1-1-1980

On the Evaluation of Powers and Monomials

Nicholas Pippenger
Harvey Mudd College

SIAM J. COMPUT.
Vol. 9, No. 2, May 1980

0097-5397/80/0902-0003 $01.00/0

ON THE EVALUATION OF POWERS AND MONOMIALS*

NICHOLAS PIPPENGER†

Abstract. Let $y_1, \cdots, y_p$ be monomials over the indeterminates $x_1, \cdots, x_q$. For every $y = (y_1, \cdots, y_p)$ there is some minimum number $L(y)$ of multiplications sufficient to compute $y_1, \cdots, y_p$ from $x_1, \cdots, x_q$ and the identity 1. Let $L(p, q, N)$ denote the maximum of $L(y)$ over all y for which the exponent of any indeterminate in any monomial is at most N. We show that if $p = (N+1)^{o(q)}$ and $q = (N+1)^{o(p)}$, then $L(p, q, N) = \min\{p, q\} \log N + H/\log H + o(H/\log H)$, where $H = pq \log (N+1)$ and all logarithms have base 2.

Key words. addition chain, computational complexity, monomial, power

1. Introduction. The result described in the abstract generalizes a number of previous results and solves a number of open problems. In 1937, Scholz [7] raised the problem of determining $L(1, 1, N)$ (computing one power of one indeterminate) and observed that

$$\log N \leqq L(1, 1, N) \leqq 2 \log N.$$

In 1939, Brauer [2] obtained the asymptotic formula

$$L(1, 1, N) \sim \log N,$$

and in 1960, Erdös [3] improved this to

$$L(1, 1, N) = \log N + \frac{\log (N+1)}{\log \log (N+1)} + o\left(\frac{\log (N+1)}{\log \log (N+1)}\right).$$

In 1963, Bellman [1] raised the problem of determining $L(1, q, N)$ (computing one monomial in several indeterminates), and in 1964, Straus [8] showed that

$$L(1, q, N) \sim \log N$$

for each fixed q.

In 1969, Knuth [4] (Section 4.6.3, Exercise 32) raised the problem of determining $L(p, 1, N)$ (computing several powers of one indeterminate), and in 1976, Yao [9] showed that

$$L(p, 1, N) \sim \log N$$

for each fixed p.

In a preliminary version of this paper [5], the author raised the problem of determining $L(p, q, N)$ and showed that if $p = 2^{o(q)}$ and $q = 2^{o(p)}$, then

$$L(p, q, 1) \sim pq/\log (pq).$$

In this paper we shall prove the following

THEOREM.

$$L(p, q, N) = v \log N + \frac{H}{\log H} U\left(\left(\frac{\log \log H}{\log H}\right)^{1/2}\right) + O(w),$$

where $v = \min\{p, q\}$, $H = pq \log (N+1)$, *and* $w = \max\{p, q\}$. *The expression* $U(\cdots)$ *denotes a factor of the form* $\exp O(\cdots)$; *if the quantity represented by the ellipsis tends to* 0, $U(\cdots)$ *is equivalent to* $1 + O(\cdots)$.

* Received by the editors November 1, 1978, and in revised form April 30, 1979.

† Mathematical Sciences Department, IBM Thomas J. Watson Research Center, Yorktown Heights, New York 10598.

Since $p = (N+1)^{o(q)}$ and $q = (N+1)^{o(p)}$ together imply (in fact, are equivalent to) $w = o(H/\log H)$, this theorem implies the result described in the abstract, as well as all the other asymptotic formulae cited above. The proof of the theorem is in two parts: a lower bound and an upper bound. The lower bound, presented in § 2, owes several ideas to the paper [3] of Erdös cited above. The upper bound, presented in § 3, would be the more difficult part of the proof if we had to start from scratch. In another paper[6], however, the author has given a result (also growing out of the preliminary version [5]) which allows the upper bound to be deduced as a corollary.

1.1. Reformulation of the problem. It is both traditional and convenient to reformulate the problem at hand in additive rather than multiplicative notation.

Let $q \geqq 1$ be a integer. A sequence

$$f = (f_1, \cdots, f_q)$$

of nonnegative integers will be called a (*q-dimensional*) *vector*, and $f_1, \cdots, f_q$ will be called its *components*. The vector

$$x_0 = (0, \cdots, 0)$$

will be called the *zero* vector, and the vectors

$$\begin{aligned} x_1 &= (1, \cdots, 0), \\ &\cdots \\ x_q &= (0, \cdots, 1) \end{aligned}$$

will be called *unit* vectors. If

$$f = (f_1, \cdots, f_q)$$

and

$$g = (g_1, \cdots, g_q),$$

the vector

$$f + g = (f_1 + g_1, \cdots, f_q + g_q)$$

will be called the *sum* of f and g.

Let $p \geqq 1$ be an integer. A sequence

$$y = (y_1, \cdots, y_p)$$

of (q-dimensional) vectors will be called a (*p-by-q*) *matrix*, and $y_1, \cdots, y_p$ will be called its *rows*.

Let $l \geqq 1$ be an integer. A sequence

$$z = (z_1, \cdots, z_l)$$

of vectors will be called a *chain*, and $z_1, \cdots, z_l$ will be called its *rows*, if each vector z_k ($1 \leqq k \leqq l$) is (1) the zero vector, (2) one of the unit vectors, or (3) the sum of two of the vectors $z_1, \cdots, z_{k-1}$ that precede it in the sequence (these two vectors need not be distinct). The zero and unit vectors will be called *basic* vectors; the others will be called *auxiliary* vectors. The number of basic vectors will be denoted by m; the number of auxiliary vectors will be denoted by n and called the *length* of the chain.

Let $N \geqq 1$ be an integer. We shall say that a vector is $(N+1)$-*ary* if all its components are in the set $\{0, 1, \cdots, N\}$, and that a matrix is $(N+1)$-*ary* if all its vectors are $(N+1)$-ary.

We shall say that a chain z *computes* a matrix y if each vector $y_i (1 \leqq i \leqq p)$ appears as one of the vectors $z_k (1 \leqq k \leqq l)$. If y is a matrix, $L(y)$ will denote the minimum possible length of a chain computing y, and $L(p, q, N)$ will denote the maximum of $L(y)$ over all p-by-q $(N+1)$-ary matrices y.

