



ELSEVIER

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt



CrossMark

Points at rational distances from the vertices of certain geometric objects

Andrew Bremner^a, Maciej Ulas^{b,*,1}

^a School of Mathematical and Statistical Sciences, Arizona State University, Tempe, AZ 85287-1804, USA

^b Jagiellonian University, Faculty of Mathematics and Computer Science, Institute of Mathematics, Łojasiewicza 6, 30 - 348 Kraków, Poland

ARTICLE INFO

Article history:

Received 28 December 2014

Received in revised form 25 May 2015

Accepted 3 June 2015

Available online 6 August 2015

Communicated by David Goss

MSC:

11D25

14J20

11G35

14G05

Keywords:

Rational points

Elliptic surfaces

Rational distances set

ABSTRACT

We consider various problems related to finding points in \mathbb{Q}^2 and in \mathbb{Q}^3 which lie at rational distance from the vertices of some specified geometric object, for example, a square or rectangle in \mathbb{Q}^2 , and a cube or tetrahedron in \mathbb{Q}^3 . In particular, as one of several results, we prove that the set of positive rational numbers a such that there exist infinitely many rational points in the plane which lie at rational distance from the four vertices of the rectangle with vertices $(0, 0)$, $(0, 1)$, $(a, 0)$, and $(a, 1)$, is dense in \mathbb{R}_+ .

© 2015 Elsevier Inc. All rights reserved.

* Corresponding author.

E-mail addresses: bremner@asu.edu (A. Bremner), maciej.ulas@uj.edu.pl (M. Ulas).

¹ The research of the second author was supported by the grant of the Polish National Science Centre no. UMO-2012/07/E/ST1/00185.

1. Introduction

Berry [1] showed that the set of rational points in the plane with rational distances to three given vertices of the unit square is infinite. More precisely, he showed that the set of rational parametric solutions of the corresponding system of equations is infinite; this generalizes some earlier work of Leech. In a related work, he was able to show that for any given triangle ABC in which the length of at least one side is rational and the squares of the lengths of all sides are rational, then the set of points P with rational distances $|PA|$, $|PB|$, $|PC|$ to the vertices of the triangle is dense in the plane of the triangle; see Berry [2]. However, it is a notorious and unsolved problem to determine whether there exists a rational point in the plane at rational distance from the *four* corners of the unit square (see Problem D19 in Guy's book [7]). Such a point corresponds to a rational solution of a Diophantine system comprising four quadratics in six-dimensional projective space. An analogous system is that for the “rational cuboid” problem, of finding a rectangular cuboid with rational edges, face diagonals, and body diagonal. This again is a notorious and unsolved problem. A great deal of computing has produced no solution, and it is tempting to believe that no solution exists. However, another naturally arising Diophantine system of four quadratics in six-dimensional projective space is that of finding a three-by-three magic square of integers in which a certain seven of the entries are perfect squares. This system *does* have a solution (although only one solution up to symmetries is known); see Bremner [3]. Because of the difficulty of this problem one can ask a slightly different question, as to whether there exist rational points in the plane which lie at rational distance from the four vertices of the *rectangle* with vertices $(0, 0)$, $(0, 1)$, $(a, 0)$, and $(a, 1)$, for $a \in \mathbb{Q}$. This problem is briefly alluded to in Section D19 on p. 284 of Guy's book. In Section 2 we reduce this problem to the investigation of the existence of rational points on members of a certain family of algebraic curves $\mathcal{C}_{a,t}$ (depending on rational parameters a, t). We show that the set of $a \in \mathbb{Q}$ for which the set of rational points on $\mathcal{C}_{a,t}$ is infinite is dense in \mathbb{R} (in the Euclidean topology).

Richard Guy has pointed out that there are immediate solutions to the four-distance unit square problem if the point is allowed to lie in three space \mathbb{Q}^3 . Indeed, $(\frac{1}{2}, \frac{1}{2}, \frac{1}{4})$ lies at rational distance to the four vertices $(0, 0, 0)$, $(0, 1, 0)$, $(1, 0, 0)$, $(1, 1, 0)$ of the square. This observation leads us to consider the more general problem, of points in \mathbb{Q}^3 which lie at rational distance from the four vertices $(0, 0, 0)$, $(0, 1, 0)$, $(1, 0, 0)$, $(1, 1, 0)$ of the unit square. In Section 3 we show that such points are dense on the line $x = \frac{1}{2}$, $y = \frac{1}{2}$, and dense on the plane $x = y$. Further, there are infinitely many parameterizations of such points on the plane $x = y$. In Section 4 we consider the general problem of finding points $(x, y, z) \in \mathbb{Q}^3$ with rational distances to the vertices of a unit square lying in the plane $z = 0$ without any assumptions on x, y, z . Attempts to show such points are dense in \mathbb{R}^3 have been unsuccessful to date. However, we are able to show that the variety related to this problem is unirational over \mathbb{Q} . In particular, this implies the existence of a parametric family of rational points with rational distances to the four vertices $(0, 0, 0)$, $(0, 1, 0)$, $(1, 0, 0)$, $(1, 1, 0)$ of the unit square. Whether there exist points in \mathbb{Q}^3 at rational

distance from the eight vertices of the unit *cube* is another seemingly intractable problem which we leave as open and certainly worthy of further investigation.

In Section 5 we consider the problem of finding points in \mathbb{Q}^3 at rational distance from the vertices of a general tetrahedron (with rational vertices) and prove that the corresponding algebraic variety is unirational over \mathbb{Q} . This is related to Section D22 in Guy's book. This result, together with the construction of a parameterized family of tetrahedra having rational edges, face areas, and volume (an independent investigation), leads to constructing a double infinity of sets of five points in \mathbb{Q}^3 with the ten distances between them all rational.

Finally, in the last section we collect some numerical results and prove that under a certain symmetry assumption it is possible to find a parametric family of points in \mathbb{Q}^3 with rational distances to six vertices of the unit cube. Without symmetry, we found just one point with five of the distances rational.

2. Points in \mathbb{Q}^2 with rational distances from the vertices of rectangles

Let $a \in \mathbb{Q}$. Consider the rectangle \mathcal{R}_a in the plane with vertices at $P_1 = (0, 0)$, $P_2 = (0, 1)$, $P_3 = (a, 0)$, and $P_4 = (a, 1)$.

Theorem 2.1. *The set of $a \in \mathbb{Q}$ such that there are infinitely many rational points with rational distance to each of the corners P_1, \dots, P_4 of \mathcal{R}_a is dense in \mathbb{R} .*

Proof. Let $M = (x, y)$ be a rational point with rational distance to each vertex P_1, \dots, P_4 of \mathcal{R} . This determines the following system of equations:

$$\begin{cases} x^2 + y^2 &= P^2 = |MP_1|^2, \\ x^2 + (1 - y)^2 &= Q^2 = |MP_2|^2, \\ (a - x)^2 + y^2 &= R^2 = |MP_3|^2, \\ (a - x)^2 + (1 - y)^2 &= S^2 = |MP_4|^2. \end{cases} \quad (1)$$

From the first and third equations, and the first and second equations, we deduce respectively

$$x = \frac{1}{2a}(a^2 + P^2 - R^2), \quad y = \frac{1}{2}(P^2 - Q^2 + 1). \quad (2)$$

Eliminating x, y from the system (1) we obtain

$$\begin{cases} P^2 - Q^2 = R^2 - S^2, \\ a^2(R^4 + a^2 + 1) + Q^4 + (1 + a^2)S^4 = 2Q^2(a^2 + S^2) + 2a^2R^2(S^2 + 1). \end{cases} \quad (3)$$

The first quadric may be parameterized by

$$R = \frac{(P+Q)t^2 + P - Q}{2t}, \quad S = \frac{(P+Q)t^2 - P + Q}{2t}. \quad (4)$$

On homogenizing, by setting $P = X/Z$, $Q = Y/Z$, the second equation at (3) becomes:

$$\begin{aligned} & (1 - 4t^2 + 6t^4 + 16a^2t^4 - 4t^6 + t^8)(X^4 + Y^4) + 4(t^2 - 1)^3(t^2 + 1)(X^2 + Y^2)XY - \\ & 8a^2t^2(1 + t^2)^2(X^2 + Y^2)Z^2 + 16a^2t^2Z^2((1 - t^4)XY + (1 + a^2)t^2Z^2) + \\ & 2(3 - 4t^2 + 2t^4 - 16a^2t^4 - 4t^6 + 3t^8)X^2Y^2 = 0. \end{aligned}$$

This equation defines a curve $\mathcal{C}_{a,t}$ of genus three over the field $\mathbb{Q}(a, t)$. It is well known that a curve of genus at least 2 defined over a function field has only finitely many points with coordinates in this field. Thus, in order to prove the theorem we must find some specialization a_0, t_0 of the rational parameters a, t , such that the corresponding curve \mathcal{C}_{a_0, t_0} , has genus at most 1. In particular, the curve $\mathcal{C}_{a,t}$ needs to have singular points. Denote the defining polynomial of $\mathcal{C}_{a,t}$ by $F = F(X, Y, Z)$. Now $\mathcal{C}_{a,t}$ has singular points when the system of equations

$$F(X, Y, Z) = \partial_X F(X, Y, Z) = \partial_Y F(X, Y, Z) = \partial_Z F(X, Y, Z) = 0 \quad (5)$$

has rational solutions. In order to find solutions of this system, consider the ideal

$$\text{Sing} = \langle F, \partial_X F, \partial_Y F, \partial_Z F \rangle$$

and compute its Gröbner basis. The basis contains the polynomial $-a^2(1+a^2)t^6(1+2at-t^2)(-1+2at+t^2)Z^7$, and to obtain something non-trivial, we require $a = \pm(1-t^2)/2t$. We choose without loss of generality $a = (1-t^2)/2t$ (the other sign corresponds to solutions in which x is replaced by $-x$). Now, $F = G^2$, where

$$G(X, Y, Z) = (t^2 - 1)((t^2 + 1)X^2 + 2(t^2 - 1)XY + (t^2 + 1)Y^2 - (t^2 + 1)Z^2)$$

and by abuse of notation we are working with the curve $\mathcal{C}_{a,t} : G(X, Y, Z) = 0$ of degree 2 defined over the rational function field $\mathbb{Q}(t)$. The genus of $\mathcal{C}_{a,t}$ is 0, and moreover, there is a $\mathbb{Q}(t)$ -rational point $(0, 1, 1)$ lying on $\mathcal{C}_{a,t}$. This point allows the parametrization of $\mathcal{C}_{a,t}$ in the following form:

$$X = 2u((1-t^2)u + (t^2+1)v), \quad Y = (t^2+1)(u^2-v^2), \quad Z = (t^2+1)(u^2+v^2) - 2(t^2-1)uv.$$

Recalling that $P = X/Z$, $Q = Y/Z$ and using the expressions for R, S at (4), x, y at (2), we get that for $a = (1-t^2)/2t$ there is the following parametric solution of the system (1):

$$x = \frac{4tu(v^2 - u^2)((t^2 - 1)u - (t^2 + 1)v)}{((t^2 + 1)u^2 - 2(t^2 - 1)uv + (1 + t^2)v^2)^2},$$

$$y = \frac{2u((t - 1)u - (t + 1)v)((t + 1)u - (t - 1)v)((t^2 - 1)u - (t^2 + 1)v)}{((t^2 + 1)u^2 - 2(t^2 - 1)uv + (1 + t^2)v^2)^2}.$$

To finish the proof, note that the rational map $a : \mathbb{R} \ni t \mapsto \frac{1-t^2}{2t} \in \mathbb{R}$ is continuous and has the obvious property

$$\lim_{t \rightarrow -\infty} a(t) = +\infty, \quad \lim_{t \rightarrow +\infty} a(t) = -\infty.$$

The density of \mathbb{Q} in \mathbb{R} together with the properties of $a(t)$ immediately imply that the set $a(\mathbb{Q}) \cap \mathbb{R}_+$ is dense in \mathbb{R}_+ in the Euclidean topology. The theorem follows. \square

Remark 2.2. Observe that the construction presented in the proof of [Theorem 2.1](#) allows deduction of the following simple result.

