Open Access
Baghdad Science Journal **Vol.13(4)2016**

DOI: http://dx.doi.org/10.21123/bsj.2016.13.3.0846

Classification of Elliptic Cubic Curves Over The Finite Field of Order Nineteen

Emad Bakr Al-Zangana

Department of Mathematics, College of Science, Al-Mustansiriyah University

E-mail: emad77_kaka@yahoo.com

Received 1/ 6/2015
Accepted 20/ 12/2015

Abstract:

Plane cubics curves may be classified up to isomorphism or projective equivalence. In this paper, the inequivalent elliptic cubic curves which are non-singular plane cubic curves have been classified projectively over the finite field of order nineteen, and determined if they are complete or incomplete as arcs of degree three. Also, the maximum size of a complete elliptic curve that can be constructed from each incomplete elliptic curve are given.

Key words: Finite geometry, Coding Theory, Elliptic cubic curve, Arc, Inflexion.

Introduction:

Let $GF(q) = F_q$ denote the Galois field of order q, where q is prime number, and

$V(3, q) = \{X = (x_1, x_2, x_3) | x_i \in F_q\}$

be the respective vector space of row vectors of length three with entries in F_q. Let $PG(2, q)$ be the corresponding projective plane. The points $P(X) = [x_1; x_2; x_3]$ of $PG(2, q)$ are the one-dimensional subspaces of $V(3, q)$. The lines of $PG(2, q)$ are the two-dimensional subspaces of $V(3, q)$. For further details, see [1][2].

Definition [1] 1: Let F be a form. A projective plane curve $\mathcal{F}$ is the set

$\mathcal{F} = \{P(X) \in PG(2, q) | F(X) = 0\}$.

A point $P(X)$ of F is a rational point of $\mathcal{F}$.

Theorem (Serre [3]) 2: If $\mathcal{F}$ is an elliptic cubic curve defined over F_q, and N_1 is the number of rational points of $\mathcal{F}$ over F_q. Then

$q + 1 - \lfloor 2\sqrt{q} \rfloor \leq N_1 \leq q + 1 + \lfloor 2\sqrt{q} \rfloor$,

where $\lfloor x \rfloor$ is the integer part of $x \in \mathbb{R}$.

Definition [2] 3: A rational inflexion point P of an elliptic cubic curve $\mathcal{F}$ is one for which the unique tangent at P has three-point contact.

The condition that the tangent line at P has triple contact with the curve is expressed algebraically by the requirement that

$$F(X_0, X_1, X_2) = f(X_0, X_1, X_2) \cdot g(X_0, X_1, X_2) + (aX_0 + bX_1 + cX_2)^3 . h(X_0, X_1, X_2),$$

where F is a form of degree n and

(i) $f(X_0, X_1, X_2)$ is the linear form defining the tangent line at P,

(ii) $g(X_0, X_1, X_2)$ is some form of degree $n - 1$,

(iii) $h(X_0, X_1, X_2)$ is a form of degree $n-3$,
(iv) $(aX_0+bX_1+cX_2)$ is some linear form vanishing at P. See [4].

Definition [2] 4: An elliptic cubic curve $\mathcal{F}$ is called harmonic or equianharmonic if the four tangents through a point form a harmonic or equianharmonic set. An elliptic cubic curve which is not harmonic or equianharmonic is called general**.**

It is well known that any elliptic cubic curve $\mathcal{F}$ has nine rational inflexions over $\bar{F}_q$, $q \not\equiv 0\ (mod\ 3)$. Over F_q, the possible number of rational inflexions on an elliptic cubic curve is 0,1,3 or 9 . An elliptic cubic curve exist with nine rational inflexions if $q \equiv 1\ (mod\ 3)$ and with three rational inflexions for all q. See [2, Chapter 11].

Theorem [2][5] 5: If P_q is the numbers of distinct elliptic cubic curves up to projective equivalence over F_q, then

$$P_q = 3q + 2 + \left(\frac{-4}{q}\right) + \left(\frac{-3}{q}\right)^2 + 3\left(\frac{-3}{q}\right).$$

Here the bracketed numbers are Legendre and Legendre–Jacobi symbols taking the values $-1, 0, 1$.

