

Central and medial quasigroups of small order

David Stanovský, Petr Vojtěchovský

Abstract. We enumerate central and medial quasigroups of order less than 128 up to isomorphism, with the exception of those quasigroups that are isotopic to $C_4 \times C_2^4$, C_2^6 , C_3^4 or C_5^3 . We give an explicit formula for the number of quasigroups that are affine over a finite cyclic group.

Mathematics subject classification: 20N05, 05A15.

Keywords and phrases: Medial quasigroup, entropic quasigroup, central quasigroup, T-quasigroup, abelian quasigroup, quasigroup affine over abelian group, abelian algebra, affine algebra, classification of quasigroups, enumeration of quasigroups.

This paper was written on the occasion of the 90th anniversary of Valentin Danilovich Belousov's birthday. Prof. Belousov pioneered enumerative results for quasigroups in his book "Fundamentals of the theory of quasigroups and loops" and his work has been a frequent source of inspiration for the Prague algebraic school.

1 Introduction

Given an abelian group $(G, +)$, automorphisms φ, ψ of $(G, +)$, and an element $c \in G$, define a new operation $*$ on G by

$$x * y = \varphi(x) + \psi(y) + c.$$

The resulting quasigroup $(G, *)$ is said to be *affine over* $(G, +)$, and it will be denoted by $\mathcal{Q}(G, +, \varphi, \psi, c)$. Quasigroups that are affine over an abelian group are called *central quasigroups* or *T-quasigroups*. We will use the terms “quasigroup affine over an abelian group” and “central quasigroup” interchangeably. Central quasigroups are precisely the abelian quasigroups in the sense of universal algebra [15].

A quasigroup (Q, \cdot) is called *medial* if it satisfies the medial law

$$(x \cdot y) \cdot (u \cdot v) = (x \cdot u) \cdot (y \cdot v).$$

Medial quasigroups are also known as *entropic* quasigroups. The fundamental Toyoda-Bruck theorem [13, Theorem 3.1] states that, up to isomorphism, medial quasigroups are precisely central quasigroups $\mathcal{Q}(G, +, \varphi, \psi, c)$ with commuting automorphisms φ, ψ .

© David Stanovský, Petr Vojtěchovský, 2016
Research partially supported by the GAČR grant 13-01832S (Stanovský), the Simons Foundation Collaboration Grant 210176 (Vojtěchovský) and the University of Denver PROF grant (Vojtěchovský).

The classification of central (or medial) quasigroups up to isotopy is trivial in the sense that it coincides with the classification of abelian groups up to isomorphism. Indeed:

- If $(G, *) = \mathcal{Q}(G, +, \varphi, \psi, c)$ is a central quasigroup then $(G, *)$ is isotopic to $(G, +)$ via the isotopism $(x \mapsto \varphi(x), x \mapsto \psi(x) + c, x \mapsto x)$.
- If two central quasigroups $Q_i = \mathcal{Q}(G_i, +_i, \varphi_i, \psi_i, c_i)$ are isotopic then the underlying groups $(G_i, +_i)$ are isotopic. But isotopic groups are necessarily isomorphic, cf. [10, Proposition 1.4].

Classifying and enumerating central and medial quasigroups up to isomorphism is nontrivial, however, and that is the topic of the present paper.

There are not many results in the literature concerning enumeration and classification of central and medial quasigroups.

Simple idempotent medial quasigroups were classified by Smith in [9, Theorem 6.1]. Sokhatsky and Syvakivskij [12] classified n -ary quasigroups affine over cyclic groups and obtained a formula for the number of those of prime order. Kirnasovsky [5] carried out a computer enumeration of central quasigroups up to order 15, and obtained more classification results in his PhD thesis [6]. Idempotent medial quasigroups of order p^k , $k \leq 4$, were classified by Hou [4, Table 1].

At the time of writing this paper, the On-line Encyclopedia of Integer Sequences [8] gives the number of medial quasigroups of order ≤ 8 up to isomorphism as the sequence A226193, and there appears to be no entry for the number of central quasigroups up to isomorphism.

Drápal [1] and Sokhatsky [11] obtained a general isomorphism theorem for quasigroups isotopic to groups, cf. [1, Theorem 2.10] and [11, Corollary 28], and for central quasigroups in particular, cf. [1, Theorem 3.2], or its restatement, Theorem 2.5. Drápal applied the machinery to calculate isomorphism classes of quasigroups of order 4 (by hand), and Kirnasovsky used Sokhatsky's theory for the calculations mentioned above. In the present paper, we use a similar approach to obtain stronger enumeration results, taking advantages of the computer system GAP [2].

We refer the reader to [10] for general theory of quasigroups, to [1] for a more extensive list of references on central quasigroups, to [11] for results on quasigroups isotopic to groups, to [13] for results on quasigroups affine over various kinds of loops, and to [14, 15] for a broader context on affine representation of general algebraic structures. The article [3] gives a gentle introduction into automorphism groups of finite abelian groups and points to original sources on that topic.

The paper is organized as follows.

In Section 2, we formulate an isomorphism theorem for central quasigroups, Theorem 2.4, which is less general than [1, Theorem 2.10] or [11, Corollary 28], and equivalent to but less technical than [1, Theorem 3.2]. We also present the enumeration algorithm in detail.

In Section 3, we establish our own version of [12, Theorem 2] and [1, Theorem 3.5] for cyclic p -groups, Theorem 3.1, providing an explicit formula for the number of isomorphism classes. We were informed that the same result was obtained by Kirnasovsky in his unpublished PhD thesis [6]. Since the automorphism groups of cyclic groups are commutative, Theorem 3.1 also yields the number of medial quasigroups up to isomorphism over finite cyclic groups, and of prime order in particular.

Finally, the results of the enumeration are presented in the Appendix.

2 Isomorphism theorem and enumeration algorithm

2.1 Elementary properties of the counting functions cq and mq

For an abelian group G , let $cq(G)$ (resp. $mq(G)$) denote the number of all central (resp. medial) quasigroups over G up to isomorphism. For $n \geq 1$, let $cq(n)$ (resp. $mq(n)$) denote the number of all central (resp. medial) quasigroups of order n up to isomorphism.

