A proof of a conjecture on trivariate permutations

Daniele Bartoli[1], Mohit Pal[2], Pantelimon Stănică[3], Tommaso Toccotelli[1]

[1] Department of Mathematics and Computer Science,
University of Perugia, 06123 Perugia, Italy;
{daniele.bartoli@unipg.it,toccotelli.tommaso@gmail.com}

[2] Department of Informatics, University of Bergen, PB 7803, N-5020,
Bergen, Norway; Mohit.Pal@uib.no

[3] Applied Mathematics Department, Naval Postgraduate School,
Monterey, CA 93943, USA; pstanica@nps.edu

May 4, 2024

Keywords: Finite fields, Permutation polynomials, Differential uniformity, varieties, irreducible components
Mathematics Subject Classification 2020: 12E20, 11T06

Abstract

In this note we show (for a large enough dimension of the underlying field) a conjecture of [C. Beierle, C. Carlet, G. Leander, L. Perrin, *A further study of quadratic APN permutations in dimension nine*, Finite Fields Appl. 81 (2022), 102049] on a trivariate permutation. This function is a global representation of two new sporadic quadratic APN permutations in dimension 9 found by [C. Beierle, G. Leander, *New instances of quadratic APN functions*, IEEE Trans. Inf. Theory 68(1) (2022), 670—678].

1 Introduction and tools from algebraic geometry

Let $q = 2^m$, $m \in \mathbb{N}$, and denote by $\mathbb{F}_q$ the finite field with q elements. For any positive integer n, we denote by $\mathbb{F}_q[X_1, \ldots, X_n]$, the ring of polynomials in n indeterminates over finite field $\mathbb{F}_q$. An element $f \in \mathbb{F}_q[X_1, \ldots, X_n]$ is called a permutation polynomial in n variables if the equation $f(X_1, \ldots X_n) = a$ has q^{n-1} solutions in $\mathbb{F}_q^n$ for each $a \in \mathbb{F}_q$. Let $F : \mathbb{F}_q^n \to \mathbb{F}_q^n$ be a map given by

$$F(X_1, \ldots, X_n) = (f_1(X_1, \ldots, X_n), \ldots, f_n(X_1, \ldots, X_n)),$$

where $f_i \in \mathbb{F}_q[X_1, \ldots, X_n]$ then F is called a vectorial permutation if it induces a permutation on $\mathbb{F}_q^n$.

Vectorial Boolean functions are fundamental building blocks in symmetric cryptography, since many block ciphers employ these as components in their S-boxes. The security of a block cipher depends upon the immunity of its substitution boxes against various kinds of cryptographic attacks. For instance, a low differential uniformity [13] to resist the differential attacks [5]. For a prime p and positive integer $n > 0$, the differential uniformity of an (n, n)-function $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ is defined as the maximum number of solutions x of the differential equation $F(x + a) - F(x) = b$, where $a \neq 0, b \in \mathbb{F}_{p^n}$. When differential uniformity is 1 then we say that the function is perfect nonlinear (or planar). It may be noted that planar functions exist only in the case of odd characteristic. The lowest possible differential uniformity of functions over finite fields of even characteristic is 2 and such functions are called almost perfect nonlinear (APN). APN functions in characteristic 2 have been studied since the 90's and a lot of research has been done in this direction in recent years (see [6] and references therein). The construction of bijective APN functions over even characteristic fields is quite challenging. Recently, Beierle and Leander [4] found two new APN permutations in dimension 9, namely

$$x \mapsto x^3 + ux^{10} + u^2x^{17} + u^4x^{80} + u^5x^{192},$$
$$x \mapsto x^3 + u^2x^{10} + ux^{24} + u^4x^{80} + u^6x^{136}.$$

Later, Beierle et al. [3] showed that, up to extended affine equivalence, the above two APN permutations can be represented by a single trivariate function $C_u : \mathbb{F}_{2^m}^3 \to \mathbb{F}_{2^m}^3$ given by

$$(X, Y, Z) \mapsto (X^3 + uY^2Z, Y^3 + uXZ^2, Z^3 + uX^2Y),$$

where $m = 3$ and $u \in \mathbb{F}_{2^m} \backslash \{0, 1\}$. For $m > 3$, the authors have proposed the following conjecture.

