JOURNAL OF ALGORITHMS 2, 13–21 (1981)

On Vectorial Addition Chains

JORGE OLIVOS

*Departamento de Matematicas, Universidad de Chile, Casilla 5272-Correo 3, Santiago, Chile**

Received May 8, 1980

We prove the equivalence between the problem of computing a multinominal $x_1^{n_1} \cdot x_2^{n_2} \cdots x_k^{n_k}$, posed by R. E. Bellman (*Amer. Math. Monthly* **70** (1963), 765), and the problem of computing simultaneously the monomials $x^{n_1}, \ldots, x^{n_k}$, posed by D. E. Knuth ("Seminumerical Algorithms," Sect. 4.6.3, Addison-Wesley, Reading, Mass., 1969.

1. INTRODUCTION

A vectorial addition chain in $\mathbb{N}^k$ is a sequence of different elements $V = (v_i;\ -k+1 \leq i \leq s)$, where $(v_i;\ -k+1 \leq i \leq 0)$ is the canonical basis of $\mathbb{R}^k$, also written $e_i = v_{1-i}$, $1 \leq i \leq k$, and each vector v_i, $i > 0$, is equal to the sum $v_j + v_h$ of two earlier ones, $j, h < i$. The integer s is called the length of the chain, and if V is a chain of minimal length for $v_s = [n_1, \ldots, n_k]$ we write $l([n_1, \ldots, n_k]) = s$.

EXAMPLE 1.1. The following sequence is a vectorial addition chain of length 9 for [7, 15, 23]:

$$[0,0,1],\ [0,1,0],\ [1,0,0],\ [0,1,1],\ [1,1,1],\ [0,1,2],$$
$$[1,2,3],\ [1,3,5],\ [2,4,6],\ [3,7,11],\ [4,8,12],\ [7,15,23].$$

We can use a vectorial addition chain V for $v = [n_1, \ldots, n_k]$ to build a succession of multiplicative binary operations that allow us to compute the multinomial $x_1^{n_1} \cdot x_2^{n_2} \cdots x_k^{n_k}$, given $x_1, \ldots, x_k$; see Bellman [1] and Straus [10]. Using the above example we get a sequence that computes $x^7 y^{15} z^{23}$. A one-dimensional addition chain $Z = (z_i; 0 \leq i \leq p)$ of length p, where $z_0 = 1$, for $n_1, \ldots, n_k$ satisfies the following property: for all $j = 1, \ldots, k$; $n_j = z_q$ for some q, $0 \leq q \leq p$, and for some $1 \leq j \leq k$ we have $n_j = z_p$. If Z is of minimal length for $r_1, \ldots, n_k$ we write $l(n_1, \ldots, n_k) = p$.

*This research was performed while the author was visiting at the Laboratoire de Recherche en Informatique, Orsay, France.

0196-6774/81/010013-09$01.00/0

EXAMPLE 1.2. The following sequence is a one-dimensional addition chain of length 7 for 7, 15, 23: $1, 2, 3, 4, \underline{7}, 8, \underline{15}, \underline{23}$. A very simple computation shows that this chain is a minimal one; then $l(7, 15, 23) = 7$. We can use a one-dimensional addition chain Z for $n_1, \ldots, n_k$ to build a sequence of multiplications allowing us to compute simultaneously the monomials $x^{n_1}, \ldots, x^{n_k}$, given x. See Knuth [4], Pippenger [6, 7], and Yao [11]. Those two problems generalize the question of addition chains (see Brauer [2], Erdös [3], Scholz [8] and Schönhage [9]). Our aim in this paper is to complete the preliminary version (cf. [5]) of the following:

THEOREM 1. *Let* $[n_1, \ldots, n_k] \in \mathbb{N}^k$; *then*

$$l([n_1, \ldots, n_k]) = l(n_1, \ldots, n_k) + (k - 1).$$

2. PROOF OF THEOREM 1

We divide the proof into three lemmas. The first lemma builds a vectorial addition chain from a one-dimensional addition chain. In the third lemma we construct the inverse procedure, after introducing the concept of memory coefficient.

