ON A PROBABILISTIC ITERATED FACTOR METHOD

THEOPHILUS AGAMA

ABSTRACT. We introduce a probabilistic version of the iterated factor method introduced in our previous investigations. Let n be drawn uniformly from $\{1, 2, \dots, M\}$. Set

$$s := s(n) = \left\lfloor \frac{\sqrt{\log_2 n}}{\log \log_2 n} \right\rfloor \quad \textbf{and} \quad t(n) = \sqrt{\log \log n}$$

and

$$k_n = \left\lfloor \frac{n}{2} \right\rfloor_s .$$

Then as $N \longrightarrow \infty$ with $Z_n \sim N(0,1)$ (normally distributed) and additionally that

$$\Pr[\nu(k_n) \leq s \quad \textbf{and} \quad |Z_n| \leq t] \longrightarrow 1$$

we show that inequality

$$\iota(2^n - 1) \leq n - 1 + \log_2 n + C\sqrt{\frac{\log_2 n}{\log \log_2 n}}$$

for some absolute constant $C > 0$. This breaks the $O(\frac{\log n}{\log \log n})$ barrier that is guaranteed to be achieved using the Brauer method [1]. This result can be seen as injecting probabilistic methods into the theory of addition chains.

1. Preliminaries and setup

Theorem 1.1 (The iterated factor method). *Let $(n)_2^j$ denote the j^{th} digit in the binary expansion of n when the digits are read from right to left. For a fixed $s \geq 1$ and for all $n \geq 2$ with $n \in \mathbb{N}$, we have*

$$\iota(2^n - 1) \leq n - 1 + s - \xi(n,s) + \frac{3}{2}\sum_{j=1}^{s}(n)_2^j + \iota^*\left(\frac{1}{2}\left\lfloor \frac{n}{2} \right\rfloor_{(s-1)} - \xi(n,s)\right)$$

where

$$\xi(n,s) = \begin{cases} \frac{1}{2} & \text{if} \quad (n)_2^s = 1 \\ 0 & \text{if} \quad (n)_2^s = 0. \end{cases}$$

Date: June 18, 2025.

2010 *Mathematics Subject Classification.* Primary 11Pxx, 11Bxx; Secondary 11Axx, 11Gxx.

Key words and phrases. probabilistic, lindeberg, levy.

We now state the following version of the central limit theorem.

Lemma 1.2 (Lindeberg-Levy central limit theorem)**.** *Suppose $X_1, \ldots, X_n$ is a sequence of identically distributed independent random variables. Denote by*

$$\overline{X_n} := \frac{1}{n}\sum_{i=1}^{n} X_i$$

with $\mathrm{E}(X_i) = \mu$ (expected value) and $\mathrm{Var}[X_i] = \sigma^2$ (variance). Then, as $n \longrightarrow \infty$, the random variable $\sqrt{n}(\overline{X_n} - \mu)$ converges in distribution to $N(0, \sigma^2)$ (normal distribution). Precisely

$$\sqrt{n}(\overline{X_n} - \mu) \sim N(0, \sigma^2).$$

With

$$\overline{X_n} = \frac{1}{n}\sum_{i=1}^{n} X_i$$

we may write

$$(\sqrt{n})(\overline{X_n} - \mu) = \frac{\sqrt{n}}{n}\left(\sum_{i=1}^{n} X_i - \mu n\right) = \frac{\sum\limits_{i=1}^{n} X_i - \mu n}{\sqrt{n}} \sim N(0, \sigma^2)$$

by Lemma 1.2 as $n \longrightarrow \infty$. Therefore, we may write

$$\sum_{i=1}^{n} X_i = \mu n + \sqrt{n} Z_n + o(\sqrt{n})$$

with $Z_n \sim N(0, \sigma^2)$ as $n \longrightarrow \infty$.
Using this version of the central limit theorem, we now give a probabilistic version of the iterated factor method.

2. Main results

In this section, we extend the *iterated* factor method (Theorem 1.1) to a probabilistic version.

