A COIN TOSSING ALGORITHM FOR COUNTING LARGE NUMBERS OF EVENTS

PETER KIRSCHENHOFER AND HELMUT PRODINGER

Department of Algebra and Discrete Mathematics
Technical University of Vienna, Austria

1. Introduction

"Approximate counters" are realized by probabilistic algorithms that maintain an approximate count in the interval 1 to n using only about $\log_2 \log_2 n$ bits. The algorithmic principle was proposed by R. Morris [7]:

Starting with counter $C = 1$, after n increments C should contain a good approximation to $\log_2 n$. Thus C should be increased by 1 after another n increments approximately. Since only C is known the algorithm has to base its decision on the content of C alone.

The principle to increment the counter is now

$$C := C + \begin{cases} 0 \text{ with probability } 1 - 2^{-C} \\ 1 \text{ with probability } 2^{-C} \end{cases} \qquad (*)$$

Flajolet [2] has analyzed this algorithm in detail; another method of analysis has been proposed by the authors [4]. In [2; p.127ff] Flajolet also discusses variants of the incremental procedure (*), essentially replacing base 2 by base a. For $a < 2$ a smoother behaviour of the counter is obtained.

The aim of this paper is twofold.

(i) On the one hand we substitute (*) by an incremental process that adds $\frac{1}{b}$ to the counter with suitable probability. For $a = 2^{1/b}$ the resulting "automaton" (compare Fig. 1) is closely related to Flajolet's smoothing procedure just described. Nevertheless we point out that our algorithm is slightly more general and flexible enough to deal with a related problem described below.

(ii) On the other hand we describe a simple coin tossing algorithm that simulates the probabilities in (*). We compare the results on this algorithm with another one whose analysis is closely related to a problem studied by Knuth in the context of binary addition [6]. It turns out that the variance in our instance is significantly smaller.

1991 *Mathematics Subject Classification.* 68Q25.

Key words and phrases. Probabilistic Algorithms, Analysis of Algorithms, Asymptotic Expansions.

In Section 2 of this paper we present the analysis of the general incremental principle mentioned in (i) above.

Section 3 refers to the coin tossing problems mentioned in (ii). It turns out that the analysis of the behaviour of these algorithms is essentially (i.e. with neglectible error terms) covered by the analysis of Section 2.

2. A general incremental procedure

We consider the following incremental procedure. Starting with $C' = 1$ we increment as follows (b is a fixed natural number, $0 < d < 2^{1/b}$).

$$C' := C' + \begin{cases} 0 \text{ with probability } \ 1 - d \cdot 2^{-C'/b} \\ 1 \text{ with probability } \ d \cdot 2^{-C'/b} \end{cases}$$

(The constant d will be chosen appropiately later on.) To get a good approximation for $\log_2 n$ it is meaningful to rescale the countervalues of counter C' by considering

$$C = 1 + \frac{C' - 1}{b}.$$

A reformulation of the incremental procedure in terms of C reads

$$C := C + \begin{cases} 0 \text{ with probability } \ 1 - d \cdot 2^{-C-\frac{1}{b}+1} \\ \dfrac{1}{b} \text{ with probability } \ d \cdot 2^{-C-\frac{1}{b}+1} \end{cases} \tag{**}$$

We denote for abbreviation the possible counter values of C by

$$c_j = 1 + \frac{j-1}{b}, \qquad j = 1, 2, 3, \cdots .$$

Then we have for the *transition* $c_j \longrightarrow c_{j+1}$ the *probability* $d \cdot 2^{-j/b}$. In the following we set

$$a = 2^{1/b}.$$

In order to illustrate the above concept we may use the following "automaton":

Fig. 1

The reader might observe that the instance $d = 1$ is the instance studied by Flajolet in [2;p.127ff]. In the following derivation we digress from Flajolet's analysis after having established the probabilities as in formula (6). Instead of Flajolet's

Mellin-type analysis we use a contour integral representation for the alternating sums coming up (compare Lemma 1).

