MATH 355 Assignment 1

Instructor: Dr Ryan Hamilton
Name: Yifeng Pan
UCID: 30063828

Fall 2019

Yifeng Pan
UCID: 30063828

1 Determine whether or not the following functions are injective, surjective or bijective. NOTE: The natural numbers $\mathbb{N}$ exclude 0.

a $f : \mathbb{R} \to \mathbb{R}, f(x) = x^2 + 1$

Not injective. Proof:
$-1, 1, 2 \in \mathbb{R}, f(1) = 2 = f(-1)$, but $1 \neq -1$.

Not surjective. Proof:
Suppose $\exists x \in R$ such that $f(x) = 0$ where $0 \in \mathbb{R}$. Then $0 = x^2 + 1$, so $x = \sqrt{-1}$. Therefore x is not real. Contradiction.

Not bijective.

b $f : \mathbb{R} \to [0, \infty), f(x) = (x-1)^2$

Not injective. Proof by example:
$0, 2 \in \mathbb{R}, f(0) = 1 = f(2)$, but $0 \neq 2$.

Surjective. Proof:
Suppose $y \in [0, \infty)$. Let $x = \sqrt{y} + 1 \in \mathbb{R}$ where $y \geq 0$. Because y is non-negative, $y = |y| = \sqrt{y}^2 = (\sqrt{y} + 1 - 1)^2 = (x-1)^2 = f(x)$.

Not bijective.

c $f : [-\frac{1}{20}, \frac{1}{20}] \to [-1, 1], f(x) = \sin(5x)$

Injective. Proof:
Suppose $f(a), f(b) \in \mathbb{R}, f(a) = f(b)$. Then,

$$\sin(5a) = \sin(5b)$$
$$5a + 2n\pi = 5b + 2m\pi \text{ where } n, m \in \mathbb{Z}$$
$$a - b = \frac{2\pi}{5}(m - n)$$

It's easy to see that the range of $(a-b)$ is $[-\frac{1}{10}, \frac{1}{10}]$, as the domain of a, b are both $[-\frac{1}{20}, \frac{1}{20}]$. Now, if $(m-n)$, which is an integer, is ≥ 1, then $(a-b) \geq 2\pi/5 > \frac{1}{10}$, which would be a contradiction. Therefore $(m-n) \leq 0$. Now, if $(m-n) \leq -1$, then $(a-b) \leq -2\pi/5 < -\frac{1}{10}$, which would again be a contradiction. Therefore $(m-n) \geq 0$. Therefore $(m-n) = 0$. Therefore $(a-b) = 0$. Therefore $a = b$.

Not surjective. Proof:
Suppose $\exists x \in [-\frac{1}{20}, \frac{1}{20}]$, such that $f(x) = 1$. Then $\arcsin(1) = 5x$. So $x = \frac{\pi + 4n\pi}{10}$ where $n \in \mathbb{Z}$. Because $x \in [-\frac{1}{20}, \frac{1}{20}]$,

$$-\frac{1}{20} \leq x \leq \frac{1}{20}$$
$$-\frac{1}{20} \leq \frac{\pi + 4n\pi}{10} \leq \frac{1}{20}$$
$$-\frac{1}{2} \leq \pi + 4n\pi \leq \frac{1}{2}$$
$$(-\frac{1}{2} - \pi)/(4\pi) \leq n \leq (\frac{1}{2} - \pi)/(4\pi)$$
$$-0.2898... \leq n \leq -0.2102...$$

Clearly n is not an integer. Therefore contradiction. Therefore there exists no such x.

Not bijective.

d $f : \mathbb{R} \to \mathbb{R}, f(x) = x^5 + 3x^3 + 2x + 1$ **(use some calculus here if you need to)**

Lemma:
$\frac{d}{dx}(f(x)) = \frac{d}{dx}(x^5 + 3x^3 + 2x + 1) = 5x^4 + 9x^2 + 2$. It's easy to see that $5x^4 + 9x^2 + 2$ is always positive. Therefore $f(x)$ is strictly increasing.

Injective. Proof with calculus:
Suppose $f(a), f(b) \in \mathbb{R}, f(a) = f(b)$. Because f is strictly increasing, if $a < b$ then $f(a) < f(b)$. Which would be a contradiction. Therefore $a \geq b$. Similarly we can prove that $b \geq a$. So it's easy to see that $a = b$.

