Quaternions are turning tomb raiders on their heads

DANIEL CHAN

What is a number? This seemingly banal question has plagued mathematicians for centuries who have questioned the legitimacy of irrational and negative numbers. The issue was raised again by 16th century Italian algebraists. To recount their story, recall that for real numbers b, c, the quadratic equation

$$x^2 + bx + c = 0$$

has real solutions if and only if the discriminant $\Delta = b^2 - 4c$ is non-negative. This fact and the quadratic formula was already known to the ancient Babylonians but the lack of solutions was never deemed a problem until the work of 16th century mathematician Gerolamo Cardano on the cubic equation

$$x^3 + px + q = 0$$

where p, q are real numbers. Cardano gave a solution in his book "Ars Magna" published in 1545 which, in modern language, can be written as

$$x = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$$

where the cube roots must be chosen so that their product is $\frac{p}{3}$. The problem arises in that, even if the cubic equation has three real roots, the term under the square root may be negative. However, Cardano's formula does give all three real solutions provided you are happy manipulating square roots of negative numbers as if they were like any other real number.

It thus seems convenient to enlarge the set of real numbers to include square roots of negative numbers. These complex numbers were first studied by Cardano and a little later by Bombelli. We will write i for $\sqrt{-1}$ and define a complex number rather imprecisely as an expression of the form $a + bi$ where a, b are real numbers. We let $\mathbb{C}$ denote the set of these complex numbers which includes the set of real numbers as expressions of the form $a + 0i$. Note that for any real quadratic equation, the quadratic formula gives two (possibly equal) complex roots. Given this new set of numbers,

the natural questions are: i) how do you manipulate complex numbers and ii)how do you know that we shouldn't include more numbers? For example, if c, d are real, then assuming usual rules of arithmetic apply to complex numbers we see,

$$(a+bi)(c+di) = ac + bci + adi + bdi^2 = (ac - bd) + (bc + ad)i$$

so the product of two complex numbers is still a complex number and not a completely new entity. We now introduce the rules of arithmetic for complex numbers which allow you to add, subtract and multiply complex numbers z, z', z'' to obtain new complex numbers.

Rules of Arithmetic for Complex Numbers

i. $i^2 = -1$.

ii. Add, subtract, multiply and divide real numbers as per usual.

iii. $(z + z') + z'' = z + (z' + z''), (zz')z'' = z(z'z'')$.

iv. $z + z' = z' + z$.

v. $(z + z')z'' = zz'' + z'z'', z''(z + z') = z''z + z''z'$.

vi. (Commutativity of Multiplication) $zz' = z'z$.

This makes our calculation for multiplying complex numbers above legitimate. Addition is even easier as the following example illustrates:

$$\begin{aligned}(2+3i) + (1+2i) &\overset{(iii)}{=} ((2+3i)+1) + 2i \overset{(iii)}{=} (2 + (3i+1)) + 2i \\ &\overset{(iv)}{=} (2 + (1+3i)) + 2i \overset{(iii)}{=} ((2+1) + 3i) + 2i \\ &\overset{(ii)}{=} (3+3i) + 2i = 3 + (3+2)i = 3 + 5i\end{aligned}$$

where, for the first few equalities, we have written which rule we used above the equals sign (the second last equality involves two rules!).

Of course one should check that on manipulating complex numbers using these rules we don't arrive at some nonsensical statement like $1 = 0$, but we shall omit this verification.

To divide by a non-zero complex number we need only invert and multiply. Inverting is easy once we introduce the complex conjugate of the complex

number $z = a + bi$ which by definition is $z^* := a - bi$. For $w \in \mathbb{C}$, a simple computation gives the following basic

Facts i) $(z+w)^* = z^* + w^*$, ii) $(zw)^* = z^* w^*$, and iii) zz^* is the real number $a^2 + b^2$.

The last fact permits us to invert non-zero $z = a + bi$ as

$$z^{-1} = (zz^*)^{-1} z^* = \frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2} i.$$

Let's return to the question of what is a number. Complex numbers no longer represent the quantity of an object, in particular, they cannot be ordered in a nice way which we make precise in the following exercises.

Ex. 1 Let P be the set of positive reals. Show that P has the following properties: i) for $a \in \mathbb{R}$ non-zero, either a or $-a$ is in P but not both, ii) for $a, b \in P$ we have $a + b, ab \in P$. (The set P gives rise to an order on $\mathbb{R}$, namely, for real numbers x, y we have $x < y$ if and only if $y - x \in P$.)

Ex. 2 If we replace $\mathbb{R}$ with $\mathbb{C}$ in the above exercise, then show there is no subset P of $\mathbb{C}$ which satisfies properties i) and ii) above.

If complex numbers don't represent quantities, then what can they represent? One answer is provided by the Argand diagram which represents the complex number $z = a + bi$ with the point on the Cartesian plane with coordinates (a, b).

