Beurling Generalized Integers with the Delone Property

Jeffrey C. Lagarias

AT&T Labs – Research
Florham Park, NJ 07932

(August 27, 1997)

Abstract

A set $\mathcal{N}$ of Beurling generalized integers consists of the unit $n_0 = 1$ plus the set $n_1 \le n_2 \le \dots$ of all power products of a set of generalized primes $1 < g_1 \le g_2 \le g_3 \le \dots$ with $g_i \to \infty$, with these power products arranged in increasing order and counted with multiplicity. We say that $\mathcal{N}$ has the Delone property if there are positive constants r, R such that $R \ge n_{i+1} - n_i \ge r$ for all $i \ge 1$. Any set $\mathcal{N}$ with the Delone property has unique factorization into irreducible elements and is therefore a subsemigroup of $\mathbb{R}^+$. We classify all such semigroups which are contained in the integers $\mathbb{Z}^+$. The set of generalized primes of any such $\mathcal{N}$ consists of all but finitely many primes, plus finitely many other composites.

Keywords: arithmetical semigroup, Beurling generalized integers, Delone set, geometric crystallography, Riemann hypothesis

AMS Classification: Primary 11N80

Beurling Generalized Integers with the Delone Property

Jeffrey C. Lagarias

AT&T Labs – Research
Florham Park,NJ 07932

(August 27, 1997)

1. Introduction

This paper studies sets of Beurling generalized integers which have an "evenly-spaced" property, the Delone property, defined below. Recall that a set $\mathcal{G}$ of *Beurling generalized prime numbers*, or *g-primes*, consists of any infinite set $\mathcal{G} = \{g_i : i \geq 1\}$ of real numbers such that

$$1 < g_1 \leq g_2 \leq g_3 \leq \dots \ , \tag{1.1}$$

with $g_i \to \infty$ as $i \to \infty$. The set $\mathcal{N}$ of *Beurling generalized integers*, or *g-integers*, associated to $\mathcal{G}$, consists of the unit 1 together with all finite power-products of g-primes, arranged in increasing order and counted with multiplicity. Thus $\mathcal{N}$ has elements

$$1 = n_0 < n_1 \leq n_2 \leq n_3 \leq \dots \tag{1.2}$$

Here $\mathcal{N}$ is the free abelian multiplicative semigroup (with unit) generated by $\mathcal{G}$, since we treat different power products of the g_i as distinct. It is an *arithmetical semigroup of* $\mathbb{R}^+$ in the sense of Knopfmacher [11], using the trivial norm $|n| = n$.

A set $\mathcal{N}$ of Beurling generalized integers has the *Delone property* if the gaps between successive members of $\mathcal{N}$ are bounded above and below, i.e. there are positive constants r and R such that

$$R \geq n_{i+1} - n_i \geq r \ , \quad \text{all } i \geq 1 \ . \tag{1.3}$$

Note that if $\mathcal{N}$ has the Delone property, then all elements of $\mathcal{N}$ have multiplicity one, hence each element of $\mathcal{N}$ uniquely factors as a product of elements of $\mathcal{G}$. It follows that $\mathcal{N}$ is a subsemigroup of $\mathbb{R}^+$ with unit, and we then call it an *arithmetical Delone semigroup*. An arithmetical Delone semigroup $\mathcal{S}$ is a subsemigroup of $\mathbb{R}^+$ with unit that has unique factorization into irreducible elements and the Delone property.

For any set $\mathcal{N}$ of Beurling generalized integers we define the *g-prime counting function*

$$\pi_{\mathcal{N}}(x) := \#\{i : g_i \leq x\} \tag{1.4}$$

and the *g-integer counting function*

$$n_{\mathcal{N}}(x) := \#\{i : n_i \leq x\} . \tag{1.5}$$

The *zeta function of $\mathcal{N}$* is

$$\zeta_{\mathcal{N}}(s) := \sum_{i=0}^{\infty} n_i^{-s} ,$$

and it clearly has the Euler product

$$\zeta_{\mathcal{N}}(s) = \prod_{i=1}^{\infty} (1 - g_i^{-s})^{-1} .$$

Beurling [2] studied conditions on a set of generalized integers $\mathcal{N}$ which imply that an analogue of the prime number theorem holds for $\mathcal{N}$. He showed that if

$$n_{\mathcal{N}}(x) = Ax + O\left(\frac{x}{(\log x)^{\gamma}}\right) \tag{1.6}$$

for some $\gamma > 3/2$, then the "prime number theorem"

$$\pi_{\mathcal{N}}(x) = \frac{x}{\log x} + o\left(\frac{x}{\log x}\right) , \tag{1.7}$$

is valid, and indicated that (1.7) should not follow for $\gamma \leq \frac{3}{2}$. Diamond [5] gave an explicit example satisfying (1.6) with $\gamma = 3/2$ where (1.7) does not hold. Later Diamond [6] also showed that if (1.6) holds for some γ with $1 < \gamma \leq \frac{3}{2}$, one can still conclude that a Chebyshev-type estimate

$$c_1 \frac{x}{\log x} < \pi_{\mathcal{N}}(x) < c_2 \frac{x}{\log x} \tag{1.8}$$

holds for positive constants c_1 and c_2 depending on $\mathcal{N}$. This set of results was completed by R. Hall [10], who gave examples of $\mathcal{N}$ where (1.6) holds with $0 < \gamma < 1$ but the Chebyshev-type bound (1.8) does not hold. Revesz [16] recently gave "almost periodic" asymptotics for $\pi_{\mathcal{N}}(x)$ assuming certain "almost periodic" asymptotics for $n_{\mathcal{N}}(x)$.

