MATHEMATICS OF COMPUTATION
VOLUME 55, NUMBER 192
OCTOBER 1990, PAGES 705-722

COMPUTING IRREDUCIBLE REPRESENTATIONS OF FINITE GROUPS

LÁSZLÓ BABAI AND LAJOS RÓNYAI

ABSTRACT. We consider the bit-complexity of the problem stated in the title. Exact computations in algebraic number fields are performed symbolically. We present a polynomial-time algorithm to find a complete set of nonequivalent irreducible representations over the field of complex numbers of a finite group given by its multiplication table. In particular, it follows that some representative of each equivalence class of irreducible representations admits a polynomial-size description.

We also consider the problem of decomposing a given representation $\mathscr{V}$ of the finite group G over an algebraic number field F into absolutely irreducible constituents. We are able to do this in deterministic polynomial time if $\mathscr{V}$ is given by the list of matrices $\{\mathscr{V}(g);\ g \in G\}$; and in randomized (Las Vegas) polynomial time under the more concise input $\{\mathscr{V}(g);\ g \in S\}$, where S is a set of generators of G.

1. INTRODUCTION

For the basic concepts of representation theory we refer to Curtis and Reiner [12]. An *algebraic number field* is a finite extension of the field $\mathbf{Q}$ of rational numbers.

We shall consider linear representations $\mathscr{V}: G \to GL(V)$ of a finite group G over an algebraic number field F. The dimension over F of the linear space V is the *degree* of $\mathscr{V}$. The *enveloping algebra* $\operatorname{env}(\mathscr{V}) \subseteq \operatorname{End}(\mathscr{V})$ is the linear closure of the set $\{\mathscr{V}(g): g \in G\}$. The space V of the representation can be viewed as a module over the group algebra $F[G]$. Constituents of $\mathscr{V}$ (restrictions to G-subspaces of V) correspond to submodules.

Recall that a representation is *absolutely irreducible* if it remains irreducible under any extension of F. Such representations correspond to irreducible representations over the complex field $\mathbf{C}$. A complete set of nonequivalent absolutely irreducible representations is a *dual object* to the group G. We consider the following two algorithmic problems.

Received May 17, 1989.

1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 68Q40; Secondary 16A64, 20F29.

The first author's research was partially supported by NSF Grant CCR 8710078; the research of both authors was partially supported by Hungarian National Foundation for Scientific Research Grant 1812.

Problem 1. Given a finite group G by its multiplication table, find its dual object, i.e., a complete set of nonequivalent irreducible representations of G over $\mathbf{C}$.

Problem 2. Given a representation $\mathscr{V}$ of the finite group G over $\mathbf{C}$, decompose $\mathscr{V}$ into irreducible components.

Regarding Problem 1, we should first note that *the required output is a finite object*, i.e., it is representable by a finite string of symbols. Indeed, there exists an algebraic number field F such that each equivalence class of irreducible representations of G has a representative over F. If $|F : \mathbf{Q}| = d$, then the elements of F can be represented by d-tuples of rational numbers.

In the case of Problem 2 we have to present the *input as a finite object.* This is accomplished by assuming that all matrix elements in the representation belong to an algebraic number field F. We also have to state in what form the input is given. One possibility is to list all the endomorphisms $\mathscr{V}(g)$ $(g \in G)$ (as matrices with respect to a given basis of V). We should note that a much more concise representation of $\mathscr{V}$ is obtained by selecting a set S of generators of G and listing the endomorphisms $\mathscr{V}(g)$ for $g \in S$ only. As customary, we measure algorithm efficiency by the maximum number of bit operations as a function of the size of the input. Thus, a polynomial-time solution with respect to a concise input is more difficult to achieve. We can only report a randomized solution under this condition (Theorem 1.3).

Our main results are polynomial-time solutions to Problems 1 and 2. Such a statement refers to the *size* of the input (the number of input bits), so we first have to clarify this concept.

The size of an integer is its number of digits. The size of a rational number p/q is $\text{size}(p) + \text{size}(q)$, where $\gcd(p, q) = 1$. The size of compound objects (polynomials, vectors, matrices) is the sum of the sizes of their components. If we have an algebraic number field $F = \mathbf{Q}(\gamma)$, given by the minimal polynomial $f \in \mathbf{Z}[x]$ of γ, $\deg(f) = n$, then an element $\alpha \in F$ can be represented uniquely as $\alpha = \sum_{i=0}^{n-1} a_i \gamma^i$, where $a_i \in \mathbf{Q}$. In this case the size of α is the sum of the sizes of the a_i plus the size of f.

Let, throughout the paper, ξ_e denote a primitive eth root of unity and $\mathbf{Q}_e = \mathbf{Q}(\xi_e)$ denote the eth *cyclotomic field*. The *exponent* of a group G is the smallest positive e such that $g^e = 1$ for every $g \in G$.

Theorem 1.1. *Given a finite group G by its multiplication table, one can find, in polynomial time, a complete set of nonequivalent complex irreducible representations of G. The matrix elements will belong to the cyclotomic field $\mathbf{Q}_e$, where e is the exponent of the group G.*

The fact that a dual object with matrix elements from $\mathbf{Q}_e$ exists was conjectured by Maschke and proved some 40 years later by R. Brauer. It was not evident, however, that a solution (whether over $\mathbf{Q}_e$ or not) admitting a short

description existed at all. The *existence* of a dual object of *polynomial size* is a *consequence of our algorithm.*

Theorem 1.2. *Given a representation $\mathscr{V}$ of the finite group G over the algebraic number field F by the list of matrices corresponding to each group element, one can decompose $\mathscr{V}$, in polynomial time, into complex irreducible constituents. The output will be given over the field $F\mathbf{Q}_e$ (the smallest field containing F and $\mathbf{Q}_e$). (Again, e stands for the exponent of G.)*

Our next result solves the same problem in the stronger sense that we start from the concise input described above. On the other hand, the result is weaker on two accounts: first, the output will be given over not necessarily abelian (or even Galois) extensions of F; second, the algorithm will be Las Vegas. (A Las Vegas algorithm uses randomization in the course of the computation. Depending on the random bits received, it either outputs a correct result, or reports failure; and the probability of failure is $\leq 1/2$. By running the algorithm t times, the failure probability is reduced to $\leq 2^{-t}$. As opposed to Monte Carlo algorithms, a Las Vegas algorithm never outputs erroneous results. A classical example of a polynomial-time Las Vegas algorithm is Berlekamp's algorithm to factor polynomials over finite fields [2].)

