Designs, Codes and Cryptography (2024) 92:681–694
https://doi.org/10.1007/s10623-023-01262-0

Counting the number of non-isotopic Taniguchi semifields

Faruk Göloğlu[1] · **Lukas Kölsch**[2]

Received: 28 July 2022 / Revised: 17 February 2023 / Accepted: 5 June 2023 /
Published online: 2 July 2023

Abstract
We investigate the isotopy question for Taniguchi semifields. We give a complete characterization when two Taniguchi semifields are isotopic. We further give precise upper and lower bounds for the total number of non-isotopic Taniguchi semifields, proving that there are around p^{m+s} non-isotopic Taniguchi semifields of order p^{2m} where s is the largest divisor of m with $2s \neq m$. This result proves that the family of Taniguchi semifields is (asymptotically) the largest known family of semifields of odd order. The key ingredient of the proofs is a technique to determine isotopy that uses group theory to exploit the existence of certain large subgroups of the autotopism group of a semifield.

Keywords Semifields · Isotopy · Projective planes

Mathematics Subject Classification Primary 12K10 · 17A35 · Secondary 51A35 · 51A40

1 Introduction

A finite **semifield** $\mathbb{S} = (S, +, \circ)$ is a finite set S equipped with two operations $(+, \circ)$ satisfying the following axioms.

(S1) $(S, +)$ is a group.
(S2) For all $x, y, z \in S$,

- $x \circ (y + z) = x \circ y + x \circ z$,
- $(x + y) \circ z = x \circ z + y \circ z$.

This is one of several papers published in *Designs, Codes and Cryptography* comprising the "Special Issue: Coding and Cryptography 2022".

✉ Lukas Kölsch
lukas.koelsch.math@gmail.com

Faruk Göloğlu
farukgologlu@gmail.com

[1] Department of Mathematics, Faculty of Mathematics and Physics, Charles University, Sokolovská 83, 186 75 Praha 8, Czech Republic

[2] University of South Florida, Tampa, USA

(S3) For all $x, y \in S$, $x \circ y = 0$ implies $x = 0$ or $y = 0$.
(S4) There exists $\epsilon \in S$ such that $x \circ \epsilon = x = \epsilon \circ x$.

An algebraic object satisfying the first three of the above axioms is called a **pre-semifield**.

If $\mathbb{P} = (P, +, \circ)$ is a pre-semifield, then $(P, +)$ is an elementary abelian p-group [15, p. 185], and $(P, +)$ can be viewed as an n-dimensional $\mathbb{F}_p$-vector space $\mathbb{F}_p^n$. A pre-semifield $\mathbb{P} = (\mathbb{F}_p^n, +, \circ)$ can be converted to a semifield $\mathbb{S} = (\mathbb{F}_p^n, +, *)$ using *Kaplansky's trick* (see e.g. [16, Section 1.1]).

Two pre-semifields $\mathbb{P}_1 = (\mathbb{F}_p^n, +, \circ_1)$ and $\mathbb{P}_2 = (\mathbb{F}_p^n, +, \circ_2)$ are said to be **isotopic** if there exist $\mathbb{F}_p$-linear bijections L, M and N of $\mathbb{F}_p^n$ satisfying

$$N(x \circ_1 y) = L(x) \circ_2 M(y).$$

Such a triple $\gamma = (N, L, M)$ is called an **isotopism** between $\mathbb{P}_1$ and $\mathbb{P}_2$. Isotopisms between a pre-semifield $\mathbb{P}$ and itself are called **autotopisms**. Isotopy of pre-semifields is an equivalence relation and the pre-semifield $\mathbb{P}$ and the corresponding semifield $\mathbb{S}$ constructed by Kaplansky's trick are always isotopic.

Research on semifields started more than 100 years ago with the work of Dickson [5]. Over time, they received much attention due to their connections to several different areas. Firstly, every semifield coordinatizes a projective plane and different semifields coordinatize isomorphic planes if and only if they are isotopic ([1], see [15, Section 3] for a detailed treatment). More recently, semifields have been the center of much attention since they are equivalent to Maximum Rank Distance codes with certain parameters (see e.g. [20]) and can be used to construct other combinatorial structures like relative difference sets (see [18]).

Deciding whether given (pre-)semifields are isotopic or not is generally a very difficult question, and finding effective ways to prove non-isotopy of semifields is considered a major open question (see e.g. [12, p. 936]). Most results on the isotopy of semifields are based on isotopy invariants like the nuclei, however it is well known that potentially many non-isotopic semifields can have the same nuclei, and having more precise tools is desirable. In [6], the authors developed a technique to settle the isotopy question for a specific family of commutative semifields. In this work, we will focus on the (non-commutative) Taniguchi semifields introduced in [22] by extending the methods introduced in [6].

Note that many constructions of semifields also yield corresponding constructions of almost perfect nonlinear (APN) functions which play a big role in the design of block ciphers for cryptography. This is also the case with the Taniguchi semifields. However, the construction used by Taniguchi for the semifields, by design, are more complicated than that for the Taniguchi APN functions. The equivalence question for the Taniguchi APN functions was recently solved in [13, 14] using a more elementary, but a very technical approach compared to the techniques we use. A variant of the approach we introduce here yields a much shorter proof for the equivalence problem for the Taniguchi APN functions. It seems that the isotopy question of the Taniguchi semifields is more complex than the equivalence question for the Taniguchi APN functions.

In Sect. 2, we give the basic definitions that are important for our problem and give some simple general results. In Sect. 3, we introduce the group theoretic techniques that are key to later sections. In Sect. 4, we investigate when two Taniguchi pre-semifields are isotopic. A complete characterization is given in Theorem 3. Section 5 deals with giving a count of non-isotopic Taniguchi pre-semifields, with precise bounds given in Theorem 5. The last section compares these results to similar results for other semifields, in particular to semifields constructed via skew-polynomial rings (or cyclic semifields).

2 The setup

The Taniguchi pre-semifields are defined in [22] on $\mathbb{F}_{p^n} \cong \mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$ with $n = 2m$ via the pre-semifield multiplication

$$(x, y) * (u, v) = ((x^q u + \alpha x u^q)^{q^2} - a(x^q v - \alpha u^q y)^q - b(y^q v + \alpha y v^q), xv + yu),$$

where

- $q = p^k$ for some $1 \leq k \leq m-1$,
- $-\alpha$ is not a $(q-1)$-st power, and
- the projective polynomial $P_{q,a,b}(x) = x^{q+1} + ax + b$ has no roots in $\mathbb{F}_{p^m}$.

In this paper, we will instead use a different, isotopic representation of the Taniguchi pre-semifield. This representation arises after taking x, u to the $\overline{q}^2$-th power, where $\overline{q} = p^{m-k}$, and then taking the second component to the q^2-th power:

$$(x, y) \circ (u, v) = (x^q u + \alpha^{q^2} x u^q - a(x v^q - \alpha^q u y^q) - b(y^q v + \alpha y v^q), x v^{q^2} + y^{q^2} u). \quad (1)$$

The benefit of this representation is that both components of the operations employ only one nontrivial field automorphism (namely, $x \mapsto x^q$ in the first, and $x \mapsto x^{q^2}$ in the second component), which gives in particular more structure to certain autotopisms as we will see later.

