ON THE COMPLEXITY OF MATRIX GROUP PROBLEMS I

László Babai*

Dept. Algebra
Eötvös University
Budapest, Hungary H-1088

Endre Szemerédi

Mathematical Institute of the
Hungarian Academy of Sciences
Budapest, Hungary H-1053

ABSTRACT

We build a theory of *black box groups*, and apply it to matrix groups over finite fields. Elements of a black box group are encoded by strings of uniform length and group operations are performed by an oracle. Subgroups are given by a list of generators. We prove that for such subgroups, *membership* and *divisor of the order* are in NP^B. (B is the *group box* oracle.) Under a plausible mathematical hypothesis on short presentations of finite simple groups, *nonmembership* and *exact order* will also be in NP^B and thus in $NP^B \cap coNP^B$. In another paper we shall prove without any unproven hypothesis that the order of a group and thus nonmembership can be certified in a statistical sense (Arthur vs. Merlin games) and therefore is in $NP^{B,A}$ for a random oracle A (with probability 1). This puts membership in matrix groups over finite fields in $NP \cap coNP^A$ for a random oracle A.

Full details will appear in COMBINATORICA.

0. INTRODUCTION.

0.1. A (finite) group may be given in many different ways. Natural questions such as membership, order, isomorphism will be of varying difficulty, depending on the representation. The least succinct of the commonly used representations is by Cayley table (multiplication table). In this case, membership in and order of subgroups generated by a given list of elements are easy. Isomorphism is subexponential but not known to be polynomial time decidable. On the other end of the scale are presentations (in terms of generators and relations). Classical results tell us that membership in a subgroup, order (even whether the order is equal to 1), and isomorphism are all undecidable.

Decidable but apparently very difficult questions arise if our group is given as the Galois group of an equation. Determining the order of this group is not known to be in PSPACE.

Determining the order of the automorphism group of a finite structure is polynomial time Turing-equivalent to graph isomorphism which is clearly in NP, unlikely to be NP-complete but not known to be in or near coNP either.

The class of group representations that has received the most attention in complexity theory lately is permutation groups, given by generators. Membership and order are polynomial time decidable. Isomorphism remains difficult. It is in PSPACE (in fact, in Σ_2^P). It is not known to be NP-hard but is clearly at least as difficult as isomorphism of groups given by Cayley tables.

0.2. An interesting class of groups, and the main focus of the present paper, is matrix groups over finite fields, given by generators. The problems here are clearly at least as hard as the corresponding problems for permutation groups, and quite likely substantially harder. Already for one by one matrices over the field of p elements, representing an element as a power of another is the discrete logarithm problem mod p. This observation appears to indicate that even for the simplest problems (membership, order), the best we may expect is putting them in $NP \cap coNP$.

0.3. We shall consider the following problems.

The *matrix group membership* problem is deciding the complexity of the class $\{(g,G): g \in G\}$.

*This work was done while visiting Dept. Math., Simon Fraser University, Burnaby, B.C., Canada. Currently visiting Dept. Computer Science, Univ. of Chicago, Chicago, IL 60637.

0272-5428/84/0000/0229$01.00 © 1984 IEEE

Here and throughout the paper, G is a group given by a list of generators. The dimension d and a reasonable representation (of length $O(\log q)$) of the field $GF(q)$ are part of the problem instance. It is understood, that $G \leq GL(d,q)$. So, strictly speaking, we consider the complexity of the class $\{(d,GF(q),g,G): g \in G \leq GL(d,q)\}$.

In a similar sense, *nonmembership* is the class $\{(g,G): g \notin G\}$ $(g \in GL(d,q) \geq G)$.

Lower bound on order means the class $\{(n,G): n \in Z, n \leq |G|\}$. We shall also consider *divisor of order:* $\{(n,G): n \in Z, n \mid |G|\}$.

Clearly, if the divisor problem is in NP then so is the lower bound. (To prove that $n \leq |G|$, just guess $m = |G|$ and verify $n \leq m \mid |G|$.)

Upper bound on order means $\{(n,G): |G| \leq n\}$. *Multiple of order* is $\{(n,G): |G| \mid n\}$. *Upper bound* reduces to *multiple* as *lower bound* to *divisor*.

Observe that *upper bound* is in coNP precisely if *lower bound* is in NP.

Exact order means $\{(n,G): |G| = n\}$. Clearly, the following are equivalent.

(a) *Exact order* is in NP.
(b) Both *upper* and *lower bound* are in NP.
(c) Both *upper* and *lower bound* are in coNP.
(d) *Exact order* is in coNP $\cap$ NP.
(e) Both *divisor* and *multiple* are in NP.

Also, if *exact order* is in NP then *membership* is in NP $\cap$ coNP. (Guess and verify the order of the group generated by g and G. If it is $|G|$ then $g \in G$, otherwise $g \notin G$.)

These observations remain valid relative to any oracle.

Isomorphism means $\{(G,H)$: G and H are isomorphic$\}$. (G and H are two matrix groups over possibly different finite fields.)

0.4. Our main results are the following.
Matrix group membership is in NP. (This is an immediate consequence of the Reachability Theorem 3.1, cf. Thm. 4.1.).
Isomorphism is in Σ_2^P (Cor. 4.9).
Divisor of order is in NP. (Theorems 9.1 and 10.1.)
Solvability, exact order of solvable groups are in NP (Cor. 5.18, Theorems 6.1 and 9.1).
Exact order is in NP^A for a random oracle A (with probability 1) (Sections 12, 13). Hence it is in $coNP^A$ for a random oracle A.

(Proofs of the results involving random oracles will appear elsewhere, [Ba 2].)

Assuming the truth of a plausible conjecture on short presentations of finite simple groups (11.1), it follows that *exact order* and thus *membership* are in NP $\cap$ coNP (Theorems 9.1, 10.1 and 11.4).