Let $p_{n,l}$ denote the probability to reach "state" c_l in n steps and $H_l(z)$ the corresponding probability generating function, i.e.

$$H_l(z) = \sum_{n\ge 0} p_{n,l} z^n. \tag{1}$$

With $\alpha_i = 1 - da^{-i}$ it follows immediately from Figure 1 that

$$\begin{aligned} H_l(z) &= \frac{1}{1-\alpha_1 z}\cdot da^{-1}z\cdot\frac{1}{1-\alpha_2 z}\cdot da^{-2}z\ldots\frac{1}{1-\alpha_l z} \\ &= d^{l-1}a^{-\binom{l}{2}}z^{l-1}\prod_{i=1}^{l}\frac{1}{1-\alpha_i z}. \end{aligned} \tag{2}$$

Let

$$H_l(z) = \sum_{j=1}^{l}\frac{A_{l,j}}{1-\alpha_j z} \tag{3}$$

denote the partial fraction decomposition of $H_l(z)$. It is a straightforward computation to derive

$$A_{l,j} = \frac{(-1)^{l-j}\,a^{-\binom{l-j}{2}}}{Q_{j-1}(a)Q_{l-j}(a)}, \tag{4}$$

where

$$Q_i(a) = \big(1-\frac{1}{a}\big)\big(1-\frac{1}{a^2}\big)\ldots\big(1-\frac{1}{a^i}\big). \tag{5}$$

From (3) and (4) we find (interchanging j and $l-j$)

$$p_{n,l} = \sum_{j=0}^{l-1}\frac{(-1)^j\,a^{-\binom{j}{2}}}{Q_j(a)\,Q_{l-1-j}(a)}\left(1-da^{j-l}\right)^n \ . \tag{6}$$

By the binomial theorem we may express $p_{n,l}$ by an *alternating sum*:

$$p_{n,l} = \sum_{k=0}^{n}\binom{n}{k}(-1)^k d^k \sum_{j=0}^{l-1}\frac{(-1)^j}{Q_j(a)Q_{l-1-j}(a)}\cdot a^{-\binom{j}{2}+(j-l)k}$$

Using Euler's famous partition identities [1]

$$\sum_{j\ge 0}\frac{(-1)^j a^{-\binom{j}{2}}t^j}{Q_j(a)} = \prod_{m\ge 0}\left(1-\frac{t}{a^m}\right) \tag{7}$$

and

$$\sum_{j\ge 0}\frac{t^j}{Q_j(a)} = \prod_{m\ge 0}\left(1-\frac{t}{a^m}\right)^{-1}, \tag{8}$$

the second sum in $p_{n,l}$ may be associated to a product.

$$p_{n,l} = \sum_{k=0}^{n} \binom{n}{k} (-1)^k \left(\frac{d}{a}\right)^k [t^{l-1}] \prod_{m=0}^{k-1} \left(1 - \frac{t}{a^m}\right) \tag{9}$$

For the expectation E_n of the value of the counter C after n steps we find

$$E_n = \sum_{l \geq 1} p_{n,l} \cdot c_l = 1 + \frac{1}{b} \sum_{k=0}^{n} \binom{n}{k} (-1)^k \left(\frac{d}{a}\right)^k \sum_{l \geq 0} l \; [t^l] \prod_{m=0}^{k-1} \left(1 - \frac{t}{a^m}\right)$$

Now $\sum_{l \geq 0} l[t^l]f(t) = f'(1)$, so that

$$E_n = 1 - \frac{1}{b} \sum_{k=1}^{n} \binom{n}{k} (-1)^k \left(\frac{d}{a}\right)^k Q_{k-1}(a) = 1 - \frac{1}{b}\Sigma_n \tag{10}$$

An asymptotic evaluation of an alternating sum as in (10) may be performed using the following

Lemma 1. [8] *Let $\mathcal{C}$ be a curve surrounding the points $s, s+1, \ldots, n$ $(s \in \mathbb{N})$ in the complex plane and let $f(z)$ be analytic inside $\mathcal{C}$. Then*

$$\sum_{k=s}^{n} \binom{n}{k} (-1)^k f(k) = -\frac{1}{2\pi i} \int_{\mathcal{C}} [n; z] f(z) dz,$$

where

$$[n; z] = \frac{(-1)^{n-1} n!}{z(z-1)\ldots(z-n)}. \quad \square$$

Extending the contour of integration it turns out that under suitable growth conditions on $f(z)$ (compare [3]) the asymptotic expansion of the alternating sum is given by

$$\sum \mathrm{Res}\left([n; z]f(z)\right) + O\left(n^{\sigma+\varepsilon}\right), \quad \text{any } \varepsilon > 0$$

where the sum is taken over all poles z_0 different from $s, \ldots, n$ with $\Re z_0 > \sigma$.

