Enumeration of nilpotent loops up to isotopy

Lucien Clavier

Abstract. We modify tools introduced in [Daly D., Vojtěchovský P., *Enumeration of nilpotent loops via cohomology*, J. Algebra **322** (2009), no. 11, 4080–4098] to count, for any odd prime q, the number of nilpotent loops of order $2q$ up to isotopy, instead of isomorphy.

Keywords: loop, nilpotent, enumeration, cohomology, isomorphy, isotopy

Classification: 20N05

1. Introduction

Recall that a set Q equipped with a binary operation $\cdot$ is a *loop* if it possesses a neutral element and if for each a, b in Q there exist unique x, y such that

$$a \cdot x = b \text{ and } y \cdot a = b.$$

As usual, we write these respectively as $x = a\backslash b$ and $y = b/a$. We abbreviate $x \cdot y$ as xy, and adopt the usual convention that multiplication should be performed first between contiguous elements, and then between dotted elements. For instance, $xy \cdot z$ is the same as $(x \cdot y) \cdot z$.

Recall that groups are exactly associative loops. Also, normalized latin squares are exactly multiplication tables of finite loops.

The *center* $Z(Q)$ of a loop Q consists of all elements x in Q such that

$$xy = yx,\ xy \cdot z = x \cdot yz,\ yx \cdot z = y \cdot xz \text{ and } yz \cdot x = y \cdot zx$$

for every y, z in Q.

Normal subloops are kernels of loop homomorphisms. The center $Z(Q)$ is a normal subloop of Q. The *upper central series* $Z_0(Q) \leq Z_1(Q) \leq \dots$ is defined inductively by

$$Z_0(Q) = 1,\ Q/Z_{i+1}(Q) = Z(Q/Z_i(Q)).$$

If $Z_{n-1}(Q) < Z_n(Q) = Q$ for some n, we say that Q is (*centrally*) *nilpotent of class* n.

A triple $t = (\alpha, \beta, \gamma)$ of bijections between two loops $(L_1, \cdot)$ and $(L_2, *)$ is an *isotopism* if

$$\alpha(x) * \beta(y) = \gamma(x \cdot y)$$

for each x, y in L_1. If such a triple exists, L_1 and L_2 are said to be *isotopic*. Isotopy defines a relation of equivalence; if two loops are isomorphic, they must be isotopic (it is the case when we can choose $\alpha = \beta = \gamma$). We write $\cong$ for the relation of isomorphy and $\simeq$ for the relation of isotopy.

An *autotopism* of a loop L is an isotopism from L to L. We write $\mathrm{Atp}(L)$ for the set of all autotopisms of a loop L; it is a group with respect to the law of composition.

We believe the present article is more or less self-contained, but we invite the reader to see [DV09] for any shortcut we may have used. Also, since both articles have the same scheme, most ideas here will appear more natural to those readers that are already well acquainted with [DV09].

Here is a summary of the paper, with A an abelian group, F a loop.

Section 2. This section is identical to Section 2 in [DV09], and was added for the sake of completeness. Namely, central extensions of A by F are in one-to-one correspondence with (normalized) cocycles. If two cocycles differ by a coboundary, their associated loops are isomorphic.

Section 3. The group $\mathrm{Atp}(F, A) = \mathrm{Atp}(F) \times \mathrm{Aut}(A)$ acts on $\mathrm{C}(F, A)$ via, for $t = (\alpha, \beta, \gamma)$:

$$(t, h) : \theta \mapsto N(h\theta(\alpha^{-1}, \beta^{-1}))$$

where N is the "normalizing" projection defined by

$$N(m)(x, y) = m(x, y) - m(x, 1) - m(1, y) + m(1, 1).$$

This induces an action on $\mathrm{H}(F, A)$; every orbit under this action consists of cocycles whose associated loops are isotopic.

Section 4. For a given cocycle θ, if every central extension of A by F isotopic to the loop $Q(F, A, \theta)$ is in the orbit of θ, we say that θ is separable. We provide some conditions under which cocycles are separable.

Section 5. We define (starred) invariant spaces of subgroups of $\mathrm{Atp}(F, A)$ in the same way as in [DV09]. Therefore, if every cocycle is separable, we can count the number of central extensions of A by F up to isotopy, as soon as we know the subgroup structure of $\mathrm{Atp}(F, A)$ and the cardinality of the starred invariant space of each subgroup of $\mathrm{Atp}(F, A)$.

Section 6. We study the case where $A = \mathbb{Z}_2$, $F = \mathbb{Z}_q$ with q an odd prime. In that case, we know from [Cla12] the subgroup structure of $\mathrm{Atp}(F)$ (see Subsection 6.1). Thus, we only have left to compute the invariant (resp. starred invariant) spaces of such subgroups. This is done in Subsection 6.2 (resp. 6.3).

Subsequently, we can compute the number $\widetilde{\mathcal{N}}(2q)$ of nilpotent loops of order $2q$ up to isotopy (Theorem 6.10), and describe the asymptotic growth of $\widetilde{\mathcal{N}}(2q)$ (Corollary 6.11).

Section 7. We provide some ideas related to the present work. See also Section 10 in [DV09].

2. Central extensions, cocycles and coboundaries

Let A be an abelian group and F a loop. A loop Q is a *central extension of A by F* if $A \le Z(Q)$ and $Q/A \cong F$.

A mapping $\theta : F \times F \to A$ is a (*normalized*) *cocycle* if it satisfies for every $x \in F$

$$\theta(1,x) = \theta(x,1) = 0.$$

For a cocycle θ, define $Q(F,A,\theta)$ to be $F \times A$ equipped with the multiplication:

$$(x,a)(y,b) = (xy, a+b+\theta(x,y)).$$

The following characterization of central loop extensions is folklore, and is in complete analogy with the associative case:

Theorem 2.1. *The loop Q is a central extension of A by F if and only if there is a cocycle θ such that $Q \cong Q(F,A,\theta)$.*

The cocycles form an abelian group $\mathrm{C}(F,A)$ with respect to the natural addition; when A is a field, $\mathrm{C}(F,A)$ is a vector space over A with the natural scalar multiplication.

Define

$$\mathrm{Map}_0(F,A) = \{\tau : F \to A;\ \tau(1) = 0\},$$
$$\mathrm{Hom}(F,A) = \{\tau : F \to A;\ \tau \text{ is a homomorphism of loops}\}.$$

Lemma 2.2. *The mapping* $\widehat{\ }: \mathrm{Map}_0(F,A) \to \mathrm{C}(F,A), \tau \mapsto \widehat{\tau}$ *defined by*

$$\widehat{\tau}(x,y) = \tau(xy) - \tau(x) - \tau(y)$$

is a group homomorphism with kernel $\mathrm{Hom}(F,A)$.

