Counting arithmetic formulas

COUNTING ARITHMETIC FORMULAS

EDINAH K. GNANG, MAKSYM RADZIWIŁŁ, AND CARLO SANNA

Abstract. An *arithmetic formula* is an expression involving only the constant 1, and the binary operations of addition and multiplication, with multiplication by 1 not allowed. We obtain an asymptotic formula for the number of arithmetic formulas evaluating to n as n goes to infinity, solving a conjecture of E. K. Gnang and D. Zeilberger. We give also an asymptotic formula for the number of arithmetic formulas evaluating to n and using exactly k multiplications. Finally we analyze three specific encodings for producing arithmetic formulas. For almost all integers n, we compare the lengths of the arithmetic formulas for n that each encoding produces with the length of the shortest formula for n (which we estimate from below). We briefly discuss the time-space tradeoff offered by each.

1. Introduction

1.1. **Counting arithmetic formulas.** An *arithmetic formula* is an expression involving only the constant 1 and the binary operations of addition and multiplication, with multiplication by 1 not allowed. For example, 4 has exactly 6 arithmetic formulas,

$$1+(1+(1+1)),\quad 1+((1+1)+1),\quad (1+(1+1))+1,$$
$$((1+1)+1)+1,\quad (1+1)+(1+1),\quad (1+1)\times(1+1)$$

A systematic study of arithmetic formulas was initiated by Patrick, Gnang and Zeilberger [6] [11]. The number of arithmetic formulas evaluating to n using only addition corresponds to the number of ways one can place a sequence of parentheses in the sum $1+1+\cdots+1$, containing n times the number 1. It is well known that there is C_{n-1} ways of doing this, where C_n is the Catalan number [14, Ch. 6, Corollary 6.2.3],

$$C_m := \frac{1}{m+1}\binom{2m}{m} \sim \frac{1}{\sqrt{\pi}}\frac{4^m}{m^{3/2}} \text{ as } m\to\infty.$$

2010 *Mathematics Subject Classification.* Primary: 05A16, 11A67, 11B75. Secondary: 11A99, 11Y16.

Key words and phrases. Arithmetic formulas, arithmetic expressions, integer encodings, asymptotic formulas.

The first and second authors were partially supported by NSF grant DMS-1128155.

On the other hand, the number of arithmetic formulas for n using addition and multiplication is more mysterious. It was conjectured by Gnang and Zeilberger [6] that there is an asymptotic of the form $c \cdot \rho^n \cdot n^{-3/2}$, with two constants $c > 0$ and $\rho > 4$ (with ρ most likely a transcendental number). Our first result is a proof of this conjecture. Let $f(n)$ be the number of arithmetic formulas for n [8].

Theorem 1.1. *There exists constants $c > 0$ and $\rho > 4$ such that*

$$f(n) \sim \frac{c\rho^n}{n^{3/2}},$$

as $n \to \infty$. In fact,

$$c = 0.145691854699979\ldots$$
$$\rho = 4.076561785276046\ldots$$

In addition our method gives an asymptotic expansion for $f(n)$. We refer the reader to the proof of Theorem 1.1 for more details. Theorem 1.1 is also motivated by some relations with the factoring problem, see Section 1.2.

We obtain a completely explicit characterization of the constant ρ. It is determined as $\rho := 1/\xi$ where $0 < \xi < 1/4$ is the smallest positive solution to the equation $\widetilde{F}(\xi) = 1/4$, with

$$\widetilde{F}(z) := z + \sum_{d=2}^{\infty} f(d)(F(z^d) - z^d) \text{ and } F(z) := \sum_{n=1}^{\infty} f(n) z^n.$$

The proof of Theorem 1.1 can be easily adapted to count the number of arithmetic formulas in which also exponentiation is allowed (and such that 1 is never an argument of exponentiation). We call such formulas *arithmetic exponential formulas*. An analogue of Theorem 1.1 holds for counting arithmetic exponential formulas but with a larger $\rho = 4.13073529514801\ldots$.

The proof of Theorem 1.1 depends on generating functions and complex analysis. A natural idea is to produce an elementary proof of Theorem 1.1 by first asking for the number $f_k(n)$ of arithmetic formulas for n using only addition and exactly k multiplication operations. This we achieve in the theorem below.

Theorem 1.2. *For all integers $k \geq 0$, we have*

$$f_k(n) \sim \frac{\sigma^k}{4\sqrt{\pi}\, k!}\, 4^n n^{k-3/2},$$

as $n \to +\infty$, where

$$\sigma := \sum_{m=1}^{\infty} \frac{1}{4^{m-1}} \sum_{\substack{d \mid m \\ 1<d<m}} f_0(d) f_0(m/d).$$

One would like to sum the above formula over all k, assuming sufficient uniformity, and claim that ρ in Theorem 1.1 is equal to $4e^\sigma$. However $\rho < 4e^\sigma$ and therefore for large k there occurs a significant break in the uniformity of Theorem 1.2. This is expected since, for example, $f_k(n) = 0$ for $k > \log n/\log 2$.

If we consider two arithmetic formulas to be *equivalent* if one can be obtained from the other through a repeated application of the commutative and associative properties (hence, for example,

$$(1+1)\times((1+1)+1),\quad (1+1)\times(1+(1+1)),\quad (1+(1+1))\times(1+1),$$

are all equivalent arithmetic formulas for 6) then the problem of counting arithmetic formulas becomes much different. Precisely, Sanna [13] proved that the number of inequivalent arithmetic formulas for n is $\exp(\beta n + O(\sqrt{n}))$, where $\beta := \log(24)/24$, as $n \to +\infty$.

1.2. **Factoring.** One motivation for our work comes from factoring. For a given positive integer n one would like to understand the following graph G_n: The nodes of the graph G_n correspond to the various arithmetic formulas for n and an edge is placed between two nodes if one can pass from one formula to the other by using only one operation of either associativity, distributivity or commutativity.

One can depict arithmetic formulas as full binary trees, so that the graph G_n is a graph whose vertices correspond to certain special full binary trees. Various arithmetic algorithms such as integer factoring algorithms can be depicted as walks starting from some particular vertex of the graph G_n (say the one corresponding to the recursive Horner encoding, see below for a definition of this encoding) and terminating at a vertex associated with a formula encoding of n whose corresponding tree is rooted at a multiplication node.

