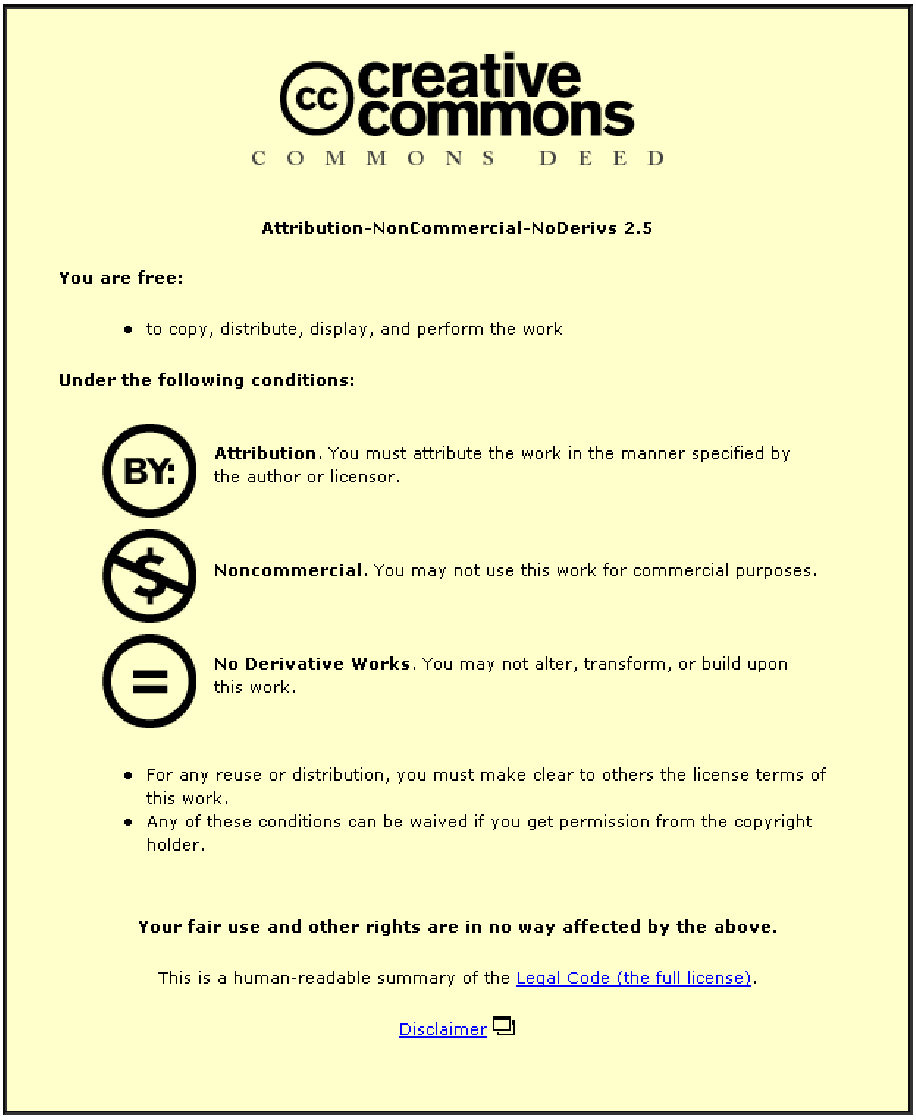

Reachability Problems in Quaternion Matrix and Rotation Semigroups

Paul C. Bell and Igor Potapov

Department of Computer Science,
University of Liverpool, Ashton Building,
Ashton St, Liverpool L69 3BX, U.K.
p.bell@lboro.ac.uk (P. Bell), igor@csc.liv.ac.uk (I. Potapov)

Abstract. We examine computational problems on quaternion matrix and rotation semigroups. It is shown that in the ultimate case of quaternion matrices, in which multiplication is still associative, most of the decision problems for matrix semigroups are undecidable in dimension two. The geometric interpretation of matrix problems over quaternions is presented in terms of rotation problems for the 2 and 3-sphere. In particular, we show that the reachability of the rotation problem is undecidable on the 3-sphere and other rotation problems can be formulated as matrix problems over complex and hypercomplex numbers.

1 Introduction

Quaternions have long been used in many fields including computer graphics, robotics, global navigation and quantum physics as a useful mathematical tool for formulating the composition of arbitrary spatial rotations and establishing the correctness of algorithms founded upon such compositions.

Many natural questions about quaternions are quite difficult and correspond to fundamental theoretical problems in mathematics, physics and computational theory. Unit quaternions actually form a *double cover* of the rotation group SO_3, meaning each element of SO_3 corresponds to two unit quaternions. This makes them expedient for studying rotation and angular momentum and they are particularly useful in quantum mechanics. The group of unit quaternions form the group SU_2 which is the special unitary group. The large number of applications has renewed interest in quaternions and quaternion matrices ([1], [8], [15], [18], [19]).

The multiplication of quaternions is not commutative and this leads to many problems with their analysis. In particular, defining the determinant and finding the eigenvalues and the inverse of a quaternion matrix are unexpectedly difficult problems [19]. In this paper we study decision questions about semigroups of quaternions, quaternion matrices and rotations, such as reachability questions, membership problems, freeness problems, etc. There are two major points of this work that we would like to highlight.

First, we investigated classical matrix decision problems for low-dimensional quaternion matrices. The results for matrices over $\mathbb{Z}, \mathbb{Q}, \mathbb{C}$ are not easily transferable to the case of quaternions and thus there are no results on *computational problems* for quaternions and quaternion matrices. Most of the problems for 2×2 matrices were open for any number field. In this paper, we show that all standard reachability problems are undecidable for 2×2 quaternion matrix semigroups. Moreover, our construction uses unitary quaternions that have a special interest in terms of rotations. After the quaternions, the hypercomplex numbers lose the associativity property and thus no longer form a semigroup. Due to this fact we think that our current research on quaternion matrices gives a more complete picture of decision problems for matrix semigroups. Then we study these problems for a case of Lipschitz integers and state several open problems.

The second important point of the paper is establishing connections between classical matrix semigroup problems and reachability problems for semigroups of rotations. In fact, using unit quaternions for encoding computational problems gives us an opportunity to formulate and prove several interesting results in terms of 3 and 4 dimensional rotations defined by quaternions. In particular, we show that the point-to-point rotation problem for the 3-sphere is undecidable. The same problem for the 2-sphere is open and can be formulated as a special case of the scalar reachability problem for matrix semigroups that we show is undecidable in general. As an additional benefit, the results on rotation semigroups give immediate corollaries for a class of orthogonal matrix semigroups.

