The perfect cuboid is one step closer to non-existence

Ralph H. Buchholz

July 2, 2014

Abstract

It is known that the non-existence of a perfect cuboid (a rectangular prism with all sides and diagonals rational) has been reduced to two conjectures, the second of which asks for a proof of non-existence of rational zeros of a particular function. We use covering curves and the technique of Chabauty to provide this proof.

Keywords : Euler brick, rational cuboid, hyperelliptic curve, Chabauty method.

Introduction

A **perfect parallelepiped** is the name used to denote a parallelepiped with rational sides, rational face diagonals and rational body diagonals. In their paper, [4], Sokolowsky et al. make a very interesting study of their discovery of an infinite family of perfect parallelepipeds with at least two non-parallel rectangular faces. In the end they make two conjectures which relate their work to the problem of the existence of a perfect cuboid.

Sokolowsky et al. parameterize the three sides of an infinite family of perfect parallelepipeds by specifying three edge vectors, $\vec{u}, \vec{v}, \vec{w}$, in terms of two rational parameters p and m. In particular, they show that

$$\begin{cases} \vec{u} &= \big(2(p^2-1), 0, 0\big) \\ \vec{v} &= (0, 4p, 0) \\ \vec{w} &= \left(0, j(p,m), \frac{A(p,m)\sqrt{h(p,m)}}{2m(m^2-1)(m^4-6m^2+1)}\right) \end{cases} \tag{1}$$

where $A(p,m)$, $h(p,m)$ and $j(p,m)$ are particular rational functions in p and m. We do not concern ourselves with $A(p,m)$ and $h(p,m)$ any further in this note.

Conjecture 1 *(Sokolowsky et al.) Up to scaling, every rational parallelepiped with at least two non-parallel rectangular faces may be found using suitable parameters in equation 1.*

Conjecture 2 *(Sokolowsky et al.) There are no rational choices of p and m for which $j(p,m) = 0$.*

We prove the second of these conjectures.

The curves and their covers

The numerator of the function $j(p,m)$, described in conjecture 2, conveniently factorises providing us with the following pleasing form,

$$j(p,m) = \frac{j_1(p,m)j_2(p,m)}{k(p,m)}$$

where

$$\begin{aligned} j_1(p,m) &= p^4(m^2(m^2-1)^2) - p^2(m^8+2m^6+14m^4+2m^2-1) + m^2(m^2-1)^2, \\ j_2(p,m) &= p^4(m^2(m^2-1)^2) + p^2(m^8-6m^6-6m^4-6m^2+1) + m^2(m^2-1)^2, \\ k(p,m) &= 2m(-1+m^2)(1-5m^2-5m^4+m^6)^2p^3. \end{aligned}$$

Since conjecture 2 asks for zeros of $j(p,m)$ it is sufficient to consider the zeros of the two factors in the numerator separately.

0.1 The first curve

We first look at the curve defined by j_1, namely,

$$C_1 : p^4(m^2(m^2-1)^2) - p^2(m^8+2m^6+14m^4+2m^2-1) + m^2(m^2-1)^2 = 0.$$

With the help of *Magma* we find that this is a curve of genus 9. Thus we can immediately infer, by Faltings' theorem, that there are only finitely many rational points on this curve. As is well known, Faltings' proof of the Mordell conjecture is not effective—so we must look elsewhere.

Notice that all the exponents are even so we can depress the squares via the map $\sigma : C_1 \to D_1$ which sends $p^2 \mapsto p$ and $m^2 \mapsto m$, giving us a new curve,

$$D_1 : p^2(m(m-1)^2) - p(m^4+2m^3+14m^2+2m-1) + m(m-1)^2 = 0$$

in which we (ab)use the same variables. Any rational point on C_1 leads to a rational point on D_1 and so finding all the rational points on C_1 can be achieved by computing all the rational points on D_1 and then constructing their preimages on C_1. Since we want to find rational points on D_1 it must be the case that the discriminant of the curve, considered as a quadratic in p, is a perfect square. We find that the squarefree part of the discriminant is a sextic in m and so D_1 is a hyperelliptic curve of genus two. In fact, a hyperelliptic model of D_1 is given by

$$H_1 : y^2 = x^6 - 5x^4 + 7x^2 - 2$$

where the transformation, $\phi_1 : D_1 \mapsto H_1$, is given by $\phi_1(p,m) = [x,y] = [X/Z, Y/Z^3]$ and

$$\begin{aligned} X &= \frac{1}{2}(m+1)^2 \\ Y &= \frac{(m+1)^2}{8}[2pm(m-1)^2 - (m^4-2m^3-14m^2-2m+1)] \\ Z &= -\frac{1}{2}(m^2-1). \end{aligned}$$

The Jacobian of the hyperelliptic curve is neatly resolved by Magma to be of rank one and its torsion subgroup is isomorphic to a group of order twelve. In particular, we have

$$J_{H_1}(\mathbb{Q}) \cong \frac{\mathbb{Z}}{2\mathbb{Z}} \oplus \frac{\mathbb{Z}}{6\mathbb{Z}} \oplus \mathbb{Z}.$$

When we apply Chabauty's technique ([2]) to the infinite order generator denoted by the divisor

$$\mathfrak{A}_1 :=< (1:-1:0), (-1:-1:1) >$$

we find that all the rational points on H_1 are given by

$$H_1(\mathbb{Q}) = \{(1:1:1), (1:-1:0), (-1:1:1), (1:1:0), (1:-1:1), (-1:-1:1)\}$$

in projective coordinates.