A vertex v of G_n corresponding to an arithmetic formula using only additions has the largest possible degree in G_n, precisely $\deg(v) = f_0(n) - 1$. So in order to understand the connectivity of the graph G_n we compare $f_0(n) - 1$ to the order of the graph G_n. The order of the graph G_n corresponds to the number $f(n)$ of representations of n using only 1's and operation of addition and multiplication. Therefore as an immediate consequence of Theorem 1.1 we obtain the following

Corollary 1.3. *Let $C = \rho/4 = 1.019140446319\ldots$. Then, for some constant $c > 0$, as $n \to \infty$,*

$$\max_{v\in G_n} \deg(v) \sim c \cdot \frac{|G_n|}{C^n}.$$

Of particular interest in the graph G_n are formulas which are short because they minimize the space needed for encoding n.

1.3. **Shortest encodings.** We will discuss three special monotone formula encoding schemes called the *first canonical form* or Goodstein encoding [7], the *second canonical form* [6] and the *Horner encoding*. We will focus on *arithmetic exponential formulas* (that is, arithmetic formulas allowing exponentiation), because a lower bound for the lengths of such formulas is also a lower bound for the length of the shortest arithmetic formula with only addition and multiplication allowed.

The Goodstein encoding consists in writing the binary expansion of an integer $n = \sum_i 2^{a_i}$ and recursively writing down the binary expansion for each integer a_i until we obtain a representation of n as formula involving only 2 and 1's, the final step will consist in replacing each 2 by $1+1$ thereby obtaining a monotone formula encoding of n which only uses additions ($+$) and exponentiations ($\wedge$) gates and has input 1. For example the Goodstein encoding for the number 31 corresponds to

$$31 = (1+1)^{\left((1+1)^{(1+1)}\right)} + \left((1+1)^{((1+1)+1)} + \left((1+1)^{(1+1)} + ((1+1)+1)\right)\right).$$

By contrast to the Goodstein encoding, the second canonical form of an integer n is slightly more intricate. We start by writing down the prime factorization $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ and subsequently we express each prime as $1 + (p_i - 1)$. Finally we recursively apply this scheme to every $(p_i - 1)$ and every exponent α_i. Thus we obtain a monotone formula encoding for n which uses a combination of addition ($+$), multiplication ($\times$), and exponentiation gates ($\wedge$) and input restricted to 1. As an example we express the second canonical form associated to 2430

$$2430 = \left((1+1) \times (1+(1+1))^{\left(1+(1+1)^{(1+1)}\right)}\right) \times \left(1 + (1+1)^{(1+1)}\right).$$

In [6] it was observed that for most integers n the second canonical form is smaller than the Goodstein encoding. Our next result provides some theoretical validation for this empirical observations. Let $S_{\text{short}}(n)$ denote the length of the shortest monotone formula encoding of n, let $S_{\text{FCF}}(n)$ and $S_{\text{SCF}}(n)$ denote respectively the size of the first and second canonical form encoding of n. The special interest in formula sizes stems from the connection between circuit complexity and integers encoding schemes. Building on a sequence of constructions by Cheng [2] and Koiran [10], Burgisser [1] showed that if the sequence of integers $\{n!\}_{n\in\mathbf{N}}$ is hard to compute, then any algebraic circuits for computing the permanent of a sequence $\{M_n \in \mathbf{Z}^{n\times n}\}_{n\in\mathbf{N}}$ of matrices using addition ($+$) and multiplication ($\times$) gates with input restricted to $\{-1, 1\}$, must have superpolynomial size.
Also related results (for example, for circuits) have been obtained in [3] and [4]. We refer the reader to the references there-in for further information on this topic.

Theorem 1.4. *For almost all positive integers n we have*

$$S_{\text{short}}(n) \geq \frac{\log n}{\log 4}.$$

Precisely, given $\varepsilon > 0$, the number of integers $n \le x$ such that

$$S_{\text{short}}(n) \le (1-\varepsilon)\frac{\log n}{\log 4}$$

is $O(x^{1-\varepsilon})$, as $x \to +\infty$.

Theorem 1.5. *Given $\varepsilon > 0$, for almost all positive integers n,*

$$S_{\text{FCF}}(n) \ge \left(\frac{1}{4(\log 2)^2} - \varepsilon\right) \cdot \log n \log\log n.$$

Theorem 1.6. *For all integers $n \ge 2$, we have*

$$S_{\text{SCF}}(n) \le 6\,\frac{\log n}{\log 2}.$$

In conclusion, while the first canonical form is rapid it provides formulas of sub-optimal length compared to the shortest formula. The second canonical form is more computationally intensive but gives rise to shorter formulas, of quality comparable to the shortest formula. The drawback is computational complexity, and this drawback is alleviated by the Horner encoding, which is obtained from a recursive factoring of the Goodstein encoding. We write below the recursive Horner encoding of the integer 53376

$$53376 = \Big(\big(((1+1)+1)(1+1)^{(1+1)}+1\big)(1+1)^{(1+1)^{(1+1)}+1}+1\Big)(1+1)^{((1+1)+1)(1+1)+1}$$

The properties of the recursive Horner encoding are similar to the second canonical form. For example we obtain essentially the same results for $S_{\text{Hor}}(n)$ as for $S_{\text{SCF}}(n)$. We suspect however that the second canonical form gives on average slightly shorter formulas than the Horner encoding. We think it is an interesting question but we did not pursue it. Finally we note that one can efficiently recover recursive Horner encodings from Goodstein encodings.

Notation. Hereafter, $\mathbf{N}$ denotes the set of positive integers and $\mathbf{N}_0 := \mathbf{N} \cup \{0\}$. We use the Landau–Bachmann o and O symbols, as well as Vinogradov's $\ll$ notation, with their usual meanings. We adopt the usual convention that empty sums and empty products, e.g. $\sum_{n=x}^{y}$ and $\prod_{n=x}^{y}$ with $x > y$, have values 0 and 1, respectively. Moreover, we employ the convention that a binomial coefficient $\binom{a}{b} = 0$ if $a < b$. Finally, if g and h are two arithmetic functions, we write $g *' h$ for their *proper* Dirichlet convolution (cf. [9, Ch. 2]), i.e., the function defined by

$$(g *' h)(n) := \sum_{\substack{d \,|\, n \\ 1<d<n}} g(d)\, h(n/d), \quad n \in \mathbf{N},$$

where the sum runs over all the proper divisors d of n.