0.5. Black box groups. This is a common generalization of permutation groups and matrix groups where group elements are represented by strings and group operations are performed by an oracle. Proofs of our matrix group results become substantially more transparent in this context. Most significantly, we shall be able to handle factor groups of matrix groups as black box groups. This is the key technique in the proof of our main result, Theorem 9.1 (*lower bound* on order).

0.6. For lack of space we had to omit most proofs. Even the main result (Theorem 9.1) is no exception. We hope, however, that sufficient detail has been included to enable the reader to understand the new concepts and central ideas.

1. BLACK BOX GROUPS.

Let $S(b) = \{0,1\}^b$ denote the set of 0-1 strings of length b.

Definition 1.1. A group box is a seven-tuple

$$B = (b, c, inv, prod, id, G_B, f_B)$$

where b and c are positive integers (b is the code length, c is the witness exponent) and

$$inv : S(b) \to S(b)$$
$$prod: S(b) \times S(b) \to S(b)$$
$$id : S(b) \times S(b^c) \to \{YES, *\}$$

are functions; furthermore G_B is a finite group (*the group in the box*) and

$$f_B: S(b) \to G_B \cup \{*\}$$

is a map satisfying the following conditions.

Let $S_B = f_B^{-1}(G_B)$. We say that $x \in S_B$ is a name of $f_B(x)$.

(i) If $x \in S_B$ then $inv(x) \in S_B$ and

$$f_B(inv(x)) = (f_B(x))^{-1}.$$

(ii) If $x,y \in S_B$ then $prod(x,y) \in S_B$ and

$$f_B(prod(x,y)) = f_B(x)f_B(y) .$$

(iii) If $x \in S(b)$ and $f_B(x) \neq 1$ and $y \in S(b^c)$ then $id(x,y) = *$.

(iv) If $x \in S(b)$ and $f_B(x) = 1$ then there exists $y \in S(b^c)$ such that $id(x,y) = YES$.

We call such a y a witness of the name x of the identity.

Comments 1.2. Informally, the group box performs group operations on names (length b codewords) of elements of an unknown group. Several points in this definition require motivation.

The typical example we have in mind is a factor group G/N of a matrix group G . Elements of this group are encoded as matrices but the names are not unique and not every matrix is a name.

It would seem natural to make id a function $S(b) \to \{YES, *\}$, which simply recognizes the names of the identity. This, however, would not generalize to factor groups (our crucial tool, see Theorem 4.6). The witness of the name x of the identity in G/N must be a proof that x is a member of N . Conditions (iii) and (iv) reflect the spirit of nondeterminism in this paper. Note that the group box will not confirm $f_B(x) \neq 1$ without an exhaustive search of all possible witnesses. This corresponds to the fact that nonmembership verification is more difficult than membership. Indeed, we shall see that matrix group membership is in NP but we can't prove the same for nonmembership (cf. 0.4).

Definition 1.3. A black box group is a tuple $(B,x_1,\ldots,x_t)$ where B is a group box and $x_1,\ldots,x_t \in S_B$.

Comment 1.4. We also use the term *black box group* to mean the subgroup of G_B generated by $f_B(x_1),\ldots,f_B(x_t)$. The phrase G *is a given black box group* will refer to a tuple, but we shall say "$x \in G$" for some $x \in S(b)$ to mean that $f_B(x)$ belongs to the group generated by $f_B(x_1),\ldots,f_B(x_t)$. We shall also refer to G having properties such as solvability, etc. Most of the time we shall not use the symbols f_B, prod, etc. and will simply write xy in place of prod(x,y), etc. This will cause no confusion.

Comment 1.5. Groups will always be given by generators. The phrase *guess a group* G will mean guess generators for G . The set of names of the generators will be the INPUT, the length of which is the base of complexity estimates. Therefore, no input will be shorter than b bits.

Regarding the economy of such representation, cf. the remark after Cor. 4.2. The following are clear.

Proposition 1.6. The order of any black box group G of code length b is

$$|G| \leq 2^b . \square$$

Corollary 1.7. Any black box group of code length b can be generated by $\leq b$ elements and can thus be represented by an input of $\leq b^2$ bits. □

2. COMPUTATION ON BLACK BOX GROUPS. CERTIFICATES.

Comment 2.1. Our model of computation is a nondeterministic RAM (endowed with a guess tape) with an extra query tape where statements of the form INV(x), PROD(x,y), ID(x,y) can be entered. The group box currently interacting with the Turing machine will (magically and at no cost) print the corresponding answers.

Such algorithms, involving a group box as an oracle, will be referred to as group box algorithms.

Definition 2.2. Let P(x) be a relation (predicate) on the set of input strings x of a certain length. A verification of P is a nondeterministic polynomial time group box algorithm which accepts x if and only if P(x) holds. A certificate of P(x) is the record of such an accepting computation.

The length of the certificate is the running time of an accepting computation on input x .

Here, polynomial time means $0(|x|^{C(c)})$, where the exponent C(c) depends solely on the witness exponent c and not otherwise on the group box B .

Remark 2.3. Our definition of polynomial time could be formalized in the context of relativized algorithms by compounding infinitely many group boxes with the same bound c* on witness exponents c into a single oracle B(c*).

Remark 2.4. The phrases *there exists a certificate of* P or P *can be certified* are equivalent to the existence of a polynomial time verification procedure in the above sense.

Example 2.5. There exists a certificate of "$f_B(x) = 1$".

Proof. Here is the procedure.

Guess witness y

Check $id(x,y) = YES$.

The length of the certificate will be dominated by $|y| = b^c = |x|^c$. □

Corollary 2.6. There exists a certificate of "$|G| = 1$".