Let us establish two fundamental properties of the counting functions.

First, by the remarks in the introduction,

$$cq(n) = \sum_{|G|=n} cq(G) \quad \text{and} \quad mq(n) = \sum_{|G|=n} mq(G),$$

where the summations run over all abelian groups of order n up to isomorphism.

Second, Proposition 2.1 shows that the classification of central and medial quasigroups can be reduced to prime power orders. As far as enumeration is concerned, Proposition 2.1 implies that the functions $cq, mq : \mathbb{N}^+ \rightarrow \mathbb{N}^+$ are multiplicative in the number-theoretic sense.

Proposition 2.1. *Let $G = H \times K$ be an abelian group such that $\gcd(|H|, |K|) = 1$. Up to isomorphism, any quasigroup affine over G can be expressed in a unique way as a direct product of a quasigroup affine over H and a quasigroup affine over K . In particular,*

$$cq(G) = cq(H) \cdot cq(K) \quad \text{and} \quad mq(G) = mq(H) \cdot mq(K).$$

Proof. Any automorphism of G decomposes uniquely as a direct product of an automorphism of H and an automorphism of K , cf. [3, Lemma 2.1]. The rest is easy. \square

2.2 The isomorphism problem for central quasigroups

Let us now consider the isomorphism problem for quasigroups affine over a fixed abelian group $(G, +)$.

Consider any group A . (Later we will take $A = \text{Aut}(G, +)$.) Then A acts on itself by conjugation, and A also acts on $A \times A$ by a simultaneous conjugation in both coordinates, i.e., $(\alpha, \beta)^\gamma = (\alpha^\gamma, \beta^\gamma)$.

Lemma 2.2. *Let A be a group. Let X be a complete set of orbit representatives of the conjugation action of A on itself. For $\xi \in X$, let Y_ξ be a complete set of orbit representatives of the conjugation action of the centralizer $C_A(\xi)$ on A . Then*

$$\{(\xi, v) : \xi \in X, v \in Y_\xi\}$$

is a complete set of orbit representatives of the conjugation action of A on $A \times A$.

Proof. For every $(\alpha, \beta) \in A \times A$ there is a unique $\xi \in X$ and some $\gamma \in A$ such that (α, β) and (ξ, γ) are in the same orbit. For a fixed $\xi \in X$ and some $\beta, \gamma \in A$, we have (ξ, β) in the same orbit as (ξ, γ) if and only if there is $\delta \in C_A(\xi)$ such that $\beta^\delta = \gamma$. \square

Lemma 2.3. *Let $(G, +)$ be an abelian group, $A = \text{Aut}(G, +)$ and $\alpha, \beta \in A$. Then $C_A(\alpha) \cap C_A(\beta)$ acts naturally on $G/\text{Im}(1 - \alpha - \beta)$.*

Proof. Let $U = \text{Im}(1 - \alpha - \beta)$. It suffices to show that for every $\gamma \in C_A(\alpha) \cap C_A(\beta)$ the mapping $u + U \mapsto \gamma(u) + U$ is well-defined. Now, if $u + U = v + U$ then $u = v + w - \alpha(w) - \beta(w)$ for some $w \in G$ and we have $\gamma(u) = \gamma(v) + \gamma(w) - \gamma\alpha(w) - \gamma\beta(w) = \gamma(v) + \gamma(w) - \alpha\gamma(w) - \beta\gamma(w) = \gamma(v) + (1 - \alpha - \beta)(\gamma(w)) \in \gamma(v) + U$. \square

We will now state a theorem that solves the isomorphism problem for central and medial quasigroups over $(G, +)$. Instead of showing how it follows from the more general [1, Theorem 2.10], we show that it is equivalent to [1, Theorem 3.2], which we restate as Theorem 2.5 here.

Theorem 2.4 (Isomorphism problem for central quasigroups). *Let $(G, +)$ be an abelian group, let $\varphi_1, \psi_1, \varphi_2, \psi_2 \in \text{Aut}(G, +)$, and let $c_1, c_2 \in G$. Then the following statements are equivalent:*

- (i) *the central quasigroups $\mathcal{Q}(G, +, \varphi_1, \psi_1, c_1)$ and $\mathcal{Q}(G, +, \varphi_2, \psi_2, c_2)$ are isomorphic;*
- (ii) *there is an automorphism γ of $(G, +)$ and an element $u \in \text{Im}(1 - \varphi_1 - \psi_1)$ such that*

$$\varphi_2 = \gamma\varphi_1\gamma^{-1}, \quad \psi_2 = \gamma\psi_1\gamma^{-1}, \quad c_2 = \gamma(c_1 + u).$$

Theorem 2.5 ([1, Theorem 3.2]). *Let $(G, +)$ be an abelian group and denote $A = \text{Aut}(G, +)$. The isomorphism classes of central quasigroups (resp. medial quasigroups) over $(G, +)$ are in one-to-one correspondence with the elements of the set*

$$\{(\varphi, \psi, c) : \varphi \in X, \psi \in Y_\varphi, c \in G_{\varphi, \psi}\},$$

where

- X is a complete set of orbit representatives of the conjugation action of A on itself;

- Y_φ is a complete set of orbit representatives of the conjugation action of $C_A(\varphi)$ on A (resp. on $C_A(\varphi)$), for every $\varphi \in X$;
- $G_{\varphi,\psi}$ is a complete set of orbit representatives of the natural action of $C_A(\varphi) \cap C_A(\psi)$ on $G/\text{Im}(1 - \varphi - \psi)$.

