SIEVES AND ITERATION RULES

A DISSERTATION
SUBMITTED TO THE DEPARTMENT OF MATHEMATICS
AND THE COMMITTEE ON GRADUATE STUDIES
OF STANFORD UNIVERSITY
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE DEGREE OF
DOCTOR OF PHILOSOPHY

Zarathustra Elessar Brady
June 2017

I certify that I have read this dissertation and that, in my opinion, it is fully adequate in scope and quality as a dissertation for the degree of Doctor of Philosophy.

(Kannan Soundararajan) Principal Adviser

I certify that I have read this dissertation and that, in my opinion, it is fully adequate in scope and quality as a dissertation for the degree of Doctor of Philosophy.

(Jacob Fox)

I certify that I have read this dissertation and that, in my opinion, it is fully adequate in scope and quality as a dissertation for the degree of Doctor of Philosophy.

(Akshay Venkatesh)

I certify that I have read this dissertation and that, in my opinion, it is fully adequate in scope and quality as a dissertation for the degree of Doctor of Philosophy.

(Jan Vondrak)

Approved for the University Committee on Graduate Studies

Acknowledgments

I would like to thank my advisor, Kannan Soundararajan, especially for his advice on reading material (I doubt I would have discovered Selberg's Lectures on Sieves [28] on my own), for suggesting interesting research problems to work on, for answering many questions I had on topics that I didn't expect him to have familiarity with, and for lending me several of his personal copies of books and preprints. I would also like to acknowledge the contributions of Jan Vondrak, who gave me some advice about some of the computational questions raised in this thesis, Arnav Tripathy, who helped me work out some of the combinatorial identities and inequalities that show up in the first Appendix, and Akshay Venkatesh, who exposed me to the stick-breaking process.

I'd also like to thank my parents, for exposing me to interesting books, ideas, and people when I was young, and for giving me room to explore my own interests without pushing me to succeed.

Contents

Chapter 1

Introduction

One of the basic problems of sieve theory - and the problem that this thesis will be focused on - may be phrased as follows. Let A be a set of integers, typically an interval, let $\mathcal{P} = \{p_1, ..., p_k\}$ be a collection of primes, and let P be the product of the primes in $\mathcal{P}$. Choose a congruence class c_i modulo each prime p_i, and define the sifted set $\mathcal{S}(A, \mathcal{P}, (c_i)_{i=1,...,k})$ to be the collection integers in the set A which are not congruent to any c_i modulo the corresponding prime p_i, that is,

$$\mathcal{S}(A, \mathcal{P}, (c_i)_{i=1,...,k}) = \{a \in A \mid \forall i \leq k, \quad a \not\equiv c_i \pmod{p_i}\}.$$

Sometimes we write $\mathcal{S}(A, \mathcal{P})$ for the above when the c_i are all 0, or when their values are irrelevant to the argument.

Problem 1. Given $A \subset \mathbb{N}$ and $\mathcal{P} = \{p_1, ..., p_k\}$ a set of primes, what are the best possible upper and lower bounds on $|\mathcal{S}(A, \mathcal{P}, (c_i)_{i=1,...,k})|$ if the congruence classes $c_i \pmod{p_i}$ are unknown?

If $\mathcal{P} = \mathcal{P}_z$ is the collection of all the primes below z, every c_i is chosen to be 0 modulo p_i, and A is taken to be an interval with endpoints between between z and z^2, then this gives upper and lower bounds on the number of primes in A.

More generally, we may consider choosing several congruence classes modulo each prime, say κ_p congruence classes modulo p - in this case, the average number of congruence classes to be chosen is referred to as the *sifting dimension*, and we will call this average value κ. When the sifting dimension κ is 2 and the congruence classes chosen modulo each prime p_i are 0 and 2, we see that sufficiently strong bounds for this problem might imply the twin prime conjecture.

Problem 2. Given $A \subset \mathbb{N}$, and $\mathcal{P} = \{\kappa_{p_1} \cdot p_1, ..., \kappa_{p_k} \cdot p_k\}$ a weighted set of primes with weights κ_{p_i}, what are the best possible upper and lower bounds on $|\mathcal{S}(A, \mathcal{P}, (c_{i,j})_{i \leq k, j \leq \kappa_{p_i}})|$ if the congruence classes $c_{i,j} \pmod{p_i}$ are unknown?

For simplicity, we will often focus on the case $\kappa = 1$, where we choose one congruence class modulo each prime. In this case, by the Chinese Remainder Theorem we may replace the choice of the congruence classes c_i by an overall shift c modulo P, so that we want to find upper and lower bounds on the size of the set $\mathcal{S}(A-c, \mathcal{P})$ of integers in $A-c$ which are relatively prime to P.

In the rest of this section, I'll describe several approaches towards solving this problem.

The linear approach

The most direct approach is to define a set A_d for every number d dividing P which consists of the integers n in A such that d divides $n-c$, and to define a variable a_d and to be the number of integers n in A such that $\gcd(n-c, P) = d$. Then (in the case that A is an interval) we see what upper and lower bounds on $a_1 = \mathcal{S}(A-c, \mathcal{P})$ can be deduced from the collection of linear inequalities

$$\frac{|A|}{d} - 1 \leq |A_d| \leq \frac{|A|}{d} + 1, \quad |A_d| = \sum_{d|k} a_k, \quad a_k \geq 0.$$

By summing these inequalities after multiplying them by certain carefully chosen sieve weights λ_d, we can produce upper and lower bounds on $|\mathcal{S}(A-c, \mathcal{P})|$. This approach may be viewed as a linear relaxation of the original problem.

More generally, for any fixed value of κ, if we take $|A| = z^s$, with s a constant greater than 1 and z going to infinity, we can ask for the asymptotically optimal bounds coming from the system of linear inequalities

$$\left| |A_d| - \kappa(d)\tfrac{|A|}{d} \right| \leq \kappa(d), \tag{1.1}$$

where $\kappa(d) = \prod_{p|d} \kappa_p$. Define sifting functions $f_\kappa(s), F_\kappa(s)$ by

$$(1+o(1))f_\kappa(s)|A| \prod_{p<z} \left(1 - \frac{\kappa_p}{p}\right) \leq \mathcal{S}(A, \mathcal{P}_z) \leq (1+o(1))F_\kappa(s)|A| \prod_{p<z} \left(1 - \frac{\kappa_p}{p}\right),$$

with $f_\kappa(s)$ as large as possible (resp. $F_\kappa(s)$ as small as possible) given that the above inequality holds for all choices of weighted sets A satisfying (1.1). Selberg, in his Lectures on Sieves [28], has shown the following.

Theorem 1 (Selberg [28])**.** *The optimal sifting functions $f_\kappa(s), F_\kappa(s)$ continuous, monotone, and* computable *for $s > 1$, and they tend to 1 exponentially as s goes to infinity.*

What's more, Selberg has outlined an algorithm to compute $f_\kappa(s), F_\kappa(s)$ to any desired accuracy in [28]. Despite this, as far as I am aware no one has ever implemented this algorithm, and even the value of $F_\kappa(2)$ is unknown for any κ other than $\kappa = \frac{1}{2}, 1$ (although there are of course upper bounds). I've described this algorithm in Chapter 6.

There are two simple but effective methods for producing bounds on the sifting functions f_κ, F_κ. The first method, known as Buchstab iteration, is based on the identity

$$\mathcal{S}(A, \mathcal{P}_z) = \mathcal{S}(A, \mathcal{P}_w) - \sum_{w \le p < z} \mathcal{S}(A_p, \mathcal{P}_p)$$

which holds for any $w < z$. Thus, given an upper bound for $|\mathcal{S}(A, \mathcal{P}_w)|$ and lower bounds for $|\mathcal{S}(A_p, \mathcal{P}_p)|$, we can find an upper bound for $\mathcal{S}(A, \mathcal{P}_z)$. Iterating this strategy, one obtains the β-sieve. The second basic method, the Selberg upper bound sieve, restricts attention to choices of sieve weights λ_d such that there exist weights ℓ_d with

$$\sum_{d|k} \lambda_d = (\sum_{d|k} \ell_d)^2,$$

in order to make it easy to check that $\sum_{d|k} \lambda_d \ge 0$. Although the resulting upper bound on $F_\kappa(s)$ is not always optimal (it is known that the β-sieve outperforms the Selberg sieve when s is very large, and the β-sieve weights are not of this form), it is easy to compute the Selberg sieve bound, and this bound appears to be nearly optimal when s is small and κ is large. When $s = 2$, Selberg's upper bound sieve gives the bound $F_\kappa(2) \le e^{\gamma\kappa}\Gamma(\kappa + 1)$, where γ is the Euler-Mascheroni constant.

A good measure of the success of a sieve is whether it can prove nontrivial lower bounds for the size of the set $|\mathcal{S}(A, \mathcal{P}_z)|$. The *sifting limit* β_κ is defined by

$$\beta_\kappa = \inf\{s \mid f_\kappa(s) > 0\},$$

and our goal is generally to show that the sifting limit is as small as possible. It is known that $\beta_{\frac{1}{2}} = 1, \beta_1 = 2$, and that $\beta_\kappa < 2\kappa$ for $\frac{1}{2} < \kappa < 1$, and it seems to be the case that the value of β_κ is given by the β-sieve in this range. When κ is very large, the best known bound for β_κ is given by variants of Selberg's lower bound sieve, the basic form of which is given by choosing λ_d such that there exist weights ℓ_d with

$$\sum_{d|k} \lambda_d = \big(1 - \sum_{p|k} 1\big)\big(\sum_{d|k} \ell_d\big)^2,$$

and Selberg [28] gets the following bound.

Theorem 2 (Selberg [28])**.** *$\beta_\kappa < 2\kappa + 0.4454$ for κ sufficiently large.*

It is currently not known whether there is any $\kappa > 1$ with $\beta_\kappa < 2\kappa$. Based on an analysis of a simplified version of the sifting problem, described later, I've found an approach which seems likely to prove a bound of the following form.

Conjecture 1. There is some $\epsilon > 0$ such that $\beta_\kappa \le 2\kappa - \epsilon\sqrt[3]{\kappa}$ for all κ sufficiently large.

Selberg [28] has also suggested a refinement of the linear relaxation approach, in which we replace

the interval A with a weighted interval, such that the weights are a smooth approximation to the indicator function of A. The idea is to take advantage of the fact that the Fourier transform of a smooth function decays more quickly than the Fourier transform of a step function, ultimately leading to better error terms in the analysis. We'll explore this refinement in Section 3.2.2.

The Fourier transform approach

A second approach to the basic sifting problem, known as the large sieve (see Montgomery [25]), involves studying the Fourier transform of the set $\mathcal{S}(A-c,\mathcal{P})$, considered as a subset of $\mathbb{Z}/P\mathbb{Z}$. One shows that if this set is too large then the Fourier transform has many large values at a collection of points $\alpha_1,...,\alpha_N \in \mathbb{R}/\mathbb{Z}$, which are well spaced in the sense that the distance between any two of them is at least δ for some $\delta > 0$. One then shows that this contradicts an upper bound on the operator norm of a matrix associated to the Fourier transform at these points. The relevant matrix has the form $NI + S$, where I is the identity matrix and S is a symmetric matrix whose i,j entry is

$$S_{i,j} = \frac{\sin \pi N(\alpha_i - \alpha_j)}{\sin \pi(\alpha_i - \alpha_j)}$$

when $i \neq j$, and with $S_{i,i} = 0$. One version of the main result is the operator norm bound

$$\|S\| \leq \frac{1}{\delta}.$$

Note that this bound is equivalent to the positive semidefiniteness of the matrices $\frac{1}{\delta}I - S$, $\frac{1}{\delta}I + S$.

Kobayashi [20] and Motohashi [26] have shown that one can combine the approaches of the Selberg sieve and the large sieve, using the Selberg sieve to get a main term and the large sieve to get a good bound on the error term.

1.1 Jacobsthal function

Definition 1. The Jacobsthal function $j(m)$ is defined to be the minimum n such that among any n consecutive integers, at least one of them is relatively prime to m.

We are mostly interested in $j(P_z)$, where P_z is the product of the primes below z. The best known asymptotic bounds on $j(P_z)$ are summarized below.

Theorem 3 ([14], [7])**.** *We have*

$$\frac{z\log(z)\log(\log(\log(z)))}{\log(\log(z))} \ll j(P_z) \ll z^2.$$

Now we'll go over some numerical computations. To simplify notation, we'll follow Hagedorn [9]

and define a function $h(n)$ by

$$h(n) = j(p_1 \cdots p_n),$$

where $p_1, ..., p_n$ are the first n primes. Hagedorn [9] has computed the value of $h(n)$ for $n \leq 49$. More recently, Ziller and Morack [33] have extended this computation to $n \leq 54$.

The next table summarizes my own numerical bounds on $h(n)$ a few values from [9] and [33] for comparison. The upper bounds were computed by a branch-and-bound brute force search, while the lower bounds were found by simulated annealing. All the computations were done on my laptop, and I didn't spend *too* much time trying to get good bounds.

n	p_n	lower bound on $h(n)$	upper bound on $h(n)$
45	197	642	642
50	229	762	762
55	257	860	980
60	281	874	1180
65	313	1002	1380
70	349	1070	1630
75	379	1220	1880
100	541	1872	3350
150	863	3134	7900
200	1223	4208	15800

In Corollary 9, I prove the explicit bound

$$j(P_{10^{10}}) < 2 \cdot 10^{18}.$$

It seems plausible that if one pushed some of the numerical methods in this thesis to their limits, one might be able to prove that for all sufficiently large z we have $j(P_z) \leq \frac{z^2}{100}$. This sort of bound has a connection with Dirichlet's theorem on primes in progressions.

Proposition 1. *Suppose that for some constant C we have $j(P_z) \leq \frac{z^2}{C}$ for all sufficiently large z. Then for any $a, b \in \mathbb{N}$ with $\gcd(a, b) = 1$ and $a < C$, the arithmetic progression $\{an + b \mid n \in \mathbb{N}\}$ contains infinitely many primes.*

Proof. Let z be large, and write $P'_z = P_z / \gcd(a, P_z)$. Since by definition of P_z we have $\gcd(a, P'_z) = 1$, there exists $\overline{a} \in \mathbb{Z}$ such that $\overline{a}a \equiv 1 \pmod{P'_z}$. Then for $an + b \in [z, z^2)$, we have $an + b$ prime if and only if $\gcd(n + \overline{a}b, P'_z) = 1$ (since no prime dividing a can divide $an + b$). So we just need to show that there is at least one $n \in [(z - b)/a, (z^2 - b)/a)$ with $\gcd(n + \overline{a}b, P'_z) = 1$. This will be true so long as we have

$$j(P'_z) < \frac{z^2 - b}{a} - \frac{z - b}{a} = \frac{z(z - 1)}{a}.$$

Since $j(P_z') \leq j(P_z) \leq \frac{z^2}{C}$, for sufficiently large z this will follow from $a < C$. □

Along these lines, the following explicit bound of Linnik is known.

Theorem 4 (Linnik's Theorem [21], [22], [11], [32]). *There exists a constant L such that for any $a, b \in \mathbb{N}$ with $\gcd(a,b) = 1$ and $b < a$, the arithmetic progression $an + b$ contains a prime p with $p \ll a^L$.*

The smallest possible choice for L in Linnik's Theorem is known as *Linnik's constant*, and the current best bound for L is $L \leq 5$, due to Xylouris [32]. The connection with the Jacobsthal function is as follows.

Proposition 2 (Kanold [17], [18], [30]). *If $j(P_z) \ll z^{2-\epsilon}$, then Linnik's constant L is at most $\frac{2}{\epsilon}$.*

Since the fact that Linnik's constant is finite seems to be rather deep (relying on results about Siegel zeros), it seems unlikely that one may easily show a bound like $j(P_z) \ll z^{2-\epsilon}$. However, there is no reason to expect it to be impossible to show a bound like $j(P_z) \ll \frac{z^2}{\log(z)}$. Such a bound would give a new type of proof of Dirichlet's theorem on primes in progressions.

1.2 Simple ways to construct sieves

The simplest sieves are the combinatorial sieves. They are based on the following result.

Proposition 3. *Suppose that λ_d satisfy $\lambda_1 = 1$, and for any $d \mid P_z$ and any prime $p < z$ which is smaller than all the prime factors of d we have*

$$\lambda_d + \lambda_{pd} \leq 0. \tag{C}$$

Then

$$\mathcal{S}(A, z) \geq \sum_{d | P_z} \lambda_d |A_d|.$$

Similarly, if for all such d, p we have $\lambda_d + \lambda_{pd} \geq 0$, then $\mathcal{S}(A,z) \leq \sum_{d|P_z} \lambda_d |A_d|$.

Proof. We just need to show that for any $n \mid P_z$ with $n \neq 1$, we have

$$\sum_{d|n} \lambda_d \leq 0.$$

Let p be the least prime dividing n. Then by (C), we have

$$\sum_{d|n} \lambda_d = \sum_{d|n/p} \lambda_d + \lambda_{pd} \leq 0.$$

The upper-bound case is similar. □

Definition 2. Any collection of sieve weights λ_d satisfying the assumptions of Proposition 3 is called a *combinatorial sieve*.

Combinatorial sieves are closely connected to Buchstab iteration, which is based on repeated applications of the following identity.

Proposition 4 (Buchstab's identity)**.** *For $w \leq z$ we have*

$$\mathcal{S}(A, z) = \mathcal{S}(A, w) - \sum_{w \leq p < z} \mathcal{S}(A_p, p).$$

Another simple type of sieve is the Selberg upper bound sieve.

Proposition 5. *Let ℓ_d be any collection of real numbers with $\ell_1 = 1$. Then*

$$\mathcal{S}(A, z) \leq \sum_{d_1, d_2 | P_z} \ell_{d_1} \ell_{d_2} |A_{[d_1, d_2]}|,$$

where $[d_1, d_2]$ is the least common multiple of d_1 and d_2.

Proof. We just have to show that for any $n \mid P_z$, we have

$$\sum_{[d_1, d_2] | n} \ell_{d_1} \ell_{d_2} \geq 0.$$

This follows from the fact that the left hand side is equal to

$$\Big(\sum_{d | n} \ell_d \Big)^2,$$

which is clearly at least 0. □

Finally, I'll describe a simple way to construct iteration rules which are useful for improving the bounds in sieves of higher dimension.

Proposition 6. *Let $\lambda_0, ..., \lambda_n$ be real numbers with $\lambda_0 = 1$, such that when we define the polynomial*

$$\theta(n) = \sum_k \lambda_k \binom{n}{k}$$

we have $\theta(n) \leq 0$ for $n \in \mathbb{N}^+$. Then for $w \leq z$, we have

$$\mathcal{S}(A, z) \geq \mathcal{S}(A, w) + \lambda_1 \sum_{w \leq p_1 < z} \mathcal{S}(A_{p_1}, w) + \cdots + \lambda_n \sum_{w \leq p_n < \cdots < p_1 < z} \mathcal{S}(A_{p_1 \cdots p_n}, w).$$

Similarly, we have the reverse inequality if the λ_ks are chosen such that $\theta(n) \geq 0$ for all $n \in \mathbb{N}$.

1.3 New approaches explored in this thesis

Approximation algorithm perspective

As a computational problem, determining whether there exists a shift c such that $|\mathcal{S}(A-c,\mathcal{P})|$ is greater than a given value (given sets A and $\mathcal{P}$ as input) is in the complexity class NP, since we can compute the size of $|\mathcal{S}(A-c,\mathcal{P})|$ quickly for any given value of c. As we will see in Chapter 2, this problem is in fact NP-complete.

Determining the maximum and minimum values of $|\mathcal{S}(A-c,\mathcal{P})|$ can be viewed as a combinatorial optimization problem, and we can ask whether there are approximation algorithms which can efficiently compute upper and lower bounds which have the right order of magnitude. For instance, we can put this problem into the form of a zero-one linear programming problem as follows: for each prime $p \in \mathcal{P}$, and for each congruence class i modulo p, we can introduce a variable $x_{p,i} \in \{0,1\}$ which is 1 if we take $c \equiv i \pmod{p}$ and 0 otherwise. Additionally, for each $i \in A$ we introduce a variable $y_i \in \{0,1\}$ which is 1 if $i-c$ is relatively prime to P. Then we have the linear constraints

$$\sum_{i=0}^{p-1} x_{p,i} = 1$$

for each $p \in \mathcal{P}$, and

$$1 - \sum_{q \in \mathcal{P}} x_{q,i} \leq y_i \leq 1 - x_{p,i}$$

for each $i \in A$ and $p \in \mathcal{P}$, and our goal is to either maximize or minimize the quantity $\sum_{i \in A} y_i$. One natural way to approach such problems is to find a tractable *relaxation* of the problem - that is, to drop some of the constraints to produce a new problem which can be solved efficiently. In the case of zero-one linear programming, a standard relaxation is the *linear relaxation*, in which we replace the constraint that all the variables are in $\{0,1\}$ with the constraint that all the variables are in $[0,1]$. In this case, it is easy to see that the standard linear relaxation doesn't buy us much when $\sum_{p \in \mathcal{P}} \frac{1}{p}$ gets large, so it is natural to introduce new variables $x_{d,i}$ for d dividing P with $x_{d,i} = 1$ when $i-c$ is a multiple of d. The linear relaxation hierarchies in the literature on zero-one linear programming take an approach like this, in which one considers the collection of variables $x_{d,i}$ with d having a bounded number of prime factors, but in this case we get better bounds by considering the collection of variables $x_{d,i}$ with d bounded by a fixed power of $|A|$. Not only does this recover the first approach to the basic sifting problem described above, including Selberg's idea of smoothing the interval before applying the sieve, it also introduces a new possibility: sieve weights which depend on both the divisors of an element of $A-c$ and on the relative position of that element within the interval.

A more advanced relaxation deserves mention, although I won't explore it in much detail in this thesis. This is the *semidefinite relaxation*, in which instead of replacing our $0,1$ variables with real

numbers in $[0,1]$, we replace them by vectors, and replace our constraints with linear constraints on the sizes of the (squared) norms and dot products between these vectors. The semidefinite relaxation is a general technique for constructing approximation algorithms to combinatorial optimization problems which is conjectured to be best possible in the case of constraint satisfaction problems (the conjecture is known to be true conditional on the Unique Games Conjecture, by a result of Raghavendra [27]). Another way of describing semidefinite programming is that it finds the best possible way to combine weighted sums of linear inequalities with the fact that certain matrices are positive semidefinite in order to get bounds, using the fact that the space of positive semidefinite matrices is convex. Since all known approaches to the basic sieve theory problem can be seen as consequences of linear inequalities and the fact that certain matrices are positive semidefinite, the corresponding semidefinite program unifies previous approaches and, with luck, might outperform them.

Sieves built using iterations

I've been able to get improved bounds on the sifting functions f_κ, F_κ when κ is slightly greater than 1 by using a new combinatorial method based on variations of Buchstab iteration. The simplest example is an upper bound iteration.

Theorem 5. *For $w \leq z$, we have*

$$\mathcal{S}(A, \mathcal{P}_z) \leq \mathcal{S}(A, \mathcal{P}_w) - \frac{2}{3} \sum_{w \leq p < z} \mathcal{S}(A_p, \mathcal{P}_w) + \frac{1}{3} \sum_{w \leq q < p < z} \mathcal{S}(A_{pq}, \mathcal{P}_w).$$

The proof of this boils down to the easy inequality $0 \leq 1 - \frac{2}{3}k + \frac{1}{3}\binom{k}{2} = (1 - \frac{k}{2})(1 - \frac{k}{3})$ for $k \in \mathbb{N}$. Such an inequality will not be produced using Selberg's Λ^2 upper bound sieve, for the simple reason that the polynomial $1 - \frac{2}{3}k + \frac{1}{3}\binom{k}{2}$ can't even be written as a positive linear combination of squares of real valued polynomials, since it takes negative values when $2 < k < 3$. There is a similar but more complicated lower bound iteration rule based on the polynomial $(1-k)(1-\frac{k}{3})(1-\frac{k}{4})$, which is ≤ 0 for $k \in \mathbb{N}^+$.

The nice thing about this iteration rule is that when the sifting dimension κ is 1, and when we take $w = \frac{|A|}{z^2}$, then in the range $\frac{5}{2} < s < 3$ the upper bound this produces for $F_1(s)$ is actually equal to $F_1(s)$, there is no loss. As we increase the dimension κ past 1, this iteration rule starts to outperform Buchstab iteration, although the best choice for w changes with κ. It's curious that this iteration rule starts to break down at $s = \frac{5}{2}$ - my suspicion is that a similar iteration rule exists which works best in the range $\frac{7}{3} < s < \frac{5}{2}$, and that in fact an infinite sequence of such iteration rules can be found, such that their limit describes an upper bound sieve which gives a better upper bound for $F_\kappa(2)$ than the Selberg sieve. Preliminary calculations indicate that the third iteration rule in this sequence might already do the job.

When the sifting dimension is slightly greater than 1, the current state of the art is obtained by applying Buchstab iteration to the Selberg sieve, and is known as the Diamond-Halberstam-Richert sieve (see [3]). Based on numerical calculations, when $\kappa = \frac{3}{2}$, the generalized sifting iteration rule described above can be used to improve on the Diamond-Halberstam-Richert sieve by a small amount. The more complicated lower bound iteration rule can then be used to improve on it further.

Selberg's model problem.

A second approach, applicable to the case in which the sifting dimension κ is very large, is based on a model problem of Selberg, described in [28], in which one assumes that all primes in $\mathcal{P}$ have the roughly the same size (for instance, they might be in a dyadic interval). In this case, there are only two important parameters: the first is

$$v = \sum_{p \in \mathcal{P}} \frac{\kappa_p}{p},$$

which behaves like the dimension κ in the usual sifting problem, and the second is $R = \min_{p \in \mathcal{P}} \lfloor \frac{\log |A|}{\log p} \rfloor$, which behaves like the parameter s. Sieve weights now depend only on the number of prime factors and not on the sizes of the prime factors, and a lower bound sieve now corresponds to a collection of sieve weights $\lambda_0, ..., \lambda_R$ such that $\lambda_0 = 1$ and such that the polynomial $\theta(n)$ given by

$$\theta(n) = \sum_{i=0}^{R} \lambda_i \binom{n}{i}$$

has $\theta(n) \leq 0$ for every strictly positive integer n. Our goal is to maximize the quantity

$$\sum_{n \geq 0} \theta(n) \frac{v^n}{n!} = e^v \sum_{n=0}^{R} \lambda_n \frac{v^n}{n!}.$$

In particular, we are interested in whether we can ever make this greater than 0. Thus we define v_R to be the largest value of v such that the above can be taken to be greater than 0.

Unexpectedly, one finds that when κ and R are both large, the asymptotic bounds we get on the ratios $\frac{R}{v_R}$ and $\frac{\beta_\kappa}{\kappa}$ using various sifting approaches in the model problem and in the standard sifting problem are the same. For instance, the analogue of the β-sieve in the model problem is to take $\lambda_i = (-1)^i$ for $i \leq 2\lfloor \frac{R-1}{2} \rfloor + 1$, and using this sieve one gets the bound

$$\limsup_{R \to \infty} \frac{R}{v_R} \leq c = 3.591...,$$

where c is defined by $ce^{c+1} = 1$. This same constant shows up as the asymptotic upper bound for $\frac{\beta_\kappa}{\kappa}$ which is derived from the β-sieve. The analogue of the Selberg lower bound sieve in the model problem is given by taking $\theta(n) = (1-n)p(n)^2$ for some polynomial $p(n)$, and on choosing the

optimal $p(n)$ Selberg [28] gets the following bound.

Theorem 6 (Selberg [28])**.** *With notation as above, we have*

$$v_R \geq \lfloor \tfrac{R+1}{2} \rfloor,$$

so $\limsup_{R\to\infty} \frac{R}{v_R} \leq 2$.

Selberg raised the question of whether the Selberg lower bound sieve gives asymptotically optimal results in this model problem as the sifting dimension goes to infinity. Recently, I found a simple proof of this, based on bounding a quadratic form associated to polynomials of the form $(1-n)p(n)p(n-1)$.

Theorem 7. *In the case of the model problem, Selberg's lower bound sieve is asymptotically optimal as v and R go to infinity, that is,*

$$\lim_{R\to\infty} \frac{R}{v_R} = 2.$$

More precisely, for $R = 2d+1$, we have $v_R \leq (\sqrt{d}+1)^2$.

From this, one can improve a lower bound Selberg gave for the sifting limit β_κ by a factor of 2.

Corollary 1. $\beta_\kappa \geq (1+o(1))\frac{2\kappa}{e}$.

On the other hand, there are lower order improvements that can still be made to the Selberg lower bound sieve in the model problem. A careful (and much more difficult) analysis shows that in fact we have the following bound.

Theorem 8. $v_R \geq \frac{R}{2} + \Omega(\sqrt[3]{R})$.

The corresponding sieve is approximately of the form

$$\theta(n) = (1-n)\cdot \prod_{i=1}^{\sqrt[3]{v_R}} (1-\tfrac{n}{2i+1})(1-\tfrac{n}{2i+2})\cdot p(n)^2,$$

for some polynomial $p(n)$ with $p(0)=1$.

This suggests a strategy for finding a (lower order) improvement to the Selberg lower bound sieve in the standard sifting problem, and I expect that this method should allow one to show that when the sifting dimension is sufficiently high, the sifting limit β_κ is strictly less than twice the sifting dimension.

Chapter 2

Computational aspects of sieving

2.1 Shifted Sifting and Transverse Partition Cover

The following problem seems like a natural generalization of the Jacobsthal problem, and seems to capture the spirit of the type of sieve theory I like.

Problem 3 (Shifted Sifting)**.** Given a finite set $A \subset \mathbb{Z}$ and a finite set $\mathcal{P}$ of primes, determine if there exists a constant $c \in \mathbb{Z}$ such that each element of $A + c$ is a multiple of at least one prime in $\mathcal{P}$.

In the case A is an interval, we recover the Jacobsthal problem. If A is the set of numbers of the form $n(n+2)$ for $n \in [z, z^2 - 2]$ and $\mathcal{P}$ is the set of primes below z, then a negative answer to this question (for infinitely many z) implies the twin prime conjecture (and in fact would be a much stronger claim than the twin prime conjecture).

This is a decision problem, and since c can be assumed to be between 0 and $\prod_{p \in \mathcal{P}} p$, the size of a "witness" is polynomial in the size of the input, so this decision problem is in NP. In order to prove NP-completeness, we first show that this is equivalent to a variant of set cover which has no direct relationship to number theory.

Problem 4 (Transverse Partition Cover)**.** Given a finite set A and a finite set $\mathcal{P} = \{P_1, ..., P_k\}$ of partitions of A, determine if there is a way to choose one part A_i of each partition P_i such that $A_1 \cup \cdots \cup A_k = A$.

Proposition 7. *Every instance $(A, \mathcal{P})$ of Shifted Sifting can be efficiently transformed to an equivalent instance $(A', \mathcal{P}')$ of Transverse Partition Cover such that $|A| = |A'|$ and $|\mathcal{P}| = |\mathcal{P}'|$, and conversely every instance of Transverse Partition Cover can be efficiently transformed to an equivalent instance of Shifted Sifting.*

Proof. Going from Shifted Sifting to Transverse Partition Cover is easy: we take $A' = A$ and replace each prime $p \in \mathcal{P}$ with a corresponding partition P of A into congruence classes modulo p. For the reverse direction, if $(A', \mathcal{P}')$ is an instance of Transverse Partition Cover with $\mathcal{P}' = \{P_1, ..., P_k\}$, we first choose $\mathcal{P}$ to be a set of k primes $\{p_1, ..., p_k\}$ such that $p_i \geq |P_i|$ for each i, and fix an injection $\iota_i : P_i \to \mathbb{Z}/p_i$. Next we enumerate the elements of A' as $a'_1, ..., a'_n$, and for each $i \leq n$ we use a constructive form of the Chinese Remainder Theorem to find an element $a_i \in \mathbb{Z}$ such that $a_i \neq a_j$ for any $j < i$ and such that for each $j \leq k$ if $a'_i \in A_{i,j} \in P_j$ then $a_i \equiv \iota_j(A_{i,j}) \pmod{p_j}$. Finally we take $A = \{a_1, ..., a_n\}$. □

2.1.1 Hardness proof

Now we'll show that the Transverse Partition Cover problem is NP-complete by finding a reduction from Set Cover. First we state the Set Cover problem.

Problem 5 (Set Cover)**.** Given a finite universe S, a parameter k, and a collection $S = \{S_1, ..., S_m\}$ of subsets of U, determine whether there is a subcollection $C \subseteq S$ with $|C| = k$ such that $\bigcup_{S_i \in C} S_i = U$.

Theorem 9. *There is a polynomial time reduction from Set Cover to Transverse Partition Cover, taking an instance (U, k, S) of Set Cover to an instance $(A, \mathcal{P})$ of Transverse Partition Cover with $|A| = |U| + k|S|$, $|\mathcal{P}| = k|S|$, and each element of $\mathcal{P}$ having size $k|S| + 1$. In particular, both the Shifted Sifting problem and the Transverse Partition Cover problem are NP-complete.*

Proof. Let (U, k, S) be an instance of Set Cover with $|S| = m$. Assume without loss of generality that $U \cap \{1, ..., k|S|\} = \emptyset$ (otherwise, rename the elements of U). Take $A = U \cup \{1, ..., k|S|\}$. Take $\mathcal{P} = \{P_{i,S_j} \mid i \leq k, S_j \in S\}$, with $P_{i,S_j} = \{U \setminus S_j, \{i\} \cup S_j, \{1\}, ..., \{\hat{i}\}, ..., \{k|S|\}\}$, where $\{\hat{i}\}$ means that $\{i\}$ is omitted. □

2.1.2 Fixed Parameter Tractability

One way to distinguish difficulty levels between NP-complete problems is to study parametrized tractability, in which we fix some parameter k associated with each instance and study how the difficulty level grows as k increases.

Definition 3. A parametrized problem is *fixed parameter tractable* if there is some function f and some fixed integer d such that any instance of the problem with size n and parameter k can be solved in time $f(k)n^d$. The set of fixed parameter tractable problems is called FPT. If there is a function f such that any instance with size n and parameter k can be solved in time $n^{f(k)}$, then we say that our parametrized problem is in the class XP.

There is a hierarchy of parametrized complexity classes between FPT and XP, called the W-hierarchy:

$$FPT = W[0] \subseteq W[1] \subseteq W[2] \subseteq \cdots \subseteq W[P] \subseteq XP.$$

The definitions of the complexity classes $W[t]$ are somewhat technical, and can be found in [5] (an attempt: $W[t]$ consists of parametrized circuit-satisfiability problems in circuits having bounded depth and having at most t gates of unbounded fan-in on any path from the inputs to the output, in which the parameter k is the number of 1s in the desired solution). k-Vertex Cover, which asks whether a graph has a subset of at most k vertices which meets every edge, is a standard example of a problem in FPT. A standard example of a $W[1]$-hard (under FPT reductions) problem is k-Clique.

One reason to believe that Transverse Partition Cover may be "easier" in some sense than Set Cover is that, while k-Set Cover (where the parameter is the number of sets in our cover) is $W[2]$-hard, Transverse Partition Cover is fixed-parameter tractable if the parameter is taken to be the number of partitions.

Theorem 10. *An instance $(A, \mathcal{P})$ with $\mathcal{P} = \{P_1, ..., P_k\}$ can be solved in time $O((k!)^2|A|)$.*

Proof. Suppose that there is a choice of parts $A_i \in P_i$ such that $A_1 \cup \cdots \cup A_k = A$. Then there must be some $i_1 \leq k$ such that $|A_{i_1}| \geq \frac{1}{k}|A|$. For each partition P_i, the number of parts of P_i of size at least $\frac{1}{k}|A|$ as at most k. Thus the number of possible choices for any part A_i of any partition P_i which has size at least $\frac{1}{k}|A|$ is at most k^2. Searching over all possible choices for A_{i_1}, we reduce to at most k^2 instances with $k-1$ partitions, and by induction this can be solved in time $O(k^2((k-1)!)^2|A|) = O((k!)^2|A|)$. □

There are other, slightly less natural choices of parameter we could make. If we take our parameter to be $|A|$, then since the problem is trivial when $|\mathcal{P}| \geq |A|$, we see that it is again fixed-parameter tractable. If instead we take the parameter to be the largest number of parts in any partition in $\mathcal{P}$, then it is no longer clear whether the problem is fixed-parameter tractable - but at least we can show that it is in the complexity class XP.

Theorem 11. *An instance $(A, \mathcal{P})$ of Transverse Partition Cover such that each partition in $\mathcal{P}$ has at most c parts can be solved in time $O(|A|^{1+\log(c)/\log(\frac{c}{c-1})})$.*

Proof. Suppose that $|\mathcal{P}| = k$. If $(\frac{c-1}{c})^k|A| < 1$, then a greedy strategy covers A. Otherwise, we have $k \leq \frac{\log(|A|)}{\log(\frac{c}{c-1})}$, so a brute force search can be carried out in time proportional to

$$c^k|A| \leq c^{\log(|A|)/\log(\frac{c}{c-1})}|A| = |A|^{1+\log(c)/\log(\frac{c}{c-1})}.$$ □

2.2 Approximation Algorithms?

The most straightforward approximation variant of the Transverse Partition Cover problem is the following.

Problem 6. Given a set A and a collection of partitions $\mathcal{P} = \{P_1, ..., P_k\}$ of A, how well can we approximate

$$\max_{A_1 \in P_1, ... A_k \in P_k} |A_1 \cup \cdots \cup A_k|?$$

The following variant is likely to be much harder, but is closer to the questions we ask in sieve theory.

Problem 7. Given a set A and a collection of partitions $\mathcal{P} = \{P_1, ..., P_k\}$ of A, how well can we approximate

$$\max_{A_1 \in P_1, ... A_k \in P_k} |A \setminus (A_1 \cup \cdots \cup A_k)|?$$

If we forget that the P_is have to be partitions and allow them to be arbitrary collections of subsets, we have the following result.

Theorem 12 ([2], [6])**.** *Given a set A and a collection of collections of subsets $\mathcal{B} = \{B_1, ..., B_k\}$ of A, there is a randomized polynomial time algorithm which can approximate the quantity*

$$\max_{A_1 \in B_1, ... A_k \in B_k} |A_1 \cup \cdots \cup A_k|$$

to within a factor of $1 - \frac{1}{e} - o(1)$. If $P \neq NP$, then $1 - \frac{1}{e}$ is the best possible approximation ratio for any polynomial time approximation algorithm.

In light of the fact that restricting to the case of partitions makes the problem fixed parameter tractable, it seems reasonable to hope that there may be better approximation algorithms in this case. If this restriction is not enough, we can introduce further restrictions that tend to show up in sieve theory, such as the following.

Definition 4. We say that a collection of partitions $\mathcal{P} = \{P_1, ..., P_k\}$ of A is *almost orthogonal* if for any $i_1 < \cdots < i_j$ and any $A_{i_1} \in P_{i_1}, ..., A_{i_j} \in P_{i_j}$ we have

$$\left| |A_{i_1} \cap \cdots \cap A_{i_j}| - \frac{|A_{i_1}|}{|A|} \cdots \frac{|A_{i_j}|}{|A|} \cdot |A| \right| \leq 1.$$

Now we can consider the promise problem where we are given an instance $(A, \mathcal{P})$ of Transverse Partition Cover which we are promised is almost orthogonal, and we wish to approximate the maximum or minimum size of $|A_1 \cup \cdots \cup A_k|$ or $|A \setminus (A_1 \cup \cdots \cup A_k)|$ as above.

2.3 A difficult convex optimization problem from sieve theory

Definition 5. If $f(x_1, ..., x_n)$ is a multivariable polynomial, we define its *Newton polytope* $\mathcal{N}_f$ to be the convex hull of the set of exponent vectors of monomials which occur in f with a nonzero coefficient.

Definition 6. If $f(x_1, ..., x_n)$ is a multivariable polynomial, we say that f is *nonnegative on the naturals* if we have

$$f(x_1, ..., x_n) \geq 0$$

whenever $x_1, ..., x_n \in \mathbb{N}$. For a given finite set $\mathcal{N} \subseteq \mathbb{N}^n$, we define $\mathcal{C}_{\mathcal{N}}$ to be the set of polynomials f with $\mathcal{N}_f \cap \mathbb{N}^n \subseteq \mathcal{N}$ which are nonnegative on the naturals.

The following problem will come up naturally when we wish to compute the sifting functions $f_\kappa(s), F_\kappa(s)$.

Problem 8. Given a finite set $\mathcal{N} \subseteq \mathbb{N}^n$ and a function $c : \mathcal{N} \to \mathbb{R}$, compute

$$\max \Big\{ \sum_{\overline{e} \in \mathcal{N}} c_{\overline{e}} \lambda_{\overline{e}} \mid f(\overline{x}) = \sum_{\overline{e} \in \mathcal{N}} \lambda_{\overline{e}} \prod_{i=1}^{n} \binom{x_i}{e_i} \text{ is nonnegative on the naturals, and } \lambda_{\overline{0}} = 1 \Big\}.$$

For any $\mathcal{N} \subseteq \mathbb{N}^n$, the set $\mathcal{C}_{\mathcal{N}}$ is clearly convex. Since our goal is to optimize a linear function over the convex set $\mathcal{C}_{\mathcal{N}}$, it's tempting to appeal to a general result of Khachiyan [10] known as the *ellipsoid algorithm* which shows that the optimum can be computed efficiently if we have access to an oracle which can quickly determine whether or not a given f is contained in $\mathcal{C}_{\mathcal{N}}$. Unfortunately, in this case such an oracle is uncomputable!

Theorem 13. *If n is sufficiently large, then there is no algorithm which determines whether a given polynomial $f \in \mathbb{Z}[x_1, ..., x_n]$ is nonnegative on the naturals.*

Proof. By Matiyasevich's resolution of Hilbert's Tenth Problem [23], if n is sufficiently large then there is no algorithm which determines whether a given polynomial $g \in \mathbb{Z}[x_1, ..., x_n]$ ever takes the value 0 for natural inputs $x_1, ..., x_n$. Now take $f(x_1, ..., x_n) = g(x_1, ..., x_n)^2 - 1$, and note that f is nonnegative on the naturals if and only if g never takes the value 0 for natural inputs. □

Nevertheless, we can still approximate the answer to any given instance of Problem 8 to whatever accuracy we like. The idea is to pick some large R, and restrict our attention to polynomials f such that whenever $x_1, ..., x_n$ are nonnegative real numbers with $x_1 + \cdots + x_n > R$, we have $f(x_1, ..., x_n) \geq 0$ (note that there is an algorithm to test this, by Tarski's theorem on the decidability of real algebra [29]). Then we just have to worry about the finitely many additional constraints $f(x_1, ..., x_n) \geq 0$ for $x_1, ..., x_n \in \{0, ..., R-1\}$. This doesn't quite solve the problem, since it isn't

clear how large we need to take R to be in order to get a good approximation, without having a bound on the sizes of the $\lambda_{\overline{e}}$s which occur in the optimal solution. In the cases of Problem 8 which come up in sieve theory, we will be able to prove such bounds on the sizes of the optimal $\lambda_{\overline{e}}$s (see Proposition 34).

Theorem 14. *For any finite $\mathcal{N} \subset \mathbb{N}^n$, any $c : \mathcal{N} \to \mathcal{N}$, and any $s : \mathcal{N} \to \mathbb{R}$ and for any $\epsilon > 0$, we can compute a lower bound to the answer to Problem 8 which is within ϵ of the true answer, under the assumption that the true answer is bounded for all c' in some open neighborhood of c.*

Proof. Write $c \cdot f$ for $\sum_{\overline{e} \in \mathcal{N}} c_{\overline{e}} \lambda_{\overline{e}}$ when $f(\overline{x}) = \sum_{\overline{e} \in \mathcal{N}} \lambda_{\overline{e}} \prod_{i=1}^{n} \binom{x_i}{e_i}$. If there is any $f \in \mathcal{C}_{\mathcal{N}}$ with $f(\overline{0}) = 0, \|f\| = 1$, and $c \cdot f \geq 0$, then there is some c' close to c with $c' \cdot f > 0$, and by taking a sufficiently large multiple of f we see that the answer to Problem 8 is not bounded for this c'. If there is no such f, then by a compactness argument we see that there exist finitely many points $\overline{x}_1, ..., \overline{x}_h \in \mathbb{N}^n$ such that the inequalities $f(\overline{x}_i) \geq 0$ and $f(\overline{0}) = 0$ together imply that $c \cdot f < 0$ for $\|f\| = 1$. We can find such a collection of points by exhaustive search (note that the search may run forever if our boundedness assumption is violated), and from such a collection of points we can compute a bound on the λs in any $f \in \mathcal{C}_{\mathcal{N}}$ with $f(\overline{0}) = 1$ such that $c \cdot f \geq c \cdot \mathbf{1}$.

Let $\mathcal{N}'$ consist of all $\overline{e}' \in \mathbb{N}^n$ such that we have $\overline{e}' \leq \overline{e}$ for some $\overline{e} \in \mathcal{N}$, and let $F_1, ..., F_k$ be the collection of all faces of the convex hull of $\mathcal{N}'$ aside from the coordinate hyperplanes. For each F_i, we let p_i be the polynomial which is given by the sum of the monomials corresponding to the elements of $F_i \cap \mathcal{N}$, and let b_i be the corresponding sum of products of binomial coefficients. Choose $\delta > 0$ such that

$$|c \cdot \delta(b_1 + \cdots + b_k)| < \epsilon/2,$$

and suppose that $f \in \mathcal{C}_{\mathcal{N}}$. Write f in the monomial basis as

$$f(\overline{x}) = \sum_{\overline{e}} a_{\overline{e}} \overline{x}^{\overline{e}},$$

and define the weighted-homogeneous parts f_i of f by

$$f_i(\overline{x}) = \sum_{\overline{e} \in F_i} a_{\overline{e}} \overline{x}^{\overline{e}}.$$

Suppose that F_i is contained in the hyperplane of $\overline{e} \in \mathbb{R}^n$ such that $\sum_j w_j e_j = d$. Then for any $\lambda > 0$ we have

$$f_i(\lambda_1^{w_1} x_1, ..., \lambda_n^{w_n} x_n) = \lambda^d f_i(x_1, ..., x_n),$$

so for any nonnegative real $x_1, ..., x_n$ we have

$$f_i(x_1, ..., x_n) = \lim_{\lambda \to \infty} \lambda^{-d} f(\lfloor \lambda_1^{w_1} x_1 \rfloor, ..., \lfloor \lambda_n^{w_n} x_n \rfloor) \geq 0.$$

Let $f_\delta = f + \delta(b_1 + \cdots + b_k)$, and note that by the definition of δ we have $c \cdot f_\delta > c \cdot f - \epsilon/2$. By the above, for nonnegative real vectors $\overline{x}$ we have

$$f_\delta(\overline{x}) \gg (\delta + O\big(\sum_i x_i^{-\eta}\big))(p_1(\overline{x}) + \cdots + p_k(\overline{x}))$$

where $\eta > 0$ only depends on $\mathcal{N}'$.

Thus, given a candidate f, we can check that either $f_\delta \in \mathcal{C}_\mathcal{N}$ or that $f \notin \mathcal{C}_\mathcal{N}$, as follows. First we check that we have

$$\overline{x} \geq 0,\ p_i(\overline{x}) = 1 \quad \Longrightarrow \quad f_i(\overline{x}) + \delta p_i(\overline{x}) > \frac{\delta}{2}$$

for each i - this can be done in finite time by Tarski's theorem on the decidability of real algebra [29]. We then find some explicit R such that whenever $x_1, ..., x_n$ are nonnegative real numbers with $x_1 + \cdots + x_n > R$, we have $f_\delta(x_1, ..., x_n) \geq 0$. Now we just check that $f(\overline{x}) \geq 0$ at the finitely many points with $x_1, ..., x_n \in \{0, ..., R-1\}$.

To finish the proof, we apply the ellipsoid algorithm [10]. □

Chapter 3

Relaxations

3.1 Usual sieve-theoretic relaxation

The standard sieve theoretic relaxation allows the set $A \subseteq \mathbb{Z}$ which we are interested in sifting to be replaced with any *weighted* subset of $\mathbb{Z}$ that satisfies similar inequalities to our original set. So we assume only that A is a weighted subset of $\mathbb{Z}$, and define a weighted set A_d for every $d \mid P$ which consists of the integers n in A such that d divides n. Additionally, we define a variable a_d to be the number of elements n in A such that $\gcd(n, P) = d$. Then we see what upper and lower bounds on $a_1 = \mathcal{S}(A, \mathcal{P})$ can be deduced from the collection of linear inequalities

$$\begin{aligned} |A_d| &\leq \frac{\kappa(d)}{d} y + R(d), \\ |A_d| &\geq \frac{\kappa(d)}{d} y - R(d), \\ |A_d| &= \sum_{d|k} a_k, \\ a_k &\geq 0, \end{aligned}$$

where κ is a multiplicative function and $R(d)$ is a small error term (usually we will take $R(d) = \kappa(d)$). By summing these inequalities after multiplying them by certain carefully chosen sieve weights λ_d, we can produce upper and lower bounds on $\mathcal{S}(A, \mathcal{P})$. In fact, if we only make the assumptions above, then by linear programming duality the best possible upper bound we can get on $\mathcal{S}(A, \mathcal{P})$ is given by

$$\mathcal{S}(A, \mathcal{P}) \leq \min \Big\{ \sum_{d|P} \frac{\lambda_d \kappa(d)}{d} y - \sum_{d|P} |\lambda_d| R(d) \;\Big|\; \lambda_1 = 1,\ \forall d \mid P \ \sum_{k|d} \lambda_k \geq 0 \Big\},$$

and the best possible lower bound is similar.

Define sifting functions $f_\kappa(s), F_\kappa(s)$ by

$$(1+o(1))f_\kappa(s)|A|\prod_{p<z}\left(1-\frac{\kappa_p}{p}\right) \leq \mathcal{S}(A,\mathcal{P}_z) \leq (1+o(1))F_\kappa(s)|A|\prod_{p<z}\left(1-\frac{\kappa_p}{p}\right),$$

with $f_\kappa(s)$ as large as possible (resp. $F_\kappa(s)$ as small as possible) given that the above inequality holds for all choices of weighted sets A satisfying the assumptions above. Selberg, in his Lectures on Sieves [28], has shown the following.

Theorem 15 (Selberg [28])**.** *The optimal sifting functions $f_\kappa(s), F_\kappa(s)$ continuous, monotone, and* computable *for $s > 1$, and they tend to 1 exponentially as s goes to infinity.*

What's more, Selberg has outlined an algorithm to compute $f_\kappa(s), F_\kappa(s)$ to any desired accuracy in [28] - I'll go over this algorithm in a later Chapter 6.

