Bull. Aust. Math. Soc. **97** (2018), 26–32
doi:10.1017/S0004972717000697

ON PERFECT *K*-RATIONAL CUBOIDS

ANDREW BREMNER

(Received 30 May 2017; accepted 6 June 2017; first published online 4 October 2017)

Abstract

Let K be an algebraic number field. A cuboid is said to be K-rational if its edges and face diagonals lie in K. A K-rational cuboid is said to be *perfect* if its body diagonal lies in K. The existence of perfect $\mathbb{Q}$-rational cuboids is an unsolved problem. We prove here that there are infinitely many distinct cubic fields K such that a perfect K-rational cuboid exists; and that, for every integer $n \geq 2$, there is an algebraic number field K of degree n such that there exists a perfect K-rational cuboid.

2010 *Mathematics subject classification*: primary 11D41; secondary 11G05, 11G35, 14G25.

Keywords and phrases: rational cuboid, perfect cuboid, cubic field, Riemann–Roch.

1. Introduction

The problem of finding a rationally sided cuboid with face diagonals and body diagonal all being rational amounts to solving in nonzero rationals the following system of Diophantine equations:

$$\begin{aligned} x^2 + y^2 &= p^2, \\ y^2 + z^2 &= q^2, \\ z^2 + x^2 &= r^2, \\ x^2 + y^2 + z^2 &= s^2. \end{aligned} \tag{1.1}$$

This notorious unsolved problem has been studied extensively in the literature; see Guy [2], Section D18, for a comprehensive list of references. The aim of this note is to prove that for every integer $n \geq 2$, there exists an algebraic number field of degree n in which the system (1.1) has a solution. The case $n = 2$ is of course quite trivial. It is straightforward to find a rational solution of the first three equations in (1.1), for example $(x, y, z;\ p, q, r) = (44, 117, 240;\ 125, 267, 244)$, and then we have a solution of the equations (1.1) with $s = 5\sqrt{2929}$. This argument is easily generalised to show that for every even integer n, there is a number field of degree n in which (1.1) has solutions; see Section 2. Accordingly, the interesting case is the existence of number fields K of odd degree in which (1.1) has solutions. In Section 3 we shall find explicit solutions in extension fields of degrees 3 and 5. In Section 4 we shall show that there exist infinitely many distinct cubic fields in which the system (1.1) has solutions; and also that there are number fields of every odd degree greater than or equal 3 in which the equations (1.1) have solutions.

2. The case n even

Saunderson, Lucasian Professor of Mathematics at Cambridge, and blind from infancy, was essentially aware (see [4]) of the parametrisation

$$\begin{aligned}(x, y, z;\ p, q, r) = (&2t(t^2-3)(3t^2-1),\ 8t(t^4-1),\ (t^2-1)(t^2-4t+1)(t^2+4t+1);\\ &2t(5t^4-6t^2+5),\ (t^2-1)(t^4+18t^2+1),\ (t^2+1)^3)\end{aligned} \tag{2.1}$$

of the first three equations in (1.1). Then the fourth equation is satisfied precisely when

$$t^8+68t^6-122t^4+68t^2+1=\square. \tag{2.2}$$

THEOREM 2.1. *Let $n = 2m$ be an even integer. There exists a number field K of degree n such that the equations (1.1) have a solution in K.*

PROOF. Let K_0 be any number field of degree m. The polynomial

$$f(t) = t^8+68t^6-22t^4+68t^2+1$$

has only simple roots, so equation (2.2) defines a curve of genus 3 and, by Faltings' theorem, has only finitely many rational points. Choose $t_0 \in K_0$ such that $K_0 = \mathbb{Q}(t_0)$ and $f(t_0) \notin K_0^2$. Then the parametrisation in (2.1) shows that

$$(x(t_0), y(t_0), z(t_0); p(t_0), q(t_0), r(t_0), \sqrt{f(t_0)})$$

is a solution of the equations (1.1) in an extension of K_0 of degree 2 and hence in a number field of degree $2m = n$. □

