THE CYCLOMATIC NUMBER OF CONNECTED GRAPHS WITHOUT SOLVABLE ORBITS

GYULA KÁROLYI[1] Department of Algebra and Number Theory, Eötvös University, Pázmány Péter sétány 1/C, H–1117 Budapest, Hungary

AMBRUS PÁL Department of Mathematics, Imperial College London, London SW7 2AZ, United Kingdom

ABSTRACT. A graph is without solvable orbits if its group of automorphisms acts on each of its orbits through a non-solvable quotient. We prove that there is a connected graph without solvable orbits of cyclomatic number c if and only if c is equal to 6, 8, 10, 11, 15, 16, 19, 20, 21, 22, or is at least 24, and briefly discuss the geometric consequences.

1. INTRODUCTION

Throughout this paper, by a graph we always mean a finite undirected graph with or without loops and multiple edges. For such a graph G let $\mathcal{V}(G)$ and $\mathcal{E}(G)$ denote its set of vertices and edges, respectively. An automorphism of G is a pair (π_1, π_2) where π_1, π_2 is a permutation of $\mathcal{V}(G)$ and $\mathcal{E}(G)$, respectively such that a vertex $v \in \mathcal{V}(G)$ is incident to an edge $e \in \mathcal{E}(G)$ if and only if $\pi_1(v)$ is incident to $\pi_2(e)$. If G is a simple graph, then π_1 uniquely determines π_2. The set of automorphisms of G forms a group with respect to composition which is denoted

[1]Visiting I.H.É.S. Research partially supported by Hungarian Scientific Research Grants OTKA T043631 and NK67867.

by $\mathrm{Aut}(G)$. We say that G is without solvable orbits if $\mathrm{Aut}(G)$ acts on the orbit of any vertex in $\mathcal{V}(G)$ and any edge in $\mathcal{E}(G)$ through a non-solvable quotient. A group Γ acts on a graph G if a homomorphism $\Gamma \to \mathrm{Aut}(G)$ is given. We say that Γ acts on G without solvable orbits if Γ acts on the orbit of any vertex in $\mathcal{V}(G)$ and any edge in $\mathcal{E}(G)$ through a non-solvable quotient. In that case each orbit of $\mathrm{Aut}(G)$ splits up into orbits of Γ and thus G is without solvable orbits, see [7], Lemma 3.2.

We define the cyclomatic number of a connected graph G as the alternating sum $c(G) = 1 - |\mathcal{V}(G)| + |\mathcal{E}(G)|$ (in the general case the term 1 must be replaced with the number of connected components of G). Thus, $1 - c(G)$ is the Euler characteristic of the graph G, viewed as a CW-complex. The topological invariant $c(G)$ equals the arithmetic genus of each projective algebraic curve with ordinary double points, defined over an algebraically closed field, whose incidence graph is isomorphic to G and whose irreducible components are all rational curves. The relevance of connected graphs without solvable orbits in arithmetic geometry has been made apparent by the second author in [7]: in the above context they yield to constructions of curves without solvable points. A more precise statement is given at the end of this paper. A principal motivation for the present work has been to explore the limitations of that method.

Theorem 1.1. *There is a connected graph without solvable orbits of cyclomatic number c if and only if c is equal to 6, 8, 10, 11, 15, 16, 19, 20, 21, 22, or is at least 24. The same holds for stable graphs.*

A graph G is stable, if it is connected and the degree of any vertex in $\mathcal{V}(G)$ is at least 3. In Proposition 3.4 of [7] it was proved that there is a stable graph without solvable orbits of cyclomatic number c for every natural number c listed above except for c equal to 19, 24, 33 and 39. It was pointed out by J. Jahnel that even the last three numbers can be represented as the cyclomatic number of certain stable graphs constructed therein. Thus one novelty here is a construction for the case $c = 19$.

In the paper quoted above it was also shown (Proposition 3.5) that there is no connected graph without solvable orbits of cyclomatic number less then 10 and different from 6 or 8. The main theme of the present paper is to show that there is no connected graph without solvable orbits in the remaining cases, that is, when c is 12, 13, 14, 17, 18 or 23.

We organize this paper as follows. In the next section we present the constructions that prove the 'if' part of Theorem 1.1. In Section 3 we review some tools from group theory. This is followed by a collection of simple observations that we will use frequently throughout the rest of the paper. In Section 5 we prove the solvability of the automorphism group of certain regular graphs. In Section 6 we show how to reduce connected graphs without solvable orbits to stable simple graphs with the same property, and study what happens to the orbits and the cyclomatic number of the graph during such a reduction process. This allows us to split up the proof of the more essential part of Theorem 1.1 into two lemmas that we prove in Sections 7 and 8, respectively. In the last section we briefly discuss the geometric implications.

2. Constructions

To prove the 'if' part of Theorem 1.1, for the sake of completeness we briefly recall the constructions from [7]. For integers $n \geq 5$, $x \geq 0$, let $K_n(x)$ denote the complete graph K_n with x loops attached to each of its n vertices. The symmetric group S_n acts on $K_n(x)$ without solvable orbits. The numbers 6, 11, 16 and 21 arise as the cyclomatic number of the graphs $K_5(x)$ for $x = 0, 1, 2$ and 3, whereas the graphs $K_6(0)$, $K_6(3)$ and $K_6(4)$ have cyclomatic number 10, 28 and 34, respectively.

For integers $n, m \geq 5$, $x, y \geq 0$, let $K_{n,m}(x, y)$ denote the complete bipartite graph $K_{n,m}$ with x loops attached to each of its n vertices in the first colour class and with y loops attached to each of its m vertices in the second colour class. The group $\mathrm{S}_n \times \mathrm{S}_m$ acts on $K_{n,m}(x, y)$ without solvable orbits. The numbers 20, 25, 26, 30, 31, 32, 35, 36, 37, 38 as well as every integer ≥ 40 can be represented as $c(K_{5,6}(x, y))$, for suitable values of x and y.

For a prime power q and a natural number x we define the graph $P_q(x)$ as follows. Its vertices are the points p and the lines ℓ of the projective plane of order q, $p\ell$ is an edge of the graph if and only if the point p is incident to ℓ, and moreover x loops are attached to each vertex p corresponding to a point on the projective plane. The group $\mathrm{PGL}_3(q)$, as well as the group $\mathrm{PSL}_3(q)$, acts on $P_q(x)$ without solvable orbits, and the graphs $P_2(0), P_2(1), P_2(2), P_2(3)$ and $P_3(0)$ have cyclomatic number 8, 15, 22, 29 and 27, respectively.

So far we have covered all the possible values of c except of 19, 24, 33 and 39. The last three cases can be handled by the bipartite construction: $c(K_{5,7}(0,0)) = 24$, $c(K_{5,8}(1,0)) = 33$ and $c(K_{5,7}(3,0)) = 39$. Our new construction for $c = 19$ goes as follows.

For an integer $n \geq 5$ we define the graph $K'_{n,n}$ as follows. Its vertices are $1, 2, \dots, 2n$. For $1 \leq i \leq n$ and $n+1 \leq j \leq 2n$ we connect i and j by an edge ij if and only if $j - i \neq n$. Thus, $K'_{n,n}$ is obtained by removing a 1-factor from the complete graph $K_{n,n}$. It is clearly stable, and its cyclomatic number is $c(K'_{n,n}) = n(n-3)+1$.

The symmetric group S_n acts on $K'_{n,n}$ as follows. If $\pi \in \mathrm{S}_n$ is a permutation, that is, a bijective function $\pi : \{1, 2, \dots, n\} \to \{1, 2, \dots, n\}$, we extend it to an automorphism $\widetilde{\pi} \in \mathrm{Aut}(K'_{n,n})$ by putting $\widetilde{\pi}(j) = \pi(j-n)+n$ for any $n+1 \leq j \leq 2n$. The vertex set splits up into two orbits $\{1, 2, \dots, n\}$ and $\{n+1, n+2, \dots, 2n\}$ under this action, whereas the action on the edge set is transitive. The action is clearly faithful on each of the three orbits, and therefore S_n acts on $K'_{n,n}$ without solvable orbits.

In particular, $K'_{6,6}$ is a stable graph without solvable orbits of cyclomatic number 19.

3. Solvable groups

The proof of the 'only if' part of Theorem 1.1 heavily depends on the solvability of groups of certain cardinality. First we recall the following well-known result, see e.g. [3], pages 221–222.

Theorem 3.1. *(Burnside) Let p, q denote primes, α, β nonnegative integers. Then every group of order $p^\alpha q^\beta$ is solvable.*

To go one step further we will use a rather deep result from the theory of finite simple groups. A minimal simple group is a simple group of composite order all of whose proper subgroups are solvable.

Theorem 3.2. *(Thompson [10]) Every minimal simple group is isomorphic to one of the following minimal simple groups:*

(i) *the projective special linear groups* $\mathrm{PSL}_2(2^p)$, *p any prime;*
(ii) $\mathrm{PSL}_2(3^p)$, *p any odd prime;*

(iii) $\mathrm{PSL}_2(p)$, *p any prime exceeding 3 such that* $p^2+1 \equiv 0 \pmod 5$*;*
(iv) *the Suzuki groups* $\mathrm{Sz}(2^p)$ *(also denoted by* ${}^2\mathrm{B}_2(2^p)$*), p any odd prime;*
(v) $\mathrm{PSL}_3(3)$.

Corollary 3.3. *Let α, β denote positive integers. Then every group whose order is $2^\alpha 3^\beta 11$ or $2^\alpha 3p$, where p is either 13 or 17, is solvable.*

Note that there exist minimal simple groups whose order is $2^\alpha 3^\beta p$ for $p = 13$ and $p = 17$: namely $|\mathrm{PSL}_3(3)| = 2^4 3^3 13$ and $|\mathrm{PSL}_2(17)| = 2^4 3^2 17$.

Proof. If a finite group is not solvable, then it has a non-abelian simple composition factor. Either it is a minimal simple group, or has a nonsolvable subgroup. Iterating this procedure, because of finiteness we eventually obtain a minimal simple group whose order divides that of the original group. It suffices to prove that no minimal simple group has an order in the form $2^\alpha 3^\beta 11$ or $2^\alpha 3p$, where p is either 13 or 17. As we have already seen, this is true for $\mathrm{PSL}_3(3)$.

The order of $\mathrm{PSL}_2(2^p)$ is $2^p(2^p-1)(2^p+1)$. The three factors involved therein are pairwise coprime integers ≥ 2, and none of them is equal to either 11, 13 or 17, if p is any prime, hence the claim.

