

## REALIZING ALGEBRAIC INVARIANTS OF HYPERBOLIC SURFACES

BOGWANG JEON

ABSTRACT. Let  $S_g$  ( $g \geq 2$ ) be a closed surface of genus  $g$ . Let  $K$  be any real number field, and let  $A$  be any quaternion algebra over  $K$  such that  $A \otimes_K \mathbb{R} \cong M_2(\mathbb{R})$ . We show that there exists a hyperbolic structure on  $S_g$  such that  $K$  and  $A$  arise as its invariant trace field and invariant quaternion algebra.

### 1. INTRODUCTION

The invariant trace field and the quaternion algebra are basic algebraic invariants of a Kleinian group. Questions around these invariants have inspired extensive research in the study of hyperbolic 3-manifolds. The following Realization Conjecture due to W. Neumann [5] is one of the fundamental questions along these lines:

**Conjecture 1.** *Let  $K$  be any nonreal complex number field, and let  $A$  be any quaternion algebra over  $K$ . Then there exists a hyperbolic 3-manifold  $M$  such that  $K$  and  $A$  arise as the invariant trace field and quaternion algebra of  $M$ .*

For the 2-dimensional case, since Mostow's rigidity theorem does not hold, trace fields and quaternion algebras are no longer topological invariants. But, in this case, we can ask the following analogous question instead, as suggested in [5].

**Question 1.** Let  $S_g$  ( $g \geq 2$ ) be a closed surface of genus  $g$ , let  $K$  be any real number field, and let  $A$  be any quaternion algebra over  $K$  such that  $A \otimes_K \mathbb{R} \cong M_2(\mathbb{R})$ .<sup>1</sup> Is there a hyperbolic structure on  $S_g$  whose invariant trace field and quaternion algebra are equal to  $K$  and  $A$ ?

This natural question had been discussed for some time, but the complete answer was unknown. Recently J. Kahn and V. Markovic announced a partial answer as follows.

**Theorem 1.1** ([3]). *Let  $K$  be any real number field, and let  $A$  be any quaternion algebra over  $K$  such that  $A \otimes_K \mathbb{R} \cong M_2(\mathbb{R})$  and  $A \not\cong (\frac{1}{K})$ .<sup>2</sup> Then there exists a closed surface  $S_g$  and a hyperbolic structure on it such that  $K$  and  $A$  are its invariant trace field and quaternion algebra.*

---

Received by the editors January 6, 2016, and, in revised form, September 11, 2016, and January 30, 2017.

2010 *Mathematics Subject Classification.* Primary 11Z05, 57M99.

<sup>1</sup>We say  $K$  is a real number field if  $K \subset \mathbb{R}$  and  $[K : \mathbb{Q}] < \infty$ . Note that the condition on  $A$  (i.e.,  $A \otimes_K \mathbb{R} \cong M_2(\mathbb{R})$ ) is necessary (see Section 2.2).

<sup>2</sup>We believe the second condition on  $A$  (i.e.,  $A \not\cong (\frac{1}{K})$ ) is removable.

Their proof uses the techniques developed in their recent proofs of two deep conjectures, the Surface Subgroup Conjecture and the Ehrenpreis Conjecture. Although Theorem 1.1 answers Question 1 partially, an important feature of this theorem is that they realize surfaces via integral traces. That is, all the traces in their construction are algebraic integers.<sup>3</sup>

The aim of this paper is to provide a complete answer to Question 1. In other words, we prove the following theorem.

**Theorem 1.2.** *Let  $S_g$  ( $g \geq 2$ ) be any closed surface of genus  $g$ . Let  $K$  be any real number field, and let  $A$  be any quaternion algebra over  $K$  such that  $A \otimes_K \mathbb{R} \cong M_2(\mathbb{R})$ . Then there exists a hyperbolic structure on  $S_g$  such that  $K$  and  $A$  arise as its invariant trace field and invariant quaternion algebra.*

Note that since invariant trace fields and quaternion algebras are invariants of commensurability classes, once we prove the above theorem for  $g = 2$ , the rest of the cases easily follow by looking at covering surfaces.

We can also ask a similar realization question about the (usual) trace field and quaternion algebra. In fact, we prove the following.

**Theorem 1.3.** *Let  $S_2$  be a genus 2 closed surface. Let  $K$  be any real number field, and let  $A$  be any quaternion algebra over  $K$  such that  $A \otimes_K \mathbb{R} \cong M_2(\mathbb{R})$ . Then there exists a hyperbolic structure on  $S_2$  such that  $K$  and  $A$  arise as its trace field and quaternion algebra. Moreover, the invariant trace field and invariant quaternion algebra of it are equal to the trace field and quaternion algebra of it, respectively.*

We split the proof of this theorem into two parts. We prove the first statement in Section 3 and, using the proof, we show the second statement in Section 4.

Our proofs are based on explicit computations as well as some elementary facts in number theory. The basic idea is to create a genus two Riemann surface by attaching two identical copies of a once-punctured torus. Then using the work of T. Gaughhofer [1], we prove that its trace field is fairly simple, generated only by the traces of three elements. We next convert the problem into a system of Diophantine equations and solve these equations. The whole process is completely elementary and natural.

## 2. PRELIMINARIES

In Sections 2.1 and 2.2, we quickly review basic definitions and facts which will be used below. For more details, see [4].

**2.1. Trace field.** Let  $\Gamma \subset \mathrm{PSL}(2, \mathbb{R})$  ( $\cong \mathrm{Isom}^+(\mathbb{H}^2)$ ) be a Fuchsian group such that  $\mathbb{H}^2/\Gamma$  is a closed hyperbolic surface. Let  $\bar{\Gamma} \subset \mathrm{SL}(2, \mathbb{R})$  be the inverse image of  $\Gamma$  under the projection  $\mathrm{SL}(2, \mathbb{R}) \rightarrow \mathrm{PSL}(2, \mathbb{R})$ . Then the *trace field* of  $\Gamma$  is defined by

$$\mathbb{Q}(\{\mathrm{tr} \gamma \mid \gamma \in \bar{\Gamma}\}).$$

This set is known to be a finite extension number field. For instance, if  $\bar{\Gamma} = \langle \gamma_1, \dots, \gamma_n \mid - \rangle$ , then its trace field is generated by the traces of the following elements:

$$(2.1) \quad \{\gamma_i, \gamma_{j_1} \gamma_{j_2}, \gamma_{k_1} \gamma_{k_2} \gamma_{k_3} \mid 1 \leq i \leq n, 1 \leq j_1 < j_2 \leq n, 1 \leq k_1 < k_2 < k_3 \leq n\}.$$

---

<sup>3</sup>However, answering the question via integral traces seems to be impossible. See Section 6.

The *invariant trace field* of  $\Gamma$  is defined by

$$\mathbb{Q}(\{\text{tr } \gamma^2 \mid \gamma \in \bar{\Gamma}\}),$$

and it is an invariant of the commensurability class of  $\Gamma$ .

**2.2. Quaternion algebra.** Let  $K$  be a number field. A *quaternion algebra* over  $K$  is a 4-dimensional algebra with basis  $\{\mathbf{1}, \mathbf{i}, \mathbf{j}, \mathbf{k}\}$  such that

$$\mathbf{i}^2 = a, \mathbf{j}^2 = b, \mathbf{ij} = -\mathbf{ji} = \mathbf{k},$$

for some  $a, b \in K^*$ , and this is often denoted by  $(\frac{a, b}{K})$ . The following equivalence relations are well known:

$$(2.2) \quad \left(\frac{a, b}{K}\right) \cong \left(\frac{au^2, bv^2}{K}\right) \cong \left(\frac{au^2, bv^2 - abw^2}{K}\right),$$

where  $u, v, w \in K$  such that  $u, v, bv^2 - abw^2 \neq 0$ .<sup>4</sup>

Let  $\Gamma$  be as in Section 2.1. The *quaternion algebra* of  $\Gamma$  is defined by

$$\left\{ \sum_{i=1}^n a_i \gamma_i \mid a_i \in \text{trace field of } \Gamma, \gamma_i \in \bar{\Gamma} \right\}.$$

This set is a quaternion algebra over the trace field of  $\Gamma$  and equivalent to

$$(2.3) \quad \left(\frac{\text{tr}^2 \gamma_1 - 4, \text{tr} [\gamma_1, \gamma_2] - 2}{\text{trace field of } \Gamma}\right),$$

where  $\gamma_1, \gamma_2 \in \bar{\Gamma}$  are two hyperbolic elements such that  $\langle \gamma_1, \gamma_2 \rangle$  is irreducible. Note that since  $\gamma_1$  is hyperbolic,  $\text{tr } \gamma_1 > 2$ , and thus

$$(2.4) \quad \left(\frac{\text{tr}^2 \gamma_1 - 4, \text{tr} [\gamma_1, \gamma_2] - 2}{K}\right) \otimes_K \mathbb{R} = \left(\frac{\text{tr}^2 \gamma_1 - 4, \text{tr} [\gamma_1, \gamma_2] - 2}{\mathbb{R}}\right) \cong \left(\frac{1, 1}{\mathbb{R}}\right) = M_2(\mathbb{R}),$$

where  $K$  is the trace field of  $\Gamma$ . The *invariant quaternion algebra* of  $\Gamma$  is the algebra generated over the invariant trace field of  $\Gamma$  by the squares of the elements of  $\bar{\Gamma}$ . This set is also an invariant of the commensurability class of  $\Gamma$ .

**2.3. Trace field coordinates of Riemann surfaces.** Each  $\gamma \in \text{PSL}(2, \mathbb{R})$  has two inverse images in  $\text{SL}(2, \mathbb{R})$ . We denote the one having the positive trace by  $\gamma_+$  and the one having the negative trace by  $\gamma_-$ .

Following the same notation given in [1], we use the matrices below as a basis of  $\text{SL}(2, \mathbb{R})$ :

$$\mathbf{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \mathbf{I} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \mathbf{J} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \mathbf{K} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

For example, in terms of the above basis,  $(\frac{a \ b}{c \ d})$  is represented by

$$\left(\frac{a+d}{2}\right)\mathbf{1} + \left(\frac{a-d}{2}\right)\mathbf{I} + \left(\frac{b+c}{2}\right)\mathbf{J} + \left(\frac{b-c}{2}\right)\mathbf{K}.$$

Let  $\mathcal{T}$  be a hyperbolic once punctured torus whose fundamental domain and picture are shown in Figures 2 and 1, respectively. Let  $\rho$  and  $\sigma$  be the hyperbolic

---

<sup>4</sup>To show the equivalence between  $A_1 = (\frac{a, b}{K})$  and  $A_2 = (\frac{au^2, bv^2 - abw^2}{K})$ , let  $\varphi : A_1 \rightarrow A_2$  be a map such that  $\varphi(\mathbf{1}) = \mathbf{1}$ ,  $\varphi(\mathbf{i}) = u\mathbf{i}$ , and  $\varphi(\mathbf{j}) = u\mathbf{j} + w\mathbf{k}$ . Then  $\varphi(\mathbf{j})\varphi(\mathbf{k}) = -\varphi(\mathbf{k})\varphi(\mathbf{j})$ , and so it can be naturally extended to an isomorphism between  $A_1$  and  $A_2$ .

elements given in Figure 2. Then  $\rho_+$  and  $\sigma_+$  can be represented in terms of the traces of  $\rho_+, \sigma_+, (\rho\sigma)_+, [\rho, \sigma]_+$  plus the attracting fixed point of  $\sigma$  as follows.<sup>5</sup>

**Theorem 2.1** ([1]). *Let  $\text{tr } \rho_+ = 2r$ , let  $\text{tr } \sigma_+ = 2s$ , let  $\text{tr } (\rho\sigma)_+ = 2t$ , let  $\text{tr } ([\rho, \sigma]_+) = 2c$ , and let  $M > 0$  be the attracting fixed point of  $\sigma$  (as shown in the picture). Then*

$$\begin{aligned}
 \rho_+ &= r\mathbf{1} + \frac{r(c+1)}{\sqrt{c^2-1}}\mathbf{I} - \frac{\tilde{M}(2rs-t+(c+\sqrt{c^2-1})t)}{2(c-1+2s^2)}(\mathbf{J}+\mathbf{K}) \\
 &\quad + \frac{2rs-t+(c-\sqrt{c^2-1})t}{2\tilde{M}(c-1)}(\mathbf{J}-\mathbf{K}), \\
 \sigma_+ &= s\mathbf{1} - \frac{s(c+1)}{\sqrt{c^2-1}}\mathbf{I} + \frac{\tilde{M}}{2}(\mathbf{J}+\mathbf{K}) - \frac{c-1+2s^2}{2\tilde{M}(c-1)}(\mathbf{J}-\mathbf{K}),
 \end{aligned}
 \tag{2.5}$$

where

$$\begin{aligned}
 \tilde{M} &= M \frac{s\sqrt{c^2-1}+(c-1)\sqrt{s^2-1}}{c-1}, \quad c = 4rst - 2r^2 - 2s^2 - 2t^2 + 1, \\
 &\text{and } c, r, s, t > 1, M > 0.
 \end{aligned}
 \tag{2.6}$$

*Remark.* In [1], it is proved that, for any  $c, r, s, t, M, \tilde{M}$  satisfying (2.6), the group generated by  $\rho_+$  and  $\sigma_+$  act discretely on  $\mathbb{H}$  and generate a fundamental domain as given in Figure 2.

