Quadratic Forms and Bhargava's Cubes

September 2, 2020

1 Introduction

This report is aimed to present what we think are the more fertile directions for the improvement of an algorithm that solves a problem involving composition of integral binary quadratic forms. Section 1 contains the basic definitions and results concerning quadratic forms necessary to state the problem. In Section 2 we discuss the notion of Bhargava cubes, closely related with the composition of integral binary quadratic forms and in which terms the problem is stated. Section 3 deals with the actual introduction of the problem and reviews an algorithm that solves it and is the best known to us. Finally, in Section 4, we develop our take on the problem as well as on some aspects that we regard as prone to yield to an algorithm that more efficiently solves the problem we are interested in.

2 Quadratic forms

2.1 Preliminaries

Definition A *quadratic form* is a polynomial with coefficients in some field K where all terms have degree two. That is, considering $n > 0$, $A_{ij} \in K$, with $1 \leq i, j \leq n$ and $\mathbf{x} = (x_1, x_2, ..., x_n) \in K^n$, the quadratic form determined by A_{ij}, evaluated in $\mathbf{x}$, is given by

$$Q(\mathbf{x}) = \sum_{i,j=1}^{n} A_{ij} x_i x_j.$$

Example 2.1.

$$\begin{aligned} Q(x, y) &= Ax^2 + By^2 \\ Q(y) &= By^2 \\ Q(x, y) &= Ax^2 + Bxy + Cy^2 \\ Q(x, y, z) &= Ax^2 + By^2 + Cz^z + Dxy + Exz + Fyz \end{aligned}$$

Remark Note that the coefficients (A_{ij}), $i, j = 1, ..., n$ completely determine the quadratic form.

This is a general definition, we are interested in what is refered to as a *binary quadratic form*, where $n = 2$ and consequently is a polynomial described by the expression $Ax^2+Bxy+Cy^2$, that we identify with the triplet (A, B, C). These quadratic form can be represented as the following matrix product

$$\begin{pmatrix} x \\ y \end{pmatrix}^T \begin{pmatrix} A & \frac{B}{2} \\ \frac{B}{2} & C \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

Hence, we can associate with every binary quadratic form a unique symmetric matrix in the aforementioned way.

Definition The *discriminant* of a quadratic form represented by the triplet (A, B, C) is the number $D = \mathrm{Disc}(A, B, C) = B^2 - 4AC$.

Remark Observe that if M is the symmetric matrix associated with (A, B, C), then $\mathrm{Disc}(A, B, C) = -4 \det M$.

Definition We say that a binary quadratic form is *primitive* if $\gcd(A, B, C) = 1$.

2.2 Gauss composition

An important problem in this theory is to find which integers can be represented as a quadratic form with integer coefficients. One of the first important results about it was given by Fermat in 1640.

Theorem 2.2. *An odd prime number p can be represented as the sum of two squares (there exist $x, y \in \mathbb{Z}$ such that $p = x^2 + y^2$), if and only if $p \equiv 1(mod 4)$.*

Since every positive integer can be expressed as a product of primes, and we already know which primes can be represented by an integral binary quadratic form, seems a good idea to know about the product of binary quadratic forms. In this spirit, an important result is that if two numbers are represented as the sum of two squares, then their product is too. This is a consequence of the identity $(u^2 + v^2)(r^2 + s^2) = (ur + vs)^2 + (us - vr)^2$.

This can be generalized to any two binary quadratic forms with the same discriminant.

Theorem 2.3 (Gauss composition)**.** *Given two binary quadratic forms $Q_1(u, v)$ and $Q_2(r, s)$ of the same discriminant, there exists a form $Q_3(x, y)$ of the same discriminant such that*

$$Q_1(u, v)Q_2(r, s) = Q_3(x, y),$$

where x and y are quadratic polynomials in u, v, r, s.

Gauss called Q_3 the *composition* of Q_1 and Q_2 and proved the previous theorem in 1804, in his famous book *Disquisitiones Arithmeticae*. We will use $Q_1 \cdot Q_2$ to denote the composition of Q_1 and Q_2.

The changes of variable involved in the prior theorem motivate the following definition.

