Spring 2022

Covering Systems and the Minimum Modulus Problem

Maria Claire Cummings

Covering Systems and the Minimum Modulus Problem

by

Maria Claire Cummings

Bachelor of Science
Randolph-Macon College 2020

Submitted in Partial Fulfillment of the Requirements

for the Degree of Master of Science in

Mathematics

College of Arts and Sciences

University of South Carolina

2022

Accepted by:

Ognian Trifonov, Director of Thesis

Michael Filaseta, Director of Thesis and Reader

Tracey L. Weldon, Vice Provost and Dean of the Graduate School

Dedication

To my mom and sister.

Abstract

A covering system or a covering is a set of linear congruences such that every integer satisfies at least one of these congruences. In 1950, Erdős posed a problem regarding the existence of a finite covering with distinct moduli and an arbitrarily large minimum modulus. This remained unanswered until 2015 when Robert Hough proved an explicit bound of 10^{16} for the minimum modulus of any such covering. In this thesis, we examine the use of covering systems in number theory results, expand upon the proof of the existence of an upper bound on the minimum modulus in the case of distinct square-free moduli, and give a sharper bound of 118 for the minimum modulus of a finite covering with distinct square-free moduli.

Table of Contents

Chapter 1

Covering Systems

1.1 Background

Let $k \geq 2$ be an integer. We define a *covering system* to be a set of linear congruences $x \equiv a_j \pmod{m_j}$ with $1 \leq j \leq k$ such that every integer satisfies at least one of these congruences. We begin with a historic background on covering systems.

For example, the congruences $x \equiv 0 \pmod 2$ and $x \equiv 1 \pmod 2$ cover the integers. We define a covering system to be *exact* if every integer satisfies exactly one congruence in the system.

Theorem 1.1.1. *If a finite covering system is exact and the minimum modulus is greater than one, then the maximum modulus is the modulus for at least two congruences in the system.*

Proof. Let $x \equiv a_j \pmod{m_j}$ with $1 \leq j \leq r$ be an exact finite covering system. Without loss of generality, we take $0 \leq a_j < m_j$. For the sake of contradiction, suppose the maximum modulus is the modulus for exactly one congruence in the system. We have $1/(1-z) = 1 + z + z^2 + \ldots$. Expressing the exponents using our covering system, we have

$$\frac{1}{1-z} = \sum_{j=1}^{r}(z^{a_j} + z^{a_j+m_j} + z^{a_j+2m_j} + \ldots) = \sum_{j=1}^{r} \frac{z^{a_j}}{1-z^{m_j}}.$$

If we let z approach $\zeta_{\max\{m_j\}}$, the left-hand side converges while the right-hand side diverges. Thus, we have a contradiction. Therefore, the maximum modulus is the modulus for at least two congruences in the system. $\square$

In 1950, Paul Erdős [3] proved that a positive proportion of odd positive integers cannot be expressed in the form $p + 2^n$ where p is prime and n is a nonnegative integer. In this proof he used the following covering system:

$$\begin{aligned} n &\equiv 0 \pmod 2 & \qquad n &\equiv 3 \pmod 8 \\ n &\equiv 0 \pmod 3 & n &\equiv 7 \pmod{12} \\ n &\equiv 1 \pmod 4 & n &\equiv 23 \pmod{24}. \end{aligned}$$

Taking k to be an integer satisfying

$$
\begin{aligned}
k &\equiv 1 \pmod{2} \\
k &\equiv 1 \pmod{3} \\
k &\equiv 1 \pmod{7} \\
k &\equiv 2 \pmod{5}
\end{aligned}
\qquad
\begin{aligned}
k &\equiv 8 \pmod{17} \\
k &\equiv 11 \pmod{13} \\
k &\equiv 121 \pmod{241},
\end{aligned}
$$

he showed that $k-2^n$ must be divisible by at least on element of $S = \{3, 5, 7, 13, 17, 241\}$, but also $k - 2^n \notin S$ for every nonnegative integer n.

We define a *Sierpiński number* to be an odd integer $k > 0$ such that $k \cdot 2^n + 1$ is composite for all positive integers n. In 1960, Wacław Sierpiński proved that a positive proportion of integers $k > 0$ are Sierpiński numbers [12]. He also used the following covering system:

$$
\begin{aligned}
n &\equiv 1 \pmod{2} \\
n &\equiv 2 \pmod{4} \\
n &\equiv 4 \pmod{8} \\
n &\equiv 8 \pmod{16}
\end{aligned}
\qquad
\begin{aligned}
n &\equiv 16 \pmod{32} \\
n &\equiv 32 \pmod{64} \\
n &\equiv 0 \pmod{64}.
\end{aligned}
$$

Similarly, he took k to be an integer satisfying

$$
\begin{aligned}
k &\equiv 1 \pmod{3} \\
k &\equiv 1 \pmod{5} \\
k &\equiv 1 \pmod{17} \\
k &\equiv 1 \pmod{257}
\end{aligned}
\qquad
\begin{aligned}
k &\equiv 1 \pmod{65537} \\
k &\equiv 1 \pmod{641} \\
k &\equiv -1 \pmod{6700417}.
\end{aligned}
$$

John Selfridge found the smallest known Sierpiński number, 78557, in 1962. Andrzej Schinzel deduced that the existence of Sierpiński numbers follows from the result of Erdős.

Similarly, using covering arguments it has been proven that there are infinitely many Riesel numbers, odd positive integers satisfying $k \cdot 2^n - 1$ is composite for all positive integers n [9], and infinitely many Brier numbers, odd positive integers satisfying $k \cdot 2^n \pm 1$ is composite for all positive integers n.

Additionally, there exist infinitely many primes p such that if any one digit of p, including any one of its infinitely many leading 0 digits, is replaced by any other digit, then the resulting number is composite [5]; and for every $r \in \mathbb{Z}^+$, there exist r consecutive primes like the above each of which is also a Brier number [4].

Ron Graham showed using a covering argument that there exist infinitely many relatively prime pairs of positive integers a and b such that the recursive Fibonacci-like sequence $u_0 = a, u_1 = b,$ and $u_{n+1} = u_n + u_{n-1}$ for all $n \geq 1$, consists entirely of composite numbers [6].

Another application of covering systems, by Lenny Jones [8], is that there are infinitely many positive integers d with $d \not\equiv 0 \pmod 3$ and $d \not\equiv 3 \pmod{10}$ such that $d \cdot 10^n + \sum_{i=1}^{n} 3 \cdot 10^{i-1}$ for $n \geq 1$ consists entirely of composite numbers. For example, $d = 410$ has the above property. Each term in the sequence $\{410, 4103, 41033, 410333, \ldots\}$ is composite.

Problem 1.1.2. *For every positive integer c, does there exist a finite covering with distinct moduli and minimum modulus $\geq c$?*

First posed by Erdős [3], Robert Hough [7] showed to the contrary that the minimum modulus must be $\leq 10^{16}$. This bound has been reduced to 616000 by P. Balister, B. Bollobás, R. Morris, J. Sahasrabudhe, and M. Tiba [2].

Problem 1.1.3. *Does there exist an odd covering of the integers, that is a finite covering with distinct odd moduli > 1?*

While no answer has been shown, P. Balister, B. Bollobás, R. Morris, J. Sahasrabudhe, and M. Tiba [2] proved that every covering with distinct odd moduli > 1 has a modulus divisible by one of 2, 9, and 15.

Problem 1.1.4. *Does there exist a finite covering with distinct moduli* > 1 *and where no modulus divides another?*

Schinzel [11] showed that if such coverings exist, then there is an odd covering of the integers. This questions has been resolved by P. Balister, B. Bollobás, R. Morris, J. Sahasrabudhe, and M. Tiba [2]. Specfically, they showed that every finite covering system with distinct moduli > 1 has some modulus which divides a different modulus.

We define a *Sierpiński polynomial* to be a polynomial $f(x) \in \mathbb{Z}[x]$ with $f(1) \neq -1$ and $f(x)x^n + 1$ reducible over the rationals for all positive integers n. It is not currently known whether a Sierpiński polynomial exists. Although for $f(x) = 5x^9 + 6x^8 + 3x^6 + 8x^5 + 9x^3 + 6x^2 + 8x + 3$, Schinzel showed $f(x)x^n + 12$ is reducible over the rationals for all positive integers n, which can be proven using the following covering:

$$n \equiv 0 \pmod 2$$

$$n \equiv 2 \pmod 3$$

$$n \equiv 1 \pmod 4$$

$$n \equiv 1 \pmod 6$$

$$n \equiv 3 \pmod{12}.$$

Theorem 1.1.5. *The following are almost equivalent:*

1. *There exists a Sierpiński polynomial.*

2. *There is a polynomial* $g(x) \in \mathbb{Z}[x]$ *such that* $f(x) = f_n(x) = x^n + g(x)$ *satisfies* $f(0) \neq 0$, $f(1) \neq 0$, *and* $f(x)$ *is reducible for every nonnegative integer* n.

3. *There is a finite covering of the integers with each modulus* > 1 *and where no modulus divides another.*

In order to have equivalence, a statement stronger than item 3 but weaker than the odd covering problem is needed. An exact statement of equivalent conditions can be found in Schinzel [11].

1.2 Answering the Minimum Modulus Problem

In this section, we discuss our main goal and give some preliminary results. As a simple result, we make use of the following to more efficiently check a covering system's validity.

Lemma 1.2.1. *Let $\mathcal{C}$ be a system of congruences consisting of moduli $m_1, \ldots, m_r$, and set $L = lcm(m_1, \ldots, m_r)$. Then, $\mathcal{C}$ is a covering system if and only if every integer in $[1, L]$ is satisfied by a congruence in $\mathcal{C}$.*

For example, consider the covering:

$$n \equiv 0 \pmod 2 \qquad n \equiv 3 \pmod 8$$

$$n \equiv 0 \pmod 3 \qquad n \equiv 7 \pmod{12}$$

$$n \equiv 1 \pmod 4 \qquad n \equiv 23 \pmod{24}.$$

Here $L = 24$. We need only check that each integer from 1 to 24 satisfies at least one congruences to verify that the above is a covering system.

Proof of Lemma 1.1. Let $\mathcal{C}$ be a system of congruences with the least common multiple of the moduli equal to L. If $\mathcal{C}$ is a covering system, then every integer in $[1, L]$ satisfies a congruence in $\mathcal{C}$. Now, suppose every integer in $[1, L]$ satisfies a congruence in $\mathcal{C}$. Let n be an integer. Let $a \equiv n \pmod L$ where $1 \leq a \leq L$. Then, there exists a congruence $x \equiv b \pmod m$ in $\mathcal{C}$ such that $a \equiv b \pmod m$. Since $a \equiv n \pmod L$ and m divides L, we have $n \equiv a \equiv b \pmod m$. Therefore, n satisfies the congruence $x \equiv b \pmod m$ in $\mathcal{C}$. Thus, $\mathcal{C}$ is a covering system. $\square$

We will now be considering finite covering systems with distinct square-free moduli

> 1. For example, the following is such a covering system:

$$
\begin{array}{lll}
n \equiv 0 \pmod{2} & n \equiv 1 \pmod{10} & n \equiv 4 \pmod{35} \\
n \equiv 0 \pmod{3} & n \equiv 1 \pmod{14} & n \equiv 5 \pmod{42} \\
n \equiv 0 \pmod{5} & n \equiv 2 \pmod{15} & n \equiv 59 \pmod{70} \\
n \equiv 1 \pmod{6} & n \equiv 2 \pmod{21} & n \equiv 104 \pmod{105} \\
n \equiv 0 \pmod{7} & n \equiv 23 \pmod{30} &
\end{array}
$$

Here, we have $L = 210 = 2 \cdot 3 \cdot 5 \cdot 7$. We can also think of covering the associated elements of $Q = S_1 \times S_2 \times S_3 \times S_4$ where $S_1 = \{1, 2\}$, $S_2 = \{1, 2, 3\}$, $S_3 = \{1, 2, 3, 4, 5\}$, and $S_4 = \{1, 2, 3, 4, 5, 6, 7\}$. With this approach each congruence covers a portion of Q. For example, the congruence $n \equiv 0 \pmod{2}$ covers $\{2\} \times S_2 \times S_3 \times S_4 \subseteq Q$. By the Chinese Remainder Theorem, each integer in $[1, L]$ uniquely corresponds to an element of Q. For example, the integer 77 corresponds to $(1, 2, 2, 7)$ in Q since $77 \equiv 1 \pmod{2}$, $77 \equiv 2 \pmod{3}$, $77 \equiv 2 \pmod{5}$, and $77 \equiv 7 \pmod{7}$.

