On variants of the larger sieve

Ernest S. Croot III and Christian Elsholtz
ecroot@math.berkeley.edu
elsholtz@math.tu-clausthal.de

September 29, 2003

1 Introduction

The large sieve has its origins in the work of Linnik and Rényi. It was developed to deal with sequences that avoid a positive proportion of residue classes. It was later simplified by Roth, Bombieri, Davenport, Halberstam, Montgomery, Gallagher and many others. For a survey see Montgomery [12] and Bombieri [1].

It is known that Montgomery's large sieve [12] is a useful method when sifting sequences that avoid many residue classes modulo primes. For example, if a sequence $\mathcal{A} \subset [1, N]$ avoids $\omega(p) = \frac{p-1}{2}$ residue classes modulo the primes $p \leq \sqrt{N}$, then the large sieve gives the upper bound $\mathcal{A}(N) \ll \sqrt{N}$. Moreover the squares are the standard example to show that here the large sieve achieves the correct order of magnitude. But for sequences that avoid on average more than half of the residue classes it is preferable to use Gallagher's *larger* sieve [7]. Recently there emerged quite a few new applications of Gallagher's larger sieve so that it seemed worthwhile looking for variants of this sieve having some advantages over Gallagher's version. (We would like to point out that Gallagher had various contributions to the large sieve. In addition to the *larger* sieve that we use here, he gave a simplified version of the large sieve [6] and developed a sieve that allows to sift modulo powers of primes, [8].)

Let us state Montgomery's large sieve and Gallagher's larger sieve first. We then state and prove our new variants of it. In the final section we discuss the advantages or disadvantages of these variants.

Theorem 1 (Montgomery [12]). *Let $\mathcal{P}$ denote the set of primes. Let $\mathcal{A} \subset [1, N]$ denote a set of integers which lies outside $\omega(p)$ residue classes modulo the prime p. Here $\omega : \mathcal{P} \to \mathbb{N}$ with $0 \leq \omega(p) \leq p - 1$. Then the following bound on the counting function $\mathcal{A}(N)$ holds:*

$$\mathcal{A}(N) \leq \frac{N + Q^2 - 1}{L}, \text{ where } L = \sum_{q \leq Q} \mu^2(q) \prod_{p|q} \frac{\omega(p)}{p - \omega(p)}.$$

One usually takes $Q = \sqrt{N}$.

Theorem 2 (Gallagher's larger sieve, [7]). *Let $\mathcal{S}$ denote a set of primes or powers of primes such that $\mathcal{A} \subset [1, N]$ lies modulo all $q \in \mathcal{S}$ in at most $\nu(q)$ residue classes. Then the following bound holds, provided the denominator is positive:*

$$|\mathcal{A}| \leq \frac{-\log N + \sum_{q\in\mathcal{S}} \Lambda(q)}{-\log N + \sum_{q\in\mathcal{S}} \frac{\Lambda(q)}{\nu(p)}}.$$

Here Λ denotes the von Mangoldt function defined by

$$\Lambda(q) = \begin{cases} \log p, & \text{if } q = p^r \text{ with prime } p, \\ 0, & \text{otherwise.} \end{cases}$$

2 New variants of the larger sieve

Theorem 3 (Variant 1). *Let $\mathcal{S}$ denote a set of primes or powers of primes such that $\mathcal{A} \subset [1, N]$ lies modulo all $q \in \mathcal{S}$ in at most $\nu(q)$ residue classes. Suppose that $\sum_{q\in\mathcal{S}} \Lambda(q) < |\mathcal{A}|$. Then,*

$$|\mathcal{A}| \leq \frac{eN \exp\left(\sum_{q\in\mathcal{S}} \frac{\Lambda(q)}{q}\right)}{\exp\left(\sum_{q\in\mathcal{S}} \frac{\Lambda(q)}{\nu(q)}\right)}.$$

For most applications one chooses $\mathcal{S}$ to be the set of primes in some interval $[2, Q]$. Then $Q \sim \sum_{q\in\mathcal{S}} \Lambda(q) \approx C \exp\left(\sum_{q\in\mathcal{S}} \frac{\Lambda(q)}{q}\right)$.