Definition Let $Q_1(x,y) = A_1x^2 + B_1xy + C_1y^2$ and $Q_2(x,y) = A_2x^2 + B_2xy + C_2y^2$ be integral binary quadratic forms. We say that Q_1 and Q_2 are equivalent, denoted by $Q_1 \equiv Q_2$, if there exist $r, s, t, u \in \mathbb{Z}$ such that $ru - st = 1$ and $Q_1(rx + sy, tx + uy) = Q_2(x,y)$.

It can be proved that this equivalence is compatible with the composition of quadratic forms. That is, if $Q_1 \sim Q_2$ and $Q_1' \sim Q_2'$, then $Q_1 \cdot Q_1' \sim Q_2 \cdot Q_2'$

A quick calculation shows that Q_1 and Q_2 are equivalent if and only if

$$\begin{aligned} Q_1(x,y) &= \begin{pmatrix} x \\ y \end{pmatrix}^T \begin{pmatrix} r & s \\ t & u \end{pmatrix}^T \begin{pmatrix} A_1 & \frac{B_1}{2} \\ \frac{B_1}{2} & C_1 \end{pmatrix} \begin{pmatrix} r & s \\ t & u \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \\ &= \begin{pmatrix} x \\ y \end{pmatrix}^T \begin{pmatrix} A_2 & \frac{B_2}{2} \\ \frac{B_2}{2} & C_2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = Q_2(x,y) \end{aligned} \tag{1}$$

As $\mathrm{Disc}(A_i, B_i, C_i) = -4 \det \begin{pmatrix} A_i & \frac{B_i}{2} \\ \frac{B_i}{2} & C_i \end{pmatrix}$, for $i \in \{1,2\}$, the former equation implies $\mathrm{Disc}(A_1, B_1, C_1) = \mathrm{Disc}(A_2, B_2, C_2)$.

The set

$$SL_2(\mathbb{Z}) = \left\{ \begin{pmatrix} r & s \\ t & u \end{pmatrix} : r, s, t, u \in \mathbb{Z} \text{ and } ru - st = 1 \right\}$$

forms a group under matrix multiplication and it is called the *Special linear group of degree 2 over the integers* and will be referred to throughout the present work simply as the *Special linear group*.

Note that Equation (1) also provides the definition of an action of $SL_2(\mathbb{Z})$ on the set of integral binary quadratic forms. Namely, if $Q = (A, B, C)$ is a quadratic form and $M = \begin{pmatrix} r & s \\ t & u \end{pmatrix} \in SL_2(\mathbb{Z})$, we define

$$Q^M = (r^2A + rtB + t^2C, 2rsA + (ru + ts)B + 2tuC, s^2A + usB + u^2C) \tag{2}$$

It is immediate that two quadratic forms are equivalent if and only if they are in the same orbit under this action. We denote by $[A, B, C]$ the orbit of (A, B, C) under the action of $SL_2(\mathbb{Z})$, and it follows from the paragraph after the definition of equivalence that $[A_1, B_1, C_1] \cdot [A_2, B_2, C_2] = [(A_1, B_1, C_1) \cdot (A_2, B_2, C_2)]$ is well defined.

With the help of the matrices $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \in SL_2(\mathbb{Z})$, with $n \in \mathbb{Z}$, it is not difficult to device an algorithm that shows that every binary quadratic form of negative discriminant is equivalent to a binary quadratic form, (A, B, C), where $|B| \leq |A| \leq |C|$. Observe that the absolute values of the coefficients of (A, B, C) are as small as possible. For this reason, a quadratic form that fulfills the previous inequality is called *reduced*. See [1] for more details.

2.3 Dirichlet composition

Dirichlet was a student of Gauss, he extensively studied Disquisitiones Arithmeticae and came up with a much simpler version of the composition. We say that two binary quadratic forms $Q_1 = (A_1, B_1, C_1)$ and $Q_2 = (A_2, B_2, C_2)$ of discriminant D are *united* if

$$\gcd\left(A_1, A_2, \frac{B_1 + B_2}{2}\right) = 1.$$

Remark Observe that $B_1 + B_2$ is always even, because if $D = B_1^2 - 4A_1C_1 = B_2^2 - 4A_2C_2$, then $B_1^2 \equiv B_2^2 (\mod 4)$ and $B_1 \equiv B_2 (\mod 2)$.

