2013

Toroidal Queens Graphs Over Finite Fields

William D. Weakley
Indiana-Purdue University at Fort Wayne, weakley@ipfw.edu

AUSTRALASIAN JOURNAL OF COMBINATORICS
Volume **57** (2013), Pages 21–38

Toroidal queens graphs over finite fields

William D. Weakley

Department of Mathematical Sciences
Indiana University — Purdue University
Fort Wayne, IN 46805
U.S.A.
weakley@ipfw.edu

Abstract

For each positive integer n, the toroidal queens graph may be described as a graph with vertex set $\mathbb{Z}_n \times \mathbb{Z}_n$ where every vertex is adjacent to those vertices in the directions $(1,0),(0,1),(1,1),(1,-1)$ from it. We here extend this idea, examining graphs with vertex set $F \times F$, where F is a finite field, and any four directions are used to define adjacency. The automorphism groups and isomorphism classes of such graphs are found.

1 Introduction

For each positive integer n, the *toroidal queens graph* Q_n^t may be defined as the graph whose vertices are the squares of an $n \times n$ chessboard covering the surface of a torus; two squares are adjacent if a chess queen can move from one to the other. (A precise definition is given below.)

This family of graphs has been widely studied. The sizes of minimum dominating sets were found in [2, 3, 7]. Determining the number of maximum independent sets (solutions of the "n-queens problem" on the torus) is an old and difficult problem, studied in [2, 5, 8]. The "regular" maximum independent sets (those generated by a repeated step) were classified in [1, 9].

We consider here a generalization of the toroidal queens graph.

Definitions. Let R be a finite commutative ring with multiplicative identity 1 and set $V_R = R \times R$.

Say that $(c,d) \in V_R$ is a *direction generator* of V_R if $|R| = |\{r(c,d) : r \in R\}|$. It is easily seen that (c,d) is a direction generator if and only if $\mathrm{ann}_R(c) \cap \mathrm{ann}_R(d) = \{0\}$, and that this condition is satisfied if $Rc + Rd = R$.

For each direction generator (c,d), let $[c,d] = \{r(c,d) : r \in R, r \neq 0\}$. Say $[c,d]$ is a *direction* in V_R, and let D_R be the set of directions in V_R.

For any subset D of D_R, let $G(R, D)$ be the graph with vertex set V_R and edge set $E_D = \{(x, y)(x + e, y + f) : (x, y) \in V_R, (e, f) \in [c, d] \in D\}$.

For each positive integer n, let $\mathbb{Z}_n$ denote the ring of integers modulo n.

Examples. (1) For each positive integer n and $D = \{[1, 0], [0, 1]\}$, $G(\mathbb{Z}_n, D)$ is the *rook's graph* R_n. More commonly, R_n is defined by saying its vertices are the squares of an $n \times n$ chessboard, and two squares are adjacent if a rook can move from one to the other. It does not matter here whether the board is considered to be on a torus or in the plane.

(2) For each positive integer n and $D = \{[1, 0], [0, 1], [1, 1], [1, -1]\}$, $G(\mathbb{Z}_n, D) = Q_n^t$.

(3) Taking R to be a finite field F, the set D_F can be seen as the underlying set of the projective line $P^1(F)$; also as the set of one-dimensional subspaces of V_F, with the zero element removed from each subspace.

Definitions. For any (x, y) in V_R and $[c, d] \in D_R$, (x, y) together with all $(x+h, y+k)$ such that $(h, k) \in [c, d]$ will be called the *line through* (x, y) *with direction* $[c, d]$.

Two vertices of the line are said to be *adjacent along* $[c, d]$. Distinct lines with the same direction are *parallel*. It is easily seen that for each direction $[c, d]$, the set of all lines of $G(R, D)$ with direction $[c, d]$ is a partition of V_R, which we call the *line family* of $[c, d]$ in $G(R, D)$.

In Example 2 above, we see that adjacency in Q_n^t is defined in terms of four directions. We will study graphs $G(R, D)$ where $|D| = 4$ and the ring R is a field. The restriction to fields has two consequences. First, as we will show in Lemma 1, lines of $G(R, D)$ with different directions always intersect if and only if R is a field. Second, any graph $G(R, D)$ with $|D| = 4$ is isomorphic to a graph $G(a)$ of a standard form (defined later).

The main result of the paper, Theorem 5, enables us to characterize line-preserving isomorphisms between graphs of form $G(a)$. Using the characterization, we are able to determine (Theorem 8) the size and some of the structure of the group $\mathrm{Aut}_\ell(G(a))$ of line-preserving automorphisms of $G(a)$.

We then examine (Lemma 9 – Proposition 12) isomorphisms between graphs of form $G(a)$ that do not preserve lines, finding that these only occur in a few cases. This allows us to describe (Theorem 13) the full automorphism group of each graph $G(a)$, and thus of any $G(F, D)$ with $|D| = 4$. Finally, Theorem 5 and Proposition 12 allow us to determine (Theorem 14) the isomorphism classes of these graphs, and count them (Theorem 15).

We will write $[a_{11}, a_{12}; a_{21}, a_{22}]$ for the 2×2 matrix with entry a_{ij} in row i and column j. The identity matrix will be denoted I.

Lemma 1 *Let R be a finite commutative ring. Then R is a field if and only if any two lines in V_R with different directions meet; in this case, the intersection vertex is*

unique.

Proof. Suppose that R is a field. We need to show that for distinct directions $[c_1, d_1]$ and $[c_2, d_2]$ in V_R and any (x_1, y_1) and (x_2, y_2) in V_R, there are $s_1, s_2 \in R$ such that $(x_1, y_1) + s_2(c_1, d_1) = (x_2, y_2) + s_1(c_2, d_2)$. Solving for s_1 and s_2 gives $d_i(x_1 - x_2) - c_i(y_1 - y_2) = s_i \cdot \det[c_1, d_1; c_2, d_2]$ for $i = 1, 2$. Since $[c_1, d_1] \neq [c_2, d_2]$, $\det[c_1, d_1; c_2, d_2] \neq 0$, so there do exist such s_1, s_2 in R, and they are unique.

Conversely, suppose that any two lines in V_R with different directions intersect and let z be any nonzero member of R. Then $[1, 0]$ and $[1, z]$ are different directions, so $(0, 0) + s_2(1, z) = (0, 1) + s_1(1, 0)$ for some s_1, s_2 in R, which implies $s_2 z = 1$. Thus every nonzero element of R has a multiplicative inverse, and R is a field. ■

From here on, we require the ring R to be a finite field.

Definitions and notation. It is well known that for any prime number p and positive integer m, there is a field of order $n = p^m$, unique up to isomorphism. We write F_n for this field. We have $F_p \cong \mathbb{Z}_p$; the prime subfield of F_n is isomorphic to $\mathbb{Z}_p$, and as there is only one nonzero ring homomorphism from $\mathbb{Z}_p$ into F_n, we will identify the prime subfield of F_n with $\mathbb{Z}_p$.

2 Line-preserving isomorphisms

Definitions. For $D, D' \subseteq D_F$, a graph isomorphism $\theta : G(F, D) \to G(F, D')$ *preserves lines* if for every line ℓ of $G(F, D)$, $\theta(\ell)$ is a line of $G(F, D')$.

Say that θ *preserves line families* if for every $[c, d] \in D$ there is $[e, f] \in D'$ such that for every line ℓ of $G(F, D)$ with direction $[c, d]$, $\theta(\ell)$ is a line of $G(F, D')$ with direction $[e, f]$.

In this case we write $\theta([c, d]) = [e, f]$, using θ to denote the induced bijection from D to D'.

Lemma 2 *Let F be a finite field, $D, D' \subseteq D_F$, and suppose $\theta : G(F, D) \to G(F, D')$ is a graph isomorphism. If θ preserves lines then θ preserves line families.*

Proof. Let ℓ_1, ℓ_2 be parallel lines of $G(F, D_1)$. Since ℓ_1 and ℓ_2 do not meet and θ is one-to-one, $\theta(\ell_1)$ and $\theta(\ell_2)$ are lines of $G(F, D_2)$ that do not meet. Then Lemma 1 implies that $\theta(\ell_1)$ and $\theta(\ell_2)$ are parallel. ■

Definitions. Let F be a finite field. For any subset D of D_F, let $\mathrm{Aut}(F, D)$ denote the group of graph automorphisms of $G(F, D)$. Let $\mathrm{Aut}_\ell(F, D)$ denote the subgroup of $\mathrm{Aut}(F, D)$ consisting of all line-preserving automorphisms.