Theorem 4 (Variant 2). *Let $\mathcal{S}$ denote a set of primes or powers of primes such that $\mathcal{A} \subset [1, N]$ lies modulo all $q \in \mathcal{S}$ in at most $\nu(q)$ residue classes. Let $G = \max_{q\in\mathcal{S}} \nu(q)$. Then the following inequality holds, provided the denominator is positive:*

$$|\mathcal{A}| \leq \frac{-G\log N + \sum_{q\in\mathcal{S}} \nu(q)\Lambda(q)}{-G\log N + \sum_{q\in\mathcal{S}} \Lambda(q)}.$$

The following two variants look odd for a sieve bound on $|\mathcal{A}|$ but they may still be useful.

Theorem 5 (Variant 3). *Let $\mathcal{S}$ denote a set of primes or powers of primes such that $\mathcal{A} \subset [1, N]$ lies modulo all $q \in \mathcal{S}$ in at most $\nu(q)$ residue classes. Suppose that $|\mathcal{A}| > \sum_{q\in\mathcal{S}} \Lambda(q)$. Then,*

$$1 + \log N \geq \sum_{q\in\mathcal{S}} \frac{\Lambda(q)}{\nu(q)}.$$

Theorem 6 (Variant 4). *Let $\mathcal{S}$ denote a set of primes or powers of primes such that $\mathcal{A} \subset [1, N]$ lies modulo all $q \in \mathcal{S}$ in at most $\nu(q)$ residue classes. Then the following inequality holds, provided the denominator is positive:*

$$|\mathcal{A}| \le \frac{-\log N + \sum_{q\in\mathcal{S}} \Lambda(q)}{-\log N + \frac{1}{|\mathcal{A}|^2}\sum_{q\in\mathcal{S}} \Lambda(q) \sum_{c=0}^{q-1} |a \in \mathcal{A} : a \equiv c \bmod q|^2}.$$

Proof of Variant 1. For any integer q let

$$B(q) := |\{(a, a') \in \mathcal{A}^2 : \ a \neq a', \ q|a - a'\}|$$

and

$$C(q) := \sum_{c=0}^{q-1} \big|\{a \in \mathcal{A} : \ a \equiv c \bmod q\}\big|^2.$$

Note that $B(q) = C(q) - |\mathcal{A}|$.

For any pair of integers $a, a' \in \mathcal{A}$, we have that

$$\sum_{q|a-a'} \Lambda(q) = \sum_{p^r|a-a'} \log p = \log|a - a'| < \log N;$$

and so,

$$\sum_{a\in\mathcal{A}} \sum_{\substack{a'\in\mathcal{A},\\ a'\neq a}} \sum_{q|a-a'} \Lambda(q) = \sum_{q\le N} B(q)\Lambda(q) < (|\mathcal{A}|^2 - |\mathcal{A}|)\log N. \tag{1}$$

$C(q)$ attains its minimum value when all the elements of $\mathcal{A}$ are as evenly distributed amongst the $\nu(q)$ progressions modulo q which $\mathcal{A}$ occupies. Thus,

$$C(q) \ge \ \nu(q)\left(\frac{|\mathcal{A}|}{\nu(q)}\right)^2 = \frac{|\mathcal{A}|^2}{\nu(q)}.$$

This gives

$$\sum_{q\in\mathcal{S}} B(q)\Lambda(q) \ge \ |\mathcal{A}|^2 \sum_{q\in\mathcal{S}} \frac{\Lambda(q)}{\nu(q)} \ - \ |\mathcal{A}| \sum_{q\in\mathcal{S}} \Lambda(q). \tag{2}$$

