Some lower and upper complexity bounds for generalized Fourier transforms

Ulrich Baum and Michael Clausen
Informatik V, Universität Bonn

February 21, 1990

Abstract

The 2-linear complexity $L_2(G)$ of a finite group G is the minimal number of additions, subtractions and multiplications (by complex constants of absolute value ≤ 2) needed to evaluate a suitable Fourier transform corresponding to G. We prove that $L_2(G) > \frac{1}{4}|G|\log|G|$ for any finite group G, and present two infinite classes of non-abelian groups G with $L_2(G) \leq 0.6|G|\log|G|$ and $L_2(G) \leq 0.8|G|\log|G|$, respectively. Thus there are non-abelian groups with even faster Fourier transforms than elementary abelian 2-groups (for which $L_2(G) \leq |G|\log|G|$) !

Key words. Fast Fourier transforms, group algebras, Frobenius groups, extra-special 2-groups.
AMS(MOS) subject classifications. 68 Q 40, 20 C 15

Running head: Complexity bounds for Fourier transforms

1 Introduction

The design and analysis of efficient algorithms for Fourier transforms on finite groups has been the subject of several recent investigations, see the references. The present paper continues the studies in [6]. Although we assume familiarity with [6] and its notations, we briefly recall the mathematical background.

By Wedderburn's theorem, the group algebra $\mathbf{C}G$ of a finite group G is isomorphic to an algebra of block diagonal matrices: $\mathbf{C}G \simeq \bigoplus_{i=1}^{h} \mathbf{C}^{d_i \times d_i}$, where the blocks correspond to the equivalence classes of irreducible representations of $\mathbf{C}G$. Every algebra isomorphism $W : \mathbf{C}G \to \bigoplus_{i=1}^{h} \mathbf{C}^{d_i \times d_i}$ is called a (generalized) *Fourier transform* for $\mathbf{C}G$. With respect to natural bases, W can be viewed as a $|G|$-square complex matrix. (E.g., if $G = C_n$ is the cyclic group of order n then $W = (\omega^{ab})_{0 \leq a,b < n}$ with $\omega = \exp(2\pi i/n)$.)

The linear complexity $L_s(A)$ of a matrix $A \in \mathbf{C}^{r \times t}$ is the minimal number of $\mathbf{C}$-operations (= additions/subtractions/scalar multiplications) sufficient to compute Ax from a (generic) input vector $x \in \mathbf{C}^t$. Since a non-abelian group G has infinitely many Fourier transforms, we define the *linear complexity* of G by $L_s(G) := \min L_s(W)$, where the minimum is taken over all possible Fourier transforms W for $\mathbf{C}G$. Combining [2] and [6], we get

$$L_s(G) \leq 9|G| \log |G|$$

for all finite metabelian groups G. (Throughout this paper, $\log = \log_2$.) If G is an abelian 2-group, the classical FFT-algorithms show that

$$L_s(G) \leq \frac{3}{2}|G| \log |G| \ .$$

For the class of elementary abelian 2-groups, i.e. $G \simeq C_2 \times \cdots \times C_2$, the fast Hadamard-Walsh transforms prove the even better bound

$$L_s(G) \leq |G| \log |G| \ .$$

All the algorithms proving the above three upper bounds use (besides additions and subtractions) only multiplications with complex constants of absolute value ≤ 2. This motivates to study the 2-*linear complexity*

$$L_2(G) := \min\{L_2(W) | W \text{ a Fourier transform for } \mathbf{C}G\}$$

of the finite group G, where $L_2(W)$ is the minimal number of $\mathbf{C}$-operations needed to evaluate the complex matrix W at an input vector when scalar multiplications are restricted to complex constants of absolute value ≤ 2. According to the above remark, $L_2(G) \leq 9|G| \log |G|$ for all finite metabelian groups.

In order to get a lower bound for the 2-linear complexity of a finite non-abelian group G, we are faced with the problem of estimating $L_2(W)$ for infinitely many Fourier transforms W on G. Nevertheless, combining a result of Morgenstern and the Schur relations we can prove in section 2 that

$$L_2(G) \geq \frac{1}{4}(1+\frac{1}{|G'|})|G|\log|G| > \frac{1}{4}|G|\log|G|$$

for any finite group G, where G' denotes the commutator subgroup of G.

How tight is this general lower bound? Up to now, the elementary abelian 2-groups satisfying $L_2(G) \leq |G|\log|G|$ seemed to have the fastest Fourier transforms. But in fact, this is not true: In sections 3 and 4 we present two infinite classes of non-abelian groups G with $L_2(G) \leq 0.6|G|\log|G|$ and $L_2(G) \leq 0.8|G|\log|G|$, respectively.