Let n_i for $i = 0,1,3,9$ be the number of projective equivalence classes with exactly i rational inflexions**.** So, according to n_i, $P_q = n_0 + n_1 + n_3 + n_9$.

Definition [2] 6: A rational inflexional triangle is a set of three lines over F_q through the nine inflexions of $\mathcal{F}$.

An elliptic cubic curve $\mathcal{F}$over F_q, $q \not\equiv 0\ (mod\ 3)$, is denoted by $\mathcal{F}_n^r$, where n is the number of rational inflexions and r is the number of rational inflexional triangles. Here, $\mathcal{F}_n^r = \mathcal{G}_n^r,\ \mathcal{H}_n^r,\ \mathcal{E}_n^r$ when $\mathcal{F}$ is respectively general, equianharmonic, harmonic. Also, if $n = 3$ and the inflexions tangent are concurrent then $\mathcal{F} = \mathcal{E}$ and if $n = 0$ and $\mathcal{F}$ is equianharmonic write $\mathcal{F} = \bar{\mathcal{E}}_0^4$. See [2].

Definition [2] 7: A $(k;r)$-arc K, is a set of k points of a projective plane such that some r, but no $r+1$ of them are collinear. It is also called arc of degree r.

Definition [2] 8: A$(k;r)$-arc is called complete if it is not contained within $(k+1;n)$-arc.

Definition [2] 9: The maximum size of a $(k;r)$-arc in $PG(2,q)$is denoted by $m_r(2,q)$.

Definition [2] 10: Let $\mathcal{M}$ be a set of points in any plane. An i-secant is a line meeting $\mathcal{M}$ in exactly i points.

In the projective plane, most of elliptic cubic curves can be regarded as an arc of degree three.

Questions about elliptic cubic curves over a finite field F_q:

(1) How many inequivalent elliptic cubic curves are there?
(2) How many complete and incomplete elliptic cubic curves are there?
(3) What is the maximum size of a complete arc of degree three that can be constructed from each incomplete arc?
(4) Is there a complete elliptic cubic curve (complete arc of degree three) constructed from the incomplete elliptic cubic curve of size equal to $m_3(2,q)$?

Question one has been investigated in [2] for F_q, $2 \le q \le 13$, and also answered for $q = 17$ in [6]. Question two and three have been answered for $q = 2,3,5,7$ in [7], $q = 11,13$ in [8] and for $q = 17$ in [6].

The largest size of an $(n;r)$-arc of $PG(k,q)$ is indicated by $m_r(k,q)$. In [4] and [5], bounds for $m_r(2,q)$ are given. In particular, $m_r(2,q) \le 2q + 1$ for $q \ge 4$; see [6].

Question four is a part of another question which is*: what is the value of* $m_r(k,q)$ *when* $r = 2$ *and* $= 2$?

The value of $m_3(2,q)$ has been given in [2] for $2 \le q \le 13$. In [7], a full classification of $(n;3)$-arc have been given for $q = 7,11$ in [9][10], and maximal arcs of degree three have been found in [11].

The aim of this paper is to answer question two and three over F_q, $q = 2,3,5,7$.

The aim of this paper is to answer these four questions over F_{19}. To do that, the following steps have been taken:

(1) Finding projectively distinct elliptic cubic curves in $PG(2,19)$.

(2) For each of these, write down the canonical form.

(3) Then list the rational points of each one.

(4) The complete and incomplete elliptic cubic curves have been determined with stabilizer group type.

(5) The size of complete arcs of degree three that contain the incomplete ones are given.

(6) Finally, the corresponding AMDS codes parameters for these arcs of degree three have been computed.

Canonical Form of an Elliptic Cubic Curve Over a Finite Field

Theorem [2] **11:** A non-singular plane cubic curve with form F and nine rational inflexions exists over F_q if and only if $q \equiv 1\ (mod\ 3)$, and then F has canonical form

$$F = X_0^3X_1^3X_2^3 - 3cX_0X_1X_2.$$

Theorem [2] **12:** A non-singular plane cubic curve with form F and three rational inflexions exists over F_q for all q. The inflexions are necessary collinear.