At one time it was hoped that the study of Beurling generalized integers might shed light on the Riemann hypothesis. Suppose that $\zeta_{\mathcal{N}}(s)$ analytically continues to the half-plane $Re(s) > \frac{1}{2}$, except for a simple pole at $s = 1$. This occurs, for example, whenever

$$n_{\mathcal{N}}(x) = Ax + O(x^{1/2}) \ . \tag{1.9}$$

The analogue of the Riemann hypothesis for such $\mathcal{N}$ is that $\zeta_{\mathcal{N}}(s)$ has no zeros in $Re(s) > \frac{1}{2}$, or, equivalently, that

$$\pi_{\mathcal{N}}(x) = \int_2^x \frac{dt}{\log t} + O(x^{1/2+\epsilon}) \ , \quad \text{any} \ \ \epsilon > 0 \ .$$

In 1961, however, Malliavin [13, Section 6] produced for each $\delta > 0$ a set of g-integers $\mathcal{N}$ such that $\zeta_{\mathcal{N}}(s)$ analytically continues to $Re(s) > 0$ and has a simple pole at $s = 1$, and also has a real zero β with $1 - \delta < \beta < 1$. Thus the analogue of the Riemann hypothesis fails for these $\mathcal{N}$. Furthermore Malliavin asserted that one can find such sets $\mathcal{N}$ contained in the positive integers $\mathbb{Z}^+$. His results actually show that the constraint on $\mathcal{N}$ imposed by the requirement that $\mathcal{N}$ be an arithmetical semigroup on $\mathbb{R}^+$ that satisfies

$$n_{\mathcal{N}}(x) = Ax + O(x^{\epsilon}) \ , \quad \text{any} \ \ \epsilon > 0 \ , \tag{1.10}$$

is not sufficient to imply the Riemann hypothesis for such $\mathcal{N}$, even if we assume that $\mathcal{N} \subseteq \mathbb{Z}^+$.

In order to obtain sets of Beurling generalized integers $\mathcal{N}$ that might satisfy a Riemann hypothesis, additional conditions of a non-multiplicative nature appear to be needed, cf. [1, p. 197]. This paper proposes the Delone property as a possible such side condition. For a set of Beurling generalized integers $\mathcal{N}$ the Delone property consists of a constraint of multiplicative type (unique factorization property) with one of additive type (gaps bounded above and below). It implies a bound

$$c_1 x < n_{\mathcal{N}}(x) < c_2 x \tag{1.11}$$

for some positive constants c_1 and c_2. The condition (1.11) is weaker than the sort of asymptotic condition (1.6) on $n_{\mathcal{N}}(x)$ that was imposed by Beurling. In particular, it does not a priori guarantee any analytic continuation of the zeta function $\zeta_{\mathcal{N}}(s)$ beyond the half-plane $Re(s) > 1$, let alone the truth of a Riemann hypothesis.

This paper characterizes arithmetical Delone semigroups that are contained in the positive integers $\mathbb{Z}^+$. The simplest example of such a semigroup is $\mathbb{Z}^+$ itself, whose generating set is the set $\mathcal{P}$ of all primes. If we take

$$\mathcal{G} = \mathcal{P} \backslash \mathcal{F} ,$$

where $\mathcal{F}$ is a finite set of primes, then we obtain an arithmetical Delone semigroup whose members fill out all arithmetic progressions $a \pmod{M}$ with $(a, M) = 1$, with $M = \prod_{p \in \mathcal{F}} p$.

Our main result is the following "rigidity" result for arithmetical Delone semigroups in $\mathbb{Z}^+$.

Theorem 1.1. *If $\mathcal{S}$ is an arithmetical Delone semigroup contained in $\mathbb{Z}^+$, then its set of generators $\mathcal{G}$ contains all but finitely many primes. The set of generators has the form*

$$\mathcal{G} = (\mathcal{P} \backslash \mathcal{E}) \cup \mathcal{C} , \tag{1.12}$$

where $\mathcal{P}$ is the set of all primes, $\mathcal{E}$ is a finite set of primes, and $\mathcal{C}$ is a finite set of composite numbers.

This result implies that for each arithmetical Delone semigroup in $\mathbb{Z}^+$ there is a squarefree modulus M with the property that $\mathcal{S}$ contains all arithmetic progressions $a \pmod{M}$ with $(a, M) = 1$.

We easily obtain from Theorem 1.1 a complete characterization of arithmetical Delone semigroups $\mathcal{S}$ in $\mathbb{Z}^+$. To state it, let $e_p(n)$ denote the largest power of p that divides n.

Theorem 1.2. *Let $\mathcal{S}$ be a semigroup with unit in $\mathbb{Z}^+$ whose set of generators $\mathcal{G}$ has the form*

$$\mathcal{G} = (\mathcal{P} \backslash \mathcal{E}) \cup \mathcal{C} ,$$

where $\mathcal{P}$ is the set of all primes, $\mathcal{E}$ is a finite set of primes, and $\mathcal{C}$ is a finite set of composite numbers.Then $\mathcal{S}$ has the Delone property if and only if it has unique factorization property, and this property holds if and only if the $|\mathcal{E}| \times |\mathcal{C}|$ matrix $M = [M_{p,c}]$ with

$$M_{p,c} = e_p(c) , \quad \textit{for} \ \ p \in \mathcal{E} , \quad c \in \mathcal{C} ,$$

has full column rank $|\mathcal{C}|$ over $\mathbb{Q}$.

It follows from Theorem 1.2 that the zeta function $\zeta_{\mathcal{S}}(s)$ of an arithmetical Delone semigroup contained in $\mathbb{Z}^+$ differs from the Riemann zeta function by a finite Euler product, so that

$$n_{\mathcal{S}}(x) = Ax + O(1) , \quad \text{as} \ \ x \to \infty , \tag{1.13}$$

for some positive constant A. Thus the zeta function $\zeta_{\mathcal{S}}(s)$ meromorphically continues to the entire complex plane $\mathbb{C}$, and the Riemann hypothesis holds for all such $\mathcal{S}$ if and only if it holds for the Riemann zeta function.

The interest of Theorem 1.1 lies in its showing that the "approximate rigidity" of the Delone condition in $\mathbb{Z}^+$ forces the absolute rigidity of the sets $\mathcal{S}$ that can satisfy it. It is slightly surprising that the additive and multiplicative properties of $\mathbb{Z}$ can be related sufficiently to obtain the result.

To understand the scope of Theorem 1.1 one would like to characterize all arithmetical Delone semigroups in $\mathbb{R}^+$. The only such semigroups I know of are contained in $\mathbb{Z}^+$. Are there any others?

