On the Parametrization of Algebraic Discrete Fourier Transforms

Armin Nückel, Andreas Klappenecker*

Universität Karlsruhe
Institut für Algorithmen und Kognitive Systeme,
Am Fasanengarten 5, D–76 128 Karlsruhe, Germany
(nueckel|klappi)@ira.uka.de

Abstract. Computing the Discrete Fourier Transform (DFT) of signals over some finite field F_q often requires an extension to a large field F_{q^n} containing an appropriate primitive root of unity. The Algebraic Discrete Fourier Transforms (ADFTs) avoid the extension of the basefield F_q and can be used to compute the spectrum of the DFT. We derive a complete parametrization of ADFT matrices and show how this knowledge can be employed to derive VLSI realizations with low implementation complexity.

1 Introduction

The results presented in this paper are part of a long term research project called IDEAS [2]. The main goal of IDEAS is the development of an intelligent environment supporting the design of algorithms and architectures in signal processing. Our design environment deals with three levels of abstraction: VLSI technology, abstract modelling of digital circuits, and algebraic specification using computer algebra systems. In the early years we started with the development of software products for hardware compilers and computer algebra software. Nowadays, there are powerful tools available and we can focus on the algebraic topics. Comparable environments are described in [9, 10]. One of the main differences is the integration of commercial products avoiding an enormous implementation overhead.

This paper is concerned with the so-called Algebraic Discrete Fourier Transforms, their algebraic structure, and integrated circuit implementation. These transforms are closely related to the general discrete Fourier transforms as described for example in the chapter on STIPS machines in [9, chap. 5].

This paper is organized as follows. In the next paragraph we summarize some definitions from the theory of finite fields. In §3 we recall the conjugacy properties of the Discrete Fourier Transform. A novel approach to the ADFT is given in §4. A complete parametrization of all ADFT matrices is derived in §5. The benefit of choosing an ADFT with low implementation complexity is discussed in §§6-7.

* This work was supported by DFG under SFB 414.

2 Basic Definitions

Recall that computing the DFT of length N signal vectors over the finite field with q elements F_q typically affords an extension to a larger field that contains a primitive Nth root of unity. This requires that the characteristic of F_q does not divide the signal vector length N. We emphasize here that the degree of such an extension F_{q^n}/F_q can be quite large, since the existence of a primitive Nth root of unity in F_{q^n} implies that N is a divisor of $q^n - 1$. Typically, there are many different choices for the basis of the extension field. As we will see in the sequel, a well-chosen basis can be used to reduce implementation complexity.

For each basis $\{\alpha_1, \ldots, \alpha_n\}$ of the extension F_{q^n}/F_q there exists a uniquely determined dual basis $\{\beta_1, \ldots, \beta_n\}$ that satisfies

$$\mathrm{tr}\,(\beta_k \alpha_l) = \begin{cases} 0 & \text{for} \quad k \neq l \\ 1 & \text{for} \quad k = l \end{cases}$$

where $\mathrm{tr}\,(x) := \mathrm{tr}_{F_{q^n}/F_q}(x) = x + x^q + \cdots + x^{q^{n-1}}$ denotes the trace function of the extension F_{q^n}/F_q. We will use the trace function to express the coordinates of the elements in F_{q^n}. Suppose that an element $u \in F_{q^n}$ is of the form

$$u = \sum_{i=1}^{n} u_i \alpha_i, \qquad u_i \in F_q.$$

Then the coordinates of u with respect to the basis $\{\alpha_1, \cdots, \alpha_n\}$ can be expressed with the help of its dual basis $\{\beta_1, \cdots, \beta_n\}$ by

$$u_k = \mathrm{tr}\,(\beta_k u) = \sum_{i=1}^{n} u_i \,\mathrm{tr}\,(\beta_k \alpha_i)\,. \tag{1}$$

We will be interested in basis that are of the following form

$$B = \{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}.$$

Such a basis is called a *normal basis*; it is known that this type of basis exists for all extensions F_{q^n}/F_q [8]. Note that the elements of B are conjugates and are linearly independent over F_q. A Galois automorphism merely permutes this basis, hence the coordinates of conjugate elements. Finally, we recall the following remarkable fact, cf. [6, 8]:

Lemma 1. *The dual basis of a normal basis is again a normal basis.*

3 Conjugacy Properties

Denote by $\omega \in F_{q^n}$ a primitive Nth root of unity. The DFT matrix can be written in the form $(\omega^{jk})_{j,k=0..N-1}$. Applying an automorphism of the Galois group $\mathrm{Gal}\,(F_{q^n}/F_q)$ to the components of the DFT matrix results in a permutation of the rows (or columns) of this matrix. As a result one obtains the well-known conjugacy properties of the DFT [7]:

Lemma 2. *Let $(s_0, \ldots, s_{N-1})$ be a signal vector in $(F_q)^N$. Denote by S_j the jth spectral coefficient*

$$S_j = \sum_{k=0}^{N-1} \omega^{jk} s_k. \tag{2}$$

Applying the Frobenius automorphism $x \mapsto x^q$ to the spectral coefficient S_j yields the spectral coefficient $S_{jq \bmod N}$, that is, ${S_j}^q = S_{jq \bmod N}$.

Proof. The values s_k are elements of the basefield F_q by assumption. Therefore, they remain fixed under the action of the Frobenius automorphism, yielding

$${S_j}^q = \left(\sum_{k=0}^{N-1} \omega^{jk} s_k \right)^q = \sum_{k=0}^{N-1} \omega^{(jq)k} s_k = S_{jq \bmod N}. \qquad \square$$

Thus, it is sufficient to compute one spectral coefficient for each conjugacy class. If we express the DFT matrix coefficients with respect to a normal basis, then the conjugate spectral coefficients can be obtained by mere permutation. More specifically, we get the following result (keeping the notations as above):

Lemma 3. *Assume that the coefficients of the spectral coefficient S_j w.r.t. the normal base B are given by $(u_0, u_1, \ldots, u_{n-1}) \in F_q^n$, that is, $S_j = \sum_{k=0}^{n-1} u_k \alpha^{q^k}$. Then the coefficients of S_{jq} w.r.t. B are given by $(u_{n-1}, u_0, \ldots, u_{n-2})$.*

Proof. Suppose that the spectral coefficient S_{jq} is expressed with respect to the basis $B = \left\{ \alpha, \alpha^q, \ldots, \alpha^{q^{n-1}} \right\}$ as $S_{jq} = \sum_{k=0}^{n-1} v_k \alpha^{q^k}$, where $v_k \in F_q$. Then we have

$${S_j}^q = \sum_{k=0}^{n-1} u_k \alpha^{q^{k+1}} = \sum_{k=0}^{n-1} u_{k-1 \bmod n} \alpha^{q^k} = \sum_{k=0}^{n-1} v_k \alpha^{q^k} = S_{jq}.$$

Comparing coefficients yields the result. $\square$

4 Algebraic Discrete Fourier Transforms

We remarked in the previous section that computing the DFT of signal vectors with values in the basefield F_q amounts to compute only *one* spectral coefficient of each conjugacy class (cf. Lemma 2). To put it differently, suppose we are given only a single spectral coefficient of each conjugacy class, then we can still reconstruct the original basefield signal from this knowledge. Essentially, it is this property that is exploited e. g. in transform decoding techniques of BCH codes [7]. From a computational perspective it is highly attractive to express the coefficients with respect to a normal basis, since then the coordinates of conjugate coefficients are obtained by cyclic shifting (Lemma 3).

Example 1. Consider the DFT for signal vectors of length 7 with values in F_2. The definition of the DFT affords an extension to the field F_{2^3}. However, since the signals merely take values in the much smaller field F_2, we only have to compute the value of the spectral coefficients S_0, S_1, and S_3 given by equation (2). The other coefficients can be computed by means of Lemma 2, namely

$$S_2 = S_1^2,\ S_4 = S_2^2; \qquad S_6 = S_3^2,\ S_5 = S_6^2.$$

Thus, the spectral coefficients can be grouped according to the cyclotomic cosets, that is, the orbits of $x \mapsto (2x \bmod 7)$ in the set $[0..6]$.

