Beurling Integers: Part 2

Isomorphisms

Devin Platt

July 11, 2015

1 Prime Factorization Sequences

In the last article we introduced the Beurling generalized integers, which can be represented as a sequence of real numbers or as a multiplication function over the natural numbers. These two representations are isomorphic, though we really only showed how to get a multiplication function from a given sequence of real numbers. To go in the opposite direction, we actually need to introduce a third representation: a sequence of prime factorizations.

To discuss prime factorizations, we need to have a way of representing the factorizations as objects themselves. One representation we can use is exponent vectors, which are best explained with examples (see Table 1).

This notation invites analogies to a vector space, although the natural numbers do not form a field so we do not have a vector space. Nonetheless, some typical operations have natural correspondence. Multiplication corresponds to vector addition and exponentiation corresponds to scalar multiplication. The prime numbers correspond to unit (basis) vectors in an infinite dimensional space. Since the vectors live in an infinite dimensional space, we require a finite representation. In the table above the vectors have their tail sequences of zeros cut off, but generally this isnt the most compact representation. We also write factorizations as sets of (prime, exponent) pairs eg.

$$\langle 2,0,5\rangle \text{ corresponds to } \{(1,2),(3,5)\}$$

This pair representation is akin to writing a vector as a linear combination of basis vectors. The set of pairs representation tends to be more convenient when a vector is sparse (ie. it has many zeros

Table 1: Comparing representations of the sequence of natural numbers

Natural Number	Prime Factorization	Sequence of Prime Exponents	Exponent Vector (Truncated Zeros)
1	none	0,0,0,0,0,0,...	$\langle 0\rangle$
2	2	1,0,0,0,0,0,...	$\langle 1\rangle$
3	3	0,1,0,0,0,0,...	$\langle 0,1\rangle$
4	2^2	2,0,0,0,0,0,...	$\langle 2\rangle$
5	5	0,0,1,0,0,0,...	$\langle 0,0,1\rangle$
6	$2\cdot 3$	1,1,0,0,0,0,...	$\langle 1,1\rangle$
7	7	0,0,0,1,0,0,...	$\langle 0,0,0,1\rangle$
8	2^3	3,0,0,0,0,0,...	$\langle 3\rangle$
9	3^2	0,2,0,0,0,0,...	$\langle 0,2\rangle$
10	$2\cdot 5$	1,0,1,0,0,0,...	$\langle 1,0,1\rangle$
11	11	0,0,0,0,1,0,...	$\langle 0,0,0,0,1\rangle$
12	$2^2\cdot 3$	2,1,0,0,0,0,...	$\langle 2,1\rangle$

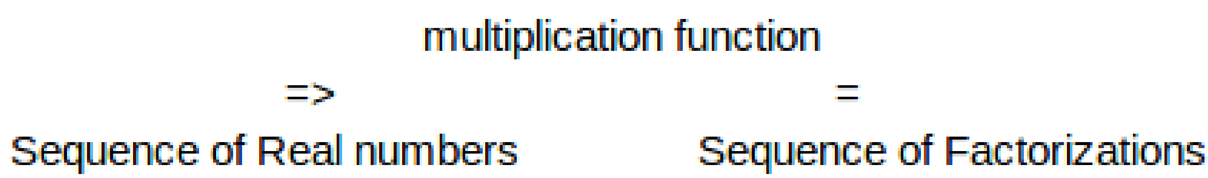
Table 2: Comparing factorization orderings of the natural numbers and the odds

Natural Number	Natural Vector	Odd Vector	Odd Number
1	$\langle 0\rangle$	$\langle 0\rangle$	1
2	$\langle 1\rangle$	$\langle 1\rangle$	3
3	$\langle 0,1\rangle$	$\langle 0,1\rangle$	5
4	$\langle 2\rangle$	$\langle 0,0,1\rangle$	7
5	$\langle 0,0,1\rangle$	$\langle 2\rangle$	9
6	$\langle 1,1\rangle$	$\langle 0,0,0,1\rangle$	11
7	$\langle 0,0,0,1\rangle$	$\langle 0,0,0,0,1\rangle$	13
8	$\langle 3\rangle$	$\langle 1,1\rangle$	15
9	$\langle 0,2\rangle$	$\{(6,1)\}$	17
10	$\langle 1,0,1\rangle$	$\{(7,1)\}$	19
11	$\langle 0,0,0,0,1\rangle$	$\langle 1,0,1\rangle$	21
12	$\langle 2,1\rangle$	$\{(8,1)\}$	23