2 Lower bounds in the L_2-model

In this section we are going to prove a general lower bound for the 2-linear complexity of any Fourier transform on a finite group G.

Theorem 1 *If G is a finite group, $\mathbf{C}G \simeq \bigoplus_{i=1}^h \mathbf{C}^{d_i\times d_i}$, then*

$$L_2(G) \geq \log\frac{|G|^{|G|/2}}{\prod_{i=1}^h d_i^{d_i^2/2}} .$$

This result has several interesting consequences.

Corollary 1 *For any finite group G,*

$$L_2(G) \geq \frac{1}{4}(1+\frac{1}{|G'|})|G|\log|G| > \frac{1}{4}|G|\log|G| .$$

PROOF. $\mathbf{C}G \simeq \bigoplus_{i=1}^h \mathbf{C}^{d_i\times d_i}$ implies $|G| = \sum_{i=1}^h d_i^2$. As the number of one-dimensional irreducible representations of G equals $[G:G']$, see e.g. [13, V,6.5], we get

$$\sum_{d_i>1} d_i^2 = |G| - [G:G'] .$$

Hence, by Theorem 1,

$$\begin{aligned}
L_2(G) &\geq \frac{|G|}{2}\log|G| - \sum_{d_i>1}\frac{d_i^2}{4}\log d_i^2 \\
&\geq \frac{|G|}{2}\log|G| - \sum_{d_i>1}\frac{d_i^2}{4}\log|G| \\
&\geq \frac{|G|}{2}\log|G| - \frac{1}{4}(1-\frac{1}{|G'|})|G|\log|G| \\
&= \frac{1}{4}(1+\frac{1}{|G'|})|G|\log|G| .
\end{aligned}$$

This proves Corollary 1. □

Corollary 2 *If G is abelian then*

$$L_2(G) \geq \frac{1}{2}|G|\log|G| \ .$$

PROOF. Use Theorem 1 and the fact that all $d_i = 1$ for an abelian group G. □

As a special case of Corollary 1 we mention

Corollary 3 *If $|G'| = 2$ then*

$$L_2(G) \geq \frac{3}{8}|G|\log|G| \ .$$

In order to prove Theorem 1 we first recall a special case of

Morgenstern's Theorem. [17] *If $A \in \mathbf{C}^{n\times n}$ is invertible, then*

$$L_2(A) \geq \log|\det A| \ .$$

As a second tool we need the so-called

Schur Relations. [13, V, Satz 5.7] *Let $D_1, \ldots, D_h$ be a full set of inequivalent irreducible matrix representations of $\mathbf{C}G$ of degrees $d_1, \ldots, d_h$, respectively. Then for all $1 \leq a, b \leq h$ and $1 \leq i, j \leq d_a$ and $1 \leq k, l \leq d_b$, the following holds:*

$$\sum_{g\in G} D_a(g)_{ij} \cdot D_b(g^{-1})_{kl} = \delta_{ab}\delta_{il}\delta_{jk}\frac{|G|}{d_a} \ .$$

Note that the right hand sides of the Schur relations only depend on the equivalence classes of the irreducible representations of $\mathbf{C}G$. We are now ready to give the

PROOF OF THEOREM 1. Let G be a finite group of order n and $D_1, \ldots, D_h$ a full set of inequivalent irreducible representations of $\mathbf{C}G$, $d_i :=$ degree(D_i). If $A \in \mathbf{C}^{n\times n}$ is a Fourier transform matrix of $\mathbf{C}G$ with respect to $D_1, \ldots, D_h$, the columns of A are parametrized by the elements of G whereas the rows of A correspond to

$$\bigcup_{1\leq a\leq h} \{(a,i,j) | 1 \leq i,j \leq d_a\} \ ,$$

i.e. (a,i,j) describes the position (i,j) in D_a. Now let $B \in \mathbf{C}^{n\times n}$ be the matrix obtained from A by first transposing A and then performing in $A^\top$

permutations of the rows corresponding to the inversion ($G \ni g \mapsto g^{-1}$) and permutations of the columns corresponding to $(a,i,j) \mapsto (a,j,i)$. According to the Schur Relations, $A \cdot B$ is a diagonal matrix with d_a^2 occurences of $|G|/d_a$ for $1 \leq a \leq h$. As $\det B = \pm \det A^\top = \pm \det A$, we get

$$\begin{aligned} |\det A|^2 &= |\det A \cdot B| = \prod_{i=1}^{h} \left(\frac{|G|}{d_i}\right)^{d_i^2} \\ &= \frac{|G|^{d_1^2+\ldots+d_h^2}}{\prod_i d_i^{d_i^2}} = \frac{|G|^{|G|}}{\prod_i d_i^{d_i^2}} . \end{aligned}$$

By Morgenstern's Theorem, our claim follows. □

The following example will illustrate (the proof of) Theorem 1.