2. The lower bound. In this section we shall prove the lower bound

$$L(p, q, N) \geqq v \log N + \frac{H}{\log H} U\left(\frac{\log \log H}{\log H}\right) + O(w).$$

2.1. The easy case. Consider first the case

$$v \log N \leqq \frac{H \log \log H}{(\log H)^2}.$$

In this case the first term, $v \log N$, is absorbed by the U-factor of the second term,

$$\frac{H}{\log H} U\left(\frac{\log \log H}{\log H}\right) = \frac{H}{\log H} + O\left(\frac{H \log \log H}{(\log H)^2}\right).$$

Thus it will suffice to show

$$L(p, q, N) \geqq \frac{H}{\log H} U\left(\frac{\log \log H}{\log H}\right) + O(w).$$

If

$$w \geqq \frac{H}{\log H},$$

the desired bound is trivial; hence we shall assume

$$w \leqq \frac{H}{\log H}.$$

If

$$L(p, q, N) \geqq \frac{H}{\log H},$$

we are done; hence we shall assume

$$L(p, q, N) \leqq \frac{H}{\log H}.$$

It follows that we may also assume

$$\begin{aligned} l &= m + n \\ &\leqq q + 1 + L(p, q, N) \\ &= O\left(\frac{H}{\log H}\right). \end{aligned}$$

Let us consider a chain and assign to each vector in it a number called its *depth*. The basic vectors are assigned the depth 0. For $d = 1, 2, \cdots$, if a vector is the sum of two preceding vectors that both have depth at most $d-1$, but is not the sum of two preceding vectors that both have depth at most $d-2$, then it is assigned the depth d. By induction, this assigns depths uniquely to all the vectors in the chain.

Let us impose upon the set of all vectors a definite total order, which will be called the *standard order.*

We shall say that a chain is *standard* if its rows are all distinct, rows of lower depth precede those of higher depth, and rows of equal depth appear in the standard order.

LEMMA 2.1–1. *If a matrix is computed by a chain z, then it is also computed by a standard chain z' of no greater length.*

Proof. Given a chain z, consider the set of all vectors appearing in z. Remove from this set all the basic vectors and arrange them in the standard order to form a chain. Then remove from the set all the vectors that are the sum of two vectors currently in the chain, arrange them in the standard order, and append them to the end of the chain. Repeat this process until no more vectors can be removed. When the process terminates, the set must be empty, for if it contains any vectors, at the very least the one that appears earliest in z can be removed. The process thus yields a chain z' which is standard by construction, which contains every vector that appears in z (so that, in particular, it computes every matrix computed by z), and which contains no other vectors (so that, in particular, it has no greater length than z). □

By virtue of this lemma, we may henceforth restrict our attention to standard chains, and all chains will be assumed to be standard even if this is not explicitly mentioned.

We shall say that a matrix is *standard* if its rows are distinct and appear in the standard order. Henceforth we shall restrict our attention to standard matrices, and all matrices will be assumed to be standard even if this is not explicitly mentioned.

LEMMA 2.1–2. *There are at least*

$$2^H U(w \log H)$$

matrices.

Proof. There are $(N+1)^q$ rows that can appear in a matrix, and thus

$$\binom{(N+1)^q}{p}$$

ways to choose p distinct rows to form a matrix. Using the bound

$$\binom{A}{B} = A(A-1)\cdots(A-B+1)/B(B-1)\cdots 1 \geqq (A/B)^B$$

we obtain

$$\begin{aligned}\binom{(N+1)^q}{p} &\geqq (N+1)^{pq}/p^p \\ &= 2^H U(p \log p) \\ &= 2^H U(w \log H)\end{aligned}$$

matrices. □

LEMMA 2.1–3. *For some value of $n \leqq L(p, q, N)$, there are at least*

$$2^H U(w \log H)$$

chains.

Proof. Each matrix is computed by some chain of length at most $L(p, q, N)$. Each of these chains computes at most

$$\begin{aligned}\binom{l}{p} &\leqq l^p \\ &= U(p \log l) \\ &= U(w \log H)\end{aligned}$$

matrices, so there are at least

$$2^H U(w \log H)/U(w \log H) = 2^H U(w \log H)$$

chains of length at most $L(p, q, N)$. Each chain has one of at most

$$L(p, q, N) = U(\log H)$$

possible lengths, so for some length $n \leqq L(p, q, N)$, there are at least

$$2^H U(w \log H)/U(\log H) = 2^H U(w \log H)$$

chains. □

With each chain z we shall associate an object, which will be called a *code*, constructed as follows. Each basic vector in z is x_j for some j such that $0 \leqq j \leqq q$. Let $\mathcal{M}$ be the subset of $\{0, 1, \cdots, q\}$ that contains the m values of j corresponding to the basic vectors in z. Each auxiliary vector z_k in z is $z_{a_k} + z_{b_k}$ for some a_k and b_k such that $1 \leqq a_k \leqq b_k \leqq k-1$. Let $\mathcal{N}$ be a subset of $\{1, \cdots, l\} \times \{1, \cdots, l\}$ that contains n ordered pairs (a_k, b_k), one corresponding to each auxiliary vector in z. The ordered pair $(\mathcal{M}, \mathcal{N})$ will be the code associated with z.

LEMMA 2.1–4. *A chain is uniquely determined by its code.*

Proof. Let $(\mathcal{M}, \mathcal{N})$ be a code. From $\mathcal{M}$, determine the set of basic vectors; arrange these in the standard order to form a chain. Remove from $\mathcal{N}$ the pairs (a, b) for which b is less than or equal to the number of vectors currently in the chain. For each such pair, compute the vector $z_a + z_b$; arrange these vectors in the standard order and append them to the end of the chain. Repeat this process until no more pairs can be removed. Clearly only the resulting chain can have the code $(\mathcal{M}, \mathcal{N})$. □

LEMMA 2.1–5. *For any value of $n \leqq L(p, q, N)$, there are at most*

$$(H^2/n)^n U(n) U(w)$$

chains.

