Counting the number of non-isotopic semifields inside some known semifield families

Faruk Göloğlu[1] and Lukas Kölsch[2]

[1] Charles University Prague
farukgologlu@gmail.com
[2] University of South Florida
lukas.koelsch.math@gmail.com

Abstract. We count the number of non-isotopic semifields inside several known families of semifields; in this extended abstract we will focus on the Taniguchi semifields. The key ingredient of the proofs is a technique to determine isotopy that was recently developed by the authors that exploits the existence of certain large subgroups of the autotopism group of a semifield.

Keywords: semifields · isotopy · projective planes.

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

(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 [7, 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*.

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**. The pre-semifield $\mathbb{P}$ and the corresponding semifield $\mathbb{S}$ constructed by Kaplansky's trick are always isotopic. Isotopy of pre-semifields is an equivalence relation.

Semifields have receive muched 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 [7, Section 3] for a detailed treatment). Semifields are further equivalent to Maximum Rank Distance codes with certain parameters (see e.g. [9]) and can be used to construct relative difference sets (see [8]).

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. [6, 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 [5], the authors developed a technique to settle the isotopy question for one specific family of semifields. We apply the same technique to other families of semifields. In this extended abstract, we will focus on the Taniguchi semifields introduced in [10].

2 The Setup

The Taniguchi pre-semifields are defined in [10] 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 $\mathbb{F}_{p^m}$. We will instead use a different, isotopic respresentation of the Taniguchi pre-semifield that arises after taking x, u to the $\overline{q}^2$-th power, where $\overline{q} = q^{m-k}$, and then taking the second component to the q^2-th power:

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

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 $a = 1$. 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 [3,2], so we believe that it makes sense to exclude them from our treatment here.

2.1 Group theoretic preliminaries

We now introduce the machinery of the technique to determine isotopy, which was developed by the authors in [5]. 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. [5]).

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

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

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

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

where m_r denotes multiplication with the finite field element $r \in \mathbb{F}_{p^m}^\times$. 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 $q = p^k$ and $\overline{q} = p^{m-k}$.*
- *Define the cyclic group*

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

  of order $p^m - 1$.
- *Let p' be a p-primitive divisor of $p^m - 1$. Such a prime p' always exists if $m > 2$ and $(p, m) \neq (2, 6)$ by Zsigmondy's Theorem.* ***We thus always stipulate*** *$m > 2$* ***and*** *$(p, m) \neq (2, 6)$* ***from now on.***
- *Let R be the unique Sylow p'-subgroup of $\mathbb{F}_{p^m}^\times$.*
- *Define*

$$Z_R^q = \{\gamma_r \colon r \in R\},$$

  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 $\mathrm{Aut}(\mathbb{P})$.

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

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

The key result that enables us to settle the question of isotopy for Taniguchi semifields is a slight adaptation from [5, Theorem 5.10.]. The proof requires slight modification compared to the one given in [5] which we omit in this abstract.

Theorem 2. *Let $T(q_1 = p^{k_1}, \alpha_1, a_1, b_1) = \mathbb{P}_1 = (\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}, +, \circ_1)$ and $T(q_2 = p^{k_2}, \alpha_1, a_1, b_1) = \mathbb{P}_2 = (\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}, +, \circ_2)$ be Taniguchi pre-semifields such that $k_1 \neq m/2$. Assume that*

C_{q_1,α_1,a_1,b_1} *contains Z^{q_1} as an index I subgroup such that p' does not divide I.* (C)

If $\mathbb{P}_1, \mathbb{P}_2$ are isotopic, then there exists an isotopism $\gamma = (N, L, M) \in \mathrm{GL}(\mathbb{F}_{p^n})^3$, with the following properties:

- *All non-zero subfunctions of N, L, M are monomials.*
- *All non-zero subfunctions of L and M have the same degree p^t.*
- *$N_2 = N_3 = 0$.*
- *We have $k_1 \equiv \pm k_2 \pmod m$.*
- *If $k_1 \equiv k_2 \pmod m$ then N_1 and N_4 are monomials of degree p^t.*
- *If $k_1 \equiv -k_2 \pmod m$ then N_1 and N_4 are monomials of degree p^{t+k_2}.*

This theorem reduces the effort required to prove non-isotopy between Taniguchi pre-semifields considerably, as long as Condition (C) is satisfied.

3 Settling the isotopy question for Taniguchi pre-semifields

We apply Theorem 2. We first have to deal with Condition (C). This can be done with fairly standard techniques following the ideas in [5]; we skip the proof.

