Analysis of Carry Propagation in Addition: An Elementary Approach

Nicholas Pippenger*
(nicholas@cs.ubc.ca)

Department of Computer Science
The University of British Columbia
Vancouver, British Columbia V6T 1Z4
CANADA

Abstract: Our goal in this paper is to analyze carry propagation in addition using only elementary methods (that is, those not involving residues, contour integration, or methods of complex analysis). Our results concern the length of the longest carry chain when two independent uniformly distributed n-bit numbers are added. First, we show using just first- and second-moment arguments that the expected length C_n of the longest carry chain satisfies $C_n = \log_2 n + O(1)$. Second, we use a sieve (inclusion-exclusion) argument to give an exact formula for C_n. Third, we give an elementary derivation of an asymptotic formula due to Knuth, $C_n = \log_2 n + \Phi(\log_2 n) + O\big((\log n)^4/n\big)$, where $\Phi(\nu)$ is a bounded periodic function of ν, with period 1, for which we give both a simple integral expression and a Fourier series. Fourth, we give an analogous asymptotic formula for the variance V_n of the length of the longest carry chain: $V_n = \Psi(\log_2 n) + O\big((\log n)^5/n\big)$, where $\Psi(\nu)$ is another bounded periodic function of ν, with period 1. Our approach can be adapted to addition with the "end-around" carry that occurs in the sign-magnitude and 1s-complement representations. Finally, our approach can be adapted to give elementary derivations of some asymptotic formulas arising in connection with radix-exchange sorting and collision-resolution algorithms, which have previously been derived using contour integration and residues.

* The work reported here was supported by an NSERC Research Grant.

1. Introduction

The study of carry propagation in addition is one of the oldest problems in the analysis of algorithms. Let C_n denote the expected length of the longest carry chain when two independent uniformly distributed n-digit binary numbers are added. (We take the "length of the longest carry chain" to be 0 if there are no carries; to be 1 if there are carries, but none of them give rise to further carries; and so forth. We shall confine our attention in this paper to binary addition, but all of our results generalize straightforwardly to base-b addition, for $b \geq 2$.) In 1946, Burks, Goldstein and von Neumann [B2] observed that

$$C_n \leq \log_2 n + 1.$$

In 1973, Claus [C] showed that

$$C_n \geq \log_2 n - 2.$$

(Claus states his result in terms of the expected number E_n of times that a "carry-save" adder must be used to clear all carries; thus $E_n = C_n + 1$. We have restated Claus's result in terms of C_n to facilitate comparison.)

In Section 2, we shall derive the formula

$$C_n = \log_2 n + O(1) \tag{1.1}$$

using only first- and second-moment arguments. In Section 3, we shall use a sieve (inclusion-exclusion) argument to derive the exact formula

$$C_n = \sum_{k\geq 1}\sum_{j\geq 1} \binom{n - j(k-1)}{j} \frac{(-1)^{j+1}}{2^{(k+1)j}}. \tag{1.2}$$

In 1978, Knuth [K1] showed that

$$C_n = \log_2 n + \gamma \log_2 e - \tfrac{3}{2} - F(\log_2 n) + O\left(\frac{(\log n)^4}{n}\right), \tag{1.3}$$

where $\gamma = 0.5772\ldots$ is Euler's constant, $e = 2.718\ldots$ is the base of natural logarithms, and $F(\nu)$ is a periodic function of ν with period 1. (Knuth states his result in terms of the expected number t_n of "steps" in a certain algorithm. This number agrees with the one used by Claus, except when the augend is 0, when it is smaller by 1; thus $t_n = E_n - 2^{-n} = C_n + 1 - 2^n$. We have restated Knuth's result in terms of C_n to facilitate comparison.) The function $F(\nu)$ has mean value 0, in the sense that $\int_0^1 F(\nu)\,d\nu = 0$. (This "mean" corresponds to choosing n randomly in such a way that $\log_2 n$ is uniformly distributed modulo 1. (The distribution of $\log_2 n$ can of course only be approximately uniform, since n assumes only natural numbers as values.) We shall use the term "mean " in this sense, while using the term "average" to refer to the uniform probability distribution on n-bit binary numbers.) Knuth gives the Fourier expansion

$$F(\nu) = (\log_2 e) \sum_{k \neq 0} \Gamma(-2\pi i k \log_2 e) \, \exp(2\pi i k \nu), \tag{1.4}$$

where the sum is over all integers, both positive and negative, not equal to 0. (As between the terms with positive and negative k, the real parts add and the imaginary parts cancel. Thus (1.4) is equivalent to the formula in Knuth [K1], which includes a factor of 2, sums only over positive k, and takes the real part of each term.) Knuth points out that the oscillations of $F(\nu)$ are very small: we have $|F(\nu)| \leq 1.573\ldots \times 10^{-6}$ for all $\nu \in [0, 1)$.

In Sections 4 and 5 we shall give an elementary derivation of (1.3), avoiding the contour integration and residues used by Knuth. Our derivation gives the simple expression

$$F(\nu) = \int_0^\infty \left(\{\nu - \log_2 y\} - \tfrac{1}{2}\right) \, e^{-y} \, dy \tag{1.5}$$

for the function $F(\nu)$, where $\{x\} = x - \lfloor x \rfloor$ denotes the fractional part of x. This expression makes it clear that $F(\nu)$ is a periodic function of ν with period 1, and that the mean value of $F(\nu)$ vanishes: $\int_0^1 F(\nu)\, d\nu = 0$. We shall go on to express the Fourier coefficients of $F(\nu)$ in terms of the Gamma function as in (1.4), again using only elementary methods. We do this to establish contact with previous work, but also because the expression in terms of the Gamma function is the most convenient for numerical estimation of the magnitude of the oscillations of $F(\nu)$. Of course, since the expression (1.4) involves values of the Gamma function for imaginary arguments, we will need to use at least a definition of Gamma as a function of a complex variable. Following Artin [A], we shall take the integral representation

$$\Gamma(s) = \int_0^\infty x^{s-1} \, e^{-x} \, dx \tag{1.6}$$

as the definition of the Gamma function. Apart from this we shall need only the functional equations

$$s \, \Gamma(s) = \Gamma(1 + s) \tag{1.7}$$

and

$$\Gamma(s) \, \Gamma(1 - s) = \frac{\pi}{\sin(\pi s)}, \qquad (1.8),$$

and the Weierstrass product formula

$$\Gamma(s) = \frac{e^{-\gamma s}}{s} \prod_{k \geq 1} \left(\frac{k}{k+s} \right) e^{s/k}. \tag{1.9}$$

All of these formulas are established for real s by elementary means from (1.6) in Artin's book. We shall only need to assume that they hold for complex s as well.

In Section 6 we shall give exact and asymptotic expressions for the variance V_n of the length of the longest carry chain. We show that

$$V_n = \tfrac{1}{6}\pi^2 (\log_2 e)^2 + \tfrac{1}{12} - \omega - G(\log_2 n) + O\left(\frac{(\log n)^5}{n} \right), \tag{1.10}$$

where $\pi = 3.14159\ldots$ is the circular ratio, $\omega = \int_0^1 F(\nu)^2 \, d\nu$ is the mean-square oscillation of $F(\nu)$, and $G(\nu)$ is a periodic function of ν, with period 1, for which the mean value vanishes: $\int_0^1 G(\nu) \, d\nu = 0$. We observe that $\pi^2 (\log_2 e)^2/6 + 1/12 = 3.507\ldots.$ Furthermore, we shall see that $\omega = 1.237\ldots \times 10^{-12}$, and that the oscillations of $G(\nu)$ are again very small: we have $|G(\nu)| \leq 5.452\ldots \times 10^{-7}$.