Here is a proof of the equivalence of Theorems 2.4 and 2.5: By Lemma 2.2, we can assume that we are investigating the equivalence of two triples (φ, ψ, c_1) and (φ, ψ, c_2) for some $\varphi \in X$, $\psi \in Y_\varphi$ and $c_1, c_2 \in G$. Let $U = \text{Im}(1 - \varphi - \psi)$. The following conditions are then equivalent for any $\gamma \in \text{Aut}(G, +)$, using Lemma 2.3: $c_2 = \gamma(c_1 + u)$ for some $u \in U$, $c_2 \in \gamma(c_1 + U) = \gamma(c_1) + U$, $c_2 + U = \gamma(c_1) + U = \gamma(c_1 + U)$. This finishes the proof.

2.3 The algorithm

Theorem 2.5 together with the results of Subsection 2.1 gives rise to the following algorithm that enumerates central and medial quasigroups of order n . In the algorithm we denote by $R(H, X)$ a complete set of representatives of the (clear from context) action of H on X .

Algorithm 2.6.

Input: positive integer n

Output: $cq(n)$ and $mq(n)$

```

cqn := 0; mqn := 0;
for G in the set of abelian groups of order n up to isomorphism do
  cqG := 0; mqG := 0;
  A := automorphism group of G;
  for f in R(A,A) do
    for g in R(C_A(f),A) do
      for c in R( Intersection(C_A(f),C_A(g)), G/Im(1-f-g) ) do
        cqG := cqG + 1;
        if f*g=g*f then mqG := mqG + 1; fi;
      od;
    od;
  od;
  cqn := cqn + cqG; mqn := mqn + mqG;
od;
return cqn, mqn;

```

The algorithm was implemented in the GAP system [2] in a straightforward fashion, taking advantage of some functionality of the LOOPS [7] package. The code is available from the second author at www.math.du.edu/~petr.

In small situations it is possible to directly calculate the orbits of the conjugation action of $A = \text{Aut}(G, +)$ on $A \times A$. For larger groups, it is safer (due to memory constraints) to work with one conjugacy class of A at a time, as in Algorithm 2.5.

Among the cases we managed to calculate, the elementary abelian group C_2^5 took the most effort, about 4 hours on a standard personal computer. It might not be difficult to calculate some of the missing entries for $mq(G)$. However, $cq(C_2^6)$, for instance, appears out of reach without further theoretical advances or more substantial computational resources.

The outcome of the calculation can be found in the Appendix.

3 Quasigroups affine over cyclic groups

Let G be a cyclic group. Since $\text{Aut}(G)$ is commutative, every quasigroup affine over G is medial.

Theorem 3.1 ([6, p. 70]). *Let p be a prime and k a positive integer. Then*

$$cq(C_{p^k}) = mq(C_{p^k}) = p^{2k} + p^{2k-2} - p^{k-1} - \sum_{i=k-1}^{2k-1} p^i.$$

Proof. Let $G = C_{p^k}$ and $A = \text{Aut}(G)$. We will identify A with the $p^k - p^{k-1}$ elements of $G^* = \{a \in G : p \nmid a\}$. We will follow Algorithm 2.6. Since A is commutative, the conjugation action is trivial and we have to consider every $(\varphi, \psi) \in A \times A$. For a fixed $(\varphi, \psi) \in A \times A$, we must consider a complete set of orbit representatives $G_{\varphi, \psi}$ of the action of $A = C_A(\varphi) \cap C_A(\psi)$ on $G/\text{Im}(1 - \varphi - \psi)$. Now, $\text{Im}(1 - \varphi - \psi)$ is equal to $p^i G$ if and only if $p^i \mid 1 - \varphi - \psi$ and $p^{i+1} \nmid 1 - \varphi - \psi$.

Case $i = 0$, i.e.,

$$\varphi + \psi \not\equiv 1 \pmod{p}.$$

In this case, we can take $G_{\varphi, \psi} = \{0\}$. How many such pairs (φ, ψ) exist? First, let us count those with $\varphi \equiv 1 \pmod{p}$. Then $\psi \in G^*$ can be chosen arbitrarily, hence we have $p^{k-1}(p^k - p^{k-1})$ such pairs. Next, let us count those with $\varphi \not\equiv 1 \pmod{p}$. Then $\psi \in G^*$ must satisfy $\psi \not\equiv 1 - \varphi \pmod{p}$, hence we have $(p^k - 2p^{k-1})(p^k - 2p^{k-1})$ such pairs. Since $|G_{\varphi, \psi}| = 1$, this case contributes to $cq(G)$ by

$$p^{k-1}(p^k - p^{k-1}) + (p^k - 2p^{k-1})^2.$$

Cases $i = 1, \dots, k-1$, i.e.,

$$\varphi + \psi \equiv 1 \pmod{p^i} \quad \text{and} \quad \varphi + \psi \not\equiv 1 \pmod{p^{i+1}}.$$

In this case, we can take $G_{\varphi, \psi} = \{0, p^0, \dots, p^{i-1}\}$. How many such pairs (φ, ψ) exist? For $\varphi \equiv 1 \pmod{p}$, any solution ψ to the congruence above is divisible by p , hence there is no such solution $\psi \in G^*$. For $\varphi \not\equiv 1 \pmod{p}$, we have precisely $p^{k-i} - p^{k-i-1}$ solutions to the conditions in G^* . Since $|G_{\varphi, \psi}| = i+1$, this case contributes to $cq(G)$ by

$$(p^k - 2p^{k-1})(p^{k-i} - p^{k-i-1})(i+1).$$

Case $i = k$, i.e.,

$$\varphi + \psi = 1.$$

In this case, we can take $G_{\varphi,\psi} = \{0, p^0, \dots, p^{k-1}\}$. How many such pairs (φ, ψ) exist? Since ψ is uniquely determined by φ and neither of φ, ψ shall be divisible by p , we have precisely $p^k - 2p^{k-1}$ such pairs. Since $|G_{\varphi,\psi}| = k + 1$, this case contributes to $cq(G)$ by

$$(p^k - 2p^{k-1})(k + 1).$$

Summarized, the cases $i = 1, \dots, k$ contribute to $cq(G)$ the total of

$$(p^k - 2p^{k-1}) \left(\left(\sum_{i=1}^{k-1} (p^{k-i} - p^{k-i-1}) \cdot (i + 1) \right) + (k + 1) \right),$$

