The Efficient Real Numbers

James Douglas, Rony Kirollos, Ben Odgers, Ross Street and Nguyen Hanh Vo

Macquarie University February 2004

In this paper we provide the details for the sketched construction of the real numbers appearing in [St]. We reproduce [St] here for ease of access and then proceed with the details that include a correction to the last paragraph of [St].

An Efficient Construction of Real Numbers

Ross Street

The ordered field R of real numbers can be constructed directly from the ring Z of integers without first manufacturing the field Q of rationals and without (explicitly) using Cauchy sequences or Dedekind cuts. This idea has avoided the wide publicity it deserves. I believed the original discoverer to be Steve Schanuel (SUNY, Buffalo, New York) who explained it to me while he was visiting Macquarie University last year. Peter Johnstone has recently told me that the construction was also proposed by Richard Lewis (Sussex, England). Does anyone know of any other independent discoverers?

By way of motivation notice that a real number α determines a function $f : Z \to Z$ given by $f(n) = [\alpha n]$, where square brackets denote "integer part". Then $\frac{f(10^r)}{10^r}$ approximates α to r decimal places. In fact $\frac{f(n)}{n} \to \alpha$ as $n \to \infty$. if α is an integer then f preserves addition; otherwise it almost does in that $|f(m+n) - f(m) - f(n)| \leq 3$.

Now to the construction. A function $u : X \to Z$ is called *bounded* when its image is finite; that is, when there exists $k \in Z$ such that $|u(x)| \leq k$ for all $x \in X$. The set Z^X of functions from X to Z is an abelian group under pointwise addition $(f + g)(x) = f(x) + g(x)$. For X an abelian group, define $f \in Z^X$ to be a *quasi-homomorphism* when $f(x + y) - f(x) - f(y)$ is bounded as a function of $(x, y) \in X \times X$. The quasi-homomorphisms form a subgroup $qh(X, Z)$ of Z^X, and, the bounded functions form a subgroup of $qh(X, Z)$.

The abelian group R is defined to be $qh(Z, Z)$ modulo the bounded functions.

Before proceeding to the multiplicative structure take $f \in qh(Z, Z)$ and suppose $|f(m+n) - f(m) - f(n)| \leq k$ for all $m, n \in Z$. It is easy to deduce the inequality

$$|f(mn) - mf(n)| \leq (|m| + 1)k$$

and hence the inequality

$$|nf(m) - mf(n)| \leq (|m| + |n| + 2)k \tag{1}$$

[If we allow ourselves to know about rationals this implies $(\frac{f(n)}{n})$ is a Cauchy sequence in Q.]

It is easy to see that $qh(Z, Z)$ is closed under composition of functions $(f \circ g)(n) = f(g(n))$. This gives a multiplication on $qh(Z, Z)$ which almost makes it into a ring; all that fails is that $f \circ (g + h)$ and $f \circ g + f \circ h$ are not necessarily equal. However, by taking $m = g(n)$ in (1), we obtain an inequality

$$|n(f \circ g)(n) - g(n)f(n)| \leq (|n| + 1)k'.$$

and hence an inequality

$$|(f \circ g)(n) - (g \circ f)(n)| \leq k''.$$

This shows that the multiplication of $qh(Z, Z)$ is almost commutative so that the failing distributive law is almost true as a consequence of the distributive law on the other side.

This proves that *composition in $qh(Z, Z)$ induces a multiplication on R which makes R a commutative ring.*

To see that *R is a field* take a quasi-homomorphism f which represents a non-zero element of α of R. Then f is not bounded above (or below). Let $\bar{f}(n)$ be the first integer m such that $f(m) \geq n$. Then $f(\bar{f}(n)) \geq n > f(\bar{f}(n) - 1) \geq f(\bar{f}(n)) + f(1) - k$. So the difference between $f \circ \bar{f}$ and the identity function is bounded. It is easy to see that $\bar{f}$ is a quasi-homomorphism and so represents an inverse for α.

