SEMIREGULAR AUTOMORPHISMS
OF CUBIC VERTEX TRANSITIVE GRAPHS

CAI HENG LI

(Communicated by John R. Stembridge)

Abstract. It is shown that for a connected cubic graph $\Gamma$, a vertex transitive group $G \leq \text{Aut} \Gamma$ contains a large semiregular subgroup. This confirms a conjecture of Cameron and Sheehan (2001).

1. Introduction

A permutation $\pi$ is called semiregular if all of its cycles have the same length. Marušić, Jordan and Klin in the 1980s independently proposed a conjecture, called the polycirculant conjecture, that any finite vertex transitive graph has a nontrivial semiregular automorphism. Some partial results for this conjecture have been obtained in various special cases; see [1, 5, 6]. In particular, Marušić and Scapellato [6] proved this conjecture for cubic graphs. A permutation group $H$ on a set $\Omega$ is called semiregular if each nonidentity element of $H$ fixes no point of $\Omega$. So each nonidentity element of a semiregular group is a semiregular permutation. Cameron and Sheehan [1] Problem BCC 17.12] proposed a conjecture that a vertex transitive automorphism group of a connected cubic graph contains a “large” semiregular subgroup, as stated in Theorem 1.1. The Cameron-Sheehan conjecture was also restated in Problem 6.3 of [2]. In a recent paper [3], a partial result for this conjecture was obtained. The purpose of this paper is to confirm this conjecture.

Theorem 1.1. There is a function $f$ satisfying $f(n) \to \infty$ as $n \to \infty$ such that a vertex transitive automorphism group of a connected cubic graph on $n$ vertices has a semiregular subgroup of order at least $f(n)$.

Naturally, one would ask whether the Cameron-Sheehan “conjecture” can be extended to more classes of graphs. We are inclined to conjecture that its following extension would be true.

Conjecture 1.2. For any given integer $k \geq 3$, there is a function $f_k$ satisfying $f_k(n) \to \infty$ as $n \to \infty$ such that a vertex transitive automorphism group of a connected graph of valency $k$ on $n$ vertices has a semiregular subgroup of order at least $f_k(n)$.
Remark. Conjecture 1.2 is verified in the quasiprimitive and bi-quasiprimitive cases in Corollary 1.2. The polycirculant conjecture and Conjecture 1.2 do not imply each other. The polycirculant conjecture is about the existence of semiregular permutations, while Conjecture 1.2 states that a sufficiently large permutation group has many semiregular permutations.

2. Some basic properties of vertex transitive graphs

In this preliminary section, we first discuss a typical method for studying vertex transitive graphs, which will be used in the proof of Theorem 1.1.

In a graph, an ordered pair of adjacent vertices is called an arc. For a graph $G$, denote by $V(G)$, $E(G)$, and $A(G)$ the vertex set, the edge set and the arc set of $G$, respectively. For a vertex $v$ of $G$, denote by $\Gamma(v)$ the neighborhood of $v$, consisting of vertices $\Gamma$ which are adjacent to $v$. A graph $G$ is called $G$-vertex transitive, $G$-edge transitive, or $G$-arc transitive if a group $G \leq \text{Aut}(G)$ is transitive on $V(G)$, $E(G)$ or $A(G)$, respectively.

Let $G$ be a connected $G$-vertex transitive graph of valency $k$. Let $H$ be a normal subgroup of $G$ which is intransitive on $V(G)$. Let $B$ be the set of $H$-orbits in $V(G)$. Then $\mathcal{B}$ is a $G$-invariant partition of $V(G)$; that is, $\mathcal{B}$ is a block system of imprimitivity for $G$. The normal quotient graph $\Gamma_N$ of $\Gamma$ induced by $N$ is defined as the graph with vertex set $\mathcal{B}$ such that $B, C \in \mathcal{B}$ are adjacent in $\Gamma_N$ if and only if some vertex in $B$ is adjacent in $\Gamma$ to some vertex in $C$. If the valency of $\Gamma_N$ equals the valency of $\Gamma$, then $\Gamma$ is called a normal cover of $\Gamma_N$.