which, after rearrangement, gives

$$(p^k - 2p^{k-1})(2p^{k-1} + p^{k-2} + p^{k-3} + \dots + p + 1).$$

The total sum is then

$$\begin{aligned} cq(G) &= p^{2k-1} - p^{2k-2} + (p^k - 2p^{k-1})(p^k - 2p^{k-1}) + (2p^{k-1} + p^{k-2} + p^{k-3} + \dots + p + 1) \\ &= p^{2k-1} - p^{2k-2} + (p^k - 2p^{k-1})(p^k + p^{k-2} + p^{k-3} + \dots + p + 1) \\ &= p^{2k} - p^{2k-1} - p^{2k-3} - \dots - p^k - 2p^{k-1}, \end{aligned}$$

which can be expressed as in the statement of the theorem. \square

Corollary 3.2. *For any $k \geq 1$ we have $cq(C_{2^k}) = mq(C_{2^k}) = 2^{2k-2}$.*

Corollary 3.3. *For any prime p we have $cq(p) = mq(p) = p^2 - p - 1$.*

Corollary 3.3 is a special case of [12, Corollary 2] for binary quasigroups.

As a counterpart to Theorem 3.1, we ask:

Problem 3.4. For a prime p and $k > 1$, find explicit formulas for $cq(C_p^k)$ and $mq(C_p^k)$.

References

- [1] A. Drápal, *Group isotopes and a holomorphic action*, Result. Math. **54** (2009), no. **3–4**, 253–272.
- [2] The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.5.5; 2012. <http://www.gap-system.org>
- [3] C. J. Hillar, D. L. Rhea, *Automorphisms of finite abelian groups*, Amer. Math. Monthly **114** (2007), 917–923.
- [4] X. Hou, *Finite modules over $\mathbb{Z}[t, t^{-1}]$* , J. Knot Theory Ramifications **21** (2012), no. **8**, 1250079, 28 pp.
- [5] O. U. Kirnasovsky, *Linear isotopes of small order groups*, Quasigroups and Related Systems **2** (1995), no. **1**, 51–82.
- [6] O. U. Kirnasovsky, *Binary and n -ary isotopes of groups: fundamental algebraic properties and characterizations*, PhD thesis, Kiev 2001 (Ukrainian).

- [7] G. P. Nagy and P. Vojtěchovský, **LOOPS**: Computing with quasigroups and loops in GAP, version 3.0.0, www.math.du.edu/loops.
- [8] OEIS Foundation Inc. (2011), The On-Line Encyclopedia of Integer Sequences, <http://oeis.org>.
- [9] J.D.H. Smith, *Finite equationally complete entropic quasigroups*, Contributions to general algebra (Proc. Klagenfurt Conf. 1978), 345–356 (1979).
- [10] J.D.H. Smith, *An introduction to quasigroups and their representations*, Chapman & Hall/CRC, 2007.
- [11] F. Sokhatsky, *On isotopes of groups, I, II, III*, Ukrainian Math. J. 47/10 (1995), 1585–1598; 47/12 (1995), 1935–1948; 48/2 (1996), 283–293.
- [12] F. Sokhatsky, P. Syvakivskij, *On linear isotopes of cyclic groups*, Quasigroups and Related Systems **1** (1994), no. **1**, 66–76.
- [13] D. Stanovský, *A guide to self-distributive quasigroups, or latin quandles*, Quasigroups and Related Systems **23** (2015), no. **1**, 91–128.
- [14] M. Stronkowski, D. Stanovský, *Embedding general algebras into modules*, Proc. Amer. Math. Soc. **138** (2010), no. **8**, 2687–2699.
- [15] Á. Szendrei, *Modules in general algebra*, Contributions to general algebra **10** (Proc. Klagenfurt Conf. 1997), 41–53 (1998).

Appendix: Central and medial quasigroups of order less than 128

The following table contains the results of our enumeration of central and medial quasigroups of order less than 128.

If a row in the table starts with n/k then: column “ G ” gives the catalog number n/k corresponding to the abelian group `SmallGroup(n,k)` of GAP; column “structure” gives a structural description of the group G from which a decomposition of G into p -primary components is readily seen and hence Proposition 2.1 can be routinely applied; column “ $|A|$ ” gives the cardinality of the group $A = \text{Aut}(G)$; column “ $|X|$ ” gives the number of conjugacy classes of A ; column “ $|O|$ ” gives the number of orbits of the conjugation action of A on $A \times A$ (with action $(f, g)^h = (f^h, g^h)$), which is a lower bound on the number of quasigroups affine over G ; column “ cq ” gives the number of quasigroups affine over G up to isomorphism; column “ $|O_c|$ ” gives the number of orbits in O with a representative (f, g) such that $fg = gf$, which is a lower bound on the number of medial quasigroups over G ; column “ mq ” gives the number of medial quasigroups over G up to isomorphism; and column “ref” gives a reference to a numbered result within this paper if the entries in the row follow from the cited result and possibly also from previously listed table entries.

If a row in the table starts with \mathbf{n} then: column “ G ” gives the order n ; column “ cq ” gives the number of central quasigroups of order n up to isomorphism; and column “ mq ” gives the number of medial quasigroups of order n up to isomorphism.

Entries that we were not able to establish are denoted by “?” or “?”.

All entries corresponding to prime-power orders were explicitly calculated by Algorithm 2.6 although the cyclic cases follow from Theorem 3.1. Many of the entries corresponding to the remaining orders were also initially obtained by Algorithm 2.6 (to test the algorithm) but in the final version they were calculated directly from earlier entries using Proposition 2.1.

To reduce the number of transcription and arithmetical errors, the entries and the L^AT_EX source of the table were computer generated.