In order to understand why some orbits are of smaller length than others, we will focus on the values that a spectral coefficient may take, as the signal values s_i vary. Denote by $F_q(S_j)$ the *value field* of the spectral coefficient S_j over F_q, that is, the field obtained by adjoining all possible values of the jth spectral coefficient to the basefield F_q:

$$F_q(S_j) = F_q(\omega^j) = F_q\left(\left\{\sum_{k=0}^{N-1} \omega^{jk} s_k \;\middle|\; s_k \in F_q\right\}\right).$$

This field is a normal subfield of F_{q^n}. By elementary Galois theory it is clear that the *number* of coefficients conjugate to the spectral coefficient S_j coincides with the *degree* of the value field $F_q(S_j) = F_q(\omega^j)$ over F_q. This fact is best appreciated with the help of a small example.

Example 2. Consider again the DFT of length 7 for signals with values in F_2, which requires an extension to $F_{2^3} = F_2(\omega)$, where ω is a primitive 7th root of unity with minimal polynomial $x^3 + x + 1$. Clearly, $F_q(S_0) = F_q(\omega^0)$ coincides with the basefield F_q, therefore S_0 has no conjugates. The value field of S_1 is given by $F_q(\omega)$, hence is of degree 3 over F_q. The value field of S_3 is given by $F_q(\omega^3)$. It can be checked that the minimal polynomial of ω^3 is given by $x^3 + x^2 + 1$. Therefore, the spectral coefficient S_3 has three conjugates.

Up to now we exploited the conjugacy properties of the DFT. Roughly speaking, a "large value field" leads to many conjugates, and thus to considerable savings. Now we want to show that, loosely speaking, a "small value field" leads to structure in the coordinate repesentation which can be exploited too. Eventually, this will lead us to the definition of the Algebraic Discrete Fourier Transform [1], which takes advantage of both properties.

The Galois group of F_{q^n}/F_q is a finite cyclic group of order n, generated by the Frobenius automorphism $x \mapsto x^q$. Hence, the Galois group of $F_{q^n}/F_q(S_j)$ is generated by a power of the Frobenius automorphism, say $G = \langle x \mapsto x^{q^k} \rangle$. In more elementary terms this means that the coordinates of the spectral coefficient S_j with respect to the normal basis B have the following structure:

$$(u_0, \ldots, u_{n-1}) = (\underbrace{u_0, \ldots, u_{k-1}}, \underbrace{u_0, \ldots, u_{k-1}}, \ldots\ldots, \underbrace{u_0, \ldots, u_{k-1}}).$$

This structure is guaranteed for *all* inputs $(s_0, \ldots, s_{N-1}) \in F_q^N$ by the definition of the value field. Moreover, it is not possible to refine this structure (meaning that no blocks smaller than k can be obtained for all inputs), since this would imply that even more Galois automorphism fix the value field $F_q(S_j)$. Moreover, elementary Galois theory tells us that the order of G multiplied with the degree of $F_q(S_j)/F_q$ equals the degree of F_{q^n}/F_q. Thus, there are exactly k automorphisms, namely $x \mapsto x$, $x \mapsto x^q$, $\ldots$, $x \mapsto x^{q^{k-1}}$, that map S_j to its conjugate spectral coefficients $S_j, S_{jq}, \ldots, S_{jq^{k-1}}$.

To summarize, for each conjugacy class of spectral coefficients with k elements we have to compute only the first k coefficients $u_0, \ldots, u_{k-1}$ of S_j with respect to a normal basis B. In view of Lemma 3 this is the same as computing the first coordinate of each spectral coefficient with respect to the normal basis B.

Definition 4. Let $N > 0$ be an integer and F_q a finite field. We assume that the characteristic of F_q does not divide N. Suppose further that F_{q^n} is a finite extension of F_q that contains a primitive Nth root of unity. Denote by

$$B = \left\{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\right\}, \qquad B' = \left\{\beta, \beta^q, \ldots, \beta^{q^{n-1}}\right\}$$

a normal base B with dual base B' of F_{q^n}/F_q. The **Algebraic Discrete Fourier Transform** of length N with respect to the normal basis generator α is defined by the $N \times N$-matrix

$$\mathrm{ADFT}_\alpha = \left(\mathrm{tr}\left(\beta\omega^{ij}\right)\right)_{i,j=0,\ldots,N-1}.$$

Let us restate the definition of the ADFT in less technical terms. Recall that the function $x \mapsto \mathrm{tr}\,(\beta x)$ maps an element $x \in F_{q^n}$ to its first coordinate with respect to the basis B; we have noticed this general property of dual bases in equation (1) above. Thus, the ADFT is obtained from the DFT-matrix by expressing each matrix entry $\omega^{ij} \in F_{q^n}$ with respect to B. This yields a vector $v_{i,j}$ of length n over F_q for each entry ω^{ij}. The first component of this vector $v_{i,j}$ coincides the (i,j)-entry of the ADFT-matrix.

