Report (Universitetet i Bergen. Matematisk institutt)

Department of PURE MATHEMATICS

ON SHELLSORT AND THE FROBENIUS PROBLEM

ERNST S. SELMER

Report No 48 February 1987

UNIVERSITY OF BERGEN
Bergen, Norway

Department of Mathematics
University of Bergen
5007 Bergen
NORWAY

ISSN - 0332-5407

ON SHELLSORT AND THE FROBENIUS PROBLEM

ERNST S. SELMER

Report No 48 February 1987

ON SHELLSORT AND THE FROBENIUS PROBLEM

ERNST S. SELMER

Department of Mathematics, University of Bergen,

N-5000 Bergen, Norway

Abstract.

A bound $O(N^{1+1/k})$ for the running time of Shellsort, with $O(\log N)$ passes, is proved very simply by application of a Frobenius basis with k elements.

1. Shellsort theory.

For a description of Shellsort and the number-theoretical problem of Frobenius, we refer to two recent papers by Sedgewick [6] and by Incerpi and Sedgewick [4]. In the former paper, Sedgewick improves the Shellsort bound $O(N^{3/2})$ to $O(N^{4/3})$, using a "result of Selmer" [7] on a Frobenius basis with three elements. It is of course nice for a number-theoretician to see that his "useless" mathematics can really be applied. In all fairness, however, it should be made clear (as stated in [7]) that "my" result is really due to Hofmeister [3], as a special case of a general and rather complicated theorem. What I did in [7] was to give a direct, simple proof for this special case.

Later (but published before [6]), Incerpi and Sedgewick [4] have improved the bound $O(N^{4/3})$ to $O(N^{1+\varepsilon})$, and further to $O(N^{1+\varepsilon/\sqrt{\log N}})$. In both cases, they circumvent the standard approach of Frobenius bases. Their proof of the latter bound is very nice, and I cannot in any way improve on it. Their proof of the bound $O(N^{1+\varepsilon})$ does, however, result in an unnecessarily complicated increment sequence. The purpose of the present paper is to describe a simpler method, using a classical result in Frobenius theory.

In [4] p. 217, an increasing "base sequence" $\{a_i\} = a_1, a_2, \ldots$ of natural numbers is used to produce the increments h_j of a Shellsort. A number c of different product sequences are <u>interleaved</u>, each such sequence consisting of certain products of c elements a_i. We shall see that <u>one</u> product sequence will suffice. In fact, we can define the increments by $h_1 = 1$ and

$$h_j = a_{j-1} a_j \ldots a_{j+c-2}\ , \quad j > 1\ .$$

From these, we form a Frobenius basis with $c+1$ elements:

(1) $$B_{c+1}^{(j)} = \{h_{j+1}, h_{j+2}, \ldots, h_{j+c+1}\} = \{b_1, b_2, \ldots, b_{c+1}\}$$

(say). Under the condition (5) below for the base sequence $\{a_i\}$, we can then determine explicitly the Frobenius number

(2) $$g(B_{c+1}^{(j)}) = \sum_{i=2}^{c+1} a_{j+i-2}\, h_{j+i} - \sum_{i=1}^{c+1} h_{j+i}\ .$$

This expression is clearly $O(h_j^{1+1/c})$ (if each term a_i is within a constant factor of the previous one). Just as in Theorem 2 of [4], we then get the running time of Shellsort bounded by $O(N^{1+1/(c+1)})$.

2. Frobenius theory.

We operate with a Frobenius basis

$$B_k = \{b_1, b_2, \ldots, b_k\}\ , \quad \gcd(b_1, b_2, \ldots, b_k) = 1\ .$$

Already Frobenius realized that a determination of $g(B_k)$ in the general case was extremely difficult. He therefore invited his audiences to look for good upper bounds for $g(B_k)$.

The first such bound was given already in the 1942 paper by A. Brauer [1] (indeed the first "serious" paper to be written on the problem of Frobenius). Let

$$d_0 = 0\ , \quad d_1 = b_1\ ; \quad d_i = \gcd(b_1, b_2, \ldots, b_i)\ , \quad 2 \leq i \leq k\ .$$

Then Brauer showed that

(3) $$g(B_k) \leq \sum_{i=1}^{k} b_i \left(\frac{d_{i-1}}{d_i} - 1\right)\ ,$$

with equality if the following condition is satisfied:

(4) $$\begin{cases} \text{For all } i = 2, 3, \ldots, k-1\ ,\ b_{i+1}/d_{i+1} \text{ is a linear} \\ \text{combination of } b_1/d_i\ ,\ b_2/d_i\ , \ldots,\ b_i/d_i \text{ with non-} \\ \text{negative integer coefficients.} \end{cases}$$

Further, Brauer and Seelbinder [2] showed that this condition is also necessary for equality in (3).

The proofs in the two papers quoted are rather complicated. Later, a very simple proof of the above results has been given by Rödseth [5].