Theorem 1.3. *Let $S \subset G$ be a set of generators of the group G. Assume a complex representation $\mathscr{V}$ of G with matrix elements from an algebraic number field F is given by the list $\{\mathscr{V}(g);\ g \in S\}$ of matrices corresponding to the generators. Then $\mathscr{V}$ can be decomposed to complex irreducible constituents in Las Vegas polynomial time.*

We have to explain the output of this algorithm. Unlike in Theorem 1.2, it may not be possible to define the decomposition of the representation space V over a single, polynomial-size extension field. Instead, we shall construct a tree with an invariant subspace associated with every node and an algebraic number field associated with every internal node such that

(i) the root corresponds to V and F;
(ii) the children of an internal node represent a direct decomposition of their parent, described over the field associated with the parent;
(iii) the leaves correspond to irreducible constituents;
(iv) the tree has depth three.

Theorem 1.3 asserts that such a tree with the corresponding fields and subspaces can be constructed in polynomial time, with the implication that a polynomial-size output of the described format exists.

Theorem 1.3 will be an immediate consequence of Brauer's theorem and the following more general result on semisimple algebras.

Theorem 1.4. *Let A be a semisimple algebra over an algebraic number field F, and M an A-module. Assume that the center of each minimal ideal of A is a Galois extension of F. Then $M \otimes_F \mathbf{C}$ can be decomposed into a direct sum of irreducible $A \otimes_F \mathbf{C}$-submodules in Las Vegas polynomial time.*

The decomposition is understood to mean, as above, the construction of a tree of field extensions and submodules satisfying conditions (i) through (iv).

The problem of computing irreducible representations has been studied before the advent of complexity theory. Some special representations were constructed by C. Brott and J. Neubüser [6]. Dixon [17] considered representations computed approximately.

A dual object is the input to the Discrete Fourier Transform over G. Algorithmic aspects of this latter have been considered for nonabelian groups by Atkinson [1], Beth [4], Clausen [10, 11], Diaconis and Rockmore [15], and others. Applications to statistical analysis are described by Diaconis [13, 14]. These works presume the dual object to be given as part of their input, and as a measure of complexity, they use the number of arithmetic operations over the complex numbers.

The main difficulty that arises when the *bit-complexity* of algorithms for the decomposition of representations is to be rigorously analyzed is how to avoid an exponential blowup of the sizes of the objects created during the process.

This aspect of the problem appears to have been ignored in previous work on the subject. The natural approach to these problems requires repeatedly finding invariant subspaces as long as the space is reducible. There are two principal difficulties here. First, each split may require a field extension, eventually leading to extension fields of exponentially large degree. Second, even if the degree of the field was under control, each iteration may require solving a system of linear equations, thus increasing the size of the basis vectors by a factor proportional to the dimension of the space.

We shall prove Theorem 1.3 in §2 by a structured version of the "split and repeat" approach, relying on Brauer's quoted result. The proofs of Theorems 1.1 and 1.2 proceed along quite different lines (§§3–6) and make use of Brauer's result that the character ring is generated by characters induced from linear characters of certain "elementary" subgroups.

The characters of absolutely irreducible representations are the *irreducible characters* of G. A problem that precedes Problems 1 and 2, both logically and in importance, is to determine the irreducible characters.

Problem 0. Compute the irreducible characters of G.

We note that the values of a character χ of degree n of G can be written as the sum of n terms, each an eth root of unity:

$$\chi(g) = \sum_{i=1}^{n} \xi_e^{l_i}, \tag{1.1}$$

where the integers l_i depend on χ and $g \in G$. This, in particular, implies that the values $\chi(g)$ have representations, as members of the field $\mathbf{Q}_e$, of size polynomial in e and n.

In contrast to Problems 1 and 2, efficient methods for solving Problem 0 have been around for a long while (cf. Burnside [8], Dixon [16, 17], Eberly [18]). We summarize the results.

Theorem 1.5. *For a finite group G, given by its multiplication table, one can compute the irreducible characters of G over $\mathbf{C}$ in time polynomial in $|G|$. The character values belong to $\mathbf{Q}_e$.* □

We remark that these methods admit efficient parallel (NC) implementations (cf. Eberly [18]). Here we offer a polynomial-time algorithm for a more general problem.

Theorem 1.6. *Let $S \subset G$ be a set of generators of the group G. Assume that a representation $\mathscr{V}: G \to GL(n, F)$ is given by the list of matrices $\{\mathscr{V}(g); g \in S\}$, where F is an algebraic number field. Then the irreducible characters involved in $\mathscr{V}$ and their multiplicities can be determined in time polynomial in the input size.*

Note that the order of a group is not bounded by a polynomial of the size of the input, so we have to clarify in what sense a character may be computed under such circumstances. First, a basis $\mathscr{B}$ of the algebra $\mathrm{env}(\mathscr{V})$ can be computed in polynomial time, observing that $\mathrm{env}(\mathscr{V})$ is generated, as an algebra, by $\{\mathscr{V}(g): g \in S \cup S^{-1}\}$. Now, each character extends to a linear function over $\mathrm{env}(\mathscr{V})$, so it suffices to list its values on $\mathscr{B}$.

2. Representations and modules

In characteristic zero, the group algebra $F[G]$ is semisimple.

Problem 1 requires splitting $\mathbf{C}[G]$, as a $\mathbf{C}[G]$-module, into the direct sum of irreducible submodules.

By Wedderburn's theorem, a finite-dimensional semisimple algebra A over a field F has a decomposition

$$A = A_1 \oplus \cdots \oplus A_h, \tag{2.1}$$

where the A_i are simple algebras over F, and they are the (uniquely determined) minimal ideals of A. Each A_i possesses an identity element c_i. The c_i are the minimal central idempotents of A, and $A_i = c_i A$. Let ρ_i be a minimal *left* ideal of A_i. Then ρ_i is an irreducible A-module, and any A-module M can be written as a direct sum

$$M = M_1 \oplus \cdots \oplus M_h, \tag{2.2}$$

where the submodule

$$M_i = c_i M \tag{2.3}$$

is a direct sum of irreducible submodules isomorphic to ρ_i.

Turning to the algorithmic aspects of finding the decomposition (2.2) of M, (2.3) shows that it is useful to first determine the Wedderburn decomposition

(2.1) of $F[G]$. Friedl and Rónyai show in [20] that if F is an algebraic number field and A is a finite-dimensional semisimple algebra over F, given by structure constants, then the Wedderburn decomposition of A can be found in polynomial time. (The algorithm relies on factoring polynomials over finite extensions of F [23, 9, 21, 22].)