The order of $\mathrm{PSL}_2(3^p)$ is $3^p(3^p-1)(3^p+1)/2$. Note that $(3^p-1, 3^p+1) = 2$. It is not possible that one of 3^p-1 and 3^p+1 is a power of 2, whereas the other is $2 \cdot 11$, $2 \cdot 13$ or $2 \cdot 17$.

The order of $\mathrm{PSL}_2(p)$ is $p(p-1)(p+1)/2$. It is not possible that one of $p-1$ and $p+1$ is a power of 2, whereas the other is $2 \cdot 11$, $2 \cdot 13$ or $2 \cdot 17$. Thus, in a hypothetical counterexample, p must be $11, 13$ or 17, whereas one of $p-1$ and $p+1$ is a power of 2, and the other is twice a power of 3. This is only possible when $p = 17$, but then $|\mathrm{PSL}_2(17)| = 2^4 3^2 17$.

Finally, the order of $\mathrm{Sz}(2^p)$ is $2^{2p}(2^{2p}+1)(2^p-1)$. The odd factors are again coprime integers ≥ 2, and none of them is equal to either 11, 13 or 17 when p is an odd prime. □

Note that one can derive Corollary 3.3 directly from Wales's classification [11] of the simple groups of order $2^\alpha 3^\beta p$, see [12, 13] for the particular cases $p = 17$ and $p = 13$, respectively. Since these results also depend on Thompson's theorem, we preferred the more direct approach.

Assume that the simple graph G has connected components $H_1, H_2, \ldots, H_m$, all isomorphic to a given simple connected graph H. $\mathrm{Aut}(H)$ can be understood as a permutation group acting on $\mathcal{V}(H)$. Then $\mathrm{Aut}(G) = \mathrm{Aut}(H) \wr \mathrm{S}_m$, see [1]. Here we use the terminology of [8] for wreath products. Consequently, $|\mathrm{Aut}(G)| = |\mathrm{Aut}(H)|^m \cdot m!$. In particular, if $m \leq 4$, and the only primes that divide $|\mathrm{Aut}(H)|$ are 2 and 3, then the order of $\mathrm{Aut}(G)$ is of the form $2^\alpha 3^\beta$, and thus it is solvable by Burnside's theorem. This will apply to every wreath product that occurs in this paper.

4. Preliminary lemmas

Throughout this section we assume that a group Γ acts on the graph G, and by an orbit we always mean an orbit under this specific action. Let G be a simple graph, and let $\overline{G}$ denote its complement, then $\mathrm{Aut}(G) \cong \mathrm{Aut}(\overline{G})$ and in general, the action of Γ on G induces in a natural way an action of Γ on $\overline{G}$ such that the two actions coincide on $\mathcal{V}(G) = \mathcal{V}(\overline{G})$.

Claim 4.1. *Γ acts on G without solvable orbits if and only if Γ acts on $\overline{G}$ without solvable orbits.*

We say that Γ acts on a set X without solvable orbits if Γ acts on every orbit in X through a non-solvable quotient. The above claim is an immediate consequence of the following

Lemma 4.2. *If Γ acts on $\mathcal{V}(G)$ without solvable orbits, then it also acts on $\mathcal{E}(G)$ without solvable orbits.*

Proof. Assume that the claim is false and let E be an orbit of edges on which Γ acts through a solvable quotient Δ. Let H be the subgraph of G whose edge set is E and whose vertices are the endpoints of the edges in E. Then Γ leaves the subgraph H invariant. Every automorphism in Γ which fixes the edges of H but not all vertices of H must interchange the endpoints of some of the edges in E. In particular it acts as an involution on H. Therefore Γ acts on H through a quotient Ξ which is the extension of Δ by an elementary abelian 2-group. Accordingly, Ξ is solvable, and Γ acts on $\mathcal{V}(H)$ through a solvable quotient, which is a contradiction. $\square$

In the sequel let G denote a connected graph, not necessarily simple. For every vertex $v \in \mathcal{V}(G)$ let $O(v)$ denote the orbit of v with respect to the action of Γ. For any orbit $V = O(v)$, all vertices in V have the same degree, so we can define the degree of the orbit as $d(V) = \deg(v)$.

Lemma 4.3. *Assume that the prime p divides the cardinality of a vertex orbit V and $p > d(U)$ for every vertex orbit $U \neq V$. Then p divides the size of each vertex orbit.*

Proof. Let U be any orbit which has a vertex adjacent to a vertex in V. The number of edges connecting a vertex in V to vertices in U is the same because the action of Γ is transitive on V, and similarly the number of edges connecting a vertex in U to vertices in V is the same. The latter number is not divisible by p. Double-counting the edges between V and U we find that the cardinality of U must be divisible by p. Since G is connected, this implies that the cardinality of each orbit is divisible by p. $\square$

We will also use frequently the following variant, that can be proved along the same lines. Let U and V be two vertex orbits and assume that $e = uv \in \mathcal{E}(G)$ for some $u \in U, v \in V$. Then each edge in the orbit of e connects a vertex in U to a vertex in V. Thus we may say that U and V are connected by an edge orbit E, and double counting as above gives the following

Lemma 4.4. *Assume that the vertex orbits U and V are connected by an edge orbit E. Then each vertex in U is incident to the same number of edges in E, and this number is a positive integer multiple of $|V|/(|U|, |V|)$.*

Suppose that the vertex set of the connected graph G splits up into $t \geq 2$ orbits $V_1, V_2, \dots, V_t$ of cardinality $n_1, n_2, \dots, n_t$, respectively, a fact we denote by $\mathcal{V}[n_1, n_2, \dots, n_t]$. It follows that

Corollary 4.5. *For any $1 \leq i \leq t$ we have*

$$d(V_i) \geq \min_{j \neq i} \frac{n_j}{(n_i, n_j)}.$$

Looking at the connections of orbits of the same given cardinality with the rest of the graph, we obtain the following variant.

Corollary 4.6. *Assume that $n_1, n_2, \dots, n_t$ are not equal to the same number. For any $n \in \{n_1, n_2, \dots, n_t\}$, there is an index $1 \leq i \leq t$ such that $n_i = n$, and*

$$d(V_i) \geq \min_{n_j \neq n} \frac{n_j}{(n, n_j)}.$$

Denote the maximum degree of the graph G by $\delta(G)$. Suppose that the edge orbit E is incident to the vertex orbit V. Each vertex in V is incident to the same number of edges in E, say δ of them. If one edge in E is incident to only one vertex in V, then so is each edge in E, and thus $|E| = \delta|V|$. If on the other hand each edge in E connects two vertices in V then $|E| = \delta|V|/2$. Since in a connected graph each vertex orbit is incident to some edge orbit and vice versa, we have:

Proposition 4.7. *Let G be a connected graph. If there is a vertex orbit whose cardinality is divisible by the odd prime p, then there is also an edge orbit with the same property. If p divides the cardinality of each vertex orbit, then it also divides the cardinality of each edge orbit. If $p > \delta(G)$ divides the cardinality of an edge orbit, then there is also a vertex orbit whose cardinality is divisible by p. If G has an edge orbit whose cardinality is a power of 2, then it also has a vertex orbit with the same property.*

In a stable simple graph G without solvable orbits, let r_d denote the number of vertices of degree d, thus $r_1 = r_2 = 0$. Note that every permutation group of degree ≤ 4 is solvable. Since $\mathrm{Aut}(G)$, and thus also Γ leaves the set of vertices of degree d invariant for each positive d, the set of vertices of the same degree splits up into complete vertex orbits. In view of all this we have:

Proposition 4.8. *In a stable simple graph G equipped with an action of Γ without solvable orbits, every orbit of Γ (vertex and edge alike) has a cardinality ≥ 5. Moreover, $r_d \geq 5$ for each d such that r_d is non-zero, and the cyclomatic number of G can be written as*

$$c(G) = 1 + \sum_{d \geq 3} \Big(\frac{d}{2} - 1\Big) r_d.$$

In particular, $c(G) \geq 4$.

Pick a vertex $v \in \mathcal{V}(G)$ and let X_i be the set of vertices connected to v by a path of length at most i. In particular, $X_0 = \{v\}$. The action of Γ on G is given by a homomorphism $\varphi : \Gamma \to \mathrm{Aut}(G)$. Introduce $\widetilde{\Gamma} = \varphi(\Gamma) \leq \mathrm{Aut}(G)$, and let Γ_i be the stabilizer of X_i in $\widetilde{\Gamma}$. Clearly the factor set $\widetilde{\Gamma}/\Gamma_0$ can be identified with the orbit of v and Γ_{i+1} is a normal subgroup in Γ_i, and also in Γ_0, but note that the latter is not necessarily a normal subgroup in $\widetilde{\Gamma}$. Since G is connected, the group Γ_i is trivial for a sufficiently large i, and we have

Proposition 4.9. $|\widetilde{\Gamma}| = |O(v)| \prod |\Gamma_i : \Gamma_{i+1}|$.

The quotient group Γ_i/Γ_{i+1} acts faithfully on the set of edges connecting vertices in $X_{i+1} \setminus X_i$ to vertices in X_i. Here $|X_0| = 1$ and $|X_1 \setminus X_0| = \deg(v)$. Therefore Γ_0/Γ_1 is isomorphic to a subgroup of $\mathrm{S}_{\deg(v)}$. For an $i \geq 1$, let $u_1, u_2, \ldots, u_k$ denote the elements of $X_i \setminus X_{i-1}$. Each vertex u_j is connected by at most $\deg(u_j) - 1$ edges to vertices in $X_{i+1} \setminus X_i$, which are permuted among themselves under the action of Γ_i/Γ_{i+1}. Consequently, Γ_i/Γ_{i+1} can be embedded into

$$\mathrm{S}_{\deg(u_1)-1} \times \mathrm{S}_{\deg(u_2)-1} \times \ldots \times \mathrm{S}_{\deg(u_k)-1},$$

and in turn also into a direct power of $\mathrm{S}_{\delta(G)-1}$. We will frequently refer to this argument. The following consequences will be particularly useful.