Corollary:
Since $f'(x) = 5x^4 + 9x^2 + 2$ which is defined for all $x \in \mathbb{R}$, f is continuous.

Surjective. Proof:
It's easy to see that $\lim_{x\to\infty}(f(x))$ approaches ∞, as $\lim_{x\to\infty}(x^5)$ approaches ∞. And it's easy to see that $\lim_{x\to-\infty}(f(x))$ approaches $-\infty$, as $\lim_{x\to-\infty}(x^5)$ approaches $-\infty$. Becasue f continuous and the domain of f is $(-\infty, \infty)$. Therefore the range of f is $(-\infty, \infty)$.

Bijective.

e $f : \mathbb{Z} \to \mathbb{Z}, f(n) = n^2 - n$

Not injective. Proof:
$1, 0 \in \mathbb{Z}, f(1) = 0 = f(0)$, but $1 \neq 0$.

Not surjective. Proof:
Suppose $\exists n \in \mathbb{Z}$ such that $f(n) = 1$ where $1 \in \mathbb{Z}$. Then $n^2 - n - 1 = 0$. Using the quadratic formula, the solutions to n are $\frac{1\pm\sqrt{5}}{2}$, which are obviously not integers.

Not bijective.

f $f : \mathbb{N} \to \mathbb{N} \cup \{0\}, f(n) = n^2 - n$

Injective. Proof:
Suppose $f(a), f(b) \in \mathbb{N}, f(a) = f(b)$. Then:

$$\begin{aligned}
a^2 - a &= b^2 - b \\
a(a-1) - b(b-1) &= 0 \\
[a(a-1) - b(b-1) + a(b-1) - b(a-1)] - a(b-1) + b(a-1) &= 0 \\
(a-b)((a-1) + (b-1)) - a(b-1) + b(a-1) &= 0 \\
(a-b)((a-1) + (b-1)) &= a(b-1) - b(a-1) \\
&= ab - a - ba + b \\
&= -a + b \\
&= -(a-b) \\
(a-b)((a-1) + (b-1)) + (a-b) &= 0 \\
(a-b)(a+b-1) &= 0
\end{aligned}$$

This means $(a-b)$ or $(a+b-1)$ is equal to zero. Since $a, b \in \mathbb{N}$, $a \geq 1, b \geq 1, a+b \geq 2, (a+b-1) \geq 1, (a+b-1) \neq 0$. Therefore, $(a-b) = 0$ or $a = b$.

Not surjective. Proof:
Suppose $\exists n \in \mathbb{N}$ such that $f(n) = 1$ where $1 \in \mathbb{N}$. Then $n^2 - n - 1 = 0$. Using the quadratic formula, the solutions to n are $\frac{1\pm\sqrt{5}}{2}$. Which are obviously not natural numbers.

Not bijective.

g $f : \mathbb{Z} \to \mathbb{Z}, f(n) = n^3 - n$

Not injective. Proof:
$1, 0 \in \mathbb{Z}, f(1) = 0 = f(0)$, but $1 \neq 0$.

Not surjective. Proof:
Suppose $\exists n \in \mathbb{Z}$ such that $f(n) = 1$ where $1 \in \mathbb{Z}$. Then $1 = n(n^2 - 1)$. It's easy to see that n and $(n^2 - 1)$ are both integers. And we know the only integer divisors of 1 are 1 and -1. Case 1: $n^2 - 1 = -1$, in which case, $n = 0$. This leads to a contradiction as $1 = 0(0^2 - 1)$. Case 2: $n^2 - 1 = 1$, in which case, $n = \sqrt{2}$. This also leads to a contradiction as $\sqrt{2} \notin \mathbb{Z}$. Therefore there does not exist $n \in \mathbb{Z}$ such that $f(n) = 1$.

