**Noname manuscript No.**
(will be inserted by the editor)

# Self-embeddings of Hamming Steiner triple systems of small order and APN permutations

**J. Rifà · F. I. Solov'eva · M. Villanueva**

Received: date / Accepted: date

**Abstract** The classification, up to isomorphism, of all self-embedding monomial power permutations of Hamming Steiner triple systems of order $n = 2^m - 1$ for small $m$ ($m \leq 22$), is given. As far as we know, for $m \in \{5, 7, 11, 13, 17, 19\}$, all given self-embeddings in closed surfaces are new. Moreover, they are cyclic for all $m$ and nonorientable at least for all $m \leq 19$. For any non prime $m$, the nonexistence of such self-embeddings in a closed surface is proven.

The rotation line spectrum for self-embeddings of Hamming Steiner triple systems in pseudosurfaces with pinch points as an invariant to distinguish APN permutations or, in general, to classify permutations, is also proposed. This invariant applied to APN monomial power permutations gives a classification which coincides with the classification of such permutations via CCZ-equivalence, at least up to $m \leq 17$.

**Keywords** APN functions, Hamming codes, self-embeddings, Steiner triple systems

**Mathematics Subject Classification (2000)** 94B15; 94A60

## 1 Introduction

Let $\mathbb{F}^n$ be the vector space of dimension $n$ over the binary field $\mathbb{F}$. The *Hamming distance* between two vectors $x, y \in \mathbb{F}^n$, denoted by $d(x, y)$, is the number of coordinate positions in which $x$ and $y$ differ. The *Hamming weight* of $x \in \mathbb{F}^n$,

---

This work was partially supported by the Spanish MICINN under Grants MTM2009-08435 and TIN2010-17358, and by the Catalan AGAUR under Grant 2009SGR1224. The work of the second author was supported by the Grant RFBR 12-01-00631-a.

---

The first and the third authors are members of the Department of Information and Communications Engineering, Universitat Autònoma de Barcelona, 08193-Bellaterra, Spain. Second author is with the Sobolev Institute of Mathematics and Novosibirsk State University, Novosibirsk, Russia

denoted by $w(x)$, is given by $w(x) = d(x, \mathbf{0})$, where $\mathbf{0}$ is the all-zero vector of length $n$ (it will always be clear from the context what is the length of the vector $\mathbf{0}$). The *support* of $x \in \mathbb{F}^n$ is the set of nonzero coordinate positions of $x$ and is denoted by $\mathrm{supp}(x)$.

Any nonempty subset $\mathcal{C}$ of $\mathbb{F}^n$ is a *binary code* and any vector subspace of $\mathbb{F}^n$ is a *binary linear code*. The elements of $\mathcal{C}$ are called *codewords*. The *minimum distance* of $\mathcal{C}$, denoted by $d_{\mathcal{C}}$, is the smallest Hamming distance between any pair of different codewords. Let $\mathcal{S}_n$ be the symmetric group of permutations of length $n$. Assume that a permutation $\pi \in \mathcal{S}_n$ acts on a vector $x = (x_1, \ldots, x_n)$ as $\pi(x) = (x_{\pi^{-1}(1)}, \ldots, x_{\pi^{-1}(n)})$. Two binary codes $\mathcal{C}_1$ and $\mathcal{C}_2$ of length $n$ are said to be *isomorphic* if there exists a coordinate permutation $\pi \in \mathcal{S}_n$ such that $\mathcal{C}_2 = \{\pi(x) : x \in \mathcal{C}_1\}$. They are said to be *equivalent* if there exists a vector $y \in \mathbb{F}^n$ and a coordinate permutation $\pi \in \mathcal{S}_n$ such that $\mathcal{C}_2 = \{y + \pi(x) : x \in \mathcal{C}_1\}$. Although the two definitions above stand for two different concepts, it follows that two binary linear codes are equivalent if and only if they are isomorphic [17].

A binary code $\mathcal{C}$ of length $n$ is a *perfect 1-error correcting code* (briefly, *perfect code*) if every $x \in \mathbb{F}^n$ is within distance 1 from exactly one codeword of $\mathcal{C}$. The perfect codes have length $n = 2^m - 1$, $2^{n-m}$ codewords and minimum distance 3. For any integer $m \geq 2$, there exists a unique, up to equivalence, perfect linear code of length $n = 2^m - 1$, called the *Hamming code* and denoted by $\mathcal{H}^n$ [17]. Let $H_m$ be a parity check matrix of the Hamming code $\mathcal{H}^n$ of length $n = 2^m - 1$. The columns in $H_m$ are all the nonzero vectors in $\mathbb{F}^m$, that is, the elements $\{\alpha^0, \alpha^1, \ldots, \alpha^{n-1}\}$, where $\alpha$ is a primitive element of $\mathbb{F}^m$. We can naturally associate, to each one of them, one element from the set $N = \{1, 2, \ldots, n\}$ as $\alpha^i \to i + 1$, $i = 0, 1, \ldots, n - 1$.

Let $F : \mathbb{F}^m \longrightarrow \mathbb{F}^m$ be a function such that $F(\mathbf{0}) = \mathbf{0}$. The function $F$ is called APN (*almost perfect nonlinear*) if all equations

$$F(x) + F(x + b) = a; \;\; a, b \in \mathbb{F}^m; \;\; b \neq \mathbf{0}, \tag{1}$$

have no more than two solutions in $\mathbb{F}^m$. In this paper, we consider APN permutations, that is, when the APN function $F : \mathbb{F}^m \longrightarrow \mathbb{F}^m$ is bijective, so it corresponds to a permutation $\pi_F \in \mathcal{S}_n$, where $n = 2^m - 1$. Let $H_F$ be the matrix

$$H_F = \begin{pmatrix} H_m \\ H_m^{(F)} \end{pmatrix} = \begin{pmatrix} \cdots & x & \cdots \\ \cdots & F(x) & \cdots \end{pmatrix}, \tag{2}$$

where $x \in \mathbb{F}^m$, $x \neq \mathbf{0}$, and let $\mathcal{C}_F$ be the linear code admitting $H_F$ as a parity check matrix. Note that $\mathcal{C}_F$ is a subcode of the Hamming code $\mathcal{H}^n$. Two functions $F, G : \mathbb{F}^m \longrightarrow \mathbb{F}^m$, with $rank(H_F) = rank(H_G) = 2m$, are *CCZ-equivalent* if and only if the extended codes $\mathcal{C}_F^*$ and $\mathcal{C}_G^*$ are equivalent [4, 8]. This equivalence relation has been used to classify APN functions, since if $F$ is an APN function and $G$ is CCZ-equivalent to $F$, then $G$ is also an APN function. Note that we will use $\circ$ to denote the function composition, that is, $(F \circ G)(x) = F(G(x))$.

In the last years, many new APN functions have been constructed [2,5,6, 10]. However, it is not always easy to prove that they are not CCZ-equivalent to any of the known ones. In order to help to distinguish them, up to CCZ-equivalence, some invariants have been defined [3,10].

A classical (block) $t$-$(n,k,\lambda)$ design is a set $N$ of $n$ elements together with a collection of blocks whose elements are $k$-subsets of $N$ such that every $t$-subset of points of $N$ is contained in exactly $\lambda$ blocks. A *Steiner triple system* of order $n$ (briefly STS$(n)$) is a 2-$(n,3,1)$ design, where the blocks will be called *triples*. Two STS$(n)$ or, in general, two designs, are called *isomorphic* if there is a permutation on the set of points such that blocks of one design are mapped to blocks of the other design. A STS$(n)$ exists if and only if $n \equiv 1$ or $3 \pmod 6$. It is well known that the supports of the codewords of weight 3 in any perfect code containing the all-zero vector define a Steiner triple system. For a Hamming code $\mathcal{H}^n$, the corresponding Steiner triple system is called *Hamming Steiner triple system* or *Boolean Steiner triple system* and denoted by STS$(\mathcal{H}^n)$. Note that since the Hamming code $\mathcal{H}^n$, for each $n = 2^m - 1$, is unique up to isomorphism, its Steiner triple system STS$(\mathcal{H}^n)$ is also unique up to isomorphism.

The relation between combinatorial designs and graph embeddings comes from the fact that when a graph is embedded in a surface, the faces that result can be regarded as the blocks of a design [12]. In the current paper, we consider the case of a complete graph with $n$ vertices, embedded into a closed surface in which all the faces are triangles. It is known [21] that this complete graph admits a triangulation of some orientable surface if and only if $n \equiv 0, 3, 4$ or $7 \pmod{12}$, and admits a triangulation of some nonorientable surface if and only if $n \equiv 0$ or $1 \pmod 3$ for $n > 7$. All necessary definitions concerning orientable and nonorientable surfaces could be found in [12,21].

A triangulation is called *face 2-colourable* if the triangular faces of an embedding into a surface can be properly 2-coloured (for example, in black and white colours), that is, in such a way that no two faces with a common edge have the same colour [21]. The case of 2-colourability is of special interest because all the triangles of the same colour on the surface induce an STS$(n)$. Therefore, we have two STS$(n)$ (black and white) *biembedded* in the surface. Such a pair of Steiner triple systems of order $n$ is called a *biembedding*. If these two STS$(n)$ are isomorphic, then it is called a *self-embedding*, and the corresponding permutation is called a *self-embedding permutation*.

If each one of the triples of a biembedding can be cyclically ordered so that every ordered pair of vertices is contained in precisely one cyclically ordered triple then the biembedding is *orientable* [22].

Two biembeddings are said to be *isomorphic* if there exists a permutation on the $n$ vertices (of the complete graph) such that it maps edges and triangles of one biembedding to edges and triangles of the other one either preserving the colour of the triangles or reversing it [13,14]. In the case when the colours of the triangles are preserved, the isomorphism is said to be *colour-preserving*.

For an embedding to be face 2-colourable, $n$ must be odd because the vertex degrees should be even. Therefore, for an orientable case, we have that $n \equiv 3$ or $7 \pmod{12}$, and it is known [21,22] that if a biembedding of a surface exists, the surface should be a sphere $S_g$ with $g = (n-4)(n-3)/12$ handles. On the other hand, for a nonorientable case, we have that $n \equiv 1$ or $3 \pmod 6$ for $n > 7$, and therefore a biembedding of a sphere $N_\gamma$ with $\gamma = (n-4)(n-3)/6$ crosscaps should exist [21,22].

The previous ideas about biembeddings in a closed surface (the sphere with $g$ handles or with $\gamma$ crosscaps) can be extended to pseudosurfaces, see for example [16]. A *pseudosurface* is the topological surface (allowing, in general, repeated triangles) which results when finitely many identifications, of finitely many points each, are made on a given surface. Specifically, distinct point $\{p_{i,j} : i = 1, 2, \ldots, k,\ j = 0, 1, \ldots, n_i\}$ on a given surface are identified to form points $p_i = \{p_{i,j} : j = 0, 1, \ldots, n_i\}$, $i = 1, 2, \ldots, k$, called *pinch points*. All necessary definitions and notions concerning embeddings in closed surfaces can be found in [12,21] and concerning embeddings in pseudosurfaces with pinch points in [12,16]. Throughout of what follows, when we refer to self-embeddings, we always mean self-embeddings in a pseudosurface in general (either a closed surface or pseudosurface with pinch points), and each time we emphasize if we just deal with a closed surface, that is, a pseudosurface without pinch points.

Despite the existence of many results devoted to embeddings of a complete graph in a closed surface or pseudosurface with pinch points, there still remain many unsolved problems, see the surveys [12,16]. For example, it is interesting to find self-embeddings in a closed surface for the Hamming Steiner triple system $\mathrm{STS}(\mathcal{H}^n)$ of order $n = 2^m - 1$, $m > 4$. For $n = 7$, it is well known that, up to isomorphism, the $\mathrm{STS}(\mathcal{H}^7)$ has only one self-embedding, which is a torus and, therefore, is orientable [21]. For $n = 15$, there are four nonisomorphic self-embeddings of $\mathrm{STS}(\mathcal{H}^{15})$, three of them are nonorientable and one is orientable [11]. On the other hand, in general, it is easy to obtain self-embeddings in a pseudosurface just taking any two isomorphic $\mathrm{STS}(\mathcal{H}^n)$, or in general any two isomorphic $\mathrm{STS}(n)$, on the same set $N$.

In this paper, we only consider self-embeddings, in closed surfaces and pseudosurfaces with pinch points, obtained from the Hamming Steiner triple systems $\mathrm{STS}(\mathcal{H}^n)$ of order $n = 2^m - 1$, $m > 4$, via monomial power permutations. We restrict ourselves to these permutations in order to develop techniques to find new self-embeddings in closed surfaces for these $\mathrm{STS}(\mathcal{H}^n)$ and investigate the connection between pseudosurfaces and APN functions which are also monomial power permutations.

