AUSTRALASIAN JOURNAL OF COMBINATORICS
Volume **42** (2008), Pages 141–158

The automorphism group of the toroidal queen's graph

William D. Weakley

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

Abstract

Denote the $n \times n$ toroidal queen's graph by Q_n^t. We find its automorphism group $\mathrm{Aut}(Q_n^t)$ for each positive integer n, showing that for $n \geq 6$, $\mathrm{Aut}(Q_n^t)$ is generated by the translations, the group of the square, the homotheties, and (for odd n) the automorphism $(x, y) \mapsto (y + x, y - x)$.

For each n we find the automorphism classes of edges of Q_n^t, in particular showing that for $n > 1$, Q_n^t is edge-transitive if and only if n is prime.

We find the number of automorphism classes of regular solutions of the toroidal n-queens problem, generalizing work of Burger, Cockayne, and Mynhardt.

1 Introduction

Consider an $n \times n$ chessboard covering the surface of a torus. We may cut the torus along the ring separating two adjacent columns and along the ring separating two adjacent rows, and draw the resulting square in the plane. Label the columns and the rows from 0 to $n - 1$, starting at the lower left corner, and refer to the square in column x and row y as (x,y). We will follow the standard practice of writing the column and row labels as integers but treating them as members of the set $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ of congruence classes modulo n. We also use $\mathbb{Z}_n$ to denote the group of congruence classes modulo n under addition.

For $k \in \mathbb{Z}_n$, the *difference diagonal* with number k is the set of all squares (x,y) such that $y - x \equiv k \pmod{n}$. The *sum diagonal* with number k is the set of all squares (x,y) such that $y + x \equiv k \pmod{n}$. Thus there are n difference diagonals and n difference diagonals, each containing n squares. The columns and rows are the *orthogonals*, and the orthogonals and diagonals are the *lines* of the board. For each $k \in \mathbb{Z}_n$, let C_k (respectively R_k, D_k, S_k) denote the set of squares in the column (respectively row, difference diagonal, sum diagonal) with number k.

Note that an arbitrary difference diagonal D_m and sum diagonal S_k intersect in a square (x,y) if and only if $y - x \equiv m \pmod{n}$ and $y + x \equiv k \pmod{n}$. This system of congruences has a unique solution if n is odd. If n is even, the system has two solutions if $m \equiv k \pmod{2}$ and none otherwise.

We define the *toroidal queen's graph* Q_n^t to be the graph whose vertices are the n^2 squares of the $n \times n$ toroidal chessboard. Two squares of Q_n^t are adjacent if they share a line of the board; that is, if a queen on one of the squares could move to the other. If n is even, each square (x,y) is adjacent to $(x + (n/2), y + (n/2))$ along both of its diagonals, but we consider this to yield just one edge of Q_n^t. Thus Q_n^t has $4n\binom{n}{2} = 2n^2(n-1)$ edges if n is odd, and $4n\binom{n}{2} - (n^2/2) = n^2(4n-5)/2$ edges if n is even.

An *automorphism* of a graph G is a bijection $\alpha : V(G) \to V(G)$ such that vertices v, w are adjacent if and only if $\alpha(v)$ and $\alpha(w)$ are adjacent. The set of all automorphisms of G is a group under composition; this is the *automorphism group* of G, denoted $\mathrm{Aut}(G)$. We are interested here in finding $\mathrm{Aut}(Q_n^t)$ for each positive integer n.

2 Determining $\mathrm{Aut}(Q_n^t)$

For $n \le 3$, it is easily seen that any two squares of Q_n^t are adjacent, and thus every permutation of the n^2 squares is an automorphism. Therefore $\mathrm{Aut}(Q_n^t)$ is isomorphic to the symmetric group $\mathcal{S}_{n^2}$ for $n \le 3$.

For each n, let ι denote the identity automorphism of Q_n^t.

Define a metric $d : V(Q_n^t) \times V(Q_n^t) \to \{0, 1, \ldots, \lfloor n/2 \rfloor\}$ by

$$d((x_1,y_1),(x_2,y_2)) = \max\{\min\{|x_2 - x_1|, n - |x_2 - x_1|\}, \min\{|y_2 - y_1|, n - |y_2 - y_1|\}\}.$$

We now define and briefly discuss some subgroups and elements of $\mathrm{Aut}(Q_n^t)$.

The translation subgroup T_n. (Order n^2.)

For each $h, k \in \mathbb{Z}_n$ define an automorphism $\tau_{h,k}$ of Q_n^t by $\tau_{h,k}(x,y) = (x+h, y+k)$. These n^2 automorphisms form the subgroup T_n of $\mathrm{Aut}(Q_n^t)$, which is isomorphic to $\mathbb{Z}_n \times \mathbb{Z}_n$.

Thus the graph Q_n^t is *vertex-transitive*; that is, for any two squares s, t of Q_n^t, there is an automorphism γ of Q_n^t such that $\gamma(s) = t$.

The square subgroup I_n. (Order 8, for $n \ge 3$.)

For a square in the plane, there are eight rigid motions of the plane that take the square to itself. We may use these to define a subgroup I_n of $\mathrm{Aut}(Q_n^t)$ that is isomorphic to the dihedral group of order 8 if $n \ge 3$; I_n is generated by the automorphisms β and μ defined by:

$\beta(x,y) = (y,x)$ [reflection across D_0]; $\mu(x,y) = (x,-y)$ [reflection across R_0].

We will write α for $\mu\beta$; α may be regarded as clockwise rotation by a quarter turn about the center of square $(0,0)$.

The homothety subgroup H_n. (Order $\phi(n)$, where ϕ denotes the Euler phi function.)

For each integer m, $1 \le m \le n$, with $\gcd(m,n) = 1$, define an automorphism λ_m of Q_n^t by $\lambda_m(x,y) = (mx, my)$. These $\phi(n)$ automorphisms form the subgroup H_n of $\mathrm{Aut}(Q_n^t)$, which is isomorphic to the group $\mathbb{Z}_n^\times$ of those congruence classes modulo n that have multiplicative inverses, with multiplication as operation.

The exceptional automorphism ρ (for odd n only). We define a mapping ρ from $V(Q_n^t)$ to itself by $\rho(x,y) = (y + x, y - x)$. Since n is odd, ρ is one-to-one and hence onto. As a transformation of the Cartesian plane, the rule of ρ yields a clockwise rotation by $\pi/4$ radians about the origin combined with a dilation by a factor of $\sqrt{2}$. As this would lead one to expect, ρ takes columns to difference diagonals, difference diagonals to rows, rows to sum diagonals, and sum diagonals to columns. Thus ρ is an automorphism of Q_n^t. It is easily checked that $\rho^2 = \lambda_2\alpha$ and $\rho^4 = \lambda_{-4}$.

Definitions and notation. For a finite set S, we write $|S|$ for the size of S.

For subsets A, B of a group G, define $AB = \{ab : a \in A, b \in B\}$.

For subsets or elements $s_1, \ldots, s_k$ of a group, let $\langle s_1, \ldots, s_k \rangle$ be the subgroup generated by $s_1, \ldots, s_k$.

If H is a normal subgroup of G, we write $H \triangleleft G$.

For even $n \ge 4$, let G_n denote the subgroup $\langle T_n, I_n, H_n \rangle$ of $\mathrm{Aut}(Q_n^t)$.

For odd $n \ge 5$, let G_n denote the subgroup $\langle T_n, I_n, H_n, \rho \rangle$ of $\mathrm{Aut}(Q_n^t)$.

To determine the basic structure and size of G_n, we use the following lemma; part (a) follows from Lemma 2.8 of [6] and part (b) is Theorem 2.B of [6].

Lemma 1 *Let G be a group with subgroups H and K.*

(a) If $hKh^{-1} \subseteq K$ for all $h \in H$, then HK is a subgroup of G, and K is a normal subgroup of HK.

(b) If H and K are finite, then $|HK| = |H||K|/|H \cap K|$.

Theorem 2 *For even $n \ge 4$, $T_n \triangleleft I_nT_n \triangleleft H_nI_nT_n = G_n$ and $|G_n| = 4n^2\phi(n)$.*
For odd $n \ge 5$, $T_n \triangleleft I_nT_n \triangleleft H_nI_nT_n \triangleleft \langle\rho\rangle H_nI_nT_n = G_n$ and $|G_n| = 8n^2\phi(n)$.

Proof. Assume $n \ge 4$. First we apply Lemma 1(a) to the subgroups I_n and T_n of G_n. For each $\tau_{h,k}$ in T_n, we have $\mu\tau_{h,k}\mu^{-1} = \tau_{h,-k}$ and $\beta\tau_{h,k}\beta^{-1} = \tau_{k,h}$. Thus I_nT_n is a subgroup of G_n and $T_n \triangleleft I_nT_n$. Each member of I_n fixes $(0,0)$ and in T_n only ι does that, so since $n > 2$, $|I_nT_n| = |I_n||T_n| = 8n^2$ by Lemma 1(b).

