

Radically solvable graphs

Bill Jackson ^{*} J.C. Owen [†]

14 March 2018

Abstract

A 2-dimensional framework is a straight line realisation of a graph in the Euclidean plane. It is quadratically, respectively radically, solvable if the vertex coordinates can be expressed as a sequence of square, respectively integer power, roots of combinations of the squared edge lengths. Quadratically solvable frameworks are also referred to as being ruler-and-compass-constructible since they can be drawn in the plane using only a ruler marked with the edge-lengths and a compass. We show that the radical/quadratic solvability of a generic framework depends only on its underlying graph and characterise which planar graphs give rise to radically/quadratically solvable generic frameworks. We conjecture that our characterisation extends to all graphs.

2010 *Mathematics Subject Classification*: 05C10, 12F10, 52C25, 68R10.

1 Introduction

Many systems of polynomial equations which are of practical interest can be represented by a graph. An important example occurs in computer aided design (CAD) when the location of the geometric elements in a drawing such as points, lines and circles (corresponding to vertices in the graph) are determined by relationships between them such as tangency, coincidence

^{*}School of Mathematical Sciences, Queen Mary University of London, Mile End Road, London E1 4NS, England. E-mail: b.jackson@qmul.ac.uk

[†]Siemens, Francis House, 112 Hills Road, Cambridge CB2 1PH, England. E-mail: owen.john.ext@siemens.com

and relative distances or angles (corresponding to edges in the graph). The ability to solve such systems of equations rapidly allows a design engineer to modify input parameters such as the values for the distances or angles (collectively called "dimensions" in a dimensioned drawing) and to realise a computer model for many variants of a basic design [12]. Most modern CAD systems incorporate the ability to solve these so-called dimensional constraint equations, see for example [14].

A simple example of dimensional constraint equations is provided by points in a plane with certain specified relative distances. The system of equations and a particular solution can both be represented by a framework (G, p) where G is a graph and p is a vector comprising of all the coordinates of the points. The graph G has a vertex for each point and an edge for each specified distance. Since the coordinates of the points are specified in (G, p) it is a simple matter to determine the relative distance corresponding to any edge of G . The framework (G, p) therefore represents both a system of polynomial equations and a particular solution to these equations. We will call these equations the framework equations - they correspond to the dimensional constraint equations referred to above. In general the framework vector p will be just one of the many possible solutions to the framework equations. (Estimates on the number of solutions have been obtained by several authors, see for example [1, 7, 15].)

Efficient algorithms for solving the framework equations are extremely useful. A particularly desirable case is when there are only a finite number of solutions, and these solutions can be expressed as a sequence of square, or integer power, roots of combinations of the squared edge lengths. Such frameworks are said to be quadratically solvable and radically solvable, respectively. A quadratically solvable framework is referred to as being ruler-and-compass-constructible in [4] since it can be drawn in the plane with a ruler marked with the edge-lengths and a compass. We will consider the problem of determining which generic frameworks are quadratically or radically solvable.

The conditions that the system of equations defined by a generic framework should have only finitely many solutions, or a unique solution, are equivalent to the statements that the framework is rigid or globally rigid, respectively. These properties have been extensively studied and we refer the reader to [18] for an excellent survey of the area. In particular characterisations and recursive constructions for graphs with the property that any generic realisation is rigid, or globally rigid, are given in [9] and [6], respectively. Previous

work on quadratic/radical solvability [12, 13] considered generic frameworks which are minimally rigid i.e. cease to be rigid when any edge is removed. It was conjectured in [12] that the family of minimally rigid graphs G with the property that any generic realisation of G is radically/quadratically solvable is equal to the recursively constructed family \mathcal{F}_{min} obtained from K_2 by recursively choosing three graphs $G_i = (V_i, E_i) \in \mathcal{F}_{min}$ with $|V_i \cap V_j| = 1$ and $V_1 \cap V_2 \cap V_3 = \emptyset = E_i \cap E_j$, and putting $G_1 \cup G_2 \cup G_3 \in \mathcal{F}_{min}$. This conjecture was verified for the special case when the underlying graph is 3-connected and planar in [13].

Theorem 1.1 *No generic realisation of a 3-connected planar minimally rigid graph is quadratically (or radically) solvable.*

We will extend the study of quadratic and radical solvability to include generic frameworks which are rigid but not necessarily minimally rigid. We first show that quadratic and radical solvability are both *generic properties* i.e. they depend only on the underlying graph when the given framework is generic. This allows us to define a graph as being quadratically, or radically, solvable if some (or equivalently every) generic realisation has this property. Our aim is to characterise these graphs. As a first step we show that a graph G is quadratically solvable if it is globally rigid. We conjecture that globally rigid graphs are the fundamental building blocks for all quadratically/radically solvable graphs. More precisely, let \mathcal{F} be the recursively defined family of graphs obtained by first putting all globally rigid graphs in \mathcal{F} . Then, for any $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ in \mathcal{F} with $V_1 \cap V_2 = \{u, v\}$ and $|V_1|, |V_2| \geq 3$ we put:

- (a) $G_1 \cup G_2$ in \mathcal{F} ;
- (b) $(G_1 - e) \cup G_2$ in \mathcal{F} if $e = uv \in E_1$;
- (c) $(G_1 - e) \cup (G_2 - e)$ in \mathcal{F} if $e = uv \in E_1 \cap E_2$ and $G_1 - e, G_2 - e$ are both rigid.

This construction is illustrated in Figure 1. (Note that all 3-connected graphs in \mathcal{F} are globally rigid.)

Conjecture 1.2 *A graph is radically (or quadratically) solvable if and only if it belongs to \mathcal{F} .*

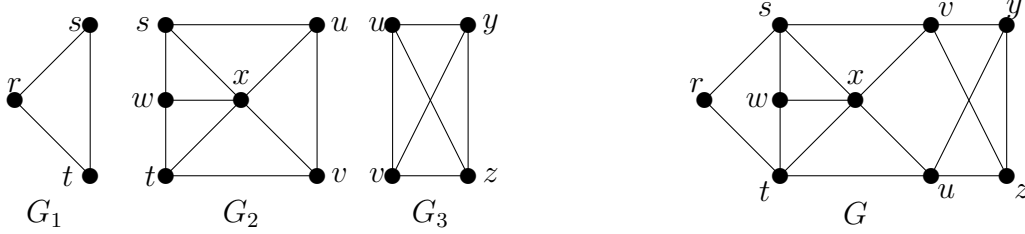


Figure 1: Three globally rigid graphs G_1, G_2, G_3 are combined to give a graph G in \mathcal{F} . We first construct $G_4 = (G_1 - st) \cup G_2$ using operation (b). We then construct $G = (G_4 - uv) \cup (G_3 - uv)$ using operation (c).

Our main results are to show that all graphs in \mathcal{F} are quadratically solvable, and that all radically solvable planar graphs belong to \mathcal{F} .

An outline of the paper is as follows. We give definitions and preliminary results on frameworks and radical/quadratic solvability in Section 2. We show that radical/quadratic solvability are generic properties in section 3. We prove that all graphs in the family \mathcal{F} are quadratically solvable in Section 4 and that all radically solvable planar graphs belong to \mathcal{F} in section 5.

2 Definitions and preliminary results

2.1 Rigid and globally rigid frameworks

All graphs considered are finite and without loops or multiple edges. Given a graph $G = (V, E)$ and two vertices $u, v \in V$ we use $G + uv$ to denote the graph obtained from G by adding the edge uv if it is not already in E .

A *real, respectively complex, framework* is a pair (G, p) where G is a graph and $p : V \rightarrow \mathbb{R}^2$, respectively $p : V \rightarrow \mathbb{C}^2$. We will also say that (G, p) is a *realisation* of G . Although we are mainly concerned with real frameworks, we will work with complex frameworks since most of our methods require an algebraically closed field and our results will still hold for the special case of real frameworks. A framework (G, p) is *generic* if the set of all coordinates of the points $p(v)$, $v \in V$, is algebraically independent over \mathbb{Q} .

Let $V = \{v_1, v_2, \dots, v_n\}$ and $E = \{e_1, e_2, \dots, e_m\}$. Given a realisation (G, p) of G and two vertices $v_i, v_j \in V$ with $p(v_i) - p(v_j) = (a, b)$ put $d_p(v_i, v_j) = a^2 + b^2$ and $d_p(e) = d_p(v_i, v_j)$ when $e = v_i v_j \in E$. Two realisations (G, p) and (G, q) are *equivalent* if $d_p(e) = d_q(e)$ for all $e \in E$, and

are *congruent* if $d_p(v_i, v_j) = d_q(v_i, v_j)$ for all $v_i, v_j \in V$. The *rigidity map* $d_G : \mathbb{C}^{2n} \rightarrow \mathbb{C}^m$ is defined by putting $d_G(p) = (d_p(e_1), d_p(e_2), \dots, d_p(e_m))$. Thus (G, p) and (G, q) are equivalent if and only if $d_G(p) = d_G(q)$. Note that, if (G, p) and (G, q) are real frameworks, then they are equivalent if and only if they have the same edge lengths and they are congruent if and only if we can transform one to the other by applying an isometry of \mathbb{R}^2 i.e. a translation, rotation or reflection of the Euclidean plane.

