SEL-68-003

ON THE TIME REQUIRED FOR GROUP MULTIPLICATION

by

P. M. Spira

January 1968

Scientific Report No. 24

Prepared under

National Aeronautics and Space Administration
Grant NsG 377

Radioscience Laboratory
Stanford Electronics Laboratories
Stanford University Stanford, California

ON THE TIME REQUIRED FOR GROUP MULTIPLICATION

by P. M. Spira

1. Introduction

This paper is concerned with the time required to perform group multiplication by means of networks of logical elements--each having a limited number of inputs and unit delay in computing their output function. Previously, Winograd [1] has considered the problem and has given a lower bound on the time required to multiply in a finite group as well as a method valid for abelian groups. Here we give a new lower bound which is, in general, higher than Winograd's but which reduces to his bound if the group of interest is abelian. In addition, a scheme to realize multiplication in any group, abelian or not, is given. This new circuit has computation time either equal to or one time unit greater than our lower bound. Also, if the group of interest is abelian, it computes at least as rapidly as Winograd's network to do the same multiplication.

2. Basic Concepts

Let C be a logical circuit composed of elements having at most r input lines, one splittable output line, and with unit delay in computing their outputs. Each line carries values from the set $J_d = \{0, 1, \ldots, d-1\}$. Let the input lines of C be partitioned into two sets with $I_{c,j}$ the set of possible configurations on the j^{th} $(j = 1,2)$. O_c is the set of output configurations. Following Winograd, such a circuit is called a (d,r) circuit.

Due to the unit delay in the elements comprising the circuit, there will be a certain delay between the time the inputs are presented and the time the output is available.

Let G be a finite group.

Definition. A circuit C is said to compute multiplication in G in time τ if there are maps $z_j\colon G \to I_{c,j}$ $(j = 1,2)$ and a 1-1 function $h\colon G \to O_c$ such that if C receives constant input $[z_1(a), z_2(b)]$ from time 0 through time $\tau-1$ the output at time τ will be $h(ab)$.

Definition. Let $h_j(x)$ be the value on the j^{th} output line of C when the overall output configuration is $h(x)$.

Definition. Let $A \subseteq G$. Then A is said to be right j-separable by C if, given $a_1, a_2 \in A$ with $a_1 \neq a_2$ then $\exists\, b \in G$ for which

$$h_j(a_1 b) \neq h_j(a_2 b)$$

Left separability is defined dually.

Definition. For any set S let $|S|$ be its cardinality. Let $\lceil x \rceil$ be the least integer $\geqq x$, and let $\lfloor x \rfloor$ be the greatest integer $\leqq x$.

Now let G be a finite group. Later on we will utilize the following definitions and lemma.

Definition. Let H be a subgroup of G. Say $P(a,H)$ holds if $\exists\, a \in H \backslash \{e\}$ contained in any non-trivial subgroup of H and say $P(H)$ holds if $P(a,H)$ holds for any $a \in H \backslash \{e\}$. Let $\alpha(G)$ be the order of the largest $H \leqq G$ such that $P(H)$ holds.

Definition. If $P(G)$ holds or $G = \{e\}$ let $\beta(G) = 1$. If not for any $c \in G \backslash \{e\}$ let $\beta(c)$ be the maximum order of any subgroup of G not containing c and let $\beta(G) = \min_{c \in G \backslash \{e\}} \{\beta(c)\}$.

Lemma 2.1. For any finite group $G, |G| \geqq \alpha(G)\, \beta(G)$.

Proof.

True trivially if $P(G)$ holds or if $G = \{e\}$. So assume not. Let $H < G$ and $a \in H$ with $P(a,H)$ holding and $|H| = \alpha(G)$. Let $K \leqq G$ with $|K| \leq \beta(G)$ and $a \notin K$. Then, since $H \cap K$ is a subgroup of H, $H \cap K = \{e\}$. Say $\exists\, g \in G$ such that

$$\{k_1, k_2\} \subseteq Hg \cap K$$

Then $\exists\ h_1, h_2 \in H$ for which $h_1 g = k_1$; $h_2 g = k_2$. Thus $k_1 k_2^{-1} \in H \cap K$. Hence $k_1 = k_2$ and there can be at most one element of K in any right coset of H. So

$$|H|\ |K| \leq G \quad ▮$$

3. The Lower Bound

We now give our lower bound after some preliminary lemmas.

Lemma 3.1. In a (d,r) circuit the output of an element at time τ can depend upon at most r^{τ} input lines.

