Universität Paderborn
Fakultät EIM, Institut für Mathematik

Fourier Analysis for Polynomials over Finite Fields

Kathrin Tofall

Diplomarbeit im Fach Mathematik

Paderborn, 28.01.2005

Betreuer:
Prof. Dr. Joachim von zur Gathen

FOURIER ANALYSIS FOR POLYNOMIALS OVER FINITE FIELDS

Kathrin Tofall

11th May 2005

Contents

1 Introduction

1.1 Motivation

In this Diplomarbeit we investigate the nature of three Boolean functions defined over the natural numbers and polynomials over finite fields, namely coprimality, irreducibility and squarefreeness. Among many other things, these functions play prominent roles in modern cryptography. Since all three functions are defined with respect to divisibility, they are very closely related.

The coprimality function can be computed very efficiently for polynomials over both finite fields and integers, because of course it suffices to compute the greatest common divisor of the two inputs. This can be done using one of the oldest and most famous algorithms, attributed to Euclid (see e.g. von zur Gathen & Gerhard 1999). Deciding irreducibility for polynomials over finite fields is easy, because they can even be factored in polynomial time. Efficient probabilistic primality tests for integers have been known for some time, the most famous being the Miller-Rabin test (see Miller 1975; Rabin 1980). One of the newest famous algorithms by Agrawal, Kayal & Saxena (2002) (AKS) even decides the language primality in determistic polynomial time. The Boolean function squarefreeness is less famous than its two companions, but it has also attracted much interest. At first it might come as a surprise that squarefreeness behaves very differently for polynomials and integers. It is a mere textbook exercise to prove that the decision problem squarefreeness for polynomials over finite fields can be reduced efficiently to coprimality (see Section 5.4). However, deciding squarefreeness for integers is thought to be hard. This incongruity stems from the underlying problem of factoring, which is not a decision problem but a master key for all three of our Boolean functions. While polynomials over finite fields can be factored efficiently (once again see von zur Gathen & Gerhard (1999) and also Bonorden *et al.* (2001)), a polynomial-time algorithm for factoring integers remains one of the holy grails of mathematics. The inability to factor integers already frustrated Carl Friedrich Gauß (see Gauß 1801) and one of the ground-breaking steps towards theoretical computer science was Kurt Gödel's hypothesis that deciding primality of a number N might be done in $\log N$ or $\log^2 N$ steps (we would nowadays say in polynomial time) in contrast to taking N steps (exponential time) to try all potential divisors. These ideas, taken from a letter to John von Neumann (see Sipser 1992), lead to the notion of both complexity classes and decision problems.

In order to investigate the complexity of the three considered Boolean functions both for polynomials over finite fields and integers, we will apply one

of the most useful tools of applied mathematics, the Fourier transform, which may seem a bit odd to begin with. Historically, the Fourier transform was developed to study problems taken directly from physics. For details and even older applications see Section 2.1. In more modern times the Fourier transform has had many applications in efficient algorithms and most notably as the basis for compression of all kinds of data. The Fast Fourier Transform (FFT) is the theoretical foundation for the JPEG and the various MPEG codecs (see von zur Gathen & Gerhard 1999).

The Fourier transform is a tool to represent a given function as the sum of an orthonormal system of certain basic functions, historically sines and cosines with ever smaller periods. We will look at systematic generalizations of this concept and then apply them to our problems. It turns out that the so-called Fourier coefficients representing a given function can be computed with formulae similar to the continuous case. Furthermore, for our functions asymptotically only a constant number of the coefficients have significant impact on the representing sum (i.e. the function could be compressed heavily with relatively little loss of quality). Moreover, as our input sizes grow, the absolutely largest coefficients converge on certain fixed values. If our ground field for polynomials is not just the binary field, we even obtain complex coefficients and highly structured plots of coefficients that inspire the imagination.

1.2 Contents of the Sections

Section 2 contains a brief history of the Fourier transform leading into the modern age. Obviously, no such section can ever be complete, but there are many references for further reading. Furthermore, it does contain all major developments and should provide a good overview in a condensed form. The section also includes the construction of the well-known used Fourier transform for Boolean functions over $\mathbb{F}_2^n$, which is also used in the main source of this Diplomarbeit, Allender, Bernasconi, Damm, von zur Gathen, Saks & Shparlinski (2003), as well as in previous publications on this topic. The next subsection contains a discussion on generalizations to arbitrary finite fields. Finally, we prove the so-called Parseval or Plancherel identity.

Section 3 is very short. There are only a few definitions and corollaries that will be necessary or at least useful for some of the following sections.

Using Maple, we conducted extensive computations of Fourier coefficients for our three Boolean functions over the ground field $\mathbb{F}_2$. Section 4 describes the results of these experiments and contains plots of the coefficients. Looking at the values and pictures, it is quite obvious that for the squarefreeness and

the coprimality function there are four coefficients that stand out significantly from the others. The results for the irreducibility function cannot very well be seen in the plots.

In Section 5 we provide formulae and give proofs for the four absolutely largest coefficients for squarefreeness and coprimality of binary polynomials. It is then easy to see that all these coefficients converge on fixed values as the input size tends to infinity, and we also receive explicit, exponentially small error terms. For the highest and lowest order Fourier coefficient the limits were already found by Allender *et al.* (2003). Finally, there is a subsection about the polynomial time reducibility of squarefreeness to coprimality for polynomials over finite fields.

Section 6 is analogous to Section 4, but now we look at functions over the finite fields $\mathbb{F}_3$, $\mathbb{F}_4$, $\mathbb{F}_5$ and $\mathbb{F}_7$. It turns out that if the ground field is not a prime field, then there are several more or less natural possibilities for a Fourier transform. Therefore this section commences with a detailed consideration of the Fourier transform for the prime base field $\mathbb{F}_3$. After that we look at a few computations we did over $\mathbb{F}_5$ and $\mathbb{F}_7$. Finally we consider the smallest non-prime field $\mathbb{F}_4$. Already for the smallest of non-prime fields there are several possible Fourier transformations. Most notably, two general possibilities are identifying $\mathbb{F}_4$ with $\mathbb{F}_2^2$ and using the addition in $\mathbb{F}_4$, which gives us the group $(\mathbb{Z}_2)^2$ versus re-doing our construction for $\mathbb{F}_4$ to arrive at a Fourier transform in its own right. This second possibility, however, yields an ambiguity that gets worse as the degree of the field extension grows.

In Section 7 we give proofs for the lowest order Fourier coefficient over finite fields for all three of our Boolean functions. This section also includes information about the number of squarefree and irreducible polynomials, as well as the number of coprime pairs of polynomials, over finite fields.

Section 8 and Section 9 contain the results of our computations of Fourier coefficients for our three Boolean functions defined now over the natural numbers, as well as the proofs for the extreme coefficients of all three functions and the necessary estimates of the frequency of squarefree and irreducible numbers and of pairs of coprime natural numbers.

In Section 10 we give a brief introduction to some important computational models corresponding to complexity measures and state a few well-known relations between them. After that we plug the results of this work into these theorems, obtaining some lower bounds for the complexity of our three decision problems. Finally we give an overview over open questions and possible directions for future work.

1.3 Originality of Some Results

To our knowledge, this Diplomarbeit contains some results that were not previously published. This includes our generalizations of the Fourier transform over the binary field to larger finite fields. Furthermore, we give asymptotic values with explicit error bounds for the four absolutely largest Fourier coefficients for the squarefreefress and coprimality functions for binary polynomials. Previously for each function the limits were only known for two of the coefficients and an (unexplicit) error bound for only one of those. Considering arbitrary finite fields we found formulae, limits and error bounds for the lowest order Fourier coefficients for all considered Boolean functions. For the irreducibility function this coefficient converges on 1 so that all the others must vanish asymptotically. During these proofs we saw the necessity to compute the number of coprime polynomials over a finite field, where the maximum degree of the two polynomials is fixed. Finally, all our formulae, limits and explicit error bounds for Fourier coefficients for functions defined over the integers seem to be original to this work.

2 Fourier Transform over Finite Fields

2.1 A Short History of the Fourier Transform

The basic idea of the Fourier transformation is that "any" periodic function can be written as a trigonometric sum, that is a sum or a series of sines and cosines with a common period. This has applications in physics, astronomy, biology, or whenever periodic phenomena are to be described. A primitive kind of Fourier transform was already used in Babylonian astronomy for predicting movements of the moon. The Babylonians arrived at a relatively high level of numerical lunar theory and had empirical schemes for predicting lunar phases. However, until now the Babylonian methods are only partially reconstructed. For more detailed information see the recent paper of Brack-Bernsen & Brack (2004) or Neugebauer (1975) for more historical background. In more modern times the Fourier transform underwent the following developments:

1747 d'Alembert (1747) started the discussion of the oscillations of a violin string with his paper "Recherches sur la courbe que forme une corde tendue mise en vibrations". Of course, d'Alembert was not the first person who thought about this problem, but he found the equation of the oscillating string. A complete description and elementary derivation can be found in Heuser (1995a).

1748 Euler (1748) published a new representation of d'Alemberts solutions in his work "Sur la vibration des cordes".

However, d'Alembert did not agree with Euler's arguments and two further mathematicans, namely Daniel Bernoulli and Lagrange, entered the scene and engaged in this problem. The four of them never reached any agreement. A main problem in this discussion was that there were different understandings of the word "function". The whole "quarreling" is accurately described in Heuser (1995a) and in Riemann's Habilitation (Riemann 1867). The next step was done by Euler, but his results remained unknown for some time (e.g. Riemann did not know about this work of Euler's):

1777 Thanks to the orthogonality of the trigonometric functions, Euler discovered an easy way to compute the values, that are nowadays known as *Fourier coefficients*: the Euler-Fourier formulae in his work "Disquisitio ulterior super seriebus secundum multipla cuiusdam anguli progredientibus". Admittedly, Euler considered only series of cosines. But the step to general trigonometric series is not so wide. This work was published post mortem in Euler (1798).

1799 Parseval wrote his "Mémoire sur les séries et sur l'intégration complète d'une équation aux différences partielles linéaires du second ordre, à coefficiens constans". This work contains the result which is now known as Parseval's identity. He gave an improved version in 1801 in the article "Intégration générale et complète des équations de la propagation du son, l'air étant considéré avec les trois dimensions". Although his method involves trigonometric series, it seems that he never tried to find a general expression for the coefficients and so he did not contribute directly to the theory of Fourier series. Parseval's results were not published until 1806 when all five papers he ever wrote were published in a single volume by the Académie des Sciences, the two interesting articles being Parseval (1806a,b).

1807 Fourier rediscovered the so-called Euler-Fourier formulae and wrote his "Mémoire sur la propagation de la Chaleur dans les corps solides" (with many errors in it). This work was presented in 1807 and a commission consisting of Lagrange, Laplace, Monge and Lacroix were to examine it. An abstract of this work can be found in Fourier (1808). The article itself disappeared for a while. The whole work was first presented in Grattan-Guinness (1972). But Fourier also wrote a revised and extended version in 1811. This paper was first published in two parts after the publication of his book, albeit unchanged in two parts (Fourier 1824, 1826). (More about the life and work of Fourier can be found in Grattan-Guinness (1969, 1972).)

1822 Fourier's book "Théorie analytique de la chaleur" (Fourier 1822) appeared.

Although Fourier really tried he could not give a proof for the claim that any piecewise smooth function can be expanded into a trigonometric sum.

1829 Dirichlet (1829) was the first to prove the possibility of expanding a function in a Fourier series under mild conditions in the article "Sur la convergence des séries trigonométriques qui servent à représenter une fonction arbitraire entre des limites données".

1854 Riemann finished a part of his Habilitation, namely "Ueber die Darstellbarkeit einer Function durch eine trigonometrische Reihe." (published in Riemann 1867) where he introduced what is now called the Riemann integral. This work was first published post mortem by Richard Dedekind in 1867.

1902 Lebesgue gave the definition of the so-called Lebesgue integral generalizing the notion of the Riemann integral in "Sur une généralisation de l'intégrale définie" (Lebesgue 1901). The full account of his work appeared in Lebesgue's doctoral thesis "Intégrale, longueur, aire" (1902). He gave an improvement in Lebesgue (1903). Later he published two books containing much of his work: "Leçons sur l'intégration et la recherche des fonctions primitives" (Lebesgue 1904) and "Leçons sur les séries trigonométriques" (1906).

1907 Riesz and Fischer each found a converse to Parseval's identity. Riesz published "Sur les systèmes orthogonaux de fonctions" (Riesz 1907a) and "Sur les systèmes orthogonaux de fonctions et l'équation de Fredholm" (Riesz 1907b). Fischer wrote the two articles "Sur la convergence en moyenne" (Fischer 1907b) and "Applications d'un théorème sur la convergence en moyenne" (Fischer 1907a). The theorem they found is nowadays called the "Riesz-Fischer theorem".

1910 Plancherel gave an analogue but also a generalization of the Parseval identity in his "Contribution à l'étude de la représentation d'une fonction arbitraire par des intégrales définies" (Plancherel 1910).

For our purposes we need Fourier series on groups. There are a lot of results, of which we mention only one:

1934 The first part of von Neumann's (and Bochner's) "Almost periodic functions in a group, I" was published (von Neumann 1934). The second part was released in the following year under the title "Almost periodic functions in groups, II" (Bochner & von Neumann 1935). In the first publication the theory of almost periodic functions is extended to arbitrary groups. In the second publication the existence and uniqueness of a Fourier expansion for any almost periodic function is deduced. More information about the mathematicians and their work in that area before von Neumann's time is also given in the mentioned papers.

Of course, this is not a complete list of all that happened in the history of the Fourier transformation. For more historical information especially for the time before Riemann see the already quoted Riemann (1867). Information about more modern works can be found in Coppel (1969). More mathematical information starting with Lebesgue's theory is contained in e.g. Dym & McKean (1972). For the developement leading up to Lebesgue's theory see Heuser (1995a,b). Another good source of (historical and mathematical) information is Hobson (1926).

2.2 Fourier Transformation on Finite Abelian Groups

A generalized Fourier transformation is a decomposition of a function in a system of basic functions. Every function f can be described by a linear combination of some basic functions χ, where we denote the coefficients by $\widehat{f}(\chi)$:

$$f = \sum_{\chi} \widehat{f}(\chi)\chi.$$

The coefficients represent the correlation between the function and the basic functions. A determination of the coefficients is only feasible if our basic system is orthogonal and becomes easier if we work with an orthonormal system. This means

$$\langle \chi_1 \ , \ \chi_2 \rangle = \begin{cases} 1, & \text{if } \chi_1 = \chi_2, \\ 0, & \text{otherwise.} \end{cases}$$

For our purposes we need Fourier transforms on finite Abelian groups. We will proceed step by step following Dym & McKean (1972), Chapter 4.5.

Our goal is to expand functions into their Fourier series. For our purposes $f\colon G \to \mathbb{C}$ is a function mapping from the given group into the complex numbers and the basic functions $\chi\colon G \to \mathbb{C}^\times$ are group homomorphisms:

Definition 2.1. *For a finite Abelian group G we define the* dual group

$$\widehat{G} = \{\chi\colon G \longrightarrow \mathbb{C}_1\colon \chi \textit{ is a group homomorphism}\},$$

where

$$\mathbb{C}_1 = \{z \in \mathbb{C}\colon |z| = 1\}$$

is the unit circle on which multiplication provides a group structure. An element $\chi \in \widehat{G}$ is called a character *of G. Since χ is a homomorphism, we have*

$$\chi(1) = 1 \textit{ and } \forall g_1, g_2 \in G\colon \chi(g_1 g_2) = \chi(g_1)\chi(g_2).$$

Now let us assume that G is a finite Abelian group. The structure theorem for finite Abelian groups says that each such group is isomorphic to $\mathbb{Z}^+_{m_1} \times \ldots \times \mathbb{Z}^+_{m_n}$ for some integers $m_1, \ldots, m_n$. So for our purposes we will without further loss of generality assume that $G = \mathbb{Z}^+_{m_1} \times \ldots \times \mathbb{Z}^+_{m_n}$. We still use multiplication for the group operation on G and consequently denote the neutral element $(0, \ldots, 0)$ by 1. There are $\#G$ characters χ or in other words $\#\widehat{G} = \#G$, which we will show in the following. But first we will take a closer look at the characters. The following useful facts we have adapted from Lidl & Niederreiter (1983), Chapter 5.

For the constant character χ_0 with $\chi_0(g) = 1$ we trivially have $\sum_{g \in G} \chi_0(g) = \#G$. For all other characters this sum equals 0:

THEOREM 2.2. *If χ is a nontrivial character of the finite Abelian group G, then*

$$\sum_{g\in G}\chi(g)=0. \tag{2.3}$$

Dually, if $g\in G$ with $g\neq 1_G$, then

$$\sum_{\chi\in\widehat{G}}\chi(g)=0. \tag{2.4}$$

This elegant proof also stems from Lidl & Niederreiter (1983):

PROOF. Since χ is nontrivial, there exists an $h\in G$ with $\chi(h)\neq 1$. Then

$$\chi(h)\sum_{g\in G}\chi(g)=\sum_{g\in G}\chi(hg)=\sum_{g\in G}\chi(g),$$

because, if g runs through G, so does hg. Thus we have

$$\Big(\chi(h)-1\Big)\sum_{g\in G}\chi(g)=0,$$

which already implies (2.3). For (2.4) we note that the function $\widehat{g}$ defined by $\widehat{g}(\chi)=\chi(g)$ for $\chi\in\widehat{G}$ is a character of the finite Abelian group $\widehat{G}$. This character is nontrivial since there exists a $\chi\in\widehat{G}$ with $\chi(g)\neq\chi(1_G)=1$. Therefore, applying (2.3) to the group $\widehat{G}$ we get

$$\sum_{\chi\in\widehat{G}}\chi(g)=\sum_{\chi\in\widehat{G}}\widehat{g}(\chi)=0. \qquad \square$$

THEOREM 2.5. *The number of characters of a finite Abelian group G is equal to $\#G$.*

PROOF. This follows from (2.3) and (2.4)

$$\#\widehat{G}=\sum_{g\in G}\sum_{\chi\in\widehat{G}}\chi(g)=\sum_{\chi\in\widehat{G}}\sum_{g\in G}\chi(g)=\#G. \qquad \square$$

However, we can prove a somewhat stronger result:

THEOREM 2.6. *The group $G = \mathbb{Z}^+_{m_1} \times \ldots \times \mathbb{Z}^+_{m_n}$ is isomorphic to its dual group via the isomorphism $G \to \widehat{G}$, $\underline{\lambda} \mapsto \chi_{\underline{\lambda}}$, where $\chi_{\underline{\lambda}}(e_j) = e^{2\pi i \lambda_j / m_j}$ for all $j \in \{1, \ldots, n\}$.*

PROOF. Any element $g \in G$ can be written as

$$g = k_1 e_1 + \ldots + k_n e_n = (k_1, \ldots, k_n),$$

where $e_j = [0, \ldots, 0, \underset{\uparrow}{1}, 0, \ldots, 0]$ and $k_1, \ldots, k_n \in \mathbb{N}$. Then for each j we have

$$\chi(e_j)^{m_j} = \chi(e_j^{m_j}) = \chi(1) = 1.$$

Thus $\chi(e_j)$ is an m_jth root of unity and there exist $\lambda_j, 0 \leq \lambda_j < m_j$, such that

$$\chi(e_j) = e^{2\pi i \lambda_j / m_j}$$

and χ is determined uniquely by $(\lambda_1, \ldots, \lambda_n) \in G$. □

Furthermore we define an appropriate inner product of complex-valued functions:

DEFINITION 2.7 (Inner product). *The* inner product *of two complex-valued functions $\varphi, \psi \colon G \to \mathbb{C}$ is*

$$\langle \varphi \ , \ \psi \rangle = \frac{1}{\#G} \sum_{g \in G} \varphi(g) \overline{\psi(g)},$$

where $\overline{x}$ denotes the complex conjugate of x.

LEMMA 2.8. *The inner product of two characters $\chi_1, \chi_2 \in \widehat{G}$ is*

$$\langle \chi_1 \ , \ \chi_2 \rangle = \begin{cases} 1, & \text{if } \chi_1 = \chi_2, \\ 0, & \text{otherwise.} \end{cases}$$

PROOF. Inserting the definition we get

$$\langle \chi_1 \ , \ \chi_2 \rangle = \frac{1}{\#G} \sum_{g \in G} \chi_1(g) \overline{\chi_2(g)} = \frac{1}{\#G} \sum_{g \in G} \frac{\chi_1(g)}{\chi_2(g)}.$$

For the case $\chi_1 = \chi_2$ we get simply:

$$\frac{1}{\#G} \sum_{g \in G} 1 = 1.$$

For the case $\chi_1 \neq \chi_2$ we get a nontrivial character $\chi = \frac{\chi_1}{\chi_2}$ and therefore

$$\frac{1}{\#G} \sum_{g \in G} \chi(g) \overset{(2.3)}{=} 0. \qquad \square$$

This means that we have an orthonormal system. It follows that for all χ_0 we have $\langle f \ , \ \chi_0 \rangle = \sum_\chi \widehat{f}(\chi) \langle \chi \ , \ \chi_0 \rangle = \widehat{f}(\chi_0)$. Now we look at the dual group $\widehat{\widehat{G}}$ of $\widehat{G}$:

$$\widehat{\widehat{G}} = \{\psi \colon \widehat{G} \longrightarrow \mathbb{C} \text{ is group homomorphism } \}$$

We can map any element $g \in G$ to a character $\widehat{\widehat{g}}$ of $\widehat{G}$ by letting

$$\widehat{\widehat{g}}(\chi) \equiv \chi(g).$$

This defines an embedding of G into its double dual $\widehat{\widehat{G}}$ for any group G. Since G is isomorphic to $\widehat{G}$, distinct $g \in G$ give rise to distinct elements in $\widehat{\widehat{G}}$. Applying Lemma 2.8 we arrive at:

COROLLARY 2.9. *For two elements $g_1, g_2 \in G$ we have*

$$\left\langle \widehat{\widehat{g}}_1 \ , \ \widehat{\widehat{g}}_2 \right\rangle = \frac{1}{\#\widehat{G}} \sum_{\psi \in \widehat{G}} \psi(g_1)\overline{\psi(g_2)} = \begin{cases} 1, & \text{if } g_1 = g_2, \\ 0, & \text{otherwise.} \end{cases}$$

$\square$

Now, we are ready for the important theorem due to Plancherel (1910):

THEOREM 2.10 (Plancherel). *Any function $f \colon G \to \mathbb{C}$ on G can be expanded into a Fourier series*

$$f = \sum_{\chi \in \widehat{G}} \widehat{f}(\chi)\chi \tag{2.11}$$

with coefficients

$$\widehat{f}(\chi) = \langle f \ , \ \chi \rangle = \#G^{-1} \sum_{g \in G} f(g)\overline{\chi(g)}.$$

Furthermore, the following identity holds:

$$||f||^2 = \sum_{g \in G} |f(g)|^2 = \#G \sum_{\chi \in \widehat{G}} |\widehat{f}(\chi)|^2 = \#G \cdot ||\widehat{f}||^2. \tag{2.12}$$

PROOF. First we prove (2.11) by insertion of an arbitrary g_0:

$$\begin{aligned}
\sum_{\chi\in\widehat{G}} \widehat{f}(\chi)\chi(g_0) &= \sum_{\chi\in\widehat{G}} \chi(g_0)\frac{1}{\#G}\sum_{g\in G} f(g)\overline{\chi(g)} \\
&= \sum_{g\in G} f(g)\frac{1}{\#G}\sum_{\chi\in\widehat{G}} \chi(g_0)\overline{\chi(g)} \\
&\overset{(2.9)}{=} f(g_0)\frac{1}{\#G}\sum_{\chi\in\widehat{G}} \chi(g_0)\overline{\chi(g_0)} \\
&= f(g_0).
\end{aligned}$$

Now we proceed with the proof of (2.12). Only the equation in the middle needs to be proven, because the other two equalities stem from the definition of the norm:

$$\begin{aligned}
\#G||\widehat{f}||^2 &= \#G\sum_{\chi\in\widehat{G}} |\widehat{f}(\chi)|^2 \\
&= \#G\sum_{\chi\in\widehat{G}} \widehat{f}(\chi)\overline{\widehat{f}(\chi)} \\
&= \#G\sum_{\chi\in\widehat{G}} \left(\frac{1}{\#G}\sum_{g_1\in G} f(g_1)\overline{\chi(g_1)}\right)\left(\frac{1}{\#G}\sum_{g_2\in G} \overline{f(g_2)}\chi(g_2)\right) \\
&= \frac{1}{\#G}\sum_{g_1,g_2\in G} f(g_1)\overline{f(g_2)}\sum_{\chi\in\widehat{G}} \overline{\chi(g_1)}\chi(g_2) \\
&\overset{(2.9)}{=} \sum_{g\in G} f(g)\overline{f(g)} \\
&= \sum_{g\in G} |f(g)|^2 = ||f||^2.
\end{aligned}$$

So we have proven (2.12). □

So for any function $f\colon G\to\mathbb{C}$ we obtain a Fourier transform $\widehat{f}\colon \widehat{G}\to\mathbb{C}$. Note that this transformation is linear.

2.3 A Fourier Transformation for Boolean Functions over $\mathbb{F}_2$

Now we will take a look at the well-known Fourier transformation for Boolean functions over $\mathbb{F}_2$ and how it comes about.

There are a lot of works containing the Fourier transform of Boolean functions over $\mathbb{F}_2$. To our knowledge Kahn *et al.* (1988) were the first to use a Fourier transform to prove results in theoretical computer science. They used it to investigate the sensitivity of Boolean functions.

A Boolean function is any function $\varphi\colon M \to \mathbb{B}$, where M is an arbitrary set and $\mathbb{B}$ has two elements. We interpret π as a predicate that states the truth or falsity of a property for each element of its domain. We want to calculate with these properties and therefore we embed $\mathbb{B}$ into $\mathbb{C}$. Normally, $\mathbb{B}$ also is interpreted as the set $\{0,1\}$ of possible states of a bit and thus we do so. Typically, M has no natural group structure. For example $\mathbb{B}^n$ with $\mathbb{B} = \{0,1\}$ has an obvious group structure, the set $\mathcal{M}(n) = \{p \in \mathbb{F}_p[x] \mid p(0) = 1, \deg(p) \leq n\}$ has not. Later on we will identify the elements of $\mathbb{B}^n$ (or $\mathbb{F}_q^n$, respectively) with polynomials over $\mathbb{F}_2$ (or $\mathbb{F}_q$, respectively) with constant coefficient 1 (this case is already mentioned as set M above) or corresponding to the binary representation of positive integers. The predicate we use will map from $\mathbb{B}^n$ to $\{+1,-1\}$. Thus instead of looking at φ we will look at the following function:

$$\psi\colon \begin{array}{ccc} G & \longrightarrow & \{+1,-1\}, \\ g & \longmapsto & (-1)^{\varphi(g)}. \end{array}$$

To arrive at the usual transformation we have to use the right quantities. For the group G we take $G = (\mathbb{B}^n, +)$ with $\#G = 2^n$ and interpret the elements of G as mentioned above. To simplify matters we retain the notion $\mathbb{B}^n$ ($\mathbb{F}_2^n$ respectivly, and so on for $(\mathbb{F}_p^e)^n$ or $\mathbb{F}_q^n$). In accordance with the literature concerning the topic of this Diplomarbeit (Allender *et al.* 2003) the group elements are denoted by u and the binary field $\mathbb{F}_2$ by $\mathbb{B}$. Plugging these into Theorem 2.10 yields the following coefficients:

$$\widehat{\psi}(\chi) = \frac{1}{2^n} \sum_{u \in \mathbb{B}^n} \psi(u)\overline{\chi(u)}. \tag{2.13}$$

To arrive at a notation similar to the used one in Allender *et al.* (2003), we establish another notation:

$$\widetilde{\varphi} = \widehat{\psi} = \widehat{(-1)^{\varphi}} = \widehat{1 - 2\varphi} = \widehat{1} - 2\widehat{\varphi},$$

where

$$\widehat{1}(u) = \begin{cases} 1, & \text{if } u = 0, \\ 0, & \text{otherwise.} \end{cases}$$

Then we have

$$\widetilde{\varphi}(\chi) = \frac{1}{2^n} \sum_{u \in \mathbb{B}^n} (-1)^{\varphi(u)} \overline{\chi(u)}. \tag{2.14}$$

Now, we will take a closer look at the characters $\chi \colon \mathbb{B}^n \to \mathbb{C}_1$. For this case we do an exemplary repetition of the proof of Theorem 2.6.

We already know that $\#\widehat{G} = \#G$ and thus there are 2^n characters. For every $w \in \mathbb{B}^n$ we consider

$$\chi_w \colon \begin{array}{ccc} \mathbb{B}^n & \longrightarrow & \mathbb{C}_1, \\ u & \longmapsto & (-1)^{w^T u}, \end{array}$$

where $w^T u$ is the inner product of the two vectors w and u. Obviously this yields 2^n distinct group homomorphisms from $(\mathbb{B}^n, +)$ to $(\mathbb{C}_1, \cdot)$. Applying χ_w to the sum of $u^{(1)}, u^{(2)} \in \mathbb{B}^n$ yields:

$$\begin{aligned} \chi_w(u^{(1)} + u^{(2)}) &= (-1)^{w^T(u^{(1)}+u^{(2)})} = (-1)^{w^T u^{(1)} + w^T u^{(2)}} \\ &= (-1)^{w^T u^{(1)}} \cdot (-1)^{w^T u^{(2)}} = \chi_w(u^{(1)}) \cdot \chi_w(u^{(2)}). \end{aligned}$$

Furthermore, if we take distinct $w^{(1)}, w^{(2)} \in \mathbb{B}^n$, then there exists an index j with

$$w_j^{(1)} \neq w_j^{(2)} \text{ and } \chi_{w^{(1)}}(e_j) \neq \chi_{w^{(2)}}(e_j)$$

and therefore $\chi_{w^{(1)}} \neq \chi_{w^{(2)}}$. Instead of χ_w we will write w to simplify the notation. Substitution of $\overline{\chi(u)}$ by $(-1)^{w^T u}$ in (2.14) yields:

$$\widetilde{\varphi}(w) = \frac{1}{2^n} \sum_{u \in \mathbb{B}^n} (-1)^{\varphi(u) + w^T u} = \frac{1}{2^n} \sum_{u \in \mathbb{B}^n} (-1)^{\varphi(u) + \sum_j u_j w_j}. \tag{2.15}$$

By Theorem 2.10 we now can write $\varphi(x)$ as follows:

$$\begin{aligned} (-1)^{\varphi(x)} &= \sum_{w \in \mathbb{B}^n} \widetilde{\varphi}(w) (-1)^{w^T x} \\ &= \sum_{w \in \mathbb{B}^n} \left(\frac{1}{2^n} \sum_{u \in \mathbb{B}^n} (-1)^{\varphi(u) + \sum_j u_j w_j} \right) (-1)^{w^T x}. \end{aligned}$$

2.4 Generalizations of this Fourier Transform

In the previous section we have seen what the Fourier coefficients for Boolean functions over $\mathbb{F}_2$ are. Now, we want to make similar transformations over arbitrary finite fields. As far as we know these results were never published before.

First we look again at the general formula for Fourier coefficients on commutative groups (see Theorem 2.10):

$$\widehat{f}(\chi) = \#G^{-1} \langle f \ , \ \chi \rangle = \#G^{-1} \sum_G f(g)\overline{\chi(g)}.$$

Analogously to the way we obtained the formula over $\mathbb{F}_2$ we get one over $\mathbb{F}_p$, $p \in \mathbb{P}$. We generalize the characters

$$\chi_w \colon \begin{array}{ccc} \mathbb{F}_p^n & \longrightarrow & \mathbb{C}_1, \\ u & \longmapsto & \zeta^{w^T u}, \end{array}$$

where ζ is a primitve pth root of unity. We start once more with a Boolean function, as in the previous section. There are two natural ways to generalize our construction for $\mathbb{F}_2$. On the one hand we can still use a function ψ that maps to $\{-1, 1\}$, but we could also have it map to $\{\zeta, 1\}$. The alternatives are identical if $p = 2$ and $\zeta = -1$. So for the second alternative we let

$$\psi \colon \begin{array}{ccc} \mathbb{F}_p^n & \longrightarrow & \{1, \zeta\}, \\ x & \longmapsto & \zeta^{\varphi(x)}. \end{array}$$

With our notation we then get the following two possibilities for a Fourier transformation over $\mathbb{F}_p$:

$$\check{\varphi}(w) = \frac{1}{p^n} \sum_{u \in \mathbb{F}_p^n} \zeta^{\varphi(u) - \sum_j u_j w_j} \tag{2.16}$$

and

$$\widetilde{\varphi}(w) = \frac{1}{p^n} \sum_{u \in \mathbb{F}_p^n} (-1)^{\varphi(u)} \cdot \zeta^{-\sum_j u_j w_j}. \tag{2.17}$$

Note that the complex conjugation in the inner product turns to a negative sign in the exponent of ζ. Of course there are more possibilities for a correct Fourier transformation. Already over $\mathbb{F}_2$ we could also have chosen another

correct transformation, for example we could drop the conversion of the Boolean function:

$$\widehat{\varphi}(w) = \frac{1}{p^n} \sum_{u \in \mathbb{F}_p^n} \varphi(u) \cdot \zeta^{-\sum_j u_j w_j}. \tag{2.18}$$

But first we will look at (2.16) and (2.17). These two equations are equivalent in a sense since

$$\zeta^{\varphi(u)} = a \cdot (-1)^{\varphi(u)} + b$$

for some $a, b \in \mathbb{C}$. We can take a closer look at the two possibilities for $\varphi(u)$. Since

$$\begin{aligned} \zeta^0 &= a \cdot (-1)^0 + b, \\ \zeta^1 &= a \cdot (-1)^1 + b, \end{aligned}$$

we get the following system of equations:

$$\left.\begin{aligned} 1 &= a + b \\ \zeta &= -a + b \end{aligned}\right\} \iff \begin{cases} a &= \frac{1-\zeta}{2} \\ b &= \frac{1+\zeta}{2}. \end{cases}$$

Thus

$$\check{\varphi} = a \cdot \widetilde{\varphi} + b \cdot \widetilde{1}.$$

Similarly, (2.18) is also equivalent to (2.16) and (2.17). For our application we choose (2.17), because the set of coefficients turns out to be symmetric for $\widetilde{\varphi}$. In Section 6 you find some images justifying this decision in an "obvious" way. (From now on we will only mention the cases analogous to (2.17) but the others still are correct transformations.)

Now only the case $q = p^e$, $e \geq 2$, is left to be considered. The most "natural" way seems to be: Choose a group structure on M by using the addition in $\mathbb{F}_q$, which gives us the group $G = \left(\mathbb{Z}_p\right)^e$. This means we use a primitive pth root of unity ζ allowing us to parametrize all of $\widehat{G}$. But also the interpretation of u and w for the sum in the exponent changes. It is then a vector of en elements in $\mathbb{F}_p$ rather than n elements in $\mathbb{F}_q$. Thus we have the same transformation as before, but have to substitute $\frac{1}{p^n}$ by $\frac{1}{p^{en}}$:

$$\widetilde{\varphi}(w) = \frac{1}{p^{en}} \sum_{u \in \mathbb{F}_p^{en}} (-1)^{\varphi(u)} \cdot \zeta^{-\sum_j u_j w_j}. \tag{2.19}$$

But we could also identifiy the elements of $\mathbb{F}_q$ with the elements of $\mathbb{Z}_q$ via a bijective mapping $\beta\colon \mathbb{Z}_q \to \mathbb{F}_q$. This yields a function

$$\psi\colon \begin{array}{ccc} \mathbb{Z}_q^n & \longrightarrow & \{-1,1\}, \\ u & \longmapsto & (-1)^{\varphi(\beta(u_1),\ldots,\beta(u_n))} \end{array}.$$

Actually, it does not matter how we choose the bijection β, all possibilities give correct transformations. There are a few "main" transformations from which we can obtain all the others by re-ordering or possibky rotating the coefficients. Taking ζ as a qth root of unity, we have

$$\widetilde{\varphi}(w) = \widehat{\psi}(w) = \frac{1}{q^n} \sum_{u \in \mathbb{Z}_q^n} \psi(u) \cdot \zeta^{-\sum_j u_j w_j}. \tag{2.20}$$

Note that here the u_j and w_j are elements of $\mathbb{Z}_q$ rather than $\mathbb{F}_q$. (A study of these transformations over $\mathbb{F}_4$ is done in Section 6.4.)