Example. The symmetric group S_3 has (up to equivalence) three irreducible $\mathbf{C}$-representations: the trivial representation

$$\iota : (S_3 \ni \pi \mapsto 1) ,$$

the alternating representation

$$\epsilon : (S_3 \ni \pi \mapsto \mathrm{sgn}(\pi)) ,$$

and a 2-dimensional representation Δ realizing S_3 as the symmetry group of a regular triangle. If we take its center of gravity as the origin in 2-space and denote its vertices by e_1, e_2, e_3, then $\{e_1, e_2\}$ is a basis and $e_3 = -e_1 - e_2$. The natural S_3-action $\pi e_i := e_{\pi i}$ yields the following realization of Δ:

$$\Delta(1) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} , \ \Delta(123) = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} , \ \Delta(132) = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}$$

$$\Delta(12) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} , \ \Delta(23) = \begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix} , \ \Delta(13) = \begin{pmatrix} -1 & 0 \\ -1 & 1 \end{pmatrix}$$

Thus

$$A = \begin{array}{|c|c|c|c|c|c|l} \hline 1 & 1 & 1 & 1 & 1 & 1 & \iota \\ \hline 1 & 1 & 1 & -1 & -1 & -1 & \epsilon \\ \hline 1 & 0 & -1 & 0 & 1 & -1 & \Delta_{11} \\ \hline 0 & -1 & 1 & 1 & -1 & 0 & \Delta_{12} \\ \hline 0 & 1 & -1 & 1 & 0 & -1 & \Delta_{21} \\ \hline 1 & -1 & 0 & 0 & -1 & 1 & \Delta_{22} \\ \hline (1) & (123) & (132) & (12) & (23) & (13) & \end{array}$$

is a Fourier transform on S_3. The corresponding matrix B reads as follows:

$$B = \begin{array}{|c|c|c|c|c|c|l}
\hline
1 & 1 & 1 & 0 & 0 & 1 & (1) \\
\hline
1 & 1 & -1 & -1 & 1 & 0 & (132) \\
\hline
1 & 1 & 0 & 1 & -1 & -1 & (123) \\
\hline
1 & -1 & 0 & 1 & 1 & 0 & (12) \\
\hline
1 & -1 & 1 & 0 & -1 & -1 & (23) \\
\hline
1 & -1 & -1 & -1 & 0 & 1 & (13) \\
\hline
\iota & \epsilon & \Delta_{11} & \Delta_{21} & \Delta_{12} & \Delta_{22} &
\end{array}$$

and $A \cdot B$ equals the diagonal matrix $\mathrm{diag}(6, 6, 3, 3, 3, 3)$.

3 FFT for a class of Frobenius groups

We are going to consider a special class of Frobenius groups G_n, constructed as follows: For $n \geq 2$, let F_n be the additive group of the finite field $GF(2^n)$ and let H_n denote the multiplicative group of that field. It is well known that F_n is an elementary abelian group of order 2^n and H_n is cyclic of order $2^n - 1$. H_n acts faithfully on F_n by automorphisms via $H_n \ni h \mapsto (F_n \ni f \mapsto hf)$. As $hf \neq f$ for every $h \in H_n \setminus \{1\}$ and $f \in F_n \setminus \{0\}$, H_n can be viewed as a fixed-point-free automorphism group of F_n. Hence the semi-direct product $G_n := F_n H_n$ is a Frobenius group of order $2^n(2^n - 1)$, see e.g. [13, V, §8]. The ordinary representation theory of Frobenius groups is well understood, see e.g. [13, V, Satz 16.13]. In our case, G_n has (up to equivalence) exactly the following irreducible representations:

(1) $2^n - 1$ one-dimensional representations χ_i $(1 \leq i < 2^n)$ obtained by composing each linear character η_i of the cyclic group H_n with the natural projection $G_n \to H_n \simeq G_n/F_n$, i.e.

$$\chi_i(fh) := \eta_i(h)$$

for all $f \in F_n$ and all $h \in H_n$.