The paper is organized as follows. In the second section we give all definitions about quaternions and their matrix representation and a mapping between words and quaternions that will be used in our proofs. The third section contains the main results of the paper on undecidable problems (freeness, membership, reachability) in quaternion matrix semigroups. We prove that the membership problem for 2×2 rational quaternion matrix semigroups is undecidable. We use a novel technique of PCP encoding, allowing us to encode pairs of words by separate matrices and force them to appear in the right order for a specific product. Then we show that the problem of deciding if any diagonal matrix is in a quaternion matrix semigroup, that has its own interest in a context of control theory, is undecidable. Then we study these problems for the case of Lipschitz integers. In the last section, the geometric interpretation of matrix problems over quaternions is presented in terms of rotation problems for the 2 and 3-sphere.

2 Preliminaries

We use the standard denotations $\mathbb{N}, \mathbb{Z}^+, \mathbb{Q}$ to denote the natural numbers, positive integers and rational numbers respectively.

In a similar style to complex numbers, rational quaternions, which are hypercomplex numbers, can be written $\vartheta = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$ where $a, b, c, d \in \mathbb{Q}$. To ease notation let us define the vector: $\mu = (1, \mathbf{i}, \mathbf{j}, \mathbf{k})$ and it is now clear that $\vartheta = (a, b, c, d) \cdot \mu$ where $\cdot$ denotes the inner or 'dot' product. We denote rational quaternions by $\mathbb{H}(\mathbb{Q})$. Quaternions with real part 0 are called *pure quaternions* and denoted by $\mathbb{H}(\mathbb{Q})_0$.

Quaternion addition is simply the componentwise addition of elements.

$$(a_1, b_1, c_1, d_1)\mu + (a_2, b_2, c_2, d_2)\mu = (a_1 + a_2, b_1 + b_2, c_1 + c_2, d_1 + d_2)\mu$$

It is well known that quaternion multiplication is not commutative. Multiplication is completely defined by the equations $\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1$, $\mathbf{ij} = \mathbf{k} = -\mathbf{ji}, \mathbf{jk} = \mathbf{i} = -\mathbf{kj}$ and

$\mathbf{ki} = \mathbf{j} = -\mathbf{ik}$. Thus for two quaternions $\vartheta_1 = (a_1, b_1, c_1, d_1)\mu$ and $\vartheta_2 = (a_2, b_2, c_2, d_2)\mu$, we can define their product as

$$\begin{array}{rl}\vartheta_1\vartheta_2 = & (a_1a_2 - b_1b_2 - c_1c_2 - d_1d_2) + (a_1b_2 + b_1a_2 + c_1d_2 - d_1c_2)\mathbf{i} \\ & +(a_1c_2 - b_1d_2 + c_1a_2 + d_1b_2)\mathbf{j} + (a_1d_2 + b_1c_2 - c_1b_2 + d_1a_2)\mathbf{k}\end{array}.$$

In a similar way to complex numbers, we define the conjugate of $\vartheta = (a, b, c, d) \cdot \mu$ by $\overline{\vartheta} = (a, -b, -c, -d) \cdot \mu$. We can now define a norm on the quaternions by $||\vartheta|| = \sqrt{\vartheta\overline{\vartheta}} = \sqrt{a^2 + b^2 + c^2 + d^2}$. Any non zero quaternion has a multiplicative (and obviously an additive) inverse [11]. Note also that $\vartheta_I = (1, 0, 0, 0)\mu \in \mathbb{H}$ is the multiplicative identity quaternion which is clear from the multiplication shown above. The other properties of being a division ring can be easily checked.

A *unit* quaternion has norm 1 and corresponds to a rotation in three dimensional space. Given a unit vector $\boldsymbol{r} = (r_1, r_2, r_3)$ and a rotation angle $0 \leq \theta < 2\pi$, we would like to find a quaternion transformation to represent a rotation of θ radians of a point $P' = (x, y, z) \in \mathbb{Q}^3$ about the $\boldsymbol{r}$ axis. To facilitate this, we require an encoding of P' as a pure quaternion P, namely $P = (0, x, y, z) \cdot \mu \in \mathbb{H}(\mathbb{Q})_0$.

Let us define a function $\psi_q : \mathbb{H}(\mathbb{Q}) \mapsto \mathbb{H}(\mathbb{Q})$ by $\psi_q(P) = qPq^{-1}$ where $q, P \in \mathbb{H}(\mathbb{Q})$ and $||q|| = 1$. If q is correctly chosen to represent a rotation of θ about a unit axis r, then this function will return a pure quaternion of the form $(0, x', y', z') \cdot \mu$ where $(x', y', z') \in \mathbb{Q}^3$ is the correctly rotated point.

It is well known (see, for example, [11]) that: $\vartheta = \left(\cos\frac{\theta}{2}, \boldsymbol{r}\sin\frac{\theta}{2}\right) \cdot \mu$ represents a rotation of angle θ about the $\boldsymbol{r}$ axis. Therefore using $\psi_\vartheta(P)$ as just described rotates P as required. This will be used in the next section.

All possible unit quaternions correspond to points on the 3-sphere. Any pair of unit quaternions p, q represent a four-dimensional rotation. Given a point $x \in \mathbb{H}(\mathbb{Q})$, we define a rotation of x, by $px\overline{q}$ [17]. Also we use the notation SU_2 to denote the special unitary group, the double cover of the rotation group SO_3.

The length of quaternions is multiplicative and the semigroup of Lipschitz integers with multiplication is closed. The fact that $||q_1q_2|| = ||q_1|| \cdot ||q_2||$ follows since the determinant of the matrix representation of a quaternion we define in Section 2.2 corresponds to the modulus and is multiplicative. This result will be required later.

2.1 Word morphisms

Let $\Sigma = \{a, b\}$ be a binary alphabet, $\boldsymbol{u} = (1, 0, 0)$ and $\boldsymbol{v} = (0, 1, 0)$. We define the homomorphism $\varphi : \Sigma^* \times \mathbb{Q} \mapsto \mathbb{H}(\mathbb{Q})$ by:

$$\varphi(a, \theta) = (\cos(\tfrac{\theta}{2}), \boldsymbol{u}\sin(\tfrac{\theta}{2})) \cdot \mu \text{ and } \varphi(b, \theta) = (\cos(\tfrac{\theta}{2}), \boldsymbol{v}\sin(\tfrac{\theta}{2})) \cdot \mu$$

where $\theta \in \mathbb{Q} \in [0, 2\pi)$, i.e. $\varphi(a, \theta)$ is a rotation of angle θ about the $\boldsymbol{u}$ axis and $\varphi(b, \theta)$ is a rotation of angle θ about the $\boldsymbol{v}$ axis. $\varphi(\varepsilon, \theta) = \vartheta_I$ is the multiplicative identity element of the division ring of rational quaternions. Note that $\boldsymbol{u} \cdot \boldsymbol{v} = 0$ and $||\boldsymbol{u}|| = ||\boldsymbol{v}|| = 1$, thus these two vectors are orthonormal.