If $a \neq 0$ we can always find an isotopic Taniguchi pre-semifield with the parameter $a = 1$ by using the transformation $y \mapsto \delta y$ and $v \mapsto \delta v$ for a suitable $\delta \in \mathbb{F}_{p^m}^*$. We thus only have to distinguish the cases $a = 0$ and $a = 1$ when discussing the isotopy question. We will denote the Taniguchi pre-semifield on $\mathbb{F}_{p^n} \cong \mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$ by $T(q, \alpha, a, b)$, where the value of m is fixed and taken from context.

We also exclude the case $k = m/2$ since in this case $q^2 \equiv 1 \pmod{p^m - 1}$ which is a special case that requires slightly different methods. Also observe that these pre-semifields are already contained in a family of Bierbrauer [2, 3], so we believe that it makes sense to exclude them from our treatment here.

It is possible to discern some isotopisms immediately:

Proposition 1 *Let $q = p^k$ and $\overline{q} = p^{m-k}$. Each Taniguchi pre-semifield $T(q, \alpha, a, b) = \mathbb{P}_1$ is isotopic to another Taniguchi pre-semifield $T(\overline{q}, 1/\alpha^{q^2}, a(\alpha^{q-1}/b), \alpha^{q^2-1}/b) = \mathbb{P}_2$.*

Proof We first perform a change of variables $x \leftrightarrow y, u \leftrightarrow v$ on $\mathbb{P}_1$ (which clearly preserves isotopy). The result is

$$(x, y) *_1 (u, v) = (y^q v + \alpha^{q^2} y v^q - a(y u^q - \alpha^q x^q v) - b(x^q u + \alpha x u^q), y u^{q^2} + x^{q^2} v).$$

We take the second component to the power $\overline{q}$ and then x, y, u, v to the power $\overline{q}$ as well. The result is

$$\begin{aligned}(x, y) *_2 (u, v) =& (y v^{\overline{q}} + \alpha^{q^2} y^{\overline{q}} v - a(y^{\overline{q}} u - \alpha^q x v^{\overline{q}}) - b(x u^{\overline{q}} + \alpha x^{\overline{q}} u), y^{\overline{q}^2} u + x v^{\overline{q}^2}) \\ =& (\alpha^{q^2}((1/\alpha^{q^2}) y v^{\overline{q}} + y^{\overline{q}} v) - a\alpha^q((1/\alpha^q) y^{\overline{q}} u - x v^{\overline{q}}) \\ & - b\alpha((1/\alpha) x u^{\overline{q}} + x^{\overline{q}} u), \\ & y^{\overline{q}^2} u + x v^{\overline{q}^2}).\end{aligned}$$

Now we can divide the first component by $-b\alpha$, which yields

$$\begin{aligned}(x, y) *_3 (u, v) =& (x^{\overline{q}}u + (1/\alpha)xu^{\overline{q}} - a(\alpha^{q-1}/b)(xv^{\overline{q}} - (1/\alpha^q)y^{\overline{q}}u) \\ & - (\alpha^{q^2-1}/b)(y^{\overline{q}}v + (1/\alpha^{q^2})yv^{\overline{q}}), \\ & xv^{\overline{q}^2} + y^{\overline{q}^2}u),\end{aligned}$$

proving the desired isotopy. □

With Proposition 1 it suffices to consider coefficients $q = p^k$ with $k < m/2$ when tackling the isotopy question (recall that we exclude the case $k = m/2$).

3 Group theoretic preliminaries

We now introduce the machinery of the technique to determine isotopy. The ideas are based on an approach developed by the authors in [6] for a family of commutative semifields.

We denote the set of all autotopisms of a pre-semifield $\mathbb{P}$ by $\mathrm{Aut}(\mathbb{P})$. It is easy to check that $\mathrm{Aut}(\mathbb{P})$ is a group under component-wise composition, i.e., $(N_1, L_1, M_1) \circ (N_2, L_2, M_2) = (N_1 \circ N_2, L_1 \circ L_2, M_1 \circ M_2)$. We will often view $\mathrm{Aut}(\mathbb{P})$ as a subgroup of $\mathrm{GL}(\mathbb{F}_{p^n})^3 \cong \mathrm{GL}(\mathbb{F}_{p^m} \times \mathbb{F}_{p^m})^3 \cong \mathrm{GL}(n, \mathbb{F}_p)^3$. Our approach is based on the following simple and well-known result (see e.g. [6]).

Lemma 1 *Let $\mathbb{P}_1 = (\mathbb{F}_p^n, +, \circ_1)$, $\mathbb{P}_2 = (\mathbb{F}_p^n, +, \circ_2)$ be isotopic pre-semifields via the isotopism $\gamma \in \mathrm{GL}(\mathbb{F}_{p^n})^3$. Then $\gamma^{-1}\,\mathrm{Aut}(\mathbb{P}_2)\gamma = \mathrm{Aut}(\mathbb{P}_1)$.*

The key fact that we will use is that the autotopism groups of the Taniguchi pre-semifields have a large and easily identifiable subgroup. We introduce some notations:

We write $\mathbb{F}_p$-linear mappings L from $\mathbb{F}_{p^n}$ to itself as 2×2 matrices of $\mathbb{F}_p$-linear mappings from $\mathbb{F}_{p^m}$ to itself. That is,

$$L = \begin{pmatrix} L_1 & L_2 \\ L_3 & L_4 \end{pmatrix}, \text{ for } L_i : \mathbb{F}_{p^m} \to \mathbb{F}_{p^m}.$$

We call the constituent functions $L_1, \ldots, L_4$ of L *subfunctions of* L. Set

$$\gamma_r = (N_r, L_r, M_r) \in \mathrm{GL}(\mathbb{F}_{p^n})^3 \text{ with } N_r = \begin{pmatrix} m_{r^{q+1}} & 0 \\ 0 & m_{r^{q^2+1}} \end{pmatrix}, \quad L_r = M_r = \begin{pmatrix} m_r & 0 \\ 0 & m_r \end{pmatrix},$$

where m_r denotes multiplication with the finite field element $r \in \mathbb{F}_{p^m}^*$. For simplicity, we write these diagonal matrices also in the form $\mathrm{diag}(m_r, m_r)$, so

$$\gamma_r = (\mathrm{diag}(m_{r^{q+1}}, m_{r^{q^2+1}}), \mathrm{diag}(m_r, m_r), \mathrm{diag}(m_r, m_r)).$$

We fix some further notation that we will use from now on:

Notation 1

- *Let p be a prime.*
- *Set $q = p^k$ with $k < m/2$ and $\overline{q} = p^{m-k}$.*
- *Define the cyclic group*

$$Z^{(q)} = \{\gamma_r : r \in \mathbb{F}_{p^m}^*\} \leq \mathrm{GL}(\mathbb{F}_{p^n})^3$$

of order $p^m - 1$. It is easy to see (Lemma 2 below) that $Z^{(q)} \leq \mathrm{Aut}(\mathbb{P})$.