The image

$$\mathrm{B}(F,A) = \widehat{\mathrm{C}(F,A)} \cong \mathrm{Map}_0(F,A)/\operatorname{Hom}(F,A)$$

is a subgroup (subspace) of $\mathrm{C}(F,A)$; its elements are referred to as *coboundaries*. Coboundaries play a prominent role in classifications due to this simple observation:

Lemma 2.3. *Let $\widehat{\tau} \in \mathrm{B}(F,A)$. Then $f : Q(F,A,\theta) \to Q(F,A,\theta+\widehat{\tau})$ defined by*

$$f(x,a) = (x, a+\tau(x))$$

is an isomorphism of loops.

Thus, it is sufficient to consider cocycles modulo coboundaries, and we define the *second cohomology*

$$\mathrm{H}(F,A) = \mathrm{C}(F,A)/\operatorname{B}(F,A).$$

3. Action of autotopism groups

Following [DV09], we are going to define an action of $\mathrm{Atp}(F, A)$ on $\mathrm{C}(F, A)$ and $\mathrm{H}(F, A)$. For any cocycle θ and any autotopism $t = (\alpha, \beta, \gamma)$ of F, we would like to define something like the map

$$(x, y) \mapsto \theta(\alpha^{-1}(x), \beta^{-1}(y))$$

but this is usually not a normalized cocycle.

Instead, let N be the function defined for any $m : F \times F \to A$ by

$$N(m)(x, y) = m(x, y) - m(x, 1) - m(1, y) + m(1, 1).$$

Notice that $N(m)$ is always a cocycle, and that N restricted to $\mathrm{C}(F, A)$ is the identity map; thus, when A is a field, N is a projection from $\mathrm{Map}(F \times F, A)$ onto $\mathrm{C}(F, A)$.

Now, let

$$\mathrm{Atp}(F, A) = \mathrm{Atp}(F) \times \mathrm{Aut}(A).$$

Write for every $t = (\alpha, \beta, \gamma) \in \mathrm{Atp}(F)$ and every $h \in \mathrm{Aut}(A)$

$${}^{(t,h)}\theta = N(h\theta(\alpha^{-1}, \beta^{-1})).$$

By convention, $\theta(\alpha^{-1}, \beta^{-1})$ stands for the element of $\mathrm{Map}(F \times F, A)$ defined by $\theta(\alpha^{-1}, \beta^{-1})(x, y) = \theta(\alpha^{-1}x, \beta^{-1}y)$.

Lemma 3.1. *The group* $\mathrm{Atp}(F, A)$ *acts on* $\mathrm{C}(F, A)$ *via*

$$(t, h) \cdot \theta =^{(t,h)} \theta.$$

Proof: The proof is straightforward. Nevertheless, we would like to prove associativity here, considering the following computation to be non-trivial from the formal point of view. For all $(t_1, h_1), (t_2, h_2) \in \mathrm{Atp}(F, A)$, $\theta \in \mathrm{C}(F, A)$ and $x, y \in F$, ${}^{(t_1,h_1)}\left({}^{(t_2,h_2)}\theta\right)(x, y)$ decomposes into 16 terms. Namely, it equals after unpacking ${}^{(t_1,h_1)}\left({}^{(t_2,h_2)}\theta\right)$ into ${}^{(t_1,h_1)}\left((x, y) \mapsto \left({}^{(t_2,h_2)}\theta\right)(x, y)\right)$:

$$\begin{array}{cccc}
 & h_1h_2\theta\left(\alpha_2^{-1}\alpha_1^{-1}(x), \beta_2^{-1}\beta_1^{-1}(y)\right) & - & h_1h_2\theta\left(\alpha_2^{-1}\alpha_1^{-1}(x), \beta_2^{-1}(1)\right) \\
- & h_1h_2\theta\left(\alpha_2^{-1}(1), \beta_2^{-1}\beta_1^{-1}(y)\right) & + & h_1h_2\theta\left(\alpha_2^{-1}(1), \beta_2^{-1}(1)\right) \\
- & h_1h_2\theta\left(\alpha_2^{-1}\alpha_1^{-1}(x), \beta_2^{-1}\beta_1^{-1}(1)\right) & + & h_1h_2\theta\left(\alpha_2^{-1}\alpha_1^{-1}(x), \beta_2^{-1}(1)\right) \\
+ & h_1h_2\theta\left(\alpha_2^{-1}(1), \beta_2^{-1}\beta_1^{-1}(1)\right) & - & h_1h_2\theta\left(\alpha_2^{-1}(1), \beta_2^{-1}(1)\right) \\
- & h_1h_2\theta\left(\alpha_2^{-1}\alpha_1^{-1}(1), \beta_2^{-1}\beta_1^{-1}(y)\right) & + & h_1h_2\theta\left(\alpha_2^{-1}\alpha_1^{-1}(1), \beta_2^{-1}(1)\right) \\
+ & h_1h_2\theta\left(\alpha_2^{-1}(1), \beta_2^{-1}\beta_1^{-1}(y)\right) & - & h_1h_2\theta\left(\alpha_2^{-1}(1), \beta_2^{-1}(1)\right) \\
+ & h_1h_2\theta\left(\alpha_2^{-1}\alpha_1^{-1}(1), \beta_2^{-1}\beta_1^{-1}(1)\right) & - & h_1h_2\theta\left(\alpha_2^{-1}\alpha_1^{-1}(1), \beta_2^{-1}(1)\right) \\
- & h_1h_2\theta\left(\alpha_2^{-1}(1), \beta_2^{-1}\beta_1^{-1}(1)\right) & + & h_1h_2\theta\left(\alpha_2^{-1}(1), \beta_2^{-1}(1)\right)
\end{array}$$

which becomes after cancellation:

$$\begin{gathered}
h_1h_2\theta\left(\alpha_2^{-1}\alpha_1^{-1}(x), \beta_2^{-1}\beta_1^{-1}(y)\right) - h_1h_2\theta\left(\alpha_2^{-1}\alpha_1^{-1}(x), \beta_2^{-1}\beta_1^{-1}(1)\right) \\
-h_1h_2\theta\left(\alpha_2^{-1}\alpha_1^{-1}(1), \beta_2^{-1}\beta_1^{-1}(y)\right) + h_1h_2\theta\left(\alpha_2^{-1}\alpha_1^{-1}(1), \beta_2^{-1}\beta_1^{-1}(1)\right)
\end{gathered}$$

We recognize $\left({}^{(t_1t_2,h_1h_2)}\theta\right)(x,y)$, and we are done. It is also easy to check that ${}^{(t,h)}(\theta_1+\theta_2) = {}^{(t,h)}\theta_1 + {}^{(t,h)}\theta_2$. □

We provided this heavy computation to emphasize that, at this point, the reason why N gives rise to an action of $\mathrm{Atp}(F,A)$ on $\mathrm{B}(F,A)$ seems to lie on a lucky coincidence. N is actually far more that just a naively-defined projection, and we will see in the proof of Theorem 4.1 that it expresses well the relation between central extensions and their principal isotopes.