A real, respectively complex, framework (G, p) is *globally real, respectively complex, rigid* if all equivalent real, respectively complex, frameworks are congruent to it. It is *real, respectively complex, rigid* if there exists an $\epsilon > 0$ such that every real, respectively complex, framework (G, q) which is equivalent to (G, p) and satisfies $\|p(v) - q(v)\|^2 < \epsilon$ for all $v \in V$, is congruent to (G, p) .¹ It is known that a real generic framework is real rigid, respectively globally real rigid, if and only if it is complex rigid, respectively globally complex rigid, and that both these properties depend only on the underlying graph when the framework is generic, see [5, 13]. We say that a graph G is *rigid* or *globally rigid* if some, or equivalently every, generic realisation of G has the same property.

2.2 Radically/quadratically solvable frameworks

Let K, L be fields with $K \subseteq L$. Then L is a *radical extension* of K if there exist fields $K = K_1 \subset K_2 \subset \dots \subset K_t = L$ such that for all $1 \leq i < t$, $K_{i+1} = K_i(x_i)$ with $x_i^{n_i} \in K_i$ for some natural number n_i . The field L is a *quadratic extension* of K if it is a radical extension with $n_i = 2$ for all $1 \leq i < t$. The field extension $L : K$ is *radically solvable*, respectively *quadratically solvable*, if L is contained in a radical, respectively quadratic, extension of K .

A framework (G, p) is *radically solvable*, respectively *quadratically solvable*, if there exists a congruent framework (G, q) such that $\mathbb{Q}(q) : \mathbb{Q}(d_G(q))$ is radically, respectively quadratically, solvable. Given a framework (G, p) , it will be useful to identify a congruent framework (G, q) which has the property that (G, p) is radically, or quadratically, solvable if and only if $\mathbb{Q}(q)$ is contained in a radical, or quadratic, extension of $\mathbb{Q}(d_G(q))$. The following concept will enable us to do this.

¹Equivalently, a real, respectively complex, framework (G, p) is real, respectively complex, rigid if every continuous motion of the points $p(v)$, in \mathbb{R}^2 , respectively \mathbb{C}^2 , which preserves the ‘edge distances’ $d_p(e)$ results in a framework which is congruent to (G, p) .

We say that a framework (G, p) with $G = (V, E)$, $V = \{v_1, v_2, \dots, v_n\}$ and $n \geq 2$ is in *standard position with respect to* (v_1, v_2) if $p(v_1) = (0, 0)$ and $p(v_2) = (0, y_2)$ with $y_2 \neq 0$. It is *collinear* if $p(u) - p(v) \in \langle s \rangle$ for all $u, v \in V$, for some fixed vector $s \in \mathbb{C}^2$.

Our first result tells us that most frameworks are congruent to a framework in standard position.

Lemma 2.1 *Let (G, p) be a complex framework, v_1, v_2 be vertices of G with $d(p(v_1) - p(v_2)) \neq 0$, and S be the set of all equivalent frameworks. Then (G, p) is congruent to a framework in standard position with respect to (v_1, v_2) . Furthermore:*

(a) *if (G, p) is not collinear, then each congruence class in S has exactly four realisations (G, q_i) , $1 \leq i \leq 4$, in standard position with respect to v_1, v_2 , and $\mathbb{Q}(q_i) = \mathbb{Q}(q_j)$ for all $1 \leq i < j \leq 4$.*

(b) *if (G, p) is collinear, then each congruence class in S has exactly two realisations (G, q_i) , $1 \leq i \leq 2$, in standard position with respect to v_1, v_2 , and $\mathbb{Q}(q_1) = \mathbb{Q}(q_2)$.*

Proof. The assertions that (G, p) is congruent to a framework in standard position with respect to (v_1, v_2) and that there are exactly four, respectively two, such realisations (G, q_i) when (G, p) is not collinear, respectively is collinear, follow from [7, Lemma 3.1]. The assertion that $\mathbb{Q}(q_i) = \mathbb{Q}(q_j)$ for $1 \leq i \leq 4$ in case (a) follows from the fact that we can order the q_i such that, if $q_1(v_k) = (x_k, y_k)$ for all $v_k \in V$, then $q_2(v_k) = (-x_k, y_k)$, $q_3(v_k) = (x_k, -y_k)$ and $q_4(v_k) = (-x_k, -y_k)$ for all $v_k \in V$. A similar proof holds in case (b). •

We can use this lemma to deduce that a framework (G, p) with $d_p(u, v) \neq 0$ for some pair of vertices u, v is radically, or quadratically, solvable if and only if it is congruent to a framework (G, q) in standard position and such that $\mathbb{Q}(q)$ is contained in a radical, or quadratic, extension of $\mathbb{Q}(d_G(q))$.

Lemma 2.2 *Suppose that (G, p) is a complex framework with, $G = (V, E)$, $V = \{v_1, v_2, \dots, v_n\}$ and $d_p(v_1, v_2) \neq 0$. Let (G, q) be a congruent realisation in standard position with respect to (v_1, v_2) . Then (G, p) is radically, respectively quadratically, solvable if and only if $\mathbb{Q}(q) : \mathbb{Q}(d_G(q))$ is radically, respectively quadratically, solvable.*

Proof. Sufficiency follows immediately from the definition of radical, respectively quadratic, solvability. To prove necessity we suppose that (G, p) is

radically, respectively quadratically, solvable. Replacing (G, p) by a congruent framework if necessary, we may assume that $\mathbb{Q}(p)$ is itself contained in a radical, respectively quadratic, extension L of $\mathbb{Q}(d_G(p))$. We can construct a framework (G, q) which is congruent to (G, p) and in standard position with respect to (v_1, v_2) by putting $\tilde{q}(v_i) = p(v_i) - p(v_1)$ for all $v_i \in V$, and

$$q(v_i) = \begin{pmatrix} y/d_0 & -x/d_0 \\ x/d_0 & y/d_0 \end{pmatrix} \tilde{q}(v_i)$$

for all $v_i \in V(G)$, where $\tilde{q}(v_2) = (x, y)$ and $d_0^2 = x^2 + y^2$. By Lemma 2.1, it will suffice to show that for this q , $\mathbb{Q}(q)$ is contained in a radical, respectively quadratic, extension of $\mathbb{Q}(d_G(q))$. Let $K = \mathbb{Q}(p, d_0)$. The definitions of \tilde{q} and q imply that $\mathbb{Q}(\tilde{q}) \subseteq \mathbb{Q}(p)$ and hence that $\mathbb{Q}(q) \subseteq K$. We have $[K : \mathbb{Q}(p)] \leq 2$ since $d_0^2 = x^2 + y^2$ and $x, y \in \mathbb{Q}(p)$. Hence $L(d_0)$ is a radical, respectively quadratic, extension of $\mathbb{Q}(d_G(p))$ which contains K . Since $\mathbb{Q}(q) \subseteq K$ and $d_G(p) = d_G(q)$, $\mathbb{Q}(q) : \mathbb{Q}(d_G(q))$ is radically, respectively quadratically, solvable. •

Remarks

1. If (G, p) is a real framework then the congruent framework (G, q) constructed in Lemma 2.2 will also be real.
2. The condition that $d_p(v_1, v_2) \neq 0$ is equivalent to $p(v_1) - p(v_2) \neq (z, \pm iz)$ for all $z \in \mathbb{C}$. When (G, p) is real this reduces to $p(v_1) \neq p(v_2)$.
3. If (G, p) is a framework with $d_p(u, v) = 0$ for all pairs of vertices u, v then (G, p) is quadratically solvable since it is congruent to the framework (G, q) with $q(v) = 0$ for all $v \in V$.

We close this section by showing that every globally complex rigid framework (G, p) is quadratically solvable. Given a field K we use \overline{K} to denote the algebraic closure of K , $K[X_1, X_2, \dots, X_n]$ to denote the ring of polynomials in the indeterminates X_1, X_2, \dots, X_n with coefficients in K and $K(X_1, X_2, \dots, X_n)$ to denote its field of fractions.

We will need the result from algebraic geometry that if I is a zero-dimensional ideal of $K[X_1, X_2, \dots, X_n]$ and b_1 is a zero of $I \cap K[X_1]$ in \overline{K} , then b_1 can be extended to a zero (b_1, b_2, \dots, b_n) of I in \overline{K}^n . This follows implicitly from Buchberger's algorithm for solving systems of polynomial equations [2], or from the following more explicit result of Kalkbrener [8, Theorem 3].