In order to have unicity for the summands in the computation of each element of a chain, we will choose among all sequences of summands realizing the chain a particular one and associate it with the chain (see Example 2.1).

LEMMA 1. *Let* $[n_1, \ldots, n_k] \in N^k$; *then*

$$l([n_1, \ldots, n_k]) \leq l(n_1, \ldots, n_k) + (k - 1). \tag{1}$$

Proof. We can suppose, without any loss of generality, that $n_i \neq n_j$, for $i \neq j$, $1 \leq i, j \leq k$. In fact, each repetition does not affect the length of the one-dimensional addition chain and implies that both k and the length of the vectorial addition chain increase by one unit each.

The proof of the lemma is in two parts:

(i) We prove by induction that if $Z = (z_i; 0 \leq i \leq p)$ is a one-dimensional addition chain, then there exists a vectorial addition chain for $[z_0, \ldots, z_p]$ of length less or equal to $2p$.

(ii) We use this result to conclude the proof by building a vectorial addition chain for $[n_1, \ldots, n_k]$ of length less than or equal to $l(n_1, \ldots, n_k) + (k - 1)$.

Part (i). The assertion is trivial for $p = 0$. Let us suppose it is true for $p - 1$; let $V = (v_i; p + 1 \leq i \leq 2p - 2)$ be a vectorial addition chain for $v_{2p-2} = [z_0, \ldots, z_{p-1}]$.

Let $z_p = z_j + z_h$ for some $j, h < p$, built from the sequence of summands realizing Z. Next we do the following transformation on every vector of V:

(a) If $j \neq h$: $v_i \to v_i' = [v_i, \pi_j(v_i) + \pi_h(v_i)]$,

where $\pi_j(v)$ denotes the $(j+1)$st component of the vector v. The only elements which leave the basis in this transformation are e_{j+1} and e_{h+1}. The elements of the new chain are renumbered with the following convention for $j < h$: $[e_{j+1}, 1] = v_1'$, $[e_{h+1}, 1] = v_2'$ and $v_i' \to v_{i+2}'$ for all $0 \leq i \leq 2p-2$. We complete the basis by adding $[e_{j+1}, 0] = v'_{-j}$, $[e_{h+1}, 0] = v'_{-h}$ and $e_{p+1} = v'_{-p}$.

(b) If $j = h$: $v_i \to v_i' = [v_i, 2\pi_j(v_i)]$,

the only vector leaving the basis is e_{j+1} but to get $[e_{j+1}, 2]$ from the new basis we must include $2e_{p+1}$ or $[e_{j+1}, 1]$. From now on we choose the first alternative. We renumbered the vectors as follows:

$$v_1' = 2e_{p+1}, \qquad v_2' = [e_{j+1}, 2], \qquad v_i' \to v_{i+2}' \qquad \text{for all } 0 < i \leq 2p-2;$$

Finally we complete the basis with $v'_{-p} = e_{p+1}$ and $v'_{-j} = [e_{j+1}, 0]$.

It follows from this construction that $V' = (v_i'; -p \leq i \leq 2p)$ is effectively a vectorial addition chain for $v = [z_0, \ldots, z_p]$, in which the length is $2p$; which proves the first part of the lemma.

Part (ii). Let $Z = (z_i; 0 \leq i \leq p)$ be a one-dimensional addition chain of minimal length for $n_1, \ldots, n_k$; so, by definition $l(n_1, \ldots, n_k) = p$. If $V = (v_i; -p \leq i \leq s)$ is a vectorial addition chain of minimal length for $v_s = [z_0, \ldots, z_p]$ we can build a vectorial addition chain for $[n_1, \ldots, n_k]$ by eliminating from each vector of V all the components corresponding to those of v_s not belonging to $(n_i; 1 \leq i \leq k)$. When we eliminate from V the jth component of each vector v_i, we have at least one repetition: in fact, let $v_i = e_j + v_h$ for $i > 0$ be the first element of the chain V, using e_j, to be computed; then after the elimination of the jth component, the new vectors v_i' and v_h' are identical; thus the length of the new chain has actually decreased by at least one unit.