(i) If the inflexional tangent are concurrent, the canonical forms are as follows:

(a) $q \equiv 0,2\ (mod\ 3)$,
$$F = X_0X_1(X_0+X_1) + X_3^3;$$

(b) $q \equiv 1\ (mod\ 3)$,
$$F = X_0X_1(X_0+X_1) + X_3^3;$$
$$F = X_0X_1(X_0+X_1) + cX_3^3;$$
$$F = X_0X_1(X_0+X_1) + cX_3^3;$$

where c is a primitive of F_q. Here, F will denote by $\bar{\mathcal{E}}$.

(ii) If the inflexional tangent are not concurrent, the canonical form is as follows:
$$F = X_0X_1X_2 + e(X_0+X_1+X_2)^3,$$
$$e \neq 0, 1/27\ .$$

Theorem [2] **13:** A non-singular plane cubic curve with form F defined over F_q, $q = p^h$ and at least one rational inflexion has one of following canonical forms.

(i) $p \neq 2,3$,
$F = X_2^2X_1 + X_0^3 + cX_0X_1^2 + dX_1^3$,
where $4c^3 + 27d^2 \neq 0$.

(ii) $p = 3$,
(a) $F = X_2^2X_1 + X_0^3 + bX_1X_0^2 + dX_1^3$,
where $bd \neq 0$.
(b) $F = X_2^2X_1 + X_0^3 + cX_0X_1^2 + dX_1^3$,
where $c \neq 0$.

(iii) $p = 2$,
(a) $F = X_1X_2^2 + X_0X_1X_2 + X_0^3 + bX_0^2X_1 + cX_0X_1^2$,

where $b = 0$ or a fixed element of trace 1, and $c \neq 0$;
(b) $F = X_2^2X_1 + X_2X_1^2 + eX_0^3 + cX_0X_1^2 + dX_1^3$,
where $e = 1$ when $(q-1,3) = 1$ and $e = 1, \alpha, \alpha^2$ when $(q-1,3) = 3$, with α a primitive element of F_q; also, $d = 0$ or a particular element of trace 1.

Theorem [2] **14:** A non-singular plane cubic curve with form F defined over F_q, $q = p^h$, with no rational inflexion has one of following canonical forms.

(i) $q \equiv -1\ (mod\ 3)$,
$$F = X_2^3 - 3c(X_0^2 - dX_0X_1 + X_1^2)X_2 - (X_0^3 - 3X_0X_1^2 + dX_1^3),$$
where $X^3 - 3X + d$ is irreducible.

(ii) $q \equiv 1\ (mod\ 3)$,
(a) $F = X_0^3 + \alpha X_1^3 + \alpha^2X_2^3 - 3cX_0X_1X_2$,
with α a primitive element of F_q.
(b) $F = X_0X_1^2 + X_0^2X_2 + eX_1X_2^3 - c(X_0^3 + eX_1^3 + e^2X_2^3 - 3eX_0X_1X_2)$,

with α a primitive element of F_q and $e = \alpha, \alpha^2$. Here, when $c \neq 0$, and $\mathcal{F}$ is equianharmonic, write $\mathcal{F} = \mathcal{E}_0^4$; when $c = 0$, and $\mathcal{F}$ is equianharmonic, write $\mathcal{F} = \bar{\mathcal{E}}_0^4$.

(iii) $q \equiv 0 \ (mod\ 3)$,

$F = X_0^3 + X_1^3 + cX_2^3 + dX_0^2X_2 + dX_0X_1^2 + d^2X_0X_2^2 + dX_1X_2^2$,
where $c \neq 1$ and $X^3 + dX - 1$ is a fixed irreducible polynomial over F_q.

Elliptic Cubic Curves Over $GF(19)$

Theorem 15: In $PG(2,19)$, the following are satisfied:

(1) $P_{19} = 62$.

(2) $n_0 = 20$, $n_1 = 26$, $n_3 = 14$, $n_9 = 2$.

(3) N_1 takes every value between 7 and 21.

(4) There are 306 elliptic cubic curve of type general with at least one inflexion and 34 of them are inequivalent.

(5) The 62 inequivalent elliptic cubic curves divided into 30 complete and 32 incomplete.

(6) An elliptic cubic curve with k points is a complete $(k;3)$-arc when k have the following values:
$18, 20, 21, 22, 23, 24, 25, 26, 27, 28$.

Full details on elliptic cubic curves over $GF(19)$ have been given in Tables 1, 2, 3, 4.