Example 3. Consider the DFT of length 7 for signals over F_2. The extension $F_{2^3} = F_2(\omega)$ is generated by a primitive 7th root of unity ω with minimal polynomial $x^3 + x + 1$. A normal base for F_{2^3}/F_2 is given by $B = \{\omega^5, \omega^3, \omega^6\}$. If we express the coefficients ω^{ij} with respect to B, then the DFT-matrix reads as follows:

$$\begin{pmatrix}
[1,1,1] & [1,1,1] & [1,1,1] & [1,1,1] & [1,1,1] & [1,1,1] & [1,1,1] \\
[1,1,1] & [1,0,1] & [1,1,0] & [0,1,0] & [0,1,1] & [1,0,0] & [0,0,1] \\
[1,1,1] & [1,1,0] & [0,1,1] & [0,0,1] & [1,0,1] & [0,1,0] & [1,0,0] \\
[1,1,1] & [0,1,0] & [0,0,1] & [1,1,0] & [1,0,0] & [1,0,1] & [0,1,1] \\
[1,1,1] & [0,1,1] & [1,0,1] & [1,0,0] & [1,1,0] & [0,0,1] & [0,1,0] \\
[1,1,1] & [1,0,0] & [0,1,0] & [1,0,1] & [0,0,1] & [0,1,1] & [1,1,0] \\
[1,1,1] & [0,0,1] & [1,0,0] & [0,1,1] & [0,1,0] & [1,1,0] & [1,0,1]
\end{pmatrix}.$$

Viewing the DFT as a transform for signals over F_2 yields a 7×21-matrix over F_2. The ADFT with respect to the normal basis generator ω^5 of B is obtained by reading off the first components $[*, \ , \ ]$, thus yielding a 7×7-matrix over F_2:

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 1 \end{pmatrix}.$$

Remark. We defined the ADFT only for DFTs over finite fields F_{q^n}/F_q. More generally, one can define the ADFT for arbitrary fields. For example, the discrete Hartley transform can be viewed as a special case of ADFTs over the real numbers. An even wider class of basefield transforms is studied in [5].

5 Parametrization

The ADFT is by no means uniquely determined by a given basefield and DFT-matrix. After fixing a specific extension F_{q^n}/F_q, we can still choose freely some normal basis generator. We exploit this freedom to optimize ADFTs for specific needs.

Lemma 5. *Let $B = (\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}})^t$ be a normal basis of F_{q^n}/F_q and let $T \in \mathrm{GL}(n, F_q)$ a base change matrix. Then TB is a normal basis of F_{q^n}/F_q if and only if T is a circulant matrix.*

Proof. Suppose that T is of the form $T = (c_{l-k \bmod n})_{k,l=0,\ldots,n-1}$. Then $TB = (\gamma_0, \ldots, \gamma_{n-1})^t$ is a basis of the form

$$\gamma_k = \sum_{l=0}^{n-1} c_{l-k \bmod n} \alpha^{q^l} = \left(\sum_{l=0}^{n-1} c_{l-k \bmod n} \, \alpha^{q^{l-k}} \right)^{q^k} = \left(\sum_{l=0}^{n-1} c_{l \bmod n} \, \alpha^{q^l} \right)^{q^k}.$$

This reduces to $\gamma_k = \gamma_0^{q^k}$. Therefore TB is a normal basis, as claimed. The other direction follows directly from the normal basis property. □

Remark. The inverse of a circulant matrix is again circulant. Therefore, a coordinate change from one normal basis to another is achieved by multiplying with some invertible matrix $(d_{j-i \bmod n})_{i,j}$.