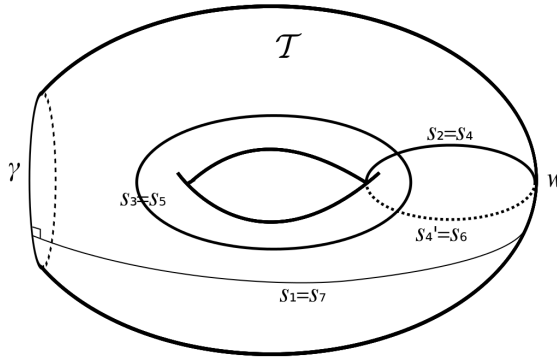


FIGURE 1

**2.4. Creating a surface  $\mathcal{S}$ .** Now we create a genus 2 surface  $\mathcal{S}$  by attaching  $\mathcal{T}$  to identical symmetric image  $\mathcal{T}'$  along their common boundary as shown in Figure 3. (That is,  $\mathcal{S}$  is the doubling of  $\mathcal{T}$ . See Figure 4 for the corresponding fundamental domain.) Let  $\rho'$  and  $\sigma'$  be the elements corresponding to  $\rho$  and  $\sigma$  (Figure 4). Then

<sup>5</sup>Note that  $[\rho_+, \sigma_+] = -[\rho, \sigma]_+ = [\rho, \sigma]_-$ .

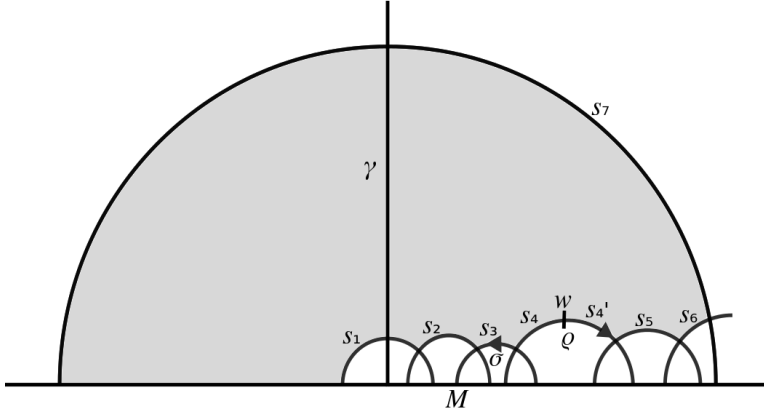


FIGURE 2.  $\rho$  and  $\sigma$  fix the geodesics containing  $s_4 \cup s'_4$  and  $s_3$  (respectively), and  $[\rho, \sigma]$  fixes the  $y$ -axis. The side pairings are given as follows:  $\rho(s_3) = s_5, \sigma(s_4) = s_2, \rho\sigma\rho^{-1}(s'_4) = s_6$ , and  $[\rho, \sigma](s_1) = s_7$ .

$(\rho')_+$  and  $(\sigma')_+$  are as follows:<sup>6</sup>

$$\begin{aligned}
 (\rho')_+ &= r\mathbf{1} + \frac{r(c+1)}{\sqrt{c^2-1}}\mathbf{I} + \frac{\tilde{M}(2rs-t+(c+\sqrt{c^2-1})t)}{2(c-1+2s^2)}(\mathbf{J}+\mathbf{K}) \\
 &\quad - \frac{2rs-t+(c-\sqrt{c^2-1})t}{2\tilde{M}(c-1)}(\mathbf{J}-\mathbf{K}), \\
 (\sigma')_+ &= s\mathbf{1} - \frac{s(c+1)}{\sqrt{c^2-1}}\mathbf{I} - \frac{\tilde{M}}{2}(\mathbf{J}+\mathbf{K}) + \frac{c-1+2s^2}{2\tilde{M}(c-1)}(\mathbf{J}-\mathbf{K}),
 \end{aligned}
 \tag{2.7}$$

where

$$\begin{aligned}
 \tilde{M} &= M \frac{s\sqrt{c^2-1}+(c-1)\sqrt{s^2-1}}{c-1}, \quad c = 4rst - 2r^2 - 2s^2 - 2t^2 + 1, \\
 &\quad \text{and } c, r, s, t > 1, M > 0.
 \end{aligned}$$

**2.5. Trace field of  $\mathcal{S}$ .** By slightly abusing notation, from now on we denote  $\rho_+, \sigma_+, (\rho')_+$ , and  $(\sigma')_+$  by  $\rho, \sigma, \rho'$ , and  $\sigma'$ , respectively. By (2.1), the trace field of  $\mathcal{S}$  is generated by the traces of the following elements:

$$\rho, \sigma, \rho', \sigma', \rho\sigma, \rho'\sigma', \rho\rho', \rho\sigma', \sigma\rho', \sigma\sigma', \rho\sigma\rho', \rho\sigma\sigma', \rho\rho'\sigma', \sigma\rho'\sigma'.
 \tag{2.8}$$

---

<sup>6</sup>If  $\frac{az+b}{cz+d}$  is a Möbius transformation representing  $\rho$ , then it is easy to check that  $\rho'$  is of the form  $\frac{az-b}{-cz+d}$ . In terms of the basis we introduced,  $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$  is equal to  $(\frac{a+d}{2})\mathbf{1} + (\frac{a-d}{2})\mathbf{I} + (\frac{b+c}{2})\mathbf{J} + (\frac{b-c}{2})\mathbf{K}$  and  $\begin{pmatrix} a & -b \\ -c & d \end{pmatrix}$  is equal to  $(\frac{a+d}{2})\mathbf{1} + (\frac{a-d}{2})\mathbf{I} - (\frac{b+c}{2})\mathbf{J} - (\frac{b-c}{2})\mathbf{K}$ . Thus the formula follows.

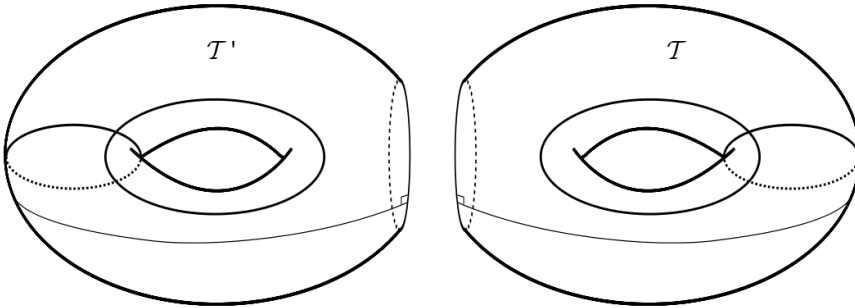


FIGURE 3

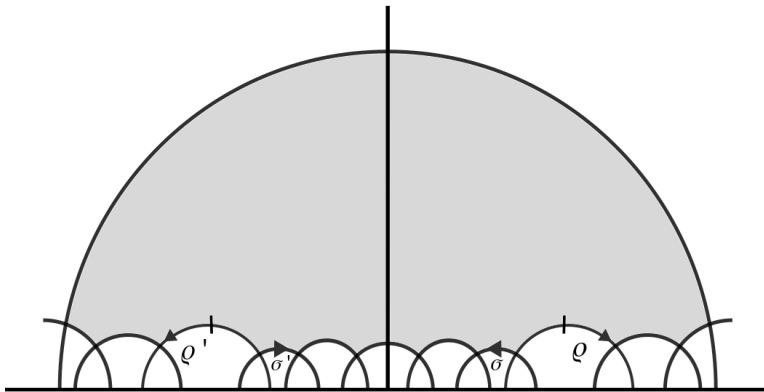


FIGURE 4

By (2.5) and (2.7), all the elements of  $\rho, \sigma, \rho',$  and  $\sigma'$  are contained in

$$(2.9) \quad \mathbb{Q}(r, s, t, M, \sqrt{s^2 - 1}, \sqrt{c^2 - 1}) \text{ where } c = 4rst - 2r^2 - 2s^2 - 2t^2 + 1,$$

and so the elements of (2.8) are contained in (2.9) as well. These imply the following simple lemma.

**Lemma 2.2.** *The trace field of  $\mathcal{S}$  is contained in (2.9).*

Now we further claim the following.

**Theorem 2.3.** *The trace field of  $\mathcal{S}$  is simply equal to  $\mathbb{Q}(r, s, t)$ .*

In other words, the trace of any element in (2.8) is represented as a rational function of  $r, s, t$  without involving  $M, \sqrt{s^2 - 1}, \sqrt{c^2 - 1}$ . Since the proof of this theorem is elementary but lengthy, we postpone it until Section 5.

## 3. PROOF OF THEOREM 1.3 (PART I)

In this section, we prove the first part of Theorem 1.3. That is, we show that any real number field and any quaternion algebra over it can be realized as the trace field and the quaternion algebra of  $\mathcal{S}$ .

By Theorem 2.3, the trace field of  $\mathcal{S}$  is equal to

$$(3.1) \quad \mathbb{Q}(r, s, t),$$

and, by (2.3), the quaternion algebra of  $\mathcal{S}$  is equivalent to

$$(3.2) \quad \left( \frac{(2r)^2 - 4, -2c - 2}{\mathbb{Q}(r, s, t)} \right),$$

where  $c = 4rst - 2r^2 - 2s^2 - 2t^2 + 1$  and  $c, r, s, t > 1$ .<sup>7</sup>

Let  $K$  be any real number field, and let  $A$  be any quaternion algebra over  $K$  such that  $A \otimes_K \mathbb{R} \cong M_2(\mathbb{R})$ . We suppose  $A$  is of the form  $\left( \frac{a, b}{K} \right)$  for some  $a, b \in K$ .<sup>8</sup> Since

$$\left( \frac{a, b}{K} \right) \cong \left( \frac{au^2, bv^2 - abw^2}{K} \right)$$

for any  $u, v, w$  (see (2.2)), to achieve the goal it is enough to find  $r, s, t, u, v, w \in \mathbb{R}$  such that

$$K = \mathbb{Q}(r, s, t) \quad \text{and} \quad \left( \frac{(2r)^2 - 4, -2c - 2}{\mathbb{Q}(r, s, t)} \right) = \left( \frac{au^2, bv^2 - abw^2}{K} \right),$$

where  $c = 4rst - 2r^2 - 2s^2 - 2t^2 + 1$  and  $c, r, s, t > 1$ . In other words, for any given number field  $K$  and  $a, b \in K$  ( $a > 0$ ), it is enough to find  $r, s, t, u, v, w \in K$  such that

$$(3.3) \quad \begin{aligned} c &= 4rst - 2r^2 - 2s^2 - 2t^2 + 1, \\ -2c - 2 &= bv^2 - abw^2, \\ (2r)^2 - 4 &= au^2 \quad (a > 0), \\ \mathbb{Q}(r, s, t) &= K, \\ c, r, s, t &> 1. \end{aligned}$$

Thus proving the first statement in Theorem 1.3 is reduced to solving the above system of Diophantine equations. To simplify the notation, we let  $2r = x', 2s = y', 2t = z, 2c = -c'$  and rewrite (3.3) as follows:

$$(3.4) \quad (x')^2 + (y')^2 + z^2 - x'y'z = c' + 2,$$

$$(3.5) \quad c' - 2 = bv^2 - abw^2,$$

$$(3.6) \quad z^2 - 4 = au^2 \quad (a > 0),$$

$$(3.7) \quad \mathbb{Q}(x', y', z) = K,$$

$$(3.8) \quad x', y', z > 2, c' < -2.$$

<sup>7</sup>Following the same notation given in Section 2, recall that  $\text{tr}([\rho_+, \sigma_+]) = -\text{tr}([\rho, \sigma]_+) = -2c$ .