An outline of the proof of Theorem 1.1 is as follows. In §2 we show that the unique factorization property implies $\pi_{\mathcal{N}}(x) \le \pi(x)$ for all $x \ge 1$, where $\pi(x) = \pi_{\mathbb{Z}^+}(x)$ is the usual prime-counting function. We then show that the bound $n_{\mathcal{N}}(x) > c_1 x$ implies that the "exceptional set" $\mathcal{E}$ of primes not in $\mathcal{G}$ satisfies

$$\sum_{p \in \mathcal{E}} \frac{1}{p} < \infty . \tag{1.14}$$

To prove (1.14) we use Philip Hall's theorem on systems of distinct representatives. In §3 we show that if $\mathcal{E}$ is infinite and satisfies the bound (1.14), then $\mathcal{N}$ cannot be relatively dense. Since $\mathcal{E}$ is infinite the Chinese remainder theorem can be used to produce arbitrarily long sequences of consecutive integers each of which is divisible by some prime $p \in \mathcal{E}$. However even though any such $p \notin \mathcal{N}$, various multiples of such p can be in $\mathcal{N}$. The crux of the proof is a combinatorial sieve to avoid all such multiples, and a proof that among all sequences of consecutive integers of a fixed length a positive proportion remain unsieved. We sieve over certain sets of shifted residue classes (mod p) for p in an infinite set, and since in general there exist choices of shifted residue classes (mod p) for which the sieved set is empty, we must show that the residue classes sieved out satisfy extra side conditions which rule out this possibility. We conclude that if $\mathcal{N}$ has the Delone property, then the "exceptional set" $\mathcal{E}$ is finite, hence $\mathcal{G}$ contains all but finitely many primes. In §4 we complete the proofs of Theorems 1.1 and 1.2.

The Delone property was originally formulated as a concept in geometric crystallography which models the "solid state," see Engel [7], [8] and Senechal [17]. A set X in $\mathbb{R}^n$ is a *Delone* *set* or (r, R)*-set* if it is uniformly discrete and relatively dense. A set is *uniformly discrete* if there is a positive r such that each ball of radius r contains at most one point of X, and is *relatively dense* if each ball of radius R contains at least one point of X. This concept was originally proposed by the Russian crystallographer and number theorist B. N. Delone in 1937 under the name (r, R)-set, according to [3]. This paper carries this property over to subsets of the positive real line $\mathbb{R}^+$. This was motivated by the question whether the crystal-like nature of $\mathbb{Z}^+$ is relevant to the (presumed) truth of the Riemann hypothesis.

2. Unique Factorization Property

Let $\mathcal{S}$ be a multiplicative semigroup with unit that is contained in the positive integers $\mathbb{Z}^+$. Let $\mathcal{G} = \{g_i : i \geq 1\}$ be the set of irreducible elements of $\mathcal{S}$, which we call *generators* of $\mathcal{S}$. Throughout this section we assume that $\mathcal{S}$ has the unique factorization property.

We study such semigroups by using the prime factorization in $\mathbb{Z}^+$ of elements of $\mathcal{G}$. For any $n \in \mathbb{Z}^+$, write its prime factorization as

$$n = \prod_{p \in \mathcal{P}} p^{e_p(n)} . \tag{2.1}$$

We begin by establishing the following property of semigroups $\mathcal{S}$ contained in $\mathbb{Z}^+$ that have the unique factorization property.

Lemma 2.1. *Let $\mathcal{S}$ be a multiplicative semigroup contained in $\mathbb{Z}^+$ which has the unique factorization property, and let $\mathcal{G}$ be its set of generators. Then there exists a one-to-one map $f_{\mathcal{G}} : \mathcal{G} \to \mathcal{P}$ such that*

$$f_{\mathcal{G}}(g) \mid g \quad \textit{for all} \quad g \in \mathcal{G} . \tag{2.2}$$

Remark. We call the map $f_{\mathcal{G}}$ a *prime transversal function* for $\mathcal{G}$. It is generally not unique. The existence of a prime transversal function is a necessary but not sufficient condition for $\mathcal{S}$ to have the unique factorization property.

Proof. Given any finite set of indices $G \subseteq \mathcal{G}$, we set

$$P(G) := \{p \in \mathcal{P} : p|g \quad \text{for some } g \in G\} .$$

We claim that

$$|P(G)| \geq |G| , \quad \text{for all} \;\; \text{finite sets } G \subseteq \mathcal{G} . \tag{2.3}$$

To prove the claim, write $P(G) = \{p_1, \ldots, p_m\}$ and consider the prime factorizations

$$g = \prod_{p \in P(G)} p^{e_p(g)} \ , \quad \text{for} \ \ g \in G \ , \tag{2.4}$$

Each generator g_i has a distinct exponent vector

$$\mathbf{v}(g) := (e_{p_1}(g), \ldots, e_{p_m}(g)) \in \mathbb{Z}^m \ , \quad \text{for} \ \ g \in G \ .$$

We now argue by contradiction. If $m = |P(G)| < |G|$, then these vectors must be linearly dependent in the vector space $\mathbb{Z}^m$, and, by clearing denominators, we obtain a nontrivial $\mathbb{Z}$-linear relation

$$\sum_{i \in I} e(g)\mathbf{v}(g) = \mathbf{0} \ . \tag{2.5}$$

This yields two distinct factorizations of an element of $\mathcal{S}$, namely

$$n = \prod_{\substack{g \in G \\ e(g) > 0}} g^{e(g)} = \prod_{\substack{g \in G \\ e(g) < 0}} g^{-e(g)} \ . \tag{2.6}$$

This contradicts the unique factorization property, hence (2.3) holds.

Next, associate to each $g \in \mathcal{G}$ the finite set

$$P(g) := \{p \in \mathcal{P} : p | g\} \subseteq \mathcal{P} \ .$$

The condition (2.3) is exactly the hypothesis needed to apply Philip Hall's theorem [9] on the existence of a system of distinct representatives ("transversal") for this set system, i.e. the existence of a one-to-one map $f_{\mathcal{G}} : \mathcal{G} \to \mathcal{P}$ such that $f_{\mathcal{G}}(g) \in P(g)$. Hall's theorem was originally proved for set systems in which $\mathcal{G}$ and $\mathcal{P}$ are finite sets, but it also holds for countably infinite sets $\mathcal{G}$ and $\mathcal{P}$, provided that each set $P(g)$ is finite, see Mirsky [14, Theorem 4.2.1] and Appendix A. Thus a map $f_{\mathcal{G}}$ exists. □

Lemma 2.2. *If a semigroup $\mathcal{S} \subseteq \mathbb{Z}^+$ has the unique factorization property, then*

$$\pi_{\mathcal{S}}(x) \le \pi(x) \ , \quad \textit{all} \ x \ge 1 \ ; \tag{2.7}$$

where $\pi(x)$ counts the number of primes less than x.