Conjecture 1 ([3])**.** Let $m > 3$ and let $u \in \mathbb{F}_{2^m}^*$. Then the function $C_u : \mathbb{F}_{2^m}^3 \to \mathbb{F}_{2^m}^3$ given by

$$(X, Y, Z) \mapsto (X^3 + uY^2Z, Y^3 + uXZ^2, Z^3 + uX^2Y)$$

is not a permutation. Furthermore, C_u is not APN.

In 2022, Bartoli and Timpanella [2] proved that C_u is not APN for $m > 20$. Together with the experimental results in small dimensions, this proved the first part of the above conjecture. It is the intent of this note to prove the remaining part of the above conjecture. It is worth mentioning here that the APN permutations given in [4] is generalised into an infinite family of APN functions in trivariate form in [12].

We use the tools from the theory of algebraic curves to show the validity of the Conjecture 1. For more details, we refer interested readers to [9, 10]. We denote, as usual, by $\mathbb{P}^r(\mathbb{F}_q)$ and $\mathbb{A}^r(\mathbb{F}_q)$ (or $\mathbb{F}_q^r$) the projective and the affine space of dimension $r \in \mathbb{N}$ over the finite field $\mathbb{F}_q$, respectively. A variety, and more specifically a curve or a surface (i.e. a variety of dimension 1 or 2, respectively), is described by a certain set of equations with coefficients in $\mathbb{F}_q$. We say that a variety $\mathcal{V}$ is *absolutely irreducible* if there are no varieties $\mathcal{V}'$ and $\mathcal{V}''$ defined over the algebraic closure of $\mathbb{F}_q$ (denoted by $\overline{\mathbb{F}_q}$) and different from $\mathcal{V}$ such that $\mathcal{V} = \mathcal{V}' \cup \mathcal{V}''$. If a variety $\mathcal{V} \subseteq \mathbb{A}^r(\mathbb{F}_q)$ is defined by $F_i(X_1, \ldots, X_r) = 0$, for $i = 1, \ldots s$, an $\mathbb{F}_q$-rational point of $\mathcal{V}$ is a point $(x_1,\ldots,x_r)\in\mathbb{A}^r(\mathbb{F}_q)$ such that $F_i(x_1,\ldots,x_r)=0$, for $i=1,\ldots,s$. The set of the $\mathbb{F}_q$-rational points of $\mathcal{V}$ is usually denoted by $\mathcal{V}(\mathbb{F}_q)$. If $s=1$, $\mathcal{V}$ is called a hypersurface and it is absolutely irreducible if the corresponding polynomial $F(X_1,\ldots,X_r)$ is absolutely irreducible, i.e. it possesses no non-trivial factors over $\overline{\mathbb{F}_q}$. Moreover, we say that $\mathcal{V}$ is a variety of degree d (and write $\deg(\mathcal{V})=d$) if $d=\#(\mathcal{V}\cap H)$, where $H\subseteq\mathbb{A}^r(\overline{\mathbb{F}_q})$ is a general projective subspace of dimension $r-s$. To determine the degree of a variety is generally not straighforward; however an upper bound to $\deg(\mathcal{V})$ is given by $\prod_{i=1}^s\deg(F_i)$. We also recall that the Frobenius map $\Phi_q : x\mapsto x^q$ is an automorphism of $\mathbb{F}_{q^k}$ and generates the group $Gal(\mathbb{F}_{q^k}/\mathbb{F}_q)$ of automorphisms of $\mathbb{F}_{q^k}$ that fixes $\mathbb{F}_q$ pointwise. The Frobenius automorphism induces also a collineation of $\mathbb{A}^r(\overline{\mathbb{F}_q})$ and an automorphism of $\overline{\mathbb{F}_q}[X_1,\ldots,X_r]$.