We now describe some automorphisms and isomorphisms involving these graphs.

For any $(e,f) \in V_F$, we may define a permutation $\tau_{(e,f)}$ of V_F by $\tau_{(e,f)}(x,y) = (x+e, y+f)$ for all $(x,y) \in V_F$. For any $D \subseteq D_F$, $\tau_{(e,f)}$ sends every line family of $G(F,D)$ to itself, so $\tau_{(e,f)}$ is a line-preserving automorphism of $G(F,D)$. Let $T_F = \{\tau_{(e,f)} : (e,f) \in V_F\}$, the *translation subgroup* of $\mathrm{Aut}(F,D)$. It is easily seen that T_F is isomorphic to the additive group of $F \times F$, and that the graph $G(F,D)$ is vertex-transitive.

For any matrix $M = [a_{11}, a_{12}; a_{21}, a_{22}]$ in the general linear group $\mathrm{GL}_2(F)$, we can define a permutation μ_M of V_F using left multiplication by M. That is, for $(x,y) \in V_F$ we set $\mu_M(x,y) = (a_{11}x + a_{12}y, a_{21}x + a_{22}y)$. Also, μ_M induces a permutation of D_F, and it is easy to verify that if $[c,d] \in D_F$, then for each vertex $(x,y) \in V_F$, the function μ_M takes the line through (x,y) with direction $[c,d]$ to the line through the vertex $\mu_M(x,y)$ with direction $[\mu_M(c,d)]$. Thus for $D \subseteq D_F$, if we let $\mu_M(D) = \{[\mu_M(c,d)] : [c,d] \in D\}$, then μ_M is a graph isomorphism from $G(F,D)$ to $G(F,\mu_M(D))$. Let $\mathcal{M}(D) = \{\mu_M : \mu_M(D) = D\}$. Then $\mathcal{M}(D)$ is a subgroup of $\mathrm{Aut}_\ell(F,D)$.

Definitions. For a finite field F, let $F' = F \setminus \{0,1\}$. For $a \in F'$, let $D(a)$ denote $\{[1,0],[0,1],[1,1],[1,a]\}$. We will write $G(a)$ for $G(F,D(a))$ when it is not important what field F is involved.

It is well-known [6, Theorem 2.2] that the action of $\mathrm{GL}_2(F)$ on D_F is sharply 3-transitive. That is, given distinct $[c_1,d_1],[c_2,d_2],[c_3,d_3]$ and distinct $[e_1,f_1],[e_2,f_2]$, $[e_3,f_3]$ in D_F, there is $M \in \mathrm{GL}_2(F)$, unique up to scalar multiple, such that $\mu_M([c_i,d_i]) = [e_i,f_i]$ for $i = 1,2,3$. Thus for any $D \subseteq D_F$ with $|D| = 4$, there is $a \in F'$ with $G(F,D) \cong G(a)$. For this reason we will now examine isomorphisms involving the graphs $G(a)$.

We are going to show (Theorem 14) that the graph $G(a)$ is isomorphic to the graph $G(b)$ if and only if $\alpha(a) = b$ for some α in the group $\Gamma(F)$ defined below.

Definitions. For any nonempty set S, let $\mathrm{Sym}(S)$ denote the group of permutations of S. If $S = \{1,\dots,n\}$ for some positive integer n, we will write $\mathcal{S}_n$ for $\mathrm{Sym}(S)$.

For a finite field F of characteristic p, $|F| > 2$, define $\alpha_1, \alpha_2 \in \mathrm{Sym}(F')$ by $\alpha_1(x) = 1 - x$ and $\alpha_2(x) = 1/x$ for all $x \in F'$. Define $\alpha_3 \in \mathrm{Sym}(F)$ by $\alpha_3(x) = x^p$. Then α_3 is the *Frobenius automorphism* of F, which will be quite important here. Note that the restriction of α_3 to F' is in $\mathrm{Sym}(F')$.

Given elements $\gamma_1,\dots,\gamma_k$ of a group Γ, we write $\langle \gamma_1,\dots,\gamma_k\rangle$ for the subgroup of Γ they generate. The identity element of a group will be denoted ι.

Let $\Gamma(F)$ be the subgroup $\langle \alpha_1, \alpha_2, \alpha_3\rangle$ of $\mathrm{Sym}(F')$. For $a,b \in F'$, we write $a \approx b$ if $\alpha(a) = b$ for some $\alpha \in \Gamma(F)$. If $a \approx b$ then a and b generate the same subfield of F; the converse is not true.

Lemma 3 *Let p be a prime, let m be a positive integer such that $p^m > 4$, and let $F = F_{p^m}$. Then $\langle \alpha_1, \alpha_2\rangle \cong \mathcal{S}_3$ and $\Gamma(F) \cong \mathcal{S}_3 \times \mathbb{Z}_m$. Thus for each $\alpha \in \Gamma(F)$ there are a unique integer j_α, $0 \le j_\alpha < m$, and a unique $\phi_\alpha \in \langle \alpha_1, \alpha_2\rangle$ such that*

$\alpha = \phi_\alpha \alpha_3^{j_\alpha} = \alpha_3^{j_\alpha} \phi_\alpha$.

Proof. For any finite field F with $|F| > 2$, there is a group homomorphism δ from $\mathcal{S}_3$ onto $\langle \alpha_1, \alpha_2 \rangle$ satisfying $\delta((1,2)) = \alpha_1$ and $\delta((1,3)) = \alpha_2$. It is easily checked that $\ker \delta = \mathcal{S}_3$ if and only if $F = F_3$ and $\ker \delta$ is the alternating group $\mathcal{A}_3$ if and only if $F = F_4$. Thus if $|F| = p^m > 4$, then $\langle \alpha_1, \alpha_2 \rangle \cong \mathcal{S}_3$.

Now assume $|F| > 4$. As no polynomial of degree less than $p^m - 2$ annihilates F', $\langle \alpha_1, \alpha_2 \rangle \cap \langle \alpha_3 \rangle = \{\iota\}$, and since α_3 commutes with α_1 and α_2, we have $\Gamma(F) \cong \mathcal{S}_3 \times \mathbb{Z}_m$, and the remaining claim follows. ■

In Theorem 5 we will consider the possibilities for a line-preserving isomorphism θ from $G(a)$ to $G(b)$ that fixes $(0,0)$ and the line family $[0,1]$. Such a θ will send the remaining line families $[1,0], [1,1], [1,a]$ of $G(a)$ to the line families $[1,0], [1,1], [1,b]$ of $G(b)$. This will be described by a bijection $\sigma : \{0,1,a\} \to \{0,1,b\}$; say that θ sends the line family $[1,d]$ to the line family $[1,\sigma(d)]$ for $d \in \{0,1,a\}$. The following lemma gives the values of σ possible for a given a and $b = \alpha(a)$.

For any $x \in F'$, the *stabilizer* in $\langle \alpha_1, \alpha_2 \rangle$ of x is $\mathrm{Stab}_{1,2}(x) = \{\beta \in \langle \alpha_1, \alpha_2 \rangle : \beta(x) = x\}$.

Definition and Lemma 4 *Let p be a prime, let m a positive integer such that $p^m > 4$, and let $F = F_{p^m}$. For each $\alpha \in \Gamma(F)$ and each $a \in F'$, say that a bijection $\sigma : \{0,1,a\} \to \{0,1,\alpha(a)\}$ is an* associate *of the pair (α, a) if*

$$\alpha_3^{j_\alpha}(a) = \frac{\sigma(a) - \sigma(0)}{\sigma(1) - \sigma(0)}. \tag{1}$$

The pair (α, a) has $|Stab_{1,2}(a)|$ associates.