For $q \notin \mathcal{S}$ we do not assume that the set $\mathcal{A}$ avoids any residue class modulo q. Thus, for each q the smallest that $B(q)$ can be occurs if all the elements of $\mathcal{A}$ are equally distributed amongst the q progressions modulo q; so we use for $q < |\mathcal{A}|$ with $q \notin \mathcal{S}$,

$$B(q) = C(q) - |\mathcal{A}| > \frac{|\mathcal{A}|^2}{q} - |\mathcal{A}|.$$

Thus,

$$\begin{aligned}\sum_{q\le|\mathcal{A}|,\,q\notin\mathcal{S}} B(q)\Lambda(q) &\ge |\mathcal{A}|^2 \sum_{q\le|\mathcal{A}|,\,q\notin\mathcal{S}} \frac{\Lambda(q)}{q} - |\mathcal{A}| \sum_{q\le|\mathcal{A}|,q\notin\mathcal{S}} \Lambda(q) \\ &> |\mathcal{A}|^2 \left(\log|\mathcal{A}| - \sum_{q\in\mathcal{S}} \frac{\Lambda(q)}{q}\right) - |\mathcal{A}| \sum_{q\le|\mathcal{A}|,\,q\notin\mathcal{S}} \Lambda(q).\end{aligned}$$

Combining this with (1) and (2), we get

$$\begin{aligned}(|\mathcal{A}|^2-|\mathcal{A}|)\log N &> \sum_{q\le|\mathcal{A}|} B(q)\Lambda(q) \\ &= \sum_{q\le|\mathcal{A}|,\,q\in\mathcal{S}} B(q)\Lambda(q) + \sum_{q\le|\mathcal{A}|,\,q\notin\mathcal{S}} B(q)\Lambda(q) \\ &= |\mathcal{A}|^2 \sum_{q\le|\mathcal{A}|,\,q\in\mathcal{S}} \frac{\Lambda(q)}{\nu(q)} - |\mathcal{A}| \sum_{q\le|\mathcal{A}|,\,q\in\mathcal{S}} \Lambda(q) \\ &\quad + |\mathcal{A}|^2 \left(\log|\mathcal{A}| - \sum_{q\le|\mathcal{A}|,\,q\in\mathcal{S}} \frac{\Lambda(q)}{q}\right) - |\mathcal{A}| \sum_{q\le|\mathcal{A}|,\,q\notin\mathcal{S}} \Lambda(q).\end{aligned}$$

Dividing through by $|\mathcal{A}|^2$, and rearranging terms gives

$$\log|\mathcal{A}| \le \log N + \sum_{q\in\mathcal{S}} \frac{\Lambda(q)}{q} - \sum_{q\in\mathcal{S}} \frac{\Lambda(q)}{\nu(q)} + 1$$

which implies that

$$|\mathcal{A}| \le \frac{eN\exp\left(\sum_{q\in\mathcal{S}} \frac{\Lambda(q)}{q}\right)}{\exp\left(\sum_{q\in\mathcal{S}} \frac{\Lambda(q)}{\nu(q)}\right)}.$$

□

Proof of Gallagher's larger sieve and of Variant 4. ¿From (1) and (2) we can also easily arrive at Gallagher's original version:

$$(|\mathcal{A}|^2-|\mathcal{A}|)\log N > \sum_{q\in\mathcal{S}} B(q)\Lambda(q) > |\mathcal{A}|^2 \sum_{q\in\mathcal{S}} \frac{\Lambda(q)}{\nu(q)} - |\mathcal{A}| \sum_{q\in\mathcal{S}} \Lambda(q).$$

Dividing through by $|\mathcal{A}|$ proves

$$|\mathcal{A}| \le \frac{-\log N + \sum_{q\in\mathcal{S}} \Lambda(q)}{-\log N + \sum_{q\in\mathcal{S}} \frac{\Lambda(q)}{\nu(q)}}.$$

