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

Hamiltonian property of the incidence graphs of quadrangles associated with symplectic forms on finite fields

Hajime SATO · Hiroshi SUZUKI

the date of receipt and acceptance should be inserted later

Abstract We show that the incidence graphs of finite generalized quadrangles associated with symplectic forms on finite fields are Hamiltonian. This is an extension of Singer's theorem [7] on generalized triangles to certain classical polygons.

Keywords Hamiltonian graph, generalized quadrangle, finite field, incidence graph.

Mathematics Subject Classification (2010) Primary 05C45; Secondary 05C38.

1 Introduction

1.1 Main results

The famous Singer's theorem [7] asserts that the incidence graph of every finite Desarguesian projective plane is Hamiltonian. The graphs in that theorem are generalized triangles. There are more simple interesting finite incidence graphs called generalized polygons. They come from point-line incidence geometry. A finite incidence geometry is a triple $S = (P,L,I)$ consisting of a finite set of points P, a finite set of lines L and a binary incidence relation $I \subseteq P \times L$. With an incidence geometry O, we naturally associate a bipartite graph having the points and lines of O as vertices, which we call the incidence graph of O.

A sequence of vertices $(p_0,\dots,p_m)$ of a graph G is a path of length m between p_0 and p_m if $\{p_i,p_{i+1}\}$ is an edge for $i = 1,2,\dots,m$. A distance $d(p_0,p_1)$ is the length of the shortest path between p_0 and p_1. The diameter of G is the largest distance in G. A cycle is a path $(p_0,\dots,p_m)$ with mutually different $p_0,\dots,p_{m-1}$ and $p_0 = p_m$. The girth of G is the length of the shortest cycle in G.

Hajime SATO
Graduate School of Mathematics, Nagoya University, Chikusa-ku, Nagoya, Japan E-mail: hsato@math.nagoya-u.ac.jp

Hiroshi SUZUKI
Graduate School of Mathematics, Nagoya University, Chikusa-ku, Nagoya, Japan E-mail: hiroshis@math.nagoya-u.ac.jp

We have the ordinary n-gon as the incidence graph of an incident geometry.

By a generalized polygon, we mean the associated graph of a finite incidence geometry $S = (P, L, I)$ satisfying the following conditions (cf. [6]).

i) S contains no ordinary k-gon (as a subgeometry), for $2 \leq k < n$.

ii) Any two elements $x, y \in P \cup L$ are contained in some ordinary n-gon (as a subgeometry).

iii) There exists an ordinary $(n+1)$-gon (as a subgeometry) in S.

When the diameter of a generalized polygon is equal to n, we say the polygon a generalized n-gon. A generalized 2-gon is a complete bipartite graph. A generalized 3-gon is equal to the projective plane. Feit and Higman [5] proved that finite generalized n-gons can exist only the following values of n:

$$2,\ 3,\ 4,\ 6,\ 8.$$

As generalized 4-gons, we consider the following classical symplectic quadrangles. They seem to be related to the symplectic geometry in the field of physical dynamics and to have some relations with the number theory.

The symplectic quadrangles are constructed as follows. We define an incidence structure $C(q)$ as follows. Let $V = \mathbb{F}_{q^4}$ be a finite field with q^4 elements considered as a four dimensional vector space over $\mathbb{F}_q$. The points of $C(q)$ are 1-dimensional subspaces of V and the lines of $C(q)$ are 2-dimensional totally isotropic subspaces. The numbers of points and lines in $C(q)$ are both equal to $(q^4-1)/(q-1)$.

Let $L(q)$ be the incidence graph of $C(q)$. The vertices of $L(q)$ are all points and lines of $C(q)$. If a point in $C(q)$ is contained in a line in $C(q)$, we put an edge in $L(q)$ between the vertices. Then it is easy to see that $C(q)$ is a generalized quadrangle such that each line contains exactly $q+1$ points and exactly $q+1$ lines through each point. The symplectic group $\mathrm{Sp}(4,q)$ acts on the graph $L(q)$. The 1-dimensional simplicial complex $L(q)$ is an example of a spherical building and is an example of $(q+1,8)$-cage. See Wong[8] for a collection of results on cages.

A graph is called *Hamiltonian* if there exists a cycle containing every vertex of the graph. Our main result in this paper is the following.

Theorem 1 *The generalized quadrangle $L(q)$ is Hamiltonian for any power $q = p^n$ of any prime number p ($n > 0$).*

When $q = 2$, we have the $(3,8)$-cage $L(2)$. The cage $L(2)$ is the unique $(3,8)$-cage called *the Tutte-Coxeter cage* and said to be the most regular of all graphs [4]. This $L(2)$ is known to be Hamiltonian. Our results extend this fact to arbitrary finite fields.

The incidence graph of the incidence structure consisting of points and lines in a finite projective plane over $\mathbb{F}_q$ is a $(q+1,6)$-cage. The minimal Hamiltonian regular graph of girth 6 is studied in [2]. It is a classical result that if the projective plane is Desarguesian and of order p^n, the $(p^n+1,6)$-cage is Hamiltonian (Singer[7]). Thus our results may be considered as a symplectic analogue of Singer's theorem (cf. [1]).

Our proof of Theorem 1 proceeds as follows. We first define a cyclic action on $L(q)$. The quotient is a graph with multiple edges. We investigate the structure of the quotient. We find a Hamiltonian cycle S_0 of the quotient. Next we lift the cycle to $L(q)$. Then we have a difference between the origin and the terminus of the lifted

path. We arrange the lift so that the gap is equal to a generator of the cyclic group. Concatenating the lifts, we obtain a Hamiltonian cycle of $L(q)$. The definition of the action and the construction of Hamiltonian cycle are done by different methods depending on whether p is equal to 2 or odd. We treat the cases in different sections. After fixing the definitions and the notation of graphs in this section 1, we treat the case when p is odd in Section 2 and the case $p = 2$ in Section 3. At the end of both sections, we give concrete pictures of the incidence graphs $L(q)$ for $q = 3, 5$ and $2, 4$.

1.2 Definition of graphs

In this section we fix the notation and describe the features of the incidence graph $L(q)$ for a power $q = p^n$ of a prime number p.

A simple *bipartite* graph $X = (\mathrm{r}(X), \mathrm{b}(X), \mathrm{e}(X))$ consists of three sets $\mathrm{r}(X)$, $\mathrm{b}(X)$ and $\mathrm{e}(X)$. An element of $\mathrm{r}(X)$ is called a *red node* of X, an element of $\mathrm{b}(X)$ is called a *blue node* of X and an element of $\mathrm{e}(X)$ is called an *edge* of X. The disjoint union $\mathrm{v}(X) = \mathrm{r}(X) \sqcup \mathrm{b}(X)$ is the set of vertices of the graph X. An edge $\eta = \{r, b\} \in \mathrm{e}(X)$ is a pair of a red node r and a blue node b. The red node $\mathrm{r}(\eta) = r$ is called the red node *incident to* the edge η and the blue node $\mathrm{b}(\eta) = b$ is called the blue node *incident to* the edge η. If a red node and a blue node are incident to an edge, we call the nodes *adjacent*. A simple bipartite graph contains no loop edge and no multiple edge. In this paper, we only treat simple bipartite graphs and in the following we call a simple bipartite graph simply a graph.

A mapping $j = (j_{\mathrm{r}}, j_{\mathrm{b}}, j_{\mathrm{e}}) : X \longrightarrow Y$ from a graph X to a graph Y consists of three mappings $j_{\mathrm{r}} : \mathrm{r}(X) \longrightarrow \mathrm{r}(Y)$, $j_{\mathrm{b}} : \mathrm{b}(X) \longrightarrow \mathrm{b}(Y)$ and $j_{\mathrm{e}} : \mathrm{e}(X) \longrightarrow \mathrm{e}(Y)$ which satisfy $j_{\mathrm{r}} \circ \mathrm{r} = \mathrm{r} \circ j_{\mathrm{e}}$ and $j_{\mathrm{b}} \circ \mathrm{b} = \mathrm{b} \circ j_{\mathrm{e}}$. The composition $j' \circ j = ({j'}_{\mathrm{r}} \circ j_{\mathrm{r}}, {j'}_{\mathrm{b}} \circ j_{\mathrm{b}}, {j'}_{\mathrm{e}} \circ j_{\mathrm{e}})$ is defined for two mappings $j : X \longrightarrow Y$ and $j' : Y \longrightarrow Z$ of graphs. An injection j of graphs is a mapping of graphs such that j_{r}, j_{b} and j_{e} are injective. An isomorphism j of graphs is a mapping of graphs such that j_{r}, j_{b} and j_{e} are bijective. An isomorphism from X to X is called an automorphism of X. A homomorphism from a group G to the automorphism group of X is called an action of G on X. Namely we say that a group G acts on X when G acts on the sets $\mathrm{r}(X)$, $\mathrm{b}(X)$, $\mathrm{e}(X)$ and the mappings r and b are G-mappings. The quotient graph X/G of X by G consists of quotient sets $\mathrm{r}(X/G) = \mathrm{r}(X)/G$, $\mathrm{b}(X/G) = \mathrm{b}(X)/G$ and $\mathrm{e}(X/G) = \{\{rG, bG\} | r \in \mathrm{r}(X), b \in \mathrm{b}(X), \{r, b\} \in \mathrm{e}(X)\}$. We have the projection mapping $p_G = (p_{G,\mathrm{r}}, p_{G,\mathrm{b}}, p_{G,\mathrm{e}}) : X \longrightarrow X/G$ of graphs which consists of the canonical projections of red nodes, blue nodes and edges. The inverse image ${p_{G,\mathrm{e}}}^{-1}(\eta)$ of an edge η of X/G is a union of some G-orbits of edges of X. When the inverse image is a union of m G-orbits, we call the edge of the quotient graph *m-edge*. We call an action of a group G on a graph X to be *free* if any nontrivial element of G does not have any fixed element in $\mathrm{r}(X)$, $\mathrm{b}(X)$ and $\mathrm{e}(X)$.

For a subset R of $\mathrm{r}(X)$ and a subset B of $\mathrm{b}(X)$, put $E = \mathrm{r}^{-1}(R) \cap \mathrm{b}^{-1}(B)$. Then E is the set of edges incident to a red node in R and a blue node in B. We have the graph $X[R, B] = (R, B, E)$. We call $X[R, B]$ the *subgraph* of X *induced* by R and B. If a set V of red and blue nodes are given, we have the graph $X \setminus V = X[\mathrm{r}(X) \setminus V, \mathrm{b}(X) \setminus V]$. This is the graph obtained from X by removing the nodes in V and the edges incident to them.

Let $\mathbb{F}_q$ be the finite field of order q. The finite field $\mathbb{F}_{q^m}$ of order q^m is the extension of $\mathbb{F}_q$ of degree m. We denote the multiplicative group of a field K by $K^\times$.

Recall the trace mapping $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q} : \mathbb{F}_{q^m} \to \mathbb{F}_q$ and the norm mapping $\mathrm{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q} : \mathbb{F}_{q^m}^\times \to \mathbb{F}_q^\times$. For an element x of $\mathbb{F}_{q^m}$, the trace of x is the sum of all the conjugates x, x^q, x^{q^2}, …, $x^{q^{m-1}}$ over $\mathbb{F}_q$;

$$\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(x) = x + x^q + x^{q^2} + \cdots + x^{q^{m-1}}.$$

The norm of an element x of $\mathbb{F}_{q^m}^\times$ is the product of all the conjugates;

$$\mathrm{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(x) = x x^q x^{q^2} \cdots x^{q^{m-1}} = x^{1+q+q^2+\cdots+q^{m-1}}.$$

We write simply $\mathrm{Tr} = \mathrm{Tr}_{\mathbb{F}_{q^4}/\mathbb{F}_{q^2}}$ and $\mathrm{N} = \mathrm{N}_{\mathbb{F}_{q^4}/\mathbb{F}_{q^2}}$.