Lemma 4.10. *Let G be a stable simple graph.*

(i) *If $\delta(G) \leq 5$ and G has a vertex v of degree 3 or 4 such that $|O(v)| = 2^a 3^b$ for some nonnegative integers a, b, then $\widetilde{\Gamma}$ is solvable.*

(ii) *If $\delta(G) \leq 5$ and either r_3 or r_4 is of the form $2^a 3^b$ for some nonnegative integers a, b, then $\widetilde{\Gamma}$ is solvable.*

Proof. The first statement follows from the fact that the cardinality of each quotient Γ_i/Γ_{i+1} can be written in the form $2^\alpha 3^\beta$ with suitable nonnegative integers α, β. In view of Proposition 4.9, the same holds for the order of $\widetilde{\Gamma}$, hence it is solvable by Burnside's theorem.

To prove the second statement, assume that $r_i = 2^a 3^b$ for some $i \in \{3, 4\}$. Were there a vertex orbit V with $d(V) = i$ such that $|V|$ is divisible by a prime $p > 5$, Lemma 4.3 would imply that p divides the cardinality of each vertex orbit of degree i, and thus also r_i, a contradiction. Since r_i is not divisible by 5, there must be a vertex v of degree i such that $|O(v)|$ is not divisible by 5 either, and thus the statement follows from (i). $\square$

Lemma 4.11. *Let G be a stable simple graph.*

(i) *If $\delta(G) \leq 5$ and either r_3 or r_4 is equal to p, $2p$ or $4p$ for some prime number $p > 5$, then there exist nonnegative integers α, β, such that $|\widetilde{\Gamma}|$ divides $2^\alpha 3^\beta p$.*

(ii) *If $\delta(G) = 3$ and $|\mathcal{V}(G)| = r_3 = 2^a p$ for some $a \in \{0, 1, 2\}$ and a prime $p > 5$, then there exists a nonnegative integer α such that $|\widetilde{\Gamma}|$ divides $2^\alpha 3p$.*

Proof. To prove the first statement, assume that $r_i = 2^a p$ for some $i \in \{3,4\}$ and $a \in \{0,1,2\}$. Were there a vertex orbit V with $d(V) = i$ such that $|V|$ is divisible by a prime $q > 5$, $q \neq p$, Lemma 4.3 would imply that q divides the cardinality of each vertex orbit of degree i, and thus also r_i, a contradiction. If there is a vertex orbit V with $d(V) = i$ such that the only primes that divide $|V|$ are 2 and 3, we find that the order of $\widetilde{\Gamma}$ is of the form $2^\alpha 3^\beta$ (see the previous proof).

Hence we may also assume that the cardinality of each vertex orbit V with $d(V) = i$ is divisible by either 5 or p. Since not all of them can be a multiple of 5, there is one such orbit whose cardinality is divisible by p. It follows from Lemma 4.3 that the cardinality of each vertex orbit is divisible by p. If there is a vertex v of degree i such that $|O(v)| = 3p$, then it must be $a = 2$, and then the remaining vertices of degree i form an orbit of cardinality p. In any case we find a vertex v of degree i such that $|O(v)| = 2^b p$. Each Γ_i/Γ_{i+1} (including the case $i = 0$) can be embedded into a direct power of S_4, and the result follows form Proposition 4.9.

In case (ii) a similar argument gives that there is a nonnegative integer b and a vertex v such that $|O(v)| \in \{2^b, 2^b p\}$. This time the order of Γ_0/Γ_1 divides $|\mathrm{S}_3| = 6$, and $|\Gamma_i/\Gamma_{i+1}|$ is a power of 2 for every $i \geq 1$, hence the result. □

5. Regular graphs

For every pair of integers $n \geq 4$ and $1 < k \leq n/2$ we define a graph $G = C_n(k)$ as follows. Let $\mathcal{V}(G) = \mathbb{Z}/n\mathbb{Z}$. For $i, j \in \mathbb{Z}/n\mathbb{Z}$ let $ij \in \mathcal{E}(G)$ if and only if either $i - j = \pm 1$ or $i - j = \pm k$. Edges of the first kind form a cycle of length n. Edges of the second kind will be referred to as edges of length k, they form an n-cycle if and only if k is coprime to n, which is always the case if n is a prime number.

The graphs $C_n(k)$ are vertex-transitive circulant graphs, in fact they are Cayley graphs on $\mathbb{Z}/n\mathbb{Z}$. It is well-known, that for n odd, the only simple eigenvalue of such a graph G is the valency of G, see [2, 9]. It is easy to determine the spectrum of $C_n(k)$, when n is a prime.

Lemma 5.1. *Let $G = C_p(k)$, where p is a prime greater than 3, and $1 < k < p/2$. The unique simple eigenvalue of G is 4. Apart from this, every eigenvalue of G has a multiplicity 2, unless $k^2 \equiv -1 \pmod p$, in which case every non-simple eigenvalue has a multiplicity 4.*

Proof. The adjacency matrix of G is the circulant 0–1 matrix whose first row is $[a_0, a_1, a_2, \dots, a_{p-1}]$, where $a_i = 1$ if and only if $i \in \{1, k, p-k, p-1\}$. Accordingly, the eigenvalues of A are

$$\lambda_i = \varepsilon^i + \varepsilon^{ki} + \varepsilon^{(p-k)i} + \varepsilon^{(p-1)i} \qquad (i = 0, 1, \dots, p-1),$$

where $\varepsilon = e^{2\pi i/p}$ is a primitive pth root of unity, see eg. [2]. Thus, $\lambda_0 = 4$, otherwise each of the pairwise different four summands of λ_i is one of $\varepsilon, \varepsilon^2, \dots, \varepsilon^{p-1}$. Since these $p-1$ numbers constitute a basis for the extension $\mathbb{Q}(\varepsilon)|\mathbb{Q}$, a coincidence $\lambda_i = \lambda_j$ for $0 < i, j < p$ can only occur if

$$\{\varepsilon^i, \varepsilon^{ki}, \varepsilon^{-ki}, \varepsilon^{-i}\} = \{\varepsilon^j, \varepsilon^{kj}, \varepsilon^{-kj}, \varepsilon^{-j}\}.$$

Here $\varepsilon^j = \varepsilon^i$ if and only if $j = i$, whereas $\varepsilon^j = \varepsilon^{-i}$ implies $j = p - i$, and in fact $\lambda_{p-i} = \lambda_i$. Moreover $\varepsilon^j = \varepsilon^{ki}$ if and only if $j \equiv ki \pmod{p}$. In this case $\varepsilon^{-j} = \varepsilon^{-ki}$, so $\lambda_j = \lambda_i$ if and only if $\{\varepsilon^i, \varepsilon^{-i}\} = \{\varepsilon^{kj}, \varepsilon^{-kj}\}$. Were $\varepsilon^i = \varepsilon^{kj}$, it would imply $\varepsilon^i = \varepsilon^{k^2 i}$, that is, $k^2 \equiv 1 \pmod{p}$, a contradiction. Thus it must be that $\varepsilon^{-i} = \varepsilon^{kj}$, which implies $\varepsilon^i = \varepsilon^{-kj}$, and also $k^2 \equiv -1 \pmod{p}$. Note that such an integer k exists if and only if $p \equiv 1 \pmod{4}$, and then there is exactly one such k satisfying $2 \le k \le p/2$. Conversely, if $k^2 \equiv -1 \pmod{p}$ and $j \equiv ki \pmod{p}$, then $\varepsilon^j = \varepsilon^{ki}$ and $\varepsilon^{-i} = \varepsilon^{kj}$, therefore $\lambda_j = \lambda_i$. A similar argument shows that $\varepsilon^j = \varepsilon^{-ki}$ if and only if $j \equiv -ki \pmod{p}$, and if this is the case then again $\lambda_j = \lambda_i$ is equivalent with the condition $k^2 \equiv -1 \pmod{p}$.

In summary, if $k^2 \not\equiv -1 \pmod{p}$, then $\lambda_j = \lambda_i$ if and only if $j = i$ or $j \equiv -i$, and if $k^2 \equiv -1 \pmod{p}$, then $\lambda_j = \lambda_i$ if and only if $j = i$, $j \equiv -i$, $j \equiv ki$ or $j \equiv -ki$, and all this four cases are pairwise different. Thus the assertion is proved. □

Let $m_0 \le m_1 \le \dots \le m_t$ be the eigenvalue multiplicities of the graph $G = C_p(k)$. Thus, if $k^2 \not\equiv -1 \pmod{p}$, then $t = (p-1)/2$, $m_0 = 1$ and $m_1 = m_2 = \dots = m_t = 2$. Accordingly, $\mathrm{Aut}(G)$ is a subgroup of $O(1) \times O(2) \times \dots \times O(2)$, hence solvable, since $O(1) \cong \mathbb{Z}/2\mathbb{Z}$, and the only finite subgroups of the orthogonal group $O(2)$ are either cyclic or dihedral. For more details, see [1, 5].

Corollary 5.2. *The automorphism group of the graphs $C_{13}(k)$ and $C_{17}(k)$ is solvable for every possible value of k.*

Proof. In view of the previous lemma, we only have to prove that $\mathrm{Aut}(C_{13}(5))$ and $\mathrm{Aut}(C_{17}(4))$ are solvable. Let first $G = C_{13}(5)$. Choose $v = 0$, and let X_i denote the set of vertices connected to v by a path of length at most i, as in

Section 4. Thus $X_0 = \{0\}$, $X_1 \setminus X_0 = \{\pm 1, \pm 5\}$ and $X_2 \setminus X_1 = \{\pm 2, \pm 3, \pm 4, \pm 6\}$. We have $X_2 = \mathcal{V}(G)$, the edges connecting v to vertices in $X_1 \setminus X_0$ as well as the edges that connect vertices in $X_1 \setminus X_0$ with vertices in $X_2 \setminus X_1$ are shown below.

Recall from Section 4, that $\Gamma_2 = 1$ and Γ_0/Γ_1 is isomorphic to a subgroup of S_4. Choose an element $\gamma \in \Gamma_1$, it leaves the vertices $0, \pm 1, \pm 5$ fixed. Since the only neighbor of 2 in $X_1 \setminus X_0$ is 1 and 2 is the only neighbor of 1 with this property, we have $\gamma(2) = 2$, and γ does not move the elements $-2, 3, -3$ either for similar reasons. Thus γ also leaves the sets $\{4, 6\}$ and $\{-4, -6\}$ fixed, hence $\Gamma_1/\Gamma_2 = \Gamma_1$ is a subgroup of $S_2 \times S_2$. It follows from Proposition 4.9 that $|\mathrm{Aut}(G)|$ divides $13 \cdot 24 \cdot 4 = 2^5 3 \cdot 13$, and thus solvable by Corollary 3.3.