G	structure	$ A $	$ X $	$ O $	cq	$ O_c $	mq	ref
1/1 1	C_1	1	1	1	1	1	1	
2/1 2	C_2	1	1	1	1	1	1	3.1
3/1 3	C_3	2	2	4	5	4	5	3.1
4/1 4/2 4	C_4 C_2^2	2	2	4	4	4	4	3.1
		6	3	11	15	8	9	
					19		13	
5/1 5	C_5	4	4	16	19	16	19	3.1
					19		19	
6/2 6	$C_2 \times C_3$	2	2	4	5	4	5	2.1
					5		5	
7/1 7	C_7	6	6	36	41	36	41	3.1
					41		41	

G	structure	$ A $	$ X $	$ O $	cq	$ O_c $	mq	ref
8/1	C_8	4	4	16	16	16	16	3.1
8/2	$C_4 \times C_2$	8	5	28	28	22	22	
8/5	C_2^3	168	6	197	341	32	35	
8					385		73	
9/1	C_9	6	6	36	48	36	48	3.1
9/2	C_3^2	48	8	136	183	56	68	
9					231		116	
10/2	$C_2 \times C_5$	4	4	16	19	16	19	2.1
10					19		19	
11/1	C_{11}	10	10	100	109	100	109	3.1
11					109		109	
12/2	$C_4 \times C_3$	4	4	16	20	16	20	2.1
12/5	$C_2^2 \times C_3$	12	6	44	75	32	45	2.1
12					95		65	
13/1	C_{13}	12	12	144	155	144	155	3.1
13					155		155	
14/2	$C_2 \times C_7$	6	6	36	41	36	41	2.1
14					41		41	
15/1	$C_3 \times C_5$	8	8	64	95	64	95	2.1
15					95		95	
16/1	C_{16}	8	8	64	64	64	64	3.1
16/2	C_4^2	96	14	400	624	168	188	
16/5	$C_8 \times C_2$	16	10	112	112	88	88	
16/10	$C_4 \times C_2^2$	192	13	564	820	146	150	
16/14	C_2^4	20160	14	20747	39767	160	179	
16					41387		669	
17/1	C_{17}	16	16	256	271	256	271	3.1
17					271		271	
18/2	$C_2 \times C_9$	6	6	36	48	36	48	2.1
18/5	$C_2 \times C_3^2$	48	8	136	183	56	68	2.1
18					231		116	
19/1	C_{19}	18	18	324	341	324	341	3.1
19					341		341	
20/2	$C_4 \times C_5$	8	8	64	76	64	76	2.1
20/5	$C_2^2 \times C_5$	24	12	176	285	128	171	2.1
20					361		247	
21/2	$C_3 \times C_7$	12	12	144	205	144	205	2.1
21					205		205	
22/2	$C_2 \times C_{11}$	10	10	100	109	100	109	2.1
22					109		109	
23/1	C_{23}	22	22	484	505	484	505	3.1
23					505		505	

G	structure	$ A $	$ X $	$ O $	cq	$ O_c $	mq	ref
24/2	$C_8 \times C_3$	8	8	64	80	64	80	2.1
24/9	$C_4 \times C_2 \times C_3$	16	10	112	140	88	110	2.1
24/15	$C_2^3 \times C_3$	336	12	788	1705	128	175	2.1
24					1925		365	
25/1	C_{25}	20	20	400	490	400	490	3.1
25/2	C_5^2	480	24	2336	2847	512	594	
25					3337		1084	
26/2	$C_2 \times C_{13}$	12	12	144	155	144	155	2.1
26					155		155	
27/1	C_{27}	18	18	324	441	324	441	3.1
27/2	$C_9 \times C_3$	108	20	864	1356	336	528	
27/5	C_3^3	11232	24	23236	34321	484	605	
27					36118		1574	
28/2	$C_4 \times C_7$	12	12	144	164	144	164	2.1
28/4	$C_2^2 \times C_7$	36	18	396	615	288	369	2.1
28					779		533	
29/1	C_{29}	28	28	784	811	784	811	3.1
29					811		811	
30/4	$C_2 \times C_3 \times C_5$	8	8	64	95	64	95	2.1
30					95		95	
31/1	C_{31}	30	30	900	929	900	929	3.1
31					929		929	
32/1	C_{32}	16	16	256	256	256	256	3.1
32/3	$C_8 \times C_4$	128	26	1216	1216	592	592	
32/16	$C_{16} \times C_2$	32	20	448	448	352	352	
32/21	$C_4^2 \times C_2$	1536	30	6224	9808	884	904	
32/36	$C_8 \times C_2^2$	384	26	2256	3280	584	600	
32/45	$C_4 \times C_2^3$	21504	30	48412	87580	804	834	
32/51	C_2^5	9999360	27	10024077	19721077	590	655	
32					19823665		4193	
33/1	$C_3 \times C_{11}$	20	20	400	545	400	545	2.1
33					545		545	
34/2	$C_2 \times C_{17}$	16	16	256	271	256	271	2.1
34					271		271	
35/1	$C_5 \times C_7$	24	24	576	779	576	779	2.1
35					779		779	
36/2	$C_4 \times C_9$	12	12	144	192	144	192	2.1
36/5	$C_2^2 \times C_9$	36	18	396	720	288	432	2.1
36/8	$C_4 \times C_3^2$	96	16	544	732	224	272	2.1
36/14	$C_2^2 \times C_3^2$	288	24	1496	2745	448	612	2.1
36					4389		1508	
37/1	C_{37}	36	36	1296	1331	1296	1331	3.1
37					1331		1331	