A non-degenerate alternating $\mathbb{F}_q$-bilinear form over $2k$-dimensional $\mathbb{F}_q$-linear space is unique up to isomorphism. In the following, we fix a non-degenerate alternating $\mathbb{F}_q$-bilinear form $(*,*)$ over the 4-dimensional $\mathbb{F}_q$-linear space $\mathbb{F}_{q^4}$.

In the following, by *incidence structure*, we mean a set of points and a set of distinguished subsets of points called lines satisfying the following conditions:

i) Every line has the same number of points.

ii) Every point is contained in the same number of lines.

Let us define an incidence structure $C(q)$ from $\mathbb{F}_{q^4}$ with an alternating form $(*,*)$. A 2-dimensional $\mathbb{F}_q$-linear subspace V of $\mathbb{F}_{q^4}$ is called *totally isotropic* if $(x,y) = 0$ for all $x, y \in V$. The points of $C(q)$ are 1-dimensional $\mathbb{F}_q$-linear subspaces of $\mathbb{F}_{q^4}$ and the lines of $C(q)$ are totally isotropic 2-dimensional $\mathbb{F}_q$-linear subspaces of $\mathbb{F}_{q^4}$.

We denote by $\langle x,y\rangle$ the $\mathbb{F}_q$-linear subspace of $\mathbb{F}_{q^4}$ generated by x and y. The set of points in $C(q)$ corresponds bijectively to the set of points of the 3-dimensional projective space $P^3(\mathbb{F}_q) = \mathbb{F}_{q^4}^\times/\mathbb{F}_q^\times$. Two points $x\mathbb{F}_q^\times \neq y\mathbb{F}_q^\times$ lie on a line if and only if $(x,y) = 0$.

A line in $C(q)$ is isomorphic to the projective line $P^1(\mathbb{F}_q)$ and consists of $q+1$ points. Let x be an element of $\mathbb{F}_{q^4}^\times$. Then $x^\perp = \{y \in \mathbb{F}_{q^4} | (x,y) = 0\}$ is a 3-dimensional $\mathbb{F}_q$-linear subspace containing x. A totally isotropic plane containing x is a 2-dimensional $\mathbb{F}_q$-linear subspace of $x^\perp$. There exist $q+1$ distinct totally isotropic planes containing x. Consequently for any point in $C(q)$ there are $q+1$ distinct lines containing the point. In total there are q^3+q^2+q+1 points and q^3+q^2+q+1 lines in $C(q)$.

Let $L(q)$ be the incidence graph of the incidence structure $C(q)$. Then $L(q)$ is the graph consisting of q^3+q^2+q+1 red nodes corresponding to points of $C(q)$, q^3+q^2+q+1 blue nodes corresponding to lines in $C(q)$ and $(q+1)(q^3+q^2+q+1)$ edges. An edge exists between a red node and a blue node if and only if the point corresponding to the red node is contained in the line corresponding to the blue node in $C(q)$.

2 Odd characteristic

In this section we assume the characteristic of the field $\mathbb{F}_q$ is an odd prime number p and we put $q = p^n$. We will define cyclic group actions of order q^2+1 and $\dfrac{q^2+1}{2}$

on $L(q)$. Let $Q(q)$ and $\widetilde{Q}(q)$ be their quotient graphs. We will show that $Q(q)$ has a Hamiltonian path and $\widetilde{Q}(q)$ has a Hamiltonian cycle. Then we can get a cyclic lift in $L(q)$ of the Hamiltonian cycle of $\widetilde{Q}(q)$. By arranging the lift and concatenating them, we get a Hamiltonian cycle of $L(q)$.

2.1 Proof of Theorem 1 for odd q.

An odd number q satisfies either $q \equiv 1 \mod 4$ or $q \equiv 3 \mod 4$.

If $q \equiv 1 \mod 4$, then we can write $q = 2^m q' + 1$ with $m \geq 2$ and an odd integer q'. Let a_0 be a primitive 2^m-th root of 1 in $\mathbb{F}_q$. Then the field $\mathbb{F}_q(\sqrt{a_0})$ is equal to $\mathbb{F}_{q^2}$ and the field $\mathbb{F}_q(\sqrt[4]{a_0})$ is equal to $\mathbb{F}_{q^4}$. Put $a = \sqrt{a_0} \in \mathbb{F}_{q^2}$.

If $q \equiv 3 \mod 4$, then let $a_0 = -1$. Then the field $\mathbb{F}_q(\sqrt{a_0})$ is equal to $\mathbb{F}_{q^2}$. We can write $q^2 = 2^m q' + 1$ with $m \geq 2$ and an odd integer q'. Let a be a primitive 2^m-th root of 1 in $\mathbb{F}_{q^2}$. Then the field $\mathbb{F}_{q^2}(\sqrt{a})$ is equal to $\mathbb{F}_{q^4}$.

In both cases we have

$$\mathbb{F}_{q^4} = \mathbb{F}_{q^2}(\sqrt{a}) \supset \mathbb{F}_{q^2} = \mathbb{F}_q(\sqrt{a_0}) \supset \mathbb{F}_q.$$

In the following we fix these elements $a_0 \in \mathbb{F}_q$ and $a \in \mathbb{F}_{q^2}$ in both cases.

Lemma 1 *Let $q = p^n$. The form $(*,*) : \mathbb{F}_{q^4} \times \mathbb{F}_{q^4} \to \mathbb{F}_q$ defined by*

$$(x,y) = \mathrm{Tr}_{\mathbb{F}_{q^4}/\mathbb{F}_q}(xy^{q^2}\sqrt{a}) \quad \textit{for } x,y \in \mathbb{F}_{q^4}$$

is a non-degenerate alternating $\mathbb{F}_q$-bilinear form.

Proof The mapping $y \mapsto y^{q^2}$ is the nontrivial element of $\mathrm{Gal}(\mathbb{F}_{q^4}/\mathbb{F}_{q^2})$ and it is $\mathbb{F}_{q^2}$-linear. Since $\mathrm{Tr}_{\mathbb{F}_{q^4}/\mathbb{F}_q}$ is $\mathbb{F}_q$-linear, the form $(*,*)$ is $\mathbb{F}_q$-bilinear. For an element $x \in \mathbb{F}_{q^4}$, we have

$$(x,x) = \mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\mathrm{Tr}(\mathrm{N}(x)\sqrt{a})) = \mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\mathrm{N}(x)\,\mathrm{Tr}(\sqrt{a})) = 0.$$

Since $\mathrm{Tr}_{\mathbb{F}_{q^4}/\mathbb{F}_q}$ is surjective, for each $y \neq 0$, we can take an element x such that $(x,y) \neq 0$. Thus $(*,*)$ is a non-degenerate alternating $\mathbb{F}_q$-bilinear form.

We use this $\mathbb{F}_q$-bilinear form in the construction of $C(q)$ and $L(q)$.

Lemma 2 *i) If $x \in \mathbb{F}_{q^4}^\times$, then the plane $x\mathbb{F}_{q^2}$ is totally isotropic.*
ii) $\mathrm{N}^{-1}(\mathbb{F}_q^\times) \cap \mathbb{F}_{q^2}^\times = \mathbb{F}_q^\times \cup \sqrt{a_0}\,\mathbb{F}_q^\times, \quad \mathrm{N}^{-1}(\mathbb{F}_q^\times) \cap \sqrt{a}\,\mathbb{F}_{q^2}^\times = \emptyset.$
iii) Let $h \in \mathrm{N}^{-1}(\mathbb{F}_q^\times) \setminus \mathbb{F}_{q^2}^\times$ and $z \in \mathbb{F}_{q^4}^\times$. The $\mathbb{F}_q$-linear subspace $\langle z, zh\rangle$ is totally isotropic if and only if $\mathrm{N}(z)\mathbb{F}_q^\times = \dfrac{\sqrt{a_0}}{\mathrm{Tr}(h\sqrt{a})}\mathbb{F}_q^\times$.
iv) If $h \in \mathrm{N}^{-1}(\mathbb{F}_q^\times) \setminus \mathbb{F}_{q^2}^\times$ and $\alpha \in \mathbb{F}_q^\times$, then $h+\alpha \notin \mathrm{N}^{-1}(\mathbb{F}_q^\times)$ and $\dfrac{h+\alpha}{h+\dfrac{\mathrm{N}(h)}{\alpha}} \in \mathrm{N}^{-1}(\mathbb{F}_q^\times)$.
Moreover the following holds;

a) $(h+\alpha)\mathbb{F}_q^\times = (h+\dfrac{\mathrm{N}(h)}{\alpha})\mathbb{F}_q^\times$ *if and only if* $\alpha = \pm\sqrt{\mathrm{N}(h)}$. *This occurs if* $h \in \mathrm{Ker}\,\mathrm{N}\cdot\mathbb{F}_q^\times$.

b) $\dfrac{h+\alpha}{h+\dfrac{\mathrm{N}(h)}{\alpha}} \in \mathrm{Ker}\,\mathrm{N}\cdot\mathbb{F}_q^\times$ *if and only if* $h \in \mathrm{Ker}\,\mathrm{N}\cdot\mathbb{F}_q^\times$.

v) Let $h \in (\mathrm{Ker}\,\mathrm{N}\cdot\mathbb{F}_q^\times)\setminus\mathbb{F}_q^\times$ *and* $z \in \mathbb{F}_{q^4}^\times$. *Suppose that the* $\mathbb{F}_q$*-linear subspace* $\langle z, zh\rangle$ *is totally isotropic as in iii). Then*

$$\mathrm{N}(z(h+\sqrt{\mathrm{N}(h)}))\,\mathrm{N}(z(h-\sqrt{\mathrm{N}(h)}))\mathbb{F}_q^\times = \frac{1}{a}\mathbb{F}_q^\times.$$

vi) For $x,\ y \in \mathbb{F}_{q^4}^\times$, *the plane* $\langle x, y\rangle$ *is totally isotropic and* $\mathrm{N}(x)\,\mathrm{N}(y)\mathbb{F}_q^\times = \dfrac{1}{a}\mathbb{F}_q^\times$ *if and only if* $y \in \sqrt{\dfrac{a_0}{a}}x^{-q^2}\mathbb{F}_q^\times$.

Proof i) Since

$$(x, x\sqrt{a_0}) = \mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\mathrm{Tr}(\mathrm{N}(x)\sqrt{a_0}\sqrt{a})) = \mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\mathrm{N}(x)\sqrt{a_0}\,\mathrm{Tr}(\sqrt{a})) = 0,$$

the $\mathbb{F}_q$-linear subspace $x\mathbb{F}_{q^2} = \langle x, x\sqrt{a_0}\rangle$ is isotropic.

ii) The restriction of the norm mapping N to $\mathbb{F}_{q^2}$ is equal to the square mapping $x \mapsto x^2$. From the equation $\mathbb{F}_q^\times \cap \mathbb{F}_{q^2}^{\times\,2} = \mathbb{F}_q^\times = \mathbb{F}_q^{\times\,2} \cup a_0\mathbb{F}_q^{\times\,2}$, we get the first assertion. Since $\sqrt{-1} \in \mathbb{F}_{q^2}$, we have $\mathrm{N}(\sqrt{a}\,\mathbb{F}_{q^2}^\times) = -a\mathbb{F}_{q^2}^{\times\,2} = a\mathbb{F}_{q^2}^{\times\,2}$. By the choice of a, we have $a\mathbb{F}_{q^2}^{\times\,2} \cap \mathbb{F}_{q^2}^{\times\,2} = \emptyset$. From the relation $\mathbb{F}_q^\times \subset \mathbb{F}_{q^2}^{\times\,2}$, we get the second assertion.

iii) For $x_1,\ x_2 \in \mathbb{F}_{q^2}$, $\mathrm{Tr}(x_1 + x_2\sqrt{a}) = 2x_1$. From $h \notin \mathbb{F}_{q^2}$, we have $\mathrm{Tr}(h\sqrt{a}) \neq 0$. For $y_1,\ y_2 \in \mathbb{F}_q$, we have $\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(y_1 + y_2\sqrt{a_0}) = 2y_1$. Thus the equation $(zh, z) = \mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\mathrm{N}(z)\,\mathrm{Tr}(h\sqrt{a})) = 0$ holds if and only if $\mathrm{N}(z)\,\mathrm{Tr}(h\sqrt{a}) \in \sqrt{a_0}\,\mathbb{F}_q$.