Moreover, it is easy to check that

$$^{(t,h)}\widehat{\tau} = \widehat{\tau'}$$

where $\tau' \in \mathrm{Map}_0$ is defined by

$$\tau'(x) = h\tau\gamma^{-1}(x) - h\tau\gamma^{-1}(1).$$

Therefore, the action of $\mathrm{Atp}(F,A)$ on $\mathrm{C}(F,A)$ induces an action on $\mathrm{B}(F,A)$ and $\mathrm{H}(F,A)$.

The following lemma asserts that any orbit for the action of $\mathrm{Atp}(F,A)$ is constituted of loops with the same isotopism type.

Lemma 3.2. *For any $t=(\alpha,\beta,\gamma)\in\mathrm{Atp}(F)$, $h\in\mathrm{Aut}(A)$, the triple $\overline{t}=(\overline{\alpha},\overline{\beta},\overline{\gamma})$ defined by*

$$\begin{cases}\overline{\alpha}(x,a) = \left(\alpha(x), ha + h\theta(x,\beta^{-1}(1))\right)\\ \overline{\beta}(y,b) = \left(\beta(y), hb + h\theta(\alpha^{-1}(1),y)\right)\\ \overline{\gamma}(z,c) = \left(\gamma(z), hc + h\theta(\alpha^{-1}(1),\beta^{-1}(1))\right)\end{cases}$$

is an isotopism from $Q(F,A,\theta)$ to $Q(F,A,{}^{(t,h)}\theta)$.

Proof: Let $\cdot_\theta$ be the multiplication in $Q(F,A,\theta)$ and $\cdot_{{}^{(t,h)}\theta}$ the multiplication in $Q(F,A,{}^{(t,h)}\theta)$. Then

$$\begin{aligned}\overline{\alpha}(x,a)\cdot_{{}^{(t,h)}\theta}\overline{\beta}(y,b) &= \left(\alpha(x), ha + h\theta(x,\beta^{-1}(1))\right)\\ &\quad \cdot_{{}^{(t,h)}\theta}\left(\beta(y), hb + h\theta(\alpha^{-1}(1),y)\right)\\ &= \left(\alpha(x)\beta(y), ha+hb+h\theta(x,\beta^{-1}(1)) + h\theta(\alpha^{-1}(1),y)\right.\\ &\quad \left.+ N(h\theta(\alpha^{-1},\beta^{-1}))(\alpha(x),\beta(y))\right)\\ &= \left(\gamma(xy), ha+hb+h\theta(x,y)+h\theta(\alpha^{-1}(1),\beta^{-1}(1))\right)\\ &= \overline{\gamma}(xy, a+b+\theta(x,y))\\ &= \overline{\gamma}((x,a)\cdot_\theta(y,b)).\end{aligned}$$

□

4. Separability

As in [DV09], we define isotopy separability in the following way:

Write $\theta \sim \mu$ if $\mu =^{(t,h)} \theta + \tau$ for some $(t,h) \in \mathrm{Atp}(F,A)$, $\tau \in \mathrm{B}(F,A)$. $\sim$ is an equivalence relation on $\mathrm{C}(F,A)$, and by Lemmas 2.3 and 3.2, if $\theta \sim \tau$, then $Q(F,A,\theta) \simeq Q(F,A,\mu)$. We say that θ is (*isotopy*) *separable* if the converse also holds, i.e. if whenever $Q(F,A,\theta) \simeq Q(F,A,\mu)$ for some cocycle μ, we also have $\theta \sim \mu$.

Theorem 4.1. *Let $\theta \in \mathrm{C}(F,A)$. Set $Q_\theta = Q(F,A,\theta)$. If $\mathrm{Aut}(Q_\theta)$ acts transitively on*

$$\{K \leq Z(Q_\theta);\ K \cong A,\ Q_\theta/K \simeq F\}$$

then θ is isotopy separable.

Proof: Let $t = (\alpha,\beta,\gamma)$ be an isotopism between Q_θ and $Q_\mu = Q(F,A,\mu)$, for some cocycle μ.

The first step of the proof is to consider the splitting of t into an isomorphism and a principal isotopism (i.e. an isotopism that has identity as its third component, see [Pfl90]).

Thus, let $(L,*)$ be the loop defined on $F \times A$ so that γ is an isomorphism from Q_θ to $(L,*)$. Then $(\overline{\alpha} = \alpha\gamma^{-1}, \overline{\beta} = \beta\gamma^{-1}, \mathrm{Id})$ is a principal isotopism between L and Q_μ.

$$\begin{tikzcd}
Q_\theta \arrow[r, "(\gamma,\gamma,\gamma)"] \arrow[d, "(\alpha,\beta,\gamma)"'] & (L,*) \arrow[dl, "(\overline{\alpha},\overline{\beta},\mathrm{Id})"] \\
Q_\mu &
\end{tikzcd}$$

We would like to understand the multiplication in L.

Let e be the neutral of the loop L. Write $(x_0,a_0) = \overline{\beta}(e)$, $(y_0,b_0) = \overline{\alpha}(e)$. $\overline{t}$ is a isotopism, thus

$$\overline{\alpha}(x,a) \cdot_\mu \overline{\beta}(y,b) = (x,a) * (y,b).$$

In particular,

$$\begin{cases} \overline{\alpha}(x,a) \cdot_\mu (x_0,a_0) = (x,a) * e = (x,a) \\ (y,b) \cdot_\mu \overline{\beta}(y,b) = (y,b) * e = (y,b) \end{cases} .$$

We can invert this system to find

$$\begin{cases} \overline{\alpha}(x,a) = (x/x_0, a - a_0 - \mu(x/x_0, x_0)) \\ \overline{\beta}(y,b) = (y_0 \backslash y, b - b_0 - \mu(y_0, y_0 \backslash y)) \end{cases} .$$

Therefore, the multiplication in L is simply

$$\begin{aligned}(x,a)*(y,b) &= \overline{\alpha}(x,a)\cdot_\mu \overline{\beta}(y,b)\\ &= \Big(x/x_0{\cdot}y_0\backslash y,\ a+b-a_0-b_0-\mu(x/x_0,x_0)-\mu(y_0,y_0\backslash y)\\ &\quad +\mu(x/x_0,y_0\backslash y)\Big).\end{aligned}$$

To put it in a more familiar form, let us write $(z_0,c_0)=e$. Now since

$$\overline{\alpha}(e)\cdot_\mu \overline{\beta}(e)=e*e=e$$

i.e.

$$(y_0,b_0)\cdot_\mu (x_0,a_0)=(y_0x_0,a_0+b_0+\mu(y_0,x_0))=(z_0,c_0)$$

we must have

$$\begin{cases} y_0x_0=z_0\\ -a_0-b_0=\mu(y_0,x_0)-c_0\end{cases}.$$

Thus the multiplication in L takes the form:

$$(x,a)*(y,b)=(x/x_0{\cdot}y_0\backslash y, a+b-c_0+\widetilde{\mu}(x,y))$$

for $\widetilde{\mu}$ defined by

$$\widetilde{\mu}(x,y)=\mu(x/x_0,y_0\backslash y)-\mu(x/x_0,y_0\backslash z_0)-\mu(z_0/x_0,y_0\backslash y)+\mu(z_0/x_0,y_0\backslash z_0).$$

The second step of the proof is now to recognize some subgroup of Q_θ on which we can apply the hypothesis.