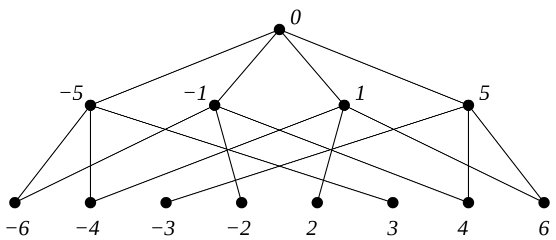

Figure 1 *The levels of the graph* $C_{13}(5)$

Consider now $G = C_{17}(4)$, and choose once again $v = 0$. In this case $X_1 \setminus X_0 = \{\pm 1, \pm 4\}$, $X_2 \setminus X_1 = \{\pm 2, \pm 3, \pm 5, \pm 8\}$ and $X_3 \setminus X_2 = \{\pm 6, \pm 7\}$. We have $X_3 = \mathcal{V}(G)$ and $\Gamma_3 = 1$. The edges between the consecutive levels of G are shown on Figure 2.

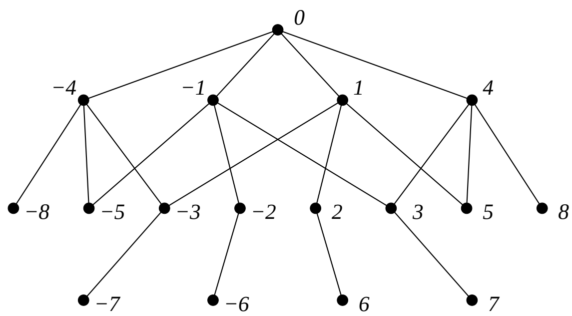

Figure 2 *The levels of the graph* $C_{17}(4)$

Γ_0/Γ_1 again is isomorphic to a subgroup of S_4. Choose an element $\gamma \in \Gamma_1$, it leaves the vertices $0, \pm 1, \pm 4$ fixed. Since the only neighbor of 2 in $X_1 \setminus X_0$ is 1 and 2 is the only neighbor of 1 with this property, we have $\gamma(2) = 2$, and γ does not move the elements $-2, 8, -8$ either for similar reasons. Since 5 is the only common neighbor of 1 and 4 in $X_2 \setminus X_1$, it is also fixed by γ, as well as -5 by symmetry. Thus 3 and -3 are also fixed, and it follows that $\Gamma_1/\Gamma_2 = 1$. Since Γ_2 fixes the vertices $\pm 2, \pm 3$, it also fixes $\pm 6, \pm 7$ and thus $\Gamma_2 = \Gamma_3$. It follows from Proposition 4.9 that $|\mathrm{Aut}(G)|$ divides $17 \cdot 24 = 2^3 3 \cdot 17$, and thus solvable by Corollary 3.3. (In fact, we could have easily derived the solvability from the Sylow theorems in this case.) $\square$

We will frequently refer to the solvability of the automorphism group of small regular simple graphs covered by the following lemma.

Lemma 5.3. *Let G be any k-regular simple graph on 8 vertices,* $1 \leq k \leq 6$, *or on 6 vertices,* $1 \leq k \leq 4$. *Then* $\mathrm{Aut}(G)$ *is solvable.*

Proof. Assume that G has 8 vertices. Since $\mathrm{Aut}(G) \cong \mathrm{Aut}(\overline{G})$, it is enough to prove the statement for $k \leq 3$. If $k = 1$, then G is the union of four disjoint edges, thus $\mathrm{Aut}(G) = \mathrm{S}_2 \wr \mathrm{S}_4$. If $k = 2$, then G is either an 8-cycle, or the union of two disjoint cycles. Accordingly, $\mathrm{Aut}(G)$ is either D_8, $\mathrm{D}_3 \times \mathrm{D}_5$, or $\mathrm{D}_4 \wr \mathrm{S}_2$. If $k = 3$ and G is not connected, then G is the union of two disjoint complete graphs, each on 4 vertices, hence $\mathrm{Aut}(G) = \mathrm{S}_4 \wr \mathrm{S}_2$. Finally, if G is a connected 3-regular graph, then the solvability of $\mathrm{Aut}(G)$ follows directly from Lemma 4.10. If G has 6 vertices, then a similar argument shows that $\mathrm{Aut}(G)$ is either $\mathrm{S}_2 \wr \mathrm{S}_3$, $\mathrm{D}_3 \wr \mathrm{S}_2$ or D_6. $\square$

Since $\mathrm{Aut}(G)$ acts on each vertex orbit V through a quotient that is a subgroup of $\mathrm{Aut}(H)$, where H denotes the regular graph induced by G on V, we have the following consequence for connected graphs.

Corollary 5.4. *Let G be a stable graph without solvable orbits such that* $\mathrm{Aut}(G)$ *has more than one vertex orbit. Then G induces an empty graph on each vertex orbit of size 6 or 8.*

We close this section with the following remark. In Section 8 we encounter several graphs whose solvability we prove via Lemma 4.11 and Corollary 3.3. Some of these graphs are 3-regular and are either circulant, thus may be handled by the method of his section, or belong to the family of the so-called generalized Petersen graphs. The automorphism group of such graphs have been completely determined in [4], and thus could have been used for our purpose. It is also quite plausible, that even in the remaining cases any reference to Thompson's theorem could have been avoided, but not without any undesirable effect on the complexity of our presentation.

6. Basic reduction

Assume that the group Γ acts on the connected graph H. Each orbit (edge or vertex) of $\mathrm{Aut}(H)$ splits up into complete orbits of Γ. In the sequel we refer to an orbit of Γ simply as an orbit. Consider the following five operations on H.

(i) Remove an orbit of loops.

(ii) Unless H is the complete graph on two vertices, remove an orbit V consisting of degree one vertices, along with the unique edge orbit E incident to it.

(iii) Unless H is a cycle of length $n \geq 3$, remove an orbit V of vertices of degree 2, along with the edge orbits incident to it, and connect the two neighbours (which may coincide) of each removed vertex v_i by a new edge e_i. More precisely, in the particular case when V consists of pairs of adjacent vertices, for each such pair v_{i1}, v_{i2} the new edge e_i should connect the two neighbours of the set $\{v_{i1}, v_{i2}\}$ (which again may coincide).

(iv) Take an orbit E that contains two parallel edges. This orbit can be partitioned into edge sets E_i of the same cardinality such that two edges are parallel if and only if they are in the same set E_i for some i. Replace each set E_i by a single edge e_i.

(v) Remove an orbit E of edges that does not contain two parallel edges, but in which each edge is parallel to some edge in a different orbit.

We say that H is reduced if none of these operations can be performed on H. H is reduced if and only if H is either a singleton, a K_2, a C_n ($n \geq 3$), or a stable simple graph. In the first three cases $\mathrm{Aut}(H)$ is either a dihedral group or of order at most 2, thus solvable. Therefore, if Γ acts on the reduced graph H without solvable orbits, then H must be a stable simple graph.

Lemma 6.1. *Assume that the group* Γ *acts on the connected graph* H *without solvable orbits, and the graph* H' *is obtained from* H *by performing one of the above operations. Then* H' *is a connected graph on which* Γ *acts without solvable orbits. Moreover, for every orbit* O *in* H *there is an orbit* O' *in* H' *whose cardinality divides* $2|O|$*, and for every orbit* O' *in* H' *there is an orbit* O *in* H *whose cardinality is an integer multiple of* $|O'|/2$.

Proof. H' is obviously connected. Assume that we have removed an edge orbit E consisting of y loops using the first operation. Then $y \geq 5$, otherwise Γ would act on E through a solvable quotient. The vertices incident to these loops form an orbit V of x vertices, each incident to the same number of loops, say k. Thus $y = kx$. Γ acts on H' via its restriction to H'. Each orbit in H' is at the same time an orbit of H, so Γ acts on H' without solvable orbits. The second statement is obvious because V is an orbit of x vertices in H'. Note that it implies $x \geq 5$. Moreover, $c(H') = c(H) - kx$.

Assume next that we have performed the second operation: it does not change the cyclomatic number. Γ acts on H' via its restriction to H'. Each orbit in H' is at the same time an orbit of H, so Γ acts on H' without solvable orbits. To prove the second statement, denote by W be the set of vertices adjacent to vertices in V. Then W is an orbit of $x \geq 5$ vertices, it is also an orbit of H'. Each vertex in W is adjacent to the same number of vertices in V, say k. Then the cardinality of the removed orbits V and E are alike kx, a multiple of $|W|$.

Operation (iii) does not change the cyclomatic number. Assume that $|V| = x$, then V is either incident to one edge orbit of size $2x$, or two edge orbits, each of size x, or (in the particular case) one edge orbit of size x and another of size $x/2$. Let $E' = \{e_1, e_2, \ldots, e_y\}$, where $y = x$ or (in the particular case) $y = x/2$. The action of Γ on H' can be combined from its restriction to $\mathcal{V}(H') \cup \mathcal{E}(H') \setminus E'$ and its natural transfer from V to E'. Obviously Γ acts then on H' without solvable orbits. The second statement is clear.

Suppose that operation (iv) was performed. Denote the common cardinality of the sets E_i by k, then $|E| = kx$ for some positive integer x, and $c(H') = c(H) - (k-1)x$. Again there is a natural way to define the action of Γ on H'. The edge set $\{e_1, e_2, \ldots, e_x\}$ is then an orbit of Γ in H'. Since $\mathcal{V}(H') = \mathcal{V}(H)$, Γ acts on $\mathcal{V}(H')$ without solvable orbits. It follows from Lemma 4.2, that Γ acts on H' without solvable orbits. In particular, we have $x \geq 5$, and E is a multiple of $|E'|$.

When operation (v) is performed, H' again inherits the action of Γ on H, in particular Γ acts on H' without solvable orbits. Assume that $|E| = x$, then $x \geq 5$ and $c(H') = c(H) - x$. The endpoints of the edges in E either form a vertex orbit of size $2x$, or two vertex orbits, each of size x, hence the second statement. $\square$

Write $\delta_c(H) = c(H) - c(H')$. Taking into account the change in the cyclomatic number and comparing it to the cardinalities of special orbits in H', introduced in the previous proof, we find the following supplement to Lemma 6.1.