2.5 Parseval/Plancherel Identity for Boolean Functions

The goal of this subsection is to prove a very useful identity concerning Theorem 2.10. This identity is generally called Parseval identity:

PARSEVAL IDENTITY 2.21. *For our Boolean functions φ it holds that the norm of the Fourier transform $\widetilde{\varphi}$ of φ equals 1:*

$$||\widetilde{\varphi}||^2 = \sum_{w \in \widehat{G}} |\widetilde{\varphi}(w)|^2 = 1.$$

PROOF. From Theorem 2.10 we have:

$$||\varphi||^2 = \sum_{g \in G} |\varphi(g)|^2 = \#G \sum_{w \in \widehat{G}} |\widetilde{\varphi}(w)|^2 = \#G||\widetilde{\varphi}||^2.$$

For every Boolean function φ we recall that

$$\psi(x) = (-1)^{\varphi(x)},$$

where ζ is a primitive root of unity. Then we get by insertion

$$||\psi||^2 = \left|\left|(-1)^{\varphi}\right|\right|^2 = \sum_{x \in \widehat{G}} |(-1)^{\varphi(x)}|^2 = \sum_{x \in \widehat{G}} 1 = \#G.$$

Hence, $||\psi||^2 = \#G = \#G \cdot ||\widetilde{\varphi}||^2$ and so

$$\sum |\widetilde{\varphi}(w)|^2 = 1. \qquad \square$$

Note that the Parseval identity is also correct for the alternative definition of Fourier coefficients in (2.16), i.e. when $\psi(x) = \zeta^{\varphi(x)}$.

3 Basics for the Fourier Transform over $\mathbb{F}_2$

In the first part of this work we consider univariate polynomials with constant coefficient 1 over $\mathbb{F}_2$. Thus we can identify polynomials of at most degree n, $n \geq 1$, with the corresponding n-bit vector

$$(u_1, \ldots, u_n) \longleftrightarrow u = u_n x^n + \ldots + u_1 x + 1.$$

Moreover we look at the following Boolean functions, first over $\mathbb{F}_2$. Later in this work we will also consider them over other finite fields.

DEFINITION 3.1. ∘ *The* irreducibility function $f\colon \{0,1\}^n \to \{0,1\}$ *is defined by*

$$f(u_1, \ldots, u_n) = \begin{cases} 1, & \textit{if } u \textit{ is irreducible,} \\ 0, & \textit{otherwise.} \end{cases}$$

∘ *The* squarefreeness function $g\colon \{0,1\}^n \to \{0,1\}$ *is defined by*

$$g(u_1, \ldots, u_n) = \begin{cases} 1, & \textit{if } u \textit{ is squarefree,} \\ 0, & \textit{otherwise.} \end{cases}$$

∘ *The* coprimality function $h\colon \{0,1\}^\ell \times \{0,1\}^\ell \to \{0,1\}$ *is defined by*

$$h(v_1, \ldots, v_\ell; w_1, \ldots, w_\ell) = \begin{cases} 1, & \textit{if } v \textit{ and } w \textit{ are coprime,} \\ 0, & \textit{otherwise.} \end{cases}$$

As in the main source for this part of the Diplomarbeit (Allender *et al.* 2003) let $\mathbb{B} = \{0,1\}$. At this point we shortly recall the definitions of squarefreeness, coprimality and irreducibility for polynomials:

DEFINITION 3.2 (Squarefreeness). *Let F be a field and m a polynomial in $F[x]$. Then m is* squarefree *if for all polynomials $u \in F[x]$, $\deg(u) \geq 1$:*

$$u^2 \nmid m.$$

DEFINITION 3.3 (Coprimality). *Let F be field. Then two polynomials $u, v \in F[x]$ are coprime if* $\gcd(u, v) = 1$.

DEFINITION 3.4 (Irreducibility). *Let F be field and $m \in F[x]$ a polynomial. Then m is irreducible if there is no non-trivial decomposition of m, i.e.*

$$\forall a, b \in F[x] \colon m = ab \Rightarrow a \in F \vee b \in F.$$

We will often consider the number of nonzero coefficients of a given bit vector.

DEFINITION 3.5 (Hamming weight). *The* Hamming weight $|u|$ *of a bit vector $u \in \mathbb{B}^n$ is the number of entries $u_i \neq 0$.*

DEFINITION 3.6 (Fourier coefficients over $\mathbb{F}_2$). *Let $\varphi \colon \mathbb{B}^n \to \mathbb{B}$ be a Boolean function. Then we know from (2.15) in Section 2.3 that the Fourier coefficients are*

$$\widetilde{\varphi}(w) = \frac{1}{2^n} \sum_{u \in \mathbb{B}^n} (-1)^{\varphi(u) + \sum_i u_i w_i}, w \in \mathbb{B}^n.$$

We call

$$d^{11}(\varphi) = \widetilde{\varphi}\,(1^n)$$

the highest order Fourier coefficient, *and*

$$d^{00}(\varphi) = \widetilde{\varphi}\,(0^n)$$

the lowest order Fourier coefficient.

Now, we will present a lemma that will be useful for a more exact determination of the highest order Fourier coefficient:

LEMMA 3.7. *For the Hamming weight $|u|$ holds*

$$\sum_{u \in \mathbb{B}^n} (-1)^{|u|} = 0.$$

PROOF. We have to calculate the sum

$$\sum_{\substack{u \in \mathbb{B}^n \\ \varphi(u)=0}} (-1)^{|u|} = \sum_{u \in \mathbb{B}^n} (-1)^{|u|} - \sum_{\substack{u \in \mathbb{B}^n \\ \varphi(u)=1}} (-1)^{|u|}.$$

Now, we study the first sum:

$$\begin{aligned} \sum_{u \in \mathbb{B}^n} (-1)^{|u|} &= \sum_{\substack{u \in \mathbb{B}^n \\ |u| = 0 \bmod 2}} 1 - \sum_{\substack{u \in \mathbb{B}^n \\ |u| = 1 \bmod 2}} 1 \\ &= 2^{n-1} - 2^{n-1} = 0. \end{aligned}$$

Evidently,

$$\sum_{\substack{u\in\mathbb{B}^n\\ \varphi(u)=0}} (-1)^{|u|} = -\sum_{\substack{u\in\mathbb{B}^n\\ \varphi(u)=1}} (-1)^{|u|}.$$

□

A generalization of this proof for all the u^j, $(u,v)^j$, $j \in \{01, 10, 11\}$ respectively, that we use for the proofs in Section 5 is possible, but tedious. However, we will show how the proof can be transferred to our other problems. Therefore we look at the u^{01} (used in Section 5.1): The binary vector of u^{01} is $(u_1, 0, u_3, 0, \ldots, u_{2\cdot\lfloor\frac{n-1}{2}\rfloor+1})$. For the calculation we will partition the binary vectors u that we have used for the sum in the previous proof, into $u^{(1)}$ and $u^{(2)}$:

$$\begin{aligned} u^{(1)} &= (u_1, u_3, \ldots, u_{2\cdot\lfloor\frac{n-1}{2}\rfloor+1}),\\ u^{(2)} &= (u_2, u_4, \ldots, u_{2\cdot\lfloor\frac{n}{2}\rfloor}). \end{aligned}$$

Then we can write the sum as follows:

$$\begin{aligned} \sum_{u\in\mathbb{B}^n} (-1)^{|u^{10}|} &= \sum_{u^{(2)}\in\mathbb{B}^{2\cdot\lfloor\frac{n}{2}\rfloor}} \sum_{u^{(1)}\in\mathbb{B}^{2\cdot\lfloor\frac{n-1}{2}\rfloor+1}} (-1)^{|u^{01}|}\\ &= \sum_{u^{(2)}\in\mathbb{B}^{2\cdot\lfloor\frac{n}{2}\rfloor}} \sum_{u^{(1)}\in\mathbb{B}^{2\cdot\lfloor\frac{n-1}{2}\rfloor+1}} (-1)^{|u^{(1)}|}\\ &= \sum_{u^{(2)}\in\mathbb{B}^{2\cdot\lfloor\frac{n}{2}\rfloor}} 0 = 0. \end{aligned}$$

LEMMA 3.8. *The highest order Fourier coefficient can be transformed to*

$$d^{11}(\varphi) = -\frac{1}{2^{n-1}} \sum_{\substack{u\in\mathbb{B}^n\\ \varphi(u)=1}} (-1)^{|u|}.$$

PROOF.

$$\begin{aligned} d^{11}(\varphi) &= \widetilde{\varphi}(1^n) = \frac{1}{2^n}\sum_{u\in\mathbb{B}^n}(-1)^{\varphi(u)+\sum_i u_i\cdot 1} = \frac{1}{2^n}\sum_{u\in\mathbb{B}^n}(-1)^{\varphi(u)+|u|} \\ &= \frac{1}{2^n}\left(\sum_{\substack{u\in\mathbb{B}^n\\ \varphi(u)=0}}(-1)^{|u|+0} + \sum_{\substack{u\in\mathbb{B}^n\\ \varphi(u)=1}}(-1)^{|u|+1}\right) \\ &= \frac{1}{2^n}\left(\sum_{\substack{u\in\mathbb{B}^n\\ \varphi(u)=0}}(-1)^{|u|} - \sum_{\substack{u\in\mathbb{B}^n\\ \varphi(u)=1}}(-1)^{|u|}\right) \\ &= \frac{1}{2^n}\left(\left(\sum_{u\in\mathbb{B}}(-1)^{|u|} - \sum_{\substack{u\in\mathbb{B}^n\\ \varphi(u)=1}}(-1)^{|u|}\right) - \sum_{\substack{u\in\mathbb{B}^n\\ \varphi(u)=1}}(-1)^{|u|}\right) \end{aligned}$$

The sum $\sum_{u\in\mathbb{B}^n}(-1)^{|u|}$ equals 0 as you can see in Lemma 3.7. Thus

$$\begin{aligned} d^{11}(\varphi) &= \frac{1}{2^n}\cdot\left(-2\cdot\sum_{\substack{u\in\mathbb{B}^n\\ \varphi(u)=1}}(-1)^{|u|}\right) \\ &= -\frac{1}{2^{n-1}}\sum_{\substack{u\in\mathbb{B}^n\\ \varphi(u)=1}}(-1)^{|u|} \end{aligned}$$

□

LEMMA 3.9. *The lowest order Fourier coefficient can be written as*

$$d^{00}(\varphi) = \frac{1}{2^n}\sum_{u\in\mathbb{B}^n}(-1)^{\varphi(u)}.$$

Note that $d^{00}(\varphi)$ is the expected value of the function $(-1)^{\varphi(u)}$ with regard to the uniform distribution in $\mathbb{F}_2$. The next lemma was also mentioned in Allender *et al.* (2003), but not proven:

LEMMA 3.10. *The sum of the absolute values of the highest and lowest order Fourier coefficient over $\mathbb{F}_2$ is less or equal to 1:*

$$\left|d^{00}(\varphi)\right| + \left|d^{11}(\varphi)\right| \leq 1.$$

PROOF. Obviously,

$$\left|d^{00}(\varphi)\right| + \left|d^{11}(\varphi)\right| = \left|\frac{1}{2^n}\sum_{u\in\mathbb{B}^n}(-1)^{\varphi(u)}\right| + \left|\frac{1}{2^n}\sum_{u\in\mathbb{B}^n}(-1)^{\varphi(u)+|u|}\right|.$$

We distinguish four different cases with respect to the signs of the two sums, as both sums could have positive or negative sign. First we look at the case that both sums yield nonnegative results:

$$\begin{aligned}&\left|\frac{1}{2^n}\sum_{u\in\mathbb{B}^n}(-1)^{\varphi(u)} + \frac{1}{2^n}\sum_{u\in\mathbb{B}^n}(-1)^{\varphi(u)+|u|}\right| \\ &= \frac{1}{2^n}\sum_{2||u|}\underbrace{2\cdot(-1)^{\varphi(u)}}_{|\cdot|\leq 2} \leq \frac{2^{n-1}\cdot 2}{2^n} = 1.\end{aligned}$$

Next we consider two negative signs for the sums:

$$\begin{aligned}&\left|-\frac{1}{2^n}\sum_{u\in\mathbb{B}^n}(-1)^{\varphi(u)} - \frac{1}{2^n}\sum_{u\in\mathbb{B}^n}(-1)^{\varphi(u)+|u|}\right| \\ &= \left|\frac{1}{2^n}\sum_{u\in\mathbb{B}^n}(-1)^{\varphi(u)} + \frac{1}{2^n}\sum_{u\in\mathbb{B}^n}(-1)^{\varphi(u)+|u|}\right| \\ &= \frac{1}{2^n}\sum_{2||u|}\underbrace{2\cdot(-1)^{\varphi(u)}}_{|\cdot|\leq 2} \leq \frac{2^{n-1}\cdot 2}{2^n} = 1.\end{aligned}$$

Now, we consider a positive sign for the first sum and a negative sign for the second one

$$\begin{aligned}&\left|\frac{1}{2^n}\sum_{u\in\mathbb{B}^n}(-1)^{\varphi(u)} - \frac{1}{2^n}\sum_{u\in\mathbb{B}^n}(-1)^{\varphi(u)+|u|}\right| \\ &= \frac{1}{2^n}\sum_{2\not|u|}\underbrace{2\cdot(-1)^{\varphi(u)}}_{|\cdot|\leq 2} \leq \frac{2^{n-1}\cdot 2}{2^n} = 1.\end{aligned}$$

and vice versa

$$\begin{aligned}&\left|-\frac{1}{2^n}\sum_{u\in\mathbb{B}^n}(-1)^{\varphi(u)} + \frac{1}{2^n}\sum_{u\in\mathbb{B}^n}(-1)^{\varphi(u)+|u|}\right| \\ &= \frac{1}{2^n}\sum_{2\not|u|}\underbrace{2\cdot(-1)^{\varphi(u)}}_{|\cdot|\leq 2} \leq \frac{2^{n-1}\cdot 2}{2^n} = 1.\end{aligned}$$

□

4 Some Experiments for the Fourier Transform over $\mathbb{F}_2[x]$

4.1 The Squarefreeness Function

Our goal is to isolate the Fourier coefficients with the greatest impact on several important Boolean functions. Our approach was to do extensive computer calculations that yielded both the candidates for the dominant coefficients as well as very good ideas of the values they converge on. Looking at the squarefreeness function g our calculations bring to light at least four relatively big coefficients that do not seem to converge on 0 but rather to other well-defined values. Figure 4.1 was done using degree $n = 12$ and plotting the Fourier coefficient $\widetilde{g}(w)$ of $w \in \{0,1\}^n$ against the number $(w)_2$, i.e. the integer value associated with the binary representation w. Note that all these coefficients are real values. Two of the absolutely large coefficients, plotted against 0 and 4095, correspond to the lowest Fourier coefficient at $w^{00} = 0^n$ and the highest at $w^{11} = 1^n$. Looking at degree $n = 15$ in Figure 4.2 we note that the

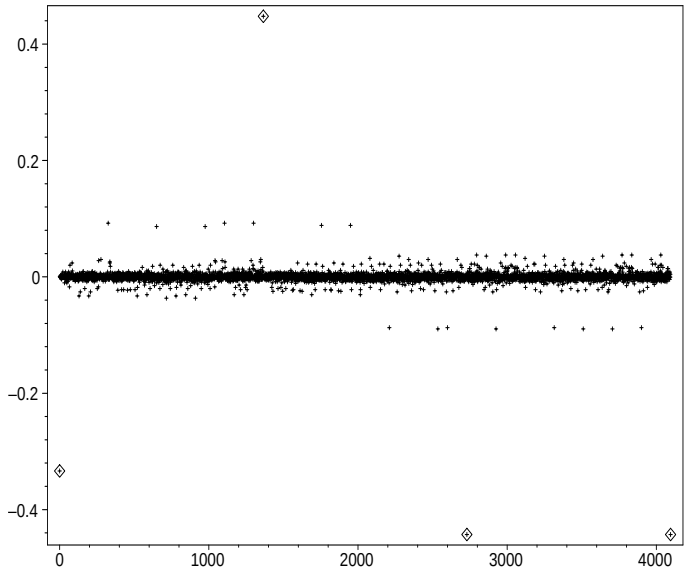


Figure 4.1: Plot of the Fourier coefficients for the squarefreeness function and maximum degree $n = 12$.

picture is quite similar apart from the fact that the two large coefficients not corresponding to constant bit strings w^{00} and w^{11} seemingly change sign.

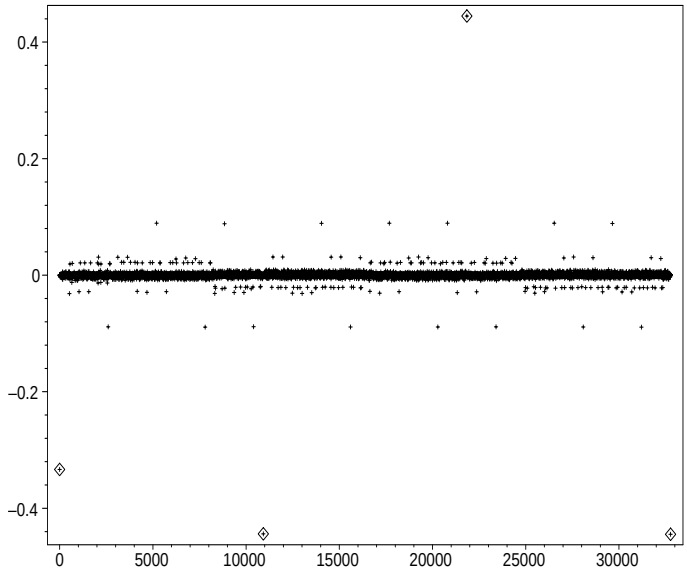


Figure 4.2: Plot of the Fourier coefficients for the squarefreeness function and maximum degree $n = 15$.

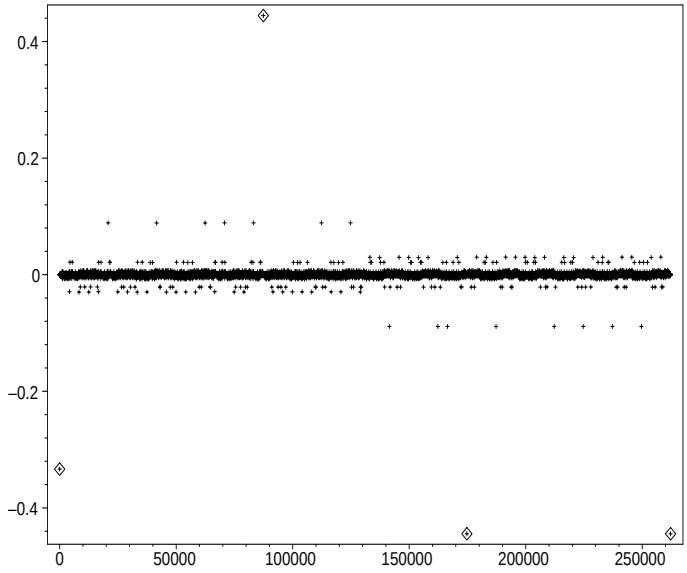


Figure 4.3: Plot of the Fourier coefficients for the squarefreeness function and maximum degree $n = 18$.

For degree $n = 18$ we have again only an "invisible" change in the greatest Fourier coefficients. But one can see that there are many more coefficients which are almost 0.

Evaluation of our data yields the following insights which are still to be proven. Apart from the highest and lowest Fourier coefficients there are two other significant coefficients which correspond to $w^{01} = \ldots 0101$ and $w^{10} = \ldots 1010$. Note that $(w^{01})_2$ lies at about $\frac{1}{3}$ and $(w^{10})_2$ at about $\frac{2}{3}$ of the x-axis if n is even, and the roles are reversed if n is odd. As mentioned above in the plots this can easily be mistaken as a change of sign of the two families of coefficients. The values these four coefficients assumed by for n from 1 to 20 are presented in Table 4.1. Their convergence on $-\frac{4}{9}$, $\frac{4}{9}$, $-\frac{4}{9}$ and $-\frac{1}{3}$ does not

n	w^{00}	w^{01}	w^{10}	w^{11}
1	-1	-1	$+0$	$+0$
2	-0.5	-0.5	$+0.5$	-0.5
3	-0.5	-0.5	$+0.5$	-0.5
4	-0.375	-0.375	$+0.625$	-0.375
5	-0.375	-0.375	$+0.5$	-0.5
6	-0.34375	-0.40625	$+0.53125$	-0.40625
7	-0.34375	-0.40625	$+0.46875$	-0.46875
8	-0.3359375	-0.4296875	$+0.4765625$	-0.4296875
9	-0.3359375	-0.4296875	$+0.453125$	-0.453125
10	-0.333984375	-0.439453125	$+0.455078125$	-0.439453125
11	-0.333984375	-0.439453125	$+0.447265625$	-0.447265625
12	-0.3334960938	-0.4428710938	$+0.4477539062$	-0.4428710938
13	-0.3334960938	-0.4428710938	$+0.4453125$	-0.4453125
14	-0.3333740234	-0.4439697266	$+0.4454345703$	-0.4439697266
15	-0.3333740234	-0.4439697266	$+0.4447021484$	-0.4447021484
16	-0.3333435059	-0.4443054199	$+0.444732666$	-0.4443054199
17	-0.3333435059	-0.4443054199	$+0.444519043$	-0.444519043
18	-0.3333358765	-0.4444046021	$+0.4445266724$	-0.4444046021
19	-0.3333358765	-0.4444046021	$+0.4444656372$	-0.4444656372
20	-0.3333339691	-0.4444332123	$+0.4444675446$	-0.4444332123
∞	$\to -\frac{1}{3}$	$\to -\frac{4}{9}$	$\to +\frac{4}{9}$	$\to -\frac{4}{9}$

Table 4.1: The values of the four most significant Fourier coefficients for the squarefreeness function and degrees up to 20. The last line indicates the limit for $n \to \infty$.

seem to be a far-fetched conjecture and will be proven in Section 5.1.

4.2 The Coprimality Function

We used the same strategy for the coprimality function. The results of our computations for $n = 12$ can be seen in Figure 4.4. Once more there are four coefficients that seem to differ significantly from the others. Two of them are again the lowest and highest order coefficients. The coprimality function is

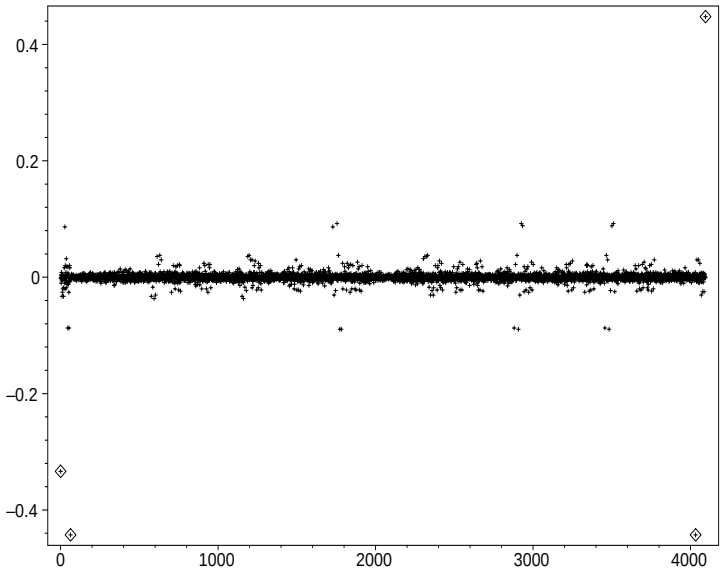


Figure 4.4: Plot of the Fourier coefficients for the coprimality function and maximum degree $n = 12$.

only defined for even n and the degree of the polynomials involved is actually at most $\frac{n}{2}$. Therefore the next step was $n = 12$, but we will actually look at $n = 18$ to see a little more development. But also for $n = 18$ there is not much of a change in the plot, Figure 4.5. Again the coefficients appear to converge on $\frac{4}{9}$, $-\frac{4}{9}$, $-\frac{4}{9}$ and $-\frac{1}{3}$. In contrast to the squarefreeness function, the coprimality function has the large coefficients at $w^{01} = 0^\ell 1^\ell$ and $w^{10} = 1^\ell 0^\ell$, where $\ell = \frac{n}{2}$. In Table 4.2 you can see the results for a few values of n.

REMARK 4.1. *The values for the Fourier coefficients at $1^\ell 0^\ell$ and $0^\ell 1^\ell$ in Table 4.2 seem to be equal. This is obvious as exchanging two polynomials does not change whether they are coprime. This will be formulated precisely in Lemma 5.17 and its proof.*

The proof that these coefficients actually converge on the apparent values is done in Section 5.2.

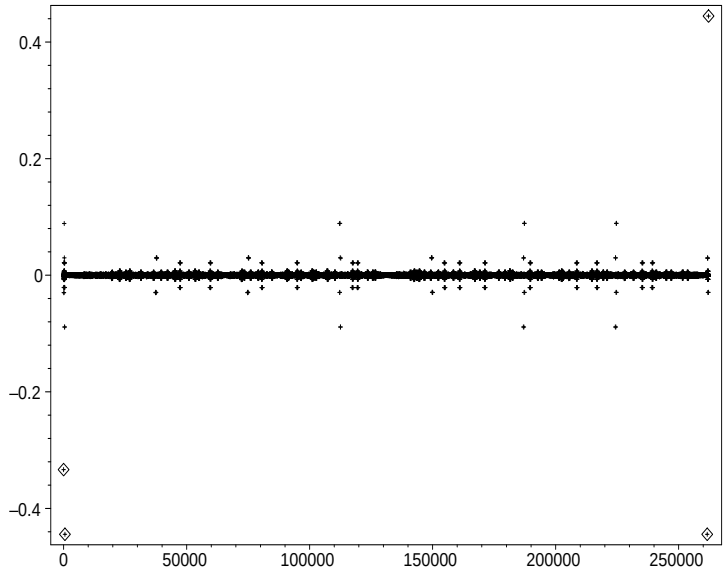


Figure 4.5: Plot of the Fourier coefficients for the coprimality function and maximum degree $n = 18$.

n	1^n	$1^\ell 0^\ell$	$0^\ell 1^\ell$	0^n
2	-0.5	-0.5	-0.5	$+0.5$
4	-0.375	-0.375	-0.375	$+0.625$
6	-0.34375	-0.40625	-0.40625	$+0.53125$
8	-0.3359375	-0.4296875	-0.4296875	$+0.4765625$
10	-0.333984375	-0.439453125	-0.439453125	$+0.455078125$
12	-0.3334960938	-0.4428710936	-0.4428710938	$+0.4477539063$
14	-0.3333740234	-0.4439697266	-0.4439697266	$+0.4454345703$
16	-0.3333435059	-0.4443054199	-0.4443054199	$+0.444732666$
18	-0.3333358765	-0.4444046021	-0.4444046021	$+0.4445266724$
20	-0.3333339691	-0.4444332123	-0.4444332123	$+0.4444675446$
∞	$\to -\frac{1}{3}$	$\to -\frac{4}{9}$	$\to -\frac{4}{9}$	$\to +\frac{4}{9}$

Table 4.2: The values of the four most significant Fourier coefficients for the coprimality function and (even) degrees up to 20.

4.3 The Irreducibility Function

Compared to the previous sections, the results for the irreducibility function were somewhat disappointing, and yet simpler. It appears that the lowest order coefficient converge on 1 as n tends to infinity while all the others converge on 0. First, we take a look at the coefficients for degree $n = 10$ in Figure 4.6. In

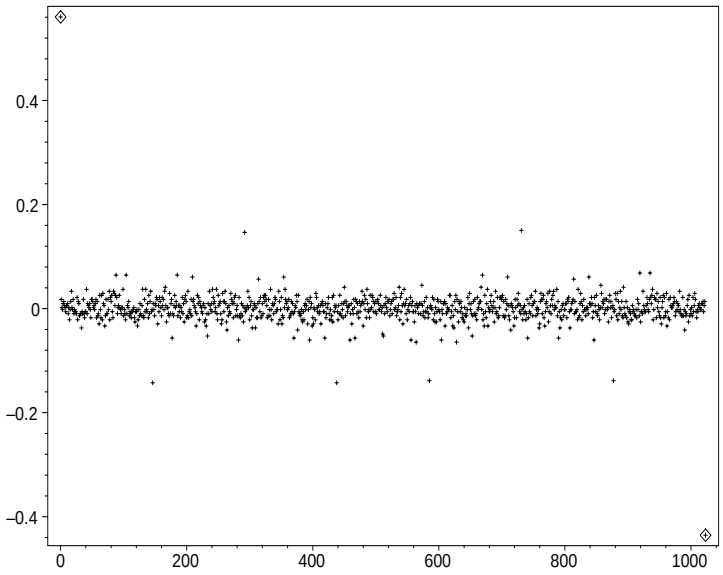


Figure 4.6: Plot of the Fourier coefficients for the irreducibility function and maximum degree $n = 10$.

the next plot we look at the much bigger $n = 18$, because at this relatively big n we can better observe the demise of the highest order coefficient towards 0 and the rise of its lowest order counterpart towards 1, see Figure 4.7. Let us look at the values of the highest and lowest order coefficients for growing values of n in Table 4.3. While the tendency seems clear, the speed of the process seems somewhat slower than what we witnessed for the squarefreeness and coprimality functions. There is no known proof for our conjectures about the Fourier coefficients of the irreducibility function proceeding in the same way as for the other two considered functions. We attribute this difficulty to the obvious differences when compared with the earlier functions. It should come as no surprise that the proofs for the squarefreeness and coprimality functions are very similar and cannot simply be put to work on irreducibility. However, in Section 7.3 there is a proof for the highest and lowest order coefficients of the irreducibility function.

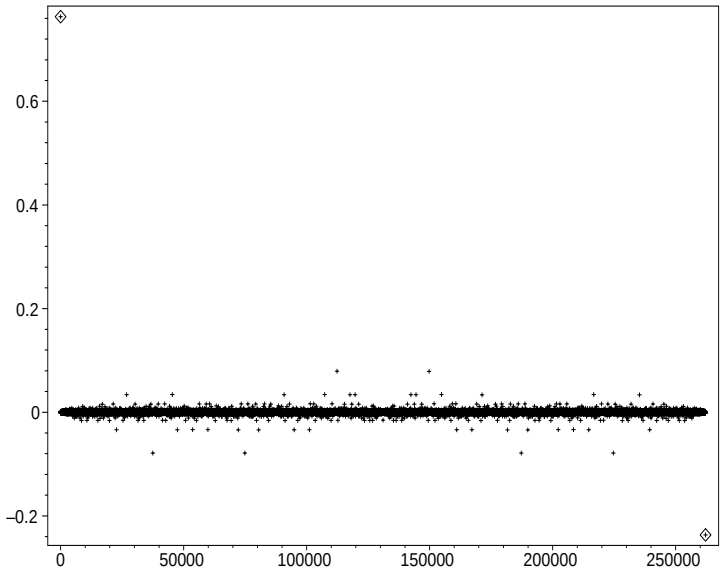


Figure 4.7: Plot of the Fourier coefficients for the irreducibility function and maximum degree $n = 18$.

n	1^n	0^n	n	1^n	0^n
1	+0	+1	11	+0.5986328125	−0.3994140625
2	+0	+0	12	+0.6357421875	−0.36328125
3	+0	−0.5	13	+0.6640625	−0.3354492188
4	+0.125	−0.625	14	+0.6903076172	−0.3094482422
5	+0.1875	−0.6875	15	+0.7119750976	−0.287902832
6	+0.3125	−0.625	16	+0.7314758301	−0.2684631348
7	+0.375	−0.59375	17	+0.7480926514	−0.2518768311
8	+0.453125	−0.53125	18	+0.7631759644	−0.2368087769
9	+0.5078125	−0.484375	19	+0.7763252258	−0.2236671448
10	+0.560546875	−0.435546875	20	+0.7882614136	−0.2117347717
			∞	$\to 1$	$\to 0$

Table 4.3: The values of the highest and lowest order Fourier coefficients for the irreducibility function and degrees up to 20.

5 The Extreme Fourier Coefficients over $\mathbb{F}_2[x]$

Throughout the next sections μ denotes the famous Möbius function for polynomials defined by

$$\mu(w) = \begin{cases} 1, & \text{if } w = 1, \\ 0, & \text{if } w \text{ is not squarefree,} \\ (-1)^{\nu(w)}, & \text{otherwise,} \end{cases}$$

where $\nu(w)$ is the number of distinct irreducible divisors of w in the used field.

5.1 The Squarefreeness Function

Looking at our calculations in Section 4.1 it becomes apparent or at the least seems highly probable that there are four Fourier coefficients that differ significantly from the others.

We consider the two "alternating" sequences

$$w^{10} = (\ldots, 1, 0, 1, 0),\ w^{01} = (\ldots, 0, 1, 0, 1),$$

the 1-sequence $w^{11} = 1^n$ and the 0-sequence $w^{00} = 0^n$, all in $\mathbb{B}^n$, which yield the four "extreme" coefficients.

For the squarefreeness function g we define the highest order coefficient $d^{11} = \widetilde{g}(w^{11})$, the lowest order coefficient $d^{00} = \widetilde{g}(w^{00})$ and additionally the coefficients which belong to the "alternating" sequences $d^{10} = \widetilde{g}(w^{10})$ and $d^{01} = \widetilde{g}(w^{01})$.

The following is the basic set on which our Boolean functions operate:

$$\mathcal{M}(n) = \{u \in \mathbb{F}_2[x] : \deg u \leq n, u \equiv 1 \bmod x\},$$

where $u \equiv 1 \bmod x \Leftrightarrow u(0) = 1 \Leftrightarrow u_0 = 1$, when $u = u_n x^n + \ldots + u_1 x + u_0 \in \mathbb{F}_2[x]$. The squarefreeness function g maps elements of $\mathcal{M}(n)$ to the binary field $\mathbb{B}$. The formal derivative of u is:

$$u' = \begin{cases} u_{n-1}x^{n-2} + \ldots + u_3 x^3 + u_1, & \text{if } n \text{ is even,} \\ u_n x^{n-1} + \ldots + u_3 x^3 + u_1, & \text{otherwise.} \end{cases}$$

For the following proof we define $u^{10} = (ux)' = u' \cdot x + u$ and $u^{01} = u' \cdot x + 1$. Furthermore the structure of these u's is important, therefore we take a closer look:

If n is even, the polynomial u^{10} is

$$\begin{aligned} u^{10} &= u' \cdot x + u \\ &= u + x \cdot (u_{n-1}x^{n-2} + \ldots + u_3x^2 + u_1) \\ &= u + u_{n-1}x^{n-1} + \ldots + u_3x^3 + u_1x \\ &= u_nx^n + u_{n-2}x^{n-2} + \ldots + u_2x^2 + 1. \end{aligned}$$

If n is odd, we have similarly

$$\begin{aligned} u^{10} &= u + u_nx^n + \ldots + u_3x^3 + u_1x \\ &= u_{n-1}x^{n-1} + u_{n-3}x^{n-3} + \ldots + u_2x^2 + 1. \end{aligned}$$

In either case, letting $u = 1^n$ the list of coefficients of u^{10} is simply w^{10}. The same procedure for u^{01} yields for n even:

$$\begin{aligned} u^{01} &= u' \cdot x + 1 \\ &= (u_{n-1}x^{n-2} + \ldots + u_3x^2 + u_1) \cdot x + 1 \\ &= u_{n-1}x^{n-1} + \ldots + u_3x^3 + u_1x + 1. \end{aligned}$$

Otherwise:

$$\begin{aligned} u^{01} &= u' \cdot x + 1 \\ &= (u_nx^{n-1} + \ldots + u_3x^2 + u_1) \cdot x + 1 \\ &= u_nx^n + \ldots + u_3x^3 + u_1x + 1. \end{aligned}$$

Once again we note that w^{01} is the sequence of the coefficients of u^{01} for $u = 1^n$.