For convenience, a vertex transitive graph is said to be basic if it is not a normal cover of a smaller vertex transitive graph. A permutation group $G$ on a set $\Omega$ is called quasiprimitive if any nontrivial normal subgroup of $G$ is transitive on $\Omega$, and $G$ is called bi-quasiprimitive if any nontrivial normal subgroup of $G$ has at most two orbits on $\Omega$ and at least one normal subgroup has exactly two orbits. A vertex transitive graph $\Gamma$ is called quasiprimitive or bi-quasiprimitive if some group $G \leq \text{Aut}(\Gamma)$ is quasiprimitive or bi-quasiprimitive on $V(\Gamma)$, respectively.

The following lemma slightly extends Lemma 2.1 of [4].

**Lemma 2.1.** Let $\Gamma$ be a connected $G$-vertex transitive graph of valency $k$, and let $N$ be a normal subgroup of $G$. Then each prime divisor of $|N_v|$ divides $|N_v^{\Gamma(v)}|$, where $v \in V(\Gamma)$. In particular, any prime divisor of $|G_v|$ is at most $k$ and divides $|G_v^{\Gamma(v)}|$.

**Proof.** Let $p$ be a prime divisor of $|N_v|$, and let $g \in N_v$ have order $p$. Let $v_0 = v, v_1, \ldots, v_l$ be a maximal path of $\Gamma$ such that $g$ fixes each $v_i$. Since $\Gamma$ is connected, there exists $w \in \Gamma(v_1)$ which is not fixed by $g$. Thus $g \in N_{v_i}$ acts nontrivially on $\Gamma(v_i)$, and so $p$ divides $|N_{v_i}^{\Gamma(v_i)}|$. Since $G$ is transitive on $V(\Gamma)$ and $N \lhd G$, the action of $N_{v_i}$ on $\Gamma(v)$ is equivalent to the action of $N_{v_i}$ on $\Gamma(v_i)$. Hence $p$ divides $|N_{v_i}^{\Gamma(v)}|$.

For a subset $B \subset V(\Gamma)$, denote by $[B]$ the induced subgraph of $\Gamma$ on $B$, that is, the subgraph with vertex set $B$ and arc set $A(\Gamma) \cap (B \times B)$. For disjoint subsets $B, C \subset V(\Gamma)$, denote by $[B, C]$ the subgraph of $\Gamma$ with vertex set $B \cup C$ and arc set $A(\Gamma) \cap (B \times C)$. Here is a property about normal quotient graphs of vertex transitive graphs.
Lemma 2.2. Let $\Gamma$ be a connected $G$-vertex transitive graph of valency $k$. Let $N$ be an intransitive normal subgroup of $G$, and let $K$ be the kernel of $G$ acting on the set of $N$-orbits on $V\Gamma$. Then the following statements hold:

(i) For two orbits $B, C$ of $N$ on $V\Gamma$, the subgraph $[B, C]$ is regular, and the valency of $\Gamma_N$ is at most $k$.

(ii) If $\Gamma$ is a cover of $\Gamma_N$, then $N = K$ is semiregular on $V\Gamma$.

Proof. (i). Assume that a vertex $u \in B$ is adjacent to a vertex $w \in C$. Then for any element $g \in N$, $\{w^g, w^g\}$ is an edge that lies between $B$ and $C$. Since $N$ is transitive on $B$, all vertices in $B$ are adjacent to the same number of vertices in $C$. Similarly, all vertices in $C$ are adjacent to the same number of vertices in $B$. Since $|B| = |C|$, we conclude that the subgraph $[B, C]$ is regular. It then follows that the valency of $\Gamma_N$ is at most $k$.