3.2 Detailed linear relaxation

3.2.1 Grids of sieve weights

Proposition 8. *If m, n are coprime natural numbers and $a \in \mathbb{Z}$, then for any $c \in \mathbb{Z}$ we have*

$$\mathbf{1}_{c\equiv a \pmod m} = \sum_{k=0}^{n-1} \mathbf{1}_{c\equiv a+km \pmod{mn}}.$$

Theorem 16. *Suppose that $A \subset \mathbb{Z}$ is a finite set and $\lambda_{a,d}$ are real numbers for $d \mid P_z$ satisfying the following conditions.*

- *All but finitely many of the $\lambda_{a,d}$s are 0.*
- *For each $a \in \mathbb{Z}$, we have $\lambda_{a,1} \leq \mathbf{1}_{a\in A}$.*
- *For each $a \in \mathbb{Z}$ and each $d \mid P_z$ with $d > 1$, we have*

$$\sum_{k|d} \lambda_{a,k} \leq 0.$$

- *For each $c \in \mathbb{Z}$, we have*

$$\sum_{d|P_z}\sum_{a\in\mathbb{Z}} \lambda_{a,d}\mathbf{1}_{c\equiv a \pmod d} = 1.$$

Then for any $c \in \mathbb{Z}$ we have

$$\mathcal{S}(A+c, z) \geq 1.$$

Conversely, if $\mathcal{S}(A+c,z) \geq 1$ for all $c \in \mathbb{Z}$, then a collection of real numbers $\lambda_{a,d}$ satisfying the above properties exists.

Proof. If there are such $\lambda_{a,d}$, then for any $c \in \mathbb{Z}$, we have

$$\begin{aligned} 1 &= \sum_{d|P_z} \sum_{a \in \mathbb{Z}} \lambda_{a,d} \mathbf{1}_{d|a-c} \\ &= \sum_{a \in \mathbb{Z}} \sum_{d|(P_z, a-c)} \lambda_{a,d} \\ &\leq \sum_{\substack{a \in \mathbb{Z} \\ (P_z, a-c)=1}} \lambda_{a,1} \\ &\leq \mathcal{S}(A-c,z). \end{aligned}$$

For the converse direction, we consider the set $\mathcal{C}$ of tuples of real numbers $(x_{a,d}, y_{a,d})_{d|P_z, a \in \mathbb{Z}/P_z}$ which satisfy the following constraints:

- For any m, n with $mn \mid P_z$, we have $x_{a,m} = \sum_{k=0}^{n} x_{a+km,mn}$,
- $x_{a,d} = x_{a+d,d}$,
- $x_{0,1} = 1$,
- $x_{a,d} = \sum_{d|k|P_z} y_{a,k}$,
- $y_{a,d} \geq 0$,

and we attempt to minimize the quantity

$$\sum_{a \in A} y_{a,1}$$

over the set $\mathcal{C}$. To any element $(x_{a,d}, y_{a,d})_{d|P_z, a \in \mathbb{Z}/P_z}$ of $\mathcal{C}$ we can associate a probability distribution μ on $\mathbb{Z}/P_z$, by taking $\mu(c) = x_{c,P_z}$. Then the constraints given above imply that

$$\mathbb{P}_{\mu(c)}[c \equiv a \pmod{d}] = x_{a,d}$$

and

$$\mathbb{P}_{\mu(c)}[(P_z, a-c) = d] = y_{a,d}.$$

Conversely, to any probability distribution μ on $\mathbb{Z}/P_z$, we can associate an element of $\mathcal{C}$ using the above formulas for $x_{a,d}$ and $y_{a,d}$. The quantity which we are trying to minimize is

$$\sum_{a \in A} y_{a,1} = \mathbb{E}_{\mu(c)}[\mathcal{S}(A-c,z)],$$

so the minimum value is just $\min_{c\in\mathbb{Z}} \mathcal{S}(A-c,z)$. If this minimum is at least 1, then the existence of $\lambda_{a,d}$ satisfying the conditions of the theorem follows from linear programming duality (the $\lambda_{a,d}$ are the coefficients of the equations $x_{a,d} = \sum_{d|k|P_z} y_{a,k}$). □

An easy way to guarantee that

$$\sum_{k|d} \lambda_{a,k} \leq 0$$

for $d \mid P_z, d > 1$ is to impose the combinatorial lower bound sieve constraint: for any $a \in \mathbb{Z}$, any $d \mid P_z$, and any prime p which is less than all prime factors of d, we just require

$$\lambda_{a,d} + \lambda_{a,pd} \leq 0. \tag{3.1}$$

A collection of weights $\lambda_{a,d}$ satisfying (3.1) on top of the conditions of the previous theorem will be called a *combinatorial grid of sieve weights*.

Example 1. We give some examples of combinatorial grids of sieve weights $\lambda_{a,d}$ which allow us to find some small values of the Jacobsthal function $j(n)$. We will write out rows corresponding to small divisors d of n, and columns corresponding to a sequence of consecutive values of $a \in \mathbb{Z}$, containing an interval A of length $j(n)$. We'll also abbreviate 1 as $+$, abbreviate -1 as $-$, and leave out 0s. For our first example, in order to see that $j(6) \leq 4$, we can use the grid

1	+	+	+	+		
2	-	-	-	-		
3	-	-	-	-	-	-
6	+	+	+	+	+	+

To see that $\sum_{d|P_z} \sum_{a\in\mathbb{Z}} \lambda_{a,d} \mathbf{1}_{c\equiv a (\mathrm{mod}\ d)} = 1$, we first group the six terms $\lambda_{a,6}\mathbf{1}_{c\equiv a(\mathrm{mod}\ 6)}$ into two arithmetic progressions having common difference 2 and length 3 in order to cancel two of the terms $\lambda_{a,2}\mathbf{1}_{c\equiv a(\mathrm{mod}\ 2)}$. Then we cancel two groups of three consecutive terms $\lambda_{a,3}\mathbf{1}_{c\equiv a(\mathrm{mod}\ 3)}$ with two of the terms $\lambda_{a,1}\mathbf{1}_{c\equiv a(\mathrm{mod}\ 1)}$. Finally, we cancel the remaining two terms $\lambda_{a,2}\mathbf{1}_{c\equiv a(\mathrm{mod}\ 2)}$ with one of the terms $\lambda_{a,1}\mathbf{1}_{c\equiv a(\mathrm{mod}\ 1)}$ and we see that there is exactly one term $\lambda_{a,1}\mathbf{1}_{c\equiv a(\mathrm{mod}\ 1)}$ left over, making the full sum come out to 1.

Actually, we can simplify this first example by noticing it is a blown-up version of the grid

1	+	+	
3	-	-	-

which shows that $j(3) \leq 2$. All the remaining examples will leave out the prime 2, which can be reintroduced by blowing up the grid in a similar way.

The next grid shows that $j(105) \leq 5$.

1	+	+	+	+	+		
3	-	-	-	-	-	-	
5	-	-	-	-	-		
7	-	-	-	-	-	-	-

Blowing this up, we see that $j(210) \leq 10$. It's easy to see that these bounds are sharp.

The next grid shows that $j(2310) \leq 7$.

1	+	+	+	+	+	+	+						
3	-	-	-	-	-	-	-						
5	-	-	-	-2	-	-	-			-		-	
7	-	-	-	-	-	-	-						
11	-	-	-	-	-	-	-	-	-	-	-		
15	+			+			+			+		+	

This is sharp. The next two examples will also be sharp.

This grid shows that $j(3 \cdot 5 \cdot 7 \cdot 11 \cdot 13) \leq 11$.

1	+	+	+	+	+	+	+	+	+	+	+			
3	-	-	-	-	-	-2	-	-	-	-	-			
5	-	-	-	-	-	-	-	-	-	-	-			
7	-	-	-	-	-2	-2	-2	-	-	-	-			
11	-	-	-	-	-	-	-	-	-	-	-			
13	-	-	-	-	-	-	-	-	-	-	-	-	-	
15	+					+					+			

Finally, this grid shows that $j(3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17) \leq 13$.

1	+	+	+	+	+	+	+	+	+	+	+	+	+												
3	-	-	-	-	-	-	-	-	-	-	-	-	-												
5	-	-	-	-	-	-	-	-	-	-	-	-	-												
7	-	-	-	-	-	-	-2	-	-	-	-	-	-												
11	-	-	-	-2	-	-	-2	-	-	-2	-	-	-			-		-		-		-		-	
13	-	-	-	-	-	-	-	-	-	-	-	-	-												
15	+	+	+			+	+	+			+	+	+												
17	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-								
33	+			+			+			+			+		+		+		+		+		+		+

Searching for combinatorial grids of sieve weights with $\lambda_{a,d}$ supported on $a, d \leq z^k$ can be done in polynomial time for any fixed k, using any polynomial time algorithm for linear programming. This can be viewed as a heierarchy of linear relaxations of the shifted sifting problem. Unfortunately, I haven't had time to experiment with how well this performs in practice once z gets large.

The next result, when combined with the parity obstruction (see Section 8.2), shows that we can't hope to find a grid of sieve weights $\lambda_{a,d}$ supported on $d \leq z^{2-\epsilon}$ which produces any nontrivial bounds on the Jacobsthal function.

Proposition 9. *Let $\lambda_{a,d}$ satisfy the conditions of Theorem 16. Then if we define*

$$\lambda_d = \frac{1}{|A|} \sum_{a \in \mathbb{Z}} \lambda_{a,d},$$

we have $\lambda_1 \leq 1$ and for any $d \mid P_z$ with $d > 1$ we have

$$\sum_{k|d} \lambda_k \leq 0,$$

so the λ_ds define a lower bound sieve. Furthermore, we have

$$\sum_d \frac{\lambda_d}{d} > 0,$$

so this lower bound sieve has a nontrivial main term.

3.2.2 Smoothed interval

The grids of sieve weights in the examples form the previous subsection get progressively more complicated as z increases. In order to simplify the picture, we'll look at grids of weights $\lambda_{a,d}$ which factor in the form

$$\lambda_{a,d} = I(a)\lambda_d,$$

where I is a function satisfying

$$0 \leq I(a) \leq \mathbf{1}_{a \in A}$$

and λ_d is a collection of lower bound sieve weights, satisfying

$$\sum_{k|d} \lambda_k \leq 0$$

for $d \mid P_z, d > 1$. We also relax the condition

$$\sum_{d|P_z} \sum_{a \in \mathbb{Z}} \lambda_{a,d} \mathbf{1}_{c \equiv a \pmod d} = 1$$

to the weaker

$$\sum_{d|P_z} \sum_{a \in \mathbb{Z}} \lambda_{a,d} \mathbf{1}_{c \equiv a \pmod d} > 0,$$

which is still strong enough to show that $\mathcal{S}(A + c, z) \geq 1$ for any $c \in \mathbb{Z}$.

An equivalent way of looking at this is that we are replacing the set A by a smaller weighted set with weights given by the function I, and applying a standard lower bound sieve to the resulting

weighted set. Although this weighted set is smaller - causing the main term of the bound we get by sieving to decrease - we can hope that smoothing out the set A decreases the error term. This idea of replacing the set A by a weighted set was suggested by Selberg in section 19 of his Lectures on Sieves [28].

Rather than searching for the optimal choice of I, we will instead focus on a specific choice in the special case where $A = [1, |A|]$ is an interval, which is motivated as follows. The idea is that the main reason the error term in the size of $|(A+c)_d|$ is so large is that we have no idea how the boundaries of $A+c$ line up with the multiples of d. In order to mitigate this, we can imagine taking the endpoints of the interval $A+c$ and moving them inwards by a random amount between 0 and W (where W is some fixed parameter with $2W \leq |A|$), giving us a roughly equal chance of a favorable error term and an unfavorable error term if W is bigger than d. This corresponds to the choice of function

$$I(a) = \begin{cases} 0 & a \leq 0 \text{ or } a \geq |A|+1, \\ \frac{a}{W} & 0 \leq a \leq W, \\ 1 & W \leq a \leq |A|+1-W, \\ \frac{|A|+1-a}{W} & |A|+1-W \leq a \leq |A|+1. \end{cases}$$

Proposition 10. *If I as defined as above, then for any $d \in \mathbb{N}^+$ and any $c \in \mathbb{R}$ we have*

$$\left| \frac{|A|+1-W}{d} - \sum_{a \equiv c \pmod d} I(a) \right| \leq \frac{d}{W} \Big\{ \frac{W}{d} \Big\} \Big\{ -\frac{W}{d} \Big\}.$$

Proof. Let $f(c)$ be defined by

$$f(c) = \sum_{a \equiv c \pmod d} I(a) - \frac{|A|+1-W}{d}.$$

Then f has period d, and has average value 0. The derivative of f is given by

$$f'(c) = \frac{1}{W} \sum_{k \in \mathbb{Z}} (\mathbf{1}_{c-kd \in [0, d\{W/d\}]} - \mathbf{1}_{c-kd \in [|A|+1-d\{W/d\}, |A|+1]}).$$

Integrating, we find that $\max_c f(c) \leq \min_c f(c) + \frac{d}{W}\{\frac{W}{d}\}$. Since the average value of f is 0, we see that $\max_c f(c)$ is maximized when f takes its maximum value at as few points as possible, i.e. when it takes its maximum value at just the points congruent to $d\{\frac{W}{d}\}$ modulo d (this occurs when $|A|+1 \equiv 2d\{\frac{W}{d}\} \pmod d$). From here, it's easy to see that

$$\max_c f(c) \leq \frac{d}{W} \Big\{ \frac{W}{d} \Big\} - \frac{1}{d} \cdot \frac{d}{W} \Big\{ \frac{W}{d} \Big\} \cdot d \Big\{ \frac{W}{d} \Big\} = \frac{d}{W} \Big\{ \frac{W}{d} \Big\} \Big\{ -\frac{W}{d} \Big\},$$

and a similar argument shows that

$$\min_c f(c) \geq -\frac{d}{W}\Big\{\frac{W}{d}\Big\} + \frac{1}{d}\cdot\frac{d}{W}\Big\{\frac{W}{d}\Big\}\cdot d\Big\{\frac{W}{d}\Big\} = -\frac{d}{W}\Big\{\frac{W}{d}\Big\}\Big\{-\frac{W}{d}\Big\}. \qquad \square$$

Theorem 17. *If the sieve weights λ_d, $d \mid P_z$, define a lower bound sieve and A is an interval, then for any $W \leq |A|/2$ we have*

$$\mathcal{S}(A,z) \geq \left(\sum_d \frac{\lambda_d}{d}\right)(|A|+1-W) - \frac{1}{W}\sum_d |\lambda_d| d\Big\{\frac{W}{d}\Big\}\Big\{-\frac{W}{d}\Big\}.$$

In particular, if $\sum_d \frac{\lambda_d}{d} > 0$ and

$$|A| \geq W + \frac{1}{W}\frac{\sum_d |\lambda_d| d\Big\{\frac{W}{d}\Big\}\Big\{-\frac{W}{d}\Big\}}{\sum_d \frac{\lambda_d}{d}},$$

then

$$\mathcal{S}(A,z) \geq 1.$$

Corollary 2. *If the sieve weights λ_d, $d \mid P_z$, define a lower bound sieve with $\sum_d \frac{\lambda_d}{d} > 0$, then*

$$j(P_z) \leq \sqrt{\frac{\sum_d |\lambda_d| d}{\sum_d \frac{\lambda_d}{d}}}.$$

Example 2. In this example we will show that among any 1900 consecutive integers, at least one of them is not a multiple of any of the first 50 primes (this is a worse bound than the one found with a brute force search, in the table of bounds on the Jacobsthal function in the introduction). We will treat the prime 2 seperately, so from now on I will try to prove that among any 950 consecutive odd numbers, at least one has no prime factors less than or equal to 229.

To make the description of the sieve weights more compact, I'll define an ordering on squarefree numbers that is weaker than ordering by size, but is stronger than ordering by divisibility. For squarefree numbers a and b, write $a = p_j \cdots p_1$ and $b = q_k \cdots q_1$, with $p_j < \cdots < p_1, q_k < \cdots < q_1$. Then I say that $a \prec b$ if $j \leq k$ and $p_i \leq q_i$ for i between 1 and j.

Now I define the set D by

$$D = \{d \mid d \text{ odd, squarefree, and } d \prec 3\cdot 229 \text{ or } d \prec 3\cdot 5\cdot 89 \text{ or } d \prec 5\cdot 7\cdot 31 \text{ or } d \prec 7\cdot 11\cdot 13\},$$

and take the sieve weights λ_d to be the combinatorial lower bound sieve defined by

$$\lambda_d = \begin{cases} \mu(d) & d \in D, \\ 0 & d \notin D. \end{cases}$$

The largest element of D is $3 \cdot 5 \cdot 89 = 1335$, which is a bit larger than the size of the interval I am sifting. The number of elements of the set D is 165, and the sum of $\frac{\mu(d)}{d}$ over $d \in D$ is about $\frac{1}{24.7993}$. So the classical sieve theoretic bound says that the number of integers relatively prime to the first 49 odd primes in an interval of length 950 is at least $\frac{950}{24.7993} - 165 = -126.6...$, but since this is less than 0 this isn't good enough.

The average size of an element of D is $\frac{4619}{15}$, or about 307.933. If we apply the simpler bound in Theorem 17 with $W = 462$, we see that among any 950 consecutive odd integers, the number that are relatively prime to the first 50 primes is at least

$$\frac{950 - 462 + 1}{24.7993} - \frac{165 \cdot 307.933}{4 \cdot 462} = -7.776...,$$

which still isn't a good enough lower bound. Using the slightly messier bound in Theorem 17, where the error term coming from d is $\frac{d}{W}\{\frac{W}{d}\}\{-\frac{W}{d}\}$, we get the lower bound

$$\frac{950 - 462 + 1}{24.7993} - 19.7165 = 0.00187...,$$

which is, at last, greater than zero.

3.3 Semidefinite relaxation and the Large Sieve

One way of motivating the semidefinite relaxation is the following generalization of the converse direction of Theorem 16. We consider the set $\mathcal{C}$ of tuples of vectors $(x_{a,d}, y_{a,d})_{d|P_z, a \in \mathbb{Z}/P_z}$ which satisfy the following constraints:

- for any m, n with $mn \mid P_z$, we have $\|x_{a,m}\|^2 = \sum_{j=0}^{n} \|x_{a+jm,mn}\|^2$,
- for any $d, e \mid P_z$, we have $x_{a,d} \cdot x_{a,e} = \|x_{a,[d,e]}\|^2$, where $[d, e]$ is the lcm of d and e,
- $x_{a,d} = x_{a+d,d}$,
- $x_{a,d} \cdot x_{b,e} = 0$ if $a \not\equiv b \pmod{\gcd(d, e)}$,
- $\|x_{0,1}\| = 1$,
- $\|x_{a,d}\|^2 = \sum_{d|k} \|y_{a,k}\|^2$,
- for any $d \mid k$, we have $x_{a,d} \cdot y_{a,k} = \|y_{a,k}\|^2$,
- $y_{a,d} \cdot y_{b,e} = 0$ if $\gcd(d, a - b)$, $\gcd(e, a - b)$, and $\gcd(d, e)$ are not all equal,

and we attempt to minimize the quantity

$$\sum_{a \in A} \|y_{a,1}\|^2$$

over the set $\mathcal{C}$.

To any element $(x_{a,d}, y_{a,d})_{d|P_z, a\in\mathbb{Z}/P_z}$ of $\mathcal{C}$ we can associate a probability distribution μ on $\mathbb{Z}/P_z$, by taking $\mu(c) = \|x_{c,P_z}\|^2$. Then the constraints given above imply that

$$\mathbb{P}_{\mu(c)}[c \equiv a \pmod d] = \|x_{a,d}\|^2,$$
$$\mathbb{P}_{\mu(c)}[c \equiv a \pmod d \wedge c \equiv b \pmod e] = x_{a,d} \cdot x_{b,e},$$

and

$$\mathbb{P}_{\mu(c)}[(P_z, a-c) = d] = \|y_{a,d}\|^2.$$

Conversely, to any probability distribution μ on $\mathbb{Z}/P_z$, we can associate an element of $\mathcal{C}$. First I'll describe a way to construct the $x_{a,d}$s. Consider the matrix M with rows and columns indexed by ordered pairs (a,d) with $d \mid P_z, a \in \mathbb{Z}/d$, such that

$$M_{(a,d),(b,e)} = \mathbb{P}_{\mu(c)}[c \equiv a \pmod d \wedge c \equiv b \pmod e].$$

The matrix M is then a positive semidefinite matrix, since it is a weighted average of rank one positive semidefinite matrices corresponding to specific values of c. Thus there exists a tuple of vectors $x_{a,d}$ such that

$$x_{a,d} \cdot x_{b,e} = M_{(a,d),(b,e)}.$$

To see that it is possible to find the *full* tuple $(x_{a,d}, y_{a,d})$, just note that for any specific value of c there corresponds a collection of 1-dimensional vectors $(x_{a,d}, y_{a,d})$ satisfying all of the constraints listed above, and then take a weighted some of orthogonal copies of these tuples of vectors over the various choices of c.

I'll illustrate one possible way to take advantage of this relaxation. Let B be a positive semidefinite matrix with rows and columns indexed by (a,d) with $d \mid P_z$, $a \in \mathbb{Z}/d$. Then since B and M are both positive semidefinite, we have

$$\mathrm{Tr}(BM) \geq 0,$$

and expanding this gives

$$\sum_{(a,d),(b,e)} B_{(a,d),(b,e)} x_{a,d} \cdot x_{b,e} \geq 0.$$

Since $x_{a,d} \cdot x_{b,e} = 0$ when $a \not\equiv b \pmod{\gcd(d,e)}$, this can be rewritten as

$$\sum_{d,e|P_z} \sum_{a\in\mathbb{Z}/[d,e]} B_{(a,d),(a,e)} \|x_{a,[d,e]}\|^2 \geq 0.$$

Next we take a lower bound sieve inequality for each a as in the section on grids of sieve weights, to get

$$\|y_{a,1}\|^2 \geq \sum_{d|P_z} \lambda_{a,d}\|x_{a,d}\|^2.$$

Summing this all up, we get the inequality

$$\begin{aligned}\mathcal{S}(A-c,z) &\geq \sum_a \sum_{d|P_z} \lambda_{a,d}\mathbf{1}_{c\equiv a \pmod d} - \sum_{d,e|P_z} \sum_{a\in\mathbb{Z}/[d,e]} B_{(a,d),(a,e)}\mathbf{1}_{c\equiv a \pmod{[d,e]}} \\ &= \sum_{d|P_z}\Big(\sum_{a\equiv c \pmod d} \lambda_{a,d} - \sum_{[d_1,d_2]=d} B_{(c,d_1),(c,d_2)}\Big),\end{aligned}$$

which holds as long as B is positive semidefinite and the $\lambda_{a,d}$s satisfy

$$\sum_{k|d} \lambda_{a,k} \leq \mathbf{1}_{d=1,a\in A}.$$

It isn't clear to me whether the inequality above is useful in practice, especially since so far we haven't really taken advantage of the $y_{a,d}$s. One way to take advantage of the $y_{a,d}$s comes up in applications of the Large Sieve. For any $\alpha \in \mathbb{R}/\mathbb{Z}$, we define a vector $S(\alpha)$ by

$$S(\alpha) = \sum_{a\in A} e^{2\pi i\alpha a} y_{a,1}. \tag{3.2}$$

Note that we have

$$\|S(\alpha)\|^2 = \sum_{a,b\in A} \cos(2\pi\alpha(a-b)) y_{a,1}\cdot y_{b,1},$$

so for any fixed α, we see that $\|S(\alpha)\|^2$ is a linear function of the dot products $y_{a,1}\cdot y_{b,1}$.

Theorem 18 (Montgomery [24]). *Suppose that for each $p<z$, the set $Z\subseteq A$ avoids κ_p congruence classes modulo p, and for any $d \mid P_z$ define $\kappa(d)=\prod_{p|d}\kappa_p$ and $\varphi_\kappa(d)=\prod_{p|d}(p-\kappa_p)$. If $y_{a,1}=\mathbf{1}_{a\in Z}$ and $S(\alpha)$ is defined as in (3.2) for $\alpha\in\mathbb{R}/\mathbb{Z}$, then for any $d\mid P_z$ we have*

$$\sum_{a\in(\mathbb{Z}/d)^*} \|S(\tfrac{a}{d})\|^2 \geq \frac{\kappa(d)}{\varphi_\kappa(d)}|Z|^2.$$

Theorem 19 (Large Sieve [25]). *If A is an interval, $\alpha_1,...,\alpha_R\in\mathbb{R}/\mathbb{Z}$ satisfy $\|\alpha_r-\alpha_s\|\geq\delta$, and the vectors $S(\alpha)$ are defined as in (3.2), then we have*

$$\sum_{r=1}^R \|S(\alpha_r)\|^2 \leq (|A|+\delta^{-1}-1)\sum_{a\in A}\|y_{a,1}\|^2.$$

Taking $\kappa_p = 1$ for all p, supposing that A is an interval, and letting Z be the set of elements of A such that $\gcd(P_z, a - c) = 1$, we see that for any y we have

$$\Big(\sum_{\substack{d|P_z \\ d\le\sqrt{y}}} \frac{1}{\varphi(d)} \Big) \mathcal{S}(A-c,z)^2 \le \sum_{\substack{d|P_z \\ d\le\sqrt{y}}} \sum_{a\in(\mathbb{Z}/d)^*} \|S(\tfrac{a}{d})\|^2 \le (|A|+y)\mathcal{S}(A-c,z),$$

so

$$\mathcal{S}(A-c,z) \le \frac{|A|+y}{\sum_{\substack{d|P_z \\ d\le\sqrt{y}}} \frac{1}{\varphi(d)}}.$$

Chapter 4

Toys and Intuition

4.1 Sifting with at most four "primes"

In this section, we will consider the following problem, parametrized by four real numbers p, q, r, s with $1 < p \leq q \leq r \leq s$.

Problem 9. What is the maximum y such that there is a weighted set A and four weighted subsets $A_p, A_q, A_r, A_s \subseteq A$ such that, if we formally define $A_1 = A$ and $A_{mn} = A_m \cap A_n$, then we have

$$-1 \leq |A_d| - \frac{y}{d} \leq 1$$

for $d = 1, p, q, r, s, pq, pr, ps, qr, qs, rs, pqr, pqs, prs, qrs, pqrs$, and such that we also have

$$A = A_p \cup A_q \cup A_r \cup A_s?$$

This is a linear programming problem, with coefficients depending continuously on p, q, r, s. Letting a_d denote the number of elements of A_d which are not also elements of any $A_{d'}$ with $d \mid d'$ (interpreted formally), we have

$$|A_d| = \sum_{d|k} a_k,$$

so the constraints can be written as

$$-1 \leq \frac{y}{d} - \sum_{d|k} a_k \leq 1 \tag{4.1}$$

together with $a_d \geq 0$ and

$$a_1 = 0.$$

Summing the constraints (4.1) with weights λ_d, we see that if

$$\sum_{k|d} \lambda_d \leq 0 \tag{4.2}$$

for $d > 1$, then

$$y \sum_{d|pqrs} \frac{\lambda_d}{d} \leq \sum_{d|pqrs} |\lambda_d| + \sum_{k|pqrs} a_k \sum_{d|k} \lambda_d \leq \sum_{d|pqrs} |\lambda_d|.$$

In particular, if

$$\sum_{d|pqrs} \frac{\lambda_d}{d} > 0,$$

then

$$y \leq \frac{\sum_{d|pqrs} |\lambda_d|}{\sum_{d|pqrs} \frac{\lambda_d}{d}}.$$

By linear programming duality, we have the following.

Proposition 11. *For any $1 < p \leq q \leq r \leq s$, we have*

$$\begin{aligned} &\max\{y \mid \exists (a_d)_{d|pqrs} \in \mathbb{R}^{16}_{\geq 0} \text{ satisfying (4.1) and } a_1 = 0\} \\ &= \min \left\{ \frac{\sum_{d|pqrs} |\lambda_d|}{\sum_{d|pqrs} \frac{\lambda_d}{d}} \mid (\lambda_d)_{d|pqrs} \in \mathbb{R}^{16} \text{ satisfy (4.2) and } \sum_{d|pqrs} \frac{\lambda_d}{d} > 0 \right\}. \end{aligned}$$

Furthermore, if a_d, λ_d are chosen optimally, then we have the following "complementary slackness" relations.

- *If $a_d > 0$, then $\sum_{k|d} \lambda_d = 0$.*
- *If $\lambda_d \neq 0$, then $\frac{y}{d} - \sum_{d|k} a_k = \begin{cases} 1 & \lambda_d > 0, \\ -1 & \lambda_d < 0. \end{cases}$*

Now we describe the various optimal sieves that appear in various ranges.

4.1.1 Range I (Eratosthenes-Legendre sieve)

Range I is given by

$$(r-1)(s-1) \leq 4. \tag{I}$$

In this range, the optimal choice for λ_d is $\lambda_d = \mu(d)$, and the optimal choice of y, a_d is given by

$$\begin{aligned} y &= \frac{16pqrs}{(p-1)(q-1)(r-1)(s-1)}, \\ a_{pqrs} &= \frac{16}{(p-1)(q-1)(r-1)(s-1)} - 1, \\ a_{qrs} &= \frac{16}{(q-1)(r-1)(s-1)} + 2, \\ a_{rs} &= \frac{16}{(r-1)(s-1)} - 4, \\ a_s &= \frac{16}{s-1} + 8, \end{aligned}$$

and the remaining a_ds are defined symmetrically.

4.1.2 Range II (combinatorial)

Range II is given by

$$3 \leq rs - r - s, \tag{II.1}$$

$$(q-1)(rs-r-s) \leq 6r, \tag{II.2}$$

$$(p-1)(q-1)(rs-r-s) \leq 6((p-1)(r-1) + (q-1)(r-1) - (p-1)(q-1)). \tag{II.3}$$

In this range, the optimal choice for λ_d is

$$\lambda_d = \begin{cases} \mu(d) & rs \nmid d, \\ 0 & rs \mid d, \end{cases}$$

and the corresponding y is

$$y = \frac{12pqrs}{(p-1)(q-1)(rs-r-s)}.$$

In the interior of this range, the set of possible values for the a_ds is three dimensional. In terms of

a_{prs}, a_{qrs}, and a_{pqrs}, the rest of the a_ds can be described as follows:

$$\begin{aligned}
a_{rs} &= 0,\\
a_{pqs} &= \frac{12r}{(p-1)(q-1)(rs-r-s)} - a_{pqrs} + 1,\\
a_{qs} &= \frac{12r}{(q-1)(rs-r-s)} - a_{qrs} - 2,\\
a_{pq} &= \frac{12}{(p-1)(q-1)} + a_{pqrs} - 3,\\
a_q &= \frac{12}{q-1} + a_{qrs} + 6,\\
a_s &= \frac{12r}{rs-r-s} + 4,
\end{aligned}$$

with the remaining a_ds defined by interchanging p and q or interchanging r and s in the above. The variables $a_{prs}, a_{qrs}, a_{pqrs}$ need to be chosen to satisfy the following system of inequalities:

$$\begin{aligned}
&\max\left\{0, \tfrac{12}{(p-1)(q-1)(rs-r-s)} - 1, 3 - \tfrac{12}{(p-1)(q-1)}\right\} \le a_{pqrs} \le \frac{12}{(p-1)(q-1)(rs-r-s)} + 1,\\
&\max\left\{0, \tfrac{12q}{(p-1)(q-1)(rs-r-s)} - a_{pqrs} - 1\right\} \le a_{prs} \le \min\left\{\tfrac{12q}{(p-1)(q-1)(rs-r-s)} - a_{pqrs} + 1, \tfrac{12r}{(p-1)(rs-r-s)} - 2\right\},\\
&\max\left\{0, \tfrac{12p}{(p-1)(q-1)(rs-r-s)} - a_{pqrs} - 1\right\} \le a_{qrs} \le \min\left\{\tfrac{12p}{(p-1)(q-1)(rs-r-s)} - a_{pqrs} + 1, \tfrac{12r}{(q-1)(rs-r-s)} - 2\right\},\\
&\frac{12pq}{(p-1)(q-1)(rs-r-s)} - 1 \le a_{prs} + a_{qrs} + a_{pqrs} \le \frac{12pq}{(p-1)(q-1)(rs-r-s)} + 1.
\end{aligned}$$

To see that the first inequality can be satisfied, note that by (II.3) we have

$$6(r-1)(s-1) \ge 6((p-1)(r-1) + (q-1)(r-1) - (p-1)(q-1)) \ge (p-1)(q-1)(rs-r-s),$$

so

$$\frac{12}{(p-1)(q-1)(rs-r-s)} + 1 \ge 3 - \frac{12}{(p-1)(q-1)}.$$

As long as $6r \ge (q-1)(rs-r-s)$ (which is (II.2)) and a_{pqrs} satisfies

$$a_{pqrs} \ge 1 - \frac{12(pr-p-r)}{(p-1)(q-1)(rs-r-s)},$$

we can find a_{prs}, a_{qrs} satisfying the second and third inequalities. What's left is to check that the fourth inequality can be satisfied. Since the set of possible values of $a_{prs} + a_{qrs} + a_{pqrs}$ is an interval, we just need to check that it can take both sufficiently large and sufficiently small values. To see that it can take sufficiently small values, take a_{pqrs} as large as possible and take a_{prs}, a_{qrs} as small as possible.

What's left is to check that $a_{prs} + a_{qrs} + a_{pqrs}$ can take a value which is $\ge \frac{12pq}{(p-1)(q-1)(rs-r-s)} - 1$.

If it is possible to choose a_{pqrs} such that we may take $a_{prs} = \frac{12q}{(p-1)(q-1)(rs-r-s)} - a_{pqrs} + 1$ and $a_{qrs} = \frac{12r}{(q-1)(rs-r-s)} - 2$ (or vice-versa), then this choice gives

$$a_{prs} + a_{qrs} + a_{pqrs} = \frac{12(rp+q-1)}{(p-1)(q-1)(rs-r-s)} - 1 \geq \frac{12pq}{(p-1)(q-1)(rs-r-s)} - 1.$$

Otherwise there are two cases. If we can take $a_{prs} = \frac{12r}{(p-1)(rs-r-s)} - 2, a_{qrs} = \frac{12r}{(q-1)(rs-r-s)} - 2$, then taking $a_{pqrs} = \frac{12}{(p-1)(q-1)(rs-r-s)} + 1$, we have

$$a_{prs}+a_{qrs}+a_{pqrs}-(\tfrac{12pq}{(p-1)(q-1)(rs-r-s)}-1) = \frac{12((p-1)(r-1)+(q-1)(r-1)-(p-1)(q-1))}{(p-1)(q-1)(rs-r-s)}-2,$$

and this is at least 0 by (II.3). In the last case, the best we can do is to take $a_{prs} = \frac{12q}{(p-1)(q-1)(rs-r-s)} - a_{pqrs} + 1, a_{qrs} = \frac{12p}{(p-1)(q-1)(rs-r-s)} - a_{pqrs} + 1$, and take a_{pqrs} as small as possible. Since we are in this last case, this smallest possible value of a_{pqrs} must satisfy the inequality

$$a_{pqrs} > 3 - \frac{12(pr-p-r)}{(p-1)(q-1)(rs-r-s)} \geq 3 - \frac{12}{(p-1)(q-1)}.$$

Thus the smallest possible choice for a_{pqrs} is either $a_{pqrs} = 0$ or $a_{pqrs} = \frac{12}{(p-1)(q-1)(rs-r-s)} - 1$. If it is the latter, then

$$a_{prs} + a_{qrs} + a_{pqrs} - (\tfrac{12pq}{(p-1)(q-1)(rs-r-s)} - 1) = 4 - \frac{12}{rs-r-s},$$

which is at least 0 by (II.1). Finally, if $a_{pqrs} = 0$, then

$$a_{prs} + a_{qrs} + a_{pqrs} - (\tfrac{12pq}{(p-1)(q-1)(rs-r-s)} - 1) = 3 - \frac{12(pq-p-q)}{(p-1)(q-1)(rs-r-s)},$$

and by (II.1) this follows from

$$rs - r - s \geq \frac{4(rs-r-s)}{(r-1)(s-1)} \geq \frac{4(pq-p-q)}{(p-1)(q-1)}.$$

4.1.3 Range III (first new sieve)

Range III is defined by

$$6((p-1)(r-1)+(q-1)(r-1)-(p-1)(q-1)) \leq (p-1)(q-1)(rs-r-s), \tag{III.1}$$

$$(p-1)(q-1)(rs-r-s) \leq 5(pq+pr-qr-1)+(p-1)r, \tag{III.2}$$

$$2(p-1)(q-1)(rs-r-s) \leq 11(2(p-1)s-(pq+pr-qr-1))+(p-1)(r-1)+(q-1)(r-1)-(p-1)(q-1). \tag{III.3}$$

The optimal λ_ds are given by

$$\lambda_d = \begin{cases} \mu(d) & d \mid pqr \text{ or } d \mid s, \\ \frac{1}{2} & d \in \{ps, qs, rs\}, \\ 0 & d \in \{pqs, prs, qrs\}, \\ -\frac{1}{2} & d = pqrs, \end{cases}$$

and the corresponding y is

$$y = \frac{11pqrs}{(p-1)(q-1)(r-1)s - pqr + \frac{1}{2}(pq+qr+pr-1)} = \frac{22pqrs}{D},$$

where

$$D = 2(p-1)(q-1)(r-1)s - 2pqr + pq + qr + pr - 1.$$

There is only one choice for the optimal a_ds: they are given by

$$\begin{aligned} a_{rs} &= 0, \\ a_{pqrs} &= \frac{22}{D} + 1, \\ a_{pqr} &= \frac{22(s-1)}{D}, \\ a_{qrs} &= \frac{11(pq+pr-qr-1)}{D} - 1, \\ a_{qr} &= \frac{22(p-1)s - 11(pq+pr-qr-1)}{D} - 1, \\ a_s &= \frac{22pqr - 11(pq+qr+pr-1)}{D} + 3, \\ a_r &= \frac{22((p-1)(q-1)s - pq + 1)}{D} + 6, \end{aligned}$$

with the remaining a_ds given by permuting p, q, r in the above.

The basic principle behind this sieve is easier to understand in terms of upper bound sieves, and gives us our first example of an iteratively constructed sieve other than the combinatorial sieve. We'll use it later to show that in the case of the linear sieve (that is, $\kappa_p = 1$ for all p), the optimal sieve is often not a combinatorial sieve.

Proposition 12. *For any $w \le z$, we have*

$$\mathcal{S}(A, z) \le \mathcal{S}(A, w) - \frac{1}{2} \sum_{z > p \ge w} \mathcal{S}(A_p, w) + \frac{1}{2} \sum_{z > p > q > r \ge w} \mathcal{S}(A_{pqr}, w).$$

4.1.4 Range IV (combinatorial)

Range IV is defined by

$$5(p-1)r \le (p-1)(q-1)(r-1)s - (p-1)qr, \tag{IV.1}$$
$$5(pq+pr-qr-1) \le (p-1)(q-1)(r-1)s - (p-1)qr, \tag{IV.2}$$
$$(p-1)(q-1)(r-1)s - (p-1)qr \le 5(p-1)s, \tag{IV.3}$$
$$(p-1)(q-1)(r-1)s - (p-1)qr \le 10qr. \tag{IV.4}$$

The optimal λ_ds are given by

$$\lambda_d = \begin{cases} \mu(d) & d \mid pqr \text{ or } d \mid ps, \\ 0 & \text{else,} \end{cases}$$

and the corresponding y is

$$y = \frac{10pqrs}{(p-1)(q-1)(r-1)s - (p-1)qr}.$$

In the interior of this range, the set of optimal a_ds is three dimensional. Set $D = (p-1)(q-1)(r-1)s - (p-1)qr$. In terms of $a_{pqs}, a_{prs}, a_{pqrs}$, the a_ds are given by:

$$\begin{aligned}
a_{qs} &= 0, \\
a_{qrs} &= 0, \\
a_{pqr} &= \frac{10s}{D} - a_{pqrs} + 1, \\
a_{ps} &= \frac{10qr}{D} - a_{pqs} - a_{prs} - a_{pqrs} - 1, \\
a_{qr} &= \frac{10s}{(q-1)(r-1)s - qr} - 2, \\
a_{pr} &= \frac{10(q-1)s}{D} - a_{prs} - 2, \\
a_s &= \frac{10qr}{(q-1)(r-1)s - qr} + 2, \\
a_r &= \frac{10(q-1)s}{(q-1)(r-1)s - qr} + 4, \\
a_p &= \frac{10}{p-1} + a_{pqs} + a_{prs} + a_{pqrs} + 5,
\end{aligned}$$

with the remaining a_ds given by swapping q and r in the above (note that $a_{qr} \ge 0$ is equivalent to

(IV.3)). The variables $a_{pqs}, a_{prs}, a_{pqrs}$ need to satisfy the following inequalities:

$$\begin{aligned}
\max\Big\{0, \frac{10p}{D} - 1\Big\} \le a_{pqrs} &\le \frac{10}{D} + 1, \\
\max\Big\{0, \frac{10pq}{D} - a_{pqrs} - 1\Big\} \le a_{prs} &\le \min\Big\{\frac{10q}{D} - a_{pqrs} + 1, \frac{10(q-1)s}{D} - 2\Big\}, \\
\max\Big\{0, \frac{10pr}{D} - a_{pqrs} - 1\Big\} \le a_{pqs} &\le \min\Big\{\frac{10r}{D} - a_{pqrs} + 1, \frac{10(r-1)s}{D} - 2\Big\}, \\
a_{prs} + a_{pqs} + a_{pqrs} &\le \frac{10qr}{D} - 1.
\end{aligned}$$

By (IV.1), we have

$$\frac{10pr}{D} - a_{pqrs} - 1 \le \frac{10r}{D} - a_{pqrs} + 1,$$

and by (IV.3), we have

$$0 \le \frac{10(p-1)s}{D} - 2 \le \frac{10(q-1)s}{D} - 2,$$

so as long as we can choose a_{pqrs} with

$$a_{pqrs} \ge \frac{10(pq - (q-1)s)}{D} + 1,$$

we can choose a_{prs}, a_{pqs} satisfying the second and third inequalities. That such an a_{pqrs} can be chosen follows from the inequality $1 \ge pq - (q-1)s$, which can be checked by adding (IV.2) and (IV.3) and using $s \ge r$.

To check that the inequality $a_{prs} + a_{pqs} + a_{pqrs} \le \frac{10qr}{D} - 1$ can be satisfied, note that if we can choose a_{pqrs} such that one of a_{pqs}, a_{prs} can be taken to be 0 and the minimum possible value for the other is not 0, then taking both a_{pqs}, a_{prs} to be their minimum allowed values works. If the minimum values of a_{pqs}, a_{prs} are always both 0, then we take a_{pqrs} to be as small as possible, and we see that this works by $\frac{10qr}{D} - 1 \ge 0$, which is (IV.4). Finally, if neither of a_{pqs}, a_{prs} can ever be 0, then we take $a_{pqrs} = \frac{10}{D} + 1$ and take a_{pqs}, a_{prs} as small as possible, which works by (IV.2).

4.1.5 Range V (second new sieve)

Range V is defined by

$$10(p-1)s - 5(pq + pr - qr - 1) \le (p-1)(q-1)(r-1)(s-1) - ps - qr + p + q + r + s - 2, \tag{V.1}$$

$$(p-1)(q-1)(r-1)(s-1) - ps - qr + p + q + r + s - 2 \le 5(pq + pr - qr - 1). \tag{V.2}$$

The optimal λ_ds are

$$\lambda_d = \begin{cases} 1 & d \in \{1, pq, pr, qs, rs\}, \\ -1 & d \in \{p, q, r, s, pqrs\}, \\ 0 & d \in \{ps, qr, pqr, pqs, prs, qrs\}, \end{cases}$$

and the correspoding y is

$$y = \frac{10pqrs}{D}, \quad D = (p-1)(q-1)(r-1)(s-1) - ps - qr + p + q + r + s - 2.$$

In the interior of this range, the set of optimal a_ds is four dimensional. In terms of $a_{pqr}, a_{pqs}, a_{prs}, a_{qrs}$, the a_ds are given by

$$\begin{aligned} a_{ps} &= 0, \\ a_{pqrs} &= \frac{10}{D} + 1, \\ a_{rs} &= \frac{10(pq-1)}{D} - a_{prs} - a_{qrs} - 2, \\ a_s &= \frac{10(pqr - pq - pr + 1)}{D} + a_{qrs} + 4, \end{aligned}$$

with the remaining a_ds given by applying powers of the cyclic permutation $(p\ q\ s\ r)$ to the above equations. The variables $a_{pqr}, a_{pqs}, a_{prs}, a_{qrs}$ need to satisfy the inequalities

$$\begin{aligned} \max\left\{0, \frac{10(p-1)}{D} - 2\right\} \le a_{qrs} &\le \frac{10(p-1)}{D}, \\ \frac{10(qr-1)}{D} - 2 \le a_{pqs} + a_{prs} &\le \frac{10(qr-1)}{D}, \\ a_{prs} + a_{qrs} &\le \frac{10(pq-1)}{D} - 2, \end{aligned}$$

and all of their cyclically permuted (by powers of $(p\ q\ s\ r)$) analogues (note that the upper bound in the second line follows from the upper bounds in cyclic analogues of the first line, and is therefore redundant). One can show that (V.1) and (V.2) are necessary fairly directly from these inequalities. Additionally, one can easily show that

$$\begin{aligned} a_{pqr} &\ge \frac{10p(s-r)}{D} + a_{pqs}, \\ a_{pqr} &\ge \frac{10p(s-q)}{D} + a_{prs}, \\ a_{pqs} &\ge \frac{10r(q-p)}{D} + a_{qrs}, \\ a_{pqs} &\ge \frac{10q(r-p)}{D} + a_{qrs}, \end{aligned}$$

and that these inequalities show that the two inequalities $a_{qrs} \geq \max\{0, \frac{10(p-1)}{D} - 2\}$ and $a_{pqr} \leq \frac{10(s-1)}{D}$ imply all their cyclically permuted analogues.

To see that (V.1) and (V.2) are sufficient, note that if we take

$$\begin{aligned} a_{qrs} &= \frac{5(pq+pr-qr-1)}{D} - 1, \\ a_{prs} &= \frac{5(pq+qr-pr-1)}{D} - 1, \\ a_{pqs} &= \frac{5(pr+qr-pq-1)}{D} - 1, \\ a_{pqr} &= \frac{5(2ps+qr-pq-pr-1)}{D} - 1, \end{aligned}$$

then all the inequalities involving sums of two of $a_{pqr}, a_{pqs}, a_{prs}, a_{qrs}$ are automatically satisfied, (V.1) is equivalent to $0 \leq a_{qrs}$, (V.2) is equivalent to $a_{pqr} \leq \frac{10(s-1)}{D}$, and (V.2) implies that $\frac{10(p-1)}{D} - 2 \leq \frac{10(p-1)s}{D} - 2 \leq a_{qrs}$.

The basic principle behind this sieve is given in the following proposition.

Proposition 13. *Let $G = (V, E)$ be a graph with vertex set equal to the set of primes below z, and let $C_{\min}$ be the set of minimal cycles (that is, cycles having no chords) of G. Then*

$$\mathcal{S}(A, z) \geq |A| - \sum_{p \in V} |A_p| + \sum_{\{p,q\} \in E} |A_{pq}| - \sum_{\{p_1, \ldots, p_k\} \in C_{\min}} |A_{p_1 \cdots p_k}|.$$

We can also make an iterative version of this inequality. So far I haven't found any case where it is useful.

4.1.6 Range VI (combinatorial)

Range VI is defined by

$$4s \leq qrs - qr - qs - rs, \tag{VI.1}$$

$$4(pq + pr - qr - 1) \leq (p-1)(qrs - qr - qs - rs), \tag{VI.2}$$

$$(p-1)(qrs - qr - qs - rs) \leq 8qr. \tag{VI.3}$$

The optimal λ_ds are given by

$$\lambda_d = \begin{cases} \mu(d) & d \in \{1, p, q, r, s, pq, pr, ps\}, \\ 0 & \text{else}, \end{cases}$$

and the corresponding y is

$$y = \frac{8pqrs}{D}, \quad D = (p-1)(qrs - qr - qs - rs).$$

In the interior of the range, the set of optimal a_ds is four dimensional. In terms of $a_{pqr}, a_{pqs}, a_{prs}, a_{pqrs}$, the other a_ds are given by

$$\begin{aligned} a_{qrs} &= 0, \\ a_{rs} &= 0, \\ a_{ps} &= \frac{8qr}{D} - a_{pqs} - a_{prs} - a_{pqrs} - 1, \\ a_p &= \frac{8}{p-1} + a_{pqr} + a_{pqs} + a_{prs} + 2a_{pqrs} + 4, \\ a_s &= \frac{8qr}{qrs - qr - qs - rs} + 2, \end{aligned}$$

with the remaining a_ds given by permuting q, r, s in the above equations. The variables $a_{pqr}, a_{pqs}, a_{prs}, a_{pqrs}$ need to satisfy the inequalities

$$\begin{aligned} \max\left\{0, \frac{8p}{D} - 1\right\} \le a_{pqrs} \le \frac{8}{D} + 1, \\ \max\left\{0, \frac{8ps}{D} - a_{pqrs} - 1\right\} \le a_{pqr} \le \frac{8s}{D} - a_{pqrs} + 1, \\ a_{pqs} + a_{prs} + a_{pqrs} \le \frac{8qr}{D} - 1, \end{aligned}$$

and all of their analogues under permuting q, r, s. Using (VI.1) we see that the first two groups of inequalities can be satisfied. For the last group of inequalities, if it is possible to take two of $a_{pqr}, a_{pqs}, a_{prs}$ equal to 0, then doing so and taking the remaining variables as small as possible works by (VI.3). Otherwise, we may as well take $a_{pqrs} = \frac{8}{D} + 1$, in which case taking $a_{pqr}, a_{pqs}, a_{prs}$ as small as possible works by (VI.2).

4.1.7 Ranges VII - X (all combinatorial)

The remaining ranges are all fairly simple, so I'll just summarize. Range VII is given by

$$9qr \le (p-1)(q-1)(r-1)s - pqr \le \frac{9}{2}(p-1)s, \tag{VII}$$

with optimal λ_d given by $\mu(d)$ for $d \in \{1, p, q, r, s, pq, pr, qr\}$ and $\lambda_d = 0$ otherwise. There is just one optimal choice for the a_ds, with the nonzero a_ds given by

$$a_{pqr} = \frac{9s}{D} + 1, \quad a_{qr} = \frac{9(p-1)s}{D} - 2, \quad a_s = \frac{9pqr}{D} + 1, \quad a_r = \frac{9(p-1)(q-1)}{D} + 4,$$

and their analogues under permuting p, q, r (here $D = (p-1)(q-1)(r-1)s - pqr$).