Theorem 6. *Assume that F_{q^n} is a finite field containing a primitive Nth root of unity $\omega \in F_{q^n}$. Denote by α a generator of a normal basis of the extension*

F_{q^n}/F_q. Then all ADFT matrices derived from $(\omega^{ij})_{i,j=0,\ldots,N-1} \in \mathrm{GL}(N, F_{q^n})$ for signals over the basefield F_q can be written in the following form:

$$\left(\sum_{\ell=0}^{n-1} d_\ell \mathrm{tr}\left(\alpha^{q^\ell} \omega^{ij}\right) \right)_{i,j=0,\ldots,N-1}$$

where the coefficients $d_0, d_1, \ldots, d_{n-1}$ are elements of F_q that generate an invertible circulant matrix $(d_{j-i})_{i,j} \in \mathrm{GL}(n, F_q)$.

Proof. After fixing an extension F_{q^n}/F_q and a DFT matrix (ω^{ij}) [mind that the choice of the primitive root ω is somewhat arbitrary], all ADFT matrices are given by the set

$$\left\{ \left(\mathrm{tr}\left(\gamma\, \omega^{ij}\right) \right)_{i,j=0,\ldots,N-1} \,\middle|\, \gamma \text{ is a normal basis generator of } F_{q^n}/F_q \right\}$$

According to the previous Lemma, the coordinate change from

$$V_{ij} := \left(\mathrm{tr}\left(\alpha\omega^{ij}\right), \mathrm{tr}\left(\alpha^q\omega^{ij}\right), \ldots, \mathrm{tr}\left(\alpha^{q^{n-1}}\omega^{ij}\right) \right)^t$$

to

$$W_{ij} := \left(\mathrm{tr}\left(\gamma\omega^{ij}\right), \mathrm{tr}\left(\gamma^q\omega^{ij}\right), \ldots, \mathrm{tr}\left(\gamma^{q^{n-1}}\omega^{ij}\right) \right)^t$$

is realized by multiplying V_{ij} with an invertible circulant matrix $T = (d_{j-i})_{i,j}$, that is, $W_{ij} = TV_{ij}$ holds for all $i, j \in \{0, \ldots, N-1\}$. More explicitly, we obtain

$$\mathrm{tr}\left(\gamma^{q^k}\omega^{ij}\right) = \sum_{\ell=0}^{n-1} d_{\ell-k}\, \mathrm{tr}\left(\alpha^{q^\ell}\omega^{ij}\right).$$

In particular, this yields for the first coordinate

$$\mathrm{tr}\left(\gamma\omega^{ij}\right) = \sum_{\ell=0}^{n-1} d_\ell\, \mathrm{tr}\left(\alpha^{q^\ell}\omega^{ij}\right),$$