Theorem 2.3 *Let K be a field, I be a zero-dimensional ideal of $K[X_1, X_2, \dots, X_n]$ and b be a zero of $I \cap K[X_1, X_2, \dots, X_{m-1}]$ in \overline{K}^{m-1} for some $m \geq 2$. Then there exists a polynomial $f \in I \cap K[X_1, X_2, \dots, X_m]$ such that $f(b, X_m)$ is a non constant polynomial which generates $\{h(b, X_m) : h \in I \cap K[X_1, X_2, \dots, X_m]\}$.*

This result implies that $b = (b_1, b_2, \dots, b_{m-1})$ can be extended to a zero (b_1, b_2, \dots, b_m) of $I \cap K[X_1, X_2, \dots, X_m]$ by choosing b_m to be a zero of $f(b_1, b_2, \dots, b_{m-1}, X_m)$ in \overline{K} . Applying this recursively, we may deduce that b_1 can be extended to a zero of I .

We will also need the following concept from rigidity theory. Two vertices v_i, v_j of a framework (G, p) are *globally linked* if for every equivalent realisation (G, q) we have $d_p(v_i, v_j) = d_q(v_i, v_j)$.

Lemma 2.4 *Let (G, p) be a complex realisation of a graph $G = (V, E)$ with $V = \{v_1, v_2, \dots, v_n\}$ and $E = \{e_1, e_2, \dots, e_m\}$. Suppose that (G, p) has only finitely many equivalent non-congruent realisations and that v_1, v_2 are globally linked in (G, p) . Then $d_p(v_1, v_2) \in \mathbb{Q}(d_G(p))$.*

Proof. The lemma is trivially true if $d_p(v_1, v_2) = 0$. Hence we can suppose that $d_p(v_1, v_2) \neq 0$. By Lemma 2.1 we may assume that (G, p) is in standard position with respect to (v_1, v_2) . Let $K = \mathbb{Q}(d_G(p))$. We again associate a pair of indeterminates (X_{2i-1}, X_{2i}) with each vertex $v_i \in V$, putting $X_1 = X_2 = X_3 = 0$ to represent a framework in standard position. Let $f_i = (X_{2j-1} - X_{2k-1})^2 + (X_{2j} - X_{2k})^2 - d((p(v_j) - p(v_k)))$ for each $e_i = v_j v_k \in E$. We introduce a new indeterminate X_{2n+1} which represents the ‘distance’ between v_1 and v_2 and put $f_{m+1} = X_{2n+1} - X_4^2$. Let $X = (X_4, X_5, \dots, X_{2n+1})$. Let I be the ideal of $K[X]$ generated by the polynomials f_1, f_2, \dots, f_{m+1} . Then I is zero-dimensional since (G, p) has only finitely many equivalent non-congruent realisations. In addition $I_{2n+1} = I \cap K[X_{2n+1}]$ is a principal ideal and hence is generated by a single polynomial $h_{2n+1} \in K[X_{2n+1}]$. Theorem 2.3 now implies that every zero of h_{2n+1} in \overline{K} extends to a zero of I in \overline{K}^{2n+1} . Since v_1, v_2 are globally linked in G , $d_p(v_1, v_2)$ must be the unique zero of h_{2n+1} . Thus $h_{2n+1} = (X_{2n+1} - d_p(v_1, v_2))^t$ for some positive integer t . Since $h_{2n+1} \in K[X_{2n+1}]$ this implies that $d_p(v_1, v_2) \in K$. •

Theorem 2.5 *Suppose that (G, p) is a globally complex rigid framework. Then (G, p) is quadratically solvable.*

Proof. We have already seen that every framework (G, p) with $d_p(u, v) = 0$ for all vertices u, v is quadratically solvable. Hence we may assume that $G = (V, E)$ with $V = \{v_1, v_2, \dots, v_n\}$, $E = \{e_1, e_2, \dots, e_m\}$ and $d_p(v_1, v_2) \neq 0$. By Lemma 2.1, we may suppose that (G, p) is in standard position with respect to (v_1, v_2) . Let $p(v_2) = (0, y_2)$, $K = \mathbb{Q}(d_G(p))$ and $K_1 = K(y_2)$. Since y_2 satisfies the quadratic equation $y_2^2 - d_p(v_1, v_2) = 0$, and since $d_p(v_1, v_2) \in K$ by Lemma 2.4, we have $[K_1 : K] \leq 2$. Let $p(v_i) = (x_i, y_i)$ for all $3 \leq i \leq n$. Then $x_i^2 + y_i^2 = d_p(v_i, v_1)$ and $x_i^2 + (y_i - y_2)^2 = d_p(v_i, v_2)$. Since G is globally rigid, v_i is globally linked to both v_1 and v_2 in G and hence, by Lemma 2.4, $\{d_p(v_i, v_0), d_p(v_i, v_1)\} \subset K$. This implies that $y_i \in K_1$ and $x_i^2 \in K_1$. Since this holds for all $3 \leq i \leq n$, (G, p) is quadratically solvable. \bullet

3 Radical and quadratic solvability of generic frameworks

We will show in this section that radical and quadratic solvability are generic properties. We first recall some definitions and results from Galois theory. We adopt the notation of [16] and refer the reader to this text for further information on the subject.

Given a field extension $L : K$ we use $[L : K]$ to denote the *degree* of the extension i.e. the dimension of L as a vector space over K . The extension is *finite* if it has finite degree. It is *normal* if L is the splitting field of some polynomial over K . When $L : K$ is finite, a *normal closure of L over K* is a field N such that $L \subseteq N$, $N : K$ is normal, and, subject to these conditions, N is minimal with respect to inclusion. It is known that normal closures exist, are finite, and are unique up to isomorphism, see [16, Theorem 11.6]. The *Galois group* $\Gamma(L : K)$ is the group of all automorphisms of L which leave K fixed. Galois theory gives us the following close relationship between radically/quadratically solvable extensions and Galois groups, see [16].

Theorem 3.1 *Let K be a field of characteristic zero, $L : K$ be a finite field extension and N be a normal closure of L over K . Then the following statements are equivalent:*

- (a) $L : K$ is radically, respectively quadratically, solvable;
- (b) $N : K$ is radically, respectively quadratically, solvable;

(c) $\Gamma(N : K)$ is a solvable group, respectively a 2-group (i.e. $|\Gamma(N : K)| = 2^m$ for some non-negative integer m).

A framework is said to be *quasi-generic* if it is congruent to a generic framework. We first show that if (G, p) is a quasi-generic rigid framework and is in standard position then $\mathbb{Q}(p) : \mathbb{Q}(d_G(p))$ is a finite field extension. We will need one more result from [7] to prove this.

Lemma 3.2 [7, Lemmas 3.4, 3.5] *Suppose that (G, p) is a quasi-generic realisation of a rigid graph $G = (V, E)$ where $V = \{v_1, v_2, \dots, v_n\}$ and $p(v_i) = (x_i, y_i)$ for $1 \leq i \leq n$. Suppose further that (G, p) is in standard position with respect to (v_1, v_2) , i.e. $x_1 = y_1 = x_2 = y_2 = 0$. Then $\{y_2, x_3, y_3, \dots, y_n\}$ is algebraically independent over \mathbb{Q} , and $\overline{\mathbb{Q}(p)} = \overline{\mathbb{Q}(d_G(p))}$.*

Lemma 3.3 *Suppose that $G = (V, E)$ is a rigid graph and that (G, p) is a quasi-generic realisation of G in standard position with respect to two vertices $v_1, v_2 \in V$. Then $\mathbb{Q}(p) : \mathbb{Q}(d_G(p))$ is a finite field extension.*

Proof. It is easy to see that $\mathbb{Q}(d_G(p)) \subseteq \mathbb{Q}(p)$. By Lemma 3.2, $\mathbb{Q}(p)$ and $\mathbb{Q}(d_G(p))$ have the same algebraic closure. This implies that each coordinate of p is a root of a polynomial with coefficients in $\mathbb{Q}(d_G(p))$ and hence $[\mathbb{Q}(p) : \mathbb{Q}(d_G(p))]$ is finite. •

Lemma 3.4 *Suppose (G, q) and (G, q') are two quasi-generic realisations of a rigid graph $G = (V, E)$ in standard position with respect to two vertices $v_1, v_2 \in V$. Let N_q and $N_{q'}$ be normal closures of $\mathbb{Q}(q) : \mathbb{Q}(d_G(q))$ and $\mathbb{Q}(q') : \mathbb{Q}(d_G(q'))$, respectively. Then $\Gamma(N_q : \mathbb{Q}(d_G(q)))$ and $\Gamma(N_{q'} : \mathbb{Q}(d_G(q')))$ are isomorphic groups.*