A crucial point in our investigation of permutation trinomials over $\mathbb{F}_{q^3}$ is to prove the existence of suitable $\mathbb{F}_q$-rational points in algebraic surfaces $\mathcal{V}$ attached to each permutation trinomial. This is reached by proving the existence of absolutely irreducible $\mathbb{F}_q$-rational components in $\mathcal{V}$ and lower bounding the number of their $\mathbb{F}_q$-rational points. To this end, generalizations of Lang-Weil type bounds for algebraic varieties are needed. To ensure the existence of a suitable $\mathbb{F}_q$-rational point of $\mathcal{V}$, we need the following result.

Theorem 2. [8, Theorem 7.1] *Let $\mathcal{V}\subseteq\mathbb{A}^n(\mathbb{F}_q)$ be an absolutely irreducible variety defined over $\mathbb{F}_q$ of dimension $r>0$ and degree δ. If $q>2(r+1)\delta^2$, then the following estimate holds:*

$$\left|\#(\mathcal{V}(\mathbb{A}^n(\mathbb{F}_q)))-q^r\right|\leq(\delta-1)(\delta-2)q^{r-1/2}+5\delta^{13/3}q^{r-1}. \tag{1}$$

In our approach we will make use of the following result

Lemma 3. [1, Lemma 2.1] *Let $\mathcal{H}$ be a projective hypersurface and $\mathcal{X}$ a projective variety of dimension $n-1$ in $\mathbb{P}^n(\mathbb{F}_q)$. If $\mathcal{X}\cap\mathcal{H}$ has a non-repeated absolutely irreducible component defined over $\mathbb{F}_q$ then $\mathcal{X}$ has a non-repeated absolutely irreducible component defined over $\mathbb{F}_q$.*

2 Main result

In this section, we shall show the validity of the Conjecture 1 for m large enough. It is easy to observe that when m is even then C_u is not a permutation as in this case $C_u(X,0,0)=(X^3,0,0)$ and the function $X\mapsto X^3$ is 3-to-1. In what follows we assume that m is odd. Note that C_u is a permutation if and only if for all $\alpha,\beta,\gamma\in\mathbb{F}_{2^m}$, $(\alpha,\beta,\gamma)\neq(0,0,0)$, the equation

$$C_u(X+\alpha,Y+\beta,Z+\gamma)+C_u(X,Y,Z)=0$$

has only the trivial solutions $\{(x,y,z)=(0,0,0)\ :\ x,y,z\in\mathbb{F}_{2^m}\}$. Such a condition reads

$$\begin{cases}\alpha X^2+\alpha^2X+u\gamma Y^2+u\beta^2Z & =\alpha^3+u\beta^2\gamma\\ \beta Y^2+\beta^2Y+u\gamma^2X+u\alpha Z^2 & =\beta^3+u\gamma^2\alpha\\ \gamma Z^2+\gamma^2Z+u\beta X^2+u\alpha^2Y & =\gamma^3+u\alpha^2\beta.\end{cases} \tag{2}$$

Before we take our algebraic geometry approach, we make some observations. First, assume that only one among α, β and γ is nonzero. Without loss of generality (here because of the symmetric property of C_u), we may assume that $\alpha \neq 0$ and $\beta = \gamma = 0$. Then System (2) becomes

$$\begin{cases} \alpha X^2 + \alpha^2 X + \alpha^3 & = 0 \\ u\alpha Z^2 & = 0 \\ u\alpha^2 Y & = 0. \end{cases}$$

It is straightforward to see that the first equation of the above system has no solution $X \in \mathbb{F}_{2^m}$ as m is odd.

Next, we assume that only one among α, β and γ is zero. Again, we may assume that $\alpha, \beta \neq 0$ and $\gamma = 0$. Then System (2) becomes

$$\begin{cases} \alpha X^2 + \alpha^2 X + u\beta^2 Z & = \alpha^3 \\ \beta Y^2 + \beta^2 Y + u\alpha Z^2 & = \beta^3 \\ u\beta X^2 + u\alpha^2 Y & = u\alpha^2\beta, \end{cases} \tag{3}$$

which can be further simplified by replacing $X \mapsto \alpha X$ and $Y \mapsto \beta Y$, i.e., System (3) is equivalent to the following system

$$\begin{cases} \alpha^3(X^2 + X + 1) + u\beta^2 Z & = 0 \\ \beta^3(Y^2 + Y + 1) + u\alpha Z^2 & = 0 \\ X^2 + Y + 1 & = 0. \end{cases} \tag{4}$$