2. Preliminaries

First of all, we need a rigorous formal definition of what arithmetic formulas are.

Definition 2.1. Let n be a positive integer. An *arithmetic formula* A for n is an $\mathbf{N}$-valued $\{+, \times\}$-labeled full binary tree such that:

(i). The value of the root is n.
(ii). The value of each leaf is 1.
(iii). All node except the leaf nodes are labelled with a $+$ (*additive node*) or $\times$ (*multiplicative node*).
(iv). The value of each additive node is $a + b$, where a and b are the values of its children.
(v). The value of each multiplicative node is ab, where a and b are the values of its children.
(vi). If a and b are the values of the children of a multiplicative node, then $a, b \geq 2$.

Similarly, an *arithmetic exponential formula* E for n is an $\mathbf{N}$-valued $\{+, \times, \wedge\}$-labeled full binary tree that satisfies all the previous points, only with (iii) slightly modified to

(iii'). All nodes except the leaf nodes are labelled with $+$ (*additive node*), $\times$ (*multiplicative node*) or $\wedge$ (*exponential node*).

and furthermore

(vii). The value of an exponential node is a^b, where a and b are the values of its left and right children, respectively.
(viii). If a and b are the values of the children of an exponential node, then $a, b \geq 2$.

Finally, we say that a multiplicative node of A or E is *primitive* if it has no multiplicative ancestor.

Now we can also define the length of an arithmetic formula.

Definition 2.2. The *size* or *length* of an arithmetic formula (or an arithmetic exponential formula) A is the number of nodes of A; equivalently, the number of symbols 1, $+$, $\times$ and $\wedge$ needed to write A in the usual infix notation, or in Polish notation. Note that parenthesis do not count.

We state below a frequently used immediate consequence of Stirling's formula.

Lemma 2.1. *We have,*

$$f_0(n) = C_{n-1} \sim \frac{1}{4\sqrt{\pi}} \frac{4^n}{n^{3/2}},$$

as $n \to +\infty$.

3. Proof of Theorem 1.1

We start with a couple of lemmas. For all integers $n \geq 2$, we denote by $f^+(n)$, respectively $f^\times(n)$, the number of arithmetic formulas for n which root node is additive, respectively multiplicative. We set also $f^+(1) := 1$ and $f^\times(1) := 0$. Thus, obviously, $f(n) = f^+(n) + f^\times(n)$, for all positive integers n. Moreover, the following lemma can be easily proved.

Lemma 3.1. *For all integers $n \geq 2$, it results*

$$f^+(n) = \sum_{h=1}^{n-1} f(n-h)f(h)$$

and $f^\times(n) = (f *' f)(n)$.

The next lemma is a first upper bound on $f(n)$ which we need to be sure that the radius of convergence of $F(z)$ is positive.

Lemma 3.2. *We have $f(n) < 8^n$, for each positive integer n.*

Proof. Consider that an arithmetic formula for n, thought of as a full binary tree, has at most $n-1$ non-leaf nodes. For any nonnegative integer k there are exactly C_k full binary trees with k non-leaf nodes. Given one of them, its non-leaf nodes can be labeled (as additive or multiplicative) in 2^k different ways. In conclusion, since $C_k \leq 4^k$, we get

$$f(n) \leq \sum_{k=0}^{n-1} 2^k C_k \leq \sum_{k=0}^{n-1} 8^k < 8^n.$$

□

As for the analytic input into our proof we will need the following version of "Darboux's method".

Lemma 3.3 (Darboux's method)**.** *Let $v(z)$ be analytic in some disk $|z| \leq 1+\eta$, and suppose that in a neighborhood of $z = 1$ it has the expansion $v(z) = \sum_{j=0}^{\infty} v_j(1-z)^j$. Let $\beta \notin \{0, 1, 2, \ldots\}$. Then, the n-th coefficient of $(1-z)^\beta v(z)$ is equal to*

$$\sum_{j=0}^{m} v_j \binom{n-\beta-j-1}{n} + O(n^{-m-\beta-2}).$$

Proof. See [15, Theorem 5.3.1]. □

We will also need the following classical result of Pringsheim.

Lemma 3.4. *Let $f(z)$ be a power series with finite radius of convergence $R > 0$. If all of the coefficients of $f(z)$ are nonnegative, then, $z = R$ is a singular point.*

Proof. See [12, Chapter 8]. □

We will use the following immediate consequence of Lemma 3.4: if $f(z)$, a power series with nonnegative coefficients, has an analytic continuation to $|z| < R+\eta$, for some $\eta > 0$, then the abscissa of the first singularity of $f(z)$ on the axis $x > 0$ is equal to the radius of convergence R. Now we are ready to prove Theorem 1.1.

Proof of Theorem 1.1. Let R be the radius of convergence of the generating function $F(z)$. First of all $R \le 1/4$ since $f(n) \ge f_0(n)$ and $f_0(n) > (4-\varepsilon)^n$ for any $\varepsilon > 0$ and all n large enough. On the other hand from Lemma 3.2 we know that $R \ge 1/8$. For each integer $d \ge 2$, it results that $F(z^d) - z^d$ has radius of convergence $R^{1/d} \ge R^{1/2}$. Hence, for any $\delta > 0$ and $|z| < R^{1/2} - \delta$ we have $|F(z^d) - z^d| \ll_\delta |z|^{2d}$ and $f(d) < (1/R + \varepsilon)^d$ for sufficiently large d. Therefore, the series $\widetilde{F}(z)$ converges absolutely for $|z| < R^{1/2}$ and it is analytic in that region, note also that $R^{1/2} > R$. For $|z| < R$, from Lemma 3.1 we obtain

$$\sum_{n=1}^{\infty} f^+(n) z^n = z + \sum_{n=2}^{\infty} \sum_{k=1}^{n-1} f(n-k) f(k) z^n = z + F(z)^2,$$

while

$$\begin{aligned}\sum_{n=1}^{\infty} f^\times(n) z^n &= \sum_{n=1}^{\infty} \sum_{\substack{d \mid n \\ 1<d<n}} f(d) f(n/d) z^n \\ &= \sum_{d=2}^{\infty} f(d) \sum_{m=2}^{\infty} f(m) z^{dm} = \sum_{d=2}^{\infty} f(d)(F(z^d) - z^d).\end{aligned}$$