Proof. For any m and n, there are at most

$$\binom{q+1}{m}\binom{l^2}{n}$$

codes, since the two factors bound the number of ways of choosing $\mathcal{M}$ and $\mathcal{N}$, respectively. Using the bounds

$$\binom{A}{B} \leqq 2^A$$

and

$$\binom{A}{B} \leqq A^B/B! \leqq (Ae/B)^B$$

(where $e = 2.718\cdots$ is the base of natural logarithms), we obtain

$$\begin{aligned}\binom{q+1}{m}\binom{l^2}{n} &\leqq 2^{q+1}(l^2 e/n)^n \\ &= (l^2/n)^n U(n)U(q) \\ &= (l^2/n)^n U(n)U(w).\end{aligned}$$

There are

$$\begin{aligned}q+1 &= U(\log q) \\ &= U(\log w)\end{aligned}$$

possible values of m, and for each value of $n \leqq L(p, q, N)$,

$$\begin{aligned}l &= O(H) \\ &\leqq HU(1).\end{aligned}$$

Thus, for any value of $n \leqq L(p, q, N)$, there are at most

$$U(\log w)(H^2 U(1)^2/n)^n U(n)U(w) = (H^2/n)^n U(n)U(w)$$

codes.

Each chain is associated with some code, and at most one chain is associated with each code. Thus the bound just derived applies to chains as well as codes. □

We can now complete the proof. By Lemmas 2.1–3 and –5, there is a value of $n \leqq L(p, q, N)$ such that

$$(H^2/n)^n U(n)U(w) \geqq 2^H U(w \log H)$$

or, by taking logarithms,

$$2n \log H - n \log n + O(n) \geqq H + O(w \log H).$$

Ignoring the $n \log n$ term for the moment, this implies

$$2n \log H + O(n) \geqq H + O(w \log H)$$

or

$$(2n \log H)U\left(\frac{1}{\log H}\right) \geqq HU\left(\frac{w \log H}{H}\right).$$

This yields

$$n \geqq \frac{H}{2 \log H} U\left(\frac{1}{\log H}\right) U\left(\frac{w \log H}{H}\right)$$

or, by taking logarithms,

$$\log n \geqq \log H + O(\log \log H) + O\left(\frac{w \log H}{H}\right).$$

Multiplication by n yields

$$\begin{aligned}n \log n &\geqq n \log H + O(n \log \log H) + O\left(\frac{nw \log H}{H}\right) \\ &= n \log H + O\left(\frac{H \log \log H}{\log H}\right) + O(w).\end{aligned}$$

With this bound on the $n \log n$ term, the original inequality implies

$$n \log H + O(n) \geqq H + O\left(\frac{H \log\log H}{\log H}\right) + O(w \log H)$$

or

$$(n \log H) U\left(\frac{1}{\log H}\right) \geqq H U\left(\frac{\log\log H}{\log H}\right) + O(w \log H).$$

Thus

$$\begin{aligned} L(p, q, N) &\geqq n \\ &\geqq \frac{H}{\log H} U\left(\frac{\log\log H}{\log H}\right) + O(w), \end{aligned}$$

which is the desired lower bound.

2.2. The hard case. Consider now the case

$$v \log N \geqq \frac{H \log\log H}{(\log H)^2}.$$

Since $H = vw \log (N+1)$, we have

$$w \leqq \frac{(\log H)^2}{\log\log H}.$$

If

$$L(p, q, N) \geqq v \log N + \frac{H}{\log H}$$

we are done; hence we shall assume

$$L(p, q, N) \leqq v \log N + \frac{H}{\log H}.$$

It follows that we may also assume

$$\begin{aligned} l &= m + n \\ &\leqq q + 1 + L(p, q, N) \\ &= O(H). \end{aligned}$$

For any vector f and any $1 \leqq j \leqq q$, let us define

$$D(f, j) = -\sum_{1 \leqq i < j} f_i + f_j - \sum_{j < i \leqq q} f_i.$$

Thus $D(f, j)$ measures the extent to which the jth component of f exceeds all the other components combined.

We shall say that a vector f is a *j-vector* if

$$D(f, j) \geqq 1.$$

Clearly, a vector can be j-vector for at most one value of j.

Let z be a chain and let $z_k (m+1 \leqq k \leqq l)$ be an auxiliary j-vector in z. We shall say that z_j is *j-immediate* if it is equal to 2 times a preceding j-vector. Let

$$h = \lceil (\log H)^2 \rceil.$$

We shall say that z_k is *j-short* if it is not j-immediate but is the sum of two preceding j-vectors, between which fewer than h j-vectors intervene. Finally, we shall say that z_k is *j-long* if it is neither j-immediate nor j-short.

Let n_j, r_j, s_j, and t_j denote the numbers of j-vectors, j-immediate vectors, j-short vectors, and j-long vectors in z. Clearly,

$$n_j = r_j + s_j + t_j.$$

Let

$$\phi = (1+5^{1/2})/2 = 1.618\cdots$$

be the golden ratio. Then

$$\phi^{-2} + \phi^{-1} = 1.$$

Let

$$\psi = h^{1/h} \leqq 3^{1/3} = 1.442\cdots.$$

Then for $h \geqq 2$,

$$\psi^{-h-2} + \psi^{-1} \leqq 1.$$

For $h = 2$, this is trivial to check. For $h \geqq 3$, it follows from

$$\psi^{-h-2} = h^{-1} \exp(-2h^{-1} \ln h),$$
$$\psi^{-1} = \exp(-h^{-1} \ln h),$$
$$\exp x \leqq 1/(1-x),$$

and

$$\ln h \geqq 1.$$

LEMMA 2.2–1. *For any chain z, any vector z_k in z, and any $1 \leqq j \leqq q$,*

$$D(z_k, j) \leqq 2^{r_j} \phi^{s_j + t_j}$$

and

$$D(z_k, j) \leqq 2^{r_j + s_j} \psi^{t_j}.$$

Proof. We shall proceed by induction on $n_j = r_j + s_j + t_j$. If $n_j = 0$, there are no auxiliary j-vectors. But if z_k is a basic vector or not a j-vector,

$$D(z_k, j) \leqq 1,$$

and the assertions of the lemma are trivial. Suppose then that $n_j \geqq 1$ and that z_k is an auxiliary j-vector. It follows that it must be j-immediate, j-short, or j-long.