Call $\alpha \in R$ *positive* when it is represented by a quasi-homomorphism f such that $f(n) \geq 0$ for all $n \geq 0$. Define $\alpha \leq \beta$ in R when $\beta - \alpha$ is positive. *This makes R an ordered field.*

To see that *R is order complete*, take a non-empty set S of positive elements of R. For each $s \in S$, let $f_s \in qh(Z, Z)$ represent s and have $f_s(n) \geq 0$ for all $n \geq 0$. Define $g(n)$ to be the first element in the set $\{f_s(n) | s \in S\}$ for $n \geq 0$. Put $g(n) = -g(-n))$ for $n < 0$. Then g represents a greatest lower bound for S.

Macquarie University

Definition 1 *Quasi-homomorphism*
A function $f : Z \longrightarrow Z$ is called a quasi-homomorphism (qhm) when $\exists k \in N$ such that $\forall m, n \in Z$:

$$|f(n+m) - f(n) - f(m)| \leq k.$$

When k is 0, f is a homomorphism. In general, k is called the *additivity constant.*

Definition 2 *Equivalent quasi-homomorphisms*
Two quasi-homomorphism f and g are called equivalent, denoted by $f \sim g$, if $\exists k \in N$ such that $\forall n \in N$:

$$|f(n) - g(n)| \leq k.$$

Theorem 1
The above equivalence property is an equivalence relation and so partitions the set of quasi-homomorphisms into disjoint equivalence classes.

Proof:

(Symmetry) If $|f(n) - g(n)| \leq k$, then $|g(n) - f(n)| = |-(f(n) - g(n))| = |f(n) - g(n)| \leq k$.

(Reflexivity) $|f(n) - f(n)| = 0 \leq k$.

(Transitivity) If $|f(n) - g(n)| \leq k_1 \in N$ and $|g(n) - h(n)| \leq k_2 \in N$ then $|f(n) - h(n)| = |f(n) - g(n) + g(n) - h(n)| \leq k_1 + k_2$, by the triangle inequality.

The set of qhms equivalent to f is denoted by $[f]$.

Define addition of two quasi-homomorphisms f and g by point-wise addition: $(f+g)(n) = f(n) + g(n)$. To see that $f+g$ is a qhm note that since f, g are qhms:

$$|f(m+n) - f(m) - f(n)| \leq k_1$$
$$|g(m+n) - g(m) - g(n)| \leq k_2$$

Applying the triangle inequality:

$$|f(m+n) - f(m) - f(n) + g(m+n) - g(m) - g(n)| \leq k_1 + k_2$$
$$|f(m+n) + g(m+n) - f(m) - g(m) - f(n) - g(n)| \leq k_1 + k_2$$
$$|(f+g)(m+n) - (f+g)(m) - (f+g)(n)| \leq k_1 + k_2$$

Define multiplication of two quasi-homomorphisms f and g by function composition: $(fg)(n) = f(g(n))$.

To show that (fg) is a qhm firstly define:

$$d_f(m,n) = f(m+n) - f(m) - f(n)$$

$$
\begin{aligned}
f(g(m+n)) - f(g(m)) - f(g(n)) &= f(g(m)+g(n)+d_g(m,n)) - f(g(m)) - f(g(n)) \\
&= f(g(n)+d_g(m,n)) \\
&+ d_f(g(m),(g(n)+d_g(m,n)) - f(g(n)) \\
&= f(d_g(m,n)) + d_f(g(n),d_g(m,n)) + d_f(g(m),g(n)+d_g(m,n))
\end{aligned}
$$

Note that d_f and d_g are bounded, and the function f is bounded over a finite domain.

Definition 3 *The set of efficient real numbers*

The set of all qhms, factored out by equivalence, is R. That is,

$$R = \{[f] \mid f \text{ a qhm}\}.$$

Definition 4 *Positive*

A qhm f is called positive if $\exists a \in Z$ such that $\forall n \in N$ f(n) $\geq a$. Let P denote the set of $[f]$ in R with f positive.

Definition 5 *Negative*

Similarly, a qhm f is called negative if $\exists b \in Z$ such that $\forall n \in N$ f(n) $\leq b$.

Definition 6 *Bounded*

A qhm f is called bounded if $|f(n)| \leq k$, for some $k \in N$.

Theorem 2 *Suppose that f is a qhm with $f(0) = 0$, additivity constant k and $\exists n \in N$ such that $f(n) > k$. Then $\forall n \in N$ f(n) $\geq -k$.*

Proof: Let $r \in N$ be the smallest natural number such that $f(r) > k$. Assume $\exists s \in N$ such that $f(s) < -k$. Since $f(0) = 0$, both r and s are strictly positive; also $r \neq s$.