Then, after $p + 1 - k$ eliminations we get a chain for $[n_1, \ldots, n_k]$ with length less than or equal to

$$s - (p + 1 - k) = l([z_0, \ldots, z_p]) - (p + 1 - k).$$

Hence

$$l([n_1, \ldots, n_k]) \leq l([z_0, \ldots, z_p]) - (p + 1 - k)$$

and from the first part of the lemma we get

$$l([n_1,\ldots,n_k]) \leq 2p - (p+1-k) = p + (k-1),$$

which concludes the proof.

The two following examples illustrate the first lemma.

EXAMPLE 2.1. We construct, by recurrence, a vectorial addition chain for $v = [1,2,3,4,7,8,15,23]$. Each transformation is denoted by the key Γ and we do not write the vector of the basis. The right column shows the sequence of summands used in the construction of the chain Z.

$\rightarrow V$

1	1	1	2	2	2	2	2	5	6	11	6	12	23	(15, 8):23 = 15 + 8
0	1	1	1	1	2	2	2	3	4	7	4	8	15	(8, 7)
1	0	0	1	1	1	1	1	2	2	4	2	4	8	(7, 1) ↑
0	0	1	0	0	1	1	1	1	2	3	2	4	7	(4, 3) Z
0	0	0	0	0	0	0	1	1	1	2	1	2	4	(3, 1)
0	0	0	0	0	0	1	0	0	1	1	1	2	3	(2, 1)
0	0	0	0	0	0	0	0	0	0	0	1	2	2	(1, 1)
0	0	0	0	1	0	0	0	1	0	1	0	0	1	

For example, to go from $\begin{smallmatrix}2 & 2\\ 0 & 1\end{smallmatrix}$ to the following stage we incorporate the basis vector on the left and we build the line 1, 1, 2, 3 by adding the two lines below. For the following stages we add the lines corresponding to the values given in brackets.

EXAMPLE 2.2. We construct a vectorial addition chain for $v = [7,15,23]$ according to Lemma 1. We first build a vectorial addition chain for 7, 15, 23, for example, as given in Example 1.2; then we must build the corresponding vectorial addition chain, for instance, to the one given above. Finally, we must delete all the V lines corresponding to the elements other than 7, 15, and 23. The chain we get after the elimination of repetitions is given in Example 1.1.

For the proof of the third lemma, we introduce a new concept: the memory associated with each stage of a vectorial or one-dimensional addition chain, provided by a particular sequence of summands realizing it.

Let $V = (v_i, -k+1 \leq i \leq s)$ be such a chain. We define M_q, the memory at stage q, for $0 \leq q \leq s$, as the set of the v_j's with $j \leq q$ for which there exists $i > q$ such that v_i is obtained in the chosen sequence of summands from v_j and a certain v_h by $v_i = v_j + v_h$ for $h < i$. Thus, at each stage, the memory is the set of all the elements effectively used in the sequence at at least one of the following stages. Therefore $M_0 = \{v_i, -k + 1 \le i \le 0\}$ and $M_s = \{v_s\}$. In a future publication we will detail properties of the memory, particularly for the one-dimensional addition chain. In the following example, we illustrate this definition.

EXAMPLE 2.3. We construct the successive memories associated with the vectorial addition chain given in example 1.1. First we choose a sequence of summands; we see that the only elements which are not well determined are [2, 4, 6] and [4, 8, 17]; we choose, in each of these cases, to consider them as the double of the preceding elements (for example, [4, 8, 12] = [2, 4, 6] + [2, 4, 6].

$$M_0 = \{[0,0,1],[0,1,0],[1,0,0]\}, M_1 = \{[0,0,1],[1,0,0],[0,1,1]\},$$
$$M_2 = \{[0,0,1],[0,1,1],[1,1,1]\}, M_3 = \{[1,1,1],[0,1,2]\},$$
$$M_4 = \{[0,1,2],[1,2,3]\},$$
$$M_5 = \{[1,2,3],[1,3,5]\}, \qquad M_6 = \{[1,3,5],[2,4,6]\},$$
$$M_7 = \{[2,4,6],[3,7,11]\},$$
$$M_8 = \{[3,7,11],[4,8,12]\}, \qquad M_9 = \{[7,15,23]\}.$$