3. The case n odd

Let K be an algebraic number field. We suppose that $x, y, z, p, q, r, s \in K$ satisfy the equations (1.1). The first three equations in (1.1) may be parametrised by

$$\begin{aligned} x &= (a^2-b^2)\lambda, & y &= 2ab\lambda, & p &= (a^2+b^2)\lambda,\\ y &= (c^2-d^2)\mu, & z &= 2cd\mu, & q &= (c^2+d^2)\mu,\\ z &= 2ef\nu, & x &= (e^2-f^2)\nu, & r &= (e^2+f^2)\nu, \end{aligned} \tag{3.1}$$

with $\lambda, \mu, \nu; a, b; c, d; e, f \in K$. Then

$$2abcd(e^2-f^2) = (a^2-b^2)(c^2-d^2)ef \quad (= (xyz/(2\lambda\mu\nu)))$$

and

$$(c^2+d^2)^2\mu^2+(e^2-f^2)^2\nu^2 = s^2.$$

https://doi.org/10.1017/S0004972717000697 Published online by Cambridge University Press

Taking the discriminant with respect to a/b of the first equation, and using $\nu/\mu = cd/ef$ in the second, gives the system

$$e^4 + \Big(\frac{c^2}{d^2} - 4 + \frac{d^2}{c^2}\Big)e^2 f^2 + f^4 = \square, \tag{3.2}$$

$$\Big(e^2 + \frac{c^2}{d^2} f^2\Big)\Big(e^2 + \frac{d^2}{c^2} f^2\Big) = \square. \tag{3.3}$$

We can find solutions of (3.2) and (3.3) over cubic number fields $\mathbb{Q}(t)$ by a direct search over minimum polynomials of t with small coefficients, then letting c/d take values quadratic in t with small coefficients and searching for points on the intersection of the two quartics. The first solution that we found in this way is the following example.

Example 3.1. Let $K = \mathbb{Q}(t)$ and $t^3 - 11t + 12 = 0$. Then

$$(a, b) = (t^2 - 5t + 5, t^2 + t - 3), \quad (c, d) = (t + 2, 1), \quad (e, f) = (2t^2 + 4t - 13, 1)$$

leads to the following point on (1.1):

$$(x, y, z;\ p, q, r, s) = (4t, t^2 + 3t - 9, t^2 - 4;\ 3t^2 + 3t - 15, t^2 + 4t - 11, t^2 + 4, t^2 + 5).$$

The system (3.2) and (3.3) may also be written as the intersection of three quadrics in the form

$$\begin{aligned} E^2 + \Big(\frac{c^2}{d^2} - 4 + \frac{d^2}{c^2}\Big)EF + F^2 &= s_1^2, \\ E^2 + \Big(\frac{c^2}{d^2} + \frac{d^2}{c^2}\Big)EF + F^2 &= s_2^2, \\ EF &= s_3^2, \end{aligned} \tag{3.4}$$

with $(E, F) = (e^2, f^2)$; and, as such, represents a curve of genus 5 over $\mathbb{Q}(c/d)$. There are three obvious coverings of curves of genus 1 obtained by 'forgetting' s_1, s_2, s_3 in turn; and an obvious covering of a genus-2 curve:

$$x\Big(x^2 + \Big(\frac{c^2}{d^2} - 4 + \frac{d^2}{c^2}\Big)x + 1\Big)\Big(x^2 + \Big(\frac{c^2}{d^2} + \frac{d^2}{c^2}\Big)x + 1\Big) = \square,$$

with $x = E/F$. This latter allows discovery of points over degree-5 number fields. For example, set $(c, d) = (2, 1)$ and define a quintic number field $K(t)$ by setting t to have minimum polynomial

$$x(x^2 + \tfrac{1}{4}x + 1)(x^2 + \tfrac{17}{4}x + 1) = 9(x^2 + x + 8)^2,$$

the right-hand term being chosen so that t, $t^2 + \frac{1}{4}t + 1$ and $t^2 + \frac{17}{4}t + 1$ are each squares in K. This gives the following point on (3.4):

$$\begin{aligned} (E, F, s_1, s_2, s_3) = (t, 1, &(-496t^4 + 2296t^3 + 13905t^2 + 46876t + 78464)/30080, \\ &(-16t^4 + 8t^3 + 655t^2 + 1828t + 5760)/1152, \\ &(-16t^4 - 120t^3 + 1807t^2 + 3756t + 17280)/6768). \end{aligned}$$

https://doi.org/10.1017/S0004972717000697 Published online by Cambridge University Press

Correspondingly, this simplifies to the following solution of (1.1):

$$\begin{aligned}&(x, y, z;\ p, q, r, s)\\ =\ &(17\tau^4 + 10\tau^3 + \tau^2 - 220\tau - 546,\ 648,\ 864;\ 5\tau^4 - 14\tau^3 + 13\tau^2 - 340\tau - 402,\\ &1080,\ 7\tau^4 + 38\tau^3 - 25\tau^2 + 28\tau - 606,\ 11\tau^4 - 2\tau^3 + 115\tau^2 - 172\tau - 366),\end{aligned} \tag{3.5}$$

where $\tau^5 - 2\tau^4 + 9\tau^3 - 40\tau^2 + 38\tau - 168 = 0$.