Proof. Take the conjunction of certificates of "$g_i = 1$" for all generators g_i of G . (Note that our input is $(x_1,\ldots,x_t)$ where $g_i = f_B(x_i)$ are the generators of G.) □

Remark 2.7. While the certifiability of the relations $P_1(x)$ = "x is the identity" and $P_2(G)$ = "$|G| = 1$" followed immediately from our definition, it is equally immediate that the negation of the P_i cannot be certified. Any proof of "$x \neq 1$" would require an exhaustive search of all possible witnesses for some x' . Thus, in order to obtain certificates of lower bounds on the order of a black box group G we need some extra device; see Section 7.

Remark 2.8. We shall frequently use the fact that primality certificates exist [Pr].

3. SHORT STRAIGHT LINE PROGRAMS IN GROUPS.

Throughout the paper, log will mean base 2 logarithms.

In this section we prove the fundamental result that, in a group of order n , every element can be generated from any set of generators in $(\log n)^c$ steps. This was conjectured by Lipton et al. [LSZ].

We begin with definitions.

Let us fix a set S of generators of the group G . We call a sequence $g_1,\ldots,g_t$ of elements of G a straight-line program of length t from S if each g_i is either a member of S or an element of the form g_j^{-1} or g_jg_k for some $j,k < i$ $(i = 1,\ldots,t)$. The members of the sequence are said to be generated by the s.l. program. The straight-line cost of an element $x \in G$ is the length of the shortest s.l. program generating x (from the given set S).

Reachability Theorem 3.1. Given a group G of order n and a set S of generators, the straight-line cost of each element of G is $\leq (1 + \log n)^2$.

Proof. For a subset H of G , let us define $c(H)$, the straight-line cost of H as the length of the shortest s.l. program $g_1,\ldots,g_t$ such that $H \subseteq \{g_1,\ldots,g_t\}$.

We shall inductively define a sequence $z_1,z_2,\ldots,z_s$ of elements of G (not a straight-line program) as follows. The length s of this sequence will also be defined in the process.

Let $K(i) = \{z_1^{\varepsilon_1}\ldots z_i^{\varepsilon_i} : \varepsilon_j = 0,1\}$ be the "cube" based on the initial segment $z_1,\ldots,z_i$, and let $c(i)$ denote the straight-line cost of the set $\{z_1,\ldots,z_i\}$. ($K(0) = \{1\}$ and $c(0) = 0$.)

If $K(i)^{-1}K(i) = G$ we set $s = i$ and stop.

Else, we define z_{i+1} to be an element of $G - K(i)^{-1}K(i)$ minimizing the cost increase $c(i+1) - c(i)$.

Claim 1. If $i < s$ then $|K(i+1)| = 2|K(i)|$. □

Corollary 1. $s \leq \log n$. □

Claim 2. $c(i+1) - c(i) \leq 2i+1$. □

Corollary 2. $c(i) \leq i^2$. □

Now the conclusion is immediate. □

4. CERTIFICATES OF MEMBERSHIP, SUBGROUPS. ECONOMICAL SETS OF GENERATORS. NORMALITY, FACTOR GROUPS. ISOMORPHISM.

Let G be a black box group. An immediate consequence of the Reachability Theorem is the existence of membership certificates for subgroups of G .

Theorem 4.1. Given elements $g_0,\ldots,g_m$ of G , there exists a certificate of the relation "g_0 is generated by $g_1,\ldots,g_m$". □

Corollary 4.2. Let the subgroups H and K of G be given by generators. Then there exist certificates of the relations $H \le K$ and $H = K$. □

In particular, we are able to remove redundant generators.

Corollary 4.3. Given a subgroup $H \le G$ (by generators), there exists a set of $t \le \log |H|$ elements $g_1,\ldots,g_t$ of G and certificate "$g_1,\ldots,g_t$ generate H". □

Normal subgroups and normal closure are the fundamental tools of group theory we have to handle next.

Theorem 4.4. Given $N \le G$, there exists a certificate of the relation "N is normal is G". □

Theorem 4.5. Given $g_1,\ldots,g_r \in G$ and $N \le H \le G$, there exists a certificate of the relation "N is the normal closure of $g_1,\ldots,g_r$ in H". □

A crucial tool in our arguments will be the simulation of factor groups by the same group box.

Theorem 4.6. Given $N \lhd G$, the factor group G/N can be viewed as a black box group with the same code length as for G. The group box for G/N can be simulated in deterministic polynomial time by the group box for G and a Turing machine (or RAM).

Comment 4.7. As in Def. 2.2., polynomial time means $O(|x|^{c(c)})$ where c is the original witness exponent and x is the input. In particular, the new witness exponent c' must depend on c only. In fact, we shall have $c' = c+3$.

Proof of 4.6. Let $G \le G_B$ where $B = (b, c, inv, prod, id, G_B, f_B)$. Let us define a new group box $B' = (b, c', inv, prod, id', G_{B'}, f_{B'})$.

Here,

$$G_{B'} = G/N ,$$

$$f_{B'}(x) = \begin{cases} f_B(x)N & \text{if } f_B(x) \in G \\ N & \text{if } f_B(x) \notin G , \end{cases}$$

$$c' = c+3 ,$$

$id'(x,y) = YES$ if y is a certificate of $f_B(x) \in N$, i.e.,

(i) $y \in S(b^{c'})$.

(ii) y is a reasonably encoded form of a sequence $x_1,\ldots,x_t,y_0$, where $x_i \in S(b)$, $y_0 \in S(b^c)$.

(iii) $x_1,\ldots,x_t$ is a straight line program from the given names of generators of N, i.e., each x_i is either such a name or $x_i = prod(s_j,x_k)$ or $x_i = inv(x_j)$ for some $j,k < i$.

(iv) y_0 is a witness to the equality $f_B(x_t) = f_B(x)$, i.e., $id(x^{-1}x_t, y_0) = YES$.

Observe that in fact y could be chosen to satisfy $|y| \le |y_0| + O(\log^2 |N|) \le b^c + O(b^2) < b^{c'}$. We then pad it out to obtain length $b^{c'}$.