In the following we will look at some useful facts that will come in handy in our proofs for certain Fourier coefficients:

5.1.1 Inclusion-Exclusion Principle

Let M be a finite set and A, B and C subsets of M. Then

$$\begin{aligned} \#(A \cup B) &= \#A + \#B - \#(A \cap B), \\ \#(A \cup B \cup C) &= \#A + \#B + \#C \\ &\quad - (\#(A \cap B) + \#(A \cap C) + \#(B \cap C)) \\ &\quad + \#(A \cap B \cap C). \end{aligned} \tag{5.1}$$

These simple facts can be generalized to the so-called inclusion-exclusion principle, which we use throughout this section.

THEOREM 5.2 (Inclusion-exclusion principle). *Let M be a finite set, $n \in \mathbb{N}$ and $A_1, \ldots, A_n$ subsets of M then*

$$\#\bigcup_{i=1}^{n} A_i = \sum_{k=1}^{n} \left((-1)^{k-1} \sum_{1 \le i_1 < \ldots < i_k \le n} \#\bigcap_{j=1}^{k} A_{i_j} \right).$$

PROOF. We will prove the inclusion-exclusion principle by induction. For $n = 1$ there is nothing to show. Now, let $n \ge 2$. By the induction hypothesis the principle holds for all $A_1, \ldots, A_n \in P(M)$. Using the formula for the cardinality of the union of two finite sets (5.1) it follows that

$$\begin{aligned} \#\bigcup_{j=1}^{n} A_j &= \#\left(\bigcup_{j=1}^{n-1} A_j \cup A_n \right) \\ &= \#\bigcup_{j=1}^{n-1} A_j + \#A_n - \#\left(\bigcup_{j=1}^{n-1} A_j \cap A_n \right) \\ &= \#\bigcup_{j=1}^{n-1} A_j + \#A_n - \#\bigcup_{j=1}^{n-1} (A_j \cap A_n) \end{aligned} \tag{5.3}$$

By the induction hypothesis we have

$$\#\bigcup_{i=1}^{n-1} A_i = \sum_{k=1}^{n-1} \left((-1)^{k-1} \sum_{1 \le i_1 < \ldots < i_k \le n-1} \#\bigcap_{j=1}^{k} A_{i_j} \right).$$

Application to $\#\bigcup_{j=1}^{n-1} (A_j \cap A_n)$ yields

$$\begin{aligned} \#\bigcup_{i=1}^{n-1} (A_i \cap A_n) &= \sum_{k=1}^{n-1} \left((-1)^{k-1} \sum_{1 \le i_1 < \ldots < i_k \le n-1} \#\bigcap_{j=1}^{k} (A_{i_j} \cap A_n) \right) \\ &= \sum_{k=1}^{n-1} \left((-1)^{k-1} \sum_{1 \le i_1 < \ldots < i_k \le n-1} \#\left(\bigcap_{j=1}^{k} A_{i_j} \cap A_n \right) \right) \end{aligned}$$

Inserting this in (5.3) we obtain

$$\begin{aligned}
\#\bigcup_{j=1}^{n} A_j &= \#\bigcup_{j=1}^{n-1} A_j + \#A_n - \#\bigcup_{j=1}^{n-1}(A_j \cap A_n) \\
&= \sum_{k=1}^{n-1}\left((-1)^{k-1}\sum_{1\le i_1<\ldots<i_k\le n-1} \#\bigcap_{j=1}^{k} A_{i_j}\right) + \#A_n \\
&\quad -\sum_{k=1}^{n-1}\left((-1)^{k-1}\sum_{1\le i_1<\ldots<i_k\le n-1} \#\left(\bigcap_{j=1}^{k} A_{i_j}\cap A_n\right)\right) \\
&= \sum_{k=1}^{n}\left((-1)^{k-1}\sum_{1\le i_1<\ldots<i_k\le n} \#\bigcap_{j=1}^{k} A_{i_j}\right).
\end{aligned}$$

This concludes the proof of the inclusion-exclusion principle. □

5.1.2 Berlekamp and Euler

From Berlekamp we know:

THEOREM 5.4 (Berlekamp's identity). *Let q be a prime power and d_m the number of distinct irreducible monic polynomials of degree m defined over the finite field $\mathbb{F}_q$. Then we have the equation for the generating function of the set of all monic polynomials over $\mathbb{F}_q$:*

$$\frac{1}{1-qz} = \prod_{m=1}^{\infty}\left(\frac{1}{1-z^m}\right)^{d_m}.$$

(For more information see Berlekamp (1968), in particular Chapter 3.3.)

First, we will study some arithmetic problems over $\mathbb{F}_2$. So, Berlekamp tells us:

$$\frac{1}{1-2z} = \prod_{m=1}^{\infty}\left(\frac{1}{1-z^m}\right)^{d_m}.$$

Let $I = \{w \in \mathbb{F}_2[x], w \text{ irreducible}\}$, $I_0 = I \setminus \{x\}$ and $I_1 = I \setminus \{x, x+1\}$. Now, Berlekamp's formula can be written as:

$$\frac{1}{1-2z} = \prod_{w\in I}\left(\frac{1}{1-z^{\deg w}}\right)^{-1}.$$

The following theorem is attributed to Euler:

THEOREM 5.5 (Euler's product formula for polynomials).

$$\sum_w \mu(w) 2^{-2 \deg w} = \prod_{w \in I} (1 - 2^{-2 \deg w}),$$

where μ is Möbius's functions for polynomials.

A proof can be done using the inclusion-exclusion principle and induction. We will only do an informal argumentation:

$$\begin{aligned} \prod_{w \in I} \left(1 - z^{-\deg w}\right) &= \sum_{S \subseteq I} (-1)^{\#S} \cdot \prod_{w \in S} z^{-\deg w} \\ &= \sum_{S \subseteq I} (-1)^{\#S} \cdot z^{-\sum_{w \in S} \deg w} \\ &= \sum_w \mu(w) \cdot z^{-\deg w}. \end{aligned}$$

The last equation is correct because by multiplication of the elements for each subset S of I we get all possible polynomials w. The replacement of $(-1)^{\#S}$ is correct because all elements of S are irreducible polynomials and the appropriate property of the Möbius function.

- Now, from Berlekamp follows with $z = 2^{-2} = \frac{1}{4}$:

$$\prod_{w \in I} (1 - 2^{-2 \deg w}) = 1 - 2 \cdot \frac{1}{4} = \frac{1}{2}.$$

- The value of $(1 - 2^{-2 \deg w})$ is $1 - 2^{-2} = \frac{3}{4}$ for $w = x$, hence

$$\prod_{w \in I_0} (1 - 2^{-2 \deg w}) = \frac{1}{2} \cdot \frac{4}{3} = \frac{2}{3}.$$

- The value of $(1 - 2^{-2 \deg w})$ also is $1 - 2^{-2} = \frac{3}{4}$ for $w = x + 1$, therefore

$$\prod_{w \in I_1} (1 - 2^{-2 \deg w}) = \frac{1}{2} \cdot \frac{4}{3} \cdot \frac{4}{3} = \frac{8}{9}.$$

Now, we pay attention at the previously mentioned Fourier coefficients. The Fourier coefficients at w^{10} and w^{11} are asymptotically very close to $-\frac{4}{9}$ and at w^{01} to $\frac{4}{9}$. For w^{11} the fact that $d^{11} = -\frac{4}{9} + \mathrm{O}(2^{-n/2})$ was already proven in Allender *et al.* (2003). Our results seem to be new: we will give an explicite error bound for the highest order coefficient and prove simultaneously the estimates for the other two coefficients, as is stated in the following lemma:

LEMMA 5.6. *For the squarefreeness function g we have*

(i) $\left|d^{11} + \frac{4}{9}\right| \leq 2^{-n/2}$,

(ii) $\left|d^{10} + \frac{4}{9}\right| \leq 2^{-n/2}$,

(iii) $\left|d^{01} - \frac{4}{9}\right| \leq 2^{-n/2}$.

PROOF. We will prove these three bounds all at once. In order to do this we look at $u^{10} = u' \cdot x + u$ and $u^{01} = u' \cdot x + 1$ and moreover we define $J = \{01, 10, 11\}$. Furthermore for the sake of achieving a uniform proof, let $u^{11} = u$. Thus for all $j \in J$:

$$d^j = \frac{1}{2^n} \sum_{u \in \mathbb{B}^n} (-1)^{g(u) + \sum_{1 \leq i \leq n} u_i w_i^j}.$$

Now we make use of the correspondence between w^j and u^j: The polynomial representation of w^{10} is $1 + x^2 + x^4 + \ldots$. The vector representation of u^{10} can have nonzero entries only at those indices where the corresponding value in the vector w^{10} is 1. The same holds for $w^{01} = 1 + x + x^3 \ldots$ and u^{01} as well as for w^{11} and u^{11}. Hence we have for all u, j:

$$\sum_{1 \leq i \leq n} u_i w_i^j = \sum_{1 \leq i \leq n} u_i^j w_i^j = \sum_{1 \leq i \leq n} u_i^j = |u^j| = u^j(1) + 1.$$

The summand 1 in the last expression stems from the fact that the bit vector u^j does by our convention not contain the constant coefficient 1 of the corresponding polynomial. Therefore, we have for all three cases:

$$d^j = \frac{1}{2^n} \sum_{u \in \mathbb{B}^n} (-1)^{g(u) + |u^j|}.$$

To continue the proof we apply some minor regrouping to this formula for d^j:

$$\begin{aligned}
d^j &= \frac{1}{2^n} \sum_{u \in \mathbb{B}^n} (-1)^{g(u)+|u^j|} \\
&= \frac{1}{2^n} \Big(\sum_{\substack{u \in \mathbb{B}^n \\ g(u)=0}} (-1)^{|u^j|} - \sum_{\substack{u \in \mathbb{B}^n \\ g(u)=1}} (-1)^{|u^j|} \Big) \\
&= \frac{1}{2^n} \Big(- \sum_{\substack{u \in \mathbb{B}^n \\ g(u)=1}} (-1)^{|u^j|} - \sum_{\substack{u \in \mathbb{B}^n \\ g(u)=1}} (-1)^{|u^j|} \Big) \\
&= -\frac{1}{2^{n-1}} \sum_{\substack{u \in \mathbb{B}^n \\ g(u)=1}} (-1)^{|u^j|}.
\end{aligned}$$

Obviously $(-1)^{|u^j|} = 1$, if the Hamming weight $|u^j|$ is even, and $(-1)^{|u^j|} = -1$, otherwise, thus we have for all $j \in J$:

$$d^j = -\frac{1}{2^{n-1}} \cdot \Big(\sum_{\substack{u \in \mathbb{B}^n \\ g(u)=1 \\ u^j(1)=1}} 1 - \sum_{\substack{u \in \mathbb{B}^n \\ g(u)=1 \\ u^j(1)=0}} 1 \Big).$$

For all $j \in J$, let D^j denote the number of squarefree polynomials $u \in \mathcal{M}(n)$ with $u^j(1) = 1$ minus the number of squarefree polynomials $u \in \mathcal{M}(n)$ with $u^j(1) = 0$:

$$\begin{aligned} D^j &= \#\{u \in \mathcal{M}(n) \colon g(u) = 1, u^j(1) = 1\} \\ &\qquad -\#\{u \in \mathcal{M}(n) \colon g(u) = 1, u^j(1) = 0\}. \end{aligned}$$

Evidently we have for $j \in J$:

$$d^j = -\frac{D^j}{2^{n-1}}.$$

Now for $m \in \mathbb{F}_2[x] \setminus \{0\}$ we define the set

$$\mathcal{R}_m = \{u \in \mathcal{M}(n) \colon u \equiv 0 \bmod m^2\} \tag{5.7}$$

and let $R_m = \#\mathcal{R}_m$ denote its size. Then $\mathcal{R}_m = \emptyset$ if $m(0) = 0$, since $x \mid m$ and $m^2 \mid u$ imply $x^2 \mid u$, hence $u \notin \mathcal{M}(n)$. Also $\mathcal{R}_m = \emptyset$ if $\deg(m) > \frac{n}{2}$.

In order to rule out these trivial cases we make the following global assumption:

$$m(0) = 1 \text{ and } \deg(m) \le \frac{n}{2}. \tag{5.8}$$

D^j can be written as

$$\begin{aligned} D^j &= \#\bigcap_{m \text{ irr.}} \{u \in \mathcal{M}(n) \colon u^j(1) = 1, m^2 \nmid u\} \\ &\qquad -\#\bigcap_{m \text{ irr.}} \{u \in \mathcal{M}(n) \colon u^j(1) = 0, m^2 \nmid u\}. \end{aligned}$$

Consider now for $m \in \mathcal{M}(n)$ and $j \in J$:

1. $\mathcal{A}_m^j = \{u \in \mathcal{R}_m \colon u^j(1) = 1\}$, $A_m^j = \#\mathcal{A}_m^j$,

2. $\mathcal{B}_m^j = \{u \in \mathcal{R}_m \colon u^j(1) = 0\}$, $B_m^j = \#\mathcal{B}_m^j$,
3. $A^j = \#\bigcup_{m \text{ irr.}} \mathcal{A}_m^j$ and $B^j = \#\bigcup_{m \text{ irr.}} \mathcal{B}_m^j$.

First we observe that if $m_1, \ldots, m_k$ are irreducible, pairwise coprime and furthermore $m = m_1 \cdot \ldots \cdot m_k$, then

$$\bigcap_{i=1}^{k} \mathcal{A}_{m_i}^j = \mathcal{A}_m^j,$$

which is a simple exercise.

Applying the inclusion-exclusion principle from Section 5.1.1 to $\bigcup_{m \text{ irr.}} \mathcal{A}_m^j$ we get:

$$\begin{aligned}
A^j &= \#\bigcup_{m \text{ irr.}} \mathcal{A}_m^j = -\sum_{1 \le k \le n/2} (-1)^k \sum_{\substack{m_1,\ldots,m_k \text{ irr., pw cop.} \\ \deg(m_1 \cdot \ldots \cdot m_k) \le n/2}} \#\bigcap_{1 \le i \le k} \mathcal{A}_{m_i}^j \\
&= -\sum_{1 \le k \le n/2} (-1)^k \sum_{\substack{\deg m \le n/2 \\ m \text{ sqf with } k \text{ irr. fact.}}} \#\mathcal{A}_m^j \\
&= -\sum_{1 \le k \le n/2} \sum_{m} \mu(m) A_m^j \\
&= -\sum_{0 < \deg m \le n/2} \mu(m) A_m^j,
\end{aligned}$$

where μ is the Möbius function for polynomials. Note that $\mathcal{A}_m^j = \emptyset$ if $\deg(m) > \frac{n}{2}$. Analogously,

$$B^j = \#\bigcup_{m \text{ irr.}} \mathcal{B}_m^j = -\sum_{0 < \deg m \le n/2} \mu(m) B_m^j.$$

Now we consider the set $\mathcal{M}(n)$. We know that $\#\mathcal{M}(n) = 2^n$. At this point we have to distinguish the three possibilities for u^j. Therefore we define the following functions for $j \in J$:

$$f_j \colon \begin{array}{ccc} \mathcal{M}(n) & \longrightarrow & \mathbb{F}_2, \\ u & \longmapsto & u^j(1) \end{array}.$$

These functions are $\mathbb{F}_2$-linear and their kernels $\mathcal{K}^j$ are the following sets

- $\mathcal{K}^{11} = \{u \in \mathcal{M}(n) \colon u(1) = 0\}$,
- $\mathcal{K}^{01} = \{u \in \mathcal{M}(n) \colon u(1) + u'(1) = 0\}$ and

- $\mathcal{K}^{10} = \{u \in \mathcal{M}(n)\colon u'(1) + 1 = 0\}$

of dimension at least $n-1$, since each map is from an n-dimensional to a one-dimensional vector space. Yet obviously $1 \in \mathcal{M}(n) \setminus \mathcal{K}^j$ for all $j \in J$ and thus $\mathcal{K}^j \subsetneq \mathcal{M}(n)$. Consequently the kernels have dimension exactly $n-1$ and therefore 2^{n-1} elements:

$$\forall j \in J : \#\mathcal{K}^j = 2^{n-1}.$$

Almost needless to say that for every $j \in J$ there are also $2^n - 2^{n-1} = 2^{n-1}$ elements of $\mathcal{M}(n)$ not in the kernel of f_j. Using the inclusion-exclusion principle we have transformed the representation of A^j and B^j, but from these two sums we can still not deduce D^j. Considering the set $\mathcal{M}(n)$ of all u (of cardinality 2^n), we define

1. $C^j := \#\{u \in \mathcal{M}(n)\colon u \,\text{squarefree}, u^j(1) = 1\}$ and
2. $\overline{C}^j := \#\{u \in \mathcal{M}(n)\colon u \,\text{squarefree}, u^j(1) = 0\}$.

Evidently $A^j + C^j = B^j + \overline{C}^j = 2^{n-1}$, because $A^j + C^j$ is the number of all u with $u^j(1) = 1$ and $B^j + \overline{C}^j$ is the number of all u with $u^j(1) = 0$. From our results and the definition of D^j it follows that

$$\begin{aligned} D^j &= C^j - \overline{C}^j = \left(2^{n-1} - A^j\right) - \left(2^{n-1} - B^j\right) = -A^j + B^j \\ &= \sum_{0<\deg m \le n/2} \mu(m) A^j_m - \sum_{0<\deg m \le n/2} \mu(m) B^j_m \\ &= \sum_{0<\deg m \le n/2} \mu(m) \underbrace{\left(A^j_m - B^j_m\right)}_{=T^j_m}. \end{aligned}$$

For $m \in \mathbb{F}_2[x] \setminus \{0\}$ we denote by T^j_m the number of $u \in \mathcal{R}_m$ with $u^j(1) = 1$ minus the number of $u \in \mathcal{R}_m$ with $u^j(1) = 0$:

$$\begin{aligned} T^j_m &= \#\{u \in \mathcal{R}_m\colon u^j(1) = 1\} - \#\{u \in \mathcal{R}_m\colon u^j(1) = 0\} \\ &= A^j_m - B^j_m. \end{aligned}$$

We can simplify the condition of the summation by including the constant polynomial $\sum_{0<\deg m \le n/2} \mu(m) T^j_m = \sum_{\deg m \le n/2} \mu(m) T^j_m$, because for $m = 1$ we have

$$\#\{u \in \mathcal{M}(n)\colon 1 \mid u, u^j(1) = 1\} = 2^{n-1} = \#\{u \in \mathcal{M}(n)\colon 1 \mid u, u^j(1) = 0\}.$$

Thus $T_1^j = 2^{n-1} - 2^{n-1} = 0$.

We will compute T_m^j by distinguishing three cases for m and j each. The results of these computations are given in the table below:

	$j = 11$	$j = 10$	$j = 01$
$m(1) = 0$	$-R_m$	$-R_m$	R_m
$\substack{m(1)=1 \\ \deg(m)<n/2}$	0	0	0
$\substack{m(1)=1 \\ \deg(m)=n/2}$	1	1	1

Before we take a closer look at the different cases, we have to know more about u^{10} and u^{01}. Only u's that are elements of $\mathcal{R}_m$ contribute to T_m^j and for these u we have $u(0) = 1$ and $u \equiv 0 \bmod m^2$. The second condition means that there is a nonzero polynomial $v \in \mathbb{F}_2[x]$ with $u = v \cdot m^2$. So we have

$$\begin{aligned} u^{10} &= (x \cdot u)' \\ &= (x \cdot v \cdot m^2)' \\ &= 1 \cdot v \cdot m^2 + x \cdot (v' \cdot m^2 + v \cdot 2mm') \\ &= v \cdot m^2 + x \cdot v' \cdot m^2 \\ &= (v + xv')m^2 \\ &\text{and} \\ u^{01} &= u' \cdot x + 1 = (vm^2)' \cdot x + 1 \\ &= v' \cdot m^2 \cdot x + v \cdot 2mm' \cdot x + 1 \\ &= v'm^2x + 1. \end{aligned}$$

Now we will deal with the three different cases for m. Within these cases we will look at the three possibilities for j:

Case $\mathbf{m(1) = 0}$:

- **$\mathbf{j = 11}$**:
$$u^{11}(1) = v(1) \cdot m(1)^2 = v(1) \cdot 0 = 0.$$
It follows directly that $T_m^{11} = -R_m$.

- **$\mathbf{j = 10}$**:
$$u^{10}(1) = (v(1) + x(1) \cdot v'(1)) \cdot m(1)^2 = 0.$$
Thus: $T_m^{10} = -R_m$.

- $\mathbf{j = 01}$:
$$u^{01}(1) = v'(1) \cdot m(1)^2 \cdot x(1) + 1 = 1.$$
It follows immediately that $T_m^{01} = R_m$.

Case $\mathbf{m(1) = 1}$ and $\mathbf{\deg(m) < \frac{n}{2}}$:
For all $j \in J$ we have to insert 1 in the corresponding representation for u^j and get the following equations for the different j:

- $\mathbf{j = 11}$: $u^{11}(1) = v(1) \cdot m(1)^2 = v(1)$.
- $\mathbf{j = 10}$: $u^{10}(1) = (v(1) + x(1) \cdot v'(1)) \cdot m(1)^2 = v(1) + v'(1)$.
- $\mathbf{j = 01}$: $u^{01}(1) = v'(1) \cdot m(1)^2 \cdot x(1) + 1 = v'(1) + 1$.

In every case $v \in \mathbb{F}_2[x] \backslash \{0\}$, $v(0) = 1$ and the maximal degree of v is determined by $\deg(m)$. Now, for all j we can look at the function ε^j that maps u^j to $u^j(1) \in \mathbb{B}$. All functions ε^j are $\mathbb{F}_2$-linear and their kernels are the sets $\{u^j(1) = 0\}$. Obviously, $\varepsilon^j(1) = 1$ for all j and consequently we have

$$\forall j \colon T_m^j = 0.$$

Case $\mathbf{m(1) = 1}$ and $\mathbf{\deg(m) = \frac{n}{2}}$:
Before we split this case, we look at the v we have to consider here. When $\deg(m) = \frac{n}{2}$, it follows that $\deg(v) = 0$, since $\deg(m^2) = 2 \cdot \deg(m) = 2 \cdot \frac{n}{2} = n$. Hence the only possible v is $v = 1$! This means that for all three cases we have to insert $v = 1$. Then we get:

- $\mathbf{j = 11}$:
$$u^{11}(1) = v(1) = 1.$$
Thus $T_m^{11} = 1$ under these conditions.
- $\mathbf{j = 10}$:
$$u^{10}(1) = v(1) + v'(1) = 1 + 0 = 1.$$
So again $T_m^{10} = 1$.
- $\mathbf{j = 01}$:
$$u^{01}(1) = v'(1) + 1 = 1.$$
Hence we also have $T_m^{01} = 1$.

For the following equations it is important to remember our global assumption (5.8) in particular $m(0) = 1$. Therefore we have for $j \in \{11, 10\}$:

$$\begin{aligned} D^j &= \sum_{\deg m \le n/2} \mu(m) T_m^j \\ &= -\sum_{\substack{\deg m \le n/2 \\ m(1)=0}} \mu(m) R_m + \sum_{\substack{\deg m = n/2 \\ m(1)=1}} \mu(m). \end{aligned} \tag{5.9}$$

For $j = 01$ the result differs in the sign for the former sum:

$$D^{01} = \sum_{\substack{\deg m \le n/2 \\ m(1)=0}} \mu(m) R_m + \sum_{\substack{\deg m = n/2 \\ m(1)=1}} \mu(m). \tag{5.10}$$

We can use the following estimates for all three values of j. First we take a closer look at the second sum. If n is odd, the sum vanishes. Otherwise, since $\mu(m) \in \{-1, 0, 1\}$ we get the trivial bound $|\mu(m)| \le 1$. There exist $2^{n/2+1}$ polynomials m with $\deg(m) \le \frac{n}{2}$. Two bits (the first and the last) are fixed from the conditions $\deg(m) = \frac{n}{2}$ and $m(0) = 1$. Under these restrictions there are $2^{n/2-1}$ polynomials left. The condition $m(1) = 1$ cuts the number of polynomials m we have to look at in half once again. We obtain:

$$\Big| \sum_{\substack{\deg m = n/2 \\ m(1)=m(0)=1}} \mu(m) \Big| \le \sum_{\substack{\deg m = n/2 \\ m(1)=m(0)=1}} |\mu(m)| \le \sum_{\substack{\deg m = n/2 \\ m(1)=m(0)=1}} 1 = 2^{n/2-2} = \frac{1}{4} \cdot 2^{n/2}. \tag{5.11}$$

For the estimate of the first sum it is useful to know a bit more about $\mathcal{R}_m$:

$$\begin{aligned} \mathcal{R}_m &= \{u \in \mathcal{M}(n) \colon u \equiv 0 \bmod m^2\} \\ &= \{u \in \mathcal{M}(n) \colon \exists\, v \in \mathbb{F}_2[x] \colon u = v \cdot m^2, v(0) = 1\} \\ &= \{u \in \mathbb{F}_2[x] \colon \exists\, v \in \mathbb{F}_2[x] \colon u = v \cdot m^2, v(0) = 1, \deg(v) \le n - 2\deg(m)\}. \end{aligned} \tag{5.12}$$

Moreover, $\deg(v) = \deg(u) - 2\deg(m)$ and $\deg u \le n$. It follows:

$$R_m = 2^{n-2\deg m}.$$

Now, we obtain for the first sum

$$\begin{aligned} \sum_{\substack{\deg m \le n/2 \\ m(1)=0}} \mu(m) R_m &= \sum_{\substack{\deg m \le n/2 \\ m(1)=0}} \mu(m) 2^{n-2\deg m} \\ &= \sum_{m(1)=0} \mu(m) 2^{n-2\deg m} - \underbrace{\sum_{\substack{\deg m > n/2 \\ m(1)=0}} \mu(m) 2^{n-2\deg m}}_{\text{error term}}. \end{aligned} \tag{5.13}$$

Here, we will first look for an upper bound for the error term. For any $d \geq 1$ we know that the number of polynomials m with $\deg m = d$ and $m(0) = 1$ is 2^{d-1}. If we require additionally that $m(1) = 0$, then the number of these m is 2^{d-2}. (This only makes sense when $d \geq 2$.) This gives:

$$
\begin{aligned}
\Big| \sum_{\substack{\deg m > n/2 \\ m(1)=0}} \mu(m) 2^{n-2\deg m} \Big| &\leq \sum_{\substack{\deg m > n/2 \\ m(1)=0}} |\mu(m) 2^{n-2\deg m}| \\
&\leq \sum_{\substack{\deg m > n/2 \\ m(1)=0}} 2^{n-2\deg m} = \sum_{d > n/2} \sum_{\substack{\deg m = d \\ m(1)=0}} 2^{n-2d} \\
&= \sum_{d > n/2} 2^{d-2} \cdot 2^{n-2d} = \sum_{d > n/2} 2^{n-d-2} \\
&= \sum_{d>0} 2^{n-n/2-d-2} = 2^{n/2-2} \sum_{d>0} 2^{-d} \\
&= 2^{n/2-2} = \frac{1}{4} \cdot 2^{n/2}.
\end{aligned} \tag{5.14}
$$

Now, there is only one sum left to estimate, this sum is the same in all considered cases. The only irreducible polynomial over $\mathbb{F}_2[x]$ with $w(1) = 0$ is $w = x+1$, because a polynomial w with $w(1) = 0$ must have at least one factor $x+1$. With that in mind, we can use Euler's product formula and Berlekamp's identity (Section 5.1.2) to obtain the following:

$$
\begin{aligned}
\sum_{\substack{m(1)=0 \\ m(0)=1}} \mu(m) 2^{-2\deg m} &= \sum_{\substack{m(1) \text{ arb.} \\ m(0)=1}} \mu(m) 2^{-2\deg m} - \sum_{\substack{m(1)=1 \\ m(0)=1}} \mu(m) 2^{-2\deg m} \\
&= \prod_{w \in I_0} \left(1 - 2^{-2\deg w}\right) - \prod_{w \in I_1} \left(1 - 2^{-2\deg w}\right) \\
&= \frac{2}{3} - \frac{8}{9} = -\frac{2}{9}.
\end{aligned} \tag{5.15}
$$

At this point we have to distinguish the different possibilities for j again, when we insert the results of our estimations to get an approximation for the D^j from (5.9) and (5.10):

- For $j \in \{11, 10\}$ the number D^j satisfies:

$$\begin{aligned} D^j &= -\sum_{\substack{\deg m \le n/2 \\ m(1)=0}} \mu(m) R_m + \sum_{\substack{\deg m = n/2 \\ m(1)=1}} \mu(m) \\ &= -\sum_{m(1)=0} \mu(m) 2^{n-2\deg m} + \sum_{\substack{\deg m > n/2 \\ m(1)=0}} \mu(m) 2^{n-2\deg m} + \sum_{\substack{\deg m = n/2 \\ m(1)=1}} \mu(m) \\ &= \frac{2}{9} \cdot 2^n + \sum_{\substack{\deg m > n/2 \\ m(1)=0}} \mu(m) 2^{n-2\deg m} + \sum_{\substack{\deg m = n/2 \\ m(1)=1}} \mu(m) \end{aligned}$$

  It follows that

$$\begin{aligned} \left| D^j - \frac{2}{9} \cdot 2^n \right| &= \left| \sum_{\substack{\deg m > n/2 \\ m(1)=0}} \mu(m) 2^{n-2\deg m} + \sum_{\substack{\deg m = n/2 \\ m(1)=1}} \mu(m) \right| \\ &\le \left| \sum_{\substack{\deg m > n/2 \\ m(1)=0}} \mu(m) 2^{n-2\deg m} \right| + \left| \sum_{\substack{\deg m = n/2 \\ m(1)=1}} \mu(m) \right| \\ &\le \frac{1}{4} \cdot 2^{n/2} + \frac{1}{4} \cdot 2^{n/2} \\ &= \frac{1}{2} \cdot 2^{n/2}. \end{aligned}$$

- In the same way we can get the following approximation for D^{01}:

$$\begin{aligned} \left| D^{01} + \frac{2}{9} \cdot 2^n \right| &= \left| \sum_{\substack{\deg m > n/2 \\ m(1)=0}} \mu(m) 2^{n-2\deg m} + \sum_{\substack{\deg m = n/2 \\ m(1)=1}} \mu(m) \right| \\ &\le \left| \sum_{\substack{\deg m > n/2 \\ m(1)=0}} \mu(m) 2^{n-2\deg m} \right| + \left| \sum_{\substack{\deg m = n/2 \\ m(1)=1}} \mu(m) \right| \\ &\le \frac{1}{4} \cdot 2^{n/2} + \frac{1}{4} \cdot 2^{n/2} \\ &= \frac{1}{2} \cdot 2^{n/2}. \end{aligned}$$

Inserting this in the three cases of the lemma, we have:

(i)
$$\begin{aligned} \left| d^{11} + \frac{4}{9} \right| = \left| \frac{4}{9} - \frac{D^{11}}{2^{n-1}} \right| &= \frac{1}{2^{n-1}} \cdot \left| D^{11} - 2^n \cdot \frac{2}{9} \right| \\ &\le \frac{1}{2^{n-1}} \cdot \frac{1}{2} \cdot 2^{n/2} = 2^{n/2-1-n+1} = 2^{-n/2}, \end{aligned}$$

$$(ii) \qquad \left|d^{10}+\frac{4}{9}\right| = \left|\frac{4}{9}-\frac{D^{10}}{2^{n-1}}\right| = \frac{1}{2^{n-1}}\cdot\left|D^{10}-2^n\cdot\frac{2}{9}\right| \leq \frac{1}{2^{n-1}}\cdot\frac{1}{2}\cdot 2^{n/2} = 2^{n/2-1-n+1} = 2^{-n/2}$$

and

$$(iii) \qquad \left|d^{01}-\frac{4}{9}\right| = \left|-\frac{4}{9}-\frac{D^{01}}{2^{n-1}}\right| = \frac{1}{2^{n-1}}\cdot\left|D^{01}+2^n\cdot\frac{2}{9}\right| \leq \frac{1}{2^{n-1}}\cdot\frac{1}{2}\cdot 2^{n/2} = 2^{n/2-1-n+1} = 2^{-n/2}$$

as was claimed. □

For n odd in all three cases the absolute value of the error term is less than $\frac{1}{2}\cdot 2^{n/2}$, because $\sum_{\substack{\deg m=n/2\\ m(1)=1}} \mu(m)$ vanishes, but the further estimates of course hold for all n.

Now, there is only one of the four extreme Fourier coefficients left to consider. We still have to look at the lowest order coefficient. The result was also mentioned in Allender *et al.* (2003), but an explicit proof was not given there. Of course, the proof here will use the same arguments as the proof for the other three extreme coefficients, but there are other ways to prove it and get a better error bound (see Section 7).

LEMMA 5.16. *For the squarefreeness function g we have*

$$\left|d^{00}+\frac{1}{3}\right| \leq 2^{-n/2}.$$

PROOF. First, we will simplify the representation of d^{00}:

$$\begin{aligned}
d^{00} &= \frac{1}{2^n}\sum_{u\in\mathbb{B}^n}(-1)^{g(u)+\sum_i u_i w_i^{00}} \\
&= \frac{1}{2^n}\sum_{u\in\mathbb{B}^n}(-1)^{g(u)+\sum_i u_i 0_i^n} \\
&= \frac{1}{2^n}\sum_{u\in\mathbb{B}^n}(-1)^{g(u)} = \frac{1}{2^n}\Big(\sum_{\substack{u\in\mathbb{B}^n\\ g(u)=0}} 1 - \sum_{\substack{u\in\mathbb{B}^n\\ g(u)=1}} 1\Big) \\
&= \frac{1}{2^n}\Big(\sum_{\substack{u\in\mathbb{B}^n\\ g(u)=0}} 1 - \Big(2^n - \sum_{\substack{u\in\mathbb{B}^n\\ g(u)=0}} 1\Big)\Big) \\
&= \frac{1}{2^n}\Big(2\cdot\sum_{\substack{u\in\mathbb{B}^n\\ g(u)=0}} 1 - 2^n\Big) = \frac{1}{2^{n-1}}\sum_{\substack{u\in\mathbb{B}^n\\ g(u)=0}} 1 - 1.
\end{aligned}$$

Let D denote the number of non-squarefree polynomials $u \in \mathcal{M}(n)$:

$$\begin{aligned} D &= \#\{u \in \mathcal{M}(n) \colon u \text{ not squarefree}\} \\ &= \#\{u \in \mathcal{M}(n) \colon g(u) = 0\}. \end{aligned}$$

Clearly

$$d^{00} = \frac{D}{2^{n-1}} - 1.$$

From (5.7) we have for $m \in \mathbb{F}_2[x] \setminus \{0\}$: $\mathcal{R}_m = \{u \in \mathcal{M}(n) \colon u \equiv 0 \bmod m^2\}$ and $R_m = \#\mathcal{R}_m$. Then as always $\mathcal{R}_m = \emptyset$, if $m(0) = 0$. Therefore once again we make the global assumption (5.8)

$$m(0) = 1 \text{ and } \deg(m) \le \frac{n}{2}.$$

Using the inclusion-exclusion principle we get

$$D = \# \bigcap_{m \,\mathrm{irr}\,.} \mathcal{R}_m = - \sum_{0 < \deg m \le n/2} \mu(m) R_m.$$

Here, it is important to exclude the one polynomial with degree 0, because unlike in the proof of Lemma 5.6, in this case the error that would be caused by including the polynomial 1 would not be canceled. For the estimate we need again that $R_m = 2^{n-2\deg m}$. Now, we can deal with D:

$$\begin{aligned} D &= - \sum_{0 < \deg m \le n/2} \mu(m) R_m \\ &= - \sum_{0 < \deg m \le n/2} \mu(m) 2^{n-2\deg m} \\ &= - \sum \mu(m) 2^{n-2\deg m} + \sum_{\deg m > n/2} \mu(m) 2^{n-2\deg m} + \mu(1) 2^{n-2\deg(1)} \\ &= -2^n \sum \mu(m) 2^{-2\deg m} + \underbrace{\sum_{\deg m > n/2} \mu(m) 2^{n-2\deg m}}_{\text{error term}} + 2^n \end{aligned}$$

We have already estimated this error term in the proof of Lemma 5.6 with the result that:

$$\Big| \sum_{\substack{\deg m > n/2 \\ m(0)=1}} \mu(m) 2^{n-2\deg m} \Big| \le 2^{n/2-1} = \frac{1}{2} \cdot 2^{n/2}.$$

So D satisfies:

$$\begin{aligned}\left|D + 2^n \sum \mu(m) 2^{-2\deg(m)} - 2^n\right| &= \left|D + 2^n \left(\sum \mu(m) 2^{-2\deg(m)} - 1\right)\right| \\ &= \Big|\sum_{\deg m > n/2} \mu(m) 2^{n-2\deg m}\Big| \\ &\leq \frac{1}{2} \cdot 2^{n/2}.\end{aligned}$$

Once again we use Euler's product formula with Berlekamp's identity to obtain the following (see (5.15)):

$$\sum_{m(0)=1} \mu(m) 2^{-2\deg m} = \frac{2}{3}.$$

Consequently,

$$\left|D + 2^n \left(\frac{2}{3} - 1\right)\right| = \left|D - \frac{1}{3} \cdot 2^n\right| \leq \frac{1}{2} \cdot 2^{n/2}.$$

Inserting this in our formula for d^{00}, it follows that

$$\begin{aligned}\left|d^{00} + \frac{1}{3}\right| &= \left|\frac{D}{2^{n-1}} - 1 + \frac{1}{3}\right| = \left|\frac{D}{2^{n-1}} - \frac{2}{3}\right| \\ &= \left|\frac{1}{2^{n-1}}\right| \left|D - \frac{1}{3} \cdot 2^n\right| \\ &\leq \frac{1}{2^{n-1}} \cdot \frac{1}{2} \cdot 2^{n/2} \\ &= 2^{-n/2}\end{aligned}$$

□

This concludes our investigation of the extreme Fourier coefficients over $\mathbb{F}_2$ for the squarefreeness function.