Let us define a specific instance of this morphism. Let $\alpha = 2\arccos(\frac{3}{5}) \in \mathbb{R}$. Now we define $\gamma : \Sigma^* \mapsto \mathbb{H}(\mathbb{Q})$ where $\gamma(a) = \varphi(a, \alpha)$, $\gamma(b) = \varphi(b, \alpha)$ and $\gamma(\varepsilon) = (1, 0, 0, 0)\mu =$

ϑ_I. This gives the homomorphism:

$$\gamma(a) = (\cos(\arccos(\tfrac{3}{5})), \boldsymbol{u}\sin(\arccos(\tfrac{3}{5}))) \cdot \mu = (\tfrac{3}{5}, \tfrac{2}{5}, 0, 0) \cdot \mu \tag{1}$$

$$\gamma(b) = (\cos(\arccos(\tfrac{3}{5})), \boldsymbol{v}\sin(\arccos(\tfrac{3}{5}))) \cdot \mu = (\tfrac{3}{5}, 0, \tfrac{2}{5}, 0) \cdot \mu \tag{2}$$

which follows from the identity $\cos^2\theta + \sin^2\theta = 1$ since $\sqrt{1 - (\frac{3}{5})^2} = \frac{2}{5}$.

We can see that the quaternions in the image of γ are unit, i.e. $\forall w \in \Sigma^*, ||\gamma(w)|| = 1$ since quaternion length is multiplicative ($||q_1q_2|| = ||q_1|| \cdot ||q_2||$, which we proved in Section 2) and $\gamma(a), \gamma(b)$ have unit length.

Lemma 1 *The mapping $\gamma : \Sigma^* \mapsto \mathbb{H}(\mathbb{Q})$ is a monomorphism.*

Proof. It was proven in [16] that if $\cos(\theta) \in \mathbb{Q}$ then the subgroup of $SO_3(\mathbb{R})$ generated by rotations of angle θ about two perpendicular axes is free iff $\cos(\theta) \neq 0, \pm\frac{1}{2}, \pm 1$. We note that in the definition of γ we use a rotation about two orthonormal axes $\boldsymbol{u}, \boldsymbol{v}$. We use a rotation of $\alpha = 2\arccos\frac{3}{5}$. From basic trigonometry, $\cos(2\arccos(\frac{3}{5})) = -\frac{7}{25}$ and $\sin(2\arccos(\frac{3}{5})) = \frac{24}{25}$ thus the cosine and sine of both angles are rational and not equal to $0, \pm\frac{1}{2}, \pm 1$ (we only require this of the cosine) as required. We showed that all elements of the quaternions are rational, thus we have a free subgroup of $SO_3(\mathbb{Q})$ generated by $\gamma(a), \gamma(b) \in \mathbb{H}(\mathbb{Q})$. Note that the conditions mentioned are guaranteed to give a free group but are not necessary for freeness, see [8].□

Post's correspondence problem (PCP) - Given two (finite) alphabets Γ, Σ and two morphisms $h, g : \Gamma^* \mapsto \Sigma^*$, it is undecidable in general whether there exists a solution $w \in \Gamma^+$ such that $h(w) = g(w)$. We can assume without loss of generality that Σ is binary by using a straightforward encoding. It was shown that the problem is undecidable when the *instance size* $|\Gamma| \geq 7$ in [13]. We denote by n_p the smallest instance size for which PCP is undecidable (thus, $n_p \leq 7$).

2.2 Matrix Representations

It is possible to represent a quaternion $\mathbb{H}(\mathbb{Q})$ by a matrix $M \in \mathbb{C}^{2\times 2}$. For a general quaternion $\vartheta = (a, b, c, d) \cdot \mu$ we define the matrix:

$$M = \begin{pmatrix} a + b\mathbf{i} & c + d\,\mathbf{i} \\ -c + d\mathbf{i} & a - b\mathbf{i} \end{pmatrix}.$$

Corollary 1 *There is a class of 2×2 complex unitary matrices forming a free group.*

Proof. We can define a morphism similar to γ which instead maps to two dimensional complex matrices:

$$\zeta(a) = \begin{pmatrix} \frac{3}{5} + \frac{4}{5}\mathbf{i} & 0 \\ 0 & \frac{3}{5} - \frac{4}{5}\mathbf{i} \end{pmatrix}, \zeta(b) = \begin{pmatrix} \frac{3}{5} & \frac{4}{5} \\ -\frac{4}{5} & \frac{3}{5} \end{pmatrix}, \zeta(\varepsilon) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Note that these matrices are unitary, therefore let $\zeta(a^{-1}) = \zeta(a)^{-1} = \zeta(a)^*$ and $\zeta(b^{-1}) = \zeta(b)^{-1} = \zeta(b)^*$ where * denotes the Hermitian transpose.

Thus we have an injective morphism $\zeta : (\Sigma \cup \overline{\Sigma})^* \mapsto \mathbb{C}^{2\times 2}$. Since γ forms a free group of quaternions, ζ forms a free group over $\mathbb{C}^{2\times 2}$.□

Also note that we can define such matrices for any three orthonormal vectors where the rotation angle θ satisfies $\cos(\theta) \in \mathbb{Q}$ and $\cos(\theta) \neq 0, \pm\frac{1}{2}, \pm 1$.

3 Quaternion Matrix Semigroups

We will now show an undecidability result similar to one considered by A. Markov, where he showed undecidability for two sets of unimodular 2×2 integral matrices, see [12] and [9].