<sup>8</sup>Since  $A \otimes_K \mathbb{R} \cong M_2(\mathbb{R})$ , at least one of  $a$  and  $b$  is positive, and, without loss of generality, we assume  $a > 0$ .

To further simplify, we combine (3.4) and (3.5), and transform the resulting equation as follows:

$$\begin{aligned}
& (x')^2 + (y')^2 + z^2 - x'y'z = c' + 2 \\
\text{(by (3.5)) } & \Rightarrow (x')^2 + (y')^2 + z^2 - x'y'z = bv^2 - abw^2 + 4 \\
& \Rightarrow \left(x' - \frac{y'z}{2}\right)^2 - \frac{(y')^2 z^2}{4} + (y')^2 + z^2 = bv^2 - abw^2 + 4 \\
& \Rightarrow \left(x' - \frac{y'z}{2}\right)^2 - \frac{(y')^2}{4}(z^2 - 4) + z^2 = bv^2 - abw^2 + 4 \\
\text{(by (3.6)) } & \Rightarrow \left(x' - \frac{y'z}{2}\right)^2 - \frac{(y')^2}{4}(au^2) + au^2 + 4 = bv^2 - abw^2 + 4 \\
& \Rightarrow \left(x' - \frac{y'z}{2}\right)^2 - \frac{(y')^2}{4}(au^2) + au^2 = bv^2 - abw^2 \\
& \Rightarrow \left(x' - \frac{y'z}{2}\right)^2 - \frac{(y')^2}{4}(au^2) + au^2 - bv^2 + abw^2 = 0.
\end{aligned}$$

Let  $x = x' - \frac{y'z}{2}$ , and let  $y = \frac{y'u}{2}$ . Then (3.4)–(3.7) are reduced to

$$\begin{aligned}
(3.9) \quad & x^2 - ay^2 + au^2 - bv^2 + abw^2 = 0, \\
& z^2 - 4 = au^2 \quad (a > 0), \\
& \mathbb{Q}\left(x, \frac{y}{u}, z\right) = K \quad (u \neq 0),
\end{aligned}$$

and (3.8) is equivalent to

$$(3.10) \quad x + \frac{yz}{2u} > 2, \quad \frac{y}{u} > 1, \quad z > 2, \quad abw^2 - bv^2 > 4.$$

Now the first statement in Theorem 1.3 follows from the theorem below.

**Theorem 3.1.** *For any real number field  $K$  and any  $a, b \in K$  ( $a > 0$ ), there exists  $x, y, z, u, v, w \in K$  satisfying the following:*

$$(3.11) \quad x^2 - ay^2 + au^2 - bv^2 + abw^2 = 0,$$

$$(3.12) \quad z^2 - 4 = au^2 \quad (a > 0),$$

$$(3.13) \quad \mathbb{Q}\left(x, \frac{y}{u}, z\right) = K,$$

$$(3.14) \quad u \neq 0, \quad x + \frac{yz}{2u} > 2, \quad \frac{y}{u} > 1, \quad z > 2, \quad abw^2 - bv^2 > 4.$$

Here is the outline of the proof. We resolve each equation step by step. First, in **Step 1**, we parameterize solutions of (3.11), using five variables  $m_i$  ( $1 \leq i \leq 5$ ), as given in (3.18). Since (3.11) is a homogeneous equation of degree 2, any constant multiple of (3.18) is again a solution of (3.11), and thus the complete set of solutions is of the form in (3.19) with six degrees of freedom.

Next, in **Step 2**, we resolve the second equation (3.12). Among those six variables obtained in the previous step, by fixing one as a function (this function is induced from (3.12)) of the remaining five variables,  $m_i$  ( $1 \leq i \leq 5$ ), we let (3.12) always hold for any  $m_i$ . In other words, instead of losing one variable, we remove (3.12) in return.

In **Step 3**, we deal with (3.13). This is the most delicate one. Intuitively, for any given real number field  $K$ , the set of generators of  $K$  is dense in  $\mathbb{R}$ . But, in our



case, since each of  $x, \frac{y}{u}$ , and  $z$  is a rational function of  $m_i$ , we need to show there is a particular way to choose  $m_i$  so that one of  $x, \frac{y}{u}$ , and  $z$  generates  $K$ . Specifically, in Lemma 3.2, we use  $\frac{y}{u}$  as a generator of  $K$  and show

$$\mathbb{Q}\left(x, \frac{y}{u}, z\right) = \mathbb{Q}\left(\frac{y}{u}\right) = K.$$

In fact, the lemma will be further reduced to a simpler but equivalent statement (i.e., Lemma 3.4), and this will be proved using subsequent claims.

In **Step 4**, it is shown one can further control the ranges of  $m_i$  to get a solution satisfying (3.14) as well.

*Proof.*

*Step 1.* Having  $(x, y, u, v, w) = (0, 1, 1, 0, 0)$  is as an initial solution, we employ a well-known technique in number theory to find other solutions of (3.11). Let

$$(3.15) \quad \frac{x}{m_1} = \frac{y-1}{m_2} = \frac{u-1}{m_3} = \frac{v}{m_4} = \frac{w}{m_5} = t.$$

Combining (3.15) with (3.11), we get

$$\begin{aligned} & (m_1 t)^2 - a(m_2 t + 1)^2 + a(m_3 t + 1)^2 - b(m_4 t)^2 + ab(m_5 t)^2 = 0 \\ \Rightarrow & (m_1 t)^2 - a((m_2 t)^2 + 2m_2 t + 1) + a((m_3 t)^2 + 2m_3 t + 1) - b(m_4 t)^2 + ab(m_5 t)^2 = 0 \\ \Rightarrow & (m_1 t)^2 - a((m_2 t)^2 + 2m_2 t) + a((m_3 t)^2 + 2m_3 t) - b(m_4 t)^2 + ab(m_5 t)^2 = 0 \\ \Rightarrow & (m_1^2 - am_2^2 + am_3^2 - bm_4^2 + abm_5^2)t^2 - 2a(m_2 - m_3)t = 0 \\ \Rightarrow & (m_1^2 - am_2^2 + am_3^2 - bm_4^2 + abm_5^2)t = 2a(m_2 - m_3) \\ \Rightarrow & t = \frac{2a(m_2 - m_3)}{m_1^2 - am_2^2 + am_3^2 - bm_4^2 + abm_5^2}. \end{aligned} \tag{3.16}$$

So, for any  $m_1, m_2, m_3, m_4, m_5 \in K$  such that

$$(3.17) \quad m_1^2 - am_2^2 + am_3^2 - bm_4^2 + abm_5^2 \neq 0,$$

the following is a solution of (3.11):

$$(3.18) \quad x = m_1 t, \quad y = (m_2 t + 1), \quad u = (m_3 t + 1), \quad v = m_4 t, \quad w = m_5 t,$$

where  $t$  is the one given in (3.16). Furthermore, since (3.11) is homogeneous, for any  $d \in K$ , the following is also a solution of (3.11):

$$(3.19) \quad x = m_1 t d, \quad y = (m_2 t + 1) d, \quad u = (m_3 t + 1) d, \quad v = m_4 t d, \quad w = m_5 t d,$$

where  $m_i$  ( $1 \leq i \leq 5$ ) and  $t$  are the same as above.

*Step 2.* Using the common factor  $d$  in (3.19), we now resolve the second equation (3.12). Since

$$z^2 - 4 = au^2 = a(m_3 t + 1)^2 d^2,$$

by letting

$$z + 2 = a(m_3 t + 1)d \quad \text{and} \quad z - 2 = (m_3 t + 1)d,$$

we get

$$(z + 2) - (z - 2) = 4 = d(m_3 t + 1)(a - 1),$$

and so

$$(3.20) \quad d = \frac{4}{(m_3t + 1)(a - 1)}.$$

Thus, by fixing  $d$  as in (3.20), we can always make (3.12) hold for any  $m_i$  ( $1 \leq i \leq 5$ ) satisfying (3.17) and  $m_3t + 1 \neq 0$ .<sup>9</sup>

*Step 3.* Next we resolve the third condition (3.13). Among three elements  $x, \frac{y}{u}, z$ , we use  $\frac{y}{u}$  as a generator of  $K$ . That is, we show the following lemma.

**Lemma 3.2.** *Let  $x, y, z, u, v$  be as given in (3.19). For any real number field  $K$ , there exists  $m_1, m_2, m_3, m_4, m_5 \in K$  such that*

$$(3.21) \quad \mathbb{Q}\left(x, \frac{y}{u}, z\right) = \mathbb{Q}\left(\frac{y}{u}\right) = K.$$

*More precisely, there exists a generator  $g$  of  $K$  and  $m_1, m_2, m_3, m_4, m_5 \in K$  such that*

$$(3.22) \quad \frac{y}{u} = \frac{m_2t + 1}{m_3t + 1} = g,$$

where  $t = \frac{2a(m_2 - m_3)}{m_1^2 - am_2^2 + am_3^2 - bm_4^2 + abm_5^2}$ .

Before proving the lemma, we first simplify (3.22) as follows:

$$\begin{aligned} & \frac{m_2t + 1}{m_3t + 1} = g \\ \Rightarrow & m_2t + 1 = g(m_3t + 1) \\ \Rightarrow & \frac{2a(m_2 - m_3)m_2}{m_1^2 - am_2^2 + am_3^2 - bm_4^2 + abm_5^2} + 1 = g \left( \frac{2a(m_2 - m_3)m_3}{m_1^2 - am_2^2 + am_3^2 - bm_4^2 + abm_5^2} + 1 \right) \\ \Rightarrow & \frac{2a(m_2 - m_3)m_2 + (m_1^2 - am_2^2 + am_3^2 - bm_4^2 + abm_5^2)}{m_1^2 - am_2^2 + am_3^2 - bm_4^2 + abm_5^2} \\ & = g \left( \frac{2a(m_2 - m_3)m_3 + (m_1^2 - am_2^2 + am_3^2 - bm_4^2 + abm_5^2)}{m_1^2 - am_2^2 + am_3^2 - bm_4^2 + abm_5^2} \right) \\ \Rightarrow & 2a(m_2 - m_3)m_2 + (m_1^2 - am_2^2 + am_3^2 - bm_4^2 + abm_5^2) \\ & = g \left( 2a(m_2 - m_3)m_3 + (m_1^2 - am_2^2 + am_3^2 - bm_4^2 + abm_5^2) \right) \\ \Rightarrow & (g - 1)(m_1^2 - am_2^2 + am_3^2 - bm_4^2 + abm_5^2) + 2ga(m_2m_3 - m_3^2) \\ & - 2a(m_2^2 - m_2m_3) = 0 \\ \Rightarrow & (g - 1)m_1^2 - (g - 1)bm_4^2 + (g - 1)abm_5^2 - (g - 1)am_2^2 + (g - 1)am_3^2 + 2gam_2m_3 \\ & - 2gam_3^2 - 2am_2^2 + 2am_2m_3 = 0 \\ \Rightarrow & (g - 1)m_1^2 - (g - 1)bm_4^2 + (g - 1)abm_5^2 - (g + 1)am_2^2 - (g + 1)am_3^2 + 2gam_2m_3 \\ & + 2am_2m_3 = 0 \\ \Rightarrow & (g - 1)m_1^2 - (g - 1)bm_4^2 + (g - 1)abm_5^2 - (g + 1)a(m_2^2 - 2am_2m_3 + m_3^2) = 0 \\ \Rightarrow & (g - 1)m_1^2 - (g - 1)bm_4^2 + (g - 1)abm_5^2 - (g + 1)a(m_2 - m_3)^2 = 0 \\ \Rightarrow & m_1^2 - bm_4^2 + abm_5^2 - \frac{a(g + 1)}{g - 1}(m_2 - m_3)^2 = 0 \end{aligned}$$

<sup>9</sup>By (2.2), we can assume  $a > 1$ . We will talk more about this in **Step 4**.

$$\begin{aligned}
 &\Rightarrow m_1^2 - bm_4^2 + abm_5^2 - a\left(1 + \frac{2}{g-1}\right)(m_2 - m_3)^2 = 0 \\
 &\Rightarrow \frac{1}{a}m_1^2 - \frac{b}{a}m_4^2 + bm_5^2 - \left(1 + \frac{2}{g-1}\right)(m_2 - m_3)^2 = 0 \\
 &\Rightarrow \frac{1}{a}\left(\frac{m_1}{m_2 - m_3}\right)^2 - \frac{b}{a}\left(\frac{m_4}{m_2 - m_3}\right)^2 + b\left(\frac{m_5}{m_2 - m_3}\right)^2 - \left(1 + \frac{2}{g-1}\right) = 0. \\
 &\Rightarrow \frac{1}{a}\left(\frac{m_1}{m_2 - m_3}\right)^2 - \frac{b}{a}\left(\frac{m_4}{m_2 - m_3}\right)^2 + b\left(\frac{m_5}{m_2 - m_3}\right)^2 = 1 + \frac{2}{g-1}.
 \end{aligned}
 \tag{3.23}$$

Thus the following lemma implies Lemma 3.2.