The paper is organized as follows. In Section 1, we defined some notions of coding theory (specifically, Hamming codes and APN functions), design theory (specifically, Steiner triple systems), and graph embeddings into a surface or pseudosurface (specifically, self-embeddings for Hamming Steiner triple systems). In Section 2, we present self-embeddings in closed surfaces for the Hamming Steiner triple systems $\mathrm{STS}(\mathcal{H}^n)$, where $n = 2^m - 1$ and $m \in \{5, 7, 11, 13, 17, 19\}$, which, as far as we know, were not described before. Actually, we give all possible self-embeddings in a closed surface constructed from an $\mathrm{STS}(\mathcal{H}^n)$ and considering only monomial power permutations, for all

$m \leq 22$. Up to isomorphism, there are exactly 1, 1, 4, 14, 12, 65 and 88 such self-embeddings for $m = 3, 5, 7, 11, 13, 17, 19$, respectively. Note that for any non prime $m$, there are no such self-embeddings. We also point out which of all these self-embedding permutations are APN permutations. In Section 3, we focus on showing that the rotation line spectrum (defined below, in Section 2) for self-embeddings of Hamming Steiner triple systems in pseudosurfaces with pinch points can be used as an invariant to classify APN permutations. Actually, this invariant gives a complete classification of all APN monomial power permutations for all $m \leq 17$, up to CCZ-equivalence. Moreover, it could be used to classify any APN permutation, or in general, any permutation, not necessarily APN. Finally, in Section 4, we present some conclusions and further research.

## 2 Self-embeddings of STS($\mathcal{H}^n$) in closed surfaces

In this section, we construct new self-embeddings in closed surfaces for Hamming Steiner triple systems STS($\mathcal{H}^n$), where $n = 2^m - 1$ and $m \in \{5, 7, 11, 13, 17, 19\}$. Moreover, up to isomorphism, we give all possible such self-embeddings for the STS($\mathcal{H}^n$), with $m \leq 22$, constructed from monomial power permutations, together with their classification.

A design defined on the set $N$ is called *cyclic* if there is a permutation on the set $N$ consisting of a single cycle of length $n$ such that blocks are mapped to blocks. We consider a cyclic STS($\mathcal{H}^n$) corresponding to a cyclic version of the Hamming code $\mathcal{H}^n$ of length $n$ (for example, the one considered in the introduction). A self-embedding is called *cyclic* if there is a cyclic automorphism of order $n$ which necessarily extends to the two STS($\mathcal{H}^n$) and $F$(STS($\mathcal{H}^n$)) conforming the self-embedding.

It is easy to see that there is only one self-embedding in a closed surface for the cyclic STS($\mathcal{H}^7$) via the permutation corresponding to the monomial power function $F(x) = x^3$ over $\mathbb{F}^3$. For $n = 15$, none of the four nonisomorphic self-embeddings of STS($\mathcal{H}^{15}$) classified in [11] are cyclic, so there are no self-embeddings in a closed surface for the cyclic STS($\mathcal{H}^{15}$) given by monomial power permutations. For $n = 31$, Bennett at al. proved that there is not any cyclic orientable self-embedding in a closed surface for the STS($\mathcal{H}^{31}$) [1]. It is still an open question to determine whether there exist noncyclic orientable self-embeddings in a closed surface for the STS($\mathcal{H}^{31}$) or not. In this section, we present new self-embeddings for the cyclic STS($\mathcal{H}^n$) with $n = 2^m - 1$, which are cyclic for all $m$ and nonorientable at least for all $m \leq 19$.

Note that there are STS($n$) which are not isomorphic to the STS($\mathcal{H}^n$) but also have permutations without fixed points in their automorphism group. For example, the STS($n$) given by the well known Bose construction [15] has an automorphism group containing a permutation with three short cycles of length $n/3$. An interesting fact is that Bose STS(15) can not be included in any perfect code of length 15, see [18]. There are several constructions of self-embeddings for the STS($n$) obtained from the Bose construction, orientable and nonorientable [12,21,23].

In order to construct these mentioned new self-embeddings in a closed surface for the cyclic STS($\mathcal{H}^n$), we only consider permutations $\pi_F \in \mathcal{S}_n$, where $n = 2^m - 1$, given by monomial power functions $F(x) = x^t$ over $\mathbb{F}^m$, so such that $\gcd(t, n) = 1$. The next proposition shows us that these constructed self-embeddings are cyclic.

**Proposition 1** *Let STS($\mathcal{H}^n$) be cyclic with the permutation $\phi \in \mathcal{S}_n$, defined by $\phi(i) = i + 1 \pmod{n}$. Let $F : \mathbb{F}^m \longrightarrow \mathbb{F}^m$ be any monomial power permutation. Then, the self-embedding for STS($\mathcal{H}^n$) given by the permutation $F$ is also cyclic.*

*Proof* Let $\alpha$ be a primitive element of the finite field $\mathbb{F}^m$. For any triple $(\alpha^i, \alpha^j, \alpha^k)$ from the cyclic STS($\mathcal{H}^n$) corresponding to the Hamming code with parity check matrix $H_m = (\alpha^0\, \alpha^1\, \dots\, \alpha^{n-1})$, we have that $F(\alpha^i, \alpha^j, \alpha^k) = (\alpha^{it}, \alpha^{jt}, \alpha^{kt})$ is a triple in $F(\text{STS}(\mathcal{H}^n))$, where $F(x) = x^t$. Moreover, the triple $(\alpha^{it+1}, \alpha^{jt+1}, \alpha^{kt+1})$ is again in $F(\text{STS}(\mathcal{H}^n))$. Indeed, since $\gcd(t, n) = 1$, there exists $t'$ such that $tt' \equiv 1 \pmod{n}$, and we have $(\alpha^{it+1}, \alpha^{jt+1}, \alpha^{kt+1}) = (\alpha^{(i+t')t}, \alpha^{(j+t')t}, \alpha^{(k+t')t}) = F(\alpha^{i+t'}, \alpha^{j+t'}, \alpha^{k+t'})$. Therefore, since the triple $(\alpha^{i+t'}, \alpha^{j+t'}, \alpha^{k+t'})$ is in STS($\mathcal{H}^n$), we proved the statement. □

In general, a biembedding in a pseudosurface has a pinch point if and only if there is a point $i \in N$ such that the cyclically ordered points of all triples containing $i$ in both black and white STS($n$) can be divided into more than one cycle. Each one of these cycles is called *rotation line* at point $i \in N$ [21]. Note that a biembedding in a closed surface has no pinch points, so the rotation line at each point contains a single cycle of length $n-1$. We collect all rotation lines at point $i \in N$ taking them in any order. The number of rotation lines at point $i \in N$ will be denoted by $rl(i)$. A biembedding in a closed surface can be considered as a biembedding in a pseudosurface such that $rl(i) = 1$ for any $i \in N$. The set of rotation lines at all the points of $N$ is called the *rotation scheme* for the biembedding.

The next proposition gives us an alternative definition for a self-embedding permutation in a closed surface for an STS($\mathcal{H}^n$). Given an STS($\mathcal{H}^n$), where $n = 2^m - 1$, if $(a, b, c)$ is a triple in STS($\mathcal{H}^n$), then we have that $a + b = c$, considering the corresponding columns in $H_m$ as elements in $\mathbb{F}^m \backslash \{\mathbf{0}\}$. Note that, from now on, we will use indistinctly the vectors in $\mathbb{F}^m \backslash \{\mathbf{0}\}$ as elements (points) of the STS($\mathcal{H}^n$) and vice versa.

**Proposition 2** *Let $F$ be any bijective function over $\mathbb{F}^m$ such that $F(\mathbf{0}) = \mathbf{0}$. The permutation $F$ is a self-embedding permutation in a closed surface for the STS($\mathcal{H}^n$) if and only if, for any $a \in \mathbb{F}^m \backslash \{\mathbf{0}\}$, the elements in the sequence $a_1, a_2, \dots, a_{2^{m-1}-1}$ are different elements in $\mathbb{F}^m$, where $a_1$ is any element in $\mathbb{F}^m \backslash \{\mathbf{0}\}$ such that $a_1 \neq a$ and $a_{i+1} = F(F^{-1}(a) + F^{-1}(a + a_i))$ for all $i \in \{1, \dots, 2^{m-1} - 2\}$.*

*Proof* Given the self-embedding permutation $F$ in a closed surface, the rotation line at any element $a \in \mathbb{F}^m\backslash\{\mathbf{0}\}$ is a sequence of $2^m - 2$ different elements:

$$[a_1, a + a_1; a_2, a + a_2; \dots; a_{2^{m-1}-1}, a + a_{2^{m-1}-1}],$$

where $a_1$ is any element in $\mathbb{F}^m\backslash\{\mathbf{0}\}$ such that $a_1 \neq a$, and $(a, a_i, a+a_i)$ is a triple in STS$(\mathcal{H}^n)$ for all $i \in \{1, \dots, 2^{m-1} - 1\}$. Note that $F(\text{STS}(\mathcal{H}^n))$ is a Steiner triple system isomorphic to STS$(\mathcal{H}^n)$. Moreover, the blocks in $F(\text{STS}(\mathcal{H}^n))$ can be seen as the triples $(a, b, F(F^{-1}(a) + F^{-1}(b)))$, where $+$ stands for the operation defined above for the STS$(\mathcal{H}^n)$. Therefore, for all $i \in \{1, \dots, 2^{m-1} - 2\}$, taking $b = a + a_i$, we have that $a_{i+1} = F(F^{-1}(a) + F^{-1}(a + a_i))$.

The converse is straightforward using the same argumentation. □

We have used Proposition 2 to find new self-embedding permutations in closed surfaces for the cyclic STS$(\mathcal{H}^n)$, where $n = 2^m - 1$ with $m \leq 22$. Note that, considering permutations $\pi_F \in \mathcal{S}_n$ given by a monomial power function $F(x) = x^t$ over $\mathbb{F}^m$ such that $\gcd(t, n) = 1$, it is only necessary to check the condition for just one element $a \in \mathbb{F}^m\backslash\{\mathbf{0}\}$.

For any self-embedding of STS$(\mathcal{H}^n)$ given by a permutation $F : \mathbb{F}^m \longrightarrow \mathbb{F}^m$ with $F(\mathbf{0}) = \mathbf{0}$, and any element $a \in \mathbb{F}^m\backslash\{\mathbf{0}\}$, we can construct the sequence $a_1, a_2, \dots, a_{r_1}$ beginning with any element $a_1 \in \mathbb{F}^m\backslash\{\mathbf{0}\}$ such that $a_1 \neq a$ and $a_{r_1+1} = a_1$, where

$$a_{i+1} = F(F^{-1}(a) + F^{-1}(a + a_i)). \tag{3}$$

Let $b_i$ be the element in $\mathbb{F}^m\backslash\{\mathbf{0}\}$ such that $(a, a_i, b_i)$ is a triple for all $i \in \{1, \dots, r_1\}$. Then, the sequence $R_1 = [a_1, b_1; a_2, b_2; \dots; a_{r_1}, b_{r_1}]$ defines a rotation line at point $a$. If the rotation line $R_1$ does not cover all elements in $\mathbb{F}^m\backslash\{\mathbf{0}\}$, we take an element out of the rotation line and construct another rotation line $R_2$ beginning with this point, and so on. Finally, we obtain a partition of all elements in $\mathbb{F}^m\backslash\{\mathbf{0}, a\}$ in different rotation lines $R_1, R_2, \dots, R_s$, where $s = rl(a)$. We simplify this information considering only the number of rotation lines and the cardinal of each one of them. In this sense, the *rotation line spectrum* at point $a$ is defined as the array

$$(s; rl(a)_1, rl(a)_2, \dots, rl(a)_s), \tag{4}$$

where $s = rl(a)$ is the number of rotation lines at point $a$, and $rl(a)_i = |R_i|$ for all $i \in \{1, \dots, s\}$. Note that the rotation line spectrum of a self-embedding permutation in a closed surface for the STS$(\mathcal{H}^n)$ is $(1; n-1)$, where $n = 2^m - 1$.

**Example 1** For $m = 5$, consider the cyclic STS$(\mathcal{H}^{31})$ corresponding to the cyclic Hamming code with parity check matrix $H_5 = (1\ \alpha\ \alpha^2\ \dots\ \alpha^{30})$, where $\alpha$ is a primitive element of the finite field $GF(32) = \mathbb{F}[x]/(x^5 + x^2 + 1)$.