If z_k is j-immediate, there exists $1 \leqq b \leqq k-1$ such that $z_k = 2z_b$. The vector z_b appears in a chain with at most $r_j + s_j + t_j - 1$ j-vectors, of which at most $r_j - 1$ are j-immediate. By inductive hypothesis,

$$D(z_b, j) \leqq 2^{r_j - 1} \phi^{s_j + t_j}$$

(since $2 \geqq \phi$), and so

$$\begin{aligned} D(z_k, j) &= 2D(z_b, j) \\ &\leqq 2^{r_j}\phi^{s_j+t_j}. \end{aligned}$$

If on the other hand z_k is not j-immediate, there exist $1 \leqq a < b \leqq k-1$ such that $z_k = z_a + z_b$. The vectors z_a and z_b both appear in a chain with at most $r_j + s_j + t_j - 1$ j-vectors, of which at most r_j are j-immediate. By inductive hypothesis,

$$D(z_a, j) \leqq 2^{r_j}\phi^{s_j+t_j-1}$$

and

$$D(z_b, j) \leqq 2^{r_j}\phi^{s_j+t_j-1}.$$

If z_b is not a j-vector,

$$D(z_b, j) \leqq 0$$

and

$$\begin{aligned} D(z_k, j) &= D(z_a, j) + D(z_b, j) \\ &\leqq D(z_a, j) \\ &\leqq 2^{r_j}\phi^{s_j+t_j-1} \\ &\leqq 2^{r_j}\phi^{s_j+t_j}. \end{aligned}$$

If on the other hand z_b is a j-vector, then z_a appears in a chain with at most $r_j + s_j + t_j - 2$ j-vectors, of which at most r_j are j-immediate. By inductive hypothesis,

$$D(z_a, j) \leqq 2^{r_j+t_j-2}$$

and so

$$\begin{aligned} D(z_k,j) &= D(z_a, j) + D(z_b, j) \\ &\leqq 2^{r_j}\phi^{s_j+t_j-2} + 2^{r_j}\phi^{s_j+t_j-1} \\ &= 2^{r_j}\phi^{s_j+t_j}. \end{aligned}$$

This proves the first assertion of the lemma.

If z_k is not j-long, there exist $1 \leqq a \leqq b \leqq k-1$ such that $z_k = z_a + z_b$. The vectors z_a and z_b both appear in a chain with at most $r_j + s_j + t_j - 1$ j-vectors, of which at most $r_j + s_j - 1$ are not j-long. By inductive hypothesis,

$$D(z_a, j) \leqq 2^{r_j+s_j-1}\psi^{t_j}$$

and

$$D(z_b, j) \leqq 2^{r_j+s_j-1}\psi^{t_j}$$

(since $2 \geqq \psi$), and so

$$\begin{aligned} D(z_k, j) &= D(z_a, j) + D(z_b, j) \\ &\leqq 2\, 2^{r_j+s_j-1}\psi^{t_j} \\ &= 2^{r_j+s_j}\psi^{t_j}. \end{aligned}$$

If on the other hand z_k is j-long, there exist $1 \leqq a < b \leqq k-1$ such that $z_k = z_a + z_b$, and at least h j-vectors intervene between z_a and z_b. The vectors z_a and z_b both appear

in a chain with at most $r_j + s_j + t_j - 1$ j-vectors, of which at most $r_j + s_j$ are not j-long. By inductive hypothesis,

$$D(z_a, j) \leqq 2^{r_j+s_j}\psi^{t_j-1}$$

and

$$D(z_b, j) \leqq 2^{r_j+s_j}\psi^{t_j-1}.$$

If z_b is not a j-vector,

$$D(z_b, j) \leqq 0$$

and

$$\begin{aligned} D(z_k, j) &= D(z_a, j) + D(z_b, j) \\ &\leqq D(z_a, j) \\ &\leqq 2^{r_j+s_j}\psi^{t_j-1} \\ &\leqq 2^{r_j+s_j}\psi^{t_j}. \end{aligned}$$

If on the other hand z_b is a j-vector, then z_a appears in a chain with at most $r_j + s_j + t_j - h - 2$ j-vectors, of which at most $r_j + s_j$ are not j-long. By inductive hypothesis,

$$D(z_a, j) \leqq 2^{r_j+s_j}\psi^{t_j-h-2}$$

and so

$$\begin{aligned} D(z_k, j) &= D(z_a, j) + D(z_b, j) \\ &\leqq 2^{r_j+s_j}\psi^{t_j-h-2} + 2^{r_j+s_j}\psi^{t_j-1} \\ &\leqq 2^{r_j+s_j}\psi^{t_j}. \end{aligned}$$

This proves the second assertion of the lemma. □

Let z be a standard chain and let z_k $(m+1 \leqq k \leqq l)$ be an auxiliary vector in z. We shall say that z_k is *immediate* if it is j-immediate for some $1 \leqq j \leqq q$. We shall say that z_k is *short* if it is j-short for some $1 \leqq j \leqq q$. Finally, we shall say that z_k is *long* if it is neither immediate nor short.

Let r, s, and t denote the numbers of immediate, short, and long vectors in z. Clearly,

$$n = r + s + t.$$

We shall say that a chain is *special* if, for each $1 \leqq u \leqq v$, it contains a vector z_k such that

$$D(z_k, u) \geqq N/2.$$

LEMMA 2.2–2. *For any special chain of length at most* $L(p, q, N)$,

$$s + t = O\left(\frac{H}{\log H}\right)$$

and

$$r + s \geqq v \log N + O\left(\frac{H \log\log H}{(\log H)^2}\right).$$

Proof. If z is a special chain, it must contain, for each $1 \leqq u \leqq v$, a vector z_k such that

$$D(z_k, u) \geqq N/2.$$

Applying the preceding lemma to this vector, we obtain

$$2^{r_u} \phi^{s_u + t_u} \geqq N/2,$$

or, by taking logarithms,

$$r_u + (s_u + t_u) \log \phi \geqq \log N - 1.$$

Summing this over $1 \leqq u \leqq v$ and using

$$\sum_{1 \leqq u \leqq v} r_u \leqq r,$$

$$\sum_{1 \leqq u \leqq v} s_u \leqq s,$$

$$\sum_{1 \leqq u \leqq v} t_u \leqq t,$$

we obtain

$$\begin{aligned} r + (s + t) \log \phi &\geqq v \log N - v \\ &= v \log N + O\left(\frac{(\log H)^2}{\log \log H}\right). \end{aligned}$$

Subtracting this from

$$\begin{aligned} r + s + t &= n \\ &\leqq L(p, q, N) \\ &\leqq v \log N + \frac{H}{\log H} \end{aligned}$$

yields

$$(s + t)(1 - \log \phi) \leqq \frac{H}{\log H} + O\left(\frac{(\log H)^2}{\log \log H}\right).$$

Since $1 - \log \phi > 0$, this proves the first assertion of the lemma.