In our sum we have $s = 1$ and $f(k) = \left(\frac{d}{a}\right)^k Q_{k-1}(a)$, which may be continued analytically by

$$f(z) = \left(\frac{d}{a}\right)^z Q_{z-1}(a), \quad \text{where} \quad Q_z(a) = \frac{Q_\infty(a)}{\prod_{j \geq 1} \left(1 - \frac{1}{a^{z+j}}\right)}.$$

In order to find the residues of $[n; z]f(z)$ at the double pole $z = 0$ we use the local expansions

$$[n; z] \sim -\frac{1}{z}(1 + zH_n)$$

$$\left(\frac{d}{a}\right)^z \sim 1 + z \log\left(\frac{d}{a}\right)$$

$$Q_{z-1}(a) \sim \frac{1}{z \log a} \left(1 + z(\log a)\left(\frac{1}{2} - \alpha_a\right)\right) \quad \text{where} \quad \alpha_a = \sum_{k \geq 1} \frac{1}{a^k - 1}.$$

With $\log a = \frac{1}{b}\log 2$ we have the following contribution $\Sigma_{n,0}$ to Σ_n:

$$-\Sigma_{n,0} = \log_a n + \frac{\gamma}{\log a} + \log_a d - \frac{1}{2} - \alpha_a \tag{11}$$

Near the simple poles $z_k = \frac{2k\pi i}{\log a} = \chi_k(a)$, $k \in \mathbb{Z}$, $k \neq 0$, we have the expansions

$$\begin{aligned}
[n; z] &\sim n^{\chi_k(a)} \cdot \Gamma\big(-\chi_k(a)\big) = e^{2k\pi i \cdot \log_a n} \cdot \Gamma\big(-\chi_k(a)\big) \\
\big(\frac{d}{a}\big)^z &\sim e^{\chi_k(a) \cdot \log d} \\
Q_{z-1}(a) &\sim \frac{1}{\log a} \cdot \frac{1}{z - \chi_k(a)},
\end{aligned}$$

so that the poles z_k yield the following fluctuating contribution $\Sigma_{n,k}$ to Σ_n :

$$\Sigma_{n,k} = \frac{1}{\log a}\Gamma\big(-\chi_k(a)\big)e^{2k\pi i \cdot \log_a(nd)}$$

In total we have

Theorem 2. *The expected value E_n of the counter C after n random increments with the generalized incremental procedure (**) fulfills*

$$E_n = \log_2 n + \frac{\gamma}{\log 2} + \log_2 d + 1 - \frac{1}{2b} - \frac{\alpha_a}{b} + \delta_1\big(\log_a n + \Delta\big) + O\left(n^{-1}\right)$$

where

$$\alpha_a = \sum_{k \geq 1} \frac{1}{a^k - 1}, \qquad a = 2^{1/b}$$

and the periodic function

$$\delta_1(x) = -\frac{1}{\log 2}\sum_{k \neq 0} \Gamma\big(-\chi_k(a)\big)e^{2k\pi i x},$$

where

$$\chi_k(a) = \frac{2k\pi i}{\log a} \qquad \text{and} \qquad \Delta = \log_a d. \quad \square$$

Since

$$|\Gamma(iy)|^2 = \frac{\pi}{y \cdot \sinh(\pi y)},$$

we have $\left|\Gamma\big(-\chi_k(a)\big)\right|^2 = O\left(be^{-\frac{2\pi^2 b}{\log 2}}\right)$ for $b \to \infty$, so that the fluctuating term, which is already very small for the classical case $b = 1$, becomes even smaller for b getting large.

In order to find the appropriate value for the constant d we consider the expectation S_n of 2^C after n random increments:

$$S_n = \sum_l p_{n,l} 2^{c_l} \tag{12}$$

Since

$$p_{n,l} = p_{n-1,l}\left(1 - da^{-l}\right) + p_{n-1,l-1}da^{1-l} \tag{13}$$

we have

$$S_n = S_{n-1} - \frac{2d}{a} + 2d, \quad n \geq 1; \quad S_0 = 2;$$

and thus

$$S_n = 2d\big(1 - \frac{1}{a}\big)n + 2. \tag{14}$$

A good choice for d is therefore

$$d = \frac{a}{2(a-1)}, \tag{15}$$

so that $S_n = n + 2$.

