Reversible rotations, or how rho lost its tail*

Richard P. Brent

Australian National University
Canberra, ACT 0200, Australia
rotations@rpbrent.com

21 July 2006

Computing by the Numbers, Berlin, 21 July 2006.
 berlin06t

Abstract

In addition to thanking the organisers and session chairmen for their heroic efforts, and the speakers for their stimulating talks, I will discuss a small problem which might be of interest to both numerical analysts and number theorists: when is a rotation, performed with rounding to nearest, reversible in the sense that we can apply the inverse rotation (again with rounding to nearest) and get back to the starting vector? I will also explain the second part of the title.

Irreversible rotations

Let Q be an orthogonal matrix, and $x \in \mathbb{R}^n$ a vector. If we compute $y = Qx$ and then $z = Q^T y$ in floating-point arithmetic, we usually find $z \neq x$. In other words, we do not get back to our starting point.

There may be two distinct vectors $x' \neq x''$ such that, if we compute $y' = Qx'$ and $y'' = Qx''$ using floating point arithmetic, then $y' = y''$. Thus, the operation of multiplication by Q is not reversible, even in principle, because some information has been lost.

The aim of this talk is to investigate when multiplication by Q is reversible. However, since the answer to the general problem is "hardly ever", and the problem as posed above using floating-point arithmetic is too hard, we shall look at a simpler (but still interesting) model problem using fixed-point arithmetic.

The model problem

We shall restrict our attention to the two-dimensional case, i.e. plane rotations. Thus, our orthogonal matrices Q have the form

$$Q = \begin{bmatrix} c & -s \\ s & c \end{bmatrix} ,$$

where

$$c^2 + s^2 = 1 .$$

To model fixed-point arithmetic, we assume that the components of the input vectors x are integers, i.e. $x \in \mathbb{Z}^2$.

Complex multiplication

$$\begin{bmatrix} c & -s \\ s & c \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} y_1 \\ y_2 \end{bmatrix}$$

iff

$$(c + is)(x_1 + ix_2) = (y_1 + iy_2) ,$$

so another viewpoint is that we are considering multiplication by complex numbers on the unit circle. This might be relevant to the FFT.

Rounding

Let $\mathcal{R}(x) = \lfloor x + 1/2 \rfloor$ be the result of rounding $x \in \mathbb{R}$ to the nearest integer[1]. We also apply $\mathcal{R}$ to vectors by rounding each component.

Rounded rotations

A *rounded rotation* is an operation of the form

$$y = \mathcal{R}\,(Qx)\ .$$

We assume that Qx is computed exactly and then the components are rounded. This is the best that we can hope for.

It is easy to see that the search for reversible rotations is hopeless unless c and s are rational. Thus, we'll make this assumption.

[1]The rule for breaking ties is not important.

Rational rotations

One way to get rational c and s is to take a rational

$$t = \tan(\theta/2) = \frac{p}{q} \ \text{ say,}$$

then let

$$c = \cos\theta = \frac{1-t^2}{1+t^2} = \frac{q^2-p^2}{q^2+p^2}\ ,$$

$$s = \sin\theta = \frac{2t}{1+t^2} = \frac{2pq}{q^2+p^2}\ .$$

Of course, we also have

$$\tan\theta = \frac{2t}{1-t^2} = \frac{2pq}{q^2-p^2}$$

provided $t \neq \pm 1$.

We'll assume that $q > 0$ and $\gcd(p, q) = 1$. Also, there is no harm in restricting attention to the case $p > 0$.

Pythagorean triples

A right-angle triangle with sides of length A, B, C, where C is the hypotenuse, satisfies

$$A^2 + B^2 = C^2\ .$$

It is well-known that we can obtain all nontrivial solutions $A, B, C \in \mathbb{Z}_{>0}$ in the parametric form

$$A = 2mn\ ,$$

$$B = n^2 - m^2\ ,$$

$$C = n^2 + m^2\ ,$$

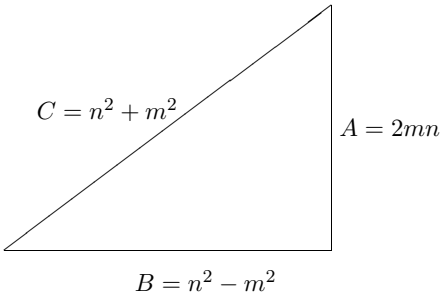
where $m, n \in \mathbb{Z},\ \ 0 < m < n$.