Not bijective.

h $f : \mathbb{N} \to \mathbb{N} \cup \{0\}, f(n) = n^3 - n$

Injective. Proof:
Suppose $f(a), f(b) \in \mathbb{N}, f(a) = f(b)$. Then:

$$\begin{aligned}
a^3 - a &= b^3 - b \\
a(a^2 - 1) - b(b^2 - 1) &= 0 \\
[a(a^2 - 1) - b(b^2 - 1) + a(b^2 - 1) - b(a^2 - 1)] - a(b^2 - 1) + b(a^2 - 1) &= 0 \\
(a - b)((a^2 - 1) + (b^2 - 1)) - a(b^2 - 1) + b(a^2 - 1) &= 0 \\
(a - b)((a - 1) + (b - 1)) &= a(b^2 - 1) - b(a^2 - 1) \\
&= ab^2 - a - ba^2 + b \\
&= (b - a)(ab + 1) \\
(a - b)((a - 1) + (b - 1) + (ab + 1)) &= 0 \\
(a - b)(a + b + ab - 1) &= 0
\end{aligned}$$

This means $(a - b)$ or $(a + b + ab - 1)$ is equal to zero. It's easy to see that $(a + b + ab - 1) \geq 2$ with similar reasoning as (1f), Therefore, $(a - b) = 0$ or $a = b$.

Not surjective. Proof by contradiction:
Suppose $\exists n \in \mathbb{N}$ such that $f(n) = 1$ where $1 \in \mathbb{N}$. Then $n^3 - n = 1$, or $1 = n(n^2 - 1)$. It's easy to see that n and $(n^2 - 1)$ are both integers. And we know the only integer divisors of 1 are 1 and -1. But, if $n = -1$, $n \notin \mathbb{N}$. This is a contradiction. Therefore $n = 1$. So $1(1^2 - 1) = 0 = 1$. This also leads to a contradiction. Therefore there does not exist $n \in \mathbb{N}$ such that $f(n) = 1$.

Not bijective.

2 Suppose that f, g, h are functions from $\mathbb{R}$ to $\mathbb{R}$.

a Show that there does not exist f, g satisfying $f(x) + g(y) = xy$ for all $x, y \in \mathbb{R}$.

Let $f, g : \mathbb{R} \to \mathbb{R}$. Suppose there exists functions f, g such that $f(x) + g(y) = xy$. Lets choose $x = 0$, then that means $f(0)+g(y) = 0$. So $f(0) = -g(y)$ for all y. Therefore $g(y)$ is a constant. So we have $f(x)+c = xy, c \in \mathbb{R}$. Now choose $x = 1, y = 1$. Then $f(1) + c = 1$. Now choose $x = 1, y = 2$. Then $f(1) + c = 2$. Which is a contradiction. Therefore there does not exist functions f, g such that $f(x) + g(y) = xy$.

b Show that there does not exist f, g satisfying $f(x)g(y) = x + y$ for all $x, y \in \mathbb{R}$.

Let $f, g : \mathbb{R} \to \mathbb{R}$. Suppose there exists functions f, g such that $f(x)g(y) = x + y$. Lets choose $x = 0$. Then $f(0)g(y) = y$. If $f(0) = 0$ then we have an immediate contradiction, as $0 = y, \forall y \in \mathbb{R}$. Therefore $f(0) \neq 0$. Therefore $g(y) = y/f(0)$. Let $c = f(0) \neq 0, c \in \mathbb{R}$. Substitute that back into the original equation to get $f(x)y/c = x + y$. Or $f(x)y = c(x + y)$. Now choose $y = 0, x \in \mathbb{R}$. Then $0 = c(x)$. And because we know $c \neq 0$, so $x = 0, \forall x \in \mathbb{R}$. Which is a contradiction. Therefore there does not exist functions f, g such that $f(x)g(y) = x + y$.

c Show that there does not exist three functions f, g, h which satisfy

$$f(x) + g(y) + h(z) = xyz$$

for all $x, y, z \in \mathbb{R}$.

Let $f, g, h : \mathbb{R} \to \mathbb{R}$. Suppose there exists functions f, g, h such that $f(x) + g(y) + h(z) = xyz$. Lets choose $x = 0, y = 0$, then that means $f(0) + g(0) + h(z) = 0$. That means $h(z)$ is a constant for all $z \in \mathbb{R}$. So now we have $f(x) + g(y) + c = xyz, c \in \mathbb{R}$. Now choose $x = y = z = 1$. Then $f(1) + g(1) + c = 1$. And now, choose $x = y = 1, z = 2$. Then $f(1) + g(1) + c = 2$. Which is a contradiction. Therefore there do not exist functions f, g, h such that $f(x) + g(y) + h(z) = xyz$.