In 1973, Briley [B1] considered the expected length C'_n of the longest carry chain when an "end-around" carry (out of the most significant position and into the least significant position) can occur, as is the case with the sign-magnitude and 1s-complement representations of signed numbers. In the Appexdix, we shall show that our method can be adapted to the analysis of carry propagation with end-around carry. We shall derive the exact formula

$$C'_n = \sum_{k \geq 1} \sum_{j \geq 1} \left[\binom{n - j(k-1)}{j} + (k-1) \binom{n - 1 - j(k-1)}{j-1} \right] \frac{(-1)^{j+1}}{2^{(k+1)j}}. \tag{1.11}$$

We shall also derive an exact formula for the variance V'_n of the length of the longest carry chain with end-around carry, and show that the asymptotic formulas (1.3) and (1.10) apply to C'_n and V'_n as well.

We remark that our method for avoiding contour integration and residues can be applied to some other problems that have previously only been solved with the aid of these methods. Examples are the evaluations of

$$\frac{1}{n} \sum_{k \geq 1} (2^k e^{-n/2^k} - 2^k + n) = \log_2 n + (\gamma - 1) \log_2 e - \tfrac{1}{2} + \Delta(\log_2 n) + O\left(\frac{\log n}{n} \right),$$

where

$$\Delta(\nu) = \log_2 \sum_{k \neq 0} \Gamma(-1 - 2\pi i k \log_2 e) \exp(2\pi i k \nu),$$

introduced by Knuth [K2] is his analysis of radix-exchange sorting, and certain expressions introduced by Mathys and Flajolet [M] in their analysis of the tree algorithm for collision-resolution in multiple-access channels. (There is in fact a relationship between carry propagation and the tree algorithm for collision resolution; the analysis by Janssen and de Jong [J] of the average and variance of the number of transmissions required by one of n contenders for the channel results in expressions similar to (1.3) and (1.10).) We do not claim, of course, that our method can replace all uses of complex analysis in the analysis of algorithms (see the masterly surveys of Flajolet, Grabner, Kirschenhofer, Prodinger and Tichy [F1], Flajolet and Golin [F2], Flajolet, Gourdon and Dumas [F3], and Flajolet and Sedgewick [F4] for an indication of the extent of application just the Mellin transform, which is the method previously used for the problems we treat here). Nevertheless, we believe it is of interest to note when elementary methods can be used to establish the oscillatory behaviour that has traditionally been the province of complex-analytic methods (another example has been given by Pippenger [P]).

2. A Rough Formula

Our goal in this section is to derive the rough bound (1.1) using just first- and second-moment arguments. Let the random variable $\mathbf{C}_n$ denote the length of the longest carry chain in the addition two independent uniformly distributed n-bit binary numbers. Then we have

$$\begin{aligned} C_n &= \sum_{k \geq 0} k \; \Pr[\mathbf{C}_n = k] \\ &= \sum_{k \geq 1} \Pr[\mathbf{C}_n \geq k] \end{aligned} \tag{2.1}$$

by partial summation.

We shall say that a bit position *generates* a carry if both summands have 1s in this position, and that a bit position *propagates* a carry if one of the summands has a 1, and the other has a 0, in this position. With independent uniformly distributed summands, the probability that a position generates a carry is 1/4, and the probability that it propagates a carry is 1/2.

A set of k consecutive bit positions will be called a *k-block*. We shall say that a k-block is *active* if its lowest-order position generates a carry and its remaining $k-1$ positions propagate a carry. The probability that a particular k-block is active is just $1/2^{k+1}$, since the lowest-order position generates a carry with probability $1/4$ and each of the remaining $k-1$ positions independently propagates a carry with probability $1/2$.

Let the random variable $\mathbf{B}_{n,k}$ denote the number of active k-blocks for two independent uniformly distributed n-bit numbers. A carry chain of length k or more occurs if and only if some k-block is active, so we have $\Pr[\mathbf{C}_n \geq k] = \Pr[\mathbf{B}_{n,k} \geq 1]$.

Since there are $n-k+1$ distinct k-blocks, each of which is active with probability $1/2^{k+1}$, we have

$$\mathrm{Ex}[\mathbf{B}_{n,k}] = (n-k+1)/2^{k+1}.$$

By Markov's inequality we have $\Pr[\mathbf{B}_{n,k} \geq 1] \leq \mathrm{Ex}[\mathbf{B}_{n,k}]$, so that

$$\begin{aligned} \Pr[\mathbf{C}_n \geq k] &= \Pr[\mathbf{B}_{n,k} \geq 1] \\ &\leq \min\{1, (n-k+1)/2^{k+1}\}. \end{aligned} \tag{2.2}$$

Substituting (2.2) into (2.1), we obtain

$$\begin{aligned} C_n &\leq \sum_{1 \leq k \leq \log_2 n - 1} 1 + \sum_{k \geq \log_2 - 1} (n-k+1)/2^{k+1} \\ &\leq \lfloor \log_2 n - 1 \rfloor + 2 \\ &\leq \log_2 + 1, \end{aligned}$$

which is the upper bound for (1.1).

Next we shall derive a lower bound for C_n. For the variance of $\mathbf{B}_{n,k}$ we have

$$\mathrm{Var}[\mathbf{B}_{n,k}] = \sum_{\beta_1, \beta_2} \Pr[\beta_1 \text{ active}, \beta_2 \text{ active}] - \Pr[\beta_1 \text{ active}] \Pr[\beta_2 \text{ active}],$$

where the summation is over all ordered pairs of k-blocks. The $(n-k+1)$ pairs with $\beta_1 = \beta_2$ contribute $(n-k+1)(1/2^{k+1} - 1/2^{2k+2}) \leq (n-k+1)/2^{k+1}$; disjoint pairs give no contribution, since the events of their being active are independent, so that $\Pr[\beta_1 \text{ active}, \beta_2 \text{ active}] = \Pr[\beta_1 \text{ active}] \Pr[\beta_2 \text{ active}]$; and overlapping but distinct pairs give a negative contribution, since generating a carry and propagating a carry are mutually exclusive events, so such blocks cannot be active simultaneously, and $\Pr[\beta_1 \text{ active}, \beta_2 \text{ active}] = 0$. Thus we have

$$\mathrm{Var}[\mathbf{B}_{n,k}] \leq (n-k+1)/2^{k+1}.$$

By Chebyshev's inequality, we have

$$\begin{aligned}\Pr[\mathbf{B}_{n,k} = 0] &\le \mathrm{Var}[\mathbf{B}_{n,k}]/\mathrm{Ex}[\mathbf{B}_{n,k}]^2 \\ &\le 2^{k+1}/(n-k+1).\end{aligned}$$

Thus we have

$$\begin{aligned}\Pr[\mathbf{C}_n \ge k] &= \Pr[\mathbf{B}_{n,k} \ge 1] \\ &= 1 - \Pr[\mathbf{B}_{n,k} = 0] \\ &\ge \max\{0, 1 - 2^{k+1}/(n-k+1)\}. \end{aligned} \tag{2.3}$$

If $k \le \log_2 n - 2$, we have $n - k + 1 \ge n/2$. Substituting (2.3) into (2.1), we obtain

$$\begin{aligned}C_n &\ge \sum_{1 \le k \le \log_2 n - 2} \left(1 - 2^{k+1}/(n-k+1)\right) \\ &\ge \lfloor \log_2 n - 2 \rfloor - 2 \\ &\ge \log_2 n - 5,\end{aligned}$$

which is the lower bound for (1.1).