A *primitive* triple is a triple (A, B, C) with $\gcd(A, B, C) = 1$. We can get all the primitive Pythagorean triples by restricting attention to (m, n) with $\gcd(m, n) = 1$ and $m + n$ odd.

Any Pythagorean triple (A, B, C) gives a rational rotation

$$\frac{1}{C}\begin{bmatrix} B & -A \\ A & B \end{bmatrix} = \frac{1}{n^2+m^2}\begin{bmatrix} n^2-m^2 & -2mn \\ 2mn & n^2-m^2 \end{bmatrix}\ .$$

Pythagorean triples



$$(n^2+m^2)^2 = (n^2-m^2)^2 + (2mn)^2$$

The connection

Suppose $p \le q$ (otherwise interchange $p \leftrightarrow q$).

We can identify our two constructions of rational rotations by taking $(m, n) = (p, q)$. This is fine if $p + q$ is odd. However, if $p + q$ is even[2] it does not give a primitive Pythagorean triple, since all components of

$$(A, B, C) = (2pq, q^2 - p^2, p^2 + q^2)$$

are even. In this case it is better to take

$$(A, B, C) = \left(pq, \frac{q^2 - p^2}{2}, \frac{p^2 + q^2}{2} \right)$$

which corresponds to

$$(m, n) = \left(\frac{q - p}{2}, \frac{p + q}{2} \right) .$$

[2] p and q are both odd here, since $\gcd(p, q) = 1$.

Example

$(p, q) = (1, 5)$ gives

$$\begin{aligned} (A, B, C) &= \left(pq, \frac{q^2 - p^2}{2}, \frac{p^2 + q^2}{2} \right) \\ &= (5, 12, 13) \end{aligned}$$

and this corresponds to parameters

$$(m, n) = \left(\frac{q - p}{2}, \frac{q + p}{2} \right) = (2, 3) .$$

What is the relationship between $\theta/2 = \arctan(1/5)$ and $\theta'/2 = \arctan(2/3)$?

We have

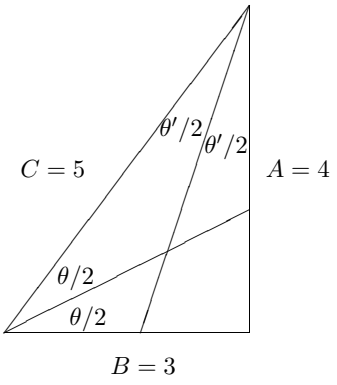
$$\tan(\theta/2 + \theta'/2) = \frac{1/5 + 2/3}{1 - 2/15} = 1 ,$$

so

$$\theta + \theta' = \frac{\pi}{2} .$$

Thus, we are just considering the same triangle from a different point of view ($A \leftrightarrow B, p \leftrightarrow q$).

The $(3, 4, 5)$ triangle



$$(p, q) = (1, 2) \text{ or } (1, 3) , \quad (m, n) = (1, 2) ,$$
$$\tan(\theta/2) = 1/2 , \quad \tan(\theta'/2) = 1/3 ,$$
$$\tan(\theta) = 4/3 , \quad \tan(\theta') = 3/4 .$$

Using periodicity mod C

Let

$$Q = \frac{1}{C} \begin{bmatrix} B & -A \\ A & B \end{bmatrix}$$

be a rational rotation defined by a Pythagorean triple (A, B, C). Our problem is: for each lattice point $x = (x_1, x_2) \in \mathbb{Z}^2$, compute

$$y = \mathcal{R}(Qx) \text{ and } z = \mathcal{R}(Q^T y) ,$$

and see if $x = z$. Since

$$Qx = \frac{1}{C} \begin{bmatrix} B & -A \\ A & B \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \frac{1}{C} \begin{bmatrix} Bx_1 - Ax_2 \\ Ax_1 + Bx_2 \end{bmatrix} ,$$

it is sufficient to consider x_1 and x_2 modulo C.