Proof. By the unique factorization property we may write $\mathcal{G}$ as

$$1 < g_1 < g_2 < g_3 < \ldots \ .$$

Number the primes $p_1 = 2,\ p_2 = 3, \ldots$ in increasing order. If $G = \{p_1, p_2, \ldots, p_k\}$ then (2.3) gives

$$|P(G)| \geq |G| = k \ .$$

It follows that $P(G)$ contains some prime $p \geq p_k$, and this prime divides g_i for some $i \in \{1, 2, \ldots, k\}$. Thus

$$g_k \geq g_i \geq p \geq p_k \ ,$$

and (2.7) follows. $\square$

Lemma 2.3. *Suppose that the multiplicative semigroup $\mathcal{S} \subseteq \mathbb{Z}^+$ has the unique factorization property, and that there is a positive constant c_1 such that*

$$n_{\mathcal{S}}(x) > c_1 x \quad \textit{for all} \quad x \geq x_0 \ . \tag{2.8}$$

Then the set of "exceptional primes" $\mathcal{E} := \{p : p \textit{ prime and } p \notin \mathcal{S}\}$ has

$$\sum_{p \in \mathcal{E}} \frac{1}{p} < \infty \ . \tag{2.9}$$

Remark. The converse also holds. For any multiplicative semigroup $\mathcal{S}$ in $\mathbb{Z}^+$ with the unique factorization property and with $\sum_{p \in \mathcal{E}} \frac{1}{p} < \infty$ there is some $c > 0$ such that $n_{\mathcal{S}}(x) > cx$ for all sufficiently large x.

Proof. The *zeta function* of a discrete semigroup $\mathcal{S}$ in $\mathbb{R}^+$ is

$$\zeta_{\mathcal{S}}(s) = \sum_{n \in \mathcal{S}} n^{-s} \quad \text{(integers counted without multiplicity)} \ .$$

Since $\mathcal{S}$ has unique factorization, $\zeta_{\mathcal{S}}(s)$ has an Euler product

$$\zeta_{\mathcal{S}}(s) = \prod_{i=1}^{\infty} (1 - g_i^{-s})^{-1} \ .$$

This Euler product converges absolutely in the half-plane $Re(s) > 1$, because $g_k \geq p_k$ for all $k \geq 1$ by Lemma 2.2. Thus

$$\log \zeta_{\mathcal{S}}(s) = -\sum_{i=1}^{\infty} \log(1 - g_i^{-s}) \ , \tag{2.10}$$

and the right side converges absolutely for $Re(s) > 1$. For real $\sigma > 1$ we have

$$\log \zeta_{\mathcal{S}}(\sigma) \geq \sum_{i=1}^{\infty} g_i^{-\sigma} \ . \tag{2.11}$$

The lower bound for $n_{\mathcal{S}}(x)$ in (2.8) implies that there is a positive constant c_2 such that for all real σ with $1 \le \sigma \le 2$,

$$\begin{aligned} \zeta_{\mathcal{S}}(\sigma) &\ge \sum_{m=\lceil x_0 \rceil}^{\infty} (\frac{m}{c_1})^{-\sigma} \\ &\ge \frac{c_1}{\sigma - 1} - c_2 \ . \end{aligned} \tag{2.12}$$

It follows that there exists a finite positive constant c_3 such that

$$\log \zeta_{\mathcal{S}}(\sigma) \ge -\log(\sigma - 1) - c_3 \ , \quad \text{for} \ \ 1 \le \sigma \le 2 \ . \tag{2.13}$$

Now (2.10) gives for $\sigma > 1$, the upper bound

$$\log \zeta_{\mathcal{S}}(\sigma) \le \sum_{i=1}^{\infty} g_i^{-\sigma} + c_4 \ , \tag{2.14}$$

where we have

$$c_4 := \sum_{i=1}^{\infty} \sum_{n=2}^{\infty} \frac{1}{n} g_i^{-n} \le \sum_{i=1}^{\infty} \frac{g_i^{-2}}{1 - g_i^{-2}} \le \frac{4}{3} \cdot \frac{\pi^2}{6} \ .$$

By Lemma 2.1 there is a one-to-one map $f_{\mathcal{G}} : \mathcal{G} \to \mathcal{P}$ such that the prime $f_{\mathcal{G}}(g)$ divides g for all $g \in \mathcal{G}$. Thus if $g \in \mathcal{G}$ is not prime then $g \ge 2 f_{\mathcal{G}}(g)$ hence, for $\sigma > 1$,

$$g^{-\sigma} - f_{\mathcal{G}}(g)^{-\sigma} \le (2 f_{\mathcal{G}}(g))^{-\sigma} - (f_{\mathcal{G}}(g))^{-\sigma} \le -(2 f_{\mathcal{G}}(g))^{-\sigma} \ .$$

Let $\mathcal{E} = \mathcal{E}_1 \cup \mathcal{E}_2$ with

$$\mathcal{E}_1 := \{p : p = f_{\mathcal{G}}(g) \quad \text{for some} \quad g \ne p\}$$

and with $\mathcal{E}_2 := \mathcal{E} \backslash \mathcal{E}_1$. The inequality above gives, for $\sigma > 1$,

$$\begin{aligned} \sum_{i=1}^{\infty} g_i^{-\sigma} &\le \sum_{i=1}^{\infty} (f_{\mathcal{G}}(g_i))^{-\sigma} - \sum_{p \in \mathcal{E}} (2p)^{-\sigma} \\ &\le \sum_{p \in \mathcal{P}} p^{-\sigma} - \sum_{p \in \mathcal{E}_2} p^{-\sigma} - \sum_{p \in \mathcal{E}_1} (2p)^{-\sigma} \\ &\le \sum_{p \in \mathcal{P}} p^{-\sigma} - \sum_{p \in \mathcal{E}} (2p)^{-\sigma} \ . \end{aligned} \tag{2.15}$$