(2) One $(2^n - 1)$-dimensional representation γ which is induced by any non-trivial linear character ϕ of F_n:

$$\gamma = \phi \uparrow G_n \ .$$

Note that the restriction of γ to F_n *equals* the direct sum of all non-trivial linear characters of F_n:

$$\gamma \downarrow F_n = \bigoplus_{1 \neq \psi \in X(F_n)} \psi \ .$$

Now we can state the main result of this section.

Theorem 2 *For the groups G_n defined above,*

$$L_2(G_n) < (\frac{1}{2} + \frac{5}{2^{n-1}})|G_n| \log |G_n| \ .$$

In particular, $L_2(G_n) \leq 0.6|G_n| \log |G_n|$ for all $n \geq 7$.

PROOF. Given $a = \sum_{g \in G_n} a_g g \in \mathbf{C}G_n$, we have to compute $\chi_1(a), \ldots, \chi_{2^n-1}(a)$ and $\gamma(a)$.

In order to compute $\gamma(a)$, write $a = \sum_{h \in H_n} \alpha_h h$ with $\alpha_h := \sum_{f \in F_n} a_{fh} f \in \mathbf{C}F_n$. Then

$$\begin{aligned} \gamma(a) &= \sum_{h \in H_n} (\gamma \downarrow F_n)(\alpha_h) \cdot \gamma(h) \\ &= \sum_{h \in H_n} (\bigoplus_{1 \neq \psi \in X(F_n)} \psi(\alpha_h)) \cdot (\phi \uparrow G_n)(h) \ . \end{aligned}$$

According to the last formula we first compute for each $h \in H_n$ all $\psi(\alpha_h)$, $\psi \in X(F_n)$, by $|H_n|$ evaluations of a $DFT(F_n)$. This can be done by fast Hadamard-Walsh transforms in at most

$$|H_n| \cdot |F_n| \log |F_n|$$

arithmetic operations. The matrices $(\phi \uparrow G_n)(h)$ are monomial with nonzero entries equal to ±1. (Observe that $\phi(F_n) = \{\pm 1\}$ because F_n is an elementary abelian 2-group.) The multiplication of the diagonal matrices $(\bigoplus_{1 \neq \psi} \psi(\alpha_h))$ by $(\phi \uparrow G_n)(h)$ is therefore free in our computational model. Moreover, the concluding summation is also free since all the summands have their nonzero entries at pairwise disjoint positions: as γ is irreducible we have $\dim \gamma(\mathbf{C}G) = |H_n|^2$. On the other hand, the summand corresponding to h has its $\leq |H_n|$ nonzero entries at the support of the monomial matrix $(\phi \uparrow G_n)(h)$.

To evaluate all $\chi_i(a)$ simultaneously we use the coefficients

$$b_h := \sum_{f \in F_n} a_{fh} = 1_{F_n}(\alpha_h)$$

already computed in the first step. According to (1),

$$\chi_i(a) = \eta_i(\sum_{h \in H_n} b_h h) \ ,$$

and we obtain all $\chi_i(a)$ by a single $DFT(H_n)$. Thus we get $\chi_1(a), \ldots, \chi_{2^n-1}(a)$ with at most $L_2(H_n)$ operations. Altogether we have

$$\begin{aligned} L_2(G_n) &\leq |H_n||F_n| \log |F_n| + L_2(H_n) \\ &\leq |G_n| \log |F_n| + 9|H_n| \log |H_n| \\ &< (n + \frac{9n}{2^n})|G_n| \ . \end{aligned}$$

As $\log|G_n| \geq 2n - 2^{1-n}$ for $n \geq 2$, we get

$$L_2(G_n) < (\frac{1}{2} + \frac{5}{2^{n-1}})|G_n|\log|G_n| \ .$$

□

Comparing upper and lower bounds for the groups G_n:

$$\frac{1}{4}(1 + \frac{1}{2^n - 1})|G_n|\log|G_n| < L_2(G_n) < \frac{1}{2}(1 + \frac{5}{2^{n-2}})|G_n|\log|G_n| \ ,$$

we see that they asymptotically differ by a factor of 2. This is quite similar to the situation for elementary abelian 2-groups G where we have

$$\frac{1}{2}|G|\log|G| \leq L_2(G) \leq |G|\log|G| \ .$$

In the next section, we will present an infinite class of groups G satisfying

$$\frac{3}{8}|G|\log|G| \leq L_2(G) \leq \frac{3}{4}(1 + \frac{2}{\log|G|})|G|\log|G| \ .$$

Again, lower and upper bounds differ by an asymptotic factor of 2.