Thus,

$$F(z) = \sum_{n=1}^{\infty} f(n) z^n = \sum_{n=1}^{\infty} f^+(n) z^n + \sum_{n=1}^{\infty} f^\times(n) z^n = F(z)^2 + \tilde{F}(z),$$

so that

$$F(z)^2 - F(z) + \tilde{F}(z) = 0. \tag{1}$$

Taking into account that $F(0) = \widetilde{F}(0) = 0$, we can solve the quadratic equation (1) and get

$$F(z) = \frac{1 - \sqrt{1 - 4\widetilde{F}(z)}}{2}, \qquad \text{for } |z| < R. \tag{2}$$

Since the coefficients of $F(z)$ are all positive, by Lemma 3.4 we have that $F(z)$ has a singularity at $z = R$. As observed before, in the region $|z| < R^{1/2}$ the function $\widetilde{F}(z)$ is analytic and $R^{1/2} > R$, thus providing an analytic continuation of $F(z)$ to

the larger region $|z| < R^{1/2}$. From (2) we expect that the first singularity of $F(z)$ on the positive real axis occur at the point ξ at which we have $\widetilde{F}(\xi) = 1/4$. Such ξ clearly exists because $\widetilde{F}(x) > x$, for $x > 0$, so that $\xi < 1/4$, while $\widetilde{F}(z)$ is analytic in $|z| < 1/\sqrt{8} \leq R^{1/2}$. We notice also that the root ξ is simple, because $F(x)$ is increasing and analytic on the segment $0 \leq x < 1/\sqrt{8}$. Thus we can write,

$$1 - 4\widetilde{F}(z) = (1 - z/\xi)G(z) \tag{3}$$

for some $G(z)$, analytic in $|z| < 1/\sqrt{8}$ and non-vanishing on $0 \leq x < 1/\sqrt{8}$. As mentioned earlier, the formula

$$F(z) = \frac{1 - \sqrt{(1 - z/\xi)G(z)}}{2}$$

provides an analytic continuation of $F(z)$ to the larger disc $|z| < 1/\sqrt{8}$, since the radius of convergence of $F(z)$ satisfies $R \leq 1/4 < 1/\sqrt{8}$. As an immediate application of Lemma 3.4 the first singularity of $F(z)$ on the positive real axis corresponds to the radius of convergence R. Thus $R = \xi$. Before applying Lemma 3.3 we need to say a few things about the location of the zeros of $G(z)$. Since $\widetilde{F}(z)$ has positive and never vanishing coefficients, we have $|\widetilde{F}(re^{i\theta})| < \widetilde{F}(r) \leq \widetilde{F}(R)$ for all $\theta \neq 0$ and $r \leq R$. Using this we notice that for $z \neq \xi$, and $|z| \leq \xi$,

$$|1 - 4\widetilde{F}(z)| \geq 1 - 4|\widetilde{F}(z)| > 1 - 4\widetilde{F}(\xi) = 0.$$

It follows that $G(z)$ has no zeros in $|z| \leq \xi$. By analyticity this implies that there exists a neighborhood $|z| \leq \xi + \eta$ for some $\eta > 0$, where $G(z)$ does not vanish, in particular $\sqrt{G(z)}$ is well-defined and does not vanish there. Now, applying Lemma 3.3 to $F(z\xi)$, or rather more precisely applying Lemma 3.3 to $-\sqrt{(1-z)G(z\xi)}/2$ (which has radius of convergence equal to 1 and differs from $F(z)$ only at the constant term) we conclude that for any $m \geq 0$, and $n \to \infty$,

$$f(n)\xi^n = -\sum_{j=0}^{m} c_j \binom{n - j - 3/2}{n} + O(n^{-m-5/2}) \tag{4}$$

where the coefficients c_j are obtained by writing

$$\sqrt{G(z\xi)} = \sum_{j \geq 0} c_j (1 - z)^j$$

in a small neighborhood of $z = 1$. Since, as $n \to \infty$,

$$\binom{n - j - 3/2}{n} \sim \frac{a_j}{n^{j+3/2}}$$

with $a_j \neq 0$, for any $m \geq 0$ equation (4) gives us an asymptotic expansion for $f(n)$.

In particular, for $m = 0$, we obtain

$$f(n) = \frac{c\rho^n}{n^{3/2}} + O(\rho^n n^{-5/2}),$$

as $n \to \infty$, where $\rho := 1/\xi$ and

$$c := -a_0 c_0 = -a_0\sqrt{G(\xi)} = \frac{\sqrt{G(\xi)}}{2\sqrt{\pi}}, \tag{5}$$

this completes the proof. □

We computed the constant $\rho = 1/\xi$ by first approximating the functions $F(z)$ and $\widetilde{F}(z)$ by high degree polynomials, and then using fixed-point iteration to find the smallest positive solution ξ to the equation $\widetilde{F}(\xi) = 1/4$. After, using (3) we found a polynomial approximation for $G(z)$ and then we computed the constant c from (5).

We performed the computation using Sage, the code can be found on [5, p. 24].

4. Proof of Theorem 1.2

We will in fact prove a result stronger than Theorem 1.2. However before stating it, we introduce the concept of a *k-trace*.

Definition 4.1. Let k be a positive integer. A *k-trace* is triple $(p, \mathbf{l}, \mathbf{r})$ where p is a positive integer and $\mathbf{l}, \mathbf{r} \in \mathbf{N}_0^p$ are tuples such that $\ell_1 + r_1 + \cdots + \ell_p + r_p + p = k$. We denote by $\mathfrak{T}_k$ the set of all *k-traces*. We define also $\mathfrak{T}_0 := \{(0, 0, 0)\}$ so that $(0, 0, 0)$ can be thought of as the only 0-trace.

We are ready to state our asymptotic formula for $f_k(n)$.