Applying (2.11) with $\mathcal{S} = \mathbb{Z}^+$ gives, for $\sigma > 1$,

$$\begin{aligned} \sum_{p \in \mathcal{P}} p^{-\sigma} &\le \log \zeta(\sigma) \\ &\le -\log(\sigma - 1) + c_5 \ , \end{aligned} \tag{2.16}$$

in which the last inequality is based on the observation that the Riemann zeta function $\zeta(s)$ has a simple pole at $s=1$ with residue 1 and $\zeta(\sigma)$ is bounded as $\sigma \to \infty$. Combining (2.14)–(2.16) yields, for $1 < \sigma < 2$, that

$$\log \zeta_{\mathcal{S}}(\sigma) \le -\log(\sigma - 1) + (c_4 + c_5) - \frac{1}{4}\sum_{p \in \mathcal{E}} p^{-\sigma} \ . \tag{2.17}$$

If $\sum_{p\in\mathcal{E}} \frac{1}{p}$ diverges, then the upper bound (2.17) eventually contradicts the lower bound (2.13) as $\sigma \to 1^+$, which completes the proof. $\square$

3. Combinatorial Sieve Argument

The main step in the proof of Theorem 1.1 is a sieve argument contained in the proof of the following theorem. Recall that the *lower asymptotic density* $\underline{d}(\mathcal{M})$ of a set $\mathcal{M} \subseteq \mathbb{Z}^+$ is

$$\underline{d}(\mathcal{M}) := \liminf_{x\to\infty} \ \frac{1}{x} \ \#\{m : m \le x \ \text{ and } \ m \in \mathcal{M}\} \ .$$

We prove:

Theorem 3.1. *Suppose that $\mathcal{S}$ is a multiplicative semigroup contained in $\mathbb{Z}^+$ with the unique factorization property, such that the set $\mathcal{E} = \{p : p \in \mathcal{P}$ and $p \notin \mathcal{S}\}$ of "exceptional primes" is infinite and satisfies*

$$\sum_{p\in\mathcal{E}} \frac{1}{p} < \infty \ .$$

Then, for each fixed positive integer r, the set

$$\mathcal{M}_r := \{m \in \mathbb{Z}^+ : m + j \notin \mathcal{S} \ \ for \ \ 1 \le j \le r\} \tag{3.1}$$

has positive lower asymptotic density.

Proof. Choose a fixed prime transversal function $f_{\mathcal{G}} : \mathcal{G} \to \mathcal{P}$, using Lemma 2.1. For all nonexceptional primes p, we must have

$$f_{\mathcal{G}}(p) = p \ , \quad p \in \mathcal{P}\backslash\mathcal{E} \ . \tag{3.2}$$

because $p \in \mathcal{G}$. The one-to-one property of $f_{\mathcal{G}}$ implies that for all composite $g \in \mathcal{G}$ we have $f_{\mathcal{G}}(g) \in \mathcal{E}$.

By hypothesis $\mathcal{E}$ is an infinite set. To prove that $\mathcal{M}_r$ has positive density we will choose r exceptional primes $p_1, p_2, \ldots, p_r$ and will study a fixed arithmetic progression (mod $p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$)

of elements m such that

$$m + j \equiv 0 \pmod{p_j^{k_j}} \quad 1 \le j \le r \ . \tag{3.3}$$

The particular exponents $k_1, \ldots, k_r \ge 1$ will be specified later in the proof. By the Chinese remainder theorem the set of m that satisfy (3.3) forms the arithmetic progression

$$m(\ell) = m_0 + \ell p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r} \ , \tag{3.4}$$

in which $0 < m_0 \le p_1^{k_1} \ldots p_r^{k_r}$ and ℓ varies over the nonnegative integers.

We will sieve out from the arithmetic progression (3.4) all elements $m(\ell)$ such that

$$m(\ell) + j \in \mathcal{S} \ \text{ for some } j \ , \quad 1 \le j \le r \ , \tag{3.5}$$

plus possibly some other elements, and show that a positive density of ℓ remain unsieved. To describe it, note that even if a prime $p \notin \mathcal{S}$, various multiples of p may be in $\mathcal{S}$. Associate to each $p \in \mathcal{P}$ the set

$$\mathcal{G}[p] := \{g \in \mathcal{G} : p | g\} \ .$$

We then have

$$p \notin \mathcal{G}[p] \Leftrightarrow p \in \mathcal{E} \ .$$

If $m \notin \mathcal{S}$ then certainly $p|m$ for some $p \in \mathcal{E}$.

The following criterion gives a sieve-type sufficient condition for $m \notin \mathcal{S}$.

Nonmembership Criterion. *Let $m \in \mathbb{Z}^+$ and suppose that $p|m$ and $p \in \mathcal{E}$. Then $m \notin \mathcal{S}$ if the following conditions all hold.*

(i). *If $q = f_{\mathcal{G}}(g)$ for $g \in \mathcal{G}[p]$, and $q \ne p$, then $q \nmid m$.*

(ii). *If $p = f_{\mathcal{G}}(g_0)$ for $g_0 \in \mathcal{G}[p]$, and $p^2 | g_0$, then $p^2 \nmid m$.*

(iii). *If $p = f_{\mathcal{G}}(g_0)$ for $g_0 \in \mathcal{G}[p]$, and $p || g_0$, set $g_0 = a_0 p$, then for some $k \ge 1$, $p^k | m$ and $a_0^k \nmid m$.*

We prove the nonmembership criterion by contradiction. If $m \in \mathcal{S}$ then m uniquely factors as

$$m = \prod_{g \in \mathcal{G}} g^{a_g(m)} \tag{3.6}$$

where the exponents $a_g(m) \geq 0$ and all but finitely many $a_g(m) = 0$. Since $p|m$, some $g \in \mathcal{G}[p]$ has $a_g(m) \geq 1$. Consider the prime $q = f_{\mathcal{G}}(g)$. It divides g, hence it divides m. Now condition (i) rules out $q \neq p$. If $q = p$, then $g = g_0$, and if $p^2|g_0$, then $p^2|m$, but condition (ii) rules this out. Finally, if $q = p$, and $p||g_0$ with $g_0 = a_0 p$, and if $p^k|m$, then necessarily $(g_0)^k|m$, because the only factors contributing powers of p to the right side of (3.6) can be g_0 and $p||g_0$. Since $a_0^k|(g_0)^k$ we have $a_0^k|m$, and condition (iii) rules this out. This covers all cases, so the nonmembership criterion follows.