Proof. Set $b = \alpha(a)$, so the left side of (1) is $\phi_\alpha^{-1}(b)$. As σ ranges over the bijections from $\{0,1,a\}$ to $\{0,1,b = \alpha(a)\}$, the right side of (1) ranges over $\{\gamma(b) : \gamma \in \langle \alpha_1, \alpha_2 \rangle\} = \{\gamma^{-1}(b) : \gamma \in \langle \alpha_1, \alpha_2 \rangle\}$. Thus there will be values of σ giving $\phi_\alpha^{-1}(b)$ for the right side of (1), and each of these is an associate of (α, a). This will occur $|\mathrm{Stab}_{1,2}(b)|$ times, and from $\alpha_3^{j_\alpha} \phi_\alpha(a) = b$ and the fact that α_3 commutes with members of $\langle \alpha_1, \alpha_2 \rangle$, it follows that $|\mathrm{Stab}_{1,2}(b)| = |\mathrm{Stab}_{1,2}(a)|$. ■

The following theorem is the main part of our characterization of isomorphisms that preserve lines.

Theorem 5 *Let p be a prime and m a positive integer such that $p^m > 4$. Set $F = F_{p^m}$, let $a \in F'$, let k be the dimension of $\mathbb{Z}_p(a)$ as a $\mathbb{Z}_p$-vector space, and let $L_a(F)$ denote the group of $\mathbb{Z}_p(a)$-vector space automorphisms of F.*

For any $b \in F'$ such that $a \approx b$, there exists $\alpha \in \Gamma(F)$ with $\alpha(a) = b$. For any such α and any $\psi \in L_a(F)$, define $\omega \in Sym(F)$ by

$$\omega = \alpha_3^{j_\alpha} \circ \psi. \tag{2}$$

Then for any associate σ of (α, a), the mapping $\theta : V_F \to V_F$ defined by

$$\theta(x, y) = (\omega(x), \sigma(0)\omega(x) + [\sigma(1) - \sigma(0)]\omega(y)) \tag{3}$$

is a graph isomorphism from $G(a)$ to $G(b)$ that preserves lines and satisfies

$$\theta(0, 0) = (0, 0) \text{ and } \theta([0, 1]) = [0, 1], \text{ and} \tag{4}$$
$$\theta([1, d]) = [1, \sigma(d)] \text{ for } d \in \{0, 1, a\}. \tag{5}$$

Conversely, for any $b \in F'$, if there exists a graph isomorphism θ from $G(a)$ to $G(b)$ that preserves lines and satisfies (4), then $a \approx b$, and there exist $\psi \in L_a(F)$, $\alpha \in \Gamma(F)$ with $\alpha(a) = b$, and an associate σ of (α, a) such that with $\omega \in Sym(F)$ defined by (2), θ is given by (3) and satisfies (5).

Proof. Assume that F is a finite field of characteristic p, $|F| > 4$, and $a, b \in F'$ with $a \approx b$, so there exists $\alpha \in \Gamma_F$ such that $\alpha(a) = b$. Let ψ be any $\mathbb{Z}_p(a)$-vector space automorphism of F, let σ be an associate of (α, a), and define ω by (2) and θ by (3). It follows from (2) and the hypothesis on ψ that

$$\omega(c + e) = \omega(c) + \omega(e) \text{ for } c, e \in F. \tag{6}$$

This and the $\mathbb{Z}_p(a)$-linearity of ψ imply for $(x, y) \in V_F$, $s \in F$, and $(u, v) \in V_{\mathbb{Z}_p(a)}$ that

$$\theta((x, y) + s(u, v)) = \theta(x, y) + (\omega(s)/\omega(1))\theta(u, v). \tag{7}$$

The definition of ω implies $\omega(0) = 0$, and then (3) gives

$$\theta(1, d) = \omega(1)(1, \sigma(d)) \text{ for } d = 0, 1. \tag{8}$$

From (3) we have $\theta(1, a) = \omega(1)(1, \sigma(0) + [\sigma(1) - \sigma(0)](\omega(a)/\omega(1)))$. Since α_3 is a field automorphism of F and ψ is $\mathbb{Z}_p(a)$-linear, (2) implies $\omega(a)/\omega(1) = \alpha_3^{j_\alpha}(\psi(a)/\psi(1)) = \alpha_3^{j_\alpha}(a)$, which equals $(\sigma(a) - \sigma(0))/(\sigma(1) - \sigma(0))$ by (1). Thus

$$\theta(1, a) = \omega(1)\left(1, \sigma(0) + [\sigma(1) - \sigma(0)]\phi_\alpha^{-1}(b)\right) = \omega(1)(1, \sigma(a)). \tag{9}$$

Combining (7), (8), and (9), we have

$$\theta((x, y) + s(1, d)) = \theta(x, y) + \omega(s)(1, \sigma(d)) \text{ for } (x, y) \in V_F, s \in F, d \in \{0, 1, a\}. \tag{10}$$

Similarly,

$$\theta((x, y) + s(0, 1)) = \theta(x, y) + \omega(s)[\sigma(1) - \sigma(0)](0, 1) \text{ for } s \in F \text{ and } (x, y) \in V_F. \tag{11}$$

Together, (10) and (11) imply that θ sends adjacent vertices of $G(a)$ to adjacent vertices of $G(b)$. As $\omega(0) = 0$, we have $\theta(0, 0) = (0, 0)$ by (3). Then (11) implies that every vertex of $G(b)$ that is adjacent to $(0, 0)$ along $[0, 1]$ is in $\theta(V_F)$, and (10) implies that for each of those vertices, every vertex adjacent to it along $[1, \sigma(0)]$ is in $\theta(V_F)$. Thus θ is onto V_F, which implies that θ is one-to-one and that θ sends

non-adjacent vertices of $G(a)$ to non-adjacent vertices of $G(b)$. Therefore θ is a graph isomorphism. As we have shown θ satisfies (4) and (5), the first part of the theorem is proved.

Assume now that $b \in F'$ and there is a line-preserving isomorphism $\theta : G(a) \to G(b)$ that satisfies (4). Then there are $\omega \in \mathrm{Sym}(F)$ and a function $\beta : V_F \to F$ such that $\theta(x, y) = (\omega(x), \beta(x, y))$ for $(x, y) \in V_F$.

As θ preserves lines, by Lemma 2 it also preserves line families, so we may define a bijection $\sigma : \{0, 1, a\} \to \{0, 1, b\}$ corresponding to the action of θ on line families other than $[0, 1]$ of $G(a)$. That is, for each $d \in \{0, 1, a\}$, θ sends the line family $[1, d]$ of $G(a)$ to the line family $[1, \sigma(d)]$ of $G(b)$.

Let $z \in F$. Since $(az, 0)$ and $(0, -az)$ are adjacent along $[1, 1]$ or equal, $\theta(az, 0) = \theta(0, -az) + s_z(1, \sigma(1))$ for some $s_z \in F$. As $\theta(0, 0) = (0, 0)$ and thus $\omega(0) = 0$, we have $s_z = \omega(az)$ and then

$$\beta(az, 0) = \beta(0, -az) + \sigma(1)\omega(az) \text{ for } z \in F. \tag{12}$$

Similarly using the fact that $(z, 0)$ and $(0, -az)$ are adjacent along $[1, a]$ or equal, we get

$$\beta(z, 0) = \beta(0, -az) + \sigma(a)\omega(z). \tag{13}$$

Then since each of $(az, 0)$ and $(z, 0)$ are equal to or adjacent along $[1, 0]$ with the vertex $(0, 0)$, which is fixed by θ,

$$\beta(az, 0) = \sigma(0)\omega(az) \text{ and } \beta(z, 0) = \sigma(0)\omega(z). \tag{14}$$

Together (12), (13), and (14) imply

$$\omega(az) = \frac{\sigma(a) - \sigma(0)}{\sigma(1) - \sigma(0)}\omega(z) \text{ for } z \in F. \tag{15}$$