In general, we let $S_1, \ldots, S_n$ be finite sets. We define a *hyperplane* to be $A = Y_1 \times \ldots \times Y_n$ where $Y_j \subseteq S_j$ and $|Y_j| \in \{1, |S_j|\}$ for $j \in \{1, \ldots, n\}$. We also define two hyperplanes A and A' to be *parallel* if $F(A) = F(A')$ where $F(A) = \{j : |Y_j| = 1\}$. We call $F(A)$ the set of fixed coordinates of A. We consider the set of natural numbers $\mathbb{N}$ to be the set of positive integers.

Theorem 1.2.2. *For every sequence of finite sets $S_1, S_2, \ldots$, each of size at least 2, satisfying $\liminf_{k \to \infty} |S_k|/k > 3$, there is a positive integer C such that the following holds. Let $\mathcal{A}$ be a collection of hyperplanes that cover $Q = S_1 \times \ldots \times S_n$ for some $n \in \mathbb{N}$, (that is, every element of Q is on some hyperplane in $\mathcal{A}$). Suppose no two hyperplanes in $\mathcal{A}$ are parallel. Then, there exists a hyperplane $A \in \mathcal{A}$ with $F(A) \subseteq \{1, \ldots, C\}$.*

One goal of this thesis is to prove the above theorem following the arguments of P. Balister, B. Bollobás, R. Morris, J. Sahasrabudhe, and M. Tiba in [1]. Our interest here is in the following corollary that they obtain, which proves a negative answer to Problem 1.1.2 for finite coverings with square-free moduli.

Corollary 1.2.3. *There is an absolute constant C_{min} such that every covering system with distinct square-free moduli has a minimum modulus which is at most C_{min}.*

Proof. Let $\mathcal{C}$ be a covering system with distinct square-free moduli. Let p_j denote the jth prime, and set $S_j = \{1, ..., p_j\}$. Observe that each S_j is of size at least 2 and satisfies $\liminf_{k\to\infty} |S_k|/k = \lim_{k\to\infty} p_k/k = \infty > 3$. Let C be as in Theorem 1.2.2. Let p_n be the largest prime dividing a modulus in $\mathcal{C}$. Set $Q = S_1 \times \ldots \times S_n$. Each congruence $x \equiv a \pmod{m}$ corresponds to a hyperplane $A_m = Y_1 \times \ldots \times Y_n \subseteq Q$ where (i) if p_j divides m, then $Y_j = \{b\}$ with $b \equiv a \pmod{p_j}$ and $b \in S_j$, and (ii) if p_j does not divides m, then $Y_j = S_j$. Then, the covering $\mathcal{C}$ corresponds to a finite collection of hyperplanes $\mathcal{A}$ which covers Q. Note that the moduli of $\mathcal{C}$ are distinct, so the hyperplanes in $\mathcal{A}$ are pairwise non-parallel. Thus, by Theorem 1.2.2, there exists an $A_m \in \mathcal{A}$ with $F(A_m) \subseteq \{1, \ldots, C\}$. Observe that this m divides $p_1 \cdots p_C$. Therefore, we can take $C_{min} = p_1 \cdots p_C$. $\square$

A second goal of this thesis is to modify the arguments by P. Balister, B. Bollobás, R. Morris, J. Sahasrabudhe, and M. Tiba in [1] to show the following.

Theorem 1.2.4. *Every covering system with distinct square-free moduli has a minimum modulus which is ≤ 118.*

As illustrated earlier in this section, there is a covering system with distinct square-free moduli and minimum modulus equal to 2. However, it is an open question as to whether there is such a covering with minimum modulus equal to 3. So a reasonable conjecture is that the bound 118 above can be replaced by 2.

Chapter 2

The Distortion Method

2.1 The Set-Up

We will prove Theorem 1.2.2 by expanding upon the method outlined in [1]. Let $S_1, S_2, \ldots$ be an infinite sequence of finite sets. For a positive integer k, define $Q_k = S_1 \times \ldots \times S_k$. Fix a positive integer n. Let $\mathcal{A}$ be a collection of hyperplanes, pairwise non-parallel, that cover Q_n. We define a *weight* on a set $X = \{x_1, \ldots, x_k\}$ to be a function mapping each x_i to $q_i \geq 0$ for $1 \leq i \leq k$ such that $q_1 + \ldots + q_k = 1$.

Let $Q = Q_n$. We define weights $w_n(x)$ on the elements x of Q. From the previous section, for covering systems, these weights correspond to weights on the integers in the interval $[1, L]$ where $L = p_1 \cdots p_n$. The weight of a subset $T \subseteq Q$ is defined as the sum of the weights of the elements in T, so $w_n(T) = \sum_{x \in T} w_n(x)$. We interpret this to mean $w_n(\emptyset) = 0$. If $x = (a_1, \ldots, a_{k-1}) \in S_1 \times \ldots \times S_{k-1}$ and $y \in S_k$, then we write $w_k(x, y) = w_k((a_1, \ldots, a_{k-1}, y)) = w_n(A)$ where A is the hyperplane

$$A = \{a_1\} \times \{a_2\} \times \ldots \times \{a_{k-1}\} \times \{y\} \times S_{k+1} \times \ldots \times S_n \tag{2.1}$$

In general, if $X \subseteq S_1 \times \ldots \times S_k$, then we identify $w_k(X)$ with $w_k(X \times S_{k+1} \times \ldots \times S_n)$. The fiber F_x associated to $x = (a_1, \ldots, a_{k-1}) \in S_1 \times \ldots \times S_{k-1}$ is the set of tuples $(a_1, \ldots, a_{k-1}, y) \in S_1 \times \ldots \times S_k$. At the kth stage, we will determine the weights of the hyperplanes in the form of (1). We define $\mathcal{A}_k = \{A \in \mathcal{A} : \max(F(A)) = k\}$. In the languages of congruences, $\mathcal{A}_1$ corresponds to the set of congruences modulo $p_1 = 2$, $\mathcal{A}_2$ corresponds to the set of congruences modulo $p_2 = 3$ and $p_1 p_2$, and so on. We also define $B_k = \bigcup_{A \in \mathcal{A}_k} A$. With regard to coverings, B_k corresponds to the elements of Q_n which are covered by a congruence with a modulus whose largest prime divisor is p_k. Note that if $A \in \mathcal{A}_k$, then $F(A) \subseteq \{1, \ldots, k\}$, so B_k can also be thought of as a subset of $Q_k = S_1 \times \ldots \times S_k$.

In our proof of Theorem 1.2.2, by assigning weights to elements of Q in the manner below and supposing $F(A) \nsubseteq \{1, \ldots, C\}$ for every hyperplane $A \in \mathcal{A}$, we prove that the collection of hyperplanes $\mathcal{A}$ does not cover Q to obtain our result by contradiction.

Let $1 \leq k \leq n$. Pick $\delta \in [0, 1/2]$. We define the weights w_k inductively. When $k = 1$, if $y \in S_1$ and $|B_1|/|S_1| \leq \delta$, we set

$$w_1(y) = \begin{cases} 0 & \text{if } y \in B_1 \\ \dfrac{1}{|S_1| - |B_1|} & \text{if } y \notin B_1. \end{cases}$$

If $y \in S_1$ and $|B_1|/|S_1| > \delta$, we set

$$w_1(y) = \begin{cases} \dfrac{(|B_1|/|S_1|) - \delta}{(|B_1|/|S_1|)(1 - \delta)} \cdot \dfrac{1}{|S_1|} & \text{if } y \in B_1 \\ \dfrac{1}{1 - \delta} \cdot \dfrac{1}{|S_1|} & \text{if } y \notin B_1. \end{cases}$$

Observe that in both cases, we have $\sum_{y \in S_1} w_1(y) = 1$ (see a similar argument below). The above weights correspond to setting $k = 1$ and replacing $\alpha_1(x)$ with $|B_1|/|S_1|$ and $w_0(x)$ with 1 in the discussion below. Suppose $k \geq 2$ and w_{k-1} is defined on Q_{k-1}. Since $Q_k = Q_{k-1} \times S_k$, each element of Q_k can be written in the form (x, y) where $x \in Q_{k-1}$ and $y \in S_k$. For each $x \in Q_{k-1}$, we define

$$\alpha_k(x) = \frac{|\{y \in S_k : (x, y) \in B_k\}|}{|S_k|} = \frac{|F_x \cap B_k|}{|S_k|},$$

which is the proportion of the fiber $F_x = \{(x, y) : y \in S_k\}$ that is covered by one or more hyperplanes in $\mathcal{A}_k$. If $\alpha_k(x) \leq \delta$, we set

$$w_k(x, y) = \begin{cases} 0 & \text{if } (x, y) \in B_k \\ \dfrac{1}{1 - \alpha_k(x)} \cdot \dfrac{w_{k-1}(x)}{|S_k|} & \text{if } (x, y) \notin B_k. \end{cases}$$

If $\alpha_k(x) > \delta$, we set

$$w_k(x,y) = \begin{cases} \dfrac{\alpha_k(x)-\delta}{\alpha_k(x)(1-\delta)} \cdot \dfrac{w_{k-1}(x)}{|S_k|} & \text{if } (x,y) \in B_k \\ \dfrac{1}{1-\delta} \cdot \dfrac{w_{k-1}(x)}{|S_k|} & \text{if } (x,y) \notin B_k. \end{cases}$$

Observe that if x is an element of Q_{k-1} and $\alpha_k(x) \le \delta$, we have

$$\begin{aligned} \sum_{y \in S_k} w_k(x,y) &= \sum_{\substack{y \in S_k \\ (x,y) \in B_k}} w_k(x,y) + \sum_{\substack{y \in S_k \\ (x,y) \notin B_k}} w_k(x,y) \\ &= \sum_{\substack{y \in S_k \\ (x,y) \in B_k}} 0 + \sum_{\substack{y \in S_k \\ (x,y) \notin B_k}} \frac{1}{1-\alpha_k(x)} \cdot \frac{w_{k-1}(x)}{|S_k|} \\ &= \frac{1}{1-\alpha_k(x)} \cdot \frac{w_{k-1}(x)}{|S_k|} \sum_{\substack{y \in S_k \\ (x,y) \notin B_k}} 1 \\ &= \frac{1}{1-\alpha_k(x)} \cdot \frac{w_{k-1}(x)}{|S_k|} \cdot (|S_k| - |S_k|\alpha_k(x)) \\ &= w_{k-1}(x). \end{aligned}$$