Nevertheless we can analyze the *variance* V_n of the content of C after n steps for arbitrary d in an analogous manner as the expectation E_n. Omitting the technical details we obtain, neglecting periodic fluctuations of mean 0,

$$V_n \sim \frac{\pi^2}{6\log^2 2} - \frac{\beta_a}{b^2} - \frac{\alpha_a}{b^2} + \frac{1}{12b^2} - \left[\delta_1^2\right]_0, \tag{16}$$

where $\left[\delta_1^2\right]_0$ is the mean of the square of the periodic function $\delta_1(x)$ defined in Theorem 2.

In order to study the influence of b on V_n, it is helpful to make use of the following remarkable transformation of the constant in (16): We have

$$\alpha_a + \beta_a = \sum_{k\geq 1} \frac{a^k}{\left(a^k - 1\right)^2} = h_1(\log a),$$

where

$$h_1(x) = \sum_{k\geq 1} \frac{e^{kx}}{\left(e^{kx} - 1\right)^2}. \tag{17}$$

Now it follows from Dedekind's functional equation for the η-function that

$$h_1(x) = \frac{\pi^2}{6x^2} - \frac{1}{2x} + \frac{1}{24} - \frac{4\pi^2}{x^2}h_1\Big(\frac{4\pi^2}{x}\Big)$$

(compare [5]; observe the typo therein). Thus we have

$$\alpha_a + \beta_a = \frac{\pi^2}{6\log^2 a} - \frac{1}{2\log a} + \frac{1}{24} - \frac{4\pi^2}{\log^2 a}h_1\Big(\frac{4\pi^2}{\log a}\Big). \tag{18}$$

On the other hand, again using $\left|\Gamma(iy)\right|^2 = \dfrac{\pi}{y \cdot \sinh(\pi y)}$, we get

$$\left[\delta_1^2\right]_0 = \frac{\log a}{\log^2 2} \sum_{k\geq 1} \frac{1}{k \cdot \sinh\left(\frac{2k\pi^2}{\log a}\right)} = \frac{2\log a}{\log^2 2} h_2\Big(\frac{2\pi^2}{\log a}\Big) \tag{19}$$

with

$$h_2(x) = \sum_{k\geq 1} \frac{(-1)^{k-1}}{k\left(e^{kx} - 1\right)}. \tag{20}$$

Combining (18) and (19) and regarding $\log a = \frac{\log 2}{b}$, we finally have

Theorem 3. *The variance V_n of the content of the counter C after n steps of the generalized incremental procedure (**) fulfills*

$$V_n = \frac{1}{2b\log 2} + \frac{1}{24b^2} + \frac{4\pi^2}{\log^2 2} h_1\Big(\frac{4\pi^2 b}{\log 2}\Big) - \frac{2}{b\log 2} h_2\Big(\frac{2\pi^2 b}{\log 2}\Big)$$
$$+ \delta_3\big(\log_a n + \Delta\big) + O\Big(\frac{\log n}{n}\Big)$$

where $h_1(x)$ and $h_2(x)$ are defined in (23) and (26), and where $\delta_3(x)$ is a periodic function of mean zero, and $\Delta = \log_a d$. $\square$

$\delta_3(x)$ is a combination of $\delta_1(x)$ and $\delta_2(x)$, whose Fourier coefficients could be computed in principle.

The reader should note that the main term is of order b^{-1} in b; the values $h_1\big(\frac{4\pi^2 b}{\log 2}\big)$ resp. $h_2\big(\frac{2\pi^2 b}{\log 2}\big)$ tend to 0 exponentially fast in b! The result quantifies the smoother behaviour of the approximate counting procedure for increasing b. For $d = 1$ Theorem 3 should be compared with Flajolet's result [2;eq.(50)], where only the leading term $\frac{1}{2b\log 2}$ appears.