A field $F \supseteq \mathbf{Q}$ is a *splitting field* for G if every irreducible representation of G over F is *absolutely irreducible.* If this is the case, then h (the number of terms in (2.1) for $A = F[G]$) equals the number of conjugacy classes of G. Let $g_1, \ldots, g_h$ be representatives of the conjugacy classes and $C_i \in F[G]$ the sum of the elements in the class of g_i. Let further χ_i denote the irreducible character afforded by the $F[G]$-module ρ_i. Then for $1 \leq j \leq h$, one can compute c_j by the formula [12, Theorem 33.8]

$$c_j = \frac{\chi_j(1)}{|G|} \sum_{i=1}^{h} \overline{\chi}_j(g_i) C_i. \tag{2.4}$$

The result of R. Brauer, mentioned after Theorem 1.1, states that *the cyclotomic field $\mathbf{Q}_e$ is a splitting field for any group with exponent e* [12, Theorem 41.1; 19, (16.3)]. In fact, this is an immediate consequence of Theorem 3.1 below, another result of R. Brauer, central to our algorithm. It will be convenient to formulate this result in terms of the Wedderburn decomposition (2.1) of the group algebra $\mathbf{Q}_e[G]$.

Theorem 2.1. *Let e be the exponent of the finite group G. Then we have*

$$\mathbf{Q}_e[G] \cong M_{n_1}(\mathbf{Q}_e) \oplus \cdots \oplus M_{n_h}(\mathbf{Q}_e). \tag{2.5}$$ □

($M_r(F)$ denotes the algebra of $r \times r$ matrices over F.) The number $n_i = \chi_i(1)$ is the degree of the ith absolutely irreducible representation of G (corresponding to the minimal left ideal ρ_i), and $n_i^2 = \dim A_i$ in (2.1).

A *polynomial-time algorithm to determine the character table of G* follows immediately. Use [20] to find the Wedderburn decomposition (2.1) of $A = \mathbf{Q}_e[G]$; this decomposition is isomorphic to (2.5). Every $g \in G$ induces a linear transformation on each A_i; let $\tau_i(g)$ denote the trace of this action. Then, by the above,

$$\chi_i(g) = \frac{1}{n_i} \tau_i(g). \tag{2.6}$$

The fact that the character table can be computed in polynomial time is not new; various versions of a method of Burnside [8] (Dixon [16], Eberly [18]) have achieved this. The method just described takes an approach different from Burnside's. We shall prove Theorem 1.3 along similar lines. We need some preparations.

Proposition 2.2. *If E/F is a Galois extension of fields, then $E \otimes_F E$ is the direct sum of copies of E.*

We leave the proof as an exercise to the reader (cf. [12, §69, Ex. 1]). □

Corollary 2.3. *If A is a simple algebra over F and the center $E = Z(A)$ is a Galois extension of F, then $A \otimes_F E$ is the direct sum of simple algebras, central over E.*

Proof. Let $B := A \otimes_F E$. Then B is semisimple because E/F is separable [12, Theorem 69.4]. Let $B = B_1 \oplus \cdots \oplus B_s$ be the Wedderburn decomposition of B. Then $Z(B) = \bigoplus_{i=1}^{s} Z(B_i)$. On the other hand, $Z(B) = Z(A) \otimes_F E = \bigoplus_{i=1}^{s} E_i$, where $E_i = E$ by Proposition 2.2. □

For the next two lemmas, let A be a central simple algebra over the algebraic number field E, $\dim_E A = n = k^2$. Let $a_1, \ldots, a_n$ be a basis of A over E. An element $a \in A$ is called a *splitting element* of A if the minimal polynomial f of a over E has no multiple roots and $\deg(f) = k$.

Lemma 2.4 (Eberly [18, §2.5.3]). *Let $H \subset E$ be a finite subset of cardinality $|H| = 2k(k-1)$. Suppose that $(\lambda_1, \ldots, \lambda_n) \in H^n$ is a random element drawn from the uniform distribution over H^n. Then with probability at least $1/2$, $a = \lambda_1 a_1 + \cdots + \lambda_n a_n$ is a splitting element of A.*

Indeed, the discriminant of the characteristic polynomial of a generic $k \times k$ matrix has degree $k(k-1)$ and a well-known lemma of J. T. Schwartz [28] applies. □

Lemma 2.5. *Let $a \in A$ be a splitting element of A and let g be an irreducible factor over E of the minimal polynomial of a over E. Put $L = E(\gamma)$, where γ is a root of g. Then $A \otimes_E L \cong M_k(L)$. Moreover, if the element a is given, then this isomorphism can be constructed in polynomial time.*

Proof. Let f be the minimal polynomial of a. First we work in the algebra $A \otimes_E \mathbf{C} \cong M_k(\mathbf{C})$. Note that A can be considered as a subring of $A \otimes_E \mathbf{C}$ via the injection $b \mapsto b \otimes 1$. We shall interpret a as a $k \times k$ matrix over $\mathbf{C}$. The conditions imply that up to a constant factor, f is the characteristic polynomial of a. Now put $h(x) = f(x)/(x - \gamma)$. Clearly, the rank of the matrix $b = h(a)$ is 1, or in other words, for the left ideal ρ generated by b we have $\dim_{\mathbf{C}} \rho = k$. But $b \in B := A \otimes_E L$, and if ϱ stands for the left ideal of B generated by b, then we have $\varrho \otimes_L \mathbf{C} = \rho$ and therefore $\dim_L \varrho = \dim_{\mathbf{C}} \rho = k$. Thus, B is central simple over L and has a k-dimensional left ideal. It follows that $B \cong M_k(L)$.

The algorithmic part of the statement follows because ϱ can be constructed efficiently. Indeed, finding f means finding a linear relation among the elements $1, a, a^2, \ldots, a^k$. Having factored f over E, a basis of ϱ is easily computed. By introducing coordinates on ϱ we obtain an explicit isomorphism $B \cong M_k(L)$. □

Lemma 2.6. *Assume we are given a semisimple algebra A over an algebraic number field K and an A-module M. Suppose further that, as part of the input, we are given a decomposition*

$$A = \rho_1 \oplus \cdots \oplus \rho_k$$

of A into a direct sum of minimal left ideals. Then M can be decomposed into a direct sum of irreducible A-modules in polynomial time.