If $r > s$ then $0 < r - s < r$, so the minimality of r implies $f(r-s) \leq k$, but then:

$$f(r) - f(r-s) - f(s) > k - k + k = k$$

Similarly, if $s > r$ then $0 < s - r < s$, so the minimality of s implies $f(s-r) \geq -k$, but then:

$$f(s) - f(s-r) - f(r) < -k + k - k = -k$$

Both cases contradict the assumption that f has additivity constant k. Hence, the assumption concerning the existence of s must be false and so $\forall n \in N$ $f(n) \geq -k$.

Corollary 3 *Every qhm is either positive or negative.*

Proof: Suppose instead that f is a qhm that is neither positive nor negative. Then $\exists n_1 \in N$ and $\exists n_2 \in N$ such that $f(n_1) > k$ *and* $f(n_2) < -k$. This, however, contradicts Theorem 2 so all qhms must be either positive or negative.

Let $f : N \longrightarrow Z$ be a qhm. Then the *extension* $\bar{f} : Z \longrightarrow Z$ of f, defined by:

$$\bar{f}(n) = \begin{cases} f(n), & \text{for n} \geq 0 \\ -f(-n). & \text{for n} < 0 \end{cases}$$

is a qhm having the same additivity constant as f and satisfying

$$\bar{f}(-n) = -\bar{f}(n)$$

for all integers n. Every qhm is equivalent to the extension of its restriction to N.

This means that when constructing a qhm it is sufficient to define $f(n)$ for $n \in N$ and to check the qhm property on the restricted domain.

Theorem 4 *Suppose that $f : Z \longrightarrow Z$ is a qhm with additivity constant k. Then for all $m, n \in Z$ $|f(mn) - mf(n)| \leq (|m| + 1)k$.*

Proof: The proof is by induction on m, with n fixed. When $m = 0$ $|f(0)| \leq k$, as $|f(0+0) - f(0) - f(0)| \leq k$. Note also that when $m = 1$, $|f(n) - f(n)| = 0 \leq k$.

Assume the result is true for some $m \geq 1$:

$$|f(mn) - mf(n)| \leq |m + 1|k \tag{2}$$

Furthermore, f is a qhm and so:

$$|f(mn + n) - f(mn) - f(n)| \leq k$$

Adding the above the equation and also (2) and applying the triangle inequality:

$$|f((m + 1)n) - (m + 1)f(n)| \leq (|m + 1| + 1)k$$

To show that the result is true for negative m note that:

$$|f(mn) - f((m - 1)n) - f(n)| \leq k$$
$$|f((m - 1)n) + f(n) - f(mn)| \leq k$$

Again, adding this inequality to (2) and applying the triangle inequality:

$$|f((m-1)n)-(m-1)f(n)| \leq (|m-1|+1)k$$

So the result is true for all $m \in Z$.

Theorem 5 *Every qhm $f: Z \longrightarrow Z$ is equivalent to one with additivity constant 1.*

Proof [A'C]:

For $p, q \in Z$ with $q \neq 0$, write $< p : q >$ for a choice of integer satisfying:

$$| < p : q > - \tfrac{p}{q}| \leq \tfrac{1}{2}$$

For any qhm $f : Z \longrightarrow Z$ with *additivity constant* $k \geq 1$, define $f' : Z \longrightarrow Z$ by:

$$f'(n) =< f(3k) : 3k >$$

Using Theorem 4, note that:

$$\begin{aligned} |f'(n) - f(n)| &\leq |f'(n) - \frac{f(3k)}{3k}| + |\frac{f(3kn)}{3k} - f(n)| \\ &\leq \frac{1}{2} + k + \frac{1}{3} \\ &\leq k + \frac{5}{6} \end{aligned}$$

So f and f' are equivalent.