Theorem 4.1. *For all integers $k \geq 0$, we have*

$$f_k(n) \sim \frac{1}{4\sqrt{\pi}} \frac{4^n}{n^{3/2}} \sum_{(p,\mathbf{l},\mathbf{r})\in\mathfrak{T}_k} \frac{n^p}{p!} \prod_{i=1}^{p} \left(\sum_{t=1}^{\infty} \frac{(f_{\ell_i} *' f_{r_i})(t)}{4^{t-1}} \right),$$

as $n \to +\infty$.

Observe that Theorem 1.2 follows immediately from Theorem 4.1, since for any $k \in \mathbf{N}$ the only $(p, \mathbf{l}, \mathbf{r}) \in \mathfrak{T}_k$ with $p \geq k$ is $(k, \mathbf{0}, \mathbf{0})$. The next definition connects k-traces to arithmetic formulas.

Definition 4.2. Suppose that A is an arithmetic formulas for n with k multiplicative nodes. If $k = 0$ then the *trace* of A is $(0, 0, 0)$. If $k \geq 1$, let $N_1, \ldots, N_p$ be the primitive nodes of A, ordered from left to right (there is no ambiguity since no primitive node is the ancestor of another primitive node). For $i = 1, \ldots, p$, let ℓ_i, respectively r_i, be the number of multiplicative nodes in the left, respectively right, subtree of N_i. Then the trace of A is the triple $(p, \mathbf{l}, \mathbf{r})$, with $\mathbf{l} = (\ell_1, \ldots, \ell_p)$ and $\mathbf{r} = (r_1, \ldots, r_p)$. Finally,

for all $k \in \mathbf{N}_0$ and $(p, \mathbf{l}, \mathbf{r}) \in \mathfrak{T}_k$ we denote by $f_{(p,\mathbf{l},\mathbf{r})}(n)$ the number of arithmetic formulas for n with trace $(p, \mathbf{l}, \mathbf{r})$.

It is easy to see that Definition 4.1 and 4.2 are consistent to each other, i.e., if A is an arithmetic formula with k multiplicative nodes then the trace of A is actually a k-trace.

We give now a combinatorial formula for $f_{(p,\mathbf{l},\mathbf{r})}$ in terms of f_0 and f_{ℓ_i}, f_{r_i}.

Lemma 4.2. *For $k \in \mathbf{N}$ and $(p, \mathbf{l}, \mathbf{r}) \in \mathfrak{T}_k$, we have*

$$f_{(p,\mathbf{l},\mathbf{r})}(n) = \sum_{n_1+\cdots+n_p+m=n+p} \binom{m}{p} f_0(m) \prod_{i=1}^{p} (f_{\ell_i} *' f_{r_i})(n_i),$$

where the sum runs over all $n_1, \dots, n_p, m \in \mathbf{N}$ such that $n_1 + \cdots + n_p + m = n + p$.

Proof. The general arithmetic formula A evaluating to n and with trace $(p, \mathbf{l}, \mathbf{r})$ is depicted in Fig. 1, where $n_1, \dots, n_p$ are all the primitive multiplicative nodes of A (we identify the nodes with their values since there is no risk of confusion). Set $m := n - (n_1 + \cdots + n_p) + p$. On the one hand, if we remove from A all the nodes below $n_1, \dots, n_p$ we get a full binary tree with m leaves. There are exactly $f_0(m)$ such trees (addition is associative) and the nodes $n_1, \dots, n_p$ can be attached to the leaves of each of them in $\binom{m}{p}$ different ways. On the other hand, any subtree of A with root a_i, respectively b_i, is an arithmetic formula for a_i, respectively b_i, and there are exactly $f_{\ell_i}(a_i)$, respectively $f_{r_i}(b_i)$, such arithmetic formulas. Hence, since $a_i b_i = n_i$, there are $(f_{\ell_i} *' f_{r_i})(n_i)$ possible subtrees of n_i. All these choices are independent so the claim follows. □

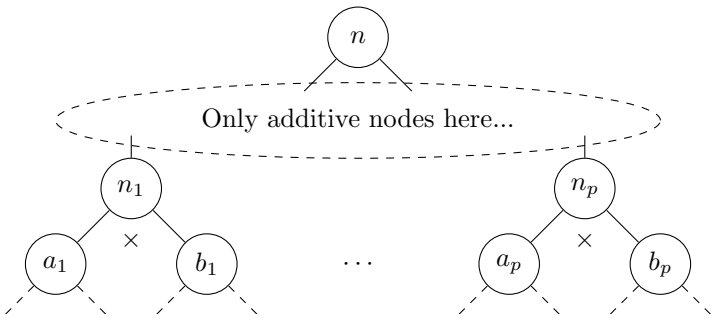

FIGURE 1. An arithmetic formula for n.

The next lemma is an easy upper bound on the proper Dirichlet convolution of two arithmetic functions.

Lemma 4.3. *Let g and h be arithmetic functions such that $g(n), h(n) \ll 4^n n^s$ for $n \in \mathbf{N}$, with $C > 0$ and $s \in \mathbf{R}$. Then $(g *' h)(n) \ll 3^n$ for $n \in \mathbf{N}$.*

Proof. We have

$$(g *' h)(n) = \sum_{\substack{d \mid n \\ 1<d<n}} g(d)\, h(n/d) \ll n^s \sum_{\substack{d \mid n \\ 1<d<n}} 4^{d+n/d} \ll 2^n n^s \sum_{\substack{d \mid n \\ 1<d<n}} 1 \ll 2^n n^{s+1} \ll 3^n,$$

since $d + n/d \leq 2 + n/2$ for all proper divisors d of n. □

At this point, we have all the tools required to prove Theorem 4.1.