3 Show that the infinite product

$$\prod_{i=1}^{\infty} \{0, 1\}$$

is uncountable (you can think of this set as infinite strings of 0s and 1s).

Let S be equal to the above set. Suppose S is countable. It is clearly not finite, therefore it's denumerable. Therefore we can list the elements of S as $\{s_1, s_2, s_3 \ldots\}$. Let $i, j \in \mathbb{N}, b^i_j \in \{0, 1\}$. Where:

$$\begin{aligned} s_1 &= (b^1_1, b^1_2, b^1_3, \ldots) \\ s_2 &= (b^2_1, b^2_2, b^2_3, \ldots) \\ s_3 &= (b^3_1, b^3_2, b^3_3, \ldots) \\ &\vdots \end{aligned}$$

Let $n \in \mathbb{N}$. Let $b'_n \in \{0, 1\}$. Let $s' = (b'_1, b'_2, b'_3, \ldots)$ such that $b'_n = \begin{cases} 1 \text{ if } b^n_n = 0 \\ 0 \text{ if } b^n_n = 1 \end{cases}$. For $n \in \mathbb{N}$, $s' \neq s_n$ as s' differs from s_n in the nth index/digit. Therefore $s' \in S$ but $s' \notin \{s_1, s_2, s_3 \ldots\}$. This is a contradiction. Therefore S is uncountable.

4 Suppose x_1, x_2, y_1, y_2 are real numbers. Show that

$$x_1y_1 + x_2y_2 \leq \sqrt{x_1^2 + x_2^2}\sqrt{y_1^2 + y_2^2}$$

Fully describe the set of points for which the above inequality is an equality.

Proof:

$$\begin{aligned} x_1y_1 + x_2y_2 &\leq |x_1y_1 + x_2y_2| \\ &= \sqrt{(x_1y_1 + x_2y_2)^2} \\ &= \sqrt{x_1^2y_1^2 + 2x_1y_1x_2y_2 + x_2^2y_2^2} \\ &\leq \sqrt{x_1^2y_1^2 + x_2^2y_1^2 + x_1^2y_2^2 + x_2^2y_2^2} \text{ (Lemma)} \\ &= \sqrt{(x_1^2 + x_2^2)(y_1^2 + y_2^2)} \\ &= \sqrt{x_1^2 + x_2^2}\sqrt{y_1^2 + y_2^2} \end{aligned}$$

Lemma:

$(\sqrt{x_1^2y_1^2 + 2x_1y_1x_2y_2 + x_2^2y_2^2} \leq \sqrt{x_1^2y_1^2 + x_2^2y_1^2 + x_1^2y_2^2 + x_2^2y_2^2})$ IFF $(2x_1y_1x_2y_2 \leq x_2^2y_1^2 + x_1^2y_2^2)$.

Proof that $(2x_1y_1x_2y_2 \leq x_2^2y_1^2 + x_1^2y_2^2)$:

$$\begin{aligned} 2x_1y_1x_2y_2 &\leq (x_2y_1 - x_1y_2)^2 + 2x_1y_1x_2y_2 \\ &= x_2^2y_1^2 + x_1^2y_2^2 - 2x_1y_1x_2y_2 + 2x_1y_1x_2y_2 \\ &= x_2^2y_1^2 + x_1^2y_2^2 \end{aligned}$$

Set of points:

Using the above proof, it's easy to see that:
$x_1y_1 + x_2y_2 = \sqrt{x_1^2 + x_2^2}\sqrt{y_1^2 + y_2^2}$ IFF ($x_1y_1 + x_2y_2 = |x_1y_1 + x_2y_2|$ AND $2x_1y_1x_2y_2 = x_2^2y_1^2 + x_1^2y_2^2$).

$x_1y_1 + x_2y_2 = |x_1y_1 + x_2y_2|$ means $x_1y_1 + x_2y_2$ is non-negative.

