SIAM J. COMPUT.
Vol. 3, No. 4, December 1974

THE NUMBER OF 1'S IN BINARY INTEGERS: BOUNDS AND EXTREMAL PROPERTIES*

M. D. McILROY†

Abstract. Closed formulas provide tight bounds for $G(n)$, the total number of 1's in the binary representations of integers less than n. This function satisfies an extremal recurrence, which gives the maximum cost of a process that creates a set of n objects by repeatedly merging pairs of smaller sets, starting from n singletons, incurring a cost equal to the size of the smaller set at each merger:

$$G(n) = \max_{1 \leqq i \leqq n/2} [i + G(i) + G(n - i)],$$

where $G(1) = 0$. The set of pairs $(i, n - i)$ at which the maximum is attained has an interesting structure.

Key words. binary numbers, extremal recurrences, set merging

1. Basic recurrences. Let $G(n)$ be the total number of 1's in the list of integers $0, 1, 2, \cdots, n - 1$ expressed in binary notation. Evidently

$$G(2^m) = \tfrac{1}{2}m2^m, \qquad m = 0, 1, \cdots, \tag{1}$$

since the list then consists of all 2^m m-bit patterns of 0's and 1's, among which half the bits are 1's. Given

$$G(1) = 0, \tag{2}$$

the definition of $G(n)$ may be extended to $n = 0, 1, \cdots$ by any of these recurrences.[1]

$$G(2^m + i) = G(2^m) + G(i) + i, \qquad 0 \leqq i \leqq 2^m, \quad m = 0, 1, \cdots, \tag{3}$$

$$G(2n) = n + 2G(n), \qquad n = 0, 1, \cdots, \tag{4a}$$

$$G(2n + 1) = n + G(n) + G(n + 1), \qquad n = 0, 1, \cdots, \tag{4b}$$

$$G(n) = \lfloor n/2 \rfloor + G(\lfloor n/2 \rfloor) + G(\lceil n/2 \rceil), \qquad n = 0, 1, \cdots, \tag{5}$$

$$G(2^m + i) = i(m + 1) + G(2^m - i), \quad 0 \leqq i \leqq 2^m, \quad m = 0, 1, \cdots. \tag{6}$$

(Some cases of (3) or (4) involving $G(0)$ are redundant; they are so written to simplify later calculations.) The recurrence (3) derives from the fact that the binary representation of $2^m + i$, $0 \leqq i < 2^m$, is just the m-bit representation of i prefixed by a 1.

To derive (4b), split the set $\{i | 0 \leqq i < 2n + 1\}$ into an odd part $\{2i + 1 | 0 \leqq i < n\}$ and an even part $\{2i | 0 \leqq i \leqq n\}$. The odd part has n final 1's plus the number of 1's in $\{2i | 0 \leqq i < n\}$, which is just $G(n)$. Similarly, the even part contains $G(n + 1)$ 1's, whence the total number of 1's is $n + G(n) + G(n + 1)$. Recursion (4a) may be derived similarly; (5) merely combines (4a) and (4b).

* Received by the editor September 27, 1973, and in revised form April 2, 1974.

† Bell Laboratories, Murray Hill, New Jersey 07974.

[1] Except for a factor of 2, (4) occurs in another context in [1].

Recursion (6) was pointed out by a referee. It follows from observing that the numbers $2^m + i - 1$ and $2^m - i$ are $(m + 1)$-bit 1's complements and that exactly i such complementary pairs make up the set $\{n|2^m - i \leqq n \leqq 2^m + i - 1\}$.

2. Bounds. The following theorem lends precision to the result $G(n) = \frac{1}{2}n \log_2 n + O(n)$, which was announced by Bellman and Shapiro [2]. The deviation of $G(n)$ from these bounds is shown in Fig. 1.