Next we apply Lemma 1(a) to H_n and I_nT_n. For each λ_m in H_n and $\tau_{h,k}$ in T_n, we have $\lambda_m\mu\tau_{h,k}\lambda_m^{-1} = \mu\tau_{mh,mk}$ and $\lambda_m\beta\tau_{h,k}\lambda_m^{-1} = \beta\tau_{mh,mk}$. Thus $H_nI_nT_n$ is a subgroup of G_n and $I_nT_n \triangleleft H_nI_nT_n$. It is not difficult to see that any member of I_nT_n preserves the metric d and $\lambda_m \in H_n$ preserves d if and only if $m = 1$ or $m = n-1$, and then that $H_n \cap I_nT_n = \{\iota, \lambda_{n-1}\}$. Thus $|H_nI_nT_n| = 8n^2\phi(n)/2 = 4n^2\phi(n)$ by Lemma 1(b).

If n is even, the definition of G_n implies $G_n = H_nI_nT_n$ and we are done.

If n is odd, apply Lemma 1(a) to $\langle\rho\rangle$ and $H_nI_nT_n$. For each λ_m in H_n and $\tau_{h,k}$ in T_n, we have $\rho\lambda_m\mu\tau_{h,k}\rho^{-1} = \lambda_m\mu\beta\mu\tau_{h+k,k-h}$ and $\rho\lambda_m\beta\tau_{h,k}\rho^{-1} = \lambda_m\mu\tau_{h+k,k-h}$. Thus $\langle\rho\rangle H_nI_nT_n$ is a subgroup of G_n and $H_nI_nT_n \triangleleft \langle\rho\rangle H_nI_nT_n$. Then the definition of G_n implies $G_n = \langle\rho\rangle H_nI_nT_n$.

If $\gamma \in \langle\rho\rangle \cap H_nI_nT_n$ then since all members of $\langle\rho\rangle$, H_n and I_n fix the square $(0,0)$, we have $\gamma \in \langle\rho\rangle \cap H_nI_n$. Since $\rho(0,1) = (1,1)$ and for each η in H_nI_n, $\eta(0,1)$ is in either column 0 or row 0, we see $\rho \notin H_nI_n$. From $\rho^2 = \lambda_2\alpha$ it then follows that $\langle\rho^2\rangle = \langle\rho\rangle \cap H_nI_n = \langle\rho\rangle \cap H_nI_nT_n$, so $|G_n| = |\langle\rho\rangle H_nI_nT_n| = 2|H_nI_nT_n| = 8n^2\phi(n)$ by Lemma 1(b). ■

Actually, each subgroup in each of the chains of Theorem 2 is normal in all later ones in its chain. In particular, $T_n \triangleleft G_n$ for $n \geq 4$.

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 vertices v, w are adjacent in $\overline{G}$ if and only if v, w are not adjacent in G. It is easily seen that $\mathrm{Aut}(G) = \mathrm{Aut}(\overline{G})$.

A *clique* of G is a subset C of $V(G)$ such that any two vertices of C are adjacent; if C has k members, we say C is a k-clique. If C is not a proper subset of another clique of G, C is a *maximal* clique.

An *independent set* in G is a set S of vertices such that no two vertices of S are adjacent. Clearly cliques of G are independent sets of $\overline{G}$ and vice versa.

To find the automorphism group of Q_n^t, we will frequently use the fact that the image of a clique (respectively independent set) under an automorphism is a clique (respectively independent set) of the same size.

Definitions. Let $a, b, d \in \mathbb{Z}_n$ with $1 \leq d \leq n/2$. Then $\{(a,b), (a+d,b), (a,b+d), (a+d, b+d)\}$ is a *two-by-two* of Q_n^t, with *side length* d.

For even n only, we define the *parity* of square (x,y) of Q_n^t to be the parity of $x+y$. We say an automorphism θ of Q_n^t *respects parity* if whenever s_1 and s_2 are squares of Q_n^t of the same parity, also $\theta(s_1)$ and $\theta(s_2)$ have the same parity. (This implies that if s_1 and s_2 have opposite parity then $\theta(s_1)$ and $\theta(s_2)$ have opposite parity.) If θ respects parity, say θ is *even* (respectively *odd*) if for every square s, s and $\theta(s)$ have the same (respectively opposite) parity.

Proposition 3 *The graph Q_n^t has a maximal 4-clique if and only if n is even. For even n, the maximal 4-cliques are exactly the two-by-twos with odd side length, except that for Q_4^t the orthogonals are also maximal 4-cliques.*

Proof. Suppose that M is a maximal 4-clique of Q_n^t. The squares of M cannot all lie in the same orthogonal unless $n = 4$, in which case it is easily verified that the orthogonal is a maximal 4-clique. The squares of M cannot all lie in the same diagonal, as each diagonal of Q_4^t is a subset of the maximal 8-clique of squares having the same parity as the number of the diagonal.

If M has exactly three squares in some line L, let γ be the automorphism of Q_n^t given by reflection across L, and let s be the fourth square of M. Since $\gamma(s)$ is adjacent to all squares of M, the maximality of M implies $\gamma(s) = s$. If L is a diagonal then γ fixes only squares of L, so L is an orthogonal. Without loss of generality, we may assume L is C_0 and s is $(a, 0)$. Then the three squares of $M \cap L$ are $(0, -a), (0, 0), (0, a)$, but $\gamma(s) = s$ implies $a \equiv -a \pmod{n}$ and then $(0, -a)$ and $(0, a)$ are the same square. So M cannot have exactly three squares in any line.

Thus it remains to consider the possibility that no line of Q_n^t contains more than two squares of M. In this case, no square of M can be adjacent to the other three squares of M along diagonals only, or along orthogonals only. Without loss of generality, we may assume $(0, 0)$ and (d, d) are in M. If $d > n/2$ then $d' = n - d \leq n/2$ and by applying $\tau_{d',d'}$ we may replace d with d', so we can assume $1 \leq d \leq n/2$.

We next establish the claim that the other squares s_1, s_2 of M are $(d, 0)$ and $(0, d)$.

Each s_i is adjacent to $(0, 0)$ along its row, column, or sum diagonal, and to (d, d) along a different one of those three lines. This implies the s_i's are among the squares $(-d, d)$, $(0, 2d)$, $(2d, 0)$, $(d, -d)$, $(d, 0)$, $(0, d)$. If $d = n/2$, the claim follows immediately, so we may assume $d < n/2$.

If the claim is false, then at least one s_i is among $(-d, d)$, $(0, 2d)$, $(2d, 0)$, $(d, -d)$; by employing the reflections across the diagonals D_0 and S_d we may assume M contains $(d, -d)$. As the column (respectively sum diagonal) of $(d, -d)$ does not contain more than two squares of M, M does not contain $(d, 0)$ (respectively $(-d, d)$). If the last square of M was $(0, d)$ or $(2d, 0)$ (respectively $(0, 2d)$), then $M \cup \{(0, 2d)\}$ (respectively $M \cup \{(2d, 0)\}$) would be a clique, contradicting the maximality of M. This establishes the claim: $M = \{(0, 0), (d, d), (d, 0), (0, d)\}$.

By the maximality of M, the difference diagonal of $(0, 0)$ and (d, d) and the sum diagonal of $(d, 0)$ and $(0, d)$ cannot intersect, which implies n is even and d is odd.

Conversely, suppose that $M = \{(0, 0), (d, 0), (0, d), (d, d)\}$ with n even, d odd, and $1 \leq d \leq n/2$. Then M is a clique that we wish to show is maximal. If not, there is a square t adjacent to all squares of M and not in M. Since n is even and d is odd, D_0 and S_d do not meet, so t cannot be diagonally adjacent to all squares of M. By symmetry we may then reduce to the possibility that t is in C_0 and adjacent to (d, d) along its sum diagonal, so t is $(0, 2d)$. But $(0, 2d)$ can only be adjacent to $(d, 0)$ along its difference diagonal, implying $2d \equiv -d \pmod{n}$, so n divides $3d$. As n is even and d is odd, this is not possible. ∎

To describe $\mathrm{Aut}(Q_4^t)$, we need to define some automorphisms.