Now,

$$\begin{aligned} 2x_1y_1x_2y_2 &= x_2^2y_1^2 + x_1^2y_2^2 \\ 0 &= x_2^2y_1^2 + x_1^2y_2^2 - 2x_1y_1x_2y_2 \\ &= (x_2y_1 - x_1y_2)^2 \end{aligned}$$

Therefore $x_2y_1 - x_1y_2 = 0, x_1y_2 = x_2y_1$.

The solutions to $x_1y_1 + x_2y_2 = \sqrt{x_1^2 + x_2^2}\sqrt{y_1^2 + y_2^2}$ are $\{x_1, x_2, y_1, y_2 \in \mathbb{R} | x_1y_1 + x_2y_2 \geq 0, x_1y_2 = x_2y_1\}$.

5

a Suppose $x < y$ are real numbers. Show that there are infinitely many distinct rational numbers q such that $x < q < y$.

Let $n \in N$ such that $1/n < (y - x)/3$ where $(y - x)/3 \in \mathbb{R}$ (corollary of the Archimedean Property). So $(yn - xn) > 3$. Therefore there are atleast two consecutive integers $i, i + 1$ between yn and xn. So we have $x < i/n < (i + 1)/n < y$, where $i/n, (i + 1)/n \in \mathbb{Q}$. Now, let $A = \{\frac{i}{n} + \frac{1}{n+k} | k \in \mathbb{N}\}$. It's easy to see that every element of A is between i/n and $(i + 1)/n$. Therefore A is an infinite set of rationals between x and y.

b Suppose $x < y$ are real numbers. Show that there are infinitely many distinct irrational numbers w such that $x < w < y$. Are there uncountably many?

Let $x, y \in \mathbb{R}$, such that $x < y$. Let $R' \subseteq \mathbb{R}$ be a set containing all reals between x and y. Let $Q' \subseteq \mathbb{Q}$ be a set containing all rationals between x and y. We know that R' is uncountably infinite. And we know that Q' is countable. Let $S = R' \setminus Q'$ be a set containing all of the irrationals between x and y. Given that a uncountably infinite set minus a countable set is still uncoutably infinite, there are an uncountably infinite number of irrationals between x and y.

6

a Find an explict injection $f : \mathbb{Q} \to \mathbb{Z}$

Let $q \in \mathbb{Q}$. Let $a \in \mathbb{Z}, b \in \mathbb{N}$ such that $(a, b) \in \mathbb{Q}$ is the irreducible fraction of q. [1] Let $m = \max(|a|, b)$. Let $n = 10$. Let $d = \lfloor \log_n(m) \rfloor + 1$ (where $\lfloor x \rfloor$ means floor of x).

$$f(q) = \begin{cases} n^{2d} + n^d a + b & \text{if } a \geq 0 \\ -(n^{2d} + n^d |a| + b) & \text{if } a < 0 \end{cases}$$

It's easy to see that $f(q) \in \mathbb{Z}$, as $n, a, b, d \in \mathbb{Z}, d \geq 1$.

Let $f^{-1} : \{f(x) | x \in \mathbb{Q}\} \to \mathbb{Q}$. Let $z \in \{f(x) | x \in \mathbb{Q}\}$. Let $n = 10$. Let $d' = \lfloor \log_n |z| \rfloor / 2$. Let $z' = |z| \mod n^{2d'}$.

$$\text{Let } a' = \begin{cases} \lfloor z' n^{-d'} \rfloor & \text{if } z \geq 0 \\ -\lfloor z' n^{-d'} \rfloor & \text{if } z < 0 \end{cases}$$

Let $b' = z' \mod n^{d'}$.

$$f^{-1}(z) = (a', b')$$

Where $(a', b') \in \mathbb{Q}$. Because there is a function from the image of f to the domain of f, f is injective.

Proof that $f^{-1}(f(q)) = q, \forall q \in \mathbb{Q}$:
The following is for the non-negative case, the negative case can be proven similarly.
$f^{-1}(f(q)) = f^{-1}(n^{2d} + n^d a + b)$. In this case $d' = \lfloor \log_n \left| n^{2d} + n^d a + b \right| \rfloor / 2 = 2d/2 = d$. [2] And $z' = (n^{2d} + n^d a + b) \mod n^{2d} = n^d a + b$. Then $a' = \lfloor (n^d a + b) n^{-d'} \rfloor = \lfloor a + b n^{-d'} \rfloor = a$. And $b' = (n^d a + b) \mod n^{d'} = b$. So $f^{-1}(f(q)) = f^{-1}(n^{2d} + n^d a + b) = (a', b') = (a, b)$, which by construction of a, b is in the same equivelence class as q.