We sieve the arithmetic progression (3.4) to remove all $m(\ell)$ not satisfying the nonmembership criterion. We first choose the primes $p_1, \ldots, p_r \in \mathcal{E}$ to satisfy the following two conditions.

(C1). Each $p_j > r$.

(C2). If $g \in \mathcal{G}[p_j]$ then $f_{\mathcal{G}}(g) > r$.

This can be done since $\mathcal{E}$ is infinite, and these two conditions only exclude finitely many primes, the second because there are at most $\pi(r)$ values $g \in \mathcal{G}$ with $f_{\mathcal{G}}(g) < r$, and it suffices to avoid all primes p which divide any of these g. We next choose the exponents k_j, for $1 \leq j \leq r$, as follows:

(K1). If $f_{\mathcal{G}}(g) \neq p_j$ for all $g \in \mathcal{G}[p_j]$, set $k_j = 1$.

(K2). If $f_{\mathcal{G}}(g) = p_j$ and $p_j^2|g$, set $k_j = 1$.

(K3). If $f_{\mathcal{G}}(g) = p_j$ and $g = a_j p_j$ with $p_j \nmid a_j$, let p_j^* be the largest prime factor of a_j and pick $k_j \geq 1$ to be the smallest positive integer k such that $(p_j^*)^k > r$.

We define $p_j^* = 1$ if it is not already defined by (K3).

We sieve the arithmetic progression (3.4) in two stages. In the first stage we sieve out various residue classes of certain prime-power moduli q below a sufficiently large cutoff value T, which satisfies

$$T > \max[r, (p_j)^{k_j+1} \text{ and } (p_j^*)^{k_j} \text{ for } 1 \leq j \leq r] , \tag{3.7}$$

and which will be further specified later. The sieve moduli used in the first stage are:

(M1). $q \in \mathcal{E}$ with $r < q < T$ and $q \neq p_1, p_2, \ldots, p_r$.

(M2). $q = p_j^{k_j+1}$ for $1 \leq j \leq r$, (M3). $q = (p_j^*)^{k_j}$ for $1 \le j \le r$, if $p_j^* \neq 1$, $p_j^* \neq p_i$ for $1 \le i \le r$, and either

$p_j^* \le r$ or $p_j^* \notin \mathcal{E}$.

At the second stage we will sieve out various residue classes of the remaining moduli

(M4). $q \in \mathcal{E}$ and $q \ge T$.

In the first stage sieving, for moduli $q \in \mathcal{E}$ with $r < q < T$ we sieve out all $m(\ell)$ with

$$m(\ell) + j \equiv 0 \ (\text{mod } q) \ , \quad 1 \le j \le r \ . \tag{3.8}$$

By hypothesis q is prime to $p_1 \dots p_r$, hence (3.9) sieves out r residue classes (mod q) of the arithmetic progression parameter ℓ.

For moduli $q = p_j^{k_j+1}$ we sieve out all $m(\ell)$ with

$$m(\ell) + j \equiv 0 \pmod{p_j^{k_j+1}} \ . \tag{3.9}$$

This is equivalent to a congruence (mod p_j) on the parameter ℓ. Note that the arithmetic progression (3.4) has

$$m(\ell) + j \equiv 0 \pmod{p_j^{k_j}} \ , \tag{3.10}$$

so it follows that

$$m(\ell) + i \neq 0 \ (\text{mod } p_j) \ , \quad 1 \le i \le r \text{ with } i \neq j \ , \tag{3.11}$$

because condition (C1) requires that all $p_j > r$.

Finally for moduli $q = (p_j^*)^{k_j}$ for which p_j^* is defined, and $p_j^* \neq p_1, \dots p_r$ we exclude the r residue classes

$$m(\ell) + j \equiv 0 \ (\text{mod } (p_j^*)^{k_j}) \ , \quad 1 \le i \le r \ . \tag{3.12}$$

This excludes r residue classes (mod $(p_j^*)^{k_j}$) of ℓ. By construction $(p_j^*)^{k_j} > r$ so not all classes (mod $(p_j^*)^{k_j}$) are sieved out. The condition (3.12) is a linear congruence (mod $(p_j^*)^{k_j}$) on the parameter ℓ, because p_j^* does not equal any of the p_i for $i \neq j$. Note that $p_j^* < T$, so if $p_j^* \in \mathcal{E}$ and $p_j > r$ then the exclusion of residue classes (3.12) was already achieved by (3.9) for p_j^* in (M1). We therefore omitted these cases from the condition (M3). Also note that if some $p_j^* = p_i$ with $i \neq j$, then the condition

$$m(\ell) + j \not\equiv 0 \ (\text{mod } (p_j^*)^{k_j}) \tag{3.13}$$

automatically holds for all $m(\ell)$ in the arithmetic progression (3.4), because

$$m(\ell) + j \not\equiv 0 \pmod{p_i} ,$$

by (3.11).

Now let

$$\mathcal{L}_T := \{\ell : m(\ell) \text{ unsieved up to cutoff } T\} .$$

The congruence conditions in (M1)–(M3) consist of distinct prime-power moduli, hence the Chinese remainder theorem applied to the arithmetic parameter ℓ, shows that the elements of $\mathcal{L}_T$ consist of a collection of arithmetic progressions to the modulus

$$R_T := \prod_{j=1}^{r} p_j (p_j^*)^{k_j} \prod_{\substack{q \in \mathcal{E} \\ r < q \le T}} q .$$

Thus $\mathcal{L}_T$ has an asymptotic density $d(\mathcal{L})$, which satisfies

$$d(\mathcal{L}) \ge c_T := \prod_{j=1}^{r} \frac{1}{p_j (p_j^*)^{k_j}} \prod_{\substack{q \in \mathcal{E} \\ r < q < T}} \left(1 - \frac{r}{q}\right) , \tag{3.14}$$

and clearly $c_T > 0$. In fact, we have

$$\#\{\ell \le x : \ell \in \mathcal{L}_T\} \ge \frac{1}{2} c_T x \quad \text{for } x \ge R_T . \tag{3.15}$$

The constant c_T is a non-increasing function of T, hence the limit

$$c_\infty := \lim_{T \to \infty} c_T$$

exists, and we have

$$c_\infty \ge c_\infty^* = \prod_{j=1}^{r} \frac{1}{p_j (p_j^*)^{k_j}} \prod_{\substack{p \in \mathcal{E} \\ p > r}} \left(1 - \frac{r}{p}\right) .$$

By hypothesis $\sum_{p \in \mathcal{E}} \frac{1}{p} < \infty$, which implies that $c_\infty^* > 0$.