iv) If $\mathrm{N}(h+\alpha) = \mathrm{N}(h) + \mathrm{Tr}(h)\alpha + \alpha^2 \in \mathbb{F}_q$, then $\mathrm{Tr}(h) \in \mathbb{F}_q$. The root h of quadratic polynomial $X^2 - \mathrm{Tr}(h)X + \mathrm{N}(h) \in \mathbb{F}_q[X]$ must belong to the unique quadratic extension $\mathbb{F}_{q^2}$ of $\mathbb{F}_q$. This contradicts the assumption of h. Thus $h+\alpha \notin \mathrm{N}^{-1}(\mathbb{F}_q^\times)$. Since $h + \dfrac{\mathrm{N}(h)}{\alpha} = \dfrac{h}{\alpha}(\alpha + h^{q^2})$, we have $\mathrm{N}(h+\dfrac{\mathrm{N}(h)}{\alpha}) = \dfrac{\mathrm{N}(h)}{\alpha^2}\,\mathrm{N}(h+\alpha)$ and $\dfrac{h+\alpha}{h+\dfrac{\mathrm{N}(h)}{\alpha}} \in \mathrm{N}^{-1}(\mathbb{F}_q^\times)$.

iv-a) Since $h \notin \mathbb{F}_{q^2}$ and 1 are linearly independent over $\mathbb{F}_q$, the equation $(h+\alpha)\mathbb{F}_q^\times = (h+\dfrac{\mathrm{N}(h)}{\alpha})\mathbb{F}_q^\times$ holds if and only if $\alpha = \dfrac{\mathrm{N}(h)}{\alpha}$. Such an element α exists when $\mathrm{N}(h) \in \mathbb{F}_q^{\times\,2} = \mathrm{N}(\mathbb{F}_q^\times)$.

iv-b) From the equation $\mathrm{N}(\dfrac{h+\alpha}{h+\dfrac{\mathrm{N}(h)}{\alpha}}) = \dfrac{\alpha^2}{\mathrm{N}(h)}$, we get iv-b).

v) If $h \in \mathbb{F}_{q^2}^\times$, we have $\mathrm{N}(h) = h^2 \in \mathbb{F}_q^{\times\,2}$ and $h \in \mathbb{F}_q^\times$. This contradicts the assumption of h. Hence $h \in \mathrm{N}^{-1}(\mathbb{F}_q^\times)\setminus\mathbb{F}_{q^2}^\times$. From iii), we get $\mathrm{N}(z)\mathbb{F}_q^\times = \dfrac{\sqrt{a_0}}{\mathrm{Tr}(h\sqrt{a})}\mathbb{F}_q^\times$. Since

$\mathrm{Tr}(h\sqrt{a}) = (h-h^{q^2})\sqrt{a}$, we have $\mathrm{Tr}(h\sqrt{a})^2 = (\mathrm{Tr}(h)^2 - 4\,\mathrm{N}(h))a$. From the equation $\mathrm{N}(h \pm \sqrt{\mathrm{N}(h)}) = 2\,\mathrm{N}(h) \pm \mathrm{Tr}(h)\sqrt{\mathrm{N}(h)}$, we get v).
vi) Since $(y,x) = \mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\mathrm{Tr}(yx^{q^2}\sqrt{a})) = 0$, we have $\mathrm{Tr}(yx^{q^2}\sqrt{a}) \in \sqrt{a_0}\,\mathbb{F}_q$. Thus $\mathrm{Tr}(yx^{q^2}\sqrt{\frac{a}{a_0}}) \in \mathbb{F}_q$. Since $\mathrm{N}(yx^{q^2}\sqrt{\frac{a}{a_0}}) = \frac{\mathrm{N}(x)\,\mathrm{N}(y)a}{a_0} \in \mathbb{F}_q$, $yx^{q^2}\sqrt{\frac{a}{a_0}}$ must belong to $\mathbb{F}_{q^2}^{\times}$. Then we have $\mathrm{Tr}(yx^{q^2}\sqrt{\frac{a}{a_0}}) = 2yx^{q^2}\sqrt{\frac{a}{a_0}}$ and $2yx^{q^2}\sqrt{\frac{a}{a_0}} \in \mathbb{F}_q$. The converse is evident.

We simply denote by Z_{q^2+1} the subgroup $\mathrm{N}^{-1}(\mathbb{F}_q^{\times})/\mathbb{F}_q^{\times} \subset \mathbb{F}_{q^4}^{\times}/\mathbb{F}_q^{\times}$ of order q^2+1 and by $\mathrm{Z}_2 \subset \mathrm{Z}_{q^2+1}$ the subgroup of order 2 generated by the element $\sqrt{a_0}\,\mathbb{F}_q^{\times}$. Similarly we denote by $\mathrm{Z}_{\frac{q^2+1}{2}}$ the subgroup $(\mathrm{Ker}\,\mathrm{N}\cdot\mathbb{F}_q^{\times})/\mathbb{F}_q^{\times} \subset \mathbb{F}_{q^4}^{\times}/\mathbb{F}_q^{\times}$. Then we have an isomorphism $\mathrm{Z}_{q^2+1} \cong \mathrm{Z}_{\frac{q^2+1}{2}} \times \mathrm{Z}_2$. The group Z_{q^2+1} acts on $L(q)$. Let $Q(q)$ and $\widetilde{Q}(q)$ be the quotient graphs $L(q)/\mathrm{Z}_{q^2+1}$ and $L(q)/\mathrm{Z}_{\frac{q^2+1}{2}}$ respectively.

Now we have a property of the quotient graph $Q(q) = L(q)/\mathrm{Z}_{q^2+1}$.

Lemma 3 *The graph $Q(q)$ consists of the following sets of red nodes $\mathrm{r}(Q(q))$, blue nodes $\mathrm{b}(Q(q))$ and edges $\mathrm{e}(Q(q))$;*

$$\mathrm{r}(Q(q)) = \{x_1,\ldots,x_{\frac{q+1}{2}},y_1,\ldots,y_{\frac{q+1}{2}}\},$$
$$\mathrm{b}(Q(q)) = \{\mathfrak{b},\mathfrak{b}',b_1,\ldots,b_{\frac{q-1}{2}},B_1,\ldots,B_{\frac{q+1}{2}}\},$$

such that

i) $\mathfrak{b} = z_0\mathbb{F}_{q^2}\mathrm{Z}_{q^2+1}$ *and* $\mathfrak{b}' = z_0'\mathbb{F}_{q^2}\mathrm{Z}_{q^2+1}$ $(z_0, z_0' \in \mathbb{F}_{q^4}^{\times})$ *are the orbits of* Z_2*–invariant totally isotropic planes* $z_0\mathbb{F}_{q^2}$ *and* $z_0'\mathbb{F}_{q^2}$,
ii) $b_i = \langle z_i, z_ih_i\rangle\mathrm{Z}_{q^2+1}$ *for some* $z_i \in \mathbb{F}_{q^4}^{\times}$, $h_i \in \mathrm{N}^{-1}(\mathbb{F}_q^{\times}) \setminus ((\mathrm{Ker}\,\mathrm{N}\cdot\mathbb{F}_q^{\times}) \cup \mathbb{F}_{q^2}^{\times})$ $(i = 1,\ldots,\frac{q-1}{2})$,
iii) $B_i = \langle z_i', z_i'h_i'\rangle\mathrm{Z}_{q^2+1}$ *for some* $z_i' \in \mathbb{F}_{q^4}^{\times}$, $h_i' \in \mathrm{Ker}\,\mathrm{N}\cdot\mathbb{F}_q^{\times}$ $(i = 1,\ldots,\frac{q+1}{2})$ *such that* $h_1'\mathbb{F}_q^{\times}$ *generates* $\mathrm{Z}_{\frac{q^2+1}{2}}$ *and* $x_2 = z_1'\mathbb{F}_q^{\times}\mathrm{Z}_{q^2+1}$.

The set of edges $e(Q(q))$ consists of the following edges. For each j, $\mathfrak{b}$ is adjacent to x_j by a 1-edge and $\mathfrak{b}'$ is adjacent to y_j by a 1-edge. For each j, B_j is adjacent to x_j and y_j by 1-edges. For each j and k, b_j is adjacent to either x_k or y_k by a 2-edge. For each $j \neq k$, B_j is adjacent to either x_k or y_k by a 2-edge. Any red node is incident to two 1-edges and $\frac{q-1}{2}$ 2-edges.

Proof Since the Z_2–invariant totally isotropic planes $z\mathbb{F}_{q^2}$ forms two Z_{q^2+1}–orbits by Lemma 2 i) and ii), we denote them by $\mathfrak{b}$ and $\mathfrak{b}'$. They are distinct two blue nodes of $Q(q)$. For $h \in \mathrm{N}^{-1}(\mathbb{F}_q^{\times}) \setminus ((\mathrm{Ker}\,\mathrm{N}\cdot\mathbb{F}_q^{\times}) \cup \mathbb{F}_{q^2}^{\times})$, by Lemma 2 iii), we can take an element $z \in \mathbb{F}_{q^4}^{\times}$ such that $\langle z, zh\rangle$ is totally isotropic. Let $\langle z, zh\rangle\mathrm{Z}_{q^2+1}$ be the orbit. By Lemma 2 iv) and iv-b), $(q+1)(q-1)$ h's correspond to the same orbit. Hence

there are $\dfrac{|\mathrm{N}^{-1}(\mathbb{F}_q^\times)\setminus((\mathrm{Ker}\,\mathrm{N}\cdot\mathbb{F}_q^\times)\cup\mathbb{F}_{q^2}^\times)|}{q^2-1}=\dfrac{q-1}{2}$ distinct orbits of this kind. We denote them by b_1, …, $b_{\frac{q-1}{2}}$. For $h\in(\mathrm{Ker}\,\mathrm{N}\cdot\mathbb{F}_q^\times)\setminus\mathbb{F}_q^\times$, by Lemma 2 iii), we can take an element $z\in\mathbb{F}_{q^4}^\times$ such that $\langle z,zh\rangle$ is totally isotropic and we consider the orbit $\langle z,zh\rangle\mathrm{Z}_{q^2+1}$. By Lemma 2 iv), iv-a) and iv-b), $(q-1)^2$ h's correspond to the same orbit. Hence there are $\dfrac{|(\mathrm{Ker}\,\mathrm{N}\cdot\mathbb{F}_q^\times)\setminus\mathbb{F}_q^\times|}{(q-1)^2}=\dfrac{q+1}{2}$ distinct orbits of this kind. We denote them by B_1, …, $B_{\frac{q+1}{2}}$. If $\langle z,zh\rangle\mathrm{Z}_{q^2+1}=B_j$, then the two orbits $z(h+\sqrt{\mathrm{N}(h)})\mathbb{F}_q^\times\mathrm{Z}_{q^2+1}$ and $z(h-\sqrt{\mathrm{N}(h)})\mathbb{F}_q^\times\mathrm{Z}_{q^2+1}$ are adjacent to B_j by 1-edges. The other edges incident to B_j, and all the edges incident to b_k are 2-edges by Lemma 2 iv), iv-a), iv-b). By Lemma 2 v), one of the two orbits is adjacent to $\mathfrak{b}$ and the other adjacent to $\mathfrak{b}'$. We denote the one adjacent to $\mathfrak{b}$ by x_j and the one adjacent to $\mathfrak{b}'$ by y_j. By Lemma 2 vi), x_1, …, $x_{\frac{q+1}{2}}$, y_1, …, $y_{\frac{q+1}{2}}$ are distinct. By Lemma 2 vi), b_j is adjacent to at most one of x_k and y_k for each k and B_j is adjacent to at most one of x_k and y_k for each $k\neq j$. Comparing the number of edges incident to a blue node, we see that b_j is adjacent to either x_k or y_k for each k and B_j is adjacent to either x_k or y_k for each $k\neq j$. We can renumber $\{b_0,b_0',x_i,y_i,b_i,B_i\}$ if necessary so that $h_1'\mathbb{F}_q^\times$ generates $\mathrm{Z}_{\frac{q^2+1}{2}}$.