between non-zero elements – it contains a large prime, but is a relatively small number). Moreover, the pair representation makes sense when discussing powers of primes because then each number has only one pair (in this case representation is really as concise as is possible). Since multiplication can be chained, we can consider it as a map from multisets (sets where multiplicity is allowed) of natural numbers to a natural number, instead of a map just from pairs of natural numbers to a natural number. If we restrict the domain to multisets of prime numbers, then the uniqueness of prime factorization guarantees that this map is injective – only one item in the domain maps to some number in the range. We could also define the map from the singleton multiset (of a prime number) as an identity mapping, which would allow the map to be surjective. This new form of the multiplication function is thus a bijection with the natural numbers as its range, which means that it is equivalent to a sequence: an ordering of its domain. So every multiplication function corresponds to an ordering of prime factorizations. For example, we can compare the orderings of the natural numbers and the odd numbers as in Table 2.

We can consider a triangle of isomorphic representations of the Beurling generalized integers as seen in Figure 1. We have shown that the multiplication functions and sequences of Factorizations are isomorphic. We have also shown that sequences of real numbers determine multiplication functions.

Figure 1: Isomorphism Triangle



Now quite obviously, a sequence of all factorizations determines the orderings of prime powers, since these are just subsequences. In section 4 of the paper, “Beurling Zeta Functions, Generalised Primes, and Fractal Membranes”, Lapidus and Hilberdink prove the isomorphism between orderings of prime powers and the sequence of real numbers representation, which completes our isomorphism triangle. I shall reproduce their proof here (using some of their notations, which hopefully can be inferred if I neglect to define them), which takes the form of two theorems and a lemma. Just proving one direction, that an ordering of prime powers determines a sequence of real numbers, should be sufficient to complete the isomorphism triangle. (As an aside, the basics of the proof rely on using the ordering to pin values of any power of any prime p_n between some power n of p_1 and the next power n+1. I had always suspected such an approach could be used in this proof, but my attempts failed in vain. For this reason the relative simplicity and the elegance of the following proofs always impressed me.)

2 The Lapidus-Hilberdink Proof

Notes:

- This proof uses some elementary real analysis. If youre not interested, you can skim or skip the proof and move on to the other posts in the series.
- For a given system of generalized integers, the authors use $\mathcal{P}$ to refer to the set of associated primes (as real numbers). They use $\mathcal{N}$ to refer to the set of integers generated by $\mathcal{P}$.
- This proof requires the infinitude of both primes and composites.
- This is largely a verbatim copy of their proof, with some small changes and my own notes thrown in.
- For the proofs of each individual theorem/lemma I provide a digest in brackets [], mostly for my own convenience as this article serves as a personal reference.

The first part of the proof comes from that the recognition that if a sequence of numbers is defined as another sequence with each element taken to some fixed power greater than zero, then the multiplication function remains the same. For example, with the squares of the natural numbers, four times four equals 16, so $m(2,2) = 4$. In general, if $b_n = a_n^\lambda$, then $b^{-1}(x) = a^{-1}(x^{1/\lambda})$ and multiplication for b_n can be defined as:

$$m(x, y) = b^{-1}(b_x \cdot b_y) = a^{-1}((a_x^\lambda \cdot a_y^\lambda)^{1/\lambda}) = a^{-1}(a_x \cdot a_y)$$

It turns out the converse is true, if the multiplication function (and hence the factorization ordering) is the same for two sequences of real numbers, then the sequences must be some power of each other. (Note that the converse is only true assuming that we have in infinite number of composite numbers.) Here is the exact theorem due to Lapidus and Hilberdink (with a nearly verbatim copy of the proof):

2.1 Theorem:

Let $\mathcal{P}_1$ and $\mathcal{P}_2$ be two generalized prime systems with generalized integers $\mathcal{N}_1$ and $\mathcal{N}_2$ respectively. If the orderings of $\mathcal{N}_1$ and $\mathcal{N}_2$ coincide, then $\mathcal{P}_1 = \mathcal{P}_2^\lambda$ for some $\lambda > 0$ and hence $\mathcal{N}_1 = \mathcal{N}_2^\lambda$.