Proof. Let $V = \{v_1, v_2, \dots, v_n\}$ and $E = \{e_1, e_2, \dots, e_m\}$. Let $q(v_i) = (x_{2i-1}, x_{2i})$ and $q'(v_i) = (x'_{2i-1}, x'_{2i})$ for $1 \leq i \leq n$. We associate a pair of indeterminates (X_{2i-1}, X_{2i}) with each vertex $v_i \in V$, putting $X_1 = X_2 = X_3 = 0$ to represent a framework in standard position. Let $X = (X_4, X_5, \dots, X_{2n})$ and $D_G(X) = (f_1, f_2, \dots, f_m)$ where $f_i = (X_{2j-1} - X_{2k-1})^2 + (X_{2j} - X_{2k})^2$ when $e_i = v_j v_k$. Since (G, q) and (G, q') are quasi-generic, Lemma 3.2 implies that $\{x_3, x_4, \dots, x_{2n}\}$ and $\{x'_3, x'_4, \dots, x'_{2n}\}$ are both algebraically independent over \mathbb{Q} . Hence $\mathbb{Q}(q) : \mathbb{Q}(d_G(q))$ and $\mathbb{Q}(q') : \mathbb{Q}(d_G(q'))$ are both isomorphic to $\mathbb{Q}(X) : \mathbb{Q}(D_G(X))$.

Let N_X be the normal closure of $\mathbb{Q}(X) : \mathbb{Q}(D_G(X))$. Then $N_q : \mathbb{Q}(d_G(q))$ and $N_{q'} : \mathbb{Q}(d_G(q'))$ are both isomorphic to $N_X : \mathbb{Q}(D_G(X))$ and hence are isomorphic to each other. It follows that $\Gamma(N_q : \mathbb{Q}(d_G(q)))$ and $\Gamma(N_{q'} : \mathbb{Q}(d_G(q')))$ are isomorphic groups. \bullet

Theorem 3.1 and Lemmas 2.2, 3.4 imply that radical/quadratic solvability are generic properties. This allows us to define a rigid graph to be *radically*, respectively *quadratically*, *solvable* if some (or equivalently every) generic realisation of G is radically, respectively quadratically, solvable. Note that Lemmas 2.2 and 3.4 also imply that this definition agrees with the one given for the radical and quadratic solvability of minimally rigid graphs in [13, Definition 3.1].

4 A family of quadratically solvable graphs

We will show that each of the graphs in the family \mathcal{F} defined immediately before Conjecture 1.2 are rigid and quadratically solvable. We will need the following rather technical lemmas to determine whether generic realisations of rigid graphs with small separating sets of vertices are radically or quadratically solvable. We will delay their proofs until the appendix.

Lemma 4.1 *Let $L : K$ be a finite field extension with $\mathbb{Q} \subseteq K \subseteq L \subseteq \mathbb{C}$, and N be the normal closure of $L : K$ in \mathbb{C} . Let $X = (X_1, X_2, \dots, X_n)$ be a vector of indeterminates. Then $N(X)$ is a normal closure of $L(X)$ over $K(X)$ and $\Gamma(N : K)$ is isomorphic to $\Gamma(N(X) : K(X))$. Furthermore, $L : K$ is radically, respectively quadratically, solvable if and only if $L(X) : K(X)$ is radically, respectively quadratically, solvable.*

Lemma 4.2 *Suppose that $X = (X_1, X_2, \dots, X_r)$, $Y = (Y_1, Y_2, \dots, Y_s)$ and $Z = (Z_1, Z_2, \dots, Z_t)$ are vectors of indeterminates, $f = (f_1, f_2, \dots, f_m) \in \mathbb{Q}[X, Y]^m$, $g = (g_1, g_2, \dots, g_n) \in \mathbb{Q}[Y, Z]^n$, and $\mathbb{Q}(X, Y, Z)$ is a finite extension of $\mathbb{Q}(f, g)$. Then $\mathbb{Q}(X, Y, Z) : \mathbb{Q}(f, g)$ is radically, respectively quadratically, solvable if and only if $\mathbb{Q}(f, Y, Z) : \mathbb{Q}(f, g)$ and $\mathbb{Q}(X, Y) : \mathbb{Q}(f, Y)$ are both radically, respectively quadratically, solvable.*

Lemma 4.3 *Let G be a rigid graph with $G = H_1 \cup H_2$ for two subgraphs $H_1 = (V_1, E_1)$ and $H_2 = (V_2, E_2)$ with $V_1 \cap V_2 = \{v_1, v_2\}$ and $E_1 \cap E_2 = \emptyset$. (a) Suppose that H_1, H_2 are both rigid. Then G is radically, respectively*

quadratically, solvable if and only if $H_1 + v_1v_2, H_2 + v_1v_2$ are both radically, respectively quadratically, solvable.

(b) Suppose that H_1 is not rigid. Then $H_1 + v_1v_2$ and H_2 are both rigid. Furthermore:

(i) if $H_1 + v_1v_2$ and H_2 are both radically, respectively quadratically, solvable then G is radically, respectively quadratically, solvable;

(ii) if G is radically, respectively quadratically, solvable then $H_1 + v_1v_2$ and $H_2 + v_1v_2$ are both radically, respectively quadratically, solvable.

(iii) if G is radically, respectively quadratically, solvable and $H_1 + v_1v_2$ is minimally rigid, then $H_1 + v_1v_2$ and H_2 are both radically, respectively quadratically, solvable.

Proof. Choose a quasi-generic realisation (G, p) of G with $p(v_1) = (0, 0)$ and $p(v_2) = (0, y)$ for some $y \in \mathbb{C}$.

(a) Suppose that $H_1 + v_1v_2$ and $H_2 + v_1v_2$ are both radically, respectively quadratically, solvable. Then $\mathbb{Q}(p|_{V_i})$ is a radically, respectively quadratically, solvable extension of $\mathbb{Q}(d_{H_i+v_1v_2}(p))$ for $i = 1, 2$. It follows that $\mathbb{Q}(p)$ is a radically, respectively quadratically, solvable extension of $\mathbb{Q}(d_{G+v_1v_2}(p))$. Since H_1, H_2 are both rigid, [7, Lemma 8.2] implies that v_1 and v_2 are globally linked in (G, p) . By Lemma 2.4, $d_p(v_1, v_2) \in \mathbb{Q}(d_G(p))$ and hence $\mathbb{Q}(d_{G+v_1v_2}(p)) = \mathbb{Q}(d_G(p))$. Thus $\mathbb{Q}(p)$ is a radically, respectively quadratically, solvable extension of $\mathbb{Q}(d_G(p))$ and G is radically, respectively quadratically, solvable.

Suppose on the other hand that G is radically, respectively quadratically, solvable. Then $\mathbb{Q}(p)$ is a radically, respectively quadratically, solvable extension of $\mathbb{Q}(d_G(p))$. Since (G, p) is quasi-generic, the non-zero components of p are algebraically independent over \mathbb{Q} . Hence we may treat them as if they were indeterminates and apply Lemma 4.2 with $f = d_{H_1}(p)$, $g = d_{H_2}(p)$, $X = p|_{V_1 \setminus \{v_1, v_2\}}$, $Y = y$, and $Z = p|_{V_2 \setminus \{v_1, v_2\}}$ to deduce that $\mathbb{Q}(p|_{V_1})$ is a radically, respectively quadratically, solvable extension of $\mathbb{Q}(d_{H_1}(p), y)$. Thus $\mathbb{Q}(p|_{V_1})$ is a radically, respectively quadratically, solvable extension of $\mathbb{Q}(d_{H_1+v_1v_2}(p))$ and so $H_1 + v_1v_2$ is radically, respectively quadratically, solvable. By symmetry, $H_2 + v_1v_2$ is also radically, respectively quadratically, solvable.

(b) The fact that $H_1 + v_1v_2$ and H_2 are both rigid follows from [7, Lemma 8.5].

Suppose that $H_1 + v_1v_2$ and H_2 are both radically, respectively quadratically, solvable. Then $\mathbb{Q}(p|_{V_2})$ is a radically, respectively quadratically, solv-

able extension of $\mathbb{Q}(d_{H_2}(p))$. We also have $\mathbb{Q}(p|_{V_1})$ is a radically, respectively quadratically, solvable extension of $\mathbb{Q}(d_{H_1+v_1v_2}(p))$. Since $y \in \mathbb{Q}(p|_{V_2})$, we have $\mathbb{Q}(p|_{V_1}, p|_{V_2})$ is a radically, respectively quadratically, solvable extension of $\mathbb{Q}(d_{H_1}(p), p|_{V_2})$. Thus $\mathbb{Q}(p)$ is a radically, respectively quadratically, solvable extension of $\mathbb{Q}(d_G(p))$ and G is radically, respectively quadratically, solvable. Hence (i) holds.