In fact, n can be any integer ≥ 2.

For example: For $n = 10$:
$f(-137/100003) = -1000137100003$.
$f^{-1}(-1000137100003) = -137/100003$.

For $n = 2$:
$f(-137/100003) = -17197926051$.
$f^{-1}(-17197926051) = -137/100003$.

[1] I've been instructed to clarify the definition of "irreducible fraction", I've provided an attempt on page 8.
[2] $a < n^d, b < n^d$ by construction, as $d = \lfloor \log_n(\max(|a|, b)) \rfloor + 1$.

b Find an explict injection $g : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Z}$

Let $q_1, q_2 \in \mathbb{Q}$. Let $a_1, a_2 \in \mathbb{Z}$ and $b_1, b_2 \in \mathbb{N}$ such that $(a_1, b_1), (a_2, b_2) \in \mathbb{Q}$ are the irreducible fractions of q_1 and q_2 respectively. Let $a_1' = |a_1|$. Let $a_2' = |a_2|$. For $i \in \{1, 2\}$, let

$$s_i = \begin{cases} 0 & \text{if } a_i \geq 0 \\ 1 & \text{if } a_i < 0 \end{cases}$$

Let

$$g(q_1, q_2) = (2^{a_1'})(3^{a_2'})(5^{b_1})(7^{b_2})(11^{s_1})(13^{s_2})$$

It's easy to see that $g(q) \in \mathbb{Z}$.

Proof that g is injective:
Suppose $g(q_1, q_2) = g(\bar{q}_1, \bar{q}_2)$. This means:

$$\begin{aligned} &(2^{a_1'})(3^{a_2'})(5^{b_1})(7^{b_2})(11^{s_1})(13^{s_2}) \\ =&(2^{\bar{a}_1'})(3^{\bar{a}_2'})(5^{\bar{b}_1})(7^{\bar{b}_2})(11^{\bar{s}_1})(13^{\bar{s}_2}) \end{aligned}$$

Due to the unique-prime-factorization theorem, $a_1' = \bar{a}_1', a_2' = \bar{a}_2'$ and so on. From the construction of a_i' and s_i in g we know:

$$a_i = \begin{cases} a_i' & \text{if } s_i = 0 \\ -a_i' & \text{if } s_i = 1 \end{cases}$$

Because $a_1' = \bar{a}_1'$ and $s_1 = \bar{s}_1$, so $a_1 = \bar{a}_1$. And similarly $a_2 = \bar{a}_2$. Therefore:

$$[q_1, q_2] = [(a_1, b_1), (a_2, b_2)] = [(\bar{a}_1, \bar{b}_1), (\bar{a}_2, \bar{b}_2)] = [\bar{q}_1, \bar{q}_2]$$

c Find an explict injection $h : \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$

The idea of this function is similar to (6a): "Allocate memory" with a leading digit, then concatenate some number using some base (n). It this case, an additional digit is allocated per number, to indicate the signs. And the third input is used to generate n (the key), and the output is the coded message and the key.

Let $z_1, z_2, z_3 \in \mathbb{Z}$. For $j \in \{1, 2, 3\}$, let $z_j' = |z_j|$. Let

$$s_j = \begin{cases} 0 & \text{if } z_j \geq 0 \\ n^{d-1} & \text{if } z_j < 0 \end{cases}$$

Where $m = \max(z_1', z_2', z_3')$, $n = z_3' + 2$, $d = \lfloor \log_n(m) \rfloor + 2$.
Let $i = n^d$. Let

$$h(z_1, z_2, z_3) = [i^3 + i^2(z_1' + s_1) + i^1(z_2' + s_2) + i^0(z_3' + s_3), n]$$

Where $h(z_1, z_2, z_3) \in \mathbb{Z} \times \mathbb{Z}$.