Lemma 3. *Let $T(q = p^k, \alpha, a, b) = \mathbb{P} = (\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}, +, \circ)$ be a Taniguchi pre-semifield with $k \neq m/2$. Then*

$$|C_{q_1,\alpha_1,a_1,b_1}| = \begin{cases} (p^{\gcd(k,m)} - 1)(p^m - 1) & \text{if } a \neq 0 \\ (p^{\gcd(k,m)} - 1)(p^m - 1) \cdot \gcd(p^m - 1, p^k + 1) & \text{if } a = 0. \end{cases}$$

In all cases, $p' \nmid |C_{q_1,\alpha_1,a_1,b_1}|/(p^m - 1)$ and Condition (C) is satisfied.

We are now ready to determine when Taniguchi pre-semifields are isotopic.

Theorem 3. *Let* $T(q_1 = p^{k_1}, \alpha_1, a_1, b_1) = \mathbb{P}_1 = (\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}, +, \circ_1)$ *and* $T(q_2 = p^{k_2}, \alpha_1, a_1, b_1) = \mathbb{P}_2 = (\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}, +, \circ_2)$ *be Taniguchi pre-semifields such that* $k_1 \neq m/2$. *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* $k_1 \neq k_2$ *and* $k_2 \equiv -k_1 \pmod m$, *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 occur:

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

Proof. 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. In particular, $\mathbb{P}_1$ and $\mathbb{P}_2$ can only be isotopic if $k_1 \equiv \pm k_2 \pmod m$.

We first show an isotopy in the case $k_1 \equiv -k_2 \pmod m$. We first perform a change of variables $x \leftrightarrow y$, $u \leftrightarrow v$ on $\mathbb{P}_1$ (which clearly preserves isotopy). The result is

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

We take the second component to the power $\overline{q}$, take x, y, u, v to the power $\overline{q}$ and set $\gamma = \alpha^{\overline{q}^2}$. The result is

$$\begin{aligned}(x, y) * (u, v) =& (y v^{\overline{q}} + \gamma y^{\overline{q}} v - a(y^{\overline{q}} u - \gamma^{\overline{q}} x v^{\overline{q}}) - b(x u^{\overline{q}} + \gamma^{\overline{q}^2} x^{\overline{q}} u), x_2^{\overline{q}^2} y_1 + x_1 y_2^{\overline{q}^2}) \\ =& (\gamma((1/\gamma) y v^{\overline{q}} + y^{\overline{q}} v) - a\gamma^{\overline{q}}((1/\gamma^{\overline{q}}) y^{\overline{q}} u - x v^{\overline{q}}) - b\gamma^{\overline{q}^2}((1/\gamma^{\overline{q}^2}) x u^{\overline{q}} + x^{\overline{q}} u), \\ & y^{\overline{q}^2} u + x v^{\overline{q}^2}).\end{aligned}$$

Now we can divide the first component by $-b\gamma^{\overline{q}^2}$ and it is clear that the result is a Taniguchi presemifield with parameter $\overline{q}$.

We can thus restrict ourselves to the case $k_1 = k_2 =: k$, i.e. $q_1 = q_2 =: q$. In this case, by Theorem 2, $N_2 = N_3 = 0$, $N_1 = a_1 x^{p^t}$, $N_4 = d_1 x p^t$. Then

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

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

$$L((x, y)) \circ_2 M((u, v)) = (a_2 x^{p^t} + b_2 y^{p^t}, c_2 x^{p^t} + d_2 y^{p^t}) \circ_2 (a_3 u^{p^t} + b_3 v^{p^t}, c_3 u^{p^t} + d_3 v^{p^t}).$$

We can infer just from comparing the degrees of the terms that the only possible solutions necessarily satisfy $b_2 = b_3 = c_2 = c_3 = 0$ and $a_2, a_3, d_2, d_3 \neq 0$. For example, if $b_2 \neq 0$, then $L((x_1, x_2)) \circ_2 M((y_1, y_2))$ would have terms of the form $b_2 c_3 (y u^{q^2})^{p^t}$ and $b_2 d_3 (y v^{q^2})^{p^t}$ in the second component, which clearly violates (2) since $(c_3, d_3) \neq (0, 0)$ by the bijectivity of M. The cases $b_3, c_2, c_3 \neq 0$ can be excluded in the same way.