Lemma 6.2. *Assume that the group Γ acts on the connected graph H without solvable orbits, and the graph H' is obtained from H by performing one of the operations (i)–(v). Then either $\delta_c(H) = 0$, or $\delta_c(H) \geq 5$. Moreover, there is an orbit O in H', whose cardinality divides $2\delta_c(H)$.*

Let G denote a connected graph without solvable orbits, and fix $\Gamma = \mathrm{Aut}(G)$. Since each operation decreases $|\mathcal{V}(G)| + |\mathcal{E}(G)|$, by a repeated application of the operations (i)–(v) we eventually obtain a reduced graph $\widetilde{G}$ on which Γ acts without solvable orbits. We say that $\mathcal{R} : G = G_0 \to G_1 \to \ldots \to G_n = \widetilde{G}$ is a *reduction sequence* if each graph G_{i+1} is obtained from G_i by one of the operations (i)–(v), and the action of Γ on G_{i+1} is derived from its action on G_i as described in the proof of Lemma 6.1. We also associate the sequence $c_i = \delta_c(G_i)$ to $\mathcal{R}$, then

$$c(G_i) = c(\widetilde{G}) + \sum_{j=i}^{n-1} c_j.$$

An immediate consequence of Lemma 6.1 is

Corollary 6.3. *Let $\mathcal{R} : G = G_0 \to G_1 \to \ldots \to G_n = \widetilde{G}$ be a reduction sequence. If the odd prime p divides the cardinality of every orbit in $\widetilde{G}$, then it also divides the size of every orbit in G_i, for each $0 \leq i \leq n$. If, for some $0 \leq i \leq n$, G_i has an orbit of size $2^\beta 7$ for some nonnegative integer β, then $\widetilde{G}$ has an orbit of size 2^α or $2^\alpha 7$ for some nonnegative integer α.*

This, coupled with Lemmas 6.1 and 6.2 yields

Lemma 6.4. *Let $\mathcal{R} : G = G_0 \to G_1 \to \ldots \to G_n = \widetilde{G}$ be a reduction sequence. If the odd prime p divides the cardinality of every orbit in $\widetilde{G}$, then it also divides c_i for each $0 \leq i \leq n$. If there is an index $0 \leq i \leq n$ such that $c_i = 2^\beta$ for some nonnegative integer β, then $\widetilde{G}$ has an orbit of size 2^α for some nonnegative* *integer α. If there is an index $0 \leq i \leq n$ such that $c_i = 7$, then $\widetilde{G}$ has an orbit of size 2^α or $2^\alpha 7$ for some nonnegative integer α.*

Now it is clear that the 'only if' part of Theorem 1.1 can be reduced to the following two lemmas.

Lemma 6.5. *Let G be a connected graph without solvable orbits such that $c(G) \in \{7, 9, 12, 13, 14, 17, 18, 23\}$. If $\mathcal{R} : G = G_0 \to G_1 \to \ldots \to G_n = \widetilde{G}$ is a reduction sequence, then $c(\widetilde{G}) \neq 6, 8, 10, 11, 15, 16$.*

Lemma 6.6. *There is no stable simple graph G without solvable orbits such that $c(G) \in \{4, 5, 7, 9, 12, 13, 14, 17, 18, 23\}$.*

7. Stable simple graphs without solvable orbits

In order to prove Lemma 6.5, in this section first we have a closer look on stable simple graphs G of cyclomatic number 6, 8, 10, 11, 15 and 16. We assume that a group Γ acts on G without solvable orbits. Recall from Section 4, that we denote by $\widetilde{\Gamma}$ the subgroup of $\mathrm{Aut}(G)$ that is actually responsible for this action. In particular, the group $\widetilde{\Gamma}$ is not solvable.

Lemma 7.1. *Let G be a stable simple graph of cyclomatic number $c(G) = 6$, and assume that the group Γ acts on G without solvable orbits. Then the cardinality of each vertex orbit is divisible by 5.*

Proof. It follows from Proposition 4.8 that at most r_3 and r_4 can be non-zero, and thus $5 = c(G) - 1 = r_3/2 + r_4$. Either $r_4 = 5$ and $r_3 = 0$, or $r_4 = 0$ and $r_3 = 10$. In the first case there is exactly one vertex orbit, whose size is 5. In the second case there is either one vertex orbit of size 10, or there are two vertex orbits, each of size 5. $\square$

We note that it is not very difficult to see that the only two stable simple graphs without solvable orbits of cyclomatic number 6 are K_5 and the Petersen graph, but we will not depend upon this fact.

Lemma 7.2. *Let G be a stable simple graph of cyclomatic number $c(G) = 8$, and assume that the group Γ acts on G without solvable orbits. Then the cardinality of each vertex orbit is divisible by 7.*

Proof. Proposition 4.8 implies that at most r_3 and r_4 can be non-zero, and accordingly $7 = r_3/2 + r_4$. Either $r_4 = 7$ and $r_3 = 0$, or $r_4 = 0$ and $r_3 = 14$. In the first case there is exactly one vertex orbit of size 7. In the second case there is either one vertex orbit of size 14, or there are two vertex orbits, each of size 7, otherwise it would be either $\mathcal{V}[5,9]$ or $\mathcal{V}[6,8]$, and thus $\widetilde{\Gamma}$ would be solvable according to Lemma 4.10. □

Lemma 7.3. *Let G be a stable simple graph of cyclomatic number $c(G) = 10$, and assume that the group Γ acts on G without solvable orbits. Then the cardinality of each vertex orbit is divisible by 3.*

Proof. It follows from Proposition 4.8 that $r_d = 0$ for $d \geq 6$, and thus $9 = r_3/2 + r_4 + 3r_5/2$. If $r_5 \neq 0$, then $r_5 = 6$ and $r_3 = r_4 = 0$, thus there is exactly one vertex orbit, whose cardinality is 6. There is no other possibility, since in the remaining cases

r_4	9	6	5	0
r_3	0	6	8	18

it follows from Lemma 4.10 that $\widetilde{\Gamma}$ is solvable, contradicting the assumption that Γ acts on G without solvable orbits. □

Lemma 7.4. *Let G be a stable simple graph of cyclomatic number $c(G) = 11$, and assume that the group Γ acts on G without solvable orbits. Then the cardinality of each vertex orbit is divisible by 5.*

Proof. It follows from Proposition 4.8 that $r_d = 0$ for $d \geq 6$, and thus $10 = r_3/2 + r_4 + 3r_5/2$. If $r_5 \neq 0$, then $r_5 = 5$, $r_4 = 0$ and $r_3 = 5$, so the cardinality of each vertex orbit is 5. Of the remaining cases

r_4	10	7	6	5	0
r_3	0	6	8	10	20

the second and the third cannot occur, because $\widetilde{\Gamma}$ would be solvable according to Lemma 4.10. In the first and the fourth cases we can argue as in the proof of Lemma 7.1. Assume that we are in the fifth case, and there is a vertex orbit whose size is not divisible by 5. Were there three vertex orbits, that is, $\mathcal{V}[5,6,9]$, $\mathcal{V}[5,7,8]$, $\mathcal{V}[6,6,8]$ or $\mathcal{V}[6,7,7]$, Lemma 4.10 would again yield to contradiction as well as in the cases of two orbits $\mathcal{V}[6,14]$, $\mathcal{V}[8,12]$ and $\mathcal{V}[9,11]$. Finally, the case $\mathcal{V}[7,13]$ can be excluded by Lemma 4.4. □

Lemma 7.5. *Let G be a stable simple graph of cyclomatic number $c(G) = 15$, and assume that the group Γ acts on G without solvable orbits. Then there is no vertex orbit whose cardinality is a power of 2.*

Proof. It follows from Proposition 4.8 that $r_d = 0$ for $d \geq 7$, and thus $14 = r_3/2 + r_4 + 3r_5/2 + 2r_6$. If $r_5 = r_6 = 0$, then the statement follows immediately from Lemma 4.10. Therefore we only review the possibilities when there exists a $d \geq 5$ with $r_d \neq 0$.

r_6	7	5	0	0	0	0
r_5	0	0	7	6	6	5
r_4	0	0	0	5	0	0
r_3	0	8	7	0	10	13

Assume that there is a vertex orbit whose cardinality k is a power of 2. Since $k \geq 5$, it should be $k = 8$, which can only happen in the second or sixth case, meaning either $\mathcal{V}[5,8]$ or $\mathcal{V}[5,5,8]$. According to Corollary 4.5, the degree of the orbit of size 8 would be at least 5, a contradiction. □

Lemma 7.6. *Let G be a stable simple graph of cyclomatic number $c(G) = 16$, and assume that the group Γ acts on G without solvable orbits. Then there is no vertex orbit whose cardinality is of the form 2^α or $2^\alpha 7$ for some nonnegative integer α.*

Proof. If there is a $d \geq 7$ such that $r_d \neq 0$, then it follows from Proposition 4.8 that either G is an 8-regular graph on 5 vertices (nonsense), or a 7-regular graph on 6 vertices (ditto), or has exactly two vertex orbits, each of size 5, of degree 7 and 3, respectively. In the remaining cases we have $15 = r_3/2 + r_4 + 3r_5/2 + 2r_6$. If $r_6 \neq 0$, then there are only 3 possibilities: either $r_6 = r_3 = 6$, $r_5 = r_4 = 0$, or $r_6 = r_4 = 5$, $r_5 = r_3 = 0$, or $r_6 = 5$, $r_5 = r_4 = 0$, $r_3 = 10$, and there is indeed no vertex orbit of cardinality 2^α or $2^\alpha 7$. We summarize the remaining cases below. If $r_5 \neq 0$, then these are

r_5	10	8	7	6	6	5	5
r_4	0	0	0	6	0	5	0
r_3	0	6	9	0	12	5	15
		$*$	$*$	$*$	$*$		

The cases marked with $*$ cannot occur, because then $\widetilde{\Gamma}$ would nevertheless be solvable, according to Lemma 4.10. We will use this convention throughout the rest of the paper without any further explanation. The claim is obvious in the first and sixth cases. In the last case the only possibility to have a vertex orbit of size 2^α or $2^\alpha 7$ would be $\mathcal{V}[5,7,8]$, which is impossible by Corollary 4.5. If $r_5 = 0$, that is

r_4	15	12	11	10	9	8	7	6	5	0
r_3	0	6	8	10	12	14	16	18	20	30
		*	*		*	*	*	*		

then in each case not excluded by Lemma 4.10, $|\mathcal{V}(G)|$ is not divisible by 7. Were there a vertex orbit whose cardinality is divisible by 7, the size of each orbit would be divisible by 7 by Lemma 4.3, a contradiction. According to Lemma 4.10, there cannot be an orbit of size 2^α either. □

Now it is easy to prove Lemma 6.5. Let $\mathcal{R} : G = G_0 \to G_1 \to \ldots \to G_n = \widetilde{G}$ be a reduction sequence, then $c(G) \geq c(\widetilde{G})$. $\widetilde{G}$ is a stable graph on which $\mathrm{Aut}(G)$ acts without solvable orbits. Assume first that $c(\widetilde{G})$ is either 6 or 11. In $\widetilde{G}$, the cardinality of each vertex orbit is divisible by $p = 5$, according to Lemmas 7.1 and 7.4. It follows from Proposition 4.7 that 5 divides the cardinality of every orbit in $\widetilde{G}$. According to Lemma 6.4, each c_i is divisible by 5. Consequently, $c(G) \equiv 1 \pmod 5$ and thus $c(G) \notin \{7, 9, 12, 13, 14, 17, 18, 23\}$.