Range XIII is given by

$$\max\{\tfrac{7}{2}(p-1)s, 7qr\} \leq pqrs - pqr - pqs - prs - qrs + qs + rs \leq 7qs, \tag{VIII}$$

with optimal λ_d given by $\mu(d)$ for $d \in \{1, p, q, r, s, pq, pr\}$ and $\lambda_d = 0$ otherwise. There is a one dimensional family of optimal a_ds, with the nonzero a_ds given in terms of a_{pqr} by

$$a_{pr} = \frac{7qs}{D} - a_{pqr} - 1, \quad a_s = \frac{7pqr}{D} + 1, \quad a_r = \frac{7(p-1)qs}{D} + 2, \quad a_p = \frac{7(qr-q-r)s}{D} + a_{pqr} + 3,$$

and their analogues under swapping q and r (here $D = pqrs - pqr - pqs - prs - qrs + qs + rs$). The variable a_{pqr} needs to satisfy the inequality

$$\max\{0, \tfrac{7ps}{D} - 1\} \leq a_{pqr} \leq \frac{7s}{D} + 1.$$

Range IX is given by

$$6qs \leq pqrs - pqr - pqs - prs - qrs + rs \leq 6rs, \tag{IX}$$

with optimal λ_d given by $\mu(d)$ for $d \in \{1, p, q, r, s, pq\}$ and $\lambda_d = 0$ otherwise. There is just one optimal choice of optimal a_ds.

Range X is given by

$$5rs \leq pqrs - pqr - pqs - prs - qrs, \tag{X}$$

with optimal λ_d given by $\mu(d)$ for $d \in \{1, p, q, r, s\}$ and $\lambda_d = 0$ otherwise. There is just one optimal choice of optimal a_ds.

4.2 Model problem - all primes have the same size

We will try to understand the asymptotics of the sifting limit β_κ as the sifting dimension κ goes to infinity, by studying a model sifting problem introduced by Selberg in Section 13 of [28], in which all of the primes have roughly the same size. One possible motivation for this is the intuition that the way we handle the large primes seems to have the most important effects on the asymptotic behavior of the sifting functions when κ gets large (this intuition will be better motivated after we see the algorithm for computing the sifting functions $F_\kappa(s), f_\kappa(s)$).

More precisely, let A be the interval $[1, y]$ and let $\mathcal{P}$ be a set of primes such that there is a number R with the property that the product of any R primes from $\mathcal{P}$ is below y, but the product of any $R+1$ primes from $\mathcal{P}$ is greater than y (note that R is within 1 of the parameter s which appears in

the usual sifting problem). Define a new parameter v, analogous to κ, by

$$v = \sum_{p \in \mathcal{P}} \frac{\kappa_p}{p}.$$

It isn't hard to see that the bounds we can get on $\mathcal{S}([1, y], \mathcal{P})$ only depend on the quantities v and R, since by an averaging argument we may assume without loss of generality that the sieve weights λ_d depend only on $\omega(d)$, the number of prime factors of d. For this reason we will switch the indices on our sieve weights from d to $\omega(d)$, so we need to optimize only $\lambda_0, ..., \lambda_R$, with $\lambda_0 = 1$. We make the definition

$$\theta(n) = \sum_{i=0}^{R} \lambda_i \binom{n}{i}.$$

Thus, the upper bound sieve reduces to trying to minimize the quantity

$$\sum_{n \geq 0} \frac{\theta(n)}{n!} v^n = e^v \sum_{n=0}^{R} \frac{\lambda_n}{n!} v^n$$

subject to the constraint $\theta(n) \geq 0$ for $n \in \mathbb{N}$. Similarly, the lower bound sieve reduces to trying to maximize the same quantity subject to the constraint $\theta(n) \leq 0$ for $n \in \mathbb{N}^+$. For every R, we let v_R be the largest v such that the optimal lower bound is nonnegative. Note that for the purpose of computing v_R, we can ignore the normalization $\lambda_0 = 1$.

Selberg [28] shows that $\lfloor \frac{R+1}{2} \rfloor \leq v_R \leq R$ (this is equation (13.22‴) of Section 13 of [28]), and that for any v, R the optimal θ takes the form

$$\theta(n) = \prod_i \left(1 - \frac{n}{\nu_i}\right)\left(1 - \frac{n}{\nu_i + 1}\right)$$

with $\nu_i \in \mathbb{N}$ for the upper bound sieve, and

$$\theta(n) = (1 - n) \prod_i \left(1 - \frac{n}{\nu_i}\right)\left(1 - \frac{n}{\nu_i + 1}\right)$$

with $\nu_i \in \mathbb{N}$ for the lower bound sieve (these are equations (13.6) and (13.6′) of Section 13 of [28]). Furthermore, Selberg [28] shows that each $\nu_i \leq \max(2R + 2v, R + 4v)$ (this is equation (13.8) of Section 13 of [28]), so for any v, R the optimal θ can be found with a finite amount of computation. An algorithm for computing the optimal θ given v, R and for computing v_R given R is described in Algorithm 1. In practice, once R gets large rounding errors start to accumulate when floating point arithmetic is used. The basic result behind the correctness of this algorithm is given in the following proposition.

Proposition 14. *For $R \in \mathbb{N}$ and $v \geq 0$, suppose that the polynomial θ has degree R, satisfies*

$\theta(0) = 1$, has $(-1)^R\theta(n) \geq 0$ for $n \in \mathbb{N}^+$, has R distinct positive integer roots, and has the property that whenever we change just one root of θ we either fail to satisfy one of the previously mentioned properties of θ or we increase the quantity

$$M_{v,R}(\theta) = (-1)^R \sum_{n \geq 0} \frac{\theta(n)}{n!} v^n.$$

Then in fact θ minimizes $M_{v,R}(\theta)$ among all polynomials of degree R satisfying $\theta(0) = 1$ and $(-1)^R\theta(n) \geq 0$ for $n \in \mathbb{N}^+$.

Proof. The set of coefficient vectors of polynomials θ of degree R satisfying $\theta(0) = 1$ and $(-1)^R\theta(n) \geq 0$ for $n \in \mathbb{N}^+$ forms a convex set, call it $\mathcal{C}_R$, bounded by hyperplanes corresponding to positive integers which might be roots of θ. Any interior point of $\mathcal{C}_R$ can be replaced by a vertex of $\mathcal{C}_R$ (that is, a point where R bounding hyperplanes of $\mathcal{C}_R$ meet, corresponding to a polynomial with R distinct positive integer roots) without decreasing $M_{v,R}(\theta)$ by replacing negative roots of θ by roots at 1, replacing pairs of complex conjugate roots of θ by their real parts, and migrating non-integral real roots or double roots of θ either upwards or downwards until they hit an integer. Furthermore, $M_{v,R}(\theta)$ is bounded below by $(-1)^R$ for θ with coefficient vector in $\mathcal{C}_R$, so there can be no rays in $\mathcal{C}_R$ which point in a direction which strictly decreases $M_{v,R}$.

Call two vertices of $\mathcal{C}_R$ *adjacent* if the segment connecting them is a 1-dimensional face of $\mathcal{C}_R$. For θ corresponding to a vertex of $\mathcal{C}_R$, the adjacent vertices correspond to the polynomials obtained by moving just one root of θ from one positive integer to another positive integer. Considering the cone around this vertex, which is defined by the R hyperplanes corresponding to the roots of θ, we see that if $M_{v,R}(\theta)$ is not minimal, then there is some one dimensional face of $\mathcal{C}_R$ which meets θ, such that $M_{v,R}$ strictly decreases as we move away from θ along this edge - so since this edge can't be an infinite ray, it must terminate in an adjacent vertex of $\mathcal{C}_R$. □

Values of v_R and the corresponding roots ν_i and sieve weights λ_n are given for some small R in the following table.

Algorithm 1 Find optimal θ, find v_R

function WEIGHTS(R, $\nu_1, ..., \nu_d$)
  if R odd **then** ▷ parity of R determines whether an upper or lower bound sieve
    $\theta(n) \leftarrow (1-n)\prod_{i=1}^{d}(1-\frac{n}{\nu_i})(1-\frac{n}{\nu_i+1})$ for $n = 0, ..., R$
  else
    $\theta(n) \leftarrow \prod_{i=1}^{d}(1-\frac{n}{\nu_i})(1-\frac{n}{\nu_i+1})$ for $n = 0, ..., R$
  $\lambda_n \leftarrow \theta(n)$ for $n = 0, ..., R$
  for $i = 0$ **to** R **do**
    for $j = R$ **to** $i+1$ **do**
      $\lambda_j \leftarrow \lambda_j - \lambda_{j-1}$
  return $(\lambda_0, ..., \lambda_R)$
function MAINTERM(v, R, $\nu_1, ..., \nu_d$)
  $(\lambda_0, ..., \lambda_R) \leftarrow$ WEIGHTS(R, $\nu_1, ..., \nu_d$)
  return $e^v \sum_{n=0}^{R} \frac{\lambda_n}{n!} v^n$ ▷ alternatively, approximate this by $\sum_{n \le 10(R+v)} \frac{\theta(n)}{n!} v^n$
function BESTTHETA(v, R)
  $d \leftarrow \lfloor \frac{R}{2} \rfloor$
  $\nu_i \leftarrow 2i - \mathbf{1}_{2|R}$ for $i = 1, ..., d$
  while $\exists i \le d$, $\pm \in \{+, -\}$ **such that** $(-1)^R$MAINTERM(v, R, $\nu_1, ..., \nu_i \pm 1, ..., \nu_d$) $> (-1)^R$ MAINTERM(v, R, $\nu_1, ..., \nu_d$) **do**
    $\nu_i \leftarrow \nu_i \pm 1$
    while $\nu_{i\pm1} = \nu_i \pm 1$ **do** ▷ push adjacent roots out of the way
      $i \leftarrow i \pm 1$
      $\nu_i \leftarrow \nu_i \pm 1$
  return $\{\nu_1, ..., \nu_d\}$
function $v_R(R)$ ▷ assume R odd, otherwise decrease it by 1
  $d \leftarrow \frac{R-1}{2}$
  $\nu_i \leftarrow 2i$ for $i = 1, ..., d$
  $v \leftarrow 0$
  while MAINTERM(v, R, $\nu_1, ..., \nu_d$) > 0 **do**
    Increase v until MAINTERM(v, R, $\nu_1, ..., \nu_d$) $= 0$. ▷ e.g. using Newton's method
    $\{\nu_1, ..., \nu_d\} \leftarrow$ BESTTHETA(v, R)
  return v

R	v_R	$\nu_1, ..., \nu_{(R-1)/2}$	$\lambda_0, ..., \lambda_R$
1	1		$1, -1$
3	2	3 *or* 4	$1, -1, \frac{5}{6}, -\frac{1}{2}$ *or* $1, -1, \frac{7}{10}, -\frac{3}{10}$
5	3.11714	$3, 7$	$1, -1, 0.91, -0.73, 0.46, -0.17$
7	4.14377	$3, 6, 11$	$1, -1, 0.94, -0.83, 0.67, -0.46, 0.24, -0.07$
9	5.23808	$3, 6, 10, 14$	$1, -1, 0.96, -0.88, 0.76, -0.61, 0.44, -0.26, 0.12, -0.03$
11	6.29164	$3, 6, 9, 13, 18$	$1, -1, 0.97, -0.91, 0.82, -0.71, 0.58, -0.43, 0.28, -0.15, ...$
13	7.30904	$3, 6, 9, 13, 17, 22$	$1, -1, 0.97, -0.93, 0.86, -0.76, 0.65, -0.52, 0.39, -0.26, ...$
15	8.33758	$3, 6, 9, 12, 16, 20, 25$	$1, -1, 0.98, -0.94, 0.88, -0.81, 0.72, -0.61, 0.50, -0.38, ...$
17	9.31968	$3, 6, 9, 12, 15, 19, 24, 29$	$1, -1, 0.98, -0.95, 0.90, -0.84, 0.76, -0.67, 0.57, -0.47, ...$
19	10.3236	$3, 6, 8, 11, 15, 18, 22, 27, 33$	$1, -1, 0.98, -0.96, 0.92, -0.87, 0.82, -0.75, 0.67, -0.58, ...$
21	11.3495	$3, 5, 8, 11, 14, 18, 22, 26, 31, 37$	$1, -1, 0.99, -0.97, 0.94, -0.91, 0.86, -0.81, 0.75, -0.68, ...$
23	12.4042	$3, 5, 8, 11, 14, 17, 21, 25, 29, 34, 41$	$1, -1, 0.99, -0.97, 0.95, -0.92, 0.88, -0.84, 0.78, -0.72, ...$
25	13.4494	$3, 5, 8, 11, 14, 17, 21, 24, 28, 33, 38, 44$	$1, -1, 0.99, -0.97, 0.95, -0.93, 0.89, -0.85, 0.81, -0.75, ...$
201	102.22	$3, 5, 7, 9, 12, 14, 16, 19, 21, 23, 26, ...$	...
1001	≈ 503.37	$3, 5, 7, 9, 11, 13, 15, 17, 20, 22, 24, ...$	...
2001	≈ 1004	...	...

Based on the numerical data, the following conjecture seems plausible.

Conjecture 2. In the model sifting problem, the optimal λ_ns always satisfy

$$(-1)^n \lambda_n \geq 0$$

and

$$1 = |\lambda_0| \geq |\lambda_1| \geq \cdots .$$

4.2.1 The combinatorial range, and coincidences at $v = 1$

It's easy to see that for R fixed (and assuming that the parity of R is determined by whether we are looking for an upper bound sieve or a lower bound sieve) v sufficiently small, the optimal sieve is combinatorial - that is, it has $\theta(n) = 0$ for $n = 1, ..., R$, with sieve weights given by $\lambda_i = (-1)^i$ for $i \leq R$. Thus there is some least v, possibly depending on R, such that the combinatorial sieve is no longer optimal.

In a surprise twist, this crossover point always happens at $v = 1$ regardless of the value of R: we have an infinite pileup of coincidences all occuring at one critical value. Before I prove this result, note that in the original sifting problem it is conjectured that for $\kappa \leq 1$ the best upper and lower bound sieves are the β-sieves, which have $\lambda_d \in \{\mu(d), 0\}$ for all d. In the last chapter of this thesis, I'll strengthen the analogy further by generalizing the infinite pileup of coincidences at $v = 1$ from

the model problem to an infinite pileup of coincidences all occuring at $\kappa = 1$ in the full sifting problem.

Theorem 20. *For $R \in \mathbb{N}$ and $0 \leq v < 1$, the polynomial θ of degree R which satisfies $\theta(0) = 1$, $(-1)^R\theta(n) \geq 0$ for $n \in \mathbb{N}^+$ and, given these constraints, minimizes the quantity*

$$M_{v,R}(\theta) = (-1)^R \sum_{n\geq 0} \frac{\theta(n)}{n!} v^n$$

is the combinatorial polynomial

$$\theta_0(n) = \sum_{i=0}^{R} (-1)^i \binom{n}{i} = \prod_{i=1}^{R} \Big(1 - \frac{n}{i}\Big) = (-1)^R \binom{n-1}{R}.$$

For $R \geq 2$ and $1 < v < 2$, the optimal θ is instead given by

$$\begin{aligned}\theta_1(n) &= \prod_{i=1}^{R-2} \Big(1 - \frac{n}{i}\Big) \cdot \Big(1 - \frac{n}{R}\Big)\Big(1 - \frac{n}{R+1}\Big) \\ &= \sum_{i=0}^{R-2} (-1)^i \binom{n}{i} + (-1)^{R-1}\Big(1 - \frac{1}{\binom{R+1}{2}}\Big)\binom{n}{R-1} + (-1)^R \frac{R-1}{R+1}\binom{n}{R}.\end{aligned}$$

Proof. By Proposition 14, we just need to check that $M_{v,R}(\theta)$ can't be decreased by moving just one root of θ from its current position to another positive integer. First we focus on the range $0 \leq v < 1$. Since $1, ..., R$ are already roots of θ, the only moves that can be made are moves that flip one of the roots $R-1, R-3, ...$ from its current value to $R+1$. Set

$$\theta_k(n) = \frac{1 - \frac{n}{R+1}}{1 - \frac{n}{R+1-2k}} \cdot (-1)^R \binom{n-1}{R} = \prod_{\substack{1\leq i\leq R+1 \\ i\neq R+1-2k}} \Big(1 - \frac{n}{i}\Big)$$

for $k = 0, ..., \lfloor \frac{R}{2} \rfloor$. We just need to show that $M_{v,R}(\theta_0) < M_{v,R}(\theta_k)$ for each $k \leq \frac{R}{2}$ when $v < 1$. We

have

$$\begin{aligned}
M_{v,R}(\theta_k - \theta_0) &= (-1)^R \frac{\theta_k(R+1-2k)}{(R+1-2k)!} v^{R+1-2k} - \sum_{n \neq R+1-2k} \left(1 - \frac{1 - \frac{n}{R+1}}{1 - \frac{n}{R+1-2k}}\right) \binom{n-1}{R} \frac{v^n}{n!} \\
&= \frac{(2k)!}{(R+1)!} v^{R+1-2k} - \sum_{n \neq R+1-2k} \frac{2kn}{(R+1)(n-R-1+2k)} \binom{n-1}{R} \frac{v^n}{n!} \\
&= \frac{(2k)!}{(R+1)!} v^{R+1-2k} - \sum_{n \geq R+1} \frac{2k}{(R+1)!(n-R-1)!(n-R-1+2k)} v^n \\
&= \frac{v^{R+1}}{(R+1)!} \left(\frac{(2k)!}{v^{2k}} - \sum_{n \geq 0} \frac{2k}{n!(n+2k)} v^n \right) \\
&= \frac{v^{R+1}}{(R+1)!} \frac{(2k)!}{v^{2k}} M_{v,2k-1}\Big(n \mapsto \binom{n-1}{2k-1}\Big) \\
&= \frac{e^v v^{R+1}}{(R+1)!} \frac{(2k)!}{v^{2k}} \sum_{n \leq 2k-1} \frac{(-v)^n}{n!}.
\end{aligned}$$

When $v \leq 1$, pairing up the summands shows that $\sum_{n \leq 2k-1} \frac{(-v)^n}{n!} \geq 0$, and that the inequality is strict for $k > 1$.

Next, we consider the case $1 < v < 2$. If we change just one root of θ_1, we can make it into θ_k for $k = 0, 2, ..., \lfloor \frac{R}{2} \rfloor$, or we can make it into θ', which is given by

$$\theta'(n) = \prod_{i=1}^{R-2} \Big(1 - \frac{n}{i}\Big) \cdot \Big(1 - \frac{n}{R+1}\Big)\Big(1 - \frac{n}{R+2}\Big).$$

We already know that $M_{v,R}(\theta_1) < M_{v,R}(\theta_0)$ for $v > 1$. For $k \geq 2$ we have

$$M_{v,R}(\theta_k - \theta_1) = \frac{e^v v^{R+1}}{(R+1)!} \Big(\frac{(2k)!}{v^{2k}} \sum_{n \leq 2k-1} \frac{(-v)^n}{n!} - \frac{2!}{v^2}(1-v) \Big),$$

and for $k \geq 3$ and $v < 2$, by standard alternating series arguments we have

$$\sum_{n \leq 2k-1} \frac{(-v)^n}{n!} > e^{-v} - \frac{v^{2k}}{(2k)!} > e^{-2} - \frac{2^6}{6!} > 0.$$

For $k = 2$, we need to check that

$$\frac{24}{v^4}\Big(1 - v + \frac{v^2}{2} - \frac{v^3}{6}\Big) > \frac{2}{v^2}(1-v)$$

for $v < 2$, which is straightforward: the difference of the two sides is $2v^{-4}(2-v)(3(2-v)+v^2) > 0$.

To finish, we just need to check that $M_{v,R}(\theta_1) < M_{v,R}(\theta')$ for $1 < v < 2$. Writing θ' in the

binomial basis, we get

$$\theta'(n) = \sum_{i=0}^{R-2}(-1)^i\binom{n}{i} + (-1)^{R-1}\Big(1 - \frac{R}{\binom{R+2}{3}}\Big)\binom{n}{R-1} + (-1)^R\frac{R(R-1)}{(R+1)(R+2)}\binom{n}{R},$$

so

$$\begin{aligned} M_{v,R}(\theta' - \theta_1) &= M_{v,R}\Big((-1)^R\Big(\frac{R}{\binom{R+2}{3}} - \frac{1}{\binom{R+1}{2}}\Big)\binom{n}{R-1} + (-1)^R\Big(\frac{R(R-1)}{(R+1)(R+2)} - \frac{R-1}{R+1}\Big)\binom{n}{R}\Big) \\ &= e^v \cdot \Big(\frac{2(R-1)}{\binom{R+1}{2}(R+2)}\frac{1}{(R-1)!}v^{R-1} - \frac{2(R-1)}{(R+1)(R+2)}\frac{1}{R!}v^R\Big) \\ &= e^v \cdot \frac{2(R-1)}{(R+2)!}v^{R-1}(2-v), \end{aligned}$$

which is greater than 0 when $v < 2$. □

4.2.2 Why is Selberg's lower bound sieve so effective?

First we will describe the analogue of Selberg's lower bound sieve in this setting.

Let $R = 2d + 1$. In order to show that $v_R \geq d + 1$, Selberg [28] finds the optimal θ of the form

$$\theta(n) = (1-n)f(n)^2.$$

If we write

$$f(n) = \sum_i \ell_i\binom{n}{i},$$

and define y_i, Δ_i by

$$y_r = (-1)^r\sum_{i\geq 0}\frac{\ell_{r+i}}{i!}v^i,$$

and $\Delta_r = y_r - y_{r+1}$, then we find that

$$e^{-v}\sum_{n\geq 0}\frac{(1-n)f(n)^2}{n!}v^n = \sum_r \frac{v^r}{r!}y_r^2 - \sum_r \frac{v^{r+1}}{r!}\Delta_r^2.$$

Since $y_r = \Delta_r + \cdots + \Delta_d$, we can apply Cauchy-Schwarz to see that

$$y_r^2 \leq (d+1-r)(\Delta_r^2 + \cdots + \Delta_d^2),$$

with equality when the Δs are all equal. Substituting this in, we see that

$$\sum_r \frac{v^r}{r!} y_r^2 - \sum_r \frac{v^{r+1}}{r!}\Delta_r^2 \le \sum_r \frac{v^r}{r!}(d+1-r)(\Delta_r^2+\cdots+\Delta_d^2) - \sum_r \frac{v^{r+1}}{r!}\Delta_r^2$$
$$= (d+1-v)\sum_j \Delta_j^2 \sum_{r\le j} \frac{v^r}{r!}.$$

Thus we see that the Selberg lower bound sieve gives a nonnegative lower bound if and only if $v \le d+1$, and in particular that $v_R \ge d+1$. Furthermore, when $v = d+1$, the optimal sieve has all Δs equal. Thus we substitute $y_r \asymp d+1-r$, so

$$\ell_r \asymp (-1)^r \sum_{i=0}^{d+1-r} \frac{d+1-r-i}{i!} v^i.$$

In order to normalize $f(n)$, we need $\ell_0 = 1$ (note, however, that the normalization doesn't actually matter if all we care about is whether we get a nonnegative lower bound). When $r = 0$ and $v = d+1$, the right hand side of the above becomes

$$\sum_{i=0}^{d+1} \frac{d+1-i}{i!}(d+1)^i = \sum_{i=0}^{d+1} \frac{(d+1)^{i+1}}{i!} - \frac{(d+1)^i}{(i-1)!} = \frac{(d+1)^{d+1}}{d!},$$

so when $v = d+1$ we get

$$\ell_r = (-1)^r \frac{d!}{(d+1)^{d+1}} \sum_{i=0}^{d+1-r} \frac{d+1-r-i}{i!}(d+1)^i.$$

In the next few subsections, we'll show that $\lim \frac{R}{v_R} = 2$, and bounds the difference between v_R and $\lfloor \frac{R+1}{2} \rfloor$ between the square root and the cube root of R (up to constants). Based on the analogy outlined earlier, this may be regarded as weak evidence for $\lim \frac{\beta_\kappa}{\kappa} = 2$, and possibly also as weak evidence for $2\kappa - \beta_\kappa \gg \sqrt[3]{\kappa}$.

Theorem 21. *For $R = 2d+1$, we have $2\sqrt{d} \ge v_R - (d+1) \ge (c+o(1))\sqrt[3]{d}$, where $c \approx \frac{1}{12.14}$ is the positive solution of the equation*

$$\int_0^\infty \frac{1}{x^{3/2}} \min\left(\sin^2\left((\tfrac{x}{3}+c)\sqrt{x}\right), \cos^2\left((\tfrac{x}{3}+c)\sqrt{x}\right)\right) dx = 2\pi c.$$

From the upper bound on v_R we can deduce a lower bound on the usual sifting limit β_κ, improving Selberg's lower bound by a factor of 2.

Corollary 3. *If β_κ is the sifting limit of a sieve of dimension $\kappa \geq 3$, then*

$$\beta_\kappa > \frac{2\lfloor \kappa - \sqrt{\kappa} \rfloor + 1}{e^{1+\frac{1}{\sqrt{\kappa}}}}.$$

Proof. Suppose $\beta_\kappa < 2d+3$ for some $d \in \mathbb{N}$. For any y, let $\mathcal{P}$ be the set of primes between $y^{\frac{1}{2d+3}}$ and y^{1/β_κ}. Then if we take $v = \sum_{p \in \mathcal{P}} \frac{\kappa}{p}$, we see that

$$v = (\kappa + o(1)) \log\left(\frac{2d+3}{\beta_\kappa}\right).$$

Since the product of any $2d+3$ primes from $\mathcal{P}$ is greater than y, if we can find a nontrivial lower bound sieve then we must certainly have

$$\kappa \log\left(\frac{2d+3}{\beta_\kappa}\right) \leq v_{2d+2} = v_{2d+1} \leq d + 2\sqrt{d} + 1.$$

Rearranging, we find that

$$\beta_\kappa \geq \frac{2d+3}{e^{\frac{d+2\sqrt{d}+1}{\kappa}}}.$$

To finish, we take $d = \lfloor \kappa - \sqrt{\kappa} \rfloor - 1$. □

Upper bound on v_R

Theorem 22. *Let $R = 2d+1$. Then $v_R \leq d + 2\sqrt{d} + 1$.*

Proof. Assume that $d \geq 1$, since it is easy to check we have equality for $d = 0$. Since any optimal θ takes the form $(1-n)f(n)f(n-1)$ for some polynomial f of degree d, it's enough to show that for $v = d + 2\sqrt{d} + 1$ and any polynomial f of degree d we have

$$\sum_{n \geq 0} \frac{(1-n)f(n)f(n-1)}{n!} v^n \leq 0.$$

Write

$$f(n) = \sum_{i=0}^{d} \ell_i \binom{n}{i}.$$

Define y_i, Δ_i, s_i by

$$y_r = (-1)^r \sum_{i \geq 0} \frac{\ell_{r+i}}{i!} v^i,$$

and $\Delta_r = y_r - y_{r+1}, s_r = \sum_{i \geq 0} y_{r+i}$. Using the identity

$$\binom{n}{a}\binom{n}{b} = \sum_k \frac{k!}{(k-a)!(k-b)!(a+b-k)!}\binom{n}{k},$$

we see that the variables y_r diagonalize the quadratic form corresponding to the Selberg upper bound sieve:

$$\sum_{n\geq 0}\frac{f(n)^2}{n!}v^n = e^v\sum_r \frac{y_r^2}{r!}v^r.$$

Since shifting the argument of f by ± 1 has the effect of replacing the y_rs with either the Δ_rs or the s_rs, we have

$$\sum_{n\geq 0}\frac{(1-n)f(n)f(n-1)}{n!}v^n = \sum_{n\geq 0}\frac{f(n)f(n-1)}{n!}v^n - v\sum_{n\geq 0}\frac{f(n+1)f(n)}{n!}v^n = e^v\sum_r\frac{v^r}{r!}y_r(s_r - v\Delta_r).$$

Dividing by e^v and rewriting this entirely in terms of the s_i, it becomes

$$\sum_r \frac{v^r}{r!}s_r(s_r - s_{r+1} - v(s_r - 2s_{r+1} + s_{r+2}) + r(s_{r-1} - 2s_r + s_{r+1})).$$

Comparing this to $\sum_r \frac{v^{r+1}}{r!}\Delta_r^2$, we get

$$\begin{aligned}&-2\sum_r \frac{v^r}{r!}s_r(s_r - s_{r+1} - v(s_r - 2s_{r+1} + s_{r+2}) + r(s_{r-1} - 2s_r + s_{r+1}))\\ =&\sum_r\frac{v^{r+1}}{r!}\Delta_r^2 + \sum_r\frac{v^r}{r!}\left((v-r-2)s_r^2 - 2(v-r-1)s_rs_{r+1} + (v-r)s_{r+1}^2\right).\end{aligned}$$

We just have to prove that the last sum above is nonnegative. Since $s_{d+1} = 0$, for any constant a we have

$$\begin{aligned}&\sum_r\frac{v^r}{r!}\left((v-r-2)s_r^2 - 2(v-r-1)s_rs_{r+1} + (v-r)s_{r+1}^2\right)\\ =\ &as_0^2 + \sum_r\frac{v^r}{r!}\left((v-r-2-a)s_r^2 - 2(v-r-1)s_rs_{r+1} + \left(v-r+a\frac{v}{r+1}\right)s_{r+1}^2\right).\end{aligned}$$

Thus it is enough to show that we can choose $0\leq a\leq v-d-2$ satisfying

$$(v-r-2-a)\left(v-r+a\frac{v}{r+1}\right)\geq (v-r-1)^2$$

for all $r<d$. It's easy to see that it is enough to check this for $r=d-1$, in which case it reduces to the inequality

$$(v-d)^2a \geq va^2 + (v+d)a + d.$$

Taking $a=\sqrt{\frac{d}{v}}$ and $v = d + 2\sqrt{d} + 1$, we get equality. □

Remark 1. Numerical calculations indicate that for large d the quadratic form

$$\sum_r \frac{v^r}{r!} y_r(s_r - v\Delta_r)$$

is negative definite for $v \approx d + \frac{\sqrt{d}}{2} + 1$, so the above argument is probably not best possible. The next result shows that the bounds we can get with this method can't be improved too much further.

Theorem 23. *For all d sufficiently large, if we take $v = d + \sqrt{\frac{d}{11}} + 1$,*

$$y_r = d + 1 - r - \frac{1}{\sqrt{2d}} \binom{d+2-r}{2},$$

and define $\Delta_r = y_r - y_{r+1}$, $s_r = \sum_{i=0}^{d-r} y_{r+i}$, then we have

$$\sum_{r=0}^{d} \frac{v^r}{r!} y_r(s_r - v\Delta_r) > 0.$$

Proof. Generally, if we let $k = v - (d+1)$ and take $y_r = d + 1 - r + a\binom{d+2-r}{2}$, then after a lengthy computation we find that

$$\begin{aligned}\sum_{r=0}^{d} \frac{v^r}{r!} y_r(s_r - v\Delta_r) = \left(\sum_{r=0}^{d} \frac{v^r}{r!}\right)\Bigg(&-\frac{1}{2}k(d+k^2+1) - \frac{1}{12}\left(3(d+1)^2 - 6k^2(2d+1) - 5k^4 + 16k(d+1)\right) a \\ &+ \frac{1}{12}\left(3k(d+1)^2 - k^3(4d-2) - k^5 + 2(d+1)^2 + 14k^2(d+1)\right) a^2\Bigg) \\ + \frac{v^{d+1}}{d!}\Bigg(&\frac{1}{2}k(k-1) - \frac{1}{12}\left(7kd + 5k^2(k-1) - 3(d+1) + 11k\right) a \\ &- \frac{1}{12}\left(d(4d+21) - k^2(3d-1) - k^4 + 13k(d+1) + k^3 - 13\right) a^2\Bigg).\end{aligned}$$

If k is within a constant factor of $\sqrt{d}$, we have the approximation

$$\frac{d!}{v^d}\sum_{r=0}^{d} \frac{v^r}{r!} = \Gamma(d+1, v)v^{-d}e^v = \operatorname{erfc}\left(\frac{k}{\sqrt{2d}}\right) e^{\frac{k^2}{2d}}\sqrt{\frac{\pi d}{2}} + O(1).$$

Plugging in $d = 11k^2$ and $a = -\frac{1}{k\sqrt{22}}$ and expanding everything to first order in k, we get the theorem. □

Remark 2. The preceding Theorem should be seen as a limitation of our method of producing upper bounds, rather than an indication that $v_R - (d+1) \gg \sqrt{d}$. Numerical calculations show that the roots of the corresponding polynomial f are almost equal to the roots of the polynomial Selberg

constructed to show $v_R \geq d+1$, except that the smallest root is approximately $\frac{5}{2}$ instead of being approximately 3. It appears that this change to the smallest root alone accounts for most of the improvement to v, and it is only permitted since we have relaxed the condition that $\theta(n) \leq 0$ for positive integers n to the much less restrictive condition that the roots of θ come in pairs that differ by at most 1.

It would be interesting to see if better upper bounds on v_R could be produced by incorporating the constraint that for every k the kth root of f is at least $2k+1$ (using the result of the next section).

Lower bound on v_R

Recall that when $v = d+1$, the Selberg lower bound sieve corresponds to taking θ of the form

$$\theta(n) = (1-n)f(n)^2,$$

where f is an arbitrary degree d polynomial with $f(0) = 1$, chosen to minimize

$$M_{v,R}(\theta) = -\sum_{n \geq 0} \frac{\theta(n)}{n!}(d+1)^n,$$

and that the optimal choice for f is given by

$$f(n) = \sum_{i=0}^{n} \ell_i \binom{n}{i}$$

with

$$\ell_r = (-1)^r \frac{d!}{(d+1)^{d+1}} \sum_{i=0}^{d+1-r} \frac{d+1-r-i}{i!}(d+1)^i.$$

We want to describe the behavior of the roots $\nu_1, ..., \nu_d$ of $f(n) = \sum_i \ell_i \binom{n}{i}$ as d gets large, so that we can determine the effects of rounding them to the nearest integer values.

Proposition 15. *The roots $\nu_1, ..., \nu_d$ of f are all real, positive, and greater than 2. For any integer n, the closed interval $[n, n+1]$ contains at most one root ν_i.*

Proof. These will all follow from the fact that f is chosen to minimize $M_{v,R}(\theta)$. If f had a negative real root, then replacing it with any positive root would decrease $M_{v,R}(\theta)$ (since doing this would decrease $|\theta(n)|$ for all $n \in \mathbb{N}^+$). Similarly, if f had a pair of complex conjugate roots, then replacing them by their real parts would decrease $M_{v,R}(\theta)$. If f has a positive root $\nu_i \leq 2$, then increasing it by a tiny amount ϵ decreases some $|\theta(n)|$ by an amount proportional to ϵ, and at most increases $|\theta(2)|$ by an amount proportional to ϵ^2, so if ϵ is small enough then increasing ν_i to $\nu_i + \epsilon$ decreases $M_{v,R}(\theta)$. Finally, if there is an integer n such that the interval $[n, n+1]$ contains two roots ν_i, ν_j,

then if we increase their sum $\nu_i + \nu_j$ by ϵ while keeping their product $\nu_i\nu_j$ constant, then we will decrease $|\theta(m)|$ by an amount proportional to ϵ for all $m \in \mathbb{N}^+$ with $m \neq n, n+1$, and we will at most increase $|\theta(n)|, |\theta(n+1)|$ by an amount proportional to ϵ^2, so if ϵ is small enough the overall effect is to decrease $M_{v,R}(\theta)$. □

Corollary 4. *If n is an integer with $f(n)f(n+2) < 0$, then the interval $(n, n+2)$ contains exactly one root ν_i, and whether ν_i is above or below $n+1$ is determined by the sign of $f(n+1)$.*

Remark 3. Numerical calculations indicate that if we sort the roots $\nu_1, ..., \nu_d$ of f, we even have $\nu_{i+1} > \nu_i + 2$ for every i. More detailed information about the roots of f can be found in the appendix.

Proposition 16. *Let n be a nonnegative integer. Then*

$$f(n+2) = \sum_k \frac{(-1)^k}{(d+1)^{k+1}} k! \binom{d}{k} \binom{n}{k}.$$

Proof. Recall that we had

$$\ell_r = (-1)^r \sum_{i=0}^{d+1-r} \frac{y_{r+i}}{i!}(d+1)^i,$$

with the $y_r = \frac{d!}{(d+1)^{d+1}} \cdot (d+1-r)$ in an arithmetic progression.

Every time we shift the argument of f by 1, we replace the y_rs with their differences. Since the y_rs are linear, after shifting the argument of f twice all but the last of them is 0, which gives us

$$f(n+2) = \frac{d!}{(d+1)^{d+1}} \sum_k \frac{(-1)^k}{(d-k)!}(d+1)^{d-k} \binom{n}{k}.$$

Rearranging this finishes the proof. □

Proposition 17. *Let $a(n,k)$ be the number of permutations of an n-set having exactly k cycles of size greater than 1. Then for n a nonnegative integer we have*

$$f(n+2) = \frac{1}{(d+1)^{n+1}} \sum_k (-1)^k a(n,k) d^k.$$

In particular, $f(n+2)$ is positive for large d if and only if $\lfloor \frac{n}{2} \rfloor$ is even.

More generally, define $a_q(n,k)$ by

$$a_q(n,k) = \sum_l \binom{n}{l} c_2(n-l,k) q^l,$$

where $c_2(m,k)$, an associated signless Stirling number of the first kind, is defined to be the number of derangements of an m-set having exactly k cycles of size greater than 1 (so that $a(n,k) = a_1(n,k)$

and $c_2(n,k) = a_0(n,k)$*). Then we have*

$$\sum_j (-1)^j (d+q)^{n-j} j! \binom{d}{j}\binom{n}{j} = \frac{n!}{2\pi i}\int_C e^{(d+q)z}(1-z)^d \frac{dz}{z^{n+1}}$$
$$= \sum_k (-1)^k a_q(n,k) d^k,$$

where C *is any contour winding counterclockwise around* 0*.*

Proof. To prove the identity

$$\sum_j (-1)^j (d+q)^{n-j} j! \binom{d}{j}\binom{n}{j} = \frac{n!}{2\pi i}\int_C e^{(d+q)z}(1-z)^d \frac{dz}{z^{n+1}}$$

we just need to evaluate the nth derivative, with respect to z, of $e^{(d+q)z}(1-z)^d$ at $z=0$. Using the Leibniz rule we see that this is precisely the left hand side.

Now suppose that C is a circle of radius less than 1. Then we may use the power series for $\log(1-z)$ to see that

$$n! e^{(d+q)z}(1-z)^d = n! \exp\left(qz - d\frac{z^2}{2} - d\frac{z^3}{3} - \cdots\right)$$
$$= \sum_{\ell_1,\ell_2,\ldots\geq 0} z^{\sum_j j\ell_j} \frac{n!}{\prod_j j^{\ell_j}\ell_j!} q^{\ell_1}(-d)^{\sum_{j\geq 2}\ell_j}.$$

Writing $l = \ell_1, k = \sum_{j\geq 2}\ell_j$, and interpreting ℓ_j as the number of cycles of length j in a permutation, we see that the z^n-coefficient of this series is precisely

$$\sum_{k,l}\binom{n}{l} c_2(n-l,k) q^l (-d)^k = \sum_k (-1)^k a_q(n,k) d^k. \qquad \square$$

For any $v \geq d+1$, we define the polynomial f_v by

$$f_v(n) = \sum_r \ell_{v,r}\binom{n}{r},$$

where

$$\ell_{v,r} = (-1)^r \frac{d!}{v^{d+1}} \sum_{k=0}^{d+1-r} \frac{d+1-r-k}{k!} v^k,$$

as in Selberg's construction.

Proposition 18. *For* $q = v - d \ll \sqrt{d}$*, we have*

$$f_v(0) = 1 - \frac{q-1}{v}\frac{d!}{v^d}\sum_r \frac{v^r}{r!} = 1 - \frac{q-1}{v}\Gamma(d+1,v)v^{-d}e^v \gg 1$$

as well as

$$\sum_n \frac{(1-n)f_v(n)^2}{n!}v^n = -e^v \frac{d!}{v^{d+1}}(q-1)f_v(0) = -(\sqrt{2\pi}+o(1))e^{\frac{q^2}{2d}}\frac{q-1}{\sqrt{d}}f_v(0).$$

Furthermore, for every nonnegative integer n we have

$$\frac{d}{dv}\left(v^{n+1}f_v(n+2)\right) = nv^n f_v(n+1)$$

and

$$\begin{aligned} f_v(n+2) &= \frac{n!}{2\pi i}\int_C e^{vz}(1-z)^d\frac{dz}{z^{n+1}} \\ &= \frac{1}{v^{n+1}}\sum_k (-1)^k a_q(n,k)d^k, \end{aligned}$$

where C is any contour winding counterclockwise around 0.

Proof. The first two claims are straightforward calculations. For the last two claims, we use an analogous argument to the proof of Proposition 16 to see that

$$f_v(n+2) = \frac{1}{v^{n+1}}\sum_j (-1)^j v^{n-j} j! \binom{d}{j}\binom{n}{j}.$$

Multiplying by v^{n+1} and differentiating each term of the sum with respect to v we get the claim about the derivative of $v^{n+1}f_v(n+2)$ with respect to v. The last claim follows from Proposition 17. □

In the appendix, I prove that the coefficients $a_q(n,k)$ are log-concave in k, and use this fact to prove several explicit bounds on connected to f and f_v. Alternatively, we can get bounds of the same quality with less work by using the saddle point method to estimate the integral $\int_C e^{vz}(1-z)^d\frac{dz}{z^{n+1}}$. Either way, we can prove the following bound.

Theorem 24. *If $n, q, d \geq 1$ with $4(n+q)^2 \leq d$, and if $v = d+q$, then we have*

$$v^{(n+2)/2}f_v(n+2) = \frac{n!e^{n/2}}{\sqrt{\pi}n^{(n+1)/2}}\mathrm{Re}\left(i^{-n}\exp\left(i(\tfrac{n}{3}+q)\sqrt{\tfrac{n}{v}}+O(\tfrac{n+q}{\sqrt{nv}})\right)\right)e^{\frac{q^2}{4v}}.$$

In particular, when n is even, $n, q \ll \sqrt{v}$, and $(\frac{n}{3}+q)\sqrt{\frac{n}{v}}$ has distance $\gg \frac{1}{\sqrt{n}}$ from the nearest odd multiple of $\frac{\pi}{2}$, f_v has a real root ν between n and $n+2$. Similarly if n is odd, $n, q \ll \sqrt{v}$, and $(\frac{n}{3}+q)\sqrt{\frac{n}{v}}$ has distance $\gg \frac{1}{\sqrt{n}}$ from the nearest multiple of π, f_v has a real root ν between n and $n+2$.

Proof. This is proved in the first appendix, using the saddle point method (see Theorem 43). □

Theorem 25. *If $R = 2d+1$ then $v_R - d \geq (c+o(1))\sqrt[3]{d}$, where $c \approx \frac{1}{12.14}$ is the positive solution of the equation*

$$\int_0^\infty \frac{1}{x^{3/2}} \min\left(\sin^2\left((\tfrac{x}{3}+c)\sqrt{x}\right), \cos^2\left((\tfrac{x}{3}+c)\sqrt{x}\right)\right) dx = 2\pi c.$$

Proof. It's easy to see that for any positive real root ν of f_v, we can find a quadratic polynomial q such that $q(0) = 1$,

$$0 \leq q(n) \leq \left(1 - \frac{n}{\nu_k}\right)^2$$

for $n \in \mathbb{N}$, and at least one of $q(\lfloor\nu\rfloor), q_k(\lceil\nu\rceil)$ is 0: for instance, we can take

$$q(n) = \left(1-\frac{n}{\nu}\right)^2 - \min\left(\frac{1}{\lfloor\nu\rfloor}\left(1-\frac{\lfloor\nu\rfloor}{\nu}\right)^2, \frac{1}{\lceil\nu\rceil}\left(1-\frac{\lceil\nu\rceil}{\nu}\right)^2\right) n.$$

Thus, there exists a polynomial θ_v of degree R such that $\theta_v(0) = f_v(0)^2$,

$$0 \geq \theta_v(n) \geq (1-n) f_v(n)^2$$

for $n \in \mathbb{N}^+$, and such that for any positive real root ν of f_v at least one of $\theta_v(\lfloor\nu\rfloor), \theta_v(\lceil\nu\rceil)$ vanishes. Thus, we have

$$\sum_n \frac{\theta_v(n)}{n!} v^n \geq \sum_n \frac{(1-n)f_v(n)^2}{n!} v^n + \sum_{\substack{f_v(\nu)=0 \\ \nu\in\mathbb{R}^+}} \min\left(\frac{(\lfloor\nu\rfloor-1)f_v(\lfloor\nu\rfloor)^2}{\lfloor\nu\rfloor!} v^{\lfloor\nu\rfloor}, \frac{(\lceil\nu\rceil-1)f_v(\lceil\nu\rceil)^2}{\lceil\nu\rceil!} v^{\lceil\nu\rceil}\right).$$

Set $v = d+q$ with $q = (c+o(1))\sqrt[3]{d}$, and let ν_j be the jth positive root of f_v. By the previous Theorem, for $j \ll \sqrt{v}$ we have

$$\nu_j \approx 2j+1+\tfrac{2}{\pi}(\tfrac{2j}{3}+q)\sqrt{\tfrac{2j}{v}} = 2j + O(\sqrt{j}).$$

Let $F_v(n)$ be defined by

$$F_v(n) = \frac{(n-1)f_v(n)^2}{n!} v^n.$$

Applying the previous Theorem, we get

$$\min\left(F_v(\lfloor\nu_j\rfloor), F_v(\lceil\nu_j\rceil)\right) \approx \frac{e^{\frac{q^2}{2v}}}{2\sqrt{\pi j^3}} \min\left(\sin^2\left((\tfrac{2j}{3}+q)\sqrt{\tfrac{2j}{v}}\right), \cos^2\left((\tfrac{2j}{3}+q)\sqrt{\tfrac{2j}{v}}\right)\right),$$

while from Proposition 18 we have

$$\sum_n \frac{(1-n)f_v(n)^2}{n!} v^n \approx -\sqrt{2\pi} e^{\frac{q^2}{2v}} \frac{q}{\sqrt{v}}.$$

Thus, we just need

$$\sum_{j\geq 1}\frac{1}{2\sqrt{\pi j^3}}\min\left(\sin^2\left((\tfrac{2j}{3}+q)\sqrt{\tfrac{2j}{v}}\right),\cos^2\left((\tfrac{2j}{3}+q)\sqrt{\tfrac{2j}{v}}\right)\right)\gtrsim\sqrt{2\pi}\frac{q}{\sqrt{v}}.$$

Writing $2j=x\sqrt[3]{v}, q=c\sqrt[3]{v}$ and approximating the sum by an integral, this becomes

$$\int_0^\infty\frac{1}{x^{3/2}}\min\left(\sin^2\left((\tfrac{x}{3}+c)\sqrt{x}\right),\cos^2\left((\tfrac{x}{3}+c)\sqrt{x}\right)\right)\mathrm{d}x\geq 2\pi c. \qquad \square$$

What does the optimal lower bound polynomial θ look like?

First we show that 2 is not a root of the optimal θ when $v=v_R$.

Theorem 26. *Let θ be the polynomial of degree R with $\theta(0)=1$ and $\theta(n)\leq 0$ for all positive integers n. Suppose that $\theta(2)=0$ and that*

$$\sum_n\frac{\theta(n)}{n!}v^n\geq 0.$$

Then there is another polynomial θ_2 of degree R with $\theta_2(0)=1$, $\theta_2(n)\leq 0$ for all positive integers n, $\theta_2(2)<0$, and

$$\sum_n\frac{\theta_2(n)}{n!}v^n>0.$$

Proof. Assume without loss of generality that θ is of the form

$$\theta(n)=(1-n)\prod_i\left(1-\frac{n}{\nu_i}\right)\left(1-\frac{n}{\nu_i+1}\right)$$

for ν_i positive integers with $\nu_1=2$, $\nu_{i+1}\geq\nu_i+2$. Let $2k$ be the first integer which is not a root of θ (it is necessarily even). Define θ_2 by

$$\theta_2(n)=\frac{n-2k}{k(n-2)}\theta(n).$$

Then we have

$$\sum_n\frac{\theta_2(n)}{n!}v^n\geq 1+\frac{\theta_2(2)}{2}v^2+\frac{1}{k}\sum_{n>2k}\frac{\theta(n)}{n!}v^n\geq 1+\frac{\theta_2(2)}{2}v^2-\frac{1}{k}\left(1+\frac{\theta(2k)}{(2k)!}v^{2k}\right).$$

We claim that

$$\frac{|\theta(2k)|}{(2k)!}>\left(\frac{|\theta_2(2)|}{2}\right)^k.$$

Since for any $\nu > 2k$ we have

$$1 - \frac{2k}{\nu} < \left(1 - \frac{2}{\nu}\right)^k,$$

we just need to show that

$$\left|1 - \frac{2k}{2}\right| \left|1 - \frac{2}{2k}\right|^{-k} \prod_{\nu \neq 2,2k} \left|1 - \frac{2k}{\nu}\right| \left|1 - \frac{2}{\nu}\right|^{-k} \geq \frac{(2k)!}{2^k},$$

but in fact the left hand side is a telescoping product which is precisely equal to the right hand side. Thus

$$1 + \frac{\theta_2(2)}{2}v^2 - \frac{1}{k}\left(1 + \frac{\theta(2k)}{(2k)!}v^{2k}\right) > 1 - \frac{|\theta_2(2)|}{2}v^2 - \frac{1}{k}\left(1 - \left(\frac{|\theta_2(2)|}{2}v^2\right)^k\right) > 0. \qquad \square$$

Based on the analysis in the previous section, it seems likely that the roots of the optimal θ are approximately the same as what we get by rounding the roots of the function f_v up and down to the nearest integers, and that additionally most of the improvement comes from rounding the small roots - rounding the large roots seems to have little impact. Since the jth root ν_j of f_v satisfies

$$\nu_j \approx 2j + 1 + \tfrac{2}{\pi}(\tfrac{2j}{3} + q)\sqrt{\tfrac{2j}{v}}$$

for $j \ll \sqrt{v}$, we get $2j + 1 \leq \nu_j \leq 2j + 2$ for $j \leq \sqrt[3]{v}$. Thus, for large R there should exist a nearly optimal sieve of the form

$$\theta(n) = (1 - n) \cdot \prod_{j=1}^{\sqrt[3]{v_R}} \left(1 - \tfrac{n}{2j+1}\right)\left(1 - \tfrac{n}{2j+2}\right) \cdot p(n)^2,$$

where p is a real polynomial with $p(0) = 1$ and all roots of p larger than $\sqrt[3]{v_R}$ (note that 2 is the only small natural number which is not a root of the above product). This prediction matches the numerical data fairly well.

