THE ARITHMETIC FUNCTION $\Omega(n)$ AND BOUNDS ON SQUARE DEPENDENCE OF INTEGERS

DENIS XAVIER CHARLES

ABSTRACT. We show that if we pick $\log^d N$ integers in the interval $[1 \cdots N]$ then the probability that there is a subset of them whose product yields a perfect square is $\exp\left(-\frac{c \log N}{\log\log N}\right)$ for any $c < \frac{1}{2d}$. The methods used to prove these results are elementary.

1. Introduction

A lot is known about the functions $\Omega(n)$ and $\omega(n)$ defined by

$$\Omega(n) = \sum_{p^\nu \backslash\backslash n} \nu$$

$$\omega(n) = \sum_{p \backslash n} 1.$$

It follows from the prime number theorem that

$$\sum_{n \le x} \omega(n) = x \log\log x + O\left(\frac{x}{\log x}\right)$$

$$\sum_{n \le x} \Omega(n) = x \log\log x + O\left(\frac{x}{\log x}\right).$$

This shows that the average value of $\Omega(n)$ is $\log\log x$. The Hardy-Ramanujan theorem [HR17] shows that this holds rather strongly, more precisely:

$$\left|\{n \ : \ n \le x, |\Omega(n) - \log\log n| > (\log\log n)^{\frac{1}{2}+\epsilon}\}\right| = o(x), \text{ for } \epsilon > 0$$

as $x \to \infty$. Turán [Tu34] gave an effective version of this theorem which states that: If $\xi(N)$ is a function such that $\lim_{N\to\infty} \xi(N) \to \infty$ then

$$\left|\{n \le N \ : \ |\Omega(n) - \log\log N| > \xi(N)\sqrt{\log\log N}\}\right| \ll \frac{N}{\xi(N)^2}.$$

This result also holds for the function $\omega(n)$. The conclusion of the theorem can be substantially strengthened if $\xi(N)$ is close to $\log N$. In particular Erdős and Nicolas [EN81] showed that

$$\sum_{n \le x, \ \omega(n) > \frac{c \log x}{\log\log x}} 1 = x^{1-c+o(1)} \text{ for } 0 < c < 1.$$

Erdős and Sárközy [ES80] proved a uniform upper bound on the analogous sum for the function $\Omega(n)$ in particular they showed:

Theorem 1.1. *For $k \ge 1$ the following bound holds uniformly:*

$$\sum_{n \le x, \ \Omega(n) > k} 1 < x \exp\Big(-k + O(\log k)\Big).$$

The upper bound is not very far from the truth for large k (see [Ni84]).

As an application of this bound we investigate an interesting question which comes up in constructing rational extensions of $\mathbb{Q}$ of high degree by adjoining square roots of integers [BC01]. Let N be a large integer, $d > 0$ be fixed, and let $n = \lfloor \log^d N \rfloor$. Suppose we pick n integers uniformly and independently at random from the interval $[1 \cdots N]$ we are interested in the probability that the product of a subset of these numbers yields a perfect square. We prove a nearly exponential upper bound on this probability. In [BC01] (Theorem 3) a bound of the form $\exp\left(-\frac{1}{\sqrt{2}}\sqrt{\log N \log\log N}\right)$ is given. The same question was investigated in [Po96] where it is shown that if $n = \exp\left(\sqrt{2\log N \log\log N}\right)$ integers are picked at random then the probability that they are square dependent is $1 - o(1)$.

2. Square dependence of random integers

Theorem 2.1. *Let $N > 0$ be an integer, $d > 0$ be a fixed real number and $n = \lceil \log^d N \rceil$. Suppose $q_1, \cdots, q_n$ are integers picked uniformly and independently at random from the interval $[1 \cdots N]$ the probability that $\exists S \subseteq \{1, \cdots, n\}$ such that $\prod_{i \in S} q_i = r^2$ is at most*

$$\frac{n \exp\big(cd \log N\big)}{\sqrt{N}} + n \exp\left\{-\left(\frac{c \log N}{\log\log N}\right)\right\}$$

for any constant $c > 0$. Thus the probability of square dependence is at most

$$\exp\left\{-\left(\frac{c\log N}{\log\log N}\right) + O(\log\log N)\right\}.$$

Proof : Let A be the event that among the n integers $\exists i \ : \ \Omega(q_i) > \frac{c \log N}{\log\log N}$, by Theorem 1.1 this happens with probability at most

$$n \exp\left\{-\left(\frac{c\log N}{\log\log N}\right) + O(\log\log N)\right\}.$$