If $c(\widetilde{G}) = 8$, then it follows from Lemma 7.2 along the same lines that $c(G) \equiv 1 \pmod 7$ and thus $c(G) \notin \{7, 9, 12, 13, 14, 17, 18, 23\}$. If $c(\widetilde{G}) = 10$, then based on Lemma 7.3 we have $c(G) \equiv 1 \pmod 3$. Note that if $c(G) \neq c(\widetilde{G})$, then $c(G) \geq c(\widetilde{G}) + 5$. Thus once again, $c(G) \notin \{7, 9, 12, 13, 14, 17, 18, 23\}$.

Assume finally that $c(\widetilde{G}) = 15$ or 16, and $c(G) \in \{7, 9, 12, 13, 14, 17, 18, 23\}$. The only possibility is $c(G) = 23$. In the first case there is an index $0 \leq i \leq n-1$ such that $c_i = 8$ and all the other c_j are zero. It follows from Lemma 6.4 that $\widetilde{G}$ has an orbit of size 2^β for some nonnegative integer β. According to Proposition 4.7, there is a vertex orbit whose size is 2^α for some nonnegative integer α, contradicting Lemma 7.5. In the second case there is an index $0 \leq i \leq n-1$ such that $c_i = 7$ and all the other c_j are zero. In this case we find by a similar argument that there is a vertex orbit in $\widetilde{G}$ whose size is 2^α or $2^\alpha 7$ for some nonnegative integer α, which contradicts Lemma 7.6.

8. The case analysis

In order to prove Lemma 6.6, we assume that G is a stable simple graph without solvable orbits such that $c(G) \in \{4, 5, 7, 9, 12, 13, 14, 17, 18, 23\}$. In most cases we will arrive at a contradiction by concluding that $\mathrm{Aut}(G)$ is solvable. Note that throughout this section we will always apply Lemmas 4.10 and 4.11 under the assumption that $\Gamma = \widetilde{\Gamma} = \mathrm{Aut}(G)$.

If $c(G) \leq 9$, then at most r_3 and r_4 can be non-zero. Lemma 4.10 applies to all the seven possible cases:

$c(G)$	4	5	7	7	9	9	9
r_4	0	0	6	0	8	5	0
r_3	6	8	0	12	0	6	16

It follows that G cannot be without solvable orbits.

When $c(G) = 12$, the equation $11 = \sum(d/2 - 1)r_d$ immediately implies that $r_d = 0$ for $d > 5$ and leaves us with the following possibilities.

r_5	5	0	0	0	0	0	0
r_4	0	11	8	7	6	5	0
r_3	7	0	6	8	10	12	22
	7		$*$	$*$	$*$	$*$	

In the first case we get into contradiction with Lemma 4.3 when it is applied with the prime number $p = 7$. This we marked with the number 7 in the last row of the table. We will also apply this convention later on without any further explanation. Whenever Lemma 4.3 can be applied in a similar way with a specific prime number p, it will appear in the bottom line.

In the second and in the last case it follows from Lemma 4.11 that $|\mathrm{Aut}(G)|$ divides $2^\alpha 3^\beta \cdot 11$ for some nonnegative integers α, β, and thus solvable either by Burnside's theorem, or by Corollary 3.3.

Assume next that $c(G) = 13$. The relation $12 = \sum(d/2 - 1)r_d$ again implies that $r_d = 0$ for $d > 5$. The complete list of possibilities

r_5	8	6	5	0	0	0	0	0	0	0
r_4	0	0	0	12	9	8	7	6	5	0
r_3	0	6	9	0	6	8	10	12	14	24
		$*$	$*$	$*$	$*$	$*$	7	$*$	5	$*$

reveals that, apart from the first case, either Lemma 4.10 or Lemma 4.3 can be applied. In the missing case it follows from Lemma 5.3 that $\mathrm{Aut}(G)$ is solvable.

Turning to the case $c(G) = 14$, it follows from Proposition 4.8 that $r_d = 0$ for $d \geq 6$, unless $r_6 = 5$, $r_5 = r_4 = 0$ and $r_3 = 6$, which is not possible according to Lemma 4.3 ($p = 5$). Therefore $13 = r_3/2 + r_4 + 3r_5/2$, and we have the following cases:

r_5	7	6	5	0	0	0	0	0	0	0	0
r_4	0	0	0	13	10	9	8	7	6	5	0
r_3	5	8	11	0	6	8	10	12	14	16	26
	7	$*$			$*$	$*$	$*$	$*$	$*$	$*$	

In the third and in the last case it follows from Lemma 4.11 that $|\mathrm{Aut}(G)|$ either divides $2^\alpha 3^\beta \cdot 11$ or $2^\alpha 3 \cdot 13$ for some nonnegative integers α, β, and thus solvable either by Burnside's theorem, or by Corollary 3.3. In the fourth case $\mathrm{Aut}(G)$ acts transitively on the vertices, otherwise we would have $\mathcal{V}[5,8]$ or $\mathcal{V}[6,7]$ which, according to Lemma 4.4, cannot occur. In particular, the order of $\mathrm{Aut}(G)$ is divisible by 13, and thus there is a $\pi \in \mathrm{Aut}(G)$ of order 13. This automorphism permutes the vertices of G cyclically. Since 13 is a prime, the orbit of any edge with respect to the subgroup $\Gamma = \langle \pi \rangle$ generated by π is a cycle of length 13. A suitable power of π then shifts the vertices by 1 along this cycle. Consider any edge e not contained in this cycle, its length is k for some $2 \leq k \leq 6$. The orbit of e under the action of Γ is the set of all edges of length k, thus G is the graph $C_{13}(k)$, whose group of automorphisms is solvable according to Corollary 5.2.

When $c(G) = 17$, it follows from Proposition 4.8 that $r_d = 0$ for $d \geq 7$, unless $r_7 = 5$ and $r_3 = 7$ (and every other r_i is zero), which nevertheless contradicts Lemma 4.3. We have $16 = r_3/2 + r_4 + 3r_5/2 + 2r_6$ otherwise. It is then easy to overview the cases when $r_6 = r_5 = 0$:

r_4	16	13	12	11	10	9	8	7	6	5	0
r_3	0	6	8	10	12	14	16	18	20	22	32
	$*$	$*$	$*$	5	$*$	$*$	$*$	$*$	$*$	5	$*$

The reason why we could indeed refer to Lemma 4.3 in the fourth case is that either there is one orbit of degree 3 vertices (of size 10), or there are two such orbits, each of size 5. The remaining cases are

r_6	8	6	5	5	0	0	0	0	0	0	0	0
r_5	0	0	0	0	9	8	7	6	6	5	5	5
r_4	0	0	6	0	0	0	0	7	0	6	5	0
r_3	0	8	0	12	5	8	11	0	14	5	7	17
			5	5		$*$	7	7	$7*$	5	5	5

The explanation for the case marked with $7*$ is the following. Either there is a vertex orbit of degree 3 whose cardinality is divisible by 7, contradicting Lemma 4.3, or there is a vertex orbit of degree 3 whose cardinality is of the form 2^a3^b, and thus $\mathrm{Aut}(G)$ is solvable by Lemma 4.10. This convention will be also used later without any explanation.

The first case can be excluded by Lemma 5.3. In the second case we have $\mathcal{V}[6,8]$. According to Corollary 5.4, each vertex orbit is an independent set. Thus, there are 36 edges connecting V_1 to V_2 and 24 edges connecting V_2 to V_1, a contradiction. In the fifth case we have $\mathcal{V}[5,9]$, and we arrive at a contradiction with Lemma 4.4.

Assume next that $c(G) = 18$. It follows from Proposition 4.8 that $r_d = 0$ for $d \geq 7$, unless or $r_7 = 5$ and $r_3 = 9$, which case can be excluded by an application of Lemma 4.3 with $p = 5$. In the remaining cases we have $17 = r_3/2 + r_4 + 3r_5/2 + 2r_6$. First we overview the cases when at least one of r_5 and r_6 is nonzero.

r_6	7	6	6	5	5	0	0	0	0	0	0	0	0	0	0	0
r_5	0	0	0	0	0	9	8	8	7	6	6	6	5	5	5	5
r_4	0	5	0	7	0	0	5	0	0	8	5	0	7	6	5	0
r_3	6	0	10	0	14	7	0	10	13	0	6	16	5	7	9	19
	7			5	5	7			7	$*$	$*$	$*$	5	$*$	$*$	5

In the first missing case each degree 4 vertex should be incident to at least 6 edges by Lemma 4.4, which is not possible. The third missing case can be excluded by a similar argument. In the fourth missing case we use Corollary 4.6, when it is $\mathcal{V}[5,5,8]$ to find a degree 3 vertex incident to at least 8 edges. Otherwise it is $\mathcal{V}[8,10]$, and it follows from Lemma 4.4 that each degree 3 vertex is incident to at least $8/(8,10) = 4$ edges, which is again impossible. In the second missing case it is either $\mathcal{V}[6,10]$ or $\mathcal{V}[5,5,6]$.

