On Addition Chains

1978

Rolf Sonntag, Richard-Wagner-Str. 27, D-3000 Hannover 1, West Germany

1. An addition chain for a positive integer n is a sequence $1=a_0<a_1<\ldots<a_r=n$ of integers such that for each $i\geq 1$, $a_i = a_j + a_k$ for some $k \leq j < i$. Define $\ell(n)$ to be the minimal length r for which an addition chain for n exists. For $r \geq 0$, let $c(r)$ be the minimal value of n such that $\ell(n) = r$ and let $d(r)$ be the number of solutions n to the equation $\ell(n) = r$ (cf. KNUTH (1969a)).

Theorem 1. If $r \geq 9$ then $2^{\lfloor \frac{r}{2} \rfloor} \leq c(r) \leq 2^{r-3} + 7$

This theorem follows from a result of GIESE (1974). An improvement of the lower bound for $c(r)$ was given by THURBER (1973).

2. UTZ (1953) conjectured that $d(r) < d(r+1)$ for all $r > 0$. KNUTH (1969a/b) computed the values of $d(r)$ for $r \leq 15$, and asked for the asymptotic growth of $d(r)$ (unsolved problem 33, p. 422).
It seems very difficult to show even Utz's conjecture, but the results of BRAUER (1939), UTZ (1953), GIOIA, SUBBARAO, SUGUNAMMA (1962), and KNUTH (1969a) allow the following lower bound:

Theorem 2. If $r > 11$ then $d(r) \geq \frac{r}{6}(r^2 - 9r + 44) - 10$

This bound covers all integers n with $\ell(n) = r$ and $\nu(n) < 4$, where $\nu(n)$ is the number of ones in the binary expansion of n. So theorem 2 (and the theorems below) could be improved immediately, if the integers n with $\ell(n) = r$ could be characterized exactly for $\nu(n) > 4$. Now since this is a somehow intricate way, a new and different attempt is necessary.

Theorem 3. If $r > 5$ then $d(r) \leq 2^{r-2} + (r-2)^2 + (r-1) - \sum_{0\leq i<r} d(i)$

Corollary 4. If $r > 3$ then $d(r) \leq 2^{r-2} - \frac{r}{24}(r^2(r-14) + 83r - 262) - 13$.

<u>Theorem 5.</u> If $r \geq 7$ then $d(r) \leq 2^{r-2} + (r-2)^2 - c(r)$.

This bound is weaker than theorem 3, but if $c(r)$ is eliminated by the lower bound of THURBER (1973), the result is asymptotically better than corollary 4. Summary:

<u>Corollary 6.</u> If $r \geq 8$ then $\frac{1}{6}(r-4)^2 < d(r) < 2^{r-2} - 2^{\lfloor \frac{r}{2} \rfloor} + (r-2)^2$.

There is still a large gap between lower and upper bound!

3. For $n \geq 1$, let $q(n)$ be the number of addition chains of minimal length $\ell(n)$.
For example, $q(7) = 5$ (minimal addition chains for 7: 1,2,3,4,7; 1,2,3,5,7; 1,2,3,6,7; 1,2,4,5,7; 1,2,4,6,7).

<u>Theorem 7.</u> (1) If $\nu(n) = 1$ then $q(n) = 1$.
(2) If $\nu(n) = 2$, i.e. $n = 2^A + 2^B$ $(A > B \geq 0)$,
then

$$q(n) = \begin{cases} \frac{A}{2}(A+1) - 3 & \text{if } B = A - 3 \\ A & \text{if } B = A - 1 \\ 2(B+1) & \text{otherwise} \end{cases} .$$

If $r \leq 8$ then $d(r) = 2^{-(r-2)} \cdot \left(\sum_{n \text{ with } \ell(n)=r} q(n) \right)$.

A minimal addition chain starts with 1,2,3,... or 1,2,4,... .
Therefore, let $q_3(n)$ be the number of minimal addition chains with $a_2 = 3$, and define $q_4(n)$ for $a_2 = 4$ likewise. Then, $q(n) = q_3(n) + q_4(n)$.