Again applying the preceding lemma to z_k, we obtain

$$2^{r_u + s_u} \psi^{t_u} \geqq N/2,$$

or, by taking logarithms,

$$r_u + s_u + t_u \log \psi \geqq \log N - 1.$$

Summing over $1 \leqq u \leqq v$, we obtain

$$\begin{aligned} r + s + t \log \psi &\geqq v \log N - v \\ &= v \log N + O\left(\frac{(\log H)^2}{\log \log H}\right). \end{aligned}$$

Since

$$t \leqq l$$
$$= O(H)$$

and

$$\log \psi = h^{-1} \log h$$
$$= O\left(\frac{\log \log H}{(\log H)^2}\right),$$

this yields

$$r + s \geqq v \log N + O\left(\frac{H \log \log H}{(\log H)^2}\right),$$

which proves the second assertion of the lemma. □

We shall say that a matrix is *special* if, for every $1 \leqq u \leqq v$, it contains a vector z_k such that

$$D(z_k, u) \geqq N/2.$$

LEMMA 2.2–3. *There are at least*

$$2^H U\left(\frac{(\log H)^4}{\log \log H}\right)$$

special matrices.

Proof. Let

$$K = \left\lfloor \frac{N+1}{4q} \right\rfloor.$$

For any $1 \leqq j \leqq q$, there are at least $(K+1)^q$ vectors f such that

$$D(f, j) \geqq N/2,$$

since if

$$0 \leqq f_i \leqq K \quad \text{for } 1 \leqq i \leqq j,$$
$$N - K \leqq f_j \leqq N,$$
$$0 \leqq f_i \leqq K \quad \text{for } j < i \leqq q,$$

then there are $K+1$ possible values for each component and

$$D(f, j) \geqq N - qK$$
$$= N - q\left\lfloor \frac{N+1}{4q} \right\rfloor$$
$$\geqq N/2.$$

It follows that there are at least

$$(K+1)^{qv}\binom{(N+1)^q}{p-v} \geqq \binom{(K+1)^q}{p}$$

special matrices. Estimating this binomial coefficient as before, we obtain

$$\begin{aligned}\binom{(K+1)^q}{p} &\geqq \left(\frac{(K+1)^q}{p}\right)^p \\ &= (K+1)^{pq} U(w \log w) \\ &\geqq \left(\frac{N+1}{4q}\right)^{pq} U(w \log w) \\ &= (N+1)^{pq} U(w^2 \log w) \\ &= 2^H U\left(\frac{(\log H)^4}{\log \log H}\right)\end{aligned}$$

special matrices. □

LEMMA 2.2–4. *For some value of t, there are at least*

$$2^H U\left(\frac{(\log H)^4}{\log \log H}\right)$$

special chains of length at most $L(p, q, N)$.

Proof. Each special matrix is computed by a special chain of length at most $L(p, q, N)$. Each of these chains computes at most

$$\begin{aligned}\binom{l}{p} &\leqq l^p \\ &= U(p \log l) \\ &= U\left(\frac{(\log H)^3}{\log \log H}\right)\end{aligned}$$

matrices, so there are at least

$$2HU\left(\frac{(\log H)^4}{\log \log H}\right) \Big/ U\left(\frac{(\log H)^3}{\log \log H}\right) = 2^H U\left(\frac{(\log H)^4}{\log \log H}\right)$$

special chains of length at most $L(p, q, N)$. Each chain has one of at most

$$\begin{aligned}L(p, q, N) &= O(H) \\ &= U(\log H)\end{aligned}$$

possible values of t, so for some value of t there are at least

$$2^H U\left(\frac{(\log H)^4}{\log \log H}\right) \Big/ U(\log H) = 2^H U\left(\frac{(\log H)^4}{\log \log H}\right)$$

special chains. □

With each special chain z we shall associate an object, which will be called a *special code*, constructed as follows. Let $\mathcal{M}$ be the set defined above. Each immediate vector z_k in z is $2z_{b_k}$ for some b_k such that $1 \leqq b_k \leqq k-1$. Let $\mathcal{R}$ be a subset of $\{1, \cdots, l\}$ that contains r elements b_k, one corresponding to each immediate vector in z. Each short vector z_k in z is a j-vector for some $1 \leqq j \leqq q$ and is $z_{a_k} + z_{b_k}$ for some a_k and b_k such that $1 \leqq a_k < b_k \leqq k-1$, z_{a_k} and z_{b_k} are both j-vectors, and the number Δ_k of j-vectors intervening between z_{a_k} and z_{b_k} satisfies $0 \leqq \Delta_k \leqq h-1$. Let $\mathcal{S}$ be a subset of $\{0, \cdots, h-1\} \times \{1, \cdots, l\}$ that contains s ordered pairs (Δ_k, b_k), one corresponding to each short

vector in z. Each long vector z_k in z is $z_{a_k}+z_{b_k}$ for some a_k and b_k such that $1 \leqq a_k < b_k \leqq k-1$. Let $\mathcal{T}$ be a subset of $\{1, \cdots, l\}\times\{1, \cdots, l\}$ that contains t ordered pairs (a_k, b_k), one corresponding to each long vector in z. The ordered quadruple $(\mathcal{M}, \mathcal{R}, \mathcal{S}, \mathcal{T})$ will be the special code associated with z.

LEMMA 2.2–5. *A special chain is uniquely determined by its special code.*

Proof. Let $(\mathcal{M}, \mathcal{R}, \mathcal{S}, \mathcal{T})$ be a special code. From $\mathcal{M}$, determine the set of basic vectors, arrange these in the standard order to form a chain. Remove from $\mathcal{R}$ all elements b, from $\mathcal{S}$ all pairs (Δ, b), and from $\mathcal{T}$ all pairs (a, b) for which b is less than or equal to the number of vectors currently in the chain. For each b removed from $\mathcal{R}$, compute $2z_b$. For each (Δ, b) removed from $\mathcal{S}$, determine j such that z_b is a j-vector, determine a such that z_a is a j-vector and exactly Δ j-vectors intervene between z_a and z_b, and compute z_a+z_b. For each (a, b) removed $\mathcal{T}$, compute z_a+z_b. Arrange the computed vectors in the standard order and append them to the end of the chain. Repeat this process until no more elements or pairs can be removed. Clearly, only the resulting chain can have the special code $(\mathcal{M}, \mathcal{R}, \mathcal{S}, \mathcal{T})$. □

LEMMA 2.2–6. *For any value of t, there are at most*

$$(H^2/t)^t U(t) U\left(\frac{H \log\log H}{\log H}\right)$$

special chains of length at most $L(p, q, N)$.