3. Approximate Counting by Coin Tossings

In this section we apply the previous results to the analysis of an approximate counting algorithm where the incremental procedure (*) is simulated by *coin tossings*. We flip a fair coin and increase the counter C by 1 after having seen C *consecutive heads* occurring *since the previous incremental step.* More formally the set of sequences yielding a counter $C = l$ is described by the *regular expression*

$$0^*1\{0,10\}^*11\{0,10,110\}^*\ldots 1^{l-1}\{0,10,\ldots,1^{l-1}0\}^*\{\varepsilon,1,\ldots,1^{l-1}\}.$$

The corresponding generating function equals

$$F_l(z) = \frac{1-z^l}{(1-z)^2} z^{\binom{l}{2}} \prod_{j=1}^{l-1} \frac{1-z}{1-2z+z^{j+2}}, \quad l \ge 1, \tag{21}$$

so that the probability $p_{n,l}$ that counter $C = l$ after n tossings is

$$p_{n,l} = 2^{-n}\,[z^n]\,F_l(z). \tag{22}$$

It is our aim to show that the analysis of this coin tossing algorithm may be reduced to the analysis of Section 2 by approximating the probabilities $p_{n,l}$ step by step.

For $l \ge 2$, $F_l(z)$ is a rational function having $l-1$ first order poles $\rho_1,\ldots,\rho_{l-1}$ of absolute value $\le \frac{3}{4}$: For z traversing the circle $|z| = \frac{3}{4}$ the value of $1-2z+z^{j+2}$ winds around the origin exactly once, so that $1-2z+z^{j+2}$ has exactly one root ρ_j in $|z| \le \frac{3}{4}$. For later purposes we note that $|1-2z+z^{j+2}| \ge \big|-\frac{1}{2}+(\frac{3}{4})^3\big| = \frac{5}{64}$ for $j \ge 1$ and $|z| = \frac{3}{4}$. Therefore

$$|F_l(z)| \le C_1\Big(\frac{3}{4}\Big)^{\binom{l}{2}}\Big(\frac{7}{4}\Big)^{l-1}\Big(\frac{64}{5}\Big)^{l-1} = O\left(\eta^{\binom{l}{2}}\right) \quad \text{for any } \eta > \frac{3}{4}. \tag{23}$$

The reader should observe that because of

$$2\rho_j = 1 + \rho_j^{j+2} \tag{24}$$

ρ_j will be close to $1/2$ for j getting large. More precisely, using *Lagrange's inversion formula*, we have

$$\rho_j = \frac{1}{2}\left(1 + \sum_{k\geq 1}\frac{1}{k}\binom{k(j+2)}{k-1}\frac{1}{2^{k(j+2)}}\right) = \frac{1}{2}\left(1 + \frac{1}{2^{j+2}} + \dots\right). \tag{25}$$

Now it follows that

$$2^n p_{n,l} = -\sum_{j=1}^{l-1}\operatorname{Res}\big(F_l(z); z=\rho_j\big)\rho_j^{-n-1} + \frac{1}{2\pi i}\int_{|z|=\frac{3}{4}} F_l(z)\frac{dz}{z^{n+1}},$$

where the integral is $O\left(\eta^{\binom{l}{2}}\left(\frac{4}{3}\right)^n\right)$ for any $\eta > \frac{3}{4}$, with an absolute O–constant. From this observation it is immediate that $p_{n,l}$ may be substituted by

$$q_{n,l} = -\sum_{j=1}^{l-1}\operatorname{Res}\big(F_l(z); z=\rho_j\big)\rho_j^{-1}\left(2\rho_j\right)^{-n} \tag{26}$$

with exponentially small errors in expectation and variance. The computation of the residues gives

$$\operatorname{Res}\big(F_l(z); z=\rho_j\big) = \frac{\left(1-\rho_j^l\right)\rho_j^{\binom{l}{2}}\left(1-\rho_j\right)^{l-1}}{\left(1-\rho_j\right)^2\left(-2+(j+2)\rho_j^{j+1}\right)}A_j\,B_{j,l}$$

where (compare (24)!)

$$\begin{aligned}
A_j\left(1-\rho_j\right)^{-2} &= \prod_{i=0}^{j-1}\left(1-2\rho_j+\rho_j^{i+2}\right)^{-1} = \prod_{i=0}^{j-1}\left(\rho_j^{i+2}-\rho_j^{j+2}\right)^{-1}\\
&= \rho_j^{1-\binom{j+2}{2}}\Big/ Q_j\left(\rho_j^{-1}\right),\\
B_{j,l} &= \rho_j^{-(j+2)(l-1-j)}(-1)^{l-1-j}\Big/ Q_{l-1-j}\left(\rho_j^{-1}\right).
\end{aligned}$$