Notice that we always have

$$(z_0,a+c_0)*(z_0,b+c_0)=(z_0,a+b+c_0).$$

Thus the map $a\mapsto(z_0,a+c_0)$ is an isomorphism from A onto

$$K_0=\{(z_0,a);a\in A\},$$

K_0 being equipped with the multiplication $*$.

Similarly, it is easy to check that $K_0\le Z(L)$. In particular, L/K_0 is a loop, and F is isotopic to it via the triple of bijections $F\to L/K_0$:

$$\begin{cases} x\mapsto (x\,x_0,0)*K_0\\ y\mapsto (y_0\,y,0)*K_0\\ z\mapsto (z,0)*K_0\end{cases}.$$

Therefore, γ^{-1} being an isomorphism between L and Q_θ, we can apply the hypothesis to $\gamma^{-1}(K_0)$; thus there exists some automorphism g of Q_θ such that

$g(1 \times A) = \gamma^{-1}(K_0)$. As a conclusion, precomposing with g if necessary, we can always assume that

$$\gamma(1 \times A) = K_0.$$

Now, what we have left to do is simply to express this fact with mappings. This is in direct analogy with [DV09].

Define a map $h : A \to A$ by

$$\gamma(1, a) = (z_0, h(a) + c_0).$$

Notice that

$$\gamma(1, a) * \gamma(1, b) = (z_0, h(a) + c_0) * (z_0, h(b) + c_0) = (z_0, h(a) + h(b) + c_0).$$

Since γ is an isomorphism between Q_θ and L, this is also

$$\gamma((1, a) \cdot_\theta (1, b)) = \gamma(1, a + b) = (z_0, h(a + b) + c_0).$$

Thus, $h \in \mathrm{Aut}(A)$.

Define also $k : F \to F$ and $\tau : F \to A$ by

$$\gamma(x, 0) = (k(x), \tau(x) + c_0).$$

We have of course $\gamma(1, 0) = e = (z_0, c_0)$, so $k(1) = z_0$ and $\tau(1) = 0$; in particular $\tau \in \mathrm{Map}_0(F, A)$.

Moreover, computing in two ways $\gamma(xy, 0) = \gamma(x, 0) * \gamma(y, 0)$ yields the following identity for k:

$$k(x)/x_0.y_0\backslash k(y) = k(xy).$$

We can now express γ in term of these maps:

$$\begin{aligned}\gamma(z, c) = \gamma((z, 0) \cdot_\theta (1, c)) &= (k(z), \tau(z) + c_0) * (z_0, hz + c_0)\\ &= (k(z), hz + \tau(z) + c_0).\end{aligned}$$

Recall that we also know the expression of $\overline{\alpha} = \alpha\gamma^{-1}$ and $\overline{\beta} = \beta\gamma^{-1}$, so by composition with γ, we get:

$$\begin{cases}\alpha(x, a) = (k(x)/x_0, hx + \tau(x) + c_0 - a_0 - \mu(k(x)/x_0, x_0))\\ \beta(y, b) = (y_0\backslash k(y), hy + \tau(y) + c_0 - b_0 - \mu(y_0, y_0\backslash k(y)))\end{cases}.$$

After writing explicitly that $\alpha(x, a) \cdot_\mu \beta(y, b)$ is always equal to $\gamma((x, a) \cdot_\theta (y, b))$, we get

$$h\theta + \widehat{\tau} = N(\mu(\widetilde{\alpha}, \widetilde{\beta}))$$

where $\widetilde{t} = (\widetilde{\alpha}, \widetilde{\beta}, \widetilde{\gamma})$ is defined to be the triple

$$\begin{cases} \widetilde{\alpha}(x) = k(x)/x_0 \\ \widetilde{\beta}(y) = y_0 \backslash k(y) \\ \widetilde{\gamma}(z) = k(z) \end{cases} .$$

Now $\widetilde{t} \in \mathrm{Atp}(F)$, $h \in \mathrm{Aut}(A)$ and $\tau \in \mathrm{Map}_0(F, A)$, so $\theta \sim \mu$.
Thus θ is separable. □

We leave to the reader to check that the following results, proved in [DV09, 3.3–3.7], still hold in our setting, thanks to Theorem 4.1 (we recall that if a loop is isotopic to a group, then it is isomorphic to it, see [Pfl90]).

Proposition 4.2. *If $Q(F, A, \theta)$ is an abelian group, and $A = \mathbb{Z}_p$ for p a prime integer, then θ is isotopy separable.*

Lemma 4.3. *Let $Q = Q_\theta$, $A = \mathbb{Z}_p$, p a prime. Assume further that one of the following conditions is satisfied:*

(i) $|Q| = p$,
(ii) $|Q| = pq$, *where q is a prime,*
(iii) $[Q : Z(Q)] \leq 2$,
(iv) $|Q| < 12$.

Then θ is isotopy separable.

5. The invariant subspaces

Following [DV09], define for $(t, h) \in \mathrm{Atp}(F, A)$:

$$\mathrm{Inv}(t, h) = \{\theta \in \mathrm{C}(F, A);\ \theta -^{(t,h)} \theta \in \mathrm{B}(F, A)\}$$

and for $\emptyset \neq H \subset \mathrm{Atp}(F, A)$:

$$\mathrm{Inv}(H) = \bigcap_{(t,h) \in H} \mathrm{Inv}(t, h).$$

We state the following, the proof of which is exactly the same as in [DV09]:

Lemma 5.1. *Let $\emptyset \neq H \subset \mathrm{Atp}(F, A)$. Then*

$$\mathrm{Inv}(H) = \mathrm{Inv}(\langle H \rangle).$$

Corollary 5.2. *Let $H, K \leq \mathrm{Atp}(F, A)$. Then*

$$\mathrm{Inv}(H) \cap \mathrm{Inv}(K) = \mathrm{Inv}(\langle H \cup K \rangle).$$

For $t, u \in \mathrm{Atp}(F)$ and $h, k \in \mathrm{Aut}(A)$, let ${}^u t = utu^{-1}$, ${}^k h = khk^{-1}$.

