ON ADDITION CHAINS $l(mn) \leqq l(n) - b$ AND LOWER BOUNDS FOR $c(r)$

EDWARD G. THURBER

An addition chain for a positive integer n is a set $1 = a_0 < a_1 < \cdots < a_r = n$ of integers such that each element a_i is the sum $a_j + a_k$ of two preceding members (not necessarily distinct) of the set. Let $l(n)$ denote the minimal r for which an addition chain for n exists. Let $\lambda(n) = [\log_2 n]$ and $\nu(n)$ denote the number of ones in the binary representation of n. Also, let $c(r)$ denote the first integer which requires r steps in an addition chain of minimal length.

The purpose of this paper is to explore two areas in the study of addition chains. First, D. E. Knuth states [2; p. 416] that it seems reasonable to conjecture that $l(2n) \geq l(n)$ and, more generally, that $l(mn) \geq l(n)$. It is now known that the inequality $l(mn) \geq l(n)$ is not true for all m and n, and it will be shown, in fact, that if b is an arbitrary nonnegative integer and $m = 2^{2k+1} + 1$ for an arbitrary nonnegative integer k, then there exist infinitely many infinite classes of integers n for which $l(mn) \leq l(n) - b$. Secondly, a set of lower bounds for $c(r)$ will be developed. An upper bound result for $l(n)$ which is an improvement over the one obtained by using the m-ary chain [2] will be derived and then used in developing the set of lower bounds for $c(r)$.

Step i in an addition chain is $a_i = a_j + a_k$ for some $k \leq j < i$. Clearly, $a_i \leq 2a_j \leq 2a_{i-1}$. Thus, either $\lambda(a_i) = \lambda(a_{i-1})$ or $\lambda(a_i) = \lambda(a_{i-1}) + 1$. If $\lambda(a_i) = \lambda(a_{i-1})$, Knuth [2; p. 405] calls step i a small step. If $\lambda(a_i) = \lambda(a_{i-1}) + 1$, step i will be called a big step. Knuth [2; p. 405] has pointed out that the length r of an addition chain for n is $\lambda(n)$ plus the number of small steps in the chain. If $N(a_i)$ denotes the number of small steps in the chain up to a_i, then $r = \lambda(n) + N(n)$.

If in an addition chain $a_i = 2a_{i-1}$, then step i is called a doubling. Otherwise, step i shall be called a nondoubling. If $a_k < a_j$ are two members of an addition chain and there are at least four nondoublings from a_k to a_j, then it is not hard to show that $a_j \leq 2^{j-k-4}(8a_k - 3)$. From this it follows that $a_j < 2^{j-k-1}a_k$ which implies that $\lambda(a_j) - \lambda(a_k) \leq j - k - 1$. The number of big steps in the chain from a_k to a_j is $\lambda(a_j) - \lambda(a_k)$ while $j - k$ is the total number of steps in the chain from a_k to a_j. Thus, there must be at least one small step from a_k to a_j. This result is a generalization of Stolarsky's [3; Lemma 1] and may be summarized by saying that if $a_k < a_j$ are two members of an addition chain and there are at least four nondoublings from a_k to a_j, then $N(a_j) \geq N(a_k) + 1$.

It has been proved [4] that if $\nu(n) \geq 9$, then $l(n) \geq \lambda(n) + 4$. In other words if $\nu(n) \geq 9$, then there are at least four small steps in any chain for n. This

Received May 14, 1973.