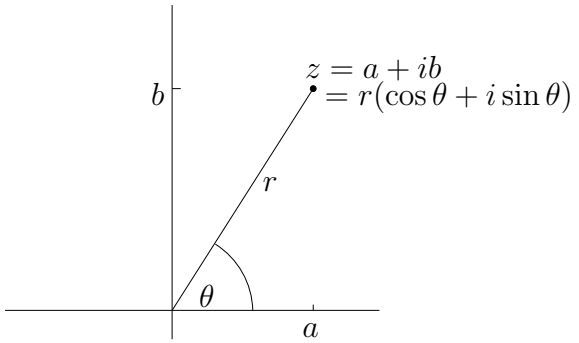

Figure 1: Argand diagram to represent complex numbers

If L is the line segment joining $(0, 0)$ to (a, b) we shall denote its length by $r = \sqrt{zz^*} = \sqrt{a^2 + b^2}$ called the modulus of z and the angle it makes with

the positive horizontal axis by θ. Then trigonometry gives the polar form $z = r(\cos\theta + i\sin\theta)$. The sum of angles formula gives the neat

Formula $r(\cos\theta + i\sin\theta)r'(\cos\theta' + i\sin\theta') = rr'(\cos(\theta+\theta') + i\sin(\theta+\theta'))$.

In particular, multiplying a complex number z by a complex number $w = \cos\theta + i\sin\theta$ of modulus one corresponds to rotating z on the Argand diagram anti-clockwise about the origin by the angle θ.

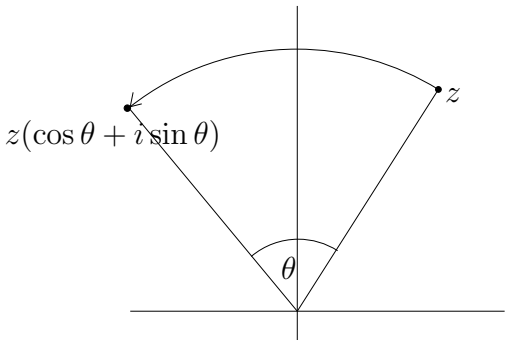

Figure 2: Rotation via complex multiplication

Quaternions

Can we further enlarge the set of complex numbers to a larger system of numbers? If we try to look for more numbers as roots of polynomial equations, then Gauss showed in his dissertation (published 1799), that you cannot: a polynomial of degree n with complex coefficients has n complex roots counting multiplicity.

Hamilton approached the question from a slightly different angle. Taking his cue from the Argand diagram, he wished to consider a new number, denoted j with square -1 and expressions of the form $a + bi + cj, a, b, c \in \mathbb{R}$ which could represent a point in three dimensional space. The question he posed was, can you add, subtract, multiply and divide such "hypercomplex" numbers using some extension of the usual rules of arithmetic? As often happens in mathematics, the question, "What is a number?" was mutated into the question, "What systems behave like a system of numbers?".

Hamilton had several false starts. He had to abandon his initial assumption that $ij = ji$ and then finally, he realised that ij could not be a number of the form $a + bi + cj$ but was a completely new entity which he denoted by

k.

We will describe his hypercomplex numbers, called quaternions, by analogy with our description of complex numbers. A quaternion is an expression of the form $a + bi + cj + dk$ where $a, b, c, d \in \mathbb{R}$. We let $\mathbb{H}$ denote the set of quaternions. We can add, subtract and multiply quaternions using the

Rules of Arithmetic for Quaternions

i. $i^2 = j^2 = k^2 = -1, ij = k = -ji, ki = j = -ik, jk = i = -kj$.

ii. Usual arithmetic for real numbers hold.

iii. Rules iii),iv),v) for manipulating complex numbers hold.

iv. Rule vi) has to be weakened to: $zz' = z'z$ if z is real.

For example we have

$$(i+j)^2 = (i+j)i+(i+j)j = i^2+ji+ij+j^2 = i^2+k-k+j^2 = i^2+j^2 = -2.$$

Note that in this case, the square of a sum is the sum of squares. This sort of new phenomenon occurs because we have dropped the rule concerning commutativity of multiplication. We say that $\mathbb{H}$ is noncommutative to signify the absence of this rule.

Division can be performed in a similar fashion as for complex numbers by introducing the hypercomplex conjugate of $z = a + bi + cj + dk$ to be $z^* := a - bi - cj - dk$. We'll also introduce the norm of z to be $N(z) := zz^*$. A straightforward calculation gives the following

Facts For $z, w \in \mathbb{H}$ we have i) $(z + w)^* = z^* + w^*$, ii) $(wz)^* = z^*w^*$, and iii) $N(z)$ is the real number $a^2 + b^2 + c^2 + d^2$.

Note that z^{-1} can be computed as $(zz^*)^{-1}z^*$ whenever $z \neq 0$. Also $N(z)$ is the square of the length of the line segment joining (a, b, c, d) to the origin $(0, 0, 0, 0)$.