Definition. With ω being the automorphism of Q_4^t defined in Figure 1 and μ being the reflection across R_0, set $\eta = \mu\omega$. (We do not define η directly as it is easier to

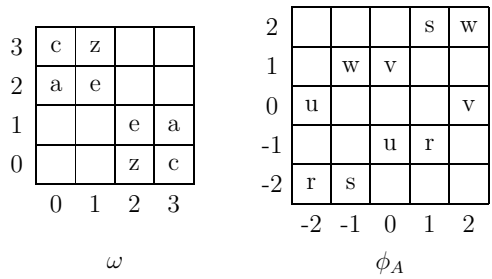

Figure 1: Automorphisms ω of Q_4^t and ϕ_A of Q_5^t are shown. In each case, the automorphism fixes blank squares and exchanges squares labelled with the same letter.

verify that μ and ω are automorphisms than η.) It is perhaps somewhat surprising that Q_4^t has an automorphism of order 3:
$\eta = ((2,0),(1,1),(1,3))((3,0),(0,1),(0,3))((2,1),(1,2),(2,3))((3,1),(0,2),(3,3))$
(using cycle notation).

Theorem 4 *The group* $Aut(Q_4^t) = G_4\langle\eta\rangle$ *so* $|Aut(Q_4^t)| = 2^7 \cdot 3 = 384$.

Proof. The eight squares of Q_4^t that have even parity form a clique, as do the eight squares of odd parity, and these are the only cliques of Q_4^t that have size eight. It follows that every automorphism of Q_4^t respects parity.

Let σ be an arbitrary automorphism of Q_4^t. There is a translation τ in T_4 such that $\sigma_1 = \tau\sigma$ fixes the square $(0,0)$. Then σ_1 is an even automorphism, so $\sigma_1(1,0)$ is an odd square adjacent to $(0,0)$, and thus $\sigma_1(1,0)$ is in $\{(\pm 1,0),(0,\pm 1)\}$. This implies there is γ in I_4 such that $\sigma_2 = \gamma\sigma_1$ fixes both $(0,0)$ and $(1,0)$.

Let $G = \{\theta \in \mathrm{Aut}(Q_4^t) : \theta(0,0) = (0,0) \text{ and } \theta(1,0) = (1,0)\}$. By Proposition 3, there are three maximal cliques of size four that contain $(0,0)$ and $(1,0)$, namely R_0 and the two-by-twos $M_{0,0} = \{(0,0),(1,0),(0,1),(1,1)\}$ and $M_{0,3} = \{(0,0),(1,0),(0,3),(1,3)\}$. Any θ in G permutes the set $S = \{R_0, M_{0,0}, M_{0,3}\}$, and this gives a homomorphism F from G to the group $\mathrm{Sym}(S)$ of permutations of S.

Since μ and ω are in G, so is η, and it is easy to verify that $F(\eta) = (M_{0,0}, M_{0,3}, R_0)$ and $F(\mu) = (M_{0,0}, M_{0,3})$, using cycle notation for members of $\mathrm{Sym}(S)$. It follows that each of the six members of $\mathrm{Sym}(S)$ is the image under F of an element $\eta^i\mu^j$ of G, where $0 \le i \le 2$ and $0 \le j \le 1$.

Then for some i and j, the automorphism $\sigma_3 = \eta^i\mu^j\sigma_2$ fixes each of R_0, $M_{0,0}$, and $M_{0,3}$ setwise. But since η, μ, and σ_2 are all even, so is σ_3, and then since σ_3 fixes $(0,0)$ and $(1,0)$, σ_3 fixes all squares of R_0, $M_{0,0}$, and $M_{0,3}$.

By repeatedly using the fact that an automorphism of Q_4^t that fixes three squares of a maximal 4-clique must fix the fourth square, we can show that $\sigma_3 = \iota$. This implies that $\sigma^{-1} = \eta^i(\mu^j\gamma)\tau$ is in the left coset $\eta^i G_4$. Taking inverses, σ is in the

right coset $G_4\eta^{-i}$, so $\mathrm{Aut}(Q_4^t) = G_4 \cup G_4\eta \cup G_4\eta^2$. To see that η is not in G_4, note that every member of G_4 sends lines to lines but $\eta(R_0) = M_{0,0}$. Thus the three right cosets G_4, $G_4\eta$, $G_4\eta^2$ are distinct, and $|\mathrm{Aut}(Q_4^t)| = 3 \cdot |G_4| = 3 \cdot 2^7 = 384$. ■

Theorem 5 *If n is even and $n \geq 6$, then $Aut(Q_n^t) = G_n$.*

Proof. Let n be even, $n \geq 6$. For each square (i, j) of Q_n^t, let M_{ij} be the two-by-two (and maximal 4-clique) $\{(i, j), (i + 1, j), (i, j + 1), (i + 1, j + 1)\}$ of Q_n^t. Let σ be an arbitrary member of $\mathrm{Aut}(Q_n^t)$. Then for each square (i, j), $\sigma(M_{ij})$ is a maximal 4-clique, which by Proposition 3 necessarily is a two-by-two of side length d_{ij} for some odd integer d_{ij} with $1 \leq d_{ij} \leq n/2$.

The cliques $M_{0,0}$ and $M_{1,0}$ share only squares $(1, 0)$ and $(1, 1)$, so $\sigma(M_{0,0})$ and $\sigma(M_{1,0})$ share only the squares $\sigma(1, 0)$ and $\sigma(1, 1)$. If these squares are diagonally adjacent, it is easily seen that they lie in a unique maximal 4-clique, which thus must contain $\sigma(M_{0,0} \cup M_{1,0})$, contradicting the fact that σ is one-to-one. Therefore $\sigma(1, 0)$ and $\sigma(1, 1)$ are orthogonally adjacent, implying $d_{0,0} = d_{1,0}$. For any (i, j) we have a sequence $M_{0,0}, M_{1,0}, \ldots, M_{i0}, M_{i1}, \ldots, M_{ij}$ of two-by-twos such that neighboring members of the sequence share exactly two squares. It follows that all d_{ij}'s have the same value d.

We show next that σ takes orthogonals to orthogonals. It suffices to show that any three consecutive squares of an orthogonal go to three squares of an orthogonal. Without loss of generality, we may consider the three consecutive squares $(1, 0)$, $(1, 1)$, and $(1, 2)$ of C_1. As shown previously, $\sigma(1, 0)$ and $\sigma(1, 1)$ are orthogonally adjacent at distance d, as are $\sigma(1, 1)$ and $\sigma(1, 2)$. Thus if $\sigma(1, 0)$, $\sigma(1, 1)$, and $\sigma(1, 2)$ are not in the same orthogonal, they are three members of a two-by-two M. Then $\sigma^{-1}(M)$ is a maximal 4-clique, so by Proposition 3, $\sigma^{-1}(M)$ is a two-by-two, contradicting the fact that $\sigma^{-1}(M)$ contains three squares of C_1. Thus $\sigma(1, 0)$, $\sigma(1, 1)$, and $\sigma(1, 2)$ are in the same orthogonal.

Therefore the image of C_1 under σ is an orthogonal, and each step of length 1 in C_1 corresponds to a step of length d in that orthogonal, with n steps required to return to the starting point. This implies that d is relatively prime to n.

Let k be the multiplicative inverse of d modulo n. Then $\sigma_1 = \lambda_k\sigma$ is an automorphism of Q_n^t that permutes $\{M_{ij} : (i, j) \in V(Q_n^t)\}$, so $\sigma_1(M_{0,0}) = M_{gh}$ for some $(g, h) \in V(Q_n^t)$. As orthogonally adjacent squares of $M_{0,0}$ must go to orthogonally adjacent squares of M_{gh} under σ_1, there are $\tau \in T_n$ and $\gamma \in I_n$ such that $\sigma_2 = \gamma\tau\sigma_1$ fixes each square of $M_{0,0}$. Then σ_2 fixes the squares of each 4-clique sharing exactly two squares with $M_{0,0}$, and this extends throughout Q_n^t, implying $\sigma_2 = \iota$. Therefore $\sigma = \lambda_k^{-1}\tau^{-1}\gamma^{-1}$ is in G_n, and $\mathrm{Aut}(Q_n^t) = G_n$. ■

Corollary 6 *For even $n \geq 4$, every automorphism of Q_n^t respects parity. For even $n \geq 6$, every automorphism of Q_n^t sends orthogonals to orthogonals and diagonals to diagonals.*

Proof. It was shown in the proof of Theorem 4 that automorphisms of Q_4^t respect parity. For even $n \geq 6$, it is easily verified that every member of H_n, of I_n, and of T_n

respects parity, takes orthogonals to orthogonals, and takes diagonals to diagonals, so the conclusion then follows from Theorems 2 and 5. ■

Another view: for even $n \geq 4$, a difference (respectively sum) diagonal of Q_n^t numbered k meets every sum (respectively difference) diagonal with number of the same parity as k in two squares, but no orthogonal meets another line in more than one square; thus no automorphism of Q_n^t can take an orthogonal to a diagonal or vice versa.