Proof. Let $v_1, \ldots, v_s$ be a basis of M over K. An A-submodule of the form $\rho_i v_j$ is either (0) or irreducible. Let $N_1, \ldots, N_r$ be an enumeration of the nonzero submodules $\rho_i v_j$. Set $J = \{i: N_i \not\subseteq \sum_{j<i} N_j\}$. Then M is the direct sum of the irreducible submodules N_i, $i \in J$. □

Corollary 2.7. *Let A be a central simple algebra over the algebraic number field E and let M be an A-module. Then one can find in Las Vegas polynomial time a field extension L/E and a decomposition of $M \otimes_E L$ into a direct sum of irreducible $(A \otimes_E L)$-submodules.*

Proof. We use Lemma 2.4 to find a splitting element $a \in A$ in Las Vegas polynomial time. We factor the minimal polynomial of a over E; let g be an irreducible factor. Let $L := E[x]/(g)$ and $B := A \otimes_E L$. Now, by Lemma 2.5 we have an explicit isomorphism $B \cong M_k(L)$. This allows us to break B into a direct sum of minimal left ideals. Indeed, if e_{ii} denotes the element of $M_k(L)$ which has 1 in position (i, i) and zeros elsewhere, then the left ideals $M_k(L)e_{ii}$ $(1 \le i \le k)$ are minimal and give a direct decomposition of $M_k(L)$. We can apply Lemma 2.6 to compute the decomposition of $M \otimes_E L$. □

Proof of Theorem 1.4. We have to construct a tree according to rules (i)–(iv) stated before Theorem 1.4.

For an A-module M, let us say that M *effectively represents* the algebra $A' = A/N(M)$, where $N(M) = \{a \in A; aM = 0\}$. Indeed, M can be viewed as a faithful A'-module.

The root of the tree (level 0) will correspond to the module M and the field F. The nodes on level 1 will correspond to modules effectively representing simple algebras; those on level 2 to modules effectively representing simple algebras, central over the field at their parent node. Finally, the leaves of the tree will be found on level 3 and correspond to irreducible modules.

We use [20] to obtain the Wedderburn decomposition (2.1) of A. We create a child l_i of the root for each minimal ideal A_i of A. The submodule at l_i will be $M_i = A_i M$. Note that the algebra effectively represented by M_i is A_i, which is indeed simple.

Let now l_i be a level 1 node with A_i-module M_i, where A_i is a simple algebra over F and the field extension E_i/F, where $E_i = Z(A_i)$ is Galois. Let us associate the field E_i with l_i. Let $B_i = A_i \otimes_F E_i$. We find the Wedderburn decomposition of B_i and, as before, we create a child l_{ij} of l_i for each minimal ideal B_{ij} of B_i. The B_i-submodule of $M_i \otimes_F E_i$ at l_{ij} will be $M_{ij} = B_{ij}(M_i \otimes_F E_i)$. Note that the algebra B_{ij}, effectively represented by M_{ij}, is simple and *central* over E_i by Corollary 2.3.

Finally, the decomposition of the modules corresponding to level 2 nodes is accomplished by Corollary 2.7. □

In order to deduce Theorem 1.3 from Theorem 1.4, we have to verify the key condition that the center of each minimal ideal of the group algebra $F[G]$ is a Galois extension of F.

Lemma 2.8. *Let F be an algebraic number field and G a finite group. Let A be a simple direct summand of the algebra $F[G]$ and put $E = Z(A)$ (the center of A). Then E/F is an abelian (and therefore Galois) field extension.*

Proof. The cyclotomic field $K := \mathbf{Q}_e$ is a splitting field for G by Theorem 2.1. This implies that KF is also a splitting field for G. Consequently, $B = A \otimes_F KF$ is a direct sum of full matrix algebras over KF. It follows that $Z(B)$ is isomorphic to a sum of some copies of KF. On the other hand,

$$\begin{aligned} Z(B) &= Z(A \otimes_F KF) = Z(A) \otimes_F KF \\ &= E \otimes_F KF = E_1 \oplus \cdots \oplus E_s, \end{aligned}$$

where E_i is a field, $E_i \supseteq E$, and $E_i \supseteq KF$ (cf. [24, Exercise 4, §12.4]). We infer that $E_i = KF$. Hence $E \subseteq KF$. This implies that E/F is abelian. □

Proof of Theorem 1.3. The proof is immediate. A basis and structure constants for $A = \text{env}(\mathscr{V})$ can easily be constructed from the given input. Moreover, A is semisimple (by Maschke's theorem) and indeed a homomorphic image of the group algebra $F[G]$. Therefore, by Lemma 2.8, A together with the representation space, viewed as an A-module, satisfy the conditions of Theorem 1.4. □

Proof of Theorem 1.6. The proof is essentially a truncation of the proof of Theorem 1.4, applied, as above, to $A = \text{env}(\mathscr{V})$: we ignore the construction of the level 3 nodes (with the implication that no randomization is needed). Making the obvious translation between modules and representations, let l be a level 2 node with representation space U over the field E corresponding to the parent of l. The enveloping algebra C (corresponding to the algebra "effectively represented" on U) is now simple and central over E, therefore the absolutely irreducible constituents at the children of l all have the same character χ. Note also, that the degree of χ is k, where k is determined by the relation $k^2 = \dim_E C$. Thus, if $m = \dim_E U$, then l has m/k children and consequently, if τ denotes the character of the representation associated with l, then $\chi = (k/m)\tau$. □

3. Induced representations

Let F be a field, G a finite group, $H \leq G$ a subgroup, and $\mathscr{T}: H \to GL(r, F)$ an r-dimensional representation of H over F. Let

$$G = g_1 H \cup g_2 H \cup \cdots \cup g_t H$$

be the left coset decomposition of G with $g_1 = 1$. Extend the definition of $\mathscr{T}$ by setting $\mathscr{T}(x) = 0 \in M_r(F)$ for $x \in G \backslash H$. The representation

$\mathscr{U}: G \to GL(rt, F)$, *induced by* $\mathscr{T}$ [12, pp. 73–75] is then given by

$$\mathscr{U}(g) = (\mathscr{T}(g_i^{-1} g g_j))_{1 \le i, j \le t}. \tag{3.1}$$

If ϕ is the character afforded by $\mathscr{T}$, then ϕ^G denotes the character of $\mathscr{U}$; it is the character of G *induced by* ϕ. Let us define the function $\tilde{\phi}$ as $\tilde{\phi}(g) = \phi(g)$ if $g \in H$, and $\tilde{\phi}(g) = 0$ if $g \in G \backslash H$. Then for $g \in G$ we have

$$\phi^G(g) = \sum_{i=1}^{t} \tilde{\phi}(g_i^{-1} g g_i). \tag{3.2}$$

If ϕ_1 and ϕ_2 are two characters of H, then $(\phi_1 + \phi_2)^G = \phi_1^G + \phi_2^G$.

Let $E \le H \le G$ be subgroups of G, and χ a character of E. Then we have $\chi^G = (\chi^H)^G$. This property is referred to as the *transitivity of induction* [12, p. 267].