The permutation $\pi_F = (2, 26, 6)(3, 20, 11)(4, 14, 16)(5, 8, 21)(7, 27, 31)(9, 15, 10)(12, 28, 25)(13, 22, 30)(17, 29, 19)(18, 23, 24) \in \mathcal{S}_{31}$, which corresponds to the bijective function $F(x) = x^5$ over $\mathbb{F}^5$, is a self-embedding permutation in a closed surface for the STS($\mathcal{H}^{31}$). The rotation line at point 1 is given by the sequence

$$\begin{aligned} R_1 =&[2,19;31,18;22,26;17,10;16,25;27,29;9,21;\\ &24,13;14,15;5,11;28,7;23,8;3,6;30,4;12,20], \end{aligned} \tag{5}$$

so the rotation line spectrum is $(1;30)$.

On the other hand, the permutation corresponding to the function $F(x) = x^3$ over $\mathbb{F}^5$ is a self-embedding permutation in a pseudosurface with pinch points for the STS($\mathcal{H}^{31}$). Note that in this case there are two rotation lines at point 1 given by the sequences

$$\begin{aligned} R_1 =&[2,19;5,11;17,10;3,6;9,21],\\ R_2 =&[27,29;24,13;12,20;31,18;14,15;28,7;22,26;16,25;23,8;30,4], \end{aligned} \tag{6}$$

so the rotation line spectrum is $(2;10,20)$. □

For any self-embedding of STS($\mathcal{H}^n$) given by a permutation $F : \mathbb{F}^m \longrightarrow \mathbb{F}^m$ with $F(\mathbf{0}) = \mathbf{0}$, we can calculate how many different values there are in the set $\{x + F^{-1}(a + F(x)) \,:\, x \in \mathbb{F}^m\}$ for any $a \in \mathbb{F}^m \backslash \{\mathbf{0}\}$. Let

$$v_F(a) = |\{x + F^{-1}(a + F(x)) \,:\, x \in \mathbb{F}^m\}|. \tag{7}$$

We can also calculate the multiset $\tilde{V}_F(a) = \{z_i : i \in \{1, \dots, 2^{m-1} - 1\}\}$, where $\{(a, a_i, a + a_i) : i \in \{1, \dots, 2^{m-1} - 1\}\}$ is the set of all triples in STS($\mathcal{H}^n$) containing the point $a$ and $(a_i, a + a_i, z_i)$ are triples in $F$(STS($\mathcal{H}^n$)) for all $i \in \{1, \dots, 2^{m-1} - 1\}$. Let $V_F(a)$ be the set associated to $\tilde{V}_F(a)$, and let $V_F^*(a)$ be the multiset containing the multiplicities of the different elements in $\tilde{V}_F(a)$. We denote by $x^\wedge s$ the elements in $V_F^*(a)$, understanding that we have $s$ different elements in $\tilde{V}_F(a)$ appearing $x$ times. In the following lemma, we give the connection between $v_F(a)$ and $V_F(a)$, and then we show these definitions by Example 2.

**Lemma 1** *Let $F$ be any bijective function over $\mathbb{F}^m$ such that $F(\mathbf{0}) = \mathbf{0}$, and let $S = STS(\mathcal{H}^n)$. If $S \cup F(S)$ is a self-embedding, then $v_F(a) = 1 + |V_F(a)|$ for any $a \in \mathbb{F}^m \backslash \{\mathbf{0}\}$.*

*Proof* We have that $\{x + F^{-1}(a + F(x)) \,:\, x \in \mathbb{F}^m\} = \{F^{-1}(y) + F^{-1}(a + F(F^{-1}(y))) \,:\, y \in \mathbb{F}^m\} = \{F^{-1}(y) + F^{-1}(a + y) \,:\, y \in \mathbb{F}^m\}$, where $y = F(x)$. Therefore,

$$v_F(a) = |\{F^{-1}(a)\} \cup \{F^{-1}(z_i) : i \in \{1, \dots, 2^{m-1} - 1\}|, \tag{8}$$

where $z_i = F(F^{-1}(a_i) + F^{-1}(a + a_i))$ and $a_1, a + a_1; a_2, a + a_2; \dots; a_{2^{m-1}-1}, a + a_{2^{m-1}-1}$ is the sequence containing all the rotation lines at point $a$. Note that regardless having a self-embedding in a closed surface or pseudosurface with pinch points, we just consider the triples $(a_i, a + a_i, z_i)$, for all $i \in \{1, \dots, 2^{m-1} - 1\}$, which are blocks in $F(S)$. Moreover, since $a \neq z_i$ for all $i \in \{1, \dots, 2^{m-1} - 1\}$ and $F$ is bijective, $F^{-1}(a) \neq F^{-1}(z_i)$. Therefore, from (8) and the definition of $V_F(a)$, we have $v_F(a) = 1 + |\{F^{-1}(z_i) : i \in \{1, \dots, 2^{m-1} - 1\}| = 1 + |\{z_i : i \in \{1, \dots, 2^{m-1} - 1\}| = 1 + |V_F(a)|$. □

**Example 2** Consider the cyclic STS($\mathcal{H}^{127}$) corresponding to the cyclic Hamming code with parity check matrix $H_7 = (1\ \alpha\ \alpha^2\ \ldots\ \alpha^{126})$, where $\alpha$ is a primitive element of the finite field $GF(128) = \mathbb{F}[x]/(x^7 + x + 1)$.

For the self-embedding in a closed surface, given by the permutation $F(x) = x^7$ over $\mathbb{F}^7$, we have that

$$\begin{aligned}\tilde{V}_F(1) = &\{109, 43, 17, 28, 56, 40, 103, 82, 64, 78, 38, 3, 52, 119, 117, 109\\ &27, 120, 90, 85, 33, 55, 111, 79, 78, 36, 127, 28, 75, 5, 103, 110,\\ &106, 90, 53, 112, 52, 42, 65, 109, 94, 30, 28, 71, 126, 55, 22, 9,\\ &78, 92, 84, 52, 105, 96, 103, 83, 2, 90, 60, 59, 55, 14, 124\},\end{aligned}$$

since the rotation line at point 1 is $R_1 = [2{,}8; 91{,}10; 74{,}79; \ldots; 36{,}110]$ and (2,8,109), (91,10,43), (74,79,17),…,(36,110,124) are triples in $F$(STS($\mathcal{H}^{127}$)). Therefore, by Lemma 1 (see also Table 3),

$$v_F(1) = 1 + |V_F(1)| = 50 \quad \text{and} \quad V_F^*(1) = \{1^\wedge 42, 3^\wedge 7\}.\square$$

**Lemma 2** *Let $F$ be any bijective function over $\mathbb{F}^m$ such that $F(\mathbf{0}) = \mathbf{0}$, and let $S = STS(\mathcal{H}^n)$. If $S \cup F(S)$ is a self-embedding, then $S \cup F(S)$ and $S \cup F^{-1}(S)$ are isomorphic.*

*Proof* It is easy to check that the permutation $F$ transforms the triples from $S$ into the triples in $F(S)$ and the triples from $F^{-1}(S)$ into the triples in $S$. $\square$

**Theorem 1** *Let $F_1, F_2$ be two bijective functions over $\mathbb{F}^m$ such that $F_1(\mathbf{0}) = F_2(\mathbf{0}) = \mathbf{0}$, and let $S = STS(\mathcal{H}^n)$. If $S \cup F_1(S)$ and $S \cup F_2(S)$ are isomorphic self-embeddings, then*

$$\{v_{F_1}(a) : a \in \mathbb{F}^m \backslash \{\mathbf{0}\}\} = \{v_{F_2}(a) : a \in \mathbb{F}^m \backslash \{\mathbf{0}\}\}, \ \textit{and}$$

$$\{V_{F_1}^*(a) : a \in \mathbb{F}^m \backslash \{\mathbf{0}\}\} = \{V_{F_2}^*(a) : a \in \mathbb{F}^m \backslash \{\mathbf{0}\}\}.$$

*Proof* By Lemma 2, it is enough to assume that the isomorphism is given by a function $F$ transforming triples into triples such that $F(S) = S$ and $F(F_1(S)) = F_2(S)$. Looking at the points as vectors in $\mathbb{F}^m \backslash \{\mathbf{0}\}$, we can consider the function $F$ as a linear transformation on $\mathbb{F}^m$.

The elements in the set $V_{F_1}(a)$ are $F_1^{-1}(z_i)$, for $i \in \{1, \ldots, 2^{m-1}-1\}$, where $z_i = F_1(F_1^{-1}(a_i) + F_1^{-1}(a + a_i))$ and $(a_i, a + a_i, z_i)$ are the triples in $F_1(S)$. For any triple $(a_i, a + a_i, z_i)$ in $F_1(S)$, we have that $(F_2(F_1^{-1}(a_i)), F_2(F_1^{-1}(a + a_i)), F_2(F_1^{-1}(z_i)))$ is a triple in $F_2(S)$ and so, as $F_2 \circ F_1^{-1} = F$, we see that $(F(a_i), F(a + a_i), F(z_i)) = (F(a_i), F(a) + F(a_i), F(z_i))$ are the corresponding triples in $F_2(S)$. Since $F$ is bijective, we conclude that $\tilde{V}_{F_1}(a) = \tilde{V}_{F_2}(F(a))$, $V_{F_1}^*(a) = V_{F_2}^*(F(a))$ and using Lemma 1 we obtain $v_{F_1}(a) = v_{F_2}(F(a))$ for all $a \in \mathbb{F}^m \backslash \{\mathbf{0}\}$. Therefore, the result follows. $\square$

**Proposition 3** *Let $F : \mathbb{F}^m \longrightarrow \mathbb{F}^m$ be any monomial power permutation, and let $S = STS(\mathcal{H}^n)$. If $S \cup F(S)$ is a self-embedding, then the parameters $v_F(a)$ and $V_F^*(a)$ do not depend on the choice of $a \in \mathbb{F}^m \backslash \{\mathbf{0}\}$, that is, $v_F(a) = v_F(1)$ and $V_F^*(a) = V_F^*(1)$ for all $a \in \mathbb{F}^m \backslash \{\mathbf{0}\}$.*

*Proof* If $F$ is a monomial power permutation, then at each point $a \in \mathbb{F}^m \backslash \{\mathbf{0}\}$ the rotation line is the same, up to a permutation and so $\tilde{V}_F(a)$ and $\tilde{V}_F(1)$ also coincide, up to a permutation. Finally, by the definitions of $v_F(a)$, $V_F^*(a)$ and Lemma 1, the result follows. □

**Example 3** For the self-embedding permutation in a closed surface, given by the permutation $F(x) = x^5$ over $\mathbb{F}^5$ defined in Example 1, we have that

$$\tilde{V}_F(1) = V_F(1) = \{23, 30, 5, 12, 31, 3, 22, 16, 2, 27, 24, 17, 14, 28, 9\}$$

since the rotation line at point 1 is $R_1$ given in (5), and the triples $(2, 19, 23)$, $(31, 18, 30)$, $(22, 26, 5)$, $(17, 10, 12)$, $(16, 25, 31)$, $(27, 29, 3)$, (9,21,22),(24,13,16), $(14, 15, 2)$, $(5, 11, 27)$, $(28, 7, 24)$, $(23, 8, 17)$, $(3, 6, 14)$, $(30, 4, 28)$, $(12, 20, 9)$ are in $F(\mathrm{STS}(\mathcal{H}^{31}))$.

Therefore,

$$v_F(1) = 1 + |V_F(1)| = 16 \quad \text{and} \quad V_F^*(1) = \{1\hat{}15\}.$$

Finally, by Proposition 3, $v_F(a) = v_F(1) = 16$ and $V_F^*(a) = V_F^*(1) = \{1\hat{}15\}$ for all $a \in \mathbb{F}^m \backslash \{\mathbf{0}\}$.

For the self-embedding in a pseudosurface with pinch points, given by the permutation $F(x) = x^3$ over $\mathbb{F}^5$ defined in Example 1, we also have that $v_F(a) = v_F(1) = 16$ and $V_F^*(a) = V_F^*(1) = \{1\hat{}15\}$ for all $a \in \mathbb{F}^m \backslash \{\mathbf{0}\}$. □

Note that $v_F(a)$ is maximum when all the elements in $\tilde{V}_F(a)$ are different, that is, when $v_F(a) = 2^{m-1}$. For both permutations in the previous example, $v_F(a)$ is maximum for all $a \in \mathbb{F}^m \backslash \{\mathbf{0}\}$. Therefore, by Proposition 6 (see Section 3, where we investigate the connection between APN functions and self-embeddings), they are APN permutations.