Now, squaring the first equation and putting $X^2 = Y + 1$ into it, we have

$$\alpha^6(Y^2 + Y + 1) + u^2\beta^4 Z^2 = 0.$$

Multiplying the above equation by α and putting $u\alpha Z^2 = \beta^3(Y^2 + Y + 1)$, we have

$$(\alpha^7 + u\beta^7)(Y^2 + Y + 1) = 0.$$

Thus, System (4) is equivalent to the following system

$$\begin{cases} (\alpha^7 + u\beta^7)(Y^2 + Y + 1) & = 0 \\ \beta^3(Y^2 + Y + 1) + u\alpha Z^2 & = 0 \\ X^2 + Y + 1 & = 0. \end{cases}$$

Notice that if $\alpha^7 + u\beta^7 = 0$, i.e., u is a 7^{th} power then the above system has nonzero solutions $(X, Y, Z) \in \mathbb{F}_q^3$ and consequently C_u is not a permutation. When u is not a 7^{th} power then the first equation of this system has no solution $X \in \mathbb{F}_{2^m}$ for m odd. Thus, in what follows, we assume that u is not a 7^{th} power and m is odd.

Now we take our general approach, which will show the conjecture if m is large enough. The above System (2) is equivalent to

$$\begin{cases} \alpha^6 + \alpha^4 X^2 + \alpha^2 X^4 + \beta^4\gamma u^2 + \beta^4 Z u^2 + \gamma Y^4 u^2 & = 0 \\ \alpha^2\gamma^2 u^2 + \alpha^2 Z^2 u^2 + \beta^6 + \beta^4 Y^2 + \beta^2 Y^4 + \gamma^2 X^2 u^2 & = 0 \\ \alpha^4\beta^2 u^2 + \alpha^4 Y^2 u^2 + \beta^2 X^4 u^2 + \gamma^3 + \gamma^2 Z + \gamma Z^2 & = 0. \end{cases} \tag{5}$$