Table 1: Elliptic cubic curves with exactly nine rational inflexions

$\mathcal{F}_n^r$	Canonical form	$\lvert\mathcal{F}_n^r\rvert$	Description	$M(\mathcal{F}_n^r)$	G
$\mathcal{E}_9^4$	$X_0^3 + X_1^3 + X_2^3$	27	Complete	–	G_{54}
$\mathcal{G}_9^4$	$X_0^3 + X_1^3 + X_2^3 + 7X_0X_1X_2$	18	Incomplete	21	$(Z_3 \times Z_3) \rtimes Z_3$

The group G_{54} has 9 elements of order 2, 26 elements of order 3, and 18 elements of order 6.

Table 2: Elliptic cubic curves with exactly three rational inflexions

$\mathcal{F}_n^r$	No.	Canonical form	$\lvert\mathcal{F}_n^r\rvert$	Description	$M(\mathcal{F}_n^r)$	G
$\mathcal{G}_3^1$	1	$X_0X_1X_2 - 6(X_0 + X_1 + X_2)^3$	12	Incomplete	27	S_3
	2	$X_0X_1X_2 + 3(X_0 + X_1 + X_2)^3$	15	Incomplete	27	S_3
	3	$X_0X_1X_2 + 4(X_0 + X_1 + X_2)^3$	15	Incomplete	27	S_3
	4	$X_0X_1X_2 + (X_0 + X_1 + X_2)^3$	18	Incomplete	21	S_3
	5	$X_0X_1X_2 - 7(X_0 + X_1 + X_2)^3$	18	Incomplete	22	S_3
	6	$X_0X_1X_2 + 2(X_0 + X_1 + X_2)^3$	21	Complete	–	S_3
	7	$X_0X_1X_2 + 5(X_0 + X_1 + X_2)^3$	21	Complete	–	S_3
	8	$X_0X_1X_2 + 9(X_0 + X_1 + X_2)^3$	24	Complete	–	S_3
	9	$X_0X_1X_2 - 9(X_0 + X_1 + X_2)^3$	24	Complete	–	S_3
	10	$X_0X_1X_2 - 3(X_0 + X_1 + X_2)^3$	24	Complete	–	S_3
	11	$X_0X_1X_2 - 2(X_0 + X_1 + X_2)^3$	24	Complete	–	S_3
	12	$X_0X_1X_2 - 8(X_0 + X_1 + X_2)^3$	27	Complete	–	S_3
$\bar{\mathcal{E}}_3^1$	13	$X_0X_1(X_0 + X_1) + 2X_2^3$	12	Incomplete	27	$S_3 \times Z_3$
	14	$X_0X_1(X_0 + X_1) + 4X_2^3$	21	Complete	–	$S_3 \times Z_3$