5.2 The Coprimality Function

Investigating the coprimality function we were also lead to believe that there are four Fourier coefficients differing significantly from the others. We got this perception from a lot of extensive calculations shown in Section 4.2. Due to the definition of the coprimality function $h\colon \{0,1\}^\ell \times \{0,1\}^\ell \to \{0,1\}$, we only look at even $n = 2\ell$. We consider the two sequences

$$w^{01} = 0^\ell 1^\ell,\ w^{10} = 1^\ell 0^\ell,$$

and furthermore, as was done before, the 1-sequence $w^{11} = 1^\ell 1^\ell = 1^n$ and the 0-sequence $w^{00} = 0^\ell 0^\ell = 0^n$, which yield the four "extreme" coefficients for this function.

For the coprimality function h we define the highest order coefficient $d^{11} = \widetilde{h}(w^{11})$, the lowest order coefficient $d^{00} = \widetilde{h}(w^{00})$ and additionally the two coefficients which belong to the other sequences mentioned above $d^{01} = \widetilde{h}(w^{01})$ and $d^{10} = \widetilde{h}(w^{10})$. As before the polynomials that we plug into our Boolean function will be elements of the following set:

$$\mathcal{M}(\ell) = \{u \in \mathbb{F}_2[x] : \deg u \leq \ell, u \equiv 1 \bmod x\}.$$

Thus $h\colon \mathcal{M}(\ell)^2 \to \mathbb{B}$. The Fourier coefficients at w^{01} and w^{10} are very close to $-\frac{4}{9}$ asymptotically and at w^{11} to $\frac{4}{9}$. A proof for d^{11} was already given by Allender *et al.* (2003), but as for the squarefreeness function there was no explicite error bound mentioned: $d^{11} = \frac{4}{9} + O(2^{-n/2})$. To our knowledge the results of the following lemma are also new:

LEMMA 5.17. *For the coprimality function h we have*

(i) $\left|d^{11} - \frac{4}{9}\right| \leq 2^{-\ell}$,

(ii) $\left|d^{10} + \frac{4}{9}\right| \leq 2^{-\ell}$,

(iii) $\left|d^{01} + \frac{4}{9}\right| \leq 2^{-\ell}$.

PROOF. For the coprimality function the joint proof of all three bounds is less complicated than the proof for the squarefreeness function. To abbreviate the proof we recall the set $J = \{01, 10, 11\}$ from the proof of Lemma 5.6. Furthermore, for the coprimality function we must always look at pairs of polynomials, consequently, in order to determine the Fourier coefficients, we

must take the sum over all pairs $(u,v) \in (\mathbb{B}^\ell)^2$. To prove all the three bounds simultaneously we define

$$\begin{aligned}(u,v)^{11} &= (u,v)\\ (u,v)^{10} &= (u,0^\ell)\\ (u,v)^{01} &= (0^\ell,v)\end{aligned}$$

As in the proof for the squarefreeness function we will have to look at the Hamming weight of $(u,v)^j$ and we will also plug 1 into the pairs of polynomials as follows:

$(u,v)^j(1) := u(1)+v(1) = u(1)-1+v(1)-1+2 = |u|+|v|+2 \equiv |(u,v)^j| \bmod 2.$

Then we have for all $j \in J$:

$$d^j = \frac{1}{2^n} \sum_{(u,v)\in(\mathbb{B}^\ell)^2} (-1)^{h(u,v)\sum_{1\le i\le n}(u,v)_i w_i^j}.$$

Again we can make use of the correspondance between w^j and $(u,v)^j$. For the coprimality function w^{01} represents the pair (a_1,a_2) of polynomials, where a_1 is the zero polynomial and $a_2 = 1+x+x^2+x^3+\ldots$. Accordingly, w^{10} represents the pair (a_2,a_1) and w^{11} the pair (a_2,a_2). We have for all $(u,v), j$:

$$\sum_{1\le i\le n} (u,v)_i w_i^j = \sum_{1\le i\le n} (u,v)_i^j w_i^j = \sum_{1\le i\le n} (u,v)_i^j = |(u,v)^j| = (u,v)^j(1).$$

Thus we have for all three cases:

$$d^j = \frac{1}{2^n} \sum_{u\in\mathbb{B}^n} (-1)^{h(u,v)+|(u,v)^j|}.$$

Therefore we can do the same regrouping as in the previous proof:

$$\begin{aligned} d^j &= \frac{1}{2^n} \sum_{(u,v)\in(\mathbb{B}^\ell)^2} (-1)^{h(u,v)+|(u,v)^j|}\\ &= \frac{1}{2^n}\Big(\sum_{\substack{(u,v)\in(\mathbb{B}^\ell)^2\\ h(u,v)=0}} (-1)^{|(u,v)^j|} - \sum_{\substack{(u,v)\in(\mathbb{B}^\ell)^2\\ h(u,v)=1}} (-1)^{|(u,v)^j|}\Big)\\ &= \frac{1}{2^n}\Big(- \sum_{\substack{(u,v)\in(\mathbb{B}^\ell)^2\\ h(u,v)=1}} (-1)^{|(u,v)^j|} - \sum_{\substack{(u,v)\in(\mathbb{B}^\ell)^2\\ h(u,v)=1}} (-1)^{|(u,v)^j|}\Big)\\ &= -\frac{1}{2^{n-1}} \sum_{\substack{(u,v)\in(\mathbb{B}^\ell)^2\\ h(u,v)=1}} (-1)^{|(u,v)^j|}. \end{aligned}$$

Now we have for all d^j, $j \in J$:

$$d^j = -\frac{1}{2^{n-1}} \cdot \Big(\sum_{\substack{(u,v)\in(\mathbb{B}^\ell)^2 \\ h(u,v)=1 \\ (u,v)^j(1)=1}} 1 - \sum_{\substack{(u,v)\in(\mathbb{B}^\ell)^2 \\ h(u,v)=1 \\ (u,v)^j(1)=0}} 1 \Big).$$

Let $\mathcal{N}$ denote the set of pairs $(u,v) \in \mathcal{M}(\ell)^2$ with $\gcd(u,v) = 1$:

$$\mathcal{N} = \{(u,v) \in \mathcal{M}(\ell)^2 \colon h(u,v) = 1\}.$$

Then for all $j \in J$ we define G^j as the number of pairs $(u,v) \in \mathcal{N}$ with $|(u,v)^j| = 0$ minus the number of $(u,v) \in \mathcal{N}$ with $|(u,v)^j| = 1$:

$$G^j = \#\{(u,v) \in \mathcal{N} \colon |(u,v)^j| = 0\} - \#\{(u,v) \in \mathcal{N} \colon |(u,v)^j| = 1\}.$$

In particular this means

$$d^j = -\frac{G^j}{2^{n-1}}.$$

For $m \in \mathbb{F}_2[x] \setminus \{0\}$ we define the subset of $\mathcal{M}(\ell)^2$ where both coordinates are multiples of m:

$$\mathcal{S}_m = \{(u,v) \in \mathcal{M}(\ell)^2 \colon u \equiv v \equiv 0 \bmod m\}$$

and let $S_m = \#\mathcal{S}_m$ denote its size. Then it is clear that $S_m = \emptyset$ if $m(0) = 0$, since $x \mid m$, $m \mid u$ and $m \mid v$ imply $x \mid u$ and $x \mid v$, but then $(u,v) \notin \mathcal{M}(\ell)^2$. Also $\mathcal{S}_m = \emptyset$ if $\deg(m) > \ell$. In order to rule out these trivial cases we make the following global assumption:

$$m(0) = 1 \text{ and } \deg(m) \le \ell. \tag{5.18}$$

For $m \in \mathbb{F}_2[x] \setminus \{0\}$ and $j \in J$ we denote by Q_m^j the number of pairs $(u,v) \in \mathcal{S}_m$ with $(u,v)^j(1) = 0$ minus the number of $(u,v) \in \mathcal{S}_m$ with $(u,v)^j(1) = 1$:

$$Q_m^j \;=\; \#\{(u,v) \in \mathcal{S}_m \colon (u,v)^j(1) = 1\} - \#\{(u,v) \in \mathcal{S}_m \colon (u,v)^j(1) = 0\}.$$

Once again we use the inclusion-exclusion principle Theorem 5.2 to obtain

$$G^j = \sum_{0<\deg m\le\ell} \mu(m) Q_m^j = \sum_{\deg m\le\ell} \mu(m) Q_m^j.$$

The latter equality follows from the fact that for the constant polynomial $m = 1$ it holds that:

$$\begin{aligned} & \#\{(u,v) \in \mathcal{M}(\ell)^2 \colon 1 \mid u, 1 \mid v, (u,v)^j(1) = 1\} \\ = \; & 2^{n-1} \\ = \; & \#\{(u,v) \in \mathcal{M}(\ell)^2 \colon 1 \mid u, 1 \mid v, (u,v)^j(1) = 0\}. \end{aligned}$$

Thus $Q_1^j = 2^{n-1} - 2^{n-1} = 0$. We have used similar reasoning before in the proof of Lemma 5.6, so now we can abstain from another tedious execution of the inclusion-exclusion principle. Below one can see the different values for Q_m^j with regard to the three cases for m and j each:

	$j = 01$	$j = 10$	$j = 11$
$m(1) = 0$	$-S_m$	$-S_m$	S_m
$\substack{m(1)=1 \\ \deg(m)<n/2}$	0	0	0
$\substack{m(1)=1 \\ \deg(m)=n/2}$	1	1	1

Only pairs (u, v) that are elements of $\mathcal{S}_m$ contribute to Q_m^j and for these pairs we have

- $u(0) = 1$ and $v(0) = 1$,
- $u \equiv v \equiv 0 \bmod m$ and hence
- there are $r_1, r_2 \in \mathbb{F}_2[x] \setminus \{0\}$ such that $u = r_1 \cdot m, v = r_2 \cdot m$.

Now, we are ready for the obligatory case distinction for Q_m^j. We look at different cases for m and within those cases consider the possible values of j:

Case $\mathbf{m(1) = 0}$:

- $\mathbf{j = 11}$: First, we look at how Q_m^{11} behaves in this case:

  $$u(1) = r_1(1) \cdot m(1) = 0 = r_2(1) \cdot m(1) = v(1).$$

  It follows directly that $Q_m^{11} = S_m$ for all m with $m(1) = 0$, because here $(u,v)^{11}(1) = u(1) + v(1) = 0$ always holds true.

- $\mathbf{j \in \{01, 10\}}$: Considering Q_m^{10} and Q_m^{01}, we have

  $$\begin{aligned} u(1) &= r_1(1) \cdot m(1) = 0, \\ v(1) &= r_2(1) \cdot m(1) = 0 \text{ and} \\ 0^\ell(1) &= 1. \end{aligned}$$

It follows that $(u,v)^j(1) = 1$ and therefore $Q_m^{10} = Q_m^{01} = -S_m$ for all m with $m(1) = 0$.

Case $\mathbf{m(1) = 1}$ and $\mathbf{deg(m) < \ell}$:

- $\mathbf{j = 11}$: When we insert 1 into the formulae for u and v, we get

$$u(1) = r_1(1) \text{ and } v(1) = r_2(1).$$

Furthermore

$$\begin{aligned} &\#\{r_1, r_2 \in \mathbb{F}_2[x] \setminus \{0\} \colon r_1(1) + r_2(1) = 0\} \\ &= \#\{r_1, r_2 \in \mathbb{F}_2[x] \setminus \{0\} \colon r_1(1) + r_2(1) = 1\}. \end{aligned}$$

So Q_m^{11} equals 0 in this case.

- $\mathbf{j \in \{01, 10\}}$: For these two remaining cases, insertion of 1 yields:

$$\begin{aligned} u(1) &= r_1(1) \cdot m(1) = r_1(1), \\ v(1) &= r_2(1) \cdot m(1) = r_2(1) \text{ and} \\ 0^\ell(1) &= 1. \end{aligned}$$

For $k \in \{1, 2\}$ the degree of r_k is determined by the degree of m, other than that r_k is not subject to restrictions except

$$r_k \in \mathbb{F}_2[x] \setminus \{0\}, r_k(0) = 1.$$

For every degree of m less than ℓ we have $\#\{r_k(1) = 1\} = \#\{r_k(1) = 0\}$ and therefore $\#\{r_k(1) + 1 = 1\} = \#\{r_k(1) + 1 = 0\}$. Therefore Q_m^{10} and Q_m^{01} equal 0 here.

Case $\mathbf{m(1) = 1}$ and $\mathbf{deg(m) = \ell}$:
From the previous case we know $u(1) = r_1(1)$ and $v(1) = r_2(1)$. The condition $\deg(m) = \ell$ implies that $\deg(r_1) = \deg(r_2) = 0$. Thus $r_1 = r_2 = 1$ and $u = v = m$, therefore $u(1) = v(1) = m(1) = 1$.

- $\mathbf{j = 11}$: $Q_m^{11} = 1$ in this case.

- $\mathbf{j \in \{01, 10\}}$: $u(1) = v(1) = 1$. So $Q_m^{10} = Q_m^{01} = 1$.

We know $G^j = \sum_{\deg m \leq \ell} \mu(m) Q_m^j$ and recall the global assumption (5.18). Currently we have for $j \in \{10, 01\}$:

$$G^j = - \sum_{\substack{\deg m \leq \ell \\ m(1)=0}} \mu(m) S_m + \sum_{\substack{\deg m = \ell \\ m(1)=1}} \mu(m). \tag{5.19}$$

For G^{11} we have a slightly different result, because of the sign of the first sum

$$G^{11} = \sum_{\substack{\deg m \leq \ell \\ m(1)=0}} \mu(m) S_m + \sum_{\substack{\deg m = \ell \\ m(1)=1}} \mu(m). \tag{5.20}$$

Anyhow, the following estimates we will do for the benefit of all cases, because for an estimate of the individual sums we do not need to pay attention to the different sign. We have already estimated the second sum in (5.11):

$$\Big| \sum_{\substack{\deg m = \ell \\ m(1)=m(0)=1}} \mu(m) \Big| \leq \frac{1}{4} \cdot 2^\ell.$$

$\mathcal{S}_m$ is defined similarly to $\mathcal{R}_m$ (5.12) and in fact we have:

$$S_m = \left(2^{\ell - \deg(m)}\right)^2 = 2^{n - 2\deg(m)} = R_m.$$

With this knowledge we proceed as we did in (5.13):

$$\begin{aligned} \sum_{\substack{\deg m \leq \ell \\ m(1)=0}} \mu(m) S_m &= \sum_{\substack{\deg m \leq \ell \\ m(1)=0}} \mu(m) 2^{n-2\deg m} \\ &= \sum_{m(1)=0} \mu(m) 2^{n-2\deg m} - \underbrace{\sum_{\substack{\deg m > \ell \\ m(1)=0}} \mu(m) 2^{n-2\deg m}}_{\text{error term}}. \end{aligned}$$

We already know an upper bound for the absolute value of the error term from (5.14):

$$\Big| \sum_{\substack{\deg m > \ell \\ m(1)=0}} \mu(m) 2^{n-2\deg m} \Big| \leq \frac{1}{4} \cdot 2^\ell.$$

Furthermore we know the value of the first sum from (5.15):

$$\sum_{\substack{m(1)=0 \\ m(0)=1}} \mu(m) 2^{-2\deg m} = -\frac{2}{9}.$$

Now we will insert the results of our various computations into equations (5.19) and (5.20).

- For $j \in \{10, 01\}$ we get:

$$\begin{aligned}\left|G^j - \frac{2}{9}\cdot 2^n\right| &= \Big|\sum_{\substack{\deg m>\ell\\ m(1)=0}} \mu(m)2^{n-2\deg m} + \sum_{\substack{\deg m=\ell\\ m(1)=1}} \mu(m)\Big| \\ &\le \Big|\sum_{\substack{\deg m>\ell\\ m(1)=0}} \mu(m)2^{n-2\deg m}\Big| + \Big|\sum_{\substack{\deg m=\ell\\ m(1)=1}} \mu(m)\Big| \\ &= \frac{1}{4}\cdot 2^\ell + \frac{1}{4}\cdot 2^\ell \\ &= \frac{1}{2}\cdot 2^\ell.\end{aligned}$$

- For G^{11} it holds that:

$$\begin{aligned}\left|G^{11} + \frac{2}{9}\cdot 2^n\right| &= \Big|\sum_{\substack{\deg m>\ell\\ m(1)=0}} \mu(m)2^{n-2\deg m} + \sum_{\substack{\deg m=\ell\\ m(1)=1}} \mu(m)\Big| \\ &\le \Big|\sum_{\substack{\deg m>\ell\\ m(1)=0}} \mu(m)2^{n-2\deg m}\Big| + \Big|\sum_{\substack{\deg m=\ell\\ m(1)=1}} \mu(m)\Big| \\ &= \frac{1}{4}\cdot 2^\ell + \frac{1}{4}\cdot 2^\ell \\ &= \frac{1}{2}\cdot 2^\ell.\end{aligned}$$

Inserting for the three cases of the lemma we get:

1. For d^{11}:

$$\begin{aligned}\left|d^{11} - \frac{4}{9}\right| &= \left|-\frac{4}{9} - \frac{G^{11}}{2^{n-1}}\right| = \frac{1}{2^{n-1}}\cdot\left|G^{11} + 2^n\cdot\frac{2}{9}\right| \\ &\le \frac{1}{2^{n-1}}\cdot\frac{1}{2}\cdot 2^\ell = 2^{\ell-1-n+1} = 2^{-\ell}.\end{aligned}$$

2. For d^j, $j \in \{10, 01\}$:

$$\begin{aligned}\left|d^j + \frac{4}{9}\right| &= \left|\frac{4}{9} - \frac{G^j}{2^{n-1}}\right| = \frac{1}{2^{n-1}}\cdot\left|G^j - 2^n\cdot\frac{2}{9}\right| \\ &\le \frac{1}{2^{n-1}}\cdot\frac{1}{2}\cdot 2^\ell = 2^{\ell-1-n+1} = 2^{-\ell}.\end{aligned}$$

This is as requested. □

Now, we still have to estimate the lowest order Fourier coefficient. The following result was already mentioned by Allender *et al.* (2003), as was the case for the squarefreeness function, but without any error bound. Actually, we will get a better error bound with another kind of proof in Section 7.2.

LEMMA 5.21. *For the coprimality function h we have*

$$\left| d^{00} + \frac{1}{3} \right| \leq 2^{-\ell}.$$

PROOF. First, we will transform the representation of d^{00} using the same notation as in the proof of Lemma 5.17:

$$d^{00} = \frac{1}{2^n} \sum_{(u,v)\in(\mathbb{B}^\ell)^2} (-1)^{h(u,v)} = \frac{1}{2^{n-1}} \sum_{\substack{(u,v)\in(\mathbb{B}^\ell)^2 \\ h(u,v)=0}} 1 - 1.$$

Let G denote the number of non-coprime pairs of polynomials $u, v \in \mathcal{M}(\ell)$:

$$\begin{aligned} G &:= \#\{u \in \mathcal{M}(\ell)^2 \colon u \text{ and } v \text{ not coprime}\} \\ &= \#\{u \in \mathcal{M}(\ell)^2 \colon h(u,v) = 0\}. \end{aligned}$$

Clearly

$$d^{00} = \frac{G}{2^{n-1}} - 1.$$

As in the previous proof we define for $m \in \mathbb{F}_2[x] \setminus \{0\}$:

$$\mathcal{S}_m = \{(u,v) \in \mathcal{M}(\ell)^2 \colon u \equiv v \equiv 0 \bmod m\} \text{ and } S_m = \#\mathcal{S}_m.$$

Then, as before, $\mathcal{S}_m = \emptyset$, if $m(0) = 0$. Therefore we once again make the global assumption (5.18):

$$m(0) = 1 \text{ and } \deg(m) \leq \frac{n}{2}.$$

By the inclusion-exclusion principle Theorem 5.2 we derive

$$G = \# \bigcap_{m \text{ irr.}} \mathcal{S}_m = - \sum_{0<\deg m\leq\ell} \mu(m) S_m.$$

For the estimation we need once again the value $S_m = 2^{n-2\deg m}$. This yields the following formula for G:

$$\begin{aligned} G &= -\sum_{0<\deg m\le \ell} \mu(m) S_m \\ &= -\sum_{0<\deg m\le \ell} \mu(m) 2^{n-2\deg m} \\ &= -2^n \sum \mu(m) 2^{-2\deg m} + \underbrace{\sum_{\deg m>\ell} \mu(m) 2^{n-2\deg m}}_{\text{error term}} + 2^n \end{aligned}$$

From the proof of Lemma 5.16 we know that

$$\Big|\sum_{\substack{\deg m>\ell \\ m(0)=1}} \mu(m) 2^{n-2\deg m}\Big| \le \frac{1}{2}\cdot 2^\ell$$

$$\text{and } -2^n \sum_{m(0)=1} \mu(m) 2^{-2\deg m} = -2^n \cdot \frac{2}{3}$$

Thus we have

$$\begin{aligned} \left|G + 2^n\cdot\frac{2}{3} - 2^n\right| &= \left|G + 2^n\left(\frac{2}{3}-1\right)\right| \\ &= \left|G - 2^n\cdot\frac{1}{3}\right| \\ &= \Big|\sum_{\deg m>\ell} \mu(m) 2^{n-2\deg m}\Big| \\ &\le \frac{1}{2}\cdot 2^\ell. \end{aligned}$$

Inserting this into the formula for d^{00} yields:

$$\begin{aligned} \left|d^{00} + \frac{1}{3}\right| &= \left|\frac{G}{2^{n-1}} - 1 + \frac{1}{3}\right| = \left|\frac{G}{2^{n-1}} - \frac{2}{3}\right| \\ &= \left|\frac{1}{2^{n-1}}\right| \left|G - \frac{1}{3}\cdot 2^n\right| \\ &\le \frac{1}{2^{n-1}}\cdot\frac{1}{2}\cdot 2^\ell \\ &= 2^{-\ell} \end{aligned}$$

This is just what was claimed. □

This concludes the proof of the extreme Fourier coefficients for the coprimality function.

5.3 The Irreducibility Function

As mentioned in Section 4.3 there is no known proof for the Fourier coefficients of the irreducibility function using the same arguments as the proofs for the squarefreeness and coprimality function in this section. However, later on we will present a proof for the highest and lowest order Fourier coefficient of the irreducibility function using different methods (see Section 7.3).

5.4 Squarefreeness vs. Coprimality

The values for the extreme coefficients of the coprimality function and those of the squarefreeness function are very similar. In both cases there are three coefficients whose absolute values converge on $\frac{4}{9}$ and one whose absolute value converges on $\frac{1}{3}$. Using the Parseval identity 2.21 there is less than $\frac{1}{3}$ left for the absolute values of the other Fourier coefficients. It seems only natural to assume that the similarity between the two functions stems from the fact that one can reduce squarefreeness to coprimality:

THEOREM 5.22. *Let $f \in \mathbb{F}_q$, where q prime power and $\deg(f) \geq 1$. Now, f is squarefree if and only if $\gcd(f, f') = 1$.*

PROOF. "$\Rightarrow$" Let us assume that the statement is false and let f be a counter-example of minimal degree. This means: f is squarefree and $g = \gcd(f, f') \neq 1$, therefore $\deg(g) \geq 1$. We consider two cases:
Case 1: $\deg(g) = \deg(f)$.
In this case the derivative of f must be 0, because $\deg(f') < \deg(f) = \deg(g)$. Hence $f = \sum_{0 \leq i \leq n} f_i x^{p \cdot i}$ for some $f_0, \ldots, f_n \in \mathbb{F}_q$. Every f_i is a pth power, since $f_i^q = f_i$ and letting $g_i = f_i^{p^{e-1}}$ we have $g_i^p = f_i^{p^e} = f_i^q = f_i$. It follows that f is a p-th power:

$$f = \sum_{0 \leq i \leq n} f_i x^{p \cdot i} = \sum_{0 \leq i \leq n} g_i^p x^{p \cdot i} = \sum_{0 \leq i \leq n} (g_i x^i)^p = \left(\sum_{0 \leq i \leq n} g_i x^i \right)^p .$$

As p is prime and therefore ≥ 2, we have arrived at a contradiction to our prerequisite that f is squarefree.

Case 2: $\deg(g) < \deg(f)$.
In this case $\deg\left(\frac{f}{g}\right) \geq 1$ and $\gcd\left(\frac{f}{g}, \frac{f'}{g}\right) = 1$. Now, we look at the formal derivative of $\frac{f}{g}$:

$$\left(\frac{f}{g}\right)' = \frac{f'g - fg'}{g^2}.$$

This yields $g^2 \mid (f'g - fg')$. Together with the obvious $g^2 \mid f'g$ it follows that $g^2 \mid fg'$ and thus $g \mid \left(\frac{f}{g} \cdot g'\right)$. Again we look at two cases:
Case A: $\gcd(g, g') = 1$.
Then g must divide $\frac{f}{g}$. Hence $g^2 \mid f$. This is a contradition to the assumption that f is squarefree in this case.
Case B: $\gcd(g, g') \neq 1$.
Here, it follows inductively that g is not squarefree, because $\deg(g) < \deg(f)$ and f was a minimal counter-example. If g is not squarefree, then f is divisible by a square and likewise not squarefree.

"$\Leftarrow$" By contradiction we assume that $\gcd(f, f') = 1$ but f is then not squarefree. This means f can be written as

$$f = g^2 \cdot h,$$

where $g, h \in F_q[x] \setminus \{0\}$ and $\deg(g) \geq 1$. We look at the derivative of f:

$$\begin{aligned} f' &= (g^2)' \cdot h + g^2 \cdot h' \\ &= 2 \cdot g \cdot g' \cdot h + g^2 \cdot h' \\ &= g \cdot (2g' \cdot h + g \cdot h') \end{aligned}$$

It follows that g is a common divisor of f and f' which are therefore not coprime after all. □

Of course, this theorem also holds over fields with characteristic 0. It is a quite simpler proof because the derivative of a polynomial f over such a field only vanishes if f is constant.

6 Some Definitions and Experiments for the Fourier Transform over $\mathbb{F}_q[x]$

In this and the following section we consider once again polynomials with constant coefficient 1, but from now on they will be defined over differing finite fields $\mathbb{F}_q$ with q a prime power. We can still identify a polynomial of degree n with the corresponding n-dimensional vector comprised of its coefficients, i.e.

$$u = u_n x^n + \ldots + u_1 x + 1 \longleftrightarrow (u_1, \ldots, u_n)\,,$$

where $u_1, \ldots, u_n \in \mathbb{F}_q$. Moreover we look at similar Boolean functions as before:

DEFINITION 6.1.
- *The* irreducibility function $f\colon \mathbb{F}_q^n \to \{0,1\}$ *is defined by*

$$f(u_1, \ldots, u_n) = \begin{cases} 1, & \text{if } u \text{ is irreducible,} \\ 0, & \text{otherwise.} \end{cases}$$

- *The* squarefreeness function $g\colon \mathbb{F}_q^n \to \{0,1\}$ *is defined by*

$$g(u_1, \ldots, u_n) = \begin{cases} 1, & \text{if } u \text{ is squarefree,} \\ 0, & \text{otherwise.} \end{cases}$$

- *The* coprimality function $h\colon \mathbb{F}_q^\ell \times \mathbb{F}_q^\ell \to \{0,1\}$ *is defined by*

$$h(v_1, \ldots, v_\ell; w_1, \ldots, w_\ell) = \begin{cases} 1, & \text{if } v \text{ and } w \text{ are coprime,} \\ 0, & \text{otherwise.} \end{cases}$$

There are two possibilities for q, either q is itself a prime number ($q = p$) or q is a prime power ($q = p^e, e \geq 2$). First we will look at the case that q is prime.

In the following we will consider in detail the Fourier transformation over $\mathbb{F}_3$ for our three Boolean functions. After that we will also look briefly at the transformations over $\mathbb{F}_5$ and $\mathbb{F}_7$.

6.1 The Fourier Transform over $\mathbb{F}_3$

6.1.1 The Squarefreeness Function

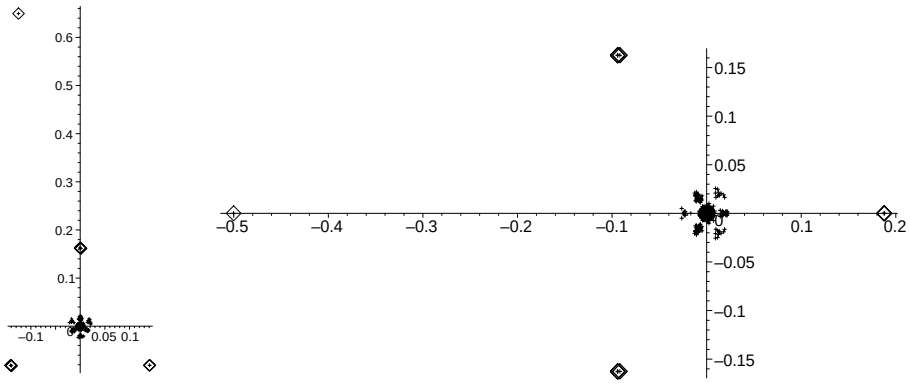
In this section we present the results of the extensive computer calculations that we did for the coefficients for the squarefreeness function over $\mathbb{F}_3$. They strongly suggest that some of the Fourier coefficients converge on certain fixed values. But first let us consider the two interesting variations of the Fourier transform. From (2.16) we get

$$(A) \qquad \check{g}(w) = \frac{1}{3^n} \sum_{u \in \mathbb{F}_3^n} \zeta^{g(u) - \sum_j u_j w_j}, \zeta = e^{\frac{2\pi i}{3}}$$

and furthermore from (2.17)

$$(B) \qquad \widetilde{g}(w) = \frac{1}{3^n} \sum_{u \in \mathbb{F}_3^n} (-1)^{g(u)} \cdot \zeta^{-\sum_j u_j w_j}, \zeta = e^{\frac{2\pi i}{3}}.$$

Obviously, a lot of these Fourier coefficients will have an imaginary part. We plot the coefficients on the complex plane for maximum degree $n = 8$ and both kinds of transformations in Figure 6.1. To us, the second plot seems more



(a) Fourier transform variant (A)

(b) Fourier transform variant (B)

Figure 6.1: Plot of the Fourier coefficients for the squarefreeness function over $\mathbb{F}_3$ with the mentioned transformations and maximum degree $n = 8$ in the complex plane.

beautiful because of its symmetry. Furthermore, we know from Section 2.4,

that (A) is only a linear transformation of (B) and vice versa. In this case, there is a little stretching (respectively compression) and a rotation of 30°. From here on we will only look at transformation (B).

Also taking into consideration the coefficients for a maximum degree $n = 12$, there seems to be only one coefficient with an exceptionally large absolute value, plotted against 0 in Figure 6.2. In Figure 6.3(a) we look at the plot

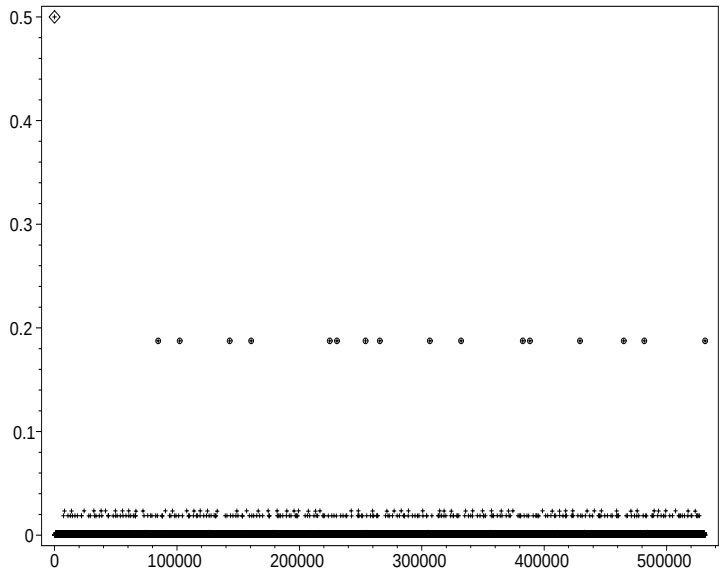


Figure 6.2: Plot of the absolute value of the Fourier coefficients for the square-freeness function over $\mathbb{F}_3$ with transformation (B) and maximum degree $n = 12$.

in the complex plane also for maximum degree $n = 12$ and Fourier transform type (B). We note that the quality of the figure changes a little. Particularly, the structure of the Fourier coefficients other than the lowest order Fourier coefficient becomes clearer. First of all, one can still see three other points in the plot in the complex plane which seem to form an equilateral triangle. Each of these points is hit by more than one coefficient. We will not give a formula for these points, but a proof for the lowest order Fourier coefficient is given in Section 7.1. Looking closer at Figure 6.3(a) we see that there are more points close to 0 that do not seem to actually converge on the origin. In Figure 6.3(b) we just zoomed in on the plot in Figure 6.3(a). The "outer" six points seem to form two equilateral triangles of different sizes, each with a peak on the horizontal axis. For the bigger triangle this point lies in the negative, for the smaller one in the positive range of this axis. We zoom even

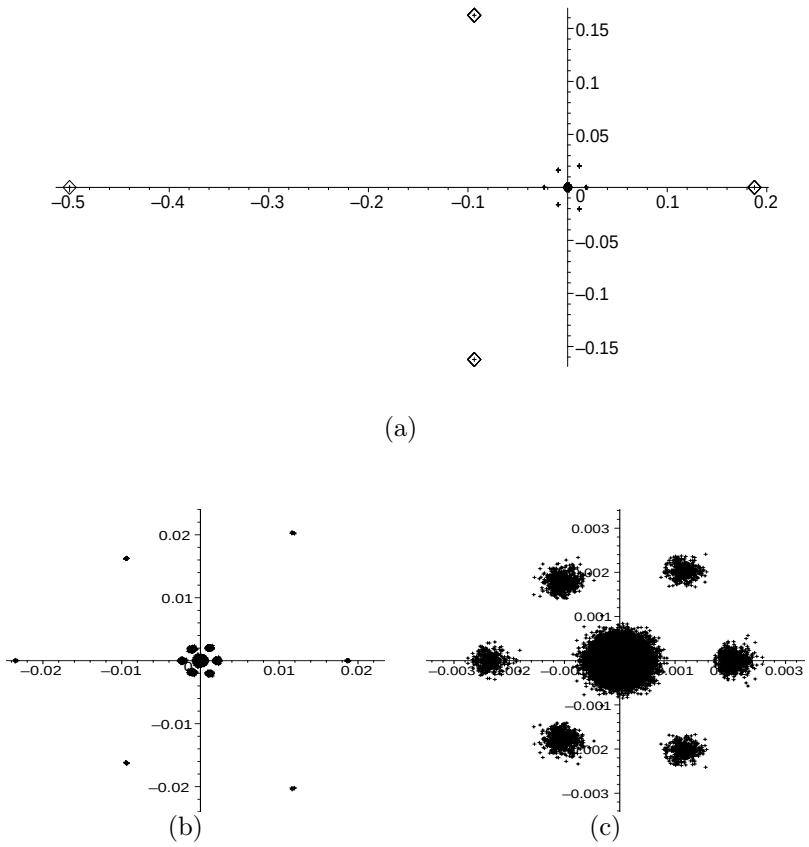


Figure 6.3: Plot of the Fourier coefficients for the squarefreeness function over $\mathbb{F}_3$ with transformation (B) and maximum degree $n = 12$ in the complex plane, zoomed in.

further in Figure 6.3(c). Here, it seems that there are again two triangles, this time rather fuzzy, but the absolute values are already quite small. The Fourier coefficients that form the greatest triangle belong to different "groups" of w's. For example one such w contributing to the larger of the two small triangles is

$$[2, 2, 0, 1, 1, 0]^{n/6}.$$

A small example illustrates this notation sufficiently:

$$[2, 2, 0, 1, 1, 0]^{n/6} \overset{n=14}{=} [2, 2, 0, 1, 1, 0, 2, 2, 0, 1, 1, 0, 2, 2],$$

where the first entry is the lowest order entry. The development of the complex and the absolute values of the lowest order coefficient and the "big triangle" coefficients are listed in Tables 6.1, 6.2, 6.3, 6.4 and 6.5. Table 6.1 displays the absolute values for the lowest order Fourier coefficient for n up to 12. For the other coefficients that apparently do not converge on 0 we only mention the development from 9 to 13 and with fewer digits.