Let

$$\begin{aligned}
f(\alpha,\beta,X,Y) &:= \frac{\alpha^7+\alpha^5X^2+\alpha^3X^4+\beta^7u+\beta^6Yu+\beta^5Y^2u}{u^2(\alpha Y^4+\beta^4X)}\\
g(\alpha,\beta,X,Y) &:= (\alpha^7+\alpha^6X+\alpha^5X^2+\alpha^4X^3+\alpha^3X^4+\alpha^2X^5+\beta^7u+\beta^6Yu\\
&\quad+\beta^5Y^2u+\beta^3Y^4u+\beta^2Y^5u+\beta Y^6u)/(u^2(\alpha Y^4+\beta^4X))\\
h(\alpha,\beta,X,Y) &:= (\alpha^{21}+\alpha^{20}X+\alpha^{18}X^3+\alpha^{17}X^4+\alpha^{15}X^6+\alpha^{14}\beta^7u+\alpha^{14}\beta^6Yu+\alpha^{14}\beta^5Y^2u\\
&\quad+\alpha^{14}\beta^3Y^4u+\alpha^{14}\beta^2Y^5u+\alpha^{14}\beta Y^6u+\alpha^{14}X^7+\alpha^{13}X^8+\alpha^{12}\beta^7X^2u\\
&\quad+\alpha^{12}\beta^6X^2Yu+\alpha^{12}\beta^5X^2Y^2u+\alpha^{11}X^{10}+\alpha^{10}\beta^7X^4u+\alpha^{10}\beta^6X^4Yu\\
&\quad+\alpha^{10}\beta^5X^4Y^2u+\alpha^{10}\beta^3X^4Y^4u+\alpha^{10}\beta^2X^4Y^5u+\alpha^{10}\beta X^4Y^6u+\alpha^{10}X^{11}\\
&\quad+\alpha^8\beta^7X^6u+\alpha^8\beta^6X^6Yu+\alpha^8\beta^5X^6Y^2u+\alpha^8X^{13}+\alpha^7\beta^{14}u^2+\alpha^7\beta^{12}Y^2u^2\\
&\quad+\alpha^7\beta^{10}Y^4u^2+\alpha^7\beta^6Y^8u^2+\alpha^7\beta^4Y^{10}u^2+\alpha^7\beta^2Y^{12}u^8+\alpha^7\beta^2Y^{12}u^2+\alpha^7X^{14}\\
&\quad+\alpha^6\beta^{14}Xu^2+\alpha^6\beta^{12}XY^2u^2+\alpha^6\beta^{10}XY^4u^2+\alpha^6\beta^7X^8u+\alpha^6\beta^6X^8Yu\\
&\quad+\alpha^6\beta^6XY^8u^8+\alpha^6\beta^5X^8Y^2u+\alpha^6\beta^3X^8Y^4u+\alpha^6\beta^2X^8Y^5u+\alpha^6\beta X^8Y^6u\\
&\quad+\alpha^5\beta^{14}X^2u^2+\alpha^5\beta^{12}X^2Y^2u^2+\alpha^5\beta^{10}X^2Y^4u^8+\alpha^5\beta^{10}X^2Y^4u^2\\
&\quad+\alpha^5\beta^6X^2Y^8u^2+\alpha^5\beta^4X^2Y^{10}u^2+\alpha^5\beta^2X^2Y^{12}u^2+\alpha^7Y^{14}u^8\\
&\quad+\alpha^4\beta^{14}X^3u^8+\alpha^4\beta^{14}X^3u^2+\alpha^4\beta^{12}X^3Y^2u^2+\alpha^4\beta^{10}X^3Y^4u^2\\
&\quad+\alpha^4\beta^7X^{10}u+\alpha^4\beta^6X^{10}Yu+\alpha^4\beta^5X^{10}Y^2u+\alpha^6\beta^4XY^{10}u^8\\
&\quad+\alpha^3\beta^{14}X^4u^2+\alpha^3\beta^{12}X^4Y^2u^2+\alpha^3\beta^{10}X^4Y^4u^2+\alpha^5\beta^8X^2Y^6u^8+\alpha^3\beta^6X^4Y^8u^2\\
&\quad+\alpha^3\beta^4X^4Y^{10}u^2+\alpha^3\beta^2X^4Y^{12}u^8+\alpha^3\beta^2X^4Y^{12}u^2+\alpha^2\beta^{14}X^5u^2+\alpha^2\beta^{12}X^5Y^2u^2\\
&\quad+\alpha^4\beta^{12}X^3Y^2u^8+\alpha^2\beta^{10}X^5Y^4u^2+\alpha^2\beta^6X^5Y^8u^8+\alpha\beta^{10}X^6Y^4u^8+\beta^{21}u^3\\
&\quad+\beta^{20}Yu^3+\beta^{18}Y^3u^3+\beta^{17}Y^4u^3+\beta^{15}Y^6u^3+\beta^{14}X^7u^8+\beta^{14}Y^7u^3+\beta^{13}Y^8u^3\\
&\quad+\beta^{11}Y^{10}u^3+\beta^{10}Y^{11}u^3+\beta^8Y^{13}u^3+\beta^7Y^{14}u^3=0.
\end{aligned}$$

Proposition 4. *Each element of*

$$\begin{aligned}\Theta := \quad &\{(x,y,z,a,b,c)\in\mathbb{F}_q^6 : ay^4+b^4x\neq 0,\ z=g(a,b,x,y),\\ &\qquad c=f(a,b,x,y), h(a,b,x,y)=0\}\end{aligned}$$

is a solution of System (5)*.*

Proof. This is easily checked via direct computations in MAGMA [7]. More precisely, in System (5), the values of $Z=g(\alpha,\beta,X,Y)$ and $\gamma=f(\alpha,\beta,X,Y)$ are substituted into each of the three equations. Subsequently, it is confirmed that the resulting equations (in the remaining variables), after eliminating the denominators, have the polynomial h as a factor. This confirmation ensures that the set Θ comprises a subset of the solutions to System (5). □