G	structure	$ A $	$ X $	$ O $	cq	$ O_c $	mq	ref
38/2 38	$C_2 \times C_{19}$	18	18	324	341 341	324	341 341	2.1
39/2 39	$C_3 \times C_{13}$	24	24	576	775 775	576	775 775	2.1
40/2	$C_8 \times C_5$	16	16	256	304	256	304	2.1
40/9	$C_4 \times C_2 \times C_5$	32	20	448	532	352	418	2.1
40/14 40	$C_2^3 \times C_5$	672	24	3152	6479 7315	512	665 1387	2.1
41/1 41	C_{41}	40	40	1600	1639 1639	1600	1639 1639	3.1
42/6 42	$C_2 \times C_3 \times C_7$	12	12	144	205 205	144	205 205	2.1
43/1 43	C_{43}	42	42	1764	1805 1805	1764	1805 1805	3.1
44/2	$C_4 \times C_{11}$	20	20	400	436	400	436	2.1
44/4 44	$C_2^2 \times C_{11}$	60	30	1100	1635 2071	800	981 1417	2.1
45/1	$C_9 \times C_5$	24	24	576	912	576	912	2.1
45/2 45	$C_3^2 \times C_5$	192	32	2176	3477 4389	896	1292 2204	2.1
46/2 46	$C_2 \times C_{23}$	22	22	484	505 505	484	505 505	2.1
47/1 47	C_{47}	46	46	2116	2161 2161	2116	2161 2161	3.1
48/2	$C_{16} \times C_3$	16	16	256	320	256	320	2.1
48/20	$C_4^2 \times C_3$	192	28	1600	3120	672	940	2.1
48/23	$C_8 \times C_2 \times C_3$	32	20	448	560	352	440	2.1
48/44	$C_4 \times C_2^2 \times C_3$	384	26	2256	4100	584	750	2.1
48/52 48	$C_2^4 \times C_3$	40320	28	82988	198835 206935	640	895 3345	2.1
49/1	C_{49}	42	42	1764	2044	1764	2044	3.1
49/2 49	C_7^2	2016	48	13896	16055 18099	2088	2344 4388	
50/2	$C_2 \times C_{25}$	20	20	400	490	400	490	2.1
50/5 50	$C_2 \times C_5^2$	480	24	2336	2847 3337	512	594 1084	2.1
51/1 51	$C_3 \times C_{17}$	32	32	1024	1355 1355	1024	1355 1355	2.1
52/2	$C_4 \times C_{13}$	24	24	576	620	576	620	2.1
52/5 52	$C_2^2 \times C_{13}$	72	36	1584	2325 2945	1152	1395 2015	2.1
53/1 53	C_{53}	52	52	2704	2755 2755	2704	2755 2755	3.1

G	structure	$ A $	$ X $	$ O $	cq	$ O_c $	mq	ref
54/2	$C_2 \times C_{27}$	18	18	324	441	324	441	2.1
54/9	$C_2 \times C_9 \times C_3$	108	20	864	1356	336	528	2.1
54/15	$C_2 \times C_3^3$	11232	24	23236	34321	484	605	2.1
54					36118		1574	
55/2	$C_5 \times C_{11}$	40	40	1600	2071	1600	2071	2.1
55					2071		2071	
56/2	$C_8 \times C_7$	24	24	576	656	576	656	2.1
56/8	$C_4 \times C_2 \times C_7$	48	30	1008	1148	792	902	2.1
56/13	$C_2^3 \times C_7$	1008	36	7092	13981	1152	1435	2.1
56					15785		2993	
57/2	$C_3 \times C_{19}$	36	36	1296	1705	1296	1705	2.1
57					1705		1705	
58/2	$C_2 \times C_{29}$	28	28	784	811	784	811	2.1
58					811		811	
59/1	C_{59}	58	58	3364	3421	3364	3421	3.1
59					3421		3421	
60/4	$C_4 \times C_3 \times C_5$	16	16	256	380	256	380	2.1
60/13	$C_2^2 \times C_3 \times C_5$	48	24	704	1425	512	855	2.1
60					1805		1235	
61/1	C_{61}	60	60	3600	3659	3600	3659	3.1
61					3659		3659	
62/2	$C_2 \times C_{31}$	30	30	900	929	900	929	2.1
62					929		929	
63/2	$C_9 \times C_7$	36	36	1296	1968	1296	1968	2.1
63/4	$C_3^2 \times C_7$	288	48	4896	7503	2016	2788	2.1
63					9471		4756	
64/1	C_{64}	32	32	1024	1024	1024	1024	3.1
64/2	C_8^2	1536	60	13568	22784	3072	3408	
64/26	$C_{16} \times C_4$	256	52	4864	4864	2368	2368	
64/50	$C_{32} \times C_2$	64	40	1792	1792	1408	1408	
64/55	C_4^3	86016	60	206144	441664	4448	4672	
64/83	$C_8 \times C_4 \times C_2$	2048	104	31168	31168	7240	7240	
64/183	$C_{16} \times C_2^2$	768	52	9024	13120	2336	2400	
64/192	$C_4^2 \times C_2^2$	147456	100	550480	1239472	9108	9656	
64/246	$C_8 \times C_2^3$	43008	60	193648	350320	3216	3336	
64/260	$C_4 \times C_2^4$	10321920	69	?	?	?	?	
64/267	C_2^6	20158709760	60	?	?	?	?	
64					?		?	
65/1	$C_5 \times C_{13}$	48	48	2304	2945	2304	2945	2.1
65					2945		2945	
66/4	$C_2 \times C_3 \times C_{11}$	20	20	400	545	400	545	2.1
66					545		545	
67/1	C_{67}	66	66	4356	4421	4356	4421	3.1
67					4421		4421	