Define $\gamma \in \mathrm{Sym}(F)$ by $\gamma(z) = \omega(z)/\omega(1)$ for $z \in F$. Then (15) with $z = 1$ implies $\gamma(a) = (\sigma(a) - \sigma(0))/(\sigma(1) - \sigma(0))$ and

$$\gamma(az) = \gamma(a)\gamma(z) \text{ for } z \in F. \tag{16}$$

For each $d \in \{0, 1, a\}$ and each $z \in F$, $(0, 0)$ and (z, dz) are adjacent along $[1, d]$ or equal, so $(\omega(z), \beta(z, dz)) = \theta(z, dz) = r_z(1, \sigma(d))$ for some $r_z \in F$, implying $r_z = \omega(z)$ and thus

$$\beta(z, dz) = \sigma(d)\omega(z) \text{ for each } d \in \{0, 1, a\} \text{ and } z \in F. \tag{17}$$

For $c, e \in F$, consider the vertices $(0, 0), (c, ac), (e, e), (c + e, ac + e)$ of $G(a)$. From (17) we have $\theta(c, ac) = (\omega(c), \sigma(a)\omega(c))$ and $\theta(e, e) = (\omega(e), \sigma(1)\omega(e))$. Then since (c, ac) and $(c + e, ac + e)$ are adjacent along $[1, 1]$ or equal,

$$\theta(c + e, ac + e) = (\omega(c), \sigma(a)\omega(c)) + s_{c,e}(1, \sigma(1)) \text{ for some } s_{c,e} \in F. \tag{18}$$

Similarly using the fact that (e,e) and $(c+e,ac+e)$ are adjacent along $[1,a]$ or equal,

$$\theta(c+e,ac+e) = (\omega(e),\sigma(1)\omega(e)) + t_{c,e}(1,\sigma(a)) \text{ for some } t_{c,e} \in F. \tag{19}$$

Solving equations (18) and (19) together gives $s_{c,e} = \omega(e)$ and $t_{c,e} = \omega(c)$. This implies (6) and (using (17))

$$\beta(c+e,ac+e) = \sigma(a)\omega(c) + \sigma(1)\omega(e) = \beta(c,ac) + \beta(e,e) \text{ for } c,e \in F. \tag{20}$$

From the definition of γ we see $\gamma(1) = 1$ and from (6) we have

$$\gamma(c+e) = \gamma(c) + \gamma(e) \text{ for } c,e \in F. \tag{21}$$

Then an induction shows $\gamma(r) = r$ for $r \in \mathbb{Z}_p$. Another induction using (16) shows that $\gamma(ra^i) = r(\gamma(a))^i$ for $r \in \mathbb{Z}_p$ and nonnegative integers i. Since every element of the extension field $\mathbb{Z}_p(a)$ has the form $\sum r_i a^i$ for some r_i's in $\mathbb{Z}_p$, (16) and (21) imply

$$\gamma(ce) = \gamma(c)\gamma(e) \text{ for } c \in F \text{ and } e \in \mathbb{Z}_p(a). \tag{22}$$

Then (21) and (22) imply that the restriction γ' of γ to the subfield $\mathbb{Z}_p(a)$ of F is a field isomorphism from $\mathbb{Z}_p(a)$ to $\gamma(\mathbb{Z}_p(a))$. We now need some facts from the theory of finite fields, which we take from Proposition 15 of [4, Chapter 14]. First, distinct subfields of a finite field are not isomorphic, so $\gamma(\mathbb{Z}_p(a)) = \mathbb{Z}_p(a)$ and γ' is a field automorphism. Second, every field automorphism of $\mathbb{Z}_p(a)$ is a power of the Frobenius automorphism $x \mapsto x^p$. Therefore there is an integer j such that

$$\alpha_3^j(a) = \gamma(a) = \frac{\sigma(a) - \sigma(0)}{\sigma(1) - \sigma(0)}. \tag{23}$$

Since $\sigma(\{0,1,a\}) = \{0,1,b\}$, the possible values of the right side of (23) are exactly the images of b under members of the subgroup $\langle \alpha_1, \alpha_2 \rangle$ of $\Gamma(F)$. Thus there is $\phi \in \langle \alpha_1, \alpha_2 \rangle$ such that $\alpha_3^j(a) = \phi^{-1}(b)$. Then setting $\alpha = \phi\alpha_3^j \in \Gamma(F)$ we have $\alpha(a) = b$, so $a \approx b$, $j = j_\alpha$, and σ is an associate of (α, a).

Solving the equations $x = c+e$ and $y = ac+e$ for c and e gives $c = (y-x)/(a-1)$ and $e = -(y-ax)/(a-1)$, and then the first equation of (20) gives $\theta(x,y) = (\omega(x), \sigma(a)\omega((y-x)/(a-1)) + \sigma(1)\omega((-(y-ax)/(a-1)))$ for $(x,y) \in V_F$. Using the definition of γ and (22, 23), we see $\omega((y-x)/(a-1)) = \omega(1)\gamma((y-x)/(a-1)) = \omega(1)\gamma(y-x)/\gamma(a-1) = [\omega(1)\gamma(y) - \omega(1)\gamma(x)]/(\gamma(a) - \gamma(1)) = [\omega(y) - \omega(x)]/[(\sigma(a) - \sigma(1))/(\sigma(1) - \sigma(0))]$ and can similarly expand $\omega((-(y-ax)/(a-1)))$, eventually obtaining (3).

Set $\psi = \alpha_3^{-j_\alpha} \circ \omega$. Since ω is in $\mathrm{Sym}(F)$ and preserves addition and α_3 is an automorphism, ψ is in $\mathrm{Sym}(F)$ and preserves addition. For $z \in F$, (15) and (23) imply $\psi(az) = \alpha_3^{-j_\alpha}(\omega(az)) = \alpha_3^{-j_\alpha}(\alpha_3^{j_\alpha}(a)\omega(z)) = a\psi(z)$. Therefore a is in $S_\psi = \{r \in F : \psi(rz) = r\psi(z) \text{ for all } z \in F\}$. Using the fact that ψ preserves addition, it is easy to show that S_ψ is a field and contains $\mathbb{Z}_p$ as well as a, and thus ψ is $\mathbb{Z}_p(a)$-linear. ■

Definitions. For any finite field F, $D \subseteq D_F$, and $\theta \in \mathrm{Aut}_\ell(F, D)$, it follows from Lemma 2 that θ induces a permutation of D: for each $[c, d] \in D$, there is $[e, f] \in D$ such that θ sends every line with direction $[c, d]$ to a line with direction $[e, f]$. We may define a group homomorphism $\Phi_D : \mathrm{Aut}_\ell(F, D) \to \mathrm{Sym}(D)$ by $\Phi_D(\theta)([c, d]) = [e, f]$. When $D = D(a)$, we will write Φ_a rather than $\Phi_{D(a)}$.

Since $|D(a)| = 4$, the group $\mathrm{Sym}(D(a))$ is isomorphic to $\mathcal{S}_4$ and thus has a subgroup isomorphic to the Klein four-group, which will be denoted by K.

Let $a \in F'$. Define matrices M, M' in $\mathrm{GL}_2(F)$ by $M = [0, 1; a, 0]$ and $M' = [1, -1/a; 1, -1]$, and let $\mathcal{M}_K(a)$ be the subgroup of $\mathcal{M}(D(a))$ generated by $\mu_M, \mu_{M'}$, and all μ_{cI}, where c is a nonzero element of F.

Lemma 6 *For any finite field F and $a \in F'$, $\Phi_a(\mathcal{M}_K(a)) = K$. Thus $\mathcal{M}_K(a)$ acts transitively on $D(a)$.*

Proof. A short computation shows that $\Phi_a(\mu_M) = ([1, 0], [0, 1])([1, 1], [1, a])$ and $\Phi_a(\mu_{M'}) = ([1, 0], [1, 1])([0, 1], [1, a])$, using cycle notation for permutations in $\mathrm{Sym}(D(a))$. It is then clear that $\Phi_a(\mathcal{M}_K(a)) = K$. ∎

We can now describe all line-preserving isomorphisms among the graphs $G(a)$.

Proposition 7 *Let F be a finite field, $|F| > 4$, and $a, b \in F'$. If there exists a line-preserving isomorphism $\eta : G(a) \to G(b)$ then $a \approx b$ and there exist $\mu_N \in \mathcal{M}_K(b)$, θ as in Theorem 5, and unique $\tau \in T_F$ such that*

$$\eta = \tau \circ \mu_N \circ \theta.$$

Conversely, if $a \approx b$ then there is a line-preserving isomorphism from $G(a)$ to $G(b)$.