Let $h^{-1} : \{h(a, b, c) | a, b, c \in \mathbb{Z}\} \to \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$. Let $(z, n) \in \{h(a, b, c) | a, b, c \in \mathbb{Z}\}$, where $n \geq 2$. Let $d = \lfloor \log_n(z) \rfloor / 3$. Let $i \in \{1, 2, 3\}$,

$$t_i = \begin{cases} z & \text{if } i = 3 \\ \lfloor n^{-d} t_{i+1} \rfloor & \text{otherwise} \end{cases}$$

$a_i = t_i \mod n^{d-1}$, and $s_i = t_i \mod n^d$. Let

$$a_i' = \begin{cases} a_i & \text{if } a_i = s_i \\ -a_i & \text{otherwise} \end{cases}$$

Let

$$h^{-1}(z, n) = (a_1', a_2', a_3')$$

Proof that $h^{-1}(h(z_1, z_2, z_3)) = (z_1, z_2, z_3), \forall z_1, z_2, z_3 \in \mathbb{Z}$:
$h^{-1}(h(z_1, z_2, z_3)) = h^{-1}(i^3 + i^2(z'_1 + s_1) + i^1(z'_2 + s_2) + i^0(z'_3 + s_3), n)$. In this case, $d' = \lfloor \log_n(i^3 + i^2(z'_1 + s_1) + i^1(z'_2 + s_2) + i^0(z'_3 + s_3)) \rfloor / 3 = 3d/3 = d$. [3] Now, substituting these values into the functions in h^{-1} we get:

$$\begin{cases} t_3 = i^3 + i^2(z'_1 + s_1) + i^1(z'_2 + s_2) + i^0(z'_3 + s_3) \\ t_2 = i^2 + i^1(z'_1 + s_1) + i^0(z'_2 + s_2) \\ t_1 = i^1 + i^0(z'_1 + s_1) \end{cases} \quad \begin{cases} s'_3 = i^0(z'_3 + s_3) \\ s'_2 = z'_2 + s_2 \\ s'_1 = z'_1 + s_1 \end{cases} \quad \begin{cases} a_3 = z'_3 \\ a_2 = z'_2 \\ a_1 = z'_1 \end{cases}$$

From the construction of z'_j and s_j in h we know:

$$z_k = \begin{cases} z'_k & \text{if } s_k = 0 \\ -z'_k & \text{if } s_k = 1 \end{cases}$$

Where $k = \{1, 2, 3\}$. And we know from h^{-1} that:

$$a'_k = \begin{cases} a_k & \text{if } a_k = s'_k \\ -a_k & \text{otherwise} \end{cases}$$

Because $a_k = z'_k$ and $(a_k = s'_k) \leftrightarrow (z'_k = z'_k + s_k) \leftrightarrow (s_k = 0)$, [4] so $z_k = a'_k$. Therefore $h^{-1}(h(z_1, z_2, z_3)) = h^{-1}(i^3 + i^2(z'_1 + s_1) + i^1(z'_2 + s_2) + i^0(z'_3 + s_3), n) = (a'_1, a'_2, a'_3) = (z_1, z_2, z_3)$

In fact, in this case, n can be any function of (z_1, z_2, z_3) where the output is an integer ≥ 2.

For example: For $n = ((137 \times z_3) \mod 100003) + 2$: [5]
$h(-631278, 432132, -1238790432) = (71109478284907550659406353357569842738 16, 2094)$.
$h^{-1}(71109478284907550659406353357569842738 16, 2094) = (-631278, 432132, -1238790432)$.

Note

Rationals numbers can be defined as equivalence classes of ordered pairs of integers (p, q) such that $q \neq 0$, where the equivalence relation is defined so that $(p_1, q_1) \sim (p_2, q_2)$ IFF $p_1 q_2 = p_2 q_1$. [6]

Definition:
Let $(p, q) \in \mathbb{Q}$. Let the **irreducible fraction** of (p, q) be defined as $(a, b) \in Q$ such that $(a, b) \sim (p, q), b > 0$, and $\forall (i, j) \in \mathbb{Q}$: if $(a, b) \sim (i, j)$ then $|a| \leq |i|$ (or equivalently: if $(a, b) \sim (i, j)$ then $b \leq |j|$).