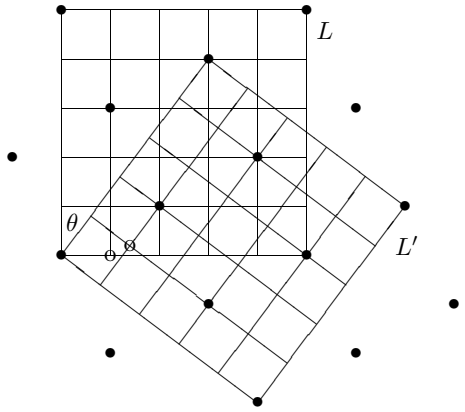
For a given triple (A, B, C), there are at most C^2 cases to consider. We'll see that this can be reduced to $O(C)$ cases.

Another way to view the problem

Instead of performing rotations through angles θ and $-\theta$, we can rotate the lattice L of integer points in $\mathbb{Z}^2$ by $-\theta$ to obtain a new lattice L'. Then we just have to round x to the "nearest" lattice point y in L', and round y back to the "nearest" lattice point z in L.

What is "nearest" ?

"nearest" depends on the lattice – essentially it means nearest in the L_∞ or max-norm, in the coordinate system defined by the (second) lattice.



Two lattices, L' rotated through angle $-\theta$ relative to L.

$$\tan(\theta) = 3/4\,, \quad \tan(\theta/2) = 1/3\,.$$

The symbol $\bullet$ indicates an exact intersection of the two lattices.

Reduction in cases to consider

Instead of considering all (x_1, x_2) modulo C, where $C = m^2 + n^2$, it is sufficient to consider the lattice points inside a square bounded by four $\bullet$ symbols. Each such square has area $C = m^2 + n^2$, so contains $O(C)$ points instead of C^2.

We can ignore the vertices of the squares (since the lattices intersect there and no rounding occurs). Thus, the number of points to consider is $C - 1$. Considerations of symmetry reduce this by a factor of 4 to $(C - 1)/4$.

Taking these shortcuts into account, there is essentially only one case to consider for the rotation defined by the $(3, 4, 5)$ triangle!

$(3, 4, 5)$ is reversible

We have seen that there is essentially only one case to consider for the $(3, 4, 5)$ triangle: any $x \in L \backslash L'$ will do. We may as well take the unit vector $x = e_1$.

$$\mathcal{R}\left(\frac{1}{5}\begin{bmatrix} 4 & -3 \\ 3 & 4 \end{bmatrix}\begin{bmatrix} 1 \\ 0 \end{bmatrix}\right) = \mathcal{R}\left(\begin{bmatrix} 4/5 \\ 3/5 \end{bmatrix}\right) = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$$

and

$$\mathcal{R}\left(\frac{1}{5}\begin{bmatrix} 4 & 3 \\ -3 & 4 \end{bmatrix}\begin{bmatrix} 1 \\ 1 \end{bmatrix}\right) = \mathcal{R}\left(\begin{bmatrix} 7/5 \\ 1/5 \end{bmatrix}\right) = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

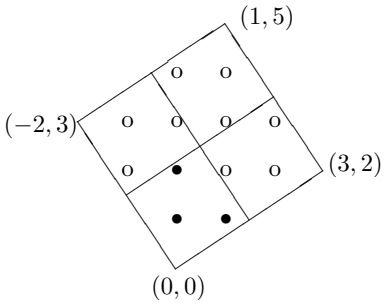
Thus, Q defined by $\tan\theta = 3/4$ is a reversible rotation.