- *Let p' be a p-primitive divisor of p^m-1, i.e. $p'|p^m-1$ and $p' \nmid p^{k'}-1$ for $k'<m$. Such a prime p' always exists if $m>2$ and $(p,m)\neq(2,6)$ by Zsigmondy's Theorem (see e.g. [7, Chapter IX., Theorem 8.3.]). We thus always stipulate $m>2$ and $(p,m)\neq(2,6)$ from now on.*
- *Let R be the unique Sylow p'-subgroup of $\mathbb{F}_{p^m}^*$.*
- *Define*

$$Z_R^{(q)} = \{\gamma_r : r \in R\},$$

which is the unique Sylow p'-subgroup of $Z^{(q)}$ with $|R|$ elements.
- *For a Taniguchi pre-semifield $\mathbb{P} = T(q,\alpha,a,b)$, denote by*

$$C_{q,\alpha,a,b} = C_{\mathrm{Aut}(\mathbb{P})}(Z_R^{(q)}),$$

the centralizer of $Z_R^{(q)}$ in $\mathrm{Aut}(\mathbb{P})$.
- *Define*

$$S = \{\mathrm{diag}(m_r, m_r) : r \in \mathbb{F}_{p^m}^*\},$$

and

$$S_R = \{\mathrm{diag}(m_r, m_r) : r \in R\}.$$

Observe that the condition $m>2$ that is necessary to work with a Zsygmondy prime is actually not restrictive since for $m=2$ the only admissible value for q is $q=p=p^{m/2}$ which is precisely the case we exclude anyway.

The crucial fact for our technique is that $\gamma_r \in \mathrm{Aut}(\mathbb{P})$ for all $r \in \mathbb{F}_{p^m}^*$ when $\mathbb{P}$ is a Taniguchi pre-semifield $T(q,\alpha,a,b)$ for arbitrary α, a, b, which can be directly verified using Eq. (1):

Lemma 2 *Let $T(q,\alpha,a,b) = \mathbb{P}$ be a Taniguchi pre-semifield on $\mathbb{F}_{p^n}$ with $n=2m$. Then $Z^{(q)} \leq \mathrm{Aut}(\mathbb{P})$.*

The key result that enables us to settle the question of isotopy for Taniguchi semifields is a slight adaptation from [6, Theorem 5.10.], which deals with certain *commutative* pre-semifields. In some sense, the result we present here is an adaptation of the one from [6] to a non-commutative semifield.

Lemma 3 *([6, Lemma 5.7.]) Let $N_{\mathrm{GL}(\mathbb{F}_{p^n})}(S_R)$, $N_{\mathrm{GL}(\mathbb{F}_{p^n})}(S)$ and $C_{\mathrm{GL}(\mathbb{F}_{p^n})}(S_R)$, $C_{\mathrm{GL}(\mathbb{F}_{p^n})}(S)$ be the normalizers and the centralizers of S_R and S in $\mathrm{GL}(\mathbb{F}_{p^n})$. Then*

(a)
$$N_{\mathrm{GL}(\mathbb{F}_{p^n})}(S_R) = N_{\mathrm{GL}(\mathbb{F}_{p^n})}(S) = \left\{ \begin{pmatrix} m_{c_1}\tau & m_{c_2}\tau \\ m_{c_3}\tau & m_{c_4}\tau \end{pmatrix} : c_1,c_2,c_3,c_4 \in \mathbb{F}_{p^m}^*, \tau \in \mathrm{Gal}(\mathbb{F}_{p^m}/\mathbb{F}_p) \right\} \cap \mathrm{GL}(\mathbb{F}_{p^n}),$$

(b)
$$C_{\mathrm{GL}(\mathbb{F}_{p^n})}(S_R) = C_{\mathrm{GL}(\mathbb{F}_{p^n})}(S) = \left\{ \begin{pmatrix} m_{c_1} & m_{c_2} \\ m_{c_3} & m_{c_4} \end{pmatrix} : c_1,c_2,c_3,c_4 \in \mathbb{F}_{p^m}^* \right\} \cap \mathrm{GL}(\mathbb{F}_{p^n}).$$

The following is an analogue of [6, Lemma 5.8.].

Lemma 4 *Let $\mathbb{P} = T(q,\alpha,a,b)$ be a Taniguchi pre-semifield. Assume that $C_{q,\alpha,a,b}$ contains $Z^{(q)}$ as an index I subgroup such that p' does not divide I. Then $Z_R^{(q)}$ is a Sylow p'-subgroup of $\mathrm{Aut}(\mathbb{P})$.*

Proof Let T be a Sylow p'-subgroup of $\mathrm{Aut}(\mathbb{P})$ that contains the p'-group $Z_R^{(q)}$. T itself is (by Sylow's Theorem) contained in a Sylow p'-subgroup of $\mathrm{GL}(\mathbb{F}_{p^n})^3$, say U. In particular, T is

abelian since all Sylow p'-subgroups of $\mathrm{GL}(\mathbb{F}_{p^n})^3$ are abelian, see [6, Proof of Lemma 5.8.]. This implies that T is a subgroup of the centralizer $C_{q,\alpha,a,b}$ of $Z_R^{(q)}$ in $\mathrm{Aut}(\mathbb{P})$. By assumption, $Z^{(q)}$ is an index I subgroup of $C_{q,\alpha,a,b}$ and p' does not divide I. Moreover, $Z_R^{(q)}$ is a Sylow p'-subgroup of $Z^{(q)}$ and therefore $p' \nmid [Z^{(q)} : Z_R^{(q)}] = I_1$. Let $[T : Z_R^{(q)}] = I_2 = p'^h$ for $h \geq 0$, since both are p'-groups. Since $I_2 | I_1 I$, and $p' \nmid I_1 I$, we must have $p' \nmid I_2$ and $I_2 = 1$. Thus, $Z_R^{(q)} = T$ and $Z_R^{(q)}$ is a Sylow p'-subgroup of $\mathrm{Aut}(\mathbb{P})$ as claimed. □

The following theorem is the main result that enables us to solve the isotopy question. It states that if two Taniguchi pre-semifields are isotopic (and a certain condition is satisfied), then there must exist an isotopism of a very simple form. Note that this does not prove that *all* isotopisms necessarily have this structure.

Theorem 2 *Let $\mathbb{P}_1 = T(q_1, \alpha, a, b)$ and $\mathbb{P}_2 = T(q_2, \alpha', a', b')$ be Taniguchi pre-semifields such that $0 < k_1 < m/2$ and $0 < k_2 \leq m/2$. Assume that*

$$C_{q_1,\alpha,a,b} \text{ contains } Z^{(q_1)} \text{ as an index } I \text{ subgroup such that } p' \text{ does not divide } I. \tag{C}$$

If $\mathbb{P}_1, \mathbb{P}_2$ are isotopic, then there exists an isotopism $\gamma = (N, L, M) \in \mathrm{GL}(\mathbb{F}_{p^n})^3$ such that all non-zero subfunctions of L, M are monomials. Moreover, all non-zero subfuncions of L and M have the same degree. (The degree of the subfunctions of L could be different than the degree of the subfunctions of M).