If we work with $C(q)$ instead of $C(q) \ge \frac{|\mathcal{A}|}{\nu(q)}$, then the same line of argument proves variant 4. □

Proof of variant 2. The proof closely follows Gallagher. Let $A(h,q)$ denote the number of elements of the set $\mathcal{A}$ with $a \equiv h \bmod q$. Then by the Cauchy-Schwarz inequality

$$|\mathcal{A}|^2 = \left(\sum_{h=1}^{q} A(h,q)\right)^2 \leq \nu(q) \sum_{h=1}^{q} (A(h,q))^2,$$

since $A(h,q) = 0$ for all but $\nu(q)$ values of h. Summing over $\mathcal{S}$ we find that

$$\begin{aligned} |\mathcal{A}|^2 \sum_{q\in\mathcal{S}} \Lambda(q) &= \sum_{q\in\mathcal{S}} \Lambda(q)\nu(q) \sum_{a\equiv a' \bmod q} 1 \\ &= \sum_{|d|\leq N} \sum_{a-a'=d} \sum_{q|d,\, q\in\mathcal{S}} \Lambda(q)\nu(q) \\ &< |\mathcal{A}| \sum_{q\in\mathcal{S}} \Lambda(q)\nu(q) + G\left(|\mathcal{A}|^2 - |\mathcal{A}|\right) \log N, \end{aligned}$$

since for $d \neq 0$ one has that $\sum_{q|d} \Lambda(q) = \log |d| < \log N$. This implies that

$$|\mathcal{A}|^2 \left(-G \log N + \sum_{q\in\mathcal{S}} \Lambda(q)\right) < |\mathcal{A}| \left(-G \log N + \sum_{q\in\mathcal{S}} \Lambda(q)\nu(q)\right),$$

which proves the theorem. □

Proof of Variant 3. This is an immediate corollary of Gallagher's original version: Suppose that

$$\sum_{q\in\mathcal{S}} \frac{\Lambda(q)}{\nu(q)} > 1 + \log N.$$

Then

$$|\mathcal{A}| \leq \frac{-\log N + \sum_{q\in\mathcal{S}} \Lambda(q)}{-\log N + \sum_{q\in\mathcal{S}} \frac{\Lambda(q)}{\nu(q)}} \leq \frac{\sum_{q\in\mathcal{S}} \Lambda(q)}{1},$$

which contradicts the assumption $|\mathcal{A}| > \sum_{q\in\mathcal{S}} \Lambda(q)$. The same holds if one takes

$$\frac{1}{|\mathcal{A}|^2} \sum_{p\leq Q} (\log p) \sum_{c=0}^{p-1} |\{a \in \mathcal{A} :\ a \equiv c \bmod p\}|^2$$

instead of $\sum_{p\leq Q} \frac{\log p}{\nu(p)}$, by the intermediate steps of the proof of Gallagher's sieve. □

3 Discussion

We now discuss the advantages of these variants of the larger sieve. In many standard applications the original version and these variants are of the same

strength. Let us consider a sieve problem with $\omega(p) = p - \nu(p) \approx cp$, where c is a constant with $0 < c < 1$. Of course, $\omega(p)$ and $\nu(p)$ are integers, so that usually one would have for example $\omega(p) = \frac{p+1}{2}$, if $c = \frac{1}{2}$, but let us put for simplicity $\omega(p) = p - \nu(p) \geq cp$. Wirsing's theorem on sums of multiplicative functions (Wirsing [18]) allows to estimate the denominator

$$L = \sum_{q \leq Q} \mu^2(q) \prod_{p|q} \frac{\omega(p)}{p - \omega(p)}$$

of Montgomery's sieve:

$$L \gg Q(\log Q)^{\frac{c}{1-c}-1}.$$

Choosing $Q = \sqrt{N}$ gives

$$|\mathcal{A}| \ll \sqrt{N}(\log N)^{\frac{1-2c}{1-c}}.$$

Using Gallagher's larger sieve, we find that for some sufficiently large constant C the choice $\mathcal{S} = \{p \leq Q = CN^{1-c}\}$ gives

$$|\mathcal{A}| \ll N^{1-c}.$$

This shows that for $\omega(p) < \frac{p}{2}$ on average one should use Montgomery's sieve; for $c = \frac{1}{2}$ both sieves are of the same strength, and for $\omega(p) > \frac{p}{2}$ Gallagher's sieve is the preferable choice.