Also, if x is an element of Q_{k-1} and $\alpha_k(x) > \delta$, we then have

$$\begin{aligned} \sum_{y \in S_k} w_k(x,y) &= \sum_{\substack{y \in S_k \\ (x,y) \in B_k}} w_k(x,y) + \sum_{\substack{y \in S_k \\ (x,y) \notin B_k}} w_k(x,y) \\ &= \sum_{\substack{y \in S_k \\ (x,y) \in B_k}} \frac{\alpha_k(x)-\delta}{\alpha_k(x)(1-\delta)} \cdot \frac{w_{k-1}(x)}{|S_k|} + \sum_{\substack{y \in S_k \\ (x,y) \notin B_k}} \frac{w_{k-1}(x)}{|S_k|(1-\delta)} \\ &= \frac{\alpha_k(x)-\delta}{\alpha_k(x)(1-\delta)} \cdot \frac{w_{k-1}(x)}{|S_k|} \sum_{\substack{y \in S_k \\ (x,y) \in B_k}} 1 + \frac{w_{k-1}(x)}{|S_k|(1-\delta)} \sum_{\substack{y \in S_k \\ (x,y) \notin B_k}} 1 \\ &= \frac{\alpha_k(x)-\delta}{\alpha_k(x)(1-\delta)} \cdot \frac{w_{k-1}(x)}{|S_k|} \cdot \alpha_k(x)|S_k| + \frac{w_{k-1}(x)}{|S_k|(1-\delta)}(|S_k| - |S_k|\alpha_k(x)) \\ &= \frac{(\alpha_k(x)-\delta)w_{k-1}(x)}{1-\delta} + \frac{(1-\alpha_k(x))w_{k-1}(x)}{1-\delta} \\ &= w_{k-1}(x). \end{aligned}$$

In both cases, we have $\sum_{y \in S_k} w_k(x,y) = w_{k-1}(x)$, so weight is preserved at each stage.

Thus, if $\alpha_k(x) \le \delta$, then we have set $w_k(x,y) = 0$ if $(x,y) \in B_k$ and increased the weight $w_k(x,y)$ proportionally on the rest of F_x. If $\alpha_k(x) > \delta$, then we have increased the weight of each element in $F_x \setminus B_k$ by a distortion factor of $1/(1-\delta)$ and decreased the weight of $F_x \cap B_k$.

For example, consider the covering:

$$\begin{array}{lll}
n \equiv 0 \pmod{2} & n \equiv 1 \pmod{10} & n \equiv 4 \pmod{35} \\
n \equiv 0 \pmod{3} & n \equiv 1 \pmod{14} & n \equiv 5 \pmod{42} \\
n \equiv 0 \pmod{5} & n \equiv 2 \pmod{15} & n \equiv 59 \pmod{70} \\
n \equiv 1 \pmod{6} & n \equiv 2 \pmod{21} & n \equiv 104 \pmod{105} \\
n \equiv 0 \pmod{7} & n \equiv 23 \pmod{30} &
\end{array}$$

Observe that the least common multiple of the moduli is $L = 210 = 2\cdot 3\cdot 5\cdot 7$. Suppose $\delta = 1/2$. Then, when $k = 1$, we consider residues modulo 2 and the congruence $n \equiv 0 \pmod{2}$. We have two residue classes: $1 \pmod{2}$ and $2 \pmod{2}$. Note that the congruence $n \equiv 0 \pmod{2}$ covers $2 \pmod{2}$ but does not cover $1 \pmod{2}$. We have $1/|S_1| = 1/2$. Then, $w_1((1)) = 1$ and $w_1((2)) = 0$, so all k-tuples beginning with 2 will have weight 0. Now, consider $k = 2$. We have three residue classes modulo 3: $1 \pmod{3}$, $2 \pmod{3}$, $3 \pmod{3}$; and we consider the congruences $n \equiv 0 \pmod{3}$ and $n \equiv 1 \pmod{6}$. Of the integers n which satisfy $n \equiv 1 \pmod{2}$, those which are $3 \pmod{3}$ are covered by the congruence $n \equiv 0 \pmod{3}$. Those that are $1 \pmod{3}$ are covered by the congruence $n \equiv 1 \pmod{6}$. However, those that are $2 \pmod{3}$ are not covered by either congruence. Hence, $\alpha_2((1)) = 2/3$. We have $w_1((1,1)) = 1/6$, $w_1((1,2)) = 2/3$, and $w_1((1,3)) = 1/6$. For $k = 3$, the weights are given in Figure 2.1. We see that the k-tuples covered least frequently by the congruences have a higher weight, and those covered frequently have lower weight.

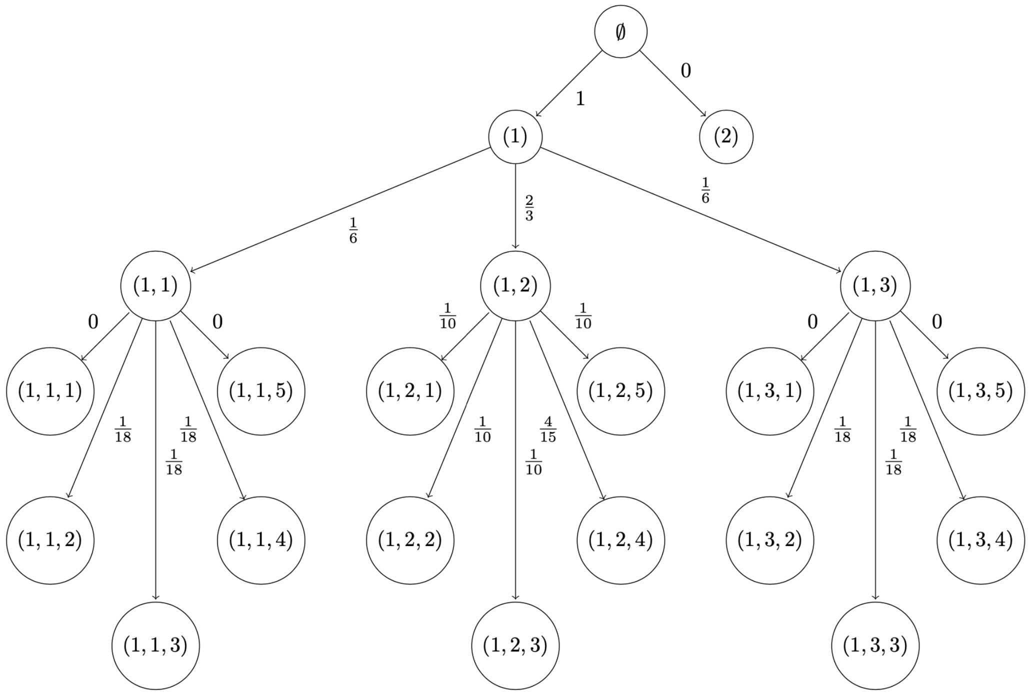

Figure 2.1 Weights for $\delta = 1/2$

2.2 Further Preliminaries

We begin with some preliminary lemmas. We define the weighted sum

$$\mathbb{E}_{k-1}[\alpha_k(x)^2] = \begin{cases} \sum_{x \in Q_{k-1}} \alpha_k(x)^2 w_{k-1}(x) & \text{if } k \geq 2 \\ (|B_1|/|S_1|)^2 & \text{if } k = 1. \end{cases}$$

Here, we have maintained the notation used in [1], where they viewed $w_{k-1}(x)$ as a probability function and $\mathbb{E}_{k-1}[\alpha_k(x)^2]$ to be the expected value of $\alpha_k(x)^2$.

Lemma 2.2.1. *Let $\mathcal{A}$ be a collection of hyperplanes in $Q = S_1 \times \ldots \times S_n$. Let $k \geq 1$. We have*

$$w_k(B_k) \leq \frac{1}{4\delta(1-\delta)} \mathbb{E}_{k-1}[\alpha_k(x)^2].$$

Proof. First, consider $w_k(B_k)$ with $k \geq 2$. We have

$$\begin{aligned} w_k(B_k) &= \sum_{x \in Q_{k-1}} \sum_{\substack{y \in S_k \\ (x,y) \in B_k}} w_k(x,y) \\ &\leq \sum_{x \in Q_{k-1}} |F_x \cap B_k| \cdot \max\left\{0, \frac{\alpha_k(x) - \delta}{\alpha_k(x)(1-\delta)}\right\} \cdot \frac{w_{k-1}(x)}{|S_k|}. \end{aligned}$$

Since $\alpha_k(x) = |F_x \cap B_k|/|S_k|$, then we have

$$w_k(B_k) \leq \frac{1}{1-\delta} \sum_{x \in Q_{k-1}} \max\{0, \alpha_k(x) - \delta\} \cdot w_{k-1}(x).$$

Observe that $4\delta^2 - 4\delta\alpha_k(x) + \alpha_k(x)^2 = (2\delta - \alpha_k(x))^2 \geq 0$, so $\alpha_x(x)^2/4\delta \geq \alpha_k(x) - \delta$. Thus,

$$\begin{aligned} w_k(B_k) &\leq \frac{1}{1-\delta} \sum_{x \in Q_{k-1}} \frac{\alpha_k(x)^2}{4\delta} \cdot w_{k-1}(x) \\ &= \frac{1}{4\delta(1-\delta)} \sum_{x \in Q_{k-1}} \alpha_k(x)^2 \cdot w_{k-1}(x) \\ &= \frac{1}{4\delta(1-\delta)} \mathbb{E}_{k-1}[\alpha_k(x)^2]. \end{aligned}$$

In the case that $k = 1$, we have

$$w_1(B_1) = \sum_{y \in B_1} w_1(y) \leq |B_1| \cdot \max\left\{0, \frac{(|B_1|/|S_1|) - \delta}{(|B_1|/|S_1|)(1-\delta)}\right\} \cdot \frac{1}{|S_1|}.$$

Following the arguments above, we obtain

$$w_1(B_1) \leq \frac{1}{4\delta(1-\delta)} \left(\frac{|B_1|}{|S_1|}\right)^2 = \frac{1}{4\delta(1-\delta)} \mathbb{E}_0[\alpha_1(x)^2].$$

The lemma follows. □

Lemma 2.2.2. *Let $\mathcal{A}$ be a collection of hyperplanes in $Q = S_1 \times \ldots \times S_n$. If*

$$\frac{1}{4\delta(1-\delta)} \sum_{k=1}^{n} \mathbb{E}_{k-1}[\alpha_k(x)^2] < 1,$$

then $\mathcal{A}$ does not cover Q.