G	structure	$ A $	$ X $	$ O $	cq	$ O_c $	mq	ref
68/2	$C_4 \times C_{17}$	32	32	1024	1084	1024	1084	2.1
68/5	$C_2^2 \times C_{17}$	96	48	2816	4065	2048	2439	2.1
68					5149		3523	
69/1	$C_3 \times C_{23}$	44	44	1936	2525	1936	2525	2.1
69					2525		2525	
70/4	$C_2 \times C_5 \times C_7$	24	24	576	779	576	779	2.1
70					779		779	
71/1	C_{71}	70	70	4900	4969	4900	4969	3.1
71					4969		4969	
72/2	$C_8 \times C_9$	24	24	576	768	576	768	2.1
72/9	$C_4 \times C_2 \times C_9$	48	30	1008	1344	792	1056	2.1
72/14	$C_8 \times C_3^2$	192	32	2176	2928	896	1088	2.1
72/18	$C_2^3 \times C_9$	1008	36	7092	16368	1152	1680	2.1
72/36	$C_4 \times C_2 \times C_3^2$	384	40	3808	5124	1232	1496	2.1
72/50	$C_2^3 \times C_3^2$	8064	48	26792	62403	1792	2380	2.1
72					88935		8468	
73/1	C_{73}	72	72	5184	5255	5184	5255	3.1
73					5255		5255	
74/2	$C_2 \times C_{37}$	36	36	1296	1331	1296	1331	2.1
74					1331		1331	
75/1	$C_3 \times C_{25}$	40	40	1600	2450	1600	2450	2.1
75/3	$C_3 \times C_5^2$	960	48	9344	14235	2048	2970	2.1
75					16685		5420	
76/2	$C_4 \times C_{19}$	36	36	1296	1364	1296	1364	2.1
76/4	$C_2^2 \times C_{19}$	108	54	3564	5115	2592	3069	2.1
76					6479		4433	
77/1	$C_7 \times C_{11}$	60	60	3600	4469	3600	4469	2.1
77					4469		4469	
78/6	$C_2 \times C_3 \times C_{13}$	24	24	576	775	576	775	2.1
78					775		775	
79/1	C_{79}	78	78	6084	6161	6084	6161	3.1
79					6161		6161	
80/2	$C_{16} \times C_5$	32	32	1024	1216	1024	1216	2.1
80/20	$C_4^2 \times C_5$	384	56	6400	11856	2688	3572	2.1
80/23	$C_8 \times C_2 \times C_5$	64	40	1792	2128	1408	1672	2.1
80/45	$C_4 \times C_2^2 \times C_5$	768	52	9024	15580	2336	2850	2.1
80/52	$C_2^4 \times C_5$	80640	56	331952	755573	2560	3401	2.1
80					786353		12711	
81/1	C_{81}	54	54	2916	3996	2916	3996	3.1
81/2	C_9^2	3888	78	35316	54405	5616	8055	
81/5	$C_{27} \times C_3$	324	60	7776	12897	3024	5157	
81/11	$C_9 \times C_3^2$	23328	74	152892	270441	4176	7167	
81/15	C_3^4	24261120	78	?	?	?	?	
81					?		?	

G	structure	$ A $	$ X $	$ O $	cq	$ O_c $	mq	ref
82/2 82	$C_2 \times C_{41}$	40	40	1600	1639 1639	1600	1639 1639	2.1
83/1 83	C_{83}	82	82	6724	6805 6805	6724	6805 6805	3.1
84/6 84/15 84	$C_4 \times C_3 \times C_7$ $C_2^2 \times C_3 \times C_7$	24 72	24 36	576 1584	820 3075 3895	576 1152	820 1845 2665	2.1 2.1
85/1 85	$C_5 \times C_{17}$	64	64	4096	5149 5149	4096	5149 5149	2.1
86/2 86	$C_2 \times C_{43}$	42	42	1764	1805 1805	1764	1805 1805	2.1
87/1 87	$C_3 \times C_{29}$	56	56	3136	4055 4055	3136	4055 4055	2.1
88/2 88/8 88/12 88	$C_8 \times C_{11}$ $C_4 \times C_2 \times C_{11}$ $C_2^3 \times C_{11}$	40 80 1680	40 50 60	1600 2800 19700	1744 3052 37169 41965	1600 2200 3200	1744 2398 3815 7957	2.1 2.1 2.1
89/1 89	C_{89}	88	88	7744	7831 7831	7744	7831 7831	3.1
90/4 90/10 90	$C_2 \times C_9 \times C_5$ $C_2 \times C_3^2 \times C_5$	24 192	24 32	576 2176	912 3477 4389	576 896	912 1292 2204	2.1 2.1
91/1 91	$C_7 \times C_{13}$	72	72	5184	6355 6355	5184	6355 6355	2.1
92/2 92/4 92	$C_4 \times C_{23}$ $C_2^2 \times C_{23}$	44 132	44 66	1936 5324	2020 7575 9595	1936 3872	2020 4545 6565	2.1 2.1
93/2 93	$C_3 \times C_{31}$	60	60	3600	4645 4645	3600	4645 4645	2.1
94/2 94	$C_2 \times C_{47}$	46	46	2116	2161 2161	2116	2161 2161	2.1
95/1 95	$C_5 \times C_{19}$	72	72	5184	6479 6479	5184	6479 6479	2.1
96/2 96/46 96/59 96/161 96/176 96/220 96/231 96	$C_{32} \times C_3$ $C_8 \times C_4 \times C_3$ $C_{16} \times C_2 \times C_3$ $C_4^2 \times C_2 \times C_3$ $C_8 \times C_2^2 \times C_3$ $C_4 \times C_2^3 \times C_3$ $C_2^5 \times C_3$	32 256 64 3072 768 43008 19998720	32 52 40 60 52 60 54	1024 4864 1792 24896 9024 193648 40096308	1280 6080 2240 49040 16400 437900 98605385 99118325	1024 2368 1408 3536 2336 3216 2360	1280 2960 1760 4520 3000 4170 3275 20965	2.1 2.1 2.1 2.1 2.1 2.1 2.1
97/1 97	C_{97}	96	96	9216	9311 9311	9216	9311 9311	3.1