$w = 0^n$

n		n	
1	-1.0000000000	7	-0.5006858711
2	-0.5555555556	8	-0.5000762079
3	-0.5555555556	9	-0.5000762079
4	-0.5061728395	10	-0.5000084676
5	-0.5061728395	11	-0.5000084676
6	-0.5006858711	12	-0.5000009408
		13	-0.5000009408

Table 6.1: The values of the lowest order Fourier coefficients for the squarefreeness function over $\mathbb{F}_3$ and degrees up to 13 for transformation (B).

	$[1,2,0]^{n/3}, [2,2,0,1,1,0]^{n/6}$		$[1,1,0,2,2,0]^{n/6}, [2,1,0]^{n/3}$	
n	complex value z	abs(z)	complex value z	abs(z)
9	$0.187471 + 0.000528i$	0.187472	$0.187471 - 0.000528i$	0.187472
10	0.187539	0.187539	0.187539	0.187539
11	$0.187488 + 0.000088i$	0.187488	$0.187488 - 0.000088i$	0.187488
12	0.187502	0.187502	0.187502	0.187502
13	$0.187498 - 0.000013i$	0.187498	$0.187498 + 0.000013i$	0.187498

Table 6.2: The values of the specified Fourier coefficients for the squarefreeness function over $\mathbb{F}_3$ and degrees up to 13 for transformations (B).

The absolute values of all these nonzero coefficients seem to converge on the same real number and the lowest order Fourier coefficient converges on $\frac{1}{2}$. We will the latter statement prove in the following section Section 7.1.

	$[0,2,1]^{n/3},[0,2,2,0,1,1]^{n/6}$		$[0,1,1,0,2,2]^{n/6},[0,1,2]^{n/3}$	
n	complex value z	abs(z)	complex value z	abs(z)
9	$-0.093278+0.162619i$	0.187472	$-0.093278-0.162619i$	0.187472
10	$-0.093770+0.162414i$	0.187539	$-0.093770-0.162414i$	0.187539
11	$-0.093668+0.162414i$	0.187488	$-0.093668-0.162414i$	0.187488
12	$-0.093756+0.162384i$	0.187507	$-0.093756-0.162384i$	0.187507
13	$-0.093741+0.162384i$	0.187410	$-0.093741-0.162384i$	0.187410

Table 6.3: The values of the specified Fourier coefficients for the squarefreeness function over $\mathbb{F}_3$ and degrees up to 13 for transformations (B).

	$[2,0,1]^{n/3},[1,0,2,2,0,1]^{n/6}$		$[2,0,1,1,0,2]^{n/6},[1,0,2]^{n/3}$	
n	complex value z	abs(z)	complex value z	abs(z)
9	$-0.094345+0.161827i$	0.187321	$-0.094345-0.161827i$	0.187321
10	$-0.093770+0.162414i$	0.187539	$-0.093770-0.162414i$	0.187539
11	$-0.093820+0.162326i$	0.187488	$-0.093820-0.162326i$	0.187488
12	$-0.093756+0.162384i$	0.187507	$-0.093756-0.162384i$	0.187507
13	$-0.093760+0.162371i$	0.187498	$-0.093760-0.162371i$	0.187498

Table 6.4: The values of the specified Fourier coefficients for the squarefreeness function over $\mathbb{F}_3$ and degrees up to 13 for transformations (B).

	$[1,2]^{n/2},2^n$		$1^n,[2,1]^{n/2}$	
n	complex value z	abs(z)	complex value z	abs(z)
9	$-0.093888-0.162619i$	0.187776	$-0.093888+0.162619i$	0.187776
10	$-0.093465-0.162414i$	0.187387	$-0.093465+0.162414i$	0.187387
11	$-0.093770-0.162414i$	0.187539	$-0.093770+0.162414i$	0.187539
12	$-0.093711-0.162384i$	0.187485	$-0.093711+0.162384i$	0.187485
13	$-0.093753-0.162384i$	0.187505	$-0.093753+0.162384i$	0.187505

Table 6.5: The values of the specified Fourier coefficients for the squarefreeness function over $\mathbb{F}_3$ and degrees up to 13 for transformations (B).

6.1.2 The Coprimality Function

From now on we will only look at the following kind of Fourier transform, because of the symmetry arguments we mentioned earlier.

$$\widetilde{h}(w) = \frac{1}{3^n} \sum_{(u,v)\in(\mathbb{F}_3^\ell)^2} (-1)^{h(u)} \cdot \zeta^{-\sum_j u_j w_j}, \zeta = e^{\frac{2\pi i}{3}}. \tag{6.2}$$

Once more we can see that there is only one really big coefficient that differs significantly from the others in its absolute value, and again it is the lowest order Fourier coefficient. In Figure 6.4 we can see the absolute values for the Fourier coefficients for $n = 12$. As for the squarefreeness function we will now

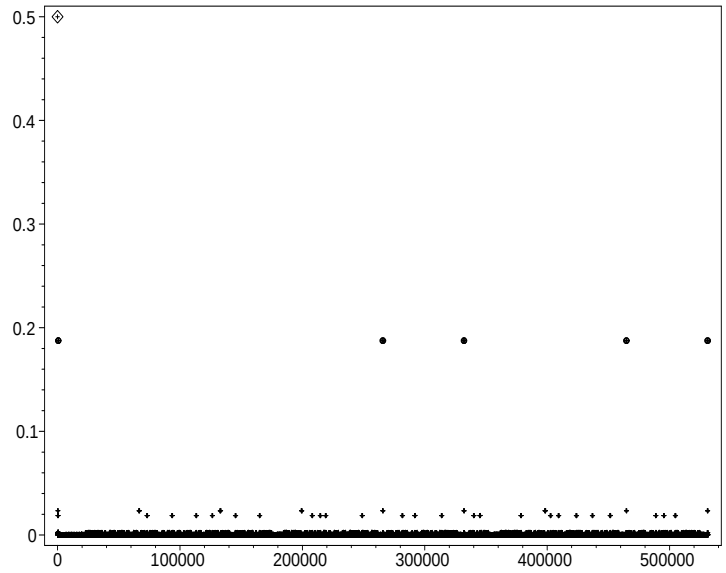


Figure 6.4: Plot of the absolute value of the Fourier coefficients for the coprimality function over $\mathbb{F}_3$ and maximum degree 6 for each polynomial (this means $n = 12$).

look at the plot in the complex plane for $n = 12$ in Figure 6.5(a). Again there is an equilateral triangle whose peaks have got the second largest absolute values (of about 0.2 as is the case for the squarefreeness function). Focussing on a smaller section of this plot in Figure 6.5(b) we see again two smaller triangles. Looking at an even smaller section (both axes from -0.004 to 0.004) we see that there are again two little triangles in Figure 6.5(c). But the absolute values are obviously very small. For the lowest order Fourier coefficient there is a proof in

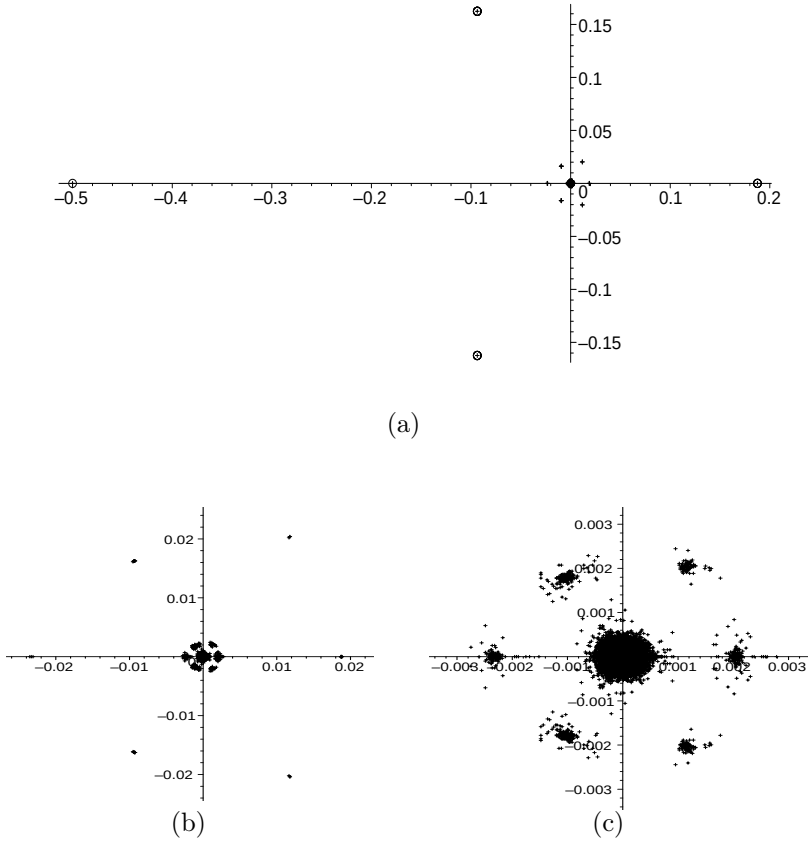


Figure 6.5: Plot of the Fourier coefficients for the coprimality function over $\mathbb{F}_3$ and maximum degree $n = 12$ in the complex plane and zoomed in.

Section 7.2. The values for that coefficient and for the Fourier coefficients that make up the greatest of the three triangles we found are given in the Tables 6.6 and 6.7. The coefficients responsible for this triangle can be split into three groups:

$$a_{\text{cop}} = \{[2^{n/2}, 1^{n/2}], [(1,2)^{n/4}, (2,1)^{n/4}], [(2,1)^{n/4}, (1,2)^{n/4}], [1^{n/2}, 2^{n/2}]\},$$

$$b_{\text{cop}} = \{[(1,2)^{n/4}, 0^{n/2}], [2^{n/2}, 0^{n/2}], [1^n], \\ [(2,1)^{n/4}, (2,1)^{n/4}], [0^{n/2}, (1,2)^{n/4}], [0^{n/2}, 2^{n/2}]\},$$

$$c_{\text{cop}} = \{[1^{n/2}, 0^{n/2}], [(2,1)^{n/4}, 0^{n/2}], [0^{n/2}, 1^{n/2}], \\ [0^{n/2}, (2,1)^{n/4}], [(1,2)^{n/4}, (1,2)^{n/4}], [2^n]\}.$$

Here we used a notation similar to the previous section. For example we look at $[(1,2)^{n/4}, (1,2)^{n/4}]$ where the exponent means

$$[(1,2)^{n/4}, (1,2)^{n/4}] \overset{n=6}{=} [1,2,1,1,2,1].$$

In the following Table 6.6 you can see the values for the lowest order Fourier coefficient and for the coefficients of a_{cop} for n from 2 to 12. For the other

n	0^n	a_{cop}
2	-0.5555555556	0.4444444444
4	-0.5061728395	0.2716049382
6	-0.5006858711	0.2030178326
8	-0.5000762079	0.1899100747
10	-0.5000084675	0.1878439940
12	-0.5000009408	0.1875466891

Table 6.6: The values of the lowest order Fourier coefficient and the coefficients of a_{cop} for the coprimality function over $\mathbb{F}_3$ and (even) degrees up to 12.

two groups one can see the complex and the absolute values (with less digits) in Table 6.7. The similarity of the behavior of the coprimality and the square-

	b_{cop}		c_{cop}	
n	complex value z	abs(z)	complex value z	abs(z)
2	-0.222222	0.222222	-0.222222	0.222222
4	$-0.098765 - 0.128300i$	0.161912	$-0.098765 + 0.128300i$	0.161912
6	$-0.093278 - 0.156811i$	0.182457	$-0.093278 + 0.156811i$	0.182457
8	$-0.093583 - 0.161563i$	0.186710	$-0.093583 + 0.161563i$	0.186710
10	$-0.093719 - 0.162267i$	0.187387	$-0.093719 + 0.162267i$	0.187387
12	$-0.093745 - 0.162365i$	0.187485	$-0.093745 - 0.162365i$	0.187485

Table 6.7: The Values of the specified Fourier coefficients for the coprimality function over $\mathbb{F}_3$ and n up to 12.

freeness function is not surprising. The connection between these two functions is known from Section 5.4. The proof that the lowest order Fourier coefficient converges on $\frac{1}{2}$ is postponed until Section 7.2.

6.1.3 The Irreducibility Function

The irreducibility function for polynomials over $\mathbb{F}_3$ behaves in a way different from the two functions considered previously. It seems that only one coefficient converges on an absolute value different from 0, namely on 1, and thus all the others converge on 0. Again we only look at of the following Fourier transformation

$$\widetilde{f}(w) = \frac{1}{3^n} \sum_{u \in \mathbb{F}_3^n} (-1)^{f(u)} \cdot \zeta^{-\sum_j u_j w_j}, \zeta = e^{\frac{2\pi i}{3}}. \tag{6.3}$$

The first two plots of Fourier coefficients in the complex plane were done for degree $n = 8$ and $n = 12$ (see Figure 6.6 and Figure 6.7). We can see a certain development of the coefficients in the plots.

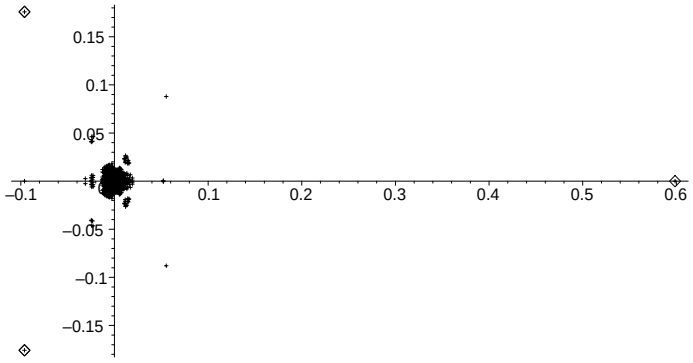


Figure 6.6: Plot of the Fourier coefficients for the irreducibility function over $\mathbb{F}_3$ and maximum degree $n = 8$ in the complex plane.

It is no surprise that once again the lowest order Fourier coefficient is the one that does not converge on 0. In Figure 6.8 and Figure 6.9 one can compare the absolute values of the Fourier coefficients for $n = 8$ and $n = 12$ and make out some tendencies. Most obviously and notably the absolute value of the lowest order coefficient converges on 1, while all the others converge on 0.

Apart from the lowest order Fourier coefficient we will take a short look at those coefficients which are relatively big in Figure 6.6 and Figure 6.7. This means we look at the coefficients at 0^n, $[1,0]^{n/2}$, $[2,0]^{n/2}$, 1^n, $[2,1]^{n/2}$, $[1,2]^{n/2}$, 2^n, $[0,1]^n$ and $[0,2]^{n/2}$. The values of the first three coefficients starting with $n = 6$ are given in Table 6.8. For the next four coefficients and their complex

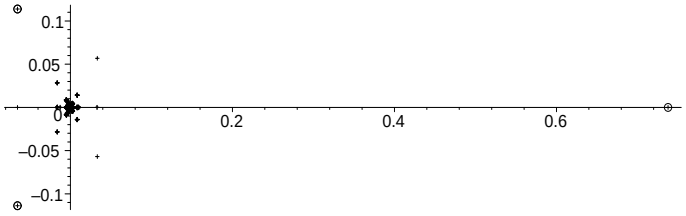


Figure 6.7: Plot of the Fourier coefficients for the irreducibility function over $\mathbb{F}_3$ and maximum degree $n = 12$ in the complex plane.

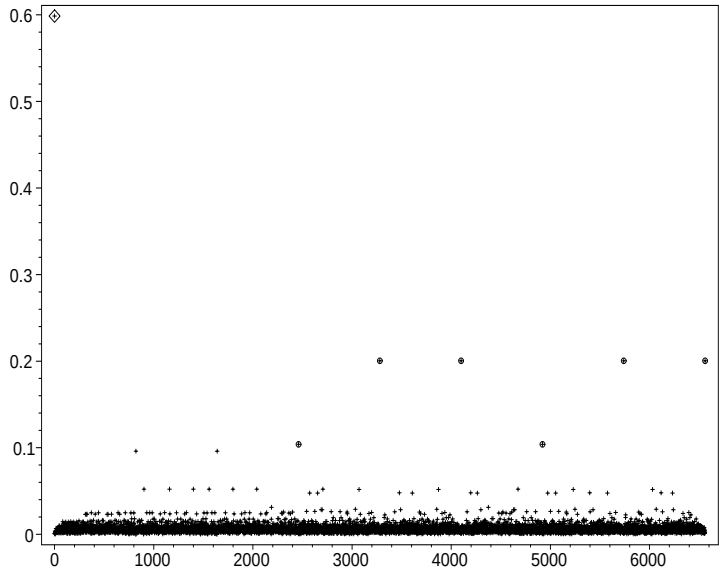


Figure 6.8: Plot of the absolute values of the Fourier coefficients for the irreducibility function over $\mathbb{F}_3$ and maximum degree $n = 8$.

and absolute values (with less digits) look at Table 6.9 and for the last two at Table 6.10.

The tendencies seem clear: The lowest order Fourier coefficient converges on 1 and all the others on 0. A proof for our conjectures about the Fourier coefficients of the irreducibility function will be given in Section 7.3.

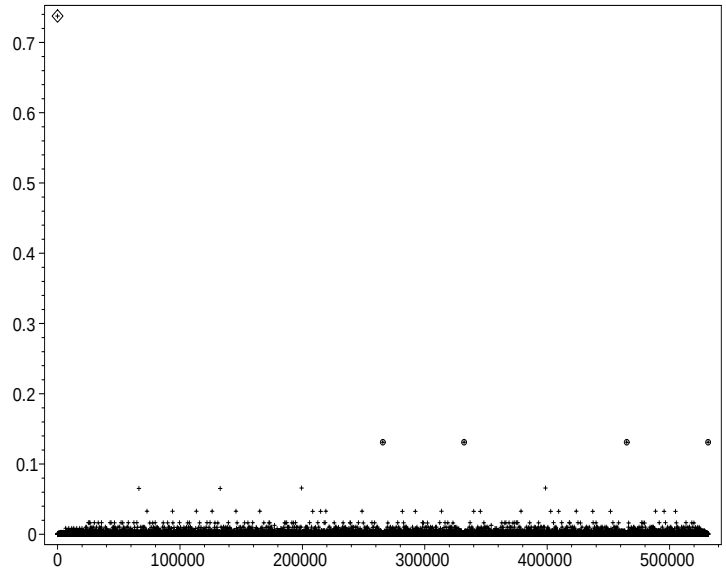


Figure 6.9: Plot of the absolute values of the Fourier coefficients for the irreducibility function over $\mathbb{F}_3$ and maximum degree $n = 12$.

n	0^n	$[1,0]^{n/2}, [2,0]^{n/2}$
6	0.4650205761	−0.1152263374
7	0.5363511660	−0.1097393690
8	0.5985368084	−0.0960219479
9	0.6442615455	−0.0874866636
10	0.6822638825	−0.0783417162
11	0.7122728581	−0.0715676811
12	0.7376754898	−0.0652904085
13	0.7587126323	−0.0602249356

Table 6.8: The values of the specified Fourier coefficients for the irreducibility function over $\mathbb{F}_3$ and degrees from 6 up to 13.

	1^n, $[2,1]^{n/2}$		$[1,2]^{n/2}$,2^n	
n	complex value z	abs(z)	complex value z	abs(z)
6	$-0.115226 + 0.237593i$	0.264059	$-0.115226 - 0.237593i$	0.264059
7	$-0.109739 + 0.202746i$	0.230540	$-0.109739 - 0.202746i$	0.230540
8	$-0.096022 + 0.175819i$	0.200331	$-0.096022 - 0.175819i$	0.200331
9	$-0.087487 + 0.154699i$	0.177724	$-0.087487 - 0.154699i$	0.177724
10	$-0.078342 + 0.138156i$	0.158822	$-0.078342 - 0.138156i$	0.158822
11	$-0.071568 + 0.124780i$	0.143847	$-0.071568 - 0.124780i$	0.143847
12	$-0.065290 + 0.113751i$	0.131157	$-0.065290 - 0.113751i$	0.131157
13	$-0.060225 + 0.104534i$	0.120642	$-0.060225 - 0.104534i$	0.120642

Table 6.9: The values of the specified Fourier coefficients for the irreducibility function over $\mathbb{F}_3$ and n from 6 up to 13.

	$[0,1]^{n/2}$		$[0,2]^{n/2}$	
n	complex value z	abs(z)	complex value z	abs(z)
6	$0.082305 - 0.118796i$	0.144522	$0.082305 + 0.118796i$	0.144522
7	$0.063100 - 0.101373i$	0.119407	$0.063100 + 0.101373i$	0.119407
8	$0.055327 - 0.087909i$	0.103871	$0.055327 + 0.087909i$	0.103871
9	$0.046182 - 0.077350i$	0.090087	$0.046182 + 0.077350i$	0.090087
10	$0.041203 - 0.069078i$	0.080433	$0.041203 + 0.069078i$	0.080433
11	$0.036461 - 0.062390i$	0.072263	$0.036461 + 0.062390i$	0.072263
12	$0.033210 - 0.056876i$	0.065861	$0.033210 + 0.056876i$	0.065861
13	$0.030301 - 0.052267i$	0.060415	$0.030301 + 0.052267i$	0.060415

Table 6.10: The values of the specified Fourier coefficients for the irreducibility function over $\mathbb{F}_3$ and n from 6 up to 13.

6.2 The Fourier Transform over $\mathbb{F}_5$

In this section we present a few plots relating to the computations we ran over $\mathbb{F}_5$.

6.2.1 The Squarefreeness Function

Figure 6.10(a) is done using the following transformation we get from (2.17):

$$\widetilde{g}(w) = \frac{1}{5^n} \sum_{u \in \mathbb{F}_5^n} (-1)^{g(u)} \cdot \zeta^{-\sum_j u_j w_j}, \zeta = e^{\frac{2\pi i}{5}}. \tag{6.4}$$

In this plot we see one coefficient that differs significantly from the others. Not surprisingly it is the lowest order Fourier coefficient. Apart from this we see five other points with a notable difference from the origin. They seem to form a regular pentagon. You can take a closer look in Figure 6.10(b). In Figure 6.10(c) we can see the direct neighborhood of 0. Now, we see ten point clusters that are also seperate from the one around the origin. Five of them are bigger than the other five and each of these sets of point clusters seems to form a regular pentagon as well.

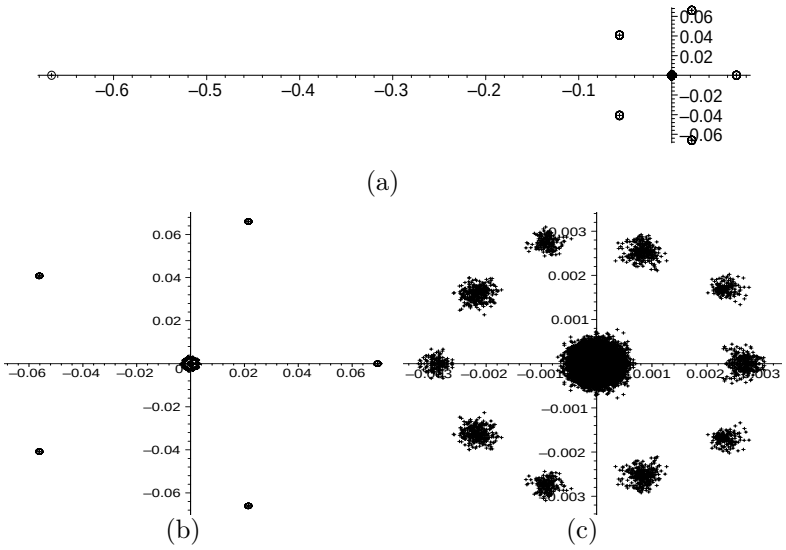


Figure 6.10: Plot of the Fourier coefficients for the squarefreeness function over $\mathbb{F}_5$ and maximum degree $n = 8$ in the complex plane and zoomed in.

6.2.2 The Coprimality Function

Figure 6.11(a) is done using the same kind of transformation that we used for the squarefreeness function:

$$\widetilde{h}(w) = \frac{1}{5^n} \sum_{(u,v)\in(\mathbb{F}_5^2)^\ell} (-1)^{h(u,v)} \cdot \zeta^{-\sum_j u_j w_j}, \zeta = e^{\frac{2\pi i}{5}}, n = 2\ell. \tag{6.5}$$

Again one Fourier coefficient differs significantly from the others and for this function this is also the lowest order coefficient. Apart from this coefficient we note five other points that are clearly different from 0. Not surprisingly, they also seem to form a regular pentagon. Zooming in on the plot, as we did for the squarefreeness function in the previous section, we obtain Figure 6.11(b) and Figure 6.11(c). And again we see two "little" pentagons near the origin.

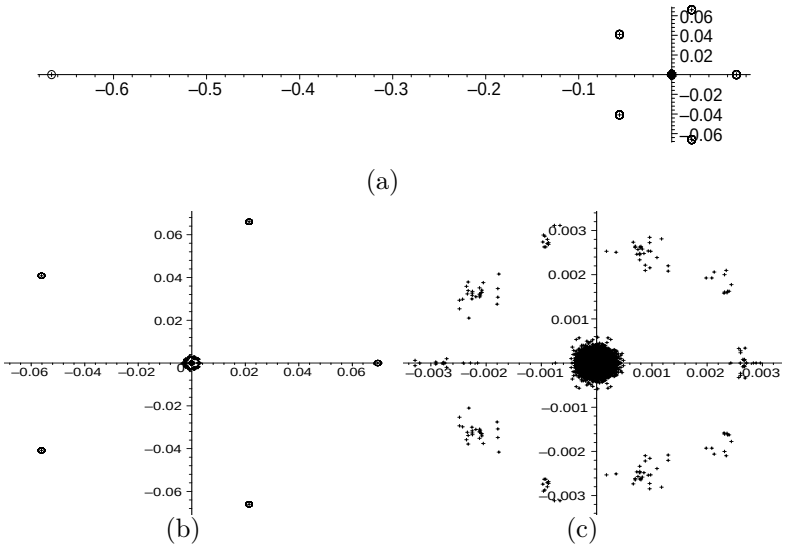


Figure 6.11: Plot of the Fourier coefficients for the coprimality function over $\mathbb{F}_5$ and maximum degree $\ell = 4$ for each polynomial in the complex plane and zoomed in.

6.2.3 The Irreducibility Function

Looking at polynomials defined over the field $\mathbb{F}_5$, the irreducibility function still behaves in a way different from the two other functions. Apparently, once again the lowest order Fourier coefficient converges on 1 whereas all the other coefficients converge on 0. The development is visible in the two following plots for $n = 6$ and $n = 8$ (Figure 6.12(a) and (b)). For these plots we used

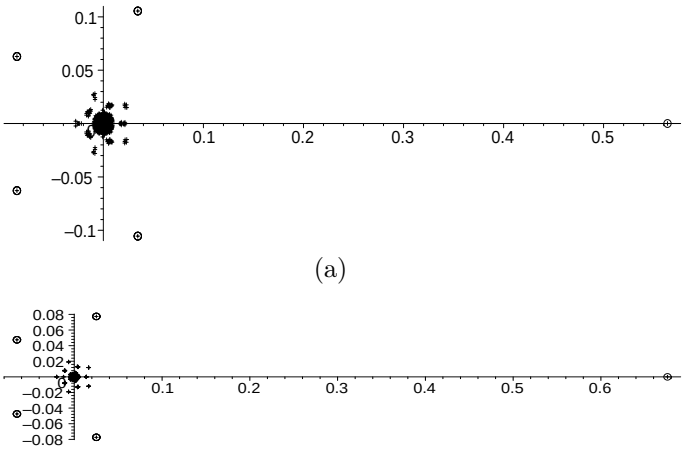


Figure 6.12: Plot of the Fourier coefficients for the irreducibility function over $\mathbb{F}_5$ and maximum degree $n = 6$ and $n = 8$ in the complex plane.

the following transformation:

$$\widetilde{f}(w) = \frac{1}{5^n} \sum_{u \in \mathbb{F}_5^n} (-1)^{f(u)} \cdot \zeta^{-\sum_j u_j w_j}, \zeta = e^{\frac{2\pi i}{5}}. \tag{6.6}$$

6.3 The Fourier Transform over $\mathbb{F}_7$

In this section we present a few plots for the transformations of type (B) over the basic field $\mathbb{F}_7$.

6.3.1 The Squarefreeness Function

As before the transformation is similar to (2.17):

$$\widetilde{g}(w) = \frac{1}{7^n} \sum_{u \in \mathbb{F}_7^n} (-1)^{g(u)} \cdot \zeta^{-\sum_j u_j w_j}, \zeta = e^{\frac{2\pi i}{7}}. \tag{6.7}$$

In Figure 6.13(a) we see that once again the lowest order Fourier coefficient stands out from all the others because it has by far the largest absolute value. Apart from this we see seven other points obviously different from 0. They seem to form a regular heptagon. We zoom in in Figure 6.13(b) and in Figure 6.13(c) we zoom in some more. From previous experiments one might expect to find

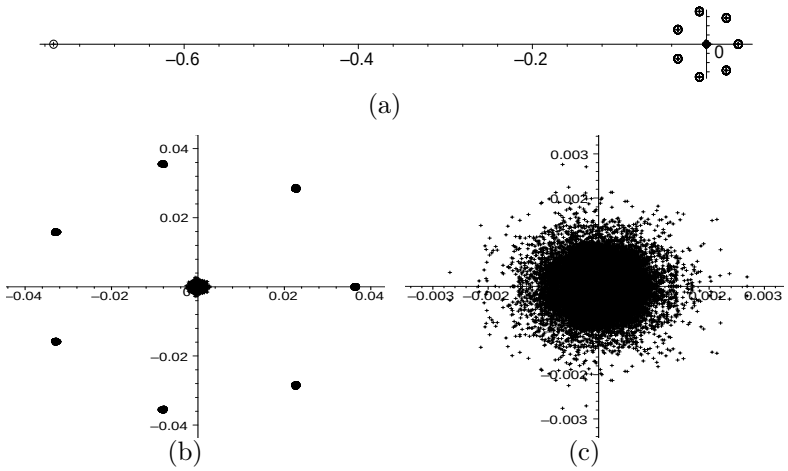


Figure 6.13: Plot of the Fourier coefficients for the squarefreeness function over $\mathbb{F}_7$ and maximum degree $n = 6$ in the complex plane and zoomed in.

two little heptagons, but we cannot make out these geometric figures. Probably they are present but superposed by those coefficients which converge on 0. This is possible because the real and imaginary parts of these coefficients, which do not converge on 0 become smaller and smaller. Also we could only do the calculation for the rather small value of $n = 6$.

6.3.2 The Coprimality Function

For the coprimality function we observe once again a similar behavior as for the squarefreeness function. Our plots are done with the following transformation similar to the one we used for the squarefreeness function:

$$\widetilde{h}(w) = \frac{1}{7^n} \sum_{(u,v)\in(\mathbb{F}_7^2)^\ell} (-1)^{h(u,v)} \cdot \zeta^{-\sum_j u_j w_j}, \zeta = e^{\frac{2\pi i}{7}}, n = 2\ell. \tag{6.8}$$

Again the absolutely largest coefficient is the lowest order Fourier coefficient. And again there are seven points apart from the lowest order coefficient that are obviously different from 0. Not surprisingly, they also seem to form a regular heptagon, see Figure 6.14(a) and Figure 6.14(b). Zooming in we do not see two little heptagons in Figure 6.14 (c).

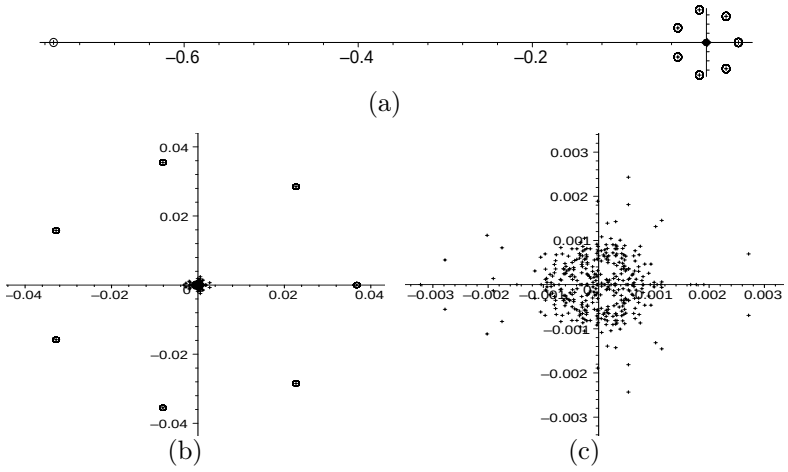


Figure 6.14: Plot of the Fourier coefficients for the coprimality function over $\mathbb{F}_7$ and maximum degree $n = 6$ in the complex plane and zoomed in.

6.3.3 The Irreducibility Function

Looking at the transformation

$$\widetilde{f}(w) = \frac{1}{7^n} \sum_{u \in \mathbb{F}_7^n} (-1)^{f(u)} \cdot \zeta^{-\sum_j u_j w_j}, \zeta = e^{\frac{2\pi i}{7}}. \tag{6.9}$$

the results for the irreducibility function over $\mathbb{F}_7$ are again different from those for the other two functions. The lowest order Fourier coefficient converges on 1 whereas all the other coefficients converge on 0. One can see this development in the two following plots for $n = 4$ and $n = 6$ (Figure 6.15(a) and (b)).

