Toward a theory of prime producing sieves

Kevin Ford
(joint work with James Maynard)

July 12, 2023

Sieving for primes in an arbitrary set (the small sieve)

$$(\mathcal{A} \subset [1,x]): \quad S(\mathcal{A}) := \#\{a \in \mathcal{A} : (a,Q) = 1\} \qquad Q = \prod_{p \leqslant \sqrt{x}} p,$$

$$= \sum_{\substack{d|Q \\ d \leqslant x}} \mu(d)|\mathcal{A}_d|, \qquad \mathcal{A}_d = \{a \in \mathcal{A} : d|a\}$$

$$\geqslant \sum_{d \leqslant D} \lambda_d^- |\mathcal{A}_d|.$$

Question: If $|\mathcal{A}_d|$ well-behaved for most $d < x^{1-\varepsilon}$, must $S(\mathcal{A})$ be large?

No! Selberg's example:

$$\mathcal{A} = \{1 \leqslant n \leqslant x : n \text{ has an even number of prime factors}\},$$

for which $|\mathcal{A}_d| \sim \frac{x}{2d}$ for $d < x^{1-\varepsilon}$, yet $\mathcal{A}$ has no primes.

Bombieri's work

Bombieri, 1970s. If $\mathcal{A}_d$ is well-behaved up to x^γ for every fixed $\gamma < 1$ (Type-I bounds), and $\mathcal{B}$ is any "sufficiently dense, parity-balanced" set (gives "equal weight" to numbers with an even number of prime factors and those with an odd number of prime factors), then get an asymptotic formula for $|\mathcal{A} \cap \mathcal{B}|$.

This excludes $\mathcal{B}$ being only primes!

Theorem (KF, 2005). The conclusion need not hold if $\mathcal{A}_d$ is well-behaved up to x^γ for a *fixed* $\gamma < 1$.

Breaking the parity barrier with bilinear sums.

Adding a hypothesis on *bilinear sums* allows one to break the parity barrier and detect primes in some *thin sets* $\mathcal{A}$ (the idea goes back to work of Vinogradov in the 1930s).

This led to many successes:

- **Friedlander and Iwaniec, 1998.** There are infinitely many primes of the form $x^2 + y^4$, with x, y integers.
- **Heath-Brown, 2001.** There are infinitely many primes of the form $x^3 + 2y^3$, with x, y positive integers.
- **Maynard, 2019.** Given any $d \in \{0, 1, \ldots, 9\}$, there are infinitely many primes that do not have digit d in base-10.

Parity breaking sieves: set-up

Sequence $a_n \geqslant 0$ for $x/2 < n \leqslant x$
Normalized to have average value 1. Set $a_n = 1 + w_n$, (simplified model)
Example: a_n is constant times indicator function of $\mathcal{A}$

Three basic parameters: γ, θ, ν.

$$\sum_{d \leqslant x^\gamma} \Big| \sum_{d|n} w_n \Big| \ll_A \frac{x}{(\log x)^A} \quad \text{(Type-I bound).}$$

For any divisor-bounded complex sequences $(\alpha_n), (\beta_n)$,

$$\Big| \sum_{x^\theta \leqslant m \leqslant x^{\theta+\nu}} \alpha_m \sum_{x/2 < mn \leqslant x} \beta_n w_{mn} \Big| \ll_A \frac{x}{(\log x)^A} \quad \text{(Type-II bound).}$$

Parity-breaking sieves: some successes

For certain (γ, θ, ν), if the Type-I / Type-II bounds hold, then

$$\sum_{p \text{ prime}} a_p \gg \frac{x}{\log x}.$$

γ	$[\theta, \theta+\nu]$	Application
3/4	$[1/4, 3/4]$	Primes of form x^2+y^4 (Friedlander-Iwaniec)
3/4	$[1/4, 1/3]$	Primes of form $x^2+(y^2+1)^2$ (Merikoski)
19/28	$[9/28, 10/28]$	Fractional part of αp (Jia)
2/3	$[1/3, 2/3]$	Primes of form x^3+2y^3 (Heath-Brown)
16/25	$[9/25, 17/40]$	Primes with a missing digit (Maynard)
1/2	$[0, 1/3]$	Solving $x^2 \equiv a \pmod{p}$ (Duke-Friedlander-Iwaniec)
1/2	$[0, 1/5]$	Dynam. systems at prime times (Sarnak-Ubis)