$(5, 12, 13)$ is reversible

Here $(m, n) = (p, q) = (2, 3)$. Using symmetry, we only need consider the $(13 - 1)/4 = 3$ lattice points "•" lying inside the square with opposite vertices at the origin and $(1/2, 5/2)$. For example,

$$\mathcal{R}\left(\frac{1}{13}\begin{bmatrix} 12 & -5 \\ 5 & 12 \end{bmatrix}\begin{bmatrix} 0 \\ 2 \end{bmatrix}\right) = \mathcal{R}\begin{bmatrix} -10/13 \\ 24/13 \end{bmatrix} = \begin{bmatrix} -1 \\ 2 \end{bmatrix}$$

$$\mathcal{R}\left(\frac{1}{13}\begin{bmatrix} 12 & 5 \\ -5 & 12 \end{bmatrix}\begin{bmatrix} -1 \\ 2 \end{bmatrix}\right) = \mathcal{R}\begin{bmatrix} -2/13 \\ 29/13 \end{bmatrix} = \begin{bmatrix} 0 \\ 2 \end{bmatrix}.$$



$(8, 15, 17)$ is not reversible

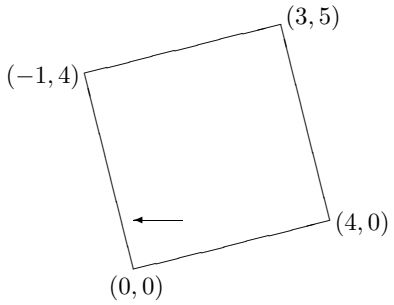
$$\mathcal{R}\left(\frac{1}{17}\begin{bmatrix} 15 & -8 \\ 8 & 15 \end{bmatrix}\begin{bmatrix} 1 \\ 1 \end{bmatrix}\right) = \mathcal{R}\left(\begin{bmatrix} 7/17 \\ 23/17 \end{bmatrix}\right) = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

and

$$\mathcal{R}\left(\frac{1}{17}\begin{bmatrix} 15 & 8 \\ -8 & 15 \end{bmatrix}\begin{bmatrix} 0 \\ 1 \end{bmatrix}\right) = \mathcal{R}\left(\begin{bmatrix} 8/17 \\ 15/17 \end{bmatrix}\right) = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

Thus, $(1, 1) \to (0, 1)$, and the rotation is not reversible.

Also, $(0, 1) \to (0, 1)$, so $(0, 1)$ has in-degree at least 2.



Geometric explanation

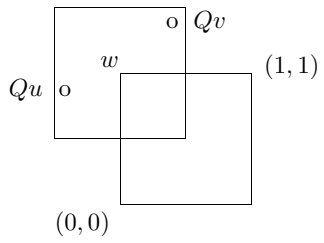
Consider

$$Q = \frac{1}{17}\begin{bmatrix} 15 & -8 \\ 8 & 15 \end{bmatrix}.$$

Let $u = (0, 1)^T, v = (1, 1)^T, w = (0, 1)^T$.
$Qu = (-8/17, 15/17)^T$, $Qv = (7/17, 23/17)^T$, so $||Qu - w||_\infty < 1/2$ and $||Qv - w||_\infty < 1/2$.

Whenever two points of $L(\theta)$ lie in a region of radius less than 0.5 (in the max-norm) from a point $w \in L(0)$, reversibility is ruled out because the in-degree of w is at least 2.

The converse is also true, so we have a purely geometric characterisation of reversibility.



The pattern

If a rotation $Q(\theta)$ through an angle θ is reversible, then so is $Q(k\pi/2 \pm \theta)$. Also, $Q(0) = I$ is trivially reversible, and $Q(\pi/4)$ is not rational. Thus, we can (if we wish) restrict attention to $\theta \in (0, \pi/4)$, although for the moment we allow $\theta \in (0, \pi/2)$.

As before, assume that $p > 0$, $q > 0$ and $\gcd(p, q) = 1$, where $\tan(\theta/2) = p/q$.