Any line-preserving isomorphism from $G(a)$ to $G(b)$ that fixes $(0, 0)$ is $\mathbb{Z}_p(a)$-linear.

Proof. Let $\eta : G(a) \to G(b)$ be a line-preserving isomorphism. For some $(s, t) \in V_F$, $\eta(0, 0) = (s, t)$. Then with $\tau = \tau_{(-s,-t)} \in T_F$, $\tau^{-1} \circ \eta$ fixes $(0, 0)$, and sends line family $[0, 1]$ of $G(a)$ to some line family $[c, d]$ of $G(b)$. By Lemma 6, there is $\mu_N \in \mathcal{M}_K(b)$ taking line family $[0, 1]$ of $G(b)$ to line family $[c, d]$ of $G(b)$. Now $\mu_N^{-1} \circ \tau^{-1} \circ \eta$ is a line-preserving isomorphism from $G(a)$ to $G(b)$ that fixes $(0, 0)$ and sends line family $[0, 1]$ of $G(a)$ to line family $[0, 1]$ of $G(b)$, so by the converse part of Theorem 5 the desired θ exists and $a \approx b$.

The converse is immediate from Theorem 5.

For the last statement, note that if η fixes $(0, 0)$ then from the first part of this theorem $\eta = \mu_N \circ \theta$. Here μ_N is F-linear from its definition, and the proof of Theorem 5 shows θ to be $\mathbb{Z}_p(a)$-linear, so η is $\mathbb{Z}_p(a)$-linear. ∎

We now look at the structure of $\mathrm{Aut}_\ell(G(a))$. We need to define some subgroups.

Definitions. For $a \in F'$, let $H(a) = \{\eta \in \mathrm{Aut}_\ell(G(a)) : \eta(0,0) = (0,0)\}$.

For any $\mathbb{Z}_p(a)$-vector space automorphism ψ of F, define $\theta_\psi : V_F \to V_F$ by $\theta_\psi(x,y) = (\psi(x), \psi(y))$. Taking $\alpha = \iota$ and $\sigma = \iota$ in Theorem 5 and its proof, we see that θ_ψ is a graph automorphism of $G(a)$ that sends each line family in $D(a)$ to itself. Let Ψ_a denote the subgroup of $\mathrm{Aut}_\ell(G(a))$ consisting of all the θ_ψ.

Theorem 8 *Let F be a finite field, $|F| = p^m > 4$, and $a \in F'$, with $|\mathbb{Z}_p(a)| = p^k$. Then $Aut_\ell(G(a))$ is the semidirect product of its subgroups T_F and $H(a)$.*

The image of $H(a)$ under Φ_a is a subgroup of Sym$(D(a))$ that contains K, so $|\Phi_a(H(a))| \in \{4, 8, 12, 24\}$, and

$$|Aut_\ell(G(a))| = p^{2m} \cdot (p^m - 1)(p^m - p^k) \cdots (p^m - p^{m-k}) \cdot |\Phi_a(H(a))|.$$

Proof. As $\tau_{(0,0)} = \iota$ is the only translation that fixes $(0,0)$, we have $T_F \cap H(a) = \{\iota\}$; Proposition 7 implies that $T_F \cdot H(a) = \mathrm{Aut}_\ell(G(a))$ and that any $\eta \in H(a)$ is additive, giving $\eta\tau_{(s,t)}\eta^{-1} = \tau_{\eta(s,t)}$ for all $\tau_{(s,t)} \in T_F$. So T_F is normal in $\mathrm{Aut}_\ell(G(a))$, which is thus a semidirect product as claimed.

As $\mathcal{M}_K(a) \subseteq H(a)$, Lemma 6 implies $\Phi_a(H(a))$ is a subgroup of $\mathrm{Sym}(D(a))$ that contains K. Since $\mathrm{Sym}(D(a)) \cong \mathcal{S}_4$, we have $|\Phi_a(H(a))| \in \{4, 8, 12, 24\}$.

We claim that $\ker(\Phi_a) \cap H(a) = \Psi_a$. It is easy to see that both $\ker(\Phi_a)$ and $H(a)$ contain Ψ_a. Suppose $\eta \in \ker(\Phi_a) \cap H(a)$. Then $\eta([0,1]) = [0,1]$, so we may use Theorem 5: there are $\alpha \in \mathrm{Sym}(F')$, $\psi \in L_a(F)$, and and an associate σ of (α, a) such that the corresponding θ of Theorem 5 equals η. Since $\theta \in \ker(\Phi_a)$, we have $\sigma = \iota$ so $\theta(x,y) = (\omega(x), \omega(y))$ with $\omega = \alpha_3^{j_\alpha} \circ \psi$, and by (1), $\alpha_3^{j_\alpha}(a) = a$, implying that $\alpha_3^{j_\alpha}$ and thus also ω are $\mathbb{Z}_p(a)$-linear. Therefore $\omega \in L_a(F)$ and $\eta = \theta \in \Psi_a$, establishing the claim.

Finally, applying the fundamental homomorphism theorem to the restriction of Φ_a to $H(a)$, we have $|H(a)| = |\Psi_a| \cdot |\Phi_a(H(a))|$. Since $T_F \cong F \times F$ and Ψ_a is isomorphic to the general linear group $\mathrm{GL}_{m/k}(\mathbb{Z}_p(a))$, the conclusion follows. ∎

Remark. It was shown in [9] that for $n \geq 6$, $\mathrm{Aut}(Q_n^t)$ is $\mathrm{Aut}_\ell(Q_n^t)$ and has size $4n^2\phi(n)$ if n is even, $8n^2\phi(n)$ if n is odd (where ϕ denotes the Euler function). When $n = p^m \geq 6$ is a prime power, it is interesting to compare $\mathrm{Aut}(Q_n^t)$ with $\mathrm{Aut}_\ell(G(a))$. Both are semidirect products of the translation subgroup T_F (of size n^2) with the subgroup of origin-fixing automorphisms, which for Q_n^t will here be denoted H_n.

The restriction of Φ_{-1} to H_n has kernel isomorphic to the group of units of the ring $\mathbb{Z}_n$, and thus of order $\phi(n)$. As just shown, the restriction of Φ_a to $H(a)$ has kernel isomorphic to $\mathrm{GL}_{m/k}(\mathbb{Z}_p(a))$, which has order $(p^m-1)(p^m-p^k)\cdots(p^m-p^{m-k})$.

For even $n \geq 6$, $\Phi_{-1}(H_n) = \langle([1,0],[0,1]),([1,1],[1,-1])\rangle$. For odd $n \geq 7$, $\Phi_{-1}(H_n) = \langle([1,0],[1,1],[0,1],[1,-1]),([1,0],[0,1])\rangle$. Thus $\Phi_{-1}(H_n)$ acts transitively on $D(-1)$ only for odd n.

From Theorem 8, $|\Phi_a(H(a))| \in \{4, 8, 12, 24\}$; in particular, when $a = -1$ and F has characteristic 3, $\Phi_a(H(a))$ can be shown to be isomorphic to $\mathcal{S}_4$, and thus has order 24.

To find the full automorphism group $\mathrm{Aut}(G(a))$, we need to consider the possibilities for automorphisms of $G(a)$ that do not preserve lines. This requires characterization of maximal cliques of $G(a)$.

3 Maximal cliques

The following lemma is easily proved, and is the reason for our investigation of maximal cliques in Propositions 10 and 11.

Lemma 9 *For $i = 1, 2$, let H_i be a finite simple graph with vertex set V_i. A bijective function $\theta : V_1 \to V_2$ is a graph isomorphism from H_1 to H_2 if and only if for every subset S of V_1, S is a maximal clique of H_1 if and only if $\theta(S)$ is a maximal clique of H_2.*

Definition. Let F be a finite field and let $D \subseteq V_F$ with $|D| = 4$. A maximal clique of size four of $G(F, D)$ that does not contain more than two vertices of any line of $G(F, D)$ is a *two-by-two* of $G(F, D)$.