In order to take a Hamiltonian path of $Q(q)$, we need the following Chvátal's theorem ([3, Corollary 1.4]).

Lemma 4 *Let G be a bipartite graph with $\dfrac{1}{2}m$ points in each part. If the non-decreasing sequence d_1, …, d_m consisting of all valencies of G satisfies*

$$d_k\leqq k\leqq\frac{1}{4}m\Longrightarrow d_{\frac{m}{2}}\geqq\frac{1}{2}m-k+1,$$

then G is Hamiltonian.

Proof (Proof of Theorem 1) Firstly we show that the induced graph $Q_0=Q(q)\setminus\{x_1,y_1,B_1,\mathfrak{b},\mathfrak{b}'\}$ has a Hamiltonian path P_0 which starts at x_2. Since this statement is evident if Q_0 has a Hamiltonian cycle, we assume that Q_0 has no Hamiltonian cycle. By Lemma 3, the valencies of half of the red nodes of Q_0 are $\dfrac{q-1}{2}$ and the valencies of the other half are $\dfrac{q+1}{2}$. This holds also for blue nodes of Q_0. Hence the non-decreasing sequence d_i of all valencies of Q_0 satisfies

$$d_i=\frac{q-1}{2}\quad\text{for }1\leqq i\leqq q-1,\qquad d_i=\frac{q+1}{2}\quad\text{for }q\leqq i\leqq 2(q-1).$$

Since x_2 is adjacent to B_1, the valency of x_2 in Q_0 is $\dfrac{q-1}{2}$. Append Q_0 an edge from x_2 to a blue node which is not adjacent to x_2. The new graph satisfies the assumption of Lemma 4 and has a Hamiltonian cycle. Since Q_0 itself does not have any Hamiltonian cycle by our assumption, Q_0 has a Hamiltonian path P_0 which begins at x_2. In any case, we get a Hamiltonian path P_0 which starts at x_2. We write the terminal blue

node of P_0 by b; $P_0 = (x_2, \cdots, b)$. Secondly we show that $Q(q)$ has a Hamiltonian path between $\mathfrak{b}$ and $\mathfrak{b}'$ which contains the path (B_1, x_2). By Lemma 3, b is adjacent to either x_1 or y_1, $\mathfrak{b}$ is adjacent to x_1, $\mathfrak{b}'$ is adjacent to y_1, and x_2 is adjacent to B_1 which is adjacent to x_1 and y_1. Hence either $(\mathfrak{b}', y_1, B_1, P_0, x_1, \mathfrak{b})$ or $(\mathfrak{b}, x_1, B_1, P_0, y_1, \mathfrak{b}')$ is a Hamiltonian path of $Q(q)$. Let P_Q be this Hamiltonian path in $Q(q)$. Finally we show that $L(q)$ is Hamiltonian which proves Theorem 1. Take a path P in $L(q)$ which is a lift of P_Q. The path P has the form

$$P = (w_1\mathbb{F}_{q^2}, w_1\mathbb{F}_q^\times, \langle z_1', h_1'z_1'\rangle, z_1'\mathbb{F}_q^\times, P_1, w_2\mathbb{F}_{q^2})$$

where P_1 is a path in $L(q)$, $z_1' \in \mathbb{F}_{q^4}^\times$ satisfies $\langle z_1', h_1'z_1'\rangle \mathrm{Z}_{q^2+1} = B_1$, $z_1'\mathbb{F}_q^\times \mathrm{Z}_{q^2+1} = x_2$ and $w_1, w_2 \in \mathbb{F}_{q^4}^\times$ are such that either $w_1\mathbb{F}_{q^2}\mathrm{Z}_{q^2+1}$ or $w_2\mathbb{F}_{q^2}\mathrm{Z}_{q^2+1}$ is equal to $\mathfrak{b}$ and the other is equal to $\mathfrak{b}'$. The action of the generator $\sqrt{a_0}\,\mathbb{F}_q^\times$ of Z_2 maps the path P to the path

$$\sqrt{a_0}P = (\sqrt{a_0}w_1\mathbb{F}_{q^2}, \sqrt{a_0}w_1\mathbb{F}_q^\times, \sqrt{a_0}\langle z_1', h_1'z_1'\rangle, \sqrt{a_0}z_1'\mathbb{F}_q^\times, \sqrt{a_0}P_1, \sqrt{a_0}w_2\mathbb{F}_{q^2}).$$

By Lemma 2 ii) and iv), the blue nodes of $L(q)$ of the form $w\mathbb{F}_{q^2}$ ($w \in \mathbb{F}_{q^2}$) are Z_2–stable and the other blue nodes and all the red nodes are not Z_2–stable. The origins of paths P and $\sqrt{a_0}P$ are the same point and so are the termini. Denote by $(\sqrt{a_0}P)^{-1}$ the inverse path of $\sqrt{a_0}P$. The concatenated path $P\cdot(\sqrt{a_0}P)^{-1}$ in $L(q)$ is a lift of a Hamiltonian cycle of the graph $\widetilde{Q}(q) = L(q)/\mathrm{Z}_{\frac{q^2+1}{2}}$. Express the path $P\cdot(\sqrt{a_0}P)^{-1}$ simply as

$$P\cdot(\sqrt{a_0}P)^{-1} = (w_1\mathbb{F}_{q^2}, w_1\mathbb{F}_q^\times, \langle z_1', h_1'z_1'\rangle, z_1'\mathbb{F}_q^\times, P_3, w_1\mathbb{F}_{q^2}),$$

where P_3 is a path in $L(q)$. Let S be a path in $L(q)$ defined by

$$S = (w_1\mathbb{F}_{q^2}, w_1\mathbb{F}_q^\times, \langle z_1', h_1'z_1'\rangle, h_1'z_1'\mathbb{F}_q^\times, h_1'P_3, h_1'w_1\mathbb{F}_{q^2}).$$

Then S is a lift of the Hamiltonian cycle of the graph $\widetilde{Q}(q)$. The path ${h_1'}^j S$ ($j = 1, 2, \ldots$) are also lifts of the Hamiltonian cycle of the graph $\widetilde{Q}(q)$. Since $h_1'\mathbb{F}_q^\times$ generates $\mathrm{Z}_{\frac{q^2+1}{2}}$, the concatenated path $\mathscr{S} = S\cdot h_1' S\cdot {h_1'}^2 S\cdot\cdots\cdot {h_1'}^{(q^2-1)/2} S$ is a Hamiltonian cycle of $L(q)$.

2.2 Examples

Example 1 When $q = 3$, we have $\mathbb{F}_{81} = \mathbb{F}_9(\sqrt{a}) \supset \mathbb{F}_9 = \mathbb{F}_3(\sqrt{a_0}) \supset \mathbb{F}_3$ with $a_0 = -1$ and $a = 1 - \sqrt{-1}$. Put $h = \dfrac{1 - a\sqrt{a}}{1 + a\sqrt{a}}$ and take a path

$$\begin{aligned} S = {} & (\mathbb{F}_9, \sqrt{-1}\mathbb{F}_3^\times, \sqrt{-1}\langle 1, \sqrt{-1} + a\sqrt{a}\rangle, \sqrt{-1}(\sqrt{-1} + a\sqrt{a})\mathbb{F}_3^\times, \\ & \langle a\sqrt{a}, 1 - \sqrt{-1}a\sqrt{a}\rangle, (1 + \sqrt{a})\mathbb{F}_3^\times, h^2\sqrt{-1}\langle 1, a\sqrt{a}\rangle, h^2\sqrt{-1}a\sqrt{a}\,\mathbb{F}_3^\times, \\ & h^2\sqrt{a}\,\mathbb{F}_9, h^2 a\sqrt{a}\,\mathbb{F}_3^\times, h^2\langle 1, a\sqrt{a}\rangle, h\sqrt{-1}(1 + \sqrt{a})\mathbb{F}_3^\times, \\ & h\sqrt{-1}\langle a\sqrt{a}, 1 - \sqrt{-1}a\sqrt{a}\rangle, h(\sqrt{-1} + a\sqrt{a})\mathbb{F}_3^\times, h\langle 1, \sqrt{-1} + a\sqrt{a}\rangle, h\mathbb{F}_3^\times, h\mathbb{F}_9) \end{aligned}$$

Then $\mathscr{S} = S\cdot hS\cdot h^2S\cdot h^3S\cdot h^4S$ is a Hamiltonian cycle of $L(3)$ (Fig. 1).

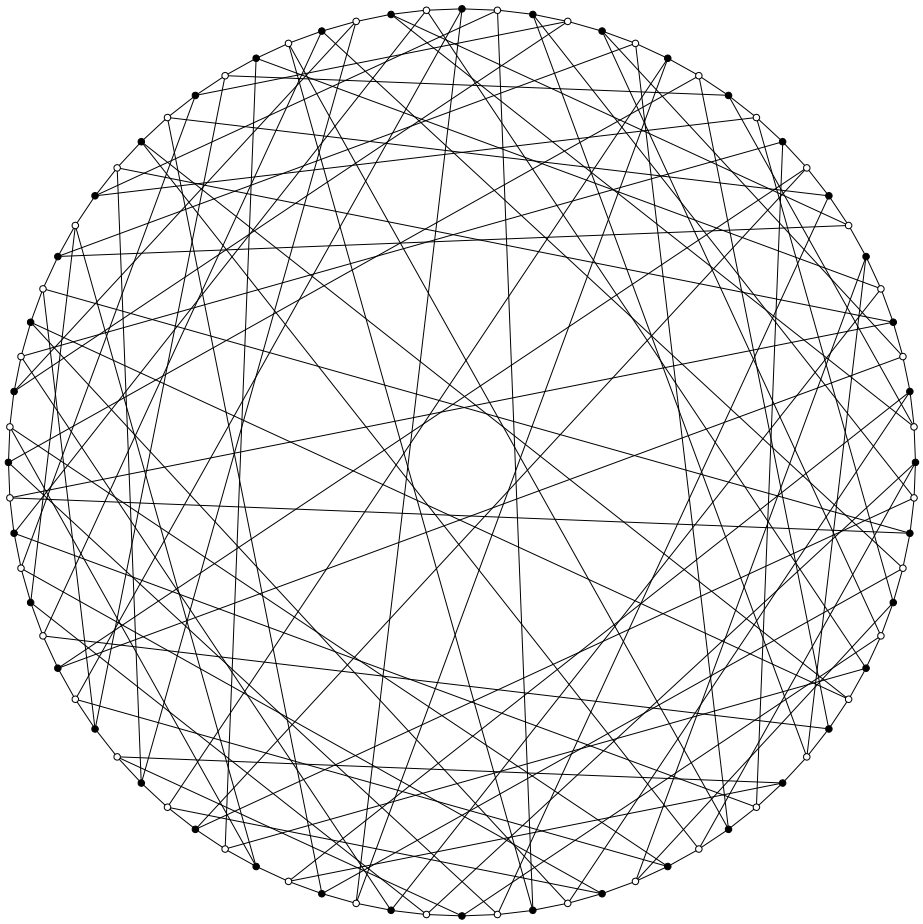

Fig. 1 $L(3)$

Example 2 When $q=5$, we have $\mathbb{F}_{625}=\mathbb{F}_{25}(\sqrt[4]{2})\supset\mathbb{F}_{25}=\mathbb{F}_5(\sqrt{2})\supset\mathbb{F}_5$ with $a_0=2$ and $a=\sqrt{2}$. Put $h=\dfrac{1-\sqrt[4]{2}}{1+\sqrt[4]{2}}$ and take a path