A subgroup $H \le G$ is called *elementary* if it is a direct product of a cyclic group and a p-group for some prime p. A subgroup $H \le G$ is called an *E-subgroup* if it is of the form $H = \langle g, P \rangle$, where $g \in G$ and P is a Sylow p-subgroup of the centralizer $C_G(g)$ for some prime p. Clearly, every E-subgroup is elementary, and every elementary subgroup is contained in an E-subgroup. We shall make use of the following theorem of R. Brauer [5, 7] (see (15.1) in [19]).

Theorem 3.1. *Every character* χ *of the finite group* G *can be represented in the form*

$$\chi = \sum a_i \psi_i^G,$$

where ψ_i *is an irreducible character of some* E*-subgroup* $H_i \le G$ *and the coefficients* a_i *are integers.* □

Actually, this result is formulated by Brauer and Tate in [7] with elementary subgroups in the place of E-subgroups. This version, however, immediately follows by the transitivity of induction and the observation that every elementary subgroup is contained in an E-subgroup. The purpose of this modification is to reduce (below a polynomial bound) the number of elementary subgroups we shall have to enumerate.

Proposition 3.2. *Let* G *be a finite group and* χ *an irreducible character of* G, *and let* $\psi_1, \psi_2, \ldots, \psi_s$ *be the irreducible characters of the* E*-subgroups of* G. *Let* m_i *denote the multiplicity of* χ *in* ψ_i^G. *Then we have* $\gcd(m_1, \ldots, m_s) = 1$.

Proof. By Theorem 3.1, $\chi = \sum a_i \psi_i^G$. Comparing the coefficients of χ on both sides, we infer $1 = \sum a_i m_i$, proving the claim. □

4. Representations of nilpotent groups

A finite group is *nilpotent* if and only if it is the direct product of its Sylow subgroups. Note that E-groups are nilpotent. It is known that the irreducible

representations of a direct product $G = H \times K$ are obtained as the Kronecker products of the irreducible representations of H and K. It suffices therefore to consider p-groups.

The following result of H. Blichfeldt [19, (10.2)] is helpful.

Lemma 4.1. *Let P be a p-group and χ a nonlinear irreducible character of P. Then*

(i) *there exists a nonprincipal linear character λ of P such that $\chi\lambda = \chi$ and $\lambda^p = 1$;*

(ii) *if λ is a character of P satisfying* (i), *then there exists an irreducible character ζ of the kernel of λ such that $\chi = \zeta^P$.* □

Suppose now that P is a p-group for a prime p, and let χ be a given nonlinear irreducible character of P. We shall find a subgroup $K \leq P$ and a linear character λ of K such that $\chi = \lambda^P$. To this end, we shall find a sequence of subgroups $P = P_0 > P_1 > \cdots > P_i$ and a sequence of characters $\chi = \chi_0, \chi_1, \ldots, \chi_i$ such that χ_j is an irreducible character of P_j and $\chi_j^{P_{j-1}} = \chi_{j-1}$ $(1 \leq j \leq i)$, as follows.

Suppose that $P_0, \ldots, P_j$ and $\chi_0, \ldots, \chi_j$ have already been found. If χ_j is a linear character of P_j, then we set $i := j$ and halt. If χ_j is nonlinear, then by inspection of the character table of P_j we find a nonprincipal linear character λ of P_j such that $\lambda^p = 1$ and $\chi_j\lambda = \chi_j$. By Lemma 4.1(i) such a character exists. Next we put $P_{j+1} = \ker\lambda$ and by inspecting the character table of P_{j+1} we find an irreducible character ζ of P_{j+1} such that $\zeta^{P_j} = \chi_j$. The existence of ζ is guaranteed by Lemma 4.1(ii). We can then put $\chi_{j+1} := \zeta$. This completes the description of the algorithm. Note also, that χ_i is a linear character of P_i and that by the transitivity of induction we have $\chi_i^P = \chi$, and thus we can put $K := P_i$ and $\lambda := \chi_i$. This procedure leads to the following result.

Theorem 4.2. *Let P be a finite p-group for some prime p, given by its multiplication table, and let χ be a given irreducible character of P. Then we can construct an irreducible representation $\mathscr{U}: P \to GL(r, \mathbf{Q}_e)$, where $r = \chi(1)$ is the degree of χ and e is the exponent of P, such that χ is the character afforded by $\mathscr{U}$. Moreover, the algorithm runs in deterministic time polynomial in $|P|$. All matrix elements in the representation are of the form* (1.1).

Proof. By Theorem 1.5, character tables of subgroups of P are computed in time polynomial in $|P|$. We note that by (1.1), the sizes of all characters encountered are uniformly polynomially bounded. Induced characters are computed by (3.2), and induced representations by (3.1). The characters λ and χ_{j+1} are found by exhaustive search of the respective character tables. □

Corollary 4.3. *Let G be a finite group given by its multiplication table. Let $\psi_1, \psi_2, \ldots, \psi_s$ be the irreducible characters of the E-subgroups of G. Then we*

can construct in time polynomial in $|G|$ *representations* $\mathscr{U}_i: G \to GL(r_i, \mathbf{Q}_e)$, *where* r_i *is the degree of* ψ_i^G *and* e *is the exponent of* G *such that* ψ_i^G *is the character afforded by* $\mathscr{U}_i$.

Proof. Put $n = |G|$.

First we observe that the number s is not too large. Indeed, every E-subgroup H can be written as $H = \langle g, P\rangle$, $g \in G$, and P is a Sylow p-subgroup of $C_G(g)$ for some prime p. Since for fixed p and $g \in G$, the number of possible choices of P is less than n, we infer that the number of E-subgroups of G is at most $n^2 \log_2 n$ and therefore $s \leq n^3 \log_2 n$. This implies that we can find all the E-subgroups of G and the irreducible characters $\psi_1, \ldots, \psi_s$ in time polynomial in n. To establish the corollary, it suffices to show that if $H \leq G$ is a given E-subgroup and ψ_i an irreducible character of H, then we can construct a representation $\mathscr{T}$ of H over $\mathbf{Q}_e$ which affords ψ_i in time polynomial in n. (Then $\mathscr{U}_i$ is constructed by (3.1).)

The construction of $\mathscr{T}$ follows from Theorem 4.2 and the remarks at the beginning of this section. □

Actually, we do not need to consider all the E-subgroups, since conjugate subgroups yield identical induced characters. This observation reduces the number of E-subgroups to consider to less than $n \log_2 n$.

5. Finding free submodules

An A-module is called *free* if it is isomorphic to a direct sum of copies of A.

For a finitely generated module M over a semisimple algebra A the number of terms in a decomposition of M into a direct sum of irreducible A-modules is independent of the decomposition selected. We denote this number by $\operatorname{rank}_A M$. For a matrix $u \in M_k(F)$ we write $\operatorname{rk}(u)$ for the rank of u. Note that for $A = M_k(F)$ we have $\operatorname{rank}_A A = k$ and $\operatorname{rank}_A Au = \operatorname{rk}(u)$ for $u \in A$.