**Lemma 3.3.** *Let  $K$  be any real number field, and let  $a, b$  be arbitrary nonzero elements in  $K$  such that  $a > 0$ . Then there exist a generator  $g$  of  $K$  and  $m_1, m_2, m_3, m_4, m_5 \in K$  satisfying*

$$\frac{1}{a}\left(\frac{m_1}{m_2 - m_3}\right)^2 - \frac{b}{a}\left(\frac{m_4}{m_2 - m_3}\right)^2 + b\left(\frac{m_5}{m_2 - m_3}\right)^2 = 1 + \frac{2}{g-1}.
 \tag{3.24}$$

By changing variables as

$$\begin{aligned}
 &(3.25) \\
 &a' = \frac{1}{a}, \quad b' = b, \quad x = \frac{m_1}{m_2 - m_3}, \quad z = \frac{m_4}{m_2 - m_3}, \quad y = \frac{m_5}{m_2 - m_3}, \quad g' = 1 + \frac{2}{g-1},
 \end{aligned}$$

Lemma 3.3 now follows by the lemma below.

**Lemma 3.4.** *Let  $K$  be any real number field, and let  $a', b'$  be arbitrary nonzero elements in  $K$ . Then there exist a generator  $g'$  of  $K$  and  $x, y, z \in K$  satisfying*

$$a'x^2 + b'y^2 - a'b'z^2 = g'.
 \tag{3.26}$$

Before proving Lemma 3.4, we first state two claims which will be used in the proof.

*Claim 3.5.* Let  $\alpha \in \bar{\mathbb{Q}}$ . If a minimal polynomial of  $\alpha$  contains a nonzero term of odd degree, then  $\mathbb{Q}(\alpha) = \mathbb{Q}(\alpha^2)$ . Thus, for any real number field  $K$ , the set of generators of  $K$  satisfying this property is dense in  $\mathbb{R}$ .

*Proof.* Let  $f(x) = 0$  be a minimal polynomial of  $\alpha$ . Since it contains a nonzero term of odd degree, we can express  $f$  as follows:

$$\begin{aligned}
 f(x) &= x(a_{2n}x^{2n} + a_{2n-1}x^{2n-1} + \cdots + a_2x^2 + a_0) \\
 &\quad + (b_{2m}x^{2m} + b_{2m-1}x^{2m-1} + \cdots + b_2x^2 + b_0).
 \end{aligned}$$

Since  $f(x)$  is a minimal polynomial of  $\alpha$ ,  $a_{2n}\alpha^{2n} + a_{2n-1}\alpha^{2n-1} + \cdots + a_2\alpha^2 + a_0 \neq 0$ , and so

$$\alpha = -\frac{b_{2m}\alpha^{2m} + b_{2m-1}\alpha^{2m-1} + \cdots + b_2\alpha^2 + b_0}{a_{2n}\alpha^{2n} + a_{2n-1}\alpha^{2n-1} + \cdots + a_2\alpha^2 + a_0},$$

which implies  $\mathbb{Q}(\alpha) = \mathbb{Q}(\alpha^2)$ .

Let  $\alpha$  be a generator of  $K$ . Then, for any nonzero  $r \in \mathbb{Q}$ , either a minimal polynomial of  $\alpha$  or a minimal polynomial of  $\alpha + r$  contains a nonzero term of odd degree. The second statement easily follows.  $\square$

*Claim 3.6.* Let  $\alpha, \beta$  be algebraic numbers. Then, except for finitely many  $r \in \mathbb{Q}$ , it always satisfies  $\mathbb{Q}(\alpha + r\beta) = \mathbb{Q}(\alpha, \beta)$ .

*Proof.* This is a well-known fact and is used to prove the existence of a primitive element in a number field. See [2], for instance, for a proof.  $\square$

*Proof of Lemma 3.4.* By Claim 3.6, there exists  $(x_0, y_0) \in \mathbb{Q}^2$  such that  $\mathbb{Q}(a'x_0^2 + b'y_0^2) = \mathbb{Q}(a', b')$ . Let  $F = \mathbb{Q}(a', b')$ , and let  $z_0$  be an element of  $K$  such that  $K = F(z_0^2)$  is obtained from Claim 3.5. By Claim 3.6, we can further assume that  $x_0$  and  $y_0$  satisfy  $\mathbb{Q}(a'x_0^2 + b'y_0^2 - a'b'z_0^2) = \mathbb{Q}(a'x_0^2 + b'y_0^2, a'b'z_0^2)$ . Now the following equalities hold:

$$\begin{aligned} \mathbb{Q}(a'x_0^2 + b'y_0^2 - a'b'z_0^2) &= \mathbb{Q}(a'x_0^2 + b'y_0^2, a'b'z_0^2) = \mathbb{Q}(a', b')(a'b'z_0^2) = \mathbb{Q}(a', b')(z_0^2) \\ &= F(z_0^2) = K. \end{aligned}$$

Taking  $g' = a'x_0^2 + b'y_0^2 - a'b'z_0^2$ , we get the desired result.  $\square$

*Step 4.* Now we find a solution satisfying (3.14). For a sufficiently small number  $\epsilon > 0$ , using (2.2), we first assume that  $a$  and  $b$  satisfy

$$(3.27) \quad 1 < a, b < 1 + \epsilon.$$

Since  $a > 1$ , we have  $z^2 > 4$  by (3.12). Also, if  $\frac{y}{u} > 1$  and  $z > 2$ , then  $\frac{yz}{2u} > 1$ . Thus (3.14) can be replaced by

$$(3.28) \quad u \neq 0, \quad x > 1, \quad \frac{y}{u} > 1, \quad abw^2 - bv^2 > 4.$$

Following the formulas given in (3.19) and (3.28) is equivalent to

$$(3.29) \quad (m_3t + 1)d \neq 0, \quad m_1td > 1, \quad \frac{m_2t + 1}{m_3t + 1} > 1, \quad ab(m_5td)^2 - b(m_4td)^2 > 4.$$

By the proof of Lemma 3.4, the set of

$$\left( \frac{m_1}{m_2 - m_3}, \frac{m_4}{m_2 - m_3}, \frac{m_5}{m_2 - m_3} \right)$$

such that

$$\frac{1}{a} \left( \frac{m_1}{m_2 - m_3} \right)^2 - \frac{b}{a} \left( \frac{m_4}{m_2 - m_3} \right)^2 + b \left( \frac{m_5}{m_2 - m_3} \right)^2$$

is a generator of  $K$  is dense in  $\mathbb{R}^3$ . Thus for sufficiently large  $L > 0$ , we can pick  $m_i$  satisfying

$$(3.30) \quad L < m_1, m_2, m_4 < L + \epsilon, \quad 2L < m_5 < 2L + \epsilon, \quad 0 < m_3 < \epsilon.$$

Then

$$m_1^2 - a(m_2^2 - m_3^3) - bm_4^2 + abm_5^2 < (L + \epsilon)^2 - (L^2 - \epsilon^2) - L^2 + (1 + \epsilon)^2(2L + \epsilon)^2 < 4L^2$$

and

$$m_1^2 - a(m_2^2 - m_3^3) - bm_4^2 + abm_5^2 > L^2 - (1 + \epsilon)(L + \epsilon)^2 - (1 + \epsilon)(L + \epsilon)^2 + (2L)^2 > 2L^2.$$

Thus

$$(3.31) \quad \frac{1}{3L} < \frac{1}{2L} \left( 1 - \frac{\epsilon}{L} \right) = \frac{2(L - \epsilon)}{4L^2} < t = \frac{2a(m_2 - m_3)}{m_1^2 - a(m_2^2 - m_3^3) - bm_4^2 + abm_5^2} < \frac{2(1 + \epsilon)(L + \epsilon)}{2L^2} < \frac{2}{L}$$

and

$$(3.32) \quad 1 < m_3t + 1 < \epsilon \frac{2}{L} + 1.$$

Now (3.31) and (3.32) imply

$$d = \frac{1}{(m_3t + 1)(a - 1)} > \frac{1}{\left(\frac{2\epsilon}{L} + 1\right)\epsilon} > \frac{1}{2\epsilon}.$$

Clearly we have  $(m_3t + 1)d \neq 0$ , and

$$m_1td > L\left(\frac{1}{3L}\right)\left(\frac{1}{2\epsilon}\right) = \frac{1}{6\epsilon} > 1$$

for sufficiently small  $\epsilon$ . Since  $m_2 > m_3$ ,  $\frac{m_2t+1}{m_3t+1} > 1$ . Lastly,

$$\begin{aligned} ab(m_5td)^2 - b(m_4td)^2 &= t^2d^2(abm_5^2 - bm_4^2) > \left(\frac{1}{3L}\right)^2\left(\frac{1}{2\epsilon}\right)^2(4L^2 - (1 + \epsilon)(L + \epsilon)^2) \\ &> \frac{1}{18\epsilon^2} > 4 \end{aligned}$$

since  $\epsilon$  is sufficiently small.

Thus it satisfies (3.29) and this completes the proof of Theorem 3.1. □

*Remark.* For later use, we introduce a simple criteria to generate infinitely many different solutions from an initial solution. This method will be used in the next section. For any real number field  $K$  and  $a, b \in K$  ( $a > 0$ ), let  $m_i = m_{i_0} \in K$  ( $1 \leq i \leq 5$ ) be numbers obtained by following the above proof of Theorem 3.1. (That is, we get  $x, y, z, u, v, w$  satisfying (3.11)–(3.14) by letting  $m_i = m_{i_0}$  in (3.19).) Then

$$\frac{1}{a}\left(\frac{m_{1_0}}{m_{2_0} - m_{3_0}}\right)^2 - \frac{b}{a}\left(\frac{m_{4_0}}{m_{2_0} - m_{3_0}}\right)^2 + b\left(\frac{m_{5_0}}{m_{2_0} - m_{3_0}}\right)^2$$

is a generator of  $K$ , and, by (3.23), we have

$$(3.33) \quad \frac{1}{a}\left(\frac{m_{1_0}}{m_{2_0} - m_{3_0}}\right)^2 - \frac{b}{a}\left(\frac{m_{4_0}}{m_{2_0} - m_{3_0}}\right)^2 + b\left(\frac{m_{5_0}}{m_{2_0} - m_{3_0}}\right)^2 = 1 + \frac{2}{\frac{y_0}{u_0} - 1},$$

where  $y_0$  and  $u_0$  are the values of  $y$  and  $u$  when  $m_i = m_{i_0}$ . For  $r \in \mathbb{Q} \setminus \{0\}$ , since

$$\frac{1}{a}\left(\frac{rm_{1_0}}{m_{2_0} - m_{3_0}}\right)^2 - \frac{b}{a}\left(\frac{rm_{4_0}}{m_{2_0} - m_{3_0}}\right)^2 + b\left(\frac{rm_{5_0}}{m_{2_0} - m_{3_0}}\right)^2$$

is also a generator of  $K$ , we get another  $x, y, z, u, v, w$  satisfying (3.11)–(3.13) from

$$(3.34) \quad (m_1, m_2, m_3, m_4, m_5) = (rm_{1_0}, m_{2_0}, m_{3_0}, rm_{4_0}, rm_{5_0}).$$

Furthermore, if  $r$  is sufficiently close to 1, then the solution satisfies (3.14) as well. Thus, in this way, we can produce infinitely many different solutions, which are all close to the initial solution. Finally, remark that if  $y_r$  and  $u_r$  are the values of  $y$  and  $u$  when  $m_i$  ( $1 \leq i \leq 5$ ) are as given in (3.34), then the following two equalities hold:

$$(3.35) \quad \frac{1}{a}\left(\frac{rm_{1_0}}{m_{2_0} - m_{3_0}}\right)^2 - \frac{b}{a}\left(\frac{rm_{4_0}}{m_{2_0} - m_{3_0}}\right)^2 + b\left(\frac{rm_{5_0}}{m_{2_0} - m_{3_0}}\right)^2 = 1 + \frac{2}{\frac{y_r}{u_r} - 1},$$

$$(3.36) \quad r^2\left(1 + \frac{2}{\frac{y_0}{u_0} - 1}\right) = 1 + \frac{2}{\frac{y_r}{u_r} - 1}$$

(the first one follows from (3.23), and the second one from (3.33) and (3.35)).