3. An Exact Formula

Our goal in this section is the derivation of the exact formula (1.2). A carry chain of length k or more occurs if and only if some k-block is active, so we have

$$\Pr[\mathbf{C}_n \ge k] = \Pr[\text{some } k\text{-block is active}],$$

and (2.1) becomes

$$C_n = \sum_{k \ge 1} \Pr[\text{some } k\text{-block is active}]. \tag{3.1}$$

There are $n - k + 1$ distinct k-blocks. By the principle of inclusion-exclusion,

$$\Pr[\text{some } k\text{-block is active}] = \sum_{j \ge 1} (-1)^{j-1} \sum_{\beta_1, \ldots, \beta_j} \Pr[\beta_1, \ldots, \beta_j \text{ active}],$$

where the inner sum is over all unordered sets $\{\beta_1, \ldots, \beta_j\}$ of j distinct k-blocks. We observe that two distinct k-blocks cannot both be active unless they are disjoint (since generating a carry and propagating a carry are mutually exclusive events), and that if they are disjoint, the events of their being active are independent. Thus we have

$$\Pr[\text{some } k\text{-block is active}] = \sum_{j\geq 1}(-1)^{j-1} \sum_{\beta_1,\ldots,\beta_j} \Pr[\beta_1 \text{ active}]\cdots\Pr[\beta_j \text{ active}], \tag{3.2}$$

where the inner sum is over all unordered sets $\{\beta_1, \ldots, \beta_j\}$ of j pairwise-disjoint k-blocks.

Each term in the inner sum of (3.2) is $1/2^{(k+1)j}$, since each of the j factors is $1/2^{k+1}$. Thus we have

$$\Pr[\text{some } k\text{-block is active}] = \sum_{k\geq 1} A_{n,j,k}\, \frac{(-1)^{j-1}}{2^{(k+1)j}}, \tag{3.3}$$

where $A_{n,j,k}$ is the number of terms in the inner sum of (3.2) (that is, the number of choices of j pairwise-disjoint k-blocks among n positions). Since the k positions of a block must be consectutive, we may imagine shrinking each block to a single position, so that $A_{n,j,k}$ is the number of choices of j positions (for the shrunken blocks) among $n - j(k-1)$ positions (these latter being j positions for the shrunken blocks plus $n - jk$ positions apart from the blocks). Thus we have

$$A_{n,j,k} = \binom{n - j(k-1)}{j}.$$

Substituting these results in (3.3), we obtain

$$\Pr[\text{some } k\text{-block is active}] = \sum_{j\geq 1} \binom{n - j(k-1)}{j} \frac{(-1)^{j-1}}{2^{(k+1)j}}, \tag{3.3}$$

and substituting this result in (3.1) yields (1.2).

4. The Approximate Distribution

For $\lambda > 0$, let $\mathbf{D}_\lambda$ be a random variable distributed over $\{0, 1, 2, \ldots\}$ such that

$$\Pr[\mathbf{D}_n \geq k] = 1 - e^{-\lambda/2^k}. \tag{4.1}$$

Our goal in this section is to show that the distribution of $\mathbf{C}_n$ is approximately that of $\mathbf{D}_{n/2}$, in the sense that

$$\Pr[\mathbf{C}_n \geq k] = \Pr[\mathbf{D}_{n/2} \geq k] + O\left(\frac{(\log n)^3}{n}\right). \tag{4.2}$$

This, together with the estimates

$$\Pr[\mathbf{C}_n \geq k] = O(n/2^k) \tag{4.3}$$

(which follows from (2.2)) and

$$\Pr[\mathbf{D}_\lambda \geq k] = O(\lambda/2^k) \tag{4.4}$$

(which follows from the power-series expansion $e^x = 1 + O(x)$), allows us to show that

$$C_n = D_{n/2} + O\left(\frac{(\log n)^4}{n}\right), \tag{4.5}$$

where

$$\begin{aligned} D_\lambda &= \sum_{k \geq 1} \Pr[\mathbf{D}_\lambda \geq k] \\ &= \sum_{k \geq 1} \left(1 - e^{\lambda/2^k}\right). \end{aligned} \tag{4.6}$$

Our derivation parallels that of Knuth [K2], with minor changes to avoid arguments based on complex analysis. Throughout this paper, the constants implicit in O-notation are absolute; in particular, the constants in (4.2), (4.3) and (4.4) are independent of k.

For $k \geq 1$ and $n \geq 0$, let $q_{n,k} = \Pr[\mathbf{B}_{n,k} = 0]$ be the probability that there is no active k-block among the n positions. This event implies that there is no active k-block among the low-order $n-1$ positions, an event which occurs with probability $q_{n-1,k}$. The difference between these events occurs when the k high-order positions form the unique active k-block among the n positions, an event which occurs with probability $q_{n-k,k}/2^{k+1}$. Thus we have

$$q_{n,k} = q_{n-1,k} - q_{n-k,k}/2^{k+1} \tag{4.7}$$

for $n \geq k$. Define the generating function

$$Q_k(z) = \sum_{n \geq 0} q_{n,k}\, z^n.$$

Multiplying (4.7) by z^n, summing over $n \geq k$ and using the condition that $q_{n,k} = 1$ for $0 \leq n < k$, we obtain

$$Q_k(z) = \frac{1}{D_k(z)},$$

where

$$D_k(z) = 1 - z + z^k/2^{k+1}.$$

To determine the asymptotic behaviour of $q_{n,k}$, we shall need information about the roots of $D_k(z)$. First we note that $D_k(1) > 0$ and $D_k(1 + 1/k) < 0$, so that $D_k(z)$ has a real root $\zeta = 1 + O(1/k)$. Setting $\zeta = 1 + \varepsilon$, we have

$$\begin{aligned} \varepsilon &= (1+\varepsilon)^k/2^{k+1} \\ &= \exp\bigl(k \log(1+\varepsilon) - (k-1)\log 2\bigr). \end{aligned} \tag{4.8}$$