(lower bound) $C(\gamma, \theta, \nu)$ is the supremum of numbers c so that any sequence satisfying the Type-I and Type-II bounds gives

$$\sum_{p \text{ prime}} a_p \geqslant \frac{c \cdot (x/2)}{\log x} \qquad \text{(large } x\text{)}.$$

(Asymptotic) Hypothesis $A(\gamma, \theta, \nu)$: for any sequence satisfying the Type-I and Type-II bounds,

$$\sum_{p \text{ prime}} a_p \sim \frac{x/2}{\log x} \qquad (x \to \infty).$$

Main questions

1. For which (γ, θ, ν) does Hypothesis $A(\gamma, \theta, \nu)$ hold?
2. For which (γ, θ, ν) is $C(\gamma, \theta, \nu) > 0$?
3. For which (γ, θ, ν) are there sequences a_n with $\sum a_p = 0$?

Comments on existing approaches

Existing results produce some ranges of (γ, θ, ν) so that we have an asymptotic for Σa_p (Hypothesis $A(\gamma, \theta, \nu)$ holds) and some ranges where $C(\gamma, \theta, \nu) > 0$, i.e., we detect primes.

Tools: identities of Linnik, Vaughan, Heath-Brown (for asymptotics)
Buchstab iteration / Harman's sieve (for lower bounds)

The methods are largely ad-hoc and do not shed any light on the optimality or the limitations of these approaches.

When $\nu = 0$ (no Type-II information), Selberg's example shows that $C(\gamma, \theta, 0) = 0$ for all $\gamma < 1$ (in fact there are sequences with $\Sigma a_p = 0$).

When $\nu > 0$, there are no examples in the literature with $\Sigma a_p = 0$ or showing that $A(\gamma, \theta, \nu)$ does not hold.

A new approach

New approach (KF, James Maynard)

- We replace iterative treatments with direct arguments, deploying *all* of the Type-I and Type-II information at once.

- In principle, we can to determine $C(\gamma, \theta, \nu)$ exactly, by reducing the problem to a combinatorial optimization problem. This optimization problem is very complex and we have solved it only in some cases.

- We have a general method to construct *examples* giving upper bounds on $C(\gamma, \theta, \nu)$, and a general, non-iterative, method to obtain lower bounds on $C(\gamma, \theta, \nu)$.

- Our upper bound and lower bound methods are connected, being motivated by the duality principle in linear programming.

Initial reductions

$$\sum_{d\leqslant x^\gamma}\Big|\sum_{d|n} w_n\Big| \ll_A \frac{x}{(\log x)^A} \qquad \text{(Type-I bound)}$$

$$\Big|\sum_{x^\theta\leqslant m\leqslant x^{\nu+\theta}} \alpha_m \sum_{x/2<mn\leqslant x} \beta_n w_{mn}\Big| \ll_A \frac{x}{(\log x)^A} \qquad \text{(Type-II bound).}$$

Initial reductions

WLOG we may assume that

- $0 \leqslant \theta < 1/2$, since Type-II $\Leftrightarrow$ Type-II in $[x^{1-\theta-\nu}, x^{1-\theta}]$.
- $\gamma \notin [\theta, \theta+\nu) \cup [1-\theta-\nu, 1-\theta)$, since Type-II $\Rightarrow$ Type-I in the same range $[x^\theta, x^{\theta+\nu}]$;

A warm-up exercise

Initial reductions

WLOG we may assume that

(a) $0 \leqslant \theta < 1/2$, since Type-II $\Leftrightarrow$ Type-II in $[x^{1-\theta-\nu}, x^{1-\theta}]$.

(b) $\gamma \notin [\theta, \theta+\nu) \cup [1-\theta-\nu, 1-\theta)$, since Type-II $\Rightarrow$ Type-I in the same range $[x^{\theta}, x^{\theta+\nu}]$;

Theorem 0. Modulo the initial reductions, $C(\gamma, \theta, \nu) = 0$ if $\gamma < 1/2$. Moreover, there are sequences with $\sum a_p = 0$.

Proof. There is α with $\gamma < \alpha < 1/2$ and $\alpha \notin [\theta, \theta+\nu]$. Define

- $a_n = 0$ on primes;
- $a_n = K$ if $n = p_1 p_2$, $p_1 \sim x^{\alpha}$, $p_2 \sim x^{1-\alpha}$;
- $a_n = 1$ otherwise.

Type-II is trivial; Type-I nontrivial only for $d = 1$.
Choose $K = K(x)$ so that $\sum w_n = \sum (a_n - 1) = 0$.