Proof. Suppose the above inequality holds. By Lemma 2.2.1, for $k \geq 1$, we know

$$w_k(B_k) \leq \frac{1}{4\delta(1-\delta)} \mathbb{E}_{k-1}[\alpha_k(x)^2].$$

Since $1/(4\delta(1-\delta)) \cdot \sum_{k=1}^{n} \mathbb{E}_{k-1}[\alpha_k(x)^2] < 1$, the total weight of all the elements of Q covered by the hyperplanes in $\mathcal{A}$ is at most

$$\sum_{k=1}^{n} w_n(B_k) = \sum_{k=1}^{n} w_k(B_k) \leq \frac{1}{4\delta(1-\delta)} \cdot \sum_{k=1}^{n} \mathbb{E}_{k-1}[\alpha_k(x)^2] < 1.$$

Since the total weight of all the elements in Q is 1, we deduce that $\mathcal{A}$ does not cover Q. $\square$

Lemma 2.2.3. *Let $\mathcal{A}$ be a collection of hyperplanes, pairwise non-parallel, in Q. Then, for $1 \leq k \leq n$, we have*

$$\mathbb{E}_{k-1}[\alpha_k(x)^2] \leq \frac{1}{|S_k|^2} \prod_{j=1}^{k-1} \left(1 + \frac{3}{(1-\delta)|S_j|}\right).$$

In order to prove Lemma 2.2.3, we make use of the following two lemmas. First, recall that for any set $X \subseteq Q_{k-1}$, weight is preserved from $k-1$ to k, so we have $w_{k-1}(X) = \sum_{y \in S_k} w_k(X, y) = w_k(X, S_k)$. To reduce notation, we set $w_k(X) = \sum_{y \in S_k} w_k(X, y) = w_k(X, S_k)$ where $X \subseteq Q_{k-1}$. For any element $x \in Q_{k-1}$ and any element $y \in S_k$, we justify that

$$w_k(x, y) \leq \frac{1}{1-\delta} \cdot \frac{w_{k-1}(x)}{|S_k|}.$$

If $k \geq 2$ and $\alpha_k(x) \leq \delta$, we have

$$w_k(x, y) \leq \frac{1}{1-\alpha_k(x)} \cdot \frac{w_{k-1}(x)}{|S_k|} \leq \frac{1}{1-\delta} \cdot \frac{w_{k-1}(x)}{|S_k|}.$$

If $k \geq 2$ and $\alpha_k(x) > \delta$ and $(x, y) \notin B_k$, our result holds by the definition of $w_k(x, y)$. If $k \geq 2$ and $\alpha_k(x) > \delta$ and $(x, y) \in B_k$, then we obtain

$$w_k(x, y) \leq \frac{\alpha_k(x) - \delta}{\alpha_k(x)(1-\delta)} \cdot \frac{w_{k-1}(x)}{|S_k|}$$

$$\leq \left(\frac{1}{1-\delta} - \frac{\delta}{\alpha_k(x)(1-\delta)}\right) \cdot \frac{w_{k-1}(x)}{|S_k|}$$

$$\leq \frac{1}{1-\delta} \cdot \frac{w_{k-1}(x)}{|S_k|}.$$

Also, if $k = 1$, then one can similarly check that for $y \in S_1$, we have

$$w_1(y) \leq \frac{1}{1-\delta} \cdot \frac{1}{|S_1|}.$$

For each $J \subseteq \{1, \ldots, n\}$, we define $\nu(J) = \prod_{j \in J} 1/((1-\delta)|S_j|)$. Also, for a hyperplane $A = Y_1 \times \ldots \times Y_n$ and a set $U \subseteq \{1, \ldots, n\}$, we define $A^U = Y_1^U \times \ldots \times Y_n^U$ to be a hyperplane with $Y_i^U = Y_i$ if $i \in U$ and $Y_i^U = S_i$ if $i \notin U$. We set $A' = A^{\{1,\ldots,k-1\}}$.

Lemma 2.2.4. *Let A be a hyperplane. Let $1 \leq k \leq n$. If $F(A) \subseteq \{1, \ldots, k\}$, then*

$$w_k(A) \leq \nu\Big(F(A)\Big) = \prod_{j \in F(A)} \frac{1}{(1-\delta)|S_j|}.$$

Proof. We will induct on k. For our base case, consider $k = 1$. Let $F(A) \subseteq \{1\}$. If $F(A) = \emptyset$, then $\nu(F(A)) = \nu(\emptyset) = 1$. Here, we deduce

$$w_1(A) = w_1(S_1) = \sum_{y \in S_1} w_1(y) = 1 = \nu(\emptyset).$$

If $F(A) = \{1\}$, then $A = \{y\}$ for some $y \in S_1$, so

$$w_1(A) = w_1(y) \leq \frac{1}{1-\delta} \cdot \frac{1}{|S_1|} = \nu(\{1\}).$$

Thus, if $F(A) \subseteq \{1\}$, we see that $w_1(A) \leq \nu(F(A))$.

For our inductive step, assume our result holds for w_{k-1} with $2 \leq k \leq n$. We consider the following two cases. In case one, suppose $k \notin F(A)$. Then $F(A) \subseteq \{1, \ldots, k-1\}$. We have $w_k(A) = w_{k-1}(A) \leq \nu(F(A))$ by our inductive hypothesis. In case two, suppose $k \in F(A)$. With $A' = A^{\{1,\ldots,k-1\}}$, we see that

$$w_k(A) \leq \frac{1}{1-\delta} \cdot \frac{w_{k-1}(A')}{|S_k|} = \frac{1}{(1-\delta)|S_k|} \cdot w_{k-1}(A').$$

Since $A' \subseteq \{1, \ldots, k-1\}$ and $F(A') = F(A) \setminus \{k\}$, then by our inductive hypothesis, we have $w_{k-1}(A') \leq \nu(F(A) \setminus \{k\})$. Thus,

$$\begin{aligned} w_k(A) &\leq \frac{1}{(1-\delta)|S_k|} \cdot w_{k-1}(A') \\ &\leq \frac{1}{(1-\delta)|S_k|} \cdot \nu(F(A) \setminus \{k\}) \\ &= \nu(F(A)), \end{aligned}$$

finishing the proof. □

Lemma 2.2.5. *Let $\mathcal{A}$ be a collection of hyperplanes, pairwise non-parallel, in Q. Then, for $2 \leq k \leq n$, we have*

$$\mathbb{E}_{k-1}[\alpha_k(x)^2] \leq \frac{1}{|S_k|^2} \sum_{F_1, F_2 \subseteq \{1, \ldots, k-1\}} \nu(F_1 \cup F_2).$$

Proof. We know

$$\alpha_k(x) = \frac{1}{|S_k|} \sum_{\substack{y \in S_k \\ (x,y) \in B_k}} 1 \leq \frac{1}{|S_k|} \sum_{y \in S_k} \sum_{\substack{A \in \mathcal{A}_k \\ (x,y) \in A}} 1 = \frac{1}{|S_k|} \sum_{A \in \mathcal{A}_k} \sum_{\substack{y \in S_k \\ (x,y) \in A}} 1.$$

Since for each $x \in Q_{k-1}$ and $A \in \mathcal{A}_k$, there exists a unique $y \in S_k$ with $(x, y) \in A$ if and only if $x \in A'$, then we have

$$\alpha_k(x) \leq \frac{1}{|S_k|} \sum_{\substack{A \in \mathcal{A}_k \\ x \in A'}} 1.$$

We then deduce

$$\alpha_k(x)^2 \leq \frac{1}{|S_k|^2} \sum_{\substack{A_1, A_2 \in \mathcal{A}_k \\ x \in A_1' \cap A_2'}} 1,$$

so that

$$\sum_{x \in Q_{k-1}} w_{k-1}(x) \alpha_k(x)^2 \leq \frac{1}{|S_k|^2} \sum_{A_1, A_2 \in \mathcal{A}_k} \sum_{\substack{x \in Q_{k-1} \\ x \in A_1' \cap A_2'}} w_{k-1}(x).$$

Thus, we conclude

$$\mathbb{E}_{k-1}(\alpha_k(x)^2) \leq \frac{1}{|S_k|^2} \sum_{A_1, A_2 \in \mathcal{A}_k} w_{k-1}(A_1' \cap A_2').$$

If the intersection of A_1' and A_2' is empty, then $w_{k-1}(A_1' \cap A_2') = 0$. If the intersection of A_1' and A_2' is non-empty, then the intersection is a hyperplane with $(F(A_1) \setminus \{k\}) \cup (F(A_2) \setminus \{k\})$ as its set of fixed coordinates. Let $F_1 = F(A_1) \setminus \{k\}$ and $F_2 = F(A_2) \setminus \{k\}$. Note that F_1 and F_2 uniquely determine A_1 and A_2 in $\mathcal{A}_k$, respectively, since no two hyperplanes in $\mathcal{A}$ are parallel. Therefore, by Lemma 2.2.4, we conclude

$$\begin{aligned}\mathbb{E}_{k-1}(\alpha_k(x)^2) &\leq \frac{1}{|S_k|^2} \sum_{A_1, A_2 \in \mathcal{A}_k} \nu(F(A_1' \cap A_2')) \\ &\leq \frac{1}{|S_k|^2} \sum_{F_1, F_2 \subseteq \{1, \dots, k-1\}} \nu(F_1 \cup F_2).\end{aligned}$$

This completes the proof. $\square$

With these two lemmas, we can now prove Lemma 2.2.3.

Proof of Lemma 2.2.3. We know

$$\begin{aligned}\sum_{F_1, F_2 \subseteq \{1, \dots, k-1\}} \nu(F_1 \cup F_2) &= \sum_{F_1, F_2 \subseteq \{1, \dots, k-1\}} \prod_{j \in F_1 \cup F_2} \left(\frac{1}{(1-\delta)|S_j|} \right) \\ &= \sum_{J \subseteq \{1, \dots, k-1\}} \sum_{\substack{F_1, F_2 \subseteq \{1, \dots, k-1\} \\ F_1 \cup F_2 = J}} \prod_{j \in J} \left(\frac{1}{(1-\delta)|S_j|} \right).\end{aligned}$$

Rearranging the order of our sum and product, we have

$$\begin{aligned}&\sum_{J \subseteq \{1, \dots, k-1\}} \sum_{\substack{F_1, F_2 \subseteq \{1, \dots, k-1\} \\ F_1 \cup F_2 = J}} \prod_{j \in J} \left(\frac{1}{(1-\delta)|S_j|} \right) \\ &\qquad = \sum_{J \subseteq \{1, \dots, k-1\}} \prod_{j \in J} \left(\frac{1}{(1-\delta)|S_j|} \right) \sum_{\substack{F_1, F_2 \subseteq \{1, \dots, k-1\} \\ F_1 \cup F_2 = J}} 1.\end{aligned}$$

Since each element of J with $F_1 \cup F_2 = J$ is either in F_1 and not F_2, in F_2 and not F_1, or in both F_1 and F_2, we deduce

$$\sum_{\substack{F_1, F_2 \subseteq \{1, \dots, k-1\} \\ F_1 \cup F_2 = J}} 1 = 3^{|J|}.$$

Substituting, we have

$$\sum_{J\subseteq\{1,\ldots,k-1\}} 3^{|J|} \prod_{j\in J}\left(\frac{1}{(1-\delta)|S_j|}\right) = \sum_{J\subseteq\{1,\ldots,k-1\}} \prod_{j\in J}\left(\frac{3}{(1-\delta)|S_j|}\right).$$

This last sum of a product can be rewritten as

$$\sum_{J\subseteq\{1,\ldots,k-1\}} \prod_{j\in J}\left(\frac{3}{(1-\delta)|S_j|}\right) = \prod_{j=1}^{k-1}\left(1+\frac{3}{(1-\delta)|S_j|}\right).$$

Thus, by Lemma 2.2.5, we conclude

$$\begin{aligned}\mathbb{E}_{k-1}[\alpha_k(x)^2] &\le \frac{1}{|S_k|^2}\sum_{F_1,F_2\subseteq\{1,\ldots,k-1\}} \nu(F_1\cup F_2)\\ &= \frac{1}{|S_k|^2}\prod_{j=1}^{k-1}\left(1+\frac{3}{(1-\delta)|S_j|}\right),\end{aligned}$$

completing the proof. □

2.3 Proof of Theorem 1.2.2

Using the above lemmas, we now can prove Theorem 1.2.2.