<u>Theorem 8.</u> (1) If $\nu(n) = 1$ then $q_3(n) = 0$, $q_4(n) = 1$.
(2) If $\nu(n) = 2$, i.e. $n = 2^A + 2^B$ $(A > B \geq 0)$,
then

$$\begin{array}{lll} q_3(n) = 1 \ , & q_4(n) = A - 1 & \text{if } B = A - 1 \\ q_3(n) = 1 \ , & q_4(n) = 2B + 1 & \text{if } B = A - 2 \\ q_3(n) = A-2 \ , & q_4(n) = \frac{A}{2}(A-1) - 1 & \text{if } B = A - 3 \\ q_3(n) = 0 \ , & q_4(n) = 2(B+1) & \text{otherwise} \end{array} .$$

This author has conjectured that $\eta_4(n) \geq 1$ for all $n \geq 4$, but he is only able to prove it true for $v(n) \leq 2$ (theorem 8) and for $n \leq 133$ (by computer calculations). If this conjecture is true, then it possibly leads to a simpler algorithm for computing addition chains.

(Proofs and further results are available in
Rolf Sonntag, "Theorie der Additionsketten", Diplomarbeit, August 1978,
Technische Universität Hannover, West Germany)

Bibliography of Addition Chains

(abbreviations: MR - Mathematical Reviews, Zbl - Zentralblatt für Mathematik und ihre Grenzgebiete/Mathematics Abstracts)

BELAGA, E.G. (1976) "Additivnaja složnost' natural'nogo čisla" (The Additive Complexity of a Natural Number), Dokl. Akad. Nauk SSSR 226,1 (1976) 15-18 (English translation in Sov. Math. Dokl. 17,1 (1976) 5-9) <MR 53 #13141; Zbl 341 #10045>

BELLMAN, R. (1963) "Problem 5125", Amer. Math. Monthly 70 (1963) 765

BRAUER, A. (1939) "On Addition Chains", Bull. Amer. Math. Soc. 45 (1939) 736-739 <MR 1, 40; Zbl 22, 111>

COTTRELL, A. (1973) "A Lower Bound for the Scholz-Brauer Problem", Ph. D. Dissertation, Univ. of Calif., Berkeley (1974) (preliminary report in Not. Amer. Math. Soc. 20 (1973) A476)

DOBKIN, D. and LIPTON, R. (1977) "Addition Chain Methods for the Evaluation of Specific Polynomials", Conf. on Theor. Comp. Sci. (1977)

ERDÖS, P. (1960) "Remarks on Number Theory III - On Addition Chains", Acta Informatica 6 (1960) 77-81 <MR 22 #12085; Zbl 219 #10064>

GIESE, R.P. (1972) "Selected Topics in Addition Chains", Ph. D. Dissertation, Univ. of Houston, Texas (1974) (preliminary report in Not. Amer. Math. Soc. 19 (1972) A688)

GIESE, R. and WHYBURN, C. "Über Additionsketten", Houston

GIOIA, A.A., SUBBARAO, M.V. and SUGUNAMMA, M. (1962) "The Scholz-Brauer Problem in Addition Chains", Duke Math. J. 29 (1962) 481-487 <MR 25 #3898; Zbl 108, 47>

GIOIA, A.A. and SUBBARAO, M.V. (1975) "The Scholz-Brauer Problem in Addition Chains II", Western Michigan Univ. and Univ. of Alberta (abstract in Not. Amer. Math. Soc. 22 (1975) A63-A64)

HANSEN, W. (1959) "Zum Scholz-Brauerschen Problem", J. für die reine u. angew. Math. 202 (1959) 129-136 <MR 25#2027; Zbl 98, 262>

HEBB, K.R. (1974) "Some Results on Addition Chains", M. Sc. Thesis, Univ. of Edmonton, Alberta (1974) (preliminary report in Not. Amer. Math. Soc. 21 (1974) A294)

IL'IN, A.M. (1965) "Ob additivnych cepočkach čisel" (On Additive Number Chains), Probl. Kibernetiki 13 (1965) 245-248 <MR 34#2552>

KATO, H. (1970) "On Addition Chains", Ph. D. Dissertation, Univ. of Southern Calif., Los Angeles (1970)

KNUTH, D.E. (1962) "Evaluation of Polynomials by Computer", Comm. ACM 5 (1962) 595-599 <MR 27#970; Zbl 106, 315>

KNUTH, D.E. (1969a) "The Art of Computer Programming, Vol. 2: Seminumerical Algorithms", Addison-Wesley (1969) <MR 44#3531; Zbl 191, 180>

KNUTH, D.E. (1969b) "Calculations on Addition Chains", Stanford Univ. (1969)