Using formula (24) it can be shown by some straightforward algebra that

$$\begin{aligned}
q_{n,l} &= \sum_{j=1}^{l-1}\frac{\left(1-\rho_j^l\right)\left(1-\rho_j^{j+1}\right)^{l-1}}{\left(1-(j+1)\rho_j^{j+2}\right)}\frac{(-1)^{l-1-j}\rho_j^{\binom{l-1-j}{2}}}{Q_j\left(\rho_j^{-1}\right)Q_{l-1-j}\left(\rho_j^{-1}\right)}\left(2\rho_j\right)^{-n}\\
&= \sum_{j=1}^{l-1} a_{l,j}\left(2\rho_j\right)^{-n}, \qquad \text{say.}
\end{aligned} \tag{27}$$

This formula suggests the quantity

$$r_{n,l} = \sum_{j=1}^{l-1} \frac{(-1)^{l-1-j} 2^{-\binom{l-1-j}{2}}}{Q_j Q_{l-1-j}} (2\rho_j)^{-n} = \sum_{j=1}^{l-1} b_{l,j} (2\rho_j)^{-n}, \quad \text{where } Q_k = Q_k(2), \tag{28}$$

as a good approximation of $q_{n,l}$. Indeed, we have

$$\sum_{l \geq j+1} l a_{l,j} = \frac{\left(1-\rho_j^{j+1}\right)^j}{\left(1-(j+1)\rho_j^{j+2}\right) Q_j\left(\rho_j^{-1}\right)} \sum_{l \geq 0} (l+j+1) s_{l,j}$$

with

$$s_{l,j} = \left(1-\rho_j^{j+1}\rho_j^l\right)\left(1-\rho_j^{j+1}\right)^l (-1)^l \rho_j^{\binom{l}{2}} \Big/ Q_l\left(\rho_j^{-1}\right). \tag{29}$$

Using Euler's identity (7)

$$\sum_{l \geq 0} s_{l,j} = \prod_{m \geq 0}\left(1-(1-\rho_j^{j+1})\rho_j^m\right) - \rho_j^{j+1} \prod_{m \geq 0}\left(1-(1-\rho_j^{j+1})\rho_j^{m+1}\right) = 0. \tag{30}$$

Differentiating formula (7) we have

$$\sum_{l \geq 0} l \frac{(-1)^l a^{-\binom{l}{2}} t^l}{Q_l(a)} = -t\left(\sum_{m \geq 0} \frac{1}{a^m - t}\right) \prod_{m \geq 0}\left(1-\frac{t}{a^m}\right), \tag{31}$$

so that, after a short computation,

$$\sum_{l \geq 0} l s_{l,j} = -\left(1-\rho_j^{j+1}\right) \prod_{m \geq 1}\left(1-(1-\rho_j^{j+1})\rho_j^m\right). \tag{32}$$

Altogether

$$\sum_{l \geq j+1} l a_{l,j} = -\frac{\left(1-\rho_j^{j+1}\right)^{j+1}}{\left(1-(j+1)\rho_j^{j+2}\right) Q_j\left(\rho_j^{-1}\right)} \prod_{m \geq 1}\left(1-(1-\rho_j^{j+1})\rho_j^m\right). \tag{33}$$

In the same way we derive

$$\sum_{l \geq j+1} l\, b_{l,j} = -\frac{Q_\infty}{Q_j}, \quad \text{where} \quad Q_\infty = Q_\infty(2),\ Q_j = Q_j(2). \tag{34}$$

The sum is up to a factor $1 + O(j2^{-j})$ the right hand side of (33). Therefore the series

$$\sum_{j \geq 1} (2\rho_j)^{-n} \sum_{l \geq j+1} l\,(a_{l,j} - b_{l,j})$$

converges absolutely and may be rearranged as $\sum_{l\ge 1} l\big(q_{n,l} - r_{n,l}\big)$.