Substituting $\varepsilon = O(1/k)$ into (4.8) we obtain $\varepsilon = O(1/2^k)$, and substituting this in turn into (4.8) we obtain $\varepsilon = 1/2^{k+1} + O(k2^{2k})$, so that

$$\zeta = 1 + \frac{1}{2^{k+1}} + O\left(\frac{k}{2^{2k}}\right).$$

Next, we shall estimate the remaining $k-1$ roots of $D_k(z)$. Dividing $2^{k+1}D_k(z) = z^k - 2^{k+1}z + 2^{k+1}$ by $z - \zeta$ yields a polynomial

$$E_k(z) = z^{k-1} + \zeta z^{k-2} + \cdots + \zeta^{k-2}z + \zeta^{k-1} - 2^{k+1}$$

that contains the remaining $k-1$ roots of $D_k(z)$. For $k \geq 2$, we have $\zeta \leq 1 + 1/k \leq 3/2$. If in addition $|z| \leq 2$, we have

$$\begin{aligned} &|z^{k-1} + \zeta z^{k-2} + \cdots + \zeta^{k-2}z + \zeta^{k-1}| \\ &\quad \leq 2^{k-1} + 3 \cdot 2^{k-3} + \cdots + 3^{k-2}/2^{k-3} + 3^{k-1}/2^{k-1} \\ &\quad = \frac{2^{k-1} - 3^k/2^{k+1}}{1 - 3/4} \\ &\quad = 2^{k+1} - 3^k/2^{k-1}, \end{aligned}$$

so that $|E_k(z)| \geq 3^k/2^{k-1}$. Thus $E_k(z)$ cannot have any roots inside the circle $|z| \leq 2$, so if $\zeta_1 = \zeta$ and $\zeta_2, \ldots, \zeta_k$ are the roots of $D_k(z)$, we have $|z_j| > 2$ for $2 \leq j \leq k$.

Finally, we observe that all the roots of $D_k(z)$ are simple. For if $D_k(z)$ had a multiple root at ζ_j, then ζ_j would also be a root of the derivative $D_k'(z) = -1 + kz^{k-1}/2^{k+1}$. For $2 \leq k \leq 3$, it is easily verified that the greatest common divisor of $D_k(z)$ and $D_k'(z)$ is trivial. For $k \geq 4$, we note all the roots of $D_k'(z)$ lie on the circle $|z| = (2^{k+1}/k)^{1/(k-1)} \leq 2$, while $D_k(z)$ has only the simple root ζ_1 inside the disk $|z| \leq 2$.

Since $D_k(z)$ has only simple roots, $Q_k(z)$ has the partial fraction expansion

$$Q_k(z) = \sum_{1 \le j \le k} \frac{-1}{(1 - z/\zeta_j)\, \zeta_j\, D_k'(\zeta_j)}.$$

Thus we have

$$\begin{aligned} q_{n,k} &= \sum_{1 \le j \le k} \frac{-1}{\zeta_j^{n+1}\, D_k'(\zeta_j)} \\ &= \sum_{1 \le j \le k} \frac{1}{\zeta_j^{n+1}\, (1 - k\zeta_j^{k-1}/2^{k+1})}. \end{aligned}$$

For the first term, $j = 1$, we have

$$\frac{1}{\zeta^{n+1}\, (1 - k\zeta^{k-1}/2^{k+1})} = \frac{1}{\left(1 + 1/2^{k+1} + O(k/2^{2k})\right)^n\, \left(1 + O(k/2^k)\right)}.$$

For the remaining $k - 1$ terms, we have

$$\frac{1}{\zeta_j^{n+1}\, (1 - k\zeta_j^{k-1}/2^{k+1})} = O\left(\frac{1}{2^n\; k}\right),$$

since the second factor in the denominator does not vanish for any k, and we have

$$\begin{aligned} |1 - k\zeta_j^{k-1}/2^{k+1}| &\ge 1 - k/4 \\ &\ge k/8 \end{aligned}$$

for $k \ge 8$. Thus we have

$$\sum_{2 \le j \le k} \frac{1}{\zeta_j^{n+1}\, (1 - k\zeta_j^{k-1}/2^{k+1})} = O\left(\frac{1}{2^n}\right),$$

and

$$q_{n,k} = \frac{1}{\left(1 + 1/2^{k+1} + O(k/2^{2k})\right)^n\, \left(1 + O(k/2^k)\right)} + O\left(\frac{1}{2^n}\right).$$

For $1 \le k \le \log_2 n - \log_2(4 \log n)$, we have

$$\Pr[\mathbf{C}_n \ge k] = 1 + O\left(\frac{1}{n^2}\right)$$

and

$$\Pr[\mathbf{D}_n \ge k] = 1 + O\left(\frac{1}{n^2}\right),$$

so that (4.2) holds for these values of k. For $k > \log_2 n - \log_2(4\log n)$, we have

$$\Pr[\mathbf{C}_n \geq k] = 1 - e^{-n/2^{k+1}}\left(1 + O\left(\frac{nk}{2^{2k}}\right)\right),$$

so (4.2) holds for all values of k. Combining (4.2) for $k \leq 3\log_2 n$ with (4.3) and (4.4) for $k > 3\log_2 n$ yields (4.3).

5. Asymptotics and Oscillations

Our goal in this section is to show that D_λ, as defined by (4.4), can be expressed as

$$D_\lambda = p\log_2\lambda + \gamma\log_2 e - \tfrac{1}{2} + F(\log_2\lambda) + O(e^{-\lambda/2}\,\log\lambda), \tag{5.1}$$

where $F(\nu)$ is a periodic function of ν, with period 1 and mean value 0. This result, combined with (4.3), will complete the derivation of (1.3). We shall also determine the Fourier expansion (1.4) of $F(\nu)$.

Using $1 - e^{-x} = \int_0^x e^{-y}\,dy$, we have

$$\begin{aligned} D_\lambda &= \sum_{k\geq 1}\left(1 - e^{-\lambda/2^k}\right) \\ &= \sum_{k\geq 1}\int_0^{n/2^k} e^{-y}\,dy \\ &= \int_0^{\lambda/2} \sum_{1\leq k\leq \log_2\lambda} e^{-y}\,dy \\ &= \int_0^{\lambda/2} \left\lfloor \log_2\frac{\lambda}{y}\right\rfloor e^{-y}\,dy. \end{aligned}$$

Using $\lfloor x\rfloor = x - \{x\}$ (where $\{x\}$ denotes the fractional part of x), we have

$$D_\lambda = (\log_2\lambda)\int_0^{\lambda/2} e^{-y}\,dy - \int_0^{\lambda/2}\log_2 y\; e^{-y}\,dy - \int_0^{\lambda/2}\left\{\log_2\frac{\lambda}{y}\right\} e^{-y}\,dy.$$

We can raise the upper limits of the three integrals from $\lambda/2$ to ∞ by using the estimates $\int_{\lambda/2}^\infty e^{-y}\,dy = e^{-\lambda/2}$, $\int_{\lambda/2}^\infty O(\log y)\; e^{-y}\,dy = O(e^{-\lambda/2}\,\log\lambda)$ and $\int_{\lambda/2}^\infty O(1)\; e^{-y}\,dy = O(e^{-\lambda/2})$, obtaining

$$D_\lambda = \log_2\lambda - \int_0^\infty \log_2 y\; e^{-y}\,dy - \int_0^\infty\left\{\log_2\frac{\lambda}{y}\right\} e^{-y}\,dy + O(e^{-\lambda/2}\,\log\lambda).$$

Next we use integral $\int_0^\infty \log y \, e^{-y} \, dy = -\gamma$, which is derived by evaluating $\Gamma'(1)$ in two ways: first by differentiating the integral representation (1.6), then setting $s = 1$; and second by differentiating the logarithm of the Weierstrass product formula (1.9), then again setting $s = 1$. The result is

$$D_\lambda = \log_2 \lambda + \gamma \log_2 e - F_1(\log_2 \lambda) + O(e^{-\lambda/2} \, \log \lambda), \tag{5.2}$$

where

$$F_1(\nu) = \int_0^\infty \{\nu - \log_2 y\} \, e^{-y} \, dy \tag{5.3}$$

is obviously a periodic function of ν, with period 1. The mean value of $F_1(\nu)$ is

$$\begin{aligned} \int_0^1 F_1(\nu) \, d\nu &= \int_0^\infty \int_0^1 \{\nu - \log_2 y\} \, d\nu \, e^{-y} \, dy \\ &= \int_0^\infty \tfrac{1}{2} e^{-y} \, dy \\ &= \tfrac{1}{2}. \end{aligned}$$

Thus we obtain (5.1), where $F(\nu)$, given by (1.5), is a periodic function of ν, with period 1 and mean value 0.