Theorem 2.3. *Let K be a number field and suppose that $\sqrt{2} \in K$. Then the set of K -rational points with K -rational distances to the vertices of the square \mathcal{R}_1 is infinite.*

Proof. Let $a = 1$ and take $t = 1 + \sqrt{2}$. Then $1 + 2at - t^2 = 0$ and using the parametrization constructed at the end of [Theorem 2.1](#) (with $v = 1$) we get that for

$$x = \frac{u(u - \sqrt{2})(1 - u^2)}{(u^2 - \sqrt{2}u + 1)^2},$$

$$y = \frac{(3 - 2\sqrt{2})u(\sqrt{2}(u - 1) - 2)(\sqrt{2}(u - 1) + \sqrt{2})((1 + \sqrt{2})u - \sqrt{2} - 2)}{2(u^2 - \sqrt{2}u + 1)^2}$$

and any given $u \in K$ such that $\sqrt{2}u^2 - 2u + \sqrt{2} \neq 0$, the distance of the point $P = (x, y)$ to the vertices P_1, P_2, P_3, P_4 of \mathcal{R}_1 is K -rational. \square

Remark 2.4. The construction of a 's and the corresponding solutions x, y of the system (1) presented in the proof of [Theorem 2.1](#) has one aesthetic disadvantage. In order that (x, y) lie *inside* the rectangle \mathcal{R} , it is necessary that $x, a - x, y, 1 - y$, all be positive. However,

$$x(a - x)y(1 - y) = -4u^2(u^2 - v^2)^2(((1 - t)u + (1 + t)v)((1 + t)u + (1 - t)v))^2 \times$$

$$\left(\frac{((1 - t^2)u + (1 + t^2)v)((1 + 2t - t^2)u + (1 + t^2)v)((1 - 2t - t^2)u + (1 + t^2)v)}{((1 + t^2)u^2 + 2(1 - t^2)uv + (1 + t^2)v^2)^4} \right)^2$$

which is evidently negative. Thus the point (x, y) can never lie within the rectangle \mathcal{R} . A natural question arises therefore as to whether it is possible to find a positive rational

number a such that the system (1) has rational solutions x, y with $x, a - x, y, 1 - y$, all positive? The answer is yes, on account of the family

$$a = \frac{2t}{t^2 - 1}, \quad x = \frac{t}{t^2 - 1}, \quad y = \frac{1}{2}$$

where $x, a - x, y, 1 - y$ are all positive when $t > 1$; however, this family is rather uninteresting, in that correspondingly $P = Q = R = S$. An equivalent question was posed by Dodge in [6] with an answer given by Shute and Yocom. They proved that if p_i, q_i, r_i are Pythagorean triples for $i = 1, 2$, and $A = p_1q_2 + p_2q_1, B = p_1p_2 + q_1q_2$, then the point $M = (p_1q_2, q_1q_2)$ lies inside the rectangle with vertices $(0, 0), (A, 0), (0, B), (A, B)$, and, moreover, the distances of M to the vertices of the rectangle are rational. Using their result one can prove that the set of those $a \in \mathbb{Q}$, such that there are infinitely many rational points inside the rectangle \mathcal{R}_a with rational distance to its vertices, is dense in \mathbb{R}_+ . Indeed, note that the point

$$P = \left(\frac{p_1q_2}{B}, \frac{q_1q_2}{B} \right)$$

lies inside the rectangle \mathcal{R}_a , with $a = A/B$. To finish the proof, it is enough to show that one can find infinitely many Pythagorean triples $p_i, q_i, r_i, i = 1, 2$, such that $a = A/B$ is constant. Put

$$\begin{aligned} p_1 &= 1 - U^2, \quad q_1 = 2U, \quad r_1 = 1 + U^2, \\ p_2 &= 1 - V^2, \quad q_2 = 2V, \quad r_2 = 1 + V^2 \end{aligned}$$

and then

$$A(U, V) = 2(U + V)(1 - UV), \quad B(U, V) = (1 + U - (1 - U)V)(1 - U + (1 + U)V).$$

Since the rectangles \mathcal{R}_a and $\mathcal{R}_{1/a}$ are equivalent under rotation by ninety degrees and scaling, we consider only the case $0 < a < 1$. Set $a = a(t) = \frac{2t}{1-t^2}$, with $0 < t < \sqrt{2} - 1$ (the transformation between \mathcal{R}_a and $\mathcal{R}_{1/a}$ is now given by $t \leftrightarrow \frac{1-t}{1+t}$). Define C_t to be the curve $A(U, V) = a(t)B(U, V)$:

$$C_t : (U + V)(1 - UV)(1 - t^2) - t(1 + U - (1 - U)V)(1 - U + (1 + U)V) = 0.$$

The triple (t, U, V) corresponds to a point P with rational distances to the vertices of \mathcal{R}_a (with $a = a(t)$) precisely when

$$0 < \frac{p_1q_2}{B} < \frac{A}{B}, \quad 0 < \frac{q_1q_2}{B} < 1, \quad (6)$$

that is, when

$$\frac{V(1-U^2)}{\Delta} > 0, \quad \frac{U(1-V^2)}{\Delta} > 0, \quad \frac{UV}{\Delta} > 0, \quad \frac{(1-U^2)(1-V^2)}{\Delta} > 0, \quad (7)$$

where

$$\Delta = (1+U-(1-U)V)(1-U+(1+U)V) = (1-U^2)(1-V^2) + 4UV.$$

Our strategy is to show that the curve C_t contains infinitely many rational points in the unit square $0 < U < 1$, $0 < V < 1$, when the inequalities (7) clearly hold, so that the inequalities (6) will follow.

The equation for C_t defines the hyperelliptic quartic curve:

$$C_t : W^2 = ((t^2 - 1)U^2 - 4tU + 1 - t^2)^2 + 4(tU^2 - (t^2 - 1)U - t)^2,$$

where $W = 2(t - U)(1 + tU)V + ((t - 1)U - t - 1)((t + 1)U + t - 1)$. Now C_t contains the point $R = (0, t^2 + 1)$, and a cubic model \mathcal{E}_t for C_t is given by

$$\mathcal{E}_t : Y^2 = X(X + (t^2 - 2t - 1)^2)(X + (t^2 + 2t - 1)^2).$$

The curve \mathcal{E}_t contains the point $H(X, Y) = (-(1 + t^2)^2, 4t(1 - t^4))$, and it is readily checked that H is of infinite order in $\mathcal{E}_t(\mathbb{Q}(t))$. We now apply theorems of Silverman [16, p. 368] and of Hurwitz [8] (see also Skolem [17, p. 78]). Silverman's theorem states that if E_t is an elliptic curve defined over $\mathbb{Q}(t)$ with positive rank, then for all but finitely many $t_0 \in \mathbb{Q}$, the curve E_{t_0} obtained from the curve E_t by the specialization $t = t_0$ has positive rank. From this result it follows that for all but finitely many $t_0 \in \mathbb{Q}$ the elliptic curve \mathcal{E}_{t_0} is of positive rank. (Indeed, a straightforward computation shows that the specialization of H at $t = t_0$ is of infinite order in $\mathcal{E}_{t_0}(\mathbb{Q})$ for all $t_0 \in \mathbb{Q}$ with $t_0 \neq 0, \pm 1$, that is, for all t_0 giving a non-singular specialization.)

The theorem of Hurwitz states that if an elliptic curve E defined over \mathbb{Q} has positive rank and one torsion point of order two (defined over the field \mathbb{R}) then the set $E(\mathbb{Q})$ is dense in $E(\mathbb{R})$. The same result holds if E has three torsion points (defined over the field \mathbb{R}) of order two under the assumption that there is a rational point of infinite order on the bounded branch of the set $E(\mathbb{R})$. Here, for $0 < t < 1$, the point H satisfies this latter condition, since for $0 < t < 1$ we have

$$-(-1 - 2t + t^2)^2 < -(1 + t^2)^2 < -(-1 + 2t + t^2)^2.$$

Applying the Hurwitz theorem we get that for all but finitely many $t_0 \in \mathbb{Q}$ the set $\mathcal{E}_{t_0}(\mathbb{Q})$ is dense in the set $\mathcal{E}_{t_0}(\mathbb{R})$. This proves that the set $\mathcal{E}_{t_0}(\mathbb{Q})$ is dense in the set

$\mathcal{E}_{t_0}(\mathbb{R})$ in the Euclidean topology. As a consequence we get that the set $\mathcal{C}_{t_0}(\mathbb{Q})$ is dense in the set $\mathcal{C}_{t_0}(\mathbb{R})$. This immediately implies that the image of the map

$$\mathcal{C}_{t_0}(\mathbb{Q}) \ni (U, W) \mapsto U \in \mathbb{R}$$

is dense in \mathbb{R} for all but finitely many $t_0 \in \mathbb{Q}$ (which is a consequence of the positivity of the polynomial defining the quartic \mathcal{C}_t).

In order to finish the proof therefore we need to show that for given rational $t \in (0, \sqrt{2}-1)$ we can find infinitely many rational points $(U, V) \in \mathcal{C}_t(\mathbb{Q})$ satisfying $0 < U < 1$ and $0 < V < 1$. Now

$$V = V(U) = (W(U) - ((t-1)U - (t+1))((t+1)U + t - 1)) / (2(t-U)(1+tU)),$$

and we consider the connected component of the curve that passes through the point $(U, V) = (0, t)$, certainly a continuous function on the interval $0 < U < t$. Using

$$\frac{dV}{dU} = \frac{-1 + t^2 - 2tU + 4tV + 2UV - 2t^2UV + V^2 - t^2V^2 + 2tUV^2}{1 - t^2 - 4tU - U^2 + t^2U^2 + 2tV - 2UV + 2t^2UV - 2tU^2V}$$

we compute that $\frac{dV}{dU}(0, t) = -\frac{(-1-2t+t^2)(-1+2t+t^2)}{(1+t^2)} < 0$. Taking $\frac{dV}{dU}$ in the form

$$\frac{dV}{dU} = -\frac{(1+U^2)(t-V)V(1+tV)}{(1+V^2)(t-U)U(1+tU)},$$

then the derivative can vanish for $0 < U < t$ only when $V = -1/t$ (forcing $U = 0$), 0 (with $U = -1/t, t$), t (with $U = 0$). Accordingly $\frac{dV}{dU}$ has constant sign (negative) for $0 < U < t$, so that $V(U)$ is a decreasing function on the interval $0 \leq U < t$. Accordingly, $0 \leq U < t$ implies $0 < V \leq t$ on this component of the curve. Thus the curve \mathcal{C}_t contains infinitely many rational points in the square $0 < U < t$, $0 < V < t$. The situation is graphed in Fig. 1.

Summing up, for all but finitely many $t \in (0, \sqrt{2}-1)$ we can find infinitely many rational points satisfying the conditions (7) and the equation $A(U, V) = a(t)B(U, V)$. This implies that for all but finitely rational numbers $t \in (0, \sqrt{2}-1)$, the corresponding point P lies inside the rectangle $\mathcal{R}_{a(t)}$. Because of the continuity of the function $a = a(t)$, we get that the set $a(\mathbb{Q} \cap (0, \sqrt{2}-1))$ with $a(t)$ having the required property, is dense in the set $\mathbb{R}_+ \cap (0, 1)$.