4.3 Stick-breaking

4.3.1 Stick-breaking process and the Dickman function

In the stick-breaking process (aka the Poisson-Dirichlet process - see [4] and [19] for more details and a more rigorous treatment of the material in this section), we begin with a stick of length 1, and cut it at a (uniformly) random location into two pieces. One piece is set aside, and the other piece is again cut at a (uniformly) random location, and so on, until we've set aside an infinite sequence of pieces whose sizes add up to 1. More formally, we might define it as follows.

Definition 7. The sequence of random variables $(x_1, x_2, ...)$ is distributed according to the stick-breaking process if for each n, when we condition on the values of $x_1, ..., x_{n-1}$, x_n is uniformly distributed between 0 and $1 - (x_1 + \cdots + x_{n-1})$.

A nice property of the stick-breaking process is the following rearrangement principle, which I think of as saying that the chance of a given piece of the stick being the first piece in the sequence is proportional to its size.

Proposition 19. *Let $(x_1, ...)$ be distributed according to the stick-breaking process, and define intervals $I_1, ...$ by $I_1 = [0, x_1), I_2 = [x_1, x_1 + x_2), ...$ so that the length of I_n is x_n. If a is a uniformly random point in the interval $[0, 1)$ (independent of the stick-breaking process), then the length of the interval I_n which contains a is uniformly distributed between 0 and 1.*

Proof. Let $f(u)$ be the probability that the length of the interval I_n which contains a is at most u. By splitting into cases based on whether $a \in I_1$ or $a \notin I_1$, we see that

$$f(u) = \int_0^1 x_1 \mathbf{1}_{x_1 \leq u} + (1 - x_1) f(\tfrac{u}{1-x_1}) dx_1.$$

Since $f(\frac{u}{1-x_1})$ is 1 when $1 - x_1 \leq u$, this can be simplified to

$$\begin{aligned} f(u) &= \tfrac{u^2}{2} + \tfrac{u^2}{2} + \int_0^{1-u} (1 - x_1) f(\tfrac{u}{1-x_1}) dx_1 \\ &= u^2 + \int_u^1 \frac{u^2}{v^3} f(v) dv. \end{aligned}$$

It's easy to check that $f(u) = u$ (for $0 \leq u \leq 1$) solves the above. To see that this solution is unique, we apply the contraction mapping principle on $L^1([0, 1])$:

$$\begin{aligned} \int_0^1 |f(u) - u| du &= \int_0^1 \Big| \int_u^1 \frac{u^2}{v^3} (f(v) - v) dv \Big| du \\ &\leq \int_0^1 \int_u^1 \frac{u^2}{v^3} |f(v) - v| dv \, du \\ &= \frac{1}{3} \int_0^1 |f(v) - v| dv, \end{aligned}$$

so $\int_0^1 |f(u) - u| du$ must be 0. □

We'll mostly be interested in the distribution of the sizes of the largest pieces of the stick.

Definition 8. We define the Dickman function $\rho(u)$ to be the probability that all of the pieces of the stick in the stick breaking process have size at most $\frac{1}{u}$.

Proposition 20. *The Dickman function satisfies the identities*

$$\rho(u) = \frac{1}{u}\int_{u-1}^{u} \rho(t)dt$$

and

$$u\rho'(u) = -\rho(u-1).$$

For any $u \geq 0$, we have the bound $\rho(u) \leq \frac{1}{\lfloor u \rfloor !}$.

Proof. Let $(x_1, ...)$ be distributed according to the stick-breaking process. Since $\frac{1}{1-x_1} \cdot (x_2, ...)$ is then also distributed according to the stick-breaking process, we have

$$\rho(u) = \int_0^{1/u} \rho((1-x_1)u)dx_1.$$

Making the change of variables $t = (1-x_1)u$ gives the first identity. Differentiating the first identity with respect to u gives the second identity.

Since ρ is decreasing, we have

$$\rho(u) = \frac{1}{u}\int_{u-1}^{u} \rho(t)dt \leq \frac{1}{u} \cdot \rho(u-1),$$

so the bound $\rho(u) \leq \frac{1}{\lfloor u \rfloor !}$ follows by induction on $\lfloor u \rfloor$. □

One crucial computation we'll need later is the following.

Proposition 21. *We have*

$$\int_0^\infty \rho(u)du = \int_0^\infty u\rho(u)du = e^\gamma,$$

where $\gamma = 0.57721...$ is the Euler-Mascheroni constant.

Proof. Since ρ decays so rapidly, its Laplace transform

$$L(t) = \int e^{-tu}\rho(u)dt$$

is entire. Multiplying by t and integrating by parts, we get

$$\begin{aligned} tL(t) &= -\int \rho(u)de^{-tu} \\ &= \int e^{-tu}\rho'(u)du \\ &= -\int e^{-tu}\frac{\rho(u-1)}{u}du. \end{aligned}$$

Differentiating both sides with respect to t, we get

$$\begin{aligned}\frac{d}{dt}(tL(t)) &= \int e^{-tu}\rho(u-1)du \\ &= e^{-t}L(t).\end{aligned}$$

Dividing both sides by $tL(t)$, we get

$$\frac{d}{dt}\log(tL(t)) = \frac{e^{-t}}{t}.$$

Since $\rho(u)$ is 1 for $0 \le u \le 1$ and is at most 1 for $u \ge 1$, we have

$$\lim_{t\to\infty} tL(t) = \lim_{t\to\infty} t\int_0^1 e^{-tu}du = \lim_{t\to\infty} t\int_0^\infty e^{-tu}du = 1.$$

Thus, we have

$$\log(tL(t)) = -\int_t^\infty \frac{e^{-x}}{x}dx,$$

so

$$\begin{aligned}L(t) &= \frac{1}{t}\exp\Big(-\int_t^\infty \frac{e^{-x}}{x}dx\Big) \\ &= \exp\Big(\int_t^1 \frac{1-e^{-x}}{x}dx - \int_1^\infty \frac{e^{-x}}{x}dx\Big).\end{aligned}$$

Taking $t = 0$, we get

$$\int \rho(u)du = L(0) = \exp\Big(\int_0^1 \frac{1-e^{-x}}{x}dx - \int_1^\infty \frac{e^{-x}}{x}dx\Big).$$

We need to show that the expression inside the integral is γ. A quick way to do this is to write

$$\begin{aligned}1 + \frac{1}{2} + \cdots + \frac{1}{n} &= \int_0^1 1 + x + \cdots + x^{n-1}dx \\ &= \int_0^1 \frac{1-x^n}{1-x}dx \\ &= \int_0^1 \frac{1-(1-x)^n}{x}dx \\ &= \int_0^n \frac{1-(1-\frac{x}{n})^n}{x}dx,\end{aligned}$$

so

$$1 + \frac{1}{2} + \cdots + \frac{1}{n} - \log(n) = \int_0^1 \frac{1-(1-\frac{x}{n})^n}{x}dx - \int_1^n \frac{(1-\frac{x}{n})^n}{x}dx.$$

Taking the limit as $n \to \infty$, we get

$$\gamma = \int_0^1 \frac{1-e^{-x}}{x} dx - \int_1^\infty \frac{e^{-x}}{x} dx.$$

To prove the formula for $\int u\rho(u)du$, we use the identity $u\rho(u) = \int_{u-1}^u \rho(t)dt$ to get

$$\begin{aligned}\int_0^\infty u\rho(u)du &= \int_0^\infty \int_{u-1}^u \rho(t)dt\ du \\ &= \int_{-1}^\infty \rho(t) \int_{\max(0,t)}^{t+1} du\ dt \\ &= \int \rho(t)dt = e^\gamma.\end{aligned}$$

□

Random permutation model

Proposition 22. *If σ is a random permutation of $\{1, ..., n\}$, then the size of the cycle of σ which contains 1 is uniformly distributed between 1 and n.*

From this we see that if we normalize the sizes of the cycles of a random permutation $\sigma \in S_n$ by dividing them by n (and sort the cycles in order of the least element of $\{1, ..., n\}$ appearing in them), we get a discretized version of the stick-breaking process.

Corollary 5. *As $n \to \infty$, the probability that a random permutation of $\{1, ..., n\}$ has all of its cycles of size at most $\frac{n}{u}$ approaches $\rho(u)$.*

Prime factorization model

Let n be a random large number - chosen uniformly randomly from some large dyadic interval $[y, 2y)$ - with prime factorization $n = p_1 \cdots p_k$. Define $x_i = \frac{\log(p_i)}{\log(n)}$, so that $\sum x_i = 1$. I claim that in the limit, the unordered collection of the x_is have the same distribution as the unordered stick-breaking process. In order to approach this claim, we can apply Proposition 19 to reintroduce the ordering - so we assume that the ordering of the p_is is randomized such that the chance of a given prime p dividing n being first is equal to $\frac{\log(p)}{\log(n)}$, and so on.

We need to check that $\log(p_1)$ is approximately uniformly distributed between 0 and $\log(n)$, and that the remaining prime factors follow a similar distribution. I'll do this by turning the problem around: instead of starting with a random n, we start with p_1 and $m = \frac{n}{p_1}$, with p_1 a random prime whose logarithm is (roughly) uniformly distributed between 0 and $\log(y)$, and m a number chosen uniformly at random from the interval $[\frac{y}{p_1}, \frac{2y}{p_1})$, and check that the product $p_1 m$ is uniformly distributed in $[y, 2y)$. The key calculation is that for any z, we have

$$\sum_{p<z} \frac{\log(p)}{p} \approx \log(z),$$

so if we choose $p_1 = p$ with probability $\frac{\log(p)}{p\log(y)}$ then $\log(p_1)$ is roughly uniformly distributed between 0 and $\log(y)$, and for a given $n \in [y, 2y)$ the probability that $p_1 m = n$ is then about

$$\sum_{p|n} \frac{\log(p)}{p\log(y)} \cdot \frac{p}{y} = \frac{\log(n)}{y\log(y)} \approx \frac{1}{y}.$$

From the above, we expect that the proportion of x-smooth numbers (that is, numbers having all divisors at most x) having size about y should be about $\rho(\frac{\log(y)}{\log(x)})$. In fact, the following very precise bound for the number of x-smooth numbers has been proved by Hildebrand.

Theorem 27 (Hildebrand [12])**.** *If $y = x^s$ with $y \geq 3$ and*

$$1 \leq s \leq \frac{\log(y)}{\log(\log(y))^{\frac{5}{3}+\epsilon}}$$

with $\epsilon > 0$, then

$$\#\{n \leq y \mid n \text{ is } x\text{-smooth}\} = y\rho(s)\Big(1 + O_\epsilon\Big(\frac{s\log(s+1)}{\log(y)}\Big)\Big).$$

We can use this to quickly estimate the product $\prod_{p<z}(1-\frac{1}{p})$. The calculation goes as follows.

$$\begin{aligned}
\prod_{p<z}(1-\tfrac{1}{p})^{-1} &= \sum_{n \ z\text{-smooth}} \frac{1}{n} \\
&\approx \int_1^\infty \frac{\rho(\frac{\log(y)}{\log(z)})}{y} dy \\
&= \int_0^\infty \rho(\tfrac{\log(y)}{\log(z)}) d\log(y) \\
&= e^\gamma \log(z).
\end{aligned}$$

4.3.2 General process, colored permutations

We'll motivate the general stick-breaking process by starting with a permutation model.

Definition 9. If κ is a whole number, then we say that (π, c) is a *κ-colored permutation* on n letters if π is a permutation of $\{1, ..., n\}$ and $c : \{1, ..., n\} \to \{1, ..., \kappa\}$ is a compatible coloring of $\{1, ..., n\}$ (i.e. $c(i) = c(\pi(i))$ for all i).

Proposition 23. *The number of κ-colored permutations on n letters is*

$$\kappa(\kappa+1)\cdots(\kappa+n-1).$$

If (π, c) is chosen uniformly randomly from the set of all κ-colored permutations on n letters, then

the probability that the cycle of π which contains 1 has size j is

$$\frac{\kappa}{n}\frac{(n-j+1)\cdots(n-j+\kappa-1)}{(n+1)\cdots(n+\kappa-1)} \approx \frac{\kappa}{n}(1-\tfrac{j}{n})^{\kappa-1}.$$

Based on this, the general stick-breaking process is defined as follows.

Definition 10. The sequence of random variables $(x_1, x_2, ...)$ is distributed according to the general stick-breaking process with parameter κ if for each n, when we condition on the values of $x_1, ..., x_{n-1}$, the fraction $\frac{x_n}{1-(x_1+\cdots+x_{n-1})}$ is randomly distributed on $[0,1]$ according to the distribution $\text{Beta}(1,\kappa)$, which has probability density function $t \mapsto \kappa(1-t)^{\kappa-1}$.

The reader can check that the general stick-breaking process satisfies an analogue of Proposition 19 for any positive κ. From the general stick-breaking process, we get the following generalization of the Dickman function.

Definition 11. For $\kappa > 0$, we define the generalized Dickman function $\rho_\kappa(s)$ to be the probability that all of the pieces of the stick in the general stick-breaking process with parameter κ have size at most $\frac{1}{s}$.

Proposition 24. *For $s < 0$ we have $\rho_\kappa(s) = 0$, for $0 < s \leq 1$ we have $\rho_\kappa(s) = 1$. For all s, we have the identities*

$$s^\kappa \rho_\kappa(s) = \int_{s-1}^{s} \rho_\kappa(t) dt^\kappa$$

and

$$s^\kappa \rho_\kappa'(s) = -\kappa(s-1)^{\kappa-1}\rho_\kappa(s-1).$$

For $s \geq 0$, we have the bound $\rho_\kappa(s) \leq \frac{\kappa^{\lfloor s \rfloor}}{\lfloor s \rfloor!}$.

An analogous prime factorization model can be given as follows. We consider the set of integers n in a large dyadic interval $[y, 2y)$, and we weight them according to the size of $\tau_\kappa(n)$, which is the number of ways of writing n as a product of κ whole numbers when $\kappa \in \mathbb{N}^+$. Then we write $n = p_1 \cdots p_k$, where the chance of a given prime p dividing n coming first is equal to $\frac{\log(p)}{\log(n)}$, and set $x_i = \frac{\log(p_i)}{\log(n)}$.

Finally, we have the following important computation.

Proposition 25. *For any $\kappa \geq 0$, we have*

$$\int_0^\infty \rho_\kappa(s) ds^\kappa = e^{\gamma\kappa}\Gamma(\kappa+1).$$

Proof. Define $L_\kappa(t)$ by

$$L_\kappa(t) = \int e^{-st}\rho_\kappa(s) ds^\kappa.$$

Similarly to Proposition 21, we find that

$$\frac{d}{dt}\log(t^\kappa L_\kappa(t)) = \frac{\kappa e^{-t}}{t},$$

and

$$\lim_{t\to\infty} t^\kappa L_\kappa(t) = \int_0^\infty e^{-s} ds^\kappa = \Gamma(\kappa+1),$$

so

$$L_\kappa(t) = \frac{\Gamma(\kappa+1)}{t^\kappa}\exp\Big(-\int_t^\infty \frac{\kappa e^{-s}}{s} ds\Big).$$

Taking $t = 0$, we get

$$\int_0^\infty \rho_\kappa(s) ds^\kappa = L_\kappa(0) = \Gamma(\kappa+1)e^{\gamma\kappa}. \qquad \square$$

4.3.3 Toy counting problem: flexible numbers and permutations

Definition 12. A natural number n is *y-flexible* if for all $1 \le x \le y$ there are natural numbers a, b with $n = ab$ such that $a \le x$ and $b \le \frac{y}{x}$.

Flexible numbers are convenient in the context of analytic number theory (see, for instance, [15] and Section 12.7 of [8]). So, it's natural to wonder how common they are:

Problem 10. How many y-flexible numbers are there, as a function of y?

There is a convenient analogue of flexible numbers in the permutation setting.

Definition 13. A permutation $\sigma \in S_n$ is *flexible* if for all $0 \le m \le n$ there is a subset $M \subseteq \{1, ..., n\}$ with $|M| = m$ such that $\sigma(M) = M$.

We have an analogous counting problem:

Problem 11. How many flexible permutations are there on n letters, as a function of n?

For $n = 1, ..., 6$ the number of flexible permutations on n letters are, respectively, $1, 1, 4, 7, 46, 221$ (surprisingly, this sequence doesn't seem to show up on OEIS).

As a first step, we have the following equivalent definition of flexibility.

Exercise 1. Suppose $\sigma \in S_n$ has cycles of sizes $c_1 \le c_2 \le \cdots \le c_m$ (including 1-cycles), so that $\sum_{i=1}^m c_i = n$. Then σ is flexible if and only if, for each $1 \le i \le m$, we have

$$1 + \sum_{j<i} c_j \ge c_i.$$

In particular, σ is flexible if and only if $2c_m \le n+1$ and deleting the largest cycle from σ produces a flexible permutation on $n - c_m$ letters.

If you want to spoil the solution, essentially the same fact is proved in Proposition 48. Defining $u(k,n)$ to be

$$u(k,n) = \frac{1}{n!}\{\sigma \in S_n \mid \sigma \text{ is flexible, with all cycles of size } \leq k\},$$

we get the recurrence

$$u(k,n) = \sum_{0 \leq m \leq \lfloor \frac{n+1-k}{k} \rfloor} \frac{1}{k^m m!} u(k-1, n-mk).$$

In particular, when $2k \leq n+1$ this gives us

$$\frac{1}{k}u(k-1,n-k) \leq u(k,n) - u(k-1,n) \leq \frac{1}{k}u(k,n-k).$$

The above recurrence is a near-perfect discretization of the differential-difference equation

$$\frac{\partial}{\partial x}u(x,y) = \begin{cases} \frac{1}{x}u(x,y-x) & y > 2x, \\ 0 & y < 2x. \end{cases} \tag{u}$$

This differential-difference equation has a "scale-invariance" property: if $u(x,y)$ is a solution, then so is $u(\lambda x, \lambda y)$ for any $\lambda > 0$. This property makes the long-term behavior very robust to errors due to discretization: as x and y increase, we can rescale the coordinates back down, which has the effect of shrinking the mesh of our discretization.

We make the following guess for the long term asymptotics of $u(x,y)$:

$$u(x,y) \approx \frac{f(\frac{y}{x})}{y^\alpha},$$

where $f \geq 0$ and f decays rapidly at infinity, and $\alpha > 0$. This leads to a single-variable differential-difference equation satisfied by f:

$$-\frac{sf'(s)}{s^\alpha} = \begin{cases} \frac{f(s-1)}{(s-1)^\alpha} & s > 2, \\ 0 & s < 2. \end{cases}$$

Playing around with this, we see that when α is too large, f changes sign occasionally: after rescaling to make $f(1) = 1$, we get

$$f(s) = 1 - \int_{t=2}^{s} \frac{t^{\alpha-1}}{(t-1)^\alpha} f(t-1)dt,$$

and in particular

$$f(3) = 1 - \int_{t=2}^{3} \frac{t^{\alpha-1}}{(t-1)^\alpha} dt,$$

so $f(3) < 0$ when $\alpha \geq 1.7$. Presumably, when α is too small f will fail to decay sufficiently rapidly at infinity.

Time to cheat. Numerically, going back to the permutation case, we have

$$\begin{aligned} u(10,10) &\approx 1.87306 \times 10^{-1}, \\ u(100,100) &\approx 2.2231 \times 10^{-2}, \\ u(10^3,10^3) &\approx 2.2746 \times 10^{-3}, \\ u(10^4,10^4) &\approx 2.27972 \times 10^{-4}, \\ u(10^5,10^5) &\approx 2.28023 \times 10^{-5}. \end{aligned}$$

This suggests taking $\alpha = 1$. By some miracle, when $\alpha = 1$ we have the exact solution

$$f(s) = \begin{cases} \rho(s-1) & s > 1, \\ 1 & s \leq 1. \end{cases}$$

So we conjecture the long-term asymptotics

$$u(x,y) \asymp \frac{\rho(\frac{y}{x} - 1)}{y}.$$

This leaves the natural question: how do we get our hands on the constant of proportionality in the above asymptotic? Since the asymptotic might take quite a while to kick in, simply comparing the two sides for various choices of x, y doesn't seem like a good approach, especially if we want error bounds. Instead, we will use the following *conservation law*, which is fairly guessable once you know what to look for (this type of conservation law is closely connected to the adjoint equations that appear in the theory of differentiable-difference equations - for the theory of adjoint equations, see Appendix B of [8], [13], or [31]).

Proposition 26. *If $u(x,y)$ satisfies* (u)*, then the value of integral*

$$\int_{y=x}^{\infty} \frac{y-x}{x} u(x,y) dy$$

is independent of x.

In fact, using the above conservation law, we can see that the only possible value for α is 1. Since

$$\int_{s=1}^{\infty} (s-1)\rho(s-1)\frac{ds}{s} = e^{\gamma} - 1,$$

our asymptotic becomes:

$$u(x,y) \approx \left(\frac{\int_{y=c}^{\infty} (y-c)u(c,y)dy}{(e^{\gamma}-1)c} \right) \frac{\rho(\frac{y}{x} - 1)}{y},$$

for c any constant greater than 0.

Now we come back to the problem of estimating the number of flexible permutations. According to the above analysis, the proportion of flexible permutations on n letters should grow like

$$u(n,n) \approx C \cdot \frac{\rho(\frac{n}{n}-1)}{n} = \frac{C}{n},$$

and the constant of proportionality C should satisfy

$$\frac{\sum_{n>k}(n-k)u(k,n)}{(e^\gamma-1)k} < C < \frac{\sum_{n\geq k}(n+1-k)u(k,n)}{(e^\gamma-1)k},$$

since the left side increases and the right side decreases as k increases, and in the limit they are both equal to C. When $k=1$, we get $1.28029 < C < 3.4802$. When $k=10$, we get $2.11614 < C < 2.39521$. When $k=100$, we get $2.26265 < C < 2.29171$. When $k=1000$, we get $2.27851 < C < 2.28144$.

An analogous analysis should show that the number of y-flexible numbers is proportional to $\frac{y}{\log(y)}$, and that more generally we have

$$\#\{x\text{-smooth } y\text{-flexible numbers}\} \asymp \rho\left(\frac{\log(y)}{\log(x)}-1\right)\frac{y}{\log(y)}$$

with a computable constant of proportionality - but in order to get the error bounds on the constant, we will probably need to use explicit forms of the prime number theorem.

4.4 True size of the sifted interval

In the case $\kappa = 1$ and $A = [1, y]$, the size of $\mathcal{S}([1, y], z)$ can be computed explicitly. Before computing the true size, let's compute the naïve guess for its size:

$$\mathcal{S}([1,y],z) \approx \prod_{p<z}(1-\tfrac{1}{p})\cdot y \approx \frac{y}{e^\gamma \log(z)}.$$

When $\frac{\log(y)}{\log(z)}$ is large, this approximation is accurate (by the Fundamental Lemma of sieve theory). However, when $\frac{\log(y)}{\log(z)}$ is smaller, this guess is off by a constant factor.

Proposition 27 (Lemma 12.1 of [8] and surrounding remarks)**.** *If $s > 1$ is fixed, then if $y = z^s$ and $z \to \infty$ we have*

$$\mathcal{S}([1,y],z) = (\omega(s)+o(1))\frac{y}{\log(z)},$$

where $\omega(s)$ solves the differential-difference equation

$$s > 2 \quad \Longrightarrow \quad \frac{d}{ds}(s\omega(s)) = \omega(s-1)$$

and has the initial condition

$$1 \le s \le 2 \quad \Longrightarrow \quad s\omega(s) = 1.$$

For s large, we have $\omega(s) = e^{-\gamma} + O(s^{-s})$, and $\omega(s) - e^{-\gamma}$ changes sign in every interval of length 1.

The function $\omega(s)$ is called the *Buchstab function.*

Chapter 5

Selberg's sieve

Recall that there are two perspectives on any collection of sieve weights: the weights λ_d themselves, and the associated function θ given by

$$\theta(d) = \sum_{k|d} \lambda_k.$$

To check that the weights form a valid sieve, one checks that $\theta(d) \geq 0$ (for an upper bound sieve) or $\theta(d) \leq 0$ for $d \mid P_z, d \geq 1$ (for a lower bound sieve). To check that the error term is manageable, one checks that the weights λ_d are supported on $d \leq y$ and are not too large. In the case of the model problem, we think of the λ_ds as coefficients (in the binomial basis) of a polynomial θ, which naturally suggests that we should try taking θ to be a square in order to get a good upper bound sieve.

The Selberg upper bound sieve corresponds to choosing (λ, θ) such that

$$\theta(d) = \theta'(d)^2$$

for some sieve (ℓ, θ') with ℓ_d supported on $d \leq \sqrt{y}$, and chosen such that $\theta(1) = \theta'(1) = 1$. In other words, we have

$$\theta(d) = \Big(\sum_{k|d} \ell_d \Big)^2.$$

Solving for the λ_ds, we get

$$\lambda_d = \sum_{[d_1,d_2]=d} \ell_{d_1} \ell_{d_2},$$

where $[d_1, d_2]$ is the least common multiple of d_1 and d_2.

The main term of the resulting sieve is

$$\sum_{d|P_z} \frac{\lambda_d \kappa(d)}{d} = \sum_{\substack{[d_1,d_2]=d \\ d_1,d_2 \le \sqrt{y}}} \ell_{d_1}\ell_{d_2} \frac{\kappa(d)}{d}$$
$$= \sum_{d_1,d_2 \le \sqrt{y}} \frac{\ell_{d_1}\kappa(d_1)}{d_1} \frac{\ell_{d_2}\kappa(d_2)}{d_2} \frac{(d_1,d_2)}{\kappa((d_1,d_2))}.$$

Our goal is to optimize this quadratic form in the ℓ_ds, subject to the linear constraint $\ell_1 = 1$. At this point, the reader is encouraged to stop reading and try deriving the optimal choice for the ℓ_ds (as well as the resulting upper bound on $\mathcal{S}(A,z)$) themself, just to see how straightforward it is.

By Möbius inversion, we have

$$\frac{d}{\kappa(d)} = \sum_{e|d} \prod_{p|e} \frac{p-\kappa(p)}{\kappa(p)},$$

so if we make the definition

$$\varphi_\kappa(d) = \prod_{p|d} (p - \kappa(p))$$

then we see that our main term is equal to

$$\sum_{d_1,d_2 \le \sqrt{y}} \frac{\ell_{d_1}\kappa(d_1)}{d_1} \frac{\ell_{d_2}\kappa(d_2)}{d_2} \sum_{e|(d_1,d_2)} \frac{\varphi_\kappa(e)}{\kappa(e)} = \sum_{\substack{e|P_z \\ e \le \sqrt{y}}} \frac{\varphi_\kappa(e)}{\kappa(e)} \Big(\sum_{e|d} \frac{\ell_d \kappa(d)}{d} \Big)^2.$$

Define the variables ξ_e by

$$\xi_e = \mu(e) \sum_{e|d} \frac{\ell_d \kappa(d)}{d}.$$

By Möbius inversion, we can express the ℓ_ds in terms of the ξ_es by

$$\ell_d = \mu(d) \frac{d}{\kappa(d)} \sum_{d|e} \xi_e.$$

Since $\lambda_1 = \ell_1$ must be 1, the ξ_e are constrained by

$$\sum_e \xi_e = 1,$$

and since the ℓ_d are supported on $d \le \sqrt{y}$, the ξ_e are also supported on $e \le \sqrt{y}$. Applying Cauchy-Schwartz to our formula for the main term of the Selberg upper bound sieve, we get

$$\sum_{d|P_z} \frac{\lambda_d \kappa(d)}{d} = \sum_{\substack{e|P_z \\ e\le\sqrt{y}}} \frac{\varphi_\kappa(e)}{\kappa(e)} \xi_e^2 \ge \frac{1}{\sum_{\substack{e|P_z \\ e\le\sqrt{y}}} \frac{\kappa(e)}{\varphi_\kappa(e)}},$$

with equality when the ξ_e are proportional to $\frac{\kappa(e)}{\varphi_\kappa(e)}$ and $\sum_e \xi_e = 1$.

Now that we've found the main term, we just need to check that the error term is small - that is, that the λ_ds are not too large. Solving for the ℓ_ds, we get

$$\begin{aligned}\ell_d &= \mu(d)\frac{d}{\kappa(d)}\Big(\sum_{\substack{d|e|P_z \\ e\le\sqrt{y}}} \frac{\kappa(e)}{\varphi_\kappa(e)}\Big)\Big(\sum_{\substack{e|P_z \\ e\le\sqrt{y}}} \frac{\kappa(e)}{\varphi_\kappa(e)}\Big)^{-1} \\ &= \mu(d)\Big(\sum_{\substack{e|P_z \\ [d,e]\le\sqrt{y}}} \frac{\kappa(e)}{\varphi_\kappa(e)}\Big)\Big(\sum_{\substack{e|P_z \\ e\le\sqrt{y}}} \frac{\kappa(e)}{\varphi_\kappa(e)}\Big)^{-1},\end{aligned}$$

so

$$0 \le \mu(d)\ell_d \le 1.$$

In particular, we have

$$|\lambda_d| \le \sum_{\substack{[d_1,d_2]=d \\ d_1,d_2\le\sqrt{y}}} 1 \le 3^{\omega(d)}.$$

Summarizing, we have the following general result.

Theorem 28 (Selberg upper bound sieve)**.** *If A satisfies*

$$|A_d| = \frac{\kappa(d)}{d}|A| + R_d$$

with κ multiplicative and $\kappa(p) < p$ for all p, then for any y we have

$$\mathcal{S}(A,z) \le \frac{|A|}{\sum_{\substack{d|P_z \\ d\le\sqrt{y}}} \frac{\kappa(d)}{\varphi_\kappa(d)}} + \sum_{\substack{d_1,d_2|P_z \\ d_1,d_2\le\sqrt{y}}} |R_{[d_1,d_2]}|,$$

where $\varphi_\kappa(d) = \prod_{p|d}(p-\kappa(p))$.

In order to apply this, we need to estimate the sum

$$\sum_{\substack{d|P_z \\ d\le\sqrt{y}}} \frac{\kappa(d)}{\varphi_\kappa(d)}$$

which appears in the denominator of the main term. As a quick sanity check, note that if we take y to ∞, we get

$$\sum_{d|P_z} \frac{\kappa(d)}{\varphi_\kappa(d)} = \prod_{p<z} \Big(1 + \frac{\kappa_p}{p - \kappa_p}\Big) = \prod_{p<z} \Big(1 - \frac{\kappa_p}{p}\Big)^{-1},$$

which is the inverse of the expected main term. In [28], Selberg gives a quick way to bound the main term for general y and κ using Rankin's trick.

Proposition 28. *If* $\sum_{p<z} \kappa_p \frac{\log(p)}{p} = \kappa \log(z)$ *and* $s = \frac{\log(y)}{\log(z)}$, *then*

$$\prod_{p<z} \Big(1 - \frac{\kappa_p}{p}\Big) \sum_{\substack{d|P_z \\ d\le\sqrt{y}}} \frac{\kappa(d)}{\varphi_\kappa(d)} \ge 1 - \exp\Big(-\tfrac{s}{2}\log(\tfrac{s}{2e\kappa}) - \kappa\Big).$$

In particular, we have

$$F_\kappa(s) \le \frac{1}{1 - \exp\big(-\frac{s}{2}\log(\frac{s}{2e\kappa}) - \kappa\big)}.$$

Proof. For any $\delta > 0$, we have

$$\begin{aligned}
\prod_{p<z} \Big(1 - \frac{\kappa_p}{p}\Big) \sum_{\substack{d|P_z \\ d\le\sqrt{y}}} \frac{\kappa(d)}{\varphi_\kappa(d)} &= 1 - \prod_{p<z} \Big(1 - \frac{\kappa_p}{p}\Big) \sum_{\substack{d|P_z \\ d>\sqrt{y}}} \frac{\kappa(d)}{\varphi_\kappa(d)} \\
&\ge 1 - \prod_{p<z} \Big(1 - \frac{\kappa_p}{p}\Big) \cdot y^{-\delta/2} \cdot \sum_{d|P_z} \frac{\kappa(d) d^\delta}{\varphi_\kappa(d)} \\
&= 1 - y^{-\delta/2} \prod_{p<z} \Big(1 - \frac{\kappa_p}{p}\Big)\Big(1 + \frac{\kappa_p p^\delta}{p - \kappa_p}\Big) \\
&= 1 - y^{-\delta/2} \prod_{p<z} \Big(1 + \frac{\kappa_p (p^\delta - 1)}{p}\Big).
\end{aligned}$$

Now we use the bound $1 + x \le e^x$ to see that this is

$$\begin{aligned}
&\ge 1 - y^{-\delta/2} \exp\Big(\sum_{p<z} \frac{\kappa_p (p^\delta - 1)}{p}\Big) \\
&\ge 1 - y^{-\delta/2} \exp\Big(\frac{z^\delta - 1}{\log(z)} \sum_{p<z} \frac{\kappa_p \log(p)}{p}\Big) \\
&= 1 - y^{-\delta/2} \exp(\kappa(z^\delta - 1)),
\end{aligned}$$

where the second inequality follows from the fact that $\frac{p^\delta - 1}{\log(p)}$ is an increasing function of p. Taking

$\delta = \frac{\log(\frac{s}{2\kappa})}{\log(z)}$, we get

$$\prod_{p<z}\Big(1-\frac{\kappa_p}{p}\Big)\sum_{\substack{d|P_z\\ d\le\sqrt{y}}}\frac{\kappa(d)}{\varphi_\kappa(d)} \ge 1-\exp\Big(-\tfrac{s}{2}\log(\tfrac{s}{2\kappa})+\kappa(\tfrac{s}{2\kappa}-1)\Big). \qquad \square$$

Corollary 6 (Fundamental Lemma of Sieve Theory)**.** *For any fixed κ, we have $F_\kappa(s) \le 1 + \exp(-\frac{s}{2}\log(s)+O(s))$ and $f_\kappa(s) \ge 1-\exp(-\frac{s}{2}\log(s)+O(s))$.*

Proof. The bound on F_κ follows the previous proposition. For the bound on f_κ, we can apply Buchstab iteration once to see that

$$\begin{aligned} f_\kappa(s) &\ge 1-\frac{1}{s^\kappa}\int_{t>s} F_\kappa(t-1)-1\ dt^\kappa \\ &\ge 1-\int_{t>s}\exp(-\tfrac{t}{2}\log(t)+O(t))dt \\ &\ge 1-\exp(-\tfrac{s}{2}\log(s)+O(s)). \end{aligned} \qquad \square$$

Now we'll try to find the asymptotic for the main term of Selberg's sieve. If we have $z \ge \sqrt{y}$, then we wish to estimate the sum

$$\sum_{d\le\sqrt{y}}{}' \frac{\kappa(d)}{\varphi_\kappa(d)},$$

where the $'$ indicates that the sum is over squarefree numbers only. Setting

$$g(s) = \prod_p\Big(1+\frac{\kappa_p}{(p-\kappa_p)p^s}\Big),$$

Perron's formula gives us

$$\sum_{d\le\sqrt{y}}{}' \frac{\kappa(d)}{\varphi_\kappa(d)} = \frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} g(s)\frac{\sqrt{y}^s}{s}ds,$$

for any $c > 0$. Writing $G(s)$ for the ratio between $g(s)$ and $\zeta(s+1)^\kappa$ (which is analytic in a neighborhood of $s \ge 0$), and using the fact that $\zeta(s+1)$ has a simple pole with residue 1 at $s = 0$, this comes out to

$$\frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} G(s)\zeta(s+1)^\kappa\frac{\sqrt{y}^s}{s}ds = (G(0)+o(1))\frac{\log(\sqrt{y})^\kappa}{\Gamma(\kappa+1)},$$

and we have

$$\begin{aligned} G(0) &= \prod_p \Big(1+\frac{\kappa_p}{p-\kappa_p}\Big)\Big(1-\frac{1}{p}\Big)^\kappa \\ &= (1+o(1))\prod_{p<z}\Big(1+\frac{\kappa_p}{p-\kappa_p}\Big)\Big(1-\frac{1}{p}\Big)^\kappa \\ &= \frac{1+o(1)}{e^{\gamma\kappa}\log(z)^\kappa}\prod_{p<z}\Big(1-\frac{\kappa_p}{p}\Big)^{-1}. \end{aligned}$$

Thus, we have

$$\prod_{p<z}\Big(1-\frac{\kappa_p}{p}\Big)\sum_{d\le\sqrt{y}}{}'\frac{\kappa(d)}{\varphi_\kappa(d)} = \frac{\log(\sqrt{y})^\kappa}{e^{\gamma\kappa}\Gamma(\kappa+1)\log(z)^\kappa}+o(1).$$

Now we want to restrict the sum to z-smooth d. Since the summand corresponding to d is weighted by $\approx \tau_\kappa(d)$, we expect that the weighted proportion of summands of size about w which happen to be z-smooth is about $\rho_\kappa(\frac{\log(w)}{\log(z)})$ (since the prime factors of a randomly chosen d, with probability weighted by $\tau_\kappa(d)$, are governed by the general stick-breaking process with parameter κ). Thus, if $y=z^s$ we predict the following asymptotic:

$$\prod_{p<z}\Big(1-\frac{\kappa_p}{p}\Big)\sum_{\substack{d|P_z\\ d\le\sqrt{y}}}\frac{\kappa(d)}{\varphi_\kappa(d)} = \frac{\int_0^{\frac{s}{2}}\rho_\kappa(t)dt^\kappa}{e^{\gamma\kappa}\Gamma(\kappa+1)}+o(1).$$

Defining

$$\sigma_\kappa(s) = \frac{\int_0^{\frac{s}{2}}\rho_\kappa(t)dt^\kappa}{e^{\gamma\kappa}\Gamma(\kappa+1)},$$

we have

$$\begin{aligned} s^{-\kappa}\sigma_\kappa(s) &= \frac{1}{(2e^\gamma)^\kappa\Gamma(\kappa+1)} && 0<s\le 2, \\ (s^{-\kappa}\sigma_\kappa(s))' &= -\kappa s^{-\kappa-1}\sigma_\kappa(s-2) && s\ge 2. \end{aligned}$$

Proposition 29. *If σ_κ is defined as above, the Selberg upper bound sieve gives us the bound*

$$F_\kappa(s)\le\frac{1}{\sigma_\kappa(s)}.$$

5.1 Asymptotic formulas for the Selberg sieve weights

Recall that we have

$$\lambda_d = \sum_{[d_1,d_2]=d}\ell_{d_1}\ell_{d_2},$$

and

$$\ell_d = \mu(d)\frac{d}{\kappa(d)}\Big(\sum_{\substack{d|e|P_z\\ e\le\sqrt{y}}}\frac{\kappa(e)}{\varphi_\kappa(e)}\Big)\Big(\sum_{\substack{e|P_z\\ e\le\sqrt{y}}}\frac{\kappa(e)}{\varphi_\kappa(e)}\Big)^{-1}.$$

We can rewrite the formula for ℓ_d as

$$\ell_d = \mu(d)\frac{d}{\varphi_\kappa(d)}\Big(\sum_{\substack{e|P_z\\ e\le\sqrt{y}/d\\ \gcd(d,e)=1}}\frac{\kappa(e)}{\varphi_\kappa(e)}\Big)\Big(\sum_{\substack{e|P_z\\ e\le\sqrt{y}}}\frac{\kappa(e)}{\varphi_\kappa(e)}\Big)^{-1}.$$

We can modify the argument of the previous section by leaving the primes dividing d out of the product defining $g(s)$ to see that if $z > \sqrt{y}/d$, we have

$$\begin{aligned}\prod_{p<z}\Big(1-\frac{\kappa_p}{p}\Big)\sum_{\substack{e|P_z\\ e\le\sqrt{y}/d\\ \gcd(d,e)=1}}\frac{\kappa(e)}{\varphi_\kappa(e)} &\approx \prod_{p|d}\Big(1-\frac{\kappa_p}{p}\Big)\cdot\frac{\log(\sqrt{y}/d)^\kappa}{e^{\gamma\kappa}\Gamma(\kappa+1)\log(z)^\kappa}\\ &= \frac{\varphi_\kappa(d)}{d}\cdot\frac{\log(\sqrt{y}/d)^\kappa}{e^{\gamma\kappa}\Gamma(\kappa+1)\log(z)^\kappa}.\end{aligned}$$

Approximating the effect of restricting to z-smooth summands by using the general stick-breaking process with parameter κ, we get the following approximation.

Proposition 30. *If $s = \frac{\log(y)}{\log(z)}, u = \frac{\log(d)}{\log(z)}$ and ℓ is defined to optimize the Selberg upper bound sieve of dimension κ, then*

$$\ell_d \approx \mu(d)\frac{\int_0^{\frac{s}{2}-u}\rho_\kappa(t)dt^\kappa}{\int_0^{\frac{s}{2}}\rho_\kappa(t)dt^\kappa}.$$

When s goes to ∞ this becomes

$$\ell_d \approx \begin{cases}\mu(d) & \text{if } d<\sqrt{y},\\ 0 & \text{else,}\end{cases}$$

and when $s \le 2$ it becomes

$$\ell_d \approx \mu(d)\Big(1-\frac{\log(d)}{\log(\sqrt{y})}\Big)_+^\kappa.$$

The only case in which the Selberg upper bound sieve is known to be optimal is when $\kappa = 1$ and $s \le 2$. In this case the Selberg sieve is given by

$$\lambda_d \approx \mu(d)\sum_{[d_1,d_2]=d}\mu((d_1,d_2))\Big(1-\frac{\log(d_1)}{\log(\sqrt{y})}\Big)_+\Big(1-\frac{\log(d_2)}{\log(\sqrt{y})}\Big)_+,$$

$$\theta_d \approx \Big(\sum_{k|d} \mu(k) \Big(1 - \frac{\log(k)}{\log(\sqrt{y})}\Big)_+ \Big)^2.$$

For $d \leq \sqrt{y}$, we have

$$\lambda_d \approx \mu(d)(1 - \sum_{p|d} \frac{\log(p)^2}{\log(\sqrt{y})^2}).$$

5.1.1 Unexpected pathology of the Selberg sieve weights

It's reasonable to conjecture that in any good sieve, λ_d should have the same sign as $\mu(d)$, and should furthermore be bounded by 1 in absolute value. Here I'll give an example where this is not the case. This example will even have $\kappa = 1$ and $s = 2$, where the Selberg upper bound sieve is known to be optimal.

Proposition 31. *Suppose that $\kappa = 1$ and $y = z^2$. Suppose d is a product of 9 primes, all of which are close to $y^{\frac{1}{12}} = \sqrt{y}^{\frac{1}{6}}$. Then the Selberg sieve weight λ_d is approximately $\frac{7}{2} > 1$, while $\mu(d) = -1$.*

Proof. This is a straightforward calculation:

$$\lambda_d \approx -\left(\binom{9}{4,5} + \binom{9}{5,4} \right)\left(1 - \frac{4}{6}\right)\left(1 - \frac{5}{6}\right) + \binom{9}{4,4,1}\left(1 - \frac{5}{6}\right)^2 = \frac{7}{2}. \qquad \square$$

Chapter 6

Computability of the sifting functions f_κ, F_κ - review of Selberg's work

Let A be a (possibly weighted) set of whole numbers, and for each positive integer d set $A_d = \{a \in A, d \mid a\}$. Let κ be a real number and by abuse of notation let $\kappa : \mathbb{N} \to \mathbb{R}$ be a multiplicative function satisfying $0 \leq \kappa(p) < p$ for all p, and

$$\sum_{p \leq x} \kappa(p) \frac{\log(p)}{p} = (\kappa + o(1)) \log(x).$$

Suppose that z, y are such that for every squarefree integer d, all of whose prime factors are less than z, we have

$$\left| |A_d| - \kappa(d) \frac{y}{d} \right| \leq \kappa(d), \tag{6.1}$$

or alternatively such that for some fixed $\epsilon > 0$ and every such d we have

$$\left| |A_d| - \kappa(d) \frac{y}{d} \right| \leq \kappa(d) \frac{y}{d \log(y/d)^{2\kappa+\epsilon}}. \tag{6.2}$$

In particular, we have $|A| = y + O(1)$ in the first case, or $|A| = y + O(y/\log(y)^{2\kappa+\epsilon})$ in the second case. We want to estimate the quantity

$$\mathcal{S}(A, z) = |\{a \in A, \forall p < z \ (a, p) = 1\}|.$$

Suppose now that $y = z^s$, s a constant, y, z going to infinity. Define sifting functions $f_\kappa(s), F_\kappa(s)$ by

$$(1+o(1))f_\kappa(s)y\prod_{p<z}\left(1-\frac{\kappa(p)}{p}\right) \leq \mathcal{S}(A,z) \leq (1+o(1))F_\kappa(s)y\prod_{p<z}\left(1-\frac{\kappa(p)}{p}\right),$$

with $f_\kappa(s)$ as large as possible (resp. $F_\kappa(s)$ as small as possible) given that the above inequality holds for all choices of A satisfying (6.1). Selberg [28] has shown (in a much more general context) that the functions $f_\kappa(s), F_\kappa(s)$ are continuous, monotone, and computable for $s > 1$, that they do not change if we replace (6.1) with (6.2), and that they tend to 1 exponentially as s goes to infinity. We'll go over the arguments used to prove these claims in this chapter.

More specifically, we'll see that $f_\kappa(s)$ and $F_\kappa(s)$ can be defined as follows. Let $\mathcal{M}$ be the collection of all finite multisubsets of $[0,1]$, and for $S \in \mathcal{M}$ let $\Sigma(S)$ be the sum of the elements of S and $|S|$ be the number of elements of S (both counted with multiplicity). When we write sums like $\sum_{A\subseteq S}$, we also count subsets A with multiplicity, so such a sum will always have $2^{|S|}$ summands. Let $\lambda : \mathcal{M} \to \mathbb{R}$ be a piecewise continuous function supported on S with $\Sigma(S) \leq 1$, and define a function $\theta : \mathcal{M} \to \mathbb{R}$ by

$$\theta(S) = \sum_{A\subseteq S}\lambda(A).$$

We say that (λ, θ) forms an upper (resp. lower) bound sieve with sifting limit s if λ is supported on multisubsets of $[0, \frac{1}{s}]$, $\theta(\emptyset) = \lambda(\emptyset) \geq 1$ (resp. $\theta(\emptyset) \leq 1$), and $\theta(S) \geq 0$ (resp. $\theta(S) \leq 0$) for all $S \subseteq [0, \frac{1}{s}]$ with $|S| \geq 1$. Then

$$F_\kappa(s) = \inf_{(\lambda,\theta)\geq 0}\sum_{n=0}^{\infty}\frac{\kappa^n}{n!}\int_0^{\frac{1}{s}}\cdots\int_0^{\frac{1}{s}}\theta(x_1,...,x_n)\frac{dx_1}{x_1}\cdots\frac{dx_n}{x_n}, \tag{6.3}$$

where the infimum is over all upper bound sieves (λ, θ) with sifting limit s, and there is a similar formula for $f_\kappa(s)$ (note that when $f_\kappa(s) = 0$, we will typically have $\lambda(\emptyset) = 0$).

6.1 Setup

We assume that $s = \frac{\log(y)}{\log(z)}$ and κ are fixed, and that there is a sequence $z_1, z_2, ...$ going off to infinity as well as a sequence of asymptotically good sieves (λ^j, θ^j) with

$$\theta^j(d) = \sum_{k|d}\lambda_k^j$$

such that $\theta^j(d) \geq 0$ if these are upper bound sieves, or $\theta^j(d) \leq 0$ for $d \mid P_{z_j}, d > 1$ if these are lower bound sieves. If these sieves are any good, then in particular their error terms must be under

control, so we must have

$$\sum_{d|P_{z_j}} |\lambda_d^j|\kappa(d) \ll z_j^s.$$

Finally, we assume that the main terms of these sieves approach the optimal main terms. The following formula is crucial.

Proposition 32. *If (λ, θ) satisfy $\theta(d) = \sum_{k|d} \lambda_k$ and κ is a multiplicative function, then we have*

$$\sum_{d|P_z} \frac{\lambda_d \kappa(d)}{d} = \prod_{p<z} \Big(1 - \frac{\kappa(p)}{p}\Big) \sum_{d|P_z} \frac{\theta(d)\kappa(d)}{\varphi_\kappa(d)},$$

where φ_κ is the multiplicative function given by $\varphi_\kappa(p) = p - \kappa(p)$.

Thus, we assume that

$$\lim_{j\to\infty} \sum_{d|P_{z_j}} \frac{\theta^j(d)\kappa(d)}{\varphi_\kappa(d)} = \begin{cases} F_\kappa(s) & \text{if } (\lambda^j, \theta^j) \text{ are upper bound sieves,} \\ f_\kappa(s) & \text{if } (\lambda^j, \theta^j) \text{ are lower bound sieves.} \end{cases}$$

6.2 Ignoring the small primes

In this section, we'll show that we can basically ignore the small primes without affecting the main terms of our upper and lower bounds too much. The argument here is based on Section 6 of [28].