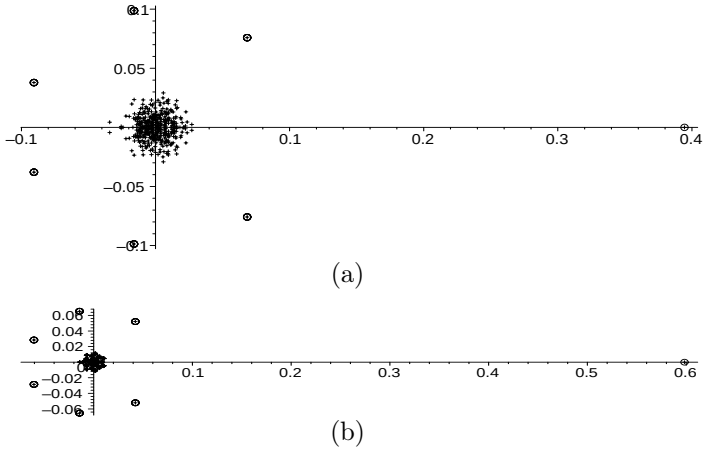


Figure 6.15: Plot of the Fourier coefficients for the irreducibility function over $\mathbb{F}_7$ and maximum degree $n = 4$ and $n = 6$ in the complex plane.

6.4 The Fourier Transform over $\mathbb{F}_4$

For $q = 4$ there are more possibilities for a correct Fourier transformation than for the examples we looked at before. This discrepancy was already mentioned in Section 2.4. We have already decided to use that transformation where the Boolean function φ is replaced by $u \to (-1)^{\varphi(u)}$. Hence there are two "main" possibilities left. In everyone of the following sections we start with the transformation of kind (2.19) and go on with kind (2.20).

6.4.1 The Squarefreeness Function

As promised we will start with the results for the first kind of transformation:

$$(A) \qquad \widetilde{g}(w) = \frac{1}{2^{2n}} \sum_{u \in \mathbb{F}_2^{2n}} (-1)^{g(u) - \sum_j u_j w_j}$$

Since the only primitive root of unity for characteristic 2 is -1, we have to work with it here and therefore a plot in the complex plane has no use at all. Hence, we plot the Fourier coefficient of w against the number $(w)_2$. Such a plot for $n = 8$ is done in Figure 6.16. For $n = 9$ there is not much of a change

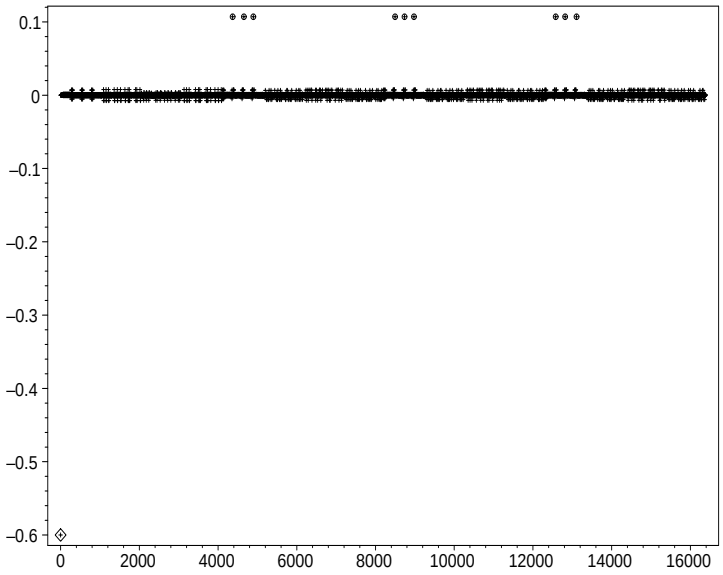


Figure 6.16: Plot of the Fourier coefficients for the squarefreeness function over $\mathbb{F}_4$, maximum degree $n = 8$ and transformation (A).

in the plot (Figure 6.17). The tendency of the lowest order Fourier coefficient

is clear and there are a few coefficients that also do not converge on 0 and that some of them seem to change sign.

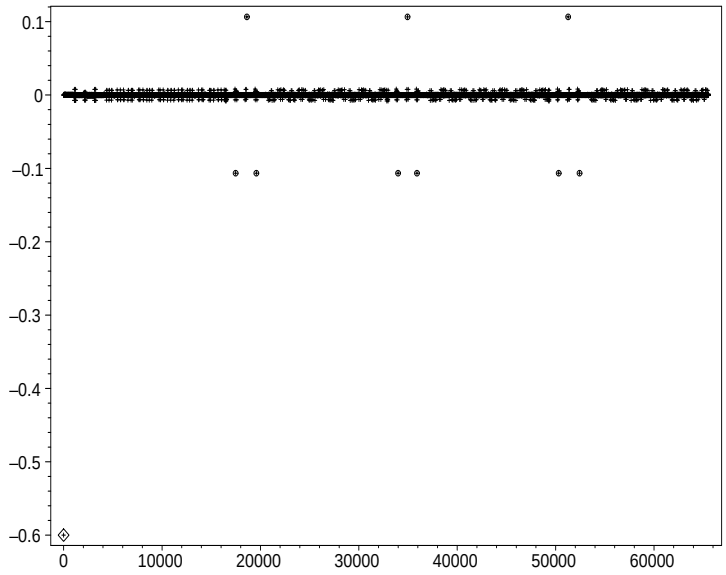


Figure 6.17: Plot of the Fourier coefficients for the squarefreeness function over $\mathbb{F}_4$, maximum degree $n = 9$ and transformation (A).

Now we take a look at the next possibility. For this we will consider an arbitrary prime power q and a primitive q-th root of unity ζ. Recall that our squarefreeness function g maps from $\mathcal{M}(n)$ to $\{0, 1\}$ where $\mathcal{M}(n) = \{u \in \mathbb{F}_q[x] \colon \deg(u) \leq n, u \equiv 1 \bmod x\}$. As stated here we have to identify the elements of $\mathbb{F}_q$ with the elements of $\mathbb{Z}_q$ via an, in principle, arbitrary bijective mapping $\beta \colon \mathbb{Z}_q \to \mathbb{F}_q$. We will also denote the corresponding map from $\mathbb{Z}_q^n$ to $\mathbb{F}_q^n$ by β. This yields a function $\psi \colon \mathbb{Z}_q^n \to \{-1, 1\},\ u \mapsto (-1)^{g(\beta(u))}$. Letting $G = \mathbb{Z}_q^n$ we get a map from G to $\{-1, 1\}$ Then we have a transformation similar to (2.20)

$$(B) \qquad \widetilde{g}^{\beta}(w) = \widehat{\psi}(w) = \frac{1}{q^n} \sum_{u \in \mathbb{Z}_q^n} \psi(u) \cdot \zeta^{-\sum_j u_j w_j}.$$

Now consider any element $w \in G$ and recall that we identify these elements with characters of G, i.e. elements of $\hat{G}$. In order to find relations between the different choices for β we look at functions $\alpha \colon \mathbb{Z}_q \to \mathbb{Z}_q$ and $\gamma \colon \mathbb{F}_q \to \mathbb{F}_q$. We look at the differences that result from using the Fourier transform induced by β and the one induced by $\gamma \circ \beta \circ \alpha$. What we find is this:

- for the case $\alpha(x) = x - c$ for some $c \in \mathbb{Z}_q$ and $\gamma(x) = x$:

$$\widetilde{g}^{\beta\alpha}(w) = \frac{1}{q^n} \sum_{u \in \mathbb{Z}_q^n} (-1)^{g(\beta(u_1-c),\ldots,\beta(u_n-c))} \cdot \zeta^{-\sum_j u_j w_j} = \zeta^{c\sum_j w_j} \cdot \widetilde{g}^{\beta}(w).$$

  Here the Fourier coefficients are permutated and multiplied by roots of unity.

- for the case $\alpha(x) = vx$ for a $v \in \mathbb{Z}_q^\times$ and $\gamma(x) = x$:

$$\widetilde{g}^{\beta\alpha}(w) = \frac{1}{q^n} \sum_{u \in \mathbb{Z}_q^n} (-1)^{g(\beta(vu_1),\ldots,\beta(vu_n))} \cdot \zeta^{-\sum_j u_j w_j} = \widetilde{g}^{\beta}(vw)$$

  Hence in this case we get only a permutation of the coefficients.

- for the case $\alpha(x) = x$ and γ an arbitrary automorphism of $\mathbb{F}_q$:

$$\widetilde{g}^{\gamma\beta}(w) = \frac{1}{q^n} \sum_{u \in \mathbb{Z}_q^n} (-1)^{g(\gamma(\beta(u_1)),\ldots,\gamma(\beta(u_n)))} \cdot \zeta^{-\sum_j u_j w_j}.$$

  Since γ ia an automorphism of $\mathbb{F}_q$, we know that u is squarefree if and only if $\gamma(u)$ is squarefree. Applying γ also does not change the irreducibility or reducibilty of a polynomial nor whether two polynomials are coprime or not. Therefore for all $u_1, \ldots, u_n \in \mathbb{F}_q$ and $\beta\colon \mathbb{Z}_q \to \mathbb{F}_q$ we have $g(\gamma(\beta(u))) = g(\beta(u))$, $h(\gamma(\beta(u))) = h(\beta(u))$ and also $f(\gamma(\beta(u))) = f(\beta(u))$

In all cases the set of Fourier coefficients remains unchanged save for multiplication by roots of unity.

Going back to the case $q = 4$ we can look at all 24 bijective mappings from $\mathbb{Z}_4$ to $\mathbb{F}_4$. They can be seen in Table 6.11, where they are also ordered and labeled β_{00} to β_{23} in a canonical fashion. In the second to last column we denoted the β with the smallest index that corresponds to the current line if you do not allow for a rotation of some coefficients and therefore have the exact same Fourier coefficients, possibly in a different order. In the last column we give the β with the smallest index that gives the same Fourier coefficients if you also allow for rotations around the origin. In the former case we are left with only seven β's to consider and the latter reduces this even further to a mere two cases, namely β_{00} and β_{02}. First we see a plot using function β_{00} and $n = 6$ in Figure 6.18(a). Already in this plot there seem to be several concentric

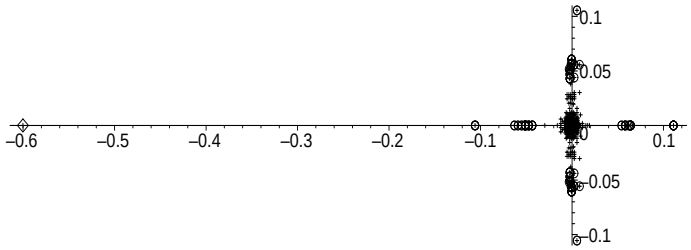
x	0	1	2	3	without shift	with shift
$\beta_{00}(x)$	0	1	α	$\alpha+1$	β_{00}	β_{00}
$\beta_{01}(x)$	0	1	$\alpha+1$	α	β_{00}	β_{00}
$\beta_{02}(x)$	0	α	1	$\alpha+1$	β_{02}	β_{02}
$\beta_{03}(x)$	0	α	$\alpha+1$	1	β_{00}	β_{00}
$\beta_{04}(x)$	0	$\alpha+1$	1	α	β_{02}	β_{02}
$\beta_{05}(x)$	0	$\alpha+1$	α	1	β_{00}	β_{00}
$\beta_{06}(x)$	1	0	α	$\alpha+1$	β_{06}	β_{00}
$\beta_{07}(x)$	1	0	$\alpha+1$	α	β_{06}	β_{00}
$\beta_{08}(x)$	1	α	0	$\alpha+1$	β_{08}	β_{02}
$\beta_{09}(x)$	1	α	$\alpha+1$	0	β_{06}	β_{00}
$\beta_{10}(x)$	1	$\alpha+1$	0	α	β_{08}	β_{02}
$\beta_{11}(x)$	1	$\alpha+1$	α	0	β_{06}	β_{00}
$\beta_{12}(x)$	α	0	1	$\alpha+1$	β_{12}	β_{00}
$\beta_{13}(x)$	α	0	$\alpha+1$	1	β_{13}	β_{02}
$\beta_{14}(x)$	α	1	0	$\alpha+1$	β_{14}	β_{00}
$\beta_{15}(x)$	α	1	$\alpha+1$	0	β_{13}	β_{02}
$\beta_{16}(x)$	α	$\alpha+1$	0	1	β_{14}	β_{00}
$\beta_{17}(x)$	α	$\alpha+1$	1	0	β_{12}	β_{00}
$\beta_{18}(x)$	$\alpha+1$	0	1	α	β_{12}	β_{00}
$\beta_{19}(x)$	$\alpha+1$	0	α	1	β_{13}	β_{02}
$\beta_{20}(x)$	$\alpha+1$	1	0	α	β_{14}	β_{00}
$\beta_{21}(x)$	$\alpha+1$	1	α	0	β_{13}	β_{02}
$\beta_{22}(x)$	$\alpha+1$	α	0	1	β_{14}	β_{00}
$\beta_{23}(x)$	$\alpha+1$	α	1	0	β_{12}	β_{00}

Table 6.11: Listing of all possible functions β.

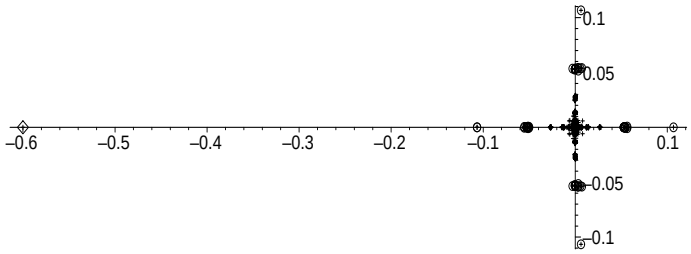
squares. This impression becomes stronger when we look at the corresponding plot for $n = 9$ or then zooming in, see Figure 6.18(b) and Figure 6.19.

Doing the same plots for function β_{02} we make a surprising detection: although we used i as primitve root of unity all the coefficients are real. You can see it in Figure 6.20(a) and Figure 6.20(b).

So, we can look at the second kind of transformation as we looked on the transformations over $\mathbb{F}_2$ by plotting a coefficient w against the number $(w)_4$ as in Figure 6.21. Apparently we have to look at the absolute values of the Fourier coefficients to compare these two transformations. The associated plots are made in Figure 6.22 and Figure 6.23.



(a)



(b)

Figure 6.18: Plot of the Fourier coefficients for the squarefreeness function over $\mathbb{F}_4$, maximum degree $n = 6$ and $n = 9$ and function β_{00} in the complex plane.

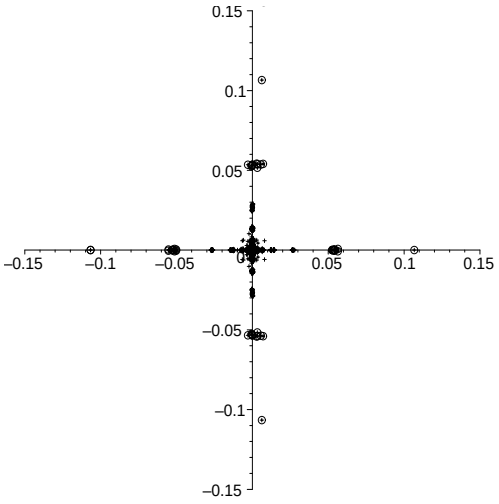
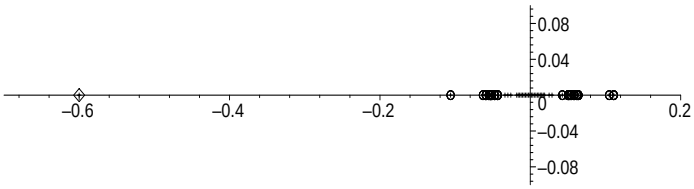
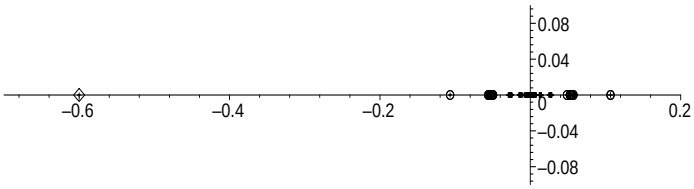


Figure 6.19: Plot of the Fourier coefficients for the squarefreeness function over $\mathbb{F}_4$, maximum degree $n = 9$, function β_{00} and both axes from -0.15 to 0.15 in the complex plane.



(a)



(b)

Figure 6.20: Plot of the Fourier coefficients for the squarefreeness function over $\mathbb{F}_4$, maximum degree $n = 6$ and $n = 9$ and function β_{02} in the complex plane.

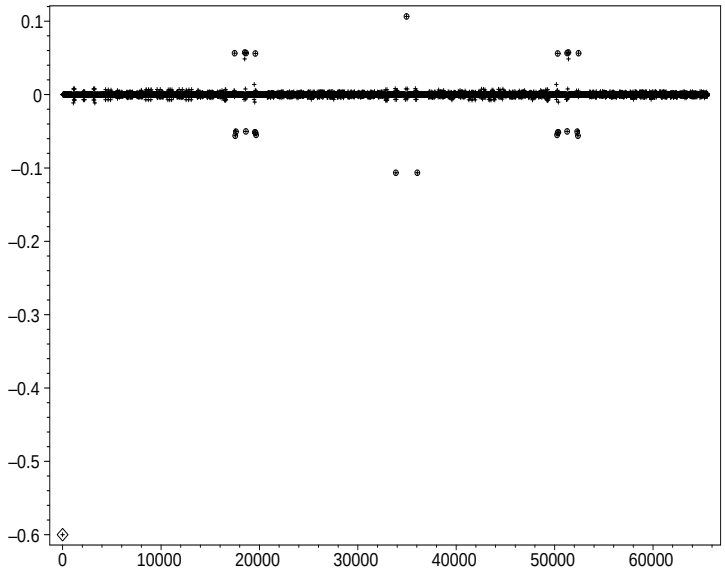


Figure 6.21: Plot of the Fourier coefficients for the squarefreeness function over $\mathbb{F}_4$, maximum degree $n = 9$ and function β_{02}.

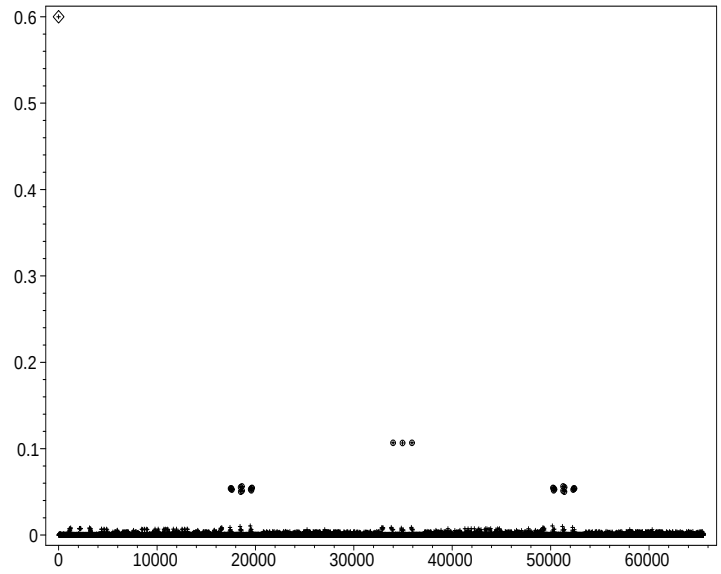


Figure 6.22: Plot of the Fourier coefficients for the squarefreeness function over $\mathbb{F}_4$, maximum degree $n = 9$ and function β_{00}.

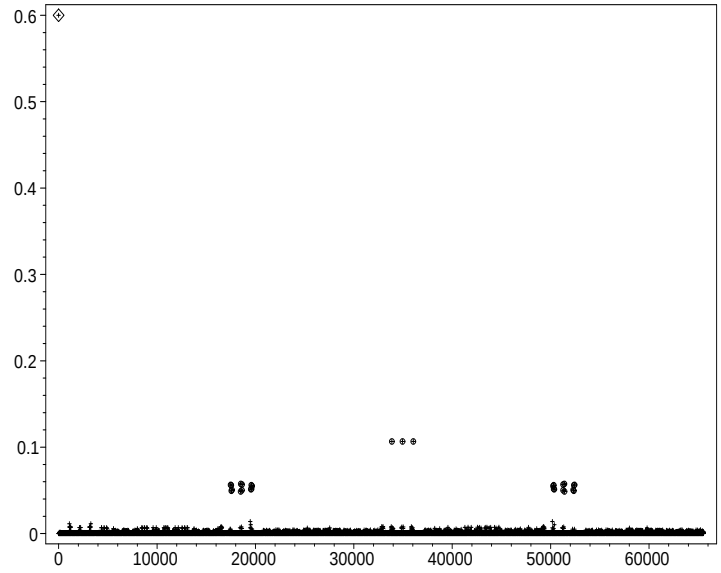


Figure 6.23: Plot of the Fourier coefficients for the squarefreeness function over $\mathbb{F}_4$, maximum degree $n = 9$ and function β_{02}.

6.4.2 The Coprimality Function

Investigating the coprimality function we use the same procedure as for the squarefreeness function. First we look at the following transformation

$$(A) \qquad \widetilde{h}(w) = \frac{1}{2^{2n}} \sum_{(u,v)\in(\mathbb{F}_2^{2\ell})^2} (-1)^{h(u)-\sum_j u_j w_j}.$$

Once again we plot a Fourier coefficient of w against the number $(w)_2$. The plot for $n = 8$ is done in Figure 6.24 and for the next n, which is $n = 10$, there is not much of a change in the plot (Figure 6.25) and the tendency of the lowest order Fourier coefficient is clear.

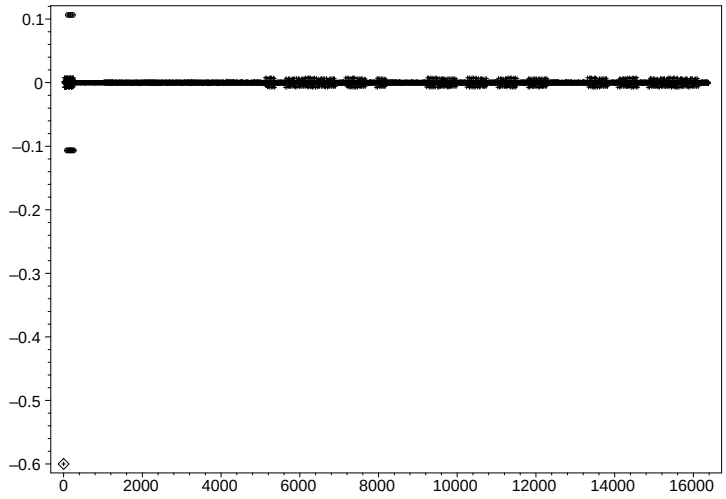


Figure 6.24: Plot of the Fourier coefficients for the coprimality function over $\mathbb{F}_4$, maximum degree $n = 8$ and transformation (A).

Again, we have to consider the other possibilities. Here the transformation is

$$(B) \qquad \widetilde{h}(w) = \widehat{\psi}(w) = \frac{1}{4^n} \sum_{(u,v)\in(\mathbb{Z}_4^{\ell})^2} \psi(u,v) \cdot i^{-\sum_j u_j w_j}.$$

As before we identifiy the elements of $\mathbb{F}_4$ with the elements of $\mathbb{Z}_4$ via a bijective mapping $\beta\colon \mathbb{Z}_4 \to \mathbb{F}_4$. This yields a function $\psi\colon \mathbb{Z}_4^n \to \{-1,1\},\ (u,v) \mapsto (-1)^{g(\beta(u),\beta(v))}$. We argued earlier (see Section 6.4.1) that we only have to look at transformations with functions β_{00} and β_{02}, where $\beta_{00}\colon \mathbb{Z}_4 \to \mathbb{F}_4,\ \{0,1,2,3\} \mapsto$

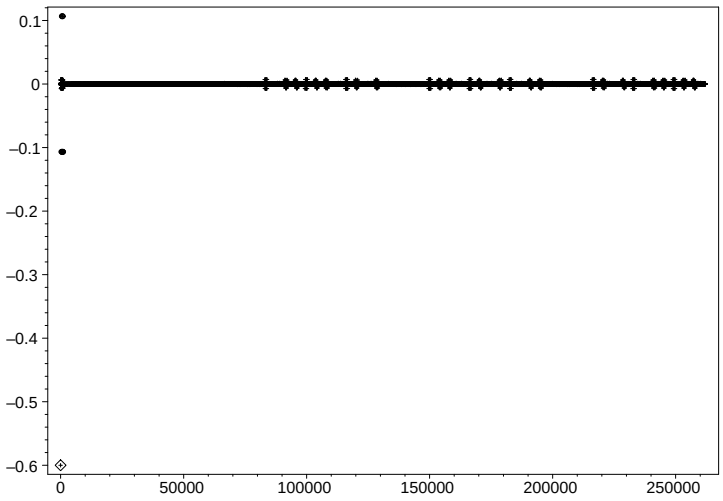
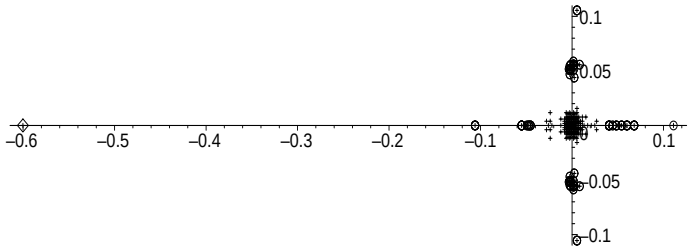


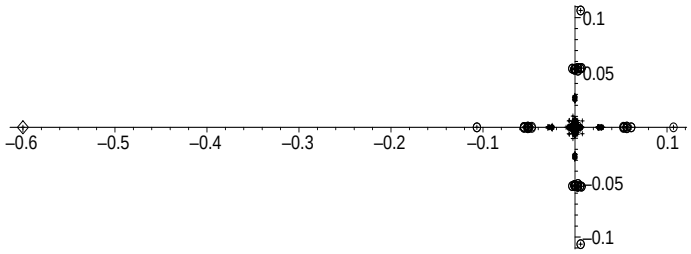
Figure 6.25: Plot of the Fourier coefficients for the coprimality function over $\mathbb{F}_4$, maximum degree $n = 10$ and transformation (A).

$\{0, 1, \alpha, \alpha{+}1\}$ and $\beta_{02} \colon \mathbb{Z}_4 \to \mathbb{F}_4,\ \{0, 1, 2, 3\} \mapsto \{0, \alpha, 1, \alpha{+}1\}$. First we plotted the transformation with function β_{00} and $n = 6$ in Figure 6.26(a). In this plot we see again several concentric squares. This impression grows stronger when we look at the similar plot for $n = 8$ or zooming in on it, see Figure 6.26(b) and Figure 6.27. Plotting with the same parameters but function β_{02} we obtain a now not surprising result: also for the coprimality function all the coefficients are real, see Figure 6.28(a) and (b). As usual we make a plot of this transformation over $\mathbb{F}_4$ by plotting a coefficient w against the number $(w)_4$ as we did in Figure 6.29. We look at the absolute values of the Fourier coefficients for both kinds of transformations in Figure 6.30 and Figure 6.31.

These plots are not very different, but they are clearly different from those we made for the squarefreeness function. Obviously, here the coefficients that do not converge on 0 differ from those we found earlier.



(a)



(b)

Figure 6.26: Plot of the Fourier coefficients for the coprimality function over $\mathbb{F}_4$, maximum degree $n = 6$ and $n = 8$ and function β_{00} in the complex plane.

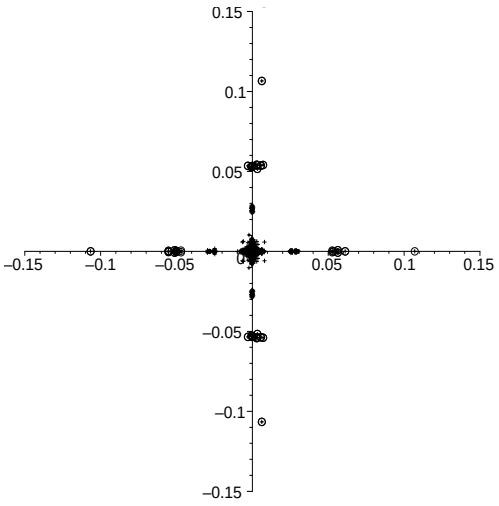
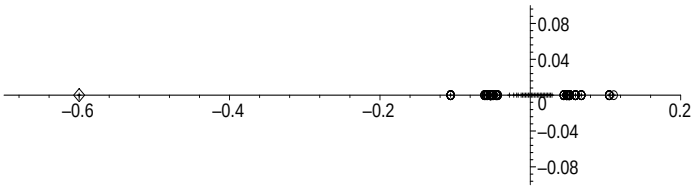
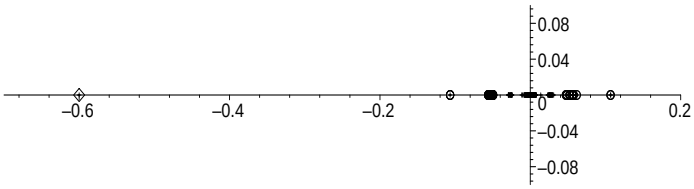


Figure 6.27: Plot of the Fourier coefficients for the coprimality function over $\mathbb{F}_4$, maximum degree $n = 8$, function β_{00} and both axes from -0.15 to 0.15 in the complex plane.



(a)



(b)

Figure 6.28: Plot of the Fourier coefficients for the coprimality function over $\mathbb{F}_4$, maximum degree $n = 6$ and $n = 8$ and function β_{02} in the complex plane.

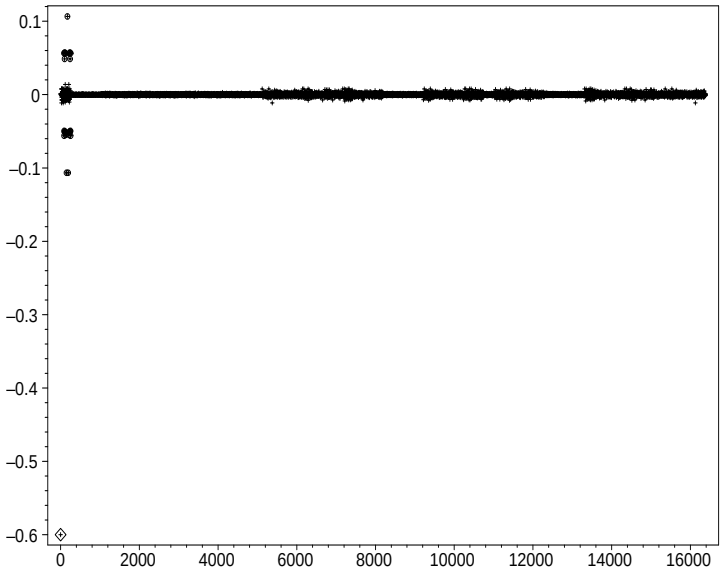


Figure 6.29: Plot of the Fourier coefficients for the coprimality function over $\mathbb{F}_4$, maximum degree $n = 8$ and function β_{02}.

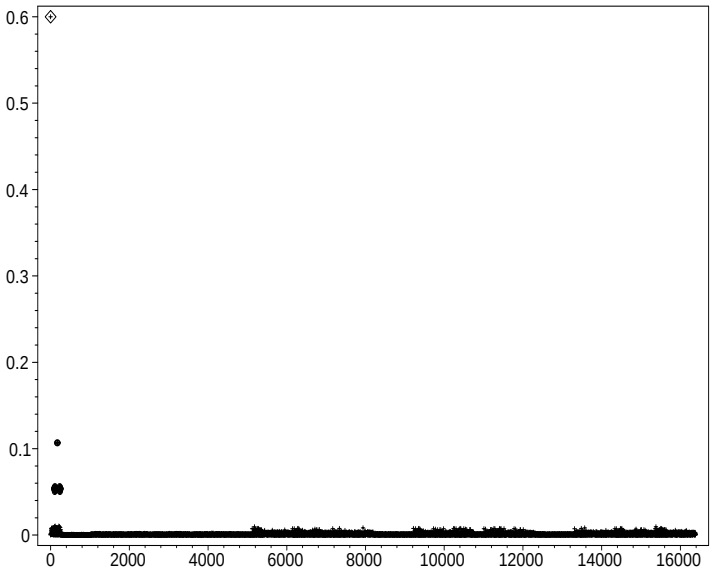


Figure 6.30: Plot of the absolute value of the Fourier coefficients for the coprimality function over $\mathbb{F}_4$, maximum degree $n = 8$ and function β_{00}.

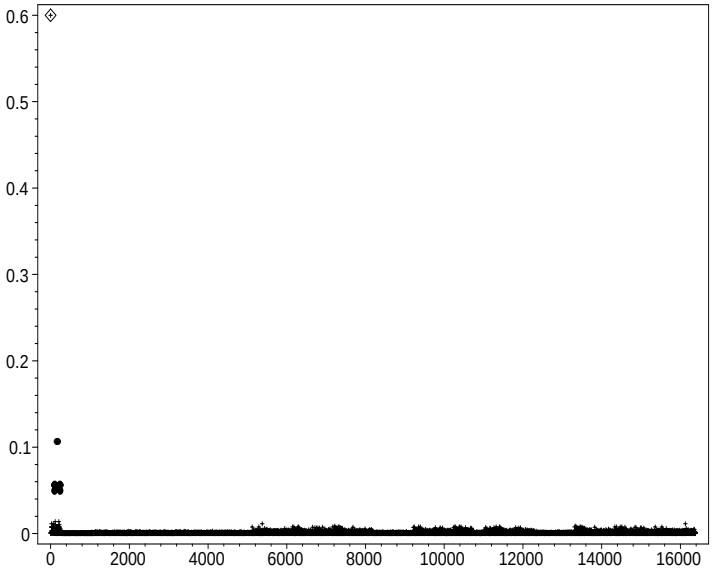


Figure 6.31: Plot of the absolute value of the Fourier coefficients for the coprimality function over $\mathbb{F}_4$, maximum degree $n = 8$ and function β_{02}.

6.4.3 The Irreducibility Function

Also for the irreducibility function there are lots of possibilities to choose a correct transformation. We start with this one:

$$(A) \qquad \widetilde{f}(w) = \frac{1}{2^{2n}} \sum_{u \in \mathbb{F}_2^{2n}} (-1)^{f(u) - \sum_j u_j w_j}$$

In Figures 6.32 and 6.33 we plot the cases $n = 6$ and $n = 9$ to visualize some development.

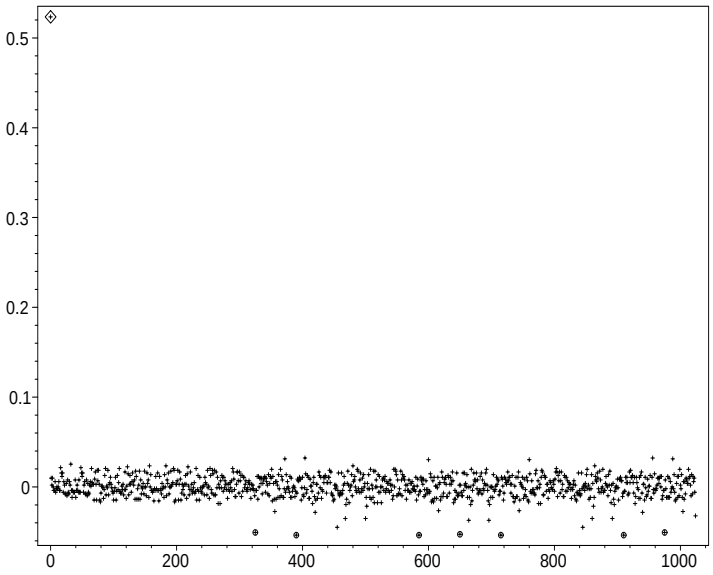


Figure 6.32: Plot of the Fourier coefficients for the irreducibility function over $\mathbb{F}_4$, maximum degree $n = 6$ and transformation (A).