Proposition 2.4. *If (A_1, B_1, C_1) and (A_2, B_2, C_2) are united forms, then there exist integers B and C such that*

$$(A_1, B_1, C_1) \sim (A_1, B, A_2C)$$

and

$$(A_2, B_2, C_2) \sim (A_2, B, A_1C).$$

Proposition 2.5. *If (A_1, B_1, C_1) and (A_2, B_2, C_2) are united forms then*

$$[A_1, B_1, C_1] \cdot [A_2, B_2, C_2] = [A_1A_2, B, C]$$

Also, it can be proved [1] that

1. $id = \begin{cases} [1, 0, \frac{D}{4}] & \text{if } D \equiv 0 (\mod 4) \\ [1, 1, \frac{1-D}{4}] & \text{if } D \equiv 1 (\mod 4) \end{cases}$.
2. $[a, b, c]^{-1} = [a, -b, c] = [c, b, a]$

Dirichlet went on to use the notion of ideals in quadratic number fields to obtain the "modern" formulation of the composition law. This approach is out of the scope of this report. It can be consulted in [1].

3 Bhargava's cubes

A *Bhargava's cube* is a configuration of eight integers placed in the vertices of a tridimensional cube. It was used by Manjul Bhargava, to study the composition laws of binary quadratic forms and other such forms.[1]

[1] This is a summary of [2]. For proofs and more detailed explanation see [2] or [1].

3.1 Definition and properties

Let $a, b, c, d, e, f, g, h \in \mathbb{Z}$ and consider a cube as in Figure 1

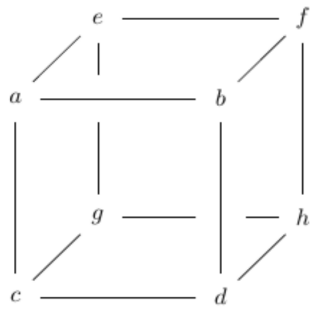
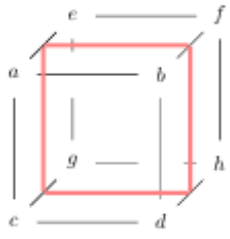
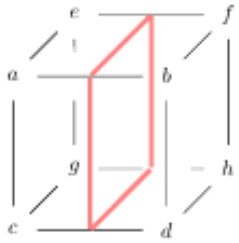


Figure 1: Bhargava's cube. Here a,b,c,d,e,f,g,h are all integers.

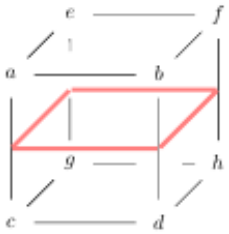
We can cut the cube to obtain two rectangles in the following three ways:



(1) Front-Back



(2) Left-Right



(3) Up-Down

Each of the cuts of the cube determines a pair of the matrices described below.

$$M_1 = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \qquad N_1 = \begin{pmatrix} e & f \\ g & h \end{pmatrix}$$

$$M_2 = \begin{pmatrix} a & c \\ e & g \end{pmatrix} \qquad N_2 = \begin{pmatrix} b & d \\ f & h \end{pmatrix}$$

and

$$M_3 = \begin{pmatrix} a & e \\ b & f \end{pmatrix} \qquad N_3 = \begin{pmatrix} c & g \\ d & h \end{pmatrix}$$

Let Γ be the product $SL_2(\mathbb{Z}) \times SL_2(\mathbb{Z}) \times SL_2(\mathbb{Z})$, where $SL_2(\mathbb{Z})$ is the special linear group defined in 2.2. Then Γ is a group that acts over the space of Bhargava cubes in the following manner.

For any $1 \leq i \leq 3$ an element $\begin{pmatrix} r & s \\ t & u \end{pmatrix}$ in the i-th $SL_2(\mathbb{Z})$ factor of $\gamma \in \Gamma$ acts on the cube by replacing (M_i, N_i) by $(rM_i + sN_i, tM_i + uN_i)$. In other words, each factor of Γ performs a "face operation" on the cube, similar to operations with row and column on a matrix. The first factor performs a face operation on the front and back faces, the second factor on the left and right faces, and the last on the up and down faces. For example if we take the cube in Figure 1 and let $(\gamma_1, \gamma_2, \gamma_3) \in \Gamma$, with

$$\gamma_1 = \begin{pmatrix} r & s \\ t & u \end{pmatrix},$$

then

$$M_1 = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \qquad N_1 = \begin{pmatrix} e & f \\ g & h \end{pmatrix}$$

and

$$rM_1 + sN_1 = \begin{pmatrix} ra + se & rb + sf \\ rc + sg & rd + sh \end{pmatrix} \qquad N_1 = \begin{pmatrix} ta + ue & tb + uf \\ tc + ug & td + uh \end{pmatrix}$$

Therefore, the cube gets transformed by γ_1 into the cube in Figure 3.