Table 3: Elliptic cubic curves with exactly one rational inflexion

$\mathcal{F}_n^r$	No.	Canonical form	$\lvert\mathcal{F}_n^r\rvert$	Description	$M(\mathcal{F}_n^r)$	G
$\mathcal{G}_1^0$	1	$X_1X_2^2 + X_0^3 - 9X_0X_1^2 - 3X_1^3$	14	Incomplete	27	Z2
	2	$X_1X_2^2 + X_0^3 - 8X_0X_1^2 + 9X_1^3$	14	Incomplete	27	Z2
	3	$X_1X_2^2 + X_0^3 - 9X_0X_1^2 + 6X_1^3$	17	Incomplete	23	Z2
	4	$X_1X_2^2 + X_0^3 - 9X_0X_1^2 - 2X_1^3$	20	Incomplete	22	Z2
	5	$X_1X_2^2 + X_0^3 - 9X_0X_1^2 + 2X_1^3$	20	Incomplete	22	Z2
	6	$X_1X_2^2 + X_0^3 - 9X_0X_1^2 - 6X_1^3$	23	Complete	21	Z2
	7	$X_1X_2^2 + X_0^3 - 9X_0X_1^2 + 3X_1^3$	26	Complete	–	Z2
	8	$X_1X_2^2 + X_0^3 - 8X_0X_1^2 - 9X_1^3$	26	Complete	–	Z2
$\mathcal{H}_1^0$	9	$X_1X_2^2 + X_0^3 + X_0X_1^2$	20	Incomplete	21	Z2
	10	$X_1X_2^2 + X_0^3 + 2X_0X_1^2$	20	Complete	–	Z2
$\mathcal{G}_1^1$	11	$X_1X_2^2 + X_0^3 - 9X_0X_1^2 + 7X_1^3$	13	Incomplete	27	Z2
	12	$X_1X_2^2 + X_0^3 - 9X_0X_1^2 - 5X_1^3$	16	Incomplete	26	Z2
	13	$X_1X_2^2 + X_0^3 - 9X_0X_1^2 - 4X_1^3$	16	Incomplete	25	Z2
	14	$X_1X_2^2 + X_0^3 - 9X_0X_1^2 + 9X_1^3$	16	Incomplete	25	Z2
	15	$X_1X_2^2 + X_0^3 - 8X_0X_1^2 + 8X_1^3$	16	Incomplete	25	Z2
	16	$X_1X_2^2 + X_0^3 - 8X_0X_1^2 - 4X_1^3$	19	Incomplete	22	Z2
	17	$X_1X_2^2 + X_0^3 - 8X_0X_1^2 + X_1^3$	19	Incomplete	21	Z2
	18	$X_1X_2^2 + X_0^3 - 8X_0X_1^2 + 6X_1^3$	22	Incomplete	23	Z2
	19	$X_1X_2^2 + X_0^3 - 8X_0X_1^2 + 7X_1^3$	22	Incomplete	23	Z2
	20	$X_1X_2^2 + X_0^3 - 8X_0X_1^2 + 5X_1^3$	25	Complete	–	Z2
	21	$X_1X_2^2 + X_0^3 - 9X_0X_1^2 - X_1^3$	25	Complete	–	Z2
	22	$X_1X_2^2 + X_0^3 - 8X_0X_1^2 + 2X_1^3$	28	Complete	–	Z2
$\mathcal{E}_1^1$	23	$X_2^2X_1 + X_0^3 + 6X_1^3$	19	Incomplete	21	Z6
	24	$X_2^2X_1 + X_0^3 - 8X_1^3$	28	Complete	–	Z6
$\mathcal{G}_1^4$	25	$X_2^2X_1 + X_0^3 - 9X_0X_1^2 + 8X_1^3$	22	Complete	–	Z2
$\mathcal{E}_1^4$	26	$X_1X_2^2 + X_0^3 - 2X_1^3$	13	Incomplete	28	Z6