The earlier remark about the equivalence of the rectangles $\mathcal{R}_{1/a}$ and \mathcal{R}_a under rotation and scaling now gives the following theorem.

Theorem 2.5. *The set of $a \in \mathbb{Q}$ such that there are infinitely many rational points lying inside the rectangle \mathcal{R}_a with rational distance to each of the corners P_1, \dots, P_4 of \mathcal{R}_a is dense in \mathbb{R}_+ .*

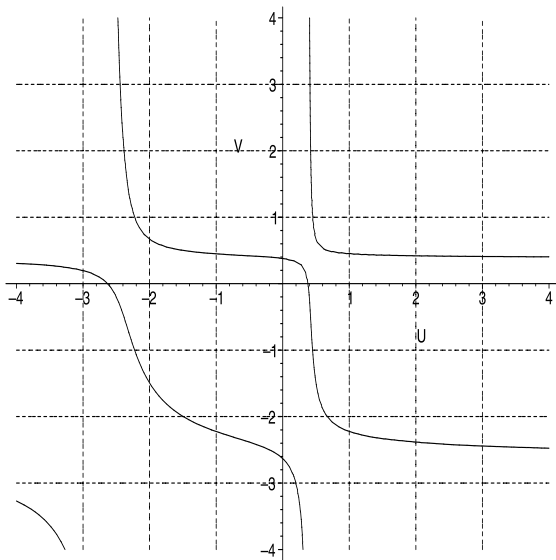


Fig. 1. The graph of C_t when $0 < t < \sqrt{2} - 1$.

Table 1
Points in \mathbb{Q}^2 at rational distance to vertices of \mathcal{R}_a .

a	x	y	a	x	y	a	x	y
13/12	88/399	55/133	12/11	24/77	32/77	19/12	35/204	7/17
9/8	120/169	50/169	17/15	15/14	11/56	13/6	273/500	34/125
9/8	15/56	5/14						

Remark 2.6. It is interesting that the family $\{\mathcal{E}_t\}_{t \in \mathbb{Q}}$ of elliptic curves arising in the proof of Theorem 2.5 is an example of a family parameterized by binary quadratic forms in the context of the paper [15, Example 5.14]. In the cited paper the computation of rank and generators of the Mordell–Weil group of an associated elliptic surface is presented.

Remark 2.7. It is interesting that all a ’s we have found above are of the form $(1 - t^2)/2t$ or $2t/(1 - t^2)$. A question arises as to whether we can find a ’s which are not of this form and such that there is a rational point with rational distances to the vertices of the rectangle \mathcal{R}_a . A small numerical search for other such triples $(a, x, y) \in \mathbb{Q}^3$ was undertaken. We wrote $(x, y) = (X/Z, Y/Z)$, $X, Y, Z > 0$, and restricted the search to height of a at most 20, and $X + Y + Z \leq 1000$. The involutions $(a, x, y) \leftrightarrow (1/a, y/a, x/a)$, $(a, x, y) \leftrightarrow (a, x - a, y)$, and $(a, x, y) \leftrightarrow (a, x, 1 - y)$ mean that we can restrict attention to solutions satisfying $a > 1$, $x \leq a/2$, $y \leq 1/2$. Of the solutions found in the range, fourteen have $x = 0$; seventeen have $x = a/2$; and forty-five have $y = 1/2$. These all imply some equalities between P , Q , R , S , and we list only those solutions found where P , Q , R , S are distinct. (See Table 1.)

3. Special points in \mathbb{Q}^3 at rational distance to the vertices of the unit square

We normalize coordinates so that the unit square lies in the plane $z = 0$, with vertices $A = \{(0, 0, 0), (0, 1, 0), (1, 0, 0), (1, 1, 0)\}$.

Proposition 3.1. *Let λ be the line in \mathbb{R}^3 given by $\lambda : x = y = \frac{1}{2}$. Then the set*

$$\Lambda = \{P \in \lambda(\mathbb{Q}) : \text{the distance } |PQ| \text{ is rational for all } Q \in A\}$$

is dense in $\lambda(\mathbb{R})$.

Proof. It is clear that $P = (\frac{1}{2}, \frac{1}{2}, z) \in \Lambda$ if and only if

$$\frac{1}{4} + z^2 = T^2,$$

for some rational T . This equation represents a conic with rational point $(z, T) = (0, \frac{1}{2})$, and so is parameterizable, for example, by:

$$z = \frac{1 - u^2}{4u}, \quad T = \frac{1 + u^2}{4u}.$$

To finish the proof, note that for the rational map $z : \mathbb{R} \ni u \mapsto \frac{1-u^2}{4u} \in \mathbb{R}$ we have $\overline{z(\mathbb{Q})} = \mathbb{R}$. This implies that $\Lambda = \{(\frac{1}{2}, \frac{1}{2}, z(u)) : u \in \mathbb{Q} \setminus \{0\}\}$ is dense in $\lambda(\mathbb{R})$. \square

Theorem 3.2. *Let π be the plane in \mathbb{R}^3 given by $\pi : x = \frac{1}{2}$. Then the set*

$$\Pi = \{M \in \pi(\mathbb{Q}) : \text{the distance } |MR| \text{ is rational for all } R \in A\}$$

is dense in $\pi(\mathbb{R})$.

Proof. Points $(\frac{1}{2}, y, z)$ which lie in Π are in one-to-one correspondence with rational points on the intersection of the following two quadric surfaces in \mathbb{R}^4 :

$$\frac{1}{4} + y^2 + z^2 = P^2, \quad \frac{1}{4} + (1 - y)^2 + z^2 = Q^2. \quad (8)$$

Subtracting the second equation from the first gives $y = \frac{1}{2}(P^2 - Q^2 + 1)$. So, on eliminating y , the problem of finding rational solutions of (8) is equivalent to finding rational points on the surface S given by the equation

$$S : 4z^2 = -2 + 2P^2 - P^4 + 2(P^2 + 1)Q^2 - Q^4 =: H(P, Q). \quad (9)$$

From a geometric point of view, the (homogenized version) of the surface S represents a del Pezzo surface of degree two which is just a blowup of seven points lying in general

position in \mathbb{P}^2 . In particular, this implies that the surface is geometrically rational which means that it is rational over \mathbb{C} . Note that this immediately implies the potential density of rational points on S , which means that there is a finite extension K of \mathbb{Q} such that $S(K)$ is dense in the Zariski topology. However, we are interested in the density of rational points in the Euclidean topology, and it seems that there is no way to use the mentioned property in order to address this. We thus provide alternative reasoning.

First, from (8) we have the inequalities $|P| \geq 1/2$, $|Q| \geq 1/2$, and because $H(P, Q) = H(\pm P, \pm Q)$ we may suppose without loss of generality that $P \geq 1/2$, $Q \geq 1/2$. We have the point on \mathcal{S} defined by $(P_0(u, v), Q_0(u, v), z_0(u, v)) =$

$$\left(\frac{u^4 + 1 - 4\frac{u(u^2-1)}{u^2+1}v + 2v^2}{4(u^2-1)v}, \frac{u^4 + 1 + 4\frac{u(u^2-1)}{u^2+1}v + 2v^2}{4(u^2-1)v}, \frac{u^4 + 1 - 2v^2}{4(u^2+1)v} \right);$$

and in the domain $\mathcal{D} := \{(u, v) \in \mathbb{R}^2 : u > 1, v > 0\}$, it is straightforward to verify that $P_0(u, v)$ has a single extremum at the point

$$(u_0, v_0) = (\alpha + \alpha^2, (1 + \alpha)(1 + \alpha^2)), \quad \alpha^2 = \frac{1 + \sqrt{5}}{2}.$$

This point is a local minimum, with minimum value $P_0(u_0, v_0) = \frac{1}{2}$. Since $P_0(u, v)$ is a continuous function in \mathcal{D} and $\lim_{u \rightarrow 1+} P_0(u, v) = \lim_{v \rightarrow 0+} P_0(u, v) = \infty$, it follows that the set of values $\{P_0(u, v) : u \in \mathbb{Q} \cap (1, \infty), v \in \mathbb{Q} \cap (0, \infty)\}$ is dense in the real interval $(\frac{1}{2}, \infty)$. Next, consider the equation

$$C : 4Z^2 = H(P_0(u, v), Q),$$

which we regard as defining a curve C over $\mathbb{Q}(u, v)$. The curve possesses the point $(Q, Z) = (Q_0(u, v), z_0(u, v))$, and has cubic model

$$\begin{aligned} E : y^2 = x^3 - & ((1 + u^2)^2(1 + u^4)^2 + 8u(1 - u^8)v + 4(5 + 6u^2 - 14u^4 + 6u^6 + 5u^8)v^2 + \\ & 16u(1 - u^4)v^3 + 4(1 + u^2)^2v^4)x^2 + 16(u^4 - 1)^2v^2((1 + u^2)(1 + u^4) + \\ & 2(1 - u)(1 + u)^3v + 2(1 + u^2)v^2)((1 + u^2)(1 + u^4) - \\ & 2(1 - u)^3(1 + u)v + 2(1 + u^2)v^2)x. \end{aligned}$$

It is easy to check that if $u', v' \in \mathbb{Q}$, then the curve $E_{u', v'}$ obtained from E by the specialization $u = u'$, $v = v'$ is singular only when $u = 1$ or $v = 0$. However, the sets $\{1\} \times \mathbb{Q}$, $\mathbb{Q} \times \{0\}$ have empty intersection with \mathcal{D} . Thus, for all $(u', v') \in (\mathbb{Q} \times \mathbb{Q}) \cap \mathcal{D} =: \mathcal{D}'$, the specialized curve $E_{u', v'}$ is an elliptic curve. Furthermore, we note that for each $u', v' \in \mathbb{Q}$, $E_{u', v'}$ has three points of order 2 defined over \mathbb{R} (this is a simple consequence of the positivity of the discriminant of the polynomial defining the curve E), with x -coordinates $0 < r_1 < r_2$, so that $(0, 0)$ lies on the bounded component of the curve.

The image $R_{u,v}$ on E of the point $(-Q_0(u, v), z_0(u, v))$ is of infinite order as element of the group $E(\mathbb{Q}(u, v))$. For any given $u' \in \mathbb{Q} \cap (1, \infty)$ it is straightforward to compute the set of rational numbers $v' \in \mathbb{Q} \cap (0, \infty)$ such that the point $R_{u',v'}$ is of finite order on $E_{u',v'}$; this set is finite in consequence of Mazur's theorem. Applying Silverman's theorem, for given $u' \in \mathbb{Q} \cap (1, \infty)$ then for all but finitely many $v' \in \mathbb{Q}$ the point $R_{u',v'}$ is of infinite order on the curve $E_{u',v'}$.

Now choose sequences $(u_n)_{n \in \mathbb{N}}$, $(v_n)_{n \in \mathbb{N}}$ of rational numbers such that

$$u_n \in \mathbb{Q} \cap (1, \infty), \lim_{n \rightarrow +\infty} u_n = \alpha + \alpha^2, \quad v_n \in \mathbb{Q} \cap (0, \infty), \lim_{n \rightarrow +\infty} v_n = (1 + \alpha)(1 + \alpha^2),$$

so that $\lim_{n \rightarrow +\infty} P_0(u_n, v_n) = 1/2$.