Theorem 1 *Given two sets $A = \{a_1, a_2, \ldots, a_n\}$ and $B = \{b_1, b_2, \ldots, b_n\}$, where $A, B \subset \mathbb{H}(\mathbb{Q})$, it is undecidable whether there exists a non-empty sequence of indices $(r_1, r_2, \ldots, r_m)$ such that $a_{r_1} a_{r_2} \cdots a_{r_m} = b_{r_1} b_{r_2} \cdots b_{r_m}$, this holds for $n = n_p$.*

Proof. We use a reduction of Post's correspondence problem and the morphism γ defined in Section 2. Given two alphabets Γ, Σ, such that Σ is binary, and an instance of the PCP, $(h, g) : \Gamma^* \mapsto \Sigma^*$. We proved in Lemma 1 that γ is a monomorphism between Σ^* and $\mathbb{H}(\mathbb{Q})$. Thus let us define a new pair of morphisms (ρ, τ) to map $\Gamma^+ \times \Gamma^+$ directly into $\mathbb{H}(\mathbb{Q}) \times \mathbb{H}(\mathbb{Q})$ (we can think of this as $\mathrm{SU}_2 \times \mathrm{SU}_2$ since each of these unit quaternions represents an element of S^3 (the 3-sphere)). For any $w \in \Gamma^+$, let $\rho(w) = \gamma(h(w))$ and $\tau(w) = \gamma(g(w))$.

Thus for an instance of PCP, $\Gamma = \{a_1, a_2, \ldots, a_m\}$, (h, g), we instead use the pair of morphisms (ρ, τ). Define two semigroups S_1, S_2 which are generated respectively by $\{\rho(a_1), \rho(a_2), \ldots, \rho(a_m)\}$ and $\{\tau(a_1), \tau(a_2), \ldots, \tau(a_m)\}$. We see their exists a solution to the given instance of PCP iff $\exists w \in \Gamma^+$ such that $\rho(w) = \tau(w)$. □

We now move to an extension of the Theorem 1 where it is no longer necessary to consider the index sequence. Markov obtained a similar result by extending the dimension of the integral matrices to 4×4 [12]. See also [3, 9], where the authors improve Markov's results to 3×3 integral matrices.

Theorem 2 *Given two semigroups S, T, generated by A, B respectively, such that $A = \{A_1, A_2, \ldots, A_n\}$ and $B = \{B_1, B_2\}$ where $A, B \subset \mathbb{H}(\mathbb{Q})^{2 \times 2}$, it is undecidable if $S \cap T = \varnothing$. Furthermore, all matrices in A, B can be taken to be diagonal.*

Proof. Given an instance of PCP, (h, g) where $h, g : \Gamma^* \mapsto \Sigma^*$. We use the monomorphisms $\rho, \tau : \Gamma^* \mapsto \mathbb{H}(\mathbb{Q})$ introduced in Theorem 1. For each $a \in \Gamma$ we define:

$$A_a = \begin{pmatrix} \rho(a) & 0 \\ 0 & \tau(a) \end{pmatrix}$$

and these matrices form the generator for the semigroup S. For the second semigroup, T, we simply wish to encode each symbol from Σ in the $[1, 1]$ and $[2, 2]$ elements using the morphism $\gamma : \Sigma^* \mapsto \mathbb{H}(\mathbb{Q})$ which was shown to be injective in Lemma 1:

$$B_1 = \begin{pmatrix} \gamma(a) & 0 \\ 0 & \gamma(a) \end{pmatrix}, \qquad B_2 = \begin{pmatrix} \gamma(b) & 0 \\ 0 & \gamma(b) \end{pmatrix}.$$

We see that there exists $M \in A$ such that $M_{[1,1]} = M_{[2,2]}$ iff there exists a solution $w \in \Gamma^+$ to the instance of the PCP. This follows since element $[1, 1]$ of M encodes $h(w)$ and element $[2, 2]$ encodes $g(w)$. Clearly any such matrix M is also in T since every matrix in T corresponds to an encoding of all words over Σ^+ in the top left and bottom right elements. Note that all matrices are diagonal and unitary. □

The previous two theorems used two separate semigroups. It is more natural to ask whether a particular element is contained within a *single* semigroup. For example, the mortality problem asks if the zero matrix is contained in an integral matrix semigroup and was shown to be undecidable in dimension 3 (see [14]). We showed that in dimension 4 the membership for any k-scalar matrix in an integral (resp. rational) matrix semigroup is undecidable where $k \in \mathbb{Z} \setminus \{0, \pm 1\}$ (resp. $k \in \mathbb{Q} \setminus \{0, \pm 1\}$), (see [4]).

Now we show that the membership problem in 2 × 2 unitary quaternion matrix semigroups in undecidable. The proof uses our new approach of encoding PCP proposed in [4]. The main idea is to store all words of the PCP separately and use an index coding to ensure they are multiplied in the correct way.

Theorem 3 *Given a unitary quaternion matrix semigroup S which is generated by $X = \{X_1, X_2, \ldots, X_n\} \subseteq \mathbb{H}(\mathbb{Q})^{2\times 2}$, it is undecidable for a matrix Y whether $Y \in S$.*

Proof. Given an instance of the PCP (h, g) where $h, g : \Gamma^* \mapsto \Sigma^*$. Then $w \in \Gamma^+$ is a solution to the PCP iff $h(w) = g(w)$. Assume now that $\forall x \in \Gamma^*$, $g(x)$ has an inverse, $g(x)^{-1}$. In terms of words over Σ, this means that if $g(x) = y$ for some $y \in \Sigma^*$ then $g(x)^{-1} = y^{-1}$ where $y^{-1} \in \overline{\Sigma}^*$ which is a new alphabet containing the inverse of each element of Σ. Formally we say $a \in \Sigma \Leftrightarrow a^{-1} \in \overline{\Sigma}$.

For example, if $g(w) = aabab$ where $w \in \Gamma^+$ and $aabab \in \Sigma^*$ then $g(w)^{-1} = (aabab)^{-1} = b^{-1}a^{-1}b^{-1}a^{-1}a^{-1} \in \overline{\Sigma}^*$.

If there exists a solution to the PCP, $w \in \Gamma^+$, such that $h(w) = g(w)$ then it can be observed that $h(w) \cdot g(w)^{-1} = \varepsilon$. We shall give an example of this simple fact. Let $w = w_1 w_2 \ldots w_k \in \Gamma^+$ be a solution to the PCP. Then $h(w) = g(w) = u$ for some $u = u_1 u_2 \ldots u_m \in \Sigma^+$. It is now clear that $h(w) \cdot g^{-1}(w) = (u_1 u_2 \ldots u_m) \cdot (u_m^{-1} u_{m-1}^{-1} \ldots u_1^{-1}) = \varepsilon$.