## 4. PROOF OF THEOREM 1.3 (PART II)

Now we complete the proof of Theorem 1.3. We will show that both the trace field and the invariant trace field of  $\mathcal{S}$  can be made equal in the proof of Theorem 3.1. Remark that once the trace field is equal to the invariant trace field, then the quaternion algebra is also equal to the invariant quaternion algebra.<sup>10</sup>

In the previous section, we used the trace of  $\sigma$  (recall  $\text{tr } \sigma = 2y/u$ ) to realize an arbitrary given real number field  $K$  as the trace field of  $\mathcal{S}$ . Since the invariant trace field of  $\mathcal{S}$  contains  $\text{tr } \sigma^2$  and

$$\text{tr } \sigma^2 = (\text{tr } \sigma)^2 - 4,$$

the following strengthened version of Theorem 3.1 implies the last statement of Theorem 1.3.

**Theorem 4.1.** *Theorem 3.1 still holds after replacing (3.13) by*

$$\mathbb{Q}\left(\frac{y}{u}\right) = \mathbb{Q}\left(\frac{y^2}{u^2}\right) = K.$$

Intuitively this theorem is clear since we have a dense set of solutions satisfying (3.11)–(3.14) in Theorem 3.1. But, for the sake of completeness, we will give the complete proof below. Before proving the theorem, we prove the following lemma first.

**Lemma 4.2.** *Let  $\alpha$  be an algebraic number, and let  $f(x) = a_n x^n + \cdots + a_0$  be a minimal polynomial of  $\alpha$ . Then  $(x-1)^n f\left(1 + \frac{2}{x-1}\right)$  is a minimal polynomial of  $1 + \frac{2}{\alpha-1}$ , and the coefficient of  $x^{n-1}$  in  $(x-1)^n f\left(1 + \frac{2}{x-1}\right)$  is*

$$\sum_{i=0}^n (-n + 2i)a_i.$$

*Proof.* Let  $\beta = 1 + \frac{2}{\alpha-1}$ . Then  $\alpha = 1 + \frac{2}{\beta-1}$ , and so the first part follows easily.

We next expand  $f\left(1 + \frac{2}{x-1}\right)$  as below:

$$\begin{aligned} & a_n \left(1 + \frac{2}{x-1}\right)^n + a_{n-1} \left(1 + \frac{2}{x-1}\right)^{n-1} + \cdots + a_1 \left(1 + \frac{2}{x-1}\right) + a_0 \\ &= a_n \left(1 + n \left(\frac{2}{x-1}\right) + \cdots + n \left(\frac{2}{x-1}\right)^{n-1} + \left(\frac{2}{x-1}\right)^n\right) \\ (4.1) \quad & + a_{n-1} \left(1 + (n-1) \left(\frac{2}{x-1}\right) + \cdots + (n-1) \left(\frac{2}{x-1}\right)^{n-2} + \left(\frac{2}{x-1}\right)^{n-1}\right) \\ & \cdots \\ & + a_1 \left(1 + \left(\frac{2}{x-1}\right)\right) + a_0. \end{aligned}$$

---

<sup>10</sup>Since both the quaternion algebra and the invariant quaternion algebra are then defined over the same field and the invariant quaternion algebra is a subalgebra of the quaternion algebra, both are the same.

Multiplying (4.1) by  $(x-1)^n$ ,  $(x-1)^n f\left(1 + \frac{2}{x-1}\right)$  is equal to

$$(4.2) \quad \begin{aligned} & a_n \left( (x-1)^n + n \cdot 2(x-1)^{n-1} + \cdots + n \cdot 2^{n-1}(x-1) + 2^n \right) \\ & + a_{n-1} \left( (x-1)^n + (n-1)2(x-1)^{n-1} + \cdots + (n-1)2^{n-2}(x-1)^2 + 2^{n-1}(x-1) \right) \\ & \cdots \\ & + a_1 \left( (x-1)^n + 2(x-1)^{n-1} \right) + a_0(x-1)^n. \end{aligned}$$

The coefficient of  $x^{n-1}$  in (4.2) is

$$a_n(-n + n \cdot 2) + a_{n-1}(-n + (n-1)2) + \cdots + a_1(-n + 2) + a_0(-n),$$

which is equal to

$$(4.3) \quad \sum_{i=0}^n (-n + 2i)a_i.$$

□

Now we are ready to prove Theorem 4.1.

*Proof of Theorem 4.1.* Let  $y = y_0$ ,  $u = u_0$  be the pair given in the Remark in the previous section (after the proof of Theorem 3.1). Let  $f(x)$  be a minimal polynomial of  $1 + \frac{2}{\frac{y_0}{u_0}-1}$ . Then, by Lemma 4.2,

$$(4.4) \quad (x-1)^{\deg f} f\left(1 + \frac{2}{x-1}\right)$$

is a minimal polynomial of  $\frac{y_0}{u_0}$ . If (4.4) contains a nonzero term of odd degree, then  $\mathbb{Q}\left(\frac{y_0}{u_0}\right) = \mathbb{Q}\left(\frac{y_0^2}{u_0^2}\right)$  by Claim 3.5, and so we are done.

Otherwise, suppose the degrees of all the nonzero terms of (4.4) are even. Let  $y_r$  and  $u_r$  be the same ones given in the remark in Section 3, and let  $f(x)$  be of the form  $a_{2n}x^{2n} + \cdots + a_0$ . Then

$$(4.5) \quad \begin{aligned} f\left(\frac{x}{r^2}\right) &= a_{2n}\left(\frac{x}{r^2}\right)^{2n} + a_{2n-1}\left(\frac{x}{r^2}\right)^{2n-1} + \cdots + a_1\left(\frac{x}{r^2}\right) + a_0 \\ &= \left(\frac{a_{2n}}{r^{4n}}\right)x^{2n} + \left(\frac{a_{2n-1}}{r^{4n-2}}\right)x^{2n-1} + \cdots + \left(\frac{a_1}{r^2}\right)x + a_0 \end{aligned}$$

is a minimal polynomial of  $r^2\left(1 + \frac{2}{\frac{y_0}{u_0}-1}\right)$ . To simplify the notation, we denote the polynomial in (4.5) by  $g(x)$  and  $r^2\left(1 + \frac{2}{\frac{y_0}{u_0}-1}\right)$  by  $\alpha$ . Then  $\alpha = 1 + \frac{2}{\frac{y_r}{u_r}-1}$  by (3.36), and so  $\frac{y_r}{u_r} = 1 + \frac{2}{\alpha-1}$ . Since  $g(x)$  is a minimal polynomial of  $\alpha$ ,  $(x-1)^{2n}g\left(1 + \frac{2}{x-1}\right)$  is a minimal polynomial of  $\frac{y_r}{u_r}$  by Lemma 4.2. By the same lemma, the coefficient of  $x^{2n-1}$  in  $(x-1)^{2n}g\left(1 + \frac{2}{x-1}\right)$  is

$$(4.6) \quad \sum_{i=0}^{2n} (-2n + 2i) \frac{a_i}{r^{2i}}.$$

Clearly there are infinitely many  $r \in \mathbb{Q}$  making (4.6) nonzero. By Claim 3.5, we have  $\mathbb{Q}\left(\frac{y_r}{u_r}\right) = \mathbb{Q}\left(\frac{y_r^2}{u_r^2}\right)$  for those  $r$ . This completes the proof. □

## 5. PROOF OF THEOREM 2.3

The proof of Theorem 2.3 is based on explicit computations. Note that we already know the traces of the first six elements in (2.8).<sup>11</sup> So, to prove the theorem, it is enough to show that the traces of the following elements are contained in  $\mathbb{Q}(r, s, t)$ :

$$(5.1) \quad \rho\rho', \rho\sigma', \sigma\rho', \sigma\sigma', \rho\sigma\rho', \rho\sigma\sigma', \rho\rho'\sigma', \sigma\rho'\sigma'.$$

Also, by the symmetry between (2.5) and (2.7), we can further reduce (5.1) to the following five elements:

$$(5.2) \quad \rho\rho', \rho\sigma', \sigma\sigma', \rho\sigma\rho', \rho\sigma\sigma'.$$

Before computing the traces of (5.2), we first prove a simple lemma which will be used subsequently in the section. When two matrices are represented in terms of the quaternion basis, the trace of their product can be simply computed as the following lemma shows.

**Lemma 5.1.** *Let*

$$\begin{aligned} A &= a_0\mathbf{1} + a_1\mathbf{I} + a_2(\mathbf{J} + \mathbf{K}) + a_3(\mathbf{J} - \mathbf{K}), \\ B &= b_0\mathbf{1} + b_1\mathbf{I} + b_2(\mathbf{J} + \mathbf{K}) + b_3(\mathbf{J} - \mathbf{K}). \end{aligned}$$

*Then their product  $AB$  is of the form*

$$(5.3) \quad \begin{aligned} &(a_0b_0 + a_1b_1 + 2a_2b_3 + 2a_3b_2)\mathbf{1} + b_0(a_1\mathbf{I} + a_2(\mathbf{J} + \mathbf{K}) + a_3(\mathbf{J} - \mathbf{K})) \\ &\quad + a_0(b_1\mathbf{I} + b_2(\mathbf{J} + \mathbf{K}) + b_3(\mathbf{J} - \mathbf{K})) \\ &\quad + (2a_2b_3 - 2a_3b_2)\mathbf{I} + (a_1b_2 - a_2b_1)(\mathbf{J} + \mathbf{K}) + (a_3b_1 - a_1b_3)(\mathbf{J} - \mathbf{K}), \end{aligned}$$

*and (thus) the trace of  $AB$  is*

$$(5.4) \quad 2(a_0b_0 + a_1b_1 + 2a_2b_3 + 2a_3b_2).$$

*Proof.* Since

$$A = \begin{pmatrix} a_0 + a_1 & 2a_2 \\ 2a_3 & a_0 - a_1 \end{pmatrix} \text{ and } B = \begin{pmatrix} b_0 + b_1 & 2b_2 \\ 2b_3 & b_0 - b_1 \end{pmatrix},$$

$AB$  is equal to

$$\begin{aligned} &\begin{pmatrix} (a_0 + a_1)(b_0 + b_1) + 4a_2b_3 & (a_0 + a_1)2b_2 + 2a_2(b_0 - b_1) \\ 2a_3(b_0 + b_1) + (a_0 - a_1)2b_3 & 4a_3b_2 + (a_0 - a_1)(b_0 - b_1) \end{pmatrix} \\ &= \begin{pmatrix} a_0b_0 + a_1b_0 + a_0b_1 + a_1b_1 + 4a_2b_3 & 2a_0b_2 + 2a_1b_2 + 2a_2b_0 - 2a_2b_1 \\ 2a_3b_0 + 2a_3b_1 + 2a_0b_3 - 2a_1b_3 & 4a_3b_2 + a_0b_0 - a_1b_0 - a_0b_1 + a_1b_1 \end{pmatrix} \\ &= \begin{pmatrix} a_0b_0 + a_1b_0 + a_0b_1 + a_1b_1 + 4a_2b_3 & 0 \\ 0 & 4a_3b_2 + a_0b_0 - a_1b_0 - a_0b_1 + a_1b_1 \end{pmatrix} \\ &\quad + \begin{pmatrix} 0 & 2a_0b_2 + 2a_1b_2 + 2a_2b_0 - 2a_2b_1 \\ 2a_3b_0 + 2a_3b_1 + 2a_0b_3 - 2a_1b_3 & 0 \end{pmatrix} \end{aligned}$$

---

<sup>11</sup>That is,  $2r = \text{tr } \rho = \text{tr } \rho'$ ,  $2s = \text{tr } \sigma = \text{tr } \sigma'$ , and  $2t = \text{tr } \rho\sigma = \text{tr } \rho'\sigma'$ .