Proofs. For any m, r, s, and t, there are at most

$$\binom{q+1}{m}\binom{l}{r}\binom{hl}{s}\binom{l^2}{t}$$

special codes, since the four factors bound the number of ways of choosing $\mathcal{M}$, $\mathcal{R}$, $\mathcal{S}$, and $\mathcal{T}$, respectively. Since

$$q+1 = O\left(\frac{(\log H)^2}{\log\log H}\right),$$

then

$$\binom{q+1}{m} \leqq 2^{q+1} = U\left(\frac{(\log H)^2}{\log\log H}\right).$$

Since

$$l = O(H)$$

and

$$m+s+t = O\left(\frac{H}{\log H}\right),$$

$$\begin{aligned}\binom{l}{r} &= \binom{l}{l-r} \\ &= \binom{l}{m+s+t} \\ &\leqq \left(\frac{le}{m+s+t}\right)^{m+s+t} = U\left(\frac{H \log\log H}{\log H}\right).\end{aligned}$$

Since

$$hl = O(H(\log H)^2)$$

and

$$s = O\left(\frac{H}{\log H}\right),$$

$$\binom{hl}{s} \leqq (hle/s)^s = U\left(\frac{H \log\log H}{\log H}\right).$$

Since

$$l = O(H),$$

$$\binom{l^2}{t} \leqq (l^2 e/t)^t = (H^2/t)^t U(t).$$

There are

$$q+1 = O\left(\frac{(\log H)^2}{\log\log H}\right)$$
$$= U(\log\log H)$$

possible values of m, and at most

$$L(p, q, N)^2 = O(H^2)$$
$$= U(\log H)$$

possible combinations of values of r and s. Thus, for any value of t, there are at most

$$(H^2/t)^t U(t) U\left(\frac{H \log\log H}{\log H}\right)$$

special codes.

Each special chain is associated with some special code, and at most one special chain is associated with each special code. Thus the bound just derived applies to special chains as well as special codes. □

We can now complete the proof. By Lemmas 2.2–4 and –6, there is a value of t such that

$$(H^2/t)^t U(t) U\left(\frac{H \log\log H}{\log H}\right) \geqq 2^H U\left(\frac{(\log H)^4}{\log\log H}\right),$$

since these quantities bound the number of special chains of length at most $L(p, q, N)$. Taking logarithms, we obtain

$$2t \log H - t \log t + O(t) \geqq H + O\left(\frac{H \log\log H}{\log H}\right).$$

Ignoring the $t \log t$ term for the moment, this implies

$$2t \log H + O(t) \geqq H + O\left(\frac{H \log\log H}{\log H}\right)$$

or

$$(2t \log H)U\left(\frac{1}{\log H}\right) \geqq HU\left(\frac{\log \log H}{\log H}\right).$$

This yields

$$t \geqq \frac{H}{2 \log H} U\left(\frac{\log \log H}{\log H}\right)$$

or, by taking logarithms,

$$\log t \geqq \log H + O(\log \log H).$$

Multiplication by t yields

$$t \log t \geqq t \log H + O(t \log \log H).$$

With this bound on the $t \log t$ term, the original inequality implies

$$t \log H + O(t \log \log H) \geqq H + O\left(\frac{H \log \log H}{\log H}\right)$$

or

$$(t \log H)U\left(\frac{\log \log H}{\log H}\right) \geqq HU\left(\frac{\log \log H}{\log H}\right).$$

Thus

$$\begin{aligned} t &\geqq \frac{H}{\log H} U\left(\frac{\log \log H}{\log H}\right). \\ &= \frac{H}{\log H} + O\left(\frac{H \log \log H}{(\log H)^2}\right) \end{aligned}$$

Since for special chains

$$r + s \geqq v \log N + O\left(\frac{H \log \log H}{(\log H)^2}\right),$$

we obtain

$$\begin{aligned} L(p, q, N) &\geqq r + s + t \\ &\geqq v \log N + \frac{H}{\log H} + O\left(\frac{H \log \log H}{(\log H)^2}\right) \\ &= v \log N + \frac{H}{\log H} U\left(\frac{\log \log H}{\log H}\right), \end{aligned}$$

which is the desired lower bound.

3. The upper bound. We shall prove

$$L(p, q, N) \leqq v \log N + \frac{H}{\log H} U\left(\left(\frac{\log \log H}{\log H}\right)^{1/2}\right) + O(w).$$

We shall begin with the preliminary upper bound

$$L(p, q, N) \leqq \frac{H}{\log H} U\left(\left(\frac{\log \log H}{\log H}\right)^{1/2}\right) + O(v \log N) + O(w),$$

which we shall deduce from a theorem on graphs.

Let y be a p-by-q $(N+1)$-ary matrix. Let $C(y)$ denote the minimum possible number of edges in a directed graph in which

(1) there are p distinguished vertices called *inputs* and q other distinguished vertices called *outputs*;

(2) there is no directed path from an input to another input, from an output to another output, or from an output to an input; and

(3) for all $1 \leqq i \leqq p$ and $1 \leqq j \leqq q$, the number of directed paths from the ith input to the jth output is equal the jth component of the ith row of y.

Let $C(p, q, N)$ denote the maximum of $C(y)$ over all p-by-q $(N+1)$-ary matrices y. In [6] it was shown that

$$C(p, q, N) \leqq \frac{H}{\log H} U\left(\left(\frac{\log \log H}{\log H}\right)^{1/2}\right) + O(v \log N) + O(w).$$

Thus the preliminary upper bound will follow if we prove $L(y) \leqq C(y)$, which implies $L(p, q, N) \leqq C(p, q, N)$.

Consider a graph with at most $C(y)$ edges that meets the conditions enumerated above. We may assume that this graph has no cycles, since the deletion of all edges involved in cycles would not affect the number of paths from an input to an output unless that number were originally infinite. From this graph we can obtain another in which the degree (the number of edges directed from) each vertex is 0, 1 or 2, which has at most $C(y)$ vertices with degree 1 or 2, and which also meets the conditions enumerated above; this is done by replacing each vertex with degree $d \geqq 3$ by $d-1$ vertices with degree 2. We can then associate with each vertex a vector which, for $1 \leqq j \leqq q$, has as its jth component the number of paths from the vertex to the jth output. It is easy to verify that these vectors can be arranged to form a chain of length at most $C(y)$ that computes y. Thus $L(y) \leqq C(y)$, which completes the proof of the preliminary upper bound.