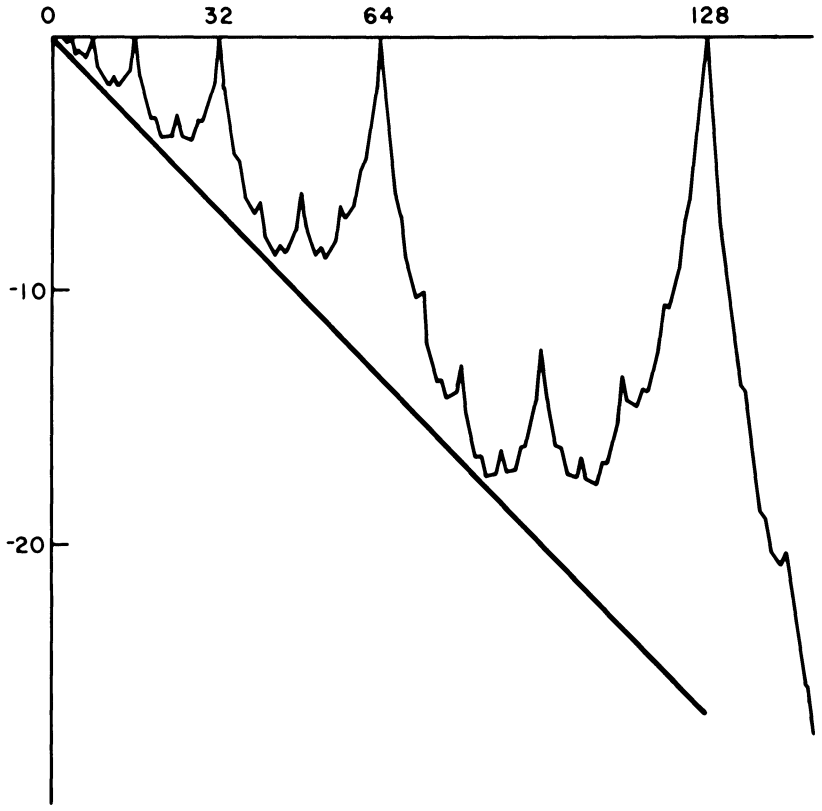

FIG. 1. *The deviation of G(n) from its bounds. The curve represents* $G(n) - \frac{1}{2}n \log_2 n$; *the straight line is* $\frac{1}{2}n \log_2 (\frac{3}{4}n) - \frac{1}{2}n \log_2 n$.

THEOREM 1. *The function G(n) defined above satisfies*

$$\lceil \tfrac{1}{2}n \log_2 (\tfrac{3}{4}n) \rceil \leqq G(n) \leqq \lfloor \tfrac{1}{2}n \log_2 n \rfloor, \qquad n = 0, 1, \cdots, \tag{7}$$

and each bound is tight for infinitely many values of n.[2]

The upper bound in (7) is evidently true for $n = 0$. Relation (1), $G(2^m) = \frac{1}{2}m2^m$, shows that the bound is valid and tight when n is a power of 2. Assuming the upper bound holds up to $n = 2^m$, we have by (3) and (1),

[2] We take $0 \log_2 0$ to be 0.

$$\begin{aligned} G(n+i) &= G(2^m) + G(i) + i && (0 \leqq i \leqq n = 2^m) \\ &\leqq \tfrac{1}{2}m2^m + \tfrac{1}{2}i \log_2 i + i \\ &= \tfrac{1}{2}n \log_2 n + \tfrac{1}{2}i \log_2 i + i \\ &\leqq \tfrac{1}{2}(n+i) \log_2 (n+i) && (0 \leqq i \leqq n = 2^m). \end{aligned}$$

The last inequality follows by considering the function

$$\tfrac{1}{2}(n+x) \log_2 (n+x) - (\tfrac{1}{2}n \log_2 n + \tfrac{1}{2}x \log_2 x + x),$$

which takes on the value 0 at $x = 0$ and $x = n$, and has a negative second derivative with respect to x throughout the open interval $(0, n)$. Thus $\tfrac{1}{2}(n+x) \log_2 (n+x)$ exceeds $\tfrac{1}{2}n \log_2 n + \tfrac{1}{2}x \log_2 x + x$ throughout that interval. The upper bound in (7) follows by induction on powers of 2.

The lower bound in (7) is evidently true for $n = 0$ and $n = 1$. Suppose that a bound of the form

$$G(n) \geqq \tfrac{1}{2}n \log_2 n - cn \tag{8}$$

is true for some $c > 0$ for all $n \leqq 2^m$. Then by (3) and (1),

$$\begin{aligned} G(n+i) &= G(2^m) + G(i) + i && (0 \leqq i \leqq n = 2^m) \\ &\geqq \tfrac{1}{2}m2^m + \tfrac{1}{2}i \log_2 i + i - ci \\ &= \tfrac{1}{2}n \log_2 n + \tfrac{1}{2}i \log_2 i + i - ci \end{aligned}$$