Theorem 29. *Let $\mathcal{P}_1, \mathcal{P}_2$ be two disjoint sets of primes, let $P_i = \prod_{p\in\mathcal{P}_i} p$, and suppose we have upper and lower bound sieves $(\lambda^{i,\pm}, \theta^{i,\pm})$, with $\lambda_d^{i,\pm}$ supported on $d \mid P_i$, $\lambda_1^{i,\pm} = 1$, and*

$$\pm\theta^{i,\pm}(d) = \pm \sum_{k|d} \lambda_k^{i,\pm} \geq 0$$

for $d \mid P_i, d > 1$. Then we can define upper and lower bound sieves $(\lambda^\pm, \theta^\pm)$ for the set of primes $\mathcal{P} = \mathcal{P}_1 \cup \mathcal{P}_2$ by

$$\lambda_d^+ = \lambda_{d_1}^{1,+}\lambda_{d_2}^{2,+}, \quad \theta^+(d) = \theta^{1,+}(d_1)\theta^{2,+}(d_2)$$

and

$$\lambda_d^- = \lambda_{d_1}^{1,+}\lambda_{d_2}^{2,-} + \lambda_{d_1}^{1,-}\lambda_{d_2}^{2,+} - \lambda_{d_1}^{1,+}\lambda_{d_2}^{2,+}, \quad \theta^-(d) = \theta^{1,-}(d_1)\theta^{2,-}(d_2) - (\theta^{1,+}(d_1) - \theta^{1,-}(d_1))(\theta^{2,+}(d_2) - \theta^{2,-}(d_2)),$$

for $d \mid P = \prod_{p\in\mathcal{P}} p$, where $d_i = \gcd(d, P_i)$. If

$$\sum_{d|P_i} \frac{\lambda_d^{i,+}\kappa(d)}{d} = F_i \prod_{p\in\mathcal{P}_i} \Big(1 - \frac{\kappa_p}{p}\Big), \quad \sum_{d|P_i} \frac{\lambda_d^{i,-}\kappa(d)}{d} = f_i \prod_{p\in\mathcal{P}_i} \Big(1 - \frac{\kappa_p}{p}\Big),$$

then we have

$$\sum_{d|P} \frac{\lambda_d^+ \kappa(d)}{d} = F \prod_{p \in \mathcal{P}} \Big(1 - \frac{\kappa_p}{p}\Big), \quad \sum_{d|P} \frac{\lambda_d^- \kappa(d)}{d} = f \prod_{p \in \mathcal{P}} \Big(1 - \frac{\kappa_p}{p}\Big),$$

where

$$F = F_1 F_2, \quad f = f_1 f_2 - (F_1 - f_1)(F_2 - f_2).$$

In particular, if $F_1, f_1 = 1 + O(\epsilon)$ *and* $f_2, F_2 = O(1)$*, then*

$$F = F_2 + O(\epsilon), \quad f = f_2 + O(\epsilon).$$

Corollary 7. *Let* $\eta > 2\epsilon > 0$*. If* $P_{z^\epsilon, z} = \prod_{z^\epsilon \leq p < z} p$ *and we have upper and lower bound sieves* $(\lambda^{\epsilon,\pm}, \theta^{\epsilon,\pm})$ *such that the* $\lambda_d^{\epsilon,\pm}$ *are bounded by a constant* C *and supported on* $d \mid P_{z^\epsilon, z}$ *with* $d < z^{s-\eta}$ *and* $\pm\theta^{\epsilon,\pm}(d) \geq 0$ *for* $d \mid P_{z^\epsilon, z}, d > 1$*, then we can construct upper and lower bound sieves* $(\lambda^\pm, \theta^\pm)$ *with the* $\lambda_d^\pm$ *bounded by* $3C \cdot 3^{\omega(d)}$ *and supported on* $d < z^{s-\eta/2}$*,* $\pm\theta^\pm(d) \geq 0$ *for* $d \mid P_z, d > 1$*, and such that if*

$$\sum_{d|P_{z^\epsilon, z}} \frac{\lambda_d^{\epsilon,+} \kappa(d)}{d} = F_\epsilon \prod_{z^\epsilon \leq p < z} \Big(1 - \frac{\kappa_p}{p}\Big), \quad \sum_{d|P_{z^\epsilon, z}} \frac{\lambda_d^{\epsilon,-} \kappa(d)}{d} = f_\epsilon \prod_{z^\epsilon \leq p < z} \Big(1 - \frac{\kappa_p}{p}\Big),$$

with $f_\epsilon, F_\epsilon = O(1)$*, then we have*

$$\sum_{d|P_z} \frac{\lambda_d^+ \kappa(d)}{d} = F \prod_{p < z} \Big(1 - \frac{\kappa_p}{p}\Big), \quad \sum_{d|P_z} \frac{\lambda_d^- \kappa(d)}{d} = f \prod_{p < z} \Big(1 - \frac{\kappa_p}{p}\Big),$$

with

$$F = F_\epsilon + O(e^{-\frac{\eta}{\epsilon}}), \quad f = f_\epsilon + O(e^{-\frac{\eta}{\epsilon}}).$$

Proof. Apply the previous theorem, using the Fundamental Lemma (see Corollary 6) upper and lower bound sieves supported on $d \mid P_{z^\epsilon}, d < z^{\eta/2}$ to handle the primes below z^ϵ. □

Note that conversely, starting from any upper bound sieve (λ^+, θ^+), we can restrict the support of λ_d^+ to $d \mid P_{z^\epsilon, z}$ to get an upper bound sieve for the set of primes between z^ϵ and z, and that the main term of the resulting sieve will only improve, since the new main term is equal to

$$\sum_{d|P_{z^\epsilon, z}} \frac{\theta^+(d)\kappa(d)}{\varphi_\kappa(d)} \leq \sum_{d|P_z} \frac{\theta^+(d)\kappa(d)}{\varphi_\kappa(d)}.$$

Similar reasoning holds for lower bound sieves.

We can also prove that the sifting functions $F_\kappa(s), f_\kappa(s)$ are continuous in s, by taking a given sieve, increasing z a little bit, and using a trivial sieve (such as the union bound) to handle the new large primes.

Proposition 33. *The functions $F_\kappa(s), f_\kappa(s)$ are monotone and continuous in s.*

6.3 Bounding the sieve weights

This argument is from Section 5 of [28].

First, note that we have

$$\sum_d \frac{\lambda_d \kappa(d)}{d} = \prod_{p<z} \Big(1 - \frac{\kappa(p)}{p}\Big) \sum_d \frac{\theta(d)\kappa(d)}{\varphi_\kappa(d)},$$

so

$$\sum_d \frac{\theta(d)\kappa(d)}{\varphi_\kappa(d)}$$

is asymptotically equal to either $F_\kappa(s)$ (if (λ, θ) is an optimal upper bound sieve) or to $f_\kappa(s)$ (if (λ, θ) is an optimal lower bound sieve). In particular, this quantity remains bounded.

Our goal is to show that $|\lambda_d|$ is in some sense bounded on average. We do this as follows: first, we let $P_{z^\epsilon, z}$ be the product of primes between z^ϵ and z. Then from

$$\lambda_d = \sum_{k|d} \mu(d/k)\theta(k)$$

we have

$$\begin{aligned}
\sum_{d|P_{z^\epsilon,z}} \frac{\kappa(d)}{d}|\lambda_d| &\le \sum_{d|P_{z^\epsilon,z}} \frac{\kappa(d)}{d} \sum_{k|d} |\theta(k)| \\
&\le \sum_{d|P_{z^\epsilon,z}} \frac{\kappa(d)}{d} \sum_{k} \frac{|\theta(k)|\kappa(k)}{k} \\
&\le \prod_{z^\epsilon \le p < z} \Big(1 + \frac{\kappa_p}{p}\Big) \sum_k \frac{|\theta(k)|\kappa(k)}{\varphi_\kappa(k)}.
\end{aligned}$$

Asymptotically, the first factor approaches $\epsilon^{-\kappa}$, and the second factor approaches either $F_\kappa(s)$ or $2 - f_\kappa(s)$. Summarizing, we have the following bound.

Proposition 34. *If (λ, θ) is an upper or lower bound sieve whose main term is $C \cdot \prod_{p<z}(1 - \frac{\kappa_p}{p})$, then for any $\epsilon > 0$ we have*

$$\sum_{d|P_{z^\epsilon,z}} \frac{\kappa(d)}{d}|\lambda_d| \le \max(C, 2 - C)\epsilon^{-\kappa + o(1)}.$$

6.4 Averaging argument

The argument in this section is based on Section 8 of [28].

Suppose we have a sequence of z_j and a sequence of upper or lower bound sieves (λ^j, θ^j) with λ^j_d supported on $d \mid P_{z_j}$, with remainder terms bounded by

$$\sum_{d|P_z} \kappa(d)|\lambda^j_d| \ll z_j^s,$$

and main terms satisfying

$$\lim_{j\to\infty} \sum_{d|P_z} \frac{\theta^j(d)\kappa(d)}{\varphi_\kappa(d)} \in \{F_\kappa(s), f_\kappa(s)\}.$$

We want to somehow average out these sieves to get an asymptotic sieve which gives a similar main term. To do this, we first fix some small $\epsilon > 0$ and ignore all the primes below z_j^ϵ. Next, we will divide the collection of primes between z_j^ϵ and z_j into N ranges (N large but fixed), and treat all of the primes in a given range the same way. To define these ranges, we choose a geometric progression $t_0, ..., t_N$ with $t_0 = \epsilon$, $t_N = 1$, and for a fixed j we set

$$\mathcal{P}_i = \{z_j^{t_{i-1}} \le p < z_j^{t_i}\}.$$

Note that asymptotically, we have

$$\sum_{p\in\mathcal{P}_i} \frac{\kappa_p}{p} = (\kappa + o(1))(\log\log(z_j^{t_i}) - \log\log(z_j^{t_{i-1}})) = (\kappa + o(1))\log(\tfrac{t_i}{t_{i-1}}) = \kappa\frac{\log(1/\epsilon)}{N} + o(1). \quad (P_i)$$

We now define functions $\ell^j_{N,\epsilon}(i_1, ..., i_k)$ by

$$\begin{aligned}\ell^j_{N,\epsilon}(i_1, ..., i_k) &= \frac{\sum_{\substack{p_1\in\mathcal{P}_{i_1},...,p_k\in\mathcal{P}_{i_k}\\ p_1,...,p_k \text{ distinct}}} \frac{\lambda^j_{p_1\cdots p_k}\kappa(p_1\cdots p_k)}{p_1\cdots p_k}}{\sum_{p_1\in\mathcal{P}_{i_1},...,p_k\in\mathcal{P}_{i_k}} \frac{\kappa(p_1\cdots p_k)}{p_1\cdots p_k}} \\ &= \Big(\frac{N}{\kappa\log(1/\epsilon)} + o(1)\Big)^k \sum_{\substack{p_1\in\mathcal{P}_{i_1},...,p_k\in\mathcal{P}_{i_k}\\ p_1,...,p_k \text{ distinct}}} \frac{\lambda^j_{p_1\cdots p_k}\kappa(p_1\cdots p_k)}{p_1\cdots p_k}\end{aligned}$$

for $1 \le i_1, ..., i_k \le N$. By the previous section, we have

$$|\ell^j_{N,\epsilon}(i_1, ..., i_k)| \le \Big(\frac{N}{\kappa\log(1/\epsilon)} + o(1)\Big)^k \max(F_\kappa(s), 2 - f_\kappa(s))\epsilon^{-\kappa+o(1)},$$

so the averages $\ell^j_{N,\epsilon}(i_1, ..., i_k)$ are bounded in absolute independently of j. Thus by compactness we

can choose a subsequence $j_1, ...$ of the js such that the limits

$$\ell_{N,\epsilon}(i_1, ..., i_k) = \lim_{m\to\infty} \ell^{j_m}_{N,\epsilon}(i_1, ..., i_k)$$

exist for all $1 \le i_1, ..., i_k \le N$. The $\ell_{N,\epsilon}$s will become our blueprint for a sieve which has a nearly optimal main term.

Next we prove the support of the functions $\ell_{N,\epsilon}$ is small. Suppose that $i_1, ..., i_k$ have $t_{i_1-1} + \cdots + t_{i_k-1} > s$. Then for each j, by our assumed bound on the remainder terms we have

$$\begin{aligned}|\ell^j_{N,\epsilon}(i_1, ..., i_k)| &\le \Big(\frac{N}{\kappa\log(1/\epsilon)} + o(1)\Big)^k \frac{1}{z_j^{t_{i_1-1}} \cdots z_j^{t_{i_k-1}}} \sum_{\substack{p_1\in\mathcal{P}_{i_1},...,p_k\in\mathcal{P}_{i_k}\\ p_1,...,p_k \text{ distinct}}} |\lambda^j_{p_1\cdots p_k}|\kappa(p_1\cdots p_k)\\ &\ll \Big(\frac{N}{\kappa\log(1/\epsilon)} + o(1)\Big)^k \frac{z_j^s}{z_j^{t_{i_1-1}} \cdots z_j^{t_{i_k-1}}},\end{aligned}$$

and in the limit this goes to 0. In fact, the same argument shows that we have the slightly stronger bound

$$\lim_{j\to\infty} \sum_{\substack{i_1,...i_k\le N\\ t_{i_1-1}+\cdots+t_{i_k-1}>s}} |\ell^j_{N,\epsilon}(i_1, ..., i_k)| = 0.$$

Finally, we can define a sieve $(\lambda^{N,\epsilon}, \theta^{N,\epsilon})$ on the primes between z^ϵ and $z^{\epsilon^{2/N}}$ by the simple step function

$$\lambda^{N,\epsilon}_{p_1\cdots p_k} = \ell_{N,\epsilon}(i_1 + 2, ..., i_k + 2),$$

for $p_1 \in \mathcal{P}_{i_1}, ..., p_k \in \mathcal{P}_{i_k}$, $i_1, ..., i_k \le N - 2$. Then $\lambda^{N,\epsilon}_{p_1\cdots p_k}$ is supported on $p_1\cdots p_k$ such that if $p_j \in \mathcal{P}_{i_j}$, we have $\sum_j t_{i_j+1} \le s$. Since $t_{i_j} = \epsilon^{1/N} t_{i_j+1}$, this gives $\sum_j t_{i_j} \le \epsilon^{1/N} s$, so $\lambda^{N,\epsilon}_d$ is supported on $d \le z^{\epsilon^{1/N}s}$. Since the $\lambda^{N,\epsilon}_d$s only take finitely many different values, this gives us the remainder bound

$$\sum_{d|P_z} \kappa(d)|\lambda^{N,\epsilon}_d| \ll z^{\epsilon^{1/N}s}\log(z)^\kappa.$$

If the (λ^j, θ^j) are all upper (resp. lower) bound sieves, then $(\lambda^{N,\epsilon}, \theta^{N,\epsilon})$ is also an upper (resp. lower) bound sieve, since we have

$$\theta^{N,\epsilon}(p_1\cdots p_k) = \Big(\frac{N}{\kappa\log(1/\epsilon)}\Big)^k \lim_{m\to\infty} \sum_{\substack{q_1\in\mathcal{P}_{i_1+2},...,q_k\in\mathcal{P}_{i_k+2}\\ q_1,...,q_k \text{ distinct}}} \frac{\theta^{j_m}(q_1\cdots q_k)\kappa(q_1\cdots q_k)}{\varphi_\kappa(q_1\cdots q_k)}$$

for $p_1 \in \mathcal{P}_{i_1}, ..., p_k \in \mathcal{P}_{i_k}$. The main term is

$$\lim_{z\to\infty} \sum_{\substack{k\geq 0\\ i_1,\dots,i_k\leq N-2}} \sum_{\substack{p_1\in\mathcal{P}_{i_1},\dots,p_k\in\mathcal{P}_{i_k}\\ p_1,\dots,p_k \text{ distinct}}} \frac{\theta^{N,\epsilon}(p_1\cdots p_k)\kappa(p_1\cdots p_k)}{\varphi_\kappa(p_1\cdots p_k)}$$

$$= \lim_{m\to\infty} \sum_{\substack{k\geq 0\\ i_1,\dots,i_k\leq N-2}} \sum_{\substack{q_1\in\mathcal{P}_{i_1+2},\dots,q_k\in\mathcal{P}_{i_k+2}\\ q_1,\dots,q_k \text{ distinct}}} \frac{\theta^{j_m}(q_1\cdots q_k)\kappa(q_1\cdots q_k)}{\varphi_\kappa(q_1\cdots q_k)}$$

$$= \lim_{m\to\infty} \sum_{d|P_{z^{\epsilon(N-2)/N},z}} \frac{\theta^{j_m}(d)\kappa(d)}{\varphi_\kappa(d)},$$

which is closer to 1 than $F_\kappa(s)$ if it is an upper bound sieve or closer to 1 than $f_\kappa(s)$ if it is a lower bound sieve.

Finally, we have to incorporate the primes below z^ϵ and the primes between $z^{\epsilon^{2/N}}$ and z into our sieve. The effect of incorporating the primes between $z^{\epsilon^{2/N}}$ and z is small as long as $\epsilon^{2/N}$ is sufficiently close to 1, by the continuity of $F_\kappa(s), f_\kappa(s)$. Since $\lambda_d^{N,\epsilon}$ is supported on $d \leq z^{\epsilon^{1/N}s}$, if we take $\eta = (1-\epsilon^{1/N})s$, we see that the effect of incorporating the small primes is small as long as η/ϵ is sufficiently large, by Corollary 7. If we choose $\epsilon = \frac{1}{N}$ then we will have

$$1 - \epsilon^{1/N} = \frac{\log(N)}{N} + O\big(\tfrac{\log(N)^2}{N^2}\big),$$

so the effect of incorporating the missing primes will go to 0 as $N \to \infty$.

Summing everything up, we have shown that there are near-optimal sieves having the following very simple form.

Theorem 30. *For any κ, s with $s > 1$ and any $\delta > 0$, there is an $\eta > 0$ and there are upper and lower bound sieves $(\lambda^\pm, \theta^\pm)$ such that $\lambda_d^\pm$ is supported on $d \mid P_z$, $d < z^{s-\eta}$, with $|\lambda_d^\pm| \ll 3^{\omega(d)}$ for all d, and such that the main terms have*

$$\sum_{d|P_z} \frac{\theta^+(d)\kappa(d)}{d} \leq F_\kappa(s) + \delta$$

and

$$\sum_{d|P_z} \frac{\theta^-(d)\kappa(d)}{d} \geq f_\kappa(s) - \delta.$$

Moreover, these sieves can be built by combining a fundamental lemma sieve to handle the small primes with a sieve having "piecewise constant" sieve weights λ_d to handle the remaining primes.

As a consequence, we can show that replacing the assumption (6.1) with (6.2) does not change the main term of the sieve.

Corollary 8. *Suppose that A satisfies*

$$\left||A_d| - \kappa(d)\frac{y}{d}\right| \ll \kappa(d)\frac{y}{d\log(y/d)^{2\kappa+\epsilon}}$$

for some $\epsilon > 0$, and that sieve weights λ_d are chosen as in the Theorem 30 (with κ, s, δ fixed). Then the remainder term in the resulting sieve is asymptotically smaller than the main term, that is, we have

$$\sum_d |\lambda_d|\kappa(d)\frac{y}{d\log(y/d)^{2\kappa+\epsilon}} \ll \frac{y}{\log(y)^{\kappa+\epsilon+o(1)}}.$$

Proof. Since the λ_d are supported on d with $d < z^{s-\eta}$ (with $\eta > 0$ depending only on δ), we have

$$\log(y/d) \geq \eta\log(z).$$

Plugging this in, we get

$$\sum_d |\lambda_d|\kappa(d)\frac{y}{d\log(y/d)^{2\kappa+\epsilon}} \ll \frac{y}{(\eta\log(z))^{2\kappa+\epsilon}}\sum_d \frac{|\lambda_d|\kappa(d)}{d}.$$

By the argument of Proposition 34, we have

$$\sum_d \frac{|\lambda_d|\kappa(d)}{d} \leq \prod_{p<z}\left(1+\frac{\kappa_p}{p}\right)\max(F_\kappa(s)+\delta, 2-f_\kappa(s)+\delta) \ll \log(z)^{\kappa+o(1)}.$$

Putting these bounds together completes the proof. □

6.5 Selberg's proposed algorithm

Based on the argument in the previous section, we can extract an algorithm (Algorithm 2) for approximating $F_\kappa(s)$, taking a parameter N and producing an upper bound on $F_\kappa(s)$ as output. If we trace through the argument used in the previous section more carefully, we can extract explicit bounds on how big we need to take N in order to guarantee that our upper bound is within δ of the true value of $F_\kappa(s)$. The algorithm for computing $f_\kappa(s)$ is similar.

6.6 Combinatorial reformulation of sifting functions

At this point we can give formulas for the sifting functions F_κ, f_κ which have nothing to do with number theory, and are purely combinatorial in nature. We will replace the set of primes below $z = y^{\frac{1}{s}}$ with the interval $[0, \frac{1}{s}]$, with the prime p corresponding to the real number $\frac{\log(p)}{\log(y)}$, and we will replace the collection of $d \mid P_z$ with the collection of subsets of $[0, \frac{1}{s}]$, with d corresponding to $\{\frac{\log(p)}{\log(y)} \mid p \mid d\}$.

Algorithm 2 Approximate $F_\kappa(s)$

procedure APPROXIMATE-$F(\kappa,s,N)$
  Set $\epsilon \leftarrow \frac{1}{N}$.
  Set $t_i \leftarrow \epsilon^{1-\frac{i}{N}}$ for $0 \le i \le N$.
  Define $\mathcal{N} \subset \mathbb{N}^N$ by $\mathcal{N} \leftarrow \{(n_1,...,n_N) \mid \sum_{i=1}^N n_i t_i \le \epsilon^{\frac{1}{N}} s\}$.
  Define $c : \mathcal{N} \to \mathbb{R}$ by $c_\kappa(n_1,...,n_N) \leftarrow \prod_{i=1}^N \frac{1}{n_i!}\left(\kappa \frac{\log(1/\epsilon)}{N}\right)^{n_i}$. ▷ see (P_i)
  Let $\mathcal{C}_\mathcal{N}$ be the (convex) set of $\lambda : \mathcal{N} \to \mathbb{R}$ such that $\lambda(\overline{0}) = 1$ and such that for all $(n_1,...,n_N) \in \mathbb{N}^N$ we have $\sum_{\overline{e}\in\mathcal{N}} \lambda(\overline{e}) \prod_{i=1}^N \binom{n_i}{e_i} \ge 0$.
  Find $\lambda \in \mathcal{C}_\mathcal{N}$ such that $\sum_{\overline{e}\in\mathcal{N}} c_\kappa(\overline{e})\lambda(\overline{e})$ is within ϵ of its minimum value. ▷ see Section 2.3
  Set $\eta \leftarrow (1-\epsilon^{1/N})s$.
  Set $F_1 \leftarrow \frac{1}{1-\exp\left(-\frac{\eta}{2\epsilon}\log(\frac{\eta}{2e\epsilon\kappa})-\kappa\right)}$. ▷ We have $F_\kappa(\eta/\epsilon) \le F_1$ by Proposition 28
  Set $F_2 \leftarrow \epsilon^{-\kappa}\sum_{\overline{e}\in\mathcal{N}} c_\kappa(\overline{e})\lambda(\overline{e})$.
  return F_1F_2. ▷ F_1F_2 is an upper bound on $F_\kappa(s)$ by Theorem 29

Definition 14. Let $\mathcal{M}$ be the collection of all finite multisubsets of $[0,1]$, and for $S \in \mathcal{M}$ let $\Sigma(S)$ be the sum of the elements of S and $|S|$ be the number of elements of S (both counted with multiplicity). When we write sums like $\sum_{A\subseteq S}$, we also count subsets A with multiplicity, so such a sum will always have $2^{|S|}$ summands.

Definition 15. Let $\lambda : \mathcal{M} \to \mathbb{R}$ be a piecewise continuous function supported on S with $\Sigma(S) \le 1$, and define a function $\theta : \mathcal{M} \to \mathbb{R}$ by

$$\theta(S) = \sum_{A\subseteq S} \lambda(A).$$

We say that (λ,θ) forms an upper (resp. lower) bound sieve with sifting limit s if λ is supported on multisubsets of $[0,\frac{1}{s}]$, $\theta(\emptyset) = \lambda(\emptyset) \ge 1$ (resp. $\theta(\emptyset) \le 1$), and $\theta(S) \ge 0$ (resp. $\theta(S) \le 0$) for all $S \subseteq [0,\frac{1}{s}]$ with $|S| \ge 1$.

Theorem 31. *We have*

$$F_\kappa(s) = \inf_{(\lambda,\theta)\ge 0} \sum_{n=0}^\infty \frac{\kappa^n}{n!} \int_0^{\frac{1}{s}} \cdots \int_0^{\frac{1}{s}} \theta(x_1,...,x_n) \frac{dx_1}{x_1} \cdots \frac{dx_n}{x_n},$$

$$f_\kappa(s) = \sup_{(\lambda,\theta)\le 0} \sum_{n=0}^\infty \frac{\kappa^n}{n!} \int_0^{\frac{1}{s}} \cdots \int_0^{\frac{1}{s}} \theta(x_1,...,x_n) \frac{dx_1}{x_1} \cdots \frac{dx_n}{x_n},$$

where the infimum is over all upper bound sieves (λ,θ) with sifting limit s, and the supremum is over all lower bound sieves (λ,θ) with sifting limit s.

Chapter 7

Optimized Combinatorial sieve

7.1 Basic principle

Proposition 35. *Suppose that λ_d satisfy $\lambda_1 = 1$, and for any $d \mid P_z$ and any prime $p < z$ which is smaller than all the prime factors of d we have*

$$\lambda_d + \lambda_{pd} \leq 0. \tag{C}$$

Then

$$\mathcal{S}(A, z) \geq \sum_{d|P_z} \lambda_d |A_d|.$$

Similarly, if for all such d, p we have $\lambda_d + \lambda_{pd} \geq 0$, then $\mathcal{S}(A, z) \leq \sum_{d|P_z} \lambda_d |A_d|$.

Proof. We just need to show that for any $n \mid P_z$ with $n \neq 1$, we have

$$\sum_{d|n} \lambda_d \leq 0.$$

Let p be the least prime dividing n. Then by (C), we have

$$\sum_{d|n} \lambda_d = \sum_{d|n/p} \lambda_d + \lambda_{pd} \leq 0.$$

The upper-bound case is similar. □

Definition 16. Any collection of sieve weights λ_d satisfying the assumptions of Proposition 35 is called a *combinatorial sieve*.

By linear programming duality and the fact that each constraint involves just one or two variables, the optimal choice of weights λ_d satisfying condition (C) has the property that each λ_d is either

equal to 0, or equal to $-\lambda_{d/p}$, where p is the least prime dividing d. By induction of the number of prime factors, we see that for each $d \mid P_z$ we have

$$\lambda_d \in \{\mu(d), 0\}$$

in an optimal combinatorial sieve. If it is an optimal lower bound combinatorial sieve and d has an even number of prime factors, then for each prime p less than the smallest prime factor of d we must have $\lambda_{pd} = -\lambda_d$ in order to satisfy (C).

What are the possible "pivots" of this linear program? For each d with an even number of prime factors, we can toggle whether the value of λ_d is determined by $\lambda_d = 0$ or $\lambda_d = -\lambda_{d/p}$. If $\lambda_{d/p} = 0$, this has no effect, leading to a large amount of degeneracy in the corresponding linear program. If we toggle the value of λ_d from 0 to 1, then the mapping $k \mapsto \lambda_{kd}$ for k having all prime factors less than the least prime factor of d defines a combinatorial lower bound sieve with z replaced by the least prime factor of d.

Proposition 36. *If we choose sieve weights λ_d for $d \mid P_z$ defining a combinatorial lower bound sieve with $\sum_d \frac{\lambda_d}{d} > 0$ in order to minimize the quantity*

$$w(z) = \min_{(\lambda_d)_{d|P_z} \text{ comb. lower bound sieve}} \frac{\sum_{d|P_z} |\lambda_d|}{\sum_{d|P_z} \frac{\lambda_d}{d}},$$

then for each d with an even number of prime factors, with p the least prime dividing d, we have

$$\lambda_d = -\lambda_{d/p} \iff dw(p) < w(z).$$

More explicitly, if $d = p_1 \cdots p_m$ with $z > p_1 > \cdots > p_m$, then

$$\lambda_d = \begin{cases} \mu(d) & \forall k \text{ s.t. } 2k \le m,\ p_1 \cdots p_{2k} w(p_{2k}) < w(z), \\ 0 & \text{otherwise.} \end{cases}$$

Proof. We just have to figure out which pivots are advantageous. Suppose that d_0 has an even number of prime factors, with p the least prime dividing d_0, and that currently we have $\lambda_{d_0} = 0$ and $\lambda_{d_0/p} = -1$. We would like to know whether toggling the value of λ_{d_0} to 1 can help. Let $(\lambda'_k)_{k|P_p}$ be a combinatorial lower bound sieve, so that the new value after toggling λ_{d_0} becomes

$$\frac{\sum_{d|P_z} |\lambda_d| + \sum_{k|P_p} |\lambda'_k|}{\sum_{d|P_z} \frac{\lambda_d}{d} + \sum_{k|P_p} \frac{\lambda'_k}{d_0 k}}.$$

Since $\frac{a+b}{c+d} < \frac{a}{c}$ if and only if $\frac{b}{d} < \frac{a}{c}$ (for positive a, b, c, d), this represents an improvement if and

only if

$$d_0 \frac{\sum_{k|P_p} |\lambda'_k|}{\sum_{k|P_p} \frac{\lambda'_k}{k}} < \frac{\sum_{d|P_z} |\lambda_d|}{\sum_{d|P_z} \frac{\lambda_d}{d}}.$$

Since the least possible value of the left hand side is $d_0 w(p)$, we see that λ_{d_0} should be toggled to 1 iff $d_0 w(p) < w(z)$. □

We can generalize this slightly to the case of giving good bounds in intervals which are significantly larger that $w(z)$. Define sets $\mathcal{D}^{\pm}_{z,y}$ by

$$\mathcal{D}^{-}_{z,y} = \{p_1 \cdots p_m \mid z > p_1 > \cdots > p_m, \forall k \text{ s.t. } 2k \leq m,\ p_1 \cdots p_{2k} w(p_{2k}) < y\}, \tag{D^-}$$

$$\mathcal{D}^{+}_{z,y} = \{p_1 \cdots p_m \mid z > p_1 > \cdots > p_m, \forall k \text{ s.t. } 2k+1 \leq m,\ p_1 \cdots p_{2k+1} w(p_{2k+1}) < y\}. \tag{D^+}$$

Proposition 37. *If A is an interval with $|A| = y$, then the best combinatorial lower bound sieve gives the bound*

$$\mathcal{S}(A,z) \geq \sum_{d \in \mathcal{D}^{-}_{z,y}} \mu(d)|A_d| \geq \Big(\sum_{d \in \mathcal{D}^{-}_{z,y}} \frac{\lambda_d}{d} \Big) y - |\mathcal{D}^{-}_{z,y}|,$$

and the best combinatorial upper bound sieve gives the bound

$$\mathcal{S}(A,z) \leq \sum_{d \in \mathcal{D}^{+}_{z,y}} \mu(d)|A_d| \leq \Big(\sum_{d \in \mathcal{D}^{+}_{z,y}} \frac{\lambda_d}{d} \Big) y + |\mathcal{D}^{+}_{z,y}|,$$

where $\mathcal{D}^{\pm}_{z,y}$ are given by (D^-) and (D^+), with $w(p)$ defined as in Proposition 36.

Making the asymptotic approximation

$$w(z) \asymp z^{\beta},$$

we recover the β-sieve, which is given in the lower bound case by

$$\lambda_d = \begin{cases} \mu(d) & \forall k \text{ s.t. } 2k \leq m,\ p_1 \cdots p_{2k} p_{2k}^{\beta} < z^s, \\ 0 & \text{otherwise,} \end{cases}$$

and given in the upper bound case by a similar formula where the role of odd and even are interchanged.

While it is easy to prove that $j(P_z) \leq w(z)$, in fact we can do slightly better by treating the prime 2 specially.

Proposition 38. *If $z > 2$, then $j(P_z) \leq \frac{w(z)}{2}$.*

Proof. We just need to show that $j(P_z/2) \leq w(z)/4$. This will follow if we can show that for odd d, we have $d \in \mathcal{D}^{-}_{z,w(z)}$ if and only if $2d \in \mathcal{D}^{-}_{z,w(z)}$ (since the effect of including the prime 2 on the value

of $w(z)$ is then multiplication by $\frac{1+1}{1-\frac{1}{2}} = 4$). If d has an even number of prime factors this is trivial, so assume d has an odd number of prime factors. Let $d = p_1 \cdots p_{2k+1}$, with $z > p_1 > \cdots > p_{2k+1} > 2$. If $k = 0$, then we need to show that $p_1 \cdot 2 \cdot w(2) = 2p_1 < w(z)$, that is, that $w(z) \geq 2z$ for all $z > 3$. If $k > 0$, then it is enough to show that $p_1 \cdots p_{2k+1} \cdot 2 \cdot w(2) \leq p_1 \cdots p_{2k} \cdot w(p_{2k})$, that is, that $2p_{2k+1} \leq w(p_{2k})$: again, this will follow if we can show that $w(z) \geq 2z$ for all $z > 3$.

So it remains to show that $w(z) \geq 2z$ for $z > 3$. For small values of z, this can be checked by hand. For large values of z, we can use the fact that $w(z) \geq j(P_z) \gg \frac{z \log(z)}{\log(\log(z))}$ by Theorem 3. □

7.2 The combinatorial sieve as the limit of Buchstab iteration

Buchstab iteration is based on the identity

$$\mathcal{S}(A, z) = |A| - \sum_{p<z} \mathcal{S}(A_p, p).$$

Applying this twice (to avoid dealing with upper bound sieves), we get

$$\mathcal{S}(A, z) = |A| - \sum_{p<z} |A_p| + \sum_{q<p<z} \mathcal{S}(A_{pq}, q).$$

In order to get a good lower bound, we will only keep summands $\mathcal{S}(A_{pq}, q)$ such that we can show $\mathcal{S}(A_{pq}, q) > 0$. In the case A is an interval, we see that we can show $\mathcal{S}(A_{pq}, q) > 0$ when

$$w(q) \leq |A_{pq}| = \frac{|A|}{pq} + O(1).$$

Thus, keeping the summands with $pqw(q) < |A|$, we get

$$\mathcal{S}(A, z) \geq |A| - \sum_{p<z} |A_p| + \sum_{\substack{q<p<z \\ pqw(q)<|A|}} \mathcal{S}(A_{pq}, q).$$

Applying this recursively, we get

$$\mathcal{S}(A, z) \geq \sum_{d \in \mathcal{D}^-_{z,|A|}} \mu(d)|A_d|,$$

which is exactly the optimal combinatorial sieve derived in the previous section.

7.3 The β-sieve

For any β, we define sets $\mathcal{D}_{z,y}^{\beta,\pm}$ by

$$\mathcal{D}_{z,y}^{\beta,-} = \{p_1 \cdots p_m \mid z > p_1 > \cdots > p_m, \forall k \text{ s.t. } 2k \le m,\ p_1 \cdots p_{2k} p_{2k}^{\beta} < y\}, \qquad (D^{\beta,-})$$
$$\mathcal{D}_{z,y}^{\beta,+} = \{p_1 \cdots p_m \mid z > p_1 > \cdots > p_m, \forall k \text{ s.t. } 2k+1 \le m,\ p_1 \cdots p_{2k+1} p_{2k+1}^{\beta} < y\}, \qquad (D^{\beta,+})$$

and define $F_\kappa^\beta(s), f_\kappa^\beta(s)$ by

$$F_\kappa^\beta(s) = \lim_{z\to\infty} \sum_{d \in \mathcal{D}_{z,z^s}^{\beta,+}} \frac{\mu(d)\kappa(d)}{d},$$
$$f_\kappa^\beta(s) = \lim_{z\to\infty} \sum_{d \in \mathcal{D}_{z,z^s}^{\beta,-}} \frac{\mu(d)\kappa(d)}{d}.$$

For a given κ, the best choice for β has $f_\kappa^\beta(\beta) = 0$, unless we can take $\beta = 1$ (which, as it turns out, occurs for $\kappa \le \frac{1}{2}$). The main result concerning the β-sieve in the range $\kappa > \frac{1}{2}$ is as follows.

Theorem 32 (Chapter 11 of [8], [16])**.** *Suppose that $\kappa > \frac{1}{2}$. Let $p_\kappa(s), q_\kappa(s)$ solve the equations*

$$\tfrac{d}{ds}(s p_\kappa(s)) = \kappa p_\kappa(s) - \kappa p_\kappa(s+1),$$
$$\tfrac{d}{ds}(s q_\kappa(s)) = \kappa q_\kappa(s) + \kappa q_\kappa(s+1),$$

with $\lim_{s\to\infty} s p_\kappa(s) = 1$ and $q_\kappa(s)$ not identically 0. Then the best choice for β in the β-sieve has $\beta - 1$ equal to the largest positive zero of $q_\kappa(s)$, and has

$$s^\kappa F_\kappa^\beta(s) = \frac{2(\beta-1)^{\kappa-1}}{p(\beta-1)} \qquad \beta - 1 \le s \le \beta + 1,$$
$$\tfrac{d}{ds}(s^\kappa F_\kappa^\beta(s)) = \kappa s^{\kappa-1} f_\kappa^\beta(s-1) \qquad s > \beta + 1,$$
$$\tfrac{d}{ds}(s^\kappa f_\kappa^\beta(s)) = \kappa s^{\kappa-1} F_\kappa^\beta(s-1) \qquad s > \beta.$$

When 2κ is an integer, $q_\kappa(s)$ is a polynomial of degree $2\kappa - 1$, and β is an algebraic number.

We mostly care about the case $\kappa = 1$, in which case $q_1(s) = s - 1$ and $\beta = 2$. When $\kappa = 1$, the β-sieve produces the optimal sifting functions $f(s) = f_1(s), F(s) = F_1(s)$ (see Section 8.2). Furthermore, for any interval A of length y and any fixed s we have the more precise error terms

$$f(s)\frac{y}{e^\gamma \log(z)} - (c + o(1))h(s)\frac{y}{\log(z)^2} \le \mathcal{S}(A, z) \le F(s)\frac{y}{e^\gamma \log(z)} + (c + o(1))H(s)\frac{y}{\log(z)^2},$$

where c is a computable constant, and in fact we will state an even more precise result due to Iwaniec

[14] below. The functions f, F, h, H are given by

$$\begin{aligned}
F(s) &= \frac{2e^\gamma}{s} && 1 \le s \le 3\\
\tfrac{d}{ds}\left(sF(s)\right) &= f(s-1) && s \ge 3\\
f(s) &= \frac{2e^\gamma \log(s-1)}{s} && 2 \le s \le 4\\
\tfrac{d}{ds}\left(sf(s)\right) &= F(s-1) && s \ge 2\\
H(s) &= \frac{1}{s^2} && 1 \le s \le 3\\
\tfrac{d}{ds}\left(s^2H(s)\right) &= -sh(s-1) && s \ge 3\\
h(s) &= \frac{1}{s^2}\left(1 + \frac{1}{s-1} - \log(s-1)\right) && 2 \le s \le 4\\
\tfrac{d}{ds}\left(s^2h(s)\right) &= -sH(s-1) && s \ge 2
\end{aligned}$$

Theorem 33 (Iwaniec [14])**.** *If A has*

$$\left||A_d| - \frac{y}{d}\right| \le 1$$

for all d, and if $y = z^s$ with $s < \frac{\log(y)}{\log(\log(3y))^{\frac{11}{5}}}$, then for $s \ge 3$ we have

$$\mathcal{S}(A,z) \le F(s)\prod_{p<z}\left(1-\frac{1}{p}\right)\cdot y + c\Big(1+\frac{s^2\log(s)^5}{\log(y)^2}\Big)^{5s}H(s)\frac{y}{\log(z)^2},$$

and for $s \ge 2$ we have

$$\mathcal{S}(A,z) \ge f(s)\prod_{p<z}\left(1-\frac{1}{p}\right)\cdot y - c\Big(1+\frac{s^2\log(s)^5}{\log(y)^2}\Big)^{5s}h(s)\frac{y}{\log(z)^2},$$

where c is an absolute, computable constant.

The functions F, f, H, h can also be expressed in terms of the Dickman function ρ and the Buchstab function ω (see the last two sections of Chapter 4 for the definitions and properties of ρ and ω). We have

$$\begin{aligned}
F(s) &= e^\gamma(\omega(s) - \rho'(s)),\\
f(s) &= e^\gamma(\omega(s) + \rho'(s)),\\
H(s) &= \tfrac{1}{2}(-\omega'(s) + \rho''(s)),\\
h(s) &= \tfrac{1}{2}(\omega'(s) + \rho''(s)).
\end{aligned}$$

7.4 Numerical computations

The next table summarizes the results of numerical computations $w(p)$ for p up to 10^{10}. Details of how these computations were performed can be found in the next subsection.

p	$w(p)$	$\lvert\mathcal{D}^-_{p,w(p)}\rvert$	$\Big(\sum_{d\in\mathcal{D}^-_{p,w(p)}} \frac{\mu(d)}{d}\Big)^{-1}$	$\log(p)^2$	$\frac{p^2}{w(p)}$
2	1	1	1	0.48	4
3	4	2	2	1.20	2.25
5	12	4	3	2.59	2.08333
7	25.7142	6	4.28571428	3.78	1.90555
11	49.4117	8	6.17647058	5.74	2.44880
101	2,702.91	152	17.7823441	21.29	3.77407
1,009	181,134.1	4,298	42.1438118	47.84	5.62059
10,007	14,774,064.1	183,842	80.3628340	84.84	6.77809
100,003	1.337874×10^9	10,370,628	129.006158	132.54	7.47498
1,000,003	1.267740×10^{11}	676,016,012	187.531120	190.86	7.88809
10,000,019	1.232150×10^{13}	47,905,251,846	257.205746	259.79	8.11592
100,000,007	1.211826×10^{15}	3,593,207,274,848	337.254693	339.32	8.25201
1,000,000,007	1.199471×10^{17}	280,366,672,910,696	427.822345	429.45	8.33700
10,000,000,019	1.191769×10^{19}	22,534,701,080,584,612	528.859876	530.18	8.39088

The first thing that jumps out is the excellent agreement between the fourth and fifth columns:

Conjecture 3. As $p \to \infty$, we have

$$\Big(\sum_{d\in\mathcal{D}^-_{p,w(p)}} \frac{\mu(d)}{d}\Big)^{-1} = \log(p)^2 + O(1).$$

Although it is not a proof, I can at least give a heuristic explanation for this coincidence. By the theory of the linear sieve, for $2 \le s \le 4$ and $z \to \infty$ we have

$$\sum_{d\in\mathcal{D}^-_{z,z^s}} \frac{\mu(d)}{d} \approx f(s) \prod_{p<z} (1-\tfrac{1}{p}) \approx \frac{f(s)}{e^\gamma \log(z)},$$

with

$$f(s) = \frac{2e^\gamma \log(s-1)}{s}$$

in this range. The important point is that

$$f'(2) = e^\gamma,$$

so if $y \asymp z^2$ and we let $y_1 = y \cdot z^\epsilon \approx y + \epsilon y \log(z)$, then

$$\sum_{d \in \mathcal{D}^-_{z,y_1} \setminus \mathcal{D}^-_{z,y}} \frac{\mu(d)}{d} \approx \frac{f'(2)\epsilon}{e^\gamma \log(z)} \approx \frac{\epsilon}{\log(z)},$$

while by the defining property of $\mathcal{D}^-_{z,y}$ we have

$$y \leq \frac{|\mathcal{D}^-_{z,y_1} \setminus \mathcal{D}^-_{z,y}|}{\sum_{d \in \mathcal{D}^-_{z,y_1} \setminus \mathcal{D}^-_{z,y}} \frac{\mu(d)}{d}} \leq y_1.$$

Setting $\delta \approx \epsilon y \log(z)$, we get

$$y \asymp z^2 \quad \Longrightarrow \quad |\mathcal{D}^-_{z,y+\delta} \setminus \mathcal{D}^-_{z,y}| \approx \frac{\epsilon y}{\log(z)} \approx \frac{\delta}{\log(z)^2}.$$

Since $w(p) \asymp p^2$, this gives the approximation

$$|\mathcal{D}^-_{p,w(p)}| \approx \frac{w(p)}{\log(p)^2}.$$

From this, we get

$$\sum_{d \in \mathcal{D}^-_{p,w(p)}} \frac{\mu(d)}{d} = \frac{|\mathcal{D}^-_{p,w(p)}|}{w(p)} \approx \frac{1}{\log(p)^2}.$$

It's somewhat harder to pin down the asymptotic behavior of the ratio between $w(p)$ and p^2. Based on the numerical data, the following conjecture seems reasonable.

Conjecture 4. For p sufficiently large, we have

$$8 < \frac{p^2}{w(p)} < 9.$$

In patricular, for z large we have $j(P_z) \leq \frac{z^2}{16}$.

Define C to be the limiting value of the ratio between $w(p)$ and p^2:

$$C = \lim_{p \to \infty} \frac{p^2}{w(p)}.$$

In order to verify that C is the correct limiting value, we'll try to analyze the size of the set $\mathcal{D}^-_{p,p^2/C}$ and compare it with $\frac{p^2}{C\log(p)^2}$. To this end, we define the functions $u_C(x,y), v_C(x,y)$ by

$$u_C(x,y) = \frac{C}{e^y}|\mathcal{D}^-_{e^x,e^y/C}|,$$
$$v_C(x,y) = \frac{C}{e^y}|\mathcal{D}^+_{e^x,e^y/C}|.$$

Then we have

$$u_C(x+\Delta x,y) = u_C(x,y) + \sum_{e^x\le p<e^{x+\Delta x}} \frac{1}{p} v_C(\log(p), y-\log(p)),$$
$$v_C(x+\Delta x,y) = v_C(x,y) + \sum_{\substack{e^x\le p<e^{x+\Delta x}\\ Cpw(p)<e^y}} \frac{1}{p} u_C(\log(p), y-\log(p)),$$

and these approximate solutions to the system of differential-difference equations

$$\frac{\partial}{\partial x}u(x,y) = \frac{1}{x}v(x,y-x),$$
$$\frac{\partial}{\partial x}v(x,y) = \begin{cases} \frac{1}{x}u(x,y-x) & 3x<y,\\ 0 & 3x>y.\end{cases}$$

Proposition 39. *If $u(x,y), v(x,y)$ satisfy the above differential-difference equations, then the quantity*

$$\int_{y\ge 2x} \frac{y(y-2x)}{x}u(x,y)dy + \int_{y\ge x}\frac{(y-x)^2}{x}v(x,y)dy$$

is independent of x.

Of course, if we guess the wrong value for C, then the approximation gets worse - so the sum of the integrals given above will drift somewhat with x. We can thus work backwards to get an estimate for the final value of C by guessing values for C, computing the sum of the integrals above numerically for x large, and seeing whether it matches up with the limiting value.

Given that $u(x,2x) \approx \frac{1}{x^2}$, the limiting solution to the above system of differential-difference equations is

$$\begin{aligned} u(x,y) &= \frac{2h(\frac{y}{x})}{x^2}, \\ v(x,y) &= \frac{2H(\frac{y}{x})}{x^2}, \\ \frac{d}{ds}(s^2 h(s)) &= -sH(s-1), \\ \frac{d}{ds}(s^2 H(s)) &= \begin{cases} -sh(s-1) & s > 3, \\ 0 & s < 3, \end{cases} \\ H(s) &= \frac{1}{s^2} \quad 1 \le s \le 3, \\ h(s) &= \frac{1}{s^2}(1 + \tfrac{1}{s-1} - \log(s-1)) \quad 2 \le s \le 4. \end{aligned}$$

Thus, the limiting value of the sum of the integrals in the previous Proposition is

$$\int_{s\ge 2} s(s-2)2h(s)ds + \int_{s\ge 1} (s-1)^2 2H(s)ds = 4(e^\gamma - 1) - e^{-\gamma},$$

where the integral was evaluated by expressing H, h in terms of the Dickman function and the Buchstab function using the formulas at the end of Section 7.3, and using the formulas $\omega(\infty) = e^{-\gamma}$ and $\int \rho(s)ds = \int s\rho(s)ds = e^\gamma$ from the last two sections of Chapter 4.

To sum up, we have the following speculative method for predicting the value of the constant C: pick some large x, compute $w(p)$ for $p < e^x$, guess a value for C, numerically approximate the functions $u_C(x,y), v_C(x,y)$, and adjust this guess for C based on how the value of

$$\int_{y\ge 2x} \frac{y(y-2x)}{x} u_C(x,y)dy + \int_{y\ge x} \frac{(y-x)^2}{x} v_C(x,y)dy$$

compares to $4(e^\gamma - 1) - e^{-\gamma}$ (note that since $u_C(x,y) = u_1(x, y - \log(C)), v_C(x,y) = v_1(x, y - \log(C))$, the sum of integrals above is a monotone increasing function of C). Carrying out this procedure for e^x greater than the first 10 primes, the first 100 primes, and so on, we get the following series of predictions.

$\pi(e^x)$	predicted value for C
10	3.47
100	6.73
1,000	7.78
10,000	8.16
100,000	8.30

Although the last prediction roughly matches the numerical data, it should probably be taken with a large grain of salt.

7.4.1 Algorithm for quick computation of $w(p)$

The main idea is to use the recursive structure of the sets $\mathcal{D}^-_{p,w(p)}$ to avoid enumerating each element of $\mathcal{D}^-_{p,w(p)}$ individually. We need the following definitions.

Definition 17. If $d = p_1 \cdots p_m$, $p_1 > \cdots > p_m$, is a squarefree number having at least two prime divisors, then we define the *rate-limiting prime* of d, written $r(d)$, to be the p_{2k} such that

$$p_1 \cdots p_{2k} w(p_{2k}) = \max_{2j \le m} \{p_1 \cdots p_{2j} w(p_{2j})\}.$$

We call d *basic* if $r(d)$ is the least prime divisor of d, and we call d *q-basic* if d is basic and $r(d) = q$.

Then by the definition of $\mathcal{D}^-_{p,w(p)}$, whenever $d \in \mathcal{D}^-_{p,w(p)}$ is basic, we also have $d\mathcal{D}^-_{r(d),w(r(d))} \subset \mathcal{D}^-_{p,w(p)}$. Moreover, we have the following result.

Proposition 40. *For any prime p, if $\pi(p)$ is the number of primes strictly below p, we have*

$$|\mathcal{D}^-_{p,w(p)}| = 1 + \pi(p) + \sum_{q<p} |\mathcal{D}^-_{q,w(q)}| \cdot |\{d \text{ } q\text{-basic},\ dw(q) < w(p)\}|$$

and

$$\sum_{d \in \mathcal{D}^-_{p,w(p)}} \frac{\mu(d)}{d} = 1 - \sum_{q<p} \frac{1}{q} + \sum_{q<p} \Big(\sum_{d_0 \in \mathcal{D}^-_{q,w(q)}} \frac{\mu(d_0)}{d_0} \Big) \sum_{\substack{d \text{ } q\text{-basic} \\ dw(q) < w(p)}} \frac{1}{d}.$$

The second trick we use is to note that whether d is basic (or q-basic) or not does not depend on the largest prime factor of d: the only way that the largest prime factor of d becomes relevant is the inequality $dw(r(d)) < w(p)$. So we will group together basic ds which differ only in their greatest prime factor p_1, and we will determine the range of possible values for p_1 by a binary search over primes.

As a small bonus, using this algorithm we can also compute the size of the contribution to $\mathcal{D}^-_{p,w(p)}$ from each possible rate-limiting prime q. Define sets

$$\mathcal{D}^-_{q,z,y} = \{d \in \mathcal{D}^-_{z,y},\ r(d) = q\}.$$

The following table summarizes the contribution from small rate-limiting primes q when p is either the first prime after 10^9 or the first prime after 10^{10}.

