Biembeddings of Small Order Hamming STS(n) and APN Monomial Power Permutations

Josep Rifà
Dep. of Inform. & Communications Eng.
Universitat Autònoma de Barcelona
08193-Bellaterra, Spain
Email: josep.rifa@uab.cat

Faina I. Solov'eva
Sobolev Inst. of Mathematics,
Novosibirsk State University
Novosibirsk, Russia
Email: sol@math.nsc.ru

Mercè Villanueva
Dep. of Inform. & Communications Eng.
Universitat Autònoma de Barcelona
08193-Bellaterra, Spain
Email: merce.villanueva@uab.cat

***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. 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. 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 proposed. This classification for APN monomial power permutations coincides with the CCZ-equivalence, at least up to $m \leq 17$.

I. Introduction

Let $\mathbb{F}^n$ be the vector space of dimension n over the binary field $\mathbb{F}$. Basic concepts such as *Hamming distance*, *Hamming weight*, *support*, *(linear) binary code* and *minimum distance* of a code can be found in [8]. 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 *equivalent* if there exists a vector $y \in \mathbb{F}^n$ and a coordinate permutation $\pi \in \mathcal{S}_n$ such that $\mathcal{C}_2 = \{y + \pi(x) : x \in \mathcal{C}_1\}$. They are called *isomorphic* if $\mathcal{C}_2 = \{\pi(x) : x \in \mathcal{C}_1\}$.

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 $\mathcal{H}^n$ [8]. 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 $\mathbb{F}^m$. We can associate to each one of them the elements in the set $N = \{1, 2, \ldots, n\}$ as well as the elements $\{\alpha^0, \alpha^1, \ldots, \alpha^{n-2}\}$, where α is a primitive element of the finite field $GF(2^m)$.

Let $F : \mathbb{F}^m \to \mathbb{F}^m$ 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 $F : \mathbb{F}^m \to \mathbb{F}^m$ 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 $\mathcal{H}^n$. It is known that two functions $F, G : \mathbb{F}^m \to \mathbb{F}^m$, 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. 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. In the last years, many new APN functions have been constructed [1], [4]. 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 [4].

A classical (block) t-(n, k, λ) 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 λ 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 $n \equiv 1 \text{ or } 3 \pmod 6$. 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* 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 results can be regarded as the blocks of a design [6]. In this 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 [10] that this complete graph triangulates some orientable surface if and only if $n \equiv 0, 3, 4$ or $7 \pmod{12}$, and triangulates some nonorientable surface if and only if $n \equiv 0$ or $1 \pmod 3$ for $n > 7$.

A triangulation is *face 2-colorable* if the triangular faces of an embedding into a surface can be properly 2-colored (say in black and white colors), that is, in such a way that no two faces with a common edge have the same color. The case of 2-colorability is of special interest because all the triangles of the same color on the surface induce a $\mathrm{STS}(n)$. Therefore, we have two $\mathrm{STS}(n)$ (black and white) *biembedded* in the surface. Such a pair of Steiner triple systems of order n is called a *biembedding*. If these two $\mathrm{STS}(n)$ are isomorphic, then it is called a *self-embedding*, and the corresponding permutation is called a *self-embedding permutation*. 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 color of the triangles or reversing it. In the case when the colors of the triangles are preserved, the isomorphism is said to be *color-preserving*.

The previous ideas about biembeddings in a closed surface can be extended to pseudosurfaces. 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. The points resulting after these identifications are called *pinch points*.

All necessary definitions and notions concerning embeddings in closed surfaces can be found in [10], [6] and concerning embeddings in pseudosurfaces with pinch points in [7], [6]. 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.

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 survey [6]. 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 [10]. For $n = 15$, there are four nonisomorphic self-embeddings of $\mathrm{STS}(\mathcal{H}^{15})$, three of them are nonorientable and one is orientable [5]. 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 I, we give the introductory notions used along the paper. In Section II, we present new self-embeddings in closed surfaces for the Hamming Steiner triple systems $\mathrm{STS}(\mathcal{H}^n)$, where $n = 2^m - 1$ and $m \in \{5, 7, 11, 13, 17, 19\}$. Actually, we give all possible self-embeddings in a closed surface constructed from a $\mathrm{STS}(\mathcal{H}^n)$ 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 III, we focus on showing that the rotation line spectrum 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 IV, we present some conclusions and further research.

II. Self-embeddings of $\mathrm{STS}(\mathcal{H}^n)$ in closed surfaces

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 $\mathrm{STS}(\mathcal{H}^n)$ corresponding to a cyclic version of the Hamming code $\mathcal{H}^n$ of length n (for example, the one considered in the introduction).

It is easy to see that there is only one self-embedding in a closed surface for the cyclic $\mathrm{STS}(\mathcal{H}^7)$ 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 $\mathrm{STS}(\mathcal{H}^{15})$ classified in [5] are cyclic, so there are no self-embeddings in a closed surface for the cyclic $\mathrm{STS}(\mathcal{H}^{15})$ given by monomial power permutations.