Note that b, inv and $prod$ are the same as for B .

These definitions provide a group box with G/N the group in the box. To make G/N a black box group, we have to name its generators; these names will be the same as the names of the generators of G .

The simulation of B' using B is easy. The operations inv and prod have not changed, and the verification of (i) - (iv) in the definition of id' is fast. □

Suppose now that we have the extra ability of non-identity verification, i.e. an additional $nonid(x,y)$ function in def. 1.1.

Proposition 4.8. Isomorphism of black box groups with nonidentity verification is in Σ_2^{P,B_1,B_2}, i.e., solvable in polynomial time by two-step alternating machines with an existential move followed by a universal one. (B_1, B_2 refer to the two group-box oracles.)

Proof. Let $x_1,\ldots,x_t$ and $y_1,\ldots,y_t$ be (the names of) the generators of the black box groups G and H, resp. The existential player guesses an isomorphism f by guessing and certifying generators $u_1,\ldots,u_s$ of H and declaring that an isomorphism $f: G \to H$ sends x_i to u_i .

The universal player disproves this claim by guessing a short s.l. program in $G \times H$ which from the (x_i,u_i) generates an element of the form $(g,1)$ or $(1,h)$, where $g,h \neq 1$. □

Corollary 4.9. Isomorphism of matrix groups over finite fields is in Σ_2^P . Consequently, the same holds for permutation groups. □

5. SOLVABILITY, NILPOTENCE, p-GROUPS.

Our general references in group theory are [Ha] and [Hu]. We recall some definitions crucial for Section 9.

The commutator of $g,h \in G$ is the element $[g,h] = g^{-1}h^{-1}gh$.

Definition 5.1. Let $K,L \leq G$. The mutual commutator subgroup $[K,L]$ is the group generated by $\{[g,h]: g \in K, h \in L\}$.

The commutator subgroup K' of K is $K' = [K,K]$.

Definition 5.2. The commutator series of a group G is the subgroup chain $G^{(0)} = G$, $G^{(i+1)} = (G^{(i)})'$. The lower central series of G is the subgroup chain $K^0(G) = G$, $K^{i+1}(G) = [G,K^i(G)]$.

Definition 5.3. G is solvable if $G^{(m)} = 1$ for some m. We call G nilpotent of class m if $K^m(G) = 1$.

Definition 5.4. The center $Z(G)$ of G is

$$Z(G) = \{x \in G: xy = yx \text{ for each } y \in G\}.$$

Fact 5.5. G is nilpotent of class 2 precisely if

$$G' \leq Z(G).$$

Definition 5.6. For p a prime, G is a p-group if the order of G is a power of p.

Definition 5.7. G is an elementary abelian p-group if G is abelian and the nonidentity elements of G have order p.

Remark 5.8. Such groups can be viewed as vector spaces over $GF(p)$. We shall thus use the term linear independence for members of an elementary abelian group.

Definition 5.9. A subgroup $H \leq G$ is characteristic (H char G) if H is invariant under all automorphisms of G.

Fact 5.10. Characteristic subgroups are normal.

Fact 5.11. If K,L are characteristic subgroups of G then so is $[K,L]$. Consequently, all members of the commutator and lower central series are characteristic.

Fact 5.12. Abelian groups and p-groups are nilpotent.

Fact 5.13. Every nilpotent group is solvable.

Fact 5.14. The Sylow subgroups of a nilpotent group are normal.

Corollary 5.15. If p is the only prime divisor of the order of every generator of a nilpotent group G then G is a p-group.

Fact 5.16. Let $K,L \leq G$ and let $x_1,\ldots,x_i$ and $y_1,\ldots,y_t$ be generators of K and L, resp. If K and L are normal in the subgroup they generate, then $[K,L]$ is the normal closure of $\{[x_i,y_j]: 1 \leq i \leq s, \ 1 \leq j \leq t\}$ in this subgroup.

We now turn to the question of certificates of group properties for black box groups. Let G be a black box group.

Lemma 5.17. For $K,L,M \leq G$, if K and L are normal in the subgroup they generate then there exists a certificate for the relation

$$M = [K,L].$$

Proof. Combine 5.16 and Theorem 4.5. □

Corollary 5.18. There exist certificates of solvability and of nilpotence of given class. □

Remark 5.19. Certificates of being abelian, elementary abelian, cyclic trivially exist.

Proposition 5.20. There exists a certificate of the property "G is a p-group".

Proof. First we have to certify that p is a prime. Then we construct a certificate of the nilpotence of G (5.18). Finally, we check that $g^{p^k} = 1$ for some k and for each generator g of G. □

6. ORDER OF SOLVABLE GROUPS: UPPER BOUND CERTIFICATE.

Let G be a black box group and n an integer.

Theorem 6.1. If G is solvable then there exists a certificate of the relation "*the order of* G *divides* n".

The idea of the proof is to guess a composition series, although at this moment we are unable to verify that there are no repeated groups in the sequence guessed.

PROCEDURE 6.2. Guess an integer m, elements $g_1,\ldots,g_m$, subgroups $G_0,G_1,\ldots,G_m$ of G and

positive integers $k_1,\ldots,k_m$ such that for $i = 1,\ldots,m$

(1) $G_0 = G$

(2) $G_m = 1$

(3) $g_i \in G_{i-1}$

(4) $G_i \lhd G_{i-1}$

(5) G_{i-1} is generated by g_i and G_i

(6) $g_i^{k_i} \in G_i$

(7) $\prod_{i=1}^{m} k_i$ divides n.

Certify the validity of (1) through (7). END.

The following two results imply Theorem 6.1.