With $R_{u_n,v'}$ of infinite order on $E_{u_n,v'}$, then either $R_{u_n,v'}$ or $R_{u_n,v'} + (0, 0)$ lies on the bounded component of the curve, and we can apply the Hurwitz theorem as before to deduce that the set $E_{u_n,v'}(\mathbb{Q})$ is dense in the set $E_{u_n,v'}(\mathbb{R})$. This immediately implies that the set $E(\mathbb{Q})$ is dense in the set $E(\mathbb{R})$. Because E is birationally equivalent to C , we get that $C(\mathbb{Q})$ is dense in $C(\mathbb{R})$. Because

$$\bigcup_{n \in \mathbb{N}} \{P_0(u_n, v') : v' \in \mathbb{Q} \cap (0, \infty)\}$$

is dense in $(\frac{1}{2}, \infty)$, it follows that $\mathcal{S}(\mathbb{Q}) \cap \{(P, Q, z) : P > 1/2\}$ is dense in the Euclidean topology in the set $\mathcal{S}(\mathbb{R}) \cap \{(P, Q, z) : P > 1/2\}$. Our theorem follows. \square

In the following discussion we present an idea which can be used alternatively in the proof. However, we were unable to perform all necessary computations.

The proof could be simplified if we were able to demonstrate finiteness of the set of $(u', v') \in \mathcal{D}'$ for which the point $R_{u',v'}$ is of finite order in $E(\mathbb{Q})$, for then the theorems of Silverman and Hurwitz could be applied directly without the necessity of selecting limiting sequences. However, this computation is difficult. By Mazur's theorem the point $R_{u',v'}$ on $E_{u',v'}$ is of finite order provided $mR_{u',v'} = \mathcal{O}$ for some $m \in \{2, \dots, 10, 12\}$. Let

$$mR_{u,v} = \left(\frac{x_m}{d_m^2}, \frac{y_m}{d_m^3} \right),$$

where $x_m, y_m, d_m \in \mathbb{Q}[u, v]$ for $m = 2, \dots, 10, 12$. We consider the denominator of the x -coordinate of the point $mR_{u',v'}$ and define the curve $C_m : d_m(u, v) = 0$. The set $C_m(\mathcal{D}')$ of points in \mathcal{D}' lying on C_m parameterize those pairs $(u', v') \in \mathcal{D}'$ which lead to $R_{u',v'}$ of order (dividing) m . Consider the map

$$\Phi : C_m(\mathcal{D}') \ni (u, v) \mapsto u \in \mathbb{Q}.$$

and put

$$B := \bigcup_{m=2}^{12} \Phi(C_m(\mathcal{D}')),$$

where for $m = 7, 11$ we put $C_m(\mathcal{D}') = \emptyset$. Indeed, the case $m = 7$ is impossible due to the existence of the rational point $(0, 0)$ of order 2 on $E_{u', v'}$ and the fact that the torsion group of $E_{u', v'}$ cannot be isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_7 \simeq \mathbb{Z}_{14}$. From the definition of B , if $u' \notin B$ then the point $R_{u', v'}$ is of infinite order on $E_{u', v'}$ for all rational $v' > 0$. In theory at least it is possible to give a precise description of the set B . Indeed, for given m the polynomial d_m may be factorized as $d_m = f_{1,m} \cdot \dots \cdot f_{k_m,m}$ in $\mathbb{Q}[u, v]$, where $f_{i,m}$ is irreducible in $\mathbb{Q}[u, v]$. Thus $d_m(u, v) = 0$ if and only if $f_{i,m}(u, v) = 0$ for some $i \in \{1, 2, \dots, k_m\}$. The equation $f_{i,m}(u, v) = 0$ defines an irreducible curve, say $C_{i,m}$, and thus

$$B = \bigcup_{m=2}^{12} \bigcup_{i=1}^{k_m} \Phi(C_{i,m}(\mathcal{D}'))$$

(where we define $C_{i,7}(\mathcal{D}') = C_{i,11}(\mathcal{D}') = \emptyset$). For example, we have $d_2(u, v) = (u^2 - 1)(u^4 - 2v^2 + 1)f_{4,2}(u, v)f_{5,2}(u, v)$. The curve $C_{3,2} : u^4 - 2v^2 + 1 = 0$ is of genus 1 and the only rational points on $C_{3,2}$ satisfy $|u| = |v| = 1$. The genus of $C_{4,2}$ is 3 and the genus of $C_{5,2}$ is 19; thus by Faltings's theorem these curves contain only finitely many rational points. However, we are unable to compute the corresponding sets. Matters are even worse for $m \geq 3$. It is a non-trivial task to compute the factorization of d_m and even when this has been done, it is still necessary to compute the genus of the corresponding curves. Indeed, although the factorization of multivariate polynomials with rational coefficients can be computed in polynomial time [12], sometimes, especially in the case of polynomials of high degree, this procedure is time and memory consuming.

When $m = 3$ we were able to compute that $d_3(u, v) = (u^2 - 1)(u^4 - 2v^2 + 1)f_{4,3}(u, v)$, where $f_{4,3}$ is irreducible of degree 72. A few hours of computation was needed in order to check that the genus of $C_{4,3}$ is ≥ 65 . To get this inequality we reduce the curve $C_{4,3}$ modulo 5 and observe that $f_{4,3} \in \mathbb{F}_5[u, v]$ is irreducible and $\deg_{\mathbb{Q}[u, v]} f_{4,3} = \deg_{\mathbb{F}_5[u, v]} f_{4,3}$. We thus get the inequality $\text{genus}_{\mathbb{C}}(C_{4,3}) \geq \text{genus}_{\mathbb{F}_5}(C_{4,3}) = 65$, where the last equality was obtained via computation in Magma [13]. When $m = 4$ we have $d_4(u, v) = (u^2 - 1)(u^4 - 2v^2 + 1)f_{4,4}(u, v)f_{5,4}(u, v)$, where $\deg f_{4,4} = 36$ and $\deg f_{5,4} = 72$. Using similar reasoning as for $m = 3$, the genus of $C_{4,4}$ is ≥ 29 and the genus of $C_{5,4}$ is ≥ 113 (in this case we performed calculations over \mathbb{F}_3). When $m = 5$ we have $d_5(u, v) = (u^2 - 1)(u^4 - 2v^2 + 1)f_{4,5}(u, v)$, where $\deg f_{4,5} = 216$. We were unable to finish the genus calculations in this case: Magma was still running after three days. However, we expect that these computations can be performed and believe that in each case the genus of the corresponding curve is ≥ 2 which would imply (via the Faltings theorem) that the set B is finite. All computations were performed on a typical notebook with 8 GB of RAM and Intel i7 processor.

Remark 3.3. The combination of the theorems of Hurwitz and Silverman which allows proof of the density results is a very useful tool and can be used in other situations too; see [2,4,18].

Remark 3.4. It is clear that the same result as in Proposition 3.2 can be obtained for the plane given by the equation $y = \frac{1}{2}$.

We are able to prove the following result (which falls short of being a density statement) concerning the existence of rational points on the plane $x = y$ with rational distances to elements of A .

Proposition 3.5. *Let π be the plane in \mathbb{R}^3 given by $\pi : x = y$. Then the set*

$$\Pi = \{P \in \pi(\mathbb{Q}) : \text{the distance } |PQ| \text{ is rational for all } Q \in A\}$$

contains images of infinitely many rational parametric curves.

Proof. We now have

$$\begin{cases} 2x^2 + z^2 &= P^2, \\ 2x^2 - 2x + 1 + z^2 &= Q^2, \\ 2(x-1)^2 + z^2 &= S^2. \end{cases} \quad (10)$$

Thus

$$P^2 - 2Q^2 + S^2 = 0, \quad x = 1/2 + (P^2 - Q^2)/2, \quad z^2 = P^2 - 2x^2.$$

The former is parametrized by

$$\tau P = m^2 + 2m - 1, \quad \tau Q = m^2 + 1, \quad \tau S = m^2 - 2m - 1,$$

giving

$$x = 1/2 - 2m(1 - m^2)/\tau^2, \quad (\tau^2 z)^2 = 1/2(\tau^2 - 8m^2)(-\tau^2 + 2(1 - m^2)^2).$$

Regard the latter as an elliptic quartic over $\mathbb{Q}(m)$. Under the quadratic base change $m = 4k/(2 + k^2)$, the curve becomes, with $\tau = t/(2 + k^2)^2$, $Z = t^2 z$,

$$\mathcal{C} : Z^2 = -\frac{1}{2}(t^2 - 128k^2(2 + k^2)^2)(t^2 - 2(4 - 12k^2 + k^4)^2),$$

which has a point at

$$(t, Z) = \left(\frac{4(2+k^2)^2(4-12k^2+k^4)}{(12-4k^2+3k^4)}, \frac{4(4-k^4)(4-12k^2+k^4)(16-352k^2-104k^4-88k^6+k^8)}{(12-4k^2+3k^4)^2} \right).$$

A cubic model of the curve is

$$\mathcal{E} : Y^2 = X(X - (4 - 16k - 12k^2 - 8k^3 + k^4)^2)(X - (4 + 16k - 12k^2 + 8k^3 + k^4)^2),$$

with point of infinite order $Q = (X, Y)$, where

$$X = \frac{(2+k^2)^2(12-4k^2+3k^4)^2}{(-2+k^2)^2},$$

$$Y = \frac{8(2+k^2)(-16+20k^2+k^6)(-4-5k^4+k^6)(12-4k^2+3k^4)}{(-2+k^2)^3}.$$

We do not present explicitly the map $\varphi : C \rightarrow \mathcal{E}$ because the formula is unwieldy. Note that the existence of Q of infinite order on \mathcal{E} implies the Zariski density of rational points on the surface \mathcal{E} (using the same reasoning as in the proof of the previous theorem). Computing $\varphi^{-1}(mQ)$ for $m \in \mathbb{Z}$, and then the expressions for x, z , we get rational parametric solutions of the system (10). This observation finishes the proof. \square

Remark 3.6. The simplest parametric solution of (10) that we find is

$$x = y = \frac{(4+2k-2k^2+k^3)(2-2k+k^2+k^3)(4-16k-12k^2-8k^3+k^4)}{2(2+k^2)^3(4-12k^2+k^4)},$$

$$z = \frac{(2-k^2)(16-352k^2-104k^4-88k^6+k^8)}{4(2+k^2)^3(4-12k^2+k^4)}.$$

4. Points in \mathbb{Q}^3 at rational distance to the vertices of the unit square

We consider here the problem of finding points in \mathbb{Q}^3 that lie at rational distance to the vertices of the unit square, i.e. we do not assume any additional constraints on the coordinates of the points. From the previous section we know that there is an infinite set \mathcal{M} of rational curves lying in the plane $x = 1/2$ (or in the plane $x = y$) with the property that each rational point on each curve $C \in \mathcal{M}$ has rational distance to the vertices of the unit square. A question arises whether in the more general situation considered here we can expect the existence of rational surfaces having the same property. Moreover, can any density result be obtained in this case? Unfortunately, we are unable to prove any density result. However, we show that there are many rational points in \mathbb{Q}^3 lying at rational distance to the vertices of the unit square.