Proof By Lemma 2, we have $Z_R^{(q_1)} \leq \mathrm{Aut}(\mathbb{P}_1)$ and $Z_R^{(q_2)} \leq \mathrm{Aut}(\mathbb{P}_2)$. Assume $\mathbb{P}_1$ and $\mathbb{P}_2$ are isotopic via the isotopism $\delta \in \mathrm{GL}(\mathbb{F}_{p^n})^3$ that maps $\mathbb{P}_1$ to $\mathbb{P}_2$. Then $\delta^{-1}\,\mathrm{Aut}(\mathbb{P}_2)\delta = \mathrm{Aut}(\mathbb{P}_1)$ by Lemma 1. Observe that $|\delta^{-1} Z_R^{(q_2)} \delta| = |R| = |Z_R^{(q_1)}|$, so $Z_R^{(q_1)}$ and $\delta^{-1} Z_R^{(q_2)} \delta$ are Sylow p'-subgroups of $\mathrm{Aut}(\mathbb{P}_1)$ by Lemma 4 as long as Condition (C) holds. In particular, these two subgroups are conjugate in $\mathrm{Aut}(\mathbb{P}_1)$ by Sylow's theorem, i.e., there exists a $\lambda \in \mathrm{Aut}(\mathbb{P}_1)$ such that

$$\lambda^{-1}\delta^{-1} Z_R^{(q_2)} \delta\lambda = (\delta\lambda)^{-1} Z_R^{(q_2)} (\delta\lambda) = Z_R^{(q_1)}. \tag{2}$$

Set $\gamma = (N, L, M) = \delta\lambda$. Note that γ is an isotopism between $\mathbb{P}_1$ and $\mathbb{P}_2$ since $\lambda \in \mathrm{Aut}(\mathbb{P}_1)$. Equation (2) then immediately implies that

$$\begin{aligned} \mathrm{diag}(m_{r^{q_2+1}}, m_{r^{q_2^2+1}})N &= N\,\mathrm{diag}(m_{s^{q_1+1}}, m_{s^{q_1^2+1}}) \\ \mathrm{diag}(m_r, m_r)L &= L\,\mathrm{diag}(m_s, m_s) \\ \mathrm{diag}(m_r, m_r)M &= M\,\mathrm{diag}(m_s, m_s) \end{aligned}$$

for all $r \in R$ and $s = \pi(r)$ where $\pi : R \to R$ is a permutation. In particular, L and M are in the normalizer of $S_R = \{\mathrm{diag}(m_a, m_a) : a \in R\}$. By Lemma 3, all of the four subfunctions of L and M are zero or monomials of the same degree. □

We will now systematically investigate isotopisms (N, L, M) where the subfunctions of L, M are monomials or zero. We want to emphasize that without this simplification, a treatment of the isotopy question is *very* complicated, whereas the calculations we will do, while still technical, are much easier to handle. We also note that the remaining question on the crucial Condition (C) is naturally answered along the way and does not require much additional work.

4 Settling the isotopy question for Taniguchi semifields

We apply Theorem 2. First, we achieve some further strong restrictions.

Proposition 2 *Let* $q_1 = p^{k_1}$, $q_2 = p^{k_2}$,

$$\mathbb{P}_1 = T(q_1, \alpha, a, b) = (\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}, +, \circ_1), \text{ and,}$$
$$\mathbb{P}_2 = T(q_2, \alpha', a', b') = (\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}, +, \circ_2)$$

be Taniguchi pre-semifields such that $0 < k_1 < m/2$, $0 < k_2 \leq m/2$. *Further, let* (N, L, M) *be an isotopism between* $\mathbb{P}_1, \mathbb{P}_2$ *such that all non-zero subfunctions of* L, M *are monomials of the same degree. Then* $N_2, N_3, L_2, L_3, M_2, M_3 = 0$, *all other subfunctions are monomials of the same degree, and* $k_1 = k_2$.

Proof Say the degree of the non-zero subfunctions of L and M is p^{t_2} and p^{t_3}, respectively. Then, for all $(x, y), (u, v) \in \mathbb{F}_{p^m}^2$,

$$\begin{aligned} L(x, y) \circ_2 M(u, v) &= (a_2 x^{p^{t_2}} + b_2 y^{p^{t_2}}, c_2 x^{p^{t_2}} + d_2 y^{p^{t_2}}) \\ &\quad \circ_2 (a_3 u^{p^{t_3}} + b_3 v^{p^{t_3}}, c_3 u^{p^{t_3}} + d_3 v^{p^{t_3}}) \\ &= (h_1(x, y, u, v), h_2(x, y, u, v)) \end{aligned}$$

for some $a_2, b_2, c_2, d_2, a_3, b_3, c_3, d_3 \in \mathbb{F}_{p^m}$.

Hence,

$$h_2 = (a_2 x^{p^{t_2}} + b_2 y^{p^{t_2}})(c_3 u^{p^{t_3}} + d_3 v^{p^{t_3}})^{q_2^2} + (c_2 x^{p^{t_2}} + d_2 y^{p^{t_2}})^{q_2^2}(a_3 u^{p^{t_3}} + b_3 v^{p^{t_3}}). \quad (3)$$

We also have

$$\begin{aligned} N((x, y) \circ_1 (u, v)) = (*, N_3(x^{q_1} u + \alpha^{q_1^2} x u^{q_1} - a(x v^{q_1} - \alpha^{q_1} u y^{q_1}) - b(y^{q_1} v + \alpha y v^{q_1})) \\ + N_4(x v^{q_1^2} + y^{q_1^2} u)). \end{aligned}$$

Set $N((x, y) \circ_1 (u, v)) = L(x, y) \circ_2 M(u, v)$. Let us assume $N_3 \neq 0$, i.e. the second component contains a term

$$c(x^{q_1} u + \alpha^{q_1^2} x u^{q_1} - a(x v^{q_1} - \alpha^{q_1} u y^{q_1}) - b(y^{q_1} v + \alpha y v^{q_1}))^{p^t}. \quad (4)$$

Note that none of these terms can be canceled out by $N_4(x v^{q_1^2} + y^{q_1^2} u)$. Thus, those monomials also have to occur in h_2. Let us consider the monomials $x^{p^{k_1+t}} u^{p^t}$, $x^{p^t} u^{p^{k_1+t}}$. Those appear in h_2 if and only if $t_2 = k_1 + t$, $t_3 + 2k_2 = t$, $t_2 + 2k_2 = t$, $t_3 = k_1 + t$, $k_1 \equiv -2k_2 \pmod m$, or $t_2 = t_3 = t$, $k_1 \equiv 2k_2 \pmod m$. In both cases we get $t_2 = t_3$ and t is uniquely determined by t_2, so N_3 is a monomial. In order for all monomials in Eq. (4) to occur in h_2, it is necessary that $a_2 a_3 b_2 b_3 c_2 c_3 d_2 d_3 \neq 0$, but then h_2 will also contain the terms $y^{p^{t_2}} u^{p^{t_3+2k_2}}$ and $y^{p^{t_2+2k_2}} u^{p^{t_3}}$ which cannot both occur in the second component of $N((x, y) \circ_1 (u, v))$ (again, by the choice of t_2, t_3 and the conditions on k_1, k_2 it is impossible that those terms are covered by $N_4(x v^{q_1^2} + y^{q_1^2} u)$). We infer $N_3 = 0$.