$$
\begin{aligned}
S=\ &(\mathbb{F}_{25},\mathbb{F}_5^\times,\langle 1,\sqrt[4]{2}\rangle,(1-\sqrt[4]{2})\mathbb{F}_5^\times,h^{12}\sqrt{2}\langle 1,\sqrt{2}+\sqrt[4]{2}\rangle,h^{12}\sqrt{2}(1-2\sqrt{2}-2\sqrt[4]{2})\mathbb{F}_5^\times,\\
&h^{11}\sqrt{2}\langle\sqrt[4]{2},1+\sqrt{2}\sqrt[4]{2}\rangle,h^{11}\sqrt{2}(1+(1+\sqrt{2})\sqrt[4]{2})\mathbb{F}_5^\times,h^5\sqrt{2}\langle 1,2\sqrt{2}+\sqrt[4]{2}\rangle,\\
&h^5\sqrt{2}(1+2\sqrt{2}+\sqrt[4]{2})\mathbb{F}_5^\times,\sqrt{2}\langle\sqrt[4]{2},2+\sqrt{2}\sqrt[4]{2}\rangle,\sqrt{2}\sqrt[4]{2}\,\mathbb{F}_5^\times,\sqrt[4]{2}\,\mathbb{F}_{25},\sqrt[4]{2}\,\mathbb{F}_5^\times,\\
&\langle\sqrt[4]{2},2+\sqrt{2}\sqrt[4]{2}\rangle,h^5(1+2\sqrt{2}+\sqrt[4]{2})\mathbb{F}_5^\times,h^5\langle 1,2\sqrt{2}+\sqrt[4]{2}\rangle,\\
&h^{11}(1+(1+\sqrt{2})\sqrt[4]{2})\mathbb{F}_5^\times,h^{11}\langle\sqrt[4]{2},1+\sqrt{2}\sqrt[4]{2}\rangle,h^{12}(1-2\sqrt{2}-2\sqrt[4]{2})\mathbb{F}_5^\times,\\
&h^{12}\langle 1,\sqrt{2}+\sqrt[4]{2}\rangle,h\sqrt{2}(1+\sqrt[4]{2})\mathbb{F}_5^\times,h\sqrt{2}\langle 1,\sqrt[4]{2}\rangle,h\sqrt{2}\mathbb{F}_5^\times,h\mathbb{F}_{25})
\end{aligned}
$$

Then $\mathscr{S}=S\cdot hS\cdot h^2S\cdots h^{11}S\cdot h^{12}S$ is a Hamiltonian cycle of $L(5)$ (Fig. 2).

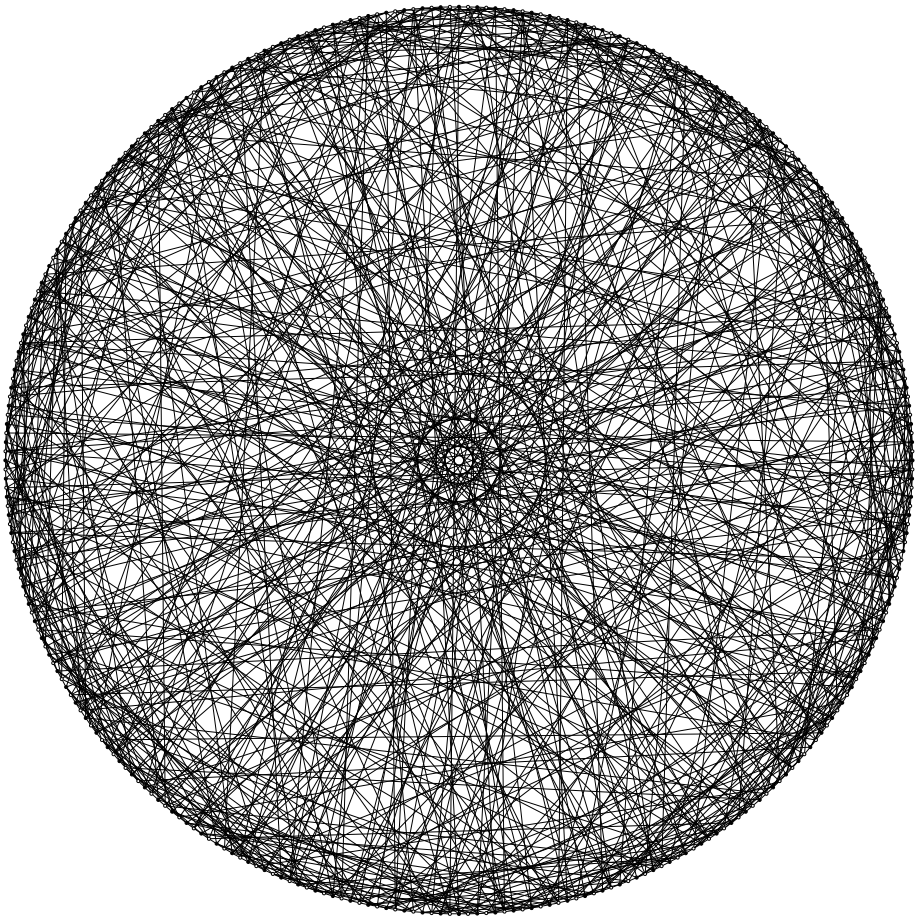

Fig. 2 $L(5)$

3 Even characteristic

In this section we assume the characteristic of the field $\mathbb{F}_q$ is 2 and we put $q = 2^n$. We define a free action on $L(q)$ of a cyclic group of order $q^2 + 1$. We denote the quotient graph by $Q(q)$. We will show that the quotient $Q(q)$ has a Hamiltonian cycle. We lift the cycle to $L(q)$. Then we have a difference between the origin and the terminus of the lifted path. We want to arrange the lift so that the gap is equal to a generator of the cyclic group. We give a numerical condition such that this arrangement works by using the $\mathrm{Gal}(\mathbb{F}_{q^4}/\mathbb{F}_2)$-action. A calculation shows that this condition is satisfied for all $q = 2^n$ $(n > 0)$. Concatenating the lifts, we obtain a Hamiltonian cycle of $L(q)$.

3.1 Proof of Theorem 1 for even q

Let $\wp : \mathbb{F}_{q^4} \longrightarrow \mathbb{F}_{q^4}$ be the polynomial mapping defined by $\wp(X) = X^2 + X$. By the Artin-Schreier theory, we can choose three elements u, t, s of $\mathbb{F}_{q^4}$ as follows. We first choose an element u in $\mathbb{F}_q \setminus \wp(\mathbb{F}_q)$. Let t be an element of $\mathbb{F}_{q^2}$ such that $t^2 + t = u$. Then $\mathbb{F}_{q^2} = \mathbb{F}_q(t)$. Since $\wp(at+b) = \wp(a)t + a^2u + \wp(b) \in \wp(\mathbb{F}_q)t + \mathbb{F}_q$ for all a and $b \in \mathbb{F}_q$, we have $ut \in \mathbb{F}_{q^2} \setminus \wp(\mathbb{F}_{q^2})$. Let s be an element of $\mathbb{F}_{q^4}$ such that $s^2 + s = ut$. Then $\mathbb{F}_{q^4} = \mathbb{F}_{q^2}(s)$. Hence we have $\mathrm{Tr}(s) = 1$ and $\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(t) = 1$. In the following we fix these three elements u, t and s.

We have the Galois groups $G_2 = \mathrm{Gal}(\mathbb{F}_{q^4}/\mathbb{F}_{q^2})$, $G_4 = \mathrm{Gal}(\mathbb{F}_{q^4}/\mathbb{F}_q)$ and $G_{4n} = \mathrm{Gal}(\mathbb{F}_{q^4}/\mathbb{F}_2)$ which are cyclic groups of order 2, 4 and $4n$ respectively. Put $\overline{G}_2 = G_4/G_2 = \mathrm{Gal}(\mathbb{F}_{q^2}/\mathbb{F}_q)$ and $\overline{G}_{2n} = G_{4n}/G_2 = \mathrm{Gal}(\mathbb{F}_{q^2}/\mathbb{F}_2)$ which are cyclic groups of order 2 and $2n$. The Galois group G_2 (resp. G_4, G_{4n}, $\overline{G}_2$, $\overline{G}_{2n}$) is generated by the Frobenius mapping $x \mapsto x^{q^2}$ (resp. x^q, x^2, x^q, x^2).

Lemma 5 *Let $q = 2^n$. The form $(*,*) : \mathbb{F}_{q^4} \times \mathbb{F}_{q^4} \to \mathbb{F}_q$ defined by*

$$(x,y) = \mathrm{Tr}_{\mathbb{F}_{q^4}/\mathbb{F}_q}(xy^{q^2}) \qquad (x, y \in \mathbb{F}_{q^4})$$

is a non-degenerate alternating $\mathbb{F}_q$-bilinear form.

Proof The mapping $y \mapsto y^{q^2}$ is the nontrivial element of $\mathrm{Gal}(\mathbb{F}_{q^4}/\mathbb{F}_{q^2})$ and it is $\mathbb{F}_{q^2}$-linear. Since $\mathrm{Tr}_{\mathbb{F}_{q^4}/\mathbb{F}_q}$ is $\mathbb{F}_q$-linear, the form $(*,*)$ is $\mathbb{F}_q$-bilinear. For an element $x \in \mathbb{F}_{q^4}$, we have

$$(x,x) = \mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\mathrm{Tr}(\mathrm{N}(x))) = \mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\mathrm{N}(x)\,\mathrm{Tr}(1)) = 0.$$

Since $\mathrm{Tr}_{\mathbb{F}_{q^4}/\mathbb{F}_q}$ is surjective, for each $y \neq 0$, we can take an element x such that $(x,y) \neq 0$. Thus $(*,*)$ is a non-degenerate alternating $\mathbb{F}_q$-bilinear form.

We use this form in the construction of $C(q)$ and $L(q)$. Since $(x^2, y^2) = (x,y)^2$, the Galois group G_{4n} acts on $L(q)$. Let η be an edge of $L(q)$ incident to a red node x and a blue node ℓ. We denote by η^{2^m} the edge of $L(q)$ incident to the red node x^{2^m} and the blue node ℓ^{2^m}. Denote by Z_{q^2+1} the subgroup $\mathrm{N}^{-1}(\mathbb{F}_q^\times)/\mathbb{F}_q^\times$ of $\mathbb{F}_{q^4}^\times/\mathbb{F}_q^\times$ of order q^2+1.