Suppose that we have $\mathcal{V}[6,10]$. According to Lemma 4.4, each vertex in V_1 is connected to 5 vertices in V_2, each vertex in V_2 is connected to 3 vertices in V_1, V_2 is an independent set and G induces a 1-regular graph H on V_1. This contradicts Corollary 5.4. The possibility of $\mathcal{V}[5,5,6]$ can be easily excluded by Corollary 4.6. It remains to study the cases when $r_d = 0$ for $d \geq 5$. These are

r_4	17	14	13	12	11	10	9	8	7	6	5	0
r_3	0	6	8	10	12	14	16	18	20	22	24	34
		$*$	$*$	$*$	$*$	5	$*$	$*$	7	$*$	$*$	

In the last case it follows from Lemma 4.11 that $|\mathrm{Aut}(G)|$ divides $2^\alpha 3 \cdot 17$ for some nonnegative integer α, and thus solvable either by Burnside's theorem, or by Corollary 3.3. In the first case $\mathrm{Aut}(G)$ acts transitively on the vertices, otherwise we would have $\mathcal{V}[5,12]$, $\mathcal{V}[6,11]$, $\mathcal{V}[7,10]$, $\mathcal{V}[8,9]$, $\mathcal{V}[5,5,7]$ or $\mathcal{V}[5,6,6]$, neither of which can occur according to Lemma 4.4 and Corollary 4.5. In particular, the order of $\mathrm{Aut}(G)$ is divisible by 17, and thus there is a $\pi \in \mathrm{Aut}(G)$ of order 17. This automorphism permutes the vertices of G cyclically. Since 17 is a prime, the orbit of any edge with respect to the subgroup $\Gamma = \langle \pi \rangle$ generated by π is a cycle of length 17. A suitable power of π then shifts the vertices by 1 along this cycle. Consider any edge e not contained in this cycle, its length is k for some $2 \leq k \leq 8$. The orbit of e under the action of Γ is the set of all edges of length k, thus G is the graph $C_{17}(k)$, whose group of automorphisms is solvable according to Corollary 5.2.

We investigate finally the most complicated case, when $c(G) = 23$. It is easily seen from Proposition 4.8 that $r_d = 0$ for $d \geq 8$, except for the following four possibilities: either $r_9 = 5$ and $r_3 = 9$, or $r_8 = 6$ and $r_3 = 8$, or $r_8 = 5$ and $r_4 = 7$, or $r_8 = 5$ and $r_3 = 14$. In the first, third and fourth cases Lemma 4.3 can be applied with $p = 5$. In the second case it is $\mathcal{V}[6,8]$ and it follows from Corollary 5.4 that both V_1 and V_2 are independent sets. Accordingly, 48 edges leaves V_1 for V_2, whereas there are only 24 edges leaving V_2 for V_1, a contradiction.

In the sequel we may assume that $r_d = 0$ for $d \geq 8$, and accordingly $22 = r_3/2 + r_4 + 3r_5/2 + 2r_6 + 5r_7/2$. First we discuss the cases when $r_d = 0$ for $d \geq 5$:

r_4	22	19	18	17	16	15	14	13	12	11	10	9
r_3	0	6	8	10	12	14	16	18	20	22	24	26
		$*$	$*$	5	$*$	$7*$	$*$	$*$	$*$		$*$	$*$

r_4	8	7	6	5	0
r_3	28	30	32	34	44
	$*$	7	$*$	5	

In each of the missing cases it follows from Lemma 4.11 that $|\mathrm{Aut}(G)|$ divides $2^\alpha 3^\beta \cdot 11$ for some nonnegative integers α, β, and thus solvable either by Burnside's theorem, or by Corollary 3.3.

Next we consider the cases when $r_d = 0$ for $d \geq 6$ and $r_5 \neq 0$, then $22 = r_3/2 + r_4 + 3r_5/2$. It is not possible that each r_i is divisible by 5, so we immediately get into a contradiction by Lemma 4.3 when $r_5 = 5$. The cases when $r_5 = 7$ can be excluded in similar way. We have the following cases when $r_5 = 6$:

r_5	6	6	6	6	6	6	6	6
r_4	13	10	9	8	7	6	5	0
r_3	0	6	8	10	12	14	16	26
		$*$	$*$	$*$	$*$	$*$	$*$	

In the first case it is either $\mathcal{V}[5,6,8]$, $\mathcal{V}[6,6,7]$ or $\mathcal{V}[6,13]$, each contradicting Corollary 4.5. In the last case the cardinality of each orbit of degree 3 must be in the form $2^a 3^b 5^c$, otherwise we get a contradiction with Lemma 4.3. Since not all of them can be divisible by 5, Lemma 4.10 implies that $\mathrm{Aut}(G)$ is solvable. The cases with $r_5 \geq 8$ are

r_5	13	12	11	10	10	9	9	9	8	8	8	8	8
r_4	0	0	0	7	0	6	5	0	10	7	6	5	0
r_3	5	8	11	0	14	5	7	17	0	6	8	10	20
		$*$		7	$7*$	$*$	7			$*$	$*$		

Of the missing cases, in the first one it is either $\mathcal{V}[5,5,8]$, $\mathcal{V}[5,6,7]$ or $\mathcal{V}[5,13]$, each contradicting Corollary 4.6. In the second case it follows from Lemma 4.11 that $|\mathrm{Aut}(G)|$ divides $2^\alpha 3^\beta \cdot 11$ for some nonnegative integers α, β, and thus solvable either by Burnside's theorem, or by Corollary 3.3. Consider now the third case. If there is an orbit of degree 3 whose cardinality is either 6,8 or 12, then we are done by Lemma 4.10. Otherwise it is either $\mathcal{V}[9,17]$, $\mathcal{V}[7,9,10]$ or $\mathcal{V}[5,5,7,9]$, each of which contradicts Corollary 4.5. In the fifth case we can exclude $\mathcal{V}[5,5,5,8]$ immediately by Corollary 4.6, and if it is $\mathcal{V}[5,8,10]$, then by Lemma 4.4, neither V_1 nor V_3 can be connected to V_2, contradicting the assumption that G is connected.

The fourth case is more delicate. $\mathcal{V}[5,5,8]$ can be excluded by Corollary 4.6, so it must be $\mathcal{V}[8,10]$. It follows from Lemma 4.4 that each vertex in V_1 is connected to 5 vertices in V_2, each vertex in V_2 is connected to 4 vertices in V_1, and both V_1 and V_2 are independent sets, thus it is a bipartite graph. $\mathrm{Aut}(G)$

acts on V_1 through a quotient Γ that we can identify with a transitive subgroup of the symmetric group acting on V_1. We define a graph H on V_1 as follows: we connect $u, v \in V_1$ with an edge for each common neighbour of u and v in V_2. Since $|V_2| = 10$ and each vertex of V_2 is connected to 4 vertices in V_1, the non-simple graph H has 60 edges. By transitivity, each vertex of H has a degree 15. For $1 \le i \le 15$, let H_i be the subgraph of H such that $\mathcal{E}(H_i)$ consists of the edges whose multiplicity is i; most of these graphs are of course empty. Let H_i' be the simple graph underlying H_i on the vertex set V_1, Then $\mathrm{Aut}(H_i')$ can be viewed as a subgroup of the symmetric group acting on V_1, it contains Γ as a subgroup. H_i' is a k_i-regular graph for some $0 \le k_i \le 7$. Since the numbers ik_i add up to 15, not all of them are divisible by 7. Therefore the solvability of Γ follows immediately from Lemma 5.3.

In the sixth case the cardinality of each orbit of degree 3 must be in the form $2^a 3^b 5^c$, otherwise we get a contradiction with Lemma 4.3. In view of Lemma 4.10 we may assume that the cardinality of each such orbit is divisible by 5. The orbit of the 8 degree 5 vertices must be connected to at least one of them, thus we immediately get into contradiction with Lemma 4.4, unless it is $\mathcal{V}[8, 20]$. It then follows from Lemma 4.4 that each vertex in V_1 is connected to 5 vertices in V_2, each vertex in V_2 is connected to 2 vertices in V_1, and V_1 is an independent set. Define a graph H on V_1, as in the previous case. This time H has 20 edges, thus it is 5-regular. The solvability of Γ follows as in the previous case.

Next we consider the cases when $r_d = 0$ for $d \ge 7$ and $r_6 \ne 0$, then $22 = r_3/2 + r_4 + 3r_5/2 + 2r_6$. It is not possible that each r_i is divisible by 5, so we can apply Lemma 4.3 when $r_6 = 5$ and $r_5 = 0$. The cases when $r_6 = 7$ and $r_5 = 0$ can be excluded in similar way. The remaining cases are

r_6	11	9	8	8	6	6	6	6	6	6	5	5	5
r_5	0	0	0	0	5	0	0	0	0	0	8	6	5
r_4	0	0	6	0	0	10	7	6	5	0	0	0	0
r_3	0	8	0	12	5	0	6	8	10	20	0	6	9
	(a)	(b)	(c)	(d)	(e)	(f)	7	(g)	(h)	(i)	(j)	(k)	(l)

Cases (b) and (j) can be excluded by Lemma 4.4, whereas in cases (e) and (l) we get a contradiction to Corollary 4.6. In case (k) the orbit V_1 of degree 3 cannot be connected to the orbit V_2 of degree 6 in view of Lemma 4.4. Thus V_2 must be connected to the orbit V_3 of degree 5, and another application of Lemma 4.4

gives that in that case each vertex in V_3 must send 5 edges to V_2, hence cannot connect to V_1, contradicting the assumption that G is connected.

In case (a), if there are two vertex orbits, then it must be $\mathcal{V}[5,6]$. According to Lemma 4.4, each vertex in V_2 is connected to 5 vertices in V_1, thus G induces a 1-factor on V_2, in contradiction with Corollary 5.4. Otherwise $\mathrm{Aut}(G) = \mathrm{Aut}(\overline{G})$ has only one vertex orbit, on which $\mathrm{Aut}(\overline{G})$ acts transitively. Consequently, all connected components of $\overline{G}$ have the same cardinality, thus $\overline{G}$ is a connected 4-regular graph on 11 vertices. Therefore $c(\overline{G}) = 12$ and $\overline{G}$ cannot be without solvable orbits, contradicting Claim 4.1.

In cases (f) and (h), except of the orbit V of 6 degree 6 vertices, the size of every orbit is either 5 or 10, so it follows from Corollary 4.5 that each vertex of V sends 5 edges to one of them and G induces a 1-factor on V, contradicting Corollary 5.4. In case (c) it is $\mathcal{V}[6,8]$, so in view of Lemma 4.4, G induces a 3-regular graph on V_2 whose automorphism group is solvable by Lemma 5.3. In case (d) it cannot be $\mathcal{V}[5,7,8]$ or $\mathcal{V}[6,6,8]$ by corollaries 4.5 and 4.6, so it must be $\mathcal{V}[8,12]$. But then G would induce a 3-regular graph on V_1, just like in case (c). In case (g) it is $\mathcal{V}[6,6,8]$, where V_1 is the orbit of degree 6 vertices. It follows from Corollary 5.4 that each orbit is an independent set. V_2 cannot be connected to V_3 in view of Lemma 4.4, so V_3 must be connected to V_1, meaning that each vertex of V_1 is connected to 4 vertices in V_3. Thus each vertex of V_1 must be connected to exactly 2 vertices in V_2, and vice versa. Consequently, G induces a 2-factor on V_2, a contradiction.