$$\begin{aligned}
 &= \begin{pmatrix} a_0b_0 + a_1b_1 + 2a_2b_3 & 0 \\ 0 & 2a_3b_2 + a_0b_0 + a_1b_1 \end{pmatrix} \\
 &+ \begin{pmatrix} a_1b_0 + a_0b_1 + 2a_2b_3 & 0 \\ 0 & 2a_3b_2 - a_1b_0 - a_0b_1 \end{pmatrix} \\
 &+ \begin{pmatrix} 0 & 2a_0b_2 + 2a_1b_2 + 2a_2b_0 - 2a_2b_1 \\ 0 & 0 \end{pmatrix} \\
 &+ \begin{pmatrix} 0 & 0 \\ 2a_3b_0 + 2a_3b_1 + 2a_0b_3 - 2a_1b_3 & 0 \end{pmatrix} \\
 &= \begin{pmatrix} a_0b_0 + a_1b_1 + 2a_2b_3 + 2a_3b_2 & 0 \\ 0 & 2a_3b_2 + a_0b_0 + a_1b_1 + 2a_2b_3 \end{pmatrix} \\
 &+ \begin{pmatrix} a_1b_0 + a_0b_1 + 2a_2b_3 - 2a_3b_2 & 0 \\ 0 & 2a_3b_2 - a_1b_0 - a_0b_1 - 2a_2b_3 \end{pmatrix} \\
 &+ \begin{pmatrix} 0 & 2a_0b_2 + 2a_1b_2 + 2a_2b_0 - 2a_2b_1 \\ 0 & 0 \end{pmatrix} \\
 &+ \begin{pmatrix} 0 & 0 \\ 2a_3b_0 + 2a_3b_1 + 2a_0b_3 - 2a_1b_3 & 0 \end{pmatrix} \\
 &= \begin{pmatrix} a_0b_0 + a_1b_1 + 2a_2b_3 + 2a_3b_2 & 0 \\ 0 & a_0b_0 + a_1b_1 + 2a_2b_3 + 2a_3b_2 \end{pmatrix} \\
 &+ \begin{pmatrix} a_0b_1 & 0 \\ 0 & -a_0b_1 \end{pmatrix} + \begin{pmatrix} a_1b_0 & 0 \\ 0 & -a_1b_0 \end{pmatrix} + \begin{pmatrix} 2a_2b_3 - 2a_3b_2 & 0 \\ 0 & 2a_3b_2 - 2a_2b_3 \end{pmatrix} \\
 &+ \begin{pmatrix} 0 & 2a_0b_2 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 2a_2b_0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 2a_1b_2 - 2a_2b_1 \\ 0 & 0 \end{pmatrix} \\
 &+ \begin{pmatrix} 0 & 0 \\ 2a_0b_3 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 2a_3b_0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 2a_3b_1 - 2a_1b_3 & 0 \end{pmatrix}.
 \end{aligned}$$

Since

$$\mathbf{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \mathbf{I} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \mathbf{J} + \mathbf{K} = \begin{pmatrix} 0 & 2 \\ 0 & 0 \end{pmatrix}, \quad \text{and} \quad \mathbf{J} - \mathbf{K} = \begin{pmatrix} 0 & 0 \\ 2 & 0 \end{pmatrix},$$

the last given formula above is equal to

$$\begin{aligned}
 &(a_0b_0 + a_1b_1 + 2a_2b_3 + 2a_3b_2)\mathbf{1} + (a_0b_1)\mathbf{I} + (a_1b_0)\mathbf{I} + (2a_2b_3 - 2a_3b_2)\mathbf{I} \\
 &+ a_0b_2(\mathbf{J} + \mathbf{K}) + a_2b_0(\mathbf{J} + \mathbf{K}) + (a_1b_2 - a_2b_1)(\mathbf{J} + \mathbf{K}) + a_0b_3(\mathbf{J} - \mathbf{K}) \\
 &+ a_3b_0(\mathbf{J} - \mathbf{K}) + (a_3b_1 - a_1b_3)(\mathbf{J} - \mathbf{K}),
 \end{aligned}$$

which is the same as (5.3). □

Now we prove Theorem 2.3. We first compute the traces of the first three elements in (5.2).

**Lemma 5.2.** *The traces of  $\rho\rho'$ ,  $\rho\sigma'$ , and  $\sigma\sigma'$  are contained in  $\mathbb{Q}(r, s, t)$ .*

*Proof.* Recall the formulas of  $\rho$  and  $\rho'$  in (2.5) and (2.7). By Lemma 5.1, the trace of  $\rho\rho'$  is equal to

$$\begin{aligned} & 2\left\{r^2 + \left(\frac{r(c+1)}{\sqrt{c^2-1}}\right)\left(\frac{r(c+1)}{\sqrt{c^2-1}}\right)\right. \\ & + 2\left(-\frac{\tilde{M}(2rs-t+(c+\sqrt{c^2-1})t)}{2(c-1+2s^2)}\right)\left(-\frac{2rs-t+(c-\sqrt{c^2-1})t}{2\tilde{M}(c-1)}\right) \\ & \left.+ 2\left(\frac{2rs-t+(c-\sqrt{c^2-1})t}{2\tilde{M}(c-1)}\right)\left(\frac{\tilde{M}(2rs-t+(c+\sqrt{c^2-1})t)}{2(c-1+2s^2)}\right)\right\}, \end{aligned}$$

which can be simplified as

$$\begin{aligned} & 2r^2 + \frac{2r^2(c+1)^2}{c^2-1} + \frac{(2rs-t+(c+\sqrt{c^2-1})t)(2rs-t+(c-\sqrt{c^2-1})t)}{(c-1+2s^2)(c-1)} \\ & + \frac{(2rs-t+(c-\sqrt{c^2-1})t)(2rs-t+(c+\sqrt{c^2-1})t)}{(c-1)(c-1+2s^2)} \\ = & 2r^2 + \frac{2r^2(c+1)^2}{c^2-1} + \frac{((2rs-t+tc)+t\sqrt{c^2-1})((2rs-t+tc)-t\sqrt{c^2-1})}{(c-1+2s^2)(c-1)} \\ & + \frac{((2rs-t+tc)-t\sqrt{c^2-1})((2rs-t+tc)+t\sqrt{c^2-1})}{(c-1)(c-1+2s^2)} \\ = & 2r^2 + \frac{2r^2(c+1)^2}{c^2-1} + \frac{2((2rs-t+ct)^2 - (c^2-1)t^2)}{(c-1+2s^2)(c-1)}. \end{aligned}$$

Clearly this is contained in  $\mathbb{Q}(r, s, t)$ . (Recall  $c \in \mathbb{Q}(r, s, t)$ .)

Similarly, the trace of  $\rho\sigma'$  is equal to

$$\begin{aligned} & 2\left\{rs + \left(\frac{r(c+1)}{\sqrt{c^2-1}}\right)\left(-\frac{s(c+1)}{\sqrt{c^2-1}}\right)\right. \\ & + 2\left(-\frac{\tilde{M}(2rs-t+(c+\sqrt{c^2-1})t)}{2(c-1+2s^2)}\right)\left(\frac{c-1+2s^2}{2\tilde{M}(c-1)}\right) \\ & \left.+ 2\left(\frac{2rs-t+(c-\sqrt{c^2-1})t}{2\tilde{M}(c-1)}\right)\left(-\frac{\tilde{M}}{2}\right)\right\}, \end{aligned}$$

which can be simplified as

$$\begin{aligned} & 2rs - \frac{2rs(c+1)^2}{c^2-1} - \frac{2rs-t+(c+\sqrt{c^2-1})t}{c-1} - \frac{2rs-t+(c-\sqrt{c^2-1})t}{c-1} \\ = & 2rs - \frac{2rs(c+1)}{c-1} - \frac{2(2rs-t+ct)}{c-1}. \end{aligned}$$

This is also an element of  $\mathbb{Q}(r, s, t)$ .

Lastly the trace of  $\sigma\sigma'$  is equal to

$$\begin{aligned} & 2 \left\{ s^2 + \left( -\frac{s(c+1)}{\sqrt{c^2-1}} \right) \left( -\frac{s(c+1)}{\sqrt{c^2-1}} \right) + 2 \left( \frac{\tilde{M}}{2} \right) \left( \frac{c-1+2s^2}{2\tilde{M}(c-1)} \right) \right. \\ & \qquad \qquad \qquad \left. + 2 \left( -\frac{c-1+2s^2}{2\tilde{M}(c-1)} \right) \left( -\frac{\tilde{M}}{2} \right) \right\} \\ &= 2s^2 + \frac{2s^2(c+1)^2}{c^2-1} + \frac{c-1+2s^2}{(c-1)} + \frac{c-1+2s^2}{(c-1)} \\ &= 2s^2 + \frac{2s^2(c+1)}{c-1} + \frac{2(c-1+2s^2)}{(c-1)}, \end{aligned}$$

which is contained in  $\mathbb{Q}(r, s, t)$  as well. This completes the proof.  $\square$

Now we compute the traces of  $\rho\sigma\rho'$  and  $\rho\sigma\sigma'$ . To do so, we first need the explicit formula of  $\rho\sigma$ .

**Lemma 5.3.**  $\rho\sigma$  is

$$\begin{aligned} & t\mathbf{1} + \frac{t\sqrt{c^2-1}}{c-1}\mathbf{I} + \frac{(c+1+\sqrt{c^2-1})\tilde{M}(r(c-1)+st-st(c+\sqrt{c^2-1}))}{2\sqrt{c^2-1}(c-1+2s^2)}(\mathbf{J}+\mathbf{K}) \\ & + \frac{(c+1-\sqrt{c^2-1})(r(c-1)+st-st(c-\sqrt{c^2-1}))}{2\tilde{M}(c-1)\sqrt{c^2-1}}(\mathbf{J}-\mathbf{K}). \end{aligned}$$

*Proof.* We restate the formulas of  $\rho$  and  $\sigma$  given in (2.5):

$$\begin{aligned} \rho &= r\mathbf{1} + \frac{r(c+1)}{\sqrt{c^2-1}}\mathbf{I} - \frac{\tilde{M}(2rs-t+(c+\sqrt{c^2-1})t)}{2(c-1+2s^2)}(\mathbf{J}+\mathbf{K}) \\ & \quad + \frac{2rs-t+(c-\sqrt{c^2-1})t}{2\tilde{M}(c-1)}(\mathbf{J}-\mathbf{K}), \\ \sigma &= s\mathbf{1} - \frac{s(c+1)}{\sqrt{c^2-1}}\mathbf{I} + \frac{\tilde{M}}{2}(\mathbf{J}+\mathbf{K}) - \frac{c-1+2s^2}{2\tilde{M}(c-1)}(\mathbf{J}-\mathbf{K}). \end{aligned}$$

To simplify the notation, we abbreviate the above  $\rho$  and  $\sigma$  as

$$\begin{aligned} \rho &= a_0\mathbf{1} + a_1\mathbf{I} + a_2(\mathbf{J}+\mathbf{K}) + a_3(\mathbf{J}-\mathbf{K}), \\ \sigma &= b_0\mathbf{1} + b_1\mathbf{I} + b_2(\mathbf{J}+\mathbf{K}) + b_3(\mathbf{J}-\mathbf{K}). \end{aligned}$$

Note that  $a_0b_0 + a_1b_1 + 2a_2b_3 + 2a_3b_2 = t$  (since we got the matrices in (2.5) by initially assuming that the trace of  $\rho\sigma$  is  $2t$ ). To get  $\rho\sigma$ , we now compute each term appearing in (5.3) explicitly as follows.