The desired result (8) follows by induction on m, provided that the following inequality holds for $0 \leqq i \leqq 2^m$:

$$\tfrac{1}{2}n \log_2 n + \tfrac{1}{2}i \log_2 i + i - ci \geqq \tfrac{1}{2}(n+i) \log_2 (n+i) - c(n+i).$$

Replace i by xn and simplify to obtain another relation whose truth would imply the result:

$$\tfrac{1}{2}x \log_2 x + x \geqq \tfrac{1}{2}(1+x) \log_2 (1+x) - c, \qquad 0 \leqq x \leqq 1.$$

Since both sides are continuous in x on $[0, 1]$, c can be chosen sufficiently large that the inequality is satisfied throughout the interval. By elementary calculus we find the smallest such c to be $\tfrac{1}{2} \log_2 \tfrac{4}{3}$, whence

$$G(n) \geqq \tfrac{1}{2}n \log_2 n - \tfrac{1}{2}n \log_2 \tfrac{4}{3}.$$

Since $G(n)$ takes on only integer values, we may round the right side up to the nearest integer, thus establishing the lower bound in (7).

The lower bound in (7) is tight for all n such that $|3n - 2^k| = 1$, $k = 0, 1, \cdots$, as may be verified directly for $k = 0$ and proved as follows for positive even k. A similar argument holds for odd k. Let $k = 2m + 2$, so that $v_m = \tfrac{1}{3}(2^{2m+2} - 1) = 2^{2m} + 2^{2m-2} + \cdots + 1$ is an integer satisfying $3v_m - 2^k = -1$. Since $v_m = 2^m + v_{m-1}$, we have by induction on (3) together with (1),

$$\begin{aligned} G(v_m) &= G(2^{2m}) + G(v_{m-1}) + v_{m-1} \\ &= \sum_{k=1}^{m} \frac{1}{2} \cdot 2k2^{2k} + G(v_0) + \sum_{k=0}^{m-1} v_k = \frac{m}{3}(2^{2m+2} - 1). \end{aligned}$$

For comparison, calculate

$$\begin{aligned}\tfrac{1}{2}v_m \log_2(\tfrac{3}{4}v_m) &= \tfrac{1}{2}\cdot\tfrac{1}{3}(2^{2m+2}-1)\log_2(\tfrac{1}{4}(2^{2m+2}-1))\\ &= \tfrac{1}{2}\cdot\tfrac{1}{3}(2^{2m+2}-1)[2m+\log_2(1-2^{-2m-2})]\\ &= \frac{m}{3}(2^{2m+2}-1)+\frac{1-2^{-2m-2}}{6\log 2}\sum_{j=1}^{\infty}\frac{(-1)^j}{j}2^{-2(m+1)(j-1)}\\ &= G(v_m)+\frac{1-2^{-2m-2}}{6\log 2}S,\end{aligned}$$

where S is the sum of the alternating series. For all $m \geqq 0$, $-1 < S \leqq 0$. It follows that

$$0 \leqq G(v_m) - \tfrac{1}{2}v_m \log_2(\tfrac{3}{4}v_m) \leqq \frac{1}{6\log 2}.$$

Since $1/(6\log 2) = .2404\cdots$ is less than 1, and $G(v_m)$ is an integer, $G(v_m)$ must in fact equal $\lceil \tfrac{1}{2}v_m \log_2(\tfrac{3}{4}v_m)\rceil$.

3. A set merging process. In various graph-theoretic algorithms, the following merging process occurs [3]. Start with n sets, each containing exactly one member. At step i, $i = 1, 2, \cdots, n-1$, merge any two sets. A cost equal to the size of the smaller set is incurred at each step. The maximum cost $\bar{G}(n)$ that can be incurred in the whole process is defined by

$$\bar{G}(1) = 0, \qquad \bar{G}(n) = \max_{1 \leqq i \leqq n/2}[i + \bar{G}(i) + \bar{G}(n-i)], \quad n = 2, 3, \cdots. \tag{9}$$

It turns out that $\bar{G}(n)$ is the same as $G(n)$ for $n = 1, 2, \cdots$. Given this fact, and noting that recurrences (3) and (4) both look like (9) with the max operation removed, we can read off two different cost-maximizing policies:

(a) Merge a set whose size is a power of 2 with a set of equal or smaller size.

(b) Merge two sets whose size differs by at most one.

Each of these policies is a special case of the general policy set forth in Theorem 2 below.

