.* Unfortunately, not all known character tables and Brauer tables are available in GAP, so the package cannot be applied in those cases. However, there are some workarounds.

Example 4.4. The Brauer table modulo 7 of PSL(2, 49) is known generically, but not yet included in the GAP Character Table Library [CTblLib]. However, our implementation allows the use of class functions of a group provided by the user. In this way, any class function may be used and it is, among other things, possible to prove (ZC) for PSL(2, 49).

Example 4.5. Let G be the projective unitary group PSU(3, 8) and A its automorphism group. Assume the goal is to check (PQ) for A. To obtain that one needs to exclude the existence of units of order $2 \cdot 19$ and $7 \cdot 19$ in $V(\mathbb{Z}A)$. The character table of G is available in GAP while that of A is not. However, inducing the second and third irreducible characters of G to characters of A, one obtains two characters of A. The HeLP constraints following from these two characters are strong enough to prove (PQ) for A.

4D. *Solving the inequalities.* Applying the HeLP method involves solving the integral linear inequalities described after Proposition 2.5. This is a hard task in general: although theoretically possible, it may take a lot of time when there are many inequalities and variables involved. A good solver of such systems is the main requirement here. Our implementation allows the use of two solvers; the software system [4ti2, version ≥1.6.5], and/or the system [Normaliz, version ≥3.1.0] for rational cones and affine models (see also [Bruns et al. 2016]). We chose those solvers because they are good solvers and there exist GAP interfaces for them [4ti2Interface; NormalizInterface]. To reduce the size of the system that must be solved, the package uses the algorithm "redund" from [lrslib, version ≥4.3] for reverse-search vertex enumeration. When using 4ti2, in many cases this leads to a remarkable speedup; however, it may slow down the calculations, so there is an option implemented to switch the use of "redund" on and off.

4E. *p-constant characters.* If one is interested especially in solving (PQ) there is often a way to reduce the system one has to solve, which was introduced by V. Bovdi and A. Konovalov [2010]. Assume one is studying the possible partial augmentations of units of order $p \cdot q$, where p and q are different primes. Let χ be a character which is constant on all conjugacy classes of elements of order p, a so called *p-constant character*. Then the coefficients appearing in the HeLP constraints provided by χ at partial augmentations of elements order p are always the same. Thus one can reduce the number of variables involved by replacing all the partial augmentations of elements of order p by their sum. This way one also does not need to know the partial augmentations of elements of order p — their sum

is 1 in any case. Often it suffices to study only p-constant characters to exclude the possibility of existence of units of order $p \cdot q$ and this functionality is also provided by the package.

The package is available as an online supplement.

REFERENCES.

[4ti2] 4ti2 team, "4ti2 — a software package for algebraic, geometric and combinatorial problems on linear spaces", available at www.4ti2.de.

[4ti2Interface] S. Gutsche, "4ti2 interface", GAP package, version 2015.11.06, available at https:// tinyurl.com/4ti2gapInterface.

[Bovdi and Hertweck 2008] V. Bovdi and M. Hertweck, "Zassenhaus conjecture for central extensions of S_5", *J. Group Theory* **11**:1 (2008), 63–74. MR Zbl

[Bovdi and Konovalov 2007] V. Bovdi and A. Konovalov, "Integral group ring of the first Mathieu simple group", pp. 237–245 in *Groups St. Andrews 2005*, vol. 1, edited by C. M. Campbell et al., London Math. Soc. Lecture Note Ser. **339**, Cambridge Univ. Press, 2007. MR Zbl

[Bovdi and Konovalov 2010] V. A. Bovdi and A. B. Konovalov, "Torsion units in integral group ring of Higman–Sims simple group", *Studia Sci. Math. Hungar.* **47**:1 (2010), 1–11. MR Zbl

[Bruns et al. 2016] W. Bruns, B. Ichim, and C. Söger, "The power of pyramid decomposition in Normaliz", *J. Symbolic Comput.* **74** (2016), 513–536. MR Zbl

[Caicedo et al. 2013] M. Caicedo, L. Margolis, and A. del Río, "Zassenhaus conjecture for cyclic-by-abelian groups", *J. Lond. Math. Soc.* (2) **88**:1 (2013), 65–78. MR Zbl

[Cohn and Livingstone 1965] J. A. Cohn and D. Livingstone, "On the structure of group algebras, I", *Canad. J. Math.* **17** (1965), 583–593. MR Zbl

[CTblLib] T. Breuer, "The GAP character table library", GAP package, version 1.2.1, available at http://www.math.rwth-aachen.de/~Thomas.Breuer/ctbllib.