Proof of Theorem 1.2.2. Let $S_1, S_2, \ldots$ be a sequence of finite sets, each of size at least 2, satisfying $\liminf_{k\to\infty} |S_k|/k > 3$. Then, there exist $N \in \mathbb{N}$, say with $N \ge 2$, and $\varepsilon \in (0,1]$ such that $|S_k| \ge (3+\varepsilon)k$ for all $k \ge N$. Observe that we can take C as large as we want and in particular $C \ge N$ in the statement of Theorem 1.2.2, so we do so. Let $\mathcal{A}$ be a collection of hyperplanes, pairwise non-parallel, that cover $Q = S_1 \times \ldots \times S_n$ for some $n \in \mathbb{N}$.

We proceed by contradiction. Assume $F(A) \not\subseteq \{1,\ldots,C\}$ for every $A \in \mathcal{A}$. Then, $B_k = \emptyset$ for $1 \le k \le C$. Therefore, $\alpha_k(x) = |\{y \in S_k : (x,y) \in B_k\}|/|S_k| = 0$ for $k \le C$ and $x \in Q_{k-1}$. In particular, since $C \ge 1$, we see that

$$\mathbb{E}_{k-1}[\alpha_k(x)^2] = 0 \qquad \text{for } 1 \le k \le C.$$

We consider now $k > C \ge N$. Set $\delta = \varepsilon/6 \in (0, 1/6]$. Then, $(1-\delta)|S_j| \ge 5/3$ for all j, and $(1-\delta)|S_j| \ge (1-\varepsilon/6)(3+\varepsilon)j$ for all $j \ge N$. Then, we have

$$\prod_{j=1}^{N-1}\left(1+\frac{3}{(1-\delta)|S_j|}\right) \le \prod_{j=1}^{N-1}\left(1+\frac{3}{5/3}\right) \le \left(\frac{14}{5}\right)^{N-1}.$$

Since $1 + x < e^x$ for all $x > 0$, we deduce that

$$\begin{aligned}\prod_{j=N}^{k-1}\left(1+\frac{3}{(1-\delta)|S_j|}\right) &< \prod_{j=N}^{k-1}\exp\left(\frac{3}{(1-\delta)|S_j|}\right)\\ &= \exp\left(\sum_{j=N}^{k-1}\frac{3}{(1-\delta)|S_j|}\right)\\ &\leq \exp\left(\sum_{j=N}^{k-1}\frac{3}{(1-\varepsilon/6)(3+\varepsilon)j}\right).\end{aligned}$$

Thus, we obtain

$$\prod_{j=1}^{k-1}\left(1+\frac{3}{(1-\delta)|S_j|}\right) \leq \left(\frac{14}{5}\right)^{N-1}\exp\left(\frac{3}{(1-\varepsilon/6)(3+\varepsilon)}\sum_{j=N}^{k-1}\frac{1}{j}\right).$$

Note that

$$\sum_{j=N}^{k-1}\frac{1}{j} \leq \int_{N-1}^{k-1}\frac{1}{x}\,dx = \log\left(\frac{k-1}{N-1}\right).$$

Then, we see that

$$\prod_{j=1}^{k-1}\left(1+\frac{3}{(1-\delta)|S_j|}\right) \leq \left(\frac{14}{5}\right)^{N-1}\left(\frac{k-1}{N-1}\right)^{3/((1-\varepsilon/6)(3+\varepsilon))}.$$

One can check that

$$\left(1-\frac{\varepsilon}{6}\right)(3+\varepsilon)\left(1-\frac{\varepsilon}{10}\right) = 3+\frac{\varepsilon(1-\varepsilon)(12-\varepsilon)}{60} \geq 3,$$

where the inequality follows since $\varepsilon \in (0,1]$. Thus, we have

$$\prod_{j=1}^{k-1}\left(1+\frac{3}{(1-\delta)|S_j|}\right) \leq \left(\frac{14}{5}\right)^{N-1}\left(\frac{k-1}{N-1}\right)^{1-\varepsilon/10}.$$

Recall that $|S_k| > 3k$ for $k > C \geq N$. By Lemma 2.2.3, for $C < k \leq n$, we deduce

$$\begin{aligned}\mathbb{E}_{k-1}[\alpha_k(x)^2] &\leq \frac{1}{|S_k|^2}\prod_{j=1}^{k-1}\left(1+\frac{3}{(1-\delta)|S_j|}\right)\\ &< \frac{1}{9\,k^2}\left(\frac{14}{5}\right)^{N-1}\left(\frac{k-1}{N-1}\right)^{1-\varepsilon/10}\\ &\leq \frac{3^{N-1}\cdot k^{1-\varepsilon/10}}{9\,k^2}\\ &\leq \frac{3^N}{9\,k^{1+\varepsilon/10}}.\end{aligned}$$

Since $\varepsilon \in (0, 1]$, we obtain

$$\frac{1}{4\delta(1-\delta)} \sum_{k=1}^{n} \mathbb{E}_{k-1}[\alpha_k(x)^2] \leq \frac{9}{\varepsilon(6-\varepsilon)} \sum_{k=C}^{n} \frac{3^N}{9\, k^{1+\varepsilon/10}}$$
$$\leq \frac{3^N}{\varepsilon} \sum_{k=C}^{n} \frac{1}{k^{1+\varepsilon/10}}.$$

The $\sum_{k=1}^{\infty} 1/k^{1+\varepsilon/10}$ is convergent. Therefore, for $C = C(N, \varepsilon)$ sufficiently large, we have

$$\frac{1}{4\delta(1-\delta)} \sum_{k=1}^{n} \mathbb{E}_{k-1}[\alpha_k(x)^2] < 1.$$

Thus, by Lemma 2.2.2, we see that $\mathcal{A}$ does not cover Q, which is a contradiction.

Since N only depends on ε and the sets $S_1, S_2, \ldots$ and since we can take $\varepsilon = 1$, we see that our choice of C can be made to only depend on the sets $S_1, S_2, \ldots$. This finishes the proof. □

Recall that by Corollary 1.2.3 which follows from the above result, we have proven the existence of a bound on the minimum modulus of finite coverings with distinct square-free moduli.

Chapter 3

Square-free Moduli

3.1 Preliminaries

In this chapter, we find an explicit bound for the minimum modulus of finite coverings with distinct square-free moduli. We first redefine weights with δ now depending on k. Let $1 \leq k \leq n$. For each k, pick $\delta_k \in [0, 1/2]$. We define the weights w_k inductively. As before, we use the same definition of $\mathcal{A}_k = \{A \in \mathcal{A} : \max(F(A)) = k\}$ and $B_k = \bigcup_{A \in \mathcal{A}_k} A$. When $k = 1$, if $y \in S_1$ and $|B_1|/|S_1| \leq \delta_1$, we set

$$w_1(y) = \begin{cases} 0 & \text{if } y \in B_1 \\ \dfrac{1}{|S_1| - |B_1|} & \text{if } y \notin B_1. \end{cases}$$

If $y \in S_1$ and $|B_1|/|S_1| > \delta_1$, we set

$$w_1(y) = \begin{cases} \dfrac{(|B_1|/|S_1|) - \delta_1}{(|B_1|/|S_1|)(1 - \delta_1)} \cdot \dfrac{1}{|S_1|} & \text{if } y \in B_1 \\ \dfrac{1}{1 - \delta_1} \cdot \dfrac{1}{|S_1|} & \text{if } y \notin B_1. \end{cases}$$

Observe that in both cases, we have $\sum_{y \in S_1} w_1(y) = 1$ (just as before). The above weights correspond to setting $k = 1$ and replacing $\alpha_1(x)$ with $|B_1|/|S_1|$ and $w_0(x)$ with 1 in the discussion below. Suppose $k \geq 2$ and w_{k-1} is defined on Q_{k-1}. For each $x \in Q_{k-1}$, we define as before

$$\alpha_k(x) = \frac{|\{y \in S_k : (x, y) \in B_k\}|}{|S_k|} = \frac{|F_x \cap B_k|}{|S_k|},$$

which is the proportion of the fiber $F_x = \{(x,y) : y \in S_k\}$ that is covered by one or more hyperplanes in $\mathcal{A}_k$. If $\alpha_k(x) \le \delta_k$, we set

$$w_k(x,y) = \begin{cases} 0 & \text{if } (x,y) \in B_k \\ \dfrac{1}{1-\alpha_k(x)} \cdot \dfrac{w_{k-1}(x)}{|S_k|} & \text{if } (x,y) \notin B_k. \end{cases}$$

If $\alpha_k(x) > \delta_k$, we set

$$w_k(x,y) = \begin{cases} \dfrac{\alpha_k(x) - \delta_k}{\alpha_k(x)(1-\delta_k)} \cdot \dfrac{w_{k-1}(x)}{|S_k|} & \text{if } (x,y) \in B_k \\ \dfrac{1}{1-\delta_k} \cdot \dfrac{w_{k-1}(x)}{|S_k|} & \text{if } (x,y) \notin B_k. \end{cases}$$

As in Section 2.1, we have $\sum_{y \in S_k} w_k(x,y) = w_{k-1}(x)$, so weight is preserved at each stage. In other words, the sum of the weights of all the elements of $S_1 \times S_2 \times \cdots \times S_{k-1}$ is 1.

In the above, if $\alpha_k(x) \le \delta_k$, then we have set $w_k(x,y) = 0$ if $(x,y) \in B_k$ and increased the weight $w_k(x,y)$ proportionally on the rest of F_x. If $\alpha_k(x) > \delta_k$, then we have increased the weight of each element in $F_x \setminus B_k$ by a distortion factor of $1/(1-\delta_k)$ and decreased the weight of $F_x \cap B_k$.

For any element $x \in Q_{k-1}$ and any element $y \in S_k$, we justify that

$$w_k(x,y) \le \frac{1}{1-\delta_k} \cdot \frac{w_{k-1}(x)}{|S_k|}.$$

If $k \ge 2$ and $\alpha_k(x) \le \delta_k$, we have

$$w_k(x,y) \le \frac{1}{1-\alpha_k(x)} \cdot \frac{w_{k-1}(x)}{|S_k|} \le \frac{1}{1-\delta_k} \cdot \frac{w_{k-1}(x)}{|S_k|}.$$

If $k \ge 2$ and $\alpha_k(x) > \delta_k$ and $(x,y) \notin B_k$, our result holds by the definition of $w_k(x,y)$. If $k \ge 2$ and $\alpha_k(x) > \delta_k$ and $(x,y) \in B_k$, then we obtain

$$\begin{aligned} w_k(x,y) &\le \frac{\alpha_k(x) - \delta_k}{\alpha_k(x)(1-\delta_k)} \cdot \frac{w_{k-1}(x)}{|S_k|} \\ &\le \left(\frac{1}{1-\delta_k} - \frac{\delta_k}{\alpha_k(x)(1-\delta_k)} \right) \cdot \frac{w_{k-1}(x)}{|S_k|} \end{aligned}$$

$$\le \frac{1}{1-\delta_k} \cdot \frac{w_{k-1}(x)}{|S_k|}.$$

Also, if $k = 1$, then one can similarly check that for $y \in S_1$, we have

$$w_1(y) \le \frac{1}{|S_1|} \le \frac{1}{1-\delta_1} \cdot \frac{1}{|S_1|}.$$

For a hyperplane $A = Y_1 \times \ldots \times Y_n$ and a set $U \subseteq \{1, \ldots, n\}$, we define $A^U = Y_1^U \times \ldots \times Y_n^U$ to be a hyperplane with $Y_i^U = Y_i$ if $i \in U$ and $Y_i^U = S_i$ if $i \notin U$. We again set $A' = A^{\{1,\ldots,k-1\}}$. For each $J \subseteq \{1, \ldots, n\}$, we redefine $\nu(J) = \prod_{j \in J} 1/((1-\delta_j)|S_j|)$, and we define

$$\|J\| = \prod_{j \in J} |S_j|.$$

Observe that although we have changed the definition of $\nu(J)$ from previous sections, the definition is the same when each δ_j is equal to some common value δ.