Theorem 2.1 (Probabilistic iterated factor method)**.** *Let n be drawn uniformly from $\{1, 2, \ldots, M\}$. Let $s := s(n)$ be a fixed integer-valued level that satisfies $1 \leq s \leq \lfloor \log_2 n \rfloor$. Put*

$$T_n = \sum_{j=1}^{s} (n)_2^j \text{ (\textbf{bit sum upto level s})}$$

and

$$k_n := \frac{1}{2}\left\lfloor \frac{n}{2} \right\rfloor_{(s-1)} - \xi(n, s)$$

with $\xi(n,s)\in\{0,\frac{1}{2}\}$. Then with high probability

$$\Pr\left[\nu(k_n)\leq \frac{s}{4}\right]\longrightarrow 1$$

as $M\longrightarrow\infty$, there is $Z_n\sim N(0,1)$ such that

$$\iota(2^n-1)\leq n-1+\log_2 n+s+\frac{3}{4}(\sqrt{s})Z_n+o(\sqrt{s}).$$

Proof. Theorem 1.1 asserts

$$\iota(2^n-1)\leq n-1+s-\xi(n,s)+\frac{3}{2}\sum_{j=1}^{s}(n)_2^j+\iota^*\left(\frac{1}{2}\left\lfloor\frac{n}{2}\right\rfloor_{(s-1)}-\xi(n,s)\right).$$

Set

$$T_n=\sum_{j=1}^{s}(n)_2^j\ (\textbf{bit sum upto level s})$$

and

$$k_n:=\frac{1}{2}\left\lfloor\frac{n}{2}\right\rfloor_{(s-1)}-\xi(n,s)$$

with $\xi(n,s)\in\{0,\frac{1}{2}\}$. We remark that $(n)_2^j\sim\text{Bernouli}(\frac{1}{2})$ so that

$$T_n:=\sum_{j=1}^{s}(n)_2^j\sim\text{Bi}(s,\frac{1}{2}).$$

Thus $\mathbb{E}[(n)_2^j]=\frac{1}{2}$ and $\text{Var}[(n)_2^j]=\text{E}[((n)_2^j)^2]-(\text{E}[(n)_2^j])^2=\frac{1}{4}$. By using Lemma 1.2, we deduce

$$T_n=\frac{s}{2}+\frac{\sqrt{s}}{2}Z_n+o(\sqrt{s})$$

with $Z_n\sim N(0,1)$. Plugging this information into the preceding inequality (Theorem 1.1), we obtain further

$$\iota(2^n-1)\leq n-1+\frac{7}{4}s+\frac{3}{4}\sqrt{s}Z_n+o(\sqrt{s})+\iota^*(k_n).$$

Now $k_n\leq\frac{n}{2^s}\iff\log_2 k_n\leq\log_2 n-s$. Using the inequality $\iota^*(k_n)\leq\log_2 k_n+\nu(k_n)-1$, then with high probability

$$\Pr\left[\nu(k_n)\leq\frac{s}{4}\right]\longrightarrow 1$$

as $M\longrightarrow\infty$, we deduce

$$\iota^*(k_n)\leq\log_2 n-\frac{3}{4}s-1.$$

Plugging this inequality yields the inequality

$$\iota(2^n-1)\leq n-1+\log_2 n+s+\frac{3}{4}\sqrt{s}Z_n+o(\sqrt{s})$$

which is the probabilistic version claimed. □

We note that existing methods only yield the inequality

$$\iota(2^n - 1) \leq n - 1 + \log_2 n + \nu(n) - 1$$

which yields

$$\iota(2^n - 1) \leq n - 1 + \log_2 n + D\frac{\log n}{\log\log n}$$

for some constant $D > 0$ under the assumption of the method. We now have the following consequence which breaks the $O(\frac{\log n}{\log\log n})$ barrier that is guaranteed to be achieved using the Brauer method. It reduces the error term to $O(\sqrt{\frac{\log n}{\log\log n}})$ in this probabilistic regime at the compromise of having a few exceptions. This result can be seen as injecting probabilistic methods into the theory of addition chains. We have the following immediate consequence.