Proof.

Just consider the fan-in with modules having r input lines each to the height of τ. ▮

Definition. For a (d,r) circuit C which multiplies in a finite group G let

$$R_j = \{x \in G : h_j(xa) = h_j(a)\ \forall a \in G\}$$

$$L_j = \{y \in G : h_j(by) = h_j(y)\ \forall b \in G\}$$

From this we obtain

Lemma 3.2. R_j and L_j are subgroups of G. A maximal size right j-separable subset of G contains exactly one element from each left coset of R_j in G; a maximal size left j-separable subset of G contains exactly one element from each right coset of L_j in G.

Proof.

If $x,y \in R_j$ then, given any $a \in G$

$$h_j(x^{-1}ya) = h_j(xx^{-1}ya) = h_j(a)$$

Thus $x^{-1}y \in R_j$, so it is a subgroup. If $h_j(xa) = h_j(ya)\ \forall a \in G$ then $h_j(y^{-1}xa) = h_j(a)\ \forall a \in G.$

Thus $y^{-1}x \in R_j$ so that $xR_j = yR_j$. The rest follows by duality. ▮

The underlying lemma used in deriving the lower bound is

Lemma 3.3. Let C be a (d,r) circuit to multiply for a group G in time τ. Then

$$\tau \geq \max_j \left\{ \left\lceil \log_r \left(\left\lceil \log_d \frac{|G|}{|R_j|} \right\rceil + \left\lceil \log_d \frac{|G|}{|L_j|} \right\rceil \right) \right\rceil \right\}$$

Proof.

The j^{th} output at time τ must depend upon at least $\left\lceil \log_d \frac{|G|}{|R_j|} \right\rceil$ input lines of $I_{c,1}$ and upon at least $\left\lceil \log_d \frac{|G|}{|L_j|} \right\rceil$ input lines of $I_{c,2}$ since there are right and left j-separable sets of size $\frac{|G|}{|R_j|}$ and $\frac{|G|}{|L_j|}$ respectively. Thus, from lemma 3.1

$$r^\tau \geq \max_j \left\{ \left\lceil \log_d \frac{|G|}{|R_j|} \right\rceil + \left\lceil \log_d \frac{|G|}{|L_j|} \right\rceil \right\} \quad ▮$$

We have enough to prove

Theorem 3.4. Let G be a finite group. Then if C is a (d,r) circuit to multiply in G in time τ

$$\tau \geq \left\lceil \log_r 2 \left\lceil \log_d \frac{|G|}{\beta(G)} \right\rceil \right\rceil$$

Proof.

Let $a \in G$ be such that $\beta(a) = \beta(G)$. Now $\exists\, j$ for which $h_j(a) \neq h_j(e)$. Thus $a \notin R_j(e)$ and $a \notin L_j(e)$. Hence

$$|R_j| \leq \beta(G) ; \qquad |L_j| \leq \beta(G)$$

and the result follows from lemma 3.3. ▮

Corollary 3.5. Also

$$\tau \geq \lceil \log_r 2 \lceil \log_d \alpha(G) \rceil \rceil$$

Thus Winograd's result is a corollary of our lower bound.

In his paper [1] Winograd indicates that, if G is abelian, then $\alpha(G)$ is the order of the largest cyclic p-subgroup of G. A complete characterization of $\alpha(G)$ is provided below. First

Definition. Q_n, the generalized quaternion group, is the group of order 2^n with two generators a and b satisfying

$$a^{2^{n-1}} = 1 \qquad b^2 = a^{2^{n-2}} \qquad ba = a^{-1}b$$

Theorem 3.6. A p-group contains a unique subgroup of order p iff it is cyclic or a generalized quaternion group. (It must be cyclic if p is odd).

Proof.

See Hall [2] p 189. ▮

Corollary 3.7. Let G be any finite group. Then $\alpha(G)$ is either the order of the largest cyclic p-subgroup of G or the order of the largest generalized quaternion group contained in G, whichever is larger.

Proof.

Let H be any subgroup of G. As noted above, if P(H) holds, then H is a p-group with $|H| = p^n$ for some prime p and integer n. But every subgroup of H contains a subgroup of order p. Hence P(H) will hold iff H contains a unique subgroup of order p. But then H is either cyclic of order p^n or a generalized quaternion. ▌

We close this section with an example of a group G with $\alpha(G)\ \beta(G) < |G|$.

Example.