Not surprisingly, the lowest order Fourier coefficient is quite big whereas all the others become smaller and smaller. Also for the irreducibility function there are other possibilities:

$$(B) \qquad \widetilde{f}(w) = \widehat{\psi}(w) = \frac{1}{4^n} \sum_{u \in \mathbb{Z}_4^n} \psi(u) \cdot i^{-\sum_j u_j w_j}.$$

Identifying the elements of $\mathbb{F}_4$ with the elements of $\mathbb{Z}_4$ via a bijective mapping $\beta \colon \mathbb{Z}_4 \to \mathbb{F}_4$ it yields a function $\psi \colon \mathbb{Z}_4^n \to \{-1, 1\},\ u \mapsto (-1)^{g(\beta(u))}$. Of course, there are still the same two functions β to look at. These are $\beta_{00} \colon \mathbb{Z}_4 \to$

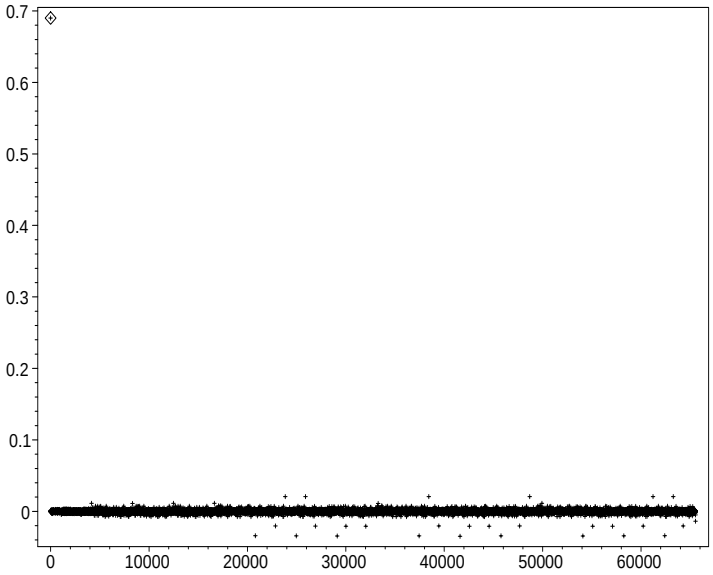


Figure 6.33: Plot of the Fourier coefficients for the irreducibility function over $\mathbb{F}_4$, maximum degree $n = 9$ and transformation (A).

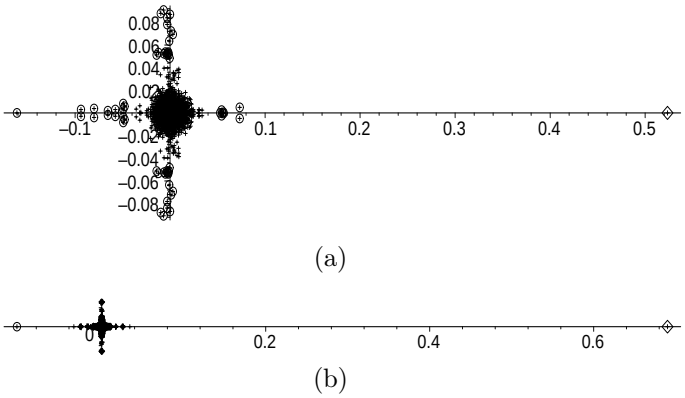


Figure 6.34: Plot of the Fourier coefficients for the irreducibility function over $\mathbb{F}_4$, maximum degree $n = 6$ and $n = 9$, function β_{00} and (B) in the complex plane.

$\mathbb{F}_4$, $\{0, 1, 2, 3\} \mapsto \{0, 1, \alpha, \alpha + 1\}$ and $\beta_{02} \colon \mathbb{Z}_4 \to \mathbb{F}_4$, $\{0, 1, 2, 3\} \mapsto \{0, \alpha, 1, \alpha + 1\}$. In the following one can see the plots in the complex plane for β_{00} and $n = 6$ in Figure 6.34(a), for β_{00} and $n = 9$ in Figure 6.34(b), for β_{02} and $n = 6$

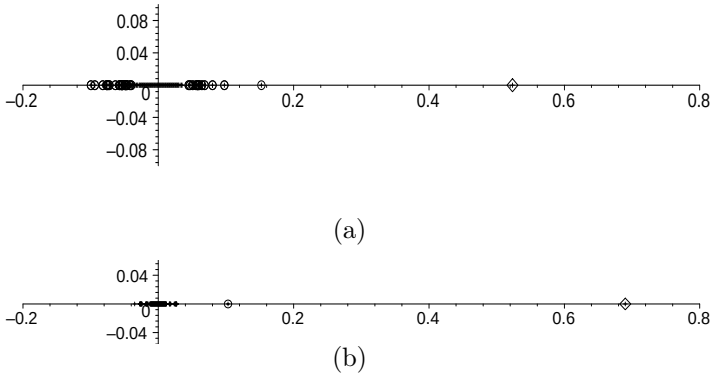


Figure 6.35: Plot of the Fourier coefficients for the irreducibility function over $\mathbb{F}_4$, maximum degree $n = 6$ and $n = 9$, function β_{02} and (B) in the complex plane.

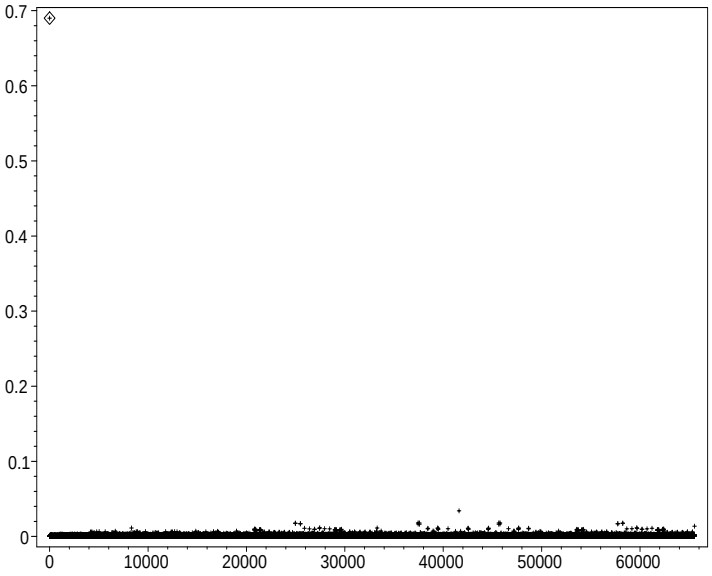


Figure 6.36: Plot of the Fourier coefficients for the irreducibility function over $\mathbb{F}_4$, maximum degree $n = 9$, function β_{00} and (B).

in Figure 6.35(a) and for β_{02} and $n = 9$ in Figure 6.35(b).

Again, using β_{02} yields only real Fourier coefficients. Furthermore, the lowest order Fourier coefficient converges on 1 whereas all the others converge

on 0. The last thing we do in this section is to look at the absolute values of the coefficients for both transformations for $n = 9$ in Figure 6.36 and Figure 6.37.

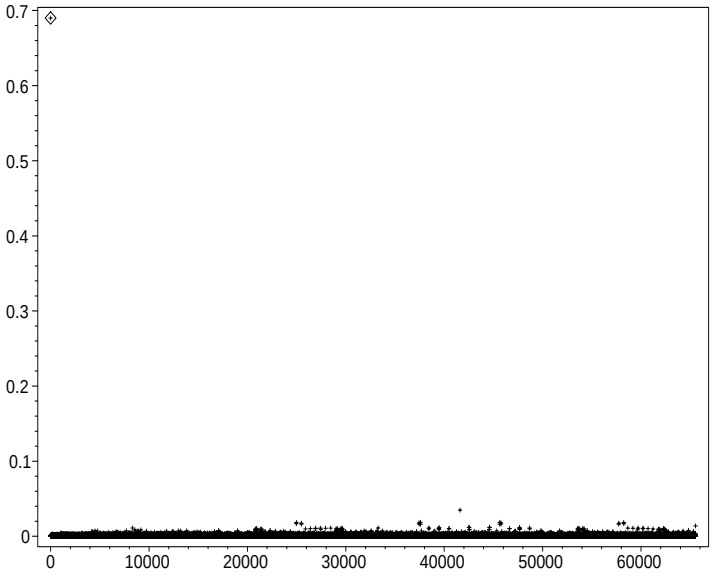


Figure 6.37: Plot of the Fourier coefficients for the irreducibility function over $\mathbb{F}_4$, maximum degree $n = 9$, function β_{02} and (B).

Obviously, for the lowest order Fourier coefficient we get the same value depending only on q and n for each of the three functions and all kinds of transformations. This is the case because for $w = 0^n$ it does not matter which group structure we choose. In the following section you can find formulae for the lowest order Fourier coefficients for all three functions for all finite fields.

7 The Lowest Order Fourier Coefficients over $\mathbb{F}_q$

In order to determine the extreme Fourier coefficients for our three functions for polynomials over $\mathbb{F}_q$, we need to count squarefree, prime and pairs of coprime polynomials, respectively with degree up to a given bound. So at the beginning of each section of this section you will find a more or less short discourse about these quantities.

We have found several Fourier transformations for Boolean functions φ over $\mathbb{F}_q$, $\varphi\colon \mathbb{F}_q^n \to \mathbb{B}$, where q is an arbitrary prime power. Due to the resulting symmetry of the coefficients (see Section 6) we decided to use (2.17):

$$\widetilde{\varphi}(w) = \frac{1}{q^n} \sum_{u \in \mathbb{F}_q^n} (-1)^{\varphi(u)} \cdot \zeta^{-\sum_j u_j w_j},$$

where ζ is some root of unity depending on the kind of transformation choose. For $w = 0^n$ we obtain:

$$\begin{aligned}
\widetilde{\varphi}(0^n) &= \frac{1}{q^n} \sum_{u \in \mathbb{F}_q^n} (-1)^{\varphi(u)} \cdot \zeta^{-\sum_j u_j 0} \\
&= \frac{1}{q^n} \sum_{u \in \mathbb{F}_q^n} (-1)^{\varphi(u)} \\
&= \frac{1}{q^n} \Big(\sum_{\substack{u \in \mathbb{F}_q^n \\ \varphi(u)=0}} 1 - \sum_{\substack{u \in \mathbb{F}_q^n \\ \varphi(u)=1}} 1 \Big)
\end{aligned}$$

Thus, the lowest order Fourier coefficient does not depend on the chosen root of unity and also it does not really matter whether or not q is prime , because the complicated part drops out for the lowest order Fourier coefficient. As usual, we only look at polynomials with constant coefficient 1. In other words our Boolean function operates on the set

$$\mathcal{M}(n) = \{u \in \mathbb{F}_q[x], \deg(u) \le n, u \equiv 1 \bmod x\}.$$

The set is known from Section 5 for the case $q = 2$. To simplify the notation we define the following sets that will be useful later on:

$$\begin{aligned}
\mathbb{F}_q[x]^{(\le n)} &= \{u \in \mathbb{F}_q[x], \deg(u) \le n\}, \\
\mathbb{F}_q[x]^{(\le n)}_{\equiv_x 1} &= \mathcal{M}(n) = \{u \in \mathbb{F}_q[x], \deg(u) \le n, u \equiv 1 \bmod x\}, \\
\mathbb{F}_q[x]^{(\le n)}_{\equiv_x 0} &= \{u \in \mathbb{F}_q[x], \deg(u) \le n, u \equiv 0 \bmod x\}, \\
\mathbb{F}_q[x]^{(\le n)}_{\not\equiv_x 0} &= \{u \in \mathbb{F}_q[x], \deg(u) \le n, u \not\equiv 0 \bmod x\}.
\end{aligned}$$

7.1 The Squarefreeness Function

For the approximation of the lowest order Fourier coefficient for the squarefreeness function we have to know the number of squarefree polynomials:

LEMMA 7.1. *Let q be a prime power, $n \in \mathbb{N}$. Then the number Q_n of squarefree monic polynomials of degree n in $\mathbb{F}_q[x]$ is*

$$Q_n = \#\{u \in \mathbb{F}_q[x]^{(\leq n)} \colon u \text{ monic}, u \text{ squarefree}\} = \begin{cases} q^n, & n < 2, \\ q^{n-1}(q-1), & n \geq 2. \end{cases}$$

For a proof see Flajolet *et al.* (2001).

Now we start with the wanted approximation. We define:

$$\lambda^{\mathrm{sqf}}(n) = \#\{u \in \mathcal{M}(n) \colon u \,\text{squarefree}\}.$$

It is easy to see that

$$\begin{aligned} \widetilde{g}(0^n) &= \frac{1}{q^n}\Big(\sum_{\substack{u \in \mathbb{F}_q^n \\ g(u)=0}} 1 - \sum_{\substack{u \in \mathbb{F}_q^n \\ g(u)=1}} 1 \Big) \\ &= \frac{1}{q^n}(q^n - 2 \cdot \lambda^{\mathrm{sqf}}(n)) \\ &= 1 - 2 \cdot \frac{\lambda^{\mathrm{sqf}}(n)}{q^n} \end{aligned} \tag{7.2}$$

Thus, actually we have to determine $\lambda^{\mathrm{sqf}}(n)$. Apparently,

$$\begin{aligned} \lambda^{\mathrm{sqf}}(n) &= \#\{u \in \mathbb{F}_q[x]^{(\leq n)}_{\equiv_x 1} \colon u \text{ squarefree}\} \\ &= \underbrace{\#\{u \in \mathbb{F}_q[x]^{(=n)}_{\equiv_x 1} \colon u \text{ squarefree}\}}_{R_n} + \#\{u \in \mathbb{F}_q[x]^{(\leq n-1)}_{\equiv_x 1} \colon u \text{ squarefree}\} \\ &= R_n + \lambda^{\mathrm{sqf}}(n-1). \end{aligned}$$

Thus we have a recursion formula for $\lambda^{\mathrm{sqf}}(n)$, all that is left to do is to determine R_n:

$$\begin{aligned} R_n &= \#\{u \in \mathbb{F}_q[x]^{(=n)}_{\equiv_x 1} \colon u \text{ squarefree}\} \\ &= \#\{u \in \mathbb{F}_q[x]^{(=n)}_{\not\equiv_x 0} \colon u \text{ squarefree and monic}\} \\ &= \#\{u \in \mathbb{F}_q[x]^{(=n)} \colon u \text{ squarefree and monic}\} \\ &\qquad\qquad -\#\{u \in \mathbb{F}_q[x]^{(=n)}_{\equiv_x 0} \colon u \text{ squarefree and monic}\} \\ &= Q_n - \#\{u \in \mathbb{F}_q[x]^{(=n-1)}_{\not\equiv 0} \colon u \text{ squarefree and monic}\} \\ &= Q_n - R_{n-1}. \end{aligned}$$

So now we found another recursion formula this one for R_n. Using Lemma 7.1 and standard techniques we obtain the following closed form for R_n:

$$R_n = \frac{q-1}{q+1}(q^n - (-1)^n)$$

and consequently for $\lambda^{\text{sqf}}(n)$

$$\begin{aligned}\lambda^{\text{sqf}}(n) &= \#\{u \in \mathbb{F}_q[x]_{\equiv_x 1}^{(\leq n)} : u \text{ squarefree}\} \\ &= \frac{q^{n+1} + q^{n \text{ rem } 2}}{q+1}.\end{aligned}$$

(This can easily be proven by induction.) To our knowledge inserting this in (7.2) yields a result that was never published before:

THEOREM 7.3. *For the squarefreeness function g for polynomials over finite fields $\mathbb{F}_q$ we have for the lowest order Fourier coefficient*

$$\widetilde{g}(0^n) = \frac{2}{q+1} - 1 - 2 \cdot \frac{q^{n \text{ rem } 2}}{q^n(q+1)}.$$

□

Therefore the limit of the lowest order Fourier coefficient is $\frac{2}{q+1} - 1$. Particularly, for $q = 2$ the lowest order Fourier coefficient converges on $-\frac{1}{3}$ and we have the error bound:

$$\left|\widetilde{g}(0^n) + \frac{1}{3}\right| \leq 2 \cdot \frac{2^{n \text{ rem } 2}}{3 \cdot 2^n} \leq \frac{1}{2^{n-1}}.$$

We already know the limit from Lemma 5.16 but this error bound is better. Because of the denominators $q+1$ and $q^n(q+1)$, the first and the last term vanish as q and n tend to infinity. Thus, we have a lowest order Fourier coefficient very close to -1. From Parseval identity 2.21 we know that

$$\sum |\widetilde{g}(w)|^2 = 1.$$

One of the coefficients $\widetilde{g}(w)$ is the lowest order Fourier coefficient which converges on 1 for $q \to \infty$ and it follows that all the other coefficients including the highest order Fourier coefficient must be rather small over a lot of fields $\mathbb{F}_q$. The results for a few smaller values for q and n for the lowest order Fourier coefficient are listed in Table 7.1 below.

q	$n = 4$	$n = 7$	$n \to \infty$
2	−0.375000000000	−0.343750000000	−0.333333333333
3	−0.506172839506	−0.500685871056	−0.500000000000
4	−0.601562500000	−0.600097656250	−0.600000000000
5	−0.667200000000	−0.666688000000	−0.666666666667
7	−0.750104123282	−0.750002124965	−0.750000000000
8	−0.777832031250	−0.777778625488	−0.777777777778
9	−0.800030483158	−0.800000376335	−0.800000000000
11	−0.833344716891	−0.833333427412	−0.833333333333
13	−0.857147858969	−0.857142886739	−0.857142857143
16	−0.882354736328	−0.882352948189	−0.882352941176
17	−0.888890219226	−0.888888893492	−0.888888888889
19	−0.900000767336	−0.900000002126	−0.900000000000
23	−0.916666964455	−0.916666667230	−0.916666666667
25	−0.923077120000	−0.923076923392	−0.923076923077

Table 7.1: The values of the lowest order Fourier coefficients for the square-freeness function g over $\mathbb{F}_q$ and prime powers q from 2 to 25.

7.2 The Coprimality Function

In this section we need to learn the number of pairs of coprime polynomials, where each polynomial does not exceed a certain degree, to approximate the lowest order Fourier coefficient for the coprimality function. Therefore we have to determine this number, because we did not find any publication that suited our purposes. In Ma & von zur Gathen (1990) there is a similar result, but our setting seems to be slightly different:

LEMMA 7.4. *Let q be a prime power, u, $v \in \mathbb{F}_q[x]$. Then the number W_q^ℓ of pairs of polynomials (u, v) with $\gcd(u, v) = 1$ and $\max\{\deg(u), \deg(v)\} = \ell$ is*

$$W_q^\ell = \begin{cases} q^2 - 1, & \ell = 0, \\ q^{2\ell-1}(q-1)^2(q+1), & \ell \geq 1. \end{cases}$$

PROOF. The degree sequence of a pair $(u, v) \in (\mathbb{F}_q[x] \setminus 0)^2$ of nonzero polynomials is $(\deg(r_0), \deg(r_1), \ldots, \deg(r_s)) \in \mathbb{N}^{s+1}$, where $r_0 = u, r_1 = v, r_2 \ldots, r_s$ are the remainders in the Euclidean algorithm for u and v. For an arbitrary given degree sequence $(n_0, n_1, \ldots, n_s) \in \mathbb{N}^{s+1}$ with $n_0 \geq n_1 > \ldots > n_s \geq 0$ for $s \geq 1$ there are precisely $(q-1)^{s+1}q^{n_0}$ pairs of polynomials with the given degree sequence (see von zur Gathen & Gerhard 1999, Exercise 4.16). If the greatest common divisor of two polynomials u and v is 1, the last entry n_s of the degree sequence has to be 0. So, we look at the following set of degree sequences starting with ℓ and ending with 0.

$$\begin{aligned} &\#\{(n_0, \ldots, n_s) : \ell = n_0 \geq n_1 > \ldots > n_s = 0\} \\ &= \#\{(n_1, \ldots, n_{s-1}) : \ell \geq n_1 > \ldots > n_{s-1} > 0\} \\ &= \binom{\ell}{s-1} \end{aligned}$$

Denoting by A_q^ℓ the number of polynomials u, v over $\mathbb{F}_q$ that are coprime with $\ell = \deg(u) \geq \deg(v)$ and using standard techniques we obtain:

$$\begin{aligned} A_q^\ell &= \#\{(u, v) \in \mathbb{F}_q[x]^2 : \ell = \deg(u) \geq \deg(v), \gcd(u, v) = 1\} \\ &= \sum_{1 \leq s \leq \ell+1} \binom{\ell}{s-1} (q-1)^{s+1} \cdot q^\ell \\ &= (1 + q - 1)^\ell (q-1)^2 q^\ell = q^{2\ell}(q-1)^2. \end{aligned}$$

However, we are looking for

$$W_q^\ell = \#\{u, v \in \mathbb{F}_q[x], \max\{\deg(u), \deg(v)\} = \ell, \gcd(u, v) = 1\}.$$

Simply doubling A_q^ℓ results in too great a number, because the pairs (u, v) with $\deg(u) = \deg(v) = \ell$ are counted twice. Hence, for the missing pairs we look at the following number of degree sequences:

$$\#\{(n_1, \ldots, n_{s-1}) : \ell > n_1 > \ldots > n_{s-1} > 0\} = \binom{\ell - 1}{s - 1}.$$

We get for B_q^ℓ:

$$\begin{aligned} B_q^\ell &= \#\{(u, v) \in \mathbb{F}_q[x]^2, \ell = \deg(u) > \deg(v), \gcd(u, v) = 1\} \\ &= \sum_{1 \le s \le \ell} \binom{\ell - 1}{s - 1} \cdot (q - 1)^{s+1} q^\ell \\ &= q^{2\ell - 1}(q - 1)^2. \end{aligned}$$

Now,

$$\begin{aligned} W_q^\ell &= A_q^\ell + B_q^\ell \\ &= q^{2\ell}(q - 1)^2 + q^{2\ell-1}(q - 1)^2 \\ &= q^{2\ell-1}(q - 1)^2(q + 1) \end{aligned}$$

This formula holds for $\ell \ge 1$, and for $\ell = 0$ we have

$$W_q^0 = q^2 - 1,$$

since for all u, $v \in \mathbb{F}_q[x]$ with $\max\{\deg(u), \deg(v)\} = 1$ we have u, $v \in \mathbb{F}_q$ and $(u, v) \neq (0, 0)$ and thus $\gcd(u, v) = 1$. □

Proceeding as in the previous section we define

$$\lambda^{\mathrm{cop}}(2\ell) = \#\{(u, v) \in (\mathcal{M}(\ell))^2 \colon \gcd(u, v) = 1\}$$

and in a similar way we obtain

$$\widetilde{h}(0^{2\ell}) = 1 - 2 \cdot \frac{\lambda^{\mathrm{cop}}(2\ell)}{q^{2\ell}}. \tag{7.5}$$

Now we will determine $\lambda^{\mathrm{cop}}(2\ell)$. From above we know the number W_q^ℓ of pairs of coprime polynomials in $\mathbb{F}_q[x]$ with $\max\{\deg(u), \deg(v)\} = \ell$. But for $\lambda^{\mathrm{cop}}(2\ell)$ we need the number of coprime pairs of polynomials in $(\mathcal{M}(\ell))^2$. Consider

$$\gamma(2\ell) = \#\{(u, v) \in \left(\mathbb{F}_q[x]^{(\le \ell)}\right)^2, \gcd(u, v) = 1\}$$

Using the two formulae for W_q^ℓ we get

$$\begin{aligned}\gamma(2\ell) &= \#\{(u,v) \in \left(\mathbb{F}_q[x]^{(\leq \ell)}\right)^2, \gcd(u,v) = 1\} \\ &= \sum_{0 \leq i \leq \ell} W_q^i \\ &= q^2 - 1 + \sum_{1 \leq i \leq \ell} q^{2i-1}(q-1)^2(q+1) \\ &= (q-1) \cdot (q^{2\ell+1} + 1).\end{aligned}$$

But we want to compute $\lambda^{\mathrm{cop}}(2\ell)$, so we split $\gamma(2\ell)$ accordingly:

$$\begin{aligned}\gamma(2\ell) &= \#\{(u,v) \in \left(\mathbb{F}_q[x]^{(\leq \ell)}_{\not\equiv_x 0}\right)^2, \gcd(u,v) = 1\} \\ &\quad +\#\{(u,v) \in \left(\mathbb{F}_q[x]^{(\leq \ell)}_{\equiv_x 0}\right)^2, \gcd(u,v) = 1\} \\ &\quad +\#\{u \in \mathbb{F}_q[x]^{(\leq \ell)}_{\not\equiv_x 0}, v \in \mathbb{F}_q[x]^{(\leq \ell)}_{\equiv_x 0}, \gcd(u,v) = 1\} \\ &\quad +\#\{u \in \mathbb{F}_q[x]^{(\leq \ell)}_{\equiv_x 0}, v \in \mathbb{F}_q[x]^{(\leq \ell)}_{\not\equiv_x 0}, \gcd(u,v) = 1\}.\end{aligned}$$

First, we notice that

- $\#\{(u,v) \in \left(\mathbb{F}_q[x]^{(\leq \ell)}_{\equiv_x 0}\right)^2, \gcd(u,v) = 1\} = 0$, because the greatest common divisor of each pair in this set is at least x.

- $\#\{(u,v) \in \left(\mathbb{F}_q[x]^{(\leq \ell)}_{\not\equiv_x 0}\right)^2, \gcd(u,v) = 1\} = (q-1)^2 \cdot \lambda^{\mathrm{cop}}(2\ell)$, because for every constant coefficient $c \in \mathbb{F}_q[x]^\times$ we can map the set $\mathbb{F}_q[x]^{(\leq \ell)}_{\not\equiv_x 0}$ onto $\mathcal{M}(\ell)$ by multiplication with c^{-1}.

- Finally, the number $\#\{u \in \mathbb{F}_q[x]^{(\leq \ell)}_{\equiv_x 0}, v \in \mathbb{F}_q[x]^{(\leq \ell)}_{\not\equiv_x 0}, \gcd(u,v) = 1\}$ equals the number $\#\{u \in \mathbb{F}_q[x]^{(\leq \ell)}_{\not\equiv_x 0}, v \in \mathbb{F}_q[x]^{(\leq \ell)}_{\equiv_x 0}, \gcd(u,v) = 1\}$.

At this point we have

$$\gamma(2\ell) = (q-1)^2 \cdot \lambda^{\mathrm{cop}}(2\ell) + 2 \cdot \underbrace{\#\{u \in \mathbb{F}_q[x]^{(\leq \ell)}_{\not\equiv_x 0}, v \in \mathbb{F}_q[x]^{(\leq \ell)}_{\equiv_x 0}, \gcd(u,v) = 1\}}_{P(\ell)}.$$

This last quantity $P(\ell)$ can be written as

$$\begin{aligned} P(\ell) &= \#\{u \in \mathbb{F}_q[x]^{(\leq \ell)}_{\not\equiv_x 0}, v \in \mathbb{F}_q[x]^{(\leq \ell)}_{\equiv_x 0}, \gcd(u,v) = 1\} \\ &= \#\{u \in \mathbb{F}_q[x]^{(\leq \ell)}_{\not\equiv_x 0}, v \in \mathbb{F}_q[x]^{(\leq \ell)}_{\equiv_x 0}, \gcd(u,v) = 1\} \\ &\quad +\#\{u \in \mathbb{F}_q[x]^{(\leq \ell)}_{\equiv_x 0}, v \in \mathbb{F}_q[x]^{(\leq \ell)}_{\equiv_x 0}, \gcd(u,v) = 1\} \\ &= \#\{u \in \mathbb{F}_q[x]^{(\leq \ell)}, v \in \mathbb{F}_q[x]^{(\leq \ell)}_{\equiv_x 0}, \gcd(u,v) = 1\} \end{aligned}$$

Consider the polynomials $u, v \in \mathbb{F}_q[x]$ both of degree $\leq \ell$ and with a divisor x of v. The polynomials u and v are coprime if and only if x is not a divisor of u and u and $\frac{v}{x}$ are coprime. Therefore, if we take the number of coprime u and $\frac{v}{x}$ $\left(\frac{v}{x} \in \mathbb{F}_q[x]^{(\leq \ell)}\right)$, then we have to subtract all those pairs where $x \mid u$ and $\gcd(\frac{u}{x}, \frac{v}{x}) = 1$. For the subtraction we only need to consider $\frac{v}{x}$ that are no longer divisible by x. Proceeding like this we obtain:

$$\begin{aligned} P(\ell) &= \#\{u \in \mathbb{F}_q[x]^{(\leq \ell)}, v \in \mathbb{F}_q[x]^{(\leq \ell-1)}, \gcd(u,v) = 1\} \\ &\quad -\#\{u \in \mathbb{F}_q[x]^{(\leq \ell-1)}, v \in \mathbb{F}_q[x]^{(\leq \ell)}_{\equiv_x 0}, \gcd(u,v) = 1\} \\ &= \#\{u \in \mathbb{F}_q[x]^{(\leq \ell)}, v \in \mathbb{F}_q[x]^{(\leq \ell-1)}, \gcd(u,v) = 1\} \\ &\quad -\#\{u \in \mathbb{F}_q[x]^{(\leq \ell-1)}, v \in \mathbb{F}_q[x]^{(\leq \ell-1)}, \gcd(u,v) = 1\} \\ &\quad +\#\{u \in \mathbb{F}_q[x]^{(\leq \ell-1)}, v \in \mathbb{F}_q[x]^{(\leq \ell-1)}_{\equiv_x 0}, \gcd(u,v) = 1\} \\ &= \#\{u \in \mathbb{F}_q[x]^{=\ell}, v \in \mathbb{F}_q[x]^{(\leq \ell-1)}, \gcd(u,v) = 1\} \\ &\quad + \underbrace{\#\{u \in \mathbb{F}_q[x]^{(\leq \ell-1)}, v \in \mathbb{F}_q[x]^{(\leq \ell-1)}_{\equiv_x 0}, \gcd(u,v) = 1\}}_{P(\ell-1)} \end{aligned}$$

Hence, we have a recursion formula for $P(\ell)$. We already know the other number in the formula from the proof of Lemma 7.4, its cardinality is $B_q^\ell = q^{2\ell-1}(q-1)^2$. It follows that

$$P(\ell) = q^{2\ell-1}(q-1)^2 + P(\ell-1). \tag{7.6}$$

In order to unwrap this recursion formula we have to find a starting point, so we look at $P(0)$:

$$\begin{aligned} P(0) &= \#\{u \in \mathbb{F}_q[x]^{(\leq 0)}, v \in \mathcal{M}_0(0), \gcd(u,v) = 1\} \\ &= \#\{u \in \{0, \ldots, q-1\}, v \in \{0\}, \gcd(u,v) = 1\} \\ &= q - 1. \end{aligned}$$

For the first values of $P(\ell)$ we have

$$\begin{aligned} P(0) &= q-1 \\ P(1) &= q\cdot(q-1)^2+(q-1) = (q-1)\cdot(q\cdot(q-1)+1) \\ P(2) &= q^3\cdot(q-1)^2+(q-1)\cdot(q\cdot(q-1)+1) \\ &= (q-1)\cdot(q^3\cdot(q-1)+q\cdot(q-1)+1) \end{aligned}$$

General techniques lead to the following formula:

$$\begin{aligned} P(\ell) &= (q-1)^2\cdot\Big(\sum_{1\le i\le \ell} q^{2i-1}\Big)+q-1 \\ &= (q-1)\cdot\frac{q^{2\ell+1}+1}{q+1}. \end{aligned}$$

(The correctness of the formula can easily be proven by induction.) The number -1 is a root of the polynomial $q^{2\ell+1}+1$, so we could cancel the factor $q+1$, but at the price of a longer formula. Now, we finally go back to $\gamma(2\ell)$:

$$\gamma(2\ell) = (q-1)^2\lambda^{\mathrm{cop}}(2\ell)+2P(\ell).$$

Solving for $\lambda^{\mathrm{cop}}(2\ell)$ and inserting the formulae for $\gamma(2\ell)$ and $P(\ell)$ yields:

$$\begin{aligned} \lambda^{\mathrm{cop}}(2\ell) &= \frac{\gamma(2\ell)-2P(\ell)}{(q-1)^2} \\ &= \frac{1}{q-1}\cdot\left((q^{2\ell+1}+1)-2\cdot\frac{q^{2\ell+1}+1}{q+1}\right) \\ &= \frac{q^{2\ell+1}+1}{q-1}\cdot\Big(1-\frac{2}{q+1}\Big) = \frac{q^{2\ell+1}+1}{q-1}\cdot\frac{q+1-2}{q+1} \\ &= \frac{q^{2\ell+1}+1}{q+1}. \end{aligned} \tag{7.7}$$

Using (7.7) we can compute the lowest order Fourier coefficient for any q and ℓ as mentioned in equation (7.5) at the beginning of this section. We have

$$\begin{aligned} \widetilde{h}(0^{2\ell}) &= 1-2\cdot\frac{\lambda^{\mathrm{cop}}(2\ell)}{q^{2\ell}} \\ &= 1-2\cdot\frac{q^{2\ell+1}+1}{q^{2\ell}\cdot(q+1)} \\ &= 1-\frac{2q}{q+1}-\frac{2}{q^{2\ell}\cdot(q+1)}. \end{aligned}$$

We obtain the following result that to our knowledge is new:

THEOREM 7.8. *For the coprimality function h for polynomials over finite fields $\mathbb{F}_q$ we have the following description for the lowest order Fourier coefficient:*

$$\widetilde{h}(0^{2\ell}) = 1 - \frac{2q}{q+1} - \frac{2}{q^{2\ell}\cdot(q+1)}.$$

□

This means that the lowest order Fourier coefficient converges on $1 - \frac{2q}{q+1}$ as n tends to infinity. Let us compare this with our results over $\mathbb{F}_2$. We have cosidered this lowest order Fourier coefficient in Lemma 5.21 and the result was that this coefficient is very close to $-\frac{1}{3}$ asymptotically. For the case $q = 2$ we have

$$\widetilde{h}(0^{2\ell}) = 1 - \frac{4}{3} - \frac{2}{3\cdot 2^{2\ell}} = -\frac{1}{3} - \frac{2}{3\cdot 2^{2\ell}}.$$

This means

$$\widetilde{h}(0^{2\ell}) \stackrel{\ell\to\infty}{\longrightarrow} -\frac{1}{3} \text{ and } \left|\widetilde{h}(0^{2\ell}) + \frac{1}{3}\right| = \frac{2}{3\cdot 2^{2\ell}} < \frac{1}{2^{2\ell}}.$$

Once again we got a better error bound than in the earlier proof we did for Lemma 5.21. Looking at an arbitrary prime power q, there are similar results for the lowest order Fourier coefficient for the coprimality function over $\mathbb{F}_q$. Note, that the values for the coprimality function (which is only defined for even n) are the same as for the squarefreeness function because for even n we have

$$\begin{aligned}
\widetilde{g}(0^n) &= -1 + \frac{2}{q+1} - \frac{2}{q^n\cdot(q+1)} \\
&= \frac{-q-1+2}{q+1} - \frac{2}{q^n\cdot(q+1)} \\
&= \frac{q+1-2q}{q+1} - \frac{2}{q^{2\ell}\cdot(q+1)} \\
&= 1 - \frac{2q}{q+1} - \frac{2}{q^{2\ell}\cdot(q+1)} = \widetilde{h}(0^n).
\end{aligned}$$

7.3 The Irreducibility Function

Proceeding as usual we begin by determining the number $\lambda^{\text{irr}}(n)$ of irreducible polynomials in $\mathcal{M}(n)$:

$$\lambda^{\text{irr}}(n) = \#\{u \in \mathcal{M}(n) \colon u \,\text{irreducible}\}.$$

This number immediately yields the lowest order Fourier coefficient:

$$\widetilde{f}(0^n) = 1 - 2 \cdot \frac{\lambda^{\text{irr}}(n)}{q^n}. \tag{7.9}$$