Algorithm 3 Combinatorial Sieve Algorithm

function BASIC-RECURSION(previous-prime, size, is-even, p, $w(p)$)
  count $\leftarrow 0$, sum $\leftarrow 0$
  if is-even **then**
    for previous-prime $< q < p$ **and** size$\cdot qq_+q_{++} < w(p)$ **do** ▷ q_+ is the next prime after q
      if size$\cdot q > w(q_+)$ **then**
        (smallcount, smallsum) $\leftarrow$ BASIC-RECURSION(q, size$\cdot q$, False, p, $w(p)$)
        count $\leftarrow$ count + smallcount
        sum $\leftarrow$ sum + smallsum$/q$
    high-prime $\leftarrow \max\{q$ with size$\cdot q < w(p), q < p\}$ ▷ to find high-prime, use a binary search
    count $\leftarrow$ count + π(high-prime) $-$ π(previous-prime)
    sum $\leftarrow$ sum + $\sum_{\text{previous-prime} < q \leq \text{ high-prime}} \frac{1}{q}$ ▷ partial sums $\sum_{r<q<p} \frac{1}{q}$ precomputed
  else
    for previous-prime $< q < p$ **and** size$\cdot qq_+ < w(p)$ **do**
      if size$> w(q)$ **then**
        (smallcount, smallsum) $\leftarrow$ BASIC-RECURSION(q, size$\cdot q$, True, p, $w(p)$)
        count $\leftarrow$ count + smallcount
        sum $\leftarrow$ sum + smallsum$/q$
  return (count, sum)
procedure MAIN(p)
  Precompute partial sums $\sum_{r<q<p} \frac{1}{q}$ for $r < p$
  Precompute $w(q), |\mathcal{D}^-_{q,w(q)}|, \sum_{d\in\mathcal{D}^-_{q,w(q)}} \frac{\mu(d)}{d}$ for q such that $q_+qw(q) < p^2$
  $w(p) \leftarrow p^2$, old-guess $\leftarrow -1$
  while $w(p) \neq$ old-guess **do**
    old-guess $\leftarrow w(p)$
    count $\leftarrow 1 + \pi(p)$
    sum $\leftarrow 1 - \sum_{q<p} \frac{1}{q}$
    for $q_+qw(q) < w(p)$ **do**
      (smallcount, smallsum) $\leftarrow$ BASIC-RECURSION(q, $qw(q)$, True, p, $w(p)$)
      count $\leftarrow$ count + smallcount$\cdot|\mathcal{D}^-_{q,w(q)}|$
      sum $\leftarrow$ sum + smallsum$\cdot \sum_{d\in\mathcal{D}^-_{q,w(q)}} \frac{\mu(d)}{d}$
    $w(p) \leftarrow \frac{\text{count}}{\text{sum}}$
  return ($w(p)$, count, sum)

q	$\lvert\mathcal{D}^-_{q,w(q)}\rvert$	$\lvert\mathcal{D}^-_{q,10^9,w(10^9)}\rvert$	$\frac{\lvert\mathcal{D}^-_{q,10^9,w(10^9)}\rvert}{\lvert\mathcal{D}^-_{10^9,w(10^9)}\rvert}$	$\lvert\mathcal{D}^-_{q,10^{10},w(10^{10})}\rvert$	$\frac{\lvert\mathcal{D}^-_{q,10^{10},w(10^{10})}\rvert}{\lvert\mathcal{D}^-_{10^{10},w(10^{10})}\rvert}$
2	1	50,847,533	0.0000%	455,052,510	0.0000%
3	2	18,349,760,829,536	6.5449%	1,442,620,675,334,628	6.4017%
5	4	38,333,203,290,684	13.6725%	2,996,015,319,999,088	13.2951%
7	6	24,191,486,460,984	8.6285%	2,266,779,123,561,216	10.0590%
11	8	13,520,893,437,048	4.8225%	1,178,595,771,091,176	5.2301%
13	12	12,443,247,328,332	4.4382%	957,429,548,615,856	4.2486%
17	16	11,150,038,237,104	3.9769%	747,723,477,554,192	3.3180%
19	22	11,764,005,379,280	4.1959%	727,334,597,533,786	3.2276%
23	26	10,341,770,277,488	3.6886%	620,459,111,164,568	2.7533%
29	32	9,033,164,601,856	3.2219%	566,427,988,603,328	2.5135%
31	36	7,966,641,918,492	2.8415%	526,373,588,863,692	2.3358%
37	44	7,003,305,009,756	2.4979%	499,299,190,340,280	2.2156%
41	48	5,870,924,209,440	2.0940%	441,952,828,945,728	1.9612%
43	52	5,100,448,581,228	1.8192%	400,530,155,031,500	1.7773%
47	60	4,581,582,628,560	1.6341%	375,413,661,818,040	1.6659%
53	68	3,975,647,612,556	1.4180%	338,494,002,091,784	1.5021%
59	72	3,281,982,008,040	1.1706%	287,891,823,076,704	1.2775%
61	84	3,213,337,574,496	1.1461%	287,406,444,998,736	1.2753%
67	88	2,690,678,425,864	0.9596%	245,710,266,702,384	1.0903%
71	96	2,432,622,482,976	0.8676%	225,751,386,157,440	1.0017%
73	100	2,162,057,965,000	0.7711%	203,334,439,375,000	0.9023%
79	108	1,899,204,550,344	0.6774%	181,542,616,343,748	0.8056%
83	122	1,806,077,438,460	0.6441%	175,163,828,943,888	0.7773%
89	130	1,594,174,393,110	0.5686%	157,243,449,924,470	0.6977%
97	144	1,447,331,807,088	0.5162%	145,506,973,198,608	0.6457%
> 100		76,212,984,767,906	27.1833%	6,539,699,901,209,750	29.0205%

Chapter 8

Linear sieve and the Jacobsthal function

8.1 Numerical computation - can we beat the combinatorial sieve?

It's a natural question to ask whether the optimal choice of lower bound sieve λ_d is combinatorial, given that we wish to maximize the quantity

$$\frac{\sum_{d|P_z} |\lambda_d|}{\sum_{d|P_z} \frac{\lambda_d}{d}}$$

which gives an upper bound on the Jacobsthal function $j(P_z)$. Setting this up as a linear program, we search for numbers a_d, y, and sieve weights λ_d, such that the following conditions are satisfied.

- For all d, $a_d \geq 0$.
- $a_1 = 0$ and $\lambda_1 = 1$.
- For all $d \mid P_z$, we have $-1 \leq \frac{y}{d} - \sum_{d|k} a_k \leq 1$.
- For all $d \mid P_z$ with $d > 1$, we have $\sum_{k|d} \lambda_k \leq 0$.
- We have $y = \frac{\sum_{d|P_z} |\lambda_d|}{\sum_{d|P_z} \frac{\lambda_d}{d}}$.
- If $a_d > 0$, then $\sum_{k|d} \lambda_d = 0$.
- If $\lambda_d \neq 0$, then $\frac{y}{d} - \sum_{d|k} a_k = \begin{cases} 1 & \lambda_d > 0, \\ -1 & \lambda_d < 0. \end{cases}$

Unfortunately, once z gets large this leads to an exponentially large linear program. In order to make the computation reasonable, we restrict the search by requiring that the λ_ds and the a_ds are supported on $d \leq z^{O(1)}$. If we make the support too small, then we will find no solutions to system of constraints above.

The only remaining difficulty is that checking whether the λ_d really form a valid lower bound sieve still requires checking exponentially many conditions. In the case that the λ_d happen to form a combinatorial sieve, this will follow from the stronger (and much easier to verify) constraint

$$p < z \ \ \& \ \ (q \mid d \implies p < q) \quad \implies \quad \lambda_d + \lambda_{pd} \leq 0.$$

Otherwise, we can attempt to check that the λ_d form a valid lower bound sieve by hand after verifying that

$$\sum_{k|d} \lambda_k \leq 0$$

for $1 < d \leq z^{O(1)}$, hoping against hope that the optimal sieve follows some sort of human-understandable principles.

The results of the computation end up being somewhat underwhelming: for all $z \leq 1225$, the optimal lower bound sieve ends up being combinatorial, and beyond this point the computations start to need too much memory to continue. At this point, it is tempting to conjecture that (in the case of the linear sieve) the optimal lower bound sieve is *always* combinatorial. Surprisingly, this turns out not to be the case!

Proposition 41. *If we take $z = 3185$, so that $\pi(z) = 450$, then the optimal lower bound sieve is* not *combinatorial.*

Proof. From the theory laid out in the previous chapter, we can quickly compute that the optimal combinatorial lower bound sieve gives

$$\min_{\lambda \text{ comb}} \frac{\sum_{d|P_z} |\lambda_d|}{\sum_{d|P_z} \frac{\lambda_d}{d}} = w(3185) = \frac{27{,}026}{59.7432...} = 1{,}614{,}620.4...,$$

so all we have to do is exhibit a sieve that beats this bound. Since

$$59 \cdot 43 \cdot w(43) = 59 \cdot 43 \cdot \frac{52}{12.2553...} = 1{,}616{,}777.4... > w(3185) > 1{,}294{,}059.1... = 59 \cdot 41 \cdot w(41),$$

we have $\lambda_{59 \cdot q} = 1$ if and only if $q \leq 41$ in the optimal combinatorial sieve. The idea is to modify the combinatorial lower bound sieve by using the upper bound sieve iteration rule

$$\mathcal{S}(A_{59}, 59) \leq \mathcal{S}(A_{59}, 41) - \frac{1}{2} \sum_{q \in \{47,43,41\}} \mathcal{S}(A_{59 \cdot q}, 41) + \frac{1}{2} \mathcal{S}(A_{59 \cdot 47 \cdot 43 \cdot 41}, 41).$$

Our new sieve has sieve weights given by

$$\lambda'_d = \begin{cases} \mu(d) & d \in \mathcal{D}^-_{3185,w(3185)},\ 59\cdot 41 \nmid d, \\ \frac{1}{2} & d \in 59\cdot\{47,43,41\}\cdot \mathcal{D}^-_{41,w(41)}, \\ -\frac{1}{2} & d = 59\cdot 47\cdot 43\cdot 41, \\ 0 & \text{else.} \end{cases}$$

Since $|\mathcal{D}^-_{41,w(41)}| = 48$ and $\sum_{d\in\mathcal{D}^-_{41,w(41)}} \frac{\mu(d)}{d} = 11.1449...$, we get

$$\begin{aligned} \frac{\sum_{d|P_{3185}} |\lambda'_d|}{\sum_{d|P_{3185}} \frac{\lambda'_d}{d}} &= \frac{|\mathcal{D}^-_{3185,w(3185)}| + \frac{1}{2}|\mathcal{D}^-_{41,w(41)}| + \frac{1}{2}}{\sum_{d\in\mathcal{D}^-_{3185,w(3185)}} \frac{\mu(d)}{d} + \frac{1}{2}\cdot\frac{1}{59}((\sum_{d\in\mathcal{D}^-_{41,w(41)}} \frac{\mu(d)}{d})(\frac{1}{47}+\frac{1}{43}-\frac{1}{41}) - \frac{1}{47\cdot 43\cdot 41})} \\ &= \frac{27{,}026 + \frac{1}{2}\cdot 48 + \frac{1}{2}}{\frac{1}{59.7432...} + \frac{1}{2}\cdot\frac{1}{59}(\frac{1}{11.1449...}(\frac{1}{47}+\frac{1}{43}-\frac{1}{41}) - \frac{1}{47\cdot 43\cdot 41})} \\ &= 1{,}614{,}616.5... < 1{,}614{,}620.4... = w(3185). \end{aligned}$$

□

We can easily generalize the calculation in the previous proposition, replacing $47, 43, 41$ by any three consecutive primes $p > q > r$ and replacing 59 by any number $d \in \mathcal{D}^-_{z,w(z)}$ having an odd number of prime factors all of which are greater than p, such that

$$\frac{|\mathcal{D}^-_{r,w(r)}| + 1}{(\sum_{d\in\mathcal{D}^-_{r,w(r)}} \frac{\mu(d)}{d})(\frac{1}{p}+\frac{1}{q}-\frac{1}{r}) - \frac{1}{pqr}} < \frac{w(z)}{d} < qw(q).$$

Plugging in the approximations $w(q) \asymp q^2$, $w(r) \asymp r^2$, the outer inequality is approximately equivalent to

$$\frac{r^2}{\frac{1}{p}+\frac{1}{q}-\frac{1}{r}} \leq q^3,$$

and this is satisfied to first order whenever we have $p + r < 2q$. So we can expect this to occur whenever $q - r \approx \log(q)$ and $p - q = O(1)$, which is something we should expect to occur infinitely often.

8.2 Parity problem

In this section, we'll follow the argument of Section 16 of [28] to show that there is no way to improve the main terms $F_1(s), f_1(s)$ beyond the bounds we get from the β-sieve.

The argument goes by introducing two weighted sets: we let A^+ be the weighted set of integers between 1 and y with the weight attached to n given by $1 - \lambda(n)$, where $\lambda(n) = (-1)^{\Omega(n)}$ is the

Liouville function, and let A^- be similar with the weight of n given by $1+\lambda(n)$. Set

$$\pi^{\pm}(y,z) = \mathcal{S}(A^{\pm}, z).$$

These functions are invariant under Buchstab iteration:

$$\pi^{\pm}(y,z) = \pi^{\pm}(y,w) - \sum_{w<p<z} \pi^{\mp}(y/p,p),$$

and by the prime number theorem, for $1 < s < 3$ we have

$$\pi^+(y,z) = 2(\pi(y)-\pi(z)) = \frac{2e^\gamma}{s}\frac{y}{e^\gamma \log(z)} + \frac{2}{s^2}\frac{y}{\log(z)^2} + O\left(\frac{y}{\log(z)^3}\right),$$

so (by an induction on $\lfloor s \rfloor$) we see that for any fixed $s > 1$ we have

$$\pi^+(y,z) = F(s)\frac{y}{e^\gamma \log(z)} + 2H(s)\frac{y}{\log(z)^2} + O\left(\frac{y}{\log(z)^3}\right), \tag{8.1}$$

$$\pi^-(y,z) = f(s)\frac{y}{e^\gamma \log(z)} - 2h(s)\frac{y}{\log(z)^2} + O\left(\frac{y}{\log(z)^3}\right), \tag{8.2}$$

where F, f, H, h are defined as in Section 7.3.

In order to finish the argument, we need to check that the weighted sets $A^{\pm}$ have sufficiently small remainder terms. It's clear that we do *not* have

$$\left||A_d^{\pm}| - \frac{y}{d}\right| \ll 1,$$

so we will instead appeal to Corollary 8 to see that we just need to check that we have

$$\left||A_d^{\pm}| - \frac{y}{d}\right| \ll \frac{y}{d\log(y/d)^{2+\epsilon}}$$

for some $\epsilon > 0$. From the definition of $A^{\pm}$, we see that this is equivalent to showing that

$$\Big|\sum_{n\le y/d} \lambda(n)\Big| \ll \frac{y}{d\log(y/d)^{2+\epsilon}}.$$

This bound is a well-known consequence of the zero-free region for the ζ function, even if we take ϵ to be arbitrarily large.

Although the argument above shows that we can't hope to improve on the main terms of the sieve when $\kappa = 1$, it doesn't show anything about whether we can improve on the error term. So although this rules out the possibility of showing that $j(P_z) \ll z^{2-\epsilon}$ using standard sieve-theoretic methods, it doesn't rule out the possibility of showing that, say, $j(P_z) \ll \frac{z^2}{\log(\log(z))}$.

8.3 Better bounds via smoothing the interval

Recall the better bound on the Jacobsthal function we got by smoothing the interval.

Proposition 42 (Corollary 2)**.** *If λ_d is a lower bound sieve with a positive main term, then*

$$j(P_z) \leq \sqrt{\frac{\sum_{d|P_z} |\lambda_d| d}{\sum_{d|P_z} \frac{\lambda_d}{d}}}$$

Mimicking the theory of the previous chapter, we can prove the following result.

Proposition 43. *If we choose sieve weights λ_d for $d \mid P_z$ defining a combinatorial lower bound sieve with $\sum_d \frac{\lambda_d}{d} > 0$ in order to minimize the quantity*

$$w_2(z) = \min_{(\lambda_d)_{d|P_z} \text{ comb. lower bound sieve}} \sqrt{\frac{\sum_{d|P_z} |\lambda_d| d}{\sum_{d|P_z} \frac{\lambda_d}{d}}},$$

then for each d with an even number of prime factors, with p the least prime dividing d, we have

$$\lambda_d = -\lambda_{d/p} \quad \Longleftrightarrow \quad d w_2(p) < w_2(z).$$

More explicitly, if $d = p_1 \cdots p_m$ with $z > p_1 > \cdots > p_m$, then

$$\lambda_d = \begin{cases} \mu(d) & \forall k \text{ s.t. } 2k \leq m,\ p_1 \cdots p_{2k} w_2(p_{2k}) < w_2(z), \\ 0 & \text{otherwise.} \end{cases}$$

A minor modification to the algorithm described in the previous chapter lets us efficiently compute $w_2(z)$. The next table has the results of these numerical calculations.

p	$w_2(p)$	$\sum_d \lvert\lambda_d\rvert d$	$\left(\sum_d \frac{\lambda(d)}{d}\right)^{-1}$	$2\log(p)^2$	$\frac{p^2}{w_2(p)}$
2	1	1	1	0.96	4
3	2.44948	3	2	2.41	3.67423
5	6	12	3	5.18	4.16666
7	10.7570	27	4.285714	7.57	4.55514
11	17.2183	48	6.176470	11.49	7.02739
101	657.457	15,819	27.324799	42.59	15.5158
1,009	37,892.1	17,739,135	80.940337	95.68	26.8678
10,007	3,057,053.2	59,316,124,245	157.555383	169.68	32.7570
100,003	270,233,209.1	2.846900×10^{14}	256.510463	265.09	37.0072
1,000,003	2.538610×10^{10}	1.722138×10^{18}	374.217331	381.73	39.3918
10,000,019	2.469099×10^{12}	1.183945×10^{22}	514.926644	519.58	40.5007
100,000,007	2.430356×10^{14}	8.759595×10^{25}	674.304411	678.64	41.1462
1,000,000,007	2.402520×10^{16}	6.748962×10^{29}	855.257961	858.90	41.6229
10,000,000,019	2.383290×10^{18}	5.373584×10^{33}	1057.036090	1060.37	41.9587

Conjecture 5. As $p \to \infty$, if the λ_ds are chosen as in the definition of $w_2(p)$, then we have

$$\Big(\sum_d \frac{\lambda_d}{d}\Big)^{-1} = 2\log(p)^2 + O(1).$$

Proposition 44. *If $z > 2$, then $j(P_z) \le \sqrt{\frac{2}{3}} w_2(z)$.*

Proof. We just need to show that $j(P_z/2) \le w_2(z)/\sqrt{6}$. This will follow if we can show that for odd d, we have $\lambda_{2d} = -\lambda_d$, and we check this as in Proposition 38. □

Corollary 9. *Every interval of length 1.95×10^{18} contains an integer which has no prime divisor below 10^{10}.*

Conjecture 6. For p sufficiently large, we have

$$41 < \frac{p^2}{w_2(p)} < 50.$$

In patricular, for z large we have $j(P_z) \le \frac{z^2}{50}$.

Further improvements can be made by using Theorem 17 in place of Corollary 2. It seems plausible that a very careful analysis might lead to the asymptotic bound $j(P_z) \le \frac{z^2}{100}$ for z sufficiently large.

Chapter 9

Sifting Iterations

9.1 Simple upper bound iteration

Theorem 34. *For any $w \le z$, we have*

$$\mathcal{S}(A,z) \le \mathcal{S}(A,w) - \frac{2}{3}\sum_{w\le p<z}\mathcal{S}(A_p,w) + \frac{1}{3}\sum_{w\le q<p<z}\mathcal{S}(A_{pq},w),$$

where p,q run over primes.

Proof. Let $a \in A$. We need to show that the number of times a is counted on the left hand side of the above is at least the number of times a is counted on the right. If a has any prime factors below w, then both quantities are clearly zero, so assume that a is has no prime factors below w. Suppose a has exactly k prime factors between w and z. If $k = 0$ then both sides count a once. Thus we just need to check that for any integer $k \ge 1$ we have

$$0 \le 1 - \frac{2}{3}k + \frac{1}{3}\binom{k}{2},$$

which follows from the identity

$$1 - \frac{2}{3}k + \frac{1}{3}\binom{k}{2} = \left(1-\frac{k}{2}\right)\left(1-\frac{k}{3}\right). \qquad \square$$

Corollary 10. *For any real $t \ge s \ge 2$, we have*

$$s^\kappa F_\kappa(s) \le t^\kappa F_\kappa(t) - \frac{2}{3}\kappa \int\limits_{\frac{1}{t}<x<\frac{1}{s}} t^\kappa f_\kappa(t(1-x))\frac{dx}{x} + \frac{1}{3}\kappa^2 \iint\limits_{\frac{1}{t}<y<x<\frac{1}{s}} t^\kappa F_\kappa(t(1-x-y))\frac{dx}{x}\frac{dy}{y}.$$

Remark 4. The optimal w in Theorem 34 above appears to be $w = \frac{y}{z^\beta}$, which corresponds to taking

$t = \frac{s}{s-\beta}$. Thus this upper bound iteration tends to be useful only for $2 \le s \le \beta + 1$.

9.1.1 Analogous lower bound iteration

Theorem 35. *For any $w \le z^2$, we have*

$$\mathcal{S}(A,z) \ge \mathcal{S}\Big(A,\sqrt{w}\Big) - \sum_{\sqrt{w}\le p<z} \mathcal{S}\Big(A_p,\frac{w}{p}\Big) + \frac{5}{6}\sum_{\frac{w}{p}\le q<p<z} \mathcal{S}\Big(A_{pq},\frac{w}{p}\Big)$$
$$- \frac{2}{3}\sum_{\substack{\frac{w}{p}\le r<q<p<z\\ qr<w}} \mathcal{S}\Big(A_{pqr},\frac{w}{p}\Big) - \frac{1}{2}\sum_{\frac{w}{q}\le r<q<p<z} \mathcal{S}\Big(A_{pqr},\frac{w}{p}\Big),$$

where p,q,r run over primes.

Proof. Let $a \in A$. First suppose that a has no prime factors below $\sqrt{w}$, and has exactly k prime factors between $\sqrt{w}$ and z. If k is 0, then both sides count a once. Otherwise, we need to check that for an integer $k \ge 1$ we have

$$0 \ge 1 - k + \frac{5}{6}\binom{k}{2} - \frac{1}{2}\binom{k}{3},$$

and this follows from the identity

$$1 - k + \frac{5}{6}\binom{k}{2} - \frac{1}{2}\binom{k}{3} = (1-k)\left(1-\frac{k}{3}\right)\left(1-\frac{k}{4}\right).$$

Now suppose that a has smallest prime factor $s < \sqrt{w}$. We group together all of the summands on the right hand side with a common p, $p \mid a$. In order for any such summand to be nonzero, we must have $s \ge \frac{w}{p}$, or equivalently $p \ge \frac{w}{s}$. Suppose that a has exactly k prime factors strictly below p. Then the number of times a is counted in such summands is at most

$$-1 + \frac{5}{6}k - \frac{1}{2}\binom{k}{2} = -\left(1-\frac{3k}{4}\right)\left(1-\frac{k}{3}\right),$$

and this is at most 0 unless $k = 2$. Thus the only bad case occurs when p is the third smallest prime factor of a, q is the second smallest prime factor of a, and $r = s$ is the smallest prime factor of a. If $qr < w$, then the contribution from these summands is just

$$-1 + \frac{5}{6}\cdot 2 - \frac{2}{3} = 0,$$

so the bad case only occurs when $qr \ge w$. But then since $q \ge \frac{w}{r} = \frac{w}{s}$, we can combine this bad group of summands with the group of summands where p is replaced by q, and the total number of

times a is counted in the two groups becomes

$$\Big(-1+\frac{5}{6}\cdot 2-\frac{1}{2}\Big)+\Big(-1+\frac{5}{6}\Big)=\frac{1}{6}-\frac{1}{6}=0. \qquad \square$$

Corollary 11. *For any real $s \geq t$ with $2t \geq s \geq 3$, we have*

$$\begin{aligned} s^\kappa f_\kappa(s) \geq (2t)^\kappa f_\kappa(2t) - \kappa & \int\limits_{\frac{1}{2t}<x<\frac{1}{s}} \frac{1}{(\frac{1}{t}-x)^\kappa} F_\kappa\Big(\frac{1-x}{\frac{1}{t}-x}\Big)\frac{dx}{x} \\ & + \frac{5}{6}\kappa^2 \iint\limits_{\frac{1}{t}-x<y<x<\frac{1}{s}} \frac{1}{(\frac{1}{t}-x)^\kappa} f_\kappa\Big(\frac{1-x-y}{\frac{1}{t}-x}\Big)\frac{dx}{x}\frac{dy}{y} \\ & - \frac{2}{3}\kappa^3 \iiint\limits_{\frac{1}{t}-x<z<y<x<\frac{1}{s}} \frac{1}{(\frac{1}{t}-x)^\kappa} F_\kappa\Big(\frac{1-x-y-z}{\frac{1}{t}-x}\Big)\frac{dx}{x}\frac{dy}{y}\frac{dz}{z} \\ & + \frac{1}{6}\kappa^3 \iiint\limits_{\frac{1}{t}-y<z<y<x<\frac{1}{s}} \frac{1}{(\frac{1}{t}-x)^\kappa} F_\kappa\Big(\frac{1-x-y-z}{\frac{1}{t}-x}\Big)\frac{dx}{x}\frac{dy}{y}\frac{dz}{z}. \end{aligned}$$

Remark 5. As with Theorem 34, it seems that the optimal w in Theorem 35 is $w = \frac{y}{z^\beta}$, corresponding to $t = \frac{s}{s-\beta}$. Thus this lower bound iteration tends to be useful only when $\beta + 1 \leq s \leq \beta + 2$.

9.1.2 Two miracles at $\kappa = 1$

When $\kappa = 1$, the β-sieve produces the optimal functions $f(s) = f_1(s), F(s) = F_1(s)$ (see Selberg [28]). Furthermore, we have the more precise error terms

$$f(s)\frac{y}{e^\gamma \log(z)} - (c+o(1))h(s)\frac{y}{\log(z)^2} \leq \mathcal{S}(A,z) \leq F(s)\frac{y}{e^\gamma \log(z)} + (c+o(1))H(s)\frac{y}{\log(z)^2},$$

where c is a computable constant (in fact a more precise result can be found in Iwaniec [14]). The functions f, F, h, H are given by

$$\begin{aligned}
F(s) &= \frac{2e^\gamma}{s} && 1 \le s \le 3 \\
\frac{d}{ds}\left(sF(s)\right) &= f(s-1) && s \ge 3 \\
f(s) &= \frac{2e^\gamma \log(s-1)}{s} && 2 \le s \le 4 \\
\frac{d}{ds}\left(sf(s)\right) &= F(s-1) && s \ge 2 \\
H(s) &= \frac{1}{s^2} && 1 \le s \le 3 \\
\frac{d}{ds}\left(s^2H(s)\right) &= -sh(s-1) && s \ge 3 \\
h(s) &= \frac{1}{s^2}\left(1 + \frac{1}{s-1} - \log(s-1)\right) && 2 \le s \le 4 \\
\frac{d}{ds}\left(s^2h(s)\right) &= -sH(s-1) && s \ge 2
\end{aligned}$$

It's natural to ask what happens to these functions when we apply the new upper and lower bound iterations to them.

Theorem 36. *If $\kappa = 1$, $\frac{5}{2} \le s \le 3$, and $t = \frac{s}{s-2}$, then the two sides of the inequality in Corollary 10 are precisely equal, that is*

$$sF(s) = tF(t) - \frac{2}{3}\int\limits_{\frac{1}{t}<x<\frac{1}{s}} tf(t(1-x))\frac{dx}{x} + \frac{1}{3}\iint\limits_{\frac{1}{t}<y<x<\frac{1}{s}} tF(t(1-x-y))\frac{dx}{x}\frac{dy}{y}.$$

Furthermore, in this case even the error terms match up:

$$s^2H(s) = t^2H(t) + \frac{2}{3}\int\limits_{\frac{1}{t}<x<\frac{1}{s}} t^2h(t(1-x))\frac{dx}{x} + \frac{1}{3}\iint\limits_{\frac{1}{t}<y<x<\frac{1}{s}} t^2H(t(1-x-y))\frac{dx}{x}\frac{dy}{y}.$$

Proof. Consider the right hand side of the first claimed equality as a function $\Phi(s,t)$ of s and t. Since $sF(s) = 2e^\gamma$ is constant for $s \le 3$, it's enough to check that $\frac{\partial\Phi}{\partial s} = \frac{\partial\Phi}{\partial t} = 0$ when $t = \frac{s}{s-2}$. We have

$$\frac{\partial\Phi}{\partial s} = \frac{2}{3}\frac{t}{s}f\left(t\left(1-\frac{1}{s}\right)\right) - \frac{1}{3}\int\limits_{\frac{1}{t}<x<\frac{1}{s}} \frac{t}{s}F\left(t\left(1-\frac{1}{s}-x\right)\right)\frac{dx}{x},$$

and up to a multiple of $\frac{2e^\gamma}{s-1}$ this is equal to

$$\begin{aligned}&\frac{2}{3}\log\left(t\left(1-\frac{1}{s}\right)-1\right)-\frac{1}{3}\left(\log\left(t-\frac{s}{s-1}\right)-\log\left(s-\frac{s}{s-1}\right)\right)\\=&\frac{1}{3}\log\left(t\frac{s-1}{s}-1\right)+\frac{1}{3}\log(s-2),\end{aligned}$$

which is indeed 0 when $t=\frac{s}{s-2}$. In order to calculate $\frac{\partial\Phi}{\partial t}$, first note that since $\frac{5}{2}\leq s$ we have $t=\frac{s}{s-2}\leq 5$, so for any $x,y>\frac{1}{t}$ we have $t(1-x-y)\leq t-2\leq 3$, so

$$\frac{\partial}{\partial t}\left(tF(t(1-x-y))\right)=0.$$

Thus we have

$$\frac{\partial\Phi}{\partial t}=f(t-1)-\frac{2}{3}f(t-1)-\frac{2}{3}\int\limits_{\frac{1}{t}<x<\frac{1}{s}}F(t(1-x)-1)\frac{dx}{x}+\frac{1}{3}\int\limits_{\frac{1}{t}<x<\frac{1}{s}}F(t(1-x)-1)\frac{dx}{x}+0,$$

and up to a multiple of $\frac{2e^\gamma}{t-1}$ this is equal to

$$\begin{aligned}&\frac{1}{3}\log(t-2)-\frac{1}{3}\left(\log\left(t-\frac{t}{t-1}\right)-\log\left(s-\frac{t}{t-1}\right)\right)\\=&\frac{1}{3}\log\left(s\frac{t-1}{t}-1\right),\end{aligned}$$

which is also equal to 0 when $t=\frac{s}{s-2}$.

The second claim is left as an involved exercise to the reader (alternatively, one can use the method of proof of the next theorem). □

Since the lower bound iteration is much more complicated, we need a better method of checking that it has the linear sieve as a fixed point. For this we use the following weighted sets, introduced by Selberg [28] in order to explain the parity problem: let A^+ be the weighted set of integers between 1 and y with the weight attached to n given by $1-\lambda(n)$, where $\lambda(n)=(-1)^{\Omega(n)}$, and let A^- be similar with the weight of n given by $1+\lambda(n)$. Set

$$\pi^\pm(y,z)=\mathcal{S}(A^\pm,z).$$

These functions are invariant under Buchstab iteration:

$$\pi^\pm(y,z)=\pi^\pm(y,w)-\sum_{w<p<z}\pi^\mp(y/p,p),$$

and by the prime number theorem, for $1 < s < 3$ we have

$$\pi^+(y,z) = 2(\pi(y) - \pi(z)) = \frac{2e^\gamma}{s}\frac{y}{e^\gamma \log(z)} + \frac{2}{s^2}\frac{y}{\log(z)^2} + O\left(\frac{y}{\log(z)^3}\right),$$

so for all $s > 1$ we have

$$\pi^+(y,z) = F(s)\frac{y}{e^\gamma \log(z)} + 2H(s)\frac{y}{\log(z)^2} + O\left(\frac{y}{\log(z)^3}\right), \tag{9.1}$$

$$\pi^-(y,z) = f(s)\frac{y}{e^\gamma \log(z)} - 2h(s)\frac{y}{\log(z)^2} + O\left(\frac{y}{\log(z)^3}\right). \tag{9.2}$$

Theorem 37. *If $\kappa = 1$, $\frac{7}{2} \le s \le 4$, and $t = \frac{s}{s-2}$, then the two sides of the inequality in Corollary 11 are equal, that is*

$$\begin{aligned} sf(s) = 2tf(2t) &- \int\limits_{\frac{1}{2t} < x < \frac{1}{s}} \frac{1}{\frac{1}{t}-x} F\Big(\frac{1-x}{\frac{1}{t}-x}\Big)\frac{dx}{x} \\ &+ \frac{5}{6}\iint\limits_{\frac{1}{t}-x<y<x<\frac{1}{s}} \frac{1}{\frac{1}{t}-x} f\Big(\frac{1-x-y}{\frac{1}{t}-x}\Big)\frac{dx}{x}\frac{dy}{y} \\ &- \frac{2}{3}\iiint\limits_{\frac{1}{t}-x<z<y<x<\frac{1}{s}} \frac{1}{\frac{1}{t}-x} F\Big(\frac{1-x-y-z}{\frac{1}{t}-x}\Big)\frac{dx}{x}\frac{dy}{y}\frac{dz}{z} \\ &+ \frac{1}{6}\iiint\limits_{\frac{1}{t}-y<z<y<x<\frac{1}{s}} \frac{1}{\frac{1}{t}-x} F\Big(\frac{1-x-y-z}{\frac{1}{t}-x}\Big)\frac{dx}{x}\frac{dy}{y}\frac{dz}{z}. \end{aligned}$$

Furthermore, the error terms are equal as well:

$$\begin{aligned} s^2h(s) = (2t)^2h(2t) &+ \int\limits_{\frac{1}{2t} < x < \frac{1}{s}} \frac{1}{(\frac{1}{t}-x)^2} H\Big(\frac{1-x}{\frac{1}{t}-x}\Big)\frac{dx}{x} \\ &+ \frac{5}{6}\iint\limits_{\frac{1}{t}-x<y<x<\frac{1}{s}} \frac{1}{(\frac{1}{t}-x)^2} h\Big(\frac{1-x-y}{\frac{1}{t}-x}\Big)\frac{dx}{x}\frac{dy}{y} \\ &+ \frac{2}{3}\iiint\limits_{\frac{1}{t}-x<z<y<x<\frac{1}{s}} \frac{1}{(\frac{1}{t}-x)^2} H\Big(\frac{1-x-y-z}{\frac{1}{t}-x}\Big)\frac{dx}{x}\frac{dy}{y}\frac{dz}{z} \\ &- \frac{1}{6}\iiint\limits_{\frac{1}{t}-y<z<y<x<\frac{1}{s}} \frac{1}{(\frac{1}{t}-x)^2} H\Big(\frac{1-x-y-z}{\frac{1}{t}-x}\Big)\frac{dx}{x}\frac{dy}{y}\frac{dz}{z}. \end{aligned}$$

Proof. By equations (9.1), (9.2), it's enough to check that for constant $\frac{7}{2} < s < 4$ and $w = \frac{y}{z^2}$ we

have

$$\mathcal{S}(A^-, z) = \mathcal{S}\Big(A^-, \sqrt{w}\Big) - \sum_{\sqrt{w}\le p<z} \mathcal{S}\Big(A_p^+, \frac{w}{p}\Big) + \frac{5}{6} \sum_{\frac{w}{p}\le q<p<z} \mathcal{S}\Big(A_{pq}^-, \frac{w}{p}\Big)$$
$$- \frac{2}{3} \sum_{\substack{\frac{w}{p}\le r<q<p<z \\ qr<w}} \mathcal{S}\Big(A_{pqr}^+, \frac{w}{p}\Big) - \frac{1}{2} \sum_{\frac{w}{q}\le r<q<p<z} \mathcal{S}\Big(A_{pqr}^+, \frac{w}{p}\Big) + O\left(\frac{y}{\log(z)^3}\right).$$

We have the easy inequality $z > \sqrt{w} > y^{3/14}$, and for $\sqrt{w} < p < z$ we have $\frac{w}{p} > \frac{w}{z} > y^{1/7}$ as well as $p\left(\frac{w}{p}\right)^5 > \frac{w^5}{z^4} > y$. Thus if n is a number below y which is counted by either side, then every prime factor of n must be at least $y^{1/7}$, and $\Omega(n)$ must be an even number strictly below $\max(\frac{14}{3}, 1+5) = 6$.

We need to estimate the number of ns below y which contribute more to the left and side than the right hand side. Since the number of nonsquarefree ns which can contribute to either side is at most $3y^{6/7}$, we can assume without loss that n is square free. If $n = pq$ with $p > q$ primes, we must have $z > p$ in order for n to contribute more to the left side than the right side. The number of such n is at most $z^2 < y^{4/7}$, so we may assume without loss that n has four distinct prime factors $p > q > r > s$, at least one of which is below z (so n isn't counted on the left hand side at all).

First consider the case $s \ge \sqrt{w}$. Since $n \le wz^2$, we have $z > q$. Then if n has $3 \le k \le 4$ prime factors below z, n is counted on the right hand side with multiplicity $1 - k + \frac{5}{6}\cdot\binom{k}{2} - \frac{2}{3}\cdot 0 - \frac{1}{2}\cdot\binom{k}{3} = (1-k)\left(1-\frac{k}{3}\right)\left(1-\frac{k}{4}\right) = 0$, so we get the same contribution to both sides.

Now suppose that $s < \sqrt{w}, rs \ge w$. Since $n \le wz^2$, we have $z > q$. Then if n has $3 \le k \le 4$ prime factors below z, n is counted on the right hand side with multiplicity $0-(k-1)+\frac{5}{6}\cdot\binom{k}{2} - \frac{2}{3}\cdot 0 - \frac{1}{2}\cdot\binom{k}{3} = (1-k)\left(1-\frac{k}{3}\right)\left(1-\frac{k}{4}\right) = 0$, as before.

Next suppose that $w > rs$ and $p > z$. We must have $z > q > \frac{w}{s}$ in order to get any contribution from n. Then n is counted on the right hand side with multiplicity $0 - 1 + \frac{5}{6}\cdot 2 - \frac{2}{3}\cdot 1 - \frac{1}{2}\cdot 0 = 0$, so we get the same contribution from both sides.

Thus any bad n must have $z \ge p > q$ and $w > rs$, $r > s > y^{1/7}$. The number of such n is at most $O\left(\frac{z}{\log(z)}\frac{z}{\log(z)}\frac{w}{\log(w)}\right) = O\left(\frac{y}{\log(z)^3}\right)$. □

9.2 Infinite family of iterations inspired by model problem

Here we will describe an infinite sequence of iteration rules, one for each $k \ge 1$, generalizing the upper and lower bound iteration rules described so far (which correspond to the cases $k = 1$ and $k = 2$). We will also prove an optimality result for these iteration rules.

Theorem 38. *If $k \geq 1$ and $w \leq z^k$, then*

$$\begin{aligned}(-1)^{k-1}\mathcal{S}(A,z) \leq (-1)^{k-1}\mathcal{S}\big(A, w^{1/k}\big) + (-1)^{k-2} \sum_{w^{1/k} \leq p_1 < z} \mathcal{S}\big(A_{p_1}, (\tfrac{w}{p_1})^{1/(k-1)}\big) + \cdots \\ + \sum_{\left(\frac{w}{p_1\cdots p_{k-2}}\right)^{1/2} \leq p_{k-1} < \cdots < p_1 < z} \mathcal{S}\big(A_{p_1\cdots p_{k-1}}, \tfrac{w}{p_1\cdots p_{k-1}}\big) \\ - \Big(1 - \tfrac{1}{\binom{k+2}{2}}\Big) \sum_{\frac{w}{p_1\cdots p_{k-1}} \leq p_k < \cdots < p_1 < z} \mathcal{S}\big(A_{p_1\cdots p_k}, \tfrac{w}{p_1\cdots p_{k-1}}\big) \\ + \sum_{\frac{w}{p_1\cdots p_{k-1}} \leq p_{k+1} < \cdots < p_1 < z} \left(1 - \frac{\#\{i \leq k+1 \mid wp_i \leq p_1\cdots p_{k+1}\}}{\binom{k+2}{2}}\right) \mathcal{S}\big(A_{p_1\cdots p_{k+1}}, \tfrac{w}{p_1\cdots p_{k-1}}\big).\end{aligned}$$

Proof. It's enough to prove this when A has just one element, say $A = \{a\}$. We may also assume that a is squarefree, and write $a = q_1q_2\cdots q_m$ with $q_1 < q_2 < \cdots < q_m$ and the q_is prime. We may assume also that $q_1 < z$, since otherwise the result is trivial. Thus we just need to prove that the right hand side is at least 0.

Note that every nonzero summand corresponds to some divisor $d = p_1\cdots p_j$ of a having j prime factors, $j \leq k+1$. Our strategy is to combine the nonzero summands into small groups according to the combinatorial structure of their prime factors, such that each group of summands has a nonnegative sum.

The first step is to combine the summand corresponding to $d = p_1\cdots p_j$ with $j \leq k-1$ and $p_j = q_1$ with the summand corresponding to d/p_j, and to note that these two summands exactly cancel each other out. After this step, the only summands that remain are those which have $d = p_1\cdots p_j$ with $j \geq k-1$ and $p_{k-1} > q_1$.

The next step is to group the summands corresponding to $d = p_1\cdots p_j$ with $j \geq k-1$, $p_{k-1} = q_l$ with $l > 1$, and $p_1\cdots p_{k-1}$ taking some fixed value P with $w \leq Pq_1$. If $l = 2$, then the total contribution from such d is $\frac{1}{\binom{k+2}{2}}$. If $l = 3$, then the total contribution from such d is

$$1 - \Big(1 - \tfrac{1}{\binom{k+2}{2}}\Big)\cdot 2 + \left(1 - \frac{\#\{p \in \{p_1, ..., p_{k-1}, q_2, q_1\} \mid wp \leq Pq_2q_1\}}{\binom{k+2}{2}}\right) = -\frac{\#\{i \leq k-1 \mid wp_i \leq Pq_2q_1\}}{\binom{k+2}{2}}.$$

If $l = 4$, then the total contribution from such d is at least

$$1 - \Big(1 - \tfrac{1}{\binom{k+2}{2}}\Big)\cdot 3 + \Big(1 - \tfrac{k+1}{\binom{k+2}{2}}\Big)\cdot 3 = \frac{\binom{k-1}{2}}{\binom{k+2}{2}}.$$

Finally, if $l \geq 5$ then the total contribution from such d is easily seen to be positive.

In order to balance out the negative contribution coming from groups corresponding to $P = p_1\cdots p_{k-1}, w \leq Pq_1, p_{k-1} = q_l$ with $l = 3$, we will assign portions of the positive excess from groups

corresponding to Ps with $l = 2$ or $l = 4$ to certain corresponding Ps with $l = 3$.

If $P = p_1 \cdots p_{k-1}, w \leq Pq_1, p_{k-1} = q_l$ with $l = 2$ and $m \geq 3$ is minimal such that q_m does not divide P, then we group the excess $\frac{1}{\binom{k+2}{2}}$ contribution from this P with the contributions corresponding to $P' = Pq_m/q_2$ - note that the least prime factor of P' is then necessarily equal to q_3.

If $P = p_1 \cdots p_{k-1}, w \leq Pq_1, p_{k-1} = q_l$ with $l = 4$, then we take $\frac{\binom{k-1}{2}}{\binom{k+2}{2}}$ of the excess contribution from this P, and divide it into $k-2$ pieces of sizes $\frac{1}{\binom{k+2}{2}}, \frac{2}{\binom{k+2}{2}}, ..., \frac{k-2}{\binom{k+2}{2}}$, and we assign the piece of size $\frac{i}{\binom{k+2}{2}}$ to $P_i' = Pq_3/p_{i+1}$ (noting once again that P_i' has least prime factor equal to q_3).

To finish the argument, we just have to show that for $P = p_1 \cdots p_{k-1}, w \leq Pq_1, p_{k-1} = q_l$ with $l = 3$, the total excess contribution that was assigned to P by the process described in the last two paragraphs is at least

$$\frac{\#\{i \leq k-1 \mid wp_i \leq Pq_2q_1\}}{\binom{k+2}{2}}.$$

To see this, let $m \geq 4$ be minimal such that q_m does not divide P (or let $m = k+2$ if $Pq_2q_1 = a$). For any $3 \leq j < m$, if we let $P_j' = Pq_2/q_j$, then the least prime factor of P_j' is q_2, and as long as $wq_j \leq Pq_2q_1$ we have $w \leq P_j'q_1$ and the excess of $\frac{1}{\binom{k+2}{2}}$ corresponding to P_j' is assigned to P. Additionally (in the case $m < k+2$) we let $P' = Pq_m/q_3$, and we see that the least prime factor of P' is q_4, that $w \leq Pq_1 < P'q_1$, and that $\frac{k+2-m}{\binom{k+2}{2}}$ of the excess corresponding to P' is assigned to P. Together, we see that the amount of excess which was assigned to P is at least

$$\frac{\#\{3 \leq j < m \mid wq_j \leq Pq_2q_1\}}{\binom{k+2}{2}} + \frac{k+2-m}{\binom{k+2}{2}} \geq \frac{\#\{i \leq k-1 \mid wp_i \leq Pq_2q_1\}}{\binom{k+2}{2}}. \qquad \square$$

9.2.1 Optimality at $\kappa = 1$

To see that the kth iteration rule is optimal when we set $\kappa = 1$, $w = \frac{y}{z^2}$, and $y = z^s$ with $k + \frac{3}{2} < s < k+2$, we argue as in Theorem 37 to see that we just need to prove the following bound.

Theorem 39. *If $A^{\pm}$ are weighted sets of integers between 1 and y defined as in the discussion before*

Theorem 37, then for any $k \geq 1$, if $y = z^s$ with $k + \frac{3}{2} < s < k + 2$ and $w = \frac{y}{z^2}$, we have

$$\begin{aligned}(-1)^{k-1}\mathcal{S}(A^{-^{k-1}}, z) = (-1)^{k-1}\mathcal{S}\big(A^{-^{k-1}}, w^{1/k}\big) + (-1)^{k-2} \sum_{w^{1/k} \leq p_1 < z} \mathcal{S}\big(A_{p_1}^{-^{k-2}}, (\tfrac{w}{p_1})^{1/(k-1)}\big) + \cdots \\ + \sum_{\left(\frac{w}{p_1 \cdots p_{k-2}}\right)^{1/2} \leq p_{k-1} < \cdots < p_1 < z} \mathcal{S}\big(A^+_{p_1 \cdots p_{k-1}}, \tfrac{w}{p_1 \cdots p_{k-1}}\big) \\ - \Big(1 - \tfrac{1}{\binom{k+2}{2}}\Big) \sum_{\frac{w}{p_1 \cdots p_{k-1}} \leq p_k < \cdots < p_1 < z} \mathcal{S}\big(A^-_{p_1 \cdots p_k}, \tfrac{w}{p_1 \cdots p_{k-1}}\big) \\ + \sum_{\frac{w}{p_1 \cdots p_{k-1}} \leq p_{k+1} < \cdots < p_1 < z} \left(1 - \frac{\#\{i \leq k+1 \mid w p_i \leq p_1 \cdots p_{k+1}\}}{\binom{k+2}{2}}\right) \mathcal{S}\big(A^+_{p_1 \cdots p_{k+1}}, \tfrac{w}{p_1 \cdots p_{k-1}}\big) \\ + O\Big(\frac{y}{\log(z)^3}\Big).\end{aligned}$$

Proof. Suppose that $a \leq y$ is counted a different number of times on both sides of the above. Then we necessarily have $\lambda(a) = (-1)^k$, and the least prime dividing a is less than z. In order for the contribution of a to the right hand side to be positive, there must be primes $p_1 > \cdots > p_{k-1}$ dividing a such that $p_1 < z$ and such that the least prime dividing a is at least $\frac{w}{p_1 \cdots p_{k-1}}$, so we conclude that any prime dividing a must be at least

$$\frac{w}{p_1 \cdots p_{k-1}} > \frac{w}{z^{k-1}} = \frac{y}{z^{k+1}} = z^{s-(k+1)} > \sqrt{z}.$$

In particular, the number of such a which have a square factor is $O(\frac{y}{\sqrt{z}})$, so we may assume without loss that a is square free. If a has at least $k+4$ prime factors, then since a has some collection of k prime factors whose product is at least w we have $a > w\sqrt{z}^4 = y$, a contradiction. Thus a has strictly less than $k+4$ prime factors, and since $\lambda(a) = (-1)^k$ we see that a has either k or $k+2$ prime factors.

If a has exactly k prime factors, then they must all be less than z in order for the contribution of a to the right hand side to be positive, so $a < z^k < \frac{y}{z^{3/2}}$, so the number of such a is at most $\frac{y}{z^{3/2}}$. Thus we may assume without loss that a has exactly $k+2$ prime factors, at least k of which are less than z.

If two of the prime factors of a are $\geq z$, then the remaining prime factors of a must have product at least w, so $a > wz^2 = y$, a contradiction. If one of the prime factors of a is $\geq z$ and the remaining $k+1$ prime factors of a are all $< z$, then the total contribution of a to the right hand side is precisely 0. Thus, we may assume that all of the prime factors of a are less than z.

If every product of k prime factors of a is $\geq w$, then the contribution of a is again precisely 0. Otherwise, we can write $a = q_1 \cdots q_{k+2}$ with $\sqrt{z} < q_1 < \cdots < q_{k+2}$, $q_1 \cdots q_k < w$, $q_{k+1} < z$, and $q_{k+2} < z$. Using an upper bound sieve to bound the number of possible values for $q_1 \cdots q_k$ by

$O(\frac{w}{\log(z)})$, we see that the number of such a is $O(\frac{wz^2}{\log(z)^3}) = O(\frac{y}{\log(z)^3})$. □

9.3 Working backwards

9.3.1 Setup

Let A be a (possibly weighted) set of whole numbers, and for each positive integer d set $A_d = \{a \in A, d \mid a\}$. Let κ be a real number and by abuse of notation let $\kappa : \mathbb{N} \to \mathbb{R}$ be a multiplicative function satisfying $0 \leq \kappa(p) < p$ for all p, and

$$\sum_{p \leq x} \kappa(p) \frac{\log(p)}{p} = (\kappa + o(1)) \log(x).$$

Suppose that z, y are such that for every squarefree integer d, all of whose prime factors are less than z, we have

$$\left| |A_d| - \kappa(d) \frac{y}{d} \right| \leq \kappa(d), \tag{9.3}$$

or alternatively such that for some fixed $\epsilon > 0$ and every such d we have

$$\left| |A_d| - \kappa(d) \frac{y}{d} \right| \leq \kappa(d) \frac{y}{d \log(y/d)^{2\kappa+\epsilon}}. \tag{9.4}$$

In particular, we have $|A| = y + O(1)$ in the first case, or $|A| = y + O(y/\log(y)^{2\kappa+\epsilon})$ in the second case. We want to estimate the quantity

$$\mathcal{S}(A, z) = |\{a \in A, \forall p < z \ (a, p) = 1\}|.$$

Suppose now that $y = z^s$, s a constant, y, z going to infinity. Define sifting functions $f_\kappa(s), F_\kappa(s)$ by

$$(1 + o(1)) f_\kappa(s) y \prod_{p<z} \left(1 - \frac{\kappa(p)}{p}\right) \leq \mathcal{S}(A, z) \leq (1 + o(1)) F_\kappa(s) y \prod_{p<z} \left(1 - \frac{\kappa(p)}{p}\right),$$

with $f_\kappa(s)$ as large as possible (resp. $F_\kappa(s)$ as small as possible) given that the above inequality holds for all choices of A satisfying (9.3).