Before stating the principal result of this section, let us recall the notion of *unirationality* of an (affine) algebraic variety $V \subset k^m$, where k is a field and $m \in \mathbb{N}_{\geq 2}$. We

say that V is unirational over k if there exists a rational map

$$\varphi : k^n \dashrightarrow V$$

defined over k such that V is the closure of the image of φ . More precisely, there is an open set $U \subset k^n$ such that $\overline{\varphi(U)} = V$ (in the Zariski topology). The map φ is called a *rational parametrization* of V . It can be shown that V is unirational over k if there exists an injection of k -algebras $\psi : k[V] \hookrightarrow k[x_1, x_2, \dots, x_n]$. A stronger notion is that of *rationality*. We say that V is rational over k if it admits a rational parametrization $\varphi : k^n \dashrightarrow V$ such that the induced field extension $k(V) \hookrightarrow k(x_1, \dots, x_n)$ is an isomorphism. It is clear that each rational variety is unirational. We should note that in general it is a difficult problem to determine whether or not a given variety is unirational or rational. In the case of curves the notion of unirationality and rationality are the same (Lüroth's theorem). The same is true in the case of surfaces defined over an algebraically closed field (Castelnuovo's theorem). In the case of dimension at least 3 these notions are different and depend on k . For example, there are cubic hypersurfaces which are unirational over \mathbb{Q} , but not rational even over \mathbb{C} ; see [5]. In fact, for any field k , a smooth cubic hypersurface with k -rational point is k -unirational [10]. It is also known that no smooth quartic threefold is rational (and there do exist unirational quartic threefolds) [9]. The interested reader can find a good introduction to these and related topics in [11].

We are ready to prove the following:

Theorem 4.1. Put $A = \{(0, 0, 0), (0, 1, 0), (1, 0, 0), (1, 1, 0)\}$ and consider the set

$$\mathcal{F} := \{P \in \mathbb{Q}^3 : \text{the distance } |PQ| \text{ is rational for all } Q \in A\}.$$

Then the algebraic variety parameterizing the set \mathcal{F} is unirational over \mathbb{Q} .

Proof. It is clear that points in \mathcal{F} are in one-to-one correspondence with rational points on the intersection in \mathbb{R}^7 of the following four quadratic threefolds:

$$\begin{cases} x^2 + y^2 + z^2 & = P^2, \\ (1-x)^2 + y^2 + z^2 & = Q^2, \\ x^2 + (1-y)^2 + z^2 & = R^2, \\ (1-x)^2 + (1-y)^2 + z^2 & = S^2. \end{cases} \quad (11)$$

We immediately have

$$x = \frac{1}{2}(P^2 - Q^2 + 1), \quad y = \frac{1}{2}(P^2 - R^2 + 1), \quad (12)$$

and $P^2 - R^2 = Q^2 - S^2$. All rational solutions of the latter are given by

$$P = uX + Y, \quad Q = uX - Y, \quad R = uY + X, \quad S = uY - X,$$

and then from (12),

$$x = 2uXY + \frac{1}{2}, \quad y = \frac{1}{2}(u^2 - 1)(X^2 - Y^2) + \frac{1}{2}.$$

Finding points on the system (11) now reduces to studying the algebraic variety

$$\mathcal{S} : V^2 = G(u, X, Y),$$

where $V = 2z$ and the polynomial G is given by

$$G(u, X, Y) = -2 + 2(u^2 + 1)(X^2 + Y^2) - (u^2 - 1)^2(X^2 - Y^2)^2 - 16u^2X^2Y^2.$$

The dimension of \mathcal{S} is 3. However, we can view the variety \mathcal{S} as a del Pezzo surface of degree two defined over the field $\mathbb{Q}(u)$. It is known then that the existence of a sufficiently general $\mathbb{Q}(u)$ -rational point on \mathcal{S} implies $\mathbb{Q}(u)$ -unirationality, and in consequence \mathbb{Q} -unirationality, of \mathcal{S} (see Manin [14, Theorem 29.4]). However, it seems that there is no general $\mathbb{Q}(u)$ -rational point on \mathcal{S} . Thus it is natural to ask how one can construct a rational base change $u = \varphi(t)$ such that the surface $\mathcal{S}_\varphi : V^2 = G(\varphi(t), X, Y)$ defined over the field $\mathbb{Q}(t)$, contains a $\mathbb{Q}(t)$ -rational point. We present the following approach to this problem. Suppose that $Q_0 = (u_0, X_0, Y_0, V_0)$ is a rational point with non-zero coordinates lying on \mathcal{S} . We construct a parametric curve \mathcal{L} lying on \mathcal{S} as follows. Define \mathcal{L} by equations

$$\mathcal{L} : u = u_0, \quad X = T + X_0, \quad Y = pT + Y_0, \quad V = qT^2 + tT + V_0,$$

where t is a rational parameter and p, q, T are to be determined. With u, X, Y, V so defined, $V^2 - G(u, X, Y) = \sum_{i=1}^4 A_i(p, q)T^i$. The expression A_1 is linear in p and takes the form $A_1 = pB_1 + B_0 + 2tV_0$, where B_0, B_1 depend only on the coordinates of the point Q . In particular, A_1 is independent of q ; so the equation $A_1 = 0$ has a non-zero solution for p if and only if $B_1 \neq 0$. The expression for B_1 is

$$B_1 = 4Y_0((-u_0^4 + 10u_0^2 - 1)X_0^2 + (u_0^2 - 1)^2Y_0^2 - u_0^2 - 1).$$

Next, observe that $A_2 = C_2p^2 + C_1p + C_0 + 2qV_0 + t^2$, where C_i depend only on the coordinates of the point Q_0 for $i = 0, 1, 2$, and thus $A_2 = 0$ can be solved for q precisely when V_0 is non-zero. To sum up, the system $A_1 = A_2 = 0$ has a non-trivial solution for p, q as rational functions in $\mathbb{Q}(t)$ when $B_1V_0 \neq 0$. With p, q computed in this way:

$$V^2 - G(u, X, Y) = T^3(A_3(p, q) + A_4(p, q)T).$$

If $A_3A_4 \neq 0$ as a function in t then the expression for T that we seek is given by $T = -A_3(p, q)/A_4(p, q)$. Thus if the point $Q_0 = (u_0, X_0, Y_0, V_0)$ satisfies certain conditions, then there exists a rational curve on the surface $\mathcal{S}_{u_0} : V^2 = G(u_0, X, Y)$. Moreover, the

curve constructed in this manner can be used to produce rational expressions for P , Q , R , S and in consequence rational expressions for x , y , z satisfying the system (11).

Let $X = X'(t)$, $Y = Y'(t)$ be parametric equations of the constructed curve. The polynomial G is invariant under the mapping $(u, X, Y) \mapsto \left(\frac{X}{Y}, uY, Y\right)$ and thus we can define a non-constant base change $u = \varphi(t) = X'(t)/Y'(t)$ such that the surface $\mathcal{S}_\varphi : V^2 = G(\varphi(t), X, Y)$ contains the $\mathbb{Q}(t)$ -rational point $(X, Y) = (u_0 Y'(t), Y'(t))$. Using the cited result of Manin we get $\mathbb{Q}(t)$ -unirationality of \mathcal{S}_φ and in consequence \mathbb{Q} -unirationality of \mathcal{S} .

Thus in order to finish the proof it suffices to find a suitable point Q_0 on the three-fold \mathcal{S} . It is straightforward to check that all the required conditions on Q_0 are met on taking

$$(u_0, X_0, Y_0, V_0) = \left(2, \frac{1}{12}, \frac{19}{36}, \frac{7}{27}\right).$$

With this choice of Q_0 , the expressions for x , y , z arising from the constructed parametric curve are as follows:

$$\begin{aligned} x &= 3(5\,522\,066\,829\,177\,276\,301\,427\,600 - 258\,403\,606\,687\,492\,419\,505\,600t \\ &\quad + 24\,350\,105\,869\,790\,104\,153\,088t^2 - 930\,272\,613\,423\,360\,964\,576t^3 \\ &\quad + 39\,295\,267\,680\,627\,366\,536t^4 - 1\,085\,485\,845\,235\,095\,088t^5 \\ &\quad + 24\,133\,448\,660\,417\,792t^6 - 401\,146\,604\,231\,320t^7 + 3\,899\,504\,263\,625t^8)/\Delta^2, \\ y &= 30(3\,992\,136\,439\,221\,148\,602\,640 - 6\,939\,554\,120\,499\,388\,567\,712t \\ &\quad + 117\,488\,065\,643\,083\,258\,096t^2 - 13\,393\,876\,262\,858\,078\,048t^3 \\ &\quad + 411\,476\,041\,942\,299\,568t^4 - 13\,249\,457\,441\,223\,848t^5 \\ &\quad + 681\,815\,047\,971\,100t^6 - 7\,562\,115\,944\,888t^7 + 337\,499\,289\,355t^8)/\Delta^2, \\ z &= 714(3\,779\,374\,597\,422\,498\,556\,400 + 529\,318\,935\,972\,209\,201\,600t \\ &\quad - 977\,278\,343\,015\,269\,168t^2 + 1\,745\,565\,618\,326\,470\,736t^3 \\ &\quad - 10\,290\,117\,484\,952\,896t^4 + 1\,635\,035\,001\,144\,368t^5 \\ &\quad - 3\,620\,551\,914\,412t^6 + 458\,263\,598\,420t^7 + 118\,863\,425t^8)/\Delta^2, \end{aligned}$$

where

$$\Delta = 18(221\,769\,748\,580 - 3\,052\,768\,504t + 670\,128\,264t^2 - 6\,059\,132t^3 + 500\,425t^4). \quad \square$$

Remark 4.2. The point (x, y, z) satisfies $0 < x, y < 1$ for values of t satisfying $t < -10.9337$, or $t > 28.2852$.

Table 2Points in \mathbb{Q}^3 at rational distance to the vertices of the unit square.

x	y	z	x	y	z
41/27	77/108	28/27	1/35	37/105	17/140
5/54	35/108	7/54	161/80	587/300	7/25
83/125	549/500	14/75	37/156	987/2704	119/676
1/189	283/756	31/189	232/189	493/756	59/189
113/190	2369/1900	287/2850	202/195	213/325	161/1300
383/348	5397/1682	2429/1682	571/476	2419/2975	94/425
203/594	119/1188	469/594	1589/594	985/1188	427/594
1/756	127/1512	307/756	1436/847	7967/3388	992/847
127/1029	341/1372	307/343	251/1029	401/1372	223/343
791/1210	5299/3630	2569/2420	1571/1210	7487/7260	509/1210
1906/2541	4019/3388	360/847	2185/2541	3819/3388	345/847
3059/2738	4487/5476	3059/8214			

Notwithstanding the large coefficient size in the above parameterization, there seem to be many points in \mathbb{Q}^3 at rational distance to the vertices A of the unit square. A (non-exhaustive) search finds the following points $(x, y, z) \in \mathbb{Q}^3$ of height at most 10^4 , $x \neq \frac{1}{2}$, $x \neq y$, having rational distances to the vertices $(0, 0, 0)$, $(0, 1, 0)$, $(1, 0, 0)$, $(1, 1, 0)$ of the unit square, and which lie in the positive octant. We list only one point under the symmetries $x \leftrightarrow 1 - x$, $y \leftrightarrow 1 - y$, $x \leftrightarrow y$. (See Table 2.)

We are motivated to make the following conjecture.

Conjecture 4.3. Put $A = \{(0, 0, 0), (0, 1, 0), (1, 0, 0), (1, 1, 0)\}$ and consider the set

$$\mathcal{F} := \{P \in \mathbb{Q}^3 : \text{the distance } |PQ| \text{ is rational for all } Q \in A\}.$$

Then \mathcal{F} is dense in \mathbb{R}^3 in the Euclidean topology.