Corollary 2.2. *Let n be drawn uniformly from $\{1, 2, \ldots, N\}$. Define*

$$s := s(n) = \left\lfloor \frac{\sqrt{\log_2 n}}{\log\log_2 n} \right\rfloor$$

and

$$t(n) = \sqrt{\log\log n}$$

and

$$k_n := \frac{1}{2}\left\lfloor \frac{n}{2} \right\rfloor_{(s-1)} - \xi(n, s)$$

with $\xi(n, s) \in \{0, \frac{1}{2}\}$. Then as $N \longrightarrow \infty$ with high probability

$$\Pr\left[\nu(k_n) \leq \frac{s(n)}{4} \quad \textbf{and} \quad |Z_n| \leq t(n)\right] \longrightarrow 1$$

there exists an absolute constant $C > 0$ such that

$$\iota(2^n - 1) \leq n - 1 + \log_2 n + C\sqrt{\frac{\log n}{\log\log n}}.$$

Theorem 2.3 (Conditional second moment bounds)**.** *Let n be drawn uniformly from $\{1, 2, \ldots, M\}$. Let $s := s(n)$ be a fixed integer-valued level that satisfies $1 \leq s \leq \lfloor \log_2 n \rfloor$. Put*

$$k_n := \frac{1}{2}\left\lfloor \frac{n}{2} \right\rfloor_{(s-1)} - \xi(n, s)$$

with $\xi(n,s) \in \{0, \frac{1}{2}\}$*. Set* $X_n := \iota(2^n - 1)$ *and define*

$$G_n := \left\{\nu(k_n) \leq \frac{s}{4}\right\}$$

and assume that

$$\Pr[G_n] \longrightarrow 1$$

as $M \longrightarrow \infty$ *then*

(i)

$$\mathbb{E}[X_n \mid G_n] \leq n + \log_2 n + s(n) + o(\sqrt{s(n)})$$

(ii)

$$\mathrm{Var}[X_n \mid G_n] \leq \frac{9}{8}s(n) + o(\sqrt{s(n)}).$$

Proof. We know that there exists a $Z_n \sim N(0,1)$ such that with $\Pr[G_n] \longrightarrow 1$ then

$$\iota(2^n - 1) \leq n + \log_2 n + s(n) + \frac{3}{4}\sqrt{s(n)}Z_n + o(\sqrt{s(n)})$$

when n is drawn uniformly from $\{1, 2, \ldots, M\}$. By the linearity and monotonicity properties of expectation $\mathbb{E}(\cdot)$, we have

$$\mathbb{E}[X_n \mid G_n] \leq n + \log_2 n + s(n) + o(\sqrt{s(n)})$$

since $\mathbb{E}[Z_n] = 0$. This proves (i).

Let $\mathbb{E}[X_n] = \mu_n$ then $\mathrm{Var}[X_n \mid G_n] = \mathbb{E}[(X_n - \mu_n)^2 \mid G_n]$. We have

$$\mathrm{Var}[X_n \mid G_n] = \mathrm{Var}\left[\frac{3}{4}\sqrt{s(n)} + o(\sqrt{s(n)})\right]$$

by invariance of the variance $\mathrm{Var}[\cdot]$ perturbed by a deterministic parameter. Using the doubly sub-additive property of $\mathrm{Var}[\cdot]$, we have

$$\mathrm{Var}[X_n \mid G_n] \leq \frac{9}{8}s(n) + o(s(n))$$

which proves (ii). □

References

1. A. Brauer, *On addition chains*, Bulletin of the American mathematical Society, vol. 45:10, 1939, 736–739.

Departement de mathematiques et de statistique, Universite Laval, Quebec, Canada

E-mail address: thaga1@ulaval.ca/Theophilus@aims.edu.gh/emperordagama@yahoo.com