We now apply this to the basis (1), and illustrate in the case $c = 3$, hence $k = 4$. If we write $\gcd(m,n) = (m,n)$, then

$$b_1 = a_j a_{j+1} a_{j+2}, \quad b_2 = a_{j+1} a_{j+2} a_{j+3}$$

$$b_3 = a_{j+2} a_{j+3} a_{j+4}, \quad b_4 = a_{j+3} a_{j+4} a_{j+5}$$

$$d_2 = a_{j+1} a_{j+2} \quad \text{if} \quad (a_j, a_{j+3}) = 1$$

$$d_3 = a_{j+2} \quad \text{if also} \quad (a_{j+1}, a_{j+3}) = (a_{j+1}, a_{j+4}) = 1$$

$$d_4 = 1 \quad \text{if also} \quad (a_{j+2}, a_{j+3}) = (a_{j+2}, a_{j+4}) = (a_{j+2}, a_{j+5}) = 1 .$$

We will therefore assume that the base sequence $\{a_i\}$ satisfies $(a_i, a_{i+r}) = 1$ for $r = 1, 2, 3$ and all $i \geq 1$. In the general case, the corresponding condition is

$$\text{(5)} \qquad \gcd(a_i, a_{i+r}) = 1, \quad r = 1, 2, \ldots, c, \quad i = 1, 2, \ldots .$$

The conditions (4) are trivially satisfied, since

$$\frac{b_3}{d_3} = a_{j+3} a_{j+4} = a_{j+4} \frac{b_2}{d_2}, \quad \frac{b_4}{d_4} = a_{j+3} a_{j+4} a_{j+5} = a_{j+5} \frac{b_3}{d_3} .$$

In the general case, we similarly have

$$\frac{b_{i+1}}{d_{i+1}} = a_{j+c+i-1} \frac{b_i}{d_i}, \quad i = 2, 3, \ldots, c .$$

We can thus use (3) with equality. Since $d_0 = 0$ and $d_{i-1}/d_i = a_{j+i-2}$, $i = 2, 3, 4$, we get

$$g(B_4^{(j)}) = \sum_{i=2}^{4} a_{j+i-2} b_i - \sum_{i=1}^{4} b_i ,$$

where $b_i = h_{j+i}$. The generalization to (2) is immediate.

It remains to find base sequences $\{a_i\}$ satisfying (5). One obvious possibility is suggested in [4]: Choose $\alpha > 1$, and a_i as the smallest prime $\geq \alpha^i$.

An interesting alternative stems from Sedgewick's first paper [6], where his Theorem 6 in fact corresponds to $c = 2$ above (but he does not give $g(B_3^{(j)})$ explicitly), with

(6) $$a_i = 2^{i+1} - 3 .$$

The conditions (5) for $r = 1, 2$ are clearly satisfied, since $a_{i+1} - a_i = 2^{i+1}$, $a_{i+2} - a_i = 3 \cdot 2^{i+1}$. In fact, the choice (6) is possible also for $c = 3$, since now $a_{i+3} - a_i = 7 \cdot 2^{i+1}$, and $7 \nmid a_i$. This stems from the fact that 2 is not a primitive root of 7, $2^3 \equiv 1$, and $2^t \not\equiv 3 \pmod 7$ for all t.

For $c = 4$, we similarly form $a_{i+4} - a_i = (2^4-1)2^{i+1} = 3 \cdot 5 \cdot 2^{i+1}$. Since 2 is a primitive root both of 3 and of 5, we must now try to make $a_i = 2^{i+m} - n$, where n (odd) is divisible by 15. The smallest choice of n also possible modulo 7 is $n = 45$, so we can put

(7) $$a_i = 2^{i+5} - 45 .$$

Quite surprisingly, this choice is possible for all $c \leqq 9$, since

$$2^5-1 = 31,\ 2^6-1 = 3^2 \cdot 7,\ 2^7-1 = 127,\ 2^8-1 = 3 \cdot 5 \cdot 17,\ 2^9-1 = 7 \cdot 73 .$$

Here 2 is not a primitive root modulo any of the primes $p = 17$, 31, 73, 127, and it turns out that always $2^t \not\equiv 45 \pmod p$ for these four primes.

For $c = 10$, however, we have $2^{10} - 1 = 3 \cdot 11 \cdot 31$, where 2 is a primitive root of 11, so we must have $11 | n$. Trying to combine with the earlier primes considered, we end up with quite a large n.

For all sorting purposes, it is hardly practical to choose $c > 9$. We can then use (7), or (6) for $c = 2, 3$. I leave it to the sorting specialists (like Sedgewick) to test whether my above procedure for Shellsort can compete with procedures described earlier.

REFERENCES

1. A. Brauer, On a problem of partitions, Amer. J. Math. 64 (1942), 299-312.

2. A. Brauer and B. M. Seelbinder, On a problem of partitions, II, Amer. J. Math. 76 (1954), 343-346.

3. G. Hofmeister, Zu einem Problem von Frobenius, Kgl. Norske Vid. Selsk. Skrifter 1966 Nr. 5, 1-37.

4. J. Incerpi and R. Sedgewick, Improved upper bounds on Shellsort, J. Comput. System Sci. 31 (1985), 210-224.

5. Ö. J. Rödseth, Two remarks on linear forms in non-negative integers, Math. Scand. 51 (1982), 193-198.

6. R. Sedgewick, A new upper bound for Shellsort, J. of Algorithms 7 (1986), 159-173.

7. E. S. Selmer, On the linear diophantine problem of Frobenius, J. reine angew. Math. 293/294 (1977), 1-17.