Proof of Theorem 4.1. We proceed by strong induction on k. For $k = 0$, the claim follows immediately from Lemma 2.1. Suppose $k \geq 1$ and that the statement holds for all nonnegative integers $k' < k$. Then, as $n \to +\infty$, we have $f_l(n), f_r(n) \ll 4^n n^{k-3/2}$ for all nonnegative integers $l, r < k$ and applying Lemma 4.3 we conclude that $(f_l *' f_r)(n) \ll 3^n$. In particular, the series

$$\sum_{t=1}^{\infty} \frac{(f_l *' f_r)(t)}{4^{t-1}}$$

converges. Since $\mathfrak{T}_k$ is finite and, since

$$f_k(n) = \sum_{(p,\mathbf{l},\mathbf{r}) \in \mathfrak{T}_k} f_{(p,\mathbf{l},\mathbf{r})}(n),$$

it suffices to prove that for all $(p, \mathbf{l}, \mathbf{r}) \in \mathfrak{T}_k$ we have

$$f_{(p,\mathbf{l},\mathbf{r})}(n) \sim \frac{1}{4\sqrt{\pi} p!}\, 4^n n^{p-3/2} \prod_{i=1}^{p} \left(\sum_{t=1}^{\infty} \frac{(f_{\ell_i} *' f_{r_i})(t)}{4^{t-1}} \right), \tag{6}$$

as $n \to +\infty$. Fix $\varepsilon > 0$ and $N \in \mathbf{N}$. In light of Lemma 2.1 and since $\binom{m}{p} \sim \frac{m^p}{p!}$ as $m \to +\infty$, there exists a positive integer $n_{\varepsilon,N} > N$ such that

$$\binom{m}{p} f_0(m) \geq \left(\frac{1}{4\sqrt{\pi} p!} - \varepsilon \right) 4^m n^{p-3/2},$$

for all positive integers $n \geq n_{\varepsilon,N}$ and $m \in [n-N+p, n]$. Consequently, using Lemma 4.2, we obtain

$$\begin{aligned} f_{(p,\mathbf{l},\mathbf{r})}(n) &\geq \sum_{\substack{n_1+\cdots+n_p+m=n+p \\ n_1+\cdots+n_p\leq N}} \binom{m}{p} f_0(m) \prod_{i=1}^{p} (f_{\ell_i} *' f_{r_i})(n_i) \\ &\geq \left(\frac{1}{4\sqrt{\pi}p!} - \varepsilon\right) n^{p-3/2} \sum_{\substack{n_1+\cdots+n_p+m=n+p \\ n_1+\cdots+n_p\leq N}} 4^m \prod_{i=1}^{p} (f_{\ell_i} *' f_{r_i})(n_i) \\ &\geq \left(\frac{1}{4\sqrt{\pi}p!} - \varepsilon\right) 4^n n^{p-3/2} \sum_{n_1+\cdots+n_p\leq N} \prod_{i=1}^{p} \frac{(f_{\ell_i} *' f_{r_i})(n_i)}{4^{n_i-1}} \end{aligned}$$

for $n \geq n_{\varepsilon,N}$, so that

$$\liminf_{n\to\infty} \frac{f_{(p,\mathbf{l},\mathbf{r})}(n)}{4^n n^{p-3/2}} \geq \left(\frac{1}{4\sqrt{\pi}p!} - \varepsilon\right) \sum_{n_1+\cdots+n_p\leq N} \prod_{i=1}^{p} \frac{(f_{\ell_i} *' f_{r_i})(n_i)}{4^{n_i-1}}.$$

Therefore, as $\varepsilon \to 0$ and $N \to +\infty$, we get

$$\begin{aligned} \liminf_{n\to\infty} \frac{f_{(p,\mathbf{l},\mathbf{r})}(n)}{4^n n^{p-3/2}} &\geq \frac{1}{4\sqrt{\pi}p!} \sum_{(n_1,\ldots,n_p)\in\mathbf{N}^p} \prod_{i=1}^{p} \frac{(f_{\ell_i} *' f_{r_i})(n_i)}{4^{n_i-1}} \\ &= \frac{1}{4\sqrt{\pi}p!} \prod_{i=1}^{p} \left(\sum_{t=1}^{\infty} \frac{(f_{\ell_i} *' f_{r_i})(t)}{4^{t-1}}\right). \end{aligned} \tag{7}$$

On the other hand, there exists $m_\varepsilon \in \mathbf{N}$ such that

$$\binom{m}{p} f_0(m) \leq \left(\frac{1}{4\sqrt{\pi}p!} + \varepsilon\right) 4^m m^{p-3/2},$$

for all $m \geq m_\varepsilon$. Thus,

$$\begin{aligned}(8)\qquad &\sum_{\substack{n_1+\cdots+n_p+m=n+p\\ m\geq m_\varepsilon}} \binom{m}{p} f_0(m) \prod_{i=1}^{p} (f_{\ell_i} *' f_{r_i})(n_i) \\ &\leq \left(\frac{1}{4\sqrt{\pi}p!} + \varepsilon\right) \sum_{\substack{n_1+\cdots+n_p+m=n+p\\ m\geq m_\varepsilon}} 4^m m^{p-3/2} \prod_{i=1}^{p} (f_{\ell_i} *' f_{r_i})(n_i) \\ &\leq \left(\frac{1}{4\sqrt{\pi}p!} + \varepsilon\right) 4^n n^{p-3/2} \sum_{n_1+\cdots+n_p\leq n+p-m_\varepsilon} \prod_{i=1}^{p} \frac{(f_{\ell_i} *' f_{r_i})(n_i)}{4^{n_i-1}} \\ &\leq \left(\frac{1}{4\sqrt{\pi}p!} + \varepsilon\right) 4^n n^{p-3/2} \prod_{i=1}^{p} \left(\sum_{t=1}^{\infty} \frac{(f_{\ell_i} *' f_{r_i})(t)}{4^{t-1}}\right).\end{aligned}$$

We claim that

$$(9)\qquad \sum_{n_1+\cdots+n_p>n+p-m_\varepsilon} \prod_{i=1}^{p} \frac{(f_{\ell_i} *' f_{r_i})(n_i)}{4^{n_i-1}} = o(n^{p-3/2}),$$

as $n \to +\infty$. This is straightforward if $p \geq 2$, since the left hand side of (9) is bounded while $n^{p-3/2} \to +\infty$. On the other hand if $p = 1$ then

$$\sum_{n_1>n+1-m_\varepsilon} \frac{(f_{\ell_1} *' f_{r_1})(n_1)}{4^{n_1-1}} = O((3/4)^n) = o(n^{-1/2}),$$