(ii). Suppose that $K$ is not semiregular on $V\Gamma$. Then $K_v \neq 1$ for some vertex $v$. By Lemma 2.1, $K_v$ acts nontrivially on $\Gamma(v)$. Let $w \in \Gamma(v)$ be not fixed by $K_v$, and let $B = \{v^g \mid g \in N\}$ and $B' = \{w^g \mid g \in N\}$. Then the subgraph $[B, B']$ is regular of valency at least 2. It follows that the valency of $\Gamma_N$ is less than $k$, which is a contradiction. Thus $K_v = 1$ and $K$ is semiregular on $V\Gamma$. In particular, $K$ is regular on each of the $N$-orbits on $V\Gamma$. It then follows that $N = K$, and so $N$ is semiregular on $V\Gamma$.

For a $G$-vertex transitive graph $\Gamma$ and an intransitive normal subgroup $N \triangleleft G$, if $\Gamma$ is a cover of $\Gamma_N$ and $R \leq G/N$ is semiregular on $V\Gamma_N$, then the extension $N.R$ is semiregular on $V\Gamma$. Thus, we have the following reduction lemma for proving Conjecture 1.2.

Lemma 2.3. Conjecture 1.2 is true if and only if it is true for basic vertex transitive graphs.

3. A PROPERTY OF FINITE SIMPLE GROUPS

Recall that for a prime $p$ and a positive integer $e$, a prime divisor $r$ of $p^e - 1$ is called a primitive prime divisor if $r$ does not divide $p^i - 1$ for all $i < e$. The property regarding finite simple groups given in the following proposition is a crucial step for proving Theorem 1.1.

Proposition 3.1. For any integer $k \geq 6$, there exists an integer $n$ such that any finite simple group $T$ of order at least $n$ contains a subgroup $R$ satisfying

(i) each prime divisor of $|R|$ is greater than $k$, and

(ii) $|R| \to \infty$ if $|T| \to \infty$.

Proof. First consider $T = A_l$. It is known that for any positive integer $m$, there exists a prime $p$ such that $m \leq p < 2m$. It follows that $T$ contains an element $x$ such that $o(x) = p \geq l/2$. Hence if $l > 2k$, then the subgroup $R = \langle x \rangle$ has order coprime to all primes at most $k$, and $|R| = p \geq l/2$ goes to infinity as $|T| = l!/2$ does.

Next assume that $T$ is a group of Lie type over $GF(p^e)$. Suppose that the characteristic $p > k$. Then a Sylow $p$-subgroup $R$ of $T$ has order coprime to each prime at most $k$ such that

$|R| \to \infty$ if $|T| \to \infty$. 

Suppose that the characteristic \( p \leq k \). Assume that \( T \) is an exceptional simple group of Lie type. Then for a sufficiently large integer \( n \), if \( |T| \geq n \), then \( e > k \geq 6 \).

Consider divisors of \( p^e - 1 \). By the well-known Zsigmondy’s theorem \([7]\), \( p^e - 1 \) has a primitive prime divisor \( r \), which is at least \( e \). Let \( R \) be a Sylow \( r \)-subgroup of \( T \). Then \( |R| \) is coprime to all primes at most \( k \). Further, as \( p \leq k \), if \( |T| \) goes to infinity, then so does \( e \), and since \( |R| \geq r \geq e \), the order \( |R| \) goes to infinity.

Next consider the classical groups of Lie type of dimension \( d \). Then \( p^r - 1 \) divides \( |T| \), where

\[
e = \begin{cases} 
    d - 2, & \text{if } T = \Omega^+_d(p^e), \\
    d - 1, & \text{if } T = \PSU_d(p^e) \text{ or } \Omega_d(p^e), \\
    d, & \text{otherwise}.
\end{cases}
\]

Since \( p \leq k \), there exists a sufficiently large integer \( n \) such that if \( |T| \geq n \), then \( ce > k \geq 6 \). By the well-known Zsigmondy’s theorem, \( p^e - 1 \) has a primitive prime divisor \( r \), which satisfies \( r \geq ce \). Let \( R \) be a Sylow \( r \)-subgroup of \( T \). Then \( |R| \) is coprime to all primes at most \( k \). Moreover, as \( p \leq k \), if \( |T| \rightarrow \infty \), then \( ce \rightarrow \infty \), and so \( |R| \rightarrow \infty \). \( \square \)

4. A partial result for Conjecture \([1,2]\)

Here we treat the case where \( G \) has a large minimal normal subgroup.