Proposition 10 *Let F be a finite field and let $D \subseteq V_F$ with $|D| = 4$. Then:*

Every maximal clique of $G(F, D)$ that does not contain more than two vertices of any line of $G(F, D)$ is a two-by-two.

The graph $G(F, D)$ has a two-by-two if and only if F has characteristic 2.

If $char(F) = 2$ then $M \subseteq V_F$ is a two-by-two if and only if $M = \{(x_0, y_0), (x_1, y_1), (x_2, y_2), (x_0 + x_1 + x_2, y_0 + y_1 + y_2)\}$, where the vertices $(x_0, y_0), (x_1, y_1), (x_2, y_2) \in V_F$ are not collinear.

Proof. Suppose that M is a maximal m-clique of $G(F, D)$ and no line of $G(F, D)$ contains more than two vertices of M. Since each vertex of M is a member of four lines, we see that $m \leq 5$, and $m = 5$ can occur only if every line of $G(F, D)$ through a vertex of M contains exactly two vertices of M. But then if h is the number of lines with direction $[0, 1]$ that contain vertices of M, we have $2h = 5$, which is not possible. Thus $m \leq 4$.

Since $|F| \geq 2$, we have $m \geq 2$. For distinct $v_1, v_2 \in M$ we can find two directions $[c_i, d_i]$, $i = 1, 2$, in D and different from the direction of the line through v_1 and v_2. For $i = 1, 2$ consider the line through v_i with direction $[c_i, d_i]$. By Lemma 1, these lines meet at a vertex that by the maximality of the clique M must be in M, so $m \geq 3$.

If $m = 3$, the three pairs of points of M determine three different directions in D. Let $[c, d]$ be the fourth direction in D. By Lemma 1, the line through v_1 with direction $[c, d]$ meets the line through the other two points of M in a vertex v, and $M \cup \{v\}$ is a clique properly containing M, a contradiction. Thus $m = 4$, and M is a two-by-two.

Let $(x_0, y_0) \in M$ and define a translation automorphism of $G(F, D)$ by $\tau(x, y) = (x - x_0, y - y_0)$. Then $M' = \tau(M)$ is a two-by-two containing $(0, 0)$; let (x'_1, y'_1), $(x'_2, y'_2), (x'_3, y'_3)$ be the other vertices of M'. Since M' is a maximal clique, the line through any pair of vertices of M' does not intersect the line through the other two vertices of M'. Then Lemma 1 implies these two lines are parallel. Thus $[x'_3 - x'_1, y'_3 - y'_1] = [x'_2, y'_2]$ and $[x'_3 - x'_2, y'_3 - y'_2] = [x'_1, y'_1]$, so there are $s, t \in F$ such that $(x'_3, y'_3) = (x'_1, y'_1) + s(x'_2, y'_2) = (x'_2, y'_2) + t(x'_1, y'_1)$. As no line contains more than two vertices of M', the directions $[x'_1, y'_1]$ and $[x'_2, y'_2]$ are different, so by Lemma 1 the only solution is $s = t = 1$, giving $x'_3 = x'_1 + x'_2$ and $y'_3 = y'_1 + y'_2$.

Then since the line through $(0, 0)$ and (x'_3, y'_3) is parallel to the line through (x'_1, y'_1) and (x'_2, y'_2), we have $0 = \det[x'_1 + x'_2, y'_1 + y'_2; x'_2 - x'_1, y'_2 - y'_1] = 2 \cdot \det[x'_1, y'_1; x'_2, y'_2]$. As $(0, 0), (x'_1, y'_1), (x'_2, y'_2)$ are not collinear, $\det[x'_1, y'_1; x'_2, y'_2] \neq 0$. Thus F has characteristic 2, and $M = \tau^{-1}(M')$ has the form given in the last sentence of this proposition.

Conversely, suppose that $\mathrm{char}(F) = 2$ and $M = \{(x_0, y_0), (x_1, y_1), (x_2, y_2), (x_0 + x_1 + x_2, y_0 + y_1 + y_2)\}$, with the vertices $(x_0, y_0), (x_1, y_1), (x_2, y_2) \in V_F$ not collinear. Then M is a 4-clique and no line contains more than two members of M. We need to show that M is a maximal clique. Suppose that some vertex v is adjacent to all vertices of M.

The pairs of vertices of M determine three of the four directions in D. To simplify notation, let $D = \{d_1, d_2, d_3, d_4\}$, set $M = \{v_1, v_2, v_3, v_4\}$, and for distinct vertices w, z of $G(F, D)$ let wz denote the unique line containing w and z. We may assume that for $i = 2, 3, 4$, the line $v_1 v_i$ has direction d_i. (Then also the line $v_3 v_4$ has direction d_2, the line $v_2 v_4$ has direction d_3, and the line $v_2 v_3$ has direction d_4.)

Since no two v_i's are adjacent along d_1, at most one v_i is adjacent to v along d_1. If there is such a v_i we may assume it is v_1 by renumbering if necessary.

Define a function $\rho : M \to D$ by saying that $\rho(v_i)$ is the direction of the line $v v_i$. Then ρ takes the value d_1 at most once, and if it does, we are assuming that $\rho(v_1) = d_1$.

If $\rho(v_2) = d_2$, then since the line $v_1 v_2$ has direction d_2, also $\rho(v_1) = d_2$, but $\rho(v_3) \neq d_2$ and $\rho(v_4) \neq d_2$ since no line contains more than two vertices of M. Similarly considering the possibilities $\rho(v_2) = d_3$ and $\rho(v_2) = d_4$, we see that ρ takes the value $\rho(v_2)$ exactly twice. The same is true for the values $\rho(v_3)$ and $\rho(v_4)$. Thus the set $\rho^{-1}(d_i)$ has either two members or none for $i = 2, 3, 4$. As $|M| = 4$, parity implies that $\rho(v_1) = d_1$ does not occur, and that ρ takes exactly two values. But this contradicts the fact that disjoint pairs of vertices of M determine parallel lines, so no such vertex v exists. ■

Definition. Let F be a finite field of characteristic 3. Say that $M \subseteq V_F$ is a *three-by-three* of $G(-1)$ if there are $x, y, t \in F$, $t \neq 0$, such that $M = \{(x + rt, y + st) : r, s \in \mathbb{Z}_3\}$.

It is straightforward to verify that a three-by-three is a clique of $G(-1)$.

Proposition 11 *Let F be a finite field, $a \in F'$, and M a maximal clique of $G(a)$*

that is neither a line nor a two-by-two. Then some line of $G(a)$ contains exactly three vertices of M, and just one of the following holds:

(i) $a \notin \{-1, 2, 1/2\}$ and $|M| = 4$;

(ii) char$(F) \neq 3$, $a \in \{-1, 2, 1/2\}$, and $|M| = 5$;

(iii) char$(F) = 3$, $a = -1$, M is a three-by-three, and $|M| = 9$.

Proof. Assume that M is a maximal clique of $G(a)$ that is neither a line nor a two-by-two. Since M is not a two-by-two, Proposition 10 implies that M has at least three vertices in some line ℓ of $G(a)$. As M is a maximal clique but not a line, M contains some vertex v not in ℓ. Since $|D(a)| = 4$, Lemma 1 implies v is adjacent to exactly three vertices in ℓ, so $|M \cap \ell| = 3$.

By Lemma 6, there is an automorphic image M' of M that has three vertices v_1, v_2, v_3 in the line C_0 through $(0, 0)$ with direction $[0, 1]$. Any other vertex v of M' is adjacent to each of v_1, v_2, v_3 along a different one of the directions $[1, 0], [1, 1], [1, a]$, so by applying a vertical translation to M' we obtain M'' containing $(0, 0)$ and $(-t, 0)$ for some $t \in F$, $t \neq 0$. Then M'' also contains the vertices $(0, t)$ and $(0, at)$ where the lines through $(-t, 0)$ with directions $[1, 1]$ and $[1, a]$ meet C_0.

We next investigate what vertices other than $(-t, 0)$ are adjacent to every vertex in $M'' \cap C_0 = \{(0, 0), (0, t), (0, at)\}$, and under what conditions these vertices are adjacent to $(-t, 0)$.