Using the Fourier series

$$\{z\} = \tfrac{1}{2} - \sum_{k \neq 0} \frac{1}{2\pi i k} \, \exp(2\pi i k z), \tag{5.4}$$

we have

$$F(\nu) = \sum_{k \neq 0} \frac{-1}{2\pi i k} \int_0^\infty y^{-2\pi i k \log_2 e} \, e^{-y} \, dy \, \exp(2\pi i k \nu). \tag{5.5}$$

From (1.6) and (1.7), we obtain the following expression for the Gamma function on the imaginary axis:

$$\Gamma(it) = \frac{1}{it} \int_0^\infty y^{it} \, e^{-y} \, dy. \tag{5.6}$$

Using this expression to evaluate the integral in (5.5), we obtain (1.4).

Finally, we estimate the magnitude of the oscillations of $F(\nu)$. First, from (1.4), we have

$$|F(\nu)| \le 2 \log_2 e \sum_{k \ge 1} |\Gamma(2\pi i k \log_2 e)|, \tag{5.7}$$

where we have introduced a factor of 2 and reduced the range of summation to positive k, since $|\Gamma(2\pi ik\log_2 e)| = |\Gamma(-2\pi ik\log_2 e)|$. From (1.7) and (1.8) we have

$$\begin{aligned}|\Gamma(it)| &= \sqrt{\Gamma(it)\,\Gamma(-it)} \\ &= \sqrt{\frac{\pi}{t\sinh(\pi t)}}.\end{aligned} \tag{5.8}$$

Applying this to (5.7) yields

$$|F(\nu)| \le \sum_{k\ge 1}\sqrt{\frac{2\log_2 e}{k\sinh(2\pi^2 k\log_2 e)}}.$$

The first term in this sum is $1.57315\ldots\times 10^{-6}$; successive terms decrease by a ratio smaller than the first term (asymptotically, by $\exp(-\pi^2\log_2 e) = 6.5486\ldots\times 10^{-7}$) so the sum, and thus $|F(\nu)|$ for all ν, is at most $1.5731\ldots\times 10^{-6}$.

6. The Variance

In this section we deal with the variance $V_n = \mathrm{Var}[\mathbf{C}_n]$ of the length of the longest carry chain. We have

$$V_n = \mathrm{Ex}[\mathbf{C}_n^2] - \mathrm{Ex}[\mathbf{C}_n]^2 \tag{6.1}$$

from the definition of the variance. For the first term on the right-hand side, we have

$$\begin{aligned}\mathrm{Ex}[\mathbf{C}_n^2] &= \sum_{k\ge 0} k^2\,\Pr[\mathbf{C}_n = k] \\ &= \sum_{k\ge 1}(2k-1)\Pr[\mathbf{C}_n \ge k],\end{aligned} \tag{6.2}$$

using summation by parts. Substituting (3.3) into (6.2) yields

$$\mathrm{Ex}[\mathbf{C}_n^2] = \sum_{k\ge 1}(2k-1)\sum_{j\ge 1}\binom{n-j(k-1)}{j}\frac{(-1)^{j-1}}{2^{(k+1)j}}.$$

Substituting this formula for the first term in (6.1) and (1.2) for the second term yields the exact formula

$$\begin{aligned}V_n = &\sum_{k\ge 1}(2k-1)\sum_{j\ge 1}\binom{n-j(k-1)}{j}\frac{(-1)^{j-1}}{2^{(k+1)j}} \\ &- \left(\sum_{k\ge 1}\sum_{j\ge 1}\binom{n-j(k-1)}{j}\frac{(-1)^{j+1}}{2^{(k+1)j}}\right)^2\end{aligned} \tag{6.3}$$

for the variance. As was the case with the exact formula (1.2) for the average C_n, the presence of large terms of alternating sign in this formula makes it unsuitable for asymptotic analysis.

To determine the asymptotic behaviour of V_n, we again use (6.1) and (6.2) to obtain

$$V_n = \sum_{k \geq 1} (2k-1) \Pr[\mathbf{C}_n \geq k] - C_n^2. \tag{6.4}$$

Similarly, for the variance $W_\lambda = \mathrm{Var}[\mathbf{D}_\lambda]$ of $\mathbf{D}_\lambda$ we have

$$W_\lambda = \sum_{k \geq 1} (2k-1) \Pr[\mathbf{D}_\lambda \geq k] - D_\lambda^2. \tag{6.5}$$

Comparing (6.4) and (6.5), using (4.2) for the terms with $k \leq 3 \log_2 n$, (4.3) and (4.4) for the terms with $k > 3 \log_2 n$, and (4.5) for the remaining terms, we obtain

$$V_n = W_{n/2} + O\left(\frac{(\log n)^5}{n} \right).$$

To determine the asymptotic behaviour of W_λ, we refer to (6.4). We have already estimated D_λ in (5.2), so it remains to estimate

$$\begin{aligned} J_\lambda &= \sum_{k \geq 1} (2k-1) \Pr[\mathbf{D}_\lambda \geq k] \\ &= \sum_{k \geq 1} (2k-1) \left(1 - e^{\lambda/2^k}\right). \end{aligned}$$

Proceeding as in Section 5, we have

$$\begin{aligned} J_\lambda &= \sum_{k \geq 1} (2k-1) \left(1 - e^{-\lambda/2^k}\right) \\ &= \sum_{k \geq 1} (2k-1) \int_0^{n/2^k} e^{-y}\, dy \\ &= \int_0^{\lambda/2} \sum_{1 \leq k \leq \log_2 \lambda} (2k-1)\, e^{-y}\, dy \\ &= \int_0^{\lambda/2} \left\lfloor \log_2 \frac{\lambda}{y} \right\rfloor^2 e^{-y}\, dy. \end{aligned}$$

Expanding the floor as before we obtain

$$
\begin{aligned}
J_\lambda = (\log_2 \lambda)^2 \int_0^{\lambda/2} e^{-y}\, dy - 2(\log_2 \lambda) \int_0^{\lambda/2} \log_2 y\ e^{-y}\, dy \\
+ \int_0^{\lambda/2} (\log_2 y)^2 e^{-y}\, dy - 2(\log_2 \lambda) \int_0^{\lambda/2} \left\{ \log_2 \frac{\lambda}{y} \right\} e^{-y}\, dy \\
+ 2 \int_0^{\lambda/2} \left\{ \log_2 \frac{\lambda}{y} \right\} \log_2 y\ e^{-y}\, dy + \int_0^{\lambda/2} \left\{ \log_2 \frac{\lambda}{y} \right\}^2 e^{-y}\, dy.
\end{aligned}
$$

We can again raise the upper limits of integration from $\lambda/2$ to ∞ by introducing an error term, this time $O\big(e^{-\lambda/2}\,(\log \lambda)^2\big)$. This yields

$$
\begin{aligned}
J_\lambda = (\log_2 \lambda)^2 + 2\gamma(\log_2 e)(\log_2 \lambda) \\
+ \int_0^{\infty} (\log_2 y)^2 e^{-y}\, dy - 2(\log_2 \lambda) \int_0^{\infty} \left\{ \log_2 \frac{\lambda}{y} \right\} e^{-y}\, dy \\
+ 2 \int_0^{\infty} \left\{ \log_2 \frac{\lambda}{y} \right\} \log_2 y\ e^{-y}\, dy + \int_0^{\infty} \left\{ \log_2 \frac{\lambda}{y} \right\}^2 e^{-y}\, dy \\
+ O\big(e^{-\lambda/2}\,(\log \lambda)^2\big),
\end{aligned}
\tag{6.6}
$$

where we have evaluated the first two resulting integrals as in the derivation of (5.2).