LEEUWEN, J.v. (1977) "An Extension of Hansen's Theorem for Star Chains", J. für die reine u. angew. Math. 295 (1977) 202-207 <Zbl 355#10040>

LEEUWEN, J.v. (1978) "Evaluating a Polynomial and its Reverse", SIGACT News 10,1 (1978) 18-21

LIPTON, R.J. and DOBKIN, D. (1975) "Complexity Measures and Hierarchies for the Evaluation of Integers and Polynomials", Seventh Ann. ACM Symp. on Th. of Computing (1975) 1-5 <MR 55#6950> , Theor. Comp. Sci. 3 (1976) 349-357 <MR 56#1802; Zbl 365#68049>

MC CARTHY, D.P. (1977) "The Optimal Algorithm to Evaluate x^n Using Elementary Multiplication Methods", Math. Comp. 31,137 (1977) 251-256 <MR 55#1811; Zbl 348#65041>

PIPPENGER, N. (1976) "On the Evaluation of Powers and Related Problems", Symp. on Found. of Comp. Sci. (1976) 258-263

SCHÖNHAGE, A. (1975) "A Lower Bound for the Length of Addition Chains", Theor. Comp. Sci. 1 (1975) 1-12 <Zbl 307#68032>

SCHOLZ, A. (1937) "Aufgabe Nr. 253", Jahresbericht d. deutschen Mathematiker-vereinigung 47 (1937) 41-42

SOUTHARD, T.H. (1974) "Addition Chains for the First n Squares", Univ. of Texas at Austin, Techn. Report CNA-84 (1974)

STOLARSKY, K.B. (1969) "A Lower Bound for the Scholz-Brauer Problem", Can. J. of Math. 21 (1969) 675-683) <MR 40#114; Zbl 179, 69>

STRAUS, E.G. (1964) "Partial Solution of Problem 5125", Amer. Math. Monthly 71 (1964) 806-808

THURBER, E.G. (1971a) "The Scholz-Brauer Problem on Addition Chains", Ph. D. Dissertation, Univ. of Southern Calif., Los Angeles (1971)

THURBER, E.G. (1971b) "The Scholz-Brauer Problem on Addition Chains", Pac. J. of Math. 49 (1973) 229-242 (preliminary report in Not. Amer. Math. Soc. 18 (1971) 1100) <MR 49#7233; Zbl 277#10040>

THURBER, E.G. (1973) "On Addition Chains $\ell(mn) \leq \ell(n) - b$ and Lower Bounds for $c(r)$", Duke Math. J. 40 (1973) 907-913 (preliminary report in Not. Amer. Math. Soc. 20 (1973) A318) <MR 48#8429; Zbl 275#10027>

THURBER, E.G. (1975) "Addition Chains and Solutions of $\ell(2n) = \ell(n)$ and $\ell(2^n-1) = n + \ell(n) - 1$", Discr. Math. 16 (1976) 279-289 (preliminary report in Not. Amer. Math. Soc. 22 (1975) A6) <MR 55#5570; Zbl 346#10032>

UTZ, W.R. (1953) "A Note on the Scholz-Brauer Problem in Addition Chains", Proc. Amer. Math. Soc. 4 (1953) 462-463 <MR 14, 949; Zbl 50, 269>

VAL'SKIJ, R.E. (1959) "O naimen'šem čisle ymnoženij dlja vozvodenija v danyju stepen'" (On the Least Number of Multiplications for Raising to a Given Power), Probl. Kibernetiki 2 (1959) 73-74 (german translation in Probl. der Kybernetik 2 (1963) 79-81) <MR 23#A875>

VEGH, E. (1975) "A Note on Addition Chains", J. Comb. Th. (A) 19 (1975) 117-118 (preliminary report in Not. Amer. Math. Soc. 22 (1975) A2-A3) <MR 51 #12771; Zbl 302#05005>

WRENCH, J.W. (1970) "Table Errata", Math. Comp. 24,110 (1970) 504 <MR 53#4473>

WHYBURN, C.T. (1965) "A Note on Addition Chains", Proc. Amer. Math. Soc. 16 (1965) 1134 <MR 31#4752>

YAO, A.C.-C. (1976) "On the Evaluation of Powers", SIAM J. Comput. 5,1 (1976) 100-103 <MR 52#16128; Zbl 326#68025>