Lemma 6.3. The output of PROCEDURE 6.2 (guesses and certificates) forms a certificate of the relation "G *is solvable and* $|G|$ *divides* n". □

Lemma 6.4. Such a certificate always exists. □

Corollary 6.5. If G is solvable, $N \lhd G$ and a certificate of the order of G is available, then certificates of the orders of N and G/N can be constructed. □

7. LOWER BOUND: THE NECESSITY OF THE INDEPENDENCE TESTER.

We wish to construct a certificate of the relation "$|G| \geq n$".

It is clear that we shall not be able to do this for black box groups without any additional gadget. In fact, even proving $|G| \neq 1$ is impossible without an exhaustive search of all possible witnesses of the possibility $g = 1$ for some product g of generators of G. But even if the group box comes with an identity tester attached, we run into trouble in the next simplest case: elementary abelian groups. As we shall see presently, it is impossible to certify linear independence of generators without a prohibitive number of group operations and queries to the identity tester.

Let G be a black box group. Assume G is an elementary abelian p-group. Assume further that for any set of at most k elements of G an oracle tells whether or not the k-tuple is independent. We call such an oracle a k-independence tester. Observe that a 1-independence tester is precisely an oracle confirming when an element is not the identity.

Theorem 7.1. If G is an elementary abelian p-group with a k-independence tester, then a certificate of the independence of $m > k$ elements must involve more than p^{m-k} independence tests. □

The case $k = 1$ shows the necessity of an independence tester even if an identiy tester is available and even for $G = Z_p^2$, since p may be exponentially large. The result also shows that no bound on k can be imposed, even if p is small.

In our spirit of nondeterminism, we define the independence tester to be used in the subsequent sections as follows.

Definition 7.2. A group box with independence tester is a triple (B, ind, c') where

$B = (b, c, inv, prod, id, G_B, f_B)$

is a group box, c' is a positive integer and ind is a function

$ind: Z \times 2^{S(b)} \times S(b^{c'}) \to \{YES, *\}$

such that

(1) if p is a prime $< 2^b$, $x_1,\ldots,x_t \in S_B$, $t \leq b$ and $f_B(x_1),\ldots,f_B(x_t)$ generate an elementary abelian p-subgroup $H \leq G_B$, then

(i) if $|H| = p^t$ then there exists a witness $y \in S(b^{c'})$ such that

$$ind(p,\{x_1,\ldots,x_t\},y) = YES$$

(ii) if $|H| < p^t$ then for each $y \in S(b^{c'})$,

$$ind(p,\{x_1,\ldots,x_t\},y) = *.$$

Comment 7.3. In the case any of the conditions (1) is violated, the output may be either YES or * and will carry no information. In particular, a YES output is not a primality certificate for p or a certificate of H being an elementary abelian p-group. These conditions have to be certified separately.

Comment 7.4. For computations in a black box group with independence tester, the only change we have to make in Comment 2.1 is that one more type of oracle query (IND(x)) is permitted. A polynomial time computation on input x will now have length $\leq |x|^{C(c,c')}$ (as opposed to $\leq |x|^{C(c)}$ in Def. 2.2).

8. CERTIFICATE OF ORDER FOR ABELIAN p-GROUPS.

We prove an auxiliary result which is a particular case of Cor. 9.2. We shall use it in the next section.

Theorem 8.1. Let G be a black box group with an independence tester. Assume G is an abelian p-group. Then there exists a certificate for the relation "$|G| = n$".

Remark 8.2. The independence tester will be used only once, for a basis of $soc(G)$, the socle of G, consisting of all elements of order p together with the identity (an elementary abelian group).

PROCEDURE 8.2. Guess integers $m, k_1, \ldots, k_m$ and elements $g_1, \ldots, g_m$ of G such that

(1) $g_1, \ldots, g_m$ generate G

(2) $g_i^{p^{k_i}} = 1 \quad (i = 1, \ldots, m)$

(3) $g_i^{p^{k_i - 1}}$ are linearly independent for $i = 1, \ldots, m$

(4) $n = \prod_{i=1}^{m} p^{k_i}$.

Certify the validity of (1) to (4). END.

The following two results imply 8.1.

Lemma 8.3. The output of PROCEDURE 8.2 (guesses and certificates) forms a certificate of the relation "$|G| = n$". □

Lemma 8.4. Such a certificate always exists. □

9. ORDER OF GROUPS: LOWER BOUND CERTIFICATES.

In this section, we present our main result.

Let G be a black box group with independence tester and let n be a positive integer.

Theorem 9.1. There exists a certificate for the relation "n *divides the order of* G".

By Theorem 6.1, we immediately conclude:

Corollary 9.2. If G has order n and is solvable then the relation "$n = |G|$" can be certified.

For extensions of this corollary, see Section 11.

Theorem 9.1 is an immediate consequence of the following result. Let p be a positive integer.

Lemma 9.3. There exists a certificate for the relation "p *is prime and* G *is a* p*-group of order* n".

To derive Theorem 9.1 from this lemma, we guess the prime factorization $n = \prod_{i=1}^{s} p_i^{\alpha_i}$, certify the primality of the p_i, guess p_i-subgroups $P_i \leq G$ such that $|P_i| = p_i^{\alpha_i}$, and use Lemma 9.3 to certify the order of each P_i $(i = 1, \ldots, s)$. □

In the proof of the Lemma we shall heavily rely on the nilpotence of p-groups [Ha, Thm. 10.3.4] (cf. Section 5).

We shall use the following well-known fact.

Proposition 9.4. If G is a nilpotent group of class 2 (i.e., $G' \leq Z(G)$) then for any $g \in G$, the g-commutator map f_g defined by $f_g(x) = [x,g]$ $(x \in G)$ is a homomorphism of G to G'. □

Another easy fact is that if G is nilpotent and H, K are normal subgroups of G then $[H,K]$ is a proper subgroup of H unless $|H| = 1$. (cf. [Hu, p. 262, Satz III.2.6.].)

