AN IMPROVED UPPER BOUND FOR $F(m, r)$

T. AGAMA

Abstract. Let us set

$$F(m,r) := \#\{n \in [2^m, 2^{m+1}) \ : \ \iota(n) \leq \lfloor m+r \rfloor\}$$

with $r := c\frac{m}{\log m}$ for $0 < c < \log 2$. Set

$$\alpha := c + \log 2 - \frac{1}{4}(1 - o(1)).$$

By exploiting the Chernoff inequality in probability theory and using ideas in [1], we obtain the improved upper bound

$$F(m, c\frac{m}{\log m}) \leq \exp\left(\alpha m - (1-\epsilon)\frac{cm \log\log m}{\log m}\right)$$

for any small $\epsilon > 0$ as $m \longrightarrow \infty$.

1. Preliminaries

Lemma 1.1. *We have*

$$\binom{A}{B} \leq 2^A \mathrm{Pr}(X \leq B)$$

where $\mathrm{Pr}(X \geq \cdot)$ *denotes the probability that* $X \geq \cdot$.

Proof. Let $\mathrm{B}(A, \frac{1}{2})$ denote the binomial probability distribution, and let $X \sim \mathrm{B}(A, \frac{1}{2})$, a random variable in this distribution. Here, the quantity $\frac{1}{2}$ is the probability of success. Then

$$\mathrm{Pr}(X = B) = \binom{A}{B}\left(\frac{1}{2}\right)^A.$$

Since $\mathrm{Pr}(X = B) \leq \mathrm{Pr}(X \leq B)$, the upper bound is an immediate consequence. □

This simple relation suggests a possible road map that leads to an improved upper bound for the binomial quantity $\binom{A}{B}$ and, consequently,

Date: June 18, 2025.

Key words and phrases. Chernoff.

for $F(m,r)$. It reduces the entire problem to studying upper bounds for $\Pr(X \leq B)$. Now, we observe that

$$\Pr(X \geq a) = \Pr(e^{Xt} \geq e^{Xa})$$

. Let $\mathbb{E}(e^{tX})$ denote the expected value of e^{tX}, then

$$\mathbb{E}(e^{tX}) = e^{tX}\Pr(e^{Xt} \geq e^{at}).$$

Thus

$$\Pr(e^{tX} \geq e^{at}) = e^{-tX}\mathbb{E}(e^{tX}) \leq e^{-ta}\mathbb{E}(e^{tx}).$$

Since this inequality holds for all $t > 0$, we can write

$$\Pr(e^{tX} \geq e^{at}) \leq \inf_{t>0} (e^{-ta}\mathbb{E}(e^{tX}))$$

which can be rewritten in the form

$$\Pr(X \geq A) \leq \inf_{t>0} \mathbb{E}(e^{t(X-a)}).$$

2. Some facts and deductions

Let $X_1, \cdots, X_n$ be identically distributed independent random variables in a Bernoulli distribution Bernoulli(n,p) for n trials with mean $\mathbb{E}(X) = n \cdot p$ and variance $\mathbb{E}(X^2) - (\mathbb{E}(X))^2 = p(p-1)$, with each X_i taking values in $\{0,1\}$. It is known that the sum $X_1 + X_2 + \cdots + X_n$ can be approximated to binomial distributions with n trials. In particular,

$$\sum_{i=1}^{n} X_i \sim \mathrm{B}(n,p)$$

as $n \longrightarrow \infty$. Using the inequality

$$\Pr(X \geq A) \leq \inf_{t>0} \mathbb{E}(e^{t(X-a)})$$

we set $X \sim \mathrm{B}(n, \frac{1}{2})$ with $X := \sum\limits_{i=1}^{n} X_i$, where each $X_i \in \{0,1\}$ and Bernoulli$(\frac{1}{2})$. Let $\mathbb{E}(X) = \mu$, then