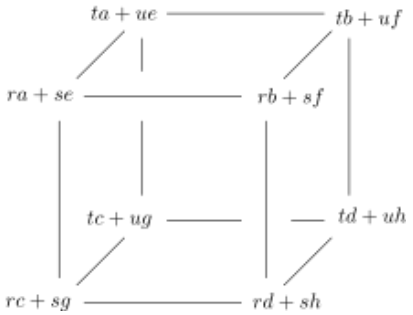


Figure 3: Transformation of Bhargava's cube by γ_1.

We can carry on similarly for γ_2, γ_3 and complete the full action of γ on the cube in thus fashion. The next result establishes that the action of γ is well defined, independently of the order in which the individual actions of its factors are executed.

Proposition 3.1. *The action of each factor of $\gamma \in \Gamma$ commutes with each other.*

The action of $\gamma \in \Gamma$ on the cube C will be denoted by $C * \gamma$.

3.2 Relation with quadratic forms

Given a cube C as in Figure 1, let us construct a binary quadratic form by defining[2]

$$Q_i(x,y) = -\det\left(M_i x + N_i y\right),\ i = 1,2,3 \tag{3}$$

Let $Q_1 = (A_1, B_1, C_1), Q_2 = (A_2, B_2, C_2)$, and $Q_3 = (A_3, B_3, C_3)$, in terms of the cube coefficients, the binary quadratic forms are determined by the upcoming system of equations.

$$\begin{aligned}
A_1 &= bc - ad \\
B_1 &= -ah + bg + cf - de \\
C_1 &= fg - eh \\
A_2 &= ce - ag \\
B_2 &= -ah - bg + cf + de \\
C_2 &= df - bh \\
A_3 &= be - af \\
B_3 &= -ah + bg - cf + de \\
C_3 &= dg - ch.
\end{aligned} \tag{4}$$

One remarkable fact about Bhargava's idea is the following proposition.

Proposition 3.2. *For any cube, the binary quadratic forms obtained as in (3) fulfill*

$$Disc(Q_1) = Disc(Q_2) = Disc(Q_3)$$

thus, this common value will be denoted only as $D = Disc(C)$, also D is invariant under the action of Γ.

Remark With a simple calculation, it can be proved that

$$D = a^2h^2 + b^2g^2 + c^2f^2 + d^2e^2 - 2(abgh + cdef + acfh + bdeg + aedh + bfdg) + 4(adfg + bceh)$$

It is worth noting that the action of Γ on the cubes behaves well with respect to the equivalence of quadratic forms. That is, for $\gamma = (\gamma_1, \gamma_2, \gamma_3) \in \Gamma$ and a cube C whose associated quadratic forms are Q_1, Q_2, Q_3, the image of C under γ is a cube with associated quadratic forms equal to $Q_1^{\tilde{\gamma}_1}$, $Q_2^{\tilde{\gamma}_2}$ and $Q_3^{\tilde{\gamma}_3}$, respectively, where $\tilde{\gamma}_i = \begin{pmatrix} r_i & -t_i \\ -s_i & u \end{pmatrix}$ and $\gamma_i = \begin{pmatrix} r & s \\ t & u \end{pmatrix}$.

If we define

$$\Gamma_i = \{(\gamma_1, \gamma_2, \gamma_3) \in \Gamma : \gamma_j = 1 \text{ for } i \neq j\},$$

an important consequence of the last remark is the proposition below.

[2]arbitrary sign choice differs from Bhargava but chosen to match competition equations to eqns 4

Proposition 3.3. *The elements of* Γ *that leave the* Q_i *invariant are exactly those in* Γ_i

The upcoming subclass of cubes is of special importance in the theory developed by Bhargava.

Definition We say that a cube C is projective if $Q_i,\ i = 1, 2, 3$ are primitive binary quadratic forms.

Let us define an addition operation on the set of (primitive) binary quadratic forms of a fixed discriminant D such that, for all triplets of primitive quadratic forms $Q_1^{(C)}, Q_2^{(C)}, Q_3^{(C)}$ defined from a cube C with discriminant D

[The Cube Law.] The sum of $Q_1^{(C)}, Q_2^{(C)}, Q_3^{(C)}$ is zero.