Let p be a prime > 2. Then there is a group generated by three generators a, b, and c with defining relations [2] (page 52)

$$a^p = b^p = c^p = e \qquad ab = bac \qquad ca = ac \qquad cb = bc$$

which has no element of order p^2. Let H be a subgroup of order p^2. Then it is easy to show that $c \epsilon H$. Hence

$$\beta(G) = p$$

But $\alpha(G)$ will also be p since, if 2 does not divide the order of a group G, then $\alpha(G)$ is the size of the largest cyclic p-subgroup of G. Hence

$$\alpha(G)\ \beta(G) = p^2 < |G|$$

This shows that our lower bound is, in general, higher than Winograd's. The following lemma shows that the two bounds are equal if G is abelian.

Lemma 3.6. Let G be abelian. Then $|G| = \alpha(G)\,\beta(G)$.

Proof.

G is abelian so $G \cong J = J_1 \times \dots \times J_s$, where each J_i is a cyclic p-group with $|J_i| = p_i^{r_i}$ and, with no loss of generality $p_i^{r_i} \geqq p_j^{r_j}$ if $i < j$. Assume $s > 1$ or else the theorem is trivial. Let b_i generate $J_i; 1 \leqq i \leqq s$, and write a generic element of J as $(b_1^{t_1}, \dots, b_s^{t_s})$. Then $P(b_1, J_1)$ holds and $\alpha(J) = p_1^{r_1}$. Similarly $b_1 \notin J_2 \times \dots \times J_s$ but is in any subgroup which intersects J_1 non-trivially. Thus

$$\beta(J) \leq \beta(b_1) = \prod_{1=2}^{s} p_i^{r_i}$$

Let $b = (b_1^{t_1}, \dots, b_s^{t_s})$ be any element of $J \setminus \{e\}$. Then $\exists\, j$ with $t_j \not\equiv 0 \pmod{p_j^{r_j}}$ and

$$b \notin \prod_{\substack{i=1\\ i \neq j}}^{s} J_i$$

Hence $\beta(b) \geqq \beta(b_1)$. Thus

$$\beta(b_1) = \beta(J) = \prod_{1=2}^{s} p_i^{r_i}$$

and the theorem is true by isomorphism. ▮

4. The Multiplication Scheme for Finite Groups

In this section we describe a scheme to multiply with a (d,r) circuit valid in any finite group G--abelian or not--and show that our computation time is never more--and often less--than that of Winograd's circuit in the case that G is abelian. In addition, our scheme will be valid for $r \geqq 2$, $d \geqq 2$ whereas his is not valid unless $r \geqq 3$.

Lemma 4.1. Let K be any subgroup of G. Then $\exists$ a (d,r) circuit to compute $\phi : G \times G \rightarrow \{0,1\}$ in time

$$\tau = 1 + \left\lceil \log_r \left\lceil \log_d \frac{|G|}{|K|} \right\rceil \right\rceil$$

where

$$\phi(a,b) = 0 \qquad \text{if} \qquad ab \in K$$

$$\phi(a,b) = 1 \qquad \text{if} \qquad ab \notin K$$

Proof.

Let $M = \frac{|G|}{|K|}$. Pick a coset representative $v_i \in Kv_i$ for each right coset of K in G. Then $\left\{v_i^{-1}\right\}$ will be a set of left coset representatives, for $v_i^{-1}K = v_j^{-1}K$ iff $v_i v_j^{-1} \in K$ iff $v_j^{-1} = v_i^{-1}$. Define maps z_1 and z_2 from G to the space of $\lceil \log_d M \rceil$ -ary vectors over J_d such that

$$z_1(g_1) = z_1(g_2) \quad \text{iff} \quad Kg_1 = Kg_2$$

$$z_1(g) \oplus z_2(g^{-1}) = \overline{0}$$

where $\overline{0}$ is the all zero vector and $\oplus$ is componentwise addition modulo d. Note that z_2 maps any two elements in the same left coset to the same vector. The first level of the circuit consists of $\lceil \log_d M \rceil$ modulo d adders. If ab is being computed these adders sum $z_1(a)$ and $z_2(b)$ componentwise mod d. Thus all outputs are 0 iff $\exists\, j$ such that $a \in Kv_j$ and $b \in v_j^{-1}K$, i.e. iff $ab \in K$. The rest of the circuit is a fan-in of r input elements having output 0 iff all inputs are 0 and output 1 if at least one input is nonzero. This fan-in has depth $\lceil \log_r \lceil \log_d M \rceil \rceil$. Thus the circuit computes ϕ in time

$$\tau = \lceil \log_r \lceil \log_d M \rceil \rceil + 1 \quad ∎$$

Corollary 4.2. There is a (d,r) circuit to tell if $ab \in Ku$ for any $u \in G$ in the same time.