[Proof notes: bound p_k^m, q_k^m by powers of p_1, q_1 to $n, n+1$, take log. Now forms of p_k^m and q_k^m are bounded by the same numbers $n, n+1$ and we can use substitution to get ps and qs in same inequality. Taking limit as $m \to \infty$ gives us our result.]

2.2 Proof:

Denote the primes in $\mathcal{P}_1$ by $p1, p_2, \ldots$, and those in $\mathcal{P}_2$ by $q_1, q_2, \ldots$. Let $k, m \in \mathbb{N}$. Then $p_k^m \in [p_1^n, p_1^n + 1)$ for some $n \in \mathbb{N}$. Since $\mathcal{N}_2$ has the same ordering as $\mathcal{N}_1$ we also have $q_k^m \in [q_1^n, q_1^n + 1)$. Taking logs gives:

$$n \leq \frac{mlog(p_k)}{log(p_1)} < n+1 \text{ and } n \leq \frac{mlog(q_k)}{log(q_1)} < n+1$$

ie. $n = \lfloor \frac{mlog(p_k)}{log(p_1)} \rfloor = \lfloor \frac{mlog(q_k)}{log(q_1)} \rfloor$. So we can relate the sequences q_n and p_n

$$\frac{mlog(p_k)}{log(p_1)} - 1 < n \leq \frac{mlog(q_k)}{log(q_1)} < n+1 \leq \frac{mlog(p_k)}{logp_1} + 1$$

and hence

$$\frac{log(p_k)}{log(p_1)} - \frac{1}{m} < \frac{log(q_k)}{log(q_1)} < \frac{log(p_k)}{log(p_1)} + \frac{1}{m}$$

This holds for all m, so letting $m \to \infty$ gives

$$\frac{log(p_k)}{log(p_1)} = \frac{log(q_k)}{log(q_1)}$$

i.e. $p_k = q_k^\lambda$, where $\lambda = \frac{log(p_1)}{log(q_1)}$, and hence $\mathcal{P}_1 = \mathcal{P}_2^\lambda$ $\square$

2.3 Axioms

Lapidus and Hilberdink note the subsequence of $\mathcal{N}$ as of powers of real numbers,

$$\mathcal{Q} = \{p^n : p \in \mathcal{P}, n \in \mathbb{N}\}$$

and remark that $\mathcal{Q}$ is isomorphic to $\mathbb{N}^2$ via the isomorphism $p_m^n \mapsto (m, n)$. They define three axioms regarding the order $\mathcal{Q}$ imposes on $\mathbb{N}^2$, which correspond to the properties we defined for multiplication earlier:

- A1: $(m, n) \leq (m, n)$ whenever both $m \leq m$ and $n \leq n$, with strict inequality if $n < n$
- A2: $(m, n) \leq (mn)$ implies $(m, kn) \leq (m, kn)$ for every $k \in \mathbb{N}$, with strict inequality if $(m, n) < (m, n)$.
- A3: Finiteness: (i) For all $n \in \mathbb{N}$, there exists $k \in \mathbb{N}$ such that $(1, n) < (k, 1)$. (ii) For all $m \in \mathbb{N}$, there exists $l \in \mathbb{N}$ such that $(m, 1) < (1, l)$.

A3 corresponds to having infinitely many composites and infinitely many primes, so that we have an order on all of $\mathbb{N}^2$. One can view A1 and A2 as corresponding to increasingness and translation invariance, respectively. The final theorem requires a lemma. The purpose of the lemma is as follows. We know that sequences of numbers generate the same system when they are powers of each other, and we just showed that this is actually the only case. Thus we should be able to generate unique values of the primes given an order of prime powers if we choose a value of the first prime (the values of all the integers are in turn determined by the values of the primes, hence why we only need to care about the order of prime powers.) We could the write the value of any k^{th} prime as a real (and non-integral) power of the first prime, $power(k)$. We can bound any power n of a k^{th} prime by powers of the first prime, and if we choose some power $f_k(n)$ to give the maximum lower bound then $f_k(n)+1$ will give the minimum upper bound (if one of these bounds need be nonstrict the other could be strict.) Now for any such n we have an inequality:

$$\frac{f_k(n)}{n} < power(k) < \frac{f_k(n)+1}{n}$$

For example, with the natural numbers $3 \approx 2^{1.58496\ldots}$, ie. $power(2) = 1.58496\ldots$ ($power(2)$ refers to 3 as the second prime). Our first inequalities imply

$$2 < 3 < 4 \implies 1 < power(2) < 2$$
$$8 < 9 < 16 \implies 1.5 < power(2) < 2$$
$$16 < 27 < 32 \implies 1.33\ldots < power(2) < 1.66\ldots$$