Lemma 5.3. *Let (t, h), $(u, k) \in \mathrm{Atp}(F, A)$. Then*

$$\theta \in \mathrm{Inv}(t, h) \text{ \textit{if and only if} } {}^{(u,k)}\theta \in \mathrm{Inv}({}^u t, {}^k h).$$

For $H \leq \mathrm{Atp}(F, A)$, let

$$\begin{aligned} \mathrm{Inv}^*(H) &= \{\theta \in \mathrm{C}(F, A);\ \theta \in \mathrm{Inv}(t, h) \text{ if and only if } (t, h) \in H\}, \\ \mathrm{Inv}^*_c(H) &= \bigcup_{(t,h)\in\mathrm{Atp}(F,A)} \mathrm{Inv}^*({}^{(t,h)}H). \end{aligned}$$

If G is a group and $H \leq G$, let $N_G(H) = \{a \in G;\ {}^aH = H\}$ be the normalizer of H in G.

Lemma 5.4. *Let $H \leq G = \mathrm{Atp}(F, A)$. Then*

$$|\mathrm{Inv}^*_c(H)| = |\mathrm{Inv}^*(H)| \cdot [G : N_G(H)].$$

For a group G, denote by $\mathrm{Sub}_c(G)$ a set of subgroups of G such that for every $H \leq G$ there is precisely one $K \in \mathrm{Sub}_c(G)$ such that K is conjugate to H.

Theorem 5.5. *Let F be a loop and A an abelian group. Assume that θ is separable for every $\theta \in \mathrm{C}(F, A)$. Let $G = \mathrm{Atp}(F, A)$. Then there are*

$$\sum_{H\in\mathrm{Sub}_c(G)} \frac{|\mathrm{Inv}^*_c(H)|}{|\mathrm{B}(F, A)| \cdot [G : H]} = \sum_{H\in\mathrm{Sub}_c(G)} \frac{|\mathrm{Inv}^*(H)|}{|\mathrm{B}(F, A)| \cdot [N_G(H) : H]}$$

central extensions of A by F, up to isotopism.

6. Nilpotent loops of order $2q$, q prime

We now investigate the $2q$ order case, with q an odd prime integer throughout. The discussion in [DV09] showing that we can suppose $A = \mathbb{Z}_2$, $F = \mathbb{Z}_q$ and that each cocycle is admissible is still valid; we can therefore use fully Theorem 5.5 in the computation of the number of nilpotent loops of order $2q$. In order to do so, the first step is to understand the structure of $\mathrm{Atp}(F)$.

6.1 Subgroup structure of $\mathrm{Atp}(\mathbb{Z}_q)$. We recall the following proposition from [Cla12].

Proposition 6.1. *Let G be a finite abelian group. Then*

$$\begin{aligned} \phi : \mathrm{Aut}(G) \ltimes G^2 &\to \mathrm{Atp}(G) \\ (h, x_0, y_0) &\mapsto t_{h,x_0,y_0} \end{aligned}$$

is an isomorphism, where the multiplication on $\mathrm{Aut}(G) \ltimes G^2$ is given by

$$(h, X)(h', X') = (hh', hX' + X)$$

and where the autotopisms t_{h,x_0,y_0} are defined by

$$\begin{cases} x \mapsto hx + x_0 \\ y \mapsto hy + y_0 \\ z \mapsto hz + x_0 + y_0 \end{cases} .$$

Let us introduce some notation. For m a generator of $F \setminus \{0\} \cong \mathbb{Z}_{q-1}$, d a divisor of $q-1$, $X \in F^2$ and $y \in F$, define

$$\begin{cases} H_d^X = \langle (m^d, X) \rangle = \{(m^{kd}, \frac{1-m^{kd}}{1-m^d} X);\ k \in \mathbb{Z}\} \\ K_y = \langle (1,(1,y)) \rangle = \{(1,(k,ky));\ k \in \mathbb{Z}\} \\ \widetilde{K} = \langle (1,(0,1)) \rangle = \{(1,(0,k));\ k \in \mathbb{Z}\} \end{cases} .$$

Since by [Cla12] for a fixed d all H_d^X are conjugate (see Table 1), we simply write H_d instead of $H_d^{(0,0)}$. Note that this notation is consistent with the one in [DV09].

Here are now all subgroups of $\mathrm{Atp}(F)$, up to conjugacy

subgroup H	normalizer $N_G(H)$	conjugates	$[N_G(H) : H]$
$\{1\}$	$\mathrm{Atp}(F)$	only itself	$q^2(q-1)$
H_d, $d \neq q-1$	$\mathrm{Aut}(F)$	every H_d^X	d
K_y or $\widetilde{K}$	$\mathrm{Atp}(F)$	only itself	$q(q-1)$
$H_d \cdot K_y$, $d \neq q-1$	$\mathrm{Aut}(F) \cdot K_y$	every $H_d^X \cdot K_y$	d
$H_d \cdot \widetilde{K}$, $d \neq q-1$	$\mathrm{Aut}(F) \cdot \widetilde{K}$	every $H_d^X \cdot \widetilde{K}$	d
$H_d \ltimes F^2$	$\mathrm{Atp}(F)$	only itself	d

Table 1. Representatives for conjugacy classes of $F = \mathrm{Atp}(\mathbb{Z}_q)$ and their normalizer.

Proof: See [Cla12, Example 3.4]. □

6.2 $\dim(\mathrm{Inv}(H))$, $H \leq \mathrm{Atp}(\mathbb{Z}_q)$. In the next proposition, we compute the dimensions of the invariant spaces of the subgroups of $\mathrm{Atp}(F)$, with as before $A = \mathbb{Z}_2$, $F = \mathbb{Z}_q$ and q an odd prime (see Subsection 6.1 for notations).

Proposition 6.2. *The dimensions of the invariant spaces of the subgroups of* $\mathrm{Atp}(F)$ *are indicated in Table* 2 *below, where d is any divisor of* $q-1$.

subgroup H	H_d	$H_d \cdot K_y$, $y \notin \{0,-1\}$	*other*
$\dim(\mathrm{Inv}(H)/\,\mathrm{B}(F,A))$	$(q-2)d$	d	*0*

Table 2. Representatives for conjugacy classes of $F = \mathrm{Atp}(\mathbb{Z}_q)$ and dimension of their invariant subspaces.

Proof: The proof will take us the entire subsection, and will be divided in lemmas and corollaries as much as possible.

Note that since the action of $\mathrm{Atp}(F,A)$ we defined on $\mathrm{C}(F,A)$ coincides (by restriction) with the action of $\mathrm{Aut}(F,A)$ defined in [DV09], the first column of Table 2 directly follows from [DV09]. Thus, let us start with the case $H = K_y$.