G	structure	$ A $	$ X $	$ O $	cq	$ O_c $	mq	ref
98/2	$C_2 \times C_{49}$	42	42	1764	2044	1764	2044	2.1
98/5	$C_2 \times C_7^2$	2016	48	13896	16055	2088	2344	2.1
98					18099		4388	
99/1	$C_9 \times C_{11}$	60	60	3600	5232	3600	5232	2.1
99/2	$C_3^2 \times C_{11}$	480	80	13600	19947	5600	7412	2.1
99					25179		12644	
100/2	$C_4 \times C_{25}$	40	40	1600	1960	1600	1960	2.1
100/5	$C_2^2 \times C_{25}$	120	60	4400	7350	3200	4410	2.1
100/8	$C_4 \times C_5^2$	960	48	9344	11388	2048	2376	2.1
100/16	$C_2^2 \times C_5^2$	2880	72	25696	42705	4096	5346	2.1
100					63403		14092	
101/1	C_{101}	100	100	10000	10099	10000	10099	3.1
101					10099		10099	
102/4	$C_2 \times C_3 \times C_{17}$	32	32	1024	1355	1024	1355	2.1
102					1355		1355	
103/1	C_{103}	102	102	10404	10505	10404	10505	3.1
103					10505		10505	
104/2	$C_8 \times C_{13}$	48	48	2304	2480	2304	2480	2.1
104/9	$C_4 \times C_2 \times C_{13}$	96	60	4032	4340	3168	3410	2.1
104/14	$C_2^3 \times C_{13}$	2016	72	28368	52855	4608	5425	2.1
104					59675		11315	
105/2	$C_3 \times C_5 \times C_7$	48	48	2304	3895	2304	3895	2.1
105					3895		3895	
106/2	$C_2 \times C_{53}$	52	52	2704	2755	2704	2755	2.1
106					2755		2755	
107/1	C_{107}	106	106	11236	11341	11236	11341	3.1
107					11341		11341	
108/2	$C_4 \times C_{27}$	36	36	1296	1764	1296	1764	2.1
108/5	$C_2^2 \times C_{27}$	108	54	3564	6615	2592	3969	2.1
108/12	$C_4 \times C_9 \times C_3$	216	40	3456	5424	1344	2112	2.1
108/29	$C_2^2 \times C_9 \times C_3$	648	60	9504	20340	2688	4752	2.1
108/35	$C_4 \times C_3^3$	22464	48	92944	137284	1936	2420	2.1
108/45	$C_2^2 \times C_3^3$	67392	72	255596	514815	3872	5445	2.1
108					686242		20462	
109/1	C_{109}	108	108	11664	11771	11664	11771	3.1
109					11771		11771	
110/6	$C_2 \times C_5 \times C_{11}$	40	40	1600	2071	1600	2071	2.1
110					2071		2071	
111/2	$C_3 \times C_{37}$	72	72	5184	6655	5184	6655	2.1
111					6655		6655	

G	structure	$ A $	$ X $	$ O $	cq	$ O_c $	mq	ref
112/2	$C_{16} \times C_7$	48	48	2304	2624	2304	2624	2.1
112/19	$C_4^2 \times C_7$	576	84	14400	25584	6048	7708	2.1
112/22	$C_8 \times C_2 \times C_7$	96	60	4032	4592	3168	3608	2.1
112/37	$C_4 \times C_2^2 \times C_7$	1152	78	20304	33620	5256	6150	2.1
112/43	$C_2^4 \times C_7$	120960	84	746892	1630447	5760	7339	2.1
112					1696867		27429	
113/1	C_{113}	112	112	12544	12655	12544	12655	3.1
113					12655		12655	
114/6	$C_2 \times C_3 \times C_{19}$	36	36	1296	1705	1296	1705	2.1
114					1705		1705	
115/1	$C_5 \times C_{23}$	88	88	7744	9595	7744	9595	2.1
115					9595		9595	
116/2	$C_4 \times C_{29}$	56	56	3136	3244	3136	3244	2.1
116/5	$C_2^2 \times C_{29}$	168	84	8624	12165	6272	7299	2.1
116					15409		10543	
117/2	$C_9 \times C_{13}$	72	72	5184	7440	5184	7440	2.1
117/4	$C_3^2 \times C_{13}$	576	96	19584	28365	8064	10540	2.1
117					35805		17980	
118/2	$C_2 \times C_{59}$	58	58	3364	3421	3364	3421	2.1
118					3421		3421	
119/1	$C_7 \times C_{17}$	96	96	9216	11111	9216	11111	2.1
119					11111		11111	
120/4	$C_8 \times C_3 \times C_5$	32	32	1024	1520	1024	1520	2.1
120/31	$C_4 \times C_2 \times C_3 \times C_5$	64	40	1792	2660	1408	2090	2.1
120/47	$C_2^3 \times C_3 \times C_5$	1344	48	12608	32395	2048	3325	2.1
120					36575		6935	
121/1	C_{121}	110	110	12100	13288	12100	13288	3.1
121/2	C_{11}^2	13200	120	144200	158199	13400	14508	
121					171487		27796	
122/2	$C_2 \times C_{61}$	60	60	3600	3659	3600	3659	2.1
122					3659		3659	
123/1	$C_3 \times C_{41}$	80	80	6400	8195	6400	8195	2.1
123					8195		8195	
124/2	$C_4 \times C_{31}$	60	60	3600	3716	3600	3716	2.1
124/4	$C_2^2 \times C_{31}$	180	90	9900	13935	7200	8361	2.1
124					17651		12077	
125/1	C_{125}	100	100	10000	12325	10000	12325	3.1
125/2	$C_{25} \times C_5$	2000	104	47200	66580	9280	13270	
125/5	C_5^3	1488000	120	?	?	?	?	
125					?		?	
126/6	$C_2 \times C_9 \times C_7$	36	36	1296	1968	1296	1968	2.1
126/16	$C_2 \times C_3^2 \times C_7$	288	48	4896	7503	2016	2788	2.1
126					9471		4756	
127/1	C_{127}	126	126	15876	16001	15876	16001	3.1
127					16001		16001	

DAVID STANOVSKÝ
Department of Algebra
Charles University
Sokolovská 83
186 75 Praha 8, CZECH REPUBLIC
E-mail: stanovsk@karlin.mff.cuni.cz

Received November 11, 2015

PETR VOJTĚCHOVSKÝ
Department of Mathematics
University of Denver
2280 S Vine St
Denver, Colorado 80208, U.S.A.
E-mail: petr@math.du.edu