The Time Required for Group Multiplication

PHILIP M. SPIRA

Stanford University, Stanford, California*

ABSTRACT. Winograd has considered the time necessary to perform numerical addition and multiplication and to perform group multiplication by means of logical circuits consisting of elements each having a limited number of input lines and unit delay in computing their outputs. In this paper the same model as he employed is adopted, but a new lower bound is derived for group multiplication—the same as Winograd's for an Abelian group but in general stronger. Also a circuit is given to compute the multiplication which, in contrast to Winograd's, can be used for non-Abelian groups. When the group of interest is Abelian the circuit is at least as fast as his. By paralleling his method of application of his Abelian group circuit, it is possible also to lower the time necessary for numerical addition and multiplication.

KEY WORDS AND PHRASES: computation complexity, logic circuits, logical design, finite-state automata, finite functions, group, addition, multiplication

CR CATEGORIES: 5.39, 6.1

1. *The Model*

The model we adopt is basically that of Winograd [1, 2]. We consider logical circuits composed of elements each having at most r input lines, one splittable output line, and unit delay in computing their outputs. Each line carries values from the set $Z_d = \{0, 1, \cdots, d - 1\}$. The input lines are partitioned into n sets with $I_{C,j}$ the set of possible configurations on the jth $(j = 1, 2, \cdots, n)$. O_C is the set of possible configurations. Such a circuit is called a (d, r) circuit.

Definition 1.1. Let $\phi: X_1 \times X_2 \times \cdots \times X_n \rightarrow Y$ be a function on finite sets. A circuit C is said to compute ϕ in time τ if there are maps $g_j: X_j \rightarrow I_{C,j}$ $(j = 1, 2, \cdots, n)$ and a one-one function $h: Y \rightarrow O_C$ such that if C receives constant input $[g_1(x_1), \cdots, g_n(x_n)]$ from time 0 through time $\tau - 1$, then the output at time τ will be $h(\phi(x_1, \cdots, x_n))$.

2. *The Basic Lemma*

We now derive a general lower bound on the time for a (d, r) circuit to compute a given finite function ϕ. It makes explicit the method underlying the results of Winograd. It is dependent upon the output code h introduced in Section 1, and makes

* Department of Electrical Engineering. Some of this material was presented at the Eighth IEEE Annual Symposium on Switching and Automata Theory. (See Spira, P. M., and Arbib, M. A., Computation time for finite groups, semigroups and automata, in IEEE Conf. Record of Eighth Annual Symp. on Switching and Automata Theory, Oct. 1967, pp. 291–295.) This research was supported in part by the National Aeronautics and Space Administration under Grant No. NsG-377 (3208) and in part by the US Air Force Office of Scientific Research, Information Sciences Directorate, under Grant No. AF-AFOSR-1198-67. It is part of the author's doctoral thesis.

use of a new concept we introduce—that of separable sets. First, some preliminary definitions are necessary.

Definition 2.1. Let $\lceil x \rceil$ be the smallest integer greater than or equal to x; let $\lfloor x \rfloor$ be the largest integer less than or equal to x; let $|S|$ be the cardinality of the set S.

Definition 2.2. For a (d, r) circuit let $h_j(y)$ be the value on the jth output line when the overall output configuration is $h(y)$.

Definition 2.3. Let $\phi: X_1 \times \cdots \times X_n \rightarrow Y$ and let C compute ϕ. Then $S \subseteq X_m$ is called an h_j-separable set for C in the mth argument of ϕ if whenever s_1 and s_2 are distinct elements of S we can find $x_1, x_2, \cdots, x_{m-1}, x_{m+1}, \cdots, x_n$ with $x_i \in X_i$ such that

$$h_j(\phi(x_1, \cdots, x_{m-1}, s_1, x_{m+1}, \cdots, x_n)) \neq h_j(\phi(x_1, \cdots, x_{m-1}, s_2, x_{m+1}, \cdots, x_n)).$$

LEMMA 2.1. *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 to the height of τ. |

This observation, first made by Winograd, plus the concept of separable sets, suffices to prove:

LEMMA 2.2 (*The basic lemma*). *Let C be a (d, r) circuit which computes ϕ in time τ. Then*

$$\tau \geq \max_j \{\lceil \log_r (\lceil \log_d |S_1(j)| \rceil + \cdots + \lceil \log_d |S_n(j)| \rceil) \rceil\},$$

where $S_i(j)$ is an h_j-separable set for C in the j-th argument of ϕ.