Suppose on the other hand that that G is radically, respectively quadratically, solvable. Then $\mathbb{Q}(p)$ is a radically, respectively quadratically, solvable extension of $\mathbb{Q}(d_G(p))$. We may apply the argument used in the second part of the proof of (a) to deduce that $\mathbb{Q}(p|_{V_1})$ is a radically, respectively quadratically, solvable extension of $\mathbb{Q}(d_{H_1+v_1v_2}(p))$, and $\mathbb{Q}(p|_{V_2})$ is a radically, respectively quadratically, solvable extension of $\mathbb{Q}(d_{H_2+v_1v_2}(p))$. Hence (ii) holds.

To prove (iii) we need to show that y belongs to a radical, respectively quadratic, extension of $\mathbb{Q}(d_{H_2}(p))$ when $H_1 + v_1v_2$ is minimally rigid. In this case [7, Lemma 5.6] implies that $X = d_{H_1}(p)$ is algebraically independent over $\mathbb{Q}(d_{H_2+v_1v_2}(p))$. Let $K = \mathbb{Q}(d_{H_2}(p))$ and $L = K(y)$. Since G is radically, respectively quadratically, solvable, $L(X) : K(X)$ is radically, respectively quadratically, solvable. Since X is algebraically independent over L , Lemma 4.1 implies that $L : K$ is radically, respectively quadratically, solvable. Part (iii) now follows since $y \in L$. •

We do not know whether the hypothesis that $H_1 + v_1v_2$ is minimally rigid can be removed from Theorem 4.3(b)(iii). The difficulty in extending the above proof when $H_1 + v_1v_2$ is not minimally rigid is that $d_{H_1}(p)$ will not be algebraically independent over $\mathbb{Q}(d_{H_2+v_1v_2}(p))$. So it is conceivable that $\mathbb{Q}(d_{H_1}(p))$ may contain algebraic numbers which enable y to belong to a radical extension of $\mathbb{Q}(d_G(p))$ but not to a radical extension of $\mathbb{Q}(d_{H_2}(p))$. On the other hand, we will see in the next section that we can side step this problem and still obtain a characterization of radically solvable rigid planar graphs. We will accomplish this by only considering certain separations (H_1, H_2) of G and applying the following result.

Corollary 4.4 *Let G be a rigid graph with $G = H_1 \cup H_2 \cup H_3$ for subgraphs $H_i = (V_i, E_i)$ with $V_i \cap V_j = \{v_k\}$ and $V_1 \cap V_2 \cap V_3 = \emptyset = E_i \cap E_j$ for all $\{i, j, k\} = \{1, 2, 3\}$. Then H_1, H_2, H_3 are rigid. Furthermore, G is radically, respectively quadratically, solvable if and only if H_1, H_2, H_3 are radically, respectively quadratically, solvable.*

Proof. Since $G = (H_1 \cup H_2) \cup H_3$ is rigid and $H_1 \cup H_2$ is not rigid, Theorem 4.3(b) implies that H_3 is rigid. We may now use symmetry to deduce that H_1, H_2 are also rigid.

Suppose G is radically, respectively quadratically, solvable. By Theorem 4.3(b)(ii), $(H_1 \cup H_2) + v_1v_2$ is radically, respectively quadratically, solvable. Since $(H_1 \cup H_2) + v_1v_2 = H_1 \cup (H_2 + v_2 + v_1v_2)$ we may again use Theorem 4.3(b)(ii) to deduce that $H_2 + v_2 + v_2v_3 + v_1v_2$ is radically, respectively quadratically, solvable. We can now express $H_2 + v_2 + v_2v_3 + v_1v_2$ as $(K_3 - v_1v_3) \cup H_2$ where $V(K_3) = \{v_1, v_2, v_3\}$. Since K_3 is minimally rigid, we may apply Theorem 4.3(b)(iii) to deduce that H_2 is radically, respectively quadratically, solvable. By symmetry H_1, H_3 are also radically, respectively quadratically, solvable.

Suppose on the other hand that H_1, H_2, H_3 are radically, respectively quadratically, solvable. Let K_3 be a complete graph with $V(K_3) = \{v_1, v_2, v_3\}$. Then K_3 is globally rigid and hence quadratically solvable, so by Theorem 4.3(b)(i), $F_1 = (K_3 - v_1v_3) \cup H_2$ is radically, respectively quadratically, solvable. We may now apply Theorem 4.3(b)(i) to $F_2 = (F_1 - v_2v_3) \cup H_1$ to deduce that F_2 is radically, respectively quadratically, solvable. Finally we apply Theorem 4.3(b)(i) to $G = (F_2 - v_1v_2) \cup H_3$ to deduce that G is radically, respectively quadratically, solvable. \bullet

Theorem 4.5 *Every graph in \mathcal{F} is rigid and quadratically solvable.*

Proof. Suppose $G \in \mathcal{F}$. We show that G is rigid and quadratically solvable by induction on $|E|$. If G is globally rigid then G is rigid, and is quadratically solvable by Theorem 2.5. Hence we may suppose that G is not globally rigid. The definition of \mathcal{F} now implies that there exist graphs $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ in \mathcal{F} with $V_1 \cap V_2 = \{u, v\}$ and such that either: $G = G_1 \cup G_2$; or $G = (G_1 - e) \cup G_2$ for $e = uv \in E_1$; or $G = (G_1 - e) \cup (G_2 - e)$ for $e = uv \in E_1 \cap E_2$ and $G_1 - e, G_2 - e$ both rigid. By induction G_1 and G_2 are both rigid and quadratically solvable.

We first show that G is rigid. Since G_1, G_2 are rigid and $|V_1 \cap V_2| \geq 2$, $G_1 \cup G_2$ is rigid. Furthermore, if $e = uv \in E_1$ then e is a redundant edge in $G_1 \cup G_2$, so $(G_1 - e) \cup G_2$ is also rigid. Finally, if $e \in E_1 \cap E_2$ and $G_1 - e$ and $G_2 - e$ are both rigid then $(G_1 - e) \cup (G_2 - e)$ is rigid. Hence G is rigid.

It remains to show that G is quadratically solvable. Since G_1 and G_2 are quadratically solvable, $G_1 + uv$ and $G_2 + uv$ are quadratically solvable.

Hence $G_1 \cup G_2$ is quadratically solvable by Theorem 4.3(a). Suppose that $e = uv \in E_1$ and let $H_1 = G_1 - e$ and $H_2 = G_2$. We can deduce that $G = H_1 \cup H_2$ is quadratically solvable by applying Theorem 4.3(a) to H_1 and $H_2 + uv$ if H_1 is rigid, and by applying Theorem 4.3(b)(i) to H_1 and H_2 if H_1 is not rigid. Thus $(G_1 - e) \cup G_2$ is quadratically solvable. Finally we suppose that $e \in E_1 \cap E_2$ and $G_1 - e, G_2 - e$ are both rigid. Then $(G_1 - e) \cup (G_2 - e)$ is quadratically solvable by Theorem 4.3(a). \bullet

5 Radically solvable planar graphs

We will show that all radically solvable planar graphs belong to \mathcal{F} . Our proof splits into two cases depending on the connectivity of the graph.

5.1 Graphs of connectivity at least three

Conjecture 1.2 implies that a 3-connected graph is radically (or quadratically) solvable if and only if it is globally rigid. We will verify this statement for 3-connected planar graphs. Our proof uses the following lemma to reduce to the case of minimally rigid graphs and then applies Theorem 1.1. The lemma is illustrated in Figure 2.

Lemma 5.1 *Let $G_1 = H_0 \cup H_1$ and $G_2 = H_0 \cup H_2$ be graphs with $V(H_0) \cap V(H_1) = V(H_0) \cap V(H_2) = V(H_1) \cap V(H_2) = U$, $|U| \geq 2$, and $E(H_0) \cap E(H_1) = E(H_0) \cap E(H_2) = \emptyset$. Suppose that G_1 and H_2 are both rigid. Then*

(a) G_2 is rigid.

(b) If G_1 and H_2 are both radically, respectively quadratically, solvable then G_2 is radically, respectively quadratically, solvable.

Proof. Choose $v_1, v_2 \in U$ and let $(G_1 \cup G_2, p)$ be a quasi-generic *real* realisation of $G_1 \cup G_2$ with $p(v_1) = (0, 0)$ and $p(v_2) = (0, y)$ for some $y \in \mathbb{R}$. Let $V_i = V(H_i) \setminus U$ for $0 \leq i \leq 2$.