Lemma 6 *i) If $x \in \mathbb{F}_{q^4}^\times$, then the plane $x\mathbb{F}_{q^2}$ is totally isotropic.*
ii) $\mathrm{N}^{-1}(\mathbb{F}_q^\times) \cap \mathbb{F}_{q^2}^\times = \mathbb{F}_q^\times$.
iii) Let $h \in \mathrm{N}^{-1}(\mathbb{F}_q^\times) \setminus \mathbb{F}_q^\times$. Then $\mathrm{Tr}(h) \notin \mathbb{F}_q$. For $z \in \mathbb{F}_{q^4}^\times$, the $\mathbb{F}_q$-linear subspace $\langle z, zh\rangle$ is totally isotropic if and only if $\mathrm{N}(z)\mathbb{F}_q^\times = \mathrm{Tr}(h)^{-1}\mathbb{F}_q^\times$.
iv) If $h \in \mathrm{N}^{-1}(\mathbb{F}_q^\times) \setminus \mathbb{F}_q^\times$ and $\alpha \in \mathbb{F}_q^\times$, then $h+\alpha \notin \mathrm{N}^{-1}(\mathbb{F}_q^\times)$ and $\dfrac{h+\alpha}{h+\dfrac{\mathrm{N}(h)}{\alpha}} \in \mathrm{N}^{-1}(\mathbb{F}_q^\times)$.
Moreover we have $(h+\alpha)\mathbb{F}_q^\times = (h+\dfrac{\mathrm{N}(h)}{\alpha})\mathbb{F}_q^\times$ if and only if $\alpha = \sqrt{\mathrm{N}(h)}$.

v) Let $h \in \mathrm{N}^{-1}(\mathbb{F}_q^\times) \setminus \mathbb{F}_q^\times$ and $z \in \mathbb{F}_{q^4}^\times$. Suppose that the $\mathbb{F}_q$-linear subspace $\langle z, zh\rangle$ is totally isotropic as in iii). Then $\mathrm{N}(z(h+\sqrt{\mathrm{N}(h)}))\mathbb{F}_q^\times = \mathbb{F}_q^\times$.
vi) For $x \in \mathbb{F}_{q^4}^\times \setminus \mathrm{N}^{-1}(\mathbb{F}_q^\times)$ and $\beta \in \mathrm{N}^{-1}(\mathbb{F}_q^\times)$, the plane $\langle x, x^q\beta\rangle$ is totally isotropic if and only if $\beta \in x^{-q(1+q)}\mathbb{F}_q^\times$. In such a case, $\langle x, x^q\beta\rangle = x\mathbb{F}_{q^2}$.
vii) There exist elements $h \in \mathrm{N}^{-1}(\mathbb{F}_q^\times)$ and $z \in \mathbb{F}_{q^4}^\times$ which satisfy the following conditions a) and b):

a) $h\mathbb{F}_q^\times$ generates Z_{q^2+1}.

b) The plane $\ell = \langle z, zh\rangle$ is totally isotropic, 2n orbits $\ell\mathrm{Z}_{q^2+1}$, $\ell^2\mathrm{Z}_{q^2+1}$, $\ell^{2^2}\mathrm{Z}_{q^2+1}$, …, $\ell^{2^{2n-1}}\mathrm{Z}_{q^2+1}$ of blue nodes are mutually distinct and 2n orbits $z\mathbb{F}_q^\times\mathrm{Z}_{q^2+1}$, $(z\mathbb{F}_q^\times)^2\mathrm{Z}_{q^2+1}$, $(z\mathbb{F}_q^\times)^{2^2}\mathrm{Z}_{q^2+1}$, …, $(z\mathbb{F}_q^\times)^{2^{2n-1}}\mathrm{Z}_{q^2+1}$ of red nodes are mutually distinct.

Proof i) Since

$$(xt, x) = \mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\mathrm{Tr}(\mathrm{N}(x)t)) = \mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\mathrm{N}(x)t\,\mathrm{Tr}(1)) = 0,$$

the $\mathbb{F}_q$-linear subspace $x\mathbb{F}_{q^2} = \langle x, xt\rangle$ is isotropic.
ii) The restriction of the norm mapping N to $\mathbb{F}_{q^2}$ is equal to the square mapping $x \mapsto x^2$. Since the orders $|\mathbb{F}_{q^2}^\times|$ and $|\mathbb{F}_q^\times|$ are odd, the square mapping are automorphisms on $\mathbb{F}_{q^2}^\times$ and $\mathbb{F}_q^\times$. Thus we have ii).
iii) If both $\mathrm{N}(h)$ and $\mathrm{Tr}(h)$ belong to $\mathbb{F}_q$, h must belong to $\mathbb{F}_{q^2}$. This contradicts ii). Hence $\mathrm{Tr}(h) \notin \mathbb{F}_q$. For $x_1, x_2 \in \mathbb{F}_q$, we have $\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(x_1 + x_2 t) = x_2$. Thus the equation $(zh, z) = \mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\mathrm{N}(z)\,\mathrm{Tr}(h)) = 0$ holds if and only if $\mathrm{N}(z)\,\mathrm{Tr}(h) \in \mathbb{F}_q$.
iv) If $\mathrm{N}(h+\alpha) = \mathrm{N}(h) + \mathrm{Tr}(h)\alpha + \alpha^2 \in \mathbb{F}_q$, then $\mathrm{Tr}(h) \in \mathbb{F}_q$. This contradicts iii). Hence $h + \alpha \notin \mathrm{N}^{-1}(\mathbb{F}_q^\times)$. Since $h + \dfrac{\mathrm{N}(h)}{\alpha} = \dfrac{h}{\alpha}(\alpha + h^{q^2})$, we have $\mathrm{N}(h + \dfrac{\mathrm{N}(h)}{\alpha}) = \dfrac{\mathrm{N}(h)}{\alpha^2}\mathrm{N}(h+\alpha)$ and $\dfrac{h+\alpha}{h + \dfrac{\mathrm{N}(h)}{\alpha}} \in \mathrm{N}^{-1}(\mathbb{F}_q^\times)$. Since $h \notin \mathbb{F}_{q^2}$ and 1 are linearly independent over $\mathbb{F}_q$, the equation $(h+\alpha)\mathbb{F}_q^\times = (h + \dfrac{\mathrm{N}(h)}{\alpha})\mathbb{F}_q^\times$ holds if and only if $\alpha = \dfrac{\mathrm{N}(h)}{\alpha}$. This condition is equivalent to $\alpha = \sqrt{\mathrm{N}(h)}$ because the order $|\mathbb{F}_q^\times|$ is odd.
v) From iii), we get $\mathrm{N}(z)\mathbb{F}_q^\times = \dfrac{1}{\mathrm{Tr}(h)}\mathbb{F}_q^\times$. Since $\mathrm{N}(h + \sqrt{\mathrm{N}(h)}) = \mathrm{Tr}(h)\sqrt{\mathrm{N}(h)}$, we have v).
vi) Since $(x^q\beta, x) = \mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\mathrm{Tr}(\beta x^q x^{q^2})) = 0$, we have $\mathrm{Tr}(\beta x^q x^{q^2}) \in \mathbb{F}_q$. Since $\mathrm{N}(\beta x^q x^{q^2}) = \mathrm{N}(\beta)\,\mathrm{N}_{\mathbb{F}_{q^4}/\mathbb{F}_q}(x) \in \mathbb{F}_q$, $\beta x^q x^{q^2}$ must belong to $\mathbb{F}_{q^2}^\times$. From ii), we have $\beta x^q x^{q^2} \in \mathbb{F}_q$. In such a case, $\dfrac{\beta x^q}{x} = \dfrac{\beta x^q x^{q^2}}{\mathrm{N}(x)} \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$. The converse is evident.

We prepare Lemma 7 to prove vii). Let φ be Euler's totient function. We define a function ψ by

$$\psi(q) = \sharp\{x \in (\mathbb{F}_{q^2}^\times/\mathbb{F}_q^\times) \setminus \{\mathbb{F}_q^\times\} \mid x^{2^k} \neq x \quad \text{for } k = 0, 1, \ldots, 2n-1\}$$

for $q = 2^n$.

Put $\mathfrak{r} = \mathbb{F}_q^\times \mathrm{Z}_{q^2+1}$ and $\mathfrak{b} = \mathbb{F}_{q^2} \mathrm{Z}_{q^2+1}$.

Lemma 7 *i) There are $\overline{G}_{2n}$-bijections*

$$f_1 : \mathrm{b}(Q(q)) \setminus \{\mathfrak{b}\} \longrightarrow (\mathbb{F}_{q^2}^\times/\mathbb{F}_q^\times) \setminus \{\mathbb{F}_q^\times\}, \quad f_2 : \mathrm{r}(Q(q)) \setminus \{\mathfrak{r}\} \longrightarrow (\mathbb{F}_{q^2}^\times/\mathbb{F}_q^\times) \setminus \{\mathbb{F}_q^\times\}.$$

ii) $\psi(q)^2 + \varphi(q^2+1) > q^2$ for all $q = 2^n$.

Proof i) The norm mapping N induces a $\overline{G}_{2n}$–bijection $f_2 : \mathrm{r}(Q(q)) \setminus \{\mathfrak{r}\} \longrightarrow (\mathbb{F}_{q^2}^\times/\mathbb{F}_q^\times) \setminus \{\mathbb{F}_q^\times\}$. Namely, for $x \in \mathbb{F}_{q^4}^\times \setminus \mathrm{N}^{-1}(\mathbb{F}_q^\times)$, we define f_2 by $f_2(x\mathbb{F}_q^\times \mathrm{Z}_{q^2+1}) = \mathrm{N}(x)\mathbb{F}_q^\times$. For $\beta \in \mathbb{F}_q$, $(t+\beta)\mathbb{F}_q^\times \in (\mathbb{F}_{q^2}^\times/\mathbb{F}_q^\times) \setminus \{\mathbb{F}_q^\times\}$, $y = s + \beta t \in \mathrm{Tr}^{-1}(1)$ and $\langle 1, y\rangle \mathrm{Z}_{q^2+1}$ is an element of $\mathrm{b}(Q(q)) \setminus \{\mathfrak{b}\}$. By Lemma 6 iii), we see that this correspondence induces a bijection $(\mathbb{F}_{q^2}^\times/\mathbb{F}_q^\times) \setminus \{\mathbb{F}_q^\times\} \to \mathrm{Tr}^{-1}(1)/\mathbb{F}_q \to \mathrm{b}(Q(q)) \setminus \{\mathfrak{b}\}$. Let f_1 be the inverse of this mapping. Namely we define f_1 by $f_1(\langle 1, s+\beta t\rangle \mathrm{Z}_{q^2+1}) = (t+\beta)\mathbb{F}_q^\times$ for all $\beta \in \mathbb{F}_q$. Since $y^2 = s + (u+\beta^2)t + \beta^2 u$ and $(t+\beta)^2 = t + (u+\beta^2)$, this bijection is a $\overline{G}_{2n}$-bijection. Hence we have i).

ii) For $q = 2^n$, define an integer v by $n = 2^v n'$ where $n' \in \mathbb{N}$ is an odd number. Let t' be an element of $\mathbb{F}_{2^{2^v+1}} \setminus \mathbb{F}_{2^{2^v}}$. Let x be an element of $(\mathbb{F}_{q^2}^\times/\mathbb{F}_q^\times) \setminus \{\mathbb{F}_q^\times\}$. Then there exists a unique $a \in \mathbb{F}_q$ such that $x = (t'+a)\mathbb{F}_q^\times$. It is easy to see that x is contained in $\{x \in (\mathbb{F}_{q^2}^\times/\mathbb{F}_q^\times) \setminus \{\mathbb{F}_q^\times\} \mid x^{2^k} \neq x \quad \text{for } k = 0, 1, \ldots, 2n-1\}$ if and only if a is contained in an intermediate field K such that $\mathbb{F}_{2^{2^v}} \subsetneqq K \subsetneqq \mathbb{F}_q$.

In fact, assume that $x^{2^k} = x$ for some $1 \leqq k \leqq 2n-1$ and $x^{2^m} \neq x$ for $1 \leqq m < k$. Let G be the maximal subgroup of $\overline{G}_{2n}$ which fixes x. Then G is of order $\dfrac{2n}{k}$. Since $q-1$ is odd and all Galois cohomology groups of multiplicative groups of finite fields are trivial, we see that the G–invariant part $(\mathbb{F}_{q^2}^\times/\mathbb{F}_q^\times)^G$ is equal to $(\mathbb{F}_{q^2}^\times)^G \mathbb{F}_q^\times/\mathbb{F}_q^\times = \mathbb{F}_{2^k}^\times \mathbb{F}_q^\times/\mathbb{F}_q^\times$. If k divides n, then $\mathbb{F}_{2^k}^\times \subset \mathbb{F}_q^\times$ and there is no such x. Hence it follows that $k = 2m$ with $m < n$, $2^v | m$ and $m | n$. Since $\mathbb{F}_{2^k}^\times \mathbb{F}_q^\times/\mathbb{F}_q^\times \cong \mathbb{F}_{2^k}^\times/(\mathbb{F}_{2^k}^\times \cap \mathbb{F}_q^\times) = \mathbb{F}_{2^k}^\times/\mathbb{F}_{2^m}^\times$ and $t' \in \mathbb{F}_{2^k}^\times \setminus \mathbb{F}_{2^m}^\times$, we have $x = (t'+a)\mathbb{F}_q^\times$ for some $a \in \mathbb{F}_{2^m}^\times$. Conversely if $x = (t'+a)\mathbb{F}_q^\times$ for some $a \in \mathbb{F}_{2^m}^\times$ with $m < n$, $2^v | m$ and $m | n$, we have $x^{2^k} = x$ with $k = 2m$. Thus $x^{2^k} = x$ holds for some $1 \leqq k \leqq 2n-1$ if and only if a belongs to $\mathbb{F}_{2^m}$ for some $m < n$ such that $2^v | m$ and $m | n$. Hence we have the equation $\psi(q) = \sharp(\mathbb{F}_q \setminus \bigcup K)$, where K runs through the intermediate fields $\mathbb{F}_{2^{2^v}} \subsetneqq K \subsetneqq \mathbb{F}_q$.