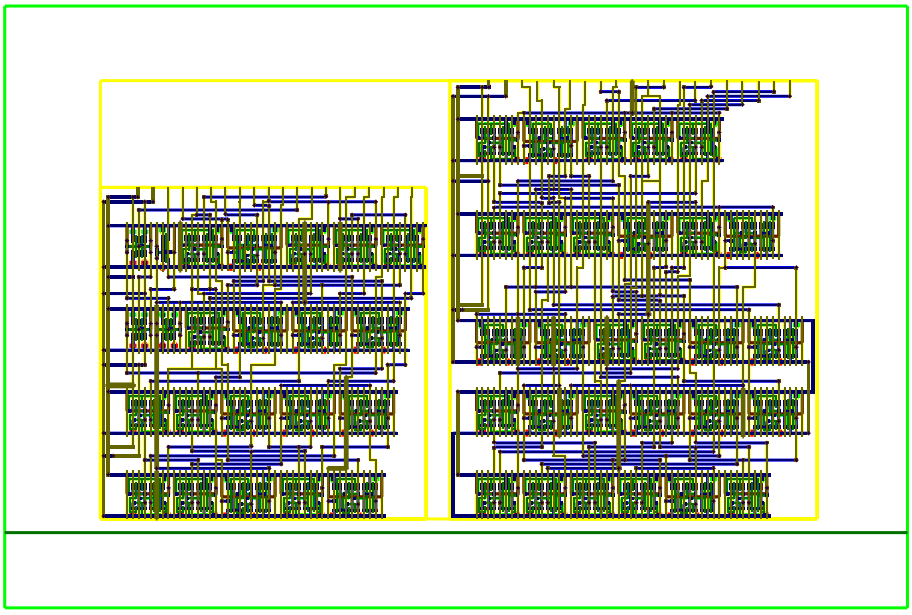
as desired. □

6 Optimization

The theorem in the previous paragraph shows that an enumeration of invertible, circulant matrices in $\mathrm{GL}(n, F_q)$ yields an enumeration of all ADFT matrices. Enumeration gets unfeasible for large basefields or large extensions. To remedy the situation, we describe now a heuristic optimization technique to derive ADFT matrices with low implementation cost. Before we do so, we discuss some examples to illustrate the benefit of these methods.

Example 4. Consider the DFT of signal vectors of length 9 over F_2. This requires an extension to F_{2^6}. Let α be a primitive element of F_{2^6} with minimal polynomial $x^6+x^4+x^3+x+1$. Then $\omega=\alpha^7$ is a primitive 9th root of unity with minimal polynomial x^6+x^3+1. The element α^{23} with minimal polynomial x^6+x^6+1 generates a normal basis; another normal basis is generated by the element α^6 with minimal polynomial $x^6+x^5+x^4+x^2+1$. The matrices $\mathrm{ADFT}_1=(\mathrm{tr}\left(\alpha^{23}\omega^{ij}\right))_{i,j=0,\ldots,8}$ and $\mathrm{ADFT}_2=(\mathrm{tr}\left(\alpha^{6}\omega^{ij}\right))_{i,j=0,\ldots,8}$ read then as follows:

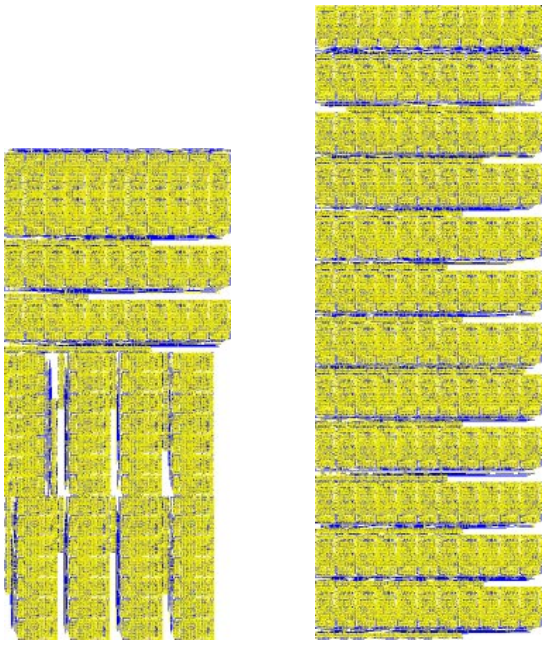
$$\mathrm{ADFT}_1=\begin{pmatrix}
1&1&1&1&1&1&1&1&1\\
1&0&1&1&0&1&0&0&0\\
1&1&0&0&0&0&1&1&0\\
1&1&0&1&1&0&1&1&0\\
1&0&0&1&0&1&0&0&1\\
1&1&0&0&1&0&1&0&0\\
1&0&1&1&0&1&1&0&1\\
1&0&1&1&0&0&0&0&1\\
1&0&0&0&1&0&1&1&0
\end{pmatrix},\quad
\mathrm{ADFT}_2=\begin{pmatrix}
1&1&1&1&1&1&1&1&1\\
1&1&0&0&0&1&1&1&1\\
1&0&0&1&1&1&0&1&1\\
1&0&1&1&0&1&1&0&1\\
1&0&1&0&1&0&1&1&1\\
1&1&1&1&0&1&0&1&0\\
1&1&0&1&1&0&1&1&0\\
1&1&1&0&1&1&1&0&0\\
1&1&1&1&1&0&0&0&1
\end{pmatrix}.$$



The figure shows a standard cell implementation of the transforms ADFT_1 and ADFT_2. Although both transforms can be used to compute the spectrum of the DFT for signals of length 7 over the basefield F_2, the implementation of the ADFT_1 requires less active elements. This reduction in silicon area was achieved by searching for an ADFT matrix with many zero-entries, which resulted in the transform ADFT_1. The ADFT_2 was obtained by an initial guess of a normal basis generator.