We next describe the construction of a certificate for the order of a p-group G. The input is (G,n,p). Of course, first we certify the primality of p and the fact that G is a p-group.

PROCEDURE 9.5. Guess positive integers m, r_i, $u(i)$, $v(i)$, $w(i)$ and subgroups G_i and H_i of G for $i = 0, \ldots, m$ such that for all sensible values of i,

(1) the G_i and H_i are normal in G

(2) $G_{i+1} \leq G_i \leq H_{i+1} \leq H_i$

(3) $G_0 = H_0 = H_1 = G$

(4) $G_m = 1$

(5) $G_{i+1} = [H_i, G_i]$

(6) $H_{i+1}/G_{i+1} \leq Z(H_i/G_{i+1})$

(7) r_i is the number of generators employed in the guess to represent H_i

(8) $|H_i/G_i| \leq u(i)$

(9) $|G_{i-1}/G_i| \leq w(i)$

(10) $|H_m| = u(m)$

(11) $v(i)u(i+1) = u(i)w(i+1)$

(12) $|Im\varphi_i| = v(i)$, where

$\varphi_i: H_i/G_{i+1} \to ((H_i/G_{i+1})')^{r_i}$

is defined by

$\varphi_i(x) = ([x,g_1],\ldots,[x,g_{r_i}])$ $(x \in H_i/G_{i+1})$

where $g_1,\ldots,g_{r_i}$ are the generators of H_i/G_{i+1} corresponding to the r_i generators of H_i.

(13) $n = \prod_{i=1}^{m} w(i)$

(14) $m, r_i \le \log n$,

$u(i), v(i), w(i) \le n$, and

all groups guessed are represented by at most log n generators.

Certify the validity of (1) through (14). END.

The following two results imply Lemma 9.3.

Lemma 9.6. The output of PROCEDURE 9.5 (guesses of certificates) forms a certificate of the relation "$|G| = n$".

Lemma 9.7. This certificate always exists.

For lack of space, we have to omit the (long) proof of these results. We remark that if (1) through (14) hold then equality holds in (6), (8) and (9) and the subgroups G_i, H_i are uniquely determined characteristic subgroups of G. The group H_m is elementary abelian. The verification of (10) is the only place in the procedure where the independence tester is used.

10. INDEPENDENCE CERTIFICATES FOR MATRIX GROUPS.

In order to apply the results of the preceding sections to matrix groups over finite fields, we have to construct independence certificates for bases of elementary abelian subgroups of matrix groups. Of course, these certificates make no reference to any group box: their input is a set of matrices.

Theorem 10.1. Let G be an elementary abelian r-subgroup of order n of GL(d,q). Then there exists a certificate of the relation "$|G| = n$".

Remark 10.2. This result clearly suffices for the implementation of the independence tester for GL(d,q). Given $g_1,\ldots,g_m$, generators of the elementary abelian r-group $G \le GL(d,q)$, we guess n (the order of G), construct a certificate of "$|G| = n$" (this is the witness), and determine if $n = r^m$.

Remark 10.3. We have to make a comment on how to represent finite fields. Let F be a field of order q and K a field of order q^r. Assume we have a representation (by strings of length $O(\log q)$) of F. (This is certainly the case if q is prime.) Now in order to represent K we only need to guess an irreducible polynomial f of degree r over F. Irreducibility test over finite fields is deterministic polynomial time [Be], cf. [Ra].

Proof of 10.1. Let $q = p^s$ where p is a prime. We have to distinguish two cases.

Case A. $r = p$.

First of all, $M_d(q)$, the d by d matrix algebra can be written as a tensor product over GF(p): $M_d(q) = GF(q) \otimes_{GF(p)} M_d(p)$. This gives us an embedding

$$GL(d,q) \le GL(ds,p).$$

(To make this effective, we need an explicit representation of GF(q) as a subalgebra of $M_s(p)$, which immediately follows from the usual representation of GF(q) as a factor algebra GF(p)[x].)

Henceforth we may thus assume $s = 1$, i.e., $q = p$.

Let P be the group of upper triangular matrices with all diagonal entries equal to 1. This is the Sylow p-subgroup of GL(d,p). Hence, by Sylow's theorem, $x^{-1}Gx \le P$ for some $x \in GL(d,p)$. First we guess x and verify $x^{-1}g_i x \in P$ for each generator g_i of G. Henceforth we may assume $G \le P$.

P has order p^m where $m = d(d-1)/2$.

Let us sort the set of $m = d(d-1)/2$ ordered pairs $\{(i,j) : 1 \le i < j \le d\}$ lexicographically. Let $f(k) = (i_k, j_k)$ denote the k^{th} member of this sequence $(1 \le k \le m)$.

For a matrix $1 \ne g = (a_{ij}) \in P$, let

$\mu(g) = \min\{k: a_{f(k)} \ne 0\}$.

We set $\mu(1) = m + 1$.

Claim. $|G| = p^t$ if and only if G has t generators $g_1,\ldots,g_t$ such that $\mu(g_1) < \mu(g_2) < \ldots < \mu(g_t)$. □

A set of generators described in the Claim is

a certificate for "$|G| = p^t$".

This completes the proof in Case A.

Case B. $r \neq p$.

In this case, rather than reducing the field we extend it to $GF(q^e)$ where e is the smallest exponent such that $r | q^e - 1$. (Clearly $e \leq d$ because $r | |GL(d,q)|$.) Thus we may assume $e=1$. This implies that $GF(q)$ contains the r^{th} roots of unity.

Now, by standard elementary arguments of representation theory (Maschke's theorem) [Ha, 16.3.2] it follows that for some $x \in GL(d,q)$, we have $x^{-1}Gx \leq D$ where D is the group of diagonal matrices with only r^{th} roots of unity in the diagonal. D is isomorphic to Z_r^d. Hence, having guessed x, our problem reduces to linear independence over $GF(r)$. Note that this reduction requires solving the discrete logarithm problem in $GF(q)$ by guessing and verifying the exponents. □

11. CERTIFICATE OF UPPER BOUND? THE GROUP PRESENTATION CONJECTURE.

In Section 6 we have established a certificate of the relation $|G| | n$ for solvable groups.