Suppose that G_2 is not rigid. Since H_2 is rigid, there exists a non-zero infinitesimal motion z_2 of (G_2, p) in \mathbb{R}^2 which keeps H_2 fixed. Then $z_1 : V(G_1) \rightarrow \mathbb{R}^2$ by $z_1(v) = (0, 0)$ for $v \in V(H_1)$ and $z_1(v) = z_2(v)$ for $v \in V(H_0)$ is a non-zero infinitesimal motion of G_1 which keeps H_1 fixed. This contradicts the hypothesis that G_1 is rigid and completes the proof of (a).

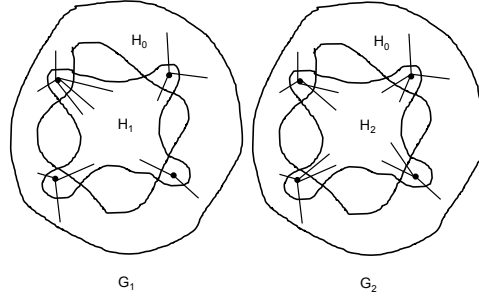


Figure 2: The graphs G_1 and G_2 of Lemma 5.1 when $|U| = 4$.

Suppose that G_1 and H_2 are both radically, respectively quadratically, solvable. The first assumption implies that $\mathbb{Q}(p|_{V_0}, p|_U, p|_{V_1})$ is a radically, respectively quadratically, solvable extension of $\mathbb{Q}(d_{H_0}(p), d_{H_1}(p))$. Since the components of $(p|_{V_0}, y, p|_{U \setminus \{v_1, v_2\}}, p|_{V_1})$ are algebraically independent over \mathbb{Q} we may treat them as if they were indeterminates and apply Lemma 4.2 with $X = p|_{V_0}$, $Y = (y, p|_{U \setminus \{v_1, v_2\}})$, $Z = p|_{V_1}$, $f = d_{H_0}(p)$, and $g = d_{H_1}(p)$ to deduce that $\mathbb{Q}(p|_{V_0}, p|_U)$ is a radically, respectively quadratically, solvable extension of $\mathbb{Q}(d_{H_0}(p), p|_U)$. We also have $\mathbb{Q}(p|_U, p|_{V_2})$ is a radically, respectively quadratically, solvable extension of $\mathbb{Q}(d_{H_2}(p))$ by the second assumption. Hence $\mathbb{Q}(d_{H_0}(p), p|_U, p|_{V_2})$ is a radically, respectively quadratically, solvable extension of $\mathbb{Q}(d_{H_0}(p), d_{H_2}(p))$. Since the components of $(p|_{V_0}, y, p|_{U \setminus \{v_1, v_2\}}, p|_{V_2})$ are algebraically independent over \mathbb{Q} , we may again apply Lemma 4.2, with $X = p|_{V_0}$, $Y = (y, p|_{U \setminus \{v_1, v_2\}})$, $Z = p|_{V_2}$, $f = d_{H_0}(p)$, and $g = d_{H_2}(p)$, to deduce that $\mathbb{Q}(p|_{V_0}, p|_U, p|_{V_2})$ is a radically, respectively quadratically, solvable extension of $\mathbb{Q}(d_{H_0}(p), d_{H_2}(p))$. Thus G_2 is radically, respectively quadratically, solvable and (b) holds. \bullet

We also need a result on graph connectivity due to W. Mader.

Lemma 5.2 [10, Satz 1] *Let G be a k -connected graph and C be a cycle in G such that each vertex of C has degree at least $k + 1$ in G . Then $G - e$ is k -connected for some $e \in E(C)$.*

For $n \geq 4$, the *wheel on n vertices* is the graph $W = (V, E)$ with $V =$

$\{v, u_1, \dots, u_{n-1}\}$ and $E = \{vu_1, vu_2, \dots, vu_{n-1}\} \cup \{u_1u_2, u_2u_3, \dots, u_{n-1}u_1\}$. We refer to the cycle $C = u_1u_2 \dots u_{n-1}u_1$ as the *rim* of W , and to the vertices of C as the *rim vertices* of W .

Lemma 5.3 *Let H_0, H_1 be graphs with $V(H_0) \cap V(H_1) = U$, $|U| \geq 3$, and $E(H_0) \cap E(H_1) = \emptyset$. Let H_2 be a wheel with U as its set of rim vertices, $V(H_0) \cap V(H_2) = U$ and $E(H_0) \cap E(H_2) = \emptyset$. Put $G_1 = H_0 \cup H_1$ and $G_2 = H_0 \cup H_2$. Suppose that G_1 is 3-connected and that each vertex of U has degree at least four in G_2 . Then $G_2 - e$ is 3-connected for some edge e on the rim of H_2 . Furthermore, if G_1 is planar and H_1 is connected, then we may choose H_2 in such a way such that $G_2 - e$ is planar and 3-connected.*

Proof. We first show that G_2 is 3-connected. Suppose not. Then $G_2 - T$ is disconnected for some $T \subseteq V(G_2)$ with $|T| \leq 2$. Since H_2 is 3-connected, $H_2 - T$ is connected. Hence $H_2 - T$ is contained in a single connected component of $G_2 - T$. This implies that $G_1 - (T \cap V(G_1))$ is disconnected and contradicts the hypothesis that G_1 is 3-connected.

We may now use Lemma 5.2 and the hypothesis that each vertex of U has degree at least four in G_2 to deduce that $G_2 - e$ is 3-connected for some edge e of C .

Finally, we suppose that G_1 is planar and H_1 is connected. Then the vertices of U must lie on the same face F of $G - (V(H_1) - U)$. If we choose H_2 such that, in the above definition of a wheel, the rim vertices u_1, u_2, \dots, u_{n-1} occur in this order around F , then the resulting G_2 will be planar. •

Lemma 5.4 *Let G be obtained by deleting an edge from the rim of a wheel on $n \geq 4$ vertices. Then G is both minimally rigid and quadratically solvable.*

Proof. It is easy to check that G can be obtained from K_3 by recursively adding vertices of degree two. The lemma now follows since K_3 is minimally rigid and quadratically solvable, and the operation of adding a vertex of degree two is known to preserve the properties of being minimally rigid, see [18], and quadratically solvable [12]. •

A graph $G = (V, E)$ is *redundantly rigid* if $G - e$ is rigid for all $e \in E$. A *non-trivial redundantly rigid component* of G is a maximal redundantly rigid subgraph of G . Edges e of G such that $G - e$ is not rigid belong to no

redundantly rigid subgraphs of G . We consider the subgraph consisting of such an edge e and its end-vertices to be a *trivial redundantly rigid component*. Thus G is minimally rigid if and only if all its redundantly rigid components are trivial and, when $|V| \geq 3$, G is redundantly rigid if and only if it has exactly one redundantly rigid component.

We can now characterise quadratic/radical solvability in 3-connected planar graphs. We use the fact that a rigid graph $G = (V, E)$ is minimally rigid if and only if $|E| = 2|V| - 3$, see [18].

Theorem 5.5 *Let $G = (V, E)$ be a rigid 3-connected planar graph. Then the following statements are equivalent.*

- (a) G is quadratically solvable.
- (b) G is radically solvable.
- (c) G is redundantly rigid.
- (d) G is globally rigid.

Proof. If G is redundantly rigid then G is globally rigid by [6] and hence is quadratically solvable by Theorem 2.5. Hence (c) implies (d) and (d) implies (a). Clearly (a) implies (b). It remains to show that (b) implies (c). We will prove the contrapositive.

Suppose that G is not redundantly rigid. We show by induction on $|E| - 2|V| + 3$ that G is not quadratically solvable. Since G is rigid we have $|E| - 2|V| + 3 \geq 0$. If equality holds then G is minimally rigid and Theorem 1.1 implies that G is not radically solvable. Hence we may suppose that $|E| > 2|V| - 3$. Then some redundantly rigid component $H_1 = (V_1, E_1)$ of G is non-trivial. Let U be the set of vertices of H_1 which are incident to edges of $E \setminus E_1$ and put $H_0 = (G - E_1) - (V_1 \setminus U)$. By Lemma 5.3, we can choose a wheel W with rim vertices U and an edge e on the rim of W such that $G' = H_0 \cup (W - e)$ is 3-connected and planar. Lemmas 5.1(a) and 5.4 imply that G' is rigid. Since G' is not redundantly rigid and $|V(G')| - 2|E(G')| + 3 < |E| - 2|V| + 3$, we may apply induction to deduce that G' is not radically solvable. Lemmas 5.1(b) and 5.4 now imply that G is not radically solvable. •

5.2 Graphs of connectivity two

We will complete our proof that Conjecture 1.2 holds for planar graphs. We first need to describe a technique for decomposing a rigid graph into ‘3-

connected rigid pieces’. This is a special case of a more general theory of Tutte [17] which decomposes 2-connected graphs into ‘3-connected pieces’.