We now need to find the preimages of these points with respect to the map ϕ_1. Notice that all the rational points have a non-zero first coordinate—hence we can divide by that and produce a finite result when necessary. Thus, given the rational point $(a_i : b_i : c_i) \in H_1(\mathbb{Q})$ we solve the equations

$$\frac{Y(p,m)}{X(p,m)^3} = \frac{b_i}{a_i^3} \quad \text{and} \quad \frac{Z(p,m)}{X(p,m)} = \frac{c_i}{a_i}.$$

To solve these, we simply run a Gröbner basis computation on the equivalent equations

$$Y(p,m) - \frac{b_i}{a_i^3} X(p,m)^3 = 0 \quad \text{and} \quad Z(p,m) - \frac{c_i}{a_i} X(p,m) = 0.$$

The only surviving points on D_1 are

$$D_1(\text{preimages}) = \{(1,-1), (0,1), (0,0)\}.$$

We also need to check that we did not lose any rational points, in passing from D_1 to H_1, via singularities of the map ϕ_1. These are given by solutions to the equations $[X, Y, Z] = [0, 0, 0]$. Another Gröbner basis computation to find these points reveals no new rational points on D_1. Thus we have

$$D_1(\mathbb{Q}) = \{(1,-1), (0,1), (0,0)\}.$$

Finally, we need to find the preimages of these three points with respect to the squaring map, σ, and here we observe that only the latter two pass through to give us

$$C_1(\mathbb{Q}) = \{(0,-1), (0,1), (0,0)\}.$$

0.2 The second curve

We summarise the same technique applied to the curve defined by j_2, namely,

$$C_2 : p^4(m^2(m^2-1)^2) + p^2(m^8 - 6m^6 - 6m^4 - 6m^2 + 1) + m^2(m^2-1)^2 = 0.$$

When we use the map σ to depress the squares of this genus 9 curve we get the genus 2 curve defined by

$$D_2 : p^2(m(m-1)^2) + p(m^4 - 6m^3 - 6m^2 - 6m + 1) + m(m-1)^2 = 0.$$

A hyperelliptic model of D_2 is given by

$$H_2 : y^2 = x^6 - 3x^4 + x^2 + 2$$

where the transformation, $\phi_2 : D_2 \mapsto H_2$, is given by $\phi_2(p, m) = [x, y] = [X/Z, Y/Z^3]$ and

$$\begin{aligned} X &= \frac{1}{2}(m+1)^2 \\ Y &= \frac{(m+1)^2}{8}[2pm(m-1)^2 + (m^4 - 6m^3 - 6m^2 - 6m + 1)] \\ Z &= -\frac{1}{2}(m^2 - 1). \end{aligned}$$

The Jacobian of the hyperelliptic curve has rank one and is given by

$$J_{H_2}(\mathbb{Q}) \cong \frac{\mathbb{Z}}{8\mathbb{Z}} \oplus \mathbb{Z}.$$

An application of Chabauty (to $\mathfrak{A}_2 :=< (-1 : -1 : 1), (-1 : 1 : 1) >$) completely determines the rational points on H_2, namely,

$$H_2(\mathbb{Q}) = \{(1 : 1 : 1), (1 : -1 : 0), (-1 : 1 : 1), (1 : 1 : 0), (1 : -1 : 1), (-1 : -1 : 1)\}.$$

Finding the preimages and possible singularities of the maps ϕ_2 and σ give us all the rational points on C_2 as

$$C_2(\mathbb{Q}) = \{(0, -1), (0, 1), (0, 0)\}.$$

Thus we find that the only possible way that $j(p, m) = 0$ can be solved for rational values of p and m are when

$$(p, m) \in \{(0, -1), (0, 1), (0, 0)\}.$$

Since these values are poles of the rational function they do not lead to affine zeros. Thus we have proved the following.

Theorem 1 *There are no rational choices of p and m for which $j(p, m) = 0$.*

References

[1] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system I : The user language*, Journal of Symbolic Computation, v. 24, pages 235-269, 1997.

[2] J. W. S. Cassels and E. V. Flynn, *Prolegomena to a Middlebrow Arithmetic of Curves of Genus 2*, LMS Lecture Note Series 230, Cambridge University Press, 1996.

[3] Richard Guy, *Unsolved Problems in Number Theory*, Springer-Verlag, 1981.

[4] Benjamin D. Sokolowsky, Amy G. VanHooft, Rachel M. Volkert, Clifford A. Reiter, *An infinite family of Perfect Parallelepipeds*, (preprint), 2014.