By Theorem 1, we have that the sets $\{v_F(a) : a \in \mathbb{F}^m \backslash \{\mathbf{0}\}\}$ and $\{V_F^*(a) : a \in \mathbb{F}^m \backslash \{\mathbf{0}\}\}$ can be used as invariants to distinguish nonisomorphic self-embedding permutations $F$. By Proposition 3, note that considering monomial power permutations, it is only necessary to compute $v_F(a)$ and $V_F^*(a)$ for one element $a \in \mathbb{F}^m \backslash \{\mathbf{0}\}$, for example $a = 1$. Let $v_F = v_F(1)$ and $V_F^* = V_F^*(1)$. We further use these invariants to classify the found self-embedding permutations in closed surfaces.

Let $C_i$ be the (binary) cyclotomic coset containing $i$, that is, the set of integers $C_i = \{i, 2i, 4i, \dots, 2^{m_i - 1} i\}$, where $m_i$ is the smallest positive integer such that $2^{m_i} \cdot i \equiv i \pmod{2^m - 1}$ [17]. The cyclotomic cosets give a partition of the integers modulo $2^m - 1$ into disjoint subsets. Let $C_i^*$ be the union of the cyclotomic coset containing $i$ and the cyclotomic coset containing the multiplicative inverse of $i$ modulo $2^m - 1$. Note that in some cases the set $C_i^*$ coincides with $C_i$, for example, $C_1^* = C_1 = \{1, 2, 4, \dots, 2^{m-1}\}$.

The following result demonstrates that if $t_1$ and $t_2$ are in the same set $C_i^*$, the self-embedding permutations corresponding to $F_1(x) = x^{t_1}$ and $F_2(x) = x^{t_2}$ are isomorphic and have the same parameters $V_{F_1}^*(a) = V_{F_2}^*(a) = V^*$ and $v_{F_1}(a) = v_{F_2}(a) = v$, which are fixed for all $a \in \mathbb{F}^m \backslash \{\mathbf{0}\}$.

**Proposition 4** *Let* $F_1, F_2 : \mathbb{F}^m \longrightarrow \mathbb{F}^m$ *be two monomial power permutations* $F_1(x) = x^{t_1}$ *and* $F_2(x) = x^{t_2}$ *such that* $t_1, t_2 \in C_i^*$, *and let* $S = STS(\mathcal{H}^n)$. *If* $S \cup F_1(S)$ *and* $S \cup F_2(S)$ *are two self-embeddings, then they are isomorphic,* $V_{F_1}^*(a) = V_{F_2}^*(a) = V^*$ *and* $v_{F_1}(a) = v_{F_2}(a) = v$ *for all* $a \in \mathbb{F}^m \backslash \{\mathbf{0}\}$.

*Proof* The Frobenius automorphisms $F(x) = x^{2^s}$ over $\mathbb{F}^m$, for $s \in \{1, 2, \ldots, m-1\}$, are well-known examples of permutations $\pi_F \in \mathcal{S}_n$ transforming $S = \mathrm{STS}(\mathcal{H}^n)$ into itself. Indeed, the triples $(a, b, c)$ of $S$ are such that $a + b = c$, where $a, b, c \in \mathbb{F}^m \backslash \{\mathbf{0}\}$, so $(a + b)^{2^s} = a^{2^s} + b^{2^s} = c^{2^s}$ giving that $(F(a), F(b), F(c))$ are also triples in $S$.

Let $t_1 \in C_i$ and $t_2 \in C_i$. Using a Frobenius automorphism $F(x) = x^{2^s}$ for some $s \in \{1, 2, \ldots, m-1\}$, we have that $F_2 = F \circ F_1$. Therefore, the two self-embeddings $S \cup F_1(S)$ and $S \cup F_2(S)$ are isomorphic.

Let $t_1 \in C_i$ and $t_2 \in C_j$, where $C_i$ and $C_j$ are the inverse cyclotomic cosets such that $C_i^* = C_i \cup C_j$. Up to a Frobenius automorphism $F(x) = x^{2^s}$ for some $s \in \{1, 2, \ldots, m-1\}$, we can assume that $t_1$ is the multiplicative inverse of $t_2$ modulo $2^m - 1$. Hence, $(x^{t_1})^{t_2} = x$, which means that $F_2(F_1(x)) = x$, and the corresponding permutations $\pi_{F_1}$ and $\pi_{F_2}$ satisfy $\pi_{F_2} = \pi_{F_1}^{-1}$. Therefore, in general, $F_2 = F_1^{-1} \circ F$, and again the two self-embeddings $S \cup F_1(S)$ and $S \cup F_2(S)$ are isomorphic.

Finally, by Theorem 1 and Proposition 3, we have that $V_{F_1}^*(a) = V_{F_2}^*(a) = V^*$ and $v_{F_1}(a) = v_{F_2}(a) = v$ for all $a \in \mathbb{F}^m \backslash \{\mathbf{0}\}$. $\square$

**Proposition 5** *For any non prime* $m$, *there is not any self-embedding in a closed surface for the* $STS(\mathcal{H}^n)$ *given by a monomial power permutation.*

*Proof* Let us assume there is a self-embedding in a closed surface for the $\mathrm{STS}(\mathcal{H}^n)$ given by a permutation $F(x) = x^t$, that is, such that $\gcd(t, n) = 1$, where $n = 2^m - 1$.

Let $m'$ be a divisor of $m$ such that $1 < m' < m$. Then, $n' = 2^{m'} - 1$ divides $n = 2^m - 1$. Let $b = n/n'$ and $\alpha$ be a primitive element in $\mathbb{F}^m$. Hence, $\alpha^b$ is a primitive element in a subfield $K \subset \mathbb{F}^m$ of $2^{m'}$ elements. Since $F$ is a permutation, $\gcd(t, n) = 1$, and we have that $F(\alpha^b) = \alpha^{tb}$ generates a finite field of $2^{m'}$ elements which coincides with $F(K) \subset \mathbb{F}^m$.

We will prove the statement by contradiction. We can construct the rotation line at point 1 as

$$[a_1, 1 + a_1; a_2, 1 + a_2; \ldots; a_{2^{m-1}-1}, 1 + a_{2^{m-1}-1}],$$

where $a_1 \neq 1$ is any element in $\mathbb{F}^m \backslash \{0\}$, $(1, a_i, a_i + 1)$ is a triple in $\mathrm{STS}(\mathcal{H}^n)$ and $a_{i+1} = F(F^{-1}(1) + F^{-1}(1 + a_i))$ by (3). Then, we can consider $a_1 = \alpha^{tb} \in F(K)$. Therefore, $a_{i+1} \in F(K)$ for $i = 1, 2, \ldots, 2^{m-1} - 2$. All these elements $a_i$, together with the element 1 and the elements $1 + a_i$, for all $i = 1, 2, \ldots, 2^{m-1} - 1$, should give us all the elements in $\mathbb{F}^m$, by Proposition 2. However, these elements belong to $F(K) \backslash \{\mathbf{0}\}$ and, since $|F(K)| = 2^{m'}$ and $m' < m$, this leads to a contradiction. $\square$

**Theorem 2** *For* $m \in \{3, 5, 7, 11, 13, 17, 19\}$*, up to isomorphism, there are exactly 1, 1, 4, 14, 12, 65 and 88 self-embedding monomial power permutations in closed surfaces for the STS(*$\mathcal{H}^n$*), where* $n = 2^m - 1$*, respectively. Moreover, at least for all* $5 \leq m \leq 19$ *these self-embeddings are nonorientable.*

*Proof* Using Proposition 2 and the Magma software package [7], we found all self-embedding permutations for the $\mathrm{STS}(\mathcal{H}^n)$ in closed surfaces, where $n = 2^m - 1$ and $m \leq 19$, given by monomial power permutations, $F(x) = x^t$ over $\mathbb{F}^m$ such that $\gcd(t, n) = 1$. We also computed the parameter $v_F(a)$ for all found self-embedding permutations $F$ and all $a \in \mathbb{F}^m \backslash \{\mathbf{0}\}$. By Propositions 3 and 4, we just had to compute $v_F$ for one representative element of the set $C_t^*$. In Appendix (Tables 1 and 2), all these values are listed. By Proposition 5, for any non prime $m$, there is not any self-embedding monomial power permutation in a closed surface.

Since the parameter $v_F$ is an invariant, by Theorem 1, the self-embeddings having different parameters $v_F$ in Tables 1 and 2 are nonisomorphic. For $m = 3$ and $m = 5$, this parameter gives a complete classification, since there is only one class. It is well known that the case $F(x) = x^3$ for $m = 3$ is the torus given by $\mathrm{STS}(\mathcal{H}^7)$. For $m = 7$, there are at most 4 classes of nonisomorphic such self-embeddings. Since the self-embedding permutations $F_1(x) = x^7$ and $F_2(x) = x^{21}$ have the same parameter $v_{F_1} = v_{F_2} = 50$, we can not assure whether they are isomorphic or not. However, using Magma, it is easy to check that the corresponding self-embeddings are not isomorphic, so there are exactly 4 classes of nonisomorphic such self-embeddings.

For the classes having the same parameter $v_F$, we computed $V_F^*$, which is also an invariant, by Theorem 1. For $m = 11$, the self-embedding permutations given by $F_1(x) = x^{21}$ and $F_2(x) = x^{687}$ over $\mathbb{F}^{11}$ have the same parameters $v_{F_1} = v_{F_2} = 815$, and $V_{F_1}^* = V_{F_2}^* = \{1\hat{}628, 2\hat{}165, 3\hat{}22\}$. However, using Magma, we checked that the weight distributions of codes $\mathcal{C}_{F_1}$ and $\mathcal{C}_{F_2}$ are different and, by Proposition 7, we can conclude that the two self-embeddings are nonisomorphic. On the other hand, for the self-embedding permutations $F_1(x) = x^{73}$ and $F_2(x) = x^{165}$ over $\mathbb{F}^{11}$, which also have the same parameter $v_{F_1} = v_{F_2} = 826$, just using that $V_{F_1}^* \neq V_{F_2}^*$, we have that they are nonisomorphic. Therefore, there are exactly 14 nonisomorphic such self-embeddings. For $m = 13, 17$ and 19, Tables 3 and 4 show the parameter $V_F^*$ for the sets $C_t^*$ having the same parameter $v_F$ in Tables 1 and 2. Note that all classes can be distinguish, either using just the invariant $v_F$ or using also the invariant $V_F^*$.

In order to check the nonorientability, we can start taking all the glued triples corresponding to the rotation line for the element 1. Then, we take any element $x \neq 1$ and glue all the triples having the element $x$ in the first chosen set of triples. After that, we check whether there is an ordered pair $(u, v)$ such that the triple $(x, u, v) \in \mathrm{STS}(\mathcal{H}^n)$ and $(1, u, v) \in F(\mathrm{STS}(\mathcal{H}^n))$ (or vice versa $(1, u, v) \in \mathrm{STS}(\mathcal{H}^n)$ and $(x, u, v) \in F(\mathrm{STS}(\mathcal{H}^n))$). If we obtain this property, then the surface is nonorientable. Finally, the computer search using the Magma software package showed that the obtained self-embeddings are nonorientable at least for all $m \leq 19$. Therefore, the result follows. □

As far as we know, all found self-embedding permutations in closed surfaces given by Theorem 2 are new with the exception of the one given for $m = 3$. By Proposition 1, these self-embeddings are cyclic for all $m$.

Moreover, note that for every $m \in \{3, 5, 7, 11, 17\}$, there exists a cyclotomic coset $C_i^*$ such that for all permutations $F(x) = x^t$ with $t \in C_i^*$, $v_F = 2^{m-1}$ is maximum, so the corresponding self-embedding permutations are also APN. In Table 1, we point out these cases with $(\cdot)^{APN}$. Note that for any non prime $m$ and for $m \in \{13, 19\}$ there are no APN self-embeddings in a closed surface.

## 3 Self-embeddings of STS($\mathcal{H}^n$) and APN permutations

This section deals with APN permutations, which can be seen as self-embeddings permutations in a pseudosurface without triples in common. Given an APN function $F$, the corresponding code $\mathcal{C}_F$ has minimum distance 5. In fact, $F$ is an APN function if and only if $\mathcal{C}_F$ has minimum distance 5 [8]. Therefore, since $\mathcal{C}_F = \mathcal{H}^n \cap \pi_F(\mathcal{H}^n)$, any APN permutation $F$ gives two nonintersecting Hamming Steiner triple systems, STS($\mathcal{H}^n$) and $F$(STS($\mathcal{H}^n$)), which can be seen as a self-embedding in a closed surface or in a pseudosurface with pinch points (and without triples in common).