This point taken with its conjugates defines an effective rational divisor D_0 of degree 5 on the genus-5 curve (3.4). By the Riemann–Roch theorem, a divisor of degree at least 9 on a genus-5 curve is linearly equivalent to an effective divisor, so denoting by Π a plane section on the curve, a divisor $n\Pi - mD_0$ with $8n - 5m \geq 9$ is linearly equivalent to an effective divisor. In this way we can construct effective divisors on the curve of every odd degree at least 9. (We have constructed effective divisors of degrees 3 and 5 in Examples 3.1 and (3.5), respectively. For a degree-7 example, see Example 4.5.)

4. Infinitely many cubic fields

We can find infinitely many cubic fields in which the system of equations (1.1) has solutions, as follows.

The parametrisation (2.1) corresponds in (3.1) to

$$\begin{aligned}(\lambda, \mu, \nu) &= (4t, t^2 - 1, 1),\\ (a, b) &= (2(t^2 - 1), t^2 + 1),\\ (c, d) &= (t^2 + 4t + 1, t^2 - 4t + 1),\\ (e, f) &= ((t - 1)(t^2 + 4t + 1), (t + 1)(t^2 - 4t + 1)).\end{aligned}$$

Then

$$e^4 + \left(\frac{c^2}{d^2} - 4 + \frac{d^2}{c^2}\right)e^2 f^2 + f^4 = 16t^2(5t^4 - 6t^2 + 5)^2,$$

and it remains to make square

$$\left(e^2 + \frac{c^2}{d^2} f^2\right)\left(e^2 + \frac{d^2}{c^2} f^2\right) = 4(t^2 + 1)^2(t^8 + 68t^6 - 122t^4 + 68t^2 + 1).$$

Equivalently, we need points on the hyperelliptic curve

$$C:\ Y^2 = X^8 + 68X^6 - 122X^4 + 68X^2 + 1 \tag{4.1}$$

which lie in a cubic number field $\mathbb{Q}(t)$. The curve C, as in (2.2), is of genus 3.

First, we find all the points on (4.1) that are defined over $\mathbb{Q}$. This enumeration is implicit in existing results, which prove that the Euler parametrisation (2.1) cannot result in a rational solution to the cuboid problem; see, for example, Spohn [5], though the result follows immediately from Pocklington [3]. But we state the theorem in the form in which we wish to use it, giving an alternative and simple proof.

https://doi.org/10.1017/S0004972717000697 Published online by Cambridge University Press

THEOREM 4.1. *The rational points on the curve* (4.1) *are precisely the two points at infinity* $(1, 1, 0)$, $(-1, 1, 0)$ *and the finite points* $(\pm x, \pm y) = (0, 1)$, $(1, 4)$.

PROOF. The curve (4.1) has the involution

$$\phi(X, Y) = \left(\frac{X+1}{X-1}, \frac{4Y}{(X-1)^4}\right)$$

and the corresponding quotient curve

$$\widetilde{C}: \ y^2 = x^3 - 3x^2 + x$$

is of rank 0. The mapping is given by

$$(x, y) = \left(\frac{32X^2(X^2-1)^2}{X^8 + 36X^6 - 58X^4 + 36X^2 + 1 - (X^2+1)^2 Y}, \right. \\ \left. \frac{8X(X^2-1)(X^2-2X-1)(X^2+2X-1)}{X^8 + 36X^6 - 58X^4 + 36X^2 + 1 - (X^2+1)^2 Y}\right).$$

There are precisely two rational points on $\widetilde{C}$, namely $(0, 1, 0)$ at infinity and the finite point $(0, 0)$ of order 2. It follows that a rational point (X, Y) on (4.1) must satisfy

$$X^8 + 36X^6 - 58X^4 + 36X^2 + 1 - (1 + X^2)^2 Y = 0 \text{ or } X(X^2 - 1) = 0.$$