4 FFT for extra-special 2-groups

In this section. we are going to present another class of finite groups with faster Fourier transforms than those of elementary abelian 2-groups.

Let G be an extra-special 2-group of order 2^{2m+1}, i.e. the center of G is of order 2 and equals the Frattini subgroup of G. Up to equivalence, G has exactly the following irreducible representations, see e.g. [13, V, 16.14]:

(1) 2^{2m} one-dimensional representations $\chi_1, \ldots, \chi_{2^{2m}}$

(2) One 2^m-dimensional representation γ which is induced by a linear character ϕ_1 of a maximal abelian normal subgroup $A \trianglelefteq G$. Note that $|A| = 2^{m+1}$ and either $A \simeq C_4 \times C_2^{m-1}$ or $A \simeq C_2^{m+1}$ (see e.g. [13, III, 13.8]). Moreover, $\gamma \downarrow A = \bigoplus_{i=1}^{2^m} \phi_i$, where the ϕ_i are distinct linear characters of A.

Thus like the groups G_n in the previous section, extra-special 2-groups have only one irreducible representation of large degree ($\approx \sqrt{|G|}$), all other irreducible representations are one-dimensional. Again, this situation leads to very fast Fourier transforms:

Theorem 3 *For an extra-special* 2*-group* G,

$$L_2(G) < \frac{3}{4}|G|\log|G| + \frac{3}{2}|G| \ .$$

PROOF. We have to evaluate $\chi_1(a), \ldots, \chi_{2^{2m}}(a)$ and $\gamma(a)$ for a given $a \in \mathbf{C}G$. As before, write $a = \sum_{h \in G/A} \alpha_h h$ with $\alpha_h \in \mathbf{C}A$ and evaluate the (unique) Fourier transform W_A of the abelian group A at all α_h. This takes at most $[G : A]L_2(A)$ linear operations.

Now we can compute $\gamma(a)$ according to the equation

$$\gamma(a) = \sum_{h \in G/A} (\gamma \downarrow A)(\alpha_h)\gamma(h) = \sum_{h \in G/A} (\bigoplus_{i=1}^{2^m} \phi_i(\alpha_h))(\phi_1 \uparrow G)(h) \ .$$

The multiplication of the diagonal matrix $(\bigoplus_{i=1}^{2^m} \phi_i(\alpha_h))$ by the monomial matrix $(\phi_1 \uparrow G)(h)$ takes at most 2^m arithmetic operations. As we can assume that one of the coset representatives $h \in G/A$ equals 1, and as the concluding summation is free (see the proof of Theorem 2), $\gamma(a)$ can be computed with at most $2^m(2^m - 1)$ operations.

It remains to compute $\chi_1(a), \ldots, \chi_{2^m}(a)$. To this end, we observe that any linear character ψ of G/A can be viewed as a linear character of G by composing it with the natural projection $G \to G/A$. It is well known that the linear characters of a finite group G form an abelian group $X(G)$ under pointwise multiplication, the so-called character group of G. Thus, if χ is a linear character of G and $\psi_1, \ldots, \psi_{2^m}$ are all linear characters of G/A, then $\chi\psi_1, \ldots, \chi\psi_{2^m} \in X(G)$ are pairwise distinct and $\chi\psi_i \downarrow A = \chi \downarrow A$. By Frobenius reciprocity, the $\chi\psi_i$ are all linear characters of G whose restriction to A equals $\chi \downarrow A$. As

$$\chi\psi_i(a) = \sum_{h \in G/A} \chi\psi_i(\alpha_h) \cdot \chi\psi_i(h) = \sum_{h \in G/A} \psi_i(hA)((\chi \downarrow A)(\alpha_h) \cdot \chi(h)) \ ,$$