Furthermore:

$$\begin{aligned} |f'(m+n) - f'(m) - f'(n)| &\leq |f'(m+n) - \frac{f(3k(m+n))}{3k}| + |\frac{f(3km)}{3k} - f'(m)| \\ &+ |\frac{f(3kn)}{3k} - f'(n)| + |\frac{f(3k(m+n))}{3k} - \frac{f(3km)}{3k} - \frac{f(3kn)}{3k}| \\ &\leq \frac{1}{2} + \frac{1}{2} + \frac{1}{2} + \frac{k}{3k} \\ &= \frac{11}{6} < 2. \end{aligned}$$

Theorem 6 *Suppose that $f : Z \longrightarrow Z$ is a qhm. Then $\exists a \in N$ such that $\forall n \in Z$ $f(n) \leq a|n| + k$.*

Proof: Letting $n = 1$ in Theorem 4

$$|f(m) - mf(1)| \leq (|m| + 1)k$$

Applying the triangle inequality:

$$|f(m)| \leq (|m|+1)k + |mf(1)| = |m|(k+|f(1)|) + k$$

It is sufficent to choose $a = k + |f(1)|$.

Theorem 7 *Suppose that* $f : Z \longrightarrow Z$ *is a qhm with additivity constant* k. *Then for all* $m,\ n \in Z$ $|nf(m) - mf(n)| \leq (|m|+|n|+2)k$.

Proof: From Theorem 4:

$$|f(mn) - mf(n)| \leq (|n|+1)k$$

By symmetry:

$$|f(nm) - nf(m)| = |nf(m) - f(nm)| \leq (|m|+1)k$$

Adding these two inequalities and applying the triangle inequality:

$$|nf(m) - mf(n)| \leq k(|m|+|n|+2)$$

The following two easy Lemmas are to aid the proof that multiplicative inverses exist in R.

Lemma 8 *Suppose that* $f : Z \longrightarrow Z$ *is a qhm with additivity constant* k. *Suppose further that* $M \in N$ *is constant. Then* $\forall n \in Z$ $|f(n+M) - f(n)| \leq k + |f(M)|$.

This result follows immediately from the triangle inequality and the qhm property.

Lemma 9 *Suppose that* $f : Z \longrightarrow Z$ *is a qhm with additivity constant* $k \in N$. *Suppose* $m, n, p \in Z$. *Then* $|f(m+n+p) - f(m) - f(n) - f(p)| \leq 2k$.

Proof: Since f is a qhm:
$|f(n+p) - f(n) - f(p)| \leq k$
$|f(m+n+p) - f(m) - f(n+p)| \leq k$
Adding these equations and applying the triangle inequality:
$|f(m+n+p) - f(m) - f(n) - f(p)| \leq 2k$.

Theorem 10 *R satisfies the following field axioms:*

1. (Additive associativity) $([f]+[g])+[h] = [f]+([g]+[h])$.

   Proof: For any $f \in [f]$, $g \in [g]$, $h \in [h]$:

$$\begin{aligned} &|((f+g)+h)(n) - (f+(g+h))(n)| \\ &\quad = |(f+g)(n) + h(n) - f(n) - (g+h)(n))| \\ &\quad = |f(n)+g(n)+h(n) - f(n) - g(n) - h(n)| \\ &\quad = 0 \end{aligned}$$

2. (Additive identity) $\exists[\underline{0}] \in R$ such that $[f] + [0] = [f]$ for all $[f] \in R$.

   Proof: Let $\underline{0}(n) = 0\ \forall n \in N$, this defines a homomorphism $\underline{0}$.
   Also for any $f \in [f]$: $|(f + \underline{0})(n) - f(n)| = |f(n) + \underline{0}(n) - f(n)| = 0$
   Note that $[\underline{0}]$ is the equivalence class of all bounded functions $Z \longrightarrow Z$.

3. (Additive inverse) For each $[f] \in R$ there is a $[g] \in R$ such that $[f]+[g] = [\underline{0}]$.

   Proof: For $f \in [f]$, define $g(n) = -f(n)$ for all n.
   now consider:
   $|(f + g)(n) - \underline{0}(n)| = |f(n) + g(n) - 0| = 0$

4. (Multiplicative commutativity) $[f][g] = [g][f]$.