Let us use $[Q]$ to denote the $SL_2(\mathbb{Z})$-equivalence class of Q. We are now in condition to enunciate two of the most important Bhargava's theorems concerning binary quadratic forms.

Theorem 3.4. *Let* D *be any integer congruent to* 0 *or* $1(mod 4)$*, and let* $Q_{id,D}$ *be any primitive binary quadratic form of discriminant* D *such that there is a cube* C_0 *with* $Q_1^{(C_0)} = Q_2^{(C_0)} = Q_3^{(C_0)} = Q_{id,D}$*. Then there exists a unique group law on the set of* $SL_2(\mathbb{Z})$*-equivalence classes of primitive binary quadratic forms of discriminant* D *such that:*

1. $[Q_{id,D}]$ *is the additive identity.*
2. *For any cube* C *of discriminant* D *such that* $Q_1^{(C)}, Q_2^{(C)}, Q_3^{(C)}$ *are primitive, we have*

$$[Q_1^{(C)}] + [Q_2^{(C)}] + [Q_3^{(C)}] = [Q_{id,D}]$$

Conversely, given Q_1, Q_2, Q_3 *with* $[Q_1] + [Q_2] + [Q_3] = [Q_{id,D}]$*, there exist a cube* C *with discriminant* D *unique up to a* Γ*-equivalence, such that* $Q_i^{(C)} = Q_i,\ i = 1, 2, 3$

The most natural choice for $Q_{id,D}$, the identity element is

$$Q_{id,D} = x^2 - \frac{D}{4}y^2 \quad \text{or} \quad Q_{id,D} = x^2 - xy + \frac{1-D}{4}y^2.$$

If the identity is defined in this way, the group law in theorem 3.4 is equivalent to Gauss composition. Theorem 3.4 actually implies something stronger than Gauss composition: not only do the primitive binary quadratic forms of discriminant D form a group, but the cubes of discriminant D that give rise to triples of primitive quadratic forms themselves constitute a group.

4 The Problem

4.1 Statement of the problem and preliminar considerations

We are finally able to state the problem at hand. Given a prime p such that $p \equiv 7 \pmod 8$, we are asked to create a python function that receives as input a cube, (a, b, c, d, e, f, g, h), with $Q_1 = Q_2$ and $D = \text{Disc}(Q_1) = \text{Disc}(Q_2) = \text{Disc}(Q_3) = -p$, and returns a new cube, $(a', b', c', d', e', f', g', h')$, such that $Q_1' = Q_2'$ and $Q_1' = Q_2' \sim Q_3$ with a computational cost as low as possible. It can be proved that this assumptions imply $(A_1, B_1) = (C_1, B_1) = 1$ and, consequently (A_1, B_1, C_1). That is, the given cube is projective. The previous sections suggest that a solution can be provided either using the cubes approach, the quadratic forms one or a combination of both.

An additional consideration for the problem comes from the fact that the program output will be then fed in again to give another solution and this process will be repeated several times. It is therefore important that we keep the magnitudes of either the coefficients of the quadratic forms or the cube values relatively small. This encourages the use of some sort of reduction during the computations. Although the notion of reduced quadratic form defined at the end of 2.2 seems the natural candidate, the solution provided in `example.py` shows that its computational cost is far too big to suit our purposes.

Let us elaborate a little further on the claim made a paragraph ago. Equations (4) can be manipulated into the following relations.

$$\begin{aligned}
bc - ad &= A_1 \\
ce - ag &= A_2 \\
be - af &= A_3 \\
cf - ah &= (B_1 + B_2)/2 \\
bg - de &= (B_1 - B_2)/2 \\
bg - ah &= (B_1 + B_3)/2 \\
cf - de &= (B_1 - B_3)/2 \\
de - ah &= (B_2 + B_3)/2 \\
cf - bg &= (B_2 - B_3)/2 \\
fg - eh &= C_1 \\
df - bh &= C_2 \\
dg - ch &= C_3
\end{aligned} \tag{5}$$

Moreover, with a extra bit of effort we can produce the following linear relations on the

cube coefficients.