Moreover, there are simple examples for which Gallagher's sieve is sharp. Let $\mathcal{A} = \{n^2 : n \leq N^{1/2}\}$ be the sequence of squares below N. These lie modulo primes in $\nu(p) = \frac{p+1}{2}$ residue classes. Montgomery's sieve, Gallagher's sieve and Variant 1 give the correct upper bound $O(\sqrt{N})$ which of course is best possible, apart from the O-constant.

But for the case of cubes, $\mathcal{A} = \{n^3 : n \leq N^{1/3}\}$, Gallagher's sieve is not optimal. Here one has that $\nu(p) = \begin{cases} 2 & \text{if } p = 2, 3 \\ p & \text{if } p \equiv -1 \bmod 6 \\ \frac{p+2}{3} & \text{if } p \equiv \quad 1 \bmod 6. \end{cases}$

Unfortunately, Gallagher's sieve is weak if $\nu(p)$ oscillates like this. For an application of Gallagher's sieve one has the choice of the set $\mathcal{S}$. In the cases above one considers whether it is better that the set $\mathcal{S}$ contains the primes $p \equiv -1 \bmod 6$ or not. In the first case one has

$$|\mathcal{A}| \ll \frac{-\log N + Q + O(1)}{-\log N + \frac{\log Q}{2} + \frac{3\log Q}{2} + O(1)} \ll \frac{Q}{-\log N + 2\log Q + O(1)} \ll N^{\frac{1}{2}},$$

with $Q = CN^{\frac{1}{2}}$. In the second case one has that

$$|\mathcal{A}| \ll \frac{-\log N + \frac{Q}{2} + O(1)}{-\log N + \frac{3\log Q}{2} + O(1)} \ll N^{\frac{2}{3}},$$

with $Q = CN^{\frac{2}{3}}$. Here, the fact that primes without any sifting effect were omitted even weakens the result.

The situation is different in the case of variant 1. Here we choose $\mathcal{S} = \{p \leq Q : p \equiv 1 \bmod 6\}$.

$$|\mathcal{A}| \ll \frac{N \exp\left(\sum_{q\in\mathcal{S}} \frac{\Lambda(q)}{q}\right)}{\exp\left(\sum_{q\in\mathcal{S}} \frac{\Lambda(q)}{\nu(q)}\right)} = \frac{N \exp\left(\frac{1}{2}\log Q\right)}{\exp\left(\frac{3}{2}\log Q\right)} = \frac{NQ^{\frac{1}{2}}}{Q^{\frac{3}{2}}} = \frac{N}{Q}.$$

In making the optimal choice of Q we have to respect $\sum_{q\in\mathcal{S}} \Lambda(q) < |\mathcal{A}|$ (or $Q \ll |\mathcal{A}|$) so that

$$|\mathcal{A}| \ll N^{\frac{1}{2}},$$

with $Q = CN^{\frac{1}{2}}$. Interesting enough, the other choice $\mathcal{S} = \{p \leq Q\}$ leads to the very same result. It is an advantage of variant 1 that an additional prime with $\nu(p) = p$ does not influence the result since here a factor of $\exp\left(\frac{\Lambda(q)}{q}\right)$ occurs in the numerator and denominator, so that these factors cancel each other. So, in the case of variant 1 the choice of $\mathcal{S}$ is easier here. It is only necessary to choose the optimal Q.