**Lemma 4.1.** For any given integer \( k \geq 3 \), there is a function \( f_k \) satisfying \( f_k(n) \rightarrow \infty \) as \( n \rightarrow \infty \) such that, for each connected graph \( \Gamma \) of valency \( k \) on \( n \) vertices, if a vertex transitive subgroup \( G \leq \text{Aut}\Gamma \) has a minimal normal subgroup with at most two orbits, then \( G \) has a semiregular subgroup of order at least \( f_k(n) \).

**Proof.** Let \( \Gamma \) be a connected vertex transitive graph with \( n \) vertices of valency \( k \). Assume that \( G \leq \text{Aut}\Gamma \) is quasiprimitive or bi-quasiprimitive on \( V\Gamma \).

Let \( M \) be a minimal normal subgroup of \( G \). Then \( M \) has at most two orbits on \( V\Gamma \). Suppose first that \( M \) is nonabelian; that is, \( M = T^m \) with \( T \) nonabelian simple and \( m \geq 1 \). By Proposition \([3,1]\) \( T \) has a large subgroup \( R \) whose order is indivisible by any prime at most \( k \), and \( |R| \) goes to infinity as \( |T| \) does. Since \( \Gamma \) is of valency \( k \), by Lemma \([2,1]\) each prime divisor of \( |G_v| \) is at most \( k \), and hence \( R \cap G_v = 1 \). Thus \( R^m \leq M \) is semiregular on \( V\Gamma \). Noting that \( n \leq 2|T|^m \), we conclude that \( f_k(n) := |R|^m \) goes to infinity as \( n \) does.

Suppose now that \( M \) is abelian. If \( M \) is transitive, then \( M \) is regular, and we have nothing further to do. Suppose that \( M \) has exactly two orbits in \( V\Gamma \). Then \( V\Gamma \) is divided into two parts \( \Delta_1 \) and \( \Delta_2 \) as \( M \)-orbits. Let \( G^+ = G_{\Delta_1} = G_{\Delta_2} \). Then \( M \triangleleft G^+ \). If \( M \) is faithful on \( \Delta_1 \), then \( M \) is also faithful on \( \Delta_2 \), so \( M \) is faithful and semiregular on \( V\Gamma \). Then \( f_k(n) := |M| = n/2 \) goes to infinity as \( n \rightarrow \infty \). Suppose that \( M \) is not faithful on \( \Delta_i \) where \( i = 1 \) or \( 2 \). Let \( K_i \) be the kernel of \( M \) acting on \( \Delta_i \). Since \( G \) is transitive on \( V\Gamma \), there exists \( g \in G \) such that \( g \) interchanges \( \Delta_1 \) and \( \Delta_2 \), and thus \( K^g = K_2 \). In particular, \( K_1 \cong K_2 \) and \( K_1 \times K_2 \leq G \), and so \( M = K_1 \times K_2 \). It follows that \( K_i \) is faithful and regular on \( \Delta_{3-i} \). Let \( R = \{(x, x^g) \mid x \in K_1\} < M \). Then \( R \) is semiregular on \( V\Gamma \), and \( |R|^2 = |M| \). It follows that \( |R| = |\Delta_1| = |V\Gamma|/2 = n/2 \). Now \( f_k(n) := |R| \) goes to infinity as \( n \) goes to infinity. \( \square \)

Then the following corollary confirms Conjecture \([1,2]\) in the quasiprimitive case and the bi-quasiprimitive case.
Corollary 4.2. For any given integer $k \geq 3$, there is a function $f_k$ satisfying $f_k(n) \to \infty$ as $n \to \infty$ such that each connected quasiprimitive and bi-quasiprimitive graph of valency $k$ on $n$ vertices has a semiregular automorphism subgroup of order at least $f_k(n)$.