Thus

$$L((x,y)) \circ_2 M((u,v)) = (a_2 x^{p^t}, d_2 y^{p^t}) \circ_2 (a_3 u^{p^t}, d_3 v^{p^t})$$
$$=((a_2x)^{p^t+q}(a_3u)^{p^t} + \alpha'^{q^2}(a_2x)^{p^t}(a_3u)^{p^t+q} - a'((a_2x)^{p^t}(d_3v)^{p^t+q} - \alpha'^{q}(a_3u)^{p^t}(d_2y)^{p^t+q}) -$$
$$b'((d_2y)^{p^t+q}(d_3v)^{p^t} + \alpha'(d_2y)^{p^t}(d_3v)^{p^t+q}), (a_2x)^{p^t}(d_3v)^{p^t+q^2} + (a_3u)^{p^t}(d_2y)^{p^t+q^2}).$$

A comparison with Eq. (2) yields for all possible terms $(x^q u)^{p^t}$, $(xu^q)^{p^t}$, $(xv^q)^{p^t}$, $(y^q u)^{p^t}$, $(y^q v)^{p^t}$, $(yv^q)^{p^t}$ in the first component and the two terms in the second component the following 8 equations:

$$a_1 = (a_2^q a_3)^{p^t} \quad (3) \qquad a_1 b^{p^t} = b'(d_2^q d_3)^{p^t} \quad (7)$$
$$a_1 \alpha^{q^2} = \alpha'^{q^2}(a_2 a_3^q)^{p^t} \quad (4) \qquad a_1 b^{p^t} \alpha = b'\alpha'(d_2 d_3^q)^{p^t} \quad (8)$$
$$a_1 a = a'(a_2 d_3^q)^{p^t} \quad (5) \qquad d_1 = (a_2 d_3^{q^2})^{p^t} \quad (9)$$
$$a_1 a \alpha^q = a'\alpha'^q (a_3 d_2^q)^{p^t}. \quad (6) \qquad d_1 = (a_3 d_2^{q^2})^{p^t}. \quad (10)$$

The third equation on the left can only be satisfied if $a = a' = 0$ or $a = a' = 1$, so we only need to consider these two cases.

Substituting Eq. (3) into Eq. (4) yields $(a_2^q a_3)^{p^t}(\alpha/\alpha')^{q^2} = (a_2 a_3^q)^{p^t}$ which leads to

$$a_2^{q-1}(\alpha/\alpha')^{p^{2k-t}} = a_3^{q-1}. \quad (11)$$

In particular, α/α' must be a $(q-1)$-st power. We set $a_3 = a_2\gamma$, where $\gamma^{q-1} = (\alpha/\alpha')^{p^{2k-t}}$. Similarly, substituting Eq. (7) into Eq. (8) yields

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

and we set $d_3 = d_2\gamma_2$ where $\gamma_2^{q-1} = (\alpha/\alpha')^{p^{m-t}}$. Comparing now Eq. (9) with Eq. (10) gives $a_2 d_2^{q^2}\gamma_2^{q^2} = a_2 d_2^{q^2}\gamma$, that is $\gamma = \gamma_2^{q^2}$. A comparison between Eq. (3) and Eq. (7) yields

$$(b'^{p^{m-t}}/b) = (a_2/d_2)^{q+1}\gamma/\gamma_2 = (a_2/d_2)^{q+1}\gamma_2^{q^2-1}$$
$$= (a_2/d_2)^{q+1}(\alpha/\alpha')^{p^{m-t}\cdot(q+1)}. \quad (12)$$

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. (5) and Eq. (6) 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/α' is a $(q-1)$-st power and (b'^{p^t}/b) is be 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. (5) and Eq. (6) give two additional conditions. We first rewrite Eq. (5) with Eq. (3). The result is $a_2 d_3^q = a_2^q a_3$ and, using Eq. (11), we get

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

Similarly, rewriting Eq. (6) with Eq. (3) yields

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

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

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

Substituting this condition into Eq. (12) gives

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

We conclude that for fixed α, α' with α/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 $0 \le t \le m-1$. □

To count the number of Taniguchi pre-semifields, we need a famous result by Bluher [4] on projective polynomials.