The following conjecture would enable us to generalize the argument to arbitrary groups.

Conjecture 11.1. Every finite simple group of order n has a presentation of length $\leq (\log n)^c$.

By a presentation we mean a definition in terms of generators and relations. The length of a presentation is the total number of characters required to write down all relations. (Although it does not matter, we may agree that exponents are written in binary.)

Remark 11.2. There is plenty of evidence in favor of the conjecture.

It holds for cyclic and alternating groups. Sporadic groups don't count. For groups of Lie type, $X(d,q)$ say (d by d matrices over $GF(q)$), $n < q^{d^2}$ and so the requirement is to have a presentation of length $\leq (d \log q)^c$. Steinberg's presentations ([St], cf. [Ca, p.190]), have length $(dq)^c$, proving the conjecture for $q < d^c$. (c denotes a different constant in each formula.)

The conjecture is known to hold for $PSL(2,p)$ (p prime) [BM], an important building block in most simple groups of Lie-type. The strongest evidence comes from the work of C.W. Curtis [Cu], whose results imply that the conjecture would follow from its restriction to small dimension. For instance, if 11.1 holds for $PSL(2,q)$ and $PSL(3,q)$ then it holds for $PSL(d,q)$.

Remark 11.3. We actually need slightly more than what 11.1 says. The presentations not only must exist but have to be verifiable, i.e., a certificate has to guarantee the standard name of the corresponding group. This is less than requiring general explicit formulas, which do, however, exist in all known cases.

Theorem 11.4. Suppose that every composition factor of a black box group G is isomorphic to a known simple group with a verifiable presentation of length $\leq (\log n)^c$. Then there exists a certificate of the relation $|G| | n$.

Proof. As in the proof of Theorem 6.1, we guess a composition series $G = G_0 \triangleright \ldots \triangleright G_m = 1$. We guess generators of G_{i-1}/G_i corresponding to the generators involved in the short presentation of the known simple group S_i isomorphic to G_{i-1}/G_i. We verify that these relations hold for G_{i-1}/G_i. The implication is that either $G_{i-1} = G_i$ or $G_{i-1}/G_i \cong S_i$. Consequently we have a certificate of $|G| | n$ where $n = \prod_{i=1}^{m} |S_i|$ is the true order of G. □

Remark 11.5. We mention, as a curiosity, that all composition factors of the automorphism group of a planar graph are cyclic or alternating [Ba 1]. Hence, if such a group is our black box group, an upper bound on its order can be certified.

Remark 11.6. If the hypothesis of 11.4 holds and the group box is complete with independence tester, then (by 9.1) the exact order of G is certifiable.

12. ARTHUR VS. MERLIN GAMES: A SHORT HIERARCHY.

Merlin tries to convince the intelligent but impatient King Arthur that an input string x belongs to the language L.

If $L \in NP$, Merlin just presents a certificate (of polynomial length).

Even if L is not known to belong to NP, Merlin may have a way of convincing Arthur provided Arthur accepts statistical evidence. Suppose there exists a combinatorial game, depending on x, between Arthur and Merlin such that

(i) Arthur's moves are random (just rolls the dice, does not think);

(ii) if $x \in L$ then Merlin has a strategy which gives him at least 99% chance of beating Arthur;

(iii) if $x \notin L$ then Merlin has less than 1% chance of winning, no matter how cleverly he plays.

Assume in addition that each move takes at most $|x|^c$ time and the game must terminate in $|x|^{c'}$ moves.

Let us call the class of languages, recognizable by such games, $AM(\underline{P})$ (P for polynomial number of moves). Let us write $AM(k)$ if the number of moves is restricted to k and Arthur moves first; and $MA(k)$ if there are at most k moves and Merlin moves first. Finally, let us write $AM = AM(2)$ and $MA = MA(2)$.

Clearly, $MA(1) = NP$ and $AM(1) = BPP$ [Gi]. Our games are like Papadimitriou's "Games against Nature" [Pa], with the very significant difference that the winning probabilities must be bounded away from 1/2. This is what makes such a game a "practical" way for Merlin to convince Arthur that $x \in L$.

One can prove that the hierarchy obtained for increasing k collapses [Ba 2]. For any constant $k \geq 2$ we have $NP \cup BPP \subseteq MA \subseteq AM = AM(k) = MA(k+1) \subseteq AM(P) \subseteq PSPACE$.

(The inclusions seem more likely to be proper.)

It is also easy to prove that for a random oracle A,

$$AM \subseteq NP^A$$

with probability 1.

13. STATISTICAL VERIFICATION OF "EXACT ORDER".

There exists a 3-move game (Merlin-Arthur-Merlin) to show that "exact order" is in MA(3) and consequently (Sect. 12) in AM and therefore in NP^A for almost every oracle A. The proof is elementary. It is based on the following.

Theorem 13.1. [BE]. Let G be a group of order n and $t = \lfloor \log n + \log \ell n\, n + 3 \rfloor$. Then there exist elements $x_1, \ldots, x_t$ of G such that every member of G occurs among the 2^t subproducts $x_1^{\varepsilon_1} \ldots x_t^{\varepsilon_t}$ where $\varepsilon_i = 0,1$. □

14. OPEN PROBLEMS.

14.1. Prove that *matrix group membership* is at least as difficult as *discrete log* or some other difficult number theoretic problem.

14.2. Shall we expect that *membership* is not harder than, say, *factoring integers*?

14.3. Prove something better than Σ_2^P for *isomorphism*. (AM is a candidate, cf. Sections 12, 13.) This problem seems to be open even for permutation groups.