3.1. The easy case. Consider first the case

$$v \log N \leqq \frac{H \log \log H}{(\log H)^2}.$$

In this case

$$v \log N = \frac{H}{\log H} O\left(\left(\frac{\log \log H}{\log H}\right)^{1/2}\right).$$

and the desired lower bound follows from

$$L(p, q, N) \leqq \frac{H}{\log H} U\left(\left(\frac{\log \log H}{\log H}\right)^{1/2}\right) + O(v \log N) + O(w),$$

which has already been proved.

At this point we have proved the case $N = 1$, since in this case $v \log N = 0$. In particular,

$$L(c, d, 1) \leqq \frac{cd}{\log (cd)} U\left(\left(\frac{\log \log (cd)}{\log (cd)}\right)^{1/2}\right) + O(c) + O(d).$$

3.2. The hard case. Consider now the case

$$v \log N \geqq \frac{H \log\log H}{(\log H)^2},$$

which, as before, implies

$$w \leqq \frac{(\log H)^2}{\log\log H}.$$

Let y be a p-by-q $(N+1)$-ary matrix. For $1 \leqq i \leqq p$ and $1 \leqq j \leqq q$, let $e_{i,j}$ denote the jth component of the ith row of y, so that

$$y_i = \sum_{i \leqq j \leqq q} e_{i,j} x_j.$$

Let

$$s = \left\lceil \left(\frac{q \log (N+1)}{p} \right)^{1/2} \right\rceil,$$

$$t = \left\lceil \left(\frac{p \log (N+1)}{q} \right)^{1/2} \right\rceil.$$

Then

$$st \geqq \log (N+1),$$

so

$$2^{st} - 1 \geqq N.$$

On the other hand

$$st \leqq \left\{ \left(\frac{q \log (N+1)}{p} \right)^{1/2} + 1 \right\} \left\{ \left(\frac{p \log (N+1)}{q} \right)^{1/2} + 1 \right\}$$

$$= \log (N+1) + \left(\frac{q \log (N+1)}{p} \right)^{1/2} + \left(\frac{p \log (N+1)}{q} \right)^{1/2} + 1,$$

so

$$pqst \leqq H + (p+q) H^{1/2} + pq$$

$$= H + O\left(\frac{H^{1/2} (\log H)^2}{\log\log H} \right).$$

Similarly,

$$vst = v \log N + O(H^{1/2}),$$

$$ps = O(H^{1/2}),$$

$$qt = O(H^{1/2}).$$

We shall consider two cases, according to whether $p \geqq q$ or $p < q$.

If $p \geqq q$, we shall compute $y_1, \cdots, y_p$ from $x_1, \cdots, x_q$ in three steps as follows.

(1) For $1 \leqq j \leqq q$ and $1 \leqq b \leqq t$, compute

$$x'_{t(j-1)+b} = 2^{s(b-1)} x_j.$$

This defines x'_g for $1 \leqq g \leqq qt$. For $1 \leqq i \leqq p$ and $1 \leqq j \leqq q$, write $e_{i,j}$ as a t-digit number in base 2^s.

$$e_{i,j} = \sum_{1 \leqq b \leqq t} e'_{i,t(j-1)+b} 2^{s(b-1)},$$

where $0 \leqq e'_{i,t(j-1)+b} \leqq 2^s - 1$. This is possible since $0 \leqq e_{i,j} \leqq N \leqq 2^{st} - 1$; it defines $e'_{i,g}$ for $1 \leqq i \leqq p$ and $1 \leqq g \leqq qt$. Now write each $e'_{i,g}$ as an s-digit number in base 2:

$$e'_{i,g} = \sum_{1 \leqq a \leqq s} e''_{s(i-1)+a,g} 2^{a-1},$$

where $0 \leqq e''_{s(i-1)+a,g} \leqq 1$. This is possible since $0 \leqq e'_{i,g} \leqq 2^s - 1$; it defines $e''_{f,g}$ for $1 \leqq f \leqq ps$ and $1 \leqq g \leqq qt$.

(2) For $1 \leqq f \leqq ps$, compute

$$y'_f = \sum_{1 \leqq g \leqq qt} e''_{f,g} x'_g.$$

(3) For $1 \leqq i \leqq p$, compute

$$y_i = \sum_{1 \leqq a \leqq s} 2^{a-1} y'_{s(i-1)+a}.$$

It is easy to verify that this computes y_i correctly:

$$\begin{aligned} y_i &= \sum_{1 \leqq a \leqq s} 2^{a-1} y'_{s(i-1)+a} \\ &= \sum_{i \leqq a \leqq s} 2^{a-1} \sum_{1 \leqq g \leqq qt} e''_{s(i-1)+a,g} x'_g \\ &= \sum_{1 \leqq a \leqq s} 2^{a-1} \sum_{1 \leqq b \leqq t} \sum_{1 \leqq j \leqq q} e''_{s(i-1)+a,t(j-1)+b} 2^{s(b-1)} x_j \\ &= \sum_{1 \leqq b \leqq t} \sum_{1 \leqq j \leqq q} e'_{i,t(j-1)+b} 2^{s(b-1)} x_j \\ &= \sum_{1 \leqq j \leqq q} e_{i,j} x_j. \end{aligned}$$

Let us now count the number of additions required to perform these steps. Consider $x'_{t(j-1)+b}$. For $b = 1$, it is x_j; for $2 \leqq b \leqq t$, it can be computed from $x'_{t(j-1)+b-1}$ using s additions:

$$x'_{t(j-1)+b} = 2^s x'_{t(j-1)+b-1}.$$

Thus step (1) requires at most

$$\begin{aligned} q(t-1)s &\leqq vst \\ &= v \log N + O(H^{1/2}) \end{aligned}$$

additions. Since $0 \leqq e''_{f,g} \leqq 1$ for $1 \leqq f \leqq ps$ and $1 \leqq g \leqq qt$, step (2) requires at most

$$\begin{aligned} L(ps, qt, 1) &\leqq \frac{pqst}{\log (pqst)} U\left(\left(\frac{\log \log (pqst)}{\log (pqst)}\right)^{1/2}\right) + O(ps) + O(qt) \\ &= \frac{H}{\log H} U\left(\left(\frac{\log \log H}{\log H}\right)^{1/2}\right) + O(H^{1/2}) \end{aligned}$$

additions, by taking $c = ps$ and $d = qt$ in the case $N = 1$. Finally, consider the sum

$$y''_{s(i-1)+r} = \sum_{r \leqq a \leqq s} 2^{a-r} y'_{s(i-1)+a}$$

For $r = s$, it is y'_{si}; for $1 \leqq r \leqq s-1$, it can be computed from $y''_{s(i-1)+r+1}$ using two additions:

$$y''_{s(i-1)+r} = y'_{s(i-1)+r} + 2y''_{s(i-1)+r+1}.$$

Since $y_i = y''_{s(i-1)+1}$, step (3) requires at most

$$\begin{aligned} 2p(s-1) &\leqq 2ps \\ &= O(H^{1/2}) \end{aligned}$$

additions. Summing these contributions completes the proof of the upper bound for $p \geqq q$.