Table 4: Elliptic cubic curves with no rational inflexions

$\mathcal{F}_n^r$	No.	Canonical form	$\lvert\mathcal{F}_n^r\rvert$	Description	$M(\mathcal{F}_n^r)$	G
$\mathcal{G}_0^1$	1	$X_0X_1^2 + X_0^2X_2 + 4X_1X_2^2 - 5(X_0^3 + 4X_1^3 - 3X_2^3 + 7X_0X_1X_2)$	12	Incomplete	27	Z_3
	2	$X_0X_1^2 + X_0^2X_2 + 4X_1X_2^2 + 9(X_0^3 + 4X_1^3 - 3X_2^3 + 7X_0X_1X_2)$	15	Incomplete	26	Z_3
	3	$X_0X_1^2 + X_0^2X_2 + 2X_1X_2^2 - 4(X_0^3 + 2X_1^3 + 4X_2^3 - 6X_0X_1X_2)$	15	Incomplete	26	Z_3
	4	$X_0X_1^2 + X_0^2X_2 + 2X_1X_2^2 - 5(X_0^3 + 2X_1^3 + 4X_2^3 - 6X_0X_1X_2)$	18	Incomplete	21	Z_3
	5	$X_0X_1^2 + X_0^2X_2 + 4X_1X_2^2 - 2(X_0^3 + 4X_1^3 - 3X_2^3 + 7X_0X_1X_2)$	18	Incomplete	21	Z_3
	6	$X_0X_1^2 + X_0^2X_2 + 2X_1X_2^2 - (X_0^3 + 2X_1^3 + 4X_2^3 - 6X_0X_1X_2)$	21	Complete	–	Z_3
	7	$X_0X_1^2 + X_0^2X_2 + 2X_1X_2^2 - 2(X_0^3 + 2X_1^3 + 4X_2^3 - 6X_0X_1X_2)$	21	Complete	–	Z_3
	8	$X_0X_1^2 + X_0^2X_2 + 2X_1X_2^2 - 8(X_0^3 + 2X_1^3 + 4X_2^3 - 6X_0X_1X_2)$	24	Complete	–	Z_3
	9	$X_0X_1^2 + X_0^2X_2 + 2X_1X_2^2 + 9(X_0^3 + 2X_1^3 + 4X_2^3 - 6X_0X_1X_2)$	24	Complete	–	Z_3
	10	$X_0X_1^2 + X_0^2X_2 + 4X_1X_2^2 - (X_0^3 + 4X_1^3 - 3X_2^3 + 7X_0X_1X_2)$	24	Complete	–	Z_3
	11	$X_0X_1^2 + X_0^2X_2 + 4X_1X_2^2 - 8(X_0^3 + 4X_1^3 - 3X_2^3 + 7X_0X_1X_2)$	24	Complete	–	Z_3
	12	$X_0X_1^2 + X_0^2X_2 + 4X_1X_2^2 - 4(X_0^3 + 4X_1^3 - 3X_2^3 + 7X_0X_1X_2)$	27	Complete	–	Z_3
$\mathcal{E}_0^1$	13	$X_0X_1^2 + X_0^2X_2 + 2X_1X_2^2$	12	Incomplete	27	$Z_3 \times Z_3$
	14	$X_0X_1^2 + X_0^2X_2 + 4X_1X_2^2$	21	Complete	–	$Z_3 \times Z_3$
$\mathcal{G}_0^4$	15	$X_0^3 + 2X_1^3 + 4X_2^3 - 3X_0X_1X_2$	18	Complete	–	$Z_3 \times Z_3$
	16	$X_0^3 + 2X_1^3 + 4X_2^3 + 7X_0X_1X_2$	18	Incomplete	24	$Z_3 \times Z_3$
	17	$X_0^3 + 2X_1^3 + 4X_2^3 + 4X_0X_1X_2$	18	Complete	–	$Z_3 \times Z_3$
	18	$X_0^3 + 2X_1^3 + 4X_2^3 - 5X_0X_1X_2$	18	Incomplete	21	$Z_3 \times Z_3$
$\mathcal{E}_0^4$	19	$X_0^3 + 2X_1^3 + 4X_2^3 - 7X_0X_1X_2$	27	Complete	–	$Z_3 \times Z_3$
$\bar{\mathcal{E}}_0^4$	20	$X_0^3 + 2X_1^3 + 4X_2^3$	27	Complete	–	$Z_3 \times Z_3 \times Z_3$

AMDS Codes of Dimension Three

A linear q-ary $[n, k, d]$ code or an $[n, k, d]_q$ -code C is a subspace of $V(n, q)$, where the dimension of C is $dim\, C = k$, and the minimum distance is

$$d(C) = d = min\{w(x) \mid x \in C\backslash\{0\}\} = min\{d(x; y) \mid x \neq y\}.$$

Here, with $x = (x_1, \dots, x_n)$ and $y = (y_1, \dots, y_n)$,

$$w(x) = |\{i \mid x_i \neq 0\}|$$

is the weight of the word x and

$$d(x, y) = |\{i | x_i \neq y_i\}|$$

is the (Hamming) distance between the words x and y.

Definition[12] 16:

(i) An $[n, k, d]_q$ –code is called MDS if $d = n - k + 1$.

(ii) An $[n, k, d]_q$ –code is called AMDS if $d = n - k$.

(iii) A linear code for which any two columns of a generator matrix are linearly independent is called a projective code.

Theorem [12] 17: There exists a projective $[n, k, d]_q$-code if and only if there exists an $(n; n - d)$ −arc in $PG(k - 1, q)$.

Corollary 18: There is a one-to-one correspondence between $(n;\, 3)$-arcs in $PG(2,19)$ and projective $[n, 3, n - 3]_{19}$-codes C.

In Table 5, the AMDS codes corresponding to the $(n;\, 3)$-arcs for $12 \leq n \leq 28$ in $PG(2,19)$ and the parameter e of errors corrected are given.