The former also implies that $X(X^2 - 1) = 0$, so that a complete listing of points on (4.1) is given by the two points $(1, 1, 0), (1, -1, 0)$ at infinity and the finite points $(\pm X, \pm Y) = (0, 1), (1, 4)$. □

We now seek identities of the following form:

$$x^8 + 68x^6 - 122x^4 + 68x^2 + 1 - (c_0 g x^2 + c_1 x - c_0)^2 \\ = (x^3 + gx^2 + hx - 1)(x^5 - gx^4 + c_2 x^3 - c_3 x^2 + c_4 x + (c_0^2 - 1)), \qquad (4.2)$$

where we shall demand irreducibility of $x^3 + gx^2 + hx - 1$. Equating coefficients of powers of x in (4.2),

$$c_2 = g^2 + 68 - h,$$
$$c_3 = g^3 + 68g - 1 - 2gh,$$
$$c_4 = g^4 + 68g^2 - 2g - 122 - (3g^2 + 68)h + h^2 - g^2 c_0^2,$$

with

$$(1 + gh)(g^2 + 69 - 2h - c_0^2) = 0.$$

If $1 + gh = 0$, then $x^3 + gx^2 + hx - 1 = (x + g)(x^2 + h)$, violating irreducibility, so necessarily $c_0^2 = g^2 + 69 - 2h$, giving

$$c_1^2 = 2g + 69 + (g^2 + 2g + 122)h + (g^2 + 68)h^2 - h^3,$$
$$2c_0 c_1 = g^2 + 2g + 122 + 2(g^2 + 68)h - 3h^2.$$

https://doi.org/10.1017/S0004972717000697 Published online by Cambridge University Press

Eliminating c_1 gives

$$D:\ (g^2-h^2)^2-4(g-h)(g+h)^2-4(7g^2-2gh+7h^2)-64(g-h)-4160=0. \quad (4.3)$$

Equation (4.3) represents a curve of genus 1, with rational point $(1, 1, 0)$ at infinity. So, it is an elliptic curve, with cubic model

$$E:\ y^2=x^3+x^2-x+15,$$

of rank 1 with generator $P=(-1,4)$. Birational maps $D \leftrightarrow E$ are given by

$$\begin{aligned}(x,y)=(&\tfrac{1}{128}(-g^3+6g^2+16g+160+(-g^2+12g-16)h+(g+6)h^2+h^3),\\ &\tfrac{1}{256}(g^3-6g^2+240g-2080-(g^3-7g^2-4g-304)h\\ &-(g^2-11g+22)h^2+(g+5)h^3+h^4))\end{aligned}$$

and

$$(g,h)=\Big(\frac{-(x+3)(x+15)-2y(x-1)}{(x-1)(x+3)},\ \frac{(x+3)(x+15)-2y(x-1)}{(x-1)(x+3)}\Big).$$

Accordingly, the infinitely many pullbacks to D of the points mP on E, for $m\in\mathbb{Z}$, result in infinitely many identities of type (4.2). If in such an identity x^3+gx^2+hx-1 is reducible, then it has a finite rational root ρ which is certainly nonzero. But (4.2) now implies that ρ is the X-coordinate of a finite rational point on (4.1), so, by Theorem 4.1, we have $\rho=\pm 1$. This implies that either $h=-g$ or $h=g-2$; in each case (g,h) being a point of D in (4.3) can only occur for irrational g. Hence, the cubics x^3+gx^2+hx-1 are guaranteed to be irreducible. Identity (4.2) now shows that $t^8+68t^6-122t^4+68t^2+1\in\mathbb{Q}(t)^2$, where $t^3+gt^2+ht-1=0$.