[Curtis and Reiner 1981] C. W. Curtis and I. Reiner, *Methods of representation theory, I: With applications to finite groups and orders*, Wiley, New York, 1981. MR Zbl

[Hales et al. 1990] A. W. Hales, I. S. Luthar, and I. B. S. Passi, "Partial augmentations and Jordan decomposition in group rings", *Comm. Algebra* **18**:7 (1990), 2327–2341. MR Zbl

[HeLP package] A. Bächle and L. Margolis, "HeLP – Hertweck–Luthar–Passi method", GAP package, version 3.1, available at http://homepages.vub.ac.be/abachle/help/.

[Hertweck 2007] M. Hertweck, "Partial augmentations and Brauer character values of torsion units in group rings", 2007. arXiv

[Hertweck 2008] M. Hertweck, "The orders of torsion units in integral group rings of finite solvable groups", *Comm. Algebra* **36**:10 (2008), 3585–3588. MR Zbl

[Higman 1940] G. Higman, "The units of group-rings", *Proc. London Math. Soc.* (2) **46** (1940), 231–248. MR Zbl

[Kimmerle 2006] W. Kimmerle, "On the prime graph of the unit group of integral group rings of finite groups", pp. 215–228 in *Groups, rings and algebras*, edited by W. Chin et al., Contemp. Math. **420**, Amer. Math. Soc., Providence, RI, 2006. MR Zbl

[lrslib] D. Avis, "lrslib", software version 6.2, available at http://cgm.cs.mcgill.ca/~avis/C/lrs.html.

[Luthar and Passi 1989] I. S. Luthar and I. B. S. Passi, "Zassenhaus conjecture for A_5", *Proc. Indian Acad. Sci. Math. Sci.* **99**:1 (1989), 1–5. MR Zbl

[Marciniak et al. 1987] Z. Marciniak, J. Ritter, S. K. Sehgal, and A. Weiss, "Torsion units in integral group rings of some metabelian groups, II", *J. Number Theory* **25**:3 (1987), 340–352. MR Zbl

[Normaliz] W. Burns, B. Ichim, R. Sieg, and C. Söger, "Normaliz", software, version 3.2.0, available at http://normaliz.uos.de.

[NormalizInterface] S. Gutsche, M. Horn, and C. Söger, "NormalizInterface", GAP package, version 0.9.8, available at http://gap-packages.github.io/NormalizInterface/.

[Sehgal 1993] S. K. Sehgal, *Units in integral group rings*, Pitman Monographs and Surveys in Pure and Applied Mathematics **69**, Longman, Harlow, 1993. MR Zbl

[Wagner 1995] R. Wagner, *Zassenhausvermutung über die Gruppen* PSL(2, *p*), Diplomarbeit, Universität Stuttgart, 1995.

[Weiss 1991] A. Weiss, "Torsion units in integral group rings", *J. Reine Angew. Math.* **415** (1991), 175–187. MR Zbl

[Zassenhaus 1974] H. Zassenhaus, "On the torsion units of finite group rings", pp. 119–126 in *Studies in mathematics* (*in honor of A. Almeida Costa*), Instituto de Alta Cultura, Lisbon, 1974. MR Zbl

ANDREAS BÄCHLE:

abachle@vub.ac.be

Vakgroep Wiskunde, Vrije Universiteit Brussel, Pleinlaan 2, 1050 Brussels, Belgium

LEO MARGOLIS:

leo.margolis@um.es

Fachbereich Mathematik, Universität Stuttgart, Pfaffenwaldring 57, 70569 Stuttgart, Germany