If $\nu(p) = p^\alpha$ (with $0 < \alpha < 1$), then Montgomery's sieve gives $|\mathcal{A}| \ll N^{\frac{\alpha}{2}}$, whereas Gallagher's sieve with $\mathcal{S} = \{p \leq Q = C(\log N)^{\frac{1}{1-\alpha}}\}$ shows that $|\mathcal{A}| \ll (\log N)^{\frac{\alpha}{1-\alpha}}$. Variant 1 cannot handle this case. Moreover, if $|\mathcal{A}|$ is very small, then $|\mathcal{A}|^2 - |\mathcal{A}| < |\mathcal{A}|^2$ in equality (1) weakens the result.

Variant 2 cannot handle the above cases with $\omega(p) \approx cp$ since one needs that $G \leq \frac{Q}{\log N}$. But it can deal with problems, that use small values $\nu(p)$. For $\nu(p) = p^\alpha$ we also find with $Q = C(\log N)^{\frac{1}{1-\alpha}}$ that $|\mathcal{A}| \ll (\log N)^{\frac{\alpha}{1-\alpha}}$.

Even though Gallagher's original version might be stronger than variant 2, for many applications variant 2 will completely suffice. In some applications it may be easier to have control over $\sum_p \nu(p)\log p$ rather than $\sum_p \frac{\log p}{\nu(p)}$. Moreover, the term $\sum_p \nu(p)\log p$ is more familiar in applications of the small sieve.

References

[1] Bombieri, E.: Le grand crible dans la théorie analytique des nombres. Second edition. Astérisque No. 18 (1987).

[2] Brüdern, J.: Einführung in die analytische Zahlentheorie. Springer, Berlin, 1995.

[3] Croot, E., Elsholtz, C.: Work in preparation that is related to the ternary case of the inverse Goldbach problem.

[4] Davenport, H.: Multiplicative number theory. Second edition. Revised by H. L. Montgomery. Graduate Texts in Mathematics, 74. Springer-Verlag, New York-Berlin, 1980.

[5] Erdős, P.: Some Recent Advances and Current Problems in Number Theory. In: Lectures on Modern Mathematics, 1965, 196–244, ed. Saaty, T.L., Wiley, Ney York.

[6] Gallagher, P.X.: The large sieve. Mathematika 14 (1967), 14–20.

[7] Gallagher, P.X.: A larger sieve. Acta Arith. 18 (1971), 77–81.

[8] Gallagher, P.X.: Sieving by prime powers. Acta Arith. 24 (1973/74), 491–497.

[9] Halberstam, H.; Richert, H.-E.: Sieve methods. London Mathematical Society Monographs, No. 4, Academic Press, London, 1974.

[10] Montgomery, H.L.: A note on the large sieve. J. London Math. Soc. 43 (1968), 93–98.

[11] Montgomery, H.L.: Topics in multiplicative number theory. Lecture Notes in Mathematics, Vol. 227. Springer, Berlin-New York, 1971.

[12] Montgomery, H.L.: The Analytic Principle of the Large Sieve. Bull. Amer. Math. Soc. 84 (1978), 547–567.

[13] Montgomery, H.L.; Vaughan, R.C.: The large sieve. Mathematika 20 (1973), 119–134.

[14] Motohashi, Y. Lectures on sieve methods and prime number theory. Tata Institute Lecture Notes, 72. Springer, Berlin, 1983.

[15] Richert, E.: Lectures on sieve methods. Tata Institute Lecture Notes, 55, Bombay (1976).

[16] Sárközy, A.: A note on the arithmetic form of the large sieve. Studia Sci. Math. Hungar. 27 (1992), 83–95.

[17] Selberg, A.: Remarks on multiplicative functions. Number theory day (Proc. Conf., Rockefeller Univ., New York, 1976), 232–241. Lecture Notes in Math., Vol. 626, Springer, Berlin, 1977.

[18] Wirsing, E.: Das asymptotische Verhalten von Summen über multiplikative Funktionen. Math. Ann. 143 (1961), 75–102.