   Proof: The aim is not to show that $f(g(n)) = g(f(n))$, but $|f(g(n)) - g(f(n))| \leq k$, that is, fg and gf are in the same equivalence class.
   Setting $m = g(n)$ in Theorem 4, and then applying Theorem 6:

   $$|nf(g(n)) - g(n)f(n)| \leq (g(n) + n)k_1 \leq nk_2$$

   Changing the roles of f and g:

   $$|ng(f(n)) - f(n)g(n)| = |f(n)g(n) - ng(f(n))| \leq nk_3$$

   Applying the triangle inequality:

   $$\begin{aligned} |nf(g(n)) - ng(f(n))| &\leq |nf(g(n)) - g(n)f(n)| + |f(n)g(n) - ng(f(n))| \\ &\leq nk_2 + nk_3 \leq nk_4 \end{aligned}$$

   $|f(g(n)) - g(f(n))| \leq k_4$

5. (Multiplicative associativity) $([f][g])[h] = [f]([g][h])$.

   Proof: For f $\in [f], g \in [g], h \in [h]$:
   $|(fg)((h(n)) - f((gh)(n))| = |f(g(h(n)) - f(g(h(n)))| = 0$.

6. (Multiplicative identity) $\exists[\underline{1}] \in R$ such that $[\underline{1}] \neq \underline{0}$ and $[f][\underline{1}] = [f]$ for all $[f] \in R$.

   Proof: Define $\underline{1}(n) = n$. Then $|f\underline{1}(n) - f(n)| = |f(\underline{1}(n)) - f(n)| = |f(n) - f(n)| = 0 \leq k$.

7. (Multiplicative inverse) For each $[f]$ in R different from $[\underline{0}]$ there $\exists[g] \in R$ such that $[f][g] = [1]$.

   Proof: Consider firstly a positive qhm $f : N \longrightarrow N \in [f]$. Define:

$$g(n) = min\{m \in N \mid f(m) \geq n\}$$

So that:

$$\begin{aligned} f(g(n)) - \underline{1}(n) &= f(g(n)) - n \\ &\geq 0 \end{aligned}$$

Since f is a qhm:

$$f(g(n)) - f(g(n) - 1) - f(1) \leq k$$

Note that $f(g(n) - 1) < n$ so:

$$f(g(n)) - n \leq k + f(1)$$

The following proof that g is a qhm is essentially that of Arthan [Ar]. Suppose that $m,\ n \in N$. From the definition of g:

$$f(g(m+n)) \geq m + n > f(g(m+n) - 1) \tag{3}$$

$$f(g(m)) \geq m > f(g(m) - 1) \tag{4}$$

$$f(g(n)) \geq n > f(g(n) - 1) \tag{5}$$

Subtracting (4), (5) from (3) we obtain:

$$f(g(m+n)) - f(g(m) - 1) - f(g(n) - 1) > 0$$

$$f(g(m+n)) - f(g(m)) + f(g(m)) - f(g(m) - 1) - f(g(n)) + \\ f(g(n)) - f(g(n) - 1) > 0$$

From Lemma 8:

$$|f(g(m)) - f(g(m) - 1)| \leq k + f(1)$$

and

$$|f(g(n)) - f(g(n) - 1)| \leq k + f(1)$$

Together the last three equations imply that:

$$f(g(m+n)) - f(g(m)) - f(g(n)) > k_1$$

Similarly one may show that:

$$f(g(m+n)) - f(g(m)) - f(g(n)) < k_2$$

Applying Theorem 7 and the triangle inequality:

$$\begin{aligned} |f(g(m+n) - g(m) - g(n))| &\leq k + |f(g(m+n)) - f(g(m)) - f(g(n))| \\ &\leq k_3 \end{aligned}$$

For $|f(g(m+n)-g(m)-g(n))|$ to be always bounded $|g(m+n)-g(m)-g(n)|$ must always be bounded, so g is a qhm.

The extension of g can be used to obtain a multiplicative inverse defined on Z.

When $[f]$ is negative, first find its positive associative inverse $[-f]$. Secondly find the multiplicative inverse $[-g]$ of $[-f]$. Then find the associative inverse $[g]$ of $[-g]$, which is a multiplicative inverse for $[f]$.

8. (Distributive law) $(i)([f]+[g])[h]=[f][h]+[g][h]$ and $(ii)[f]([g]+[h])=[f][g]+[f][h]$.

   Proof: In fact, $(f+g)\circ h = f\circ h + g\circ h$, so (i) follows. Then (ii) follows by multiplicative commutativity.