Example 5. Consider the DFT of length 12 signals over the basefield F_5. This requires an extension to F_{5^2}. Denote by α a primitive element of F_{5^2} with minimal polynomial $x^2 + 4x + 2$. In this field there are four primitive 12th roots of unity, namely $\alpha^2, \alpha^{10}, \alpha^{14}$, and α^{22}; let us choose $\omega = \alpha^{22}$, an element with minimal polynomial $x^2 + 2x + 4$. A normal basis for F_{5^2}/F_5 is generated by α or alternatively by α^{10}. Then the matrices $\mathrm{ADFT}_1 = (\mathrm{tr}\left(\alpha\omega^{ij}\right))_{i,j=0,\ldots,11}$ and $\mathrm{ADFT}_2 = (\mathrm{tr}\left(\alpha^{10}\omega^{ij}\right))_{i,j=0,\ldots,11}$ read as follows:

$$\mathrm{ADFT}_1 = \begin{pmatrix}
1&1&1&1&1&1&1&1&1&1&1&1\\
1&3&0&3&4&0&4&2&0&2&1&0\\
1&0&4&4&0&1&1&0&4&4&0&1\\
1&3&4&2&1&3&4&2&1&3&4&2\\
1&4&0&1&4&0&1&4&0&1&4&0\\
1&0&1&3&0&3&4&0&4&2&0&2\\
1&4&1&4&1&4&1&4&1&4&1&4\\
1&2&0&2&4&0&4&3&0&3&1&0\\
1&0&4&1&0&4&1&0&4&1&0&4\\
1&2&4&3&1&2&4&3&1&2&4&3\\
1&1&0&4&4&0&1&1&0&4&4&0\\
1&0&1&2&0&2&4&0&4&3&0&3
\end{pmatrix}, \quad \mathrm{ADFT}_2 = \begin{pmatrix}
2&2&2&2&2&2&2&2&2&2&2&2\\
2&4&4&1&2&2&3&1&1&4&3&3\\
2&4&2&3&1&3&2&4&2&3&1&3\\
2&1&3&4&2&1&3&4&2&1&3&4\\
2&2&1&2&2&1&2&2&1&2&2&1\\
2&2&3&1&1&4&3&3&2&4&4&1\\
2&3&2&3&2&3&2&3&2&3&2&3\\
2&1&4&4&2&3&3&4&1&1&3&2\\
2&1&2&2&1&2&2&1&2&2&1&2\\
2&4&3&1&2&4&3&1&2&4&3&1\\
2&3&1&3&2&4&2&3&1&3&2&4\\
2&3&3&4&1&1&3&2&2&1&4&4
\end{pmatrix}$$



The left figure shows the layout of ADFT_1 using $2266 \times 4936\mu\mathrm{m}^2$ silicon area. The right figure shows the implementation of ADFT_2 requiring an area of $2266 \times 6347\mu\mathrm{m}^2$. Both realizations are designed for a 1μ CMOS technology.

For our heuristic optimization we consider the circulant base change matrix $(d_{j-i})_{i,j}$ as a matrix with elements of the ring $F_q[d_1, \ldots, d_{n-1}]$ in the indeterminates d_i. This yields the Parametrized Algebraic Discrete Fourier Transform:

$$PADFT := \left(\sum_{\ell=0}^{n-1} d_\ell \mathrm{tr}\left(\alpha^{q^\ell \omega^{ij}}\right) \right)_{i,j=0,\ldots,N-1}.$$

Let us illustrate this construction for signals of length 7 over F_2. The DFT matrix given in Example 3 translates directly into the following PADFT:

$$\begin{pmatrix}
d_s & d_s & d_s & d_s & d_s & d_s & d_s \\
d_s & d_0+d_2 & d_0+d_1 & d_1 & d_1+d_2 & d_0 & d_2 \\
d_s & d_0+d_1 & d_1+d_2 & d_2 & d_0+d_2 & d_1 & d_0 \\
d_s & d_1 & d_2 & d_0+d_1 & d_0 & d_0+d_2 & d_1+d_2 \\
d_s & d_1+d_2 & d_0+d_2 & d_0 & d_0+d_1 & d_2 & d_1 \\
d_s & d_0 & d_1 & d_0+d_2 & d_2 & d_1+d_2 & d_0+d_1 \\
d_s & d_2 & d_0 & d_1+d_2 & d_1 & d_0+d_1 & d_0+d_2
\end{pmatrix},$$

where d_s denotes the term $d_s := d_0 + d_1 + d_2$. Note that all terms in the PADFT are linear combinations of the parameters d_i.