In the second stage sieveing, for each $q \in \mathcal{E}$ with $q > T$, we sieve out the r residue classes

$$m(\ell) + j \equiv 0 \pmod{q} , \quad 1 \le j \le r . \tag{3.16}$$

Each condition (3.16) asserts that

$$m_0 + \ell p_1^{k_1} \dots p_r^{k_r} + j = k^* q \tag{3.17}$$

for some integer k^*. The left side of (3.17) is positive, hence $k^* \geq 1$. This bounds the smallest solution ℓ to (3.17) by

$$\ell \geq \frac{q-(m_0+j)}{p_1^{k_1}\dots p_r^{k_r}} \geq \frac{q}{2p_1^{k_1}\dots p_r^{k_r}} \ , \tag{3.18}$$

whenever $q \geq 2(m_0+r)$, and this certainly holds if

$$T \geq 2(q_1^{k_1}\dots q_r^{k_r}+r) \geq 2(m_0+r) \ . \tag{3.19}$$

Now (3.18) implies that

$$\#\{\ell \leq x : m(\ell)+j \equiv 0 \pmod{q}\} \leq \left(\frac{2p_1^{k_1}\dots p_r^{k_r}}{q}\right) x \tag{3.20}$$

is valid for all $x \geq 1$. Thus an upper bound on the number of elements ℓ up to x that are sieved out in the second stage, provided that (3.19) holds, is

$$S_T(x) := 2rp_1^{k_1}\dots p_r^{k_r}\left(\sum_{\substack{q\in\mathcal{E}\\ q>T}}\frac{1}{q}\right) x \ , \tag{3.21}$$

and we emphasize that this is valid *for all* $x \geq 1$.

We now choose T, and take it large enough so that (3.7) and (3.19) hold, and also so that

$$\sum_{\substack{q\in\mathcal{E}\\ q>T}}\frac{1}{q} < \frac{1}{8}\frac{c_\infty^*}{rp_1^{k_1}\dots p_r^{k_r}} \ . \tag{3.22}$$

Let $\mathcal{L}_\infty$ denote the unsieved values of ℓ that remain after the second stage sieveing. Combining (3.15) and (3.20)–(3.22) yields

$$\begin{aligned}
\#\{\ell \leq x : \ell \in \mathcal{L}_\infty\} \ &\geq \ \frac{1}{x}\{\ell \leq x : \ell \in \mathcal{L}_T\} - S_T(x) \\
&\geq \ \frac{1}{2}c_T x - \frac{1}{4}c_\infty^* x \quad \text{for all} \quad x \geq R_T \ , \\
&\geq \ \frac{1}{4}c_T x \quad \text{for all } x \geq R_T \ .
\end{aligned}$$

Thus the set of unsieved elements $\mathcal{L}_\infty$ in the arithmetic progression (3.4) has a positive lower asymptotic density $\underline{d}(\mathcal{L}_\infty) \geq \frac{1}{4}c_T$.

It remains to verify that all unsieved elements $m(\ell)+j \notin \mathcal{S}$ for $1 \leq j \leq r$, by verifying that the nonmembership criterion holds. Consider a fixed j, and by construction

$$p_j^{k_j} | m(\ell) + j \ .$$

The sieveing process guarantees that

$$q \nmid m(\ell) + j \ ,$$

for all $q \in \mathcal{E}$ with $q > r$, and Condition (C2) on p_j ensures that all $q = f_{\mathcal{G}}(g)$ with $g \in \mathcal{G}[p_j]$ satisfy this. Thus condition (i) of the nonmembership criterion holds. Condition (ii) of the criterion is verified by the sieveing on (M2), since we choose $k_j = 1$ according to (K2). Finally, condition (iii) of the criterion is verified by the sieveing on (M3), where we used (K3) to choose k_j so that $(p_j^*)^{k_j} > r$, and $(p_j^*)^{k_j} \nmid m(\ell)$ implies that $(a_j)^{k_j} \nmid m(\ell)$, which is (iii). Thus the nonmembership criterion applies to give $m(\ell) + j \notin \mathcal{S}$, and this holds for $1 \leq j \leq r$. $\square$

Remark. The proof of Theorem 3.1 sifts out by (several) nonzero residue classes $(\bmod\ q)$ over a possibly infinite sequence of primes q. Given any infinite sequence of primes $\{q_j : j \geq 1\}$, however sparse, it is possible to sieve out exactly one residue class (mod q_j) for each $j \geq 1$ in such a way as to sieve out *every* integer; at stage j choose that residue class (mod q_j) which sieves out the least integer currently unsieved. The proof of Theorem 3.1 rules out this pathology via the inequality (3.18).

4. Main Results

We complete the proofs of Theorems 1.1 and 1.2.