PROOF. The jth output line at time τ must depend upon at least $\lceil \log_d |S_i(j)| \rceil$ input lines from $I_{C,i}$ or else there would be two elements of $S_i(j)$ which were not h_j-separable. Thus the jth output depends upon at least $\lceil \log_d |S_1(j)| \rceil + \cdots + \lceil \log_d |S_n(j)| \rceil$ input lines and this number is at most r^τ. |

With Lemma 2.2 we expose the methodology implicit in Winograd's treatment of the times required for addition and multiplication. By making it explicit we not only quickly obtain some of Winograd's results in the rest of this section but also shall give a deeper analysis of other concepts and shall treat a much wider class of functions in the sequel.

COROLLARY 2.1. *Let $\phi: Z_N \times Z_N \rightarrow \{0, 1\}$ be*

$$\phi(x, y) = \begin{cases} 1 & \text{if } x \leq y, \\ 0 & \text{if } x > y. \end{cases}$$

Then if C is a (d, r) circuit to compute ϕ in time τ, we have $\tau \geq \lceil \log_r 2 \lceil \log_d N \rceil \rceil$.

PROOF. Pick j such that $h_j(0) \neq h_j(1)$. Then Z_N is an h_j-separable set for C in both the first and the second arguments of ϕ since, if $x > y$, $\phi(x, y) \neq \phi(y, y)$ and $\phi(x, y) \neq \phi(x, x)$. |

COROLLARY 2.2. *Let $\phi: Z_N \times Z_N \rightarrow Z_N$ be*

$$\phi(x_1, x_2) = \left\lfloor \frac{x_1 \cdot x_2}{N} \right\rfloor.$$

Then, if C computes ϕ in time τ, $\tau \geq \lceil \log_r 2 \lceil \log_d \lfloor N^{\frac{1}{2}} \rfloor \rceil \rceil$.

PROOF. Pick j such that $h_j(0) \neq h_j(1)$. Let $m = \lfloor N^{\frac{1}{2}} \rfloor$. Then $\{1, 2, \cdots, m\}$ is an h_j-separable set for C in both arguments of ϕ, since for each $x \neq y$ with $x, y \in \{1, 2, \cdots, m\}$ we may chose $w \in Z_N$ such that $x \cdot w < N \leq y \cdot w < 2N$ to yield $\phi(x, w) = 0$, $\phi(y, w) = 1$. By symmetry this holds for the second argument as well and Lemma 2.2 yields the result. |

We close this section with an example which shows that the size of separable sets can be strongly dependent upon the output code of the circuit which computes a given ϕ.

Example 2.1. Let $\phi : Z_N \times Z_N \rightarrow Z_{N^2}$ be numerical multiplication with $N = 2^8$. Consider an output code in which if the output value is M then the ith line carries the ith bit in the binary expansion for M. Then there are sixteen output lines. Pick any $x \neq y$ with $x, y \in Z_N$. Then their binary expansions differ in at least one place, say the kth. Choose $z = 2^{8-k}$. Then $h_j(\phi(y, z)) \neq h_j(\phi(x, z))$ and $h_j(\phi(z, y)) \neq h_j(\phi(z, x))$. So there is an h_8-separable set of size 2^8 in both arguments of ϕ.

Now consider the same ϕ but let the output code for z be the binary representation of the exponents in its prime decomposition. Let the first six output lines code the exponent of two in the result. Pick $x, y \in Z_N$ such that x and y do not have the same power of two in their prime decomposition, the powers differing in, say, the kth place of their binary expansion. Then, letting $z = 2^{3-k}$, $h_3(\phi(x, z)) \neq h_3(\phi(y, z))$ and $h_3(\phi(z, x)) \neq h_3(\phi(z, y))$. Thus, since an element of Z_N can have eight different exponents of two in its prime decomposition, there is an h_3-separable set of size 8 in both arguments of ϕ. One easily sees that this is the maximal size of any separable set, since two is the smallest prime. Note, however, that this output code requires thirty-nine output lines.