Asymptotic formulas for primes

Theorem 1 [FM]. Assume reductions (a),(b), $1/2 \leqslant \gamma < 1$. Hypothesis $A(\gamma, \theta, \nu)$ holds if and only if both of the following hold:

(A_1) For every integer $n \geqslant M + 1$, $\exists\, a \in \mathbb{N}$ with $\frac{a}{n} \in [\theta, \theta + \nu]$, where

$$\frac{1}{M+1} < 1 - \gamma \leqslant \frac{1}{M}, \qquad M \in \mathbb{N};$$

(A_2) For some integer $h \geqslant 1$, $h(1-\gamma) \in [\theta, \theta+\nu] \cup [1-\theta-\nu, 1-\theta]$.

In particular, Hypothesis $A(\gamma, \theta, \nu)$ holds when $\gamma + \nu \geqslant 1$.

The case $\gamma = 1/2$

Theorem: Hypothesis $A(1/2, \theta, \nu)$ iff $\theta = 0$, $\nu \geqslant 1/3$.

Proof. The reductions imply $\theta + \nu < 1/2$.
Then $\theta = 0$ by (A_2): $h = 1$ not possible, so $h = 2$ must work
Then $\nu \geqslant \frac{1}{3}$ by (A_1), since $M = 2$.

Special case: $\gamma = 1/2$, $\theta = 0$

Theorem 2 [FM]. We have

- $C(1/2, 0, \nu) = 0$ for $\nu \leqslant 0.163$;
- $C(1/2, 0, \nu) > 0$ for $\nu \geqslant 0.1676$;
- an exact value of $C(1/2, 0, \nu)$ for $\nu \geqslant 1/5$, e.g.

$$C(1/2, 0, 1/5) = 0.362\ldots$$

DFI showed $C(1/2, 0, 1/5) \geqslant 0.23$.

Special case: $\gamma = 1 - \theta$, $\nu = 1 - 3\theta$

Theorem 3 [FM]. We have

- An exact value of $C(1-\theta, \theta, 1-3\theta)$ for $\frac{1}{4} \leqslant \theta \leqslant \frac{3}{10}$
- $C(0.7, 0.3, 0.1) \approx 0.84$; Harman showed $\geqslant 0.80$
- There is a $\theta_0 < 1/3$ so that $C(1-\theta, \theta, 1-3\theta) = 0$ for $\theta_0 \leqslant \theta < 1/3$. Moreover, there are examples with $a_p = 0$ for all p.

How much Type-II information is needed to detect primes?

Theorem 4 [FM]. (examples with no primes) For every $\gamma < 1$, there is a $\nu_0(\gamma) > 0$ so that whenever $0 \leqslant \nu \leqslant \nu_0(\gamma)$ we have $C(\gamma, \theta, \nu) = 0$. In fact, there are sequences with $a_p = 0$ for all primes p.

We use a function $\widetilde{\lambda}$, which is similar to the Liouville function:

- $\widetilde{\lambda}$ is completely multiplicative;
- $\widetilde{\lambda}$ is supported on integers with no prime factor $\leqslant x^\delta$, $\delta > 0$ fixed;
- $\widetilde{\lambda}$ satisfies the Type-I bounds up to x^γ, i.e.,

$$\sum_{d \leqslant x^\gamma} \Bigg| \sum_{\substack{x/2 < n \leqslant x \\ d | n}} \widetilde{\lambda}(n) \Bigg| \ll_A \frac{x}{\log^A x};$$

- $\widetilde{\lambda}(p) \approx -1$ for all primes $p \in (x^\delta, x]$.

Linnik's identity

Linnik: $$t(n) := \frac{\Lambda(n)}{\log n} = \sum_{j=1}^{\infty} \frac{(-1)^{j+1}}{j} \sum_{\substack{n=d_1\cdots d_j \\ d_i \geqslant 2\ (1\leqslant i\leqslant j)}} 1.$$

Proof. $\log \zeta(s) = \sum_{j=1}^{\infty} \frac{(-1)^{j+1}}{j} (\zeta(s)-1)^j.$

Truncated Linnik: $$t_y(n) := \sum_{j=1}^{\infty} \frac{(-1)^{j+1}}{j} \sum_{\substack{n=d_1\cdots d_j \\ 2\leqslant d_i \leqslant y\ (1\leqslant i\leqslant j)}} 1, \quad y = x^{1-\gamma}.$$

Truncated Linnik: $t_y(n) := \sum_{j=1}^{\infty} \frac{(-1)^{j+1}}{j} \sum_{\substack{n=d_1\cdots d_j \\ 2\leqslant d_i\leqslant y\ (1\leqslant i\leqslant j)}} 1, \quad y = x^{1-\gamma}$.