We call this type of word an *inverse palindrome*. This allows us to calculate the solution to the PCP instead as a single word. For each new symbol $a \in \Gamma$ we wish to add to the existing word $w \in \Gamma^*$, we concatenate $h(a)$ to the left and $g(a)^{-1}$ to the right of the current word $v \in \Sigma^*$, i.e. $v' = h(a) \cdot v \cdot g(a)^{-1}$. A solution then exists iff $v' = \varepsilon$ after a positive number of steps.

Within a semigroup this constraint is difficult to impose; we cannot say "multiply to the left by U_i and the right by V_i". Such a constraint *is* possible however by encoding *two* words simultaneously. In the first word we store the main word corresponding to the PCP itself such as described above. In the second word, we store the index of the word or its inverse.

Given some $a_i \in \Gamma$, we define two matrices in the semigroup generator Y_{i1}, Y_{i2} corresponding to this symbol. In Y_{i1} we store the two words $h(a_i)$ and $\sigma(i)$ where σ is an injective morphism for each $i \in \mathbb{Z}^+$, $\sigma(i) = a^i b$ where $a, b \in \Sigma$. In Y_{i2}, we store the two words $g(a_i)^{-1}$ and $\mu(i)$ where $\mu(i) = \overline{a}^i \overline{b}$ ($\overline{a} = a^{-1}$, $\overline{b} = b^{-1}$ and γ is the injective group morphism).

We need to store two words separately in one matrix. Let $\Gamma = \{a_1, a_2, \ldots, a_m\}$ and (h, g) be an instance of the PCP. Then for each $1 \leq i \leq m$, define

$$Y_{i1} = \begin{pmatrix} \gamma(h(a_i)) & 0 \\ 0 & \gamma(\sigma(i)) \end{pmatrix}, \; Y_{i2} = \begin{pmatrix} \gamma(g(a_i))^{-1} & 0 \\ 0 & \gamma(\mu(i)) \end{pmatrix}$$

Note that all quaternions used are unit. Now define two special matrices:

$$M = \begin{pmatrix} \gamma(h(a_1)) & 0 \\ 0 & \gamma(b) \end{pmatrix}, N = \begin{pmatrix} \gamma(g(a_1))^{-1} & 0 \\ 0 & \gamma(b)^{-1} \end{pmatrix}$$

We store the mapping of symbol a_1 in M, N, using the modified PCP to ensure that if there is a solution then there exists a solution using this symbol first. This avoids the pathological case of a product with only M and N in it.

Note that if matrix N appears once in a product equal to I_2 then matrix M appears once also due to the above construction (For the bottom right element to equal 1, $\gamma(b)$ must multiply with $\gamma(b)^{-1}$ at some point, see also [10]). Thus if we consider a semigroup, S, generated by $\{Y_{i1}, Y_{i2}, M\}$ where $1 \leq i \leq m$, then $N^{-1} \in S$ iff the instance of PCP has a solution, thus membership is undecidable. All matrices are diagonal and unitary quaternion matrices which are equivalent to *double quaternions*. Thus the membership for a semigroup of double quaternions is undecidable.□

Corollary 2 *The vector reachability problem for a semigroup of* 2×2 *quaternion matrices is undecidable.*

Proof. The vector reachability question for quaternions is defined as: "Given two vectors $a, b \in \mathbb{H}(\mathbb{Q})^n$ and a semigroup of matrices $S \subset \mathbb{H}(\mathbb{Q})^{n \times n}$, does there exist some $M \in S$ such that $Ma = b$?". The undecidability is straightforward from the Theorem 3. Let $x, y \in \mathbb{H}(\mathbb{Q})^2$ and $x = (1,1)^T, y = N^{-1}(1,1)^T$. Then, for some $R \in S$, it is clear that $Rx = y$ iff $R = N^{-1} = Y$ since we use only diagonal matrices. Since determining if $Y \in S$ is undecidable, the vector reachability problem is undecidable.□

The next problem was given as an open problem over matrices of natural numbers $\mathbb{N}$ in any dimension [5]. We show it is undecidable over $\mathbb{H}(\mathbb{Q})^{2\times 2}$.

Theorem 4 *It is undecidable for a finitely generated semigroup* $S \subseteq \mathbb{H}(\mathbb{Q})^{2\times 2}$ *whether there exists* any *diagonal matrix* $D \in S$.

Proof. As before, let $h, g : \Gamma^* \mapsto \Sigma^*$ be an instance of the PCP where $|\Sigma| = 2$. We use the morphisms $\rho, \tau : \Gamma^* \mapsto \mathbb{H}(\mathbb{Q})$ defined for any $w \in \Gamma^*$ as $\rho(w) = \gamma(h(w))$ and $\tau(w) = \gamma(g(w))$. Thus $u, v \in \Gamma^*$, $\rho(u) = \tau(v)$ iff $u = v$. For any two quaternions $q, r \in \mathbb{H}(\mathbb{Q})$ we define

$$\Psi(q, r) = \frac{1}{2} \begin{pmatrix} q + r & q - r \\ q - r & q + r \end{pmatrix}.$$

It is clear that this is still homomorphic [6], since $\Psi(q_1, r_1) \cdot \Psi(q_2, r_2) = \Psi(q_1 q_2, r_1 r_2)$ which is verified easily via:

$$\frac{1}{2} \begin{pmatrix} q_1 + r_1 & q_1 - r_1 \\ q_1 - r_1 & q_1 + r_1 \end{pmatrix} \cdot \frac{1}{2} \begin{pmatrix} q_2 + r_2 & q_2 - r_2 \\ q_2 - r_2 & q_2 + r_2 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} q_1 q_2 + r_1 r_2 & q_1 q_2 - r_1 r_2 \\ q_1 q_2 - r_1 r_2 & q_1 q_2 + r_1 r_2 \end{pmatrix}$$

It is now obvious that $\Psi(u, v)$ is diagonal iff $u = v$ since the top right and bottom left elements of the matrix equal 0 only if the two quaternions are equal.

Thus we can create one such matrix for each pair of images of letters from Γ using τ and ρ. S contains a diagonal matrix iff a PCP solution exists.

Unfortunately this does not hold when we convert the matrices to four dimensional rational matrices since we only get a *block diagonal* matrix. Thus the decidability for whether any matrix in a semigroup is diagonal remains open for integers, rationals and complex rational numbers. □

Another problem which can be stated is that of *freeness* of quaternion matrix semigroups. We use an almost identical proof to that in [7] to show undecidability, but we obtain the result for matrices over $\mathbb{H}(\mathbb{Q})^{2\times 2}$ rather than $(\mathbb{Z}^+)^{3\times 3}$:

Theorem 5 *Given a semigroup S, finitely generated by $M = \{M_1, \ldots, M_n\} \subset \mathbb{H}(\mathbb{Q})^{2\times 2}$, deciding whether S is free is algorithmically undecidable.*

Proof. Since we can store two words within a matrix $M_i \in \mathbb{H}(\mathbb{Q})^{2\times 2}$ we can use an almost identical proof that was used in [7]. We will give very brief sketch of the proof and refer to [7] for details.