Every 2-connected graph G which is distinct from K_3 and is not 3-connected has a pair of edge-disjoint subgraphs $H_1 = (V_1, E_1)$ and $H_2 = (V_2, E_2)$ such that $H_1 \cup H_2 = G$, $|V_1 \cap V_2| = 2$, and $V_1 \setminus V_2 \neq \emptyset \neq V_2 \setminus V_1$. We refer to such a pair of subgraphs (H_1, H_2) as a *2-separation* of G and to the vertex set $V_1 \cap V_2$ as a *2-separator* of G .

Given a rigid graph G with at least three vertices, we recursively construct the set \mathcal{C}_G of *cleavage units* of G as follows. If G is 3-connected or $G = K_3$ then we put $\mathcal{C}_G = \{G\}$. Otherwise G has a 2-separation (H_1, H_2) , where $V(H_1) \cap V(H_2) = \{u, v\}$. In this case $G_1 = H_1 + uv$ and $G_2 = H_2 + uv$ are both rigid by Theorem 4.3(b), and we put $\mathcal{C}_G = \mathcal{C}_{G_1} \cup \mathcal{C}_{G_2}$.² Note that the cleavage units of G may not be subgraphs of G since G_1 and G_2 may not be subgraphs of G . (We have $uv \in E(G_1) \cap E(G_2)$ but we may not have $uv \in E(G)$. For example the cleavage units of the graph G in Figure 1 are G_1 , $G_2 + st$ and G_3 , and none of these are subgraphs of G .)

Lemma 5.6 *Let G be a rigid graph on at least three vertices. Then every cleavage unit of G is either equal to K_3 or is 3-connected and rigid. Furthermore, if G is radically, respectively quadratically, solvable, then every cleavage unit of G is radically, respectively quadratically, solvable.*

Proof. If G itself is K_3 or is 3-connected then the lemma is trivially true. Hence we may suppose that G has a 2-separation (H_1, H_2) , where $V(H_1) \cap V(H_2) = \{u, v\}$. Theorem 4.3 implies that $H_1 + uv, H_2 + uv$ are both rigid, and are radically, respectively quadratically, solvable if G is radically, respectively quadratically, solvable. The lemma now follows by induction on $|V(G)|$ using the fact that $\mathcal{C}_G = \mathcal{C}_{H_1+uv} \cup \mathcal{C}_{H_2+uv}$. •

We can now obtain our promised characterization of quadratic/radical solvability for planar graphs.

Theorem 5.7 *Let G be a rigid planar graph. Then the following statements are equivalent.*

²In order to obtain a unique decomposition of a 2-connected graph G into cleavage units Tutte [17] only considers *excisable 2-separations* i.e. 2-separations (H_1, H_2) such that at least one of H_1, H_2 is 2-connected. When G is rigid, Theorem 4.3(b) tells us that for every 2-separation (H_1, H_2) , at least one of H_1, H_2 will be rigid (and hence 2-connected) so all 2-separations of a rigid graph are excisable.

- (a) G is quadratically solvable.
- (b) G is radically solvable.
- (c) G belongs to the family \mathcal{F} defined immediately before Conjecture 1.2.

Proof. We have (c) implies (a) by Lemma 4.5, and (a) implies (b) by definition. It remains to show that (b) implies (c). We proceed by contradiction. Suppose there exists a radically solvable rigid planar graph G such that $G \notin \mathcal{F}$. We may assume that G is chosen to have as few vertices as possible (and hence every radically solvable rigid planar graph with fewer vertices than G belongs to \mathcal{F}). Since $G \notin \mathcal{F}$, $G \neq K_2, K_3$. If G were 3-connected then G would be globally rigid by Theorem 5.5 and hence we would have $G \in \mathcal{F}$. Thus G is not 3-connected and we may choose a 2-separation (H_1, H_2) of G , where $V(H_1) \cap V(H_2) = \{u, v\}$. By Theorem 4.3, $H_1 + uv, H_2 + uv$ are both rigid and radically solvable. Since they are also planar and have fewer vertices than G we have $H_1 + uv, H_2 + uv \in \mathcal{F}$. If $uv \in E(G)$ then $G = (H_1 + uv) \cup (H_2 + uv) \in \mathcal{F}$ by operation (a) in the definition of \mathcal{F} . Hence $uv \notin E(G)$. If H_1, H_2 are both rigid then $G = H_1 \cup H_2 \in \mathcal{F}$ by operation (c) in the definition of \mathcal{F} . Thus, for every 2-separator $\{u, v\}$ of G , $uv \notin E(G)$, and for every 2-separation (H_1, H_2) of G , one of H_1 and H_2 is not rigid.

We now modify our choice of the 2-separation (H_1, H_2) if necessary so that H_1 is not rigid and, subject to this condition, H_1 has as few vertices as possible. We continue to assume that $V(H_1) \cap V(H_2) = \{u, v\}$.

Claim 1 *There exists a unique cleavage unit G_1 of G with $\{u, v\} \subset V(G_1) \subseteq V(H_1)$. In addition we have $G_1 = K_3$.*

Proof. Suppose that there are two distinct cleavage units G_3, G_4 of G with $\{u, v\} \subset V(G_i) \subseteq V(H_1)$ for $i = 3, 4$. Then H_1 has a 2-separation (H_3, H_4) with $V(H_3) \cap V(H_4) = \{u, v\}$ and $V(G_i) \subseteq V(H_i)$ for $i = 3, 4$, see Figure 3(a). Since $H_1 = H_3 \cup H_4$ is not rigid, at least one of H_3 and H_4 , say H_3 , is not rigid. Then $(H_3, H_2 \cup H_4)$ is a 2-separation of G in which H_3 is not rigid and has fewer vertices than H_1 . This contradicts the choice of (H_1, H_2) . Hence there is a unique cleavage unit G_1 of G with $\{u, v\} \subset V(G_1) \subseteq V(H_1)$.

Suppose $G_1 \neq K_3$. Then G_1 is 3-connected and radically solvable by Lemma 5.6. Since G_1 is planar, Theorem 5.5 now implies that G_1 is redundantly rigid and hence that $G_1 - uv$ is rigid. Let $\{u_i, v_i\}$, $1 \leq i \leq m$, be the 2-separators of $H_1 + uv$ with $\{u_i, v_i\} \subset V(G_1)$. Then $u_i v_i \in E(G_1)$ for $1 \leq i \leq m$, see Figure 3(b). For each $1 \leq i \leq m$ we may choose a 2-separation

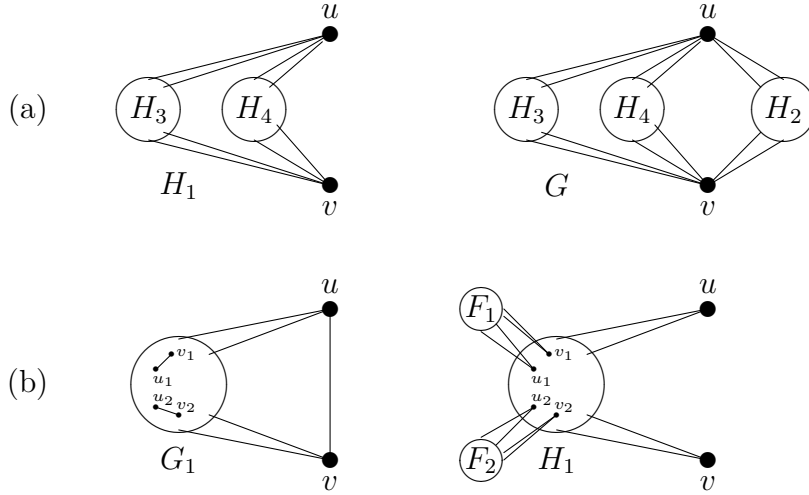


Figure 3: Proof of Claim 1. (a) The case when there are two distinct cleavage units G_3, G_4 of G with $\{u, v\} \subset V(G_i) \subseteq V(H_1)$ for $i = 3, 4$. (b) The case when $G_1 \neq K_3$.