$$\mathbb{E}(X) = \sum_{i=1}^{n} \mathbb{E}(X_i)$$

by the linearity property of expectation. Under the assumption that $X_i \sim$ Bernoulli$(\frac{1}{2})$, we deduce

$$\mathbb{E}(X) = \sum_{i=1}^{n} (\frac{1}{2} + 0) = \frac{n}{2}$$

which implies that $\mathbb{E}(X) := \mu = \frac{n}{2}$. Now, let us put $a := (1+\delta^{'})\mu$ for an arbitrary small $\delta^{'} > 0$, then we obtain

$$\Pr(X \geq (1+\delta^{'})\mu) \leq \inf_{t>0} e^{-ta}\ \mathbb{E}(e^{tX}).$$

Since X_i $(1 \leq i \leq n)$ are independent random variables and $X = \sum_{i=1}^{n} X_i$, it follows from the property $\mathbb{E}(X_iX_j) = \mathbb{E}(X_i)\mathbb{E}(X_j)$ that

$$\mathbb{E}(e^{tX}) = \mathbb{E}(e^{t\sum_{i=1}^{n} X_i}) = \mathbb{E}(\prod_{i=1}^{n} e^{tX_i}) = \prod_{i=1}^{n} \mathbb{E}(e^{tX_i}).$$

Since $X_i \sim \text{Bernoulli}(\frac{1}{2})$, it follows that $e^{tX_i} \sim \text{Bernoulli}(\frac{1}{2})$ and hence $\mathbb{E}(e^{tX_i}) = \frac{1}{2}e^t + \frac{1}{2}$. Hence

$$\mathbb{E}(e^{tX}) = \left(\frac{e^t+1}{2}\right)^n$$

so that by putting this information in the bound for the probability, we have

$$\Pr(X \geq (1+\delta^{'})\mu) \leq \inf_{t>0} \exp(n\log(\frac{e^t+1}{2}) - t(1+\delta^{'})).$$

Now, we set $\phi(t) := n\log(\frac{e^t+1}{2}) - t(1+\delta^{'})$ then the value of t for which $\phi^{'}(t) = 0$ gives the minimal bound for $\Pr(X \geq (1+\delta^{'})\mu)$. A quick verification gives

$$t = \log\left(\frac{1+\delta^{'}}{1-\delta^{'}}\right).$$

Putting this value of t in the inequality with $\mu = \frac{n}{2}$, we have the upper bound

$$\Pr(X \geq (1+\delta^{'})\mu) \leq \exp\left(-n\left((\frac{1+\delta^{'}}{2})\log(1+\delta^{'}) + (\frac{1-\delta^{'}}{2})\log(1-\delta^{'})\right)\right).$$

Using the lower bound

$$(\frac{1+\delta^{'}}{2})\log(1+\delta^{'}) + (\frac{1-\delta^{'}}{2})\log(1-\delta^{'}) \geq \frac{\delta^{'2}}{2+\delta^{'}}$$

yields the upper bound

$$\Pr(X \geq (1+\delta^{'})\mu) \leq \exp(-n\frac{\delta^{'2}}{2+\delta^{'}}).$$

We now state an alternative version in the following lemma.

Lemma 2.1 (Chernoff inequality)**.** *Let $X_1, \cdots, X_n$ be identically distributed independent random variables taking values in $\{0,1\}$. Let*

$$X := \sum_{i=1}^{n} X_i$$

such that $\mathbb{E}(X) = \mu$, then

$$\Pr(X \leq (1-\delta^{'})\mu) \leq \exp(-n\frac{\delta^{'^2}}{2}).$$

3. Application to counting $F(m,r)$

We now apply the Chernoff type inequality to obtain an improved upper bound for the quantity $F(m,r)$ with $r := \frac{cm}{\log m}$.