3. *Review of Previous Results*

Several authors have investigated the computation time necessary for a (d, r) circuit to add modulo N. Ofman [3] gave a circuit for the special case $N = 2^n$. Significant results were obtained by Winograd [1, 2]. He derived a lower bound which we review, and a (d, r) circuit with computation time near the lower bound. Since any finite Abelian group is the direct product of cyclic groups [4, p. 40], his results are applicable to Abelian group multiplication as well.

Definition 3.1. Let H be a group. Say H has property P and write $P(H) = 1$, in case there is an element $a \in H$ with $a \neq e$ such that every nontrivial subgroup of H contains a. This is denoted by $P(a, H) = 1$. Let $\alpha(G)$ be the maximal order of $H \leq G$ such that $P(H) = 1$.

Lemma 3.1 (Winograd [1]). *If G is Abelian, $\alpha(G)$ is the maximal order of a prime power cyclic subgroup contained in G.*

Proof. See [1, p. 280]. |

We now give a complete characterization of $\alpha(G)$.

Definition 3.2. The generalized quaternion group Q_n is the group of order 2^n with two generators a and b satisfying

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

Theorem 3.1. *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 [4, p. 189]. |

Corollary 3.1. *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. If $P(H) = 1$ then $|H| = p^n$ for some prime p, for if not there would be another prime q dividing $|H|$ and consequently there would be elements u and v in H with $o(u) = p$ and $o(v) = q$. But then $\langle u \rangle \cap \langle v \rangle$ would contain only the identity. Assume $|H| = p^n$. Then every nontrivial subgroup of H contains a subgroup of order p. Thus $P(H) = 1$ iff H contains a unique subgroup of order p, i.e. iff H is cyclic or a generalized quaternion group. |

The quantity $\alpha(G)$ is critical to Winograd's lower bound time for group multiplication, which we now state. In Section 4 we give a new lower bound which is in general higher but is the same as his if the group of interest is Abelian.

THEOREM 3.2 (Winograd [1]). *Let G be any finite group. Let C be a (d, r) circuit which computes $\phi: G \times G \to G$ where $\phi(a, b) = ab$. Then C requires computation time τ where $\tau \geq \lceil \log_r 2 \lceil \log_d \alpha(G) \rceil \rceil$.*

PROOF. See Winograd [1]. |

Winograd also gives a procedure for constructing a circuit to multiply in an Abelian group G with computation time

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

which is valid for $r \geq 3$ and $d \geq 2$. We give a completely different method for constructing circuits, which is valid for $r \geq 2$ and $d \geq 2$ and which works whether or not the group is Abelian. Furthermore, for a given Abelian group and a given d and r, our computation time underbounds Winograd's.

4. *The Lower Bound*

In this section we give a new lower bound for the time required for a (d, r) circuit to perform group multiplication and compare it to Winograd's bound. Let G be any finite group and let $\phi: G \times G \to G$ be group multiplication. Let C be a (d, r) circuit which computes ϕ. Let $h_j(g)$ be the value on the jth output line of C when the output is $h(g)$.

Definition 4.1. Let $x, y \in G$. Then we say that x and y are R_j-equivalent if $h_j(gx) = h_j(gy)$ for all $g \in G$ and that they are L_j-equivalent if $h_j(xg) = h_j(yg)$ for all $g \in G$. Then clearly R_j and L_j are equivalence relationships and we write $R_j(g)$ for the R_j-equivalence class of g and $L_j(g)$ for the L_j-equivalence class of g.

LEMMA 4.1. *$R_j = R_j(e)$ and $L_j = L_j(e)$ are groups for all output lines of C. Furthermore, for any $g \in G$, $R_j(g) = R_j g$ and $L_j(g) = gL_j$.*

PROOF. Say $a, b \in R_j$. Let $c \in G$. Then $h_j(ab^{-1}c) = h_j(bb^{-1}c) = h_j(c)$. So $ab^{-1} \in R_j$ and it is a group. Now pick any $g \in G$. Then $d \in R_j(g)$ iff $h_j(dc) = h_j(gc)$ for all $c \in G$. But this is true iff $h_j(dg^{-1}c) = h_j(c)$, i.e. iff $dg^{-1} \in R_j$. The other half of the lemma follows dually. |

Maximal separable sets are determined by

LEMMA 4.2. *A maximal size h_j-separable set in the first argument of ϕ consists of exactly one representative from each left coset of R_j in G. It thus has size $|G|/|R_j|$. A dual result is true for separable sets in the second argument.*

PROOF. Direct from Lemma 4.1 and the definition of separable sets. |

We now have all the pieces we need for a lower bound on group multiplication which is output code dependent.