The mixed modification PCP (or MMPCP) is a variant of the standard Post correspondence problem. As in the original PCP, we are given two (finite) alphabets Σ, Δ and two morphisms $h, g : \Sigma^+ \to \Delta^+$. The MMPCP asks whether there exists a word $w = w_1 w_2 \cdots w_m \in \Sigma^+$ such that:

$$h_1(w_1)h_2(w_2)\cdots h_m(w_m) = g_1(w_1)g_2(w_2)\cdots g_m(w_m)$$

where each $h_i, g_i \in \{h, g\}$ and $h_j \neq g_j$ for some $1 \leq j \leq m$. Now, define the set of 2×2 quaternion matrices:

$$M = \left\{ \begin{pmatrix} \gamma(a) & 0 \\ 0 & h(a) \end{pmatrix}, \begin{pmatrix} \gamma(a) & 0 \\ 0 & g(a) \end{pmatrix} ; \quad a \in \Sigma \right\}$$

and it can be seen that if S is not free then there is a word $w = w_1 w_2 \cdots w_n \in \Sigma^+$ such that $h_1(w_1)h_2(w_2)\cdots h_m(w_m) = g_1(w_1)g_2(w_2)\cdots g_m(w_m)$ since any equal matrix product in S must have the same word w in the top left element and the same element in the bottom right which was generated by *different* matrices. Thus the problem of freeness for 2×2 rational quaternion matrix semigroups is undecidable. See [7] for fuller details of the proof method.

Note that an alphabet size of $|\Sigma| = 7$ was required for the undecidability of MMPCP (see [10]), thus the problem is undecidable for 7 matrices. □

We now consider a problem which is *decidable* over complex numbers, but *undecidable* over rational quaternions. This gives a bound between the computational power of complex numbers and quaternions. We must first state the following lemma.

Lemma 2 *[2] Given a semigroup S of commutative matrices of any dimension, then the membership problem for S is decidable.*

Corollary 3 *The problems for diagonal matrices stated in Theorems 1, 2 and 3 are decidable when taken instead over any field up to the complex numbers.*

Proof. In Theorem 1, for each $1 \leq k \leq n$ let us define $M_k = \begin{pmatrix} q_{ik} & 0 \\ 0 & q_{jk} \end{pmatrix} \in \mathbb{C}^{2\times 2}$, and define a semigroup S generated by $\{M_1, M_2, \ldots, M_n\}$. The problem thus becomes "Does there exist a matrix X in S such that $X_{[1,1]} = X_{[2,2]}$?". This is decidable since the matrices commute by Lemma 2.

Theorem 2 concerns the emptiness testing of the intersection of two semigroups A, B. However, B is just the set of matrices with equal elements on the diagonal generated by $\gamma(a)$ and $\gamma(b)$. Thus the problem when taken for complex numbers is simply: "Does there exist some matrix, $X \in A$ with $X_{[1,1]} = X_{[2,2]}$" as in the previous paragraph. Again, since the matrices are diagonal and complex, they commute and the problem is decidable.

For Theorem 3, all matrices in the semigroup commute since they are diagonal with complex entries. By Lemma 2 we can decide if any Y is in the semigroup (in polynomial time) thus concluding the proof. □

3.1 Computational Problems in Lipschitz Integers

We also consider decision problems on the *Lipschitz integers* denoted by $\mathbb{H}(\mathbb{Z})$ which are quaternions with integral parts.

Corollary 4 *The problems stated in Theorems 1 and 2 are undecidable when taken instead over the Lipschitz integers* $\mathbb{H}(\mathbb{Z})$.

Proof. Note that in Lemma 1 we showed γ is injective and in Section 2.2 we showed an isomorphism between quaternions and a subgroup of the 2 dimensional complex matrices, $\mathbb{H}(\mathbb{Q}) \cong \mathbb{C}^{2\times 2}$. If we examine the definition of ζ in 2.2 we see that all elements have 5 as their denominator thus we can multiply $\zeta(a), \zeta(b)$ by the scalar matrix with element 5 thus giving 2 dimensional matrices over the Gaussian integers. This will still be free and is equivalent to the (non-unit) quaternions $q_1 = 5(\frac{3}{5}, \frac{4}{5}, 0, 0)\cdot\mu = (3, 4, 0, 0)\cdot\mu$ and $q_2 = 5(\frac{3}{5}, 0, \frac{4}{5}, 0) \cdot \mu = (3, 0, 4, 0) \cdot \mu$ which will now form a free semigroup. We therefore define $\lambda : \Sigma^* \mapsto \mathbb{H}(\mathbb{Z})$ by

$$\lambda(x) = \begin{cases} 5 \cdot \gamma(x) \text{ if } x \neq \varepsilon \\ \quad \gamma(x) \text{ if } x = \varepsilon \end{cases}$$

Thus in Theorems 1 and 2 we can replace the definitions of ρ, τ to use λ and this will give a free morphism over the Lipschitz integers $\mathbb{H}(\mathbb{Z})$. This cannot be extended to Theorem 3 since the inverse of a non-identity Lipschitz integer is not itself a Lipschitz integer (obviously it must have rational coefficients). □

Theorem 6 *Given a set of Lipschitz integers $S \in \mathbb{H}(\mathbb{Z})$ forming a semigroup $\langle S, \rangle$, the problem of deciding for an arbitrary $L \in \mathbb{H}(\mathbb{Z})$ if $L \in \langle S, \cdot\rangle$ is decidable.*

Proof. Note that all non-zero quaternions have modulus $d \in \mathbb{R}^+$. Furthermore, it is obvious that for any non-zero Lipschitz integer $L \in \mathbb{H}(\mathbb{Z})$, that $d \geq 1$, with equality iff $L \in \Phi = \{(\pm 1, 0, 0, 0)\cdot\mu, (0, \pm 1, 0, 0)\cdot\mu, (0, 0, \pm 1, 0)\cdot\mu, (0, 0, 0, \pm 1)\cdot\mu\}$. We have named this set for ease of explanation.