In order to construct the mentioned new self-embeddings in a closed surface for the cyclic $\mathrm{STS}(\mathcal{H}^n)$, 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 $\gcd(t, n) = 1$. Therefore, since the $\mathrm{STS}(\mathcal{H}^n)$ is cyclic, these constructed self-embeddings are also cyclic, according to the next proposition.

Proposition 2.1: Let $\mathrm{STS}(\mathcal{H}^n)$ be cyclic and $F : \mathbb{F}^m \to \mathbb{F}^m$ be any monomial power permutation. Then, $F(\mathrm{STS}(\mathcal{H}^n))$ is also cyclic.

The next proposition gives us an alternative definition for a self-embedding permutation in a closed surface for a $\mathrm{STS}(\mathcal{H}^n)$. Given a $\mathrm{STS}(\mathcal{H}^n)$, where $n = 2^m - 1$, for all $a, b \in \mathbb{F}^m \backslash \{\mathbf{0}\}$ with $a \neq b$, we have $a + b = c$ if (a, b, c)

is a triple in STS($\mathcal{H}^n$). 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 2.2: 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 $a_1, a_2, \ldots, a_{2^{m-1}-1}$ 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 $i\in\{1,\ldots,2^{m-1}-2\}$.

We have used Proposition 2.2 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 $a\in\mathbb{F}^m\backslash\{\mathbf{0}\}$.

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), with the ordering determined by the biembedding, can be divided into more than one cycle. Each one of these cycles is called *rotation line* at point $i\in N$. 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.

For any self-embedding of STS($\mathcal{H}^n$) given by a permutation $F:\mathbb{F}^m\rightarrow\mathbb{F}^m$ with $F(\mathbf{0})=\mathbf{0}$, and any element $a\in\mathbb{F}^m\backslash\{\mathbf{0}\}$, we can construct the sequence $a_1, a_2, \ldots, a_{r_1}$ 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 $i\in\{1,\ldots,r_1\}$. Then, the sequence $R_1 = [a_1, b_1; a_2, b_2; \ldots; a_{r_1}, b_{r_1}]$ define 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 $R_1, R_2, \ldots, R_s$, where $s=rl(a)$. We simplify this information considering only the number of rotation lines and the cardinal of each one of them. The *rotation line spectrum* at point a will be the array

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

where $s=rl(a)$ is the number of rotation lines at point a, and $rl(a)_i = |R_i|$ for all $i\in\{1,\ldots,s\}$. 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 2.3: For $m=5$, consider the cyclic STS($\mathcal{H}^{31}$) corresponding to the cyclic Hamming code with parity check matrix $H_5 = (1\ \alpha\ \alpha^2\ \ldots\ \alpha^{30})$, where α is a primitive element of $GF(32)=\mathbb{F}[x]/(x^5+x^2+1)$.

The permutation corresponding to the 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

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

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 $R_1=[2,19;5,11;17,10;3,6;9,21]$, $R_2=[27,29;24,13;12,20;31,18;14,15;28,7;22,26;16,25;23,8;30,4]$, so the rotation line spectrum is $(2; 10, 20)$. △

For any self-embedding of STS($\mathcal{H}^n$) given by a permutation $F:\mathbb{F}^m\rightarrow\mathbb{F}^m$ 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

$$v_F(a) = |\{x+F^{-1}(a+F(x)) : x\in\mathbb{F}^m\}|. \tag{6}$$

Take the multiset $\tilde{V}_F(a)=\{z_i : i\in\{1,\ldots,2^{m-1}-1\}\}$, where $\{(a, a_i, a+a_i) : i\in\{1,\ldots,2^{m-1}-1\}\}$ 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 $i\in\{1,\ldots,2^{m-1}-1\}$. 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. It can be proven that if $S\cup F(S)$ is a self-embedding, then $v_F(a)=1+|V_F(a)|$.

Example 2.4: 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 α is a primitive element of $GF(128)=\mathbb{F}[x]/(x^7+x+1)$.

For the self-embedding in a closed surface, given by $F(x)=x^7$, 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 $(2,8,109)$, $(91,10,43)$, $(74,79,17)$, $\ldots,(36,110,124)$ are triples in F(STS($\mathcal{H}^{127}$)). Therefore, $v_F(1)=1+|V_F(1)|=50$ and $V_F^*(1)=\{1{\wedge}42, 3{\wedge}7\}$. △

Theorem 2.5: Let F_1, F_2 be bijective functions over $\mathbb{F}^m$ such that $F_1(\mathbf{0})=F_2(\mathbf{0})=\mathbf{0}$, and $S=$STS($\mathcal{H}^n$). If $S\cup F_1(S)$ and $S\cup F_2(S)$ are isomorphic self-embeddings, then

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

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

Proposition 2.6: Let $F:\mathbb{F}^m\rightarrow\mathbb{F}^m$ 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 $a \in \mathbb{F}^m \backslash \{\mathbf{0}\}$.

Example 2.7: For the self-embedding permutations, given by $F(x) = x^3$ and $F(x) = x^5$ over $\mathbb{F}^5$ defined in Example 2.3, we 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 3.1 (see Section III, where we investigate the connection between APN functions and self-embeddings), they are APN permutations.