As we extend our definition of the weights to include S_k, we still maintain that the sum of the weights of all the elements of $S_1 \times S_2 \times \cdots \times S_k$ is 1. With this in mind, corresponding to Lemma 2.2.2, we can make use of the following.

Lemma 3.1.1. *Let $\mathcal{A}$ be a collection of hyperplanes in $Q = S_1 \times \ldots \times S_n$. If*

$$\sum_{k=1}^{n} w_k(B_k) < 1,$$

then $\mathcal{A}$ does not cover Q.

Also, if A is a hyperplane corresponding to some congruence with square-free modulus m in a covering system, then $\|F(A)\| = m$. We are interested in showing that the modulus of some congruence is bounded above by some number which we denote by C_0. Hence, we will want to assume

$$\|F(A)\| > C_0 \qquad \text{for all } A \in \mathcal{A}, \tag{3.1}$$

with a goal of obtaining a contradiction.

3.2 Upper bounds on $w_k(B_k)$ for bounded k

We begin with the following result which will help us formulate a bound on $w_k(B_k)$ which we will use when k is small.

Lemma 3.2.1. *Let $\mathcal{A}$ be a collection of hyperplanes, pairwise non-parallel. Then, for $k \geq 1$, we have*

$$w_k(B_k) \leq \sum_{A \in \mathcal{A}_k} w_k(A) \leq \sum_{A \in \mathcal{A}_k} \nu(F(A)) = \sum_{A \in \mathcal{A}_k} \prod_{j \in F(A)} \frac{1}{(1-\delta_j)|S_j|}.$$

Proof. Since $B_k = \bigcup_{A \in \mathcal{A}_k} A$, we have $w_k(B_k) \leq \sum_{A \in \mathcal{A}_k} w_k(A)$. We will induct on k to prove $w_k(A) \leq \nu(F(A))$ for $A \in \mathcal{A}_k$. For our base case, consider $k = 1$. Let $F(A) \subseteq \{1\}$. Since $k = 1$ and $A \in \mathcal{A}_k$, we see that $F(A) = \{1\}$. Since $F(A) = \{1\}$, we obtain $A = \{y\}$ for some $y \in S_1$, so

$$w_1(A) = w_1(y) \leq \frac{1}{1-\delta_1} \cdot \frac{1}{|S_1|} = \nu(\{1\}).$$

Thus, if $F(A) \subseteq \{1\}$, we see that $w_1(A) \leq \nu(F(A))$.

For our inductive step, assume our result holds for w_{k-1} with $2 \leq k \leq n$. As before, we have $k \in F(A)$. With $A' = A^{\{1,\ldots,k-1\}}$, we see that

$$w_k(A) \leq \frac{1}{1-\delta_k} \cdot \frac{w_{k-1}(A')}{|S_k|} = \frac{1}{(1-\delta_k)|S_k|} \cdot w_{k-1}(A').$$

Since $A' \subseteq \{1, \ldots, k-1\}$ and $F(A') = F(A) \setminus \{k\}$, then by our inductive hypothesis, we have $w_{k-1}(A') \leq \nu(F(A) \setminus \{k\})$. Thus, for $k \geq 1$, we have

$$\begin{aligned} w_k(A) &\leq \frac{1}{(1-\delta_k)|S_k|} \cdot w_{k-1}(A') \\ &\leq \frac{1}{(1-\delta_k)|S_k|} \cdot \nu(F(A) \setminus \{k\}) \\ &= \nu(F(A)). \end{aligned}$$

Therefore, we conclude

$$w_k(B_k) \leq \sum_{A \in \mathcal{A}_k} w_k(A) \leq \sum_{A \in \mathcal{A}_k} \nu(F(A)) = \sum_{A \in \mathcal{A}_k} \prod_{j \in F(A)} \frac{1}{(1-\delta_j)|S_j|},$$

which completes our proof. $\square$

Corollary 3.2.2. *Let $\mathcal{A}$ be a collection of hyperplanes, pairwise non-parallel, satisfying* (3.1)*. Then*

$$\begin{aligned} w_k(B_k) &\leq \frac{1}{(1-\delta_k)|S_k|} \sum_{\substack{J \subseteq \{1,\ldots,k-1\} \\ \|J\| > C_0/|S_k|}} \nu(J) \\ &= \frac{1}{(1-\delta_k)|S_k|} \sum_{\substack{J \subseteq \{1,\ldots,k-1\} \\ \|J\| > C_0/|S_k|}} \prod_{j \in J} \frac{1}{(1-\delta_j)|S_j|}. \end{aligned}$$

Proof. With $A \in \mathcal{A}_k$ satisfying (3.1), we see that

$$F(A) = J \cup \{k\}$$

for some $J \subseteq \{1, \ldots, k-1\}$. For such A and J, we have

$$\|F(A)\| = \|J\| \cdot |S_k|.$$

In particular, $\|F(A)\| > C_0$ is equivalent to $\|J\| > C_0/|S_k|$. Also, since the hyperplanes in $\mathcal{A}$ are pairwise non-parallel, different $A \in \mathcal{A}_k$ correspond to different $J \subseteq \{1, \ldots, k-1\}$. Since every $A \in \mathcal{A}_k$ satisfies (3.1), we see that the result follows from the inequality

$$w_k(B_k) \leq \sum_{A \in \mathcal{A}_k} \prod_{j \in F(A)} \frac{1}{(1-\delta_j)|S_j|}$$

in Lemma 3.2.1. □

Lemma 3.2.3. *Let $\mathcal{A}$ be a collection of hyperplanes in $Q = S_1 \times \ldots \times S_n$. Let $k \geq 1$. We have*

$$w_k(B_k) \leq \frac{1}{4\delta_k(1-\delta_k)} \mathbb{E}_{k-1}[\alpha_k(x)^2].$$

Proof. First, consider $w_k(B_k)$ with $k \geq 2$. We have

$$\begin{aligned} w_k(B_k) &= \sum_{x \in Q_{k-1}} \sum_{\substack{y \in S_k \\ (x,y) \in B_k}} w_k(x,y) \\ &\leq \sum_{x \in Q_{k-1}} |F_x \cap B_k| \cdot \max\left\{0, \frac{\alpha_k(x) - \delta_k}{\alpha_k(x)(1-\delta_k)}\right\} \cdot \frac{w_{k-1}(x)}{|S_k|}. \end{aligned}$$

Since $\alpha_k(x) = |F_x \cap B_k|/|S_k|$, then we obtain

$$w_k(B_k) \le \frac{1}{1-\delta_k} \sum_{x \in Q_{k-1}} \max\{0, \alpha_k(x) - \delta_k\} \cdot w_{k-1}(x).$$

Observe that $4\delta_k^2 - 4\delta_k\alpha_k(x) + \alpha_k(x)^2 = (2\delta_k - \alpha_k(x))^2 \ge 0$, so $\alpha_x(x)^2/4\delta_k \ge \alpha_k(x) - \delta_k$. Thus,

$$\begin{aligned} w_k(B_k) &\le \frac{1}{1-\delta_k} \sum_{x \in Q_{k-1}} \frac{\alpha_k(x)^2}{4\delta_k} \cdot w_{k-1}(x) \\ &= \frac{1}{4\delta_k(1-\delta_k)} \sum_{x \in Q_{k-1}} \alpha_k(x)^2 \cdot w_{k-1}(x) \\ &= \frac{1}{4\delta_k(1-\delta_k)} \mathbb{E}_{k-1}[\alpha_k(x)^2]. \end{aligned}$$

In the case that $k = 1$, we have

$$w_1(B_1) = \sum_{y \in B_1} w_1(y) \le |B_1| \cdot \max\left\{0, \frac{(|B_1|/|S_1|) - \delta_1}{(|B_1|/|S_1|)(1-\delta_1)}\right\} \cdot \frac{1}{|S_1|}.$$

Following the arguments above, we obtain

$$w_1(B_1) \le \frac{1}{4\delta_1(1-\delta_1)} \left(\frac{|B_1|}{|S_1|}\right)^2 = \frac{1}{4\delta_1(1-\delta_1)} \mathbb{E}_0[\alpha_1(x)^2].$$

The lemma follows. $\square$

We now generalize Lemma 2.2.5.

Lemma 3.2.4. *Fix a constant $C_0 \ge 0$. Let $\mathcal{A}$ be a collection of hyperplanes, pairwise non-parallel, in Q satisfying* (3.1)*. Then, for each integer $k \in [1, n]$, we have*

$$\mathbb{E}_{k-1}[\alpha_k(x)^2] \le \frac{1}{|S_k|^2} \sum_{\substack{F_1, F_2 \subseteq \{1,\ldots,k-1\} \\ \|F_1\| > C_0/|S_k|,\ \|F_2\| > C_0/|S_k|}} \prod_{j \in F_1 \cup F_2} \frac{1}{(1-\delta_j)|S_j|}.$$

Proof. Similar to the proof of Corollary 3.2.2, for A_1 and A_2 in $\mathcal{A}_k$ with $\|F(A_1)\| > C_0$ and $\|F(A_2)\| > C_0$, we write

$$F(A_1) = F_1 \cup \{k\} \qquad \text{and} \qquad F(A_2) = F_2 \cup \{k\}$$

for some F_1 and F_2 in $\{1,\dots,k-1\}$. Then

$$\|F(A_1)\| = \|F_1\| \cdot |S_k| \qquad \text{and} \qquad \|F(A_2)\| = \|F_2\| \cdot |S_k|.$$

Note that $\|F(A_i)\| > C_0$ is equivalent to $\|F_i\| > C_0/|S_k|$ for $i \in \{1,2\}$. The proof of Lemma 2.2.5 carries through here word for word, but now we have the added condition $\|F_i\| > C_0/|S_k|$ for $i \in \{1,2\}$. Hence,

$$\begin{aligned}\mathbb{E}_{k-1}[\alpha_k(x)^2] &\le \frac{1}{|S_k|^2} \sum_{\substack{F_1,F_2\subseteq\{1,\dots,k-1\}\\ \|F_1\|>C_0/|S_k|,\ \|F_2\|>C_0/|S_k|}} \nu(F_1\cup F_2)\\ &= \frac{1}{|S_k|^2} \sum_{\substack{F_1,F_2\subseteq\{1,\dots,k-1\}\\ \|F_1\|>C_0/|S_k|,\ \|F_2\|>C_0/|S_k|}} \prod_{j\in F_1\cup F_2} \frac{1}{(1-\delta_j)|S_j|}.\end{aligned}$$

This finishes the proof. □

As a consequence of Lemma 3.2.3 and Lemma 3.2.4, we immediately obtain the following.