Lemma 5.1. *Let* F *be a field of characteristic zero and* M *a module over the algebra* $A = M_k(F)$. *Assume* $\operatorname{rank}_A M \geq k$. *Let* $u_1, u_2, \ldots, u_m$ *be a basis of* M *over* F *and let* $u \in M$ *be an element such that* $\operatorname{rank}_A Au < k$. *Then there exist integers* i, j, $1 \leq i \leq k$ *and* $1 \leq j \leq m$, *such that* $\operatorname{rank}_A A(u + iu_j) > \operatorname{rank}_A Au$.

Proof. As M is completely reducible, there exist A-modules M_1 and M_2 such that $M = Au \oplus M_1 \oplus M_2$ and $\operatorname{rank}_A Au \oplus M_1 = k$. We work in the module $N = M/M_2$. Let v and v_j be the images in N of u and u_j, resp. By comparing ranks, we infer that $N \cong A$ as an A-module. Also we have $\operatorname{rank}_A Au = \operatorname{rank}_A Av = r$, and the elements v_j $(j = 1, \ldots, m)$ generate N as an F-space. By the isomorphism $N \cong A$ we can interpret the elements of N as $k \times k$ matrices over F. In particular, for an element $w \in N$ we have $\operatorname{rank}_A Aw = \operatorname{rk}(w)$, and it suffices to prove that for appropriate i and j we have $\operatorname{rk}(v + iv_j) > r$. To this end, let $a, b \in M_k(F)$ be nonsingular matri-

ces such that $avb = I_r$, where I_r denotes the matrix having 1 in positions (i, i) for $1 \le i \le r$ and zeros elsewhere. Also put $w_j = av_jb$. The matrices $w_1, \dots, w_m$ generate $M_k(F)$ as a linear space over F; consequently, there exists a j such that the entry c in position $(r+1, r+1)$ of w_j is not 0. Now let $f(x) \in F[x]$ be the determinant of the $(r+1) \times (r+1)$ principal minor in the top left corner of the matrix $I_r + xw_j$, where x is a variable. We have $\deg f \le k$, $f(0) = 0$, and $f \ne 0$ because the coefficient of x in f is $c \ne 0$. We conclude that there exists an i, $1 \le i \le k$, such that $f(i) \ne 0$, and this in turn implies that $\mathrm{rk}(I_r + iw_j) > r$. Multiplying by a^{-1} and b^{-1} on the respective sides, the lemma follows. □

Next we consider the problem of finding a large free submodule in a given module M over $A = M_k(F)$, where F is an algebraic number field represented in the usual way (see §1).

Suppose that $\mathrm{rank}_A M = lk+1$. Our objective is to efficiently find a submodule $N \le M$ such that $\mathrm{rank}_A N = lk$. We may identify the additive group of M with the linear space $V = V_m(F)$ of column vectors of length $m = (lk+1)k$ over F. The action of A is specified by giving the action of a basis $v_1, \dots, v_{k^2}$ of A over F on the standard unit vectors $e_i \in V$ $(1 \le i \le m)$:

$$v_j e_i = \lambda_{ij1} e_1 + \cdots + \lambda_{ijm} e_m, \tag{5.1}$$

where $\lambda_{ijs} \in F$.

The output is represented by a list S of elements $u_1, \dots, u_l \in V$ such that they constitute a set of free generators for N (as an A-module).

Algorithm findfree.

Step 1. Initialize: $N := (0)$, $S :=$ emptylist.

Step 2. If $|S| = l$, then terminate. Else, set $u := 0$.

Step 3. Find integers i, j, where $1 \le i \le k$, $1 \le j \le m$, such that $\mathrm{rank}_A(N + A(u + ie_j)) > \mathrm{rank}_A(N + Au)$ and set $u := u + ie_j$. If $\mathrm{rank}_A(N + Au) = \mathrm{rank}_A N + k$, then set $N := N + Au$, add u to S and go back to Step 2, else go back to Step 3.
End.

Lemma 5.2. *If* $\mathrm{rank}_A M = kl + 1$, *then algorithm* **findfree** *finds a submodule* N *of* M *such that* $\mathrm{rank}_A N = kl$. *The elements of* S *constitute a set of free generators for* N, *and if* $u \in S$, $u = \alpha_1 e_1 + \cdots + \alpha_n e_m$, *then the* α_i *are nonnegative integers and* $\sum \alpha_i \le k^2$. *Moreover, if the size of the numbers* λ_{ijs} *in* (5.1) *is bounded by* Λ, *then the algorithm runs in time polynomial in* n, m, *and* Λ.

Proof. First we observe that throughout the process, N is a free module over A and the elements of S are free generators for N. Indeed, this is true at the start ($N = (0)$, S is empty). Each time before updating N and S in Step 3,

we have $\operatorname{rank}_A(N + Au)/N = k$ and therefore $Au \cong A$ is a free A-module and $Au \cap N = (0)$.

Lemma 5.1 applied to the module M/N ensures that each time we enter Step 3, we can find appropriate i and j. Note also that upon completing Step 3 the rank of the module $N + Au$ always increases. This shows that after at most kl executions of Step 3 the algorithm terminates.

As for the coefficients α_i, the initial value of u is 0, and in Step 3 we perform at most k assignments of the form $u := u + ie_j$ $(1 \le i \le k)$ before adding u to S; therefore we have $0 \le \alpha_i \in \mathbf{Z}$ and $\sum \alpha_i \le k^2$.

The rank-computations can be performed by finding a basis over F of the submodule in question. Note that we always work with modules of the form $N + Au$ $(u \in V)$, where the coordinates of u with respect to the basis $\{e_i\}$ are nonnegative integers not greater than k^2. By the above discussion, this also holds for the free generators u_i of N stored in S. A basis of $N + Au$ can be obtained by selecting a maximal set of linearly independent elements over F from among the elements $v_j u_i$ and $v_j u$. The number of arithmetic operations over F required by this task is clearly polynomial in m. The size of the coefficients of the elements $v_j u_i$ and $v_j u$ with respect to the basis $\{e_i\}$ is bounded by $\Lambda(\log_2 k + 1)$ and therefore the statement follows. □

6. Construction of irreducible modules

In this section we describe the method of constructing an irreducible representation of G over $\mathbf{Q}_e$ with a given character χ. The method will consist of first "pasting" together a number of representations induced from elementary subgroups, then "cutting" out most of the result.