For every $y_0 \in F$, define on $\mathrm{C}(F,A)$ the operator S (depending on y_0) by:

$$\begin{aligned} S : \mathrm{C}(F,A) &\to \mathrm{C}(F,A) \\ \theta &\mapsto^{(1,t_{1,1,y_0})} \theta - \theta \end{aligned}$$

using the notation of Proposition 6.1; otherwise put, S is defined for every $\theta \in \mathrm{C}(F,A)$ by

$$S\theta(x,y) = \theta(x+1,y+y_0) - \theta(x+1,y_0) - \theta(1,y+y_0) + \theta(1,y_0) - \theta(x,y).$$

Similarly, define on the space $\mathrm{Map}(F \times F, A)$ of non-normalized cocycles the operator $\widetilde{S}$ by:

$$\begin{aligned} \widetilde{S} : \mathrm{Map}(F \times F, A) &\to \mathrm{Map}(F \times F, A) \\ \mu &\mapsto \mu(\cdot+1,\cdot+y_0) - \mu \end{aligned}$$

i.e. for every $\mu \in \mathrm{Map}(F \times F, A)$:

$$\widetilde{S}\mu(x,y) = \mu(x+1,y+y_0) - \mu(x,y).$$

Like in [DV09], since $\mathrm{Inv}(K_{y_0}) = S^{-1}(\mathrm{B}(F,A))$, we are interested in computing the kernel $\operatorname{Ker} S$ first. In analogy with [DV09], we are going to prove that it is spanned by these cocycles Λ_i that take the value 1 on exactly one orbit of the action on F^2 by the translation $(x,y) \mapsto (x+1,y+y_0)$; or rather by their *image* $N(\Lambda_i)$ under N (this is the content of Corollary 6.5).

Namely, for $0 \le i \le q-1$, define $\Lambda_i \in \mathrm{Map}(F \times F, A)$ by

$$\Lambda_i(k,ly_0) = \delta_{l-k,i} = \begin{cases} 1 \text{ if } l-k=i \mod q \\ 0 \text{ otherwise} \end{cases}.$$

Note that these span $\operatorname{Ker} \widetilde{S}$. Also,

$$\operatorname{Ker} S = N(\operatorname{Ker} \widetilde{S} + V)$$

where V is some vector space spanned by particular solutions to the systems

$$\widetilde{S}\mu = \nu$$

for every ν in a chosen basis of $\operatorname{Ker} N$.

Lemma 6.3. *For any $y_0 \in F$, we can choose V so that $V \subset \operatorname{Ker} N$.*

Proof: We have to separate two cases.

Suppose first that $y_0 \neq 0$. For $0 \le i,j \le q-1$, define L_i, C_j by

$$\begin{cases} L_i(x,y) = \delta_{x,i} \\ C_j(x,y) = \delta_{y,j} \end{cases}.$$

Note that these elements of $\mathrm{Map}(F\times F, A)$ are in $\operatorname{Ker} N$; write $1=\sum_i L_i=\sum_j C_j$ for the constant map equalling 1 everywhere. Now, $\operatorname{Ker} N$ is easily seen to have dimension $2q-1$, with basis for instance

$$\{1, L_1, \dots, L_{q-1}, C_1, \dots, C_{q-1}\}$$

or, better,

$$\{1, L_0-L_1, \dots, L_{q-2}-L_{q-1}, C_0-C_{y_0}, \dots, C_{(q-2)y_0}-C_{(q-1)y_0}\}.$$

Therefore, we can choose L_{i+1} (resp. $C_{(j+1)y_0}$), with $0\le i,j\le q-2$ as solutions to

$$\widetilde{S}\mu = L_i - L_{i+1} \text{ (resp. } C_{jy_0}-C_{(j+1)y_0})$$

and V has dimension at least $2(q-1)$. Let us show that it cannot be more, by showing that the constant map 1 does not have any solution in $\mathrm{Map}(F\times F, A)$.

Indeed, if it were the case, an easy induction for such a solution μ would imply that for every integer $k\ge 1$

$$\mu(k, ky_0)=\mu(0,0)+k.$$

In particular for $k=q$,

$$\mu(0,0)=\mu(q,qy_0)=\mu(0,0)+q=\mu(0,0)+1.$$

This is absurd, so V has dimension $2(q-1)$, and can be chosen to be included in $\operatorname{Ker} N$.

Now, assume $y_0=0$. This case is similar, but here no C_j for $0\le j\le q-1$ has a solution in $\mathrm{Map}(F\times F, A)$. Indeed, were it the case,

$$\mu(k,j)=\mu(0,j)+k$$

would hold for every integer $k\ge 1$; taking $k=q$, we would have $\mu(q,j)=\mu(0,j)+1$, absurd. Thus we can choose $V=\mathrm{Span}_{1\le i\le q-1}(L_i)$, and we are done. □

Lemma 6.4. *For any* $y_0\ne 0$, $\operatorname{Ker}\widetilde{S}\cap\operatorname{Ker} N=\mathrm{Span}(1)$.

Proof: Suppose we have some $\mu\in\operatorname{Ker}\widetilde{S}\cap\operatorname{Ker} N$. Then for every integers $k,l\ge 1$, we have

$$\mu(k+1,(l+1)y_0)=\mu(k+1,0)+\mu(0,(l+1)y_0)-\mu(0,0).$$

But this is also

$$\mu(k,ly_0)=\mu(k,0)+\mu(0,ly_0)-\mu(0,0).$$

Thus $\mu(k+1,0)-\mu(k,0)$ does not depend on k, i.e.

$$\mu(k+1,0)=\mu(k,0)+c$$

for some constant $c \in A$. Then by a quick induction

$$\mu(0,0) = \mu(q,0) = \mu(0,0) + qc = \mu(0,0) + c$$

so $c = 0$. Therefore $\mu(k+1,0) = \mu(k,0)$ for all k.

Similarly, $\mu(0,(l+1)y_0) = \mu(0,ly_0)$ for all l. But then μ must be constant, and we are done. □

Corollary 6.5. *If* $y_0 = 0$, *then* $\operatorname{Ker} S = 0$. *Else,* $\operatorname{Ker} S$ *has dimension* $q-1$ *and basis* $\{N\Lambda_i\}_{1\leq i\leq q-1}$.

Proof: This is a direct corollary of Lemmas 6.3 and 6.4. □

The last step is now to compute the intersection $\operatorname{Ker} S \cap B$.

Lemma 6.6. *If* $y_0 = -1$ *then* $\operatorname{Ker} S \subset B$. *Else,* $\operatorname{Ker} S \cap B = 0$.

Proof: In this proof, we use $A = \mathbb{Z}_2$ without warning. For convenience, we also define $z_0 = y_0 + 1$.