Proof of Theorem 1.1. Lemma 2.3 applies to show that the set of "exceptional primes" $\mathcal{E} = \{p \in \mathcal{P} : p \notin \mathcal{G}\}$ has $\sum_{p \in \mathcal{E}} \frac{1}{p} < \infty$. If $\mathcal{E}$ were infinite, Theorem 3.1 shows that $\mathcal{S}$ omits arbitrarily long intervals $(m+1, \ldots, m+r)$, hence $\mathcal{S}$ is not relatively dense. This contradicts $\mathcal{S}$ having the Delone property, hence $\mathcal{E}$ is finite. It remains to show that the set $\mathcal{C}$ of composite numbers in $\mathcal{G}$ is finite. In fact it contains at most $|\mathcal{E}|$ elements, for if it contained at least $|\mathcal{E}|+1$ elements, then unique factorization of $\mathcal{S}$ would fail to hold. To see this, set $e = |\mathcal{E}|$ and choose $\mathcal{C}^* = \{c_i : 1 \leq i \leq e+1\} \subseteq \mathcal{C}$, and define the finite set

$$\mathcal{F} := \{p \in \mathcal{P} \backslash \mathcal{E} : p | c_i \text{ for some } i\} \ .$$

Now $\mathcal{C}^* \cup \mathcal{F} \subseteq \mathcal{G}$. Recall that $P(G) = \{p : p|g \text{ for some } g \in \mathcal{G}\}$. Then

$$|P(\mathcal{C}^* \cup \mathcal{F})| = |\mathcal{F}| + e < |\mathcal{C} \cup \mathcal{F}| = |\mathcal{F}| + e + 1 \ .$$

This violates (2.3), so $\mathcal{S}$ doesn't have unique factorization. $\square$

Proof of Theorem 1.2. If the matrix M does not have full column rank, then it contains a $\mathbb{Z}$-linear dependence of columns, which yields two factorizations

$$n_1 = \prod_{c \in \mathcal{C}} c^{e_1(c)} \text{ and } n_2 = \prod_{c \in \mathcal{C}} c^{e_2(c)}$$

such that n_1 and n_2 have prime factorizations differing only at nonexceptional primes $p \in \mathcal{P} \backslash \mathcal{E} \subseteq \mathcal{G}$. Multiplying n_1 and n_2 by appropriate powers of these nonexceptional primes yields an element $s \in \mathcal{S}$ with two factorizations, a contradiction.

Conversely, any nonunique factorization in $\mathcal{S}$ when restricted in its action to primes in $\mathcal{E}$, will yield a $\mathbb{Z}$-linear dependency among the columns of M. $\square$

Appendix A. Hall's theorem for Countable Families of Finite Sets

This proof is due to R. Rado and appears in Mirsky [14, p. 55].

Theorem A.1. *Let $\mathcal{U} = \{A_i : i \in \mathbb{N}\}$ be a countable family of finite sets contained in a countable set $\mathcal{P}$, and suppose that Hall's condition*

$$|\bigcup_{i\in I} A_i| \geq |I| \quad \textit{for all finite} \quad I \subseteq \mathbb{N} ,$$

is satisfied. Then there exists a one-to-one map $f : \mathbb{N} \to \mathcal{P}$ such that

$$f(i) \in A_i \quad \textit{for all} \quad i \in I ,$$

i.e. f is a transversal of $\mathcal{U}$.

Proof. By the finite case of Hall's theorem (see for example [12, Chapter 1], [15], [18]) for each $r \geq 1$ there exist r distinct elements $p_{r,1} \in A_1, \ldots, p_{r,r} \in A_r$. Now the $p_{r,1}$ all belong to the finite set A_1. So there is an infinite subsequence $\mathbb{N}_1$ of natural numbers with all $p_{r,1} = p_1$, say. Extract from this a subsequence $\mathbb{N}_2 \subseteq \mathbb{N}_1$ of natural numbers such that $p_{r,2} = p_2$, say. Repeating this argument yields a sequence of distinct representatives

$$p_n \in A_n \quad \text{for all} \quad n \geq 1 ,$$

and we set $f(n) = p_n$. $\square$

References

[1] P. T. Bateman and H. Diamond, Asymptotic distribution of Beurling's generalized prime numbers, in: *Studies in Number Theory* (W. LeVeque, Ed.), MAA Studies in Math. Vol. 6, Prentice-Hall: Englewood Cliffs, NJ, 1969.

[2] A. Beurling, Analyse de la loi asymptotique de la distribution des nombres premiers généralisés I, Act Math. **68** (1937) 255–291.

[3] B. N. Delone, N. P. Dolbilin, M. I. Shtogrin, R. V. Galiulin, A local criterion for regularity of a system of points, Sov. Math. Dokl. **17** No. 2 (1976), 319–322.

[4] H. G. Diamond, Asymptotic distribution of Beurling's generalized prime numbers, Illinois J. Math. **14** (1970), 12–28.

[5] H. G. Diamond, A set of generalized numbers showing Beurling's theorem to be sharp, Illinois J. Math. **14** (1970), 29–34.

[6] H. G. Diamond, Chebyshev estimates for Beurling generalized prime numbers, Proc. Amer. Math. Soc. **39** (1973), 503–508.

[7] P. Engel, *Geometric Crystallography*, D. Reidel Publ. Co., Dordrecht 1986.

[8] P. Engel, *Geometric Crystallography*, in: *Handbook of Convex Geometry, Volume B* (P. Gruber and J. M. Willis, Ed.) North-Holland: Amsterdam 1993, pp. 989–1041.

[9] P. Hall, On representatives of subsets, J. London Math. Soc. **10** (1935), 26–30.

[10] R. S. Hall, Beurling generalized prime number systems in which the Chebyshev inequalities fail, Proc. Amer. Math. Soc. **40** (1973), 79–82.

[11] J. Knopfmacher, *Abstract Analytic Number Theory*, North-Holland Publ. Co.: Amsterdam 1975.

[12] L. Lovasz and M. D. Plummer, *Matching Theory*, North-Holland: Amsterdam 1986.

[13] P. Malliavin, Sur le reste la loi asymptotique de répartition des nombres premiers generalisés de Beurling, Acta Math. **106** (1961), 281–298.

[14] L. Mirsky, *Transversal Theory*, Academic Press: New York 1971.

[15] L. Mirsky and H. Perfect, Systems of Representatives, J. Math. Anal. Appl. **15** (1966), 520–568.

[16] Sz. Revesz, On Beurling's prime number theorem, Period. Math. Hungarica **28** (1994), 195–210.

[17] M. Senechal, *Quasicrystals and Geometry*, Cambridge University Press: New York 1995.

[18] J. H. van Lint, *A Course in Combinatorics*, Cambridge University Press: New York 1992.

address: Room C235
AT&T Labs -- Research
180 Park Avenue
Florham Park, NJ 07932-0971
USA
email: jcl@research.att.com