$$\begin{aligned} aC_3 + gA_1 &= c(B_1 + B_3)/2 \\ aC_1 + gA_3 &= e(B_1 + B_3)/2 \\ bC_3 + hA_1 &= d(B_1 + B_3)/2 \\ bC_1 + hA_3 &= f(B_1 + B_3)/2 \end{aligned} \tag{6}$$

$$\begin{aligned} eA_1 - cA_3 &= a(B_1 - B_3)/2 \\ fA_1 - dA_3 &= b(B_1 - B_3)/2 \\ cC_1 - eC_3 &= g(B_1 - B_3)/2 \\ dC_1 - fC_3 &= h(B_1 - B_3)/2 \end{aligned}$$

$$\begin{aligned} eA_1 - bA_2 &= a(B_1 - B_2)/2 \\ gA_1 - dA_2 &= c(B_1 - B_2)/2 \\ bC_1 - eC_2 &= f(B_1 - B_2)/2 \\ dC_1 - gC_2 &= h(B_1 - B_2)/2 \end{aligned} \tag{7}$$

$$\begin{aligned} aC_2 + fA_1 &= b(B_1 + B_2)/2 \\ cC_2 + hA_1 &= d(B_1 + B_2)/2 \\ aC_1 + fA_2 &= e(B_1 + B_2)/2 \\ cC_1 + hA_2 &= g(B_1 + B_2)/2 \end{aligned}$$

$$\begin{aligned} bA_2 - cA_3 &= a(B_2 - B_3)/2 \\ fA_2 - gA_3 &= e(B_2 - B_3)/2 \\ cC_2 - bC_3 &= d(B_2 - B_3)/2 \\ gC_2 - fC_3 &= h(B_2 - B_3)/2 \end{aligned} \tag{8}$$

$$\begin{aligned} dA_3 + aC_2 &= b(B_3 + B_2)/2 \\ aC_3 + dA_2 &= c(B_3 + B_2)/2 \\ hA_3 + eC_2 &= f(B_3 + B_2)/2 \\ eC_3 + hA_2 &= g(B_3 + B_2)/2 \end{aligned}$$

Although Equations (6-8) do not completely encode the relations given by the quadratic equations in (5) (there are two degrees of freedom), they are easier to solve. A good strategy then is to produce a solution for (6-8) and then meet the additional restrictions using the quadratic ones. One consequence of this is that given the previous sets of equations, for

every three primitive quadratic forms with the same discriminant that fulfill the cube law, then there is, up to an overall sign change on its coefficients, a unique cube whose quadratic forms are the three given ones.

4.2 The existent solution

Of the given solutions for the problem, the one that performs the required computations with the smallest cost is provided in `example2.py`.

The script begins with a setup routine that takes the discriminant (that is, $-p$) as input. The routine then obtains the boundary

$$L = \left\lfloor \sqrt{\left\lfloor \sqrt{\frac{p}{4}} \right\rfloor} \right\rfloor \approx \frac{\sqrt[4]{p}}{\sqrt{2}}$$

and constructs the quadratic form $(A, B, C) = (2, 1, \frac{1+p}{8})$, of discriminant $-p$. Observe that, since $p \equiv 7 \pmod 8$, the last entry of this triplet is an integer and this quadratic form is reduced if $p > 7$.

The next step is to call the function `nudupl_cube` with the reduced form (A, B, C) and L as input. This function first constructs a cube of the form $(-1, b, 0, A, b, f, A, B)$, where b and f are solutions of the equation $Af - Bb = C$ such that $|b|$ is minimum. Recall that $\gcd(A, B) = 1$, so this equation always has a solution. It follows from (4) that, for this cube, $A_1 = A_2 = A$, $B_1 = B_2 = B$ and $C_1 = C_2 = C$.

After this cube is constructed, the algorithm transforms it using an element of the form $(1, 1, \gamma) \in \Gamma$ to obtain $(a', b', c', d', b', f', d', h') = (1, 1, \gamma) * (-1, 0, b, 0, A, b, f, A, B)$, in such a way that $|b'| \leq L$ or $d = 0$, done with the aim of keeping the absolute value of the cube coefficients around the boundary L. Recall from 3.3 that $(1, 1, \gamma)$ fixes the first two quadratic forms, which are reduced by construction. Finally, the algorithm returns $(a', b', c', d', b', f', d', h')$ as an output.

5 Our take on the problem

The solution just exposed is a clever way to obtain a cube as required while keeping the size of the coefficients under control, but it comes with the enormous cost of tossing the whole cube away and obtain the new one in terms of just the desired quadratic form.