For odd n, "all lines are alike," as the automorphism ρ interchanges orthogonals and diagonals.

Theorem 7 *The group $Aut(Q_5^t) = \langle G_5, \phi_A \rangle$ and is isomorphic to a semidirect product of $\mathcal{S}_5 \times \mathcal{S}_5$ and $\mathbb{Z}_2$. Thus $Aut(Q_5^t)$ has order 28 800.*

Proof. It is well known [1] that maximal independent sets of Q_5^t have size five. We check that there are exactly ten such sets. Clearly a maximal independent set I of Q_5^t contains one square of each column. If $(0, j)$ is in I then the square of C_1 in I must be either $(1, j + 2)$ or $(1, j - 2)$. If it is $(1, j + 2)$, the square of C_2 in I cannot be $(2, j)$, as this shares its row with $(0, j)$, so must be $(2, j + 4)$. Continuing in this way, we see that each maximal independent set of Q_5^t is obtained by starting with one of the five squares of C_0 and then either applying the "knight's move" $\tau_{1,2}$ repeatedly, or similarly using $\tau_{1,-2}$. (Such *regular* independent sets will be further examined later.)

Label the maximal independent sets as follows: for $i = 1, \ldots, 5$, set $A_i = \{(j, 3 - i - 2j) : 0 \leq j \leq 4\}$ and $B_i = \{(j, -3 + i + 2j) : 0 \leq j \leq 4\}$. Let $L_A = \{A_1, \ldots, A_5\}$, $L_B = \{B_1, \ldots, B_5\}$, and $L = L_A \cup L_B$.

As the image of an independent set under an automorphism is an independent set of the same size, any automorphism of Q_5^t permutes L. This gives a homomorphism F from $\mathrm{Aut}(Q_5^t)$ to the group $\mathrm{Sym}(L)$ of permutations of L. Any square s of Q_5^t is a member of just one A_i and one B_j, and $A_i \cap B_j = \{s\}$. Thus any $\sigma \in \mathrm{Aut}(Q_5^t)$ that fixes each A_i and B_j setwise will fix each square, so $\ker F = \{\iota\}$ and $\mathrm{Aut}(Q_5^t)$ is isomorphic to its image under F.

The automorphism ϕ_A defined in Figure 1 satisfies $F(\phi_A) = (A_2, A_4)$, and $F(\tau_{1,2}) = (A_1, A_2, A_3, A_4, A_5)$, using cycle notation for members of $\mathrm{Sym}(L)$. As any 2-cycle and 5-cycle in $\mathcal{S}_5$ generate $\mathcal{S}_5$, $F(\langle \phi_A, \tau_{1,2} \rangle)$ is a subgroup of $\mathrm{Sym}(L)$ which we may identify with $\mathrm{Sym}(L_A)$.

Recall μ is reflection across R_0. It is easily checked that $F(\mu) = (A_1, B_1)(A_2, B_2)(A_3, B_3)(A_4, B_4)(A_5, B_5)$. Set $\phi_B = \mu\phi_A\mu^{-1}$ and note $\tau_{1,-2} = \mu\tau_{1,2}\mu^{-1}$. Then $F(\phi_B) = (B_2, B_4)$ and $F(\tau_{1,-2}) = (B_1, B_2, B_3, B_4, B_5)$, so $F(\langle \phi_B, \tau_{1,-2} \rangle)$ is a subgroup of $\mathrm{Sym}(L)$ which we may identify with $\mathrm{Sym}(L_B)$. Let $G = \langle \phi_A, \phi_B, \tau_{1,2}, \tau_{1,-2} \rangle$. Then $F(G)$ is the internal direct product $\mathrm{Sym}(L_A)\mathrm{Sym}(L_B)$, which is isomorphic to $\mathcal{S}_5 \times \mathcal{S}_5$, so $G \cong \mathcal{S}_5 \times \mathcal{S}_5$.

Given any $\sigma \in \mathrm{Aut}(Q_5^t)$, there is τ in T_5 such that $\sigma_1 = \tau\sigma$ fixes $(0, 0)$. As A_3 and B_3 are the maximal independent sets that contain $(0, 0)$, σ_1 sends $\{A_3, B_3\}$ to itself. So there is e in $\{0, 1\}$ such that $\sigma_2 = \mu^e\sigma_1$ fixes each of A_3 and B_3 setwise.

We will show $\sigma_2(L_A) = L_A$ and $\sigma_2(L_B) = L_B$. If not, there is $i \neq 3$ such that $\sigma_2(A_i) = B_j$ for some j. But then $\emptyset = \sigma_2(A_3 \cap A_i) = \sigma_2(A_3) \cap \sigma_2(A_i) = A_3 \cap B_j \neq \emptyset$, a contradiction. Thus $F(\sigma_2)$ is in $\mathrm{Sym}(L_A)\mathrm{Sym}(L_B)$, implying $\sigma_2 \in G$. As $T_5 = \langle \tau_{1,2}, \tau_{1,-2} \rangle$, we see $\sigma \in \langle G, \mu \rangle$, and thus $\mathrm{Aut}(Q_5^t) = \langle G, \mu \rangle$. Since $\mu G \mu^{-1} = G$ and μ has order two, $\mathrm{Aut}(Q_5^t)$ is a semidirect product as stated. Finally, $\mathrm{Aut}(Q_5^t) = \langle G, \mu \rangle = \langle \phi_A, \phi_B, \tau_{1,2}, \tau_{1,-2}, \mu \rangle \subseteq \langle \mu, \tau_{1,2}, \phi_A \rangle \subseteq \langle G_5, \phi_A \rangle \subseteq \mathrm{Aut}(Q_5^t)$, so $\mathrm{Aut}(Q_5^t) = \langle G_5, \phi_A \rangle$. ■

To approach $\mathrm{Aut}(Q_n^t)$ for odd $n \geq 7$, we need to define more kinds of cliques.

Definitions. Let $a, b \in \mathbb{Z}_n$ and $k \in \mathbb{Z}$ with $1 \leq k \leq n/2$. Then $\{(a,b), (a+k,b), (a-k,b), (a,b+k), (a,b-k)\}$ is an *orthogonal quincunx* of Q_n^t, and $\{(a,b), (a+k,b+k), (a-k,b+k), (a+k,b-k), (a-k,b-k)\}$ is a *diagonal quincunx* of Q_n^t. The union of the two quincunxes just given is a *three-by-three* of Q_n^t.

Each of the quincunxes above and the three-by-three have *radius* k, and the quincunxes have *center* (a,b).

It is easily seen that a quincunx is a clique.

If n is odd and U is a quincunx of radius k in Q_n^t, then $\rho(U)$ is a quincunx of the other type that has radius k', where $k' = 2k$ if $2k < n/2$ and $k' = n - 2k$ otherwise. Note that if $n = 3k$ then $k' = k$.

This implies that if T is a three-by-three of radius k then $\rho(T)$ is a three-by-three of radius k'.

Proposition 8 *Let n be an odd positive integer. A set M of squares of Q_n^t is a maximal clique if and only if one of the following holds:*

(i) M is a line of Q_n^t and $n \neq 3$;

(ii) M is a three-by-three of radius k and $n = 3k$;

(iii) M is a quincunx of radius k and $n \neq 3k$.

Proof. Let n be an odd positive integer, let M be a maximal clique of Q_n^t, and let h be the maximum of $|M \cap L|$ over all lines L of Q_n^t. We will show that M has one of the three forms given in the statement of the proposition; that the three types of set mentioned are maximal cliques will be apparent from the discussion.

Suppose first that $h \geq 4$. Since n is odd, any square of Q_n^t that is not in a particular line is adjacent to exactly three squares of that line. Thus there is a line L with $M \subseteq L$, and then maximality of the clique M implies $M = L$.

Suppose next that $h = 3$. Using a power of ρ and a translation if needed, we can find an automorphic image M_1 of M that meets column C_0 in a set M_1' of three squares. Then M_1 is a maximal clique but M_1' is not. (Note that $V(Q_3^t)$ is a clique, so no line of Q_3^t is a maximal clique.) As we have shown in Proposition 3 that Q_n^t has no maximal 4-clique if n is odd, M_1 contains at least two squares not in M_1', and thus not in C_0. Then employing a vertical translation, and reflection across C_0 if needed, we can find an automorphic image M_2 of M_1 such that $|M_2 \cap C_0| = 3$ and M_2 contains a square $(k,0)$ with $0 < k < n/2$. This implies $M_2 \cap C_0 = \{(0,-k), (0,0), (0,k)\}$. Call this set M_2'.