The line through $(0, 0)$ along $[1, 0]$, the line through $(0, at)$ along $[1, 1]$, and the line through $(0, t)$ along $[1, a]$ all meet if and only if $at = t/a$; since $t \neq 0$ and $a \neq 1$, this is true if and only if $a = -1$. In this case the intersection is $(t, 0)$, which is adjacent to $(-t, 0)$ along $[1, 0]$.

The line through $(0, t)$ along $[1, 0]$, the line through $(0, 0)$ along $[1, 1]$, and the line through $(0, at)$ along $[1, a]$ all meet if and only if $a = 1/2$. In this case the intersection is (t, t), which is adjacent to $(-t, 0)$ along $[1, a]$.

The line through $(0, t)$ along $[1, 0]$, the line through $(0, at)$ along $[1, 1]$, and the line through $(0, 0)$ along $[1, a]$ all meet if and only if $a^2 - a + 1 = 0$. In this case the intersection is $((1 - a)t, t)$, which is adjacent to $(-t, 0)$ if and only if $a = 2$.

The line through $(0, at)$ along $[1, 0]$, the line through $(0, 0)$ along $[1, 1]$, and the line through $(0, t)$ along $[1, a]$ all meet if and only if $a^2 - a + 1 = 0$. In this case the intersection is (at, at), which is adjacent to $(-t, 0)$ if and only if $a = -1$.

The line through $(0, at)$ along $[1, 0]$, the line through $(0, t)$ along $[1, 1]$, and the line through $(0, 0)$ along $[1, a]$ all meet if and only if $a = 2$. In this case the intersection is $(t, 2t)$, which is adjacent to $(-t, 0)$ along $[1, 1]$.

We can now complete the proof.

If $a \notin \{-1, 2, 1/2\}$ then the above analysis implies no vertex is adjacent to $(-t, 0)$ and also to every vertex of $M'' \cap C_0$, so $|M| = |M''| = 4$.

If $\text{char}(F) \neq 3$ and $a \in \{-1, 2, 1/2\}$, then exactly one of $a = -1$, $a = 2$, and $a = 1/2$ holds and $a^2 - a + 1 \neq 0$, so $|M| = |M''| = 5$.

Finally, if $\mathrm{char}(F) = 3$ and $a \in \{-1, 2, 1/2\}$, then $a = -1 = 2 = 1/2$ and $a^2 - a + 1 = 0$ so M'' contains nine squares, as does M, and M'' and M are three-by-threes. ■

4 Conclusions

Proposition 12 *Let F_n be a finite field. There is a graph isomorphism $\theta : G(a) \to G(b)$ that does not preserve lines if and only if one of the following conditions holds:*

(i) $n \in \{3, 4, 5\}$ and $a, b \in F_n'$;

(ii) $n = 9$ and $a = b = -1$.

Thus if such an isomorphism exists then there also exists a graph isomorphism from $G(a)$ to $G(b)$ that preserves lines.

Proof. Let F be a finite field. For $F = F_3$, since $|D(a)| = |D(b)| = 4$, necessarily $a = b = -1$, $D(a) = D_F$ and $G(a)$ is the complete graph on nine vertices, so any permutation of V_F is an automorphism of $G(a)$. Thus there are many automorphisms of $G(a)$ that do not preserve lines. For the remainder of the proof, we may assume $|F| \geq 4$.

We next show that for each of $n = 4, 5, 9$, there is $a \in F_n'$ such that $G(a)$ has a graph automorphism that does not preserve lines. For F_5 and $a = -1$ such an automorphism (taken from [9]) is shown in Figure 1 on the right.

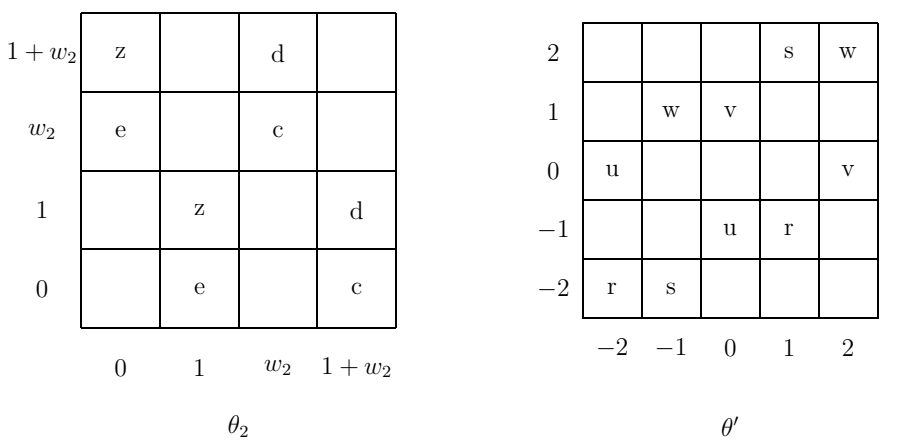

Figure 1: Automorphisms θ_2 of $G(F_4, D(w_2))$ and θ' of $G(F_5, D(-1))$ are shown. In each case, the automorphism fixes blank squares and exchanges squares labelled with the same letter, and does not preserve lines.

For each of $p = 2, 3$, let w_p be an element of F_{p^2} that is not in $\mathbb{Z}_p$. Then $\{1, w_p\}$ is a basis for F_{p^2} as a vector space over $\mathbb{Z}_p$, so each $u \in F_{p^2}$ has a unique expression as a linear combination $u = t_0 + t_1 w_p$ with $t_0, t_1 \in \mathbb{Z}_p$.

For $p = 2$, let $a = w_2$; for $p = 3$, let $a = -1$. Then for $p = 2, 3$, define $\theta_p : G(F_{p^2}, D(a)) \to G(F_{p^2}, D(a))$ by

$$\theta_p(t_0 + t_1 w_p, t_2 + t_3 w_p) = (t_3 + t_1 w_p, t_2 + t_0 w_p) \text{ for all } t_0, t_1, t_2, t_3 \in \mathbb{Z}_p.$$

Clearly θ_p is a bijection and is its own inverse, so if it preserves adjacency then θ_p is a graph automorphism. For $s \in F_{p^2}$, write $s = s_0 + s_1 w_p$ with $s_0, s_1 \in F_p$. Then for $z \in F_p$ and $t_0, t_1, t_2, t_3 \in \mathbb{Z}_p$,

$$\theta_p((t_0 + t_1 w_p, t_2 + t_3 w_p) + (s_0 + s_1 w_p)(1, z)) = \theta_p(t_0 + t_1 w_p, t_2 + t_3 w_p) + (w_p + z)(s_1, s_0) \tag{24}$$

and

$$\theta_p((t_0 + t_1 w_p, t_2 + t_3 w_p) + (s_0 + s_1 w_p)(0, 1) = \theta_p(t_0 + t_1 w_p, t_2 + t_3 w_p) + (s_1, s_0). \tag{25}$$

This implies that θ_3 sends each line of $G(-1) = G(F_9, D(-1))$ to a three-by-three, so θ_3 is an automorphism of $G(-1)$.

Since $w_2^2 = w_2 + 1$, $\theta_2((t_0 + t_1 w_2, t_2 + t_3 w_2) + (s_0 + s_1 w_2)(1, w_2)) = \theta_2(t_0 + t_1 w_2, t_2 + t_3 w_2) + (s_1(w_2 + 1) + s_0)(1, w_2)$. Combined with (24) and (25), this shows that θ_2 sends lines with direction $[1, w_2]$ to lines with direction $[1, w_2]$, and the remaining three-fourths of the lines to two-by-twos. Thus θ_2 is an automorphism of $G(w_2) = G(F_4, D(w_2))$; it is shown on the left in Figure 1.

Now we will show for $n \geq 4$ that if there is a graph isomorphism $\theta : G(F_n, D(a)) \to G(F_n, D(b))$ that does not preserve lines then $n \in \{4, 5, 9\}$. Suppose there is such an isomorphism.