5. Proof of Theorem 1.1

By Lemma 2.3 we only need to consider basic graphs. Thus let $Γ$ be a basic $G$-vertex transitive cubic graph with $n$ vertices. By Lemma 1.1 we may further assume that each minimal normal subgroup of $G$ has at least three orbits on $VΓ$.

Let $M$ be a minimal normal subgroup of $G$. Then the normal quotient graph $Γ_M$ has valency 2; that is, $Γ_M = C_l$ with $l ≥ 3$. By Lemma 2.1 for a vertex $v$, the stabiliser $G_v$ is a $(2, 3)$-group. Suppose that $|G_v|$ is divisible by 3. Then by Lemma 2.1 $|G_v^{Γ(v)}|$ is divisible by 3, and $1 ≠ M_v^{Γ(v)} \triangleleft G_v^{Γ(v)}$. Hence $M_v^{Γ(v)}$ is transitive, and it follows that $Γ_M$ has valency 1, which is a contradiction. So $G_v$ is a 2-group. Let $B$ be the set of $M$-orbits in $VΓ$, and let $K$ be the kernel of $G$ acting on $B$. Since $G$ is vertex transitive on $Γ$, the factor group $G/K ≤ \text{Aut}Γ$ is vertex transitive on the quotient graph $Γ_M$, and so $G/K ≅ \mathbb{Z}_l$ or $D_{2l}$. In particular, $K = MK_v$, and hence $K/M$ is a 2-group.

Write $M = T^m$, with $T$ simple and $m ≥ 1$. Suppose that $G$ has another minimal normal subgroup $N ≠ M$. Let $L$ be the kernel of $G$ acting on the set of $N$-orbits on $VΓ$. Since $L \cap M$ is normal and $M$ is minimal normal, we have either $M \cap L = M$, or $M \cap L = 1$. In the first case, we have that $M ≤ L$, $M \cap N = 1$, and $L = NL_v$. Thus $M = M/(M \cap N) ≅ MN/N ≤ L/N ≅ L_v/N_v$, a 2-group. In the latter case, $M$ is isomorphic to a subgroup of $G/L$ which is dihedral or cyclic, and hence $M ≅ \mathbb{Z}_p$ with $p$ an odd prime. Therefore, one of the following three cases occurs:

(i) $M$ is the only minimal normal subgroup of $G$;
(ii) $M ≅ \mathbb{Z}_2^m$;
(iii) $M = \mathbb{Z}_p$, where $p$ is an odd prime.

Case (i). Assume that $M$ is the only minimal normal subgroup of $G$. Assume further that $T$ is nonabelian. Then by Proposition 3.1 $T$ has a large subgroup $R$ of order prime to 6, and so $R^m$ fixes no vertex of $Γ$, such that $|T|$ goes to infinity, so does $|R|$. Since $M$ is the only minimal normal subgroup of $G$, we have that $G ≤ \text{Aut}(M) = \text{Aut}(T) ≤ S_m$ and so $|G| ≤ |\text{Aut}(T)|^m m!$. Moreover, since $G$ is transitive, $n ≤ |G| ≤ |\text{Aut}(T)|^m m!$. Hence the order of the semiregular subgroup $R$ satisfies that $f(n) := |R|^m$ goes to infinity as $n → \infty$.

Suppose now that $M = \mathbb{Z}_p^m$, where $p$ is a prime. The case where $p = 2$ will be treated in Case (ii). Here we assume that $p$ is odd. Then $M$ is semiregular, and $G ≤ \text{AGL}(p, m)$. Since $n \mid |G|$, as $n$ goes to infinity, the order $|\text{AGL}(p, m)|$ does, and hence $|M| = p^m$ goes to infinity too. So the semiregular subgroup $M$ has order such that $f(n) := |M| → \infty$ as $n → \infty$.