as $n \to +\infty$. Hence,

$$\begin{aligned}(10)\qquad &\sum_{\substack{n_1+\cdots+n_p+m=n+p\\ m<m_\varepsilon}} \binom{m}{p} f_0(m) \prod_{i=1}^{p} (f_{\ell_i} *' f_{r_i})(n_i) \\ &\leq \left(\max_{m<m_\varepsilon} 4^{-m} \binom{m}{p} f_0(m)\right) \sum_{\substack{n_1+\cdots+n_p+m=n+p\\ m<m_\varepsilon}} 4^m \prod_{i=1}^{p} (f_{\ell_i} *' f_{r_i})(n_i) \\ &\ll 4^n \sum_{n_1+\cdots+n_p>n+p-m_\varepsilon} \prod_{i=1}^{p} \frac{(f_{\ell_i} *' f_{r_i})(n_i)}{4^{n_i-1}} = o(4^n n^{p-3/2})\end{aligned}$$

as $n \to +\infty$. Therefore, summing (8) and (10), and using Lemma 4.2, we obtain

$$\limsup_{n\to\infty} \frac{f_{(p,\mathbf{l},\mathbf{r})}(n)}{4^n n^{p-3/2}} \leq \left(\frac{1}{4\sqrt{\pi}p!} + \varepsilon\right) \prod_{i=1}^{p} \left(\sum_{t=1}^{\infty} \frac{(f_{\ell_i} *' f_{r_i})(t)}{4^{t-1}}\right).$$

We conclude that as $\varepsilon \to 0$, we get

$$\limsup_{n\to\infty} \frac{f_{(p,\mathbf{l},\mathbf{r})}(n)}{4^n n^{p-3/2}} \le \frac{1}{4\sqrt{\pi}p!} \prod_{i=1}^{p} \left(\sum_{t=1}^{\infty} \frac{(f_{\ell_i} *' f_{r_i})(t)}{4^{t-1}} \right).$$

Combining this with (7) give (6) concludes the proof.

5. Proof of Theorem 1.4

Set $c := (1-\varepsilon)/\log 4$ and for $x > 0$ define

$$E(x) := \{n \le x : S_{\text{short}}(n) < c \log n\}.$$

For each positive integer k, let $\ell(k)$ be the number of exponential arithmetic formulas of length k. Writing such formulas in Polish notation we see that $\ell(k) \le 4^k$. In fact, for each of the k symbols of the Polish notation we have at most 4 choices, corresponding to addition, multiplication, exponentiation or 1. Furthermore, observe that if A_n denote a shortest length arithmetic formula for n, then clearly $A_m \ne A_n$ for all $m \ne n$. In conclusion,

$$|E(x)| \le \sum_{k<c\log x} \ell(k) \le \sum_{k<c\log x} 4^k = O(x^{1-\varepsilon}),$$

which is our claim. □

6. Proof of Theorem 1.5

Throughout this section, given a positive integer n, we write

$$n = \sum_{j=0}^{\infty} d_j(n) 2^j, \text{ with } d_j(n) \in \{0,1\},$$

for its binary expansion. In particular, we define

$$s_2(n) := |\{j \ge 0 : d_j(n) = 1\}| = \sum_{j=0}^{\infty} d_j(n),$$

i.e., the number of nonzero binary digits of n. Furthermore, let $\operatorname{lb} x := \log x/\log 2$ be the binary logarithm of x.

Lemma 6.1. *For fixed $\varepsilon > 0$, if*

$$S_\varepsilon(x) := \left\{n \le x : s_2(n) \le \left(\tfrac{1}{2} - \varepsilon\right)\operatorname{lb} x\right\},$$

then $|S_\varepsilon(x)| = o(x)$, as $x \to \infty$.

Proof. Let N be the positive integer such that $2^{N-1} \le x < 2^N$. Moreover, let $X_1, \dots, X_N$ be a sequence of independent random variables with

$$\mathbf{P}(X_i = 0) = \mathbf{P}(X_i = 1) = \tfrac{1}{2}, \text{ for } i = 1, \dots, N.$$

Then, for each nonnegative integer $k \le N$,

$$|\{n < 2^N : s_2(n) = k\}| = 2^N \cdot \mathbf{P}(X_1 + \cdots + X_N = k).$$

By the weak law of large numbers,

$$\mathbf{P}\left(\Big|\frac{X_1 + \cdots + X_N}{N} - \frac{1}{2}\Big| > \varepsilon\right) \to 0$$

as $N \to \infty$. Therefore,

$$|S_\varepsilon(x)| \le \big|\big\{n < 2^N : s_2(n) \le \big(\tfrac{1}{2} - \varepsilon\big)N\big\}\big| = o(2^N) = o(x),$$

as $x \to \infty$, since $2^N \le 2x$. □

We are now ready to prove Theorem 1.5.

Proof of Theorem 1.5. Fix $\varepsilon > 0$ and let $\delta \in \,]0, \varepsilon]$ be arbitrary. According to Lemma 6.1, for x sufficiently large we have $|S_\varepsilon(x)| < \delta x$ and also $|S_\varepsilon(\operatorname{lb} x)| < \delta \operatorname{lb} x$. Let $T_\varepsilon(x) := [1, x] \setminus S_\varepsilon(x)$, so that $|T_\varepsilon(x)| > (1 - \delta)x$. It is easily seen that $S_{\mathrm{FCF}}(n) \ge s_2(n)$ for all positive integers n. Hence, for each $n \in T_\varepsilon(x)$ we have

$$\begin{aligned} S_{\mathrm{FCF}}(n) &\ge \sum_{\substack{j \le \operatorname{lb} x \\ d_j(n) = 1}} S_{\mathrm{FCF}}(j) \ge \sum_{\substack{j \le \operatorname{lb} x \\ d_j(n) = 1}} s_2(j) \ge \sum_{\substack{j \le \operatorname{lb} x \\ d_j(n) = 1 \\ j \notin S_\varepsilon(\operatorname{lb} x)}} s_2(j) \\ &> (\tfrac{1}{2} - \varepsilon) \cdot \operatorname{lb}\operatorname{lb} x \sum_{\substack{j \le \operatorname{lb} x \\ d_j(n) = 1 \\ j \notin S_\varepsilon(\operatorname{lb} x)}} 1 \\ &> (\tfrac{1}{2} - \varepsilon)(\tfrac{1}{2} - \varepsilon - \delta) \operatorname{lb} x \operatorname{lb}\operatorname{lb} x \\ &\ge (\tfrac{1}{2} - 2\varepsilon)^2 \operatorname{lb} n \operatorname{lb}\operatorname{lb} n. \end{aligned}$$