$\chi\psi_1(a), \ldots, \chi\psi_{2^m}(a)$ can be computed from the $(\chi \downarrow A)(\alpha_h)$ by a DFT of the elementary abelian 2-group G/A and $[G : A] - 1$ additional multiplications. To evaluate all linear characters of G, we repeat this process 2^m times. This takes at most $2^m(L_2(G/A) + [G : A] - 1)$ operations. Altogether, we have

$$L_2(G) \le [G : A]L_2(A) + 2^m(2^m - 1) + 2^m(L_2(G/A) + [G : A] - 1) \ .$$

For $A \simeq C_4 \times C_2^{m-1}$, $L_2(A) \le 9 \cdot 2^{m-1} + 4(m-1)2^{m-1}$, and

$$\begin{aligned} L_2(G) &\le 2^m(9 \cdot 2^{m-1} + 4(m-1)2^{m-1} + 2^m - 1 + m2^m + 2^m - 1) \\ &< 2^{2m+1}(\frac{9}{4} + \frac{3}{2}m) \end{aligned}$$

$$
\begin{aligned}
&= \frac{6m+9}{4(2m+1)}(2m+1)2^{2m+1} \\
&= \frac{3}{4}|G|\log|G| + \frac{3}{2}|G| \ .
\end{aligned}
$$

For $A \simeq C_2^{m+1}$, we obtain the slightly better bound

$$L_2(G) < \frac{3}{4}|G|\log|G| + \frac{3}{4}|G| \ .$$

□

References

[1] M.D. ATKINSON, *The Complexity of Group Algebra Computations*, Theor. Comp. Sci., 5 (1977), pp. 205–209.

[2] U. BAUM, M. CLAUSEN, B. TIETZ, *Improved Upper Complexity Bounds for the Discrete Fourier Transform*, Research Report, Universität Bonn, 1990.

[3] T. BETH, *Verfahren der schnellen Fourier-Transformation*, Teubner, Stuttgart, 1984.

[4] T. BETH, *On the Computational Complexity of the General Discrete Fourier Transform*, Theor. Comp. Sci., 51 (1987), pp. 331–339.

[5] L.I. BLUESTEIN, *A Linear Filtering Approach to the Computation of the Discrete Fourier Transform*, IEEE Trans. AU-18 (1970), pp. 451–455.

[6] M. CLAUSEN, *Fast Fourier Transforms for Metabelian Groups*, SIAM J. Comput., 18 (1989), pp. 584–593.

[7] M. CLAUSEN, *Fast Generalized Fourier Transforms*, Theor. Comp. Sci. 67 (1989), pp. 55–63.

[8] M. CLAUSEN, D. GOLLMANN, *Spectral Transforms for Symmetric Groups – Fast Algorithms and VLSI Architectures*, Proceedings of 3rd. International Workshop on Spectral Techniques, University of Dortmund F.R.G., Oct. 1988.

[9] J.W. COOLEY, J.W. TUKEY, *An Algorithm for the Machine Calculation of Complex Fourier Series*, Math. Comp. 19 (1965), pp. 297–301.

[10] C.W. CURTIS, I. REINER, *Representation Theory of Finite Groups and Associative Algebras*, Wiley & Sons, New York, 1962.

[11] P. DIACONIS, *Spectral Analysis for Ranked Data*, Ann. Statistics, to appear.

[12] P. DIACONIS, D. ROCKMORE, *Efficient Computation of the Fourier Transform on Finite Groups*, Technical Report, Stanford University, April 1988.

[13] B. HUPPERT, *Endliche Gruppen I*, Springer, Berlin, 1967.

[14] S.L. HURST, D.M. MILLER, J.C. MUZIO, *Spectral Techniques in Digital Logic*, Academic Press, 1985.

[15] M.G. KARPOVSKY, *Fast Fourier Transforms on Finite Non-Abelian Groups*, IEEE Trans. Computers 26/10 (1977), pp. 1028–1030.

[16] M.G. KARPOVSKY (ed.), *Spectral Techniques and Fault Detection*, Academic Press, 1985.

[17] J. MORGENSTERN, *Note on a Lower Bound of the Linear Complexity of the Fast Fourier Transform*, J. ACM 20 (1973), pp. 305–306.

[18] H.J. NUSSBAUMER, *Fast Fourier Transform and Convolution Algorithms*, Springer, Berlin, 1981.

[19] C.M. RADER, *Discrete Fourier Transform when the Number of Data Points is Prime*, Proc. IEEE 56 (1968), pp. 1107–1108.

[20] D. ROCKMORE, *Fast Fourier Analysis for Abelian Group Extensions*, preprint, Harvard University, Dec. 1988.

[21] D. ROCKMORE, *Computation of Fourier Transforms on the Symmetric Group*, in: E. Kaltofen and S.M. Watt (eds.): Computers in Mathematics, Springer, New York, 1989.

[22] S. WINOGRAD, *On Computing the Discrete Fourier Transform*, Proc. Nat. Acad. Sci. USA 73 (1976), pp. 1005–1006.

[23] S. WINOGRAD, *Arithmetic Complexity of Computations*, SIAM, 1980.