As in the previous section, we consider the (cyclic) Hamming Steiner triple system STS($\mathcal{H}^n$) and permutations $\pi_F \in \mathcal{S}_n$, where $n = 2^m - 1$, given by monomial power functions $F(x) = x^t$ over $\mathbb{F}^m$, so such that $\gcd(t, n) = 1$. In this case, we show that the rotation line spectrum of the corresponding self-embeddings in pseudosurfaces can be used as an invariant to distinguish between classes of APN permutations or, in general, to classify permutations. Moreover, we see that the rotation line spectrum gives a complete classification of monomial power permutations up to CCZ-equivalence, at least for all $m \leq 17$, so we can say that this classification coincides with the one given by the self-embedding isomorphism. Actually, the invariants $v_F$ and $V_F^*$ given in Section 2, can be also used to distinguish between CCZ-equivalent classes of monomial power permutations, not necessarily APN.

The next proposition gives a characterization of the APN permutations using the parameter $v_F(a)$, defined in the previous section for all $a \in \mathbb{F}^m \backslash \{\mathbf{0}\}$.

**Proposition 6** *Let $F$ be any bijective function over $\mathbb{F}^m$ such that $F(\mathbf{0}) = \mathbf{0}$. The permutation $F$ is APN if and only if, for all $a \in \mathbb{F}^m \backslash \{\mathbf{0}\}$, we have that $v_F(a) = 2^{m-1}$.*

*Proof* Given $a \in \mathbb{F}^m \backslash \{\mathbf{0}\}$, assume that $v_F(a) = |\{x + F^{-1}(a + F(x)) : x \in \mathbb{F}^m\}| = 2^{m-1}$. This means that there are $2^{m-1}$ different values $b \in \mathbb{F}^m \backslash \{\mathbf{0}\}$, such that the equation

$$x + F^{-1}(a + F(x)) = b \tag{9}$$

has two solutions, and there is no solution for the other values of $b$. Since (9) is equivalent to (1), $F$ is an APN permutation.

Vice versa, assume that $F$ is an APN permutation, and the values $x + F^{-1}(a + F(x))$ are not all different (up to a multiplicity of two), for a fixed $a \in \mathbb{F}^m \backslash \{\mathbf{0}\}$. Hence, there exists a value $b \neq \mathbf{0}$ such that (9) has more than two solutions. Again, from (9), we obtain that (1) has more than two solutions, which contradicts the assumption about $F$ being APN. $\square$

The concept of CCZ-equivalence is not so fine than the concept of self-embedding equivalence as we show in the next two propositions.

**Proposition 7** *Let $F_1$ and $F_2$ be two bijective functions over $\mathbb{F}^m$ such that $F_1(\mathbf{0}) = \mathbf{0}$ and $F_2(\mathbf{0}) = \mathbf{0}$. If $F_1$ and $F_2$ are isomorphic self-embedding permutations for the STS($\mathcal{H}^n$), then the corresponding codes $\mathcal{C}_{F_1}$ and $\mathcal{C}_{F_2}$ are equivalent.*

*Proof* It is straightforward. $\square$

**Corollary 1** *Any two isomorphic self-embedding permutations for the same STS($\mathcal{H}^n$) are CCZ-equivalent.*

*Proof* Let $F_1$ and $F_2$ be two self-embedding permutations for the STS($\mathcal{H}^n$). By Proposition 7, the codes $\mathcal{C}_{F_1}$ and $\mathcal{C}_{F_2}$ are equivalent, so the extended codes are equivalent, too. Then, we conclude that $F_1, F_2$ are CCZ-equivalent. $\square$

By Corollary 1, it is possible to use the classification given by the self-embedding isomorphism, in order to obtain a classification given by the CCZ-equivalence. Note that the inverse of this result is not true in general. For example, for $m = 4$, the permutations $\pi_{F_1} = (1,15)(2,3)(4,5)(6,7)(9,10)(11,12)(13,14)$ and $\pi_{F_2} = (1,15)(2,9)(3,10)(4,11)(5,12)(6,13)(7,14)$ are CCZ-equivalent [19,20], but they do not define two isomorphic self-embedding permutations, since they have 6 and 14 pinch points, respectively. However, we can establish a weaker result considering just monomial power permutations, given by the next proposition.

**Proposition 8** *Let $F_1$, $F_2$ be two CCZ-equivalent monomial power permutations. Then, $V^*_{F_1} = V^*_{F_2}$ and $v_{F_1} = v_{F_2}$.*

*Proof* Given a monomial power permutation $F$, by Proposition 3, we have that $v_F = v_F(a)$ and $V^*_F = V^*_F(a)$ for any $a \in \mathbb{F}^m \backslash \{\mathbf{0}\}$, so we can just take $a = 1$. Moreover, we know that $v_F(1)$ is the number of values $b \neq \mathbf{0}$ for which (1) has solutions in $\mathbb{F}^m$ for $a = 1$. Note that if $x$ is a solution of this equation, then $x + b$ is also a solution, so the solutions come in pairs and the maximum value of $v_F$ is $2^{m-1}$, which is reached when $F$ is an APN permutation, by Proposition 6. Hence, the permutations $F$ in all classes of CCZ-equivalent monomial power permutations which are APN satisfy that $v_F = 2^{m-1}$ and $V^*_F = \{1^\wedge(2^{m-1} - 1)\}$. Note that if $F_1$ is an APN function and $F_2$ is CCZ-equivalent to $F_2$, then $F_2$ is also an APN function [8].

If $F$ is not an APN permutation, then (1) has more than a pair of solutions for some values of $b$ and $a = 1$. When this happens, there is a connection with the quadruples in $\mathcal{C}_F^*$, which is the extended code of $\mathcal{C}_F$. For example, if $x, x+b$ and $y, y+b$ are two different pairs of solutions of (1), then the codeword given by the quadruple $(x, x+b, y, y+b)$ belongs to $\mathcal{C}_F^*$, since $F(x)+F(x+b) = F(y)+F(y+b) = a = 1$. Or, for instance, if $x, x+b$; $y, y+b$; and $z, z+b$ are three different pairs of solutions, the quadruples $(x, x+b, y, y+b)$, $(x, x+b, z, z+b)$, $(y, y+b, z, z+b)$ give three codewords in $\mathcal{C}_F^*$ for the same argument. In general, if $n_b$ is the number of solutions of (1) for $b$ and $a = 1$, there are $c_b = \binom{n_b/2}{2}$ quadruples in $\mathcal{C}_F^*$ associated to $b$. Note that if $n_b = 2$, there is only a pair of solutions of (1) and we have that $c_b = 0$. Since the same quadruple is associated to $\frac{1}{2}\binom{4}{2} = 3$ different values of $b$, the total number of quadruples in $\mathcal{C}_F^*$ is

$$\frac{2^m - 1}{3} \sum_{b \in \mathbb{F}^m \setminus \{\mathbf{0}\}} c_b. \tag{10}$$

Let $V_F^* = \{1^\wedge v_1^{(F)}, 2^\wedge v_2^{(F)}, \ldots\}$, where $v_i^{(F)}$ is the number of elements that appear $i$ times in the multiset $\tilde{V}_F$. Then, $v_F - 1 = \sum_{i \geq 1} v_i^{(F)}$. The sum in (10) has $\sum_{i>1} v_i^{(F)}$ nonzero terms corresponding to the values $b$ for which (1) has more than a pair of solutions.

Let $F_1$ and $F_2$ be two CCZ-equivalent monomial power permutations, such that they are not APN. Then, there exists a bijection between the codewords corresponding to the quadruples in both codes $\mathcal{C}_{F_1}^*$ and $\mathcal{C}_{F_2}^*$, given by a permutation $\pi$. Hence, the set of $c_b$ quadruples in $\mathcal{C}_{F_1}^*$ goes to a set of $c_{\bar{b}}$ quadruples in $\mathcal{C}_{F_2}^*$ for an appropriate $\bar{b}$. Then, the number of quadruples in both codes $\mathcal{C}_{F_1}^*$ and $\mathcal{C}_{F_2}^*$ is the same:

$$\frac{2^m - 1}{3} \sum_{b \in \mathbb{F}^m \setminus \{\mathbf{0}\}} c_b = \frac{2^m - 1}{3} \sum_{\bar{b} \in \mathbb{F}^m \setminus \{\mathbf{0}\}} c_{\bar{b}},$$

where for each $b \in \mathbb{F}^m \setminus \{\mathbf{0}\}$ there exists an appropriate $\bar{b} \in \mathbb{F}^m \setminus \{\mathbf{0}\}$ such that $c_b = c_{\bar{b}}$. Not only the number of nonzero terms in the corresponding sums are the same, but also the repeated values. Hence, $v_i^{(F_1)} = v_i^{(F_2)}$ for $i > 1$. Moreover, since $\sum_{i \geq 1} i \cdot v_i^{(F_1)} = \sum_{i \geq 1} i \cdot v_i^{(F_2)} = 2^{m-1} - 1$ and $v_i^{(F_1)} = v_i^{(F_2)}$ for $i > 1$, we can extend the equality for $i = 1$. Therefore, we can conclude that $V_{F_1}^* = V_{F_2}^*$ and $v_{F_1} = 1 + \sum_{i \geq 1} v_i^{(F_1)} = 1 + \sum_{i \geq 1} v_i^{(F_1)} = v_{F_2}$. $\square$

It is clear that dealing with monomial power permutations, the rotation lines at any two points are the same up to a permutation. Therefore, it is enough to consider the rotation lines at one point, for example, the point 1. The rotation line spectrum at point 1 can be used to classify monomial power permutations, up to self-embedding isomorphism, since any two isomorphic self-embedding permutations (regardless of they are monomial or not) have equivalent rotation schemes, so also the same rotation line spectrums up to a permutation.

For any $m \leq 17$, Tables 5 and 6 show all APN monomial power permutations $F(x) = x^t$ over $\mathbb{F}^m$, taking just one representative up to self-embedding isomorphism by Proposition 4. For each class, the tables include the following information: the cyclotomic coset $C_t^*$, where the exponent $t$ belongs, the number of rotation lines $rl(1)$ at point 1, and a reduced rotation line spectrum at point 1. For lack of space, the full rotation line spectrum is not given in these tables. However, we describe a reduced rotation line spectrum including only the different cardinalities of all rotation lines at point 1, since this is enough to distinguish all the cyclotomic classes $C_t^*$, which represent all the nonisomorphic classes of APN monomial power permutations. Note that at least for all $m \leq 17$, all APN monomial power permutations in the same CCZ-equivalent class have the same number of rotation lines, so the classification given by the self-embedding isomorphism coincides with the CCZ-equivalence.

**Proposition 9** *Let* $F(x) = x^{-1}$, *so* $\mathcal{C}_F$ *is the Melas code. If* $m$ *is odd, then in each point there are* $(2^m - 2)/6$ *rotation lines with 6 points each. If* $m$ *is even, then in each point there are* $(2^m - 4)/6$ *rotation lines with 6 points each, and one rotation line with 2 points.*

*Proof* Note that $F^{-1}(x) = F(x)$, since $F^2(x) = x$ for all $x \in \mathbb{F}^m \backslash \{\mathbf{0}\}$. Without loss of generality, we can consider any point $a$ as the starting point. By the arguments shown after Proposition 2, the rotation lines $R_1, R_2, \ldots, R_s$ at point $a$, where $s = rl(a)$, give a partition of the $n-1 = 2^m-2$ elements in $\mathbb{F}^m \backslash \{\mathbf{0}, a\}$. Given any of the rotation lines, $R_j$, we can write it as

$$R_j = [a_1, a + a_1; a_2, a + a_2; \ldots; a_{r_j}, a + a_{r_j}],$$

where $a_1$ is any element in $\mathbb{F}^m \backslash \{\mathbf{0}\}$ such that $a_1 \neq a$ and $a_{i+1} = F(F^{-1}(a) + F^{-1}(a + a_i))$ for all $i \in \{1, \ldots, r_j - 1\}$. It is easy to check that $a_2 = a_1$ if and only if $x^2 + x + 1 = 0$ has solutions over $\mathbb{F}^m$, so if and only if $m$ is even. When $m$ is even, the equation has two solutions and we obtain a rotation line with 2 points. Otherwise, when $a_1 \neq a_2$, then $a_4 = a_1$, and the rest of rotation lines have always 6 points. □

From Tables 5 and 6, it can be observed that the minimum number of points in a rotation line is 6. In the next proposition, we prove that this is true in general for any $m$ and any APN permutation.