If in the sequence of summands we substitute the decomposition of [4, 8, 12] as [1, 1, 1] + [3, 7, 11], then $M'_q = M_q$ for $0 \le q \le 3$ and

$$M'_4 = \{[1,1,1],[0,1,2],[1,2,3]\}, M'_5 = \{[1,1,1],[1,2,3],[1,3,5]\},$$
$$M'_6 = \{[1,1,1],[1,3,5],[2,4,6]\}, M'_7 = \{[1,1,1],[3,7,11]\},$$
$$M'_8 = \{[3,7,11],[4,8,12]\}, \qquad M'_9 = \{[7,15,23]\};$$

generally the memory depends on the chosen sequence.

It is easy to see that if there is a vector v_q such that $v_q \notin M_q$ the vectorial addition chain V will not be of minimal length for v because this stage is redundant. From now on, we suppose without loss of generality that the sequence of summands in such a chain V satisfies this condition.

LEMMA 2. *Let $V = (v_i;\ -k + 1 \le i \le s)$ be a vectorial addition chain for v, and $M_q = v_t;\ \{1 \le t \le r\}$ be the memory at stage q; then*

(a) *at stage q we have*

$$v = c_1 v'_1 + \cdots + c_r v'_r, \tag{2}$$

where the c_t for $1 \le t \le r$, called the memory coefficients, are unique and strictly positive.

(b) *If* $q \leq s-1$ *and* $v_{q+1} = v'_j + v'_h$, *then at stage* $(q+1)$ *we have*

(i) $$\text{If } j \neq h\colon v = \sum_{t \neq j,h} c_t v'_t + (c_j - d)v'_j + (c_h - d)v'_h + d(v'_j + v'_h), \tag{3}$$

(ii) $$\text{If } j = h\colon v = \sum_{t \neq j} c_t v'_t + (c_j - 2d)v'_j + d(2v'_j), \tag{4}$$

for some $d > 0$.

Proof. (a) From the definition of M_q, we associate with each memory element a canonical vector in $\mathbb{N}^r$: $v'_t \to e_t$ for $1 \leq t \leq r$ and then we match it with $(v_j;\ q+1 \leq j \leq s)$, a vectorial addition chain in $\mathbb{N}^r$. If $[c_1, \ldots, c_r]$ is the unique vector (because we use the sequence of summands) associated with v in this sequence we deduce (2) and also the fact that all the coefficients are different from zero.

(b) $d > 0$ because v_{q+1} must belong to M_{q+1}. We deduce (3) and (4) because the representation of v in terms of the memory M_{q+1} is unique and in the chain built in (a) we associate either $e_j + e_h$ or $2e_j$ to v_{q+1}.

We shall say that expression (2) is the representation of v at the stage q. The following example illustrates the second lemma.

EXAMPLE 2.4. We construct the successive representations of $v = [7, 15, 23]$ for the vectorial addition chain given in Example 1.1. We choose a sequence of summands where $[2,4,6] = [1,2,3]$ and $[4,8,12] = [1,1,1] + [3,7,11]$. At each stage the transformation of the representation of V will be symbolized by an arrow:

$$7\cdot[1,0,0] + 15\cdot[0,1,0] + 23\cdot[0,0,1] \to 7\cdot[1,0,0] + 8\cdot[0,0,1] + 15\cdot[0,1,1]$$

$$\to 8\cdot[0,0,1] + 8\cdot[0,1,1] + 7\cdot[1,1,1] \to 7\cdot[1,1,1] + 8\cdot[0,1,2]$$

$$\to 1\cdot[1,1,1] + 2\cdot[0,1,2] + 6\cdot[1,2,3] \to 1\cdot[1,1,1] + 4\cdot[1,2,2] + 2\cdot[1,3,5]$$