What are the possibilities for a square not in C_0 but adjacent to all squares of M_2'? It must be adjacent to one square of M_2' along its difference diagonal, to another along its row, and to the last square of M_2' along its sum diagonal. Thus there are at most $3! = 6$ such squares; together with the squares of M_2', they form a three-by-three T of radius k. However, the four squares $(\pm k, \pm k)$ of T each are adjacent to all squares of M_2' if and only if $n = 3k$. For example, the difference diagonal of $(0,0)$ and row of $(0,k)$ intersect at (k,k), which can only be adjacent to $(0,-k)$ if they share the same sum diagonal. This would mean $-k \equiv 2k \pmod{n}$, which is equivalent to n dividing $3k$. Since $0 < k < n/2$, that means $n = 3k$. Similar arguments apply to the squares $(k,-k)$, $(-k,k)$, and $(-k,-k)$.

Therefore $M_2 \subseteq T$. If $n = 3k$ then T induces a subgraph of Q_n^t that is isomorphic to Q_3^t, which is a clique, so T is a clique. As then T contains all squares adjacent to the three squares of M_2', T is a maximal clique and $M_2 = T$. Then M is the image of T under an automorphism composed of a power of ρ and a translation, so M is a three-by-three of radius k.

If $n \neq 3k$, then M_2 is contained in the orthogonal quincunx U with center $(0,0)$ and radius k, and since $|M_2| \geq 5$ we have $M_2 = U$. Then M is the image of U under an automorphism composed of a power of ρ and a translation, so M is a quincunx, and since it is a maximal clique, its radius cannot be $n/3$.

If $h = 2$, let t be a square of M. The four lines through t contain at most four other vertices of M, so $|M| \leq 5$. By Proposition 3, $|M| \neq 4$, and then since $h = 2$ and M is a maximal clique, $|M| = 3$ or 5. If $|M| = 3$ then M contains two squares in a diagonal D and one square s not in D. Let γ be the automorphism of Q_n^t given by reflection across D. Then $M \cup \{\gamma(s)\}$ is a clique of Q_n^t that properly contains M, a contradiction. Thus $|M| = 5$ which implies that any line containing a square of M contains exactly two squares of M. So if j is the number of columns containing squares of M, we have $2j = |M| = 5$, which is not possible.

If $h = 1$ then $|M| = 1$ so $n = 1$, and we may regard $M = V(Q_1^t)$ as a line of Q_1^t. ■

Theorem 9 *If n is odd and $n \geq 7$, then $Aut(Q_n^t) = G_n$.*

Proof. Let n be an odd integer, $n \geq 7$.

First we establish that each automorphism of Q_n^t takes lines to lines. For $n \neq 9$, this follows from Proposition 8, as the lines of Q_n^t are the only maximal cliques of size n. Suppose that η is an automorphism of Q_9^t that takes a line L to a three-by-three T of radius 3. Consider a set S containing any three consecutive squares s_1, s_2, s_3 of L. As S is a subset of a quincunx of radius 1, which is a maximal clique of Q_9^t by Proposition 8, $\eta(S)$ is a subset of some quincunx which is a maximal clique of Q_9^t, and thus cannot have radius 3. But also $\eta(S) \subseteq T$, so for distinct $i, j \in \{1,2,3\}$ we have $d(\eta(s_i), \eta(s_j)) = 3$, where d is the metric defined earlier. This contradiction implies no such η exists.

Let σ be an arbitrary automorphism of Q_n^t. By the preceding paragraph, $\sigma(R_0)$ is a line of Q_n^t. For some non-negative integer h and τ in T_n, the automorphism $\sigma_1 = \tau\rho^h\sigma$ has the property that $\sigma_1(R_0) = R_0$ and $\sigma_1(0,0) = (0,0)$.

For each $j \neq 0$, $R_j \cap R_0 = \emptyset$ so $\sigma_1(R_j)$ is a line of Q_n^t that does not meet R_0, thus is a row.

For each $i \in \mathbb{Z}_n$, let $U_i = \{(i-1,0),(i,0),(i+1,0),(i,1),(i,-1)\}$ be the orthogonal quincunx with center $(i,0)$ and radius 1 of Q_n^t. As each U_i is a maximal clique of Q_n^t, $\sigma_1(U_i)$ is also, and since $n > 5$, $\sigma_1(U_i)$ must be a quincunx, say of radius d_i. For each i, $|U_i \cap R_0| = 3$ so $|\sigma_1(U_i) \cap R_0| = 3$, implying $\sigma_1(U_i)$ is an orthogonal quincunx. Also, $\cup_{i=0}^{n-1} U_i = R_0 \cup R_1 \cup R_{-1}$, so $\cup_{i=0}^{n-1} \sigma_1(U_i)$ is the union of three rows. This implies all d_i's have the same value d; by composing σ_1 with reflection across R_0 if necessary, we may obtain σ_2 such that $\sigma_2(R_0) = R_0$, $\sigma_2(0,0) = (0,0)$, and $\sigma_2(R_1) = R_d$.

Looking at the overlap between U_i and U_{i+1} for each i, we see that $\sigma_2(i,0) = (di,0)$ for each i. Then $\sigma_2(R_0) = R_0$ implies that d and n are relatively prime. Let k be the multiplicative inverse of d modulo n and set $\sigma_3 = \lambda_k \sigma_2$, so σ_3 fixes each square of R_0 and fixes R_1 setwise. This implies σ_3 fixes each square of each U_i, so σ_3 fixes each square of R_1. Continuing in this way shows $\sigma_3 = \iota$, so σ is in G_n. ■

Remarks. (1) A straightforward but lengthy proof shows that the center of $\mathrm{Aut}(Q_n^t)$ is $\{\iota, \tau_{n/2,n/2}\}$ for even $n \geq 4$ and is trivial for other n. It is interesting to compare this to the fact that the center of the automorphism group of the n-dimensional hypercube, $n \geq 1$, has one nontrivial member: the antipodal map.

(2) No nonabelian simple group has order dividing $|\mathrm{Aut}(Q_4^t)|$ (found in Theorem 4), so $\mathrm{Aut}(Q_4^t)$ is solvable. For $n > 4$, it is apparent from the definitions of the groups T_n, I_n, H_n, and $\langle\rho\rangle$ that they are solvable. It then follows from Theorems 2, 5, 7, and 9 that $\mathrm{Aut}(Q_n^t)$ is solvable except for $n = 3$, when the alternating group $\mathcal{A}_9$ is a composition factor, and $n = 5$, when $\mathcal{A}_5$ appears twice as a composition factor.

Table 1 summarizes much of what we have found about $\mathrm{Aut}(Q_n^t)$.

n	$\mathrm{Aut}(Q_n^t)$	$\lvert\mathrm{Aut}(Q_n^t)\rvert$
$1,2,3$	$\cong \mathcal{S}_{n^2}$	$(n^2)!$
4	$= G_4\langle\eta\rangle$	$384 = 2^7 \cdot 3$
5	$= \langle G_5, \phi_A\rangle \cong (\mathcal{S}_5 \times \mathcal{S}_5) \rtimes \mathbb{Z}_2$	$28\,800 = 2^7 \cdot 3^2 \cdot 5^2$
≥ 6	$= G_n$	$4n^2\phi(n)$ if n even, $8n^2\phi(n)$ if n odd.

Table 1: A summary of information about $\mathrm{Aut}(Q_n^t)$.

3 Edges and $\mathrm{Aut}(Q_n^t)$

We now examine the interplay of automorphisms and edges for Q_n^t.

Definitions. Let $e = (v_1, v_2)$ and $f = (w_1, w_2)$ be edges of a finite, simple graph U and let G be a subgroup of $\mathrm{Aut}(U)$. Say edges e and f are *G-related* if there is θ in G such that either $\theta(v_i) = w_i$ for $i = 1, 2$, or $\theta(v_i) = w_{3-i}$ for $i = 1, 2$. (If $G = \mathrm{Aut}(U)$, we just say e and f are related.) It is easily seen that this is an equivalence relation

on the edge set of U. The equivalence class of edge e will be denoted $[e]_G$ unless $G = \mathrm{Aut}(U)$, when $[e]$ will be used; we say $[e]$ is the *edge class* of e. We write $\psi(U)$ for the number of edge classes of U.

For each positive integer n, let $\tau(n)$ denote the number of positive divisors of n.

The proof of our theorem on edge classes will require the following elementary lemma, whose proof will be omitted.

Lemma 10 *For nonzero integers i, j, n, the following conditions are equivalent:*
(i) There exists an integer m such that $\gcd(m, n) = 1$ and $mi \equiv j \pmod{n}$;
(ii) $\gcd(i, n) = \gcd(j, n)$.