Proof that every element of $\mathbb{Q}$ has an irreducible fraction:
Let $(p, q) \in \mathbb{Q}$. Let $n = gcd(p, q)$ as $q \neq 0$. If $q > 0$, then let $a = p/n, b = q/n$. If $q < 0$, then let $a = -p/n, b = -q/n$. It's obvious that a and b are both integers and $gcd(a, b) = 1$, and $b > 0$ in both cases. Now, $p(q/n) = (p/n)q$ and $p(-q/n) = (-p/n)q$. Therefore $(a, b) \sim (p, q)$ in both cases.

Now suppose $(i, j) \in \mathbb{Q}$ such that $(a, b) \sim (i, j)$. So $aj = bi$. If $gcd(i, j) = 1$, then $gcd(i, a) = |i|$ (this follows from the fact that aj and bi has the same prime factorization). As $gcd(a, b) = 1$ by construction, so $gcd(i, a) = |a|$. Therefore $|a| = |i|$. If $gcd(i, j) = n > 1$, then let $c = i/n, d = j/n$ where $gcd(c, d) = 1$. So $and = bnc$, $ad = bc$. From here we can prove that $|a| = |c|$ similarly from before. [7] Therefore $|a| = |c| = |i/n| < |i|$. Therefore $|a| \leq |i|$ in both cases.

Proof that the irreducible fraction is unique for each equivalence class:
Suppose $(a, b), (c, d)$ are irreducible fractions of any equivalence class of $\mathbb{Q}$. So $(a, b) \sim (c, d)$. Therefore $b \leq |d|$. Similarly we can prove that $d \leq |b|$. And because b, d are both positive, $b = d$. Now, we know $ad = cb$. Therefore $a = c$. Therefore the irreducible fraction is unique.

[3] $\forall j \in \{1, 2, 3\}, (z'_j + s_j) < i = n^d$ by construction in h.
[4] And "otherwise" IFF $s_k = 1$, as theres only two cases.
[5] Using a Haskell script I wrote: `https://pastebin.com/nTEV7QvR`
[6] From `https://en.wikipedia.org/wiki/Rational_number`.
[7] $gcd(a, b) = gcd(c, d) = 1$.

7 Supoose A and B are both bounded subsets of $\mathbb{R}$. Find an property $\mathcal{X}$ so that the statement $\sup A = \inf B$ if and only if $\mathcal{X}$ is true.

Property $\mathcal{X}$: $\forall a \in A, \forall b \in B, a \leq b$ AND $\forall \epsilon \in \mathbb{R}, \epsilon > 0, \exists x \in A, y \in B$ such that $y - x < \epsilon$.

If $\mathcal{X}$ then $\sup A = \inf B$. Proof:
Suppose $\mathcal{X}$. Suppose $\sup A > \inf B$. We know that $\forall a \in A, \forall b \in B, a \leq b$. Therefore $\inf B$ is an upper-bound of A. Contradiction. Now suppose $\sup A < \inf B$. Now, set $\epsilon = \inf B - \sup A > 0$. Then $\forall a \in A, b \in B$: $b - a \geq \sup B - a \geq \sup B - \inf A = \epsilon$. Therefore $b - a \not< \epsilon$. Contradiction. Therefore $\sup A = \inf B$.

If $\sup A = \inf B$ then $\mathcal{X}$. Proof:
Suppose $\sup A = \inf B$. This means that $\forall a \in A, b \in B, a \leq \sup A = \inf B \leq b$. Now, let $\epsilon \in \mathbb{R}, \epsilon > 0$. We know $\exists x \in A$ such that $x > \sup A - \epsilon/2$ (otherwise $\sup A - \epsilon/2$ would be a upper bound). We also know that $\exists y \in B$ such that $y < \inf B + \epsilon/2$ (otherwise $\inf B + \epsilon/2$ would be a lower bound). Now,

$$\begin{aligned}
\epsilon &= \epsilon + \inf B - \inf B \\
&= (\inf B + \frac{\epsilon}{2}) - (\inf B - \frac{\epsilon}{2}) \\
&= (\inf B + \frac{\epsilon}{2}) - (\sup A - \frac{\epsilon}{2}) \\
&> y - (\sup A - \frac{\epsilon}{2}) \\
&> y - x
\end{aligned}$$

Therefore $\mathcal{X}$.

Therefore $\sup A = \inf B$ IFF $\mathcal{X}$.

Citations

Proofread by Devin Kwok (UCID: 10016484).