**Proposition 10** *Let* $F$ *be any bijective function over* $\mathbb{F}^m$ *such that* $F(\mathbf{0}) = \mathbf{0}$. *If the permutation* $F$ *is APN, then any rotation line at any point has at least 6 points and at most* $2^m - 2$ *points.*

*Proof* Note that the minimum distance of the code $\mathcal{C}_F = \mathcal{H}^n \cap \pi_F(\mathcal{H}^n)$ corresponding to an APN permutation $F$ is 5 [8]. Therefore, there is not any rotation line having 2 points, because there are no common triples in the Hamming codes $\mathcal{H}^n$ and $\pi_F(\mathcal{H}^n)$. Let us assume that there is a rotation line having 4 points for some element $a$: $[a_1, a + a_1; a_2, a + a_2]$. Then, the triples $(a, a_1, a+a_1)$, $(a, a_2, a+a_2)$ belong to $\mathcal{H}^n$ and the triples $(a, a+a_1, a_2)$, $(a, a+a_2, a_1)$ belong to $\pi_F(\mathcal{H}^n)$. Since $\mathcal{H}^n$ and $\pi_F(\mathcal{H}^n)$ are linear codes, we obtain the common quadruple $(a_1, a+a_1, a_2, a+a_2) \in \mathcal{H}^n \cap \pi_F(\mathcal{H}^n) = \mathcal{C}_F$. Therefore, the minimum distance in $\mathcal{C}_F$ would be 4, which is a contradiction. Then, any rotation line at any point has at least 6 points.

The upper bound corresponds to the case when there is only one rotation line at a given point, so it has $2^m - 2$ points. □

The lower bound given in Proposition 10 is attainable by the APN permutation $F$ corresponding to the Melas code $\mathcal{C}_F$ for any length $n = 2^m - 1$, where $m$ is odd, by Proposition 9. On the other hand, the upper bound corresponds to an APN self-embedding permutation in a closed surface. These self-embeddings are pointed out in Table 1 with $(\cdot)^{APN}$. Recall that they exist at least for $m \in \{3, 5, 7, 11, 17\}$, and there are none, at least for any non prime $m$ and for $m \in \{13, 19\}$.

## 4 Conclusions

We classified, up to isomorphism, all self-embedding monomial power permutations in closed surfaces of the Hamming Steiner triple system $\mathrm{STS}(\mathcal{H}^n)$ for $m \leq 22$. The existence of such self-embeddings and their classification for all prime $m \geq 23$ is still an open problem. The found and classified ones are cyclic and nonorientable. The cyclicity is proven for all $m$, and the nonorientability is checked only for all $m \leq 19$ using MAGMA. For $m \in \{3, 5, 7, 11, 17\}$, there exists one class of these permutations which is also APN, but for $m \in \{13, 19\}$, there is not any APN monomial power self-embedding permutations in a closed surface.

We established new invariants, $v_F$ and $V_F^*$, to distinguish CCZ-equivalent monomial power permutations. Up to $m \leq 17$, the classification of APN monomial power permutations, given by the self-embedding isomorphism, coincides with the CCZ-equivalence. It is still not known whether this is also true for any $m \geq 19$. In any case, since two isomorphic self-embedding permutations are CCZ-equivalent, we can use the rotation line spectrum as a first step to obtain a classification, up to CCZ-equivalence, for any permutation not only for monomial power permutations.

## References

1. G. K. Bennett, M. J. Grannel, T. S. Griggs., *Cyclic bi-embeddings of Steiner triple systems on 31 points.* Glasgov Mathematical, 43, 2001, pp. 145-151.
2. C. Bracken, E. Byrne, N. Markin, G. McGuire, *A few more quadratic APN functions*, Cryptogr. Commun., vol. 3, no. 1, 2011, pp. 43-53.
3. C. Bracken, E. Byrne, G. McGuire, G. Nebe, *On the equivalence of quadratic APN functions*, Des. Codes Cryptogr., vol. 61, no. 3, 2011, pp. 261-272.
4. K. A. Browning, J. F. Dillon, R. E. Kibler and M. T. McQuistan, *APN Polynomials and Related Codes*, J. of Combinatorics, Information & Systems, vol. 34, no. 1-4, 2009, pp. 135-159.
5. L. Budaghyan, C. Carlet, and G. Leander, *Constructing new APN functions from known ones*, Finite Fields and Their Applications, vol. 15, no. 2, 2009, pp. 150-159.
6. L. Budaghyan, C. Carlet, and A. Pott, *New Classes of Almost Bent and Almost Perfect Nonlinear Functions*, IEEE Trans. Inform. Theory, vol. 52, no. 3, 2006, pp. 1141-1152.

7. J. J. Cannon and W. Bosma (Eds.) *Handbook of* MAGMA *Functions*, Edition 2.13, 4350 pages, 2006.
8. C. Carlet, P. Charpin and V. Zinoviev, *Codes, Bent Functions and Permutations Suitable for DES-like Cryptosystems*, Des. Codes, Cryptogr., vol. 15, no. 2, 1998, pp. 125-156.
9. Y. Edel, G. Kyureghyan, and A. Pott, *A new APN function which is not equivalent to a power mapping*, IEEE Trans. Inform. Theory, vol. 52, no. 2, 2006, pp. 744-747.
10. Y. Edel and A. Pott, *A new almost perfect nonlinear function which is not quadratic*, Advances in Mathematics of Communications, vol. 3, no. 1, 2009, pp. 59-81.
11. M. J. Grannel, G. K. Bennett and T. S. Griggs, *Bi-embeddings of the projective space PG(3,2).* Journal of Statistical Planning and Inference, 86, 2000, pp. 321-329.
12. M. J. Grannell, T. S. Griggs, *Designs and Topology*, "Surveys in Combinatorics 2007", Cambridge University Press, London Mathematical Society Lecture Note Series 346, 2007, pp. 121-174.
13. M. J. Grannell, T. S. Griggs, and J. Širáň, *Recursive constructions for triangulations*, Journal of Graph Theory, 39, 2002, pp. 87-107.
14. M. J. Grannell and M. Knor, *A construction for biembeddings of Latin squares*, Electronic Journal of Combinatorics, 18(1), 2011, P190, 17pp.
15. M. Jr. Hall, *The theory of groups*, New York: The Macmillan Company, 1959.
16. W. Kühnel, *Topological aspects of twofold triple systems.* Expositiones Mathematicae, vol. 16, no. 4, 1998, pp. 289-332.
17. F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland Publishing Company, 1977.
18. P. R. J. Östergård and O. Pottonen, *There exist Steiner triple systems of order 15 that do not occur in a perfect binary one-error-correcting code*, Journal of Combin. Designs, vol. 15, 2007, pp. 65-468.
19. J. Rifà, F. I. Solov'eva and M. Villanueva, "Hamming codes avoiding Hamming subcodes", *Proceedings of the 12th International Workshop on Algebraic and Combinatorial Coding Theory (ACCT'2010)*, Novosibirsk (Russia), September 5-11, 2010, pp. 256-261.
20. J. Rifà, F. I. Solov'eva and M. Villanueva, *Intersection of Hamming codes avoiding Hamming subcodes*, Des. Codes and Cryptogr., vol. 62, 2012, pp. 209-223.
21. G. Ringel, *Map color theorem*, Springer-Verlag, Yew York/Berlin, 1974.
22. H. Seifert and W. Threlfall, *Lehrbuch der Topologie.* Leipzig and Berlin, Teubner, 1934. vii+353 pp.
23. F. I. Solov'eva, *Tilings of nonorientable surfaces by Steiner triple systems*, Problems of Inform. Transm., vol. 43, no. 3, 2007, pp. 167-178.

*E-mail address:* josep.rifa@autonoma.edu
*E-mail address:* sol@math.nsc.ru
*E-mail address:* merce.villanueva@uab.cat

# Appendix

| $m$ | $C_t^*$ | $v_F$ |
|---|---|---|
| 3 | $C_3^*$ | $4^{\mathrm{APN}}$ |
| 5 | $C_5^*$ | $16^{\mathrm{APN}}$ |
| 7 | $C_{19}^*$ | 43 |
| 7 | $C_7^*, C_{21}^*$ | 50 |
| 7 | $C_9^*$ | $64^{\mathrm{APN}}$ |
| 11 | $C_{39}^*$ | 683 |
| 11 | $C_{59}^*$ | 694 |
| 11 | $C_{371}^*$ | 738 |
| 11 | $C_{181}^*$ | 760 |
| 11 | $C_{37}^*$ | 771 |
| 11 | $C_{25}^*$ | 793 |
| 11 | $C_{21}^*, C_{687}^*$ | 815 |
| 11 | $C_{73}^*, C_{165}^*$ | 826 |
| 11 | $C_{101}^*$ | 837 |
| 11 | $C_{127}^*$ | 870 |
| 11 | $C_{317}^*$ | 881 |
| 11 | $C_{107}^*$ | $1024^{\mathrm{APN}}$ |
| 13 | $C_{51}^*$ | 2887 |
| 13 | $C_{587}^*$ | 3004 |
| 13 | $C_{659}^*$ | 3108 |
| 13 | $C_{295}^*$ | 3186 |
| 13 | $C_{249}^*, C_{661}^*$ | 3199 |
| 13 | $C_{75}^*$ | 3251 |
| 13 | $C_{151}^*$ | 3316 |
| 13 | $C_{133}^*, C_{605}^*$ | 3342 |
| 13 | $C_{875}^*$ | 3381 |
| 13 | $C_{93}^*$ | 3407 |
| 17 | $C_{6827}^*$ | 50457 |
| 17 | $C_{13803}^*$ | 50610 |
| 17 | $C_{5451}^*$ | 50661 |
| 17 | $C_{6059}^*$ | 50678 |
| 17 | $C_{1129}^*$ | 50712 |
| 17 | $C_{15691}^*$ | 50746 |
| 17 | $C_{8081}^*$ | 50814 |
| 17 | $C_{4457}^*, C_{24285}^*$ | 50865 |
| 17 | $C_{2185}^*$ | 50933 |
| 17 | $C_{2387}^*, C_{6705}^*$ | 50950 |
| 17 | $C_{1223}^*$ | 51001 |
| 17 | $C_{5681}^*$ | 51018 |
| 17 | $C_{23987}^*$ | 51069 |
| 17 | $C_{2043}^*$ | 51154 |
| 17 | $C_{4533}^*$ | 51171 |
| 17 | $C_{10171}^*$ | 51273 |
| 17 | $C_{5003}^*$ | 51307 |
| 17 | $C_{249}^*$ | 51324 |
| 17 | $C_{2363}^*, C_{11071}^*$ | 51341 |
| 17 | $C_{1673}^*, C_{9909}^*$ | 51358 |
| 17 | $C_{3163}^*, C_{8917}^*$ | 51409 |
| 17 | $C_{5965}^*$ | 51460 |
| 17 | $C_{11955}^*$ | 51494 |
| 17 | $C_{2335}^*$ | 51511 |
| 17 | $C_{285}^*$ | 51528 |
| 17 | $C_{4285}^*$ | 51579 |
| 17 | $C_{4233}^*$ | 51596 |
| 17 | $C_{3689}^*, C_{4743}^*$ | 51613 |
| 17 | $C_{421}^*$ | 51630 |
| 17 | $C_{543}^*, C_{7143}^*$ | 51647 |
| 17 | $C_{1791}^*, C_{4931}^*, C_{5947}^*$ | 51715 |
| 17 | $C_{2851}^*, C_{4519}^*$ | 51749 |
| 17 | $C_{1201}^*, C_{1949}^*$ | 51783 |
| 17 | $C_{2621}^*$ | 51851 |
| 17 | $C_{1517}^*$ | 51868 |
| 17 | $C_{4635}^*, C_{5663}^*$ | 51936 |
| 17 | $C_{1891}^*$ | 51953 |
| 17 | $C_{1313}^*$ | 52021 |
| 17 | $C_{1395}^*$ | 52038 |
| 17 | $C_{137}^*, C_{3309}^*$ | 52089 |
| 17 | $C_{1001}^*, C_{2979}^*$ | 52123 |
| 17 | $C_{3757}^*$ | 52157 |
| 17 | $C_{6967}^*$ | 52480 |
| 17 | $C_{6249}^*$ | 52531 |
| 17 | $C_{1431}^*$ | 52548 |
| 17 | $C_{2673}^*$ | 52599 |
| 17 | $C_{151}^*$ | 52616 |
| 17 | $C_{2281}^*$ | 52633 |
| 17 | $C_{907}^*$ | 52837 |
| 17 | $C_{4499}^*$ | 53279 |
| 17 | $C_{257}^*$ | $65536^{\mathrm{APN}}$ |

**Table 1** Classification of all self-embedding monomial power permutations in closed surfaces, $F(x) = x^t$ over $\mathbb{F}^m$, based on the invariant $v_F$ for $m \in \{3, \ldots, 18\}$.