LEMMA 4.3. *Let C be a (d, r) circuit to multiply in 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. Direct from Lemmas 2.2 and 4.2. |

A bound over all output codes is derived by maximizing the minimal size of K_j and L_j for a given group.

Definition 4.2. If $G = \{e\}$ let $\delta(G) = 1$. Otherwise let $\delta(c)$ be the maximal order of any subgroup of G not containing c and let $\delta(G) = \min_{c \in G - \{e\}} \{\delta(c)\}$.

Since we are only dealing with finite groups $\delta(G)$ is always well defined and finite. Note that if $P(a, G) = 1$ then $\delta(a) = 1$ so that $\delta(G) = 1$. Note also that if G is nontrivial and $P(G) \neq 1$ then $\delta(G) > 1$ always. A simple lemma needed in the sequel is:

LEMMA 4.4. *Let H and K be subgroups of a finite group G such that $H \cap K = \{e\}$. Then $|H| |K| \leq |G|$.*

PROOF. Let $h_1, h_2 \in H$ and $k_1, k_2 \in K$ such that $h_1k_1 = h_2k_2$. Then $h_1h_2^{-1} = k_2k_1^{-1} \in H \cap K$. Hence $h_1 = h_2$ and $k_1 = k_2$. Thus $| \{hk : h \in H, k \in K\} | \geq |H| |K|$. But it is also a subset of G. |

The crucial property of $\delta(G)$ is:

LEMMA 4.5. *For any finite group G, $\alpha(G)\delta(G) \leq G$.*

PROOF. If $\delta(G) = 1$ the lemma is true, so assume not. Pick $H < G$ and $e \neq a \in H$ with $P(a, H) = 1$ and $|H| = \alpha(G)$. Choose $K < G$ with $a \notin K$ and $|K| = \delta(a)$. Then, since $H \cap K$ is a subgroup of H not containing a, $H \cap K = \{e\}$. Hence, by Lemma 4.3 and the fact that $\delta(G) \leq \delta(a)$, $\alpha(G)\delta(G) \leq \alpha(G)\delta(a) = |H| |K| \leq |G|$. |

The universal lower bound for any (d, r) circuit to compute multiplication in a finite group G can now be stated.

THEOREM 4.1. *Let G be a finite group, $\phi : G \times G \to G$ be group multiplication, and C be a (d, r) circuit to compute ϕ for $d \geq 2$ and $r \geq 2$. Then, if C has computation time τ,*

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

PROOF. Assume $\delta(G) > 1$ and choose $a \in G$ such that $\delta(a) = \delta(G)$. There must be an output line of C, say the jth, such that $h_j(e) \neq h_j(a)$. But then both R_j and L_j are subgroups of G which do not contain a. They hence have order at most $\delta(G)$. Thus, the result follows from Theorem 4.1. If $\delta(G) = 1$ then either $G = \{e\}$ or $|G| = \alpha(G)$. In the former case the theorem is true trivially. In the latter case choose $g \in G$ such that $P(g, G) = 1$ and pick an output line, say the ith, such that $h_i(e) \neq h_i(g)$. Then $R_j = L_j = \{e\}$ and the result follows from Theorem 4.1. |

Lemma 4.5 implies that this lower bound is no weaker than Winograd's result given in Theorem 3.2; and, indeed, the following example shows that it is stronger.

Example 4.1. Let p be an odd prime. Then there is a group with three generators a, b, and c and defining relations [4, p. 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. It is easy to show that any subgroup of order p^2 must contain c. Thus $\delta(G) = \delta(c) = p$. But, clearly, $\alpha(G) = p$. Thus $\alpha(G)\delta(G) < |G|$. In one important case, however, the two bounds are the same.