If n has a prime factor $> y$ then $t_y(n) = 0$.

$$\sum_p w_p \approx \sum_n w_n t(n)$$

$$\overset{(I)}{\approx} \sum_n w_n t_y(n)$$

$$\overset{(II)}{\approx} \sum_{n\in U} w_n t_y(n),$$

where $U = \{x/2 < n \leqslant x : \underbrace{y - \text{smooth}}_{\text{Type-I}}, \underbrace{\text{no divisor in } [x^\theta, x^{\theta+\nu}]}_{\text{Type-II}}\}$.

The asymptotic, revisited.

$$(*) \qquad \sum_p w_p \approx \sum_{n\in U} w_n t_y(n),$$

$$U = \{\tfrac{x}{2} < n \leqslant x : y-\text{smooth, no divisor in } [x^\theta, x^{\theta+\nu}]\}.$$

Main correspondence: $n = p_1 \cdots p_k \quad \leftrightarrow \quad \mathbf{v}_n = \left(\frac{\log p_1}{\log n}, \ldots, \frac{\log p_k}{\log n}\right)$

Vector analog of U:

$$\mathscr{U} = \left\{(x_1, \ldots, x_k) \in (0, 1-\gamma)^k : k \geqslant 1, \Sigma x_i = 1, \text{ no subsum in } [\theta, \theta+\nu]\right\}.$$

Theorem 1 reformulation. Hypothesis $A(\gamma, \theta, \nu)$ holds iff $\mathscr{U}$ is empty.

e.g., if $\mathbf{x} = (x_1, \ldots, x_k) \in (0, 1-\gamma)^k$, then the subsums of $\mathbf{x}$ have gaps less than $1-\gamma$. Thus, if $\gamma + \nu \geqslant 1$, then always one such subsum lies in $[\theta, \theta+\nu]$, hence $\mathscr{U}$ is empty.

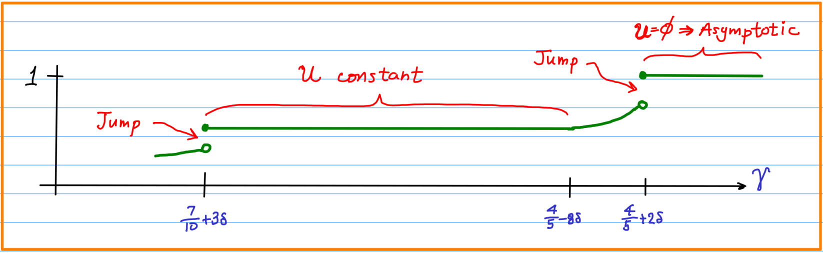
Analysis when $\mathscr{U}$ is nonempty

- Our analysis when $\mathscr{U}$ is nonempty depends on geometric and combinatorial properties of $\mathscr{U}$.
- We believe that $C(\gamma, \theta, \nu)$ is some function of the set $\mathscr{U}$.
- The vectors in $\mathscr{U}$ naturally break into two parts - those components $\leqslant \nu$ and those $> \nu$; the former cannot have a large sum.
- $\mathscr{U}$ nonempty means that either (A_1) fails or (A_2) fails. A state transition (from holding to failing) of (A_2) can lead to *sudden infusion* of a *big mass* in $\mathscr{U}$.

Main Conjecture: $C(\gamma, \theta, \nu) = \text{function}(\mathcal{U})$

Fix $[\theta, \theta+\nu] = [2/5 + 6\delta,\ 3/5 - 6\delta]$, $\delta > 0$ small, fixed

Plot $C(\gamma, \theta, \nu)$ with variable γ



Lower bounds on $C(\gamma, \theta, \nu)$ when $\mathscr{U}$ is nonempty

A restricted lower bound sieve

Let $\mathcal{N} = \{x/2 < n \leqslant x : n \neq \text{prime, no divisor in } [x^\theta, x^{\theta+\nu}]\}$.
Let $g : [1, x^\gamma] \to \mathbb{R}$ satisfy

- $g(1) = 1$;
- For all $n \in \mathcal{N}$, $\sum_{d|n} g(d) \leqslant 0$.

$$\begin{aligned}
\sum_{n\in\mathcal{N}} (1 \star g)(n) &\leqslant - \sum_{n\in\mathcal{N}} (1 \star g)(n) w_n \quad (\text{since } w_n \geqslant -1) \\
&= - \sum_{d\leqslant x^\gamma} g(d) \sum_{n\in\mathcal{N}, d|n} w_n \\
&\overset{(II)}{\approx} - \sum_{d\leqslant x^\gamma} g(d) \sum_{d|n, n\neq\text{prime}} w_n \\
&\overset{(I)}{\approx} \sum_{p} w_p.
\end{aligned}$$