Lemma 4.3. Say G has subgroups $K_1, \ldots, K_n$ such that $\bigcap_{j=1}^{n} K_j = \{e\}$. Then knowing the right cosets containing any $a \in G$ suffices to determine a.

Proof.

Say $\exists a_1, a_2 \in G$ such that $K_j a_1 = K_j a_2 \forall j$. Then $\bigcap_{j=1}^{n} K_j a_1 = \bigcap_{j=1}^{n} K_j a_2$. Thus $a_1 = a_2$. ▮

Corollary 4.4. If $K_1, \ldots, K_n$ is such a set of subgroups then $\exists$ a (d,r) circuit to compute multiplication in G in time

$$\tau = 1 + \max_{1 \leq j \leq n} \left\lceil \log_d \left\lceil \log_r \frac{|G|}{|K_j|} \right\rceil \right\rceil$$

We now immediately obtain

Theorem 4.5. For any $d \geqq 2$ and any $r \geqq 2$ there is a (d,r) circuit to multiply in a finite group G in time

$$\tau = 1 + \left\lceil \log_d \left\lceil \log_r \frac{|G|}{\beta(G)} \right\rceil \right\rceil$$

Furthermore this circuit is within one time unit of the fastest obtainable.

Proof.

The first part follows from lemma 4.3 and the definition of $\beta(G)$; the rest follows from the fact that

$$\lceil \log_d \lceil \log_r x \rceil \rceil + 1 \geqq \lceil \log_d 2 \lceil \log_r x \rceil \rceil \text{ ▮}$$

From lemma 3.5 it follows that if G is abelian there is a (d,r) circuit to multiply in G in time

$$\tau = 1 + \lceil \log_d \lceil \log_r \alpha(G) \rceil \rceil$$

In his paper [1] Winograd derives a (d,r) circuit which performs multiplication in such an abelian group in time

$$\tau = 2 + \left\lceil \log_{\left\lfloor \frac{(r+1)}{2} \right\rfloor} \left(\frac{1}{\left\lfloor \frac{r}{2} \right\rfloor} \right) \lceil \log_d \alpha(G) \rceil \right\rceil \quad \text{for} \quad r \geqq 3$$

From the fact that this number is always at least as great as

$$1 + \left\lceil \log_{\left\lfloor \frac{(r+1)}{2} \right\rfloor} \lceil \log_d \alpha(G) \rceil \right\rceil$$

and in addition

$$\left\lfloor \frac{r+1}{2} \right\rfloor < r \quad \text{for} \quad r \geqq 3$$

it follows that his computation time is never less than ours and often greater.

Example.

Say $r = 4$ and $\lceil \log_d \alpha(G) \rceil = 2^{2k}$ for some $k \geqq 1$.

Then Winograd's time is $1 + 2k$ and our computation time is $1 + k$, i.e., his circuit requires about twice as long.

The reader can easily construct a myriad of similar examples.

It has been pointed out to the author by Winograd [3] that our construction can be altered as follows. If there is an integer k for which $2k \leqq r$, then each element in the first level of the circuit can actually test k components of the input vectors. This results in a computation time of

$$1 + \left\lceil \log_r \frac{1}{k} \left\lceil \log_d \frac{|G|}{\beta(G)} \right\rceil \right\rceil$$

Thus a computation time of

$$1 + \left\lceil \log_r \left(\frac{1}{\left\lfloor \frac{r}{2} \right\rfloor} \right) \left\lceil \log_d \frac{|G|}{\beta(G)} \right\rceil \right\rceil$$

can be achieved. This means that there are cases in which our original construction has time one greater than the lower bound but this altered version is as rapid as possible. This is true, e.g., if

$$\left\lceil \log_d \frac{|G|}{\beta(G)} \right\rceil = 5 \quad \text{and} \quad r = 4$$

REFERENCES

1. Winograd, "On the Time Required To Perform Addition," J. of the ACM, Vol. 12, No. 2, April, 1965, pp. 277-285.

2. Marshall Hall, Jr., The Theory of Groups, The Macmillan Company, New York, 1959.

3. S. Winograd, private communication.