4. Proof of extremality. To prove that the extremal property (9) is possessed by $G(n)$, consider the function

$$F(p, q) = G(p+q) - [p + G(p) + G(q)], \qquad 0 \leqq p \leqq q. \tag{10}$$

$F(p, q)$ is the "deficiency" by which the cost of a set of $p + q$ elements would fall short of $G(p+q)$ if that set were created by merging sets of size p and q created by extremal routes whose costs were $G(p)$ and $G(q)$. A recurrence for $F(p, q)$ follows from substituting (5) into (10).

$$F(p,q) = \left\lfloor \frac{p+q}{2} \right\rfloor + G\left(\left\lfloor \frac{p+q}{2} \right\rfloor\right) + G\left(\left\lceil \frac{p+q}{2} \right\rceil\right)$$
$$- \{p + \lfloor p/2 \rfloor + G(\lfloor p/2 \rfloor) + G(\lceil p/2 \rceil) + \lfloor q/2 \rfloor + G(\lfloor q/2 \rfloor) + G(\lceil q/2 \rceil)\}$$
$$= G\left(\left\lfloor \frac{p+q}{2} \right\rfloor\right) - \{\lfloor p/2 \rfloor + G(\lfloor p/2 \rfloor) + G(\lceil q/2 \rceil)\}$$
$$+ G\left(\left\lceil \frac{p+q}{2} \right\rceil\right) - \{\lceil p/2 \rceil + G(\lceil p/2 \rceil) + G(\lfloor q/2 \rfloor)\}$$
$$+ \left\{\left\lfloor \frac{p+q}{2} \right\rfloor + \lceil p/2 \rceil - p - \lfloor q/2 \rfloor\right\}.$$

The last bracketed quantity is 1 when both p and q are odd and is 0 otherwise, so can be more compactly written as $pq \pmod 2$. Unless p is even and q is odd, the middle line is exactly $F(\lfloor p/2 \rfloor, \lceil q/2 \rceil)$ and the next is $F(\lceil p/2 \rceil, \lfloor q/2 \rfloor)$. But in that special case exchange the places of

$$G\left(\left\lfloor \frac{p+q}{2} \right\rfloor\right) \quad \text{and} \quad G\left(\left\lceil \frac{p+q}{2} \right\rceil\right)$$

to see the same thing. Thus

$$F(p,q) = F(\lfloor p/2 \rfloor, \lceil q/2 \rceil) + F(\lceil p/2 \rceil, \lfloor q/2 \rfloor) + (pq \pmod 2), \quad 0 \leqq p < q. \tag{11a}$$

The domain must be restricted to $0 \leqq p < q$ lest $F(\lceil p/2 \rceil, \lfloor q/2 \rfloor)$ go outside the original domain of (10) when $p = q$. The boundary conditions[3]

$$F(p,p) = F(p,p+1) = F(0,q) = 0, \qquad p,q = 0,1,\cdots, \tag{11b}$$

follow from the facts that

$$G(2p+1) = p + G(p) + G(p+1), \quad G(2p) = p + 2G(p), \quad G(1) = G(0) = 0.$$

We are now in a position to justify the assertion that $G(n)$ is indeed the largest cost that can be incurred in the merging problem, or that $G(n)$ satisfies (9). The proof by induction on G assumes that G satisfies (9) up to $n-1$. Then

$$\max_{1 \leqq i \leqq n/2} [i + G(i) + G(n-i)] = G(n) - \min_i [G(n) - i - G(i) - G(n-i)] \tag{12}$$
$$= G(n) - \min_i F(i, n-i)$$

Now by (11), F is obviously nonnegative, and by (11b), F does take on the value zero at (i,i) or $(i,i+1)$, whence expression (12) is exactly $G(n)$.

5. Extremal policies. The set of maximum cost merges is the set of pairs (p,q) with $0 \leqq p \leqq q$ such that $G(p+q) = p + G(p) + G(q)$, or equivalently,

[3] These conditions are not mutually independent. An independent set would be $F(p,p) = F(0,1) = 0$.

such that $F(p, q) = 0$. When p and q are both odd and unequal, (11a) shows $F(p, q)$ to be nonzero. For other (p, q) we must chase the recurrence down to an unequal odd pair to show that $F(p, q) \neq 0$, or else chase all paths to the boundary (11b) without encountering such a pair to show that $F(p, q) = 0$.