Corollary 3.2.5. *Fix a constant $C_0 \ge 0$. Let $\mathcal{A}$ be a collection of hyperplanes, pairwise non-parallel, in $Q = S_1 \times \ldots \times S_n$ satisfying* (3.1)*. Then, for each integer $k \in \{1,2,\dots,n\}$, we have*

$$w_k(B_k) \le \frac{1}{4\delta_k(1-\delta_k)|S_k|^2} \sum_{\substack{F_1,F_2\subseteq\{1,\dots,k-1\}\\ \|F_1\|>C_0/|S_k|,\ \|F_2\|>C_0/|S_k|}} \prod_{j\in F_1\cup F_2} \frac{1}{(1-\delta_j)|S_j|}.$$

We also indicate a different way to express the same bound on $w_k(B_k)$ which leads however to easier computations. For this, for r a positive integer, we denote the r^{th} prime by p_r.

Corollary 3.2.6. *Fix a constant $C_0 \ge 0$. Let $\mathcal{A}$ be a collection of hyperplanes, pairwise non-parallel, in $Q = S_1 \times \cdots \times S_n$ such that for every hyperplane $A \in \mathcal{A}$ we have $\|F(A)\| > C_0$. Fix $k \in \{1,2,\dots,n\}$. Let r be minimal such that $|S_t| > C_0/|S_k|$ for all $t \ge r$. Define*

$$U = \sum_{\substack{F_1\subseteq\{1,\dots,r-1\}\\ \|F_1\|\le C_0/|S_k|}} \sum_{\substack{F_2\subseteq\{1,\dots,r-1\}\\ \|F_2\|\le C_0/|S_k|}} \prod_{j\in F_1\cup F_2} \frac{1}{(1-\delta_j)|S_j|}$$

and

$$V = \sum_{\substack{F_1\subseteq\{1,\ldots,r-1\}\\ \|F_1\|\le C_0/|S_k|}} \sum_{\substack{F_2\subseteq\{1,\ldots,r-1\}\\ \|F_2\|> C_0/|S_k|}} \prod_{j\in F_1\cup F_2} \frac{1}{(1-\delta_j)|S_j|}.$$

Then

$$\begin{aligned} w_k(B_k) \le \frac{1}{4\delta_k(1-\delta_k)|S_k|^2}\Bigg(\prod_{j=1}^{k-1}\left(1+\frac{3}{(1-\delta_j)|S_j|}\right) \\ - 2\,(U+V)\prod_{j=r}^{k-1}\left(1+\frac{1}{(1-\delta_j)|S_j|}\right)+U\Bigg). \end{aligned}$$

Proof. From Corollary 3.2.5, we obtain

$$\begin{aligned} (4\delta_k(1-\delta_k)|S_k|^2)w_k(B_k) &\le \sum_{\substack{F_1,F_2\subseteq\{1,\ldots,k-1\}\\ \|F_1\|>C_0/|S_k|,\ \|F_2\|>C_0/|S_k|}} \prod_{j\in F_1\cup F_2}\frac{1}{(1-\delta_j)|S_j|} \\ &\le \sum_{J\subseteq\{1,\ldots,k-1\}} \sum_{\substack{F_1,F_2\subseteq\{1,\ldots,k-1\}\\ F_1\cup F_2=J}} \prod_{j\in J}\frac{1}{(1-\delta_j)|S_j|} \\ &\quad - \sum_{\substack{F_1\subseteq\{1,\ldots,k-1\}\\ \|F_1\|\le C_0/|S_k|}} \sum_{F_2\subseteq\{1,\ldots,k-1\}} \prod_{j\in F_1\cup F_2}\frac{1}{(1-\delta_j)|S_j|} \\ &\quad - \sum_{\substack{F_2\subseteq\{1,\ldots,k-1\}\\ \|F_2\|\le C_0/|S_k|}} \sum_{F_1\subseteq\{1,\ldots,k-1\}} \prod_{j\in F_1\cup F_2}\frac{1}{(1-\delta_j)|S_j|} \\ &\quad + \sum_{\substack{F_1\subseteq\{1,\ldots,k-1\}\\ \|F_1\|\le C_0/|S_k|}} \sum_{\substack{F_2\subseteq\{1,\ldots,k-1\}\\ \|F_2\|\le C_0/|S_k|}} \prod_{j\in F_1\cup F_2}\frac{1}{(1-\delta_j)|S_j|}. \end{aligned}$$

For $i\in\{1,2\}$, if $\|F_i\|\le C_0/|S_k|$, then $F_i\subseteq\{1,2,\ldots,r-1\}$, which we obtain from the definition of r. Hence, we deduce

$$\begin{aligned} (4\delta_k(1-\delta_k)|S_k|^2)w_k(B_k) &\le \sum_{J\subseteq\{1,\ldots,k-1\}} \sum_{\substack{F_1,F_2\subseteq\{1,\ldots,k-1\}\\ F_1\cup F_2=J}} \prod_{j\in J}\frac{1}{(1-\delta_j)|S_j|} \\ &\quad - \sum_{\substack{F_1\subseteq\{1,\ldots,r-1\}\\ \|F_1\|\le C_0/|S_k|}} \sum_{F_2\subseteq\{1,\ldots,k-1\}} \prod_{j\in F_1\cup F_2}\frac{1}{(1-\delta_j)|S_j|} \\ &\quad - \sum_{\substack{F_2\subseteq\{1,\ldots,r-1\}\\ \|F_2\|\le C_0/|S_k|}} \sum_{F_1\subseteq\{1,\ldots,k-1\}} \prod_{j\in F_1\cup F_2}\frac{1}{(1-\delta_j)|S_j|} \end{aligned}$$

$$+\sum_{\substack{F_1\subseteq\{1,\ldots,r-1\}\\ \|F_1\|\le C_0/|S_k|}}\sum_{\substack{F_2\subseteq\{1,\ldots,r-1\}\\ \|F_2\|\le C_0/|S_k|}}\prod_{j\in F_1\cup F_2}\frac{1}{(1-\delta_j)|S_j|}.$$

The last double sum of a product above is equal to U. Considering the second double sum of a product on the right-hand side of the above inequality, we can express F_2 as $A\cup B$ where $A\subseteq\{1,\ldots,r-1\}$ and $B\subseteq\{r,\ldots,k-1\}$, so we obtain

$$\sum_{\substack{F_1\subseteq\{1,\ldots,r-1\}\\ \|F_1\|\le C_0/|S_k|}}\sum_{F_2\subseteq\{1,\ldots,k-1\}}\prod_{j\in F_1\cup F_2}\frac{1}{(1-\delta_j)|S_j|}$$

$$=\sum_{\substack{F_1\subseteq\{1,\ldots,r-1\}\\ \|F_1\|\le C_0/|S_k|}}\sum_{A\subseteq\{1,\ldots,r-1\}}\sum_{B\subseteq\{r,\ldots,k-1\}}\prod_{j\in F_1\cup(A\cup B)}\frac{1}{(1-\delta_j)|S_j|}$$

$$=\sum_{\substack{F_1\subseteq\{1,\ldots,r-1\}\\ \|F_1\|\le C_0/|S_k|}}\sum_{A\subseteq\{1,\ldots,r-1\}}\sum_{B\subseteq\{r,\ldots,k-1\}}\prod_{j\in F_1\cup A}\frac{1}{(1-\delta_j)|S_j|}\prod_{j\in B}\frac{1}{(1-\delta_j)|S_j|}$$

$$=\sum_{\substack{F_1\subseteq\{1,\ldots,r-1\}\\ \|F_1\|\le C_0/|S_k|}}\sum_{A\subseteq\{1,\ldots,r-1\}}\prod_{j\in F_1\cup A}\frac{1}{(1-\delta_j)|S_j|}\sum_{B\subseteq\{r,\ldots,k-1\}}\prod_{j\in B}\frac{1}{(1-\delta_j)|S_j|},$$

where the second to last equality holds since $(F_1\cup A)\cap B=\emptyset$. Observe that

$$\sum_{B\subseteq\{r,\ldots,k-1\}}\prod_{j\in B}\frac{1}{(1-\delta_j)|S_j|}=\prod_{j=r}^{k-1}\left(1+\frac{1}{(1-\delta_j)|S_j|}\right).$$

We also have

$$\sum_{\substack{F_1\subseteq\{1,\ldots,r-1\}\\ \|F_1\|\le C_0/|S_k|}}\sum_{A\subseteq\{1,\ldots,r-1\}}\prod_{j\in F_1\cup A}\frac{1}{(1-\delta_j)|S_j|}$$

$$=\sum_{\substack{F_1\subseteq\{1,\ldots,r-1\}\\ \|F_1\|\le C_0/|S_k|}}\sum_{\substack{A\subseteq\{1,\ldots,r-1\}\\ \|A\|>C_0/|S_k|}}\prod_{j\in F_1\cup A}\frac{1}{(1-\delta_j)|S_j|}$$

$$+\sum_{\substack{F_1\subseteq\{1,\ldots,r-1\}\\ \|F_1\|\le C_0/|S_k|}}\sum_{\substack{A\subseteq\{1,\ldots,r-1\}\\ \|A\|\le C_0/|S_k|}}\prod_{j\in F_1\cup A}\frac{1}{(1-\delta_j)|S_j|}$$

$$=U+V.$$

Thus, we deduce

$$\sum_{\substack{F_1\subseteq\{1,\ldots,r-1\}\\ \|F_1\|\le C_0/|S_k|}}\sum_{F_2\subseteq\{1,\ldots,k-1\}}\prod_{j\in F_1\cup F_2}\frac{1}{(1-\delta_j)|S_j|}=(U+V)\prod_{j=r}^{k-1}\left(1+\frac{1}{(1-\delta_j)|S_j|}\right).$$

Similarly, we also obtain

$$\sum_{\substack{F_2\subseteq\{1,\ldots,r-1\}\\ \|F_2\|\le C_0/|S_k|}}\ \sum_{F_1\subseteq\{1,\ldots,k-1\}}\ \prod_{j\in F_1\cup F_2}\frac{1}{(1-\delta_j)|S_j|}=(U+V)\prod_{j=r}^{k-1}\left(1+\frac{1}{(1-\delta_j)|S_j|}\right).$$

As demonstrated in the proof of Lemma 2.2.3, we have

$$\sum_{J\subseteq\{1,\ldots,k-1\}}\ \sum_{\substack{F_1,F_2\subseteq\{1,\ldots,k-1\}\\ F_1\cup F_2=J}}\ \prod_{j\in J}\frac{1}{(1-\delta_j)|S_j|}=\prod_{j=1}^{k-1}\left(1+\frac{3}{(1-\delta_j)|S_j|}\right).$$

Therefore, we conclude that

$$\begin{aligned} w_k(B_k)\le \frac{1}{4\delta_k(1-\delta_k)|S_k|^2}&\left(\prod_{j=1}^{k-1}\left(1+\frac{3}{(1-\delta_j)|S_j|}\right)\right.\\ &\left.-2\,(U+V)\prod_{j=r}^{k-1}\left(1+\frac{1}{(1-\delta_j)|S_j|}\right)+U\right),\end{aligned}$$

which completes the proof. □

3.3 Upper bounds on $w_k(B_k)$ for large k

The idea is to apply the prior upper bounds for $w_k(B_k)$ to estimate the value of $w_k(B_k)$ for $k\le N$, where we will take $N=10^6$. In this section, we show how to find an upper bound for $w_k(B_k)$ for $k>N$ and then find an upper bound for

$$\sum_{k>N} w_k(B_k).$$

We require below $N\ge 61$ and $k>N$. Note that we view N as fixed, so we will allow constants below to depend on N. We set $\delta_j=1/2$ for all $j>N$. As we will be using Corollary 3.2.6 to compute $w_k(B_k)$ for $k=N$, we will have already calculated the value of

$$M_0=\prod_{j=1}^{N}\left(1+\frac{3}{(1-\delta_j)|S_j|}\right),$$

and also make use of it. Finally, we denote the j^{th} prime by p_j and the number of primes $\le x$ by $\pi(x)$.