The following subsections discuss two approaches that are, to our understanding, probable ways to get a computationally cheaper solution.

5.1 The first approach

This idea goes more or less along the lines of the algorithm described in section 4.2, but it considers a simpler starting cube. Our premise is that this simplicity may be reflected in

the reduction process, provided that we come up with a way to carry the process that is compatible with the structure of the cube.

In the following paragraphs we describe the proposed starting cube and justify why is it always possible to construct such a cube to solve our problem.

Suppose that we have a projective cube. Equations (4) implies that the greatest common divisor of its entries is 1. Therefore, by applying elements of Γ we can obtain a cube where $a = 1$, this can be used to clear out the adjacent entries, which can be arranged to be $b = c = e = 0$. Thus, we see that any projective cube can be transformed by an element of Γ to some cube of the form

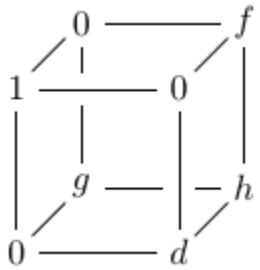


Figure 4

The three binary forms associated to this cube are

$$\begin{aligned} Q_1 &= -dx^2 + hxy + fgy^2 \\ Q_2 &= -gx^2 + hxy + dfy^2 \\ Q_3 &= -fx^2 + hxy + dgy^2 \end{aligned}$$

Now, since the solution of our problem requires $Q_1 = Q_2$, then $d = g$ and, consequently, from (4) we obtain that the cube we need to find is such that

$$(-d, h, fd) \sim (b_0e_0 - a_0f_0, -a_0h_0 + b_0g_0 - c_0f_0 + d_0e_0, d_0g_0 - c_0h_0) = (A, B, C),$$

where $(a_0, b_0, c_0, d_0, e_0, f_0, g_0, h_0)$ is the cube provided as input.

This suggests that in order to solve the problem it is sufficient to get a small enough representative of the class $[A, B, C]$, whose first entry divides its last.

This divisibility problem is computationally cheaper than solving a linear system, which is the approach of the one described in 4.2.

An initial strategy to get the desired representative could be, for example, apply to (A, B, C) a well suited element of the form $\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$ or maybe play around with the degrees of freedom provided by the entire group Γ to obtain the desired element.

5.2 Group theoretic approach

The main idea behind the second course of action we propose is that if we can extend in a convenient way the action of the group Γ to a group Γ' such that $\Gamma \leq \Gamma'$, that is, in such a fashion that the action performed in the cube has an effect on the quadratic forms is convenient to our purposes.

To put the previous idea in clearer terms, it is necessary to make a preliminary remarks.

Let C be a cube and Q_1, Q_2, Q_3 be its associated binary quadratic forms, the cube law establishes that $Q_1 \cdot Q_2 \cdot Q_3 = Q_{id,D}$. In our particular case, we have $Q_1 = Q_2$, which implies $Q_1^2 \sim Q_3^{-1}$, that is to say $Q_1^{-2} \sim Q_3$. On the other hand, we are required to find a cube $C' = (a', b', c', d', e', f', g', h')$ such that its associated quadratic forms, Q_1', Q_2', Q_3', are such that $Q_1' = Q_2' \sim Q_3$. But Equations (4) and (7) imply that $Q_1' = Q_2'$ if and only if $e' = b'$ and $d' = g'$. See Figure 5.

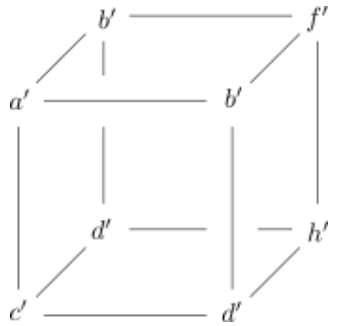


Figure 5

Furthermore, since every cube we seek satisfies $Q_1'^{-2} \sim Q_3'$, the cube law implies that $Q_3' \sim Q_3^{-2}$, from which we conclude that every solution of the problem must be of the form described in Figure 5 and on the same orbit as the cube determined by the quadratic forms Q_3, Q_3 and Q_3^{-2}.