We have $\psi(q)^2 \geqq (q^2+1) - 3(q^2+1)^{2/3}$. Indeed, write $n = 2^v p_1^{v_1} \cdots p_m^{v_m}$ with odd primes $p_1 < \cdots < p_m$ and positive numbers $v_1, \ldots, v_m$. The set of maximal fields K such that $\mathbb{F}_{2^{2^v}} \subsetneqq K \subsetneqq \mathbb{F}_q$ is equal to $\{\mathbb{F}_{2^{n/p_1}}, \mathbb{F}_{2^{n/p_2}}, \ldots, \mathbb{F}_{2^{n/p_m}}\}$. Since p_j and p_{j+1} are odd primes, we have $\dfrac{n}{p_j} - \dfrac{n}{p_{j+1}} = \dfrac{(p_{j+1}-p_j)n}{p_j p_{j+1}} \geqq 2$. Hence we have

$$\begin{aligned} \sharp(\bigcup K) &\leqq 2^{n/p_1} + \sum_{j=2}^{m} 2^{n/p_j} \leqq 2^{n/p_1} + \sum_{j=2}^{n/p_1} 2^{(n/p_1)-j} \\ &< 2^{n/p_1} + 2^{(n/p_1)-1} = \frac{3}{2} 2^{n/p_1}. \end{aligned}$$

Consequently we have $\psi(q) \geqq 2^n - \frac{3}{2}2^{n/p_1} \geqq 2^n - \frac{3}{2}2^{n/3}$ and

$$\begin{aligned}\psi(q)^2 &\geqq (2^n - \frac{3}{2}2^{n/3})^2 = 2^{2n} - 3\cdot 2^{4n/3} + \frac{9}{4}2^{2n/3} \\ &\geqq (q^2+1) - 3(q^2+1)^{2/3}.\end{aligned}$$

A prime number $a \geq 5$ such that $a \equiv 1 \mod 4$ appears as a divisor of a number of the form q^2+1. But a prime number $b \geq 3$ such that $b \equiv 3 \mod 4$ does not divide any q^2+1. Note that the function $\frac{x-1}{x^{2/3}} = x^{1/3} - x^{-2/3}$ is monotonically increasing for $x > 0$. Write $q^2+1 = p_1^{v_1}p_2^{v_2}\cdots p_m^{v_m}$ with distinct primes p_1, …, p_m and positive numbers v_1, …, v_m. Put $\alpha_j = \frac{p_j - 1}{p_j^{2/3}}$ for $j = 1, 2, \ldots, m$. Then we have

$$\begin{aligned}\varphi(q^2+1) &= \varphi(p_1^{v_1})\varphi(p_2^{v_2})\cdots\varphi(p_m^{v_m}) \\ &= (p_1-1)p_1^{v_1-1}(p_2-1)p_2^{v_2-1}\cdots(p_m-1)p_m^{v_m-1} \\ &= \alpha_1 p_1^{(v_1-1)/3}\cdots\alpha_m p_m^{(v_m-1)/3}(p_1^{v_1}p_2^{v_2}\cdots p_m^{v_m})^{2/3} \\ &= \alpha_1 p_1^{(v_1-1)/3}\cdots\alpha_m p_m^{(v_m-1)/3}(q^2+1)^{2/3}.\end{aligned}$$

By an elementary numerical estimate, we see the inequality $\varphi(q^2+1) \geqq 3(q^2+1)^{2/3}$ holds if one of the following conditions are satisfied: (1) q^2+1 is divisible by a prime $p \geqq 31$; (2) q^2+1 is divisible by pp' with primes p, $p' \geqq 13$; (3) q^2+1 is divisible by $5p$ with a prime $p \geqq 17$; (4) q^2+1 is divisible by 5^2p with a prime $p \geqq 5$. Consequently we obtain

$$\psi(q)^2 + \varphi(q^2+1) > q^2$$

except when $q^2+1 = 5$, 13, 17, 19, 23, 29, 25, 65. Since $q = 2^n$, it is sufficient to consider the three cases $q^2+1 = 5$, 17 and 65. For these three cases a direct calculation shows the following: For $q = 2$, $\psi(2) = 2$ and $\varphi(5) = 4$. For $q = 4$, $\psi(4) = 4$ and $\varphi(17) = 16$. For $q = 8$, $\psi(8) = 6$ and $\varphi(65) = 48$. Hence these three cases satisfy the inequality.
Thus the inequality

$$\psi(q)^2 + \varphi(q^2+1) > q^2$$

holds for all $q = 2^n$ with $n > 0$.

Proof (Proof of Lemma 6 vii).) For $h \in \mathrm{N}^{-1}(\mathbb{F}_q^\times) \setminus \mathbb{F}_q^\times$, we can take an element $z \in \mathbb{F}_{q^4}^\times$ such that $\langle z, zh\rangle$ is totally isotropic. By Lemma 6 i)-vi), the mapping $(\mathrm{Z}_{q^2+1} \setminus \{1\})/G_2 \longrightarrow (\mathrm{b}(Q(q)) \setminus \{\mathfrak{b}\}) \times (\mathrm{r}(Q(q)) \setminus \{\mathfrak{r}\})/\overline{G}_2$ which maps $(h\mathbb{F}_q^\times)G_2$ to $(\langle z, zh\rangle\mathrm{Z}_{q^2+1}, (z\mathbb{F}_q^\times \mathrm{Z}_{q^2+1})\overline{G}_2)$ is bijective. Hence by Lemma 7 i), the number of $h\mathbb{F}_q^\times$'s which satisfy Lemma 6 vii-b) is equal to $\psi(q)^2$. Since the number of $h\mathbb{F}_q^\times$'s which satisfy Lemma 6 vii-a) is equal to $\varphi(q^2+1)$, Lemma 7 ii) shows that the sum of the number of $h\mathbb{F}_q^\times$'s which satisfy Lemma 6 vii-b) and the number of $h\mathbb{F}_q^\times$'s which satisfy Lemma 6 vii-a) is greater than q^2 , which is equal to the number of all $h\mathbb{F}_q^\times$'s in $\mathrm{Z}_{q^2+1} \setminus \{1\}$. Hence there exists an h which satisfies both Lemma 6 vii-b) and vii-a).

Now we study properties of the quotient graph $Q(q) = L(q)/\mathrm{Z}_{q^2+1}$. By definition, $\mathrm{Gal}(\mathbb{F}_{q^4}/\mathbb{F}_2)$ acts on $Q(q)$.

Lemma 8 *The graph $Q(q)$ consists of the following sets of red nodes $\mathrm{r}(Q(q))$, blue nodes $\mathrm{b}(Q(q))$ and edges $e(Q(q))$;*

$$\mathrm{r}(Q(q)) = \{\mathfrak{r}, x_1, \dots, x_{\frac{q}{2}}, y_1, \dots, y_{\frac{q}{2}}\},$$
$$\mathrm{b}(Q(q)) = \{\mathfrak{b}, b_1, \dots, b_{\frac{q}{2}}, B_1, \dots, B_{\frac{q}{2}}\},$$

where $b_i = \langle z_i, z_i h_i \rangle \mathrm{Z}_{q^2+1}$ for some $z_i \in \mathbb{F}_{q^4}^\times$, $h_i \in \mathrm{Ker}\,\mathrm{N} \cdot \mathbb{F}_q^\times$ $(i = 1, \dots, \frac{q}{2})$ such that $h_1 \mathbb{F}_q^\times$ generates Z_{q^2+1}, $b_1 = \langle z_1, z_1 h_1 \rangle$, $x_1 = z_1 \mathbb{F}_q^\times$, $b_2 = b_1^2$, $x_2 = x_1^2$, …, $b_n = b_1^{2^{n-1}}$, $x_n = x_1^{2^{n-1}}$, and $B_j = b_j^q$, $y_j = x_j^q$ for $j = 1$, …, $\frac{q}{2}$. The set of edges $e(Q(q))$ consists of the following edges. The blue node $\mathfrak{b}$ is adjacent to every red node by a 1-edge. The red node $\mathfrak{r}$ is adjacent to every blue node by a 1-edge. For each j, b_j is adjacent to x_j by a 2-edge. For each j, B_j is adjacent to y_j by a 2-edge. For each $j \neq k$, b_j is adjacent to one of x_k and y_k by a 2-edge and B_j is adjacent the other by a 2-edge.

Proof Since $\mathbb{F}_{q^4}^\times / \mathrm{N}^{-1}(\mathbb{F}_q^\times) = q+1$ and $q^2 \equiv 1 \mod (q+1)$, each red node of $Q(q)$ is $\mathrm{Gal}(\mathbb{F}_{q^4}/\mathbb{F}_{q^2})$-invariant and $\mathfrak{r} = \mathbb{F}_q^\times \mathrm{Z}_{q^2+1}$ is the unique $\mathrm{Gal}(\mathbb{F}_{q^4}/\mathbb{F}_q)$-invariant red node. Denote these red nodes except $\mathfrak{r}$ by x_1, …, $x_{\frac{q}{2}}$, $y_1 = x_1^q$, …, $y_{\frac{q}{2}} = x_{\frac{q}{2}}^q$. The blue node $\mathfrak{b} = \mathbb{F}_{q^2} \mathrm{Z}_{q^2+1}$ is also $\mathrm{Gal}(\mathbb{F}_{q^4}/\mathbb{F}_q)$-invariant and is adjacent to all the red nodes by 1-edges. For $h \in \mathrm{N}^{-1}(\mathbb{F}_q^\times) \setminus \mathbb{F}_q^\times$, we can take an element $z \in \mathbb{F}_{q^4}^\times$ such that $\langle z, zh \rangle$ is totally isotropic by Lemma 6 iii), and we consider the orbit $\langle z, zh \rangle \mathrm{Z}_{q^2+1}$. By Lemma 6 iv), $q(q-1)$ h's determine one orbit. Hence there are $\dfrac{|\mathrm{N}^{-1}(\mathbb{F}_q^\times) \setminus \mathbb{F}_q^\times|}{q(q-1)} = q$ distinct orbits of this kind. Since $z\langle 1, h \rangle = zh\langle 1, h^{-1} \rangle = zh\langle 1, h^{q^2} \rangle$, each orbit of this kind is $\mathrm{Gal}(\mathbb{F}_{q^4}/\mathbb{F}_{q^2})$-invariant. In the inverse image of each 2-edge of $Q(q)$, the nontrivial element of $\mathrm{Gal}(\mathbb{F}_{q^4}/\mathbb{F}_{q^2})$ induces the transposition of two Z_{q^2+1}-orbits of edges. By Lemma 6 vi), each orbit $\langle z, zh \rangle \mathrm{Z}_{q^2+1}$ of this kind is not $\mathrm{Gal}(\mathbb{F}_{q^4}/\mathbb{F}_q)$-invariant. We denotes these orbits by b_1, …, $b_{\frac{q}{2}}$, $B_1 = b_1^q$, …, $B_{\frac{q}{2}} = b_{\frac{q}{2}}^q$. Comparing the numbers of blue nodes, we see that $\mathrm{b}(Q(q))$ consists of $\mathfrak{b}$ and these q orbits. By Lemma 6 v), every blue node is adjacent to $\mathfrak{r}$ by a 1-edge. By Lemma 2 vi), b_j is adjacent to at most one of x_k and y_k for each k. Comparing the number of edges incident to a blue node, we see that b_j is adjacent to either x_k or y_k for each k and B_j is adjacent to the other. Changing x_j and y_j, we may assume b_j is adjacent to x_j. By Lemma 6 vii), we can arrange so that the additional conditions are satisfied.