Thus

$$N((x, y) \circ_1 (u, v)) = (*, N_4(x v^{q_1^2} + y^{q_1^2} u)).$$

Comparing with Eq. (3) immediately yields that N_4 is a monomial, say of degree p^t, and either $t = t_2 = t_3$, $q_1 = q_2$, $b_2 = c_2 = b_3 = c_3 = 0$ or $t_2 + 2k_2 = t$, $t_3 = t + 2k_1$, $t + 2k_1 = t_2$, $t = t_3 + 2k_2$. The second case leads to $t_2 = t_3$ and $k_1 \equiv -k_2 \pmod m$, which

is by our condition $0 < k_1 < m/2$, $0 < k_2 \leq m/2$ impossible. So $q_1 = q_2$, $t = t_2 = t_3$, $b_2 = c_2 = b_3 = c_3 = 0$ (implying $L_2 = L_3 = M_3 = M_3 = 0$).

Let us now check the first component. We have

$$\begin{aligned} N((x, y) \circ_1 (u, v)) =& (N_1(x^{q_1}u + \alpha^{q_1^2} x u^{q_1} \\ & - a_1(x v^{q_1} - \alpha^{q_1} u y^{q_1}) \\ & - b_1(y^{q_1} v + \alpha y v^{q_1})) \\ & + N_2(x v^{q_1^2} + y^{q_1^2} u), *) \end{aligned}$$

and

$$\begin{aligned} h_2 =& C_1 x^{p^{k_1+t_2}} u^{p^{t_2}} + \alpha'^{q_1^2} C_2 x^{p^{t_2}} u^{p^{k_1+t_2}} \\ & - a'(C_3 x^{p^{t_2}} v^{p^{k_1+t_2}} - \alpha'^{q_1} C_4 u^{p^{t_2}} y^{p^{k_1+t_2}}) \\ & - b'(C_5 y^{p^{k_1+t_2}} v^{p^{t_2}} + \alpha' C_6 y^{p^{t_2}} v^{p^{k_1+t_2}}) \end{aligned}$$

for non-zero coefficients $C_1, \ldots, C_6$. A comparison of degrees immediately shows $N_2 = 0$ and that N_1 is a monomial of degree p^t as desired. □

In the next step, we determine the remaining subfunctions. This also immediately verifies Condition (C).

Proposition 3 *Let* $q_1 = p^{k_1}$, $q_2 = p^{k_2}$,

$$\begin{aligned} \mathbb{P}_1 &= T(q_1, \alpha, a, b) = (\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}, +, \circ_1), \text{ and,} \\ \mathbb{P}_2 &= T(q_2, \alpha', a', b') = (\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}, +, \circ_2) \end{aligned}$$

be Taniguchi pre-semifields such that $0 < k_1 < m/2$ *and* $0 < k_2 \leq m/2$. *Further, let* (N, L, M) *be an isotopism between* $\mathbb{P}_1, \mathbb{P}_2$ *such that all non-zero subfunctions of* M, N *are monomials of the same degree. Then*

- $a = a' = 0$, α^{p^t}/α' *is a* $(q-1)$*-st power in* $\mathbb{F}_{p^m}^*$ *and* b'^{p^t}/b *is a* $(q+1)$*-st power in* $\mathbb{F}_{p^m}^*$ *for some* $0 \leq t \leq m-1$, *or*
- $a = a' = 1$, α^{p^t}/α' *is a* $(q-1)$*-st power in* $\mathbb{F}_{p^m}^*$ *and* $b = b'^{p^t}$ *for some* $0 \leq t \leq m-1$.

Moreover,

$$|C_{q_1,\alpha,a,b}| = \begin{cases} (p^{\gcd(k,m)} - 1)(p^m - 1) & \text{if } a \neq 0 \\ (p^{\gcd(k,m)} - 1)(p^m - 1) \cdot \gcd(p^m - 1, p^k + 1) & \text{if } a = 0. \end{cases}$$

Proof From Proposition 2, we infer that $L_2, L_3, N_2, N_3, M_2, M_3 = 0$, all other subfunctions are monomials of the same degree p^t, and $q_1 = q_2 =: p^k = q$.

Set $N_1 = a_1 x^{p^t}$, $N_4 = d_1 x^{p^t}$. Then

$$\begin{aligned} N((x, y) \circ_1 (u, v)) = (& a_1(x^q u + \alpha^{q^2} x u^q - a(x v^q - \alpha^q y^q u) - b(y^q v + \alpha y v^q))^{p^t}, \\ & d_1(x v^{q^2} + y^{q^2} u)^{p^t}). \end{aligned} \tag{5}$$

Likewise, the subfunctions of L and M are monomials of degree p^t, so

$$L((x, y)) \circ_2 M((u, v)) = (a_2 x^{p^t}, d_2 y^{p^t}) \circ_2 (a_3 u^{p^t}, d_3 v^{p^t}).$$

Thus

$$L(x, y) \circ_2 M(u, v) = (A_1(x, y, u, v), A_2(x, y, u, v))$$

where

$$\begin{aligned} A_1(x,y,u,v) =& (a_2x)^{p^t+k}(a_3u)^{p^t} + \alpha'^{q^2}(a_2x)^{p^t}(a_3u)^{p^{t+k}} \\ &- a'\left((a_2x)^{p^t}(d_3v)^{p^{t+k}} - \alpha'^{q}(a_3u)^{p^t}(d_2y)^{p^{t+k}}\right) \\ &- b'\left((d_2y)^{p^{t+k}}(d_3v)^{p^t} + \alpha'(d_2y)^{p^t}(d_3v)^{p^{t+k}}\right), \end{aligned}$$

and

$$A_2(x,y,u,v) = (a_2x)^{p^t}(d_3v)^{p^{t+2k}} + (a_3u)^{p^t}(d_2y)^{p^{t+2k}}.$$

A comparison with Eq. (5) yields for all possible terms $(x^qu)^{p^t}$, $(xu^q)^{p^t}$, $(xv^q)^{p^t}$, $(y^qu)^{p^t}$, $(y^qv)^{p^t}$, $(yv^q)^{p^t}$ in the first component and the two terms in the second component the following 8 equations:

$$a_1 = (a_2^q a_3)^{p^t} \tag{6}$$
$$a_1\alpha^{q^2+p^t} = \alpha'^{q^2}(a_2a_3^q)^{p^t} \tag{7}$$
$$a_1a = a'(a_2d_3^q)^{p^t} \tag{8}$$
$$a_1a\alpha^{q+p^t} = a'\alpha'^{q}(a_3d_2^q)^{p^t} \tag{9}$$
$$a_1b^{p^t} = b'(d_2^q d_3)^{p^t} \tag{10}$$
$$a_1b^{p^t}\alpha^{p^t} = b'\alpha'(d_2d_3^q)^{p^t} \tag{11}$$
$$d_1 = (a_2d_3^{q^2})^{p^t} \tag{12}$$
$$d_1 = (a_3d_2^{q^2})^{p^t}. \tag{13}$$

Eq. (8) can only be satisfied if $a = a' = 0$ or $a = a' = 1$, so we only need to consider these two cases.