(F_i, F'_i) of $H_1 + uv$ with $V(G_1) \subset V(F'_i)$. Then $(F_i, (F'_i - uv) \cup H_2)$ is a 2-separation of G . The choice of H_1 and the fact that F_i is properly contained in H_1 now implies that F_i is rigid for all $1 \leq i \leq m$. Since $G_1 - uv$ is rigid, this implies that

$$H_1 = [(G_1 - uv) - \{u_i v_i : 1 \leq i \leq m\}] \cup \bigcup_{i=1}^m F_i$$

is rigid. This contradicts the choice of H_1 . Thus $G_1 = K_3$. •

We can now complete the proof of the theorem. Since $G_1 = K_3$ we can express G as $G = H'_1 \cup H''_1 \cup H_2$ where $H'_1 \cup H''_1 = H_1$, $V(H'_1) \cap V(H_2) = \{u\}$, $V(H''_1) \cap V(H_2) = \{v\}$, $V(H'_1) \cap V(H''_1) = \{w\}$ for some $w \in V(H_1) \setminus \{u, v\}$, and H'_1, H''_1, H_2 are pairwise edge-disjoint. Corollary 4.4 now implies that H'_1, H''_1, H_2 are rigid and radically solvable. Since they are planar and have fewer vertices than G , we have $H'_1, H''_1, H_2 \in \mathcal{F}$. Since G can be obtained from K_3, H'_1, H''_1, H_2 by applying operations (a) and (b) in the definition of \mathcal{F} at most three times, we have $G \in \mathcal{F}$. This contradicts the choice of G . •

Since the operations (a), (b) and (c) used in the construction of \mathcal{F} preserve planarity, Theorem 5.7 implies that the family of quadratically solvable planar graphs can be constructed recursively from the family of globally rigid planar graphs by applying operations (a), (b) and (c).

6 Closing remarks

1. The proof technique of Theorems 5.5 and 5.7 can be used to show that Conjecture 1.2 is equivalent to the conjecture of the second author mentioned in the Introduction, that a minimally rigid graph is radically (or quadratically) solvable if and only if it belongs to \mathcal{F}_{min} . We have verified both conjectures for the smallest 3-connected non-planar minimally rigid graph by showing that $K_{3,3}$ is not radically solvable using a similar proof technique to that used for the prism, or doublet, graph in [13, Theorem 8.4].

2. Since the radical solvability of a graph is preserved by the addition of edges, it is tempting to conjecture that a graph is radically solvable if and only if it has a spanning subgraph in \mathcal{F}_{min} . This is not the case however. The complete bipartite graph $K_{3,4}$ is globally rigid and hence quadratically solvable, but for each edge e , $K_{3,4} - e$ is minimally rigid and does not belong to \mathcal{F}_{min} . In addition, we can use Theorem 4.3(b)(iii) and the fact that $K_{3,3}$ is not radically solvable to deduce that $K_{3,4} - e$ is not radically solvable, so $K_{3,4}$ is ‘minimally radically solvable’ but not minimally rigid.

Acknowledgement We would like to thank John Bray for helpful comments. We would also like to thank the Fields Institute for support during its 2011 thematic programme on Discrete Geometry and Applications.

Appendix: Proofs of Lemmas 4.1 and 4.2

The definitions of radically and quadratically solvable field extensions immediately imply the following result.

Proposition 1 *Let $K \subseteq L \subseteq M$ be fields. Then $M : K$ is radically, respectively quadratically, solvable if and only if $M : L$ and $L : K$ are both radically, respectively quadratically, solvable.*

Suppose M, N are field extensions of a field K which are both contained in a common extension P of K . Then MN denotes the smallest subfield of

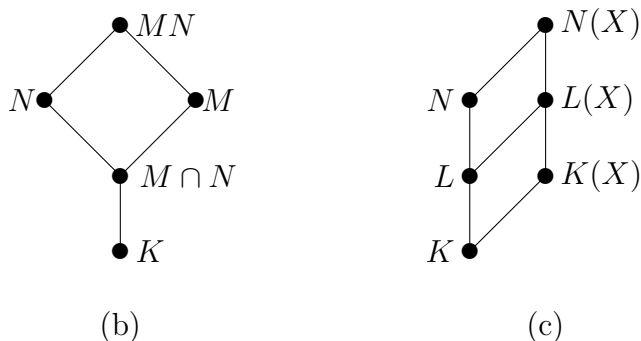


Figure 4: The field extensions of Proposition 2 and Lemma 4.1

P which contains both M and N . We will need the following result from Galois Theory, see for example [11, Proposition 3.18].

Proposition 2 *Let K be a field of characteristic zero and M, N be field extensions of K which are both contained in a common extension of K . Suppose that N is a normal extension of K . Then $MN : M$ and $N : M \cap N$ are normal extensions, and $\Gamma(MN : M)$ and $\Gamma(N : M \cap N)$ are isomorphic groups.*

Proof of Lemma 4.1 Let a_1, a_2, \dots, a_m be a basis for $L : K$, f_i be the minimum polynomial of a_i over K , R_i be the set of all complex roots of f_i , and $R = \bigcup_{i=1}^m R_i$. Then $N = L(R)$ is the normal closure of L over K in \mathbb{C} . Since X_1, X_2, \dots, X_n are indeterminates, a_1, a_2, \dots, a_m is also a basis for $L(X) : K(X)$ and f_i is the minimum polynomial of a_i over $K(X)$. Thus $L(R)(X) = N(X)$ is a normal closure of $L(X) : K(X)$. We now apply Proposition 2 with $M = K(X)$. We have $NK(X) = N(X)$ and $N \cap K(X) = K$. Hence $\Gamma(N : K)$ is isomorphic to $\Gamma(N(X) : K(X))$.

The final part of the lemma now follows from Theorem 3.1 and Proposition 2. •

Proof of Lemma 4.2 This follows from Proposition 1 (which tells us that $\mathbb{Q}(X, Y, Z) : \mathbb{Q}(f, g)$ is radically, respectively quadratically, solvable if and only if $\mathbb{Q}(f, Y, Z) : \mathbb{Q}(f, g)$ and $\mathbb{Q}(X, Y, Z) : \mathbb{Q}(f, Y, Z)$ are both radically, respectively quadratically, solvable) and Lemma 4.1 (which tells us that $\mathbb{Q}(X, Y, Z) : \mathbb{Q}(f, Y, Z)$ is radically, respectively quadratically, solvable if and only if $\mathbb{Q}(X, Y) : \mathbb{Q}(f, Y)$ is radically, respectively quadratically, solvable). •

References

- [1] C. Borcea and I. Streinu, The number of embeddings of minimally rigid graphs, *Discrete Comput. Geom.*, 31 (2004) 287–303.
- [2] B. Buchberger: Gröbner Bases: An Algorithmic Method in Polynomial Ideal Theory, in *Recent Trends in Multidimensional Systems Theory*, N.K. Bose (ed.), D. Reidel Publ. Comp. (1985) 184-232.
- [3] R. Connelly, Generic global rigidity, *Discrete Comput. Geom.*, 31 (2004), 287–303.
- [4] X.S. Gao and Shang-Ching Chou, Solving geometric constraint systems, II. A symbolic approach and decision of re-constructability, *Computer Aided Design*, 30 (1998), 115–122
- [5] S.J. Gortler and D.P. Thurston, Generic global rigidity in complex and pseudo-Euclidean spaces, in *Rigidity and Symmetry*, Fields Institute Communications, 70 (2014), 131–154
- [6] B. Jackson and T. Jordán, Connected rigidity matroids and unique realizations of graphs, *J. Combin. Theory Ser. B* 94 (2005), 1–29.
- [7] B. Jackson and J. C. Owen, The number of complex realisations of a rigid graph, *Discrete Applied Mathematics*, in press.
- [8] M. Kalkbrener, Solving systems of algebraic equations by using Groebner bases, in *Proc. Eurocal 87, Lecture Notes in Computer Science 378*, Springer-Verlag, 1989, 282–292.
- [9] G. Laman, On graphs and rigidity of plane skeletal structures, *J. Engineering Math.* 4 (1970), 331-340.
- [10] W. Mader, Ecken vom Grad n in minimalen n -fach zusammenhängenden Graphen, *Archive der Mathematik* 23 (1972), 219–224.
- [11] J. S. Milne, *Fields and Galois Theory*, online notes available at <http://www.jmilne.org/math/CourseNotes/FT.pdf>
- [12] J.C. Owen, Algebraic solution for geometry from dimensional constraints, in *ACM Symposium on Foundations in Solid Modeling*, Austin, Texas, 1991, 397–407.

- [13] J. C. Owen and S. C. Power, The non-solvability by radicals of generic 3-connected planar Laman graphs, *Trans. Amer. Math. Soc.*, 359 (2007), 2269–2303.
- [14] Siemens D-Cubed Components webpage:
<http://www.plm.automation.siemens.com/d-cubed/index/shtml>
- [15] R. Steffens and T. Theobald, Mixed volume techniques for embeddings of Laman Graphs, *Comput. Geom*, 43 (2010), 84–93.
- [16] I. Stewart, *Galois Theory*, 3rd ed., Chapman and Hall/CRC Mathematics, 2004.
- [17] W.T. Tutte, *Connectivity in Graphs*, University of Toronto Press, 1966.
- [18] W. Whiteley, Some matroids from discrete applied geometry, in *Matroid theory*, *Contemp. Math.* 197, Amer. Math. Soc., Providence, RI, 1996, 171–311.