

Galois Theory and Wavelet Transforms

Andreas Klappenecker¹ and Thomas Beth

Universität Karlsruhe, Institut für Algorithmen und Kognitive Systeme,
D-76 128 Karlsruhe, Germany, e-mail: klappi@ira.uka.de

Abstract — Computing the Fast Wavelet Transform of rational input sequences using algebraic scaling coefficients affords only a finite extension field K over \mathbb{Q} rather than the field of complex numbers. We use Galois theoretic methods to study this extension field.

I. INTRODUCTION

Orthonormal wavelet bases are usually constructed by the tools of multiresolution analysis, cf. [2]. At the heart of a multiresolution analysis stands a so-called *scaling function* φ . This scaling function satisfies a dilation equation, which can be written in Fourier space as $\hat{\varphi}(\omega) = m_0(\omega/2) \hat{\varphi}(\omega/2)$, where $m_0(\omega) = \sum h_n e^{-in\omega}$. In what follows, we assume compactly supported scaling functions with algebraic coefficients h_n , i.e., every coefficient h_n is element of an algebraic number field. From the multiresolution analysis axioms one derives the simple relation $|m_0(\omega)|^2 + |m_0(\omega + \pi)|^2 = 1$. Therefore, it is convenient to construct the transfer function $m_0(\omega)$ from its squared modulus $|m_0(\omega)|^2$ with the help of the following:

Theorem 1 (Fejér-Riesz) *Let $A(\omega)$ be a real nonnegative even trigonometric polynomial*

$$A(\omega) = \sum_{m=0}^M a_m \cos m\omega, \quad \text{with } a_m \in \mathbb{R}.$$

Then it is possible to construct a real trigonometric polynomial $B(\omega) = \sum_{m=0}^M b_m e^{im\omega}$, with $b_m \in \mathbb{R}$, of the same order M , such that $A(\omega) = |B(\omega)|^2$.

II. ALGEBRAIC SCALING COEFFICIENTS

In the case of trigonometric polynomials $|m_0(\omega)|^2$ with algebraic coefficients, the following theorem ensures that $m_0(\omega)$ has algebraic coefficients, too.

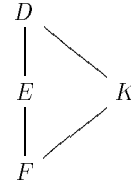
Theorem 2 ([1]) *The coefficients a_m of the trigonometric polynomial $A(\omega)$ are algebraic if and only if the coefficients b_m of $B(\omega)$ are also algebraic.*

Theorem 2 can be proved by extending DAUBECHIES' proof of Theorem 1 [2], but using minimal splitting fields instead of the algebraically closed field \mathbb{C} . The main steps in the proof can be sketched as follows:

1. Rewrite the trigonometric polynomial $A(\omega)$ as a polynomial p_A in $\cos \omega$. The polynomial p_A can be factorized over a minimal splitting field E as $\text{lc}(p_A) \prod_{n=1}^M (c - c_j)$. Here, $\text{lc}(\cdot)$ denotes the leading coefficient.
2. Build a self-reciprocal polynomial P_A by substituting $c := (z + z^{-1})/2$ in $p_A(c)$ and multiplying with z^M . Therefore, the resulting polynomial is of the following form $P_A(\omega) = \text{lc}(p_A) \prod_{n=1}^M (1/2 - c_j z + 1/2 z^2)$. Factorize $P_A(z)$ in a minimal splitting field D .

3. Choose a zero z_j from every factor $(1/2 - c_j z + 1/2 z^2)$, $1 \leq j \leq M$, and build a new trigonometric polynomial $P_B(z) = \nu \prod_{j=1}^M (z - z_j)$, where $\nu \in K$ is just a normalization factor. The trigonometric polynomial $B(\omega)$ is obtained from P_B by $B(\omega) = P_B(e^{-i\omega})$. Thus, the field K is generated by elementary symmetric functions of the zeros z_j .

Hence, from a field theoretic point of view the situation can be summarized by the following diagram:



III. GALOIS THEORETIC ANALYSIS

From the very construction, we see that the fields E and D are Galois extensions over F . We discuss some of their properties through a sequence of lemmas and corollaries.

Lemma 1 *The Galois group $\text{Gal}(D/E)$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^m$, with $m \leq M$.*

From this observation we easily derive the following result about the structure of the Galois group.

Lemma 2 *The Galois group $\text{Gal}(D/F)$ is the extension of the elementary abelian normal 2-subgroup $\text{Gal}(D/E)$ by the group $\text{Gal}(E/F)$.*

As a consequence, we get an upper bound for the order of the Galois group $\text{Gal}(D/F)$, which is helpful in the estimation of this group.

Corollary 3 *We have the following upper bound for the field degree of D/F :*

$$[D : F] \leq 2^M \cdot |\text{Gal}(E/F)| \leq M! \cdot 2^M.$$

By carefully studying the structure of K , we obtain

Lemma 4 *The field D is generated by the composition field EK .*

Corollary 5 *The field degree $[K : F]$ is at least $|\text{Gal}(D/E)|$.*

The close connection between the fields D and K can be exemplified by the following

Lemma 6 *If the field degree D/E is maximal, i.e., $[D : E] = 2^M$, then the Galois closure of K is the field D .*

REFERENCES

- [1] T. Beth, A. Klappenecker, and A. Nückel. Construction of algebraic wavelet coefficients. *Proc. ISITA '94, Sydney*, 1994.
- [2] I. Daubechies. *Ten Lectures on Wavelets*. CBMS-NSF Reg. Conf. Series Appl. Math. SIAM, 1992.

¹This work was supported by DFG under project Be 877/6-2.