5. Points with rational distances from the vertices of a tetrahedron

Let P_0, P_1, P_2, P_3 be given points in \mathbb{Q}^3 , not all lying on a plane. Without loss of generality we may assume that $P_0 = (0, 0, 0)$. Put $P_i = (a_{i1}, a_{i2}, a_{i3})$ for $i = 1, 2, 3$, and define $d_{ij} = |P_i P_j|$ for $0 \leq i < j \leq 3$, i.e. d_{ij} is the distance between the points P_i, P_j . The constraint on the points P_i implies that the points define the vertices of a genuine tetrahedron with non-zero volume, so that the determinant of the matrix $[a_{ij}]_{1 \leq i, j \leq 3}$ is non-zero. Let $P = (x, y, z)$ be a point in \mathbb{Q}^3 with rational distance to each of the points P_0, P_1, P_2, P_3 . The corresponding system of Diophantine equations is thus

$$\begin{cases} x^2 + y^2 + z^2 &= Q_0^2 \\ (x - a_{i1})^2 + (y - a_{i2})^2 + (z - a_{i3})^2 &= Q_i^2, \quad \text{for } i = 1, 2, 3, \end{cases}$$

or equivalently, on replacing the second, third, and fourth equations by their differences with the first equation,

$$\begin{cases} x^2 + y^2 + z^2 &= Q_0^2 \\ a_{i1}x + a_{i2}y + a_{i3}z &= \frac{1}{2}(Q_0^2 - Q_i^2 + d_{0i}^2), \quad \text{for } i = 1, 2, 3. \end{cases} \quad (13)$$

Since the determinant of the matrix $A = [a_{ij}]_{1 \leq i, j \leq 3}$ is non-zero, the (linear) system consisting of the last three equations from (13) can be solved with respect to x, y, z . The solution takes the following form:

$$x = \frac{\det A_1}{\det A}, \quad y = \frac{\det A_2}{\det A}, \quad z = \frac{\det A_3}{\det A} \quad (14)$$

where A_i , for $i = 1, 2, 3$, is obtained from the matrix A by replacing the i -th column by the column comprising the right-hand sides of the last three equations from (13). In particular, x, y, z are (inhomogeneous) quadratic forms in four variables Q_0, Q_1, Q_2, Q_3 , with coefficients in $\mathbb{K} := \mathbb{Q}(\{a_{ij} : i, j \in \{1, 2, 3\}\})$. Putting these computed values of x, y, z into the first equation, there results one inhomogeneous equation of degree four in four variables. We homogenize this equation by introducing new variables $Q_i = R_i/R_4$ for $i = 0, 1, 2, 3$, and work with the quartic threefold, say \mathcal{X} , defined by an equation of the form $\mathcal{F}(\mathbf{R}) = 0$, where for ease of notation we put $\mathbf{R} = (R_0, R_1, R_2, R_3, R_4)$. Using Mathematica, the set $\text{Sing}(\mathcal{X})$ of singular points of the variety \mathcal{X} is computed to be

$$\begin{aligned} \text{Sing}(\mathcal{X}) = \{ & (0, \pm d_{01}, \pm d_{02}, \pm d_{03}, 1), (\pm d_{01}, 0, \pm d_{12}, \pm d_{13}, 1), \\ & (\pm d_{02}, \pm d_{12}, 0, \pm d_{23}, 1), (\pm d_{03}, \pm d_{12}, \pm d_{23}, 0, 1), (1, \pm 1, \pm 1, \pm 1, 0) \}. \end{aligned}$$

Thus for generic choice of P_1, P_2, P_3 , the variety \mathcal{X} contains 40 isolated singular points.

We now prove that for generic choice of P_1, P_2, P_3 , there is a solution depending on three (homogeneous) parameters of the equation defining the variety \mathcal{X} . We thus regard a_{ij} as independent variables and work with \mathcal{X} as a quartic threefold defined over the rational function field \mathbb{K} . In order to find a parameterization we will use the rational double point $P = (1, 1, 1, 1, 0)$ lying on \mathcal{X} and the idea used in the proof of Theorem 4.1. Put

$$R_0 = T + 1, \quad R_i = (p_i + 1)T + 1, \quad \text{for } i = 1, 2, 3, \quad \text{and} \quad R_4 = p_4 T,$$

where p_i and T are to be determined. On substituting these expressions into the equation $\mathcal{F}(\mathbf{R}) = 0$, there results $T^2(C_2 + C_3T + C_4T^2) = 0$, where C_i is a homogeneous form of degree i in the four variables p_1, \dots, p_4 . Certainly under the assumption on the points $P_i, i = 0, 1, 2, 3$ (namely, $\det A \neq 0$), the form C_2 is non-zero as an element of $\mathbb{K}[p_1, p_2, p_3, p_4]$. Indeed, we have $C_2(0, 0, 0, p_4) = -(\det A)^2 p_4^2$. We also checked that for a generic choice of the points P_1, P_2, P_3 , the polynomial C_2 is genuinely dependent upon the variables p_1, \dots, p_4 , in that there are no linear forms $L_j(p_1, \dots, p_4)$, $j = 1, 2, 3$, such that $C_2(L_1, L_2, L_3)$ is a form in three or fewer variables.

Consider now the quadric $\mathcal{Y} : C_2(p_1, p_2, p_3, p_4) = 0$, regarded as a quadric defined over \mathbb{K} . There are \mathbb{K} -rational points on \mathcal{Y} , namely $Y_j = (a_{1j}, a_{2j}, a_{3j}, 1)$, $j = 1, 2, 3$,

and so in particular, \mathcal{Y} can be rationally parameterized with parametrization of the form $p_i = X_i(q_1, q_2, q_3)$, for homogeneous quadratic forms X_i , $i = 1, 2, 3, 4$. Thus, after the substitution $p_i \rightarrow X_i$ there results an equation $T^3(C'_3 + C'_4 T) = 0$, where $C'_i = C_i(X_1, X_2, X_3, X_4)$ and $C'_i \neq 0$ as an element of $\mathbb{K}[q_1, q_2, q_3]$ for $i = 3, 4$. This equation has a non-zero \mathbb{K} -rational root $T = \varphi(q_1, q_2, q_3) = -C'_3/C'_4$ and accordingly we get a rational parametric solution in three (homogeneous) parameters of the equation defining \mathcal{X} , in the form

$$Q_0 = \frac{1}{X_4(\mathbf{q})} \left(1 + \frac{1}{\varphi(\mathbf{q})} \right), \quad Q_i = \frac{1}{X_4(\mathbf{q})} \left(1 + X_i(\mathbf{q}) + \frac{1}{\varphi(\mathbf{q})} \right), \quad i = 1, 2, 3,$$

where we put $\mathbf{q} = (q_1, q_2, q_3)$. It is straightforward to check that the image of the map $\Phi : \mathbb{P}(\mathbb{K})^2 \ni (q_1, q_2, q_3) \mapsto (Q_0, Q_1, Q_2, Q_3) \in \mathcal{X}(\mathbb{K})$ is not contained in a curve lying on the variety \mathcal{X} . Using now the expressions for Q_0, Q_1, Q_2, Q_3 , we can recover the corresponding expressions for x, y, z given by (14).

It is possible to write down from the Jacobian matrix of $\mathbf{R}(q_1, q_2, q_3)$ all the conditions on $\{a_{ij}\}$, $i, j \in \{1, 2, 3\}$, which guarantee that the parameterization is genuinely dependent on three (homogeneous) parameters. However, we refrain from doing so, because the computation is massively memory intensive, and the resulting equations complicated and unenlightening. If we choose particular values of a_{ij} , then this independence of q_1, q_2, q_3 is readily checked (as happens, for example, when $P_1 = (1, 0, 0)$, $P_2 = (0, 1, 0)$, $P_3 = (0, 0, 1)$). In general, there results an explicit rational parameterization in three independent parameters. There may, however, be some choices of vertices P_i for which this approach (with the particular rational double point chosen in the construction) results in the image of the map Φ being a curve lying on \mathcal{X} .

To sum up, we have the following result.

Theorem 5.1. *Let $P_0 = (0, 0, 0)$ and let $P_i = (a_{i1}, a_{i2}, a_{i3})$ be generic points in \mathbb{Q}^3 for $i = 1, 2, 3$. Then the variety parameterizing the points $P \in \mathbb{Q}^3$ with rational distances to P_i , $i = 0, 1, 2, 3$ is a quartic threefold \mathcal{X} ; and the set of rational parametric solutions of the equation defining \mathcal{X} is non-empty.*

We believe that much more is true.

Conjecture 5.2. *Let $P_0 = (0, 0, 0)$ and P_1, P_2, P_3 be generic rational points such that no three lie on a line and the points do not all lie on a plane. Then the variety, say \mathcal{X} , parameterizing those $P \in \mathbb{Q}^3$ with rational distances to P_i , $i = 0, 1, 2, 3$, is unirational over \mathbb{Q} .*

One can also state the following natural question.

Question 5.3. *Let \mathcal{X} be defined as in Conjecture 5.2. Is the set $\mathcal{X}(\mathbb{Q})$ dense in the Euclidean topology in the set $\mathcal{X}(\mathbb{R})$?*

We expect that the answer is yes.

Remark 5.4. The construction above finds a double infinity of points in \mathbb{Q}^3 at rational distance from the four vertices of the tetrahedron. If we suppose that the initial tetrahedron has rational edges, then we thus deduce infinitely many sets of five points in \mathbb{Q}^3 where the ten mutual distances are rational. We take as example the tetrahedron with vertices

$$P_1 = (0, 0, 0), \quad P_2 = (1, 0, 0), \quad P_3 = \left(\frac{11}{200}, \frac{117}{800}, 0 \right), \quad P_4 = \left(\frac{7}{25}, \frac{63}{325}, \frac{21}{260} \right).$$

This is chosen as an example of a tetrahedron, discovered by Rathbun, where the edges, face areas, and volume, are all rational. It corresponds to the first example in the list in Section D22 of Guy [7]. The explicit parametrization as computed above takes several computer screens to display, so we do not present it. However, on computing specializations, the point with smallest coordinates (minimizing the least common multiple of the denominators of x, y, z) that we could find is

$$\left(\frac{617}{4900}, \frac{2553}{63700}, \frac{3}{25480} \right),$$

which in fact lies within the tetrahedron.

Remark 5.5. The fact in the above proof that the matrix $A = [a_{ij}]_{1 \leq i, j \leq 3}$ is non-singular follows from the assumption that the points P_0, P_1, P_2, P_3 define a genuine tetrahedron. A question arises as to what can be said in the situation when $\det A = 0$? We need to consider two cases: where the rank $\text{rk}(A)$ is 2 or 1, corresponding respectively to the four points being coplanar, and the four points being collinear. Consider first the case of $\text{rk}(A) = 2$. Note that we encounter this situation in Section 4. The vectors P_1, P_2, P_3 are linearly dependent, and without loss of generality we can assume that P_1, P_2 are linearly independent, so that $P_3 = pP_1 + qP_2$ for some $p, q \in \mathbb{Q}$. It follows that the linear forms in x, y, z from the system (13) are linearly dependent. Let A_{ij} be the 2×2 matrix obtained from A by deleting the i -th row and the j -th column. Then at least one of A_{31}, A_{32}, A_{33} has non-zero determinant. Without loss of generality, suppose $\det A_{31} \neq 0$. Solving the first two equations at (13) with respect to y, z :

$$y = -\frac{\det A_{32}}{\det A_{31}}x - \frac{1}{2\det A_{31}}(a_{23}d_{01}^2 - a_{13}d_{02}^2 + (a_{23} - a_{13})Q_0^2 - a_{23}Q_1^2 + a_{13}Q_2^2),$$

$$z = -\frac{\det A_{33}}{\det A_{31}}x - \frac{1}{2\det A_{31}}(a_{22}d_{01}^2 - a_{12}d_{02}^2 + (a_{22} - a_{12})Q_0^2 - a_{22}Q_1^2 + a_{12}Q_2^2).$$

Moreover, Q_0, Q_1, Q_2, Q_3 need to satisfy the equation

$$\mathcal{Q}: (p + q - 1)Q_0^2 - pQ_1^2 - qQ_2^2 + Q_3^2 = d_{03}^2 - pd_{01}^2 - qd_{02}^2. \quad (15)$$

The quadric \mathcal{Q} may be viewed as a quadric defined over the function field $\mathbb{K} := \mathbb{Q}(\{a_{ij} : i = 1, 2, j = 1, 2, 3\})$. The quadric \mathcal{Q} contains the point at infinity $(Q_0 : Q_1 : Q_2 : Q_3 : T) = (1 : 1 : 1 : 1 : 0)$ and thus \mathcal{Q} can be parameterized by rational functions, say $Q_i = f_i(\mathbf{R}) \in \mathbb{K}(\mathbf{R})$, where $\mathbf{R} = (R_0, R_1, R_2)$ are (non-homogeneous) coordinates.