We see that $\forall q \in \Phi$ that q is of unit length i.e. $||q|| = q\overline{q} = \sqrt{a^2+b^2+c^2+d^2} = 1$. It can be also noted that their fourth powers are all equal to the identity element: $\forall q \in \Phi, q^4 = \vartheta_I = (1,0,0,0) \cdot \mu$ which is easily checked.

For a given L whose membership in S we wish to check, it will have a magnitude $||L|| = m \in \mathbb{R}$. If $m < 1$ then L cannot be a product a Lipschitz integers since the modulus must be at least 1 by definition of the quaternion modulus. If $m = 1$ then L can only be a product of elements from Φ and membership is trivial. Otherwise, $m > 1$. Let $S' = S \setminus \Phi$ (i.e. the generator set S minus any elements of Φ). We can see that there exists only a finite number of products to check since $m > 1$ and for all $x \in [S']$ we have that $||x|| > 1$.

Thus, excluding Φ we have a *finite* set of products of *finite* length to check. However if a (non-identity) element of Φ is in the generator, we must include these in the products. For each product $P = p_1 p_2 \cdots p_n \in S'$ whose magnitude equals m, i.e. $||P|| = m$, we define the set of products:

$$\left\{ P = \left(\prod_{t=1}^{n} r_t p_t \right) r_{n+1} \, | r_t, p_t \in \mathbb{H}(\mathbb{Z}) \right\},$$

where each r_t varies over all elements of $[(\Phi \cap S) \cup \vartheta_I]$ for $1 \leq t \leq n+1$. We must simply prove that $[\Phi]$ (the semigroup over elements of Φ) is finite. This is true since the only Lipschitz integers with moduli 1 are in Φ, the quaternion moduli is multiplicative and the product of two Lipschitz integers is a Lipschitz integer, all of which are very easy to prove. Thus $[\Phi]$ is a finite semigroup and there exists a finite set of products to check for equality to $L \in \mathbb{H}(\mathbb{Q})$ and thus this is a decidable problem. □

4 Geometric Interpretations

In this section, we will move from algebraic point of view to geometric interpretations of quaternion matrix semigroup problems. This leads to an interesting set of problems which we shall now outline.

Problem 1 - Point Rotation Problem (PRP(n)) - *Given points $x, y \in \mathbb{Q}^n$ on the unit length $(n-1)$-sphere and a semigroup S of n-dimensional rotations. Does there exist $M \in S$ such that M rotates x to y?*

In general, we can consider PRP(n) with a semigroup of n-dimensional rotation matrices (i.e. orthogonal matrices with determinant 1). In 3-dimensions, we may take S to be a semigroup of quaternions and define the rotation problem to be $qx'q^{-1} = y'$ where $q \in S$ and $x', y' \in \mathbb{H}(\mathbb{Q})_0$ are pure quaternions with imaginary components corresponding to the vectors x, y.

We shall show that this problem is *decidable* for 2-dimensions. Further, it is *undecidable* in 4-dimensions, and its decidability status is open in 3-dimensions.

Theorem 7 *The Point Rotation Problem, PRP(2) is decidable.*

Proof. Since the rotation of two-dimensional points is commutative, we can represent the problem as a vector reachability problem with a semigroup $S \subset \mathbb{Q}^{2\times 2}$. Since S is commutative, there exists a polynomial time algorithm to solve the membership problem [2].□

Problem 2 - **Quaternion Scalar Reachability Problem (QSRP(n))** - *Given vectors $u, v \in \mathbb{H}(\mathbb{Q})^n$ a scalar $r \in \mathbb{H}(\mathbb{Q})$ and a semigroup of matrices $S' \subset \mathbb{H}(\mathbb{Q})^{n\times n}$. Does there exist $M \in S'$ such that $u^T M v = r$?*

Theorem 8 *The Point Rotation Problem PRP(3) is reducible to the Quaternion Scalar Reachability Problem QSRP(2).*

Proof. Since we are using 3-dimensional rotations, we can convert all elements of the PRP(3) instance to quaternions. We define $x', y' \in \mathbb{H}(\mathbb{Q})_0$ to be pure quaternions with imaginary parts corresponding to x, y vectors respectively. We convert each 3D rotation, R in S to an equivalent unit quaternion q i.e. such that the imaginary vector in $qx'q^{-1}$ is equivalent to Rx for example.

Each quaternion q in the PRP is unit length it is invertible, thus if $qxq^{-1} = y$ we may write $qx = yq$. Let $G = \{q_0, q_1, \ldots, q_m\} = S' \setminus S'^2$ be the generator of S'. Define $\alpha = (y, 1)$ and $\beta = (-1, x)^T$ and let $G' = \{M_0, M_1, \ldots, M_m\}$ where $M_i = \begin{pmatrix} q_i & 0 \\ 0 & q_i \end{pmatrix}$ and let $T = \langle G', \cdot \rangle$ be a new semigroup. Then there exists $M \in T$ such that $\alpha M \beta = 0$ iff $\exists q \in S$ such that $qxq^{-1} = y$. To see this, note that $\alpha M \beta = qx - qy$ where $M = \begin{pmatrix} q & 0 \\ 0 & q \end{pmatrix}$ and $qx - yq = 0 \Rightarrow qx = yq \Rightarrow qxq^{-1} = y$ as required. □

In fact we know that QSRP(2) is undecidable in general:

Theorem 9 *Quaternion Scalar Reachability Problem is undecidable for a semigroup S generated by 5 two-dimensional diagonal quaternion matrices.*

Proof. Let $\gamma : \Sigma^* \mapsto \mathbb{H}(\mathbb{Q})$ be defined as previously and $\{(u_1, v_1), (u_2, v_2), \ldots, (u_n, v_n)\}$ be a Claus instance of PCP. Then we see that if $M_i = \begin{pmatrix} \gamma(u_i) & 0 \\ 0 & \gamma(v_i) \end{pmatrix}$ for each $2 \leq i \leq n-1$ and $\alpha = (\gamma(u_1), \gamma(v_1))$, $\beta = (\gamma(u_n), -\gamma(v_n))^T$ and $r = 0$ then:

$$\alpha M_w \beta = \gamma(u_1 u_w u_n) - \gamma(v_1 v_w v_n) = 0 \Leftrightarrow u_1 u_w u_n = v_1 v_w v_n$$

where $M_w = M_{w_1} M_{w_2} \cdots M_{w_k}$ and $1 \leq w_i \leq n-1$ for each $1 \leq i \leq k$. Since there exists a Claus instance of PCP which is undecidable for $n = 7$ [10], the problem is undecidable for 5 matrices (putting the first and last elements inside α, β). □

But the decidability status of PRP(3) remains open (since the reduction is one way). We next show that PRP(4) is undecidable.