First, if $y_0 = -1$, every Λ_i is in B. Thus, let us suppose y_0 is neither 0 nor -1, and take some

$$\widehat{\tau} = \sum_{c\neq 0} \lambda_c \widehat{\tau_c}$$

that verifies $S\widehat{\tau} = 0$, where as in [DV09] we define every τ_c by

$$\tau_c(x) = \delta_{x,c}$$

Since

$$S\widehat{\tau_c} = \begin{cases} \widehat{\tau_{c-z_0}} + \widehat{\tau_c} \text{ if } c \neq z_0 \\ \sum_{c'\neq 0,\, c'\neq z_0} \widehat{\tau_c'} \text{ otherwise} \end{cases}$$

we have

$$\begin{aligned} S\widehat{\tau} &= \sum_{c\neq 0,\, c\neq z_0} \lambda_c(\widehat{\tau_{c-z_0}} + \widehat{\tau_c}) \;+\; \lambda_{z_0} \cdot \sum_{c\neq 0,\, c\neq z_0} \widehat{\tau_c} \\ &= \sum_{c\neq 0,\, c\neq z_0,\, c\neq -z_0} (\lambda_{c+z_0} + \lambda_c + \lambda_{z_0})\widehat{\tau_c} \\ &\quad + \lambda_{2z_0}\widehat{\tau_{z_0}} + (\lambda_{z_0} + \lambda_{-z_0})\widehat{\tau_{-z_0}}. \end{aligned}$$

Because the τ_c for $c \neq 0$ form a basis of $\mathrm{B}(F,A)$, we must conclude that

$$\begin{aligned} \lambda_{2z_0} &= 0 = 2\lambda_{z_0} \\ \lambda_{3z_0} &= \lambda_{2z_0} + \lambda_{z_0} = 3\lambda_{z_0} \\ &\;\;\cdots \\ \lambda_{(q-1)z_0} &= (q-1)\lambda_{z_0} = 0 \\ \lambda_{-z_0} &= \lambda_{z_0}. \end{aligned}$$

Thus $\lambda_{z_0} = 0$, so $\lambda_{kz_0} = 0$ for every k, hence $\widehat{\tau} = 0$. □

As a quick corollary, we are done for the second column of Table 2, in the case $d = q - 1$:

Corollary 6.7. $\dim(\mathrm{Inv}(K_y)/\,\mathrm{B}(F,A)) = q-1$ *whenever* $y \notin \{0,-1\}$. *Moreover, the invariant spaces of* K_0, K_{-1} *and* $\widetilde{K}$ *are null mod* $\mathrm{B}(F,A)$.

Proof: The only case that was not already investigated is $H = \widetilde{K}$, but this is symmetric to the case $H = K_0$. □

Note that any subgroup H in the third column of Table 2 has either K_0, K_{-1} or $\widetilde{K}$ as a subgroup. Thus, its invariant space is also null mod $\mathrm{B}(F,A)$.

The only remaining cases in Proposition 6.2 are $H = H_d \cdot K_y$, for $y \notin \{0,-1\}$ and $d \neq q-1$. Start with a cocycle $\theta \in \mathrm{Span}_{1\le i\le q-1}(N\Lambda_i) \oplus \mathrm{B}(F,A)$

$$\theta = \sum_{i\neq 0} \lambda_i N\Lambda_i \,+\, \tau.$$

Then ${}^{(h,(0,0))}\theta - \theta \in \mathrm{B}(F,A)$ if and only if

$$\sum_{i\neq 0} \lambda_i (N\Lambda_{hi} - N\Lambda_i) \in \mathrm{B}(F,A)$$

but since the Λ_i are linearly independent over $\operatorname{Ker} N$, this is equivalent to

$$\sum_{i\neq 0} \lambda_i (\Lambda_{hi} - \Lambda_i) = 0$$

i.e.

$$\sum_{i\neq 0} \Lambda_i (\lambda_{h^{-1}i} - \lambda_i) = 0$$

i.e. $\lambda_i = \lambda_{hi}$ for all i. Thus for any $y \notin \{0,-1\}$,

$$\dim\Big(\mathrm{Inv}\left(\{(h,(0,0))\} \cup K_y\right)/\,\mathrm{B}(F,A)\Big) = \frac{q-1}{|h|}$$

and all the cases in Proposition 6.2 are covered. □

6.3 $|\,\mathrm{Inv}^*(H)|$, $H \le \mathrm{Atp}(\mathbb{Z}_q)$ and $\widetilde{\mathcal{N}}(2q)$.

Before computing the number of nilpotent loops of order $2q$ up to isotopism, we still have to compute the cardinalities of the starred invariant spaces for the subgroups of $\mathrm{Atp}(F,A)$. This is the content of Proposition 6.8.

Proposition 6.8. *The cardinalities of the starred invariant spaces for the subgroups of* $\mathrm{Atp}(F,A)$ *are provided in Table* 3 *below, where as in* [DV09], *we define for every integer d:*

$$\mathrm{Pred}(d) = \{d';\ 1 \le d' < d,\ d/d' \textit{ is a prime}\}.$$

subgroup H	*cardinality* $\lvert \mathrm{Inv}^*(H)\rvert$
$\{1\}$	$2^{(q-2)(q-1)} + q^2 \cdot \sum_{D \subset \mathrm{Pred}(q-1)} (-1)^{\lvert D\rvert} 2^{(q-2)\gcd(D)}$ $-(q-2)\Big(2^{q-1} + q^2 \cdot \sum_{D \subset \mathrm{Pred}(q-1)} (-1)^{\lvert D\rvert} 2^{\gcd(D)}\Big)$ $-(q-3)(q-1)(q+1)$
H_d, $d \notin \{1, q-1\}$	$2^{(q-2)d} + \sum_{D \subset \mathrm{Pred}(d)} (-1)^{\lvert D\rvert} 2^{(q-2)\gcd(D)}$ $-(q-2)\Big(2^d + \sum_{D \subset \mathrm{Pred}(d)} (-1)^{\lvert D\rvert} 2^{\gcd(D)}\Big)$
H_1	$2^{q-2} - (q-1)$
K_y, $y \notin \{0, -1\}$	$2^{q-1} + q \cdot \sum_{D \subset \mathrm{Pred}(q-1)} (-1)^{\lvert D\rvert} 2^{\gcd(D)} + q - 1$
$H_d \cdot K_y, d \notin \{1, q-1\}$ $y \notin \{0, -1\}$	$2^d + \sum_{D \subset \mathrm{Pred}(d)} (-1)^{\lvert D\rvert} 2^{\gcd(D)}$
$H_1 \cdot K_y$, $y \notin \{0, -1\}$	1
$\mathrm{Atp}(F, A)$	*1*
other	*0*

Table 3. Representatives for conjugacy classes of $F = \mathrm{Atp}(\mathbb{Z}_q)$ and their starred invariant spaces.

Proof: The proof is straightforward, using the following expression, together with Proposition 6.2 and a standard inclusion/exclusion argument.

$$\begin{aligned} \mathrm{Inv}^*(H) &= \mathrm{Inv}(H) \setminus \bigcup_K \mathrm{Inv}(K) \\ &= (\mathrm{Inv}(H) \setminus \{0\}) \setminus (\bigcup_K \mathrm{Inv}(K) \setminus \{0\}) \end{aligned}$$

where the union is taken for subgroups K such that H is a maximal subgroup of K; Table 4 below provides for each subgroup H the subgroups K in which H is maximal.