$$\begin{aligned}
& \text{(i)} \quad b_0(a_1\mathbf{I} + a_2(\mathbf{J} + \mathbf{K}) + a_3(\mathbf{J} - \mathbf{K})) + a_0(b_1\mathbf{I} + b_2(\mathbf{J} + \mathbf{K}) + b_3(\mathbf{J} - \mathbf{K})) \\
&= s \left( \frac{r(c+1)}{\sqrt{c^2-1}}\mathbf{I} - \frac{\tilde{M}(2rs-t+(c+\sqrt{c^2-1})t)}{2(c-1+2s^2)}(\mathbf{J} + \mathbf{K}) \right. \\
&\quad \left. + \frac{2rs-t+(c-\sqrt{c^2-1})t}{2\tilde{M}(c-1)}(\mathbf{J} - \mathbf{K}) \right) \\
&\quad + r \left( -\frac{s(c+1)}{\sqrt{c^2-1}}\mathbf{I} + \frac{\tilde{M}}{2}(\mathbf{J} + \mathbf{K}) - \frac{c-1+2s^2}{2\tilde{M}(c-1)}(\mathbf{J} - \mathbf{K}) \right) \\
&= \left( \frac{sr(c+1)}{\sqrt{c^2-1}}\mathbf{I} - \frac{s\tilde{M}(2rs-t+(c+\sqrt{c^2-1})t)}{2(c-1+2s^2)}(\mathbf{J} + \mathbf{K}) \right. \\
&\quad \left. + \frac{s(2rs-t+(c-\sqrt{c^2-1})t)}{2\tilde{M}(c-1)}(\mathbf{J} - \mathbf{K}) \right) \\
&\quad + \left( -\frac{rs(c+1)}{\sqrt{c^2-1}}\mathbf{I} + \frac{r\tilde{M}}{2}(\mathbf{J} + \mathbf{K}) - \frac{r(c-1+2s^2)}{2\tilde{M}(c-1)}(\mathbf{J} - \mathbf{K}) \right) \\
&= \left( -\frac{s\tilde{M}(2rs-t+(c+\sqrt{c^2-1})t)}{2(c-1+2s^2)}(\mathbf{J} + \mathbf{K}) + \frac{s(2rs-t+(c-\sqrt{c^2-1})t)}{2\tilde{M}(c-1)}(\mathbf{J} - \mathbf{K}) \right) \\
&\quad + \left( \frac{r\tilde{M}}{2}(\mathbf{J} + \mathbf{K}) - \frac{r(c-1+2s^2)}{2\tilde{M}(c-1)}(\mathbf{J} - \mathbf{K}) \right) \\
&= \left( \frac{r\tilde{M}}{2} - \frac{s\tilde{M}(2rs-t+(c+\sqrt{c^2-1})t)}{2(c-1+2s^2)} \right) (\mathbf{J} + \mathbf{K}) \\
&\quad - \left( \frac{r(c-1+2s^2)}{2\tilde{M}(c-1)} - \frac{s(2rs-t+(c-\sqrt{c^2-1})t)}{2\tilde{M}(c-1)} \right) (\mathbf{J} - \mathbf{K}) \\
&= \left( \frac{r\tilde{M}(c-1+2s^2)}{2(c-1+2s^2)} - \frac{s\tilde{M}(2rs-t+(c+\sqrt{c^2-1})t)}{2(c-1+2s^2)} \right) (\mathbf{J} + \mathbf{K}) \\
&\quad - \left( \frac{r(c-1+2s^2)}{2\tilde{M}(c-1)} - \frac{s(2rs-t+(c-\sqrt{c^2-1})t)}{2\tilde{M}(c-1)} \right) (\mathbf{J} - \mathbf{K}) \\
&= \frac{r\tilde{M}(c-1+2s^2) - s\tilde{M}(2rs-t+(c+\sqrt{c^2-1})t)}{2(c-1+2s^2)} (\mathbf{J} + \mathbf{K}) \\
&\quad - \frac{r(c-1+2s^2) - s(2rs-t+(c-\sqrt{c^2-1})t)}{2\tilde{M}(c-1)} (\mathbf{J} - \mathbf{K}) \\
&= \frac{\tilde{M}(rc-r+2s^2r) - \tilde{M}(2s^2r-st+st(c+\sqrt{c^2-1}))}{2(c-1+2s^2)} (\mathbf{J} + \mathbf{K}) \\
&\quad - \frac{rc-r+2s^2r - (2s^2r-st+st(c-\sqrt{c^2-1}))}{2\tilde{M}(c-1)} (\mathbf{J} - \mathbf{K}) \\
&= \frac{\tilde{M}(r(c-1)+st-st(c+\sqrt{c^2-1}))}{2(c-1+2s^2)} (\mathbf{J} + \mathbf{K}) - \frac{r(c-1)+st-st(c-\sqrt{c^2-1})}{2\tilde{M}(c-1)} (\mathbf{J} - \mathbf{K}); \\
\end{aligned}
\tag{5.5}$$

$$\begin{aligned}
 & \text{(ii)} \quad 2(a_2b_3 - a_3b_2)\mathbf{I} \\
 & = 2 \left\{ \left( -\frac{\tilde{M}(2rs - t + (c + \sqrt{c^2 - 1})t)}{2(c - 1 + 2s^2)} \right) \left( -\frac{c - 1 + 2s^2}{2\tilde{M}(c - 1)} \right) \right. \\
 & \quad \left. - \left( \frac{2rs - t + (c - \sqrt{c^2 - 1})t}{2\tilde{M}(c - 1)} \right) \left( \frac{\tilde{M}}{2} \right) \right\} \mathbf{I} \\
 & = \left( \frac{2rs - t + (c + \sqrt{c^2 - 1})t}{2(c - 1)} - \frac{2rs - t + (c - \sqrt{c^2 - 1})t}{2(c - 1)} \right) \mathbf{I} \\
 (5.6) \quad & = \frac{t\sqrt{c^2 - 1}}{(c - 1)} \mathbf{I};
 \end{aligned}$$

$$\begin{aligned}
 & \text{(iii)} \quad (a_1b_2 - a_2b_1)(\mathbf{J} + \mathbf{K}) \\
 & = \left\{ \left( \frac{r(c + 1)}{\sqrt{c^2 - 1}} \right) \left( \frac{\tilde{M}}{2} \right) \right. \\
 & \quad \left. - \left( -\frac{\tilde{M}(2rs - t + (c + \sqrt{c^2 - 1})t)}{2(c - 1 + 2s^2)} \right) \left( -\frac{s(c + 1)}{\sqrt{c^2 - 1}} \right) \right\} (\mathbf{J} + \mathbf{K}) \\
 & = \left( \frac{\tilde{M}r(c + 1)}{2\sqrt{c^2 - 1}} - \frac{s(c + 1)\tilde{M}(2rs - t + (c + \sqrt{c^2 - 1})t)}{2\sqrt{c^2 - 1}(c - 1 + 2s^2)} \right) (\mathbf{J} + \mathbf{K}) \\
 & = \left( \frac{\tilde{M}r(c + 1)(c - 1 + 2s^2)}{2\sqrt{c^2 - 1}(c - 1 + 2s^2)} - \frac{s(c + 1)\tilde{M}(2rs - t + (c + \sqrt{c^2 - 1})t)}{2\sqrt{c^2 - 1}(c - 1 + 2s^2)} \right) (\mathbf{J} + \mathbf{K}) \\
 & = \frac{(c + 1)\tilde{M}(r(c - 1 + 2s^2) - 2s^2r + st - st(c + \sqrt{c^2 - 1}))}{2\sqrt{c^2 - 1}(c - 1 + 2s^2)} (\mathbf{J} + \mathbf{K}) \\
 & = \frac{(c + 1)\tilde{M}(r(c - 1) + st - st(c + \sqrt{c^2 - 1}))}{2\sqrt{c^2 - 1}(c - 1 + 2s^2)} (\mathbf{J} + \mathbf{K}); \\
 (5.7) \quad &
 \end{aligned}$$

$$\begin{aligned}
 & \text{(iv)} \quad (a_3b_1 - a_1b_3)(\mathbf{J} - \mathbf{K}) \\
 & = \left\{ \left( \frac{2rs - t + (c - \sqrt{c^2 - 1})t}{2\tilde{M}(c - 1)} \right) \left( -\frac{s(c + 1)}{\sqrt{c^2 - 1}} \right) \right. \\
 & \quad \left. - \left( \frac{r(c + 1)}{\sqrt{c^2 - 1}} \right) \left( -\frac{c - 1 + 2s^2}{2\tilde{M}(c - 1)} \right) \right\} (\mathbf{J} - \mathbf{K}) \\
 & = \left( -\frac{s(c + 1)(2rs - t + (c - \sqrt{c^2 - 1})t)}{2\tilde{M}(c - 1)\sqrt{c^2 - 1}} + \frac{r(c + 1)(c - 1 + 2s^2)}{2\tilde{M}(c - 1)\sqrt{c^2 - 1}} \right) (\mathbf{J} - \mathbf{K}) \\
 & = \frac{-s(c + 1)(2rs - t + (c - \sqrt{c^2 - 1})t) + r(c + 1)(c - 1 + 2s^2)}{2\tilde{M}(c - 1)\sqrt{c^2 - 1}} (\mathbf{J} - \mathbf{K}) \\
 & = \frac{(c + 1)(-2s^2r + st - st(c - \sqrt{c^2 - 1})) + (c + 1)(r(c - 1) + 2s^2r)}{2\tilde{M}(c - 1)\sqrt{c^2 - 1}} (\mathbf{J} - \mathbf{K}) \\
 & = \frac{(c + 1)(r(c - 1) + st - st(c - \sqrt{c^2 - 1}))}{2\tilde{M}(c - 1)\sqrt{c^2 - 1}} (\mathbf{J} - \mathbf{K}). \\
 (5.8) \quad &
 \end{aligned}$$

Combining (5.5)–(5.8) together with  $a_0b_0 + a_1b_1 + 2a_2b_3 + 2a_3b_2 = t$ , we get  $\rho\sigma$  is equal to

$$\begin{aligned}
& t\mathbf{1} + \frac{t\sqrt{c^2-1}}{(c-1)}\mathbf{I} \\
& + \frac{\tilde{M}(r(c-1) + st - st(c + \sqrt{c^2-1}))}{2(c-1 + 2s^2)}(\mathbf{J} + \mathbf{K}) \\
& + \frac{(c+1)\tilde{M}(r(c-1) + st - st(c + \sqrt{c^2-1}))}{2\sqrt{c^2-1}(c-1 + 2s^2)}(\mathbf{J} + \mathbf{K}) \\
& - \frac{(r(c-1) + st - st(c - \sqrt{c^2-1}))}{2\tilde{M}(c-1)}(\mathbf{J} - \mathbf{K}) \\
& + \frac{(c+1)(r(c-1) + st - st(c - \sqrt{c^2-1}))}{2\tilde{M}(c-1)\sqrt{c^2-1}}(\mathbf{J} - \mathbf{K}) \\
= & t\mathbf{1} + \frac{t\sqrt{c^2-1}}{(c-1)}\mathbf{I} \\
& + \left( \frac{\sqrt{c^2-1}\tilde{M}(r(c-1) + st - st(c + \sqrt{c^2-1}))}{2\sqrt{c^2-1}(c-1 + 2s^2)} \right. \\
& \quad \left. + \frac{(c+1)\tilde{M}(r(c-1) + st - st(c + \sqrt{c^2-1}))}{2\sqrt{c^2-1}(c-1 + 2s^2)} \right)(\mathbf{J} + \mathbf{K}) \\
& + \left( -\frac{\sqrt{c^2-1}(r(c-1) + st - st(c - \sqrt{c^2-1}))}{2\tilde{M}(c-1)\sqrt{c^2-1}} \right. \\
& \quad \left. + \frac{(c+1)(r(c-1) + st - st(c - \sqrt{c^2-1}))}{2\tilde{M}(c-1)\sqrt{c^2-1}} \right)(\mathbf{J} - \mathbf{K}) \\
= & t\mathbf{1} + \frac{t\sqrt{c^2-1}}{c-1}\mathbf{I} + \frac{(c+1 + \sqrt{c^2-1})\tilde{M}(r(c-1) + st - st(c + \sqrt{c^2-1}))}{2\sqrt{c^2-1}(c-1 + 2s^2)}(\mathbf{J} + \mathbf{K}) \\
& + \frac{(c+1 - \sqrt{c^2-1})(r(c-1) + st - st(c - \sqrt{c^2-1}))}{2\tilde{M}(c-1)\sqrt{c^2-1}}(\mathbf{J} - \mathbf{K}).
\end{aligned}$$

This completes the proof of Lemma 5.3.  $\square$

Using the above lemma, we compute the traces of  $\rho\sigma\rho'$  and  $\rho\sigma\sigma'$ .