Substituting Eq. (6) into Eq. (7) yields $(a_2^q a_3)^{p^t}(\alpha^{p^t}/\alpha')^{q^2} = (a_2a_3^q)^{p^t}$ which leads to

$$a_2^{q-1}(\alpha^{p^t}/\alpha')^{p^{2k-t}} = a_3^{q-1}. \tag{14}$$

In particular, α^{p^t}/α' must be a $(q-1)$-st power. We set $a_3 = a_2\gamma$, where $\gamma^{q-1} = (\alpha^{p^t}/\alpha')^{p^{2k-t}}$. Similarly, substituting Eq. (10) into Eq. (11) yields

$$d_2^{q-1}(\alpha^{p^t}/\alpha')^{p^{m-t}} = d_3^{q-1},$$

and we set $d_3 = d_2\gamma_2$ where $\gamma_2^{q-1} = (\alpha^{p^t}/\alpha')^{p^{m-t}}$. Comparing now Eq. (12) with Eq. (13) gives $a_2d_2^{q^2}\gamma_2^{q^2} = a_2d_2^{q^2}\gamma$, that is $\gamma = \gamma_2^{q^2}$. A comparison between Eq. (6) and Eq. (10) yields

$$\begin{aligned} (b'^{p^{m-t}}/b) &= (a_2/d_2)^{q+1}\gamma/\gamma_2 = (a_2/d_2)^{q+1}\gamma_2^{q^2-1} \\ &= (a_2/d_2)^{q+1}(\alpha^{p^t}/\alpha')^{p^{m-t}\cdot(q+1)}. \end{aligned} \tag{15}$$

Thus $(b'^{p^{m-t}}/b)$ must also be a $(q+1)$-st power; in other words b and $b'^{p^{m-t}}$ have to be in the same coset of the subgroup of $(q+1)$-st powers in $\mathbb{F}_{p^m}^*$.

We now consider the case $a = a' = 0$. Then Eq. (8) and Eq. (9) always hold and the conditions we have gathered so far cover all equations. We can thus find an isotopism between

$T(q,\alpha,0,b)$ and $T(q,\alpha',0,b')$ if and only if α^{p^t}/α' is a $(q-1)$-st power and (b'^{p^t}/b) is a $(q+1)$-st power for some $t \in \mathbb{N}$.

Now consider the case $a = a' = 1$. Of course, all previously derived constraints still apply, and Eq. (8) and Eq. (9) give two additional conditions. We first rewrite Eq. (8) with Eq. (6). The result is $a_2 d_3^q = a_2^q a_3$ and, using Eq. (14), we get

$$d_3^q = \frac{a_3^q}{\gamma^{q-1}} = a_3^q(\alpha'/\alpha^{p^t})^{p^{2k-t}}.$$

Similarly, rewriting Eq. (9) with Eq. (6) yields

$$a_2^q \alpha^{p^k}/\alpha'^{p^{k-t}} = d_2^q.$$

We show that these two statements are equivalent under the previous conditions. Indeed, we have

$$\begin{aligned}
& d_3^q = a_3^q(\alpha'/\alpha^{p^t})^{p^{2k-t}} \\
\Leftrightarrow\ & d_2^q\gamma_2^q = a_2^q\gamma^q(\alpha'/\alpha^{p^t})^{p^{2k-t}} \\
\Leftrightarrow\ & d_2^q = a_2^q\gamma_2^{q^3-q}(\alpha'/\alpha^{p^t})^{p^{2k-t}} = a_2^q\left((\alpha^{p^t}/\alpha')^{p^{m-t}}\right)^{q(q+1)}(\alpha'/\alpha^{p^t})^{p^{2k-t}} \\
\Leftrightarrow\ & d_2^q = a_2^q(\alpha^{p^t}/\alpha')^{p^{k-t}} = a_2^q\alpha^{p^k}/\alpha'^{p^{k-t}}.
\end{aligned}$$

Substituting this condition into Eq. (15) gives

$$(b'^{p^{m-t}}/b) = (\alpha'/\alpha^{p^t})^{p^{m-t}\cdot(q+1)}(\alpha^{p^t}/\alpha')^{p^{m-t}\cdot(q+1)} = 1.$$

We conclude that for fixed α, α', t with α^{p^t}/α' a $(q-1)$-st power, the presemifields $T(q,\alpha,1,b)$ and $T(q,\alpha',1,b')$ are isotopic if and only if $b = b'^{p^t}$ for some $0 \le t \le m-1$.

It remains to prove the statement on the centralizer. By Lemma 3, we only have to check autotopisms where the subfunctions of L, M are monomials of degree 1. This is a special case of this proposition, which is realized by setting $\mathbb{P}_1 = \mathbb{P}_2$ and $t = 0$. To compute the size of the centralizer, we have to go through our previous calculations and count the autotopisms of this form. For $a = 0$, we have $a_3 = a_2\gamma$, $d_3 = d_2\gamma^{\overline{q}^2}$ and $a_2^{q+1} = d_2^{q+1}$, where γ is $(q-1)$-st root of unity (see Eqs. (14) and (15)), and all other coefficients are uniquely determined from that. So there are in total $p^m - 1$ choices for a_2, $p^{\gcd(k,m)} - 1$ choices of γ and $\gcd(p^k+1, p^m-1)$ choices for d_2.