Example 4.2. The generator $P(-1,4)$ corresponds to $(g,h)=(3,-11)$, with cubic field $\mathbb{Q}(\tau)$, $\tau^3+3\tau^2-11\tau-1=0$. The corresponding point of (1.1) using (2.1) simplifies to

$$\begin{aligned}&x:y:z:p:q:r:s\\ &=\tau^2-8\tau+13:5\tau^2-2\tau-19:-3\tau^2-4\tau+23:\\ &\quad 2(\tau^2-7\tau+11):2(3\tau^2-15):2(6\tau-13):-7\tau^2+33. \qquad (4.4)\end{aligned}$$

Theorem 4.3. *There exist infinitely many distinct cubic fields K in which the system (1.1) has solutions.*

Proof. Two isomorphic cubic fields will have discriminants differing by a perfect square. The discriminant of X^3+gX^2+hX-1, with g,h as above, is equal to $16F(x)/((x-1)^4(x+3)^2)$, where

$$F(x)=x^8-19x^7-44x^6-5x^5+272x^4-2621x^3+1168x^2+21237x+45547$$

is irreducible. Inductively, suppose that we have constructed as above $k\geq 1$ distinct cubic fields in which system (1.1) has points. Let the respective discriminants be Δ_i, $i=1,\ldots,k$. The curves $F(x)=\Delta_i y^2$, for $i=1,\ldots,k$, are each of genus 3 and so, by Faltings' theorem, the set S_k of $x\in\mathbb{Q}$ such that $F(x)=\Delta_i y^2$, for some $i=1,\ldots,k$, is finite. Now choose $m\in Z$ so that $x_m\notin S_k$, where $(x_m,y_m)=mP$; then (x_m,y_m) pulls back to (g,h), corresponding to a cubic field distinct from the previous k. □

https://doi.org/10.1017/S0004972717000697 Published online by Cambridge University Press

Theorem 4.4. *Let $n \geq 3$ be an odd integer. Then there exists a number field K of degree n in which the system (1.1) has solutions.*

Proof. We have already discovered a solution of (1.1) in a cubic number field, so we can henceforth suppose that $n \geq 5$. The cubic point of (1.1) in (4.4) corresponds to the cubic point $(\tau, 30\tau^2 - 96\tau - 10)$ on (4.1) and so determines on (4.1) an effective divisor D_0 of degree 3. The curve (4.1) is of genus 3, so the Riemann–Roch theorem implies that a divisor in (4.1) of degree at least 5 is linearly equivalent to an effective divisor. We can certainly find positive integers m, k such that $8m - 3k = n$. Denoting by Π a (weighted) plane section on the curve, then the divisor $m\Pi - kD_0$ has degree n and so is linearly equivalent to an effective divisor. Such a divisor depends on $n - 3$ independent parameters; in general therefore such a divisor should be irreducible (the Hilbert irreducibility theorem guarantees that there is a specialisation of the parameters which will give an irreducible divisor; see, for example, Coray [1, Section 2]). Such an irreducible divisor pulls back via the parametrisation (2.1) to a point on (1.1) defined over an extension field of degree n. □

As illustration of the technique in Theorem 4.4, we find a solution of (1.1) in an extension field of degree 7.

Example 4.5. Since $2\Pi - 3D_0$ has degree 7, we construct a curve such as

$$\begin{aligned} Y^2 &+ (-9X^3 - 39X^2 + 91X - 27)Y \\ &= 2X^8 + 41X^7 + 427X^6 + 979X^5 - 623X^4 + 27X^3 - 487X^2 + 241X - 15, \end{aligned}$$

having intersection with (4.1) containing $3D_0$ (there are four degrees of freedom, so it is not difficult either to construct such a curve or to ensure that the residual divisor of degree 7 is irreducible; rather, the difficulty is in trying to ensure that the coefficients do not become unduly large). The residual intersection on (4.1) is then a divisor of degree 7, defined in this instance by

$$X^7 + 49X^6 + 347X^5 + 767X^4 + 375X^3 + 87X^2 - 1459X + 473 = 0.$$

References

[1] D. F. Coray, ‘Algebraic points on cubic hypersurfaces’, *Acta Arith.* **30** (1976), 267–296.

[2] R. K. Guy, *Unsolved Problems in Number Theory*, 3rd edn (Springer, New York, 2004).

[3] H. C. Pocklington, ‘Some Diophantine impossibilities’, *Proc. Cambridge Philos. Soc.* **17** (1914), 110–118.

[4] N. Saunderson, *The Elements of Algebra*, Book 6 (Cambridge University Press, Cambridge, 1740), 429–431.

[5] W. G. Spohn, ‘On the integral cuboid’, *Amer. Math. Monthly* **79** (1972), 57–59.

ANDREW BREMNER, School of Mathematical and Statistical Sciences,
Arizona State University, Tempe AZ 85287-1804, USA
e-mail: bremner@asu.edu

https://doi.org/10.1017/S0004972717000697 Published online by Cambridge University Press