To evaluate the first integral in (6.6), we use the integral $\int_0^\infty (\log y)^2\ e^{-y}\, dy = \frac{1}{6}\pi^2 + \gamma^2$, which is derived by evaluating $\Gamma''(1)$ in two ways: first by twice differentiating the integral representation (1.6), then setting $s = 1$; and second by twice differentiating the logarithm of the Weierstrass product formula (1.9), then again setting $s = 1$. This then requires the sum $\sum_{k\geq 1} \frac{1}{k^2} = \frac{1}{6}\pi^2$, which is derived by applying Parseval's Theorem,

$$
\int_0^1 \left| \sum_k c_k \exp(2\pi i k z) \right|^2 dz = \sum_k |c_k|^2, \tag{6.7}
$$

to the Fourier series (5.4). The result is

$$
\int_0^\infty (\log_2 y)^2 e^{-y}\, dy = \tfrac{1}{6}\pi^2 (\log_2 e)^2 + \gamma^2 (\log_2 e)^2. \tag{6.9}
$$

To evaluate the second integral in (6.6), we use the definition (5.3). The result is

$$
2(\log_2 \lambda) \int_0^\infty \left\{ \log_2 \frac{\lambda}{y} \right\} e^{-y}\, dy = 2(\log_2 \lambda)\ F_1(\log_2 \lambda). \tag{6.8}
$$

To evaluate the third and fourth integrals in (6.6), we define

$$G_1(\nu) = \int_0^\infty \{\nu - \log_2 y\} \log_2 y \; e^{-y} \, dy$$

and

$$G_2(\nu) = \int_0^\infty \{\nu - \log_2 y\}^2 \; e^{-y} \, dy.$$

We then have

$$2\int_0^\infty \left\{\log_2 \frac{\lambda}{y}\right\} \log_2 y \; e^{-y} \, dy + \int_0^\infty \left\{\log_2 \frac{\lambda}{y}\right\}^2 \; e^{-y} \, dy = 2G_1(\log_2 \lambda) + G_2(\log_2 \lambda). \quad (6.10)$$

Substituting (6.8), (6.9) and (6.10) into (6.6) yields

$$\begin{aligned} J_\lambda = {} & (\log_2 \lambda)^2 + 2\gamma(\log_2 e)(\log_2 \lambda) + \tfrac{1}{6}\pi^2(\log_2 e)^2 + \gamma^2(\log_2 e)^2 \\ & - 2(\log_2 \lambda) \; F_1(\log_2 \lambda) + 2G_1(\log_2 \lambda) + G_2(\log_2 \lambda) + O\big(e^{-\lambda/2} \, (\log \lambda)^2\big), \end{aligned}$$

and substituting this equation and (5.2) into (6.4) yields

$$W_\lambda = \Psi(\log_2 \lambda) + O\big(e^{-\lambda/2} \, (\log \lambda)^2\big),$$

where

$$\Psi(\nu) = \tfrac{1}{6}\pi^2(\log_2 e)^2 + 2G_1(\nu) + G_2(\nu) - 2\gamma(\log_2 e) \; F_1(\nu) - F_1(\nu)^2$$

is obviously a periodic function of ν, with period 1. The mean value of $\Psi(\nu)$ is

$$\int_0^1 \Psi(\nu) \, d\nu = \tfrac{1}{6}\pi^2(\log_2 e)^2 + \tfrac{1}{12} - \omega,$$

where

$$\omega = \int_0^1 F(\nu)^2 \, d\nu,$$

since the mean values of $2G_1(\nu)$ and $2\gamma(\log_2 e) \; F_1(\nu)$ cancel, the mean value of $G_2(\nu)$ is $\frac{1}{3}$, and the mean value of $F_1(\nu)^2 = \big(\frac{1}{2} + F(\nu)\big)^2$ is $\frac{1}{4} + \omega$. To evaluate ω, we apply Parseval's Theorem (6.7) to the Fourier series (1.4), obtaining

$$\begin{aligned} \omega &= 2(\log_2 e)^2 \sum_{k \ge 1} |\Gamma(-2\pi i k \log_2 e)|^2 \\ &= (\log_2 e) \sum_{k \ge 1} \frac{1}{k \sinh(2\pi^2 k \log_2 e)}. \end{aligned}$$

The first term in this sum is $1.23741\ldots\times 10^{-12}$; successive terms decrease by a ratio smaller than the first term (asymptotically, by $\exp(-2\pi^2\log_2 e) = 4.2885\ldots\times 10^{-13}$) so the sum ω is at most $1.2374\ldots\times 10^{-12}$. Since $\frac{1}{6}\pi^2(\log_2 e)^2 + \frac{1}{12} = 3.50704\ldots$, the contribution of ω to the mean value of $\Psi(\nu)$ is negligible, and this mean value is $3.5070\ldots$.

Thus we obtain (1.10), where

$$\begin{aligned} G(\nu) = 2\int_0^\infty &\big(\{\nu-\log_2 y\}-\tfrac12\big)\big(\log_2 y-\gamma\log_2 e\big)\,e^{-y}\,dy \\ &+\int_0^\infty \big(\{\nu-\log_2 y\}^2-\tfrac13\big)\,e^{-y}\,dy \\ &-\left(\int_0^\infty \big(\{\nu-\log_2 y\}-\tfrac12\big)\,e^{-y}\,dy\right)^2+\omega \end{aligned} \tag{6.11}$$

is a periodic function of ν with period 1 and mean 0.