Proof (Proof of Theorem 1) By Lemma 8, we have a Hamiltonian cycle $\overline{S}$ of $Q(q)$ containing (b_i, x_i) or (x_i, b_i) for all $1 \leqq i \leqq \dfrac{q}{2}$ and (B_i, y_i) or (y_i, B_i) for all $1 \leqq i \leqq \dfrac{q}{2}$. Take a path S in $L(q)$ which begins at $\mathbb{F}_q^\times$ and is a lift of the Hamiltonian cycle $\overline{S}$ as follows: If $\overline{S}$ contains (b_i, x_i) with $1 \leqq i \leqq n$, its lift in S has the form $(\langle z, zh_1^{2^i} \rangle, gz\mathbb{F}_q^\times)$. If $\overline{S}$ contains (x_i, b_i) with $1 \leqq i \leqq n$, its lift in S has the form $(h_1^{2^i} z\mathbb{F}_q^\times, \langle z, zh_1^{2^i} \rangle)$. We denote this edge by η_i. If $\overline{S}$ contains (B_i, y_i) with $1 \leqq i \leqq n$, its lift in S has the

form $(\langle z, zh_1^{2^{n+i}}\rangle, z\mathbb{F}_q^\times)$. If $\overline{S}$ contains (y_i, B_i) with $1 \leqq i \leqq n$, its lift in S has the form $(zh_1^{2^{n+i}}\mathbb{F}_q^\times, \langle z, zh_1^{2^{n+i}}\rangle)$. We denote this edge by η_{n+i}. Denote the terminus of S by $h_0\mathbb{F}_q^\times$. By Lemma 8, there are two edges incident to b_i and x_i. If we arrange S at η_i by choosing the other edge incident to b_i and x_i, we can take another lift S_i in $L(q)$ of $\overline{S}$. This another lift S_i is expressed as

$$S_i = (\mathbb{F}_q^\times, \cdots, \langle z, zh_1^{2^i}\rangle, zh_1^{2^i}\mathbb{F}_q^\times, \cdots, h_0h_1^{2^i}\mathbb{F}_q^\times)$$

or

$$S_i = (\mathbb{F}_q^\times, \cdots, h_1^{2^i}z\mathbb{F}_q^\times, h_1^{2^i}\langle z, zh_1^{2^i}\rangle, \cdots, h_0h_1^{2^i}\mathbb{F}_q^\times)$$

which terminates at $h_0h_1^{2^i}\mathbb{F}_q^\times$. Similarly, if we arrange S at η_{n+i}, we have the other lift

$$S_{n+i} = (\mathbb{F}_q^\times, \cdots, \langle z, zh_1^{2^{n+i}}\rangle, zh_1^{2^{n+i}}\mathbb{F}_q^\times, \cdots, h_0h_1^{2^{n+i}}\mathbb{F}_q^\times)$$

or

$$S_{n+i} = (\mathbb{F}_q^\times, \cdots, h_1^{2^{n+i}}z\mathbb{F}_q^\times, h_1^{2^{n+i}}\langle z, zh_1^{2^{n+i}}\rangle, \cdots, h_0h_1^{2^{n+i}}\mathbb{F}_q^\times)$$

which terminates at $h_0h_1^{2^{n+i}}\mathbb{F}_q^\times$. If we arrange S at η_{j_1}, …, η_{j_s}, we have a lift of $\overline{S}$ from $\mathbb{F}_q^\times$ to $h_0h_1^{2^{j_1}+\cdots+2^{j_s}}\mathbb{F}_q^\times$. The sum $2^{j_1}+\cdots+2^{j_s}$ for distinct numbers $1 \leq j_1$, …, $j_s \leq 2n$ with $0 \leq s \leq 2n$ takes all the values from 0 to $2^{2n}-1$. Since h_1 generates Z_{q^2+1}, the element $h_0h_1^{2^{j_1}+\cdots+2^{j_s}}\mathbb{F}_q^\times$ runs all the element of Z_{q^2+1} except $h_0h_1^{-1}\mathbb{F}_q^\times$. Hence there exists a lift $\widetilde{S}$ from $\mathbb{F}_q^\times$ to $h'\mathbb{F}_q^\times$ such that $h'\mathbb{F}_q^\times$ generates Z_{q^2+1}. Thus we have a Hamiltonian cycle $\mathscr{S} = \widetilde{S}\cdot h'\widetilde{S}\cdot (h')^2\widetilde{S}\cdot\cdots\cdot (h')^{q^2}\widetilde{S}$ of $L(q)$.

3.2 Examples

Example 3 When $q=2$, the element u is equal to 1. We have $\mathbb{F}_{16} = \mathbb{F}_4(s) \supset \mathbb{F}_4 = \mathbb{F}_2(t) \supset \mathbb{F}_2$ with $s^2+s=t$ and $t^2+t=1$. Put $h = \dfrac{s+1}{s}$, then $h = (t+1)s+t \neq 1$ and $h\mathbb{F}_2^\times$ is a generator which satisfies the conditions of Lemma 6 vii). Take a path

$$S = (\mathbb{F}_2^\times, \langle 1, s\rangle, s\mathbb{F}_2^\times, h^2\mathbb{F}_4, h^2t\mathbb{F}_2^\times, h\langle 1, s+t\rangle, h\mathbb{F}_2^\times).$$

The equations $s\mathbb{F}_2^\times = h^2(t+1)\mathbb{F}_2^\times$ and $h^2t\mathbb{F}_2^\times = h(s+t+1)\mathbb{F}_2^\times$ show that S is a path. Then $\mathscr{S} = S\cdot hS\cdot h^2S\cdot h^3S\cdot h^4S$ is a Hamiltonian cycle of $L(2)$ (Fig. 3).

This graph is the Tutte-Coxeter cage.

Example 4 When $q=4$ we have $\mathbb{F}_{256} = \mathbb{F}_{16}(s) \supset \mathbb{F}_{16} = \mathbb{F}_4(t) \supset \mathbb{F}_4 = \mathbb{F}_2(u) \supset \mathbb{F}_2$ with $s^2+s=ut$, $t^2+t=u$ and $u^2+u=1$. Put $h = \dfrac{s+1}{s}$, then $h = u(t+1)s+ut+u+1 \neq 1$ and $h\mathbb{F}_4^\times$ is a generator which satisfies the condition of Lemma 6 vii). Take a path

$$\begin{aligned} S' = {} & (\mathbb{F}_4^\times, \langle 1, s\rangle, s\mathbb{F}_4^\times, h^3\langle 1, s+ut\rangle, h^3(s+ut)\mathbb{F}_4^\times, h^2\mathbb{F}_{16}, h^2(t+1)\mathbb{F}_4^\times, \\ & h^6\langle 1, s+(u+1)t\rangle, h^6(s+(u+1)t)\mathbb{F}_4^\times, h\langle 1, s+t\rangle, h\mathbb{F}_4^\times). \end{aligned}$$

The equations $s\mathbb{F}_4^\times = h^3(s+ut+u)\mathbb{F}_4^\times$, $h^3(s+ut)\mathbb{F}_4^\times = h^2t\mathbb{F}_4^\times$, $h^2(t+1)\mathbb{F}_4^\times = h^6(s+(u+1)t+u+1)\mathbb{F}_4^\times$, $h^6(s+(u+1)t)\mathbb{F}_4^\times = h(s+t)\mathbb{F}_4^\times$ show that S' is a path. Hence $\mathscr{S} = S'\cdot hS'\cdot h^2S'\cdots h^{16}S'$ is a Hamiltonian cycle of $L(4)$ (Fig. 4).

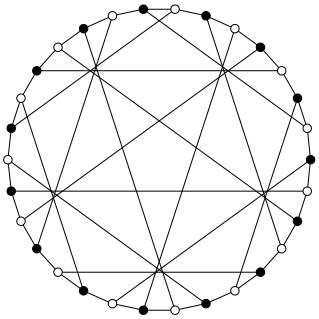

Fig. 3 Tutte-Coxeter Cage $L(2)$

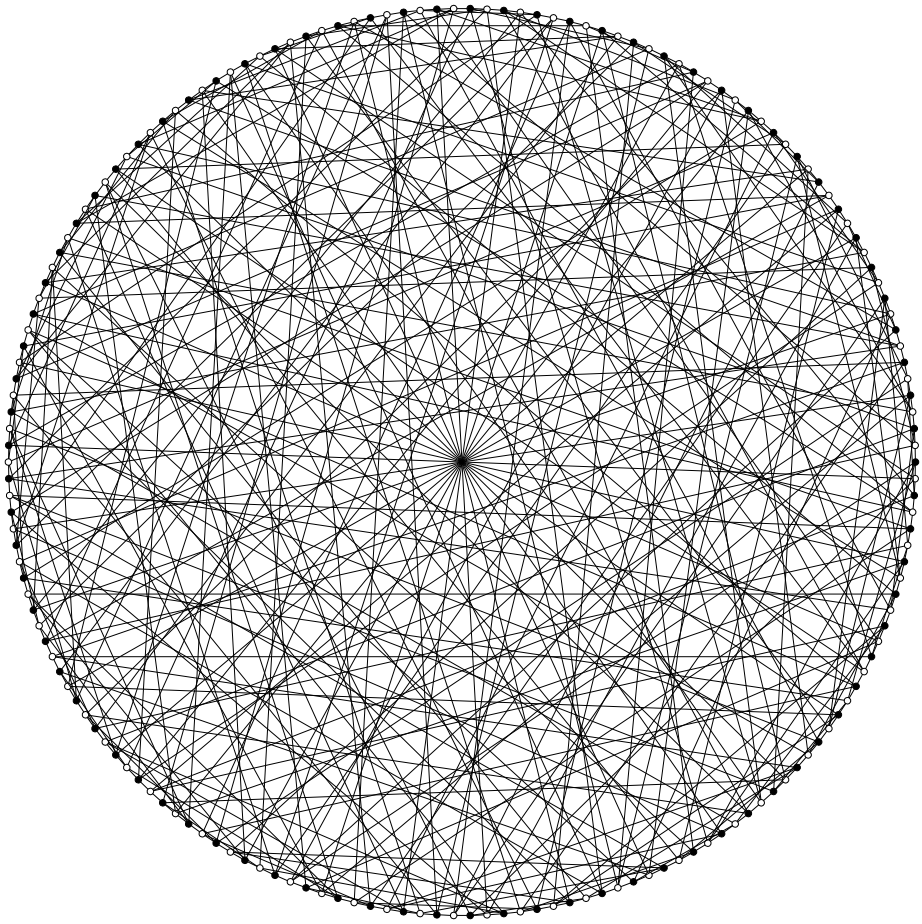

Fig. 4 $L(4)$

References

1. R. C. Bose, An affine analogue of Singer's theorem, J. Indian Math. Soc., 6 (1942), 1–15.
2. W. G. Brown, On Hamiltonian regular graphs of girth six, J. London Math. Soc., 42 (1967), 514–520.
3. V. Chvátal, On Hamilton's ideals, J. Combinatorial Theory, 12(B) (1972), 163–168.
4. H. S. M. Coxeter, Self-dual configurations and regular graphs, Bull. Amer. Math. Soc., 56 (1950), 413–455.
5. W. Feit and G. Higman, The nonexistence of certain generalized polygons, J. Algebra, 1 (1964), 114–131.
6. H. van Maldeghem, Generalized polygons, Monographs in Mathematics, 93, Birkhäuser Verlag, Basel (1998), xvi+502 pp.
7. J. Singer, A theorem in finite geometry and some applications to number theory, Trans. Amer. Math. Soc., 43 (1938), 377-385.
8. Pak-ken Wong, Cages — A Survey, J. Graph Theory, 6 (1982), 1–22.