Definition 7 $[f] \geq [g]$

$[f] \geq [g]$ *iff* $f-g$ *is positive.*

Theorem 11 *R satisfies the following order axioms:*

1. (Additive Closure) $([f],[g] \in P) \Longrightarrow [f]+[g] \in P$.

   Proof: Let $f \in [f]$ and $g \in [g]$. Since $[f],[g]$ are positive $\exists a_1, a_2 \in N$ such that $\forall n \in N$:
   $f(n) > a_1$,
   $g(n) > a_2$. Now consider:
   $f(n)+g(n) > a_1 + a_2$
   $(f+g)(n) > a_1 + a_2 = a_3 \in N$

   i.e. $f+g \in P$

2. (Multiplicative Closure) $([f],[g] \in P) \Longrightarrow [f][g] \in P$.

   Proof: Since $[f]$ is positive $\exists a_1 \in N$ such that $\forall n \in N$:
   $f(n) > a_1$.
   In particular $\forall n \in N$ if $g(n) \in N$: $f(g(n)) > a_1$ so that fg is positive.

3. (Exclusivity) $([f] \in P) \Longrightarrow [-f] \notin P$.

   Proof: Let $f \in [f]$. Then $\exists a \in Z$ such that $\forall n \in N f(n) > a$. This implies that: $-f(n) < -a$.
   $(-f)(n) < -a$.
   So that $[-f]$ is negative.

4. (Trichotomy law) $([f] \in R) \Longrightarrow ([f] = [\underline{0}])$ or $([f] \in P)$ or $([-f] \in P)$.

   Proof: This is proved in Theorem 3.

Theorem 12 *Every nonempty set $S \subseteq R$ which has a lower bound has a greatest lower bound.*

Proof: Without loss of generality we can suppose that $\underline{0}$ is a lower bound for S so that S consists of positive elements. The least upper bound can be constructed in the following way. For each $s \in$ S, choose f_s representing s with additivity constant 1 and such that $\forall n \in N \ f_s(n) \geq 0$. Define:

$$\begin{aligned} g(n) &= min\{f_s(n)|s \in S\} \\ &= f_{s_n}(n) \end{aligned}$$

for an appropriate $s_n \in S$.
So that:

$$g(n) = f_{s_n}(n) \leq f_s(n) \text{ for all } s \in S.$$

Now we show that g is a qhm :

$$\begin{aligned} g(m+n) - g(m) - g(n) &\leq f_{s_{m+n}}(m+n) - f_{s_m}(m) - f_{s_n}(n) \\ &\leq f_{s_{m+m}}(m+n) - f_{s_{m+n}}(m) - f_{s_{m+n}}(n) \\ &\leq 1 \end{aligned}$$

Assume that $f_{s_n} \geq f_{s_m}$. Then $f_{s_n}(r) - f_{s_m}(r) \geq -2$ from Theorem 2. So:

$$\begin{aligned} g(m+n) - g(m) - g(n) &= f_{s_{m+n}}(m+n) - f_{s_m}(m) - f_{s_n}(n) \\ &\leq f_{s_{m+n}}(m) - f_{s_m}(m) + (-f_{s_m}(n) + f_{s_m}(n)) - f_{s_n}(n) \\ &\leq (f_{s_{m+n}}(m) - f_{s_m}(m) - f_{s_m}(n)) + (f_{s_m}(n) - f_{s_n}(n)) \\ &= 1 + 2 = 3 \end{aligned}$$

Now suppose that h is a lower bound. Then $\exists a \in N$ such that $\forall s \in S$ and $\forall n \in N$:

$$\begin{aligned} h(n) &\leq f_s(n) - a \\ &\leq min\{f_s(n)|s \in S\} - a \\ &= g(n) - a \end{aligned}$$

This implies that $h \leq g$ and so g is the greatest lower bound.

R is a complete ordered field and so must be isomorphic to the usual ordered field of real numbers.

References

[St] Ross Street, An efficient construction of the real numbers, Gazette of the Australian Math. Soc. 12 (1985) 57- 58
[A'C] Nobert A'Campo, A natural construction for the real numbers, arXiv:math.GN/0301015 v1 (3 Jan 2003)
[Ar] R. D. Arthan, The Eudoxus Real Numbers (preprint, September 2003)