It is easily seen that $\sum_{j\ge 1}(2\rho_j)^{-n}O(2^{-j})$ is $o(1)$ for $n \to \infty$. In order to get a sharper estimate we may apply Lemma 1: We have $(2\rho_j)^{-1} = 1 - \delta_j$, where $\delta_j = O(2^{-j})$ so that

$$\sum_{j\ge 1}(2\rho_j)^{-n}\, O(2^{-j}) = \sum_{k=0}^{n}\binom{n}{k}(-1)^k f(k)$$

with $f(k) = \sum_{j\ge 1}\delta_j^k O(2^{-j})$. Since $\sum_{j\ge 1}\delta_j^z O(2^{-j})$ defines an analytic function for $\Re z > -1$ we find from Lemma 1 that the whole sum is $O(n^{-1+\varepsilon})$ for any $\varepsilon > 0$.

Thus the expectation E_n of the content of the counter C after n tossings fulfills

$$\begin{aligned} E_n &= \sum_{l\ge 1} l q_{n,l} + O\Big(\big(\frac{2}{3}\big)^n\Big) = \sum_{l\ge 1} l r_{n,l} + \sum_{l\ge 1} l\big(q_{n,l} - r_{n,l}\big) + O\Big(\big(\frac{2}{3}\big)^n\Big) \\ &= \sum_{l\ge 1} l r_{n,l} + O(n^{-1+\varepsilon}), \quad \text{any } \varepsilon > 0. \end{aligned}$$

In order to evaluate $\sum_{l\ge 1} l\, r_{n,l}$ we approximate $(2\rho_j)^{-1}$ by $1 - 2^{-j-2}$ (compare (25)):

$$\begin{aligned} \Delta_n &= \sum_{j\ge 1}\Big((2\rho_j)^{-n} - \big(1 - 2^{-j-2}\big)^n\Big)\frac{Q_\infty}{Q_j} \\ &= \sum_{k=1}^{n}\binom{n}{k}(-1)^k \sum_{j\ge 1}\Big(\delta_j^k - 2^{-(j+2)k}\Big)\frac{Q_\infty}{Q_j} \end{aligned}$$

where $(2\rho_j)^{-1} = 1 - \delta_j$. From (31) we have $\delta_j^k - 2^{-(j+2)k} = O(j2^{-2j}k2^{-j(k-1)}) = O(kj2^{-j(k+1)})$ so that $f(z) = \sum_{j\ge 1}\Big(\delta_j^z - 2^{-(j+2)z}\Big)\frac{Q_\infty}{Q_j}$ is again an analytic function for $\Re z > -1$. Since $f(0) = 0$, $[n;z]f(z)$ has a removable singularity at $z = 0$ and $\Delta_n = O(n^{-1+\varepsilon})$, any $\varepsilon > 0$.

We finally have

$$\begin{aligned} E_n &= \sum_{l\ge 1} l\, r_{n,l} + O(n^{-1+\varepsilon}) = \sum_{l\ge 1} l \sum_{j=1}^{l-1} b_{l,j}\,(2\rho_j)^{-n} + O(n^{-1+\varepsilon}) \\ &= \sum_{l\ge 1} l \sum_{j=1}^{l-1} b_{l,j}\,\big(1 - 2^{-j-2}\big)^n + O(n^{-1+\varepsilon}) \\ &= \sum_{l\ge 1} l\, t_{n,l} - \sum_{l\ge 1} l b_{l,0}\big(\frac{3}{4}\big)^n + O(n^{-1+\varepsilon}) \\ &= \sum_{l\ge 1} l\, t_{n,l} + O(n^{-1+\varepsilon}) \end{aligned} \tag{35}$$

where $t_{n,l}$ coincides with $p_{n,l}$ from (6) for $a = 2$, $d = \frac{1}{2}$. Therefore E_n from this section coincides with E_n from Section 2 with an error of order $O(n^{-1+\varepsilon})$. The same result may be proved for the variance V_n by an analogous reasoning.

Theorem 4. *The expected value E_n of counter C after n coin tossings fulfills*

$$E_n = \log_2 n + \frac{\gamma}{\log 2} - \frac{1}{2} - \alpha + \delta_1\big(\log_2 n\big) + O\left(n^{-1+\varepsilon}\right), \quad \text{any } \varepsilon > 0,$$

with

$$\alpha = \sum_{k\ge 1} \frac{1}{2^k - 1} \approx 1.6066\ldots.$$

The variance V_n fulfills for any $\varepsilon > 0$

$$V_n = \frac{1}{2\log 2} + \frac{1}{24} + \frac{4\pi^2}{\log^2 2} h_1\Big(\frac{4\pi^2}{\log 2}\Big) - \frac{2}{\log 2} h_2\Big(\frac{2\pi^2}{\log 2}\Big) + \delta_3\big(\log_2 n\big) + O\left(n^{-1+\varepsilon}\right) \approx 0.7630\ldots$$

with $\delta_1, \delta_3, h_1, h_2$ from Theorems 2 and 3.