Since $|D(a)| = 4$, Lemma 1 implies that a vertex of $G(a)$ that is not in a particular line is adjacent to exactly three vertices of that line. This and $|F_n| \geq 4$ imply every line of $G(a)$ is a maximal clique. The same is true for $G(b)$. Since $G(a)$ and $G(b)$ each have exactly $4n$ lines, Lemma 9 and the assumption that θ does not preserve lines imply that both $G(a)$ and $G(b)$ have maximal cliques of size m that are not lines. From Propositions 10 and 11 we see this can only occur if $n \in \{4, 5, 9\}$. For F_9, Proposition 11 implies $a = b = -1$, so the last statement of the proposition holds for F_9.

For $n = 4, 5$, there is only one orbit of F_n' under the action of $\Gamma(F_n)$, so Theorem 5 implies the last statement of the proposition for these values of n. Finally, we have shown for $F = F_4$ with $a = w_2$ and for $F = F_5$ with $a = -1$ the existence of automorphisms of $G(F, D(a))$ that do not preserve lines, and since composing such an automorphism with an isomorphism that preserves lines will yield an isomorphism that does not preserve lines, we are done. ■

Remark. The toroidal queens graph $Q_9^t = G(\mathbb{Z}_9, D(-1))$ has three-by-threes, but as shown in the proof of [9, Theorem 9], every automorphism of Q_9^t preserves lines.

Definitions. Let G be a graph without loops or multiple edges. The *complement* of G is the graph $\overline{G}$ having the same vertex set as G, with the property that distinct vertices v, w are adjacent in $\overline{G}$ if and only if v, w are not adjacent in G. It is easily seen that $\mathrm{Aut}(G) = \mathrm{Aut}(\overline{G})$.

We will write $N \rtimes H$ for the semidirect product of the groups N and H.

Theorem 13 *For $n \in \{3, 4, 5\}$ and $a \in F_n'$, we have:*
$Aut(F_3, D(a)) \cong \mathcal{S}_9$,
$Aut(F_4, D(a)) \cong (\mathcal{S}_4)^5$,
$Aut(F_5, D(a)) \cong (\mathcal{S}_5 \times \mathcal{S}_5) \rtimes \mathbb{Z}_2$.

Also $Aut(F_9, D(-1)) \cong Aut_\ell(F_9, D(-1)) \rtimes \mathbb{Z}_2$.

For all other prime powers n and $a \in F_n'$, $Aut(F_n, D(a)) = Aut_\ell(F_n, D(a))$.

Proof. For $G = G(F_3, D(-1))$, $\overline{G}$ is the empty graph on nine vertices, which implies the claim.

The members of F_4' are the roots of $x^2 - x + 1$. With either of these roots as a and $G = G(F_4, D(a))$, we have $\overline{G} \cong G(F_4, \{[0, 1]\})$. This has automorphism group $(\mathcal{S}_4)^5$, since the four lines, and the vertices of each line, may be independently permuted.

For any $a \in F_5'$ we have $a \approx -1$ so it suffices to examine $G = G(F_5, D(-1))$. Its automorphism group was found in [9, Theorem 7]. Here we offer a simpler proof: $\overline{G} = G(F_5, \{[1, 2], [1, 3]\})$ which by the transitivity [6, Theorem 2.2] of the action of $GL_2(F_5)$ on D_{F_5} is isomorphic to $G(F_5, \{[1, 0], [0, 1]\})$, the rook's graph on F_5. This has the claimed automorphism group since the five rows can be permuted in any way, as can the five columns, and there is an automorphism that switches rows and columns.

By Proposition 12 there is an automorphism θ of $G = G(F_9, D(-1))$ that does not preserve lines. By Proposition 11 there is a line ℓ of G such that $\theta(\ell)$ is a three-by-three. Consider the 27 lines $\ell_1, \ldots, \ell_{27}$ of G that are not parallel to ℓ. By Lemma 1, each ℓ_i meets ℓ in exactly one square; if $\theta(\ell_i)$ were a line, it would meet $\theta(\ell)$ in either three squares or none. Thus each $\theta(\ell_i)$ is a three-by-three. Replacing ℓ with ℓ_1, we see by a similar argument that each line in the family of ℓ is sent by θ to a three-by-three. As G has exactly 36 three-by-threes, θ must also send every three-by-three to a line. Thus if θ, θ' are any two automorphisms of G that do not preserve lines, then $\theta \circ \theta'$ does preserve lines, implying that the index of $\mathrm{Aut}_\ell(F_9, D(-1))$ in $\mathrm{Aut}(F_9, D(-1))$ is two.

The final statement of the theorem follows from Proposition 12. ∎

The following summarizes our work on the isomorphism classes of the graphs $G(a)$.

Theorem 14 *Let F be a finite field. Then:*

For any $D \subseteq D_F$ with $|D| = 4$, there is $a \in F'$ such that $G(F, D) \cong G(a)$.

For $a, b \in F'$, $G(a) \cong G(b)$ if and only if $a \approx b$.

Thus the isomorphism classes of graphs $G(F, D)$ with $|D| = 4$ are in one-to-one correspondence with the orbits of F' under the action of $\Gamma(F)$.

Proof. Let $D \subseteq D_F$ with $|D| = 4$. Since $\mathrm{GL}_2(F)$ acts 3-transitively on D_F [6, Theorem 2.2], there are a matrix $M \in \mathrm{GL}_2(F)$ and $a \in F'$ such that $\mu_M(D) = D(a)$. Then μ_M is an isomorphism from $G(F, D)$ to $G(a)$, which establishes the first claim.

Suppose that $\theta_1 : G(a) \to G(b)$ is a graph isomorphism. By Proposition 12 we may assume θ preserves lines, and then $a \approx b$ by Proposition 7.

Conversely, assume $a \approx b$. Then there is $\alpha \in \Gamma(F)$ with $\alpha(a) = b$. With this α, any associate σ of (α, a), and $\psi = \iota$, Theorem 5 gives an isomorphism $\theta : G(a) \to G(b)$. ■

Definition. For each prime power $p^m > 2$, let $\chi(p^m)$ denote the number of isomorphism classes of graphs $G(F, D)$ with F a finite field of order p^m and $|D| = 4$.

Using the Burnside Counting Theorem, it is possible to find the following values of $\chi(p^m)$; the proof is straightforward but lengthy and complicated, so we omit it.

Theorem 15 *For prime $p > 2$, $\chi(p) = \lceil p/6 \rceil$.*

For any prime p:

For $m = 2, 3$, $\chi(p^m) = \lceil (p^m + 2mp - 2)/6m \rceil$; $\chi(p^4) = \lceil (p^4 + 4p^2 + 8p)/24 \rceil$;

For prime $m \geq 5$, $\chi(2^m) = (2^m - 2)/6m$ and for $p > 2$, $\chi(p^m) = (p^m - p)/6m + \lceil p/6 \rceil$.

Acknowledgements

I would like to thank Mohammad Reza Salarian for some helpful conversations.

References

[1] A. B. Burger, E. J. Cockayne and C. M. Mynhardt, Regular solutions of the n-queens problem on the torus, *Util. Math.* **65** (2004), 219–230.

[2] A. B. Burger, C. M. Mynhardt and E. J. Cockayne, Queens graphs for chessboards on the torus, *Australas. J. Combin.* **24** (2001), 231–246.

[3] A. B. Burger, C. M. Mynhardt and W. D. Weakley, The domination number of the toroidal queens graph of size $3k \times 3k$, *Australas. J. Combin.* **28** (2003), 137-148.

[4] D. S. Dummit and R. M. Foote, *Abstract Algebra*, Prentice Hall, Englewood Cliffs, New Jersey, 1991.

[5] M. R. Engelhardt, A group-based search for solutions of the n-queens problem, *Discrete Math.* **307** (2007) no. 21, 2535–2551.

[6] H. Levy, *Projective and Related Geometries*, Macmillan, New York, 1964.

[7] C. M. Mynhardt, Upper bounds for the domination numbers of toroidal queens graphs, *Discuss. Math. Graph Theory* **23** (2003) no. 1, 163–175.

[8] I. Rivin, I. Vardi and P. Zimmerman, The n-queens problem, *Amer. Math. Monthly* **101** (1994) no. 7, 629–639.

[9] W. D. Weakley, The automorphism group of the toroidal queen's graph, *Australas. J. Combin.* **42** (2008), 141–158.

(Received 31 Dec 2011; revised 1 Feb 2013, 14 June 2013)