$$\to 1\cdot[1,1,1] + 2\cdot[1,3,5] + 2\cdot[2,4,6] \to 1\cdot[1,1,1] + 2\cdot[3,7,11]$$

$$\to 1\cdot[3,7,11] + 1\cdot[4,8,12] \to 1\cdot[7,15,23].$$

For example, to go from the representation of v at stage 3, $v = 7\cdot[1,1,1] + 8\cdot[0,1,2]$, to the representation of v at stage 4 we introduce the vector $v_4 = [1,2,3]$ in the memory M_3 and we write the subsequence $(v_i;\ 5 \leq i \leq 9)$ in terms of the new memory M_4, where we have $[1,1,1] \to [1,0,0]$, $[0,1,2] \to [0,1,0]$, $[1,2,3] \to [0,0,1]$. We then have $[1,3,5] \to [0,1,1]$, $[2,4,6] \to [0,0,2]$, $[3,7,11] \to [0,1,3]$, $[4,8,12] \to [1,1,3]$, $[7,15,23] \to$

$[1,2,6]$. Then the representation of v at the stage 4 is

$$v = 1\cdot[1,1,1] + 2\cdot[0,1,2] + 6\cdot[1,2,3].$$

We shall say that a coefficient of memory c_i is *decomposed* at stage q if $c_i = c_j + c_h$ with c_j and c_h strictly positive.

LEMMA 3. *Let* $[n_1,\dots,n_k] \in \mathbb{N}^k$; *then*

$$l([n_1,\dots,n_k]) \le l(n_1,\dots,n_k) + (k-1). \tag{5}$$

Proof. Let $V = (v_i;\ -k+1 \le i \le s)$ be a vectorial addition chain of minimal length for $v = [n_1,\dots,n_k]$ together with a sequence of summands realizing it. From the paragraph preceding Lemma 2, we know that v_q belongs to M_q for all $q \ge 0$, because the chain is of minimal length for v.

The proof of the lemma is in two parts:

(i) The analysis of the representation of v at each stage, that is, the study of the memory coefficients and also of their sizes.

(ii) The explicit construction of a one-dimensional addition chain for $n_1,\dots,n_k$ which will allow us to prove the stated inequality. This construction will use the analysis above.

Part (i). At stage 0 we have the representation $v = n_1e_1 + \dots + n_ke_k$ and at stage s: $v = 1\cdot v_s$. Let (2) be the representation of v at stage q. We deduce from (3) and (4) that at stage $q+1$ we have:

(a) $\mathrm{Card}(M_{q+1}) = \mathrm{Card}(M_q) - 1$ if and only if we make an addition of type (3) with $d = c_j = c_h$. Then we do not decompose any of the coefficients at stage $q+1$. Let $\mathrm{Card}(M)$ denote the number of elements in M.

(b) $\mathrm{Card}(M_{q+1}) = \mathrm{Card}(M_q)$ if and only if we decompose only one coefficient: if (3) and $d = c_j$ then we decompose c_h into $(c_h - c_j)$ and c_j; if (4) then $2d = c_j$ and we decompose c_j into d and d.

(c) $\mathrm{Card}(M_{q+1}) = \mathrm{Card}(M_q) + 1$ if and only if we decompose two coefficients: if (3) we decompose c_j into $(c_j - d)$ and d; and c_h into $(c_h - d)$ and d; if (4) we decompose c_j into $(c_j - 2d)$ and $2d$, and $2d$ into d and d. In that case the size of the memory will be reduced eventually in a way such as to equilibrate this augmentation.

This completes the analysis of the representation of v at each stage.