Cayley showed that quaternions could be used to represent rotations in three and four dimensional space, much as complex numbers can be used to describe planar rotations. The recipe for three dimensional rotations goes as follows.

We'll identify three dimensional space with the set $\mathbb{H}_-$ of quaternions of the form $xi + yj + zk$ which represent the point (x, y, z). These quaternions

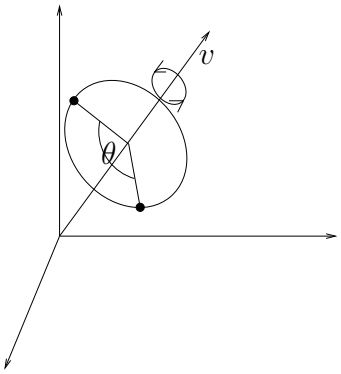

Figure 3: 3D Rotation

can be described as those $q \in \mathbb{H}$ with the property that $q^* = -q$. Suppose we wish to rotate through an angle θ around the axis joining the quaternions 0 and $v \in \mathbb{H}_-$. By scaling v, we may as well assume that v has unit norm. Set

$$u = \cos\frac{\theta}{2} + (\sin\frac{\theta}{2})v$$

and note that we still have $N(u) = 1$.

3D Rotation The rotation of $q = xi + yj + zk$ about the axis through v by an angle θ is given by uqu*.

We won't prove this fact which is not difficult. Rather, we'll give some plausibility arguments. We first check that uqu^* does indeed represent a point in three dimensional space i.e. $uqu^* \in \mathbb{H}_-$.

$$(uqu^*)^* = u^{**}q^*u^* = u(-q)u^* = -uqu^* \Rightarrow uqu^* \in \mathbb{H}_- \,.$$

Similar short calculations give

Ex. 3 For $q, q' \in \mathbb{H}$ and $\lambda, \lambda' \in \mathbb{R}$, show that we have $u(\lambda q + \lambda' q')u^* = \lambda uqu^* + \lambda' uq'u^*$. This corresponds to the fact that rotation takes lines to lines.

Ex. 4 Show $N(q) = N(uqu^*)$. This corresponds to the fact that rotation preserves distances between points.

Ex. 5 For $a \in \mathbb{R}$ show that $u(av)u^* = av$. This explains why the axis of rotation is the line through v and the origin.

Our recipe describes a rotation using a single quaternion u of unit norm. Suppose we rotate using u, and follow this up with another rotation described by another quaternion t of unit norm. What is the composite transformation? Well, the composite takes $q \in \mathbb{H}_-$ to $tuqu^*t^* = (tu)q(tu)^*$. This shows the composite of the two rotations is another rotation, in fact the rotation corresponding to the unit norm quaternion tu.

Quaternions and their Generalisations in the 21st Century

- Recently, computer game programmers have used quaternions in their animation to rotate objects. "Tomb Raider" was one such game using this technology. Quaternions have several advantages over other methods used, such as 3×3 matrices or recording rotations via their axis and rotation angle. For example, a quaternion is specified by 4 real numbers whereas a 3×3 matrix requires 9 numbers. The matrix method is thus more costly computationally and there is more room for errors to creep in. Representing rotations via axis and rotation angle has the problem that it's very difficult to compute the composite of two such rotations. Composing rotations recorded as quaternions is easy, just use the rules of arithmetic to multiply.

- Let's continue with Hamilton's game by adding extra new numbers to i, j, k, call them $l_1, \ldots l_r$. Can you add, subtract, multiply and divide quantities of the form $a + bi + cj + dk + e_1l_1 + \ldots + e_rl_r$ using the rules ii)-iv) for quaternion arithmetic and some modification of rule i)? Frobenius showed that the answer is no. However, if you further weaken rule iv), then you can get more "systems of numbers". These are called division algebras and there is still a lot of research into them today. They are classified by an object that mathematicians call the Brauer group. This Brauer group appears in many places and so provides a link between algebra and various other branches of mathematics. For example, the Brauer group is useful in number theory where one is interested in integer solutions to polynomial equations. Also, division algebras give interesting geometric objects called Brauer-Severi varieties which are "twisted" versions of projective space.

- The notion of division algebras can be further generalised if we drop the requirement that we can divide by non-zero quantities. This leads to the notion of an algebra. Noncommutative algebras occur typically

as sets of operators where multiplication is composition of operators. For example, with the quaternions of unit norm, these can be construed as rotation operators and their product corresponds to the composite rotation. Operators are ubiquitous in mathematics and consequently, so are algebras. To name some examples, they arise naturally in the theory of symmetry, called group theory, in the theory of differential equations and in quantum mechanics.

References

- van der Waerden, B.L., "A History of Algebra", Springer -Verlag, Berlin, 1985
- Bobick N., "Rotating objects using quaternions", Game Developer, February 1998