It remains to discuss case (i). We get a contradiction with Lemma 4.3, unless the cardinality of each orbit is of the form $2^a 3^b 5^c$. If each orbit of degree 3 vertices has a cardinality divisible by 5, then it follows from Corollary 4.5 that G induces a 1-factor on the orbit of 6 degree 6 vertices, contradicting Corollary 5.4. So it must be either $\mathcal{V}[6,5,6,9]$, $\mathcal{V}[6,6,6,8]$ or $\mathcal{V}[6,8,12]$, where V_1 stands for the orbit of degree 6, of which the first case can be immediately excluded by Lemma 4.5. If it is $\mathcal{V}[6,6,6,8]$, then it follows from Corollary 5.4 that G induces an independent set on each orbit. According to Lemma 4.4, V_4 can only be connected to V_1, each vertex in V_1 sending 4 edges to V_4. The only possibility then is that each vertex in V_1 is connected to exactly 1 vertex both in V_2 and in V_3, and the orbits V_2, V_3 form the colour classes of a 2-regular bipartite graph H. The graph H can be easily understood, and it follows that $\mathrm{Aut}(G)$ acts on V_2 through a quotient that is a subgroup of either $\mathrm{S}_2 \wr \mathrm{S}_3$, $\mathrm{S}_2 \times \mathrm{D}_4$, $\mathrm{D}_3 \wr \mathrm{S}_2$ or D_6, thus solvable. In the third case $\mathcal{V}[6,8,12]$ G must induce an independent set on V_1 and on V_2. According to Lemma 4.4, each vertex of V_1 is connected to 4 vertices in V_2 and thus to 2 vertices in V_3. Consequently, each vertex in V_3 sends exactly 1 edge to V_1 and G induces a 2-regular graph H on V_3. Thus $\mathrm{Aut}(G)$ acts on V_3 through a quotient, which is a subgroup of $\mathrm{Aut}(H)$, but the latter must be one of $\mathrm{D}_3 \wr \mathrm{S}_4$, $(\mathrm{D}_3 \wr \mathrm{S}_2) \times \mathrm{D}_6$, $\mathrm{D}_3 \times \mathrm{D}_4 \times \mathrm{D}_5$, $\mathrm{D}_4 \wr \mathrm{S}_3$, $\mathrm{D}_3 \times \mathrm{D}_9$, $\mathrm{D}_4 \times \mathrm{D}_8$, $\mathrm{D}_5 \times \mathrm{D}_7$, $\mathrm{D}_6 \wr \mathrm{S}_2$, or D_{12}, thus solvable.

Finally we assume that $r_7 \neq 0$. We have 5 possibilities ($r_6 = r_5 = 0$ in each of them):

r_7	7	6	6	5	5
r_4	0	7	0	5	0
r_3	9	0	14	9	19
	7			5	5

In the missing cases, it is either $\mathcal{V}[6,7]$, $\mathcal{V}[5,6,9]$, $\mathcal{V}[6,7,7]$, $\mathcal{V}[6,6,8]$, or $\mathcal{V}[6,14]$. The first three possibilities contradict Corollary 4.6. Assume it is $\mathcal{V}[6,6,8]$, where the vertices of degree 7 are in V_1, each orbit is an independent set by Corollary 5.4. The orbit V_3 cannot be connected to V_2 by Lemma 4.4, thus it is connected to V_1. Another application of Lemma 4.4 reveals, that each vertex in V_1 is connected to 4 vertices in V_3. Since the independent set V_2 must be connected to V_1, it follows from Lemma 4.4 that each vertex in V_1 sends exactly 3 edges to V_2 and vice versa. Let H be the graph induced by G on $V_1 \cup V_2$. $\mathrm{Aut}(G)$ acts on H without solvable orbits, and thus H itself is a graph without solvable orbits. If H is connected, then $c(H) = 7$, but we have already proved that such graphs do not exist. It follows that H is the union of two disjoint copies of $K_{3,3}$, but then $\mathrm{Aut}(H) = (S_3 \wr S_2) \wr S_2$, thus $|\mathrm{Aut}(H)| = 2^\alpha 3^\beta$, hence $\mathrm{Aut}(H)$ is solvable.

It only remains to exclude the case $\mathcal{V}[6,14]$. According to Lemma 4.4, each vertex in V_1 is connected to 7 vertices in V_2, each vertex in V_2 is connected to 3 vertices in V_1, and both V_1 and V_2 are independent sets. $\mathrm{Aut}(G)$ acts on V_1 through a quotient, which is a subgroup of S_6. This quotient, being non-solvable, must contain an element of order 5. Thus there is a $\pi \in \mathrm{Aut}(G)$ that cyclically permutes 5 elements of V_1 and leaves the sixth element v fixed. It must leave the set W of 7 neighbours of v in V_2 fixed. If the order of $\pi|_W$ is divisible by 5, then π^2 leaves two elements of W fixed. Otherwise the cycle decomposition of $\pi|_W$ reveals that π^{12} fixes every element of W. In any case, there is an element $w \in W$ such that $\pi^{12}(w) = w$. Thus π^{72} also leaves the 3 neighbours of w in

V_1 fixed, which is not possible, since the restriction of π^{72} to V_1 has an order $5/(5,72) = 5$.

9. Projective algebraic curves without solvable points

In this section we formulate the strongest version of one of the main results of [7] which can be derived using the methods of the above cited paper, taking into account the new constructions and the non-existence results presented in this article, for the convenience of the reader.

We say that a finite extension of a field K is solvable if it is separable and the Galois group of its normal closure over K is solvable. Let X be a quasi-projective variety over a field K. We say that P is a solvable point of X over K if P is a rational point of X defined over a finite solvable extension of K.

Theorem 9.1. *Let K be a field complete with respect to a discrete valuation. Assume that the absolute Galois group of the residue field of K has quotients isomorphic to $S_5 \times S_7$, $S_5 \times S_8$,* $\mathrm{PGL}_3(2)$, *and* $\mathrm{PGL}_3(3)$. *Then there is a smooth, projective, geometrically irreducible curve over K without solvable points over K whose genus is equal to 6, 8, 10, 11, 15, 16, 19, 20, 21, 22 or it is at least 24.*

The derivation of the above theorem is the same as that of the corresponding result in [7]. There we pointed out that S_5 acts transitively on the six-element set. Hence S_5 acts without solvable orbits on $K'_{6,6}$, $K_5(n)$, $K_6(n)$, and $K_{5,6}(n,m)$ for every pair of natural numbers n and m. Therefore there is an action of the absolute Galois group of the residue field of K on each graph appearing in Section 2 without solvable orbits, which is the condition for the argument of [7] to work. Of course we have some freedom in choosing the groups listed in the theorem above. For example we may use projective special linear groups instead of the corresponding general linear groups.

The assumptions of the theorem on the field K are quite general. For example it is satisfied by the Laurent series ring $F((t))$ where F is any field such that every finite group appears as a Galois group of a finite Galois extension over F. The latter condition holds for the rational function field $L(x)$ over every algebraically closed field L by Harbater's theorem (see [6]), and it is conjectured to be true for example for every number field. On the other hand the list of groups in the theorem above only consists of finitely many groups of small order hence it is possible to verify numerically that they are Galois groups for a given field.

It was proved in [7] that every smooth, projective, and geometrically irreducible curve whose genus is equal to 0, 2, 3 or 4 over any field K has a solvable point over K. It is an interesting question whether there is a natural number g not covered by Theorem 9.1 such that there is a smooth, projective, and geometrically irreducible curve over some field K without solvable points over K whose genus is equal to g.

Acknowledgment Part of this work has been achieved thanks to the support of the European Commission through its 6th Framework Programme "Structuring the European Research Area" and the contract Nr. RITA-CT-2004-505493 for the provision of Transnational Access implemented as Specific Support Action.

References

[1] L. Babai, Automorphism groups, isomorphism, reconstruction, in: Handbook of Combinatorics, Vol II (R. L. Graham, M. Grötschel, L. Lovász, eds.), Elsevier, Amsterdam (1995), pp. 1447–1540

[2] N. Biggs, Algebraic Graph Theory, Cambridge University Press (1974)

[3] C. W. Curtis and I. Reiner, Methods of Representation Theory, Vol I, John Wiley&Sons, New York (1981)

[4] R. Frucht, J. E. Graver, and M. E. Watkins, The groups of the generalized Petersen graphs, *Proc. Cambridge Philos. Soc.* **70** (1971) 211–218

[5] C. D. Godsil, Graphs, groups and polytopes, in: Combinatorial Mathematics, *Lect. Notes Math.* **686** Springer, Berlin (1978), pp. 157–164

[6] D. Harbater, Mock covers and Galois extensions, *J. Algebra* **91** (1984) 281–293

[7] A. Pál, Solvable points on projective algebraic curves, *Canad. J. Math.* **56** (2004) 612–637

[8] D. S. Passman, Permutation Groups, W. A. Benjamin, New York (1968)

[9] M. Petersdorf and H. Sachs, Spektrum und Automorphismengruppe eines Graphen, in: Combinatorial Theory and its Applications, III, North-Holland, Amsterdam (1969), pp. 891-907

[10] J. G. Thompson, Nonsolvable finite groups all of whose local subgroups are solvable, *Bull. Amer. Math. Soc.* **74** (1968) 383–437

[11] D. Wales, Classification of simple groups of order $p \cdot 3^a \cdot 2^b$, p a prime, in: Representation Theory of Finite Groups and Related Topics, *Proc. Sympos. Pure Math.* **XXI** Amer. Math. Soc., Providence, RI (1971), pp. 161–163

[12] D. Wales, Simple groups of order $17 \cdot 3^a \cdot 2^b$, *J. Algebra* **17** (1971) 429–433

[13] D. Wales, Simple groups of order $13 \cdot 3^a \cdot 2^b$, *J. Algebra* **20** (1972) 124–143

E-mail address: karolyi@cs.elte.hu
E-mail address: a.pal@imperial.ac.uk