Part (ii). To build the one-dimensional addition chain from memory coefficients, we use the following procedure: for each stage of the preceding analysis there is a step corresponding the construction of the chain. To the initial stage there corresponds the sequence of initial memory coefficients, written in any order. Each time a coefficient is decomposed (that is, when we are in case (b) or case (c)), we write its components at the beginning of the sequence, unless they already exist, and we move it just in front of the last element previously decomposed; or at the end if it is the first one. This procedure assures us that at each step of the construction the sequence is decomposed into two parts: the second part includes all the elements already decomposed, written in the order of decomposition, and the first part contains the others. Finally, since the number 1 cannot be decomposed the first part of the sequence will contain only this element and the second part the others, classified in the order of decomposition. This fact assures us of the unicity of the chain we obtained. This sequence can include repetitions. Actually it is a one-dimensional addition chain for $n_1, \dots, n_k$, since by construction each of its elements has been decomposed into two previous ones, and can be recomposed from them by addition. Let p be the length of this chain, once the repeated elements have been eliminated. We have $p \geq l(n_1, \dots, n_k)$ by definition. Let m_a, m_b, m_c be the respective numbers of stages of types (a), (b), (c). The length of the vectorial addition chain is then $s = m_a + m_b + m_c$. Now $m_a = (k-1) + m_c$ and the one-dimensional addition chain length is $p \leq m_b + 2m_c$, with equality holding if there is no repetition. Thus

$$s \geq p + (k-1) \geq l(n_1, \dots, n_k) + (k-1).$$

The following example illustrates the third lemma.

EXAMPLE 2.5. Construction of a one-dimensional addition chain for $7, 15, 23$ from the vectorial addition chain for $[7, 15, 23]$ given in Example 1.1. We use the construction of successive representations of $v = [7, 15, 23]$ given in Example 2.4 in order to deduce from it the one-dimensional addition chain. The elements already decomposed at each stage are underlined.

$$15, 23, 7 \to 8, 15, 7, \underline{23} \to 8, 7, \underline{15}, \underline{23} \to 8, 7, \underline{15}, \underline{23}$$

$$\to 1, 2, 6, \underline{8}, \underline{7}, \underline{15}, \underline{23} \to 4, 1, 2, \underline{6}, \underline{8}, \underline{7}, \underline{15}, \underline{23} \to 1, 2, \underline{4}, \underline{6}, \underline{8}, \underline{7}, \underline{15}, \underline{23}$$

$$\to 1, 2, \underline{4}, \underline{6}, \underline{8}, \underline{7}, \underline{15}, \underline{23} \to 1, \underline{2}, \underline{4}, \underline{6}, \underline{8}, \underline{7}, \underline{15}, \underline{23} \to 1, \underline{2}, \underline{4}, \underline{6}, \underline{8}, \underline{7}, \underline{15}, \underline{23}.$$

ACKNOWLEDGMENTS

I wish to thank M. J. Vuillemin for the fruitful discussions I had with him, and for his numerous remarks that have helped me to improve the manuscript.

REFERENCES

1. R. E. BELLMAN, Addition chains of vectors, *Amer. Math. Monthly* **70** (1963), 765.
2. A. BRAUER, On addition chains, *Bull. Amer. Math. Soc.* **45** (1939), 736–739.
3. P. ERDÖS, Remarks on number theory. III. On addition chains, *Acta Arith.* **6** (1960), 77–81.
4. D. E. KNUTH, "The Art of Computer Programming," Vol. 2, "Seminumerical Algorithms," Sect. 4.6.3, Addison-Wesley, Reading, Mass., 1969.
5. J. OLIVOS, Sur les chaines d'addition vectorielles, *in* "R. C. P. Algorithmique, Strasbourg, France, 18–20 Oct. 1979," pp. 13–14.
6. N. PIPPENGER, On the evaluation of powers and related problems, *in* "Proceedings, 19th Annual IEEE Symposium on the Foundations of Computer Science, Houston, Tex., 25–27 Oct. 1976," pp. 258–263.
7. N. PIPPENGER, On the evaluation of powers and monomials, *SIAM, J. Comput.*, in press.
8. A. SCHOLZ, *Jahresber. Deutsch. Math. Verein. (II)* **47** (1937), 41.
9. SCHÖNHAGE, A lower bound for the length of addition chains, *Theor. Comp. Sci.* **1** (1975), 1–12.
10. E. G. Straus, Addition-chains of vectors, *Amer. Math. Monthly* **71** (1964), 806–808.
11. A. C-C. YAO, On the evaluation of powers, *SIAM J. Comput.* vol. **5** (1976), 100–103.