Suppose that we could find a group, $\Gamma' \geq \Gamma$ that extends the action of Γ on the cube. If there is an element of Γ' in the set-wise stabilizer of the set of cubes of the form $(a', b', c', d', b', f', d', h')$ such that the associated action of Γ' on the quadratic forms sends Q_1 to Q_1^{-2} or Q_3 to Q_3^{-2}, then we are done.

Although this approximation seems a bit unfathomable, if we consider the group

$$GL_2(\mathbb{Z}) = \left\{ \begin{pmatrix} r & s \\ t & u \end{pmatrix} : r, s, t, u \in \mathbb{Z} \text{ and } ru - st = \pm 1 \right\},$$

there is a natural way to extend the action of Γ to an action of $\Gamma' = GL_2(\mathbb{Z}) \times GL_2(\mathbb{Z}) \times GL_2(\mathbb{Z})$. Namely, for $\gamma = \begin{pmatrix} r & s \\ t & u \end{pmatrix} \in GL_2(\mathbb{Z})$, we define the action of $(\gamma, 1, 1)$ on the

cube (a, b, c, d, e, f, g, h) exactly as in Figure 3, with the other factors acting in an analogous way. Observe that for $\gamma = \begin{pmatrix} r & s \\ t & u \end{pmatrix} \in GL_2(\mathbb{Z})$, if the cube C has (A_1, B_1, C_1) as its first associated quadratic form, then the image of C under $(\gamma, 1, 1)$ has

$$(r^2A_1 + rsB_1 + s^2C, -2trA_1 - (ts + ru)B_1 - 2usC_1, t^2A_1 + tuB_1 + u^2C)$$

as its first associated quadratic form. In particular, $(\gamma, 1, 1)$, with $\gamma = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ transforms C into a cube with (C_1, B_1, A_1) as its first associated quadratic form, and

$$[A_1, B_1, C_1] \cdot [C_1, B_1, A_1] = [Q_{id,D}].$$

This sheds some light into the matter, and possibly looking into extensions of $SL_2(\mathbb{Z})$ (or $GL_2(\mathbb{Z})$), it only remains to find an element of an extension that sends $[A_1, B_1, C_1]$ to its square (or its square inverse). We can look, say, into the cyclic or central extensions of either $GL_2(\mathbb{Z})$ or $SL_2(\mathbb{Z})$, that have simple enough ways to act on the same sets.

5.2.1 Another way to extend the group

As a closing remark, we briefly discuss a second way to extend the acting group.

The actual mathematical objects that Bhargava identifies with his cubes are elements of the space $\mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2$. This space can also be identified with the 4×2 matrices with integer coefficients, on which $SL_4(\mathbb{Z})$ acts on the left in a natural way. A few computations show that we can encode within this group the action of the factors of Γ. For example, since

$$\begin{pmatrix} r & s & 0 & 0 \\ t & u & 0 & 0 \\ 0 & 0 & r & s \\ 0 & 0 & t & u \end{pmatrix} \begin{pmatrix} a & b \\ c & d \\ e & f \\ g & h \end{pmatrix} = \begin{pmatrix} ra + sc & rb + sd \\ ta + uc & tb + ud \\ re + sg & rf + sh \\ te + ug & tf + uh \end{pmatrix},$$

then the subgroup

$$\left\{ \begin{pmatrix} r & s & 0 & 0 \\ t & u & 0 & 0 \\ 0 & 0 & r & s \\ 0 & 0 & t & u \end{pmatrix} : r, s, t, u \in \mathbb{Z} \text{ and } ru - st = 1 \right\}$$

of $SL_4(\mathbb{Z})$ is isomorphic to $SL_2(\mathbb{Z})$ and acts on the 4×2 matrices with integer coefficients in the same way as $1 \times 1 \times SL_2(\mathbb{Z})$ acts on the cubes. It should be clear now that there are several ways we can explore this perspective and that many of these ways provide a lot of room to experiment with the transformations allowed on the Bhargava cubes, that might very well lead to a more theoretic approximation to tackle the problem, hence simplifying the final computational costs when an algorithm is developed.

References

[1] Séguin, F. Composition of Binary Quadratic Forms. Reson 24, 633–651 (2019). https://doi.org/10.1007/s12045-019-0822-4

[2] Bhargava, M. Higher composition laws I: A new view on Gauss composition, and quadratic generalizations. December 2003, Annals of Mathematics 159(1):217-250 DOI: 10.4007/annals.2004.159.217