After differentiating (1.6) and (1.7), we obtain

$$\Gamma(it)+it\,\Gamma'(it)=\int_0^\infty y^{it}\,\log y\,e^{-y}\,dy. \tag{6.12}$$

Formulas (5.4), (5.6) and (6.12), together with the Fourier series

$$\{z\}=\tfrac13-\sum_{k\neq 0}\left(\frac{1}{2\pi ik}-\frac{2}{(2\pi ik)^2}\right)\exp(2\pi ikz),$$

allow us to evaluate the first two integrals in (6.11):

$$\begin{aligned} 2\int_0^\infty &\big(\{\nu-\log_2 y\}-\tfrac12\big)\big(\log_2 y-\gamma\log_2 e\big)\,e^{-y}\,dy+\int_0^\infty \big(\{\nu-\log_2 y\}^2-\tfrac13\big)\,e^{-y}\,dy \\ &=\log_2 e\sum_{k\neq 0}\big(2\log_2 e\,\Gamma'(-2\pi ik\log_2 e)+(1-2\gamma\log_2 e)\,\Gamma(-2\pi ik\log_2 e)\big)\exp(2\pi ik\nu). \end{aligned}$$

The last two terms in (6.11) are evaluated by substituting (1.4) for the integral in (1.5):

$$\begin{aligned} -&\left(\int_0^\infty \big(\{\nu-\log_2 y\}-\tfrac12\big)\,e^{-y}\,dy\right)^2+\omega \\ &=(\log_2 e)^2\sum_{k\neq 0}\left(\sum_{0\neq j\neq k}\Gamma\big(-2\pi ij\log_2 e\big)\,\Gamma\big(-2\pi i(k-j)\log_2 e\big)\right)\exp(2\pi ik\log_2 e). \end{aligned}$$

Combining these results yields

$$G(\nu) = \log_2 e \sum_{k \neq 0} \Bigl(2 \log_2 e \, \Gamma'(-2\pi i k \log_2 e) + (1 - 2\gamma \log_2 e) \, \Gamma(-2\pi i k \log_2 e)$$
$$+ \log_2 e \sum_{0 \neq j \neq k} \Gamma\bigl(-2\pi i j \log_2 e\bigr) \, \Gamma\bigl(-2\pi i (k-j) \log_2 e\bigr) \Bigr) \exp(2\pi i k \log_2 e).$$

Finally, we estimate the magnitude of the oscillations of $G(\nu)$. First, we have

$$|G(\nu)| \leq 2 \log_2 e \sum_{k \geq 1} \Bigl(2 \log_2 e \, \bigl|\Gamma'(-2\pi i k \log_2 e)\bigr| + \bigl|(1 - 2\gamma \log_2 e) \, \Gamma(-2\pi i k \log_2 e)\bigr|$$
$$+ \log_2 e \sum_{0 \neq j \neq k} \bigl|\Gamma\bigl(-2\pi i j \log_2 e\bigr) \, \Gamma\bigl(-2\pi i (k-j) \log_2 e\bigr)\bigr| \Bigr), \quad (6.13)$$

where we have introduced a factor of 2 and reduced the range of summation to positive k. We estimate the terms involving $\Gamma(\cdots)$ using (5.8). For the terms involving $\Gamma'(\cdots)$, we write $\Gamma'(s) = \Gamma(s) \, \psi(s)$, where

$$\begin{aligned} \psi(s) &= \frac{d}{ds} \log \Gamma(s) \\ &= -\gamma - \frac{1}{s} + \sum_{k \geq 1} \frac{s}{k(k+s)}. \end{aligned}$$

Substituting these results in (6.13) yields

$$|G(\nu)| \leq \sum_{k \geq 1} \Biggl(\Bigl(2 \log_2 e \, |\psi(-2\pi i k \log_2 e)| + 2\gamma \log_2 e - 1 \Bigr) \sqrt{\frac{2 \log_2 e}{k \, \sinh(2\pi^2 k \log_2 e)}}$$
$$+ \log_2 e \sum_{0 \neq j \neq k} \sqrt{\frac{1}{j(k-j) \, \sinh\bigl(2\pi^2 j \log_2 e\bigr) \, \sinh\bigl(2\pi^2 (k-j) \log_2 e\bigr)}} \Biggr).$$

The first term in the summand for $k = 1$ in the outer sum is $5.357360\ldots \times 10^{-6}$; the largest contributions from the inner sum for $k = 1$ arise from the terms with $j = -1$ and $j = 2$; these two terms together contribute $1.14159\ldots \times 10^{-18}$; thus the term for $k = 1$ in the outer sum is $5.35736\ldots \times 10^{-6}$. Successive terms in the outer sum decrease by a ratio smaller than the first term (asymptotically, by $\exp(-\pi^2 \log_2 e) = 6.5486\ldots \times 10^{-7}$) so the outer sum, and thus $|G(\nu)|$ for all ν, is at most $5.3573\ldots \times 10^{-6}$.

8. Conclusion

We have presented a new method of analyzing carry propagation that avoids the use of contour integration and residues that have previously been employed for this purpose. Another problem to which this method should be applicable is the analysis of carry propagation when a uniformly distributed n-bit number is tripled by adding it to its double (or is multiplied by some other number with two 1s in its binary representation by adding it to a shifted version of itself). A further problem that we have not succeeded in solving by this method is the evaluation of

$$\sum_{k\geq 1}\left(\frac{1}{e^{n/2^k}-1}-\frac{2^k}{n}+\frac{1}{2}\right)=\tfrac{1}{2}\log_2 n-\tfrac{1}{2}\log_2\pi+\tfrac{1}{2}\gamma\log_2 e-\tfrac{3}{4}+E(\log_2 n)+O\left(\frac{\log n}{n}\right),$$

where

$$E(\nu)=\log_2 e\sum_{k\neq 0}\zeta(-2\pi ik\log_2 e)\,\Gamma(-2\pi ik\log_2 e)\,\exp(2\pi ik\nu),$$

introduced by Knuth [K2] in his analysis of Patricia trees (see also Spankowski [S]). The similarity of this sum to those we have succeeded in analyzing with our method suggests that it may not lie beyond the reach of elementary methods.

9. References

[A] E. Artin, *The Gamma Function*, Holt, Rinehart and Winston, 1964 (translation of *Einfürung in die Theorie der Gammafunktion*, Teubner, 1931).

[B1] B. E. Briley, "Some Results on Average Worst Case Carry", *IEEE Trans. Computers*, 22 (1973) 459–463.

[B2] A. W. Burks, H. H. Goldstein and J. von Neumann, "Preliminary Discussion of the Logical Design of an Electronic Computing Instrument", in: A. H. Taub (Ed.), *Collected Works of John von Neumann*, Macmillan, 1963, v. 5, pp. 34–79.

[C] V. Claus, "Die mittlere Additionsdauer eines Paralleladdierwerks", *Acta Informatica*, 2 (1973) 283–291.

[F1] P. Flajolet, P. Grabner, P. Kirshenhofer, H. Prodinger and R. F. Tichy, "Mellin Transforms and Asymptotics: Digital Sums", *Theoretical Computer Science*, 123 (1994) 291–314.

[F2] P. Flajolet and M. Golin, "Mellin Transforms and Asymptotics: The Mergesort Recurrence", *Acta Informatica*, 31 (1994) 673–696.

[F3] P. Flajolet, X. Gourdon and P. Dumas, "Mellin Transforms and Asymptotics: Harmonic Sums", *Theoretical Computer Science*, 144 (1995) 3–58.

[F4] P. Flajolet and R. Sedgewick, "Mellin Transforms and Asymptotics: Finite Differences and Rice's Integrals", *Theoretical Computer Science*, 144 (1995) 101–124.

[J] A. J. E. M. Janssen and M. J. M. De Jong, "Analysis of Contention Tree Algorithms", *IEEE Trans. on Information Theory*, 46 (2000) 2163–2172.

[K1] D. E. Knuth, "The Average Time for Carry Propagation", *Nederl. Akad. Wettensch. Indag. Math.*, 40 (1978) 238–242.