Recall from Section 6.6 that $f_\kappa(s)$ and $F_\kappa(s)$ can be defined as follows. Let $\mathcal{M}$ be the collection of all finite multisubsets of $[0, 1]$, and for $S \in \mathcal{M}$ let $\Sigma(S)$ be the sum of the elements of S and $|S|$ be the number of elements of S (both counted with multiplicity). When we write sums like $\sum_{A \subseteq S}$, we also count subsets A with multiplicity, so such a sum will always have $2^{|S|}$ summands. Let $\lambda : \mathcal{M} \to \mathbb{R}$ be a piecewise continuous function supported on S with $\Sigma(S) \leq 1$, and define a

function $\theta : \mathcal{M} \to \mathbb{R}$ by

$$\theta(S) = \sum_{A \subseteq S} \lambda(A).$$

We say that (λ, θ) forms an upper (resp. lower) bound sieve with sifting limit s if λ is supported on multisubsets of $[0, \frac{1}{s}]$, $\theta(\emptyset) = \lambda(\emptyset) \geq 1$ (resp. $\theta(\emptyset) \leq 1$), and $\theta(S) \geq 0$ (resp. $\theta(S) \leq 0$) for all $S \subseteq [0, \frac{1}{s}]$ with $|S| \geq 1$. Then

$$F_\kappa(s) = \inf_{(\lambda,\theta) \geq 0} \sum_{n=0}^{\infty} \frac{\kappa^n}{n!} \int_0^{\frac{1}{s}} \cdots \int_0^{\frac{1}{s}} \theta(x_1, ..., x_n) \frac{dx_1}{x_1} \cdots \frac{dx_n}{x_n}, \tag{9.5}$$

where the infimum is over all upper bound sieves (λ, θ) with sifting limit $\frac{1}{s}$, and there is a similar formula for $f_\kappa(s)$ (note that when $f_\kappa(s) = 0$, we will typically have $\lambda(\emptyset) = 0$).

The Selberg upper bound sieve corresponds to choosing $\theta = \theta'^2$ for some other sieve (ℓ, θ'), with ℓ supported on $\Sigma(S) \leq \frac{1}{2}$. In terms of the sieve weights λ, this corresponds to

$$\lambda(S) = \sum_{A \cup B = S} \ell(A)\ell(B).$$

In order to describe the weights ℓ, we use the following generalization of the Dickman function. For $s < 0$ we set $\rho_\kappa(s) = 0$, for $0 < s \leq 1$ we set $\rho_\kappa(s) = 1$, and for $s \geq 1$ we define $\rho_\kappa(s)$ by the differential-difference equation

$$s^\kappa \rho'_\kappa(s) = -\kappa(s-1)^{\kappa-1}\rho_\kappa(s-1),$$

or equivalently by the integral equation

$$s^\kappa \rho_\kappa(s) = \int_{s-1}^{s} \rho_\kappa(t) dt^\kappa.$$

When κ is a whole number, the function $\rho_\kappa(s)$ has a combinatorial interpretation. Let n be large, and consider the collection of all ordered pairs (π, c) where π is a permutation of $\{1, ..., n\}$ and $c : \{1, ..., n\} \to \{1, ..., \kappa\}$ is a compatible coloring of $\{1, ..., n\}$ (i.e. $c(i) = c(\pi(i))$ for all i). Choosing an ordered pair (π, c) uniformly at random, $\rho_\kappa(s)$ is the limit, as n goes to ∞, of the probability that every cycle of π has length at most $\frac{n}{s}$.

The optimal choice for the weights ℓ is given in terms of ρ_κ by

$$l(S) = (-1)^{|S|} \frac{\int_0^{\frac{s}{2} - s\Sigma(S)} \rho_\kappa(t) dt^\kappa}{\int_0^{\frac{s}{2}} \rho_\kappa(t) dt^\kappa}.$$

When s goes to ∞ this becomes

$$l(S) \approx \begin{cases} (-1)^{|S|} & \text{if } \Sigma(S) < \frac{1}{2}, \\ 0 & \text{else,} \end{cases}$$

and when $s \leq 2$ it becomes

$$l(S) = (-1)^{|S|}(1 - 2\Sigma(S))_+^{\kappa}.$$

Setting

$$\sigma_\kappa(s) = \frac{\int_0^{\frac{s}{2}} \rho_\kappa(t) dt^\kappa}{e^{\gamma\kappa}\Gamma(\kappa+1)},$$

we have

$$\begin{aligned} s^{-\kappa}\sigma_\kappa(s) &= \frac{1}{(2e^\gamma)^\kappa \Gamma(\kappa+1)} && 0 < s \leq 2, \\ (s^{-\kappa}\sigma_\kappa(s))' &= -\kappa s^{-\kappa-1}\sigma_\kappa(s-2) && s \geq 2, \end{aligned}$$

and the Selberg sieve gives us the upper bound

$$F_\kappa(s) \leq \frac{1}{\sigma_\kappa(s)}.$$

The only case in which this is known to be optimal is when $\kappa = 1$ and $s \leq 2$, in which case the Selberg sieve (λ^S, θ^S) is given by

$$\lambda^S(S) = (-1)^{|S|} \sum_{A \cup B = S} (-1)^{|A \cap B|}(1 - 2\Sigma(A))_+(1 - 2\Sigma(B))_+,$$

$$\theta^S(S) = \Big(\sum_{A \subseteq S} (-1)^{|A|}(1 - 2\Sigma(A))_+ \Big)^2.$$

For $\Sigma(S) \leq \frac{1}{2}$, we have

$$\lambda^S(S) = (-1)^{|S|}\big(1 - 4\sum_{x \in S} x^2\big).$$

The β-sieve $(\lambda^\beta, \theta^\beta)$ is given as follows. The formula

$$\lambda^\beta(S) = \begin{cases} (-1)^{|S|} & \text{if } \forall A \subseteq S,\ |A| \text{ odd } \implies \Sigma(A) + \beta \min(A) \leq 1, \\ 0 & \text{else,} \end{cases}$$

gives the upper bound sieve weights, while the lower bound sieve weights are given by the same formula with "odd" replaced by "even". Here β is chosen such that $\beta - 1$ is the largest zero of the

function $q(s)$, where q solves the differential-difference equation

$$(sq(s))' = \kappa q(s) + \kappa q(s+1).$$

When κ is a half-integer, $q(s)$ is a polynomial of degree $2\kappa - 1$ and β is an algebraic number (see [8] for details). When $\kappa = 1$, we have $\beta = 2$.

The β-sieve is best understood in terms of Buchstab iteration:

$$\mathcal{S}(A, z) = |A| - \sum_{p<z} \mathcal{S}(A_p, p).$$

This leads to the inequalities

$$s^\kappa f_\kappa(s) \geq s^\kappa - \kappa \int_{t>s} t^{\kappa-1}(F_\kappa(t-1) - 1)dt,$$
$$s^\kappa F_\kappa(s) \leq s^\kappa + \kappa \int_{t>s} t^{\kappa-1}(1 - f_\kappa(t-1))dt.$$

A variant of Buchstab iteration is given by

$$\mathcal{S}(A, z) = \mathcal{S}(A, w) - \sum_{w \leq p < z} \mathcal{S}(A_p, p)$$

for any $w \leq z$. If $y = w^t$ and we already have an upper bound sieve $(\lambda_t^+, \theta_t^+)$ with sifting limit t and lower bound sieves $(\lambda_u^-, \theta_u^-)$ with sifting limit u for $s - 1 \leq u \leq t - 1$, the upper bound sieve (λ', θ') we obtain from Buchstab iteration is given by

$$\lambda'(S) = \begin{cases} \lambda_t^+(S) & \text{if } S \subseteq [0, \frac{1}{t}), \\ -\lambda^-_{\frac{1}{x}-1}(T) & \text{if } S = T \cup \{x\}, T \subseteq [0, x], \frac{1}{t} \leq x < \frac{1}{s}. \end{cases}$$

When $\kappa = 1$, the optimal sifting functions f, F are fixed points of Buchstab iteration. To see they are optimal, we introduce two weighted sets A^+, A^- satisfying (9.4). Both are supported on $[1, y]$, with the weight on n given by $1 - \lambda(n)$ in A^+ and given by $1 + \lambda(n)$ in A^-, where by $\lambda(n)$ we mean $(-1)^{\Omega(n)}$ (and not a sieve weight). Setting

$$\pi^\pm(y, z) = \mathcal{S}(A^\pm, z),$$

we have

$$\pi^\pm(y, z) = \pi^\pm(y, w) - \sum_{w<p<z} \pi^\mp(y/p, p),$$

and by the prime number theorem, for $1 < s < 3$ we have

$$\pi^+(y,z) = 2(\pi(y) - \pi(z)) = \frac{2e^\gamma}{s}\frac{y}{e^\gamma \log(z)} + O\left(\frac{y}{\log(z)^2}\right),$$

so for all $s > 1$ we have

$$\pi^+(y,z) = F(s)\frac{y}{e^\gamma \log(z)} + O\left(\frac{y}{\log(z)^2}\right),$$
$$\pi^-(y,z) = f(s)\frac{y}{e^\gamma \log(z)} + O\left(\frac{y}{\log(z)^2}\right).$$

Our strategy for constructing sieves in dimension $1+\epsilon$ is to find an optimal upper bound sieve (λ, θ) in dimension 1 (i.e., a sieve such that the expression inside the infimum on the right hand side of (9.5) is equal to $F(s)$) such that the sum

$$\sum_{n=1}^{\infty} \frac{1}{(n-1)!} \int_0^{\frac{1}{s}} \cdots \int_0^{\frac{1}{s}} \theta(x_1, ..., x_n) \frac{dx_1}{x_1} \cdots \frac{dx_n}{x_n}$$

is as small as possible, since this sum is the rate of change of the expression inside the infimum on the right hand side of (9.5) at $\kappa = 1$. For (λ, θ) an optimal upper bound sieve with sifting limit $2 \leq s \leq 3$, set

$$a_n^\theta = \frac{1}{n!} \int_0^{\frac{1}{2}} \cdots \int_0^{\frac{1}{2}} \theta(x_1, ..., x_n) \frac{dx_1}{x_1} \cdots \frac{dx_n}{x_n}.$$

We then have $a_0^\theta = 1, a_n^\theta \geq 0$, and

$$e^\gamma = F(2) = 1 + a_1^\theta + a_2^\theta + \cdots,$$

while the quantity we wish to minimize is

$$a_1^\theta + 2a_2^\theta + 3a_3^\theta + \cdots.$$

Note that this is the same as *maximizing* the quantity

$$2e^\gamma - 2 - (a_1^\theta + 2a_2^\theta + 3a_3^\theta + \cdots) = a_1^\theta - a_3^\theta - 2a_4^\theta - \cdots.$$

As a consequence, it seems that a good rule of thumb is to simply try to maximize $a_1^\theta = \int_0^{\frac{1}{2}} \theta(x)\frac{dx}{x}$. Letting $a_n^S = a_n^{\theta^S}, a_n^\beta = a_n^{\theta^\beta}$, we have

$$a_1^S = \frac{1}{2},\ a_2^S = \frac{\pi^2 - 9}{12} \approx 0.0724,\ a_3^S \approx 0.03966,$$

and

$$a_1^\beta = \log(3/2) \approx 0.405,\ a_2^\beta = \frac{\log(3/2)^2}{2} \approx 0.0822,\ a_3^\beta \approx 0.06705.$$

Additionally, from the analysis of the Selberg sieve we have

$$e^\gamma = \frac{\partial}{\partial \kappa} e^{\gamma\kappa}\Gamma(\kappa+1)\bigg|_{\kappa=1} = a_1^S + 2a_2^S + 3a_3^S + \cdots.$$

9.3.2 Constraints on optimal sieves in dimension 1

The "complementary slackness" constraints on optimal solutions to linear optimization problems imply that if A is a weighted set satisfying (9.4) with $\mathcal{S}(A,z)$ maximal and (λ,θ) is an optimal upper bound sieve, then if for d squarefree we set $S_d = \{\frac{\log(p)}{\log(y)} \text{ s.t. } p \mid d\}$ we get

$$\begin{aligned} p \mid n, p < z, n \in A &\implies \theta(S_n) = 0, \\ \lambda(S_d) > 0 &\implies |A_d| - \frac{y}{d} = \frac{y}{d\log(y/d)^{2+\epsilon}}, \\ \lambda(S_d) < 0 &\implies |A_d| - \frac{y}{d} = -\frac{y}{d\log(y/d)^{2+\epsilon}}. \end{aligned}$$

We know that the set A^+ maximizes $\mathcal{S}(A,z)$ to first order. Since the number of $n \in A^+$ with $n \le y^{1-\epsilon}$ is small for any $\epsilon > 0$, while the number of $n \in A^+$ with $S_n \approx S$ is large if $\Sigma(S) = 1$, we conclude that, at least away from a measure zero set,

$$\Sigma(S) = 1,\ \min(S) < \frac{1}{s},\ |S| \text{ odd} \implies \theta(S) = 0 \tag{O}$$

for any optimal sieve, and it seems that any nice upper bound sieve satisfying (O) is optimal (although making this precise is tricky).

Proposition 45. *If $|S|$ is odd, $\min(S) < \frac{1}{s}$, and $\Sigma(S) = 1$, then $\theta^S(S) = 0$ and $\theta^\beta(S) = 0$ outside the measure zero subset where the three smallest elements of S are all equal.*

Proof. Although this morally follows from the fact that the Selberg sieve and the β sieve are optimal, we will give a direct proof. We have

$$\theta^S(S) = \bigg(\sum_{A\subseteq S} (-1)^{|A|}(1 - 2\Sigma(A))_+\bigg)^2,$$

and from $\Sigma(S) = 1$ and $|S|$ odd we have

$$(-1)^{|A|}(1-2\Sigma(A))_+ + (-1)^{|S\setminus A|}(1-2\Sigma(S\setminus A))_+ = (-1)^{|A|}(1-2\Sigma(A))$$

for $A \subseteq S$. If $S = \{x_1, ..., x_n\}$, then since $|S| \geq 2$ we have

$$\sum_{A \subseteq S} (-1)^{|A|}(1 - 2\Sigma(A))_+ = \frac{1}{2}\sum_{A \subseteq S}(-1)^{|A|}(1 - 2\Sigma(A)) = \frac{1}{2}\sum_{A \subseteq S}(-1)^{|A|} - \sum_{i=1}^{n} x_i \sum_{x_i \in A \subseteq S}(-1)^{|A|} = 0.$$

Now we turn to $\theta^\beta(S)$. Supposing that $x_1 \geq \cdots \geq x_n$, we just need to show that for all $A \subseteq S \setminus \{x_n\}$ we have $\lambda^\beta(A) \neq 0 \iff \lambda^\beta(A \cup \{x_n\}) \neq 0$. The only case in which this is not obvious is when $|A|$ is even and $\Sigma(A) + x_n + 2x_n > 1$, and in this case we have

$$\Sigma(A) > 1 - 3x_n \geq 1 - x_n - x_{n-1} - x_{n-2} = \Sigma(S \setminus \{x_n, x_{n-1}, x_{n-2}\}),$$

so in fact we must have $A = S \setminus \{x_n\}$. But then from $\lambda^\beta(A) \neq 0$ we must have

$$x_1 + \cdots + x_{n-2} + 2x_{n-2} \leq 1 = x_1 + \cdots + x_{n-2} + x_{n-1} + x_n,$$

so in fact we must have $x_{n-2} = x_{n-1} = x_n$. □

Proposition 46. *If (λ, θ) is an upper bound sieve with sifting limit s satisfying* (O)*, then for any $0 \leq x < \min(\frac{1}{s}, 1 - \frac{2}{s})$ we have $\lambda(x) = -1$.*

More generally, if S is a set with $\min(S) < \frac{1}{s}$ and either $|S|$ odd and $\Sigma(S) < 1 - \frac{2}{s}$ or $|S|$ even and $\Sigma(S) < 1 - \frac{1}{s}$, then $\theta(S) = 0$. In particular, if S is any set such that $\max(S) < \frac{1}{s}$ and $\Sigma(S) < 1 - \frac{2}{s}$, then $\lambda(S) = (-1)^{|S|}$.

Proof. Note that $\frac{1-x}{2} > \frac{1}{s}$, so for any set A containing $\frac{1-x}{2}$ we have $\lambda(A) = 0$. Taking $S = \{x, \frac{1-x}{2}, \frac{1-x}{2}\}$ in (O), we have

$$0 = \theta(S) = \sum_{A \subseteq S} \lambda(A) = 1 + \lambda(x),$$

so $\lambda(x) = -1$.

The more general statement follows by a similar argument, using the fact that $\theta(A) = \theta(A \cap [0, \frac{1}{s}])$ for every set A. □

Since we conjecturally have $||A_d^+| - \frac{y}{d}| \leq \left(\frac{y}{d}\right)^{\frac{1}{2}+o(1)}$, it seems that the other complementary slackness condtions should be treated with some care. If we assume that some version of Pólya's conjecture is true on average, so that $|A_d^+| > \frac{y}{d}$ for most d having an even number of prime factors and $|A_d^+| < \frac{y}{d}$ for most d having an odd number of prime factors, then we might conjecture that

$$(-1)^{|S|}\lambda(S) \geq 0 \tag{A}$$

for optimal upper bound sieves which also have small error terms. It turns out that the Selberg upper bound sieve (λ^S, θ^S) does *not* satisfy condition (A): taking S to be a set consisting of 9 copies

of $\frac{1}{12}$, we get

$$(-1)^9\lambda^S\left(\left\{9\cdot\frac{1}{12}\right\}\right)=2\binom{9}{4}\left(1-2\cdot\frac{4}{12}\right)\left(1-2\cdot\frac{5}{12}\right)-9\binom{8}{4}\left(1-2\cdot\frac{5}{12}\right)^2=-\frac{7}{2}<0.$$

On the other hand, the Selberg upper bound sieve does not have a very good error term in comparison with the β-sieve, which does satisfy (A). Additionally, the Selberg upper bound sieve satisfies (A) for sets S with $\Sigma(S)\leq\frac{1}{2}$.

Generally speaking, linear optimization problems tend to have unique solutions, corresponding to vertices of some associated polytope. When the solution is nonunique, then the problem is said to be degenerate - this corresponds to the polytope having a face which is contained in a level set of the linear function we are trying to optimize. In the case of the linear sieve (i.e. $\kappa=1$), the problem turns out to be infinitely degenerate. From this point of view, the Selberg upper bound sieve method corresponds to restricting ourselves to some ellipsoid contained in our polytope. Since the Selberg upper bound sieve is actually optimal when $\kappa=1$ and $s=2$, this means it "should" correspond to some sort of interior point of the degenerate top face of our polytope. Thus if $\theta^S(S)=0$ for sets S satisfying some simple property, then it seems likely that $\theta(S)=0$ for any optimal upper bound sieve and any set S satisfying the same property.

Proposition 47. *For $|S|\geq 2$, $\min(S)<\frac{1}{s}$, $\Sigma(S)\leq\frac{1}{2}$, we have $\theta^S(S)=\theta^\beta(S)=0$.*

Proof. We have

$$\theta^S(S)=\left(\sum_{A\subseteq S}(-1)^{|A|}(1-2\Sigma(A))_+\right)^2,$$

and from $\Sigma(S)\leq\frac{1}{2}$ we have $(1-2\Sigma(A))_+=1-2\Sigma(A)$ for $A\subseteq S$. If $S=\{x_1,...,x_n\}$, then

$$\sum_{A\subseteq S}(-1)^{|A|}(1-2\Sigma(A))=\sum_{A\subseteq S}(-1)^{|A|}-2\sum_{i=1}^n x_i\sum_{x_i\in A\subseteq S}(-1)^{|A|}=0.$$

Now we turn to $\theta^\beta(S)$. Supposing that $x_1\geq\cdots\geq x_n$, we just need to show that for all $A\subseteq S\setminus\{x_n\}$ we have $\lambda^\beta(A)\neq 0\iff\lambda^\beta(A\cup\{x_n\})\neq 0$. The only case in which this is not obvious is when $|A|$ is even and $\Sigma(A)+x_n+2x_n>1$, and in this case we have

$$\Sigma(S)\geq nx_n\geq 2x_n>1-(\Sigma(A)+x_n)\geq 1-\Sigma(S)\geq\frac{1}{2},$$

a contradiction. □

Based on this, we conjecture that any optimal upper bound sieve has the property

$$|S|\geq 2,\ \min(S)<\frac{1}{s},\ \Sigma(S)\leq\frac{1}{2}\implies\theta(S)=0. \tag{$\frac{1}{2}$}$$

If we assume $(\frac{1}{2})$, we get the nice formula

$$\max(S) < \frac{1}{s},\ \Sigma(S) \le \frac{1}{2} \implies \lambda(S) = (-1)^{|S|}\big(1 - \sum_{x \in S} \theta(x)\big)$$

which determines many of the sieve weights in terms of the sieve weights attached to singletons, so it seems that the most important thing to focus on is the function $\theta(x)$. By Proposition 46, we have $\theta(x) = 0$ for $0 \le x < \min(\frac{1}{s}, 1 - \frac{2}{s})$, and since the sifting limit is s we have $\theta(x) = 1$ for $x > \frac{1}{s}$. The Selberg upper bound sieve has

$$\theta^S(x) = \begin{cases} 4x^2 & \text{if } 0 \le x \le \frac{1}{2}, \\ 1 & \text{else,} \end{cases}$$

while the β-sieve has

$$\theta^\beta(x) = \begin{cases} 0 & \text{if } 0 \le x \le \min(\frac{1}{s}, \frac{1}{3}), \\ 1 & \text{else.} \end{cases}$$

The following conjecture is natural, if unjustified:

$$x \ge y \implies \theta(x) \ge \theta(y). \tag{>}$$

Now we consider the support of λ. In the case of the Selberg upper bound sieve, we clearly have

$$\lambda^S(S) \ne 0 \implies \exists A \subseteq S,\ \Sigma(A) \le \frac{1}{2},\ \Sigma(S \setminus A) \le \frac{1}{2}.$$

The β-sieve has a more interesting constraint on its support.

Definition 18. A set S is *flexible* if for every $0 \le x \le 1$ there exists $A \subseteq S$ such that $\Sigma(A) \le x$ and $\Sigma(S \setminus A) \le 1 - x$.

Proposition 48 (from section 12.7 of [8])**.** *If for every $A \subseteq S$ we have $\Sigma(A) + \min(A) \le 1$, then S is flexible. In particular, if $\lambda^\beta(S) \ne 0$ then S is flexible.*

Proof. Set $u = \min(S)$, $S' = S \setminus \{u\}$. By induction on $|S|$, we see that S' is flexible. Let $0 \le x \le 1$, and suppose that $A' \subseteq S'$ satisfies $\Sigma(A') \le x$, $\Sigma(S' \setminus A') \le 1 - x$. Since

$$\Sigma(A' \cup \{u\}) + \Sigma((S' \setminus A') \cup \{u\}) = \Sigma(S) + \min(S) \le 1$$

by assumption, we must have one of $\Sigma(A' \cup \{u\}) \le x$, $\Sigma((S' \setminus A') \cup \{u\}) \le 1 - x$, so at least one of the choices $A = A'$ or $A = A' \cup \{u\}$ satisfies $\Sigma(A) \le x$, $\Sigma(S \setminus A) \le 1 - x$.

Now suppose that $\lambda^\beta(S) \ne 0$, so that for any $A \subseteq S$ with $|A|$ odd we have $\Sigma(A) + 2\min(A) \le 1$.

Then for any $A \subseteq S$ with $|A|$ even, if $A' = A \setminus \{\min(A)\}$ then $|A'|$ is odd, so

$$\Sigma(A) + \min(A) = \Sigma(A') + 2\min(A) \leq \Sigma(A') + 2\min(A') \leq 1. \qquad \square$$

It seems that as s decreases from ∞ to 2, the supports of optimal sieves get gradually less flexible, although it isn't clear what the correct weakening of flexibility should be. The following conjecture seems plausible:

$$S \subseteq \big[1 - \frac{2}{s}, \frac{1}{s}\big],\ \lambda(S) \neq 0 \implies \Sigma(S) \leq \frac{2}{s}. \tag{F}$$

9.3.3 Upper bound iteration rules

Here by an iteration rule we mean a special type of sieve, used to get new bounds on $\mathcal{S}(A, z)$ given upper and lower bounds on $\mathcal{S}(A_d, w)$ for squarefree numbers d having all their prime factors between w and z. Supposing $y = z^s = w^t$, if $(\lambda^{it}, \theta^{it})$ is an upper bound sieve such that every set in the support of λ^{it} is contained in $[\frac{1}{t}, \frac{1}{s}]$, then the corresponding iteration rule is given by

$$\mathcal{S}(A, z) \leq \sum_{\substack{d \text{ squarefree} \\ p|d \implies w \leq p < z}} \lambda^{it}(S_d)\mathcal{S}(A_d, w),$$

where $S_d = \{\frac{\log(p)}{\log(y)} \text{ s.t. } p \mid d\}$. This leads to an iterative inequality on $F_\kappa(s)$ in terms of F_κ, f_κ in an obvious way. The main advantage of using iteration rules is that it is typically very easy to check that $(\lambda^{it}, \theta^{it})$ is a valid upper bound sieve. Our main concern is with iteration rules which are *optimal* when $\kappa = 1$, i.e. such that the pair of functions F, f is a fixed point of the iteration rule.

Theorem 40. *Suppose that the upper bound sieve $(\lambda^{it}, \theta^{it})$ has λ^{it} supported on sets contained in $[1-\frac{2}{s}, \frac{1}{s}]$, and satisfies the conditions* (O), (A), (F) *for all sets $S \subseteq [1-\frac{2}{s}, \frac{1}{s}]$. Then the corresponding iteration rule is optimal in dimension $\kappa = 1$.*

Proof. Set $t = \frac{1}{1-\frac{2}{s}}$, $w = y^{\frac{1}{t}}$. By condition (A), the iteration rule is given to first order by

$$F(s)\frac{y}{e^\gamma \log(z)} \leq \sum_{\substack{\mu(d)=1 \\ p|d \implies w \leq p < z}} \lambda^{it}(S_d)F(t - t\Sigma(S_d))\frac{y/d}{e^\gamma \log(w)} + \sum_{\substack{\mu(d)=-1 \\ p|d \implies w \leq p < z}} \lambda^{it}(S_d)f(t - t\Sigma(S_d))\frac{y/d}{e^\gamma \log(w)}.$$

The main idea is to exploit the fact that $\mathcal{S}(A^+, z) = F(s)\frac{y}{e^\gamma \log(z)} + O\left(\frac{y}{\log(z)^2}\right)$ and $\mathcal{S}(A^-, z) = f(s)\frac{y}{e^\gamma \log(z)} + O\left(\frac{y}{\log(z)^2}\right)$ for all $s > 1$. Since $\lambda^{it}(S_d) \neq 0$ implies $t - t\Sigma(S_d) \geq t - t \cdot \frac{2}{s} = 1$ by

condition (F), we just need to check that

$$\mathcal{S}(A^+, z) = \sum_{\substack{\mu(d)=1 \\ p|d \implies w \le p < z}} \lambda^{it}(S_d)\mathcal{S}(A_d^+, w) + \sum_{\substack{\mu(d)=-1 \\ p|d \implies w \le p < z}} \lambda^{it}(S_d)\mathcal{S}(A_d^-, w) + O\bigg(\frac{y}{\log(z)^2}\bigg).$$

Since nonsquarefree numbers don't have a large contribution to either side, and since A_d^+ is supported on numbers with an odd number of prime factors while A_d^- is supported on numbers with an even number of prime factors, this follows from condition (O). □

We can describe the sieve weights produced by an iteration rule as follows. For every u, let $(\lambda_u^+, \theta_u^+)$ be an upper bound sieve with sifting limit u and let $(\lambda_u^-, \theta_u^-)$ be a lower bound sieve with sifting limit u. Let $(\lambda^{it}, \theta^{it})$ be our iteration rule sieve, with λ^{it} supported on sets contained in $[\frac{1}{t}, \frac{1}{s}]$. Then the resulting upper bound sieve (λ, θ) is given by

$$\lambda(S) = \begin{cases} \lambda^{it}(S \cap [\frac{1}{t}, \frac{1}{s}])\lambda^+_{t-t\Sigma(S\cap[\frac{1}{t},\frac{1}{s}])}(S \setminus [\frac{1}{t}, \frac{1}{s}]) & \text{if } \lambda^{it}(S \cap [\frac{1}{t}, \frac{1}{s}]) \ge 0, \\ \lambda^{it}(S \cap [\frac{1}{t}, \frac{1}{s}])\lambda^-_{t-t\Sigma(S\cap[\frac{1}{t},\frac{1}{s}])}(S \setminus [\frac{1}{t}, \frac{1}{s}]) & \text{if } \lambda^{it}(S \cap [\frac{1}{t}, \frac{1}{s}]) \le 0. \end{cases}$$

In particular, for a singleton set we have

$$\theta(x) = \begin{cases} \theta_t^+(x) & \text{if } 0 \le x < \frac{1}{t}, \\ \theta^{it}(x) & \text{if } \frac{1}{t} \le x \le \frac{1}{s}, \\ 1 & \text{else.} \end{cases}$$

9.4 The range $\frac{5}{2} \le s \le 3$ and probability distributions on the triangle

We will assume throughout that we are working with an optimal upper bound sieve (λ, θ) with sifting limit $\frac{5}{2} \le s \le 3$ satisfying conditions (O), (A), (F), and trying to maximize the quantity $a_1 = \int_0^{\frac{1}{2}} \theta(x)\frac{dx}{x}$ subject to these constraints. By Theorem 40, we only need to consider the constraints involving sets S contained in $[1 - \frac{2}{s}, \frac{1}{s}]$.

By condition (F), if $S \subseteq [1 - \frac{2}{s}, \frac{1}{s}]$ and $\lambda(S) \ne 0$, then $|S| < 4$ since $4(1 - \frac{2}{s}) \ge \frac{2}{s}$ for $s \ge \frac{5}{2}$. By condition (A) we have $\lambda(S) \le 0$ if $|S| = 3$, so if for some $x, y, z \in [1 - \frac{2}{s}, \frac{1}{s}]$ we had $\lambda(x, y, z) < 0$, then we would have

$$\theta(\{k \cdot x, k \cdot y, k \cdot z\}) = \sum_{0 \le a,b,c \le k} \binom{k}{a}\binom{k}{b}\binom{k}{c}\lambda(\{a \cdot x, b \cdot y, c \cdot z\}) \le k^3\lambda(x, y, z) + O(k^2) < 0$$

for k sufficiently large, a contradiction. Thus $\lambda(x, y, z) = 0$ for $x, y, z \in [1 - \frac{2}{s}, \frac{1}{s}]$.

Note that for any $x, y, z \in [1 - \frac{2}{s}, \frac{1}{s}]$, $\lambda(x, y, z) = 0$ implies that

$$\theta(x, y, z) = \theta(x, y) + \theta(x, z) + \theta(y, z) - \theta(x) - \theta(y) - \theta(z) + 1.$$

Applying Proposition 46 (which used condition (O)) to the set $\{x, y\}$ of size 2, we find

$$x + y \leq 1 - \frac{1}{s} \implies \theta(x, y) = 0.$$

Using condition (O) directly, we also have

$$x + y + z = 1,\ x, y, z \leq \frac{1}{s} \implies \theta(x) + \theta(y) + \theta(z) = \theta(x, y) + \theta(x, z) + \theta(y, z) + 1.$$

It's convenient to replace the interval $[1 - \frac{2}{s}, \frac{1}{s}]$ by the interval $[0, 1]$. Let $r_s(x) = 1 - \frac{2}{s} + (\frac{3}{s} - 1)x$. Let $f(x) = \theta(r_s(x))$, and let $g(x, y) = \theta(r_s(x), r_s(y))$. Note that $r_s(\frac{2}{3}) = \frac{1}{3}$, so if $x + y + z = 2$ then $r_s(x) + r_s(y) + r_s(z) = 1$.

Theorem 41. *Suppose $f : [0, 1] \to \mathbb{R}_{\geq 0}$ and $g : [0, 1]^2 \to \mathbb{R}_{\geq 0}$ are nonnegative functions such that*

$$x + y \leq 1 \implies g(x, y) = 0,$$

$$\forall x, y, z \in [0, 1] \quad f(x) + f(y) + f(z) \leq g(x, y) + g(x, z) + g(y, z) + 1,$$

and

$$x + y + z = 2 \implies f(x) + f(y) + f(z) = g(x, y) + g(x, z) + g(y, z) + 1.$$

Then we have

a) f is nondecreasing,

b) for every integer $n > 1$,

$$\frac{f(\frac{1}{n}) + \cdots + f(\frac{n-1}{n})}{n - 1} \leq \frac{1}{3} \leq \frac{f(\frac{0}{n}) + \cdots + f(\frac{n}{n})}{n + 1},$$

c) f is integrable and $\int_0^1 f(x)dx = \frac{1}{3}$,

d) g is nondecreasing in either argument, and moreover satisfies the inequality

$$w \leq x, y \leq z \implies g(x, z) - g(w, z) \geq g(x, y) - g(w, y),$$

e) if f, g are continuous then they come from a symmetric probability distribution μ supported on

the simplex $\{a, b, c \in [0,1]^3 \mid a+b+c = 2\}$, *according to the formulae*

$$f(x) = \mathbb{P}_{\mu(a,b,c)}[a \leq x],\ g(x,y) = \mathbb{P}_{\mu(a,b,c)}[a \leq x \wedge b \leq y]?$$

Proof. Part a): suppose $0 \leq a < b \leq 1$, we will show that $f(a) \leq f(b)$. Choose a nonnegative integer k such that

$$2a - b < k(b-a) < b.$$

For each $0 \leq i \leq k$, set

$$x_{2i} = 1 - \frac{b + (k-2i)(b-a)}{2},\ x_{2i+1} = 1 - \frac{b + (2i-k)(b-a)}{2}.$$

Note that by the choice of k we have $a + x_0 = a + x_{2k+1} < 1$ and $1 - b < x_i < 1$ for all $0 \leq i \leq 2k+1$. Furthermore, for each i we have $b + x_{2i} + x_{2i+1} = 2$ and $a + x_{2i-1} + x_{2i} = 2$. Thus, for each $0 \leq i \leq k$ we have

$$\begin{aligned} f(b) + f(x_{2i}) + f(x_{2i+1}) &= g(b, x_{2i}) + g(b, x_{2i+1}) + g(x_{2i}, x_{2i+1}) + 1, \\ f(a) + f(x_{2i}) + f(x_{2i+1}) &\leq g(a, x_{2i}) + g(a, x_{2i+1}) + g(x_{2i}, x_{2i+1}) + 1, \end{aligned}$$

and for each $1 \leq i \leq k$ we have

$$\begin{aligned} f(b) + f(x_{2i-1}) + f(x_{2i}) &\leq g(b, x_{2i-1}) + g(b, x_{2i}) + g(x_{2i-1}, x_{2i}) + 1, \\ f(a) + f(x_{2i-1}) + f(x_{2i}) &= g(a, x_{2i-1}) + g(a, x_{2i}) + g(x_{2i-1}, x_{2i}) + 1. \end{aligned}$$

Adding together the inequalities and subtracting the equalities, we get

$$\begin{aligned} f(a) &\leq f(b) + g(a, x_0) + g(a, x_{2k+1}) - g(b, x_0) - g(b, x_{2k+1}) \\ &= f(b) - g(b, x_0) - g(b, x_{2k+1}) \leq f(b). \end{aligned}$$

Part b): first we prove the left hand inequality. For every ordered triple of integers $0 < i, j, k < n$ satisfying $i + j + k = 2n$, we have an equality

$$f(\tfrac{i}{n}) + f(\tfrac{j}{n}) + f(\tfrac{k}{n}) = g(\tfrac{i}{n}, \tfrac{j}{n}) + g(\tfrac{i}{n}, \tfrac{k}{n}) + g(\tfrac{j}{n}, \tfrac{k}{n}) + 1.$$

Also, for every ordered triple $0 < i, j, k < n$ satisfying $i + j + k = 2n - 1$, we have the inequality

$$f(\tfrac{i}{n}) + f(\tfrac{j}{n}) + f(\tfrac{k}{n}) \leq g(\tfrac{i}{n}, \tfrac{j}{n}) + g(\tfrac{i}{n}, \tfrac{k}{n}) + g(\tfrac{j}{n}, \tfrac{k}{n}) + 1.$$

Adding the inequalities and subtracting the equalities, and using $g(\frac{i}{n}, \frac{j}{n}) = 0$ when $i + j = n$, gives

the left hand inequality of b). For the right hand inequality of b) one uses equalities corresponding to triples $0 \leq i, j, k \leq n$ with $i + j + k = 2n$, and inequalities corresponding to triples $0 \leq i, j, k \leq n$ with $i + j + k = 2n + 1$.

Part c) follows immediately from parts a) and b).

The proofs of parts d) and e) can be found in the second appendix. □

Thus $\theta(x)$ is increasing, and the average value of $\theta(x)$ on the interval $[1 - \frac{2}{s}, \frac{1}{s}]$ is $\frac{1}{3}$. Since $\frac{1}{x}$ is decreasing, in order to maximize $\int_{1-\frac{2}{s}}^{\frac{1}{s}} \theta(x)\frac{dx}{x}$ we must take $\theta(x) = \frac{1}{3}$ identically on this interval. In terms of λ, this is corresponds to taking $\lambda(x) = -\frac{2}{3}$, $\lambda(x, y) = \frac{1}{3}$ for all $x, y \in [1 - \frac{2}{s}, \frac{1}{s}]$, which we can easily check gives an optimal upper bound sieve iteration. For $s = \frac{5}{2}$ the resulting sieve has

$$a_1 = \int_0^{\frac{1}{2}} \theta(x)\frac{dx}{x} = \frac{\log(2)}{3} + \log\left(\frac{5}{4}\right) \approx 0.454.$$

9.5 Further iteration rules as we approach $s = 2$?

First attempt:

Theorem 42. *If A is such that $|A_d| = 0$ for all d with $d \geq y^{\frac{13}{12}}$, and if $z^{\frac{12}{5}} < y < z^{\frac{5}{2}}$, then*

$$\begin{aligned}
\mathcal{S}(A,z) \leq \mathcal{S}(A,\frac{y}{z^2}) &- \frac{4}{5}\sum_{\frac{y}{z^2}\leq p<\frac{z^3}{y}} \mathcal{S}(A_p,\frac{y}{z^2}) - \frac{2}{3}\sum_{\frac{z^3}{y}\leq p<\frac{y^2}{z^4}} \mathcal{S}(A_p,\frac{y}{z^2}) \\
&- \frac{8}{15}\sum_{\frac{y^2}{z^4}\leq p<z} \mathcal{S}(A_p,\frac{y}{z^2}) + \frac{3}{5}\sum_{\frac{y}{z^2}\leq q<p<\frac{z^3}{y}} \mathcal{S}(A_{pq},\frac{y}{z^2}) \\
&+ \frac{7}{15}\sum_{\frac{y}{z^2}\leq q<\frac{z^3}{y}\leq p<\frac{y^2}{z^4}} \mathcal{S}(A_{pq},\frac{y}{z^2}) + \frac{1}{3}\sum_{\substack{\frac{y}{z^2}\leq q<\frac{z^3}{y}\\ \frac{y^2}{z^4}\leq p<z}} \mathcal{S}(A_{pq},\frac{y}{z^2}) \\
&+ \frac{1}{3}\sum_{\frac{z^3}{y}\leq q<p<\frac{y^2}{z^4}} \mathcal{S}(A_{pq},\frac{y}{z^2}) + \frac{4}{15}\sum_{\frac{z^3}{y}\leq q<\frac{y^2}{z^4}\leq p<z} \mathcal{S}(A_{pq},\frac{y}{z^2}) \\
&+ \frac{1}{5}\sum_{\frac{y^2}{z^4}\leq q<p<z} \mathcal{S}(A_{pq},\frac{y}{z^2}) - \frac{2}{5}\sum_{\substack{\frac{y}{z^2}\leq r<q<p<\frac{z^3}{y}\\ pqr^2<z^2}} \mathcal{S}(A_{pqr},\frac{y}{z^2}) \\
&- \frac{4}{15}\sum_{\frac{y}{z^2}\leq r<q<\frac{z^3}{y}\leq p<\frac{y^2}{z^4}} \left(1-\frac{3\log(qr)}{8\log(y/p)}\right)\mathcal{S}(A_{pqr},\frac{y}{z^2}) \\
&+ \frac{1}{5}\sum_{\substack{\frac{y}{z^2}\leq s<r<q<p<\frac{z^3}{y}\\ pqr^2<z^2}} \mathcal{S}(A_{pqr},\frac{y}{z^2}) \\
&+ \frac{1}{10}\sum_{\frac{y}{z^2}\leq s<r<q<\frac{z^3}{y}\leq p<\frac{y^2}{z^4}} \left(1-\frac{\log(qrs)}{\log(y/p)}\right)_+ \mathcal{S}(A_{pqr},\frac{y}{z^2}).
\end{aligned}$$

9.6 Numerical computations at $\kappa = \frac{3}{2}$

When $\kappa = \frac{3}{2}$, we have $\alpha_\kappa^D = 3.9114..., \beta_\kappa^D = 3.11582...$ [3]. In particular, we have $\alpha_\kappa^D < \beta_\kappa^D + 1$, so Corollary 10 can be applied to s in the range $\alpha_\kappa^D < s < \beta_\kappa^D + 1$ with $t = \frac{s}{s-\beta_\kappa^D}$. The improvement to the value of $F_\kappa(s)$ in this range is nonzero, but very small. Combining this with ordinary Buchstab iteration for the lower bound, one can show that $\beta(\frac{3}{2}) < 3.11570$.

If we apply the iteration from Corollary 11 directly to F_κ^D, f_κ^D, then the values of s, t for which the quantity $s^\kappa f_\kappa(s)$ is improved the most are given by $s \approx 4.85, t \approx 5.52$. This results in the bound $\beta(\frac{3}{2}) < 3.11554$.

Iteratively combining the improvements from Corollaries 10 and 11, we get $\beta(\frac{3}{2}) < 3.11549$.

Appendix A

Proof of bounds connected to Selberg's model problem

A.1 Saddle point method

For any $v \geq d+1$, we defined the polynomial f_v by

$$f_v(n) = \frac{d!}{v^{d+1}} \sum_r \ell_r \binom{n}{r},$$

where

$$\ell_r = (-1)^r \sum_{k=0}^{d+1-r} \frac{d+1-r-k}{k!} v^k,$$

as in Selberg's construction.

Theorem 43. *If $n, q, d \geq 1$ with $4(n+q)^2 \leq d$, and if $v = d+q$, then we have*

$$v^{(n+2)/2} f_v(n+2) = \frac{n! e^{n/2}}{\sqrt{\pi} n^{(n+1)/2}} \Re\left(i^{-n} \exp\left(i(\tfrac{n}{3}+q)\sqrt{\tfrac{n}{v}} + O(\tfrac{n+q}{\sqrt{nv}}) \right) \right) e^{\frac{q^2}{4v}}.$$

Proof. We compute $f_v(n+2)$ by the following formula from Proposition 18:

$$v^{n+1} f_v(n+2) = \frac{n!}{2\pi i} \int_C e^{vz} (1-z)^d z^{-n} \frac{\mathrm{d}z}{z},$$

where the contour is taken to be a circle of radius $\sqrt{\frac{n}{v}}$ centered at the origin. Since the logarithmic derivative of the integrand is $v - \frac{d}{1-z} - \frac{n}{z}$, the integrand has saddle points at $z_0, \bar{z}_0$, where z_0 is the root of $vz_0^2 - (n+q)z_0 + n = 0$ having positive imaginary part.

Writing $z = \sqrt{\frac{n}{v}}e^{i\theta}$, $z_0 = \sqrt{\frac{n}{v}}e^{i\theta_0}$, we have

$$v^{(n+2)/2} f_v(n+2) = \frac{n!}{2\pi n^{n/2}} \int_0^{2\pi} e^{vz - in\theta}(1-z)^d \mathrm{d}\theta.$$

To see that we may restrict the integral to a small interval around θ_0 and $2\pi - \theta_0$, we consider the real part of the logarithm of the integrand as a function of $\cos(\theta)$:

$$\log|e^{vz-in\theta}(1-z)^d| = \sqrt{nv}\cos(\theta) + d\log\left|1 - \sqrt{\tfrac{n}{v}}e^{i\theta}\right| = \sqrt{nv}\cos(\theta) + \frac{d}{2}\log\Big(1 + \frac{n}{v} - 2\sqrt{\tfrac{n}{v}}\cos(\theta)\Big).$$

Taking the second derivative with respect to $\cos(\theta)$, we obtain

$$\frac{\mathrm{d}^2}{(\mathrm{d}\cos(\theta))^2}\log|e^{vz-in\theta}(1-z)^d| = -\frac{2dn}{v\Big(1 + \frac{n}{v} - 2\sqrt{\frac{n}{v}}\cos(\theta)\Big)^2} \le -\frac{2dnv}{(\sqrt{v}+\sqrt{n})^4},$$

so

$$|e^{vz}(1-z)^d| \le |e^{vz_0}(1-z_0)^d| e^{-\frac{dv}{(\sqrt{v}+\sqrt{n})^4} n(\cos(\theta)-\cos(\theta_0))^2},$$

and we see that we may restrict our attention to θ with $|\cos(\theta) - \cos(\theta_0)| \ll \frac{\log(n)}{\sqrt{n}}$. Since $\cos(\theta_0) = \frac{n+q}{2\sqrt{nv}} \le \frac{1}{4}$, this is equivalent to restricting to the ranges $|\theta - \theta_0| \ll \frac{\log(n)}{\sqrt{n}}$ and $|\theta - (2\pi - \theta_0)| \ll \frac{\log(n)}{\sqrt{n}}$.

Around θ_0, the integrand can be written as

$$e^{vz_0 - in\theta_0}(1-z_0)^d \exp\left(\alpha(\theta-\theta_0)^2 + \beta(\theta-\theta_0)^3 + O(n(\theta-\theta_0)^4)\right),$$

with

$$\alpha = -\frac{vz_0}{2} + \frac{dz_0}{2(1-z_0)} + \frac{dz_0^2}{2(1-z_0)^2} = -n + \frac{(q-n)(vz_0-n)}{2d} = -n + O\Big((n+q)\sqrt{\tfrac{n}{v}}\Big),$$
$$\beta = -\frac{ivz_0}{6} + \frac{idz_0}{6(1-z_0)} + \frac{idz_0^2}{2(1-z_0)^2} + \frac{idz_0^3}{3(1-z_0)^3} = -\frac{2in}{3} + O\Big((n+q)\sqrt{\tfrac{n}{v}}\Big).$$

Thus we have

$$\exp\left(\alpha(\theta-\theta_0)^2 + \beta(\theta-\theta_0)^3 + O(n(\theta-\theta_0)^4)\right) = e^{\alpha(\theta-\theta_0)^2}(1 + \beta(\theta-\theta_0)^3 + O(n(\theta-\theta_0)^4 + n^2(\theta-\theta_0)^6)),$$

and after integrating we get

$$\int_0^{2\pi} e^{vz-in\theta}(1-z)^d \mathrm{d}\theta = 2\Re\left(e^{vz_0 - in\theta_0}(1-z_0)^d \frac{\sqrt{\pi}}{\sqrt{n}}(1 + O(\tfrac{n+q}{\sqrt{nv}}))\right).$$

By the defining equation for z_0 we have $\frac{v}{n}z_0^2 = -1 + \frac{n+q}{n}z_0$, so

$$e^{-in\theta_0} = i^{-n}\left(1 - \frac{n+q}{n}z_0\right)^{-n/2} = i^{-n}\exp\left(\frac{n+q}{2}z_0 - \frac{(n+q)^2}{4v} + O(\tfrac{n+q}{\sqrt{nv}})\right).$$

Also, we have

$$e^{vz_0}(1-z_0)^d = \exp\left(\frac{n}{2} + \left(\frac{n}{3} + q - \frac{n+q}{2}\right)z_0 + \frac{n(n-2q)}{12v} + O(\tfrac{n+q}{\sqrt{nv}})\right),$$

so, using $z_0 = i\sqrt{\frac{n}{v}} + \frac{n+q}{2v} + O(\frac{(n+q)^2}{v^2})$, we have

$$v^{(n+2)/2}f_v(n+2) = \frac{n!}{\sqrt{\pi}n^{(n+1)/2}}\Re\left(i^{-n}\exp\left(\tfrac{n}{2} + i(\tfrac{n}{3}+q)\sqrt{\tfrac{n}{v}} + \tfrac{q^2}{4v} + O(\tfrac{n+q}{\sqrt{nv}})\right)\right). \qquad \square$$

A.2 Log-concavity method

We'll repeat the definitions and a few of the results from Section 4.2, focusing on the case $v = d+1$. We define the polynomial f of degree d by

$$f(n) = \sum_{i \le d} \ell_i \binom{n}{i},$$

where

$$\ell_r = (-1)^r \frac{d!}{(d+1)^{d+1}} \sum_{i=0}^{d+1-r} \frac{d+1-r-i}{i!}(d+1)^i,$$

and we wish to describe the behavior of the roots $\nu_1, ..., \nu_d$ of $f(n) = \sum_i \ell_i \binom{n}{i}$ as d gets large.

Proposition 49 (Proposition 15)**.** *The roots $\nu_1, ..., \nu_d$ of f are all real, positive, and greater than 2. For any integer n, the closed interval $[n, n+1]$ contains at most one root ν_i.*

Corollary 12 (Corollary 4)**.** *If n is an integer with $f(n)f(n+2) < 0$, then the interval $(n, n+2)$ contains exactly one root ν_i, and whether ν_i is above or below $n+1$ is determined by the sign of $f(n+1)$.*

From here on we assume that $\nu_1 < \cdots < \nu_d$.