LEMMA 4.6. *Let G be a finite Abelian group. Then $\alpha(G)\delta(G) = |G|$.*

PROOF. By the decomposition theorem for Abelian groups [4, p. 40], $G = Z_1 \times \cdots \times Z_n$, where each Z_i is a cyclic p-group, say $|Z_i| = p_i^{r_i}$; and, with no loss of generality,

$$i < j \Rightarrow p_i^{r_i} \geq p_j^{r_j}. \tag{*}$$

If $n = 1$ the theorem is true since $P(G) = 1$ and $\delta(G) = 1$. Assume $n > 1$ and let a_i generate Z_i $(i = 1, 2, \cdots, n)$. Now if we choose any $g \neq e$,

$$g = (a_1^{k_1}, \cdots, a_n^{k_n}),$$

where at least one exponent, say k_i, is nonzero, then

$$g \notin \left(\prod_{\substack{j \neq i \\ j = i}}^{n} Z_j\right) \times \{e_i\},$$

where e_i is the identity in Z_i. It follows that

$$\delta(g) \geq \prod_{\substack{j \neq i \\ j = i}}^{n} p_j^{r_j} \geq \prod_{j=2}^{n} p_j^{r_j}$$

by (*). Thus

$$\delta(G) \geq \prod_{j=2}^{n} p_j^{r_j}.$$

But any subgroup of order greater than $\prod_{j=2}^{n} p_j^{r_j}$ must intersect Z_1 nontrivially and thus must contain

$$(a_1^{p_1^{(r_1-1)}}, e_2, \cdots, e_n) \notin \{e_1\} \times Z_2 \times \cdots \times Z_n .$$

Thus

$$\delta(G) \leq \delta\left((a_1^{p_1^{(r_1-1)}}, e_2, \cdots, e_n)\right) = \prod_{j=2}^{n} p_j^{r_j}. \quad |$$

For the sake of completeness we give some examples of non-Abelian groups G_i, each having $\alpha(G_i)\delta(G_i) = |G_i|$.

Example 4.2. Let p be an odd prime. Let G_1 be the group generated by a and b having relations [4, p. 52] $a^{p^2} = b^p = e$; $b^{-1}ab = a^{1+p}$. Then $\alpha(G_1) = p^2$ and any group of order p^2 must contain a^p.

Example 4.3. Let G_2 be the direct product of two groups A and B such that $\alpha(A)\delta(A) = |A|$; $\alpha(B)\delta(B) = |B|$. Then it is easy to see that

$$\alpha(G_2) = \max \{\alpha(A), \alpha(B)\}; \qquad \delta(G_2) = \min \{|B|\ \delta(A), |A|\ \delta(B)\};$$

and thus $\alpha(G_2)\delta(G_2) = |G_2|$. In particular, these properties hold if G_2 is non-Abelian but all of its subgroups are normal [4, p. 190].

5. *A Circuit for Group Multiplication*

In this section we give a method to construct a (d, r) circuit to multiply in any finite group G which is valid for $d \geq 2$ and $r \geq 2$. The computation time of the circuit is at most one unit greater than the lower bound just derived. If G is Abelian and $r \geq 3$ our circuit can be compared to that of Winograd. It can be seen that our computation time underbounds his, and that, in fact, we can give a group for which the difference in computation time is arbitrarily large.

LEMMA 5.1. *Let K be any subgroup of G. Then there is a (d, r) circuit to compute $\phi : G \times G \rightarrow \{0, 1\}$ in time*[1]

$$\tau = 1 + \left\lceil log_r \left\lceil \frac{1}{\lfloor r/2 \rfloor} \left\lceil log_d \frac{|G|}{|K|} \right\rceil \right\rceil \right\rceil,$$