| $m$ | $C_t^*$ | $v_F$ |
|---|---|---|
| 19 | $C_{12895}^*$ | 201439 |
| 19 | $C_{7989}^*$ | 203491 |
| 19 | $C_{13643}^*$ | 204365 |
| 19 | $C_{21847}^*$ | 204631 |
| 19 | $C_{28565}^*$ | 204669 |
| 19 | $C_{38283}^*$ | 204688 |
| 19 | $C_{50799}^*$ | 204707 |
| 19 | $C_{7021}^*$ | 204726 |
| 19 | $C_{1257}^*$ | 204745 |
| 19 | $C_{15003}^*$ | 204821 |
| 19 | $C_{6501}^*, C_{37561}^*, C_{59999}^*$ | 204840 |
| 19 | $C_{19367}^*$ | 204935 |
| 19 | $C_{35373}^*$ | 205106 |
| 19 | $C_{24533}^*$ | 205125 |
| 19 | $C_{24041}^*$ | 205296 |
| 19 | $C_{80573}^*$ | 205334 |
| 19 | $C_{15593}^*$ | 205353 |
| 19 | $C_{8487}^*, C_{38045}^*$ | 205372 |
| 19 | $C_{28495}^*, C_{64441}^*$ | 205429 |
| 19 | $C_{4779}^*$ | 205524 |
| 19 | $C_{16077}^*$ | 205543 |
| 19 | $C_{12661}^*, C_{26441}^*$ | 205638 |
| 19 | $C_{4277}^*, C_{23311}^*$ | 205676 |
| 19 | $C_{27385}^*$ | 205733 |
| 19 | $C_{14699}^*$ | 205809 |
| 19 | $C_{4729}^*$ | 205828 |
| 19 | $C_{877}^*$ | 205942 |
| 19 | $C_{1211}^*, C_{8871}^*$ | 205961 |
| 19 | $C_{7011}^*$ | 205980 |
| 19 | $C_{62651}^*$ | 206018 |
| 19 | $C_{15449}^*, C_{56575}^*$ | 206075 |
| 19 | $C_{38891}^*$ | 206113 |
| 19 | $C_{10475}^*$ | 206132 |
| 19 | $C_{12213}^*, C_{18267}^*$ | 206227 |
| 19 | $C_{54003}^*$ | 206265 |
| 19 | $C_{35571}^*$ | 206284 |
| 19 | $C_{2391}^*, C_{26219}^*, C_{32479}^*$ | 206341 |
| 19 | $C_{2987}^*, C_{31923}^*$ | 206398 |
| 19 | $C_{42579}^*$ | 206436 |
| 19 | $C_{22475}^*$ | 206512 |
| 19 | $C_{11513}^*$ | 206531 |
| 19 | $C_{11039}^*, C_{12447}^*$ | 206550 |
| 19 | $C_{1531}^*, C_{46503}^*$ | 206569 |
| 19 | $C_{7147}^*$ | 206607 |
| 19 | $C_{13127}^*, C_{17629}^*$ | 206797 |
| 19 | $C_{13225}^*$ | 206816 |
| 19 | $C_{10633}^*$ | 206835 |
| 19 | $C_{42213}^*$ | 206949 |
| 19 | $C_{235}^*$ | 206968 |
| 19 | $C_{28461}^*$ | 207006 |
| 19 | $C_{1275}^*$ | 207025 |
| 19 | $C_{30917}^*$ | 207158 |
| 19 | $C_{4665}^*$ | 207177 |
| 19 | $C_{32359}^*, C_{62927}^*$ | 207234 |
| 19 | $C_{7769}^*$ | 207253 |
| 19 | $C_{48967}^*$ | 207291 |
| 19 | $C_{58295}^*$ | 207310 |
| 19 | $C_{16949}^*$ | 207405 |
| 19 | $C_{38521}^*$ | 207804 |
| 19 | $C_{9515}^*$ | 207861 |
| 19 | $C_{9539}^*$ | 207880 |
| 19 | $C_{30677}^*$ | 207956 |
| 19 | $C_{4369}^*$ | 208013 |
| 19 | $C_{47463}^*$ | 208051 |
| 19 | $C_{3337}^*$ | 208070 |
| 19 | $C_{5057}^*$ | 208146 |
| 19 | $C_{7241}^*$ | 208241 |
| 19 | $C_{23803}^*$ | 208355 |
| 19 | $C_{9785}^*$ | 208678 |
| 19 | $C_{503}^*$ | 208925 |
| 19 | $C_{20657}^*$ | 208963 |
| 19 | $C_{28201}^*$ | 209837 |

**Table 2** Classification of all self-embedding monomial power permutations in closed surfaces, $F(x) = x^t$ over $F^m$, based on the invariant $v_F$ for $m = 19$.

| $m$ | $C_t^*$ | $v_F$ | $V_F^*$ |
|---|---|---|---|
| 7 | $C_{7}^*$ | 50 | {1^42, 3^7} |
| 7 | $C_{21}^*$ | 50 | {1^42, 3^7} |
| 11 | $C_{21}^*$ | 815 | {1^627, 2^165, 3^22} |
| 11 | $C_{687}^*$ | 815 | {1^627, 2^165, 3^22} |
| 11 | $C_{73}^*$ | 826 | {1^660, 2^132, 3^33} |
| 11 | $C_{165}^*$ | 826 | {1^682, 2^99, 3^33, 4^11} |
| 13 | $C_{249}^*$ | 3199 | {1^2444, 2^624, 3^117, 4^13} |
| 13 | $C_{661}^*$ | 3199 | {1^2470, 2^585, 3^117, 4^26} |
| 13 | $C_{133}^*$ | 3342 | {1^2691, 2^546, 3^104} |
| 13 | $C_{605}^*$ | 3342 | {1^2678, 2^585, 3^65, 4^13} |
| 17 | $C_{4457}^*$ | 50865 | {1^38675, 2^10132, 3^1700, 4^289, 5^68} |
| 17 | $C_{24285}^*$ | 50865 | {1^38692, 2^10013, 3^1853, 4^272, 5^34} |
| 17 | $C_{2387}^*$ | 50950 | {1^38692, 2^10183, 3^1836, 4^221, 5^17} |
| 17 | $C_{6705}^*$ | 50950 | {1^38352, 2^10829, 3^1581, 4^153, 5^34} |
| 17 | $C_{2363}^*$ | 51341 | {1^39202, 2^10234, 3^1768, 4^119, 5^17} |
| 17 | $C_{11071}^*$ | 51341 | {1^39304, 2^10166, 3^1615, 4^221, 5^34} |
| 17 | $C_{1673}^*$ | 51358 | {1^39304, 2^10149, 3^1683, 4^221} |
| 17 | $C_{9909}^*$ | 51358 | {1^39576, 2^9707, 3^1785, 4^255, 5^34} |
| 17 | $C_{3163}^*$ | 51409 | {1^39168, 2^10591, 3^1462, 4^153, 5^17, 6^17} |
| 17 | $C_{8917}^*$ | 51409 | {1^39423, 2^10149, 3^1581, 4^204, 5^51} |
| 17 | $C_{3689}^*$ | 51613 | {1^40171, 2^9265, 3^1921, 4^221, 5^17, 6^17} |
| 17 | $C_{4743}^*$ | 51613 | {1^39933, 2^9656, 3^1836, 4^153, 5^34} |
| 17 | $C_{543}^*$ | 51647 | {1^39848, 2^9996, 3^1564, 4^187, 5^51} |
| 17 | $C_{7143}^*$ | 51647 | {1^39848, 2^9877, 3^1768, 4^136, 5^17} |
| 17 | $C_{1791}^*$ | 51715 | {1^39882, 2^10030, 3^1632, 4^153, 5^17} |
| 17 | $C_{4931}^*$ | 51715 | {1^39916, 2^9962, 3^1683, 4^119, 5^34} |
| 17 | $C_{5947}^*$ | 51715 | {1^39848, 2^10149, 3^1479, 4^238} |
| 17 | $C_{2851}^*$ | 51749 | {1^39916, 2^10064, 3^1615, 4^119, 5^34} |
| 17 | $C_{4519}^*$ | 51749 | {1^40290, 2^9367, 3^1870, 4^204, 5^17} |
| 17 | $C_{1201}^*$ | 51783 | {1^40052, 2^9945, 3^1598, 4^136, 5^51} |
| 17 | $C_{1949}^*$ | 51783 | {1^40307, 2^9520, 3^1700, 4^187, 5^68} |
| 17 | $C_{4635}^*$ | 51936 | {1^40358, 2^9690, 3^1751, 4^136} |
| 17 | $C_{5663}^*$ | 51936 | {1^40392, 2^9724, 3^1598, 4^204, 5^17} |
| 17 | $C_{137}^*$ | 52089 | {1^40562, 2^9962, 3^1292, 4^187, 5^85} |
| 17 | $C_{3309}^*$ | 52089 | {1^40596, 2^9741, 3^1547, 4^204} |
| 17 | $C_{1001}^*$ | 52123 | {1^40851, 2^9418, 3^1615, 4^204, 5^17, 6^17} |
| 17 | $C_{2979}^*$ | 52123 | {1^40783, 2^9452, 3^1734, 4^119, 5^34} |

**Table 3** Classification of some self-embedding monomial power permutations in closed surfaces, $F(x) = x^t$ over $\mathbb{F}^m$, based on the invariants $v_F$ and $V_F^*$ for $m \in \{7, 11, 13, 17\}$.