Remark 6. Numerical calculations indicate that we even have $\nu_{i+1} > \nu_i + 2$ for every i.

Proposition 50 (Proposition 16)**.** *Let n be a nonnegative integer. Then*

$$f(n+2) = \sum_k \frac{(-1)^k}{(d+1)^{k+1}} k! \binom{d}{k}\binom{n}{k}.$$

Furthermore, we have $f(0) = \frac{(d+1)^{d+1}}{d!}$.

Proposition 51 (Proposition 17)**.** *Let $a(n,k)$ be the number of permutations of an n-set having exactly k cycles of size greater than 1. Then for n a nonnegative integer we have*

$$f(n+2) = \frac{1}{(d+1)^{n+1}} \sum_k (-1)^k a(n,k) d^k.$$

In particular, $f(n+2)$ is positive for large d if and only if $\lfloor \frac{n}{2} \rfloor$ is even.

More generally, define $a_q(n,k)$ by

$$a_q(n,k) = \sum_l \binom{n}{l} c_2(n-l,k) q^l,$$

where $c_2(m,k)$, an associated signless Stirling number of the first kind, is defined to be the number of derangements of an m-set having exactly k cycles of size greater than 1 (so that $a(n,k) = a_1(n,k)$ and $c_2(n,k) = a_0(n,k)$). Then we have

$$\sum_j (-1)^j (d+q)^{n-j} j! \binom{d}{j} \binom{n}{j} = \frac{n!}{2\pi i} \int_C e^{(d+q)z} (1-z)^d \frac{dz}{z^{n+1}} = \sum_k (-1)^k a_q(n,k) d^k,$$

where C is any contour winding counterclockwise around 0.

Corollary 13. *If k is fixed then ν_k approaches $2k+1$ from above as d goes to ∞.*

Proof. By the previous proposition, for any $m \geq 1$ we can find d_0 sufficiently large that for any $d \geq d_0$ we have $\nu_j \in (2j+1, 2j+2)$ for $1 \leq j \leq k+m^2$. For any $d \geq d_0$, we then have

$$\prod_{j \neq k} \left| \frac{\nu_j - (2k+1)}{\nu_j - (2k+2)} \right| \geq \prod_{1 \leq j < k} \frac{2j-1}{2j} \prod_{1 \leq j \leq m} \frac{2j+1}{2j} \gg_k \sqrt{m}.$$

By the previous proposition, we have

$$\prod_j \left| \frac{\nu_j - (2k+1)}{\nu_j - (2k+2)} \right| = \frac{|f(2k+1)|}{|f(2k+2)|} \to \frac{a(2k-1,k-1)}{a(2k,k)}$$

as $d \to \infty$, so we must have $\left| \frac{\nu_k - (2k+1)}{\nu_k - (2k+2)} \right| \ll_k \frac{1}{\sqrt{m}}$ for d sufficiently large. Taking m to infinity, we see that $\lim_{d \to \infty} \nu_k = 2k+1$. □

Proposition 52. *The coefficients $a(n,k)$ are log-concave in k, that is,*

$$a(n,k)^2 \geq a(n,k-1) a(n,k+1).$$

More generally, for any $q \geq 0$ the coefficients $a_q(n,k)$ are log-concave in k.

Proof. This will be an application of Theorem 2.5.2 of Francesco Brenti's memoir on log concavity

[1] (since the proof is short, we'll reproduce it here). We will show more generally that if q_i is a finite nonnegative log-concave sequence without internal zeros, then the expression

$$c_k = \sum_{m \geq 0} \frac{k!}{m!} c_2(m,k) q_m$$

is log-concave in k. Plugging in $q_m = m!\binom{n}{m} q^{n-m}$ gives (a stronger form of) the Proposition.

We start with the easy observation that for any i, j we have

$$\binom{i+j}{i} c_2(m, i+j) = \sum_{x+y=m} \binom{m}{x} c_2(x,i) c_2(y,j).$$

Thus, if we define the matrix L by $L_{k,m} = \frac{k!}{m!} c_2(m,k)$, then L has the "semigroup property" of Francesco Brenti [1], that is, the $i+j$th row of the matrix L is the convolution of the ith row and the jth row for any i, j.

The second ingredient we need is that every two by two minor of L is nonnegative. Since every entry of L is nonnegative, with $L_{k,n} = 0$ exactly when $2k > n$, this will follow from the inequality

$$c_2(n,k) c_2(n+1,k+1) \geq c_2(n,k+1) c_2(n+1,k). \tag{A.1}$$

Applying the recurrence

$$c_2(m,l) = (m-1)(c_2(m-1,l) + c_2(m-2,l-1))$$

with $(m,l) = (n+1,k+1), (n+1,k), (n,k)$, and $(n-1,k-1)$, we see that (A.1) is equivalent to

$$(n-1)(c_2(n-1,k)+c_2(n-2,k-1))c_2(n-1,k) \geq (n-2)c_2(n,k+1)(c_2(n-2,k-1)+c_2(n-3,k-2)),$$

which follows from the log-concavity of $c_2(m+l,l)$ in l for $m = n-k-1$ fixed. The log-concavity of $c_2(m+l,l)$ in l is well-known and can be proved by an easy induction on m using the above recurrence (in fact, by Theorem 6.7.2 of [1] $c_2(m+l,l)$ is even a Pólya frequency sequence in l).

Now we can apply the proof of Theorem 2.5.2 of [1]. Let Q be the matrix defined by $Q_{i,j} = q_{i+j}$, then if q_i is log-concave every two by two minor of Q will be nonpositive. By the Cauchy-Binet identity, we see that every two by two minor of

$$C = LQL^t$$

is nonpositive as well. We have

$$\begin{aligned} C_{i,j} &= \sum_{x,y} L_{i,x} Q_{x,y} L_{j,y} \\ &= \sum_{m} \left(\sum_{x+y=m} L_{i,x} L_{j,y} \right) q_m \\ &= \sum_{m} L_{i+j,m} q_m \\ &= c_{i+j}, \end{aligned}$$

so the nonpositivity of the two by two minors of C implies the log-concavity of c_k, and we are done. □

Corollary 14. *If $\nu_k \geq 2k+2$, then*

$$4k^3 + 9k^2 - 4k \geq 9d.$$

Furthermore, for any fixed j, if k_j is the first integer k such that $\nu_k \geq 2k+1+j$ then as d goes to infinity we have

$$\lim_{d\to\infty} \frac{(2k_j)^3}{d} = \left(\frac{3\pi j}{2}\right)^2.$$

Proof. By the previous propositions, for the first claim it's enough to show that for $4k^3+9k^2-4k < 9d$ we have $a(2k,k)d > a(2k,k-1)$. We have

$$a(2k,k) = (2k-1)(2k-3)\cdots 1 = (2k-1)!!,$$

and

$$a(2k,k-1) = \binom{2k}{2}(2k-3)!! + 2\cdot 2k\binom{2k-1}{3}(2k-5)!! + \frac{2^2}{2!}\binom{2k}{6}\binom{6}{3}(2k-7)!! + 6\cdot\binom{2k}{4}(2k-5)!!,$$

so

$$\frac{a(2k,k-1)}{a(2k,k)} = k + \frac{4k(k-1)}{3} + \frac{4k(k-1)(k-2)}{9} + k(k-1) = \frac{4k^3+9k^2-4k}{9}.$$

For the second claim, we will apply Corollary 4 by showing that for every $k \ll \sqrt[3]{d}$, we have at least one of $f(k-1)f(k+1) < 0$ or $f(k)f(k+2) < 0$, depending on whether k is even or odd and on the size of $\sqrt{\frac{(2k)^3}{9d}}$ modulo 2π. More precisely, we will show that for $L \geq \frac{k^3}{d}$, we have

$$(-1)^k \frac{(d+1)^{2k+1}}{d^k a(2k,k)} f(2k+2) = \sum_l \frac{(-1)^l}{d^l} \frac{a(2k,k-l)}{a(2k,k)} = \cos\left(\sqrt{\tfrac{(2k)^3}{9d}}\right) + O_L(\tfrac{1}{k}) + O(\tfrac{1}{L!})$$

and

$$(-1)^k \frac{(d+1)^{2k+2}}{d^k a(2k+1,k)} f(2k+3) = \sum_l \frac{(-1)^l}{d^l} \frac{a(2k+1,k-l)}{a(2k+1,k)} = \sqrt{\tfrac{9d}{(2k)^3}} \sin\left(\sqrt{\tfrac{(2k)^3}{9d}}\right) + O_L(\tfrac{1}{k}) + O(\tfrac{1}{L!}).$$

In order to determine the size of $a(2k,k)$, we note that for any fixed l and k large, the largest contribution of permutations on $2k$ symbols with $k-l$ nontrivial cycles comes from the permutations with as few 2-cycles as possible, so we have

$$\frac{a(2k,k-l)}{a(2k,k)} = \frac{2^{2l}}{(2l)!}\binom{2k}{6l}\binom{6l}{3,...,3}\frac{(2k-6l-1)!!}{(2k-1)!!} + O_l(k^{3l-1}) = \frac{(2k)^{3l}}{(2l)!3^{2l}} + O_l(k^{3l-1}).$$

Using the log-concavity of the $a(n,k)$s, we see that if we take L even and large enough that $a(2k,k-L)/d^L > a(2k,k-(L+1))/d^{L+1}$, then we have

$$\sum_{l\le L+1} \frac{(-1)^l}{(2l)!}\Big(\frac{(2k)^3}{9d}\Big)^l + O_L\Big(\frac{k^{3L+2}}{d^{L+1}}\Big) \le \sum_l \frac{(-1)^l}{d^l}\frac{a(2k,k-l)}{a(2k,k)} \le \sum_{l\le L} \frac{(-1)^l}{(2l)!}\Big(\frac{(2k)^3}{9d}\Big)^l + O_L\Big(\frac{k^{3L-1}}{d^L}\Big).$$

Taking $L \ge \frac{(2k)^3}{9d}$, we get

$$\sum_l \frac{(-1)^l}{d^l}\frac{a(2k,k-l)}{a(2k,k)} = \cos\left(\sqrt{\tfrac{(2k)^3}{9d}}\right) + O_L(\tfrac{1}{k}) + O(\tfrac{1}{L!}).$$

Similarly, for large k we have

$$\frac{a(2k+1,k-l)}{a(2k+1,k)} = \frac{(2k)^{3l}}{(2l+1)!3^{2l}} + O_l(k^{3l-1}),$$

which gives

$$\sum_l \frac{(-1)^l}{d^l}\frac{a(2k+1,k-l)}{a(2k+1,k)} = \sqrt{\tfrac{9d}{(2k)^3}} \sin\left(\sqrt{\tfrac{(2k)^3}{9d}}\right) + O_L(\tfrac{1}{k}) + O(\tfrac{1}{L!}).$$

Taking L sufficiently large, we see that for $k^3 \le Ld$ (and k,d large) the sign of $f(k)f(k+2)$ is negative unless either k is even and $\sqrt{\frac{(2k)^3}{9d}}$ is close to a multiple of π, or k is odd and $\sqrt{\frac{(2k)^3}{9d}}$ is close to an odd multiple of $\frac{\pi}{2}$. Using Corollary 4, we see that

$$\lim_{d\to\infty} \frac{(2k_{2j-1})^3}{9d} = \left(\pi j - \frac{\pi}{2}\right)^2$$

and

$$\lim_{d\to\infty} \frac{(2k_{2j})^3}{9d} = (\pi j)^2 .$$

□

Remark 7. Numerical calculations support the approximation

$$\nu_k \approx 2k+1+\frac{2}{3\pi}\sqrt{\frac{\nu_k^3}{d}}$$

when k is small compared to d. When $d=1000$ and $k\le 100$, the absolute error is less than 0.05. On the other hand, we seem to have $\nu_d \approx 4d$, so the approximation breaks down for large k.

Proposition 53. *Let*

$$\theta(n) = (1-n)f(n)^2.$$

For $(2k+2)^3 \le 18\alpha d$, $\alpha \le 1$, *we have*

$$\frac{|\theta(2k+2)|}{(2k+2)!}(d+1)^{2k+2} \ge (1-\alpha)^2\frac{d^{2k}}{(d+1)^{2k}}\frac{1}{2}\frac{C_k}{4^k},$$

where $C_k = \frac{1}{k+1}\binom{2k}{k}$ *is the* k*th Catalan number, and*

$$\frac{|\theta(2k+1)|}{(2k+1)!}(d+1)^{2k+1} \ge \left(1-\frac{\alpha}{3}\right)^2\frac{d^{2k-2}}{(d+1)^{2k-2}}\frac{2k(k+1)(2k+1)}{9(d+1)}\frac{C_k}{4^k}.$$

Proof. By the log-concavity of the $a(n,k)$s, since $4k^3+9k^2-4k \le \frac{1}{2}(2k+2)^3 \le 9\alpha d$ we have

$$|f(2k+2)| \ge \frac{d^k}{(d+1)^{2k+1}}\left(a(2k,k)-\frac{1}{d}a(2k,k-1)\right) \ge (1-\alpha)\frac{(2k-1)!!d^k}{(d+1)^{2k+1}},$$

so

$$\frac{|\theta(2k+2)|}{(2k+2)!}(d+1)^{2k+2} \ge (1-\alpha)^2\frac{d^{2k}}{(d+1)^{2k}}\frac{(2k+1)((2k-1)!!)^2}{(2k+2)!} = (1-\alpha)^2\frac{d^{2k}}{(d+1)^{2k}}\frac{1}{2}\frac{C_k}{4^k}.$$

Similarly, using the formulas

$$a(2k-1,k-1) = (2k-1)!! + 2!\binom{2k-1}{3}(2k-5)!! = \frac{(2k+1)!!}{3}$$

and

$$\begin{aligned}a(2k-1,k-2) &= \binom{2k-1}{3}(2k-5)!! + 2!\binom{2k-1}{3}\binom{2k-4}{2}(2k-7)!!\\ &\quad + 3!\binom{2k-1}{4}(2k-5)!! + 4!\binom{2k-1}{5}(2k-7)!!\\ &\quad + \frac{2!^2}{2!}\binom{2k-1}{6}\binom{6}{3}(2k-7)!! + 2!3!\binom{2k-1}{3}\binom{2k-4}{4}(2k-9)!!\\ &\quad + \frac{2!^3}{3!}\binom{2k-1}{9}\binom{9}{3,3,3}(2k-11)!!\\ &= \frac{(k-1)(20k^2+35k-123)}{405}(2k+1)!!,\end{aligned}$$

we see that since $(k-1)(20k^2+35k-123) \le \frac{5}{2}(2k+2)^3 \le 135\frac{\alpha}{3}d$, we have

$$|f(2k+1)| \ge \frac{d^{k-1}}{(d+1)^{2k}}\left(a(2k-1,k-1) - \frac{1}{d}a(2k-1,k-2)\right) \ge \left(1-\frac{\alpha}{3}\right)\frac{(2k+1)!!d^{k-1}}{3(d+1)^{2k}},$$

so

$$\begin{aligned}\frac{|\theta(2k+1)|}{(2k+1)!}(d+1)^{2k+1} &\ge \left(1-\frac{\alpha}{3}\right)^2\frac{d^{2k-2}}{(d+1)^{2k-2}}\frac{2k((2k+1)!!)^2}{9(d+1)(2k+1)!}\\ &= \left(1-\frac{\alpha}{3}\right)^2\frac{d^{2k-2}}{(d+1)^{2k-2}}\frac{2k(k+1)(2k+1)}{9(d+1)}\frac{C_k}{4^k}.\end{aligned}$$

□

We can now give our first improvement on Selberg's lower bound sieve, at $v = d+1$.

Theorem 44. *For every $d \ge 4$ there is a polynomial θ_d of degree $2d+1$ with $\theta_d(0) = 1$, $\theta_d(n) \le 0$ for $n \in \mathbb{N}^+$, and*

$$\sum_n \frac{\theta_d(n)}{n!}(d+1)^n \gg \frac{1}{\sqrt[6]{d}}.$$

Proof. It's easy to see that for any root ν_k of g, we can find a quadratic polynomial q_k such that $q_k(0) = 1$,

$$0 \le q_k(n) \le \left(1-\frac{n}{\nu_k}\right)^2$$

for $n \in \mathbb{N}$, and at least one of $q_k(\lfloor \nu_k \rfloor), q_k(\lceil \nu_k \rceil)$ is 0: for instance, we can take

$$q_k(n) = \left(1-\frac{n}{\nu_k}\right)^2 - \min\left(\frac{1}{\lfloor \nu_k \rfloor}\left(1-\frac{\lfloor \nu_k \rfloor}{\nu_k}\right)^2, \frac{1}{\lceil \nu_k \rceil}\left(1-\frac{\lceil \nu_k \rceil}{\nu_k}\right)^2\right)n.$$

We define θ_d by

$$\theta_d(n) = (1-n)\prod_k q_k(n).$$

If we set $\theta(n) = (1-n)f(n)^2$, then we have

$$\sum_n \frac{\theta_d(n)}{n!}(d+1)^n \geq \sum_n \frac{\theta(n)}{n!}(d+1)^n + \sum_k \min\left(\frac{|\theta(\lfloor \nu_k \rfloor)|}{\lfloor \nu_k \rfloor !}(d+1)^{\lfloor \nu_k \rfloor}, \frac{|\theta(\lceil \nu_k \rceil)|}{\lceil \nu_k \rceil !}(d+1)^{\lceil \nu_k \rceil}\right).$$

Since $\sum_n \frac{\theta(n)}{n!}(d+1)^n = 0$ and $2k+1 \leq \nu_k \leq 2k+2$ for $(2k+2)^3 \leq 18d$, we can apply the previous Proposition to see that

$$\sum_n \frac{\theta_d(n)}{n!}(d+1)^n \geq \sum_{(2k+2)^3 \leq 18d} \left(1 - \frac{(2k+2)^3}{18d}\right)^2 \frac{d^{2k}}{(d+1)^{2k}} \min\left(\frac{1}{2}, \frac{2k(k+1)(2k+1)}{9(d+1)}\right) \frac{C_k}{4^k} \gg \frac{1}{\sqrt[6]{d}}.$$

□

We come at last to trying to prove a lower bound on v_R. For any $v \geq d+1$, we define the polynomial f_v by

$$f_v(n) = \frac{d!}{v^{d+1}} \sum_r \ell_r \binom{n}{r},$$

where

$$\ell_r = (-1)^r \sum_{k=0}^{d+1-r} \frac{d+1-r-k}{k!} v^k,$$

as in Selberg's construction.

Proposition 54. *For $q = v - d \ll \sqrt{d}$, we have*

$$f_v(0) = 1 - \frac{q-1}{v}\frac{d!}{v^d}\sum_r \frac{v^r}{r!} = 1 - \frac{q-1}{v}\Gamma(d+1, v)v^{-d}e^v \gg 1$$

as well as

$$\sum_n \frac{(1-n)f_v(n)^2}{n!}v^n = -e^v \frac{d!}{v^{d+1}}(q-1)f_v(0) = -(\sqrt{2\pi} + o(1))e^{\frac{q^2}{2d}}\frac{q-1}{\sqrt{d}}f_v(0).$$

Furthermore, for every nonnegative integer n we have

$$\frac{d}{dv}\left(v^{n+1}f_v(n+2)\right) = nv^n f_v(n+1)$$

and

$$f_v(n+2) = \frac{1}{v^{n+1}}\sum_k (-1)^k a_q(n,k)d^k.$$

Proof. The first two claims are easy calculations. For the last two claims, we use an analogous argument to the proof of Proposition 16 to see that

$$f_v(n+2) = \frac{1}{v^{n+1}}\sum_j (-1)^j v^{n-j} j! \binom{d}{j}\binom{n}{j}.$$

Multiplying by v^{n+1} and differentiating each term of the sum with respect to v we get the claim about the derivative of $v^{n+1}f_v(n+2)$. The last claim follows from Proposition 17. □

Lemma 1. *For $0 \le k = v - d - 1 \le \frac{\sqrt[3]{d}}{3}$ and $1 \le j \le \sqrt[3]{d} - 1$ we have*

$$d^{j-1}\left(\frac{2j+1}{3} + k\right)(2j-1)!! \ge (-1)^{j-1}v^{2j}f_v(2j+1) \ge \left(1 - \frac{4}{27}\right)d^{j-1}\frac{(2j+1)!!}{3}$$

and

$$d^j(2j-1)!! \ge (-1)^j v^{2j+1}f_v(2j+2) \ge d^{j-1}\left(\frac{5d}{9} - \frac{2kj(2j+1)}{3} - k^2 j\right)(2j-1)!! \ge 0.$$

Proof. We prove these inequalities by induction on j. For the base case we use the identity $vf_v(2) = 1$. By the previous Proposition, we have

$$v^{2j}f_v(2j+1) = (d+1)^{2j}g(2j+1) + (2j-1)\int_{u=d+1}^{v} u^{2j-1}f_u(2j)du.$$

By the induction hypothesis, we have $(-1)^{j-1}f_u(2j) \ge 0$ and $(-1)^{j-1}u^{2j-1}f_u(2j) \le d^{j-1}(2j-3)!!$, so the claim follows from the bounds established on $g(2j+1)$ in Proposition 53. The second bound is proved the same way, except this time $(-1)^j v^{2j+1}f_v(2j+2)$ is decreasing in v. □

Theorem 45. *If $R = 2d+1$ and $d \ge 8$ then $v_R - (d+1) \gg \sqrt[3]{d}$.*

Proof. By the same argument as the one used in the proof of Theorem 44, for any $v \le d + 1 + \frac{\sqrt[3]{d}}{3}$ we can find a polynomial θ_v of degree $2d+1$ with $\theta_v(0) = f_v(0)^2$,

$$0 \ge \theta_v(n) \ge (1-n)f_v(n)^2$$

for $n \in \mathbb{N}^+$, and such that for any $1 \le j \le \sqrt[3]{d} - 1$ at least one of $\theta_v(2j+1), \theta_v(2j+2)$ vanishes. Setting $k = v - d - 1$, we see that

$$\sum_n \frac{\theta_v(n)}{n!}v^n \ge \sum_n \frac{(1-n)f_v(n)^2}{n!}v^n + \sum_{1 \le j \le \sqrt[3]{d}-1} \min\left(\frac{2jf_v(2j+1)^2}{(2j+1)!}v^{2j+1}, \frac{(2j+1)f_v(2j+2)^2}{(2j+2)!}v^{2j+2}\right).$$

By the previous Lemma and Proposition, this is at least

$$-e^v\frac{d!}{v^{d+1}}k + \sum_{1 \le j \le \sqrt[3]{d}-1} \min\left(\left(1 - \frac{4}{27}\right)^2 \frac{2j(j+1)(2j+1)d^{2j-2}}{9v^{2j-1}}, \right.$$
$$\left. \frac{1}{2}\left(\frac{5d}{9} - \frac{2kj(2j+1)}{3} - k^2 j\right)^2 \frac{d^{2j-2}}{v^{2j}}\right)\frac{C_j}{4^j}.$$

The sum in the above is easily seen to be $\gg \frac{1}{\sqrt[6]{d}}$, and $e^v \frac{d!}{v^{d+1}} k \ll \frac{k}{\sqrt{d}}$, so for $k \ll \sqrt[3]{d}$ the above is positive. □

The implied constant in the previous Theorem is very small. In order to get a better constant, we have to get more accurate bounds for f_v, and further we need the bounds to be valid in a larger range for j, k. One can argue similarly to Corollary 14 to show that if $j, k, d \to \infty$ with $j^3, k^3 \ll d$, and $v = d + k + 1$, then we have

$$(-1)^{j-1} v^{2j} f_v(2j+1) \approx d^{j-1} \sqrt{\tfrac{d}{2j}} \sin\left(\left(\tfrac{2j}{3} + k\right)\sqrt{\tfrac{2j}{d}}\right)(2j-1)!!$$

and

$$(-1)^{j} v^{2j+1} f_v(2j+2) \approx d^{j} \cos\left(\left(\tfrac{2j}{3} + k\right)\sqrt{\tfrac{2j}{d}}\right)(2j-1)!!.$$

Appendix B

Solution to system of functional inequalities

In this appendix, we will state and prove the full form of Theorem 41. In order to state it correctly, we need to first define the topological space on which the associated measure is constructed.

B.1 Decorated reals and the decorated triangle

In order to choose how to break ties in inequalities, we will "decorate" real numbers with exponents from $\{+,-\}$, so that x^+ should be thought of as a number infinitesimally greater than x while x^- should be thought of as a number infinitesimally smaller than x.

Definition 19. A *decorated real* is an element $(x,\pm)$ of $\mathbb{R}\times\{+,-\}$. We write $x^\pm$ as shorthand for $(x,\pm)$, and we call the choice of sign $\pm$ the *decoration* of $x^\pm$. We write $\mathbb{R}^\pm$ for the set of decorated real numbers. We define an ordering on $\mathbb{R}^\pm$ by $a^\mp < b^\pm$ if either $a<b$ or $a=b$ and $\mp<\pm$. We define the *decorated interval* $I^\pm$ to be $I^\pm=[0^-,1^+]$. We define the topology on $\mathbb{R}^\pm$ to be the open interval topology.

Now we collect a few basic facts about this topological space.

Proposition 55. *$\mathbb{R}^\pm$ is a totally disconnected Hausdorff space, and the sets $[a^+,b^-]$ with $a<b$ form a base of open sets for $\mathbb{R}^\pm$. If $I^\pm=[0^-,1^+]$ with the induced topology, then $I^\pm$ is compact, and every clopen set of $I^\pm$ is a finite union of basic open sets of $\mathbb{R}^\pm$ and possibly endpoints $0^-,1^+$ of $I^\pm$.*

Any nondecreasing function $f:[0,1]\to[0,1]$ can be associated to a probability measure on $I^\pm$, such that the measure of the set $[0^-,a^-]$ is $f(a)$. The main result of this section can be viewed as a sort of 2-dimensional generalization of this fact.

Definition 20. The *decorated triangle* $\Delta^{\pm}$ is the set of $(x^{\pm}, y^{\pm}, z^{\pm}) \in (I^{\pm})^3$ such that $x+y+z = 2$ and such that the three decorations are not all equal. A polygon contained in $\Delta^{\pm}$ is called *aligned* if every edge is perpendicular to one of the x, y, or z axes, and if it is clopen. An aligned polygon is called an *xy-rectangle* if it is convex and every edge is perpendicular to either the x-axis or to the y-axis.

Proposition 56. *$\Delta^{\pm}$ is a closed subset of $(I^{\pm})^3$, and is therefore compact. The clopen subsets of $\Delta^{\pm}$ are exactly the finite unions of aligned polygons and possibly clopen subsets of the edges $\{x^{\pm} = 1^+\}, \{y^{\pm} = 1^+\}, \{z^{\pm} = 1^+\}$ of $\Delta^{\pm}$. If an aligned polygon P of $\Delta^{\pm}$ is written as a disjoint union of an arbitrary set of aligned polygons, then the union must actually be a finite dissection of P.*

We will eventually construct a measure on $\Delta^{\pm}$ by first defining it on xy-rectangles and aligned triangles. To that end, we need the following result.

Theorem 46. *If μ is a function taking xy-rectangles and aligned triangles to $[0, 1]$, then it can be extended to a measure on the σ-algebra generated by the aligned polygons if and only if it satisfies the following three dissection conditions.*

a) If an xy-rectangle S can be dissected into two aligned triangles T_1, T_2, then $\mu(S) = \mu(T_1)+\mu(T_2)$ (note that in this case, S must be "square").

b) If an xy-rectangle R is dissected into two smaller xy-rectangles R_1, R_2 (by cutting it in either the x direction or the y direction), then $\mu(R) = \mu(R_1) + \mu(R_2)$.

c) If an aligned triangle T is dissected into an xy-rectangle R and two smaller aligned triangles T_1, T_2, then $\mu(T) = \mu(R) + \mu(T_1) + \mu(T_2)$.

Proof. First we describe how to extend μ to arbitrary aligned polygons. Let P be an aligned polygon. We say that a finite set of line segments L contained in P is *good* if it satisfies the following conditions:

- every edge of P is in L,
- every element of L has its endpoints on the boundary of P,
- every element of L which is not a boundary segment of P is perpendicular to either the x-axis or the y-axis,
- at any point p where two elements of L meet, there is a segment from L passing through p which are perpendicular to the x-axis and a segment from L through p perpendicular to the y-axis.

First we show that a finite good set of lines L exists. Only the last condition on the set L poses any trouble, but we can satisfy it by adding sequences of lines that "bounce" off the edges of P

perpendicular to the z-axis finitely many times. It's easy to see that the segments in a good set L dissect P into finitely many rectangles and triangles, and we define $\mu(P)$ to be the sum of μ applied to all these rectangles and triangles. To see that this is well-defined, let L and L' be two good collections of lines, and note that $L \cup L'$ is also a good collection of lines, and that $L \cup L'$ may be obtained from either L or L' by a sequence of dissections as in conditions b) and c) of the theorem statement.

To see that μ is finitely additive on clopen sets, it's enough to check that if P is an aligned polygon and l is any line segment dividing P into two aligned polygons P_1, P_2, then $\mu(P) = \mu(P_1) + \mu(P_2)$. If l is perpendicular to either the x-axis or the y-axis, this follows from the fact that $\mu(P)$ is well-defined. Otherwise, we can cover l with small xy-squares and apply condition a) to get rid of it, then extend all the edges of these xy-squares to the boundary of P and finish using the fact that $\mu(P)$ is well-defined.

To see that μ is *countably* additive on clopen sets, we just note that by compactness, if any countable disjoint union of clopen sets is clopen, then it must in fact be a finite union. Thus we may apply Carathéodory's extension theorem to finish the proof. □

B.2 Going from functions to measures

Theorem 47 (Theorem 41)**.** *Suppose $f : [0,1] \to \mathbb{R}_{\geq 0}$ and $g : [0,1]^2 \to \mathbb{R}_{\geq 0}$ are nonnegative functions such that, for some $\epsilon > 0$, we have*

$$x + y \leq 1 \implies g(x,y) = 0,$$

$$|x + y + z - 2| < \epsilon \implies f(x) + f(y) + f(z) \leq g(x,y) + g(x,z) + g(y,z) + 1,$$

and

$$x + y + z = 2 \implies f(x) + f(y) + f(z) = g(x,y) + g(x,z) + g(y,z) + 1.$$

Then we have

a) f is nondecreasing,

b) for every integer $n \geq \frac{1}{\epsilon}$,

$$\frac{f(\frac{1}{n}) + \cdots + f(\frac{n-1}{n})}{n-1} \leq \frac{1}{3} \leq \frac{f(\frac{0}{n}) + \cdots + f(\frac{n}{n})}{n+1},$$

c) f is integrable and $\int_0^1 f(x)dx = \frac{1}{3}$,

d) g is nondecreasing in either argument, and moreover satisfies the inequality

$$x_1 \leq x_2,\ y_1 \leq y_2 \implies g(x_2, y_2) - g(x_1, y_2) \geq g(x_2, y_1) - g(x_1, y_1),$$

e) there is a symmetric probability distribution μ on the σ-algebra generated by the clopen subsets of $\Delta^{\pm}$, such that for all $x, y \in \mathbb{R}$ we have

$$f(x) = \mathbb{P}_{\mu(a,b,c)}[a < x],\ g(x, y) = \mathbb{P}_{\mu(a,b,c)}[a < x \wedge b < y].$$

Proof. Part a): suppose $0 \leq a < b \leq 1$ with $b - a < \epsilon$, we will show that $f(a) \leq f(b)$. Choose a nonnegative integer k such that

$$2a - b < k(b - a) < b.$$

For each $0 \leq i \leq k$, set

$$x_{2i} = 1 - \frac{b + (k - 2i)(b - a)}{2},\ x_{2i+1} = 1 - \frac{b + (2i - k)(b - a)}{2}.$$

Note that by the choice of k we have $a + x_0 = a + x_{2k+1} < 1$ and $1 - b < x_i < 1$ for all $0 \leq i \leq 2k+1$. Furthermore, for each i we have $b + x_{2i} + x_{2i+1} = 2$ and $a + x_{2i-1} + x_{2i} = 2$. Thus, for each $0 \leq i \leq k$ we have

$$\begin{aligned} f(b) + f(x_{2i}) + f(x_{2i+1}) &= g(b, x_{2i}) + g(b, x_{2i+1}) + g(x_{2i}, x_{2i+1}) + 1, \\ f(a) + f(x_{2i}) + f(x_{2i+1}) &\leq g(a, x_{2i}) + g(a, x_{2i+1}) + g(x_{2i}, x_{2i+1}) + 1, \end{aligned}$$

and for each $1 \leq i \leq k$ we have

$$\begin{aligned} f(b) + f(x_{2i-1}) + f(x_{2i}) &\leq g(b, x_{2i-1}) + g(b, x_{2i}) + g(x_{2i-1}, x_{2i}) + 1, \\ f(a) + f(x_{2i-1}) + f(x_{2i}) &= g(a, x_{2i-1}) + g(a, x_{2i}) + g(x_{2i-1}, x_{2i}) + 1. \end{aligned}$$

Adding together the inequalities and subtracting the equalities, we get

$$\begin{aligned} f(a) &\leq f(b) + g(a, x_0) + g(a, x_{2k+1}) - g(b, x_0) - g(b, x_{2k+1}) \\ &= f(b) - g(b, x_0) - g(b, x_{2k+1}) \leq f(b). \end{aligned}$$

Part b): first we prove the left hand inequality. For every ordered triple of integers $0 < i, j, k < n$ satisfying $i + j + k = 2n$, we have an equality

$$f(\tfrac{i}{n}) + f(\tfrac{j}{n}) + f(\tfrac{k}{n}) = g(\tfrac{i}{n}, \tfrac{j}{n}) + g(\tfrac{i}{n}, \tfrac{k}{n}) + g(\tfrac{j}{n}, \tfrac{k}{n}) + 1.$$

Also, for every ordered triple $0 < i, j, k < n$ satisfying $i + j + k = 2n - 1$, we have the inequality

$$f(\tfrac{i}{n}) + f(\tfrac{j}{n}) + f(\tfrac{k}{n}) \leq g(\tfrac{i}{n}, \tfrac{j}{n}) + g(\tfrac{i}{n}, \tfrac{k}{n}) + g(\tfrac{j}{n}, \tfrac{k}{n}) + 1.$$

Adding the inequalities and subtracting the equalities, and using $g(\frac{i}{n}, \frac{j}{n}) = 0$ when $i + j = n$, gives the left hand inequality of b). For the right hand inequality of b) one uses equalities corresponding to triples $0 \leq i, j, k \leq n$ with $i + j + k = 2n$, and inequalities corresponding to triples $0 \leq i, j, k \leq n$ with $i + j + k = 2n + 1$.

Part c) follows immediately from parts a) and b).

First we prove part d) in the case $x_2 - x_1 = y_2 - y_1 < \epsilon$. If $x_2 + y_1 = x_1 + x_2 < 1$, it is immediate. If $x_2 + y_1 = x_1 + y_2 \geq 1$, then adding the inequalities and subtracting the equalities in

$$\begin{aligned}
f(x_2) + f(y_1) + f(2 - x_2 - y_1) &= g(x_2, y_1) + g(x_2, 2 - x_2 - y_1) + g(y_1, 2 - x_2 - y_1) + 1, \\
f(x_1) + f(y_2) + f(2 - x_2 - y_1) &= g(x_1, y_2) + g(x_1, 2 - x_2 - y_1) + g(y_2, 2 - x_2 - y_1) + 1, \\
f(x_1) + f(y_1) + f(2 - x_2 - y_1) &\leq g(x_1, y_1) + g(x_1, 2 - x_2 - y_1) + g(y_1, 2 - x_2 - y_1) + 1, \\
f(x_2) + f(y_2) + f(2 - x_2 - y_1) &\leq g(x_2, y_2) + g(x_2, 2 - x_2 - y_1) + g(y_2, 2 - x_2 - y_1) + 1,
\end{aligned}$$

we get

$$g(x_2, y_2) - g(x_1, y_2) \geq g(x_2, y_1) - g(x_1, y_1).$$

Note that the constraint on x_1, x_2, y_1, y_2 is that the four points (x_i, y_i) form a square of side length at most ϵ. Since any rectangle whose sidelengths are rational multiples of each other can be dissected into finitely many squares of arbitrarily small sidelength, we see that the inequality above holds whenever $x_2 - x_1$ is a rational multiple of $y_2 - y_1$.

Next, we note that for any $x_1 < x_2$ and any y in $[0, 1]$, there is some $0 \leq y' \leq y$ such that $x_1 + y' < 1$ and $y - y'$ is a rational multple of $x_2 - x_1$, since the rationals are dense in the reals. Choosing such a y', we get

$$g(x_2, y) - g(x_1, y) \geq g(x_2, y') - g(x_1, y') = g(x_2, y') \geq 0.$$

Thus g is increasing in the first argument. Since our assumptions easily imply that g is symmetric (swap y and z in the third assumption to see that $g(y, z) = g(z, y)$ when $y + z \geq 1$), g is also increasing in the second argument.

To finish the proof of part d), assume for a contradiction that for some x_1, x_2, y_1, y_2 with $x_1 < x_2$ and $y_1 < y_2$ we have

$$g(x_2, y_2) - g(x_1, y_2) < g(x_2, y_1) - g(x_1, y_1).$$

Let $\alpha = g(x_2, y_2) - g(x_1, y_2)$, and let $\beta = g(x_2, y_1) - g(x_1, y_1)$. We will show that for any u, v with

$y_1 \leq u < v \leq y_2$, we have

$$g(x_1, v) \geq g(x_1, u) + \beta - \alpha.$$

Applying this repeatedly, we will see that $g(x_1, y_2) \geq g(x_1, y_1) + k(\beta - \alpha)$ for all $k \in \mathbb{N}$, giving us a contradiction when we take k sufficiently large.

Start by picking u' with $u < u' < v$ such that $u' - y_1$ is a rational multiple of $x_2 - x_1$, so that we have

$$g(x_2, u') - g(x_1, u') \geq g(x_2, y_1) - g(x_1, y_1) = \beta.$$

Next we pick v' with $u' < v' < v$ such that $y_2 - v'$ is a rational multiple of $x_2 - x_1$, so that we have

$$\alpha = g(x_2, y_2) - g(x_1, y_2) \geq g(x_2, v') - g(x_1, v').$$

Combining these two inequalities with the fact that g is increasing in the second argument, we have

$$\begin{aligned} g(x_1, v) &\geq g(x_1, v') \\ &\geq g(x_2, v') - \alpha \\ &\geq g(x_2, u') - \alpha \\ &\geq g(x_1, u') + \beta - \alpha. \end{aligned}$$

In preparation for part e), we will need a variation on part d). If $a < b$ and $b - a < \epsilon$, then

$$\begin{aligned} f(a) + f(1-b) + f(1) &\leq g(a, 1) + g(1-b, 1) + 1, \\ f(b) + f(1-b) + f(1) &= g(b, 1) + g(1-b, 1) + g(b, 1-b) + 1, \end{aligned}$$

so

$$f(b) - f(a) \geq g(b, 1) - g(a, 1) + g(b, 1-b).$$

Part e): we need to define μ and check that it is symmetric. By Proposition 56 and Theorem 46, in order to define μ we just need to define μ on aligned triangles, xy-rectangles, and basic intervals on the boundary of $\Delta^{\pm}$ and check that our definition satisfies the compatibility conditions a), b), c) of Theorem 46. We will define the triangle $\Delta_{a,b,c} \subset \Delta^{\pm}$ to be the set of points $(x^{\pm}, y^{\pm}, z^{\pm}) \in \Delta^{\pm}$ such that either all three of the inequalities $x^{\pm} < a$, $y^{\pm} < b$, $z^{\pm} < c$ hold or all three of them fail.

Then we define μ by

$$\begin{aligned}
\mu(\Delta_{x,y,z}) &= g(x,y) + g(x,z) + g(y,z) - f(x) - f(y) - f(z) + 1, \\
\mu\big(((x_1,x_2)\times(y_1,y_2)\times I^{\pm})\cap\Delta^{\pm}\big) &= g(x_2,y_2) - g(x_1,y_2) - g(x_2,y_1) + g(x_1,y_1), \\
\mu\big(((x_1,x_2)\times\{1^+\}\times I^{\pm})\cap\Delta^{\pm}\big) &= f(x_2) - f(x_1) - g(x_2,1) + g(x_1,1), \\
\mu\big(((x_1,x_2)\times(1-x_2,1-x_1)\times\{1^+\})\cap\Delta^{\pm}\big) &= g(x_2,1-x_1) - g(x_1,1-x_1) - g(x_2,1-x_2) - \mu(\Delta_{x_2,1-x_1,1}), \\
\mu(\{(1^+,1^+,0^-)\}) &= 1 - 2f(1) + g(1,1) = f(0) - 2g(0,1).
\end{aligned}$$

To check compatibility condition a) of Theorem 46, consider the square with sides at x-coordinates x_1, x_2 and y-coordinates at y_1, y_2, such that $x_2 - x_1 = y_2 - y_1$, and define z by

$$z = 2 - x_2 - y_1 = 2 - x_1 - y_2.$$

Then we have

$$\begin{aligned}
\mu\big(((x_1,x_2)\times(y_1,y_2)\times I^{\pm})\cap\Delta^{\pm}\big) &= g(x_2,y_2) - g(x_1,y_2) - g(x_2,y_1) + g(x_1,y_1) \\
&= \mu(\Delta_{x_2,y_2,z}) - \mu(\Delta_{x_1,y_2,z}) - \mu(\Delta_{x_2,y_1,z}) + \mu(\Delta_{x_1,y_1,z}) \\
&= \mu(\Delta_{x_2,y_2,z}) + \mu(\Delta_{x_1,y_1,z})
\end{aligned}$$

since $\mu(\Delta_{x_1,y_2,z}) = \mu(\Delta_{x_2,y_1,z}) = 0$ by the definition of z and our third assumption.

Compatibility condition b) of Theorem 46 follows directly from the way we defined μ on xy-rectangles. For compatibility condition c), suppose that x_1, x_2, y_1, y_2, z have $(x_2 - x_1)(y_2 - y_1) > 0$ and $x_2 + y_2 + z = 2$, so that $\Delta_{x_1,y_1,z}$ is dissected into $\Delta_{x_1,y_2,z}, \Delta_{x_2,y_1,z}$, and the xy-rectangle with sides at x-coordinates x_1, x_2 and y-coordinates y_1, y_2. Then

$$\begin{aligned}
\mu(\Delta_{x_1,y_1,z}) &= \mu(\Delta_{x_1,y_1,z}) + \mu(\Delta_{x_2,y_2,z}) \\
&= \mu(\Delta_{x_1,y_2,z}) + \mu(\Delta_{x_1,y_2,z}) + \mu\big(((x_1,x_2)\times(y_1,y_2)\times I^{\pm})\cap\Delta^{\pm}\big)
\end{aligned}$$

since $\mu(\Delta_{x_2,y_2,z}) = 0$ (by $x_2 + y_2 + z = 0$ and our third assumption).

By our second assumption, part d), and the inequality proved just after part d), μ takes nonnegative values on all sufficiently small aligned triangles, xy-rectangles, and clopen subsets of the boundary of $\Delta^{\pm}$, and thus it takes nonnegative values on all clopen subsets of $\Delta^{\pm}$.

Finally, we check that μ is symmetric with respect to permuting the coordinates. Since μ is determined by its values on aligned triangles and xy-rectangles (and subsets of the boundary of $\Delta^{\pm}$, which we leave to the reader), and since the definition of $\mu(\Delta_{x,y,z})$ is clearly invariant under permuting x, y, z, we just need to check that the measure assigned to an xy-rectangle doesn't change when we swap the y and z coordinates. Consider the xy-rectangle with sides at x-coordinates x_1, x_2

and y-coordinates y_1, y_2. After swapping the y and z coordinates, we can dissect the resulting aligned parallelogram into $\Delta_{x_1,2-x_1-y_2,y_1}, \Delta_{x_2,2-x_2-y_1,y_2}$, and a signed copy of the xy-rectangle with sides at x-coordinates x_1, x_2 and y-coordinates $2-x_2-y_1, 2-x_1-y_2$. So we need to check the identity

$$\begin{aligned} g(x_2,y_2)-g(x_1,y_2)-g(x_2,y_1)+g(x_1,y_1) = \\ \mu(\Delta_{x_1,2-x_1-y_2,y_1})+\mu(\Delta_{x_2,2-x_2-y_1,y_2})+g(x_2,2-x_1-y_2) \\ -g(x_1,2-x_1-y_2)-g(x_2,2-x_2-y_1)+g(x_1,2-x_2-y_1). \end{aligned}$$

After the dust settles, the difference of the two sides comes out to

$$\mu(\Delta_{x_1,y_2,2-x_1-y_2})+\mu(\Delta_{x_2,y_1,2-x_2-y_1})=0,$$

and we are done. □

Bibliography

[1] F. Brenti. *Unimodal, Log-concave and Pólya Frequency Sequences in Combinatorics*. Number no. 413 in Memoirs of the AMS Series. American Mathematical Soc.

[2] Gruia Calinescu, Chandra Chekuri, Martin Pál, and Jan Vondrák. Maximizing a monotone submodular function subject to a matroid constraint. *SIAM J. Comput.*, 40(6):1740–1766, 2011.

[3] H. Diamond, H. Halberstam, and H.-E. Richert. Combinatorial sieves of dimension exceeding one. *J. Number Theory*, 28(3):306–346, 1988.

[4] Peter Donnelly and Geoffrey Grimmett. On the asymptotic distribution of large prime factors. *J. London Math. Soc. (2)*, 47(3):395–404, 1993.

[5] Rod G. Downey and Michael R. Fellows. Fixed-parameter tractability and completeness. I. Basic results. *SIAM J. Comput.*, 24(4):873–921, 1995.

[6] Uriel Feige. A threshold of ln n for approximating set cover. *J. ACM*, 45(4):634–652, July 1998.

[7] K. Ford, B. Green, S. Konyagin, J. Maynard, and T. Tao. Long gaps between primes. *ArXiv e-prints*, December 2014.

[8] John Friedlander and Henryk Iwaniec. *Opera de cribro*, volume 57 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, RI, 2010.

[9] Thomas R. Hagedorn. Computation of Jacobsthal's function $h(n)$ for $n < 50$. *Math. Comp.*, 78(266):1073–1087, 2009.

[10] L. G. Hačijan. Polynomial algorithms in linear programming. *Zh. Vychisl. Mat. i Mat. Fiz.*, 20(1):51–68, 260, 1980.

[11] D. R. Heath-Brown. Zero-free regions for Dirichlet L-functions, and the least prime in an arithmetic progression. *Proc. London Math. Soc. (3)*, 64(2):265–338, 1992.

[12] Adolf Hildebrand. On the number of positive integers $\leq x$ and free of prime factors $> y$. *J. Number Theory*, 22(3):289–307, 1986.

[13] Adolf Hildebrand and Gérald Tenenbaum. On a class of differential-difference equations arising in number theory. *J. Anal. Math.*, 61:145–179, 1993.

[14] H. Iwaniec. On the error term in the linear sieve. *Acta Arith.*, 19:1–30, 1971.

[15] Henryk Iwaniec. A new form of the error term in the linear sieve. *Acta Arith.*, 37:307–320, 1980.

[16] Henryk Iwaniec. Rosser's sieve. *Acta Arith.*, 36(2):171–202, 1980.

[17] H.-J. Kanold. Über primzahlen m arithmetischen folgen. *Mathematische Annalen*, 156:393–396, 1964.

[18] H.J. Kanold. Über eine zahlentheoretische funktion von jacobsthal. *Mathematische Annalen*, 170:314–326, 1967.

[19] J. F. C. Kingman, S. J. Taylor, A. G. Hawkes, A. M. Walker, David Roxbee Cox, A. F. M. Smith, B. M. Hill, P. J. Burville, and T. Leonard. Random discrete distribution. *J. Roy. Statist. Soc. Ser. B*, 37:1–22, 1975. With a discussion by S. J. Taylor, A. G. Hawkes, A. M. Walker, D. R. Cox, A. F. M. Smith, B. M. Hill, P. J. Burville, T. Leonard and a reply by the author.

[20] Isamu Kobayashi. A note on the Selberg sieve and the large sieve. *Proc. Japan. Acad.*, 49:1–5, 1973.

[21] U. V. Linnik. On the least prime in an arithmetic progression. I. The basic theorem. *Rec. Math. [Mat. Sbornik] N.S.*, 15(57):139–178, 1944.

[22] U. V. Linnik. On the least prime in an arithmetic progression. II. The Deuring-Heilbronn phenomenon. *Rec. Math. [Mat. Sbornik] N.S.*, 15(57):347–368, 1944.

[23] Yu. V. Matiyasevich. *Desyataya problema Gil'berta*, volume 26 of *Matematicheskaya Logika i Osnovaniya Matematiki [Monographs in Mathematical Logic and Foundations of Mathematics]*. VO "Nauka", Moscow, 1993.

[24] H. L. Montgomery. A note on the large sieve. *Journal of the London Mathematical Society*, s1-43(1):93–98, 1968.

[25] Hugh L. Montgomery. The analytic principle of the large sieve. *Bull. Amer. Math. Soc.*, 84(4):547–567, 1978.

[26] Yoichi Motohashi. A note on the large sieve. II. *Proc. Japan Acad. Ser. A Math. Sci.*, 53(4):122–124, 1977.

[27] Prasad Raghavendra. *Approximating np-hard problems efficient algorithms and their limits.* PhD thesis, University of Washington, 2009.

[28] Atle Selberg. *Collected papers. Vol. II.* Springer-Verlag, Berlin, 1991. With a foreword by K. Chandrasekharan.

[29] Alfred Tarski. *A decision method for elementary algebra and geometry.* University of California Press, Berkeley and Los Angeles, Calif., 1951. 2nd ed.

[30] R. C. Vaughan. On the order of magnitude of Jacobsthal's function. *Proc. Edinburgh Math. Soc. (2)*, 20(4):329–331, 1976/77.

[31] Ferrell S. Wheeler. Two differential-difference equations arising in number theory. *Trans. Amer. Math. Soc.*, 318(2):491–523, 1990.

[32] Triantafyllos Xylouris. *Über die Nullstellen der Dirichletschen L-Funktionen und die kleinste Primzahl in einer arithmetischen Progression*, volume 404 of *Bonner Mathematische Schriften [Bonn Mathematical Publications]*. Universität Bonn, Mathematisches Institut, Bonn, 2011. Dissertation for the degree of Doctor of Mathematics and Natural Sciences at the University of Bonn, Bonn, 2011.

[33] M. Ziller and J. F. Morack. Algorithmic concepts for the computation of Jacobsthal's function. *ArXiv e-prints*, November 2016.