Theorem 10 *The four-dimensional Point Rotation Problem is undecidable.*

Proof. The set of all unit quaternions forms a 3-dimensional sphere (3-sphere) and any pair of unit quaternions a and b can represent a rotation in $4D$ space. We can rotate a point $x = (x_1, x_2, x_3, x_4)$ on the 3-sphere, represented by a quaternion $q_x = (x_1, x_2, x_3, x_4)$, in the following way: aq_xb^{-1}.

Given a finite set of rotations, $\{(a_1, b_1), \ldots, (a_n, b_n)\}$, represented by pairs of quaternions. The question of whether a point x on the 3-sphere can be mapped to itself by the above set of rotations is equivalent to the problem whether there exists a non-empty sequence of indices $(r_1, \ldots, r_m)$ such that $a_{r_1} \cdots a_{r_m} q_x b_{r_m}^{-1} \cdots b_{r_1}^{-1} = q_x$.

If x is a point represented by quaternion $(1, 0, 0, 0) \cdot \mu$, then the above equation only holds when $a_{r_1} a_{r_2} \cdots a_{r_m} = b_{r_1} b_{r_2} \cdots b_{r_m}$. According to Theorem 1 we have that the four-dimensional Point Rotation Problem is undecidable for 7 rotations. Moreover it is easy to see that PRP(4) is undecidable even for 5 rotations using the idea of Claus instances of PCP [10] where two of the rotations (the first and the last one) can be fixed and used only once. □

Corollary 5 *The vector reachability problem for $n \times n$ rational orthogonal matrix semigroups is decidable when $n \leq 2$ and undecidable for $n \geq 4$ with at least 5 matrices in the semigroup generator.*

Open Problem 1 *Given a semigroup of rational quaternions, S, generated by a finite set $Q \subset \mathbb{H}(\mathbb{Q})$, is membership decidable for S? I.e. can we decide if $x \in S$ for any $x \in \mathbb{H}(\mathbb{Q})$?. Also, is the freeness of semigroup S decidable?*

A related open problem mentioned above can also be stated:

Open Problem 2 *Given two points on the 2-sphere, $x, y \in \mathbb{Q}^3$, and a semigroup of rotations S generated by a finite set G. Does there exist an algorithm to determine whether there exists a rotation $R \in S$ such that R rotates x to y?*

The rotation problem $PRP(3)$ is not only related to problems on quaternions but can also be reformulated as a 1-dimensional vector reachability problem for a semigroup or a group of rational linear functions over the complex field also known as Möbius transformations. In geometry, a Möbius transformation is a function, $f : \mathbb{C} \mapsto \mathbb{C}$ defined by:

$$f(z) = \frac{az + b}{cz + d},$$

where $z, a, b, c, d \in \mathbb{C}$ are complex numbers satisfying $ad - bc \neq 0$. Möbius transformations may be performed by taking a stereographic projection from a plane to a sphere, rotating and moving the sphere to a new arbitrary location and orientation, and making a stereographic projection back to the plane. Since there is a unique mapping between rotations of the 2-sphere and Möbius transformations, problem $PRP(3)$ is equivalent to the reachability problem of nondeterministic iterative maps: "Given a finite set M of one-dimensional linear rational functions over the complex field and two points x and y on the complex plane. Does there exist an algorithm to determine whether it is possible to map x to y by a finite sequence of linear rational functions from the set M?".

References

1. Y. H. Au-Yeung, On the Eigenvalues and Numerical Range of a Quaternionic Matrix, Preprint, (1994).
2. L. Babai, R. Beals, J. Cai, G. Ivanyos and E. M. Luks, Multiplicative Equations over Commuting Matrices, Proc. 7th ACM-SIAM Symp. on Discrete Algorithms , 498-507, (1996).
3. P. Bell, A Note on the Emptiness of Semigroup Intersections, Fundamenta Informaticae, 79, 1-4, (2007).
4. P. Bell, I. Potapov, On the Membership of Invertible Diagonal and Scalar Matrices, Theoretical Computer Science, 37-45, (2007).
5. V. Blondel, A. Megretski, Unsolved Problems in Mathematical Systems and Control Theory, Princeton University Press, (2004).
6. V. Blondel, E. Jeandel, P. Koiran, N. Portier, Decidable and Undecidable Problems about quantum automata, SIAM Journal on Computing, 34:6, 1464-1473, (2005).
7. J. Cassaigne, T. Harju, J. Karhumäki, On the Undecidability of Freeness of Matrix Semigroups, Intern. J. Alg. & Comp. 9, 295-305, (1999).
8. F. D'Allesandro, Free Groups of Quaternions, Intern. J. of Alg and Comp. (IJAC), Volume 14, Number 1, February, (2004).
9. V. Halava, T. Harju, On Markov's Undecidability Theorem for Integer Matrices, TUCS Technical Report, Number 758, (2006).
10. V. Halava, T. Harju, M. Hirvensalo, Undecidability Bounds for Integer Matrices using Claus Instances, TUCS Technical Report, Number 766, (2006).
11. E. Lengyel, Mathematics for 3D Game Programming & Computer Graphics, Charles River Media, (2004).
12. A. Markov, On Certain Insoluble Problems Concerning Matrices, Doklady Akad. Nauk SSSR, 539-542, (1947).
13. Y. Matiyasevich, G. Senizergues, Decision Problems for Semi-Thue Systems with a Few Rules, Theoretical Computer Science, 330(1), 145-169, (2005).
14. M. Paterson, Unsolvability in 3 × 3 Matrices, Studies in Applied Mathematics, 49, (1970).
15. W. So, R. C. Thomson, F. Zhang, Numerical Ranges of Matrices with Quaternion Entries, Linear and Multilinear Algebra, 37:175-195, (1994).
16. S. Swierczkowski, A Class of Free Rotation Groups, Indag. Math. 5, no.2, 221-226, (1994).
17. D. Velichova, S.Zacharias, Projection from 4D to 3D, Journal for Geometry and Graphics, volume 4, No.1, 55-69, (2000).
18. N. A. Wiegmann, Some Theorems on Matrices with Real Quaternion Elements, Can. Jour. Math. 7, (1955).
19. F. Zhang, Quaternions and Matrices of Quaternions, Linear Algebra Appl. 251, 21-57, (1997).