In conclusion, for any $\delta \in \,]0, \varepsilon]$ we have that for sufficiently large x,

$$S_{\mathrm{FCF}}(n) \ge \left(\frac{1}{2} - 2\varepsilon\right)^2 \cdot \operatorname{lb} n \operatorname{lb}\operatorname{lb} n > \left(\frac{1}{2} - 2\varepsilon\right)^2 \frac{1}{(\log 2)^2} \cdot \log n \log\log n, \tag{11}$$

holds for at least $(1 - \delta)x$ positive integers $n \le x$. Therefore, (11) holds for almost all positive integers, and our claim follows. □

7. Proof of Theorem 1.6

Fix a positive integer n. In the second canonical form of n, we replace any occurrence of $(1+1)$ by the symbol 2. For example, after this process the second canonical form of 51 becomes $(1+2)(1+2^{2^2})$. Now let $t(n)$ be the number of 2's in this formula for n. Then, upon ignoring every addition, and by repeatedly using the inequality $2^y \geq 2 \cdot y$, it follows that $n \geq 2^{t(n)}$. To continue the example,

$$51 = (1+2)(1+2^{2^2}) \geq 2 \cdot 2^{2^2} \geq 2 \cdot 2^{2 \cdot 2} \geq 2 \cdot (2 \cdot (2 \cdot 2)).$$

Hence $t(n) \leq \log n / \log 2$ and to prove Theorem 1.6 it is sufficient to show that $S_{\mathrm{SCF}}(n) \leq 6t(n) - 1$ for each integer $n \geq 2$. We proceed by strong induction on n. For $n = 2$ and $n = 3$ the claim is true, hence assume $n \geq 4$ and that the inequality holds for all integers in $[2, n-1]$. If n is a prime number then we have three cases:

(i). $n = 1 + (1+1) \cdot m$, with m an odd integer such that $2 \leq m < n$.
(ii). $n = 1 + (1+1)^s$, with $s \geq 2$ an integer.
(iii). $n = 1 + (1+1)^s \cdot m$, with m and s integers such that m is odd, $2 \leq m < n$ and $s \geq 2$.

We do only case (iii), the others are similar. It results $t(n) = 1 + t(s) + t(m)$, so by inductive hypothesis

$$S_{\mathrm{SCF}}(n) = 7 + S_{\mathrm{SCF}}(s) + S_{\mathrm{SCF}}(m) \leq 7 + (6t(s) - 1) + (6t(m) - 1) = 6t(n) - 1.$$

If n is composite, let $n = p_1 \cdots p_k q_1^{b_1} \cdots q_h^{b_h}$ be its prime factorization, with $b_i \geq 2$. We have

$$t(n) = \sum_{i=1}^{k} t(p_i) + \sum_{j=1}^{h} (t(q_j) + t(b_j)).$$

Since $2 \leq p_i, q_j, b_j < n$ for all $i = 1, \ldots, k$ and $j = 1, \ldots, h$, by inductive hypothesis we obtain

$$\begin{aligned} S_{\mathrm{SCF}}(n) &= k + 2h - 1 + \sum_{i=1}^{k} S_{\mathrm{SCF}}(p_i) + \sum_{j=1}^{h} (S_{\mathrm{SCF}}(q_j) + S_{\mathrm{SCF}}(b_j)) \\ &\leq 6 \sum_{i=1}^{k} t(p_i) + 6 \sum_{j=1}^{h} (t(q_j) + t(b_j)) - 1 \\ &= 6t(n) - 1, \end{aligned}$$

hence the proof is complete.

8. Acknowledgements

We would like to thank the IAS for providing excellent working conditions and Noga Alon for the proof of the lower bound for $S_{\text{short}}(n)$. We also thank the referees for their careful reading and useful comments.

References

[1] P. Bürgisser. On defining integers and proving arithmetic circuit lower bounds. *Comput. Complexity*, 18(1):81–103, 2009.
[2] Qi Cheng. On the ultimate complexity of factorials. *Theoret. Comput. Sci.*, 326(1-3):419–429, 2004.
[3] C. G. T. de A. Moreira. On asymptotic estimates for arithmetic cost functions. *Proc. Amer. Math. Soc.*, 125(2):347–353, 1997.
[4] W. de Melo and B. F. Svaiter. The cost of computing integers. *Proc. Amer. Math. Soc.*, 124(5):1377–1378, 1996.
[5] E. K. Gnang. Integer formula encoding SageTex package, arXiv:1407.0039.
[6] E. K. Gnang and D. Zeilberger. Zeroless arithmetic: Representing integers ONLY using ONE. *J. Difference Equ. Appl.*, 19(11):1921–1926, 2013.
[7] R. L. Goodstein. On the restricted ordinal theorem. *J. Symbolic Logic*, 9:33–41, 1944.
[8] A. P. Heinz. The on-line encyclopedia of integer sequences, http://oeis.org, Sequence A214833.
[9] Chan Heng Huat. *Analytic number theory for undergraduates*, volume 3 of *Monographs in Number Theory*. World Scientific, New Jersey, 2009.
[10] P. Koiran. Valiant's model and the cost of computing integers. *Comput. Complexity*, 13(3-4):131–146, 2004.
[11] D. Patrick and E. K. Gnang. Some integer formula encodings and related algorithms. *Adv. in Appl. Math.*, 51(4):536–541, 2013.
[12] R. Reinhold. *Theory of complex functions*, volume 122 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1991. Translated from the second German edition by Robert B. Burckel, Readings in Mathematics.
[13] C. Sanna. On the number of arithmetic formulas. *Int. J. Number Theory*, to appear.
[14] R. P. Stanley. *Enumerative Combinatorics: volume 2*. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 2001.
[15] H. S. Wilf. *generatingfunctionology*. A K Peters, Ltd., Wellesley, MA, third edition, 2006.

School of Mathematics, Institute for Advanced Study, 1 Einstein Drive, Princeton, NJ, USA
E-mail address: gnang@ias.edu

School of Mathematics, Institute for Advanced Study, 1 Einstein Drive, Princeton, NJ, USA
E-mail address: maksym@ias.edu

Università degli Studi di Torino, Department of Mathematics, Turin, Italy
E-mail address: carlo.sanna.dev@gmail.com