**Lemma 5.4.** *The trace of  $\rho\sigma\rho'$  is equal to*

$$2tr + \frac{2tr(c+1)}{c-1} + \frac{2(c+1)(r-2st)t}{c-1+2s^2} + \frac{2(2stc-r(c-1))(2rs-t+tc)}{(c-1)(c-1+2s^2)}.$$

*Proof.* Recall the formulas of  $\rho\sigma$  and  $\rho'$  given in Lemma 5.3 and (2.7). By Lemma 5.1, the trace of  $\sigma\rho\rho'$  is equal to

$$\begin{aligned}
 & 2 \left\{ tr + \left( \frac{t\sqrt{c^2-1}}{c-1} \right) \left( \frac{r(c+1)}{\sqrt{c^2-1}} \right) \right. \\
 & + 2 \left( \frac{(c+1+\sqrt{c^2-1})\tilde{M}(r(c-1)+st-st(c+\sqrt{c^2-1}))}{2\sqrt{c^2-1}(c-1+2s^2)} \right) \\
 & \times \left( -\frac{2rs-t+(c-\sqrt{c^2-1})t}{2\tilde{M}(c-1)} \right) \\
 & + 2 \left( \frac{(c+1-\sqrt{c^2-1})(r(c-1)+st-st(c-\sqrt{c^2-1}))}{2\tilde{M}(c-1)\sqrt{c^2-1}} \right) \\
 & \left. \times \left( \frac{\tilde{M}(2rs-t+(c+\sqrt{c^2-1})t)}{2(c-1+2s^2)} \right) \right\} \\
 = & 2 \left\{ tr + \frac{tr(c+1)}{c-1} \right. \\
 & - \frac{(c+1+\sqrt{c^2-1})(r(c-1)+st-st(c+\sqrt{c^2-1}))(2rs-t+(c-\sqrt{c^2-1})t)}{2(c-1)\sqrt{c^2-1}(c-1+2s^2)} \\
 & + \left. \frac{(c+1-\sqrt{c^2-1})(r(c-1)+st-st(c-\sqrt{c^2-1}))(2rs-t+(c+\sqrt{c^2-1})t)}{2(c-1)\sqrt{c^2-1}(c-1+2s^2)} \right\} \\
 = & 2tr + \frac{2tr(c+1)}{c-1} \\
 & - \frac{(c+1+\sqrt{c^2-1})(r(c-1)+st-stc-st\sqrt{c^2-1})(2rs-t+tc-t\sqrt{c^2-1})}{\sqrt{c^2-1}(c-1)(c-1+2s^2)} \\
 & + \frac{(c+1-\sqrt{c^2-1})(r(c-1)+st-stc+st\sqrt{c^2-1})(2rs-t+tc+t\sqrt{c^2-1})}{\sqrt{c^2-1}(c-1)(c-1+2s^2)} \\
 = & 2tr + \frac{2tr(c+1)}{c-1} \\
 & - \frac{(c+1+\sqrt{c^2-1})((r-st)(c-1)-st\sqrt{c^2-1})(2rs-t+tc-t\sqrt{c^2-1})}{\sqrt{c^2-1}(c-1)(c-1+2s^2)} \\
 & + \frac{(c+1-\sqrt{c^2-1})((r-st)(c-1)+st\sqrt{c^2-1})(2rs-t+tc+t\sqrt{c^2-1})}{\sqrt{c^2-1}(c-1)(c-1+2s^2)} \\
 = & 2tr + \frac{2tr(c+1)}{c-1} \\
 & - \frac{((c^2-1)(r-st)+(-(c+1)st+(r-st)(c-1))\sqrt{c^2-1}-st(c^2-1))(2rs-t+tc-t\sqrt{c^2-1})}{\sqrt{c^2-1}(c-1)(c-1+2s^2)} \\
 & + \frac{((c^2-1)(r-st)+((c+1)st-(r-st)(c-1))\sqrt{c^2-1}-st(c^2-1))(2rs-t+tc+t\sqrt{c^2-1})}{\sqrt{c^2-1}(c-1)(c-1+2s^2)}
 \end{aligned}$$

$$\begin{aligned}
&= 2tr + \frac{2tr(c+1)}{c-1} \\
&\quad - \frac{\left((c^2-1)(r-st) + (-2stc+r(c-1))\sqrt{c^2-1} - st(c^2-1)\right) \left(2rs-t+tc-t\sqrt{c^2-1}\right)}{\sqrt{c^2-1}(c-1)(c-1+2s^2)} \\
&\quad + \frac{\left((c^2-1)(r-st) + (2stc-r(c-1))\sqrt{c^2-1} - st(c^2-1)\right) \left(2rs-t+tc+t\sqrt{c^2-1}\right)}{\sqrt{c^2-1}(c-1)(c-1+2s^2)} \\
&= 2tr + \frac{2tr(c+1)}{c-1} \\
&\quad - \frac{\left((c^2-1)(r-2st) - (2stc-r(c-1))\sqrt{c^2-1}\right) \left((2rs-t+tc) - t\sqrt{c^2-1}\right)}{\sqrt{c^2-1}(c-1)(c-1+2s^2)} \\
&\quad + \frac{\left((c^2-1)(r-2st) + (2stc-r(c-1))\sqrt{c^2-1}\right) \left((2rs-t+tc) + t\sqrt{c^2-1}\right)}{\sqrt{c^2-1}(c-1)(c-1+2s^2)} \\
&= 2tr + \frac{2tr(c+1)}{c-1} + \frac{2\left((c^2-1)(r-2st)\right) \left(t\sqrt{c^2-1}\right)}{\sqrt{c^2-1}(c-1)(c-1+2s^2)} \\
&\quad + \frac{2\left((2stc-r(c-1))\sqrt{c^2-1}\right) \left(2rs-t+tc\right)}{\sqrt{c^2-1}(c-1)(c-1+2s^2)} \\
&= 2tr + \frac{2tr(c+1)}{c-1} + \frac{2(c+1)(r-2st)t}{c-1+2s^2} + \frac{2(2stc-r(c-1))(2rs-t+tc)}{(c-1)(c-1+2s^2)}.
\end{aligned}$$

This completes the proof.  $\square$

**Lemma 5.5.** *The trace of  $\rho\sigma\sigma'$  is equal to*

$$2ts - \frac{2ts(c+1)}{c-1} + \frac{2(r(c-1) + st - stc)}{c-1} - \frac{2(c+1)st}{c-1}.$$

*Proof.* Recall the formulas of  $\rho\sigma$  and  $\sigma'$  given in Lemma 5.3 and (2.5). By Lemma 5.1, the trace of  $\rho\sigma\sigma'$  is equal to

$$\begin{aligned}
&2 \left\{ ts + \left( \frac{t\sqrt{c^2-1}}{c-1} \right) \left( -\frac{s(c+1)}{\sqrt{c^2-1}} \right) \right. \\
&\quad + 2 \left( \frac{(c+1 + \sqrt{c^2-1})\tilde{M}(r(c-1) + st - st(c + \sqrt{c^2-1}))}{2\sqrt{c^2-1}(c-1+2s^2)} \right) \left( \frac{c-1+2s^2}{2\tilde{M}(c-1)} \right) \\
(5.9) \quad &\quad \left. + 2 \left( \frac{(c+1 - \sqrt{c^2-1})(r(c-1) + st - st(c - \sqrt{c^2-1}))}{2\tilde{M}(c-1)\sqrt{c^2-1}} \right) \left( -\frac{\tilde{M}}{2} \right) \right\}.
\end{aligned}$$



This can be simplified as

$$\begin{aligned}
 & 2 \left\{ ts - \frac{ts(c+1)}{c-1} + \frac{(c+1 + \sqrt{c^2-1})(r(c-1) + st - st(c + \sqrt{c^2-1}))}{2\sqrt{c^2-1}(c-1)} \right. \\
 & \quad \left. - \frac{(c+1 - \sqrt{c^2-1})(r(c-1) + st - st(c - \sqrt{c^2-1}))}{2\sqrt{c^2-1}(c-1)} \right\} \\
 &= 2ts - \frac{2ts(c+1)}{c-1} + \frac{(c+1 + \sqrt{c^2-1})(r(c-1) + st - stc - st\sqrt{c^2-1})}{\sqrt{c^2-1}(c-1)} \\
 & \quad - \frac{(c+1 - \sqrt{c^2-1})(r(c-1) + st - stc + st\sqrt{c^2-1})}{\sqrt{c^2-1}(c-1)} \\
 &= 2ts - \frac{2ts(c+1)}{c-1} + \frac{(c+1 + \sqrt{c^2-1})(r(c-1) + st - stc - st\sqrt{c^2-1})}{\sqrt{c^2-1}(c-1)} \\
 & \quad - \frac{(c+1 - \sqrt{c^2-1})(r(c-1) + st - stc + st\sqrt{c^2-1})}{\sqrt{c^2-1}(c-1)} \\
 &= 2ts - \frac{2ts(c+1)}{c-1} + \frac{2(r(c-1) + st - stc)\sqrt{c^2-1}}{\sqrt{c^2-1}(c-1)} - \frac{2(c+1)st\sqrt{c^2-1}}{\sqrt{c^2-1}(c-1)} \\
 &= 2ts - \frac{2ts(c+1)}{c-1} + \frac{2(r(c-1) + st - stc)}{c-1} - \frac{2(c+1)st}{c-1},
 \end{aligned}$$

which is equal to (5.9). This completes the proof.  $\square$

By Lemmas 5.2, 5.4, and 5.5, the traces of the elements in (5.2) are all contained in  $\mathbb{Q}(r, s, t)$ , which implies Theorem 2.3.

## 6. FINAL REMARK

Although Theorem 1.2 answers Question 1, we can ask the following stronger question in the spirit of Theorem 1.1.

**Question 2.** Let  $S_g$  ( $g \geq 2$ ) be a closed surface of genus  $g$ . Given any real number field  $K$  and any quaternion algebra  $A$  over  $K$  such that  $A \otimes_K \mathbb{R} \cong M_2(\mathbb{R})$ , is there a hyperbolic structure on  $S_g$  with integral traces such that its invariant trace field and quaternion algebra are equal to  $K$  and  $A$ ?

In this case, based on our work, we expect a negative answer. Instead, we propose the following conjecture.

**Conjecture 2.** For each  $g$  ( $g \geq 2$ ), there exists only a finite number of real number fields and quaternion algebras which arise as the invariant trace field and quaternion algebra of a hyperbolic structure of  $S_g$  with integral traces.

For each fixed genus surface, as stated above, only finitely many real number fields and quaternion algebras are expected to arise, via integral traces, as invariant trace field and quaternion algebras of hyperbolic structures of it. But, according to Theorem 1.1, for any real number field  $K$  and quaternion algebra  $A$  such that  $A \otimes_K \mathbb{R} \cong M_2(\mathbb{R})$  and  $A \not\cong \left(\frac{1}{K}\right)$ , it is always possible to construct a hyperbolic surface of sufficiently large genus, having  $K$  and  $A$  as its invariant trace field and quaternion algebra with integral traces. Thus, conjecturally, we do not expect any uniform bound on the number of real number fields and quaternion algebras, which

are realizable, via integral traces, as the invariants trace fields and quaternion algebras of hyperbolic structures of a fixed genus surface. Instead, it would be interesting to find the growth rate of these numbers with respect to genera of surfaces. Lastly we remark, in the spirit of the above conjecture and the discussion so far, that both Theorems 1.1 and 1.2 are complementary to each other.

#### ACKNOWLEDGMENTS

I thank Walter Neumann for suggesting this question as well as providing many helpful conversations, and Jeremy Kahn for showing his interest in this work. I also thank Ilya Kofman and the anonymous referee for their careful reading and valuable comments. Lastly I would like to thank Vlad Markovic and Ian Agol for helpful correspondence and pointing out a mistake in the statement of the main theorem in an earlier version of the paper.

#### REFERENCES

- [1] T. Gaughhofer, *Trace coordinates of Teichmüller spaces of Riemann surfaces*, PhD thesis, EPFL, 2005.
- [2] Pierre Antoine Grillet, *Abstract algebra*, 2nd ed., Graduate Texts in Mathematics, vol. 242, Springer, New York, 2007. MR2330890
- [3] J. Kahn and V. Markovic, *Finding cocompact Fuchsian groups of given trace field and quaternion algebra*, Talk at *Geometric structures on 3-manifolds*, IAS, Oct 2015.
- [4] Colin Maclachlan and Alan W. Reid, *The arithmetic of hyperbolic 3-manifolds*, Graduate Texts in Mathematics, vol. 219, Springer-Verlag, New York, 2003. MR1937957
- [5] Walter D. Neumann, *Realizing arithmetic invariants of hyperbolic 3-manifolds*, Interactions between hyperbolic geometry, quantum topology and number theory, Contemp. Math., vol. 541, Amer. Math. Soc., Providence, RI, 2011, pp. 233–246, DOI 10.1090/conm/541/10687. MR2796636

DEPARTMENT OF MATHEMATICS, COLUMBIA UNIVERSITY, 2990 BROADWAY, NEW YORK, NEW YORK 10027

*Current address:* Department of Mathematics, POSTECH, 77 Cheong-Am Ro, Pohang, South Korea

*Email address:* bogwang.jeon@gmail.com