Lemma 3.1. *Let A, B, C, D be fixed steps sizes of types $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D}$ in an addition chain leading to n of length $\lfloor m+r \rfloor$. If $S(A,B,C,D,m,r)$ denotes the number of ways to choose steps of sizes A, B, C, D, then*

$$S(A,B,C,D,m,r) \leq \exp\left((\log 2 - \frac{1}{4}(1-o(1)))m + O(\frac{m}{\log m})\right).$$

Proof. Let us put the additive steps into k blocks, and set

$$(1-\delta^{'})\frac{\lfloor m+r \rfloor}{2} = k \iff \delta^{'} := 1 - \frac{2k}{\lfloor m+r \rfloor}.$$

Thus $\delta^{'} = 1 - o(1)$ as $m \longrightarrow \infty$. By Lemma 2.1, we deduce

$$\binom{\lfloor m+r \rfloor}{k} \leq 2^{m+r}\Pr(X \leq k) \leq 2^{m+r}\Pr\left(-\frac{\delta^{'^2}}{4}\lfloor m+r \rfloor\right).$$

It follows that

$$\binom{\lfloor m+r \rfloor}{k} \leq \exp\left((\log 2 - \frac{1}{4}(1-o(1)))m + O(\frac{m}{\log m})\right).$$

Using the upper bound

$$S(A,B,C,D,m,r) \leq \binom{\lfloor m+r \rfloor}{k} e^{O(r)}$$

the upper bound is immediate. □

In [1] the upper bound for $F(m,r)$ has been improved leveraging the structure of additive blocks to count only valid addition chains. The ideas espoused in [1] suggest that small steps contribute substantially to each additive block. In the same paper, it has been shown that the number of ways of choosing integers to be added in small steps is at most

$$\leq \exp\left(D\log m - D\log\log m + o(\frac{m\log\log m}{\log m})\right).$$

Using Lemma **??**, it follows that

$$N(A,B,C,D,m,r) \leq \exp\left((\log 2 - \frac{1}{4}(1-o(1)))m + O(\frac{m}{\log m})\right)$$

$$\times\exp(D\log m - D\log\log m + o(\frac{m\log\log m}{\log m})).$$

Hence

$$N(A,B,C,D,m,r) \leq \exp\left((\alpha m - D\log\log m + o(\frac{m\log\log m}{\log m})\right).$$

with

$$\alpha := c + \log 2 - \frac{1}{4}(1-o(1))$$

Using the requirement $D \gg r = \frac{cm}{\log m}$, we deduce

$$N(A,B,C,D,m,r) \leq \exp\left((\alpha m - \frac{(1-\epsilon)cm\log\log m}{\log m}\right)$$

with

$$\alpha := c + \log 2 - \frac{1}{4}(1-o(1))$$

with $0 < c < \log 2$. We finally deduce

$$F(m,r) = \sum_{A,B,C,D\leq m+r} N(A,B,C,D,m,r)$$
$$\leq \exp(\log(\mathrm{m+r}))\ \max\ (N(A,B,C,D,m,r))$$

and the upper bound follows immediately.

It follows from the preceding deduction that

Theorem 3.2. *For any small $\epsilon > 0$ and with*

$$\alpha := c + \log 2 - \frac{1}{4}(1-o(1))$$

for $0 < c < \log 2$, we have for m sufficiently large

$$F(m, c\frac{m}{\log m}) < \exp\left((\alpha m - \frac{(1-\epsilon)cm\log\log m}{\log m}\right).$$

This upper bound improves on the upper bound

$$F(m, c\frac{m}{\log m}) < \exp\left((cm + \frac{\epsilon m \log\log m}{\log m}\right)$$

in the paper [1], at the compromise of the coefficient of the leading term $0 < c < \log 2$ replaced by $\alpha := c + \log 2 - \frac{1}{4}(1 - o(1))$

References

1. J.M. De Koninck, N. Doyon and W. Verreault *On the minimal length of addition chains*, arXiv preprint arXiv:2504.07332, 2025.