For $a = 1$, we have again $a_3 = a_2\gamma$ and the additional conditions determine all other coefficients uniquely. So the centralizer has size $(p^m-1)(p^{\gcd(k,m)}-1)$ because there are again $p^m - 1$ choices for a_2 and $p^{\gcd(k,m)} - 1$ choices of γ. □

We are now able to piece everything together in the following result:

Theorem 3 *Let* $q_1 = p^{k_1}$, $q_2 = p^{k_2}$,

$$\begin{aligned}
\mathbb{P}_1 &= T(q_1,\alpha,a,b) = (\mathbb{F}_{p^m}\times\mathbb{F}_{p^m},+,\circ_1), \text{ and,} \\
\mathbb{P}_2 &= T(q_2,\alpha',a',b') = (\mathbb{F}_{p^m}\times\mathbb{F}_{p^m},+,\circ_2)
\end{aligned}$$

be Taniguchi pre-semifields such that $k_1 \ne m/2$ *and* $a, a' \in \{0,1\}$. *If* $k_2 \equiv -k_1 \pmod m$ *then, for fixed* α', a', b', *there exist* α, a, b *such that* $\mathbb{P}_1$ *and* $\mathbb{P}_2$ *are isotopic. If* $k_1 \not\equiv k_2 \pmod m$ *and* $k_1 \not\equiv -k_2 \pmod m$, *the pre-semifields* $\mathbb{P}_1$ *and* $\mathbb{P}_2$ *are not isotopic.*

$T(q,\alpha,a,b)$ *and* $T(q,\alpha',a',b')$ *are isotopic if and only if one of the two following cases occurs:*

- $a = a' = 0$, α^{p^t}/α' *is a* $(q-1)$*-st power in* $\mathbb{F}_{p^m}^*$ *and* b'^{p^t}/b *is a* $(q+1)$*-st power in* $\mathbb{F}_{p^m}^*$ *for some* $0 \le t \le m-1$.
- $a = a' = 1$, α^{p^t}/α' *is a* $(q-1)$*-st power in* $\mathbb{F}_{p^m}^*$ *and* $b = b'^{p^t}$ *for some* $0 \le t \le m-1$.

Proof Let us first check Condition (C) from Theorem 2. By Proposition 3,

$$|C_{q_1,\alpha,a,b}| \in \{(p^{\gcd(k_1,m)}-1)(p^m-1), (p^{\gcd(k_1,m)}-1)(p^m-1)\cdot\gcd(p^m-1, p^{k_1}+1)\}.$$

Observe that $p' \nmid (p^{\gcd(k_1,m)}-1)$ since p' is a p-primitive divisor and $p' \nmid p^{k_1}+1$ since otherwise $p'|(p^{k_1}+1)(p^{k_1}-1) = p^{2k_1}-1$ which is not possible since $2k_1 \neq m$ and, again, p' is a p-primitive divisor. So $(p^m-1)p' \nmid |C_{q_1,\alpha,a,b}|$ and Condition (C) is satisfied.

Assume $\mathbb{P}_1$ and $\mathbb{P}_2$ are isotopic. Then there is an isotopism (N, L, M) between $\mathbb{P}_1$ and $\mathbb{P}_2$ with the properties stated in Theorem 2. We already dealt with the case $k_1 \equiv -k_2 \pmod m$ in Proposition 1, so we can assume $k_2 < m/2$. The statement then follows from Proposition 3.□

5 Counting the number of non-isotopic Taniguchi semifields

To count the number of Taniguchi (pre-)semifields, we need a famous result by Bluher [4] on projective polynomials and a well known basic lemma.

Theorem 4 *([4, Theorem 5.6.]) Let* $q = p^k$ *and denote by* $N(p,m)$ *the number of polynomials* $P(x) = x^{q+1} + x + b$ *with* $b \in \mathbb{F}_{p^m}$ *such that* P *does not have a root in* $\mathbb{F}_{p^m}$. *Set* $d = \gcd(k,m)$ *and* $l = m/d$. *Then*

$$N(p,m) = \begin{cases} \frac{p^{m+d}-p^d}{2(p^d+1)} & \text{if } l \text{ is even,} \\ \frac{p^{m+d}-1}{2(p^d+1)} & \text{if } p, l \text{ are odd,} \\ \frac{p^{m+d}+p^d}{2(p^d+1)} & \text{if } p \text{ is even and } l \text{ is odd.} \end{cases}$$

Lemma 5 *Let* $k, m \in \mathbb{N}$ *and* p *be a prime. Then*

- $\gcd(p^k-1, p^m-1) = p^{\gcd(k,m)}-1$.
- $\gcd(p^k+1, p^m-1) = \begin{cases} 1 & \text{if } m/\gcd(k,m) \text{ odd, and } p=2, \\ 2 & \text{if } m/\gcd(k,m) \text{ odd, and } p>2, \\ p^{\gcd(k,m)}+1 & \text{if } m/\gcd(k,m) \text{ even.} \end{cases}$

Theorem 5 *Let* $N_T(p,k,m,a)$ *be the number of non-isotopic Taniguchi semifields* $T(q,\alpha,a,b)$ *on* $\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$ *with* $k \neq m/2$. *Set* $d = \gcd(k,m)$ *and* $l = m/d$. *Then*

$$(p^d-2)\cdot N(p,m)/m \le N_T(p,k,m,1) \le (p^d-2)\cdot N(p,m),$$

where $N(p,m)$ *is determined in Theorem 4. Further,*

$$(p^d-2)\cdot p^d/m \le N_T(p,k,m,0) \le (p^d-2)\cdot p^d$$

if l *is even,*

$$(p^d-2)/m \le N_T(p,k,m,0) \le p^d-2$$

if p, l *are odd and* $N_T(p,k,m,0) = 0$ *if* p *is even and* l *is odd. The total number of non-isotopic Taniguchi semifields with* $k \neq m/2$ *is*

$$N_T(p,m) = \sum_{k=1}^{\lfloor \frac{m}{2} \rfloor} (N_T(p,k,m,0) + N_T(p,k,m,1)).$$

Proof By Theorem 3, $T(q, \alpha, 1, b)$ and $T(q, \alpha', 1, b')$ are isotopic if and only if there is a t such that α^{p^t}/α' is a $(q-1)$-st power and $b'^{p^t} = b.\alpha^{p^t}/\alpha'$ is a $(q-1)$-st power if and only if α^{p^t}, α' are in the same coset of the cyclic subgroup with $(p^m-1)/\gcd(q-1, p^m-1) = (p^m-1)/(p^d-1)$ elements of $\mathbb{F}^*_{p^m}$. There are thus p^d-1 such cosets. But $-\alpha, -\alpha'$ must not be $(q-1)$-st powers themselves by the necessary conditions for Taniguchi pre-semifields, so there are between $(p^d-2)/m$ and p^d-2 possible choices for α that yield non-isotopic pre-semifields. The overall number of permissible b is (by Theorem 4) $N(p, m)$. For a fixed b, t there is exactly one choice of b' that yields an isotopic semifields, so there are $N(p, m)$ many non-isotopic choices for b, yielding the desired bound.

For $a = 0$, we have again between $(p^d-2)/m$ and p^d-2 choices for α for ranging t. b, b' yield isotopic pre-semifields if and only if b'^{p^t}/b is a $(q+1)$-st power for some t. Here, similar to before, this means that b'^{p^t} and b are in the same coset of the cyclic subgroup with $(p^m-1)/\gcd(q+1, p^m-1)$ elements of $\mathbb{F}^*_{p^m}$. By Lemma 5, we have $\gcd(q+1, p^m-1) = p^d+1$ if l is even and $\gcd(q+1, p^m-1) = 2$ if l, p are odd and $\gcd(q+1, p^m-1) = 1$ if $p = 2$ and l is odd. So the number of cosets is p^d+1, 2 or 1 depending on p, l. Since $-b, -b'$ themselves must not be $(q+1)$-st powers (by the conditions on the Taniguchi pre-semifield $x^{q+1}+b$ has no roots) we thus have p^d, 1 or 0 valid cosets.