where

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

$$\phi(a, b) = 1 \quad \textit{if} \quad ab \notin K.$$

PROOF. Let $M = |G|/|K|$. Pick a coset representative $v_i \in Kv_i$ for each right coset of K in G. Then $\{v_i^{-1}\}$ is a set of left coset representatives, for $v_i^{-1}K = v_j^{-1}K$ iff $v_i v_j^{-1} \in K$. Pick a map z_1 from G to the space of $\lceil \log_d M \rceil$-ary vectors over Z_d such that $z_1(g_1) = z_1(g_2)$ iff $Kg_1 = Kg_2$ and then define another map z_2 with same domain and range by $z_1(g) \oplus z_2(g^{-1}) = \mathbf{0}$, where $\mathbf{0}$ 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. There are $\lceil (1/\lfloor r/2 \rfloor) \lceil \log_d M \rceil \rceil$ similar elements in the first level of the circuit. If ab is being computed these modules each sum components of $z_1(a)$ and $z_2(b)$ mod d (the last adder will sum less than $\lfloor r/2 \rfloor$ if $\lfloor r/2 \rfloor$ does not divide M). An element has output 0 if all pairs of input components are congruent to 0 mod d. If not, its output is 1. Thus all outputs are 0 iff there is some j such that $a \in Kv_j$ and $b \in v_j^{-1}K$. 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 $\lceil \log_r \lceil (1/\lfloor r/2 \rfloor) \lceil \log_d M \rceil \rceil \rceil$. Thus the circuit computes ϕ in time

$$\tau = 1 + \left\lceil \log_r \left\lceil \frac{1}{\lfloor r/2 \rfloor} \left\lceil \log_d M \right\rceil \right\rceil \right\rceil. \quad |$$

COROLLARY 5.1. *There is a (d, r) circuit to tell if $ab \in Kv$ for any $v \in G$ with the same computation time.*

Definition 5.1. A complete set of subgroups of a group G is a set $\{K_i\}$ of subgroups for which $\bigcap_i K_i = \{e\}$.

LEMMA 5.2. *If K_i is a complete set of subgroups of G then, for any $a \in G$, knowledge of the right cosets containing a is sufficient to determine a.*

PROOF. $\bigcap (K_i a) = (\bigcap K_i)a = a.$ |

Note that a complete set of subgroups always exists for any G, e.g. the set consisting of $\{e\}$ alone. Unless $P(G) = 1$, there are other complete sets as well.

LEMMA 5.3. *Let $\{K_i\}$ be a complete set of subgroups of G. Then there is a (d, r) circuit to multiply in G in time*

[1] The original statement of this lemma had $\tau = 1 + \lceil \log_r \lceil \log_d (|G| / |K|) \rceil \rceil$. The refinement was pointed out to the author by Winograd.

$$\tau = 1 + \max_i \left\{ \left\lceil log_r \left\lceil \frac{1}{\lfloor r/2 \rfloor} \left\lceil log_d \frac{|G|}{|K_i|} \right\rceil \right\rceil \right\rceil \right\}.$$

PROOF. Follows from Lemma 5.1, Corollary 5.1, and Lemma 5.2. |

Now we are able to prove

THEOREM 5.1. *Let G be any finite group. Then for any $d \geq 2$ and any $r \geq 2$ there is a (d, r) circuit to multiply in a finite group G in time*

$$\tau = 1 + \left\lceil log_r \left\lceil \frac{1}{\lfloor r/2 \rfloor} \left\lceil log_d \frac{|G|}{\delta(G)} \right\rceil \right\rceil \right\rceil.$$

Furthermore, the circuit has computation time exceeding the lower bound by at most one time unit.

PROOF. Assume $\delta(G) > 1$. For any $g \in G$ with $g \neq e$ there is a subgroup K_g of order $\delta(g)$ not containing g. Thus $\{K_g : g \in G - \{e\}\}$ is a complete set of subgroups with $\min \{ |K_g| : g \in G - \{e\}\} = \delta(G)$. If $\delta(G) = 1$ then use the complete set consisting of $\{e\}$. The second statement of the theorem follows from the fact that

$$\left\lceil \log_r \left\lceil \frac{1}{\lfloor r/2 \rfloor} \left\lceil \log_d x \right\rceil \right\rceil \right\rceil \leq \lceil \log_r 2 \lceil \log_d x \rceil \rceil$$

for $r \geq 2$. |

COROLLARY 5.2. *If G is Abelian or if $\delta(G) = 1$ there is a (d, r) circuit to multiply in G in time*

$$\tau = 1 + \left\lceil log_r \left\lceil \frac{1}{\lfloor r/2 \rfloor} \left\lceil log_d \, \alpha(G) \right\rceil \right\rceil \right\rceil.$$

As noted, Winograd's circuit for an Abelian group G requires time

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

Since

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

it follows that our computation time is less than his.