Details are left to the reader. □

For convenience, let us write $\widetilde{\mathcal{N}}(n)$ for the number of nilpotent loops of order n counted up to isotopism, and $\mathcal{N}(n)$ the number of nilpotent loops of order n counted up to isomorphism. This notation is consistent with the one in [DV09], and we recall the following:

subgroup H	subgroups K in which H is maximal
$\{1\}$	every H_d^X for $d \in \mathrm{Pred}(q-1)$, any X every K_y for $y \in \{1,\dots,q-2\}$
H_d, $d \neq q-1$	every $H_{d'}$ for $d' \in \mathrm{Pred}(d)$, every $H_d \cdot K_y$ for $y \in \{1,\dots,q-2\}$
K_y, $y \in \{1,\dots,q-2\}$	every $H_d^X \cdot K_y$ for $d \in \mathrm{Pred}(q-1)$ and $X \in \{(0,0),\dots(q-1,0)\}$
$H_d \cdot K_y$, $y \in \{1,\dots,q-2\}$	every $H_{d'} \cdot K_y$ for $d' \in \mathrm{Pred}(d)$ and $y \in \{1,\dots,q-2\}$

Table 4. Representatives for conjugacy classes of $F = \mathrm{Atp}(\mathbb{Z}_q)$ and the non-null invariant-space subgroups in which they are maximal.

Theorem 6.9. *Let q be an odd prime. Then the number $\mathcal{N}(2q)$ of nilpotent loops of order $2q$ counted up to isomorphism is*

$$\mathcal{N}(2q) = \sum_{d \text{ divides } q-1} \frac{1}{d}\left(2^{(q-2)d} + \sum_{D \subset \mathrm{Pred}(d)} (-1)^{|D|} 2^{(q-2)\gcd(D)}\right).$$

Proof: See [DV09, Theorem 7.1]. □

We have now all ingredients in hand for Theorem 6.10.

Theorem 6.10. *Let q be an odd prime. Then the number $\widetilde{\mathcal{N}}(2q)$ of nilpotent loops of order $2q$ counted up to isotopism is*

$$\begin{aligned}\widetilde{\mathcal{N}}(2q) = {} & \frac{2^{(q-2)(q-1)}}{q^2(q-1)} + \frac{1}{q-1} \sum_{D \subset \mathrm{Pred}(q-1)} (-1)^{|D|} 2^{(q-2)\gcd(D)} \\ & + \sum_{d \text{ strictly divides } q-1} \frac{1}{d}\left(2^{(q-2)d} + \sum_{D \subset \mathrm{Pred}(d)} (-1)^{|D|} 2^{(q-2)\gcd(D)}\right) \\ & + \frac{1}{q^2}\Big((q-2)2^{q-1} + 3)\Big) \\ = {} & \mathcal{N}(2q) + \frac{1}{q^2}\big(-(q+1)2^{(q-2)(q-1)} + (q-2)2^{q-1} + 3\big).\end{aligned}$$

Proof: Combine Theorem 5.5 and Proposition 6.8. □

Recall from [DV09] the following theorem.

Theorem 6.11. *Let q be an odd prime. Then the number of nilpotent loops of order $2q$ counted up to isomorphism is approximately $2^{(q-2)(q-1)}/(q-1)$. More* *precisely,*

$$\lim_{q \text{ prime},\, q\to\infty} \mathcal{N}(2q) \cdot \frac{q-1}{2^{(q-2)(q-1)}} = 1.$$

Proof: See [DV09, Theorem 7.3]. □

We can now compare the estimates for $\mathcal{N}(2q)$ and $\widetilde{\mathcal{N}}(2q)$, this is the purpose of the following corollary.

Corollary 6.12. *Let q be an odd prime. Then the number of nilpotent loops of order $2q$ counted up to isotopism is approximately $2^{(q-2)(q-1)}/q^2(q-1)$. Thus, the ratio between the number of such loops counted up to isomorphism and up to isotopism is approximately q^2. More precisely,*

$$\lim_{q \text{ prime},\, q\to\infty} \widetilde{\mathcal{N}}(2q) \cdot \frac{q^2(q-1)}{2^{(q-2)(q-1)}} = 1,$$
$$\lim_{q \text{ prime},\, q\to\infty} \frac{\mathcal{N}(2q)}{q^2 \cdot \widetilde{\mathcal{N}}(2q)} = 1.$$

Proof: This is immediate from Theorems 6.10 and 6.11. □

Table 5 below provides $\widetilde{\mathcal{N}}(2q)$ for any odd prime $q \le 17$. Like in [DV09], it is not a problem to compute $\widetilde{\mathcal{N}}(2q)$ for bigger primes, but this would not fit nicely in a table.

q	$\widetilde{\mathcal{N}}(2q)$
3	2
5	63
7	3,658,003
11	1,023,090,941,561,683,953,759,579
13	2,684,673,506,279,593,406,254,437,209,960,379,083
17	382,103,603,974,564,085,117,495,134,243,710,834,769,544,696,954,218,618,882,023,686,506,659

Table 5. Number $\widetilde{\mathcal{N}}(2q)$ of nilpotent loops of order $2q$ up to isotopism, for odd primes $q \le 17$.

7. Conclusion

We invite the reader desiring to know about related works and topics to check Section 10 in [DV09].

Note that in the present paper we did not compute the number of nilpotent loops of small order (say less that 24) up to isotopy. Undertaking such counting appears of interest to us. Possible trouble could be the isotopy non-invariance of the set of large center cocycles (see Section 8 in [DV09]), since isotopy does not preserve centers.

Also of interest is the enumeration of nilpotent loops of small order in Bol-Moufang varieties (see [PV05]) up to isomorphy, and up to isotopy (here also, isotopy invariance should be a concern).

The computation of Table 5 was undertaken using the GAP System for Computational Discrete Algebra (see http://www.gap-system.org/). This paper comes with the code used for Table 5 and a file containing the numbers $\widetilde{\mathcal{N}}(2q)$ of nilpotent loops of order $2q$ for every odd prime q less than 100. The two files can be downloaded at http://www.math.cornell.edu/~lpc49/.

Acknowledgment. We would like to take this opportunity to give our warmest thanks to Petr Vojtěchovský and Dan Daly for their continued interest and helpful comments concerning the present work.

References

[Cla12] Clavier L., *About the autotopisms of abelian groups*, 2012, `http://arxiv.org/abs/1201.5655`.

[DV09] Daly D., Vojtěchovský P., *Enumeration of nilpotent loops via cohomology*, J. Algebra **322** (2009), no. 11, 4080–4098.

[Pfl90] Pflugfelder H.O., *Quasigroups and Loops: Introduction*, Heldermann, Berlin, 1990.

[PV05] Phillips J.D., Vojtěchovský P., *The varieties of loops of Bol-Moufang type*, Algebra Universalis **54** (2005), no. 3, 259–271.

Cornell University, 120 Malott Hall, Ithaca, NY 14853, USA

(*Received* February 16, 2012, *revised* April 10, 2012)