Proposition 5. *Let $\mathcal{V}\subset\mathbb{A}^6(\mathbb{F}_q)$ be the variety defined by*

$$\begin{cases} X_6 = g(X_1,X_2,X_3,X_4)\\ X_5 = f(X_1,X_2,X_3,X_4)\\ h(X_1,X_2,X_3,X_4)=0.\end{cases}$$

Then $\mathcal{V}$ contains an absolutely irreducible component defined over $\mathbb{F}_q$, distinct from $X_1 = X_2 = X_5 = 0$, of degree at most 216, and not contained in $X_1X_4^4 \neq X_2^4X_3$.

Proof. Note that $h(X_1, X_2, X_3, X_4) = 0$ is a homogeneous polynomial of degree 21 and thus it defines a surface $\mathcal{S}$ in $\mathbb{P}^3(\mathbb{F}_q)$. It is possible to show that the intersection $\mathcal{S}'$ between $\mathcal{S}$ and the plane $X_4 = 0$ contains an absolutely irreducible $\mathbb{F}_q$-rational component which is not repeated. More precisely, we examine the (affine) curve $\mathcal{C} := \mathcal{S}' \cap (X_5 = 0) \cap (X_4 = 1)$. This curve is of degree 21, and its highest homogeneous part factorizes into $\prod_{\lambda \in \mathbb{F}_8^*}(X_1 + \lambda\overline{u}X_2)^3$, where $\overline{u}$ represents a fixed 7-th root of u. Consequently, linear components of $\mathcal{C}$ can be expressed as $X_1 + \lambda\overline{u}X_2 + \mu = 0$, where $\mu \in \overline{\mathbb{F}}$. However, a verification confirms this is not the case. It is evident that $\mathcal{C}$ cannot decompose into components all of degree 2. Potential components of degree 3 take the form $(X_1 + \lambda_1\overline{u}X_2)(X_1 + \lambda_2\overline{u}X_2)(X_1 + \lambda_3\overline{u}X_2) + H(X_1, X_2) = 0$, with $\deg H(X_1, X_2) \leq 2$. A detailed analysis reveals that at least one these cubic components is $\mathbb{F}_q$-rational. Thus, we can dismiss the possibility of $\mathcal{C}$ containing cubic components as well. The only remaining possibility is that $\mathcal{C}$ splits into three absolutely irreducible components of degree 7. Once again, further analysis demonstrates that if this scenario occurs, at least one of them is $\mathbb{F}_q$-rational. By Lemma 3, $\mathcal{S}$ contains an absolutely irreducible $\mathbb{F}_q$-rational component $\mathcal{S}'$. It is easily seen that such a component of $\mathcal{S}$ is different from $X_1 = X_2 = 0$.

Clearly, $\mathcal{S}'$ extends to a variety $\mathcal{V}'$ contained in $\mathcal{V}$, absolutely irreducible and $\mathbb{F}_q$-rational (by considering the two extra equations $X_6 = g(X_1, X_2, X_3, X_4)$ $X_5 = f(X_1, X_2, X_3, X_4)$). Since $\mathcal{S}$ is different from $X_1 = X_2 = 0$, $\mathcal{V}'$ is different from $X_1 = X_2 = X_5 = 0$. The degree of $\mathcal{V}'$ is upper bounded by the degree of $\mathcal{V}$, that is at most $6^3 = 216$. □

The following is the main result of our paper.