Theorem 4 shows that our coin tossing algorithm is a very good simulation of the general incremental procedure mentioned in the first two sections with parameters $b = 1$, $d = 1/2$.

We finally compare these results with the following alternative variant of a coin tossing algorithm: The Counter C is incremented by 1 if after another flipping of the coin the sequence ends up with a run of C ones. With other words, C maintains 1 plus the length of the longest run of ones. Results on this problem may be found e.g. in [9], [10]; the analysis is closely related to Knuth's analysis of the average time for carry propagation in binary addition [6]. Intuitively it is clear that the latter proposal leads to a less smooth behaviour than our algorithm from above.

The regular expression corresponding to the set of sequences yielding a counter $C \le l$ is

$$\{0, 10, \ldots, 1^{l-1}0\}^* \{\varepsilon, 1, \ldots, 1^{l-1}\}$$

with corresponding generating function

$$F_l(z) = \frac{1 - z^l}{1 - 2z + z^{l+1}}.$$

The dominating singularity is ρ_{l-1}, where ρ_j fulfills (24). In Knuth's analysis [6] the corresponding generating function is

$$G_l(z) = \frac{1}{1 - 2z + \frac{1}{2}z^l}.$$

The dominating singularity τ_{l-1} of $G_l(z)$ fulfills $\tau_{l-1} = \rho_{l-1} + O(l2^{-2l})$, so that Knuth's asymptotic result on the expectation covers the coin tossing problem, too. For comparison we cite the results from [6] and [10]:

Expectation E_n and variance V_n of the counter C in the modified algorithm are asymptotic to (neglecting the small periodic fluctuations of mean zero)

$$\begin{aligned} E_n &\sim \log_2 n + \frac{\gamma}{\log 2} - \frac{1}{2}, \\ V_n &\sim \frac{\pi^2}{6\log^2 2} + \frac{1}{12} - \left[\delta_1^2\right]_0 \approx 3.5070\ldots \end{aligned} \tag{36}$$

with δ_1 from Theorem 2. Comparing with (16) we find that the variance in our algorithm is smaller by $\alpha + \beta = \sum_{k\ge1} \frac{2^k}{(2^k-1)^2} \approx 2.7440\ldots$.

References

1. G. E. Andrews, *The Theory of Partitions*, Addison Wesley, 1976.
2. P. Flajolet, *Approximate Counting: A Detailed Analysis*, BIT **25** (1985), 113–134.
3. P. Flajolet and R. Sedgewick, *Digital Search Trees Revisited*, SIAM J. Comput. **15** (1986), 748–767.
4. P. Kirschenhofer and H. Prodinger, *Approximate Counting: An Alternative Approach*, RAIRO Informatique Théorique et Applications **25** (1991), 43–48.
5. P. Kirschenhofer, H. Prodinger, and J. Schoißengeier, *Zur Auswertung gewisser numerischer Reihen mit Hilfe modularer Funktionen*, Zahlentheoretische Analysis II (E. Hlawka, ed.), Lecture Notes in Math. 1262, Springer, Berlin, 1987, pp. 108–110.
6. D. E. Knuth, *The Average Time for Carry Propagation*, Indagationes Mathematicæ **40** (1978), 238–242.
7. R. Morris, *Counting Large Numbers of Events in Small Registers*, Comm.ACM **21** (1978), 840–842.
8. N. E. Nörlund, *Vorlesungen über Differenzenrechnung*, Chelsea, New York, 1954.
9. H. Prodinger, *Über längste 0–1–Folgen*, Zahlentheoretische Analysis II (E. Hlawka, ed.), Lecture Notes in Math. 1262, Springer, Berlin, 1987, pp. 124–133.
10. U. Schmid, *Abzählprobleme der theoretischen Informatik*, Diplomarbeit, TU Wien, 1985.

TU Vienna
Wiedner Hauptstrasse 8-10
A-1040 Vienna
Austria