Even after the first few inequalities, we are able to bound $1.5 < power(2) < 1.66\ldots$, which given $p_1 = 2$ puts our guess for 3s value at $2.8284\ldots < 3 < 3.1718\ldots$ We would hope that $sup\frac{f_k(n)}{n} = power(n)$ or even that $lim_{n\to\infty}\frac{f_k(n)}{n} = power(n)$. (This basically is what I had hoped before finding the Lapidus-Hilberdink paper, but I was never able to arrive at a proof.)

The following lemma aids in our proof of the theorem by showing a condition for which the limit of $\frac{f_k(n)}{n}$ exists.

2.4 Lemma

Let $f : \mathbb{N} \to \mathbb{R}$ be such that for all $m, n \in \mathbb{N}$

$$\left|\frac{f(mn)}{mn} - \frac{f(n)}{n}\right| \le \frac{1}{n} \tag{1}$$

then $lim_{n\to\infty}\frac{f(n)}{n}$ exists.

[Proof notes: show that $\frac{f(n)}{n}$ is bounded. Then show that $\frac{f(mn)}{mn}$ approaches the same limit as $\liminf \frac{f(n)}{n}$ (using the fact that there exists a sequence n_k for which $\frac{f(n_k)}{n_k}$ approaches this limit). Then use this to show that $\frac{f(n)}{n}$ approaches this limit.]

2.5 Proof

By putting $n = 1$ into the condition (1) it follows that $\frac{f(n)}{n}$ is bounded. Let

$$\alpha = \liminf_{n\to\infty} \frac{f(n)}{n}$$

By definition of α, there exists sequence n_k tending to infinity with k such that

$$\frac{f(n_k)}{n_k} \to \alpha \text{ as } k \to \infty$$

Hence, for fixed $m \in \mathbb{N}$, we have $\frac{f(mn_k)}{mn_k} \to \alpha$ as $k \to \infty$, since

$$\left|\frac{f(mn_k)}{mn_k} - \frac{f(n_k)}{n_k}\right| \le \frac{1}{n_k}$$

(and $\frac{f(n_k)}{n_k} \to \alpha$ while $\frac{1}{n_k} \to 0$) Now fix $n \in \mathbb{N}$, put $m = n_k$ in the initial condition and let $k \to \infty$. Then

$$\left|\frac{f(nn_k)}{nn_k} - \frac{f(n)}{n_k}\right| \le \frac{1}{n}$$

Since $\frac{f(nn_k)}{nn_k} \to \alpha$ as $m \to \infty$ we have

$$\left|\frac{f(n)}{n} - \alpha\right| \leq \frac{1}{n}$$

and the result follows. $\square$

2.6 Theorem

Given an order on $\mathbb{N}^2$ satisfying axioms A1-A3, there exists a generalized prime system $\mathcal{P}$ which induces this order.

[Proof notes: Fix the k^{th} prime. Bound the n^{th} power of this prime (k, n) from below by some maximal power $f_k(n)$ of p_1 (so $f_k(n)+1$ bounds it above). Note that this inequality is preserved if we replace n by some mn (because it is simply a substitution), or if we multiply all the powers by some m (due to translation invariance). We mix these these derived inequalities since the middle term (k, mn) is the same. For this proof Lapidus specifically gives that the lefthand side of one inequality is less than the righthand side of the other, since the inequalities have the same middle term, but note that an even stronger result is quite obvious: since $f_k(mn)$ gives a maximal lower bound (and hence $f_k(mn)$ gives a minimal upper bound) we have that the lower bound $mf_k(n) \leq f_k(mn)$ and the upper bound $m(f_k(n) + 1) \geq f_k(mn)$. We can write this in one line:

$$(1, mf_k(n)) \leq (1, f_k(mn)) \leq (k, mn) < (1, f_k(mn) + 1) \leq (1, m(f_k(n) + 1))$$

and it is even more apparent that the first term is less than the fourth term and the second term is less than the fifth. Taking those two inequalities, we can create corresponding inequalities for the exponents, since the inequalities are on powers of the same prime. These new inequalities can be combined and adjusted so that the condition (1) of the Lemma is applicable. We define our sequence of real numbers by letting $p_k = p_1^{\alpha_k}$, where α_k is the limit of $\frac{f_k(n)}{n}$. At this point, letting $m \to \infty$ leads to our result, since inequalities $p_n^m < p_{n'}^{m'}$ on our sequence of real numbers imply inequalities on $f_k(n)$, which in turn implies inequalities $(m, n) < (m', n')$ on our ordering of $\mathbb{N}^2$.]

2.7 Proof

Fix $k \in \mathbb{N}$. For $n \in \mathbb{N}$, let $f_k(n)$ be the unique positive integer for which

$$(1, f_k(n)) \leq (k, n) < (1, f_k(n) + 1) \tag{2}$$

(*Im not sure why nonstrict inequality is necessary here (for k=1?), but it doesnt really matter.) This exists on account of A2 and A3, and is unique by A1. Replacing n by mn, we have

$$(1, f_k(mn)) \leq (k, mn) < (1, f_k(mn) + 1) \tag{3}$$

On the other hand, A2 implies that (given the first equation, (2))

$$(1, mf_k(n)) \leq (k, mn) < (1, m(f_k(n) + 1)) \tag{4}$$

(3) and (4) give

$$\begin{aligned}&(1, f_k(mn)) < (1, m(f_k(n) + 1)), \text{ and}\\&(1, mf_k(n)) < (1, f_k(mn) + 1)\end{aligned}$$

These inequalities involve the same prime base and thus we can apply the inequality to their exponents

$$f_k(mn) < mf_k(n) + m \text{ and} \tag{5}$$
$$mf_k(n) < f_k(mn) + 1 \tag{6}$$

Combining these and dividing through by mn gives

$$\frac{f_k(n)}{n} - \frac{1}{mn} < \frac{f(mn)}{mn} < \frac{f_k(n)}{n} + \frac{1}{n} \tag{7}$$

Thus $f_k(n)$ satisfies the condition of the Lemma (1), that its distance from $\frac{f(mn)}{mn}$ is less than $\frac{1}{n}$. This means that $\frac{f_k(n)}{n} \to \alpha_k$ for some α_k. Now choose some $p_1 > 1$ and define a system of generalized primes such that $p_k = p_1^{\alpha_k}$. We shall prove that this system induces the given ordering on prime powers.

Letting $m \to \infty$ in (6) we have that

$$f_k(n) < n\alpha_k < f_k(n) + 1$$

If $p_m^n < p_m^n$ (i.e. $n\alpha_m < n\alpha_m$) then,

$$f_m(n) \leq n\alpha_m < n\alpha_m \leq f_m(n) + 1$$

Since $f_m(n)$ and $f_m(n)$ are integers, this implies that $f_m(n) \leq f_m(n)$, i.e. $(m,n) \leq (m,n)$. [The equality case can be illustrated by example. Imagine the numbers 25 and 27 in the case of the natural numbers. We have that $p_3^2 < p_2^3$, but that $f_3(2) = f_2(3)$. However, $\lfloor log_2(25^3) \rfloor < \lfloor log_2(27^3) \rfloor$, so $f_3(3 \cdot 2) < f_2(3 \cdot 3)$. So we can amend the argument with a call to translation invariance.]

Now if $(m,n) = (m,n)$, then $(m,kn) = (m,kn)$ for all $k \in \mathbb{N}$ by A2. Hence $\frac{f_m(kn)}{k} = \frac{f_m(kn)}{k}$ and, letting $k \to \infty$, we have $n\alpha_m = n\alpha_m$, i.e. $p_m^n = p_m^n$. This shows that $p_m^n < p_m^n$ implies that $(m,n) < (m,n)$. $\square$

This proof concludes Part 2 of the series and our introduction to the Beurling generalized integers. The following articles in the series will explore the partial order that the generalized integers impose on the set of factorizations.