Moreover, the numerator of f_i is of degree ≤ 2 for $i = 0, 1, 2$; and the same is true for the common denominator of $f_i, i = 0, 1, 2$. Using this parametrization we compute the expressions for y, z . Next, substitute the computed values of y, z and Q_0 into the equation $x^2 + y^2 + z^2 = Q_0^2$. This equation is a quadratic equation in x of the form

$$C_2 x^2 + C_1 x + C_0 = 0,$$

where $C_i \in \mathbb{K}(\mathbf{R})$ for $i = 0, 1, 2$. We arrive at the problem of finding rational points on the threefold

$$\mathcal{X} : V^2 = C_1^2 - 4C_0C_2 =: F(\mathbf{R})$$

defined over the field \mathbb{K} . The polynomial F is of degree 6. However, one can check that with respect to each $R_i, i = 0, 1, 2$, the degree of F is 4, and thus \mathcal{X} can be viewed as a hyperelliptic quartic (of genus ≤ 1) defined over the field $\mathbb{K}(\mathbf{R}')$, where \mathbf{R}' is a vector comprising exactly two variables from R_0, R_1, R_2 . We thus expect that for most rational points P_1, P_2, P_3 with $P_3 = pP_1 + qP_2$, there is a specialization of R_0, R_1 (say), to rational numbers such that \mathcal{X}_{R_0, R_1} represents a curve of genus one with infinitely many rational points. Tracing back the reasoning in this case we will get infinitely many rational points with rational distances to the points P_0, P_1, P_2, P_3 .

What can be done in the case when $\text{rk}(A) = 1$ (which corresponds to the points P_0, P_1, P_2, P_3 being collinear)? In order to simplify the notation, put $P_1 = (a, b, c)$ and $d_{01} = d$. Without loss of generality we can assume that $P_2 = pP_1, P_3 = qP_1$ for some $p, q \in \mathbb{Q} \setminus \{0\}$. Then the system (13) comprises just one linear form in x, y, z which needs to be represented by three non-homogeneous quadratic forms. More precisely,

$$ax + by + cz = \frac{1}{2}(Q_0^2 - Q_1^2 + d^2) = \frac{1}{2p}(Q_0^2 - Q_2^2 + p^2 d^2) = \frac{1}{2q}(Q_0^2 - Q_3^2 + q^2 d^2). \quad (16)$$

Let \mathcal{V} be the variety defined by the last two equations. After homogenization by $Q_i \mapsto Q_i/T$ and simple manipulation, we get

$$\mathcal{V} : \begin{cases} Q_2^2 = (1-p)Q_0^2 + pQ_1^2 + p(p-1)d^2T^2, \\ Q_3^2 = (1-q)Q_0^2 + qQ_1^2 + q(q-1)d^2T^2. \end{cases}$$

The point $(Q_0 : Q_1 : Q_2 : Q_3 : T) = (1 : 1 : 1 : 1 : 0)$ lies on \mathcal{V} and can be used to find parametric solutions of the system defining \mathcal{V} . However, observe that any point which lies on \mathcal{V} with $T \neq 0$ allows us to compute the value of z from equation (16). This

expression for z depends on x, y , and substituting into the first equation at (13), namely $x^2 + y^2 + z^2 = Q_0^2$, we are left with one equation of the form

$$\mathcal{W}: C_0x^2 + C_1xy + C_2y^2 + C_3x + C_4y + C_5 = 0,$$

where C_i depends on p, q, a, b, c and the solution of the system defining the variety \mathcal{V} . In general, \mathcal{W} is a conic and thus has genus 0. Thus, provided that we can find a rational point on \mathcal{W} , we can find infinitely many rational points (in fact a parameterized curve) with rational distances to the four collinear points P_0, P_1, P_2, P_3 . As example here, assume that $d = \sqrt{a^2 + b^2 + c^2}$ is a rational number. Then the variety \mathcal{V} contains the rational line

$$(Q_0 : Q_1 : Q_2 : Q_3 : T) = (u - d/2 : u + d/2 : u - (1/2 - p)d : u - (1/2 - q)d : 1).$$

In this case (16) reduces to the one equation $ax + by + cz = d(d - 2u)/2$. Solving for z , and performing the necessary computations, the equation for the quadric \mathcal{W} takes the following form:

$$V^2 = b^2 + c^2 - d^2 + 4adX - 4(a^2 + b^2 + c^2)X^2 = -a^2 + 4adX - 4d^2X^2 = -(a - 2dX)^2,$$

where $V = (2(b^2 + c^2)y - b(d^2 - 2du - 2ax))/(c(d - 2u))$ and $X = x/(d - 2u)$, the last identity following from the equality $a^2 + b^2 + c^2 = d^2$. From the assumption on rationality of d , we can find x, y, z in the following form:

$$x = \frac{a(d - 2u)}{2d}, \quad y = \frac{b(d - 2u)}{2d}, \quad z = \frac{c(d - 2u)}{2d},$$

with

$$Q_0 = \frac{d - 2u}{2}, \quad Q_1 = \frac{d + 2u}{2}, \quad Q_2 = dp - \frac{d - 2u}{2}, \quad Q_3 = dq - \frac{d - 2u}{2},$$

giving rational solutions of the original system.

Remark 5.6. Guy [7] gives one parameterized family of tetrahedra which have rational edges, face areas, and volume. He also lists nine examples due to John Leech of such tetrahedra comprised of four congruent acute-angled Heron triangles appropriately fitted together. The six edges of the tetrahedron thus fall into three equal pairs. We discover that it is straightforward to write down an infinite family of such tetrahedra as follows.

If the Heron triangle has sides p, q, r , then the area and volume conditions for the tetrahedron become

$$\begin{aligned} (p + q + r)(-p + q + r)(p - q + r)(p + q - r) &= \square, \\ 2(-p^2 + q^2 + r^2)(p^2 - q^2 + r^2)(p^2 + q^2 - r^2) &= \square. \end{aligned}$$

Using the Brahmagupta parameterization of Heron triangles, we set

$$(p, q, r) = ((v + w)(u^2 - vw), v(u^2 + w^2), w(u^2 + v^2)),$$

reducing the two conditions above to the single demand

$$-(u^2 - v^2)(u^2 - w^2)(u^2 - u(v + w) - vw)(u^2 + u(v + w) - vw) = \square.$$

Setting $W = w/u$, this is equivalent to

$$-(1 - W^2) \left(\frac{u + v}{u - v} - W \right) \left(\frac{u - v}{u + v} + W \right) = \square.$$

This elliptic quartic has cubic form

$$Y^2 = X(X + v^2(u^2 - v^2))(X - u^2(u^2 - v^2)).$$

Demanding a point with $X = 2uv^2(u + v)$ gives

$$2(3u - v)(-u + 2v) = \square,$$

parameterized by

$$(u, v, w) = (m^2 + 4, 3m^2 + 2), \text{ with } w = \frac{(2m^2 + 3)(m^2 + 4)}{4m^2 + 1}.$$

This in turn leads to the tetrahedron with vertices

$$\begin{aligned} P_1 &= (0, 0, 0), \\ P_2 &= (10(m^4 - 1)(m^4 + 3m^2 + 1), 0, 0), \\ P_3 &= \left(\frac{2(m^2 - 1)(m^2 + 4)(3m^2 + 2)^2}{5}, \frac{(m^2 + 4)(2m^2 + 3)(3m^2 + 2)(4m^2 + 1)}{5}, 0 \right), \\ P_4 &= \left(\frac{2(m^2 - 1)(2m^2 + 3)^2(4m^2 + 1)}{5}, \right. \\ &\quad \left. - \frac{(2m^2 + 3)(2m^2 - 5m - 2)(2m^2 + 5m - 2)(3m^2 + 2)}{5}, \right. \\ &\quad \left. 4(m^2 - 1)m(2m^2 + 3)(3m^2 + 2) \right); \end{aligned}$$

edge lengths (p, q, r) given by

$$\begin{aligned} p &= 10(m^4 - 1)(m^4 + 3m^2 + 1), \\ q &= (m^2 + 4)(3m^2 + 2)(2m^4 + 2m^2 + 1), \\ r &= (2m^2 + 3)(4m^2 + 1)(m^4 + 2m^2 + 2); \end{aligned}$$

face areas given by

$$(m^4 - 1)(m^2 + 4)(4m^2 + 1)(2m^2 + 3)(3m^2 + 2)(1 + 3m^2 + m^4);$$

and volume equal to

$$\frac{1}{62\,208}m(m^2 - 1)(m^4 - 1)(m^2 + 4)(4m^2 + 1)(2m^2 + 3)^2(3m^2 + 2)^2(1 + 3m^2 + m^4).$$

6. The unit cube

Finding an infinity of points in \mathbb{Q}^3 , if indeed such exist, that lie at rational distance from the *eight* vertices (i, j, k) , $i, j, k = 0, 1$, of the unit cube seems to be an intractable problem. If we restrict attention to the plane $x = y$, we are aware of the following two points (equivalent under the symmetry $x \leftrightarrow 1 - x$) where distances to the vertices of the unit square are rational, and distances to the two cube vertices $(1, 0, 1)$, $(0, 1, 1)$ are rational:

$$(x, y, z) = \left(\frac{31}{108}, \frac{31}{108}, \frac{1519}{1080} \right), \quad \left(\frac{77}{108}, \frac{77}{108}, \frac{1519}{1080} \right). \quad (17)$$

The defining system of equations for this situation is

$$\begin{cases} 2x^2 + z^2 & = P^2, \\ 2x^2 - 2x + 1 + z^2 & = Q^2, \\ 2(x - 1)^2 + z^2 & = S^2, \\ (1 - x)^2 + x^2 + (1 - z)^2 & = T^2. \end{cases}$$

Then $1 + Q^2 - 2z = T^2$, so we obtain

$$z^2 = 1/2(1 - 8m^2/t^2)(-1 + 2(1 - m^2)^2/t^2), \quad 1 + (1 + m^2)^2/t^2 - 2z = T^2.$$

Equivalently,

$$2(t^2 - 8m^2)(-t^2 + 2(1 - m^2)^2) = (t^2 + (1 + m^2)^2 - U^2)^2,$$

where $U = Tt$, $Z = t^2z$. A search over this surface up to a height of 5000 resulted in discovering only the point $(m, t, U) = (-24, 360, 313)$ and symmetries, leading to the points at (17).