Lower bounds on $C(\gamma, \theta, \nu)$ when $\mathscr{U}$ is nonempty

A restricted lower bound sieve

Let $\mathcal{N} = \{x/2 < n \leqslant x : n \neq \text{prime, no divisor in } [x^\theta, x^{\theta+\nu}]\}$.
Let $g : [1, x^\gamma] \to \mathbb{R}$ satisfy

- $g(1) = 1$;
- For all $n \in \mathcal{N}$, $\sum_{d|n} g(d) \leqslant 0$.

$$h = -(1 \star g) : \quad \sum_p w_p \approx \sum_{n \in \mathcal{N}} h(n) w_n \geqslant -\sum_{n \in \mathcal{N}} h(n).$$

Refinement of the method: replace $\mathcal{N}$ with smaller set $\mathcal{N}'$.

The inequality is best possible if there is Optimality if exists (w_n) with $w_n = -1$ for all $n \in \text{Supp}(h)$ (this idea comes from linear programming).

Finding $C(\frac{5}{7}, \frac{2}{7}, \frac{1}{7})$: lower bound. Vector version

$\mathcal{W} = \{(x_1, \ldots, x_k) : k \geqslant 2, \Sigma x_i = 1,\ x_i \geqslant \frac{1}{7}$ (all i), no subsum in $[\frac{2}{7}, \frac{3}{7}]\}$.

All components in $[\frac{1}{7}, \frac{2}{7}] \cup [\frac{3}{7}, \frac{4}{7}] \cup [\frac{5}{7}, \frac{6}{7}]$.

Define g by $g(\varnothing) = 1$ and

- $g(x) = -\mathbb{1}(x \leqslant \frac{1}{2})$;
- $g(x_1, x_2) = \mathbb{1}(x_1 + x_2 \leqslant \frac{1}{2})$.

Then $h = -(1 \star g)$ (meaning $h(x_1, \ldots, x_k) = -\sum_{A \subseteq [k]} g(x_i : i \in A)$) satisfies $h(\mathbf{x}) \geqslant 0$ on $\mathcal{W}$. Also, $h(\mathbf{x}) = 0$ except $h(x_1, x_2, x_3) = 2$ when $x_1, x_2 \in [\frac{1}{7}, \frac{2}{7}], x_3 \in [\frac{3}{7}, \frac{1}{2})$.

Get

$$C(\tfrac{5}{7}, \tfrac{2}{7}, \tfrac{1}{7}) \geqslant 1 - K,\ K = 2 \underset{\substack{u_1+u_2+u_3=1 \\ \frac{1}{7} \leqslant u_1 < u_2 \leqslant \frac{2}{7} \\ u_1+u_2 \geqslant 1/2}}{\int \cdots \int} \frac{1}{u_1 u_2 u_3} = 0.0785176 \ldots.$$

Constructions: $\theta = \frac{2}{7}, \gamma = \frac{5}{7}, \nu = \frac{1}{7}$

Set $w_n = f(\mathbf{v}_n)$, $f(\mathbf{v}) \geqslant -1$; $\forall k$, $f(v_1, \ldots, v_k)$ symmetric.

f supported on $\mathbf{v}$ with no subsum in $[\theta, \theta + \nu] \Rightarrow$ Type-II is trivial.

Type-I bounds $\Leftrightarrow$ f satisfies some integral identities.
It turns out that if we define f arbitrarily on vectors with components all $\leqslant 1 - \gamma$, Type-I determines f uniquely on all other vectors.

linear programming slackness: We desire $f(\mathbf{v}) = -1$ when $h(\mathbf{v}) \neq 0$.
For $\beta_1 + \beta_2 \geqslant 1/2 \geqslant \alpha \geqslant \frac{3}{7}$ we desire

$$f(\beta_1, \beta_2, \alpha) = -1 = -\alpha \int \cdots \int_{\substack{\alpha = \beta_3 + \beta_4 \\ \beta_3 < \beta_4}} \frac{f(\beta_1, \beta_2, \beta_3, \beta_4)}{\beta_3 \beta_4}$$

We find $f(\beta_1, \beta_2, \beta_3, \beta_4)$ by theory of Volterra integral equations. Get

$$C(\tfrac{5}{7}, \tfrac{2}{7}, \tfrac{1}{7}) \leqslant 1 - K.$$