Conjecture

For $\theta \in (0, \pi/2)$, $Q(\theta)$ is reversible iff $m = n - 1 \geq 1$. (An equivalent condition is $C = A + 1$.)

Equivalent conjecture

For $\theta \in (0, \pi/4)$, $Q(\theta)$ is reversible iff $p = 1$ and $q \geq 3$ is odd.

Note: $(p, q) = (n - 1, n)$ gives $\theta > \pi/4$ so we have to replace θ by $\pi/2 - \theta$ which gives $(p, q) = (1, 2n - 1)$. For example, in the case $(5, 12, 13)$ we have $(m, n) = (2, 3)$, $(p, q) = (1, 5)$.

Evidence

- The conjecture has been verified for $0 < m < n \leq 1000$.
- We can prove certain cases, e.g. if $p = 1$ and $q = 4k$ then Q is not reversible.

Proving that $Q(\theta)$ is reversible if $m = n - 1$ should be straightforward, and I hope to complete the details soon (watch this space).

Genesis of the problem

Wallace's method for generating pseudo-random numbers with a normal distribution depends on applying orthogonal transformations to a pool of normally-distributed numbers. Wallace used 4×4 transformations Q with entries $\pm 1/2$ (scaled Hadamard matrices), but in my implementation I used 2×2 transformations of the form $Q(\theta)$ where $\tan\theta = 3/4$ or $4/3$.

Wallace's transformations have small order ($Q^8 = I$), which seems risky, even though the way the transformations are used in his normal random number generator may be satisfactory.

I chose transformations $Q(\theta)$ where θ/π is irrational. Thus, the order of Q is infinite for exact arithmetic. Naturally I was interested in the order when floating-point arithmetic was used, and I investigated the simpler problem of fixed-point arithmetic to gain some insight.

Finding the tail and cycle

In order to find the cycle length, I started from some nonzero lattice point $x^{(0)} \in \mathbb{Z}^2$, and considered the sequence defined by

$$x^{(k)} = \mathcal{R}\left(Qx^{(k-1)}\right) .$$

I searched for the first positive k such that

$$x^{(2k)} = x^{(k)}$$

in a manner that will be familiar to those of you who know the Floyd cycle-finding and Pollard rho integer factoring algorithms. The latter is named "rho" because of the shape of the Greek letter

$$\rho$$

which has a "tail" attached to a "loop" or "cycle".

Using the Floyd-Pollard idea I could find the non-periodic "tail" of the sequence, say $x^{(0)}, \ldots, x^{(\alpha-1)}$, and the periodic "cycle" $x^{(\alpha)}, \ldots, x^{(\alpha+\tau-1)}$, where $x^{(\alpha+\tau)} = x^{(\alpha)}$. The minimal such $\tau > 0$ is the period and the minimal $\alpha \geq 0$ is the length of the tail.

In general, as expected, $\alpha > 0$. However, I found $\alpha = 0$ when using the $(3, 4, 5)$ and $(5, 12, 13)$ triangles, and soon discovered the pattern: $\alpha = 0$ if $m = n - 1$, and usually $\alpha > 0$ if $m < n - 1$.

Summary. When $n = m + 1$, "ρ" loses its tail.

Remark. If Q is reversible, then my age divides ABC.

The period

If we start with w-bit integers as components of $x^{(0)}$, the period appears to be $2^{O(w)}$, where the exponent is larger for reversible rotations than for irreversible rotations. It is plausible that the correct exponent is $2w/3$ in the irreversible case.

For example, with $w = 16$ and 100 trials, we found a mean cycle length of 5.98×2^w for the $(3, 4, 5)$ triple, and $0.136 \times 2^w = 5.47 \times 2^{2w/3}$ for the $(8, 15, 17)$ triple.

The points on the cycle appear to be uniformly distributed in a thin annulus close to the circle of radius $||x^{(0)}||_2$.

Other rounding rules

If we round away from zero, the iterates appear to diverge (they spiral out to infinity).

If we round towards zero, the iterates spiral in and eventually get stuck in a small cycle close to the origin.