Theorem 11

$$\psi(Q_n^t) = \begin{cases} \tau(n) - 1 \text{ for odd } n, \\ 1 \text{ for } n = 2, \\ 3 \text{ for } n = 4, \\ 2(\tau(n) - 1) \text{ for even } n \geq 6. \end{cases}$$

A complete set of edge class representatives for each $n > 1$ is:
for $n = 2$ and for odd $n \geq 3$, $\{((0,0),(d,0)) : d \text{ divides } n \text{ and } 1 \leq d < n\}$;
for $n = 4$, $\{((0,0),(1,0)),((0,0),(2,0)),((0,0),(2,2))\}$;
for even $n \geq 6$, $\{((0,0),(d,0)),((0,0),(d,d)) : d \text{ divides } n \text{ and } 1 \leq d < n\}$.

Proof. As previously noted, for $n = 2, 3$, every permutation of the squares of Q_n^t is an automorphism, so $\psi(Q_2^t) = \psi(Q_3^t) = 1$. For the remainder of the proof, we will assume $n \geq 4$.

Let G be a subgroup of $\mathrm{Aut}(Q_n^t)$ that contains the translation subgroup T_n and the square subgroup I_n. Since $T_n \subseteq G$, every class $[e]_G$ contains an edge having $(0,0)$ as one end. Since $I_n \subseteq G$, for each orthogonal (respectively diagonal) edge e, the class $[e]_G$ contains an edge of form $((0,0),(i,0))$ (respectively $((0,0),(i,i))$) for some i in $\mathbb{Z}_n$. Finally, we note that we can use an automorphism in G to "reverse" an edge : this follows from $\beta\mu\beta\tau_{-i,0}((0,0),(i,0)) = ((i,0),(0,0))$ and $\mu\beta\mu\tau_{-i,-i}((0,0),(i,i)) = ((i,i),(0,0))$. Thus in determining the equivalence classes of edges under the action of G, it suffices to consider edges of form $((0,0),(i,0))$ and $((0,0),(i,i))$ and automorphisms in G that fix $(0,0)$.

We first take $G = G_n$.

Suppose that n is odd, and the edge $((0,0),(i,0))$ is G_n-related to $((0,0),(j,0))$. By Theorem 2, $G_n = \langle\rho\rangle H_n I_n T_n$, so there are a non-negative integer p, λ_m in H_n, γ in I_n, and τ in T_n such that $\rho^p\lambda_m\gamma\tau$ sends $(0,0)$ to $(0,0)$ and $(i,0)$ to $(j,0)$. Since ρ, λ_m, and γ send $(0,0)$ to $(0,0)$, we see $\tau = \iota$ and then $(j,0) = \rho^p\lambda_m\gamma(i,0)$. By the Division Algorithm, there are integers q and r such that $p = 2q + r$ and $0 \leq r \leq 1$. Then using $\rho^2 = \lambda_2\alpha$ and the fact that members of H_n commute with members of I_n, we have $(j,0) = \rho^p\lambda_m\gamma(i,0) = \rho^r(\alpha^q\gamma)(\lambda_2^q\lambda_m)(i,0) = \rho^r\gamma'(2^q mi, 0)$, where $\gamma' = \alpha^q\gamma$ is in I_n. As $\gamma'(2^q mi, 0)$ is in $\{(\pm 2^q mi, 0), (0, \pm 2^q mi)\}$, we have $r = 0$ and $\pm 2^q mi \equiv j \pmod{n}$. Since n is odd, $\gcd(2^q m, n) = 1$, so (i) implies (ii) of

Lemma 10 gives $\gcd(i,n) = \gcd(j,n)$. Calling this common value d, it is easily seen from (ii) implies (i) of Lemma 10 that the edge $((0,0),(d,0))$ is G_n-related to both $((0,0),(i,0))$ and $((0,0),(j,0))$. A similar proof shows that for odd n, edges $((0,0),(i,i))$ and $((0,0),(j,j))$ are G_n-related if and only if $\gcd(i,n) = \gcd(j,n)$, and that then both are G_n-related to $((0,0),(d,d))$ for $d = \gcd(i,n)$. Finally, for any divisor d of n, $\rho(d,d) = (2d,0)$, so the edge $((0,0),(d,d))$ is G_n-related to the edge $((0,0),(2d,0))$, and since n is odd, $((0,0),(2d,0))$ is G_n-related to $((0,0),(d,0))$.

Thus for each odd $n \geq 5$, a complete set of representatives of G_n-equivalence classes of edges is the set given in the theorem statement as a complete set of edge class representatives. By Theorem 9, $G_n = \mathrm{Aut}(Q_n^t)$ for odd $n \geq 7$, so the theorem is proved for these n. Above we have shown that there is only one G_5-equivalence class of edges of Q_5^t so since $G_5 \subseteq \mathrm{Aut}(Q_5^t)$, $\psi(Q_5^t) = 1$.

The proof for even n is similar to and simpler than that for odd n, so we will mention only a few points.

First, for even $n \geq 6$, no diagonal edge is G_n-related to any orthogonal edge. To see this, suppose instead that there is θ in G_n such that θ sends edge $((0,0),(i,0))$ to $((0,0),(j,j))$. By Theorem 5 there are λ_m in H_m, γ in I_n, and τ in T_n such that $\lambda_m\gamma\tau$ sends $(0,0)$ to $(0,0)$ and $(i,0)$ to (j,j). As before, since λ_m and γ send $(0,0)$ to $(0,0)$, we see $\tau = \iota$ and then $(j,j) = \lambda_m\gamma(i,0) = \gamma(mi,0)$. But $\gamma(mi,0)$ is a member of $\{(\pm mi,0),(0,\pm mi)\}$, and thus cannot equal (j,j).

For even $n \geq 6$, $G_n = \mathrm{Aut}(Q_n^t)$ by Theorem 5, so the theorem is proved for these n.

For $n = 4$, we have shown that a complete set of equivalence class representatives under the action of G_4 is $\{((0,0),(1,0)),((0,0),(2,0)),((0,0),(1,1)),((0,0),(2,2))\}$. The first edge given here joins an even square to an odd one, and since every automorphism of Q_4^t respects parity (Corollary 6), this edge is not related to any of the other three. With η as defined before Theorem 4, $\eta((0,0),(2,0)) = ((0,0),(1,1))$, so two of the G_4-equivalence classes are contained in a single edge class. Lastly we show that $((0,0),(2,0))$ is not related to $((0,0),(2,2))$. If these edges are related, by Theorem 4 there is an integer p (with $0 \leq p \leq 2$), λ_m in H_4, γ in I_4, and τ in T_4 such that $\eta^p\lambda_m\gamma\tau$ takes $(0,0)$ to itself and $((0,0),(2,0))$ to $((0,0),(2,2))$. As before this implies $\tau = \iota$, and then $\eta^p\lambda_m\gamma(2,0) = (2,2)$. Applying η^{3-p} gives $\lambda_m\gamma(2,0) = (2,2)$ and then $\gamma(2m,0) = (2,2)$, which cannot happen since $\gamma(2m,0)$ is a member of $\{(\pm 2m,0),(0,\pm 2m)\}$. Thus the set of edge class representatives for Q_4^t stated in the theorem is correct. ■

Recall that a graph is *edge-transitive* if any two edges are related by the automorphism group of the graph. The corollary below follows from Theorem 11.

Corollary 12 *For $n > 1$, Q_n^t is edge-transitive if and only if n is prime.*

4 Regular solutions of the toroidal n-queens problem

The *n-queens problem* is the problem of placing n queens on an $n \times n$ chessboard so that no two queens attack each other. For the usual chessboard, Ahrens [1] showed this is possible for $n = 1$ and $n \geq 4$. For the toroidal chessboard, Pólya (cited in [1]) showed that solutions exist if and only if $n \equiv \pm 1 \pmod 6$.

We examine the type of toroidal n-queens solutions defined next.

Definitions. A *regular* solution of the toroidal n-queens problem is a solution of the form

$$S = \{(x + a, kx + b) : x \in \mathbb{Z}_n\} \tag{1}$$

for some fixed $k, a, b \in \mathbb{Z}_n$. We refer to k as the *step* of the regular solution S. Let $\mathrm{Reg}(n)$ denote the set of regular solutions of the toroidal n-queens problem.

Regular solutions were studied by Pólya, who used them to prove (see [8] or [7]) Fermat's theorem that a prime number of the form $4k + 1$ is the sum of two squares.

We will determine the number of regular solutions that are distinct up to automorphism of Q_n^t. This extends work of Burger, Cockayne, and Mynhardt [4], where the number of regular solutions up to isometry was found; we follow their approach.

Which k occur as steps of regular solutions?

Definitions. For odd $n > 1$, set $\mathbf{P}_n = \{i \in \mathbb{Z}_n : \gcd(i, n) = 1\}$ and $\mathbf{R}_n = \{i \in \mathbb{Z}_n : i - 1, i, i + 1 \in \mathbf{P}_n\}$.