| $m$ | $C_t^*$ | $v_F$ | $V_F^*$ |
|---|---|---|---|
| 19 | $C_{6501}^*$ | 204840 | $\{1{}^\wedge157377, 2{}^\wedge38779, 3{}^\wedge7676, 4{}^\wedge855, 5{}^\wedge152\}$ |
| 19 | $C_{37561}^*$ | 204840 | $\{1{}^\wedge156522, 2{}^\wedge40527, 3{}^\wedge6764, 4{}^\wedge893, 5{}^\wedge114, 7{}^\wedge19\}$ |
| 19 | $C_{59999}^*$ | 204840 | $\{1{}^\wedge156503, 2{}^\wedge40565, 3{}^\wedge6764, 4{}^\wedge817, 5{}^\wedge190\}$ |
| 19 | $C_{8487}^*$ | 205372 | $\{1{}^\wedge157206, 2{}^\wedge40584, 3{}^\wedge6726, 4{}^\wedge722, 5{}^\wedge114, 7{}^\wedge19\}$ |
| 19 | $C_{38045}^*$ | 205372 | $\{1{}^\wedge157567, 2{}^\wedge39748, 3{}^\wedge7182, 4{}^\wedge836, 5{}^\wedge38\}$ |
| 19 | $C_{28495}^*$ | 205429 | $\{1{}^\wedge157719, 2{}^\wedge39881, 3{}^\wedge6783, 4{}^\wedge912, 5{}^\wedge133\}$ |
| 19 | $C_{64441}^*$ | 205429 | $\{1{}^\wedge157529, 2{}^\wedge40318, 3{}^\wedge6479, 4{}^\wedge988, 5{}^\wedge95, 6{}^\wedge19\}$ |
| 19 | $C_{12661}^*$ | 205638 | $\{1{}^\wedge158669, 2{}^\wedge38969, 3{}^\wedge6745, 4{}^\wedge988, 5{}^\wedge247, 6{}^\wedge19\}$ |
| 19 | $C_{26441}^*$ | 205638 | $\{1{}^\wedge157833, 2{}^\wedge40147, 3{}^\wedge6707, 4{}^\wedge855, 5{}^\wedge95\}$ |
| 19 | $C_{4277}^*$ | 205676 | $\{1{}^\wedge157814, 2{}^\wedge40109, 3{}^\wedge7011, 4{}^\wedge646, 5{}^\wedge76, 6{}^\wedge19\}$ |
| 19 | $C_{23311}^*$ | 205676 | $\{1{}^\wedge158042, 2{}^\wedge39881, 3{}^\wedge6745, 4{}^\wedge931, 5{}^\wedge76\}$ |
| 19 | $C_{1211}^*$ | 205961 | $\{1{}^\wedge158004, 2{}^\wedge40831, 3{}^\wedge6061, 4{}^\wedge1026, 5{}^\wedge38\}$ |
| 19 | $C_{8871}^*$ | 205961 | $\{1{}^\wedge158327, 2{}^\wedge40242, 3{}^\wedge6346, 4{}^\wedge931, 5{}^\wedge114\}$ |
| 19 | $C_{15449}^*$ | 206075 | $\{1{}^\wedge158612, 2{}^\wedge39843, 3{}^\wedge6745, 4{}^\wedge760, 5{}^\wedge114\}$ |
| 19 | $C_{56575}^*$ | 206075 | $\{1{}^\wedge158916, 2{}^\wedge39444, 3{}^\wedge6574, 4{}^\wedge1083, 5{}^\wedge57\}$ |
| 19 | $C_{12213}^*$ | 206227 | $\{1{}^\wedge158878, 2{}^\wedge39653, 3{}^\wedge6840, 4{}^\wedge836, 5{}^\wedge19\}$ |
| 19 | $C_{18267}^*$ | 206227 | $\{1{}^\wedge158840, 2{}^\wedge39862, 3{}^\wedge6707, 4{}^\wedge646, 5{}^\wedge152, 6{}^\wedge19\}$ |
| 19 | $C_{2391}^*$ | 206341 | $\{1{}^\wedge159315, 2{}^\wedge39216, 3{}^\wedge6954, 4{}^\wedge741, 5{}^\wedge114\}$ |
| 19 | $C_{26219}^*$ | 206341 | $\{1{}^\wedge158764, 2{}^\wedge40470, 3{}^\wedge6080, 4{}^\wedge950, 5{}^\wedge57, 6{}^\wedge19\}$ |
| 19 | $C_{32479}^*$ | 206341 | $\{1{}^\wedge158726, 2{}^\wedge40147, 3{}^\wedge6783, 4{}^\wedge646, 5{}^\wedge38\}$ |
| 19 | $C_{2987}^*$ | 206398 | $\{1{}^\wedge158479, 2{}^\wedge40793, 3{}^\wedge6498, 4{}^\wedge551, 5{}^\wedge76\}$ |
| 19 | $C_{31923}^*$ | 206398 | $\{1{}^\wedge159011, 2{}^\wedge39881, 3{}^\wedge6669, 4{}^\wedge817, 5{}^\wedge19\}$ |
| 19 | $C_{11039}^*$ | 206550 | $\{1{}^\wedge158707, 2{}^\wedge40983, 3{}^\wedge6023, 4{}^\wedge779, 5{}^\wedge57\}$ |
| 19 | $C_{12447}^*$ | 206550 | $\{1{}^\wedge159600, 2{}^\wedge39235, 3{}^\wedge6859, 4{}^\wedge798, 5{}^\wedge38, 6{}^\wedge19\}$ |
| 19 | $C_{1531}^*$ | 206569 | $\{1{}^\wedge159011, 2{}^\wedge40641, 3{}^\wedge5909, 4{}^\wedge931, 5{}^\wedge57, 6{}^\wedge19\}$ |
| 19 | $C_{46503}^*$ | 206569 | $\{1{}^\wedge159068, 2{}^\wedge40432, 3{}^\wedge6099, 4{}^\wedge931, 5{}^\wedge38\}$ |
| 19 | $C_{13127}^*$ | 206797 | $\{1{}^\wedge159752, 2{}^\wedge39919, 3{}^\wedge6099, 4{}^\wedge874, 5{}^\wedge152\}$ |
| 19 | $C_{17629}^*$ | 206797 | $\{1{}^\wedge159790, 2{}^\wedge39672, 3{}^\wedge6441, 4{}^\wedge779, 5{}^\wedge114\}$ |
| 19 | $C_{32359}^*$ | 207234 | $\{1{}^\wedge160037, 2{}^\wedge40413, 3{}^\wedge5947, 4{}^\wedge760, 5{}^\wedge57, 6{}^\wedge19\}$ |
| 19 | $C_{62927}^*$ | 207234 | $\{1{}^\wedge160531, 2{}^\wedge39254, 3{}^\wedge6745, 4{}^\wedge665, 5{}^\wedge19, 6{}^\wedge19\}$ |

**Table 4** Classification of some self-embedding monomial power permutations in closed surfaces, $F(x) = x^t$ over $\mathbb{F}^m$, based on the invariants $v_F$ and $V_F^*$ for $m = 19$.

| $m$ | $C_t^*$ | $rl(1)$ | reduced rotation line spectrum at point 1 |
|---|---|---|---|
| 3 | $C_3^*$ | 1 | $(1;6)$ |
| 5 | $C_5^*$ | 1 | $(1;30)$ |
| 5 | $C_3^*$ | 2 | $(2;10,20)$ |
| 5 | $C_{15}^*$ | 5 | $(5;6)$ |
| 7 | $C_9^*$ | 1 | $(1;126)$ |
| 7 | $C_5^*$ | 2 | $(2;28,98)$ |
| 7 | $C_3^*$ | 4 | $(4;14,28,42)$ |
| 7 | $C_{23}^*$ | 4 | $(4;14,84)$ |
| 7 | $C_{11}^*$ | 15 | $(15;6,10,14)$ |
| 7 | $C_{63}^*$ | 21 | $(21;6)$ |
| 9 | $C_{47}^*$ | 3 | $(3;6,234,270)$ |
| 9 | $C_5^*$ | 5 | $(5;6,120,144)$ |
| 9 | $C_{13}^*$ | 5 | $(5;6,54,126,270)$ |
| 9 | $C_{17}^*$ | 5 | $(5;6,72,144)$ |
| 9 | $C_3^*$ | 10 | $(10;6,24,36,54,72,90)$ |
| 9 | $C_{19}^*$ | 14 | $(14;6,18,36,40,54)$ |
| 9 | $C_{255}^*$ | 85 | $(85;6)$ |
| 11 | $C_{107}^*$ | 1 | $(1;2046)$ |
| 11 | $C_{35}^*$ | 3 | $(3;264,682,1100)$ |
| 11 | $C_{95}^*$ | 4 | $(4;22,374,1276)$ |
| 11 | $C_5^*$ | 6 | $(6;22,88,132,396,462,946)$ |
| 11 | $C_{57}^*$ | 6 | $(6;22,44,66,88,440,1386)$ |
| 11 | $C_{17}^*$ | 8 | $(8;22,66,110,132,154,264,396,902)$ |
| 11 | $C_9^*$ | 13 | $(13;22,136,528)$ |
| 11 | $C_{33}^*$ | 13 | $(13;22,88,176)$ |
| 11 | $C_{13}^*$ | 14 | $(14;88,112,176,550)$ |
| 11 | $C_3^*$ | 18 | $(18;22,44,66,88,110,132,154,176,198,242)$ |
| 11 | $C_{43}^*$ | 19 | $(19;18,44,66,88,308,330,396,550)$ |
| 11 | $C_{1023}^*$ | 341 | $(341;6)$ |
| 13 | $C_{71}^*$ | 3 | $(3;312,364,7514)$ |
| 13 | $C_9^*$ | 3 | $(3;26,338,7826)$ |
| 13 | $C_{67}^*$ | 3 | $(3;104,7982)$ |
| 13 | $C_{171}^*$ | 3 | $(3;26,2002,6162)$ |
| 13 | $C_5^*$ | 5 | $(5;156,234,338,806,6656)$ |
| 13 | $C_{287}^*$ | 6 | $(6;26,156,390,754,2496,4368)$ |
| 13 | $C_{33}^*$ | 6 | $(6;26,78,338,1196,6474)$ |
| 13 | $C_{191}^*$ | 6 | $(6;26,52,286,3302,4472)$ |
| 13 | $C_{17}^*$ | 8 | $(8;26,52,78,806,1976,2262,2964)$ |
| 13 | $C_{13}^*$ | 9 | $(9;26,52,78,156,624,3536,3666)$ |
| 13 | $C_{65}^*$ | 13 | $(13;630)$ |
| 13 | $C_{57}^*$ | 18 | $(18;16,52,130,234,260,7306)$ |
| 13 | $C_3^*$ | 52 | $(52;26,32,78,104,130,156,182,208,234,260,286,312,338,364,468)$ |
| 13 | $C_{4095}^*$ | 1365 | $(1365;6)$ |

**Table 5** Classification of all APN monomial power permutations for $m \leq 13$ using the invariant given by the rotation line spectrum.

| $m$ | $C_t^*$ | $rl(1)$ | reduced rotation line spectrum at point 1 |
|---|---|---|---|
| 15 | $C_{131}^*$ | 10 | $(10; 6, 30, 2170, 8720)$ |
| 15 | $C_{241}^*$ | 15 | $(15; 6, 10, 20, 180, 380, 1500, 2330, 22860)$ |
| 15 | $C_{13}^*$ | 16 | $(16; 6, 10, 20, 36, 90, 720, 10560)$ |
| 15 | $C_{1371}^*$ | 16 | $(16; 6, 30, 210, 288, 430, 750, 1230, 4770, 5490, 17550)$ |
| 15 | $C_{383}^*$ | 25 | $(25; 6, 10, 20, 158, 180, 330, 900, 2530, 21360)$ |
| 15 | $C_5^*$ | 30 | $(30; 6, 30, 70, 108, 208, 9600)$ |
| 15 | $C_{17}^*$ | 47 | $(47; 6, 10, 20, 30, 32, 306, 430, 1040, 2640, 2700, 3750, 11700)$ |
| 15 | $C_{129}^*$ | 117 | $(117; 6, 30, 60, 150, 300)$ |
| 15 | $C_3^*$ | 260 | $(260; 6, 10, 20, 22, 36, 40, 50, 60, 66, 70, 72, 78, 80, 90, 110, 120, 130, 140, 150,$<br>$160, 180, 200, 210, 240, 250, 260, 300, 330, 350, 360, 390, 420, 450, 480,$<br>$510, 540, 570, 600, 660, 690, 720, 750, 1020, 1050, 1110)$ |
| 15 | $C_{3657}^*$ | 341 | $(341; 6, 10, 12, 16, 18, 20, 22, 82, 86, 184, 220, 264, 278, 364, 384, 462)$ |
| 15 | $C_{16383}^*$ | 5461 | $(5461; 6)$ |
| 17 | $C_{257}^*$ | 1 | $(1; 131070)$ |
| 17 | $C_{65}^*$ | 4 | $(4; 170, 680, 4386, 125834)$ |
| 17 | $C_{271}^*$ | 6 | $(6; 34, 102, 306, 4420, 24684, 101524)$ |
| 17 | $C_9^*$ | 9 | $(9; 34, 102, 238, 544, 850, 1632, 11798, 28186, 87686)$ |
| 17 | $C_{683}^*$ | 9 | $(9; 272, 748, 1156, 2720, 5746, 9656, 11288, 15878, 83606)$ |
| 17 | $C_{1151}^*$ | 10 | $(10; 68, 714, 1224, 4522, 4828, 4964, 6086, 45934, 57902)$ |
| 17 | $C_{33}^*$ | 12 | $(12; 102, 238, 306, 476, 646, 1972, 2550, 3298, 6018, 17850, 41956, 55658)$ |
| 17 | $C_{129}^*$ | 12 | $(12; 68, 102, 136, 272, 374, 1972, 15096, 16082, 20876, 24174, 51816)$ |
| 17 | $C_{13}^*$ | 14 | $(14; 34, 68, 204, 714, 884, 1394, 2380, 6936, 12580, 12988, 18904, 26486, 47464)$ |
| 17 | $C_{259}^*$ | 21 | $(21; 34, 204, 1122, 7628)$ |
| 17 | $C_{767}^*$ | 24 | $(24; 68, 510, 718, 1632, 3468, 5882, 29614, 77690)$ |
| 17 | $C_5^*$ | 25 | $(25; 34, 68, 306, 11152, 16830, 35360, 66708)$ |
| 17 | $C_{57}^*$ | 25 | $(25; 68, 136, 646, 816, 850, 1156, 3318, 3332, 67660)$ |
| 17 | $C_{241}^*$ | 26 | $(26; 34, 90, 510, 748, 1700, 1734, 24582, 24684, 75514)$ |
| 17 | $C_{993}^*$ | 40 | $(40; 34, 128, 136, 190, 340, 8806, 116212)$ |
| 17 | $C_{17}^*$ | 59 | $(59; 34, 160, 204, 442, 1384, 1462, 1632, 3022, 5542, 17272, 26860)$ |
| 17 | $C_3^*$ | 388 | $(388; 34, 36, 44, 50, 54, 64, 68, 102, 104, 136, 170, 204, 238, 272, 306, 340,$<br>$408, 442, 476, 510, 544, 578, 612, 646, 680, 748, 782, 816, 850, 884,$<br>$918, 952, 1020, 1054, 1088, 1156, 1190, 1224, 1292, 1326, 1360,$<br>$1394, 1462, 1496, 1564, 1598, 1768, 1904, 1972, 2006)$ |
| 17 | $C_{65535}^*$ | 21845 | $(21845; 6)$ |

**Table 6** Classification of all APN monomial power permutations for $m \in \{15, 17\}$ using the invariant given by the rotation line spectrum.