Theorem 6 shows that all ADFT matrices can be obtained from the PADFT by specializing the parameters $d_0, \ldots, d_{n-1}$ to values in F_q such that $T = (d_{j-i \bmod n})_{i,j}$ is invertible. For instance, from the PADFT matrix above one derives the ADFT given in Example 3 by choosing the parameters $d_0 := 1, d_1 := 0$, and $d_2 := 0$; the circulant matrix T yields for these parameters a permutation matrix, which is of course invertible.

The generic representation of the ADFT matrix allows to compute for example sparse ADFT matrices. The following algorithm searches for a specialization that leads to a high number of zero-entries. The algorithm proceeds in a greedy way and tries to specialize the terms that occur most often to zero. This is done by constructing a system of linear equations, which represent constraints on the specialization parameters. The aim is to find a specialization τ of the parameters d_i that yields an invertible matrix $\tau(T) = (\tau(d_{j-i \bmod n}))_{i,j}$ and satisfies as many contraints as possible.

```
# Input: a PADFT matrix M in the indeterminates d_i over F_q
# Output: an ADFT matrix
H := list of terms occuring as entries in M,
     sorted by number of occureny;
E := [];
for i from 1 to length(H) do
   LinearEq := append(E,H[i]=0);
   T := solve(LinearEq);
   if {τ | τ ∈ T, det(τ(T)) ≠ 0} ≠ ∅ then E:= LinearEq; fi;
od;
T := solve(E); τ := choose({τ | τ ∈ T, det(τ(T)) ≠ 0});
return(τ(M));
```

This algorithm presents the basic idea of heuristical optimization: the transform is determined by implementation issues. The same idea can be used for more elaborate optimization algorithms.

7 Conclusion

We have presented general results on Algebraic Discrete Fourier Transforms. We have shown that these results can be used to find efficient implementations of those transforms. The computation of sparse matrices in only one specific example. It is possible to combine our methods with implementations strategies as described in [3, 4].

Acknowledgement

We thank Professor Thomas Beth for introducing us to the the ADFT.

References

1. T. Beth, W. Fumy, and R. Mühlfeld. Zur Algebraischen Diskreten Fourier-Transformation. *Arch. Math.*, 40:238–244, 1983.
2. T. Beth, A. Klappenecker, T. Minkwitz, and A. Nückel. The ART behind IDEAS. In Jan van Leeuwen, editor, *Computer Science Today*, volume 1000 of *Lecture Notes in Computer Science*, pages 141–158. Springer Verlag, 1995.
3. J. Hong and M. Vetterli. Hartley transforms over finite fields. *IEEE Trans. on Information Theory*, 39(5):1628–1638, 1993.
4. J. Hong, M. Vetterli, and P. Duhamel. Basefield transforms with the convolution property. *Proc. of the IEEE*, 82(3):400–412, 1994.
5. A. Klappenecker. Basefield transforms derived from character tables. In *Proc. of 1997 Int. Conf. on Acoustics, Speech, and Signal Processing, ICASSP 1997*, volume 3, pages 1997–2000. IEEE, 1997.
6. R. Lidl and H. Niederreiter. *Finite Fields.* Addison-Wesley, Reading, MA, 1983.
7. F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error Correcting Codes.* Elsevier Science B. V., Amsterdam, 1977.
8. A. J. Menezes, editor. *Applications of Finite Fields.* Kluwer Academic Press, 1993.
9. F. Pichler and H. Schwärtzel. *CAST: Computerunterstützte Systemtheorie; Aufbau und Anwendungen von Systemtheorie-Methodenbanken.* Springer-Verlag, 1990.
10. De Man Rabaey. Computer aided design of digital signal processing systems. *Proc. of IEEE*, pages 134–137, 1987.