A point on the plane $x = 1/2$ at rational distance from the vertices of the cube results in four pairs of equal distance, with defining equations

$$\begin{cases} 1/4 + y^2 + z^2 &= P^2, \\ 1/4 + (1-y)^2 + z^2 &= Q^2, \\ 1/4 + y^2 + (1-z)^2 &= R^2, \\ 1/4 + (1-y)^2 + (1-z)^2 &= S^2, \end{cases} \quad (18)$$

and we found no solution. However, if we ask only for *three* pairs of distances to the cube vertices be rational, rather than four, e.g. consider the system of equations defined by the first three equations from (18), then we are able to prove the following result.

Theorem 6.1. *Let \mathcal{A} be the set of rational curves lying on the plane $x = 1/2$ with the property that each rational point on $A \in \mathcal{A}$ has rational distances to six vertices of the unit cube. Then \mathcal{A} is infinite.*

Proof. We consider only the system of equations defined by the first three equations from the system (18) above (other cases are treated in the same manner). The six distances now fall into three equal pairs, requiring

$$y = (P^2 - Q^2 + 1)/2, \quad z = (P^2 - R^2 + 1)/2,$$

together with the equation which can be written in homogeneous coordinates in the following form:

$$\mathcal{V}: (P^2 - R^2)^2 + (P^2 - Q^2)^2 - 2(Q^2 + R^2)T^2 + 3T^4 = 0.$$

We prove that the set of rational curves lying on \mathcal{V} is infinite. Consider the intersection of \mathcal{V} with the family of planes $L_a: T = a(P - R)$. Remarkably, the intersection $\mathcal{V} \cap L_a$ defines a singular curve, say \mathcal{C} , in the projective plane $\mathbb{P}^2(\mathbb{Q}(a))$, with singular points $[P : Q : R] = [1 : \pm 1 : 1]$. In fact, the curve \mathcal{C} is of genus 1. By homogeneity we can assume that $R = 1$. Making a change of variables

$$(P, Q) = (p + 1, pq + 1) \quad \text{with inverse} \quad (p, q) = \left(P - 1, \frac{Q - 1}{P - 1} \right)$$

the (inhomogeneous) equation of \mathcal{C} takes the form $p^2 H(p, q) = 0$, where

$$H(p, q) = (2 + 3a^4 - 2(a^2 + 1)q^2 + q^4)p^2 + 4(2 - (1 + a^2)q - q^2 + q^3)p + 4(q^2 - 2q - a^2 + 2).$$

In other words, the curve \mathcal{C} is the set-theoretic sum of the (double) line $p = 0$ and the curve of degree 6, given by the equation $\mathcal{C}': H(p, q) = 0$. The equation for \mathcal{C}' can be rewritten as

$$\mathcal{C}' : W^2 = (a^2 - 1)q^4 - 2(a^2 - 1)q^3 - (2a^2 - 1)^2q^2 + 2a^2(3a^2 - 2)q + a^2(3a^4 - 6a^2 + 2),$$

where we put $W = \frac{1}{2}(q^4 - 2(a^2 + 1)q^2 + 3a^4 + 2)p + q^3 - q^2 - (a^2 + 1)q + 2$. In order to guarantee the existence of rational points on \mathcal{C}' (and hence on \mathcal{C}) we consider a quadratic base change $a = (t^2 + 1)/2t$. Then $a^2 - 1 = ((t^2 - 1)/2t)^2$ and thus the curve \mathcal{C}' contains a $\mathbb{Q}(t)$ -rational point at infinity. The birational model \mathcal{E}' of the curve \mathcal{C}' is given by the equation in short Weierstrass form $\mathcal{E}' : Y^2 = X^3 + AX + B$, where

$$A = -108(13t^{16} - 20t^{12} + 78t^8 - 20t^4 + 13),$$

$$B = 864(23t^{24} - 132t^{20} + 129t^{16} - 296t^{12} + 129t^8 - 132t^4 + 23).$$

The curve \mathcal{E}' contains the point of infinite order

$$Z = (12(2t^8 + 3t^6 - 2t^4 + 3t^2 + 2), 108t(t^2 + 1)(t^8 - 1)).$$

The point $2Z$ leads to a non-trivial curve lying on \mathcal{V} (the equations for this curve are too unwieldy to present explicitly here), and correspond to the following y, z satisfying the first three equations of our system:

$$\begin{aligned} y = & (t^{48} - 8t^{47} + 20t^{46} + 8t^{45} - 24t^{44} - 1528t^{43} + 6684t^{42} - 4872t^{41} - 69\,302t^{40} \\ & + 96\,040t^{39} + 771\,532t^{38} - 2\,467\,368t^{37} - 4\,047\,800t^{36} + 22\,047\,704t^{35} \\ & + 12\,635\,044t^{34} - 107\,433\,944t^{33} - 23\,948\,593t^{32} + 342\,788\,016t^{31} + 24\,622\,088t^{30} \\ & - 780\,080\,048t^{29} - 638\,000t^{28} + 1\,324\,015\,696t^{27} - 37\,969\,832t^{26} - 1\,716\,035\,152t^{25} \\ & + 57\,538\,508t^{24} + 1\,716\,035\,152t^{23} - 37\,969\,832t^{22} - 1\,324\,015\,696t^{21} - 638\,000t^{20} \\ & + 780\,080\,048t^{19} + 24\,622\,088t^{18} - 342\,788\,016t^{17} - 23\,948\,593t^{16} + 107\,433\,944t^{15} \\ & + 12\,635\,044t^{14} - 22\,047\,704t^{13} - 4\,047\,800t^{12} + 2\,467\,368t^{11} + 771\,532t^{10} - 96\,040t^9 \\ & - 69\,302t^8 + 4872t^7 + 6684t^6 + 1528t^5 - 24t^4 - 8t^3 + 20t^2 + 8t + 1)/(2t\Delta), \\ z = & (3t^{48} - 16t^{47} + 56t^{46} - 32t^{45} + 1096t^{44} - 5696t^{43} + 15\,928t^{42} + 11\,472t^{41} \\ & + 51\,710t^{40} - 551\,056t^{39} + 1\,282\,392t^{38} + 3\,181\,248t^{37} - 11\,188\,440t^{36} - 701\,152t^{35} \\ & + 39\,387\,992t^{34} - 55\,013\,168t^{33} - 75\,669\,523t^{32} + 272\,885\,472t^{31} + 75\,471\,984t^{30} \\ & - 744\,371\,648t^{29} + 210\,064t^{28} + 1\,377\,115\,648t^{27} - 116\,092\,816t^{26} - 1\,850\,031\,968t^{25} \\ & + 173\,321\,252t^{24} + 1\,850\,031\,968t^{23} - 116\,092\,816t^{22} - 1\,377\,115\,648t^{21} + 210\,064t^{20} \\ & + 744\,371\,648t^{19} + 75\,471\,984t^{18} - 272\,885\,472t^{17} - 75\,669\,523t^{16} + 55\,013\,168t^{15} \\ & + 39\,387\,992t^{14} + 701\,152t^{13} - 11\,188\,440t^{12} - 3\,181\,248t^{11} + 1\,282\,392t^{10} \\ & + 551\,056t^9 + 51\,710t^8 - 11\,472t^7 + 15\,928t^6 + 5696t^5 + 1096t^4 + 32t^3 + 56t^2 \\ & + 16t + 3)/((t^2 - 1)\Delta), \end{aligned}$$

Table 3Points in \mathbb{Q}^3 with five rational distances to vertices of the unit cube.

x	y	z	d_1	d_2	d_3	d_4	d_5
77/108	41/27	-28/27	71/36	67/36	49/36	43/36	95/36
83/125	-49/500	-14/75	389/300	349/300	209/300	119/300	409/300

where

$$\begin{aligned} \Delta = & 4(t-1)(t+1)(t^2+1)^2(t^8-4t^7+10t^6+12t^5-14t^4-12t^3+10t^2+4t+1) \times \\ & (t^{16}-4t^{14}+168t^{12}-492t^{10}+718t^8-492t^6+168t^4-4t^2+1) \times (t^{16}+4t^{14} \\ & -32t^{13}+232t^{12}+160t^{11}-756t^{10}-320t^9+1102t^8+320t^7-756t^6-160t^5 \\ & +232t^4+32t^3+4t^2+1). \end{aligned}$$

Computing the points mZ for $m = 3, 4, \dots$ and the corresponding points on \mathcal{C} , we get infinitely many rational curves lying on \mathcal{V} ; and the result follows. \square

We know (up to symmetry) precisely two points $(x, y, z) \in \mathbb{Q}^3$, with $x \neq \frac{1}{2}$, $x \neq y$, where the distances to the vertices $(0, 0, 0)$, $(0, 1, 0)$, $(1, 0, 0)$, $(1, 1, 0)$ of the unit square are rational, and where there is also rational distance to a fifth vertex $(0, 0, 1)$ of the unit cube. (See Table 3.)

References

- [1] T.G. Berry, Points at rational distance from the corners of a unit square, *Ann. Sc. Norm. Super. Pisa Cl. Sci.* 17 (4) (1990) 505–529.
- [2] T.G. Berry, Points at rational distance from the vertices of a triangle, *Acta Arith.* 62 (4) (1992) 391–398.
- [3] A. Bremner, On squares of squares. II, *Acta Arith.* 99 (3) (2001) 289–308.
- [4] A. Bremner, M. Ulas, Rational points in geometric progressions on certain hyperelliptic curves, *Publ. Math. Debrecen* 82 (3–4) (2013) 669–683.
- [5] H.C. Clemens, P.A. Griffiths, The intermediate Jacobian of the cubic threefold, *Ann. of Math.* (2) 95 (2) (1972) 281–356.
- [6] C.W. Dodge, Problem 966, *Math. Mag.* 49 (1976) 43;
C.W. Dodge, *Math. Mag.* 50 (1977) 166–167, partial solution;
C.W. Dodge, *Math. Mag.* 59 (1986) 52, comment.
- [7] R.K. Guy, *Unsolved Problems in Number Theory*, 3rd edition, Springer, 2004.
- [8] A. Hurwitz, Über ternäre diophantische Gleichungen dritten Grades, *Vierteljahrsschr. Nat.forsch. Ges. Zür.* 62 (1917) 207–229.
- [9] V.A. Iskovskih, Yu.I. Manin, Three-dimensional quartics and counterexamples to the Lüroth problem, *Mat. Sb., Novaya Seriya* 86 (1971) 140–166.
- [10] J. Kollár, Unirationality of cubic hypersurfaces, *J. Inst. Math. Jussieu* 1 (3) (2002) 467–476.
- [11] J. Kollár, K. Smith, A. Corti, *Rational and Nearly Rational Varieties*, Cambridge Stud. Adv. Math., vol. 92, Cambridge University Press, 2004.
- [12] A. Lenstra, Factoring multivariate polynomials over algebraic number fields, *SIAM J. Comput.* 16 (1987) 591–598.
- [13] Wieb Bosma, John Cannon, Catherine Playoust, The Magma algebra system. I. The user language, *J. Symbolic Comput.* 24 (3–4) (1997) 235–265.
- [14] Yu.I. Manin, *Cubic Forms: Algebra, Geometry, Arithmetic*, second edition, North-Holland Math. Lib., vol. 4, North-Holland Publishing Co., Amsterdam, 1986. Translated from Russian by M. Hazewinkel.

- [15] B. Naskręcki, Mordell–Weil ranks of families of elliptic curves parametrized by binary quadratic forms, submitted for publication.
- [16] J.H. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 1986.
- [17] Th. Skolem, *Diophantische Gleichungen*, Chelsea Publishing Company, New York, 1950.
- [18] M. Ulas, Rational points in arithmetic progressions on $y^2 = x^n + k$, *Canad. Math. Bull.* 55 (1) (2012) 193–207.