[K2] D. E. Knuth, *The Art of Computer Programming, Volume 3: Sorting and Searching*, Addison-Wesley, 1998. (In the first (1973) edition of this book, the discussion of radix-exchange sorting contains some errors that are corrected in the second (1998) edition.)

[P] N. Pippenger, "An Elementary Approach to Some Analytic Asymptotics", *SIAM J. Math. Anal.*, 24 (1993) 1361–1377.

[S] W. Spankowski, "Patricia Trees Again Revisited", *J. ACM*, 37 (1990) 691–711.

Appendix

Our goal in this appendix is to show that the asymptotic results in Sections 2, 5 and 6 concerning carry propagation hold without change in the presence of an end-around carry (that is, when a carry out of the most significant bit position propagates into the least significant bit position), and that the exact formulas in Sections 3 and 6 hold with minor revisions.

In the presence of an end-around carry, we have n *cyclic k-blocks*, these being the $n-k+1$ old k-blocks together with $k-1$ new *wrap-around* k-blocks. We shall use primes on various quantities to indicate their versions with an end-around carry. Thus $\mathbf{B}'_{n,k}$ denotes the number of active cyclic k-blocks, $\mathbf{C}'_n$ denotes the length of the longest carry chain with end-around carry, and C'_n and V'_n denote the expectation and variance, respectively, of $\mathbf{C}'_n$.

We begin by oserving that all the results of Section 2 go through with only the change of the number of k-blocks from $n-k+1$ to n. In particular,

$$\Pr[\mathbf{C}'_n \geq k] \leq \min\{1, n/2^{k+1}\} \tag{A.1}$$

and

$$C'_n = \log_2 n + O(1) \tag{A.2}$$

are the revised versions of (2.2) and (2.1), respectively.

To derive (1.11), the revised version of (1.2), we proceed as in Section 3. The analogue of (3.3) is

$$\Pr[\text{some cyclic } k\text{-block is active}] = \sum_{k \geq 1} B_{n,j,k} \, \frac{(-1)^{j-1}}{2^{(k+1)j}}, \tag{A.3}$$

where $B_{n,j,k}$ is the number of choices of j pairwise-disjoint cyclic k-blocks among n positions. In addition to the $A_{n,j,k}$ sets of old k-blocks, we now have those in which one cyclic k-block wraps aound. There are $k-1$ ways i which a cyclic k-block can wrap around, and for each of these there are $A_{n-k,j-1,k}$ choices for the $j-1$ remaining k-blocks among the $n-k$ remaining positions. Thus we have

$$B_{n,j,k} = \binom{n - j(k-1)}{j} + (k-1)\binom{n-1-j(k-1)}{j-1}.$$

Substituting this result into (A.3) yields (1.11). Similarly, we obtain

$$\begin{aligned} V'_n = & \sum_{k \geq 1} (2k-1) \sum_{j \geq 1} \left[\binom{n - j(k-1)}{j} + (k-1)\binom{n-1-j(k-1)}{j-1} \right] \frac{(-1)^{j-1}}{2^{(k+1)j}} \\ & - \left(\sum_{k \geq 1} \sum_{j \geq 1} \left[\binom{n - j(k-1)}{j} + (k-1)\binom{n-1-j(k-1)}{j-1} \right] \frac{(-1)^{j+1}}{2^{(k+1)j}} \right)^2 \end{aligned}$$

as the analogue of (6.3).

To rederive the results of Sections 5 and 6 in the presence of an end-around carry, we must avoid the use of the recurrence (4.7) in Section 4. We do this by directly relating the distributions of $\mathbf{C}_n$ and $\mathbf{C}'_n$, then using the results concerning $\mathbf{C}_n$ derived in Sections 4, 5 and 6. In particular, we shall show that

$$\Pr[\mathbf{C}'_n \geq k] = \Pr[\mathbf{C}_n \geq k] + O\left(\frac{\log n}{n}\right). \tag{A.4}$$

Then, comparing

$$C'_n = \sum_{k \geq 1} \Pr[\mathbf{C}'_n \geq k]$$

and (2.1), using $(A.4)$ for the terms with $k \leq 2\log_2 n$ and $(A.1)$ and (2.2) for the terms with $k > 2\log_2 n$, we obtain

$$C'_n = C_n + O\left(\frac{(\log n)^2}{n}\right),$$

giving the analogue of (1.3) for C'_n. Similarly, we obtain

$$V'_n = V_n + O\left(\frac{(\log n)^3}{n}\right),$$

giving the analogue of (1.10) for V'_n.

To establish $(A.4)$, let the random variable $\mathbf{E}_0$ be a pair of independent uniformly distribued n-bit numbers. For $1 \leq j \leq n-1$, let $\mathbf{E}_j$ denote the result of cyclically shifting the numbers of $\mathbf{E}_0$ to the left by j positions. Let the random variable $\mathbf{E}$ denote the results of choosing one of $\mathbf{E}_0, \ldots, \mathbf{E}_{n-1}$ with equal probability. We observe that $\mathbf{E}_0, \ldots, \mathbf{E}_{n-1}$ and $\mathbf{E}$ all have the same distribution. Let $\mathbf{C}_{n,0}, \ldots, \mathbf{C}_{n,n-1}$ and $\mathbf{C}_n$ denote the length of the longest carry chain in $\mathbf{E}_0, \ldots, \mathbf{E}_{n-1}$ and $\mathbf{E}$, respectively, and let $\mathbf{C}'_{n,0}, \ldots, \mathbf{C}'_{n,n-1}$ and $\mathbf{C}'_n$ denote the length of the longest carry chain with end-around carry in $\mathbf{E}_0, \ldots, \mathbf{E}_{n-1}$ and $\mathbf{E}$, respectively. We observe that this is consistent with our previous uses of $\mathbf{C}_n$ and $\mathbf{C}'_n$.

We have $\mathbf{C}'_{n,0} = \cdots = \mathbf{C}'_{n,n-1} = \mathbf{C}'_n$, since end-around carry chains are not affected by cyclic shifts. Furthermore, we have $\mathbf{C}_{n,j} = \mathbf{C}'_{n,j}$ unless $\mathbf{E}_j$ has a unique longest carry chain that involves an end-around carry, in which case we have $\mathbf{C}_{n,j} < \mathbf{C}'_{n,j}$. When there is a unique longest carry chain of length l, it will involve an end-around carry for exactly $l-1$ of the n values of j. Thus we conclude

$$\Pr[\mathbf{C}_n = l] \geq \Pr[\mathbf{C}'_n = l]\left(1 - \frac{l-1}{n}\right).$$

Summing and using $(A.2)$, we have

$$\begin{aligned}
\Pr[\mathbf{C}_n \geq k] &\geq \Pr[\mathbf{C}'_n \geq k] - \frac{1}{n}\sum_{l \geq k}(l-1)\,\Pr[\mathbf{C}'_n = l] \\
&\geq \Pr[\mathbf{C}'_n \geq k] - \frac{C'_n - 1}{n} \\
&\geq \Pr[\mathbf{C}'_n \geq k] + \left(\frac{\log n}{n}\right).
\end{aligned}$$

Since we obviously have

$$\Pr[\mathbf{C}_n \geq k] \leq \Pr[\mathbf{C}'_n \geq k],$$

we have completed the proof of $(A.4)$.