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*

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

Theorem 5. *Let $N_T(p,m,a)$ be the number of non-isotopic Taniguchi semifields $T(q = p^k, \alpha, a, b)$ 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*

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

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

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

if l is even,

$$N_T(p,m,0) = \lfloor (m-2)/2 \rfloor \cdot (p^d-2)$$

if p, l are odd and $N_T(p,m,0) = 0$ if p is even and l is odd. The total number of non-isotopic Taniguchi semifields is

$$N_T(p,m) = N_T(p,m,0) + N_T(p,m,1).$$

Proof. By Theorem 3 $T(q_1, \alpha_1, 1, b_1)$ and $T(q_2, \alpha_2, 1, b_2)$ are isotopic if and only if $q_1 = q_2$ or $q_1 q_2 \equiv 1 \pmod{p^m - 1}$, α_1/α_2 is a $(q-1)$-st power and there is a t such that $b_2^{p^t} = b_1$. α_1/α_2 is a $(q-1)$-st power if and only if α_1, α_2 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 $\mathbb{F}_{p^m}^\times$. There are thus p^d-1 such cosets. But α_1, α_2 must not be $(q-1)$-st powers themselves by the necessary conditions for Taniguchi pre-semifields, so there are $p^d - 2$ possible choices for α that yield non-isotopic presemifields. The overall number of permissible b is (by Theorem 4) $N(p, m)$, but since b_2, b_1 yield isotopic semifields if $b_2^{p^t} = b_1$ for some t, there are between $N(p, m)/m$ and $N(p, m)$ many non-isotopic choices for b. The number of non-isotopic choices for q is $\lfloor (m-2)/2 \rfloor$.

For $a = 0$, we have again $\lfloor (m-2)/2 \rfloor$ choices for q and $p^d - 2$ choices for α. b_1, b_2 yield isotopic pre-semifields if and only if $b_2^{p^t}/b_1$ is a $(q+1)$-st power for some t. Here, similar to before, this means $b_2^{p^t}$ and b_1 are in the same coset of the cyclic subgroup with $(p^m-1)/\gcd(q+1, p^m-1)$ elements of $\mathbb{F}_{p^m}^\times$. We have $\gcd(q+1, p^m-1) = p^d + 1$ if l is even and $\gcd(q+1, p^m-1) = 2$ is 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_1, b_2 themselves must not be $(q+1)$-st powers (by the conditions on the Taniguchi pre-semifield) we thus have p^d, 1 or 0 valid cosets. The choice of t yields that $b_2^{p^t}$ can be in at most m different cosets, proving the result. □

Remark 1.
- The precise values for $N_T(p, m, a)$ in Theorem 5 depend on the divisors of m and $p^d - 1$. Since a factor $1/m$ does not change the asymptotics of the result, we elected to not go into more detail.
- A similar technique can be used to determine the number of non-isotopic semifields found in [2,3] or some Knuth semifields; however the steps become more complicated and do not fit this extended abstract.

Acknowledgements The first author is supported by GAČR Grant 18-19087S - 301-13/201843. The second author is supported by NSF grant 2127742.

References

1. A. A. Albert, *Finite division algebras and finite planes*, Proc. Sympos. Appl. Math., Vol. 10, American Mathematical Society, Providence, R.I., 1960, pp. 53–70. MR 0116036
2. Daniele Bartoli, Jürgen Bierbrauer, Gohar Kyureghyan, Massimo Giulietti, Stefano Marcugini, and Fernanda Pambianco, *A family of semifields in characteristic 2*, Journal of Algebraic Combinatorics **45** (2017), no. 2, 455–473.
3. Jürgen Bierbrauer, *Projective polynomials, a projection construction and a family of semifields*, Des. Codes Cryptogr. **79** (2016), no. 1, 183–200. MR 3470785
4. Antonia W. Bluher, *On* $x^{q+1} + ax + b$, Finite Fields Appl. **10** (2004), no. 3, 285–305. MR 2067599
5. Faruk Göloğlu and Lukas Kölsch, *An exponential bound on the number of non-isotopic commutative semifields*, 2021, arXiv:2109.04923.

6. William M. Kantor and Michael E. Williams, *Symplectic semifield planes and $\mathbb{Z}_4$-linear codes*, Trans. Amer. Math. Soc. **356** (2004), no. 3, 895–938. MR 1984461
7. Donald E. Knuth, *Finite semifields and projective planes*, J. Algebra **2** (1965), 182–217. MR 175942
8. Alexander Pott, Kai-Uwe Schmidt, and Yue Zhou, *Semifields, relative difference sets, and bent functions*, Algebraic curves and finite fields, De Gruyter, 2014, pp. 161–178.
9. John Sheekey, *13. mrd codes: Constructions and connections*, Combinatorics and Finite Fields, de Gruyter, 2019, pp. 255–286.
10. Hiroaki Taniguchi, *On some quadratic apn functions*, Designs, Codes and Cryptography **87** (2019), no. 9, 1973–1983.