Example 5.1. Say $r = 4$ and $\lceil \log_d \alpha(G) \rceil = 2^{2^k}$ for some $k \geq 1$. Then Winograd's time is $2 + 2k$ and our time is $1 + k$, i.e. his circuit requires twice as long. The reader can easily construct a myriad of similar examples.

Winograd [2] has extended his group results to numerical addition and multiplication by noting that a circuit which can multiply in the cyclic group of order $2N - 1$ can also add two numbers between 0 and N and that numerical multiplication can be done by adding the exponents in the prime decompositions of the two factors. Since we are able to lower the time necessary to multiply in cyclic groups, we can achieve a corresponding decrease in the time for numerical addition and multiplication as well. We present this result in the framework of Winograd's definitions. The reader interested in the details of the relationship between group multiplication and these other two operations is referred to Winograd's original paper.

Definition 5.2. For an integer m let $Q_m = \text{l.c.m.}\{1, 2, \cdots, m\}$ and let $\gamma(N) = \min\{m : Q_m \geq N\}$.

Then, paralleling Winograd's application of his group multiplication time, we employ Corollary 5.2 and obtain Theorems 5.2 and 5.3.

Theorem 5.2. *Let* $\phi : Z_N \times Z_N \rightarrow Z_{2N-1}$ *be* $\phi(a, b) = a + b$. *Then there is a* (d, r) *circuit to compute* ϕ *in time*

$$\tau_\phi = 1 + \left\lceil log_r \left\lceil \frac{1}{\lfloor r/2 \rfloor} \left\lceil log_d \gamma(2N - 1) \right\rceil \right\rceil \right\rceil; \qquad r \geq 2, \quad d \geq 2.$$

Theorem 5.3. *Let* $\psi : \{1, 2, \cdots, N\} \times \{1, 2, \cdots, N\} \rightarrow \{1, 2, \cdots, N^2\}$ *be* $\psi(a, b) = ab$. *Then for any* $r \geq 2$ *and any* $d \geq 2$ *there is a* (d, r) *circuit to compute* ψ *in time*

$$\tau_\psi = 1 + \left\lceil log_r \left\lceil \frac{1}{\lfloor r/2 \rfloor} \left\lceil log_d \gamma(2 \lfloor log_2 N \rfloor - 1) \right\rceil \right\rceil \right\rceil.$$

In closing we note for reference that Winograd has lower bounded τ_ϕ and τ_ψ as follows:

Theorem 5.4 (Winograd [2]). *For any* $d \geq 2$ *and any* $r \geq 2$ *then any* (d, r) *circuit to compute* ϕ *requires time* τ_ϕ *where*

$$\tau_\phi \geq \left\lceil log_r 2 \left\lceil log_d \gamma\left(\left\lceil \frac{N}{2} \right\rceil\right) \right\rceil \right\rceil$$

and any (d, r) *circuit which computes* ψ *requires time*

$$\tau_\psi \geq \left\lceil log_r 2 \left\lceil log_d \gamma\left(\left\lceil \frac{\lfloor log_2 2N \rfloor}{2} \right\rceil\right) \right\rceil \right\rceil.$$

The proximity of the results of Theorem 5.2 and Theorem 5.3 to these lower bounds is indicated by the fact that $\gamma(4x) \leq 2 + \gamma(x)$.

Acknowledgment. The author gratefully acknowledges the assistance of his thesis advisor, Professor M. A. Arbib, and also thanks Dr. S. Winograd for several very helpful discussions.

REFERENCES

1. Winograd, S. On the time required to perform addition. *J. ACM 12*, 2 (April 1965), 277–285.
2. ——. On the time required to perform multiplication. *J. ACM 14*, 4 (Oct. 1967), 793–802.
3. Ofman, Yu. On the algorithmic complexity of discrete functions. *Dokl. Akad. Nauk SSSR 145*, 1 (1962), 48–51.
4. Hall, M., Jr. *The Theory of Groups*. Macmillan Co., New York, 1959.

Received May, 1968