Table 5: AMDS code over $PG(2, 19)$

(n; 3)−arc	AMDS code	e	(n; 3) −arc	AMDS code	e
(12; 3)-rc	$[12, 3, 9]_{19}$	4	(21; 3)-arc	$[21, 3, 8]_{19}$	8
(13;3)-arc	$[13, 3, 10]_{19}$	4	(22; 3)-arc	$[22, 3,19]_{19}$	9
(14;3)-arc	$[14, 3, 11]_{19}$	5	(23; 3)-arc	$[23, 3,20]_{19}$	9
(15;3)-arc	$[15, 3, 12]_{19}$	5	(24; 3)-arc	$[24, 3,21]_{19}$	10
(16;3)-arc	$[16, 3, 13]_{19}$	6	(25; 3)-arc	$[25, 3,22]_{19}$	10
(17;3)-arc	$[17, 3, 14]_{19}$	6	(26; 3)-arc	$[26, 3,23]_{19}$	11
(18;3)-arc	$[18, 3, 15]_{19}$	7	(27; 3)-arc	$[27,3, 24]_{19}$	11
(19;3)-arc	$[19, 3, 16]_{19}$	7	(28; 3)-arc	$[28, 3,25]_{19}$	12
(20;3)-arc	$[20, 3, 17]_{19}$	8			

References:

[1] Hirschfeld, J. W. P.; Korchmros, G. and Torres, F. 2008. Algebraic curves over a finite field. Princeton University Press.

[2] Hirschfeld, J. W. P.; Projective geometries over finite fields, 2nd edition. 1998. Oxford Mathematical Monographs, The Clarendon Press, Oxford University Press, New York.

[3] Hirschfeld, J. W. P., The numbers of points on a curve, and applications. 2006. Rend. Mat., Ser. VII, 26: Roma, 13-28.

[4] Bruen, A. A.; Hirschfeld, J. W. P. and Wehlau, D. L.; Cubic curves, finite geometry and cryptography. 2011. Acta Appl. Math., 115.

[5] Hirschfeld, J. W. P.; Curves of genus 3. 2010. Rend. Mat. Appl., (30):77-88.

[6] Al-Seraji, N. A.; The geometry of the plane of order seventeen and its application to error-correcting codes. 2010. Ph.D. Thesis, University of Sussex, United Kingdom.

[7] Al-Zangana E. B.; On Non-Singular Plane Cubics Curves Over F_q, $q = 2,3,5,7$. 2013. J. of Education, Al-Mustansiriyah University, Iraq, (1):149-160.

[8] Al-Zangana E. B.; Complete and incomplete elliptic curves over the finite field of order 11 1nd 13. 2013. J. of Science, Al-Mustansiriyah University, Iraq, 24(1):135-142.

[9] Marcugini, S., Milani, A and Pambianco, F.; Classification of the

$(n;3)$-arcs in $PG(2,7)$. 2004. J. Geom. (80):179-184.

[10] Cook, G.R., Arcs in a finite projective plane. 2011. Ph.D. Thesis, University of Sussex, United Kingdom.

[11] Marcugini, S.; Milani, A. and Pambianco, F.; Maximal$(n;3)$-arcs in $PG(2,13)$. 2005. Discrete Mathematics, 294: 139-145**.**

[12] Ball, S. and Hirschfeld, J. W. P.; Bounds on (n; r)-arcs and their application to linear codes. 2005. Finite Fields Appl., (11): 326-336.

تصنيف المنحنيات التكعيبية الاهليليجية على الحقل المنتهي من الرتبة 19

عماد بكر الزنكنة

قسم الرياضيات، كلية العلوم، الجامعة المستنصرية.

الخلاصة:

المنحنيات التكعيبية في المستوي يمكن تصنيفها حسب تكافؤ زمري او تكافؤ اسقاطي. في هذا البحث المنحنيات التكعيبية الاهليلجيه الغير متكافئة والتي هي منحني تكعيبي غير شاذ في المستوي قد تم تصنيفها اسقاطياً على الحقل المنتهي من الرتبة 19 و تم تحديد اذا كان تام او غير تام كقوس من الدرجة الثالثة . وكذلك اعظم سعة لمنحني اهليلجي كامل من الدرجة الثالثة التي يمكن بنائها من كل منحني اهليلجي غير تام قد اعطي.

الكلمات المفتاحية: الهندسة المنتهية، نظرية التشفير،المنحنيات التكعيبية الاهليليجية، القوس.