14.4. It is clear [Pa] (cf. Sect. 12) that $AM \subseteq AM(P) \subseteq PSPACE$. How does AM compare with members of the polynomial time hierarchy? Give evidence that $AM \neq coNP$. Could $AM \subseteq \Sigma_2^P$ hold?

14.5. Let G be a matrix p-group. Find a certificate of the center of G. (For permutation groups - not necessarily p-groups - finding the center is in P [Lu 2], cf. [Ho].)

14.6. Find a certificate of the intersection of two p-subgroups of a matrix group. (For permutation p-groups, finding the intersection is in P [Lu 1].)

14.7. Find a certificate of simplicity. (For permutation groups, simplicity can be decided in polynomial time, [Lu 3], cf. [BKL].)

14.8. There are many group-theoretic problems solvable in polynomial time for permutation groups. (Cf. 14.5 - 14.7. Further examples: membership, normal closure, solvability [FHL], finding elements of order p and Sylow subgroups [Ka], [KT] (cf. [BKL]), finding composition factors [Lu 3].) Can any of these be done in polynomial (sub-exponential) time for matrix groups? Positive results are available for 2 by 2 matrix groups [FM].

REFERENCES

[Ba 1] L. Babai, Automorphism groups of planar graphs II, in: Infinite and Finite Sets, Proc. Conf. Keszthely 1973 (A. Hajnal et al. eds.), North-Holland 1975, pp. 29-84.

[Ba 2] L. Babai, Arthur vs. Merlin games: a short hierarchy, in preparation.

[BE] L. Babai and P. Erdős, Representation of group elements as short products, in: Theory and Practice of Combinatorics (A. Rosa et al., eds.), Annals of Discr. Math. 12 (1982), pp. 27-30.

[BKL] L. Babai, W.M. Kantor and E.M. Luks, Computational complexity and the classification of finite simple groups, in: Proc. 24th IEEE Symp. Found. Comp. Sci., Tucson, Ariz. 1983, pp. 162-171.

[BL] L. Babai and E.M. Luks, Canonical labeling of graphs, in: Proc. 15th ACM Symp. Thy. Computing, Boston 1983, pp. 171-183.

[BM] H. Behr and J.L. Mennicke, A presentation of the groups PSL(2,p), Canad. J. Math. 20 (1968), 1432-1438.

[Be] E. R. Berlekamp, Factoring polynomials over large finite fields, Math. Comput. 24 (1970), 713-735.

[Ca] R. Carter, Simple groups of Lie type, Wiley-Interscience, N.Y., 1972.

[Cu] C.W. Curtis, Central extensions of groups of Lie type, J. Reine Angew. Math. 220 (1965), 174-185.

[FM] Faith Fich and G.L. Miller, private communication, 1982.

[FHL] M.L. Furst, J. Hopcroft and E.M. Luks, Polynomial-time algorithms for permutation groups, in: Proc. 21st IEEE Symp. Found. Comp. Sci., Syracuse, N.Y., 1980, pp. 36-41.

[Go] D. Gorenstein, Finite Simple Groups: An Introduction to their Classification, Plenum, N.Y., 1982.

[Ha] M. Hall, Jr., The Theory of Groups, MacMillan, N.Y., 1959.

[Ho] C.M. Hoffmann, Group Theoretic Algorithms and Graph Isomorphism, Lecture Notes in Comp. Sci. 136, Springer, N.Y. 1982.

[Hu] B. Huppert, Endliche Gruppen I, Springer, Berlin 1967.

[Jo] D.S. Johnson, The NP-completeness column: an ongoing guide, J. Algorithms, September 1984.

[Ka] W.M. Kantor, Polynomial time algorithms for finding elements of prime order and Sylow subgroups, to appear.

[KT] W.M. Kantor and D.E. Taylor, Polynomial-time versions of Sylow's theorem, to appear.

[LM] Susan Landau and G.L. Miller, Solvability by radicals is in polynomial time, in: Proc. 15th ACM Symp. on Theory of Computing, Boston 1983, pp. 140-151.

[LSZ] R.J. Lipton, L. Snyder and Y. Zalcstein, The complexity of word and isomorphism problems for finite groups. (Preliminary Report) in: Proc. 10th Conf. on Info. Sci. and Systems, Johns Hopkins Univ., Baltimore 1976, pp. 33-35.

[Lu 1] E.M. Luks, Isomorphism of graphs of bounded valence can be tested in polynomial time, J. Comp. Syst. Sci., 25 (1982), 42-65.

[Lu 2] E.M. Luks, The complexity of permutation group problems, 1980 (unpublished).

[Lu 3] E.M. Luks, Testing simplicity of permutation groups, in preparation.

[Mi] K.A. Mihailova, The occurrence problem for direct products of groups (Russian), Dokl. Akad. Nauk SSSR 119 (1958), 1103-1105 and Mat. Sb. (N.S.) 70(112)(1966), 241-251.

[Pa] C.H. Papodimitriou, Games against Nature, in: Proc. 24th IEEE Symp. Found. Comp. Sci., Tucson, Ariz., 1983, pp. 446-450.

[Pr] V.R. Pratt, Every prime has a succinct certificate, SIAM J. Computing 4 (1975), 214-220.

[Ra] M.O. Rabin, Probabilistic algorithms in finite fields, SIAM J. Comp. 9 (1980), 273-280.

[Sim] C.C. Sims, Some group theoretic algorithms, in: Lect. Notes in Math. 697, Springer, N.Y., 1978, pp. 108-124.

[Sin] A. Sinkov, The number of abstract definitions of LF(2,p) as a quotient group of (2,3,n), J. of Algebra 12 (1969), 525-532.

[St] R. Steinberg, Générateurs, relations et revêtements de groupes algèbriques, in: Colloque sur la théorie des groupes algèbriques, C.B.R.M., Brussels 1962, pp. 113-127.