We may assume that χ is nonlinear. Let $k = \chi(1)$ be the degree of χ and put $n = |G|$. Let $B \triangleleft \mathbf{Q}_e[G]$ be the minimal ideal corresponding to χ, and ρ be a minimal left ideal of B. Since $\mathbf{Q}_e$ is a splitting field of G, we see that $B \cong M_k(\mathbf{Q}_e)$, as algebras over $\mathbf{Q}_e$.

First we construct representations $\mathscr{U}_i: G \to GL(r_i, \mathbf{Q}_e)$ with characters ψ_i^G for $1 \le i \le s$ such that all entries of the matrices in these representations have the form (1.1), where $\psi_1, \ldots, \psi_s$ are the irreducible characters of the E-subgroups of G. This can be done in time polynomial in n (Corollary 4.3). Next we compute, by (2.4), the minimal central idempotent $c \in \mathbf{Q}_e[G]$ corresponding to the character χ. Note that $c\mathbf{Q}_e[G] = B$.

Let N_i denote the $\mathbf{Q}_e[G]$-module corresponding to the representation $\mathscr{U}_i$ (cf. §2). We compute the submodules $M_i := cN_i \le N_i$ $(1 \le i \le s)$. The submodule M_i is a direct sum of irreducible submodules isomorphic to ρ. Let a_i be the multiplicity of ρ in M_i. Clearly, we have $0 \le a_i \le n$.

What follows next is the "pasting" operation.

By Proposition 3.2 we have $\gcd(a_1, \ldots, a_s) = 1$. Note that we have $k^2 < n$ and $s \le n^3 \log_2 n$. We can therefore rapidly select $r \le \log_2 k$ numbers (say,

$a_1, \ldots, a_r$) from the $\{a_i\}$ such that $\gcd(a_1, \ldots, a_r, k) = 1$ holds. Similarly, we can quickly find integers $0 \leq b_i < k$ such that

$$t := \sum_{i=1}^{r} a_i b_i \equiv 1 \pmod{k}.$$

Here we have $t < n \log_2 n$. Next we take b_i isomorphic copies of M_i and form their direct sum. Let $M_{(i)}$ denote the resulting module. Then we form the direct sum

$$M = M_{(1)} \oplus M_{(2)} \oplus \cdots \oplus M_{(s)}.$$

Note that M is now isomorphic to a direct sum of $t = kl + 1$ copies of ρ for some nonnegative integer l.

Having done the "pasting", one "cutting" step remains.

Let us consider the action of $\mathbf{Q}_e[G]$ on M. Since for every minimal central idempotent $c_i \neq c$ we have $c_i M = (0)$, we can view M as a B-module and the $\mathbf{Q}_e[G]$-submodules and the B-submodules of M coincide. We can therefore apply Lemma 5.2 with $A = B$: we can find in time polynomial in n a submodule $N \leq M$ such that $\operatorname{rank}_B N = kl$.

Let us now consider the quotient module $N' = M/N$. (For computational purposes, one can represent N' by extending a basis (over $\mathbf{Q}_e$) of N to one of M and computing the action of $\mathbf{Q}_e[G]$ on the additional basis vectors modulo N.)

From $\dim_{\mathbf{Q}_e} N' = k$ we infer that $\operatorname{rank}_{\mathbf{Q}_e[G]} N' = \operatorname{rank}_B N' = 1$, hence N' is an irreducible $\mathbf{Q}_e[G]$-module. The fact that N' is a B-module as well implies that N' corresponds to the character χ. We have thus shown how to find an irreducible representation which affords the given irreducible character χ, thus completing the proof of Theorem 1.1. □

Our next task is to decompose $\mathbf{Q}_e[G]$ into the direct sum of minimal left ideals.

The action of B on N' defines an algebra homomorphism $B \to \operatorname{End}_{\mathbf{Q}_e} N'$. This is injective since B is simple. By comparing dimensions it follows that it is onto as well. In particular, there exists exactly one $b_i \in B$ $(1 \leq i \leq k)$ such that $b_i e_j = \delta_{ij} e_j$ for $1 \leq j \leq k$. Moreover, b_i can be found efficiently by solving a system of linear equations. It is straightforward to check that Bb_i is a minimal left ideal of B and

$$B = Bb_1 \oplus \cdots \oplus Bb_k.$$

Thus, from an irreducible B-module we can efficiently find a decomposition of B into a direct sum of minimal left ideals. By doing so for all the minimal ideals appearing in the Wedderburn decomposition (2.1) of $A = \mathbf{Q}_e[G]$, we obtain a decomposition of $\mathbf{Q}_e[G]$ itself.

Corollary 6.1. *One can find minimal left ideals* $\rho_1, \ldots, \rho_t$ *of* $\mathbf{Q}_e[G]$ *such that*

$$\mathbf{Q}_e[G] = \rho_1 \oplus \cdots \oplus \rho_t$$

in time polynomial in $|G|$. □

Now we are ready to prove Theorem 1.2.

Proof. Let r be the degree of $\mathscr{V}$ and set $K = \mathbf{Q}_e F$. Clearly, $\mathscr{V}$ can be considered as a representation over K. Let M denote the resulting $K[G]$-module. The algebra $K[G]$ has a decomposition

$$K[G] = \varrho_1 \oplus \cdots \oplus \varrho_t,$$

where $\varrho_i = \rho_i \otimes_{\mathbf{Q}_e} K$ $(1 \leq i \leq t)$, with $\rho_1, \ldots, \rho_t$ taken from Corollary 6.1. Note that a basis of ρ_i over $\mathbf{Q}_e$ remains a basis of ϱ_i over K, and that ϱ_i is an irreducible $K[G]$-module because $\mathbf{Q}_e$ is a splitting field for G. An application of Lemma 2.6 completes the proof. □

7. Discussion and open problems

For a finite group given by its multiplication table, we have solved in polynomial time the problem of decomposing the group algebra into minimal left ideals over a splitting field of the group. It is natural to ask if such restriction on the field is indeed necessary. We are unable, for instance, to solve the following problem.

Problem 7.1. Find the irreducible constituents over $\mathbf{Q}$ of a representation $G \to GL(n, \mathbf{Q})$ of a finite group G in polynomial time.

A more general problem would be to decompose a semisimple algebra over $\mathbf{Q}$ into minimal left ideals. This, however, seems to be computationally intractable. Indeed, the problem of finding a minimal left ideal of a 4-dimensional simple algebra A over $\mathbf{Q}$, given by structure constants, is *at least as difficult as factoring squarefree integers* (Rónyai [26]). (The reduction here is randomized and the proof assumes the generalized Riemann hypothesis. We remark that W. Eberly deduces from [26] that it is hard to find an invariant subspace with respect to a 4-dimensional representation over $\mathbf{Q}$ of a finitely generated group [18, Corollary 3.2.18].)