By Theorem 2.5, 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 2.6, 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 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 $C_i = \{i, 2i, 4i, \ldots, 2^{m_i - 1} i\}$, where m_i is the smallest positive integer such that $2^{m_i} \cdot i \equiv i \pmod{2^m - 1}$ [8]. 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, $C_1^* = C_1 = \{1, 2, 4, \ldots, 2^{m-1}\}$.

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 2.8: Let $F_1, F_2 : \mathbb{F}^m \to \mathbb{F}^m$ 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 $a \in \mathbb{F}^m \backslash \{\mathbf{0}\}$.

Proposition 2.9: 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.

Theorem 2.10: 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.

As far as we know, all found self-embedding permutations in closed surfaces given by Theorem 2.10 are new with the exception of the one given for $m = 3$. By Proposition 2.1, 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 I, we point out these cases in the last column. Note that for any non prime m and for $m \in \{13, 19\}$ there are no APN self-embeddings in a closed surface.

m	t	APN
3	3	3
5	5	5
7	$7, 9, 19, 21$	9
11	$21, 25, 37, 39, 59, 73, 101, 107, 127, 165, 181, 317, 371, 687$	107
13	$51, 75, 93, 133, 151, 249, 295, 587, 605, 659, 661, 875$	
17	$137, 151, 249, 257, 285, 421, 543, 907, 1001, 1129, 1201, 1223, 1313, 1395, 1431, 1517, 1673, 1791, 1891, 1949, 2043, 2185, 2281, 2335, 2363, 2387, 2621, 2673, 2851, 2979, 3163, 3309, 3689, 3757, 4233, 4285, 4457, 4499, 4519, 4533, 4635, 4743, 4931, 5003, 5451, 5663, 5681, 5947, 5965, 6059, 6249, 6705, 6827, 6967, 7143, 8081, 8917, 9909, 10171, 11071, 11955, 13803, 15691, 23987, 24285$	257
19	$235, 503, 877, 1211, 1257, 1275, 1531, 2391, 2987, 3337, 4277, 4369, 4665, 4729, 4779, 5057, 6501, 7011, 7021, 7147, 7241, 7769, 7989, 8487, 8871, 9515, 9539, 9785, 10475, 10633, 11039, 11513, 12213, 12447, 12661, 12895, 13127, 13225, 13643, 14699, 15003, 15449, 15593, 16077, 16949, 17629, 18267, 19367, 20657, 21847, 22475, 23311, 23803, 24041, 24533, 26219, 26441, 27385, 28201, 28461, 28495, 28565, 30677, 30917, 31923, 32359, 32479, 35373, 35571, 37561, 38045, 38283, 38521, 38891, 42213, 42579, 46503, 47463, 48967, 50799, 54003, 56575, 58295, 59999, 62651, 62927, 64441, 80573$	

TABLE I

CLASSIFICATION OF ALL NONISOMORPHIC SELF-EMBEDDING MONOMIAL POWER PERMUTATIONS IN CLOSED SURFACES, $F(x) = x^t$ OVER $\mathbb{F}^m$, FOR $m \leq 22$.

III. SELF-EMBEDDINGS OF STS$(\mathcal{H}^n)$ AND APN PERMUTATIONS

This section deals with APN permutations, which can be seen as self-embedding 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 [3]. 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 II, 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 3.1: 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 $v_F(a) = 2^{m-1}$.

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

Proposition 3.2: If two self-embedding permutations F_1 and F_2 of the STS($\mathcal{H}^n$) are isomorphic, then the corresponding codes $\mathcal{C}_{F_1}$ and $\mathcal{C}_{F_2}$ are equivalent.

From the last proposition, it follows that any two isomorphic self-embedding permutations for the STS($\mathcal{H}^n$) are CCZ-equivalent.

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 [9], 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 3.3: Let F_1, F_2 be two CCZ-equivalent monomial power permutations. Then, $V^*_{F_1} = V^*_{F_2}$ and $v_{F_1} = v_{F_2}$.

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.

It is important to highlight 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 3.4: 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.

The lower bound given in Proposition 3.4 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. On the other hand, the upper bound corresponds to an APN self-embedding permutation in a closed surface. 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 $m \in \{13, 19\}$.

IV. Conclusions

We classified, up to isomorphism, all self-embedding monomial power permutations in close surfaces of the Hamming Steiner triple system 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 for all m. 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.

Acknowledgment

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 also partially supported by the Grant RFBR 12-01-00631-a.

References

[1] 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.

[2] J. J. Cannon and W. Bosma (Eds.) *Handbook of* MAGMA *Functions*, Edition 2.13, 4350 pages, 2006.

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] W. Kühnel, *Topological aspects of twofold triple systems.* Expositiones Mathematicae, vol. 16, no. 4, 1998, pp. 289-332.

[8] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland Publishing Company, 1977.

[9] 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.

[10] G. Ringel, *Map color theorem*, Springer-Verlag, Yew York/Berlin, 1974.