It is easily seen that the squares in $S = \{(x + a, kx + b) : x \in \mathbb{Z}_n\}$ have distinct row numbers (respectively difference diagonal numbers, sum diagonal numbers) if and only if the set $\{ki : i \in \mathbb{Z}_n\}$ (respectively $\{(k-1)i : i \in \mathbb{Z}_n\}$, $\{(k+1)i : i \in \mathbb{Z}_n\}$) equals $\mathbb{Z}_n$, which is equivalent to $k - 1, k, k + 1$ all being relatively prime to n. This establishes the following, which is [4, Proposition 3].

Proposition 13 *For $a, b, k \in \mathbb{Z}_n$, $S = \{(x + a, kx + b) : x \in \mathbb{Z}_n\}$ is a solution of the toroidal n-queens problem if and only if k is in $\mathbf{R}_n$.*

In particular, suppose that $n > 1$ and $n \equiv \pm 1 \pmod 6$. Then n is relatively prime to 2 and 3, so 2 is in $\mathbf{R}_n$ and thus $k = 2$ gives a regular solution for every such n.

Part (a) of the next proposition is proved in [4, Theorem 10]. Part (b) is implicit in [4]; it follows from the fact that for any k in $\mathbf{R}_n$, a regular solution of step k can include any square of C_0, and is determined by that square and k.

Proposition 14 *Let $n > 1$ and $n \equiv \pm 1 \pmod 6$, and let $p_1, \ldots, p_t$ be the distinct primes that divide n. Then:*

(a) $|\mathbf{R}_n| = n \prod_{i=1}^{t} (1 - \frac{3}{p_i})$;

(b) The number of regular solutions of the toroidal n-queens problem is $n|\mathbf{R}_n|$.

For both the usual chessboard and the toroidal one, many methods of constructing solutions to the n-queens problem have been found and considerable effort has been

devoted to determining the number of solutions for each n. See [9] for a summary. There is a connection between the two problems: Pólya [1, 9] showed that any toroidal $n \times n$ solution and any usual $m \times m$ solution may be composed to get a usual $mn \times mn$ solution, by replacing each empty square of the $m \times m$ board with an empty $n \times n$ board and each occupied square of the $m \times m$ board with a copy of the toroidal $n \times n$ solution.

The regular toroidal solutions may be seen as the simplest ones for the toroidal n-queens problem. For an interesting method of altering regular toroidal solutions to get more toroidal solutions, see [3].

Definition. Let $n \geq 1$ and $n \equiv \pm 1 \pmod 6$, and let θ be an automorphism of Q_n^t. We say θ *respects step* if for any S_1, S_2 in $\mathrm{Reg}(n)$ that have the same step, $\theta(S_1)$ and $\theta(S_2)$ are in $\mathrm{Reg}(n)$ and have the same step.

Lemma 15 *Let $n \geq 1$ and $n \equiv \pm 1 \pmod 6$. Every automorphism of Q_n^t respects step.*

Proof. There is nothing to prove for $n = 1$ so let $n \equiv \pm 1 \pmod 6$ and $n \geq 5$. As remarked after Theorem 2, the image of an independent set of vertices of a graph under an automorphism is an independent set of the same size. Thus the image of any regular solution under an automorphism is a solution of the n-queens problem, and it will be clear from the following discussion that it is regular. By Theorems 2, 7, and 9, any automorphism of Q_n^t can be written as a product of elements of the subgroups $\langle\rho\rangle$, H_n, I_n, T_n, and (if $n = 5$) $\langle\phi_A\rangle$, so it suffices to show that every member of each of these subgroups preserves step. The following equations establish this (recall $I_n = \langle\beta, \mu\rangle$). With S as in (1):

$\mu(S) = \{(x+a, -kx-b) : x \in \mathbb{Z}_n\} = \{(x+a, (-k)x-b) : x \in \mathbb{Z}_n\}$. Thus μ sends regular solutions with step k to regular solutions with step $-k$. This corresponds to a bijection $k \mapsto -k$ from $\mathbf{R}_n$ to $\mathbf{R}_n$.

$\beta(S) = \{(kx+b, x+a) : x \in \mathbb{Z}_n\} = \{(k(k^{-1}i)+b, k^{-1}i+a) : i \in \mathbb{Z}_n\} = \{(i+b, k^{-1}i+a) : i \in \mathbb{Z}_n\}$: bijection $k \mapsto 1/k$.

$\tau_{h,j}(S) = \{x+a+h, kx+b+j) : x \in \mathbb{Z}_n\}$: bijection $k \mapsto k$.

$\lambda_m(S) = \{(m(m^{-1}i+a), m(km^{-1}i+b)) : i \in \mathbb{Z}_n\} = \{(i+ma, ki+mb) : i \in \mathbb{Z}_n\}$: bijection $k \mapsto k$.

$\rho(S) = \{((k+1)x+a+b, (k-1)x+b-a) : x \in \mathbb{Z}_n\} = \{((k+1)(k+1)^{-1}i+a+b, (k-1)(k+1)^{-1}i+b-a) : i \in \mathbb{Z}_n\} = \{(i+a+b, (k-1)(k+1)^{-1}i+b-a) : i \in \mathbb{Z}_n\}$: bijection $k \mapsto \frac{k-1}{k+1}$.

For $n = 5$: using the notation of the proof of Proposition 7, each B_i is a regular solution of step 2 and each A_i is a regular solution of step 3. It was shown that ϕ_A induces the permutation (A_2, A_4) of the set $L = \{A_1, \ldots, A_5, B_1, \ldots, B_5\}$. Thus ϕ_A respects step and gives the bijection $k \mapsto k$. ∎

Definitions. Say that S, S' in $\mathrm{Reg}(n)$ are *automorphic*, denoted $S \sim S'$, if there is an automorphism θ of Q_n^t such that $\theta(S) = S'$.

Two members k, k' of $\mathbf{R}_n$ are *similar*, denoted $k \approx k'$, if $S \sim S'$ for every regular solution S with step k and every regular solution S' with step k'.

It is clear that these are equivalence relations on $\mathrm{Reg}(n)$ and $\mathbf{R}_n$, respectively. We write $[S]$ for the automorphism class of the regular solution S, and $\mathrm{Reg}^*(n)$ for the set of all automorphism classes. Let $\delta(n) = |\mathrm{Reg}^*(n)|$.

The similarity class of k under $\approx$ is $[k]$, and the set of all similarity classes is $\mathbf{R}_n^*$.

The analysis in [4] was carried out using the isometry subgroup I_nT_n of $\mathrm{Aut}(Q_n^t)$ where we are using $\mathrm{Aut}(Q_n^t)$. The proof of Lemma 15 shows that the automorphism ρ makes the difference between the two approaches.

Lemma 16 *For any k, k' in $\mathbf{R}_n$, the following are equivalent:*

(i) $k \approx k'$;

(ii) there exist S, S' in Reg(n) with steps k, k' such that $S \sim S'$.

Proof. We may assume $n \equiv \pm 1 \pmod 6$ and $n \geq 5$. That (i) implies (ii) is clear from the definition of the relation $\approx$. Assume that (ii) holds; then there is θ in $\mathrm{Aut}(Q_n^t)$ with $\theta(S) = S'$. For every S'' in $\mathrm{Reg}(n)$ with step k, Lemma 15 implies that $\theta(S'')$ has step k'. Since any two regular solutions with step k' are automorphic by a translation, we see $k \approx k'$. ∎

We may then define $H : \mathrm{Reg}^*(n) \to \mathbf{R}_n^*$ by $H([S]) = [k]$, where k is the step of the regular solution S. By Lemma 16, H is well-defined, and it is then not difficult to see that H is a one-to-one correspondence. Thus $\delta(n) = |\mathbf{R}_n^*|$, the number of similarity classes in $\mathbf{R}_n$. To find $|\mathbf{R}_n^*|$, we need [4, Theorem 9], given next.

Theorem 17 *Let $n > 1$ be an odd integer, let $p_1, \ldots, p_t$ be the distinct primes dividing n, and let a in $\mathbf{P}_n$. The congruence*

$$x^2 \equiv a \pmod n \tag{2}$$

has a solution if and only if each of the congruences $x^2 \equiv a \pmod{p_i}$, $i = 1, \ldots, t$ has a solution, in which case (2) has exactly 2^t solutions. These solutions (modulo n) are in $\mathbf{P}_n$, and are in $\mathbf{R}_n$ if and only if $a - 1$ (mod n) is in $\mathbf{P}_n$.