By Theorem 3, different choices for $1 \leq k < m/2$ yield non-isotopic semifields, proving our result. □

Remark 1 The precise values for $N_T(p, k, m, a)$ in Theorem 5 depend on the precise values of m and d, and could be computed with additional effort, see [14, Section 5] where a similar computation is applied for the $p = 2$, $d = 1$ case. However, these calculations are quite involved and since the factor $1/m$ that lies between the bounds in Theorem 5 does not change the asymptotics of the result, we choose to not go into any more details.

6 Comparison with other semifield families and conclusion

Theorem 5 (together with Theorem 4) shows that the total amount of pairwise non-isotopic Taniguchi semifields of order p^{2m} is approximately p^{m+s} where s is the largest divisor of m, excluding $m/2$. In particular if $3|m$, the number of semifields is around $p^{\frac{4}{3}m}$.

On the other hand,

- the best known lower bound on the number of pairwise non-isotopic odd-order semifields of order p^n constructed using skew-polynomial rings (or, equivalently, cyclic semifields; see [17] for details) is less than $p^{n/2}$ [8, Theorem 10].
- The number of pairwise non-isotopic generalized twisted fields of order p^n is around p^t, where t is the largest divisor of n that is less than $n/2$ [19, Theorem 27].
- The best known lower bound on the number of pairwise non-isotopic semifields of order p^{4l} constructed with the HMO construction is less than p^{2l} [10]. We are not aware of any other construction of odd-order semifields that yields better lower bounds.

The count in Theorem 5 thus shows that the family of Taniguchi semifields yields a better bound compared to the best currently known lower bounds. In particular, the results in this paper show that the family of Taniguchi semifields is the largest known family of odd-order semifields to date. Interestingly, the amount of non-isotopic Taniguchi semifields is even larger than the known upper bound on the number of non-isotopic odd-order semifields of order p^n constructed using skew-polynomial rings, which is $p^{n/2}\log_2(p^n)$ [11]. Note that

the family of semifields constructed via skew-polynomial rings was recently extended [21], however it remains so far unclear how much this changes the bound mentioned above. The upper bound given by Kantor [10, Theorem 1.6.] on the number of non-isotopic semifields from the HMO construction is larger than the number of non-isotopic Taniguchi semifields. However, it is unclear how strict this bound is.

Note that the situation for non-isotopic semifields of even order is quite different, as the construction by Kantor and Williams [12] yields bounds that are much higher. More precisely, the number of non-isotopic semifields of even order is not bounded from below by a polynomial in the order of the semifield (see [9]). Whether the number of non-isotopic semifields of odd order is also not bounded by a polynomial in the order of the semifield is an open problem, widely known as Kantor's conjecture. In fact, even the number of *commutative* semifields of odd order is asymptotically not much different from the current state-of-the-art bound for non-commutative semifields, with [6] giving a family of around $p^{n/4}$ non-isotopic, commutative semifields of order p^n. It is thus desirable to construct new, larger families of (non-commutative) semifields especially of odd order.

Acknowledgements The athors would like to thank William Kantor and Yue Zhou for their comments, and bringing some literature on non-commutative semifields referred to in Conclusion to their attention. We further thank an anonymous reviewer for spotting a calculation error in Proposition 3. The first author is supported by GAČR Grant 18-19087 S - 301-13/201843. The second author is supported by NSF Grant 2127742.

Data availibility Data sharing not applicable to this article as no datasets were generated or analysed during the current study.

Declarations

Conflicts of interest The authors have no conflicts of interest to declare that are relevant to the content of this article.

References

1. Albert, A.A.: Finite division algebras and finite planes. In: Proceedings of Symposia in Applied Mathematics Volume 10, American Mathematical Society, Providence, R.I., (1960), pp. 53–70.
2. Bartoli D., Bierbrauer J., Kyureghyan G., Giulietti M., Marcugini S., Pambianco F.: A family of semifields in characteristic 2. J. Algebr. Comb. **45**(2), 455–473 (2017).
3. Bierbrauer J.: Projective polynomials, a projection construction and a family of semifields. Des. Codes Cryptogr. **79**(1), 183–200 (2016).
4. Antonia W.: Bluher, on $x^{q+1} + ax + b$. Finite Fields Appl. **10**(3), 285–305 (2004).
5. Dickson L.E.: On commutative linear algebras in which division is always uniquely possible. Trans. Am. Math. Soc. **7**(4), 514–522 (1906).
6. Göloğlu, F., Kölsch, L.: An exponential bound on the number of non-isotopic commutative semifields, (2021), arXiv:2109.04923.
7. Huppert B., Blackburn N.: Finite Groups. II, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 242. Springer, Berlin (1982).
8. Johnson N.L., Marino G., Polverino O., Trombetti R.: On a generalization of cyclic semifields. J. Algeb. Comb. **29**(1), 1–34 (2009).
9. William M.: Kantor, commutative semifields and symplectic spreads. J. Algebra **270**(1), 96–114 (2003).
10. Kantor W.M.: HMO-planes. Adv. Geom **9**, 31–43 (2009).
11. Kantor W.M., Liebler R.A.: Semifields arising from irreducible semilinear transformations. J. Aust. Math. Soc. **85**(3), 333–339 (2008).
12. Kantor W.M., Williams M.E.: Symplectic semifield planes and $\mathbb{Z}_4$-linear codes. Trans. Am. Math. Soc. **356**(3), 895–938 (2004).
13. Kaspers, C.: Equivalence problems of almost perfect nonlinear functions and disjoint difference families, Ph.D. thesis, Otto-von-Guericke-Universität Magdeburg, Fakultät für Mathematik, (2021).

14. Kaspers C., Zhou Y.: The number of almost perfect nonlinear functions grows exponentially. J. Cryptol. **34**, 1–4 (2021).
15. Donald E.: Knuth, Finite semifields and projective planes. J. Algebra **2**, 182–217 (1965).
16. Lavrauw, M., Polverino, O.: Finite semifields. In: Current Research Topics in Galois Geometry (2011), pp. 131–160.
17. Lavrauw M., Sheekey J.: Semifields from skew polynomial rings. Adv. Geom. **13**(4), 583–604 (2013).
18. Pott A., Schmidt K.-U., Zhou Y.: Semifields, Relative Difference Sets, and Bent Functions, pp. 161–178. De Gruyter, Algebraic curves and finite fields, Berlin (2014).
19. Purpura W.: Counting the generalized twisted fields. Note di Matematica **27**(1), 53–59 (2007).
20. Sheekey J.: MRD Codes: Constructions and Connections, Combinatorics and Finite Fields, pp. 255–286. de Gruyter, Berlin (2019).
21. Sheekey J.: New semifields and new MRD codes from skew polynomial rings. J. Lond. Math. Soc. **101**(1), 432–456 (2020).
22. Taniguchi H.: On some quadratic APN functions. Des. Codes Cryptogr. **87**(9), 1973–1983 (2019).