Theorem 6. *If m is large enough, Conjecture 1 is true.*

Proof. By Proposition 5 and Theorem 2, if m is large enough, the absolutely irreducible $\mathbb{F}_q$-rational component $\mathcal{V}'$ (and thus $\mathcal{V}$) possesses roughly q^3 of $\mathbb{F}_q$-rational points. Since $\mathcal{V}'$ is not $X_1 = X_2 = X_5 = 0$ and it not contained in $X_1X_4^4 \neq X_2^4X_3$, the set Θ is not empty and the claim follows. □

Remark 7. Using Theorem 2 it is possible to give a more accurate estimate for the minimum integer m that confirms the conjecture. First, notice that points of $\mathcal{V}'$ not belonging to $X_1X_4^4 = X_2^4X_3$ correspond to quadruples $(x_1, x_2, x_3, x_4) \in \mathbb{F}_q^4$ such that $h(x_1, x_2, x_3, x_4) = 0$ and $x_1x_4^4 \neq x_2^4x_3$. Since $(X_1X_4^4 + X_2^4X_3)$ and $h(X_1, X_2, X_3, X_4)$ are homogeneous polynomials of degree 5 and 21 respectively and $(X_1X_4^4 + X_2^4X_3) \nmid h(X_1, X_2, X_3, X_4)$ their intersection is a projective space curve of degree 105 and it contains at most $104q + 1$ projective $\mathbb{F}_q$-rational points; see [11]. This shows the existence of at most $(104q + 1)(q - 1)$ quadruples $(x_1, x_2, x_3, x_4) \in \mathbb{F}_q^4$ such that $h(x_1, x_2, x_3, x_4) = 0$ and $x_1x_4^4 = x_2^4x_3$. All the other quadruples (x_1, x_2, x_3, x_4) satisfying $h(x_1, x_2, x_3, x_4) = 0$ and $x_1x_4^4 \neq x_2^4x_3$ also verify $x_1 \neq x_2$. If $m \geq 37$, by Theorem 2 the number of $\mathbb{F}_q$-rational points in $\mathcal{V}'$ is at least

$$q^3 - 215 \cdot 214 \cdot q^{5/2} - 5 \cdot (216)^{13/3}q^2 - (104q + 1)(q - 1),$$

that is larger than 0 and thus Conjecture 1 holds true.

References

[1] Y. Aubry, G. McGuire, F. Rodier, *A few more functions that are not APN infinitely often*, In Finite fields: theory and applications, vol. 518 of Contemp. Math. Amer. Math. Soc., Providence, RI, 2010, pp. 23–31.

[2] D. Bartoli, M. Timpanella, *On a conjecture on APN permutations*, Cryptogr. Commun. 14 (2022), 925–931.

[3] C. Beierle, C. Carlet, G. Leander, L. Perrin, *A further study of quadratic APN permutations in dimension nine*, Finite Fields Appl. 81 (2022), 102049.

[4] C. Beierle, G. Leander, *New instances of quadratic APN functions*, IEEE Trans. Inf. Theory 68(1) (2022), 670—678.

[5] E. Biham, A. Shamir, *Differential cryptanalysis of DES-like cryptosystems*, J. Cryptol. 4(1) (1991), 3–72.

[6] L. Budaghyan, M. Calderini, C. Carlet, D. Davidova, N. Kaleyski, *On two fundamental problems on APN power functions*, IEEE Trans. Inf. Theory 68(5) (2022) 3389–3403.

[7] W. Bosma, J. Cannon, C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. 24(3-4) (1993), 235–265.

[8] A. Cafure, G. Matera, *Improved explicit estimates on the number of solutions of equations over a finite field*, Finite Fields Appl. 12(2) (2006), 155–185.

[9] R. Hartshorne, Algebraic geometry, Graduate Texts in Mathematics, no. 52, Springer–Verlag, New York-Heidelberg, 1977.

[10] J.W.P. Hirschfeld, G. Korchmáros, F. Torres, Algebraic curves over a finite field, Princeton University Press, 2013.

[11] M. Homma, *A bound on the number of points of a curve in projective space over a finite field*, Theory and Applications of Finite Fields in: Contemp. Mat. 579, 103–110 (2012).

[12] K. Li, N. Kaleyski, *Two new infinite families of apn functions in trivariate form*, IEEE Trans. Inf. Theory 70(2) (2024), 1436–1452.

[13] K. Nyberg, *Differentially uniform mappings for cryptography*, In: Helleseth, T. (ed.) EUROCRYPT 1993, LNCS, vol. 765, pp. 55-64. Springer, Heidelberg (1994)