Case (ii). Assume that $M = \mathbb{Z}_2^m$. Let $N = O_2(G)$, the largest normal 2-subgroup of $G$. Since $K = MK_v$ and $K_v < G_v$ is a 2-group, we conclude that both $M$ and $K$ are normal in $N$.

Claim 1. $M ≤ \mathbb{Z}(N)$, the center of $N$.

Since $M$ is a minimal normal subgroup and $\mathbb{Z}(N)$ is normal in $G$, we have that $M \cap \mathbb{Z}(N) = 1$ or $M$. Considering $M$ as a vector space over $GF(2)$, $N$ acts by
conjugation on $M$ as a 2-group of linear transformations and so it has a nontrivial fixed vector $x \in M$. This means $1 \neq x \in M \cap Z(N)$, and hence $M \cap Z(N) = M$.

Claim 2. $M$ is semiregular on $V\Gamma$, and $K = M$.

Fix $v \in V\Gamma$ and let $B$ be the $M$-orbit containing $v$. The restriction of $M$ to any $M$-orbit is transitive and abelian, so it is regular. Hence $M_v$ fixes $B$ pointwise. There are exactly two $M$-orbits, call them $B'$ and $B''$, that are connected to $B$ in $\Gamma_M$. Since $v$ is connected to exactly one vertex $w' \in B'$ and one vertex $w'' \in B''$, the group $M_v$ must fix $w'$ and $w''$ and so it must fix $B'$ and $B''$ pointwise. Continuing this argument, we see that $M_v$ fixes pointwise the $M$-orbits connected to $B'$ and $B''$ in $\Gamma_M$ and since $\Gamma$ is connected, eventually we obtain that $M_v = 1$.

By Claim 1, $M$ centralizes $K$. Since a transitive abelian permutation group is self-centralizing, it follows that the restriction of $K$ to each $M$-orbit is the same as the restriction of $M$. In particular, $K|_B = M|_B$. Hence $K_v$ fixes $B$ pointwise, and arguing as for $M$, we obtain $K_v = 1$. Since $K \geq M$ and $M$ is transitive on $B$, it follows that $K = M$.

Claim 3. For $y \in G$ whose image in $G/K$ has order $l$, $\langle y \rangle$ is semiregular on $V\Gamma$.

Now $y^l \in K = M$. If $y^l = 1$, then every cycle in $y$ has length $l$ and $\langle y \rangle$ is semiregular. If $y^l \neq 1$, then $o(y) = 2l$, and by Claim 2 every cycle in $y^l$ has length 2, so every cycle in $y$ has order $2l$ and $\langle y \rangle$ is semiregular.

Finally, the group $\langle M, y \rangle$ is transitive, and so $|M|o(y) \geq n$. By Claims 2 and 3, either $M$ or $\langle y \rangle$ is a semiregular subgroup of order at least $\sqrt{n}$.

Case (iii). Assume that every minimal normal subgroup of $G$ is cyclic of odd order. Let $S$ be the socle of $G$, the product of all minimal normal subgroups of $G$. Then $S = \mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2} \times \cdots \times \mathbb{Z}_{p_l}$, where $p_1, p_2, \ldots, p_l$ are primes. Since $S$ is the socle of $G$, it follows that $G \leq \langle \mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2} \times \cdots \times \mathbb{Z}_{p_1} \rangle$. Hence we have that $n \leq |G| < |S|^2$. Since $G_v$ is a 2-group and $S$ has odd order, $S$ is semiregular, whose order goes to infinity as $n$ does.

\[ \square \]

REFERENCES


Department of Mathematics, Yunnan University, Kunming 650031, People’s Republic of China; and School of Mathematics and Statistics, The University of Western Australia, Crawley 6009, WA, Australia

E-mail address: li10maths.uwa.edu.au