This obstacle indicates that it may be inevitable to rely on some specific properties of the group algebras $\mathbf{Q}[G]$ not shared by algebras in general. (See, however Problem 7.2 below.)

We remark that such difficulties do not occur over finite fields. Semisimple algebras over finite fields can be decomposed into the sum of minimal left ideals in Las Vegas polynomial time [20, 27]. (Las Vegas because no deterministic polynomial-time algorithm is known to factor polynomials over finite fields.)

In connection with the algebra approach to Theorem 1.1, the following are natural subproblems.

Problem 7.2. Let A be a finite-dimensional simple algebra over $\mathbf{Q}$, given by structure constants with respect to a basis $a_1, \ldots, a_n$. Suppose that we know somehow that $A \cong M_k(\mathbf{Q})$ $(k^2 = n)$. Assume further that the minimal polynomial $f_i \in \mathbf{Q}[x]$ of a_i over $\mathbf{Q}$ splits into linear factors in $\mathbf{Q}$ for every i. Is it possible to find a minimal left ideal of A in polynomial time?

Problem 7.3. Given a central simple algebra A over $\mathbf{Q}$ by structure constants, find a maximal subfield of A in polynomial time.

We even do not know whether a maximal subfield of polynomial size exists. (The notion of *size* was explained in §1 before Theorem 1.1.)

Problem 7.4. Given a permutation group $G \leq \mathrm{Sym}(\Omega)$ by a list of generators, can one find representatives of the conjugacy classes in time polynomial in the input *and in the output*?

Problem 7.5. Let G be a permutation group of degree n and χ an irreducible character of G. Find a bound in terms of n and $\chi(1)$ for the degree of the field extension $\mathbf{Q}(\chi(g): g \in G)/\mathbf{Q}$.

Problem 7.6. Given a permutation group $G \leq \mathrm{Sym}(\Omega)$ by a list of generators plus a set of representatives of the conjugacy classes, in what time bound can one find the character table of G?

A solution to Problem 7.5 will give information on the size of the output.

Problem 7.7. Given a permutation group G as in the preceding problem and an (absolutely) irreducible character χ of G such that all values $\chi(g)$ $(g \in G)$ are rational, find a representation of G affording χ.

If $n = \chi(1)$, the argument in the proof of Theorem 1.6 shows that $n\chi$ is the character of a representation of G over $\mathbf{Q}$ (corresponding to a simple ideal of the group algebra $\mathbf{Q}[G]$).

BIBLIOGRAPHY

1. M. D. Atkinson, *The complexity of group algebra computations*, Theoret. Comput. Sci. **5** (1977), 205–209.
2. E. R. Berlekamp, *Factoring polynomials over large finite fields*, Math. Comp. **24** (1970), 713–735.
3. M. Ben-Or, *Probabilistic algorithms in finite fields*, Proc. 22nd IEEE FOCS, 1981, pp. 394–398.
4. T. Beth, *On the computational complexity of the general discrete Fourier transform*, Theoret. Comput. Sci. **51** (1987), 331–339.
5. R. Brauer, *Applications of induced characters*, Amer. J. Math. **69** (1947), 709–716.
6. C. Brott and J. Neubüser, *A programme for the calculation of characters and representations of finite groups*, Computational Problems in Abstract Algebra (J. Leech, ed.), Pergamon Press, 1970.
7. R. Brauer and J. Tate, *On the characters of finite groups*, Ann. of Math. (2) **62** (1955), 1–7.

8. W. Burnside, *Theory of groups of finite order*, 2nd ed., Dover, 1955.
9. A. L. Chistov and D. Yu. Grigoryev, *Polynomial time factoring of the multivariable polynomials over a global field*, LOMI preprint E-5-82, Leningrad, 1982.
10. M. Clausen, *Fast Fourier transform for metabelian groups*, SIAM J. Comput. **18** (1989), 584–593.
11. ——, *Fast generalized Fourier transforms*, Theoret. Comput. Sci. (to appear).
12. C. W. Curtis and I. Reiner, *Representation theory of finite groups and associative algebras*, Wiley, 1966.
13. P. Diaconis, *Spectral analysis for ranked data*, Ann. Statist. (to appear).
14. ——, *Group representations in probability and statistics*, Inst. of Math. Stat., Hayward, CA, 1988.
15. P. Diaconis and D. Rockmore, *Efficient computation of the Fourier transform on finite groups*, manuscript, 1988.
16. J. D. Dixon, *High speed computation of group characters*, Numer. Math. **10** (1967), 446–450.
17. ——, *Computing irreducible representations of groups*, Math. Comp. **24** (1970), 707–712.
18. W. Eberly, *Computations for algebras and group representations*, Ph.D. Thesis, Department of Computer Science, University of Toronto, 1989.
19. W. Feit, *Characters of finite groups*, Benjamin, 1967.
20. K. Friedl and L. Rónyai, *Polynomial time solutions of some problems in computational algebra*, Proc. 17th ACM Sympos. on Theory of Computing, 1985, pp. 153–162.
21. S. Landau, *Factoring polynomials over algebraic number fields*, SIAM J. Comput. **14** (1985), 184–195.
22. A. K. Lenstra, *Factoring polynomials over algebraic number fields*, Proc. EUROCAL, Lecture Notes in Comput. Sci., vol. 162, Springer, 1983, pp. 245–254.
23. A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovász, *Factoring polynomials with rational coefficients*, Math. Ann. **261** (1982), 515–534.
24. R. S. Pierce, *Associative algebras*, Graduate Texts in Math., vol. 88, Springer, 1982.
25. L. Rónyai, *Simple algebras are difficult*, Proc. 19th ACM Sympos. on Theory of Computing, 1987, pp. 398–408.
26. ——, *Zero divisors in quaternion algebras*, J. Algorithms **9** (1988), 494–506.
27. ——, *Computing the structure of finite algebras*, J. Symb. Comput. **9** (1990), 355–373.
28. J. T. Schwartz, *Fast probabilistic algorithms for verification of polynomial identities*, J. Assoc. Comput. Mach. **27** (1980), 701–717.

DEPARTMENT OF COMPUTER SCIENCE, UNIVERSITY OF CHICAGO, CHICAGO, ILLINOIS 60637

AND

EÖTVÖS UNIVERSITY, BUDAPEST, HUNGARY H-1088
E-mail address: laci@cs.uchicago.edu

COMPUTER AND AUTOMATION INSTITUTE, HUNGARIAN ACADEMY OF SCIENCES, BUDAPEST, P.O.B. 63, HUNGARY H-1502
E-mail address: sztaki!ronyai@relay.EU.net