It is easy to verify that as long as the first member of the pair remains even, n-fold application of (11a) visits only the points $(p/2^i, \lfloor q/2^i \rfloor)$ and $(p/2^i, \lceil q/2^i \rceil)$, $i = 1, 2, \cdots, n$. Now suppose that p and q may be represented by $p = 2^a p_0$ and $q = 2^b q_0$, where $a \geqq b$ and p_0 and q_0 are both odd. Then the recurrence cannot reach an odd pair until the ath iteration, where we will have typical terms $F(p_0, \lfloor q/2^a \rfloor)$ and $F(p_0, \lceil q/2^a \rceil)$. If $\lfloor q/2^a \rfloor$ is odd, then for $F(p, q)$ to be zero we must have $\lfloor q/2^a \rfloor = p_0$. If $\lfloor q/2^a \rfloor$ is even, then $\lceil q/2^a \rceil$ is odd, since otherwise q_0 would have been even, and hence $F(p, q)$ is nonzero. Similarly if $a < b$, we find that $F(p, q)$ is nonzero unless $\lfloor p/2^b \rfloor = q_0 - 1$. In other words, $F(p, q)$ is zero if and only if

$$p = 2^a p_0 \quad \text{and} \quad q \in \{p, p + 1, \cdots, p + 2^a - 1\}, \qquad a = 0, 1, 2, \cdots, \quad p_0 \text{ odd},$$

or

$$q = 2^b q_0 \quad \text{and} \quad p \in \{q - 2^b + 1, \cdots, q - 1, q\}, \qquad b = 0, 1, 2, \cdots, \quad q_0 \text{ odd},$$

or

$$p = 0.$$

Stated still another way for nonzero p and q, this criterion is Theorem 2.

THEOREM 2. *Let a set of n objects be created by $n - 1$ merges of pairs of sets starting from n singletons. If a cost equal to the size of the smaller of the pair is incurred at each step, then the maximal total cost for the process is $G(n)$ and is achieved if and only if for every merged pair, the sizes of the two sets differ by less than the largest power of 2 that divides one of the two sizes.*

The locus of maximal cost merges makes the interesting recursive pattern shown in Fig. 2.

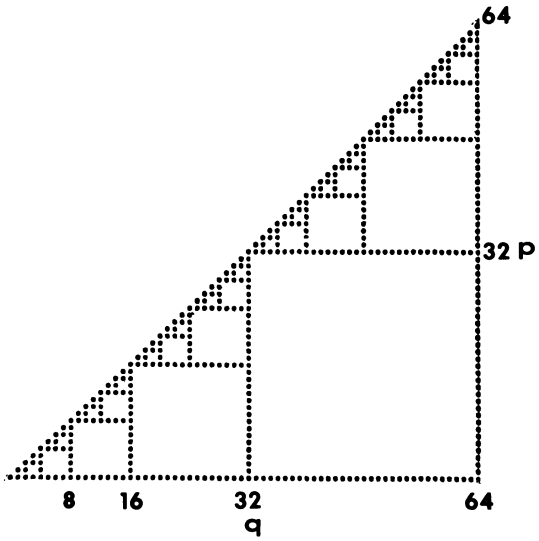

FIG. 2. *Maximum cost merging strategies. Dots mark all places where the inequality $G(p + q) \geqq p + G(p) + G(q)$ is tight.*

6. Related work. Hopcroft and Ullman have a "practically linear" algorithm for performing the bookkeeping connected with the set-merging process [4]. Functions or extremal recurrences similar to $G(n)$ have been studied in [5]–[8].

REFERENCES

[1] E. N. GILBERT, *Games of identification and convergence*, SIAM Rev., 4 (1962), pp. 16–24.
[2] R. BELLMAN AND H. N. SHAPIRO, *On a problem in additive number theory*, Ann. of Math., 49 (1948), pp. 333–340.
[3] D. E. KNUTH, *Complexity analysis of equivalence algorithms*, Unpublished notes, Mathematisk Institutt, Blindern, Norway, 1972.
[4] J. E. HOPCROFT AND J. D. ULLMAN, *Set merging algorithms*, this Journal, 2 (1973), pp. 294–303.
[5] M. L. FREDMAN AND D. E. KNUTH, *Recurrences based on minimization*, CS–72–248, Dept. of Computer Sci., Stanford Univ., Stanford, Calif., 1971.
[6] E. WONG, *A linear search problem*, SIAM Rev., 6 (1964), pp. 168–174.
[7] R. MORRIS, *Some theorems on sorting*, SIAM J. Appl. Math., 17 (1967), pp. 1–6.
[8] L. CARLITZ, *A sorting function*, Duke Math. J., 38 (1971), pp. 561–568.