If $p < q$, we shall compute $y_1, \cdots, y_p$ from $x_1, \cdots, x_q$ in three steps as follows.

(1) For $1 \leqq j \leqq q$ and $1 \leqq b \leqq t$, compute

$$x'_{t(j-1)+b} = 2^{b-1} x_j.$$

This defines x'_g for $1 \leqq g \leqq qt$. For $1 \leqq i \leqq p$ and $1 \leqq j \leqq q$, write $e_{i,j}$ as an s-digit number in base 2^t:

$$e_{i,j} = \sum_{1 \leqq a \leqq s} e'_{s(i-1)+a,j} 2^{t(a-1)},$$

where $0 \leqq e'_{s(i-1)+a,j} \leqq 2^t - 1$. This is possible since $0 \leqq e_{i,j} \leqq N \leqq 2^{st} - 1$; it defines $e'_{f,j}$ for $1 \leqq f \leqq ps$ and $1 \leqq j \leqq q$. Now write each $e'_{f,j}$ as a t-digit number in base 2:

$$e'_{f,j} = \sum_{1 \leqq b \leqq t} e''_{f,t(j-1)+b} 2^{b-1},$$

where $0 \leqq e''_{f,t(j-1)+b} \leqq 1$. This is possible since $0 \leqq e'_{f,j} \leqq 2^t - 1$; it defines $e''_{f,g}$ for $1 \leqq f \leqq ps$ and $1 \leqq g \leqq qt$.

(2) For $1 \leqq f \leqq ps$, compute

$$y'_f = \sum_{1 \leqq g \leqq qt} e''_{f,g} x'_g.$$

(3) For $1 \leqq i \leqq p$, compute

$$y_i = \sum_{1 \leqq a \leqq s} 2^{t(a-1)} y'_{s(i-1)+a}.$$

It is again easy to verify that this computes y_i correctly:

$$\begin{aligned} y_i &= \sum_{1 \leqq a \leqq s} 2^{t(a-1)} y'_{s(i-1)+a} \\ &= \sum_{1 \leqq a \leqq s} 2^{t(a-1)} \sum_{1 \leqq g \leqq qt} e''_{s(i-1)+a,g} x'_g \\ &= \sum_{1 \leqq a \leqq s} 2^{t(a-1)} \sum_{1 \leqq b \leqq t} \sum_{1 \leqq j \leqq q} e''_{s(i-1)+a,t(j-1)+b} 2^{b-1} x_j \\ &= \sum_{1 \leqq a \leqq s} 2^{t(a-1)} \sum_{1 \leqq j \leqq q} e'_{s(i-1)+a,j} x_j \\ &= \sum_{1 \leqq j \leqq q} e_{i,j} x_j. \end{aligned}$$

Let us again count the number of additions required to perform these steps. Consider $x'_{t(j-1)+b}$. For $b = 1$, it is x_j, for $2 \leqq b \leqq t$, it can be computed from $x'_{t(j-1)+b-1}$ using one addition:

$$x'_{t(j-1)+b} = 2x'_{t(j-1)+b-1}.$$

Thus step (1) requires at most

$$\begin{aligned} q(t-1) &\leqq qt \\ &= O(H^{1/2}) \end{aligned}$$

additions. Since $0 \leqq e''_{f,g} \leqq 1$ for $1 \leqq f \leqq qs$ and $1 \leqq g \leqq qt$, step (2) requires at most

$$L(ps, qs, 1) \leqq \frac{H}{\log H} U\left(\left(\frac{\log \log H}{\log H}\right)^{1/2}\right) + O(H^{1/2})$$

additions, as in the case $p \geqq q$. Finally, consider the sum

$$y''_{s(i-1)+r} = \sum_{r \leqq a \leqq s} 2^{t(a-r)} y'_{s(i-1)+a}.$$

For $r = s$, it is y'_{si}; for $1 \leqq r \leqq s-1$, it can be computed from $y''_{s(i-1)+r+1}$ using $t+1$ additions:

$$y''_{s(i-1)+r} = y'_{s(i-1)+r} + 2^t y''_{s(i-1)+r+1}.$$

Since $y_i = y''_{s(i-1)+1}$, step (3) requires at most

$$\begin{aligned} p(s-1)(t+1) &\leqq vst + ps \\ &= v \log N + O(H^{1/2}) \end{aligned}$$

additions. Summing these contributions completes the proof of the upper bound.

REFERENCES

[1] R. E. BELLMAN, *Addition chains of vectors*, Amer. Math. Monthly, 70 (1963), p. 765.

[2] A. BRAUER, *On addition chains*, Bull. Amer. Math. Soc., 45 (1939), pp. 736–739.

[3] P. ERDÖS, *Remarks on number theory, III: On addition chains*, Acta Arith., 6 (1960), pp. 77–81.

[4] D. E. KNUTH, *The Art of Computer Programming, Volume 2: Seminumerical Algorithms*, Addison-Wesley, Reading, MA, 1969.

[5] N. PIPPENGER, *On the evaluation of powers and related problems*, Proc. 17th Ann. IEEE Symp. on Found. of Computer Sci. (Houston, TX), 25-27 Oct. 1976, pp. 258–263.

[6] ———, *The minimum number of edges in graphs with prescribed paths*, Math. Systems Theory, to appear.

[7] A. SCHOLZ, *Jahresbericht der Deutschen Mathematiker-Vereinigung (II)*, 47 (1937), pp. 41–42.

[8] E. G. STRAUS, *Addition chains of vectors*, Amer. Math. Monthly, 71 (1964), pp. 806–808.

[9] A. C.-C. YAO, *On the evaluation of powers*, this Journal, 5 (1976), pp. 100–103.