We will assume that A does not occur in which case we have $\forall i \ : \ \Omega(q_i) < \frac{c\log N}{\log\log N}$.
Let E be the event that there is a square dependence among the n integers q_i we have:

$$\begin{aligned}
\Pr[E] &= \sum_{S \subseteq \{1,\cdots,n\}} \Pr\left[\prod_{i\in S} q_i = t^2\right] \\
&\leq \sum_{S\subseteq\{1,\cdots,n\}, |S|=m} \frac{\max\{r_m(h) \ : \ h \leq N^m, h \text{ is } N\text{-smooth } \}\psi(\sqrt{N^m}, N)}{N^m}
\end{aligned}$$

where $r_m(h)$ counts the number of ways (including order) that h can be written as a product of m different numbers. This is because every number $h \leq N^m$ which is N-smooth occurs $r_m(h)$ times when we list all possible guesses for $\prod_i q_i$, and of these $\Psi(\sqrt{N^m}, N)$ are squares.
Now conditional on the assumption that the event A did *not* occur, we can upper bound $r_m(h)$ since every number q_i has less than $\frac{c\log N}{\log\log N}$ prime factors we have:

$$r_m(h) \leq m^{\frac{cm \log N}{\log\log N}}.$$

Substituting in our expression for $\Pr[E]$ we have conditioned on the event $\neg A$:

$$\begin{aligned}
\Pr[E] &\le \sum_{1\le m\le n} \binom{n}{m} \frac{m^{\frac{cm\log N}{\log\log N}}}{\sqrt{N^m}} \\
&\le \sum_{1\le m\le n} \binom{n}{m} \left(\frac{n^{\frac{c\log N}{\log\log N}}}{\sqrt{N}}\right)^m \\
&= \left(1+\frac{n^{\frac{c\log N}{\log\log N}}}{\sqrt{N}}\right)^n - 1 \\
&\approx n\left(\frac{n^{\frac{c\log N}{\log\log N}}}{\sqrt{N}}\right) \\
&= \exp\left\{cd\log N - \frac{1}{2}\log N + O(\log\log N)\right\}.
\end{aligned}$$

Since d is a fixed constant and c is arbitrary, we can choose c small enough to make this essentially $\exp\{-(\frac{1}{2}+\delta)\log N\}$. Now the theorem follows because

$$\Pr[E] \le \exp\left\{cd\log N - \frac{1}{2}\log N + O(\log\log N)\right\} + \Pr[A].$$

$\square$

Remark 2.2. If we pick $n = \log^d N$ integers where now $d = \log^\epsilon N$ is variable $0 < \epsilon < \frac{1}{2}$ then the above proof yields an upper bound of

$$n\exp\left\{-\left(c\frac{\log N}{\log\log N}\right)^{1-\epsilon}\right\}$$

for the probability of square dependence. Clearly when $n \approx \exp(\sqrt{N})$ the upper bound diverges, and from [Po96] we know that it approaches 1.

References

[BC01] Bach, Eric; Cai, Jin-Yi, *On testing for zero polynomials by a set of points with bounded precision*, Proceedings of the 7th Annual International Conference on Computing and Combinatorics (COCOON 2001), *To Appear.*

[EN81] Erdős, P.; Nicolas, J.-L., *Sur la fonction: nombre de facteurs premiers de N*, Enseign. Math., **27**, 3-27, 1981.

[ES80] Erdős, P.; Sárközy, A., *On the number of prime factors in integers.* Acta Sci. Math. (Szeged), **42**, no. 3-4, 237-246, 1980.

[HR17] Hardy G. H.; Ramanujan S., *The normal number of prime factors of a number n*, Quart. J. Math., **48**, 76-92, 1917.

[Ni84] Nicolas, J.-L., *Sur la distribution des nombres entiers ayant une quantité fixée de nombres premiers*, Acta Arith., **44**, 191-200, 1984.

[Po96] Pomerance, C., *Multiplicative independence for random integers*, Analytic Number Theory, Proceedings of a Conference in Honor of Heini Halberstam, Vol 2, Progr. Math. 139, 703-711, Birkhäuser, 1996.

[Tu34] Turán, P., *On a theorem of Hardy and Ramanujan*, J. London Math. Soc. **9**, 274-276, 1934.