Lemma 3.3.1. *With the above notation, we set*

$$c_1 = -\log\log p_N + \frac{1}{\log^2 p_N} \qquad \textit{and} \qquad c_2 = 1 + \frac{3}{2\log p_N}.$$

If $|S_j| = p_j$ for every $j > N$, then

$$\sum_{k>N} w_k(B_k) \le \frac{2c_2M_0e^{6c_1}}{p_N} \cdot \Big(\log^5 p_N + 5\log^4 p_N + 20\log^3 p_N$$

$$+ 60\log^2 p_N + 120\log p_N + 120\Big).$$

Proof. From $\delta_k = 1/2$ and Corollary 3.2.6, we see that

$$w_k(B_k) \le \frac{1}{4\delta_k(1-\delta_k)|S_k|^2} \prod_{j=1}^{k-1}\left(1 + \frac{3}{(1-\delta_j)|S_j|}\right) = \frac{1}{|S_k|^2}\prod_{j=1}^{k-1}\left(1+\frac{3}{(1-\delta_j)|S_j|}\right). \tag{3.2}$$

Since $k > N$ and $\delta_j = 1/2$ for all $j > N$, we obtain

$$\prod_{j=1}^{k-1}\left(1+\frac{3}{(1-\delta_j)|S_j|}\right) = M_0 \prod_{j=N+1}^{k-1}\left(1+\frac{6}{|S_j|}\right) \le M_0 \exp\left(6\sum_{j=N+1}^{k-1}\frac{1}{|S_j|}\right). \tag{3.3}$$

where we have used that $1 + x \le e^x$ for all real numbers x (the function e^x is convex up and $y = 1 + x$ is a tangent line to its graph at $x = 0$).

We are now ready to make use of the specification that $|S_j| = p_j$ for every $j > N$. From the work of J. B. Rosser and L. Schoenfeld [10, Theorem 5], we have the estimates

$$\log\log x + B - \frac{1}{2\log^2 x} \le \sum_{p \le x}\frac{1}{p} < \log\log x + B + \frac{1}{2\log^2 x}, \qquad \text{for } x \ge 286,$$

for some constant $B \approx 0.2614972128$. As $N+1 \ge 62$ and $p_{62} = 293 > 286$, we deduce that

$$\sum_{j=N+1}^{k-1}\frac{1}{|S_j|} = \sum_{j=N+1}^{k-1}\frac{1}{p_j} = \sum_{p\le p_{k-1}}\frac{1}{p} - \sum_{p\le p_N}\frac{1}{p}$$

$$< \left(\log\log p_{k-1} + B + \frac{1}{2\log^2 p_{k-1}}\right) - \left(\log\log p_N + B - \frac{1}{2\log^2 p_N}\right)$$

$$= \log\log p_{k-1} - \log\log p_N + \frac{1}{2\log^2 p_{k-1}} + \frac{1}{2\log^2 p_N}$$

$$\leq \log\log p_{k-1} - \log\log p_N + \frac{1}{2\log^2 p_N} + \frac{1}{2\log^2 p_N} = \log\log p_{k-1} + c_1.$$

From (3.3), we now see that

$$\prod_{j=1}^{k-1}\left(1 + \frac{3}{(1-\delta_j)|S_j|}\right) \leq M_0 \exp\Big(6\log\log p_{k-1} + 6c_1\Big) = M_0 e^{6c_1} \log^6 p_{k-1}.$$

From (3.2), we obtain the estimate for $w_k(B_k)$ for $k > N$ that we want, namely

$$w_k(B_k) \leq M_0 e^{6c_1} \frac{\log^6 p_k}{p_k^2}.$$

Next, we want an estimate of the sum over $k > N$ of this bound for $w_k(B_k)$. We make use of a Riemann-Stieltjes integral to obtain

$$\sum_{k=N+1}^{\infty} \frac{\log^6 p_k}{p_k^2} \leq \int_{p_N}^{\infty} \frac{\log^6 t}{t^2}\, d\,\pi(t)$$

$$= \frac{\pi(t)\log^6 t}{t^2}\bigg|_{p_N}^{\infty} - \int_{p_N}^{\infty} \pi(t)\, d\bigg(\frac{\log^6 t}{t^2}\bigg)$$

$$\leq 2\int_{p_N}^{\infty} \frac{\pi(t)\log^6 t}{t^3}\, dt,$$

where we have used that

$$d\bigg(\frac{\log^6 t}{t^2}\bigg) = \bigg(\frac{6\log^5 t}{t^3} - \frac{2\log^6 t}{t^3}\bigg)\, dt$$

and ignored negative quantities. From J. B. Rosser and L. Schoenfeld [10, Theorem 1], we have

$$\pi(x) < \frac{x}{\log x}\bigg(1 + \frac{3}{2\log x}\bigg) \qquad \text{for all } x > 1.$$

Thus, for $t \geq p_N$, we obtain $\pi(t) \leq c_2\, t/\log t$. Thus,

$$\sum_{k=N+1}^{\infty} \frac{\log^6 p_k}{p_k^2} \leq 2c_2 \int_{p_N}^{\infty} \frac{\log^5 t}{t^2}\, dt.$$

The latter integral can be computed exactly to obtain

$$\sum_{k=N+1}^{\infty} \frac{\log^6 p_k}{p_k^2} \leq \frac{2c_2}{p_N}\bigg(\log^5 p_N + 5\log^4 p_N + 20\log^3 p_N$$

$$+ 60\log^2 p_N + 120\log p_N + 120\bigg).$$

Combining the above, the lemma follows. □

3.4 Proof of Theorem 1.2.4

We will now prove Theorem 1.2.4, which states that every covering system with distinct square-free moduli has a minimum modulus which is ≤ 118.

Proof. Let $\mathcal{A}$ be a collection of hyperplanes covering $Q = S_1 \times \ldots \times S_n$ corresponding to a covering system with distinct square-free moduli (see the proof of Corollary 1.2.3). Recall that $p_k = |S_k|$ and if A is a hyperplane corresponding to some congruence with square-free modulus m in a covering system, then $\|F(A)\| = m$. For the sake of contradiction, assume that $\|F(A)\| > C_0 = 118$ for all $A \in \mathcal{A}$. For our computations, we use Maple 2019.

We choose δ_j as below:

$$\delta_1 = \cdots = \delta_7 = 0, \quad \delta_8 = 0.171, \quad \delta_9 = 0.190, \quad \delta_{10} = 0.199,$$

$$\delta_{11} = 0.210, \quad \delta_{12} = 0.210, \quad \delta_{13} = 0.224, \quad \delta_{14} = 0.233,$$

$$\delta_{15} = 0.237, \quad \delta_{16} = 0.237, \quad \delta_{17} = 0.237, \quad \delta_{18} = 0.252,$$

$$\delta_{19} = 0.252, \quad \delta_{20} = 0.255, \quad \delta_{21} = 0.260, \quad \delta_{22} = 0.261,$$

$$\delta_{23} = 0.263, \quad \delta_{24} = 0.264, \quad \delta_{25} = 0.262, \quad \delta_{26} = 0.265, \quad \delta_{27} = 0.269,$$

$$\delta_j = 0.279 \ \ (\text{for } 28 \le j \le 35), \qquad \delta_j = 0.289 \ \ (\text{for } 36 \le j \le 45),$$

$$\delta_j = 0.297 \ \ (\text{for } 46 \le j \le 60), \qquad \delta_j = 0.307 \ \ (\text{for } 61 \le j \le 99),$$

$$\delta_j = 0.331 \ \ (\text{for } 100 \le j \le 1000), \qquad \delta_j = 0.372 \ \ (\text{for } 1001 \le j \le 10000),$$

$$\delta_j = 0.418 \ \ (\text{for } 10001 \le j \le 1000000), \qquad \delta_j = 0.5 \ \ (\text{for } j \ge 1000001).$$

Using Corollary 3.2.2, we compute that $w_1(B_1) = w_2(B_2) = w_3(B_3) = 0$, $w_4(B_4) = 1/210$, $w_5(B_5) = 3/110$, $w_6(B_6) = 50/1001$, and $w_7(B_7) = 43/715$, so we have

$$\sum_{k=1}^{7} w_k(B_k) = \frac{194}{1365} = 0.142124542124542124542124542124\ldots. \tag{3.4}$$

Using Corollary 3.2.6, we calculate

$$\sum_{k=8}^{10^6} w_k(B_k) = 0.856857558639508798126627002701\ldots. \tag{3.5}$$

Using Lemma 3.3.1, we compute

$$\sum_{k>10^6} w_k(B_k) \leq 0.000402960685094785665517210549223O\ldots. \tag{3.6}$$

Combining (3.4), (3.5), and (3.6), we obtain

$$\sum_{k=1}^{\infty} w_k(B_k) \leq 0.999385061449145708334268755375\ldots < 1. \tag{3.7}$$

Thus, by Lemma 3.1.1, $\mathcal{A}$ does not cover Q, which is a contradiction. Therefore, every covering system with distinct square-free moduli has a minimum modulus which is ≤ 118. $\square$

Bibliography

[1] P. Ballister, B. Bollobás, R. Morris, J. Sahasrabudhe, and M. Tiba. "Erdős covering systems". In: *Acta Mathematica Hungarica* 161.2 (2020), pp. 540–549.

[2] P. Ballister, B. Bollobás, R. Morris, J. Sahasrabudhe, and M. Tiba. "On the Erdős covering problem: the density of the uncovered set". In: *Invent. math.* 228 (2022), pp. 377–414.

[3] P. Erdős. "On integers of the form $2^k + p$ and some related problems". In: *Summa Brasil. math.* 2 (1950), pp. 113–123.

[4] M. Filaseta and J. Juillerat. "Consecutive primes which are widely digitally delicate". In: *INTEGERS: Ron Graham Memorial Volume* 21A.A12 (2021), pp. 1–37, see also *Number Theory and Combinatorics: A Collection in Honor of the Mathematics of Ronald Graham*, De Gruyter, (2022), pp. 209–248.

[5] M. Filaseta and J. Southwick. "Primes that become composite after changing as arbitrary digit". In: *Math. of Comp.* 90.328 (2021), pp. 979–993.

[6] R. Graham. "A Fibonacci-like sequence of composite numbers". In: *Math. Mag.* 37 (1964), pp. 322–324.

[7] R. Hough. "Solution of the minimum modulus problem for covering systems". In: *Ann. Math.* 181 (2015), pp. 361–382.

[8] L. Jones. "When does appending the same digit repeatedly on the right of a positive integer generate a sequence of composite integers?" In: *Amer. Math. Monthly* 118.2 (2011), pp. 153–160.

[9] H. Riesel. "Några stora primtal". In: *Elementa* 39 (1956), pp. 258–260.

[10] J. B. Rosser and L. Schoenfeld. “Approximate formulas for some functions of prime numbers”. In: *Illinois J. Math.* 6 (1962), pp. 64–94.

[11] A. Schinzel. “Reducibility of polynomials and covering systems of congruences”. In: *Acta Arith.* 13 (1967), pp. 91–101.

[12] W. Sierpiński. “Sur un problème concernant les nombres $k \cdot 2n + 1$”. In: *Elem. Math.* 15 (1960), pp. 73–74.