Theorem 18 *Let $n > 1$ with $n \equiv \pm 1 \pmod 6$ and let $p_1, \ldots, p_t$ be the distinct primes dividing n. For each k in $\mathbf{R}_n$:*

$[k] = \{k, -k\}$ with $|[k]| = 2$ if and only if $k^2 \equiv -1 \pmod n$;

$[k] = \{k, -k, \frac{1}{k}, \frac{-1}{k}\}$ with $|[k]| = 4$ if and only if $(k \pm 1)^2 \equiv 2 \pmod n$;

$[k] = \{k, -k, \frac{1}{k}, \frac{-1}{k}, \frac{k-1}{k+1}, -\frac{k-1}{k+1}, \frac{k+1}{k-1}, -\frac{k+1}{k-1}\}$ with $|[k]| = 8$ otherwise. Then:

$$\delta(n) = \begin{cases} \frac{1}{8}\left(5 \cdot 2^t + n\prod_{i=1}^t (1 - \frac{3}{p_i})\right) & \text{if } p_i \equiv 1 \pmod 8 \text{ for all } i; \\ \frac{1}{8}\left(3 \cdot 2^t + n\prod_{i=1}^t (1 - \frac{3}{p_i})\right) & \text{if } p_i \equiv 1 \text{ or } 5 \pmod 8 \text{ for all } i \\ & \text{and } p_i \equiv 5 \pmod 8 \text{ for some } i; \\ \frac{1}{8}\left(2 \cdot 2^t + n\prod_{i=1}^t (1 - \frac{3}{p_i})\right) & \text{if } p_i \equiv 1 \text{ or } 7 \pmod 8 \text{ for all } i \\ & \text{and } p_i \equiv 7 \pmod 8 \text{ for some } i; \\ \frac{n}{8}\prod_{i=1}^t (1 - \frac{3}{p_i}) & \text{otherwise.} \end{cases}$$

Proof. From the proof of Lemma 15, for each k in $\mathbf{R}_n$, the class $[k]$ is the smallest subset of $\mathbf{R}_n$ that contains k and is closed under the three bijections from $\mathbf{R}_n$

to $\mathbf{R}_n$ that send k to $-k, 1/k$, and $(k-1)/(k+1)$ respectively. Under composition, these bijections generate a subgroup D of $\mathrm{Sym}(\mathbf{R}_n)$ that is isomorphic to the dihedral group of order eight. We will refer to each bijection in D by its value at k, abusing notation to avoid introducing more names. With this convention, $D = \{k, -k, \frac{1}{k}, -\frac{1}{k}, \frac{k-1}{k+1}, -\frac{k-1}{k+1}, \frac{k+1}{k-1}, -\frac{k+1}{k-1}\}$.

Letting D act on $\mathbf{R}_n$ in the natural way, $[k]$ is the orbit $Dk = \{g(k) : g \in D\}$. By [2, Proposition 7.3.5(b)], $|[k]|$ is the index in D of the isotropy subgroup $D_k = \{g \in D : g(k) = k\}$. We find D_k for each k in $\mathbf{R}_n$.

Since n is odd and $k \neq 0$, also $k \neq -k$, so the bijection $-k$ is not in D_k. For any k in $\mathbf{R}_n$, both $k-1$ and $k+1$ are relatively prime to n, so $k^2 - 1 \not\equiv 0 \pmod{n}$, and thus $k \neq 1/k$ so the bijection $1/k$ is not in D_k. In particular these facts imply $D_k \neq D$ for any k in $\mathbf{R}_n$.

The bijection $-1/k$ is in D_k if and only if $k^2 = -1$, which is true if and only if the bijection $\frac{k-1}{k+1}$ is in D_k. As $|\langle\frac{k-1}{k+1}\rangle| = 4$ and $D_k \neq D$, we see that $D_k = \langle\frac{k-1}{k+1}\rangle$ if and only if $k^2 = -1$, and in this case $|[k]| = [D : D_k] = 2$ so $[k] = \{k, -k\}$. By Theorem 17, the congruence

$$x^2 \equiv -1 \pmod{n} \tag{3}$$

is solvable if and only if for each i, the congruence $x^2 \equiv -1 \pmod{p_i}$ is solvable. By [5, Corollary, page 93], this occurs if and only if $p_i \equiv 1 \pmod 4$ for each i, and then by Theorem 17, (3) has 2^t solutions, which are in $\mathbf{R}_n$ since -2 is in $\mathbf{P}_n$. These 2^t solutions pair off to give 2^{t-1} similarity classes of size two.

Otherwise we may assume that the intersection of D_k with each of the subgroups $\langle\frac{k-1}{k+1}\rangle$ and $\langle -k, 1/k\rangle$ of D is trivial, which leaves three possibilities:

The isotropy subgroup D_k is trivial. Then $[k]$ has eight members as given.

The isotropy subgroup $D_k = \langle -\frac{k-1}{k+1}\rangle$. The equation $k = -\frac{k-1}{k+1}$ is equivalent to $(k+1)^2 = 2$ and also to $k(k+2) = 1$. By Theorem 17, the congruence

$$x^2 \equiv 2 \pmod{n} \tag{4}$$

is solvable if and only if for each i, the congruence $x^2 \equiv 2 \pmod{p_i}$ is solvable. By [5, Theorem 9-6] this occurs if and only if $p_i \equiv \pm 1 \pmod 8$ for each i, and in this case there are 2^t solutions of (4), which are in $\mathbf{R}_n$ since 1 is in $\mathbf{P}_n$. Say $\pm y$ are two solutions of (4) and set $k+1 = y$. Then $k = y-1$ is in $\mathbf{P}_n$ since y is in $\mathbf{R}_n$; to show k is in $\mathbf{R}_n$, we need $k - 1 = y - 2$ in $\mathbf{P}_n$, which follows from $y(y-2) = 2 - 2y = 2(1-y)$, since y, 2 and $1-y$ are in $\mathbf{P}_n$. Here $|D_k| = 2$ so $|[k]| = [D : D_k] = 4$. From $k(k+2) = 1$ we see $[k] = \{k, -k, \frac{1}{k}, \frac{-1}{k}\} = \{k, -k, k+2, -k-2\} = \{\pm y \pm 1\}$. Thus each of the 2^{t-1} pairs $\pm y$ of solutions of (4) gives a similarity class $\{\pm y \pm 1\}$ of size four. In each of these classes, $y-1$ and $-y-1$ have isotropy subgroup $\langle -\frac{k-1}{k+1}\rangle$.

The isotropy subgroup $D_k = \langle\frac{k+1}{k-1}\rangle$. The equation $k = \frac{k+1}{k-1}$ is equivalent to $(k-1)^2 = 2$. If we define k' by $k' = k - 2$, then $(k'+1)^2 = 2$. Therefore this case reduces to the previous one, with the same 2^{t-1} similarity classes of size four. In each similarity class $\{\pm y \pm 1\}$ discussed there, $y+1$ and $-y+1$ have isotropy subgroup $\langle\frac{k+1}{k-1}\rangle$.

It is now straightforward to determine $\delta(n)$ for each n; we only examine the most complex case: $p_i \equiv 1 \pmod 8$ for $i = 1, \ldots, t$. Here there are 2^{t-1} similarity classes of size two and 2^{t-1} similarity classes of size four in $\mathbf{R}_n$, leaving $(|\mathbf{R}_n| - 2 \cdot 2^{t-1} - 4 \cdot 2^{t-1})/8$ classes of size 8. Then using the value for $\mathbf{R}_n$ from Proposition 14(a) gives $\delta(n)$ the value stated. ■

References

[1] W. Ahrens, *Mathematische unterhaltungen und spiele*, B. G. Teubner, Leipzig-Berlin, 1910.

[2] J. Beachy and W. D. Blair, *Abstract Algebra*, 3rd edition, Waveland Press, Long Grove, 2006.

[3] J. Bell, A new method for constructing nonlinear modular n-queens solutions, *Ars. Combin.* **78** (2006), 151–155.

[4] A. Burger, E. Cockayne and C. Mynhardt, Regular Solutions of the n-Queens Problem on the Torus, *Utilitas Math.* **65** (2004), 219–230.

[5] D. M. Burton, *Elementary Number Theory*, 3rd edition, Wm. C. Brown, Dubuque, 1994.

[6] I. N. Herstein, *Topics in Algebra*, Xerox, Lexington and Toronto, 1964.

[7] L. Larson, A Theorem About Primes Proved on a Chessboard, *Math. Mag.* **50** (1977), no. 2, 69–74.

[8] G. Pólya, Über die "doppelt-periodischen" Lösungen des n-Damen Problems, in *Mathematische Unterhaltungen und Spiele*, W. Ahrens, vol. 2, 2nd ed., B. G. Teubner, Leipzig, 1918, 363–374.

[9] I. Rivin, I. Vardi and P. Zimmerman, The n-queens problem, *Amer. Math. Monthly* **101** (1994), 629–639.

(Received 13 Aug 2007; revised 29 Apr 2008)