E.g. from von zur Gathen & Gerhard (1999), Chapter 14.9, we know that the number $I(n,q)$ of irreducible monic polynomials of degree n in $\mathbb{F}_q[x]$ is

$$I(n,q) = \frac{1}{n} \cdot \sum_{d|n} \mu\Big(\frac{n}{d}\Big) q^d$$

for $n \geq 1$. There are no irreducible polynomials of degree $n \leq 0$. Obviously, the number of arbitrary (monic and nonmonic) irreducible polynomials of degree n in $\mathbb{F}_q[x]$ is

$$(q-1) \cdot I(n,q) = \frac{q-1}{n} \cdot \sum_{d|n} \mu\Big(\frac{n}{d}\Big) q^d.$$

For $\lambda^{\text{irr}}(n)$ we actually only count those irreducible polynomials with constant coefficient 1. The number $\iota(n)$ of irreducible polynomials in $\mathbb{F}_q[x]^{(\leq n)}$ is on the one hand:

$$\begin{aligned} \iota(n) &= \sum_{1 \leq j \leq n} (q-1) \cdot I(j,q) \\ &= (q-1) \sum_{1 \leq j \leq n} \frac{1}{j} \cdot \sum_{d|j} \mu\Big(\frac{j}{d}\Big) q^d. \end{aligned}$$

On the other hand we have the obvious relation between $\lambda^{\text{irr}}(n)$ and $\iota(n)$:

$$\iota(n) = (q-1) \cdot \lambda^{\text{irr}}(n) + q - 1.$$

This becomes clear when we look a little bit closer at the make-up of $\iota(n)$:

$$\begin{aligned} \iota(n) &= \#\{u \in \mathbb{F}_q[x]^{(\leq n)} \colon u \,\text{irreducible}\} \\ &= \#\{u \in \mathbb{F}_q[x]^{(\leq n)}_{\not\equiv_x 0} \colon u \,\text{irreducible}\} + \#\{u \in \mathbb{F}_q[x]^{(\leq n)}_{\equiv_x 0} \colon u \,\text{irreducible}\}. \end{aligned}$$

Evidently, the second quantity is 1 because x divides every polynomial in $\mathbb{F}_q[x]^{(\leq n)}_{\equiv_{x^0}}$ and only one of them, namely x, is irreducible. The first number evidently equals $(q-1)\cdot\lambda^{\mathrm{irr}}(n)$. So, we get this for $\lambda^{\mathrm{irr}}(n)$:

$$\begin{aligned}\lambda^{\mathrm{irr}}(n) &= \frac{\iota(n)}{q-1} - 1 \\ &= \sum_{1\leq j\leq n} \frac{1}{j}\cdot\sum_{d|j}\mu\Big(\frac{j}{d}\Big)q^d - 1.\end{aligned}$$

Now, we will estimate $\lambda^{\mathrm{irr}}(n)$. There are well-known estimations for $I(n,q)$, for example in von zur Gathen & Gerhard (1999), Lemma 14.38 in Chapter 14.9:

$$\frac{q^n - 2\cdot q^{\frac{n}{2}}}{n} \leq I(n,q) \leq \frac{q^n}{n}.$$

Apparently

$$\lambda^{\mathrm{irr}}(n) \leq \sum_{1\leq j\leq n}\frac{q^j}{j}.$$

To estimate this sum we use the inequality

$$3\cdot\frac{q^{n-1}}{n-1} \leq 2\cdot\frac{q^n}{n}, \tag{7.10}$$

which holds for

$$n \geq \frac{2q}{2q-3}.$$

The limit of $\frac{2q}{2q-3}$ obviously is 1. For $q=2$ (the smallest prime power) we have $n\geq 4$ (the largest lower bound for n). Now we will prove by induction that for $n\geq 1$ holds

$$\sum_{1\leq j\leq n}\frac{q^j}{j} \leq 3\cdot\frac{q^n}{n} \quad (\textbf{Induction claim}). \tag{7.11}$$

We begin by proving the claim for $n=1,2,3$:

$$\begin{aligned} n=1 \quad & \sum_{1\leq j\leq 1}\frac{q^j}{j} = q \leq 3q, \\ n=2 \quad & \sum_{1\leq j\leq 2}\frac{q^j}{j} = q + \frac{q^2}{2} = \frac{2q+q^2}{2} \leq \frac{3q^2}{2}, \\ n=3 \quad & \sum_{1\leq j\leq 3}\frac{q^j}{j} = q + \frac{q^2}{2} + \frac{q^3}{3} = \frac{2q^3+3q^2+6q}{6} \leq \frac{6q^3}{6} = q^3. \end{aligned}$$

(The validity of this claim for all $q \geq 2$ can easily be verified another induction.)
Induction step $n-1 \to n$, $n \geq 4$:

$$\begin{aligned}\sum_{1\leq j\leq n} \frac{q^j}{j} &= \sum_{1\leq j\leq n-1} \frac{q^j}{j} + \frac{q^n}{n} \\ &\overset{(7.11)}{\leq} 3 \cdot \frac{q^{n-1}}{n-1} + \frac{q^n}{n} \\ &\overset{(7.10)}{\leq} 2 \cdot \frac{q^n}{n} + \frac{q^n}{n} \\ &= 3 \cdot \frac{q^n}{n}.\end{aligned}$$

Thus

$$\lambda^{\mathrm{irr}}(n) \leq \sum_{1\leq j\leq n} \frac{q^j}{j} \leq 3 \cdot \frac{q^n}{n}.$$

At this point we recall (7.9):

$$\widetilde{f}(0^n) = 1 - 2 \cdot \frac{\lambda^{\mathrm{irr}}(n)}{q^n}.$$

Obviously,

$$0 \leq \frac{\lambda^{\mathrm{irr}}(n)}{q^n} \leq 3 \cdot \frac{q^n}{q^n \cdot n} = \frac{3}{n}$$

and the limit of $\frac{3}{n}$ equals 0. Thus we have

$$\begin{aligned} & 1 - \widetilde{f}(0^n) = 2 \cdot \frac{\lambda^{\mathrm{irr}}(n)}{q^n} \leq \frac{6}{n} \\ \Leftrightarrow \quad & \widetilde{f}(0^n) \geq 1 - \frac{6}{n} \\ \Leftrightarrow \quad & |\widetilde{f}(0^n)| \geq \left|1 - \frac{6}{n}\right|. \end{aligned}$$

Obviously, the limit of the lowest order Fourier coefficient is

$$\lim_{n\to\infty} \widetilde{f}(0^n) = 1.$$

From Lemma 3.10 we know that the absolute values of the lowest and highest order Fourier coefficients sum to at most 1:

$$\left|\widetilde{f}(0^n)\right| + \left|\widetilde{f}(1^n)\right| \leq 1.$$

for the Fourier transformation over $\mathbb{F}_2$. Plugging in our lower bound for the lowest order Fourier coefficient we get $n \geq 6$:

$$|\widetilde{f}(1^n)| \leq \frac{6}{n}.$$

Obviously, the limit of the highest order Fourier coefficient is:

$$\lim_{n\to\infty} |\widetilde{f}(1^n)| = \lim_{n\to\infty} \frac{6}{n} = 0.$$

For the other finite fields $\mathbb{F}_q$, $q \neq 2$, we remember Parseval identity 2.21

$$\sum \widetilde{f}(w)^2 = 1.$$

Clearly, the square of the lowest order Fourier coefficient which converges on 1 also converges on 1 for all q and we see here that all the other Fourier coefficients of the irreducibility function must vanish over all finite fields $\mathbb{F}_q$.

8 Some Definitions and Experiments for the Fourier Transform over the Natural Numbers

In this section we will consider nonnegative integers in their binary representation $(u_n, \ldots, u_0)$ and denote the integer itself by $(u)_2$. We will look at the Fourier transform for our three functions now defined over the integers. We use the same Fourier transformation that we used for polynomials over the field $\mathbb{F}_2$.

$$\hat{\varphi}(w) = \frac{1}{2^n} \sum_{u \in \mathbb{B}^n} (-1)^{\varphi(u)+\sum_i u_i w_i}, w \in \mathbb{B}^n.$$

Here $\varphi\colon \{0,1\}^n \to \{0,1\}$ is one of the Boolean functions squarefreeness g^{int}, coprimality h^{int}, and primality f^{int}:

DEFINITION 8.1.
- *The integer* irreducibility function $f^{\text{int}}\colon \{0,1\}^n \to \{0,1\}$ *is defined by*

$$f^{\text{int}}(u_1, \ldots, u_n) = \begin{cases} 1, & \text{if } (u)_2 \text{ is irreducible,} \\ 0, & \text{otherwise,} \end{cases}$$

  where $(u_0, \ldots, u_n)$ *is the binary representation of the integer number* u*.*

- *The integer* squarefreeness function $g^{\text{int}}\colon \{0,1\}^n \to \{0,1\}$ *is defined by*

$$g^{\text{int}}(u_0, \ldots, u_n) = \begin{cases} 1, & \text{if } (u)_2 \text{ is squarefree,} \\ 0, & \text{otherwise,} \end{cases}$$

  where $(u_0, \ldots, u_n)$ *is the binary representation of the integer number* u*.*

- *The integer* coprimality function $h^{\text{int}}\colon \{0,1\}^\ell \times \{0,1\}^\ell \to \{0,1\}$ *is defined by*

$$h^{\text{int}}(v_1, \ldots, v_\ell; w_1, \ldots, w_\ell) = \begin{cases} 1, & \text{if } (v)_2 \text{ and } (w)_2 \text{ are coprime,} \\ 0, & \text{otherwise,} \end{cases}$$

  where $(v_1, \ldots, v_\ell)$ *and where* $(w_1, \ldots, w_\ell)$ *are the binary representations of the integer numbers* v *and* w*.*

At this point we will recall briefly the well-known definitions for squarefreeness, coprimality and primality:

DEFINITION 8.2 (Squarefreeness). *An integer $a \in \mathbb{Z}$ is called* squarefree *if there is no prime number p such that $p^2 \mid a$.*

DEFINITION 8.3 (Coprimality). *Two integers $a, b \in \mathbb{Z}$ are said to be* coprime *if* $\gcd(a, b) = 1$.

DEFINITION 8.4 (Primality). *A natural number is said to be* prime *if and only if it is greater than* 1 *and has no natural divisors other than* 1 *and itself.*

Since the integers are a unique factorization domain here primality and irreducibility are one and the same:

THEOREM 8.5. *An integer is prime if and only if it is irreducible.*

8.1 The Squarefreeness Function

The first figure (Figure 8.1(a)) was done using bit size 10, i.e. u's from 0 to $2^{10}-1$, and plotting the Fourier coefficients of $w \in \{0,1\}^n$ against the number $(w)_2$. We bear witness to four large Fourier coefficients, namely the first four. Looking at a plot for all u's with $0 \leq u < 2^{11}$ we note that the quality of the figure (Figure 8.1(b)) does not change much.

n	$w = (00)_2$	$w = (10)_2$	$w = (01)_2$	$w = (11)_2$
6	-0.2187500000	$+0.3750000000$	$+0.4687500000$	$+0.3125000000$
7	-0.2187500000	$+0.3906250000$	$+0.4687500000$	$+0.3281250000$
8	-0.2265625000	$+0.4062500000$	$+0.4296875000$	$+0.3750000000$
9	-0.2265625000	$+0.4023437500$	$+0.4140625000$	$+0.4023437500$
10	-0.2187500000	$+0.4003906250$	$+0.4179687500$	$+0.3964843750$
11	-0.2158203125	$+0.4042968750$	$+0.4091796875$	$+0.4003906250$
12	-0.2163085938	$+0.4052734375$	$+0.4067382812$	$+0.4033203125$
13	-0.2163085938	$+0.4050292969$	$+0.4062500000$	$+0.4045410156$
14	-0.2160644531	$+0.4051513672$	$+0.4055175781$	$+0.4051513672$
15	-0.2158203125	$+0.4050903320$	$+0.4058837891$	$+0.4047241211$
16	-0.2159423828	$+0.4054260254$	$+0.4058227539$	$+0.4046325684$
17	-0.2159423828	$+0.4052276611$	$+0.4053649902$	$+0.4053192139$
18	-0.2158203125	$+0.4052200317$	$+0.4053192139$	$+0.4052658081$
19	-0.2158393860	$+0.4053115845$	$+0.4053077698$	$+0.4052124023$
20	-0.2158603668	$+0.4052810669$	$+0.4053058624$	$+0.4052696228$
∞	$\to 1 - \frac{12}{\pi^2}$	$\to \frac{4}{\pi^2}$	$\to \frac{4}{\pi^2}$	$\to \frac{4}{\pi^2}$
	(-0.2158542037)	$(+0.4052847346)$	$(+0.4052847346)$	$(+0.4052847346)$

Table 8.1: The values of the four most significant Fourier coefficients for the squarefreeness function over the natural numbers and upper bounds for bit size from 6 up to 20.

In contrast to the polynomials over finite fields, this time around we cannot immidiately make out candidates for the limits of the large coefficients, but three of them seem to converge on the same value. In Section 9.1 we will determine the asymptotic values of all four coefficients. You can already see the limits in Table 8.1 in the line labeled ∞.

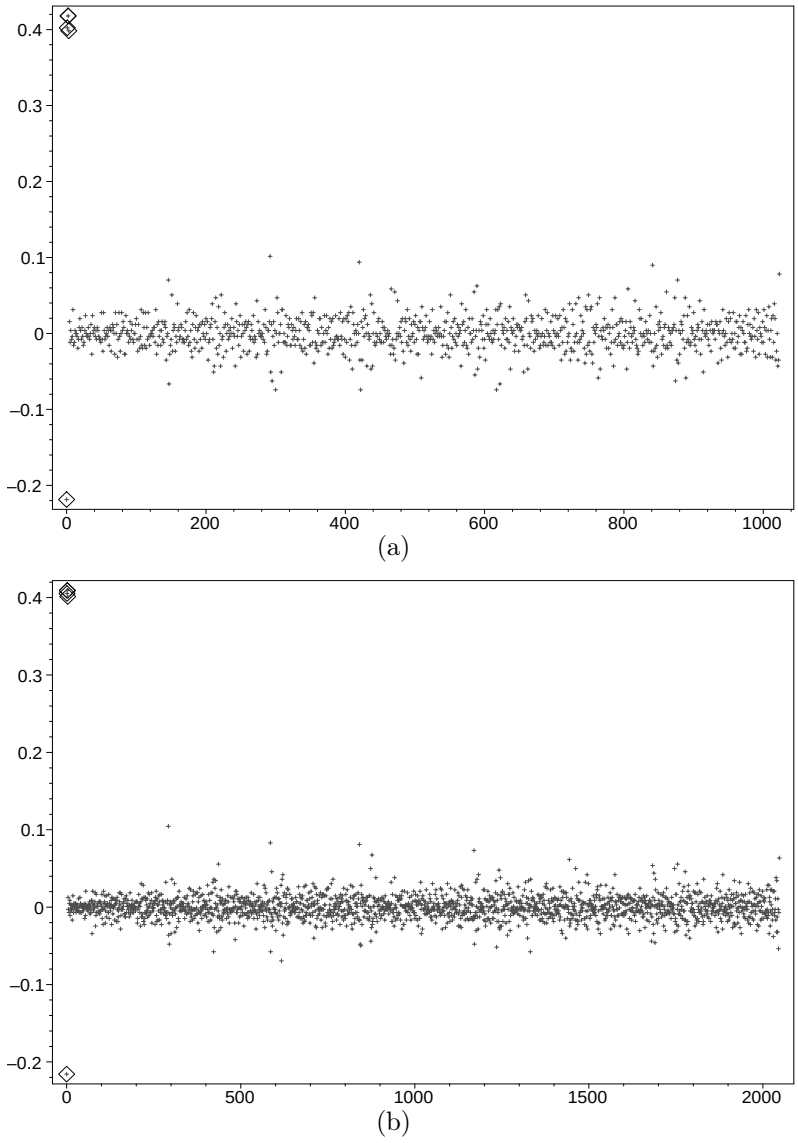


Figure 8.1: Plot of the Fourier coefficients for the squarefreeness function over the natural numbers and maximum input $u = 2^{10} - 1$ and $u = 2^{11} - 1$.

8.2 The Coprimality Function

We used the same strategy for the coprimality function h^{int}. The results of our computations for the upper bound $2^{10}-1$ can be seen in Figure 8.2. Once more there are four coefficients that seem to differ significantly from the others; two of them are again the first two coefficients. We defined the coprimality function

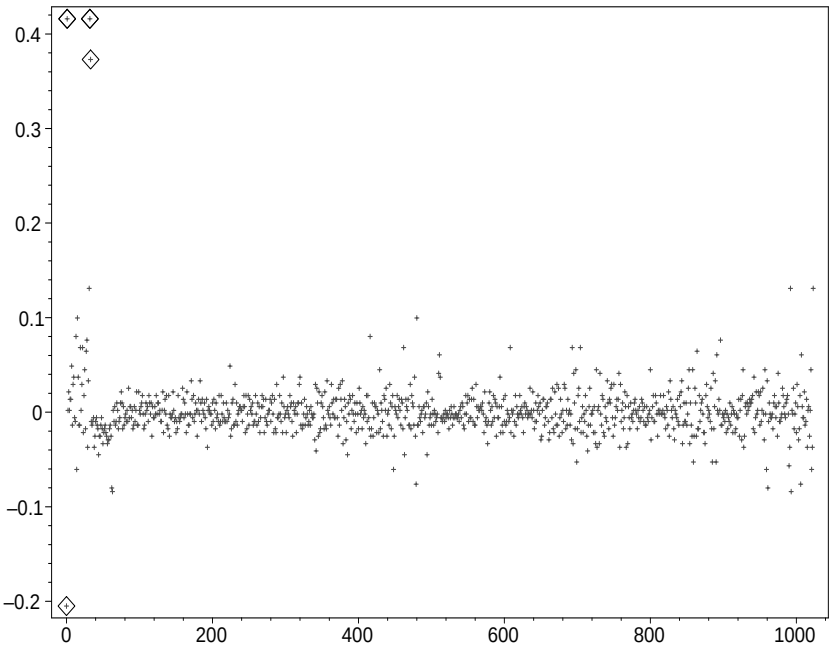


Figure 8.2: Plot of the Fourier coefficients for the coprimality function over the natural numbers and maximum for each half of an input (u, v) is $2^5 - 1$.

only for even input sizes n, so that the binary representation can always be cut into two equal halves. This means the upper bound for each integer in a pair is $2^{\frac{n}{2}} - 1$ and the next step is to look at $n = 12$. Again there is not much of a development in the plot (Figure 8.3). The coefficients appear to converge on the same values as the coefficients of the squarefreeness function but in a different order. This can be seen in Figures 8.2, 8.3 and in Table 8.2, where we again mention in the line labeled ∞ the results of our proof for these coefficients in Section 9.2.

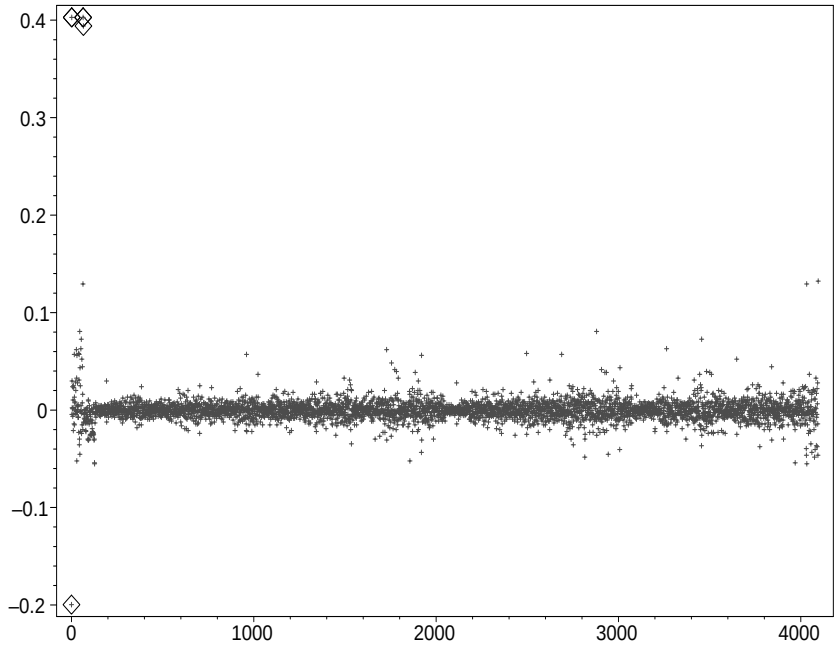


Figure 8.3: Plot of the Fourier coefficients for the coprimality function over the natural numbers and maximum bit size 6 for each half of an input (u, v).

n	$w = [0]_{10}$	$w = [1]_{10}$	$w = [2^{\frac{n}{2}}]_{10}$	$w = [2^{\frac{n}{2}} + 1]_{10}$
2	$+0,0000000000$	$+0,0000000000$	$+0,0000000000$	$+0,0000000000$
4	$-0,5000000000$	$+0,0000000000$	$+0,5000000000$	$+0,0000000000$
6	$-0,3750000000$	$+0,2500000000$	$+0,3750000000$	$+0,2500000000$
8	$-0,2187500000$	$+0,4375000000$	$+0,2812500000$	$+0,3750000000$
10	$-0,1640625000$	$+0,4218750000$	$+0,3203125000$	$+0,3906250000$
12	$-0,2050781250$	$+0,4296875000$	$+0,3769531250$	$+0,3906250000$
14	$-0,2099609375$	$+0,4155273438$	$+0,3935546875$	$+0,3989257812$
16	$-0,2113037109$	$+0,4123535156$	$+0,3961181641$	$+0,4023437500$
18	$-0,2113952637$	$+0,4071044922$	$+0,4007263184$	$+0,4034423828$
20	$-0,2142715454$	$+0,4067382812$	$+0,4037551880$	$+0,4037475586$
22	$-0,2153091431$	$+0,4058856964$	$+0,4049034119$	$+0,4045124054$
∞	$\to 1 - \frac{12}{\pi^2}$	$\to \frac{4}{\pi^2}$	$\to \frac{4}{\pi^2}$	$\to \frac{4}{\pi^2}$
	(-0.2158542037)	$(+0.4052847346)$	$(+0.4052847346)$	$(+0.4052847346)$

Table 8.2: The values of the four most significant Fourier coefficients for the coprimality function over the natural numbers and (even) bit sizes n up to 22.

8.3 The Primality Function

As was the case for the irreducibility function defined over the polynomials the results for the primality function are different from these for the squarefreeness and coprimality functions and somewhat simpler. It appears that the lowest order Fourier coefficient converges on 1 while all the others vanish. First we take a look at the coefficients for the upper bound $2^{10} - 1$ in Figure 8.4. In the

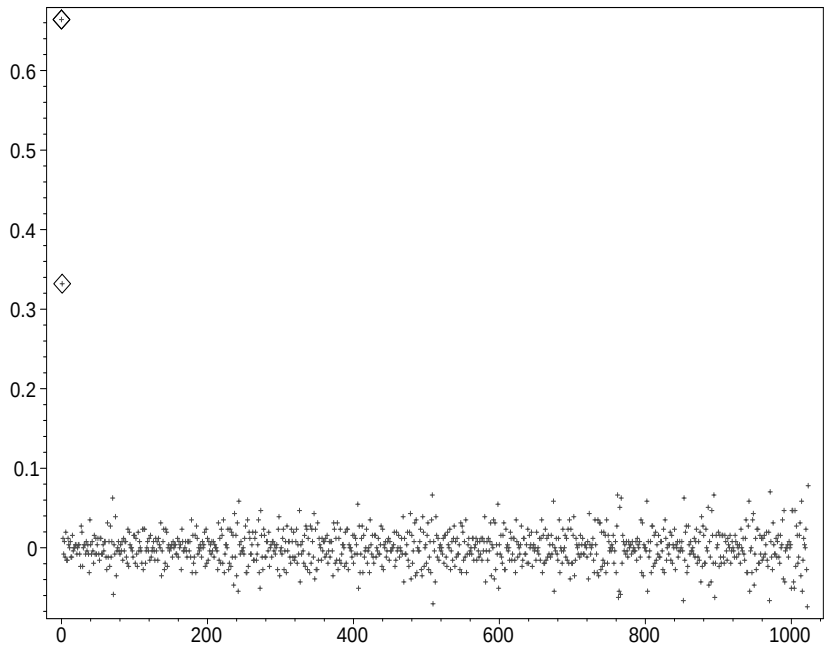


Figure 8.4: Plot of the Fourier coefficients for the primality function over the natural numbers and input size $n = 10$.

next plot for $n = 11$ we see the demise of the Fourier coefficient at 1 towards 0 and the rise of the lowest order coefficient towards 1, see Figure 8.5. We look at the values of the first two coefficients for growing values of n in Table 8.3. While the tendency seems clear, the speed of the process seems somewhat slower than what we witnessed for the squarefreeness and coprimality functions. The apparent tendency will be proven in Section 9.3.

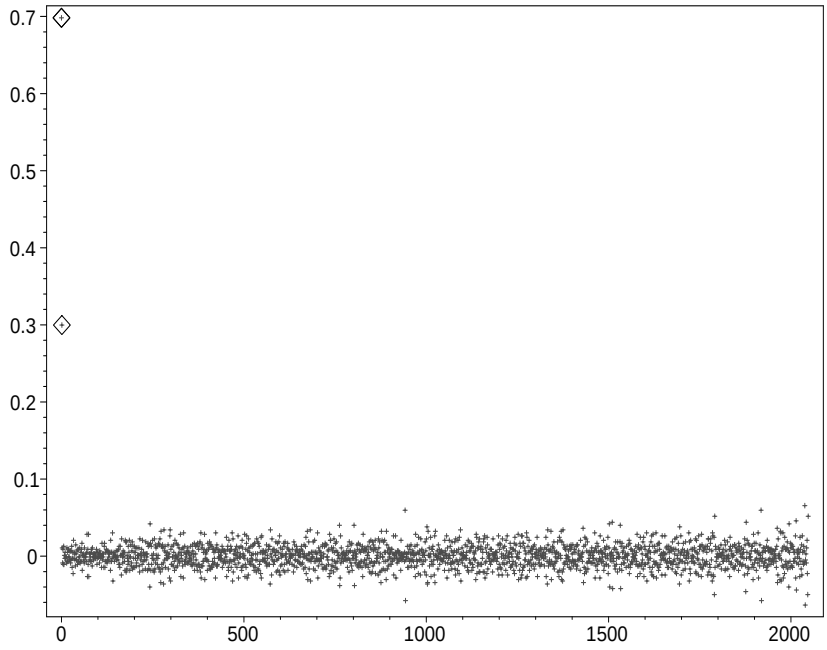


Figure 8.5: Plot of the Fourier coefficients for the primality function over the natural numbers and upper bound for the input u is $2^{11} - 1$.

n	$w = [0]_2$	$w = [1]_2$	n	$w = [0]_2$	$w = [1]_2$
1	$+0,0000000000$	$+0,0000000000$	11	$+0,6972656250$	$+0,2998046875$
2	$-0,5000000000$	$+0,0000000000$	12	$+0,7241210938$	$+0,2744140625$
3	$-0,2500000000$	$+0,5000000000$	13	$+0,7487792969$	$+0,2504882812$
4	$+0,1250000000$	$+0,5000000000$	14	$+0,7679443359$	$+0,2316894531$
5	$+0,2500000000$	$+0,5625000000$	15	$+0,7855834961$	$+0,2142333984$
6	$+0,4062500000$	$+0,5000000000$	16	$+0,8003234863$	$+0,1995849609$
7	$+0,5000000000$	$+0,4531250000$	17	$+0,8130493164$	$+0,1869049072$
8	$+0,5703125000$	$+0,4062500000$	18	$+0,8245162964$	$+0,1754608154$
9	$+0,6171875000$	$+0,3710937500$	19	$+0,8344764709$	$+0,1655120850$
10	$+0,6621093750$	$+0,3320312500$	20	$+0,8435478210$	$+0,1564464569$
			∞	$\rightarrow 1$	$\rightarrow 0$

Table 8.3: The values of the first two Fourier coefficients for the primality function over the natural numbers and input size n up to 20.

9 The Extreme Fourier Coefficients for the Natural Numbers

In order to determine the extreme Fourier coefficients for our chosen three functions over the natural numbers (in binary representation) we need to count squarefree numbers, prime numbers and pairs of coprime numbers, respectively, up to a given bound. So at the beginning of each section of this section you will find a short discourse about these quantities.

Throughout this section μ denotes the well-known Möbius function for natural numbers:

$$\mu(n) = \begin{cases} 1, & \text{if } n = 1, \\ (-1)^k, & \text{if } n \text{ is the product of } k \text{ distinct primes}, \\ 0, & \text{if } n \text{ is not squarefree.} \end{cases}$$

You can read more about the Möbius function in e.g. Apostol (1976), Chapter 2. Moreover ζ denotes the famous Riemann zeta function which is defined as

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

For our purposes we will make use of the fact that

$$\sum_{q=1}^{\infty} \frac{\mu(q)}{q^2} = \frac{1}{\zeta(2)} = \frac{6}{\pi^2}.$$

This and more information about the zeta function and some of its properties can be found e.g. in Apostol (1976), Chapters 11 and 12.

In the following sections the Fourier coefficients we look at will be described as e.g. $\widetilde{g^{\text{int}}}(010^{n-2})$, which is just an abbreviation for the coefficient $\widetilde{g^{\text{int}}}(01\underbrace{0\ldots0}_{n-2})$.

9.1 The Squarefreeness Function

Our calculations in Section 8.1 lead us to believe that there are four extreme coefficients for the squarefreeness function over the integers, namely the lowest four. Thus we have to look at the coefficients $\widetilde{g^{\text{int}}}(0^n)$, $\widetilde{g^{\text{int}}}(10^{n-1})$, $\widetilde{g^{\text{int}}}(010^{n-2})$

and $\widetilde{g^{\text{int}}}(110^{n-2})$. To this end it will be useful to consider the frequency of squarefree u's:

$$\overline{\sigma}(n) = 2^{-n} \cdot \#\{0 \le u < 2^n : u \text{ squarefree}\}.$$

Generally, the probability that a random natural number a is squarefree is well-known to be

$$\frac{\#\{1 \le a \le N : a \text{ is squarefree}\}}{N} \in \frac{6}{\pi^2} + \mathrm{O}\Big(\frac{1}{\sqrt{N}}\Big),$$

which can also be wirtten in slightly different ways. See, for example, Hardy & Wright (1985), Chapter 18.6 or von zur Gathen & Gerhard (1999), end of Chapter 3. We choose an explicite estimate for that we did not find any publication:

LEMMA 9.1. *Let $Q(x)$ be the number of squarefree numbers not exceeding x. We have the following approximation:*

$$\Big|\frac{Q(x)}{x} - \frac{6}{\pi^2}\Big| < \frac{2}{\sqrt{x}}.$$

PROOF. Take $n \le x$ and suppose that q^2 is the largest squared integer that divides n. So n is squarefree if and only if q equals 1. The number of such n is $Q(\frac{x}{q^2})$ and every number up to x corresponds to some q for which $1 \le q \le \sqrt{x}$. Hence we have

$$\lfloor x \rfloor = \sum_{1 \le q \le \sqrt{x}} Q\Big(\frac{x}{q^2}\Big)$$

or, letting $y = \sqrt{x}$,

$$\lfloor y^2 \rfloor = \sum_{1 \le q \le y} Q\Big(\frac{y^2}{q^2}\Big).$$

To go on with this proof we need the following inversion formula: If

$$G(x) = \sum_{1 \le n \le x} F\Big(\frac{x}{n}\Big)$$

for all positive x, then

$$F(x) = \sum_{1 \le n \le x} \mu(n) G\Big(\frac{x}{n}\Big).$$

For a proof see Hardy & Wright (1985), Theorem 268. Plugging in $G(y) = \lfloor y^2 \rfloor$ and $F(y) = Q(y^2)$ we get:

$$Q(y^2) = \sum_{1 \le q \le y} \mu(q) \Big\lfloor \frac{y^2}{q^2} \Big\rfloor .$$

Replacing y^2 by x and y by $\sqrt{x}$ we get

$$\begin{aligned} Q(x) &= \sum_{1 \le q \le \sqrt{x}} \mu(q) \Big\lfloor \frac{x}{q^2} \Big\rfloor \\ &= x \sum_{1 \le q \le \sqrt{x}} \frac{\mu(q)}{q^2} - \sum_{1 \le q \le \sqrt{x}} \mu(q) \underbrace{\Big(\frac{x}{q^2} - \Big\lfloor \frac{x}{q^2} \Big\rfloor \Big)}_{|\cdot| < 1} \\ &= x \sum_{q \ge 1} \frac{\mu(q)}{q^2} - x \sum_{q > \sqrt{x}} \frac{\mu(q)}{q^2} - \sum_{1 \le q \le \sqrt{x}} \mu(q) \underbrace{\Big(\frac{x}{q^2} - \Big\lfloor \frac{x}{q^2} \Big\rfloor \Big)}_{|\cdot| < 1} . \end{aligned}$$

We consider the three sums one at a time. The result for the first sum is this:

$$\sum_{q=1}^{\infty} \frac{\mu(q)}{q^2} = \frac{1}{\zeta(2)} = \frac{6}{\pi^2}.$$

The absolute value of the second sum can be bounded from above:

$$\Big| \sum_{q > \sqrt{x}}^{\infty} \frac{\mu(q)}{q^2} \Big| \le \sum_{q > \sqrt{x}}^{\infty} \frac{1}{q^2} \le \int_{\lfloor \sqrt{x} \rfloor}^{\infty} \frac{dt}{t^2} = \frac{1}{\lfloor \sqrt{x} \rfloor}.$$

The error term induced by the last sum is on the same order:

$$\Big| \sum_{1 \le q \le \sqrt{x}} \mu(q) \Big(\frac{x}{q^2} - \Big\lfloor \frac{x}{q^2} \Big\rfloor \Big) \Big| < \sum_{1 \le q \le \sqrt{x}} 1 = \lfloor \sqrt{x} \rfloor .$$

Now, we have

$$\begin{aligned} \Big| Q(x) - \frac{6x}{\pi^2} \Big| &\le x \Big| \sum_{q > \sqrt{x}} \frac{\mu(q)}{q^2} \Big| + \Big| \sum_{1 \le q \le \sqrt{x}} \mu(q) \Big(\frac{x}{q^2} - \Big\lfloor \frac{x}{q^2} \Big\rfloor \Big) \Big| \\ &< \frac{x}{\lfloor \sqrt{x} \rfloor} + \lfloor \sqrt{x} \rfloor \\ &< 2\sqrt{x} + 1 \text{ for } x \ge 1. \end{aligned}$$

□

We we can write $\overline{\sigma}$ as:

$$\overline{\sigma}(n) = 2^{-n} \cdot \#\{1 \leq u < 2^n : u \text{ squarefree}\} = 2^{-n} \cdot Q(2^n - 1).$$

For all $n \geq 2$ the power 2^n is not squarefree and the notation is easier if we let:

$$\overline{\sigma}(n) = 2^{-n} \cdot \#\{1 \leq u \leq 2^n : u \text{ squarefree}\} = 2^{-n} \cdot Q(2^n).$$

The error term does not grow much when substituting $2^n - 1$ by 2^n and for a shorter formula we would have done it anyway. We start with the lowest order Fourier coefficient. Here we have

$$\begin{aligned}
\widetilde{g^{\text{int}}}(0^n) &= \frac{1}{2^n} \sum_{u \in \mathbb{B}^n} (-1)^{g^{\text{int}}(u)+0} \\
&= \frac{1}{2^n} \left(\sum_{\substack{u \in \mathbb{B}^n \\ g^{\text{int}}(u)=0}} 1 - \sum_{\substack{u \in \mathbb{B}^n \\ g^{\text{int}}(u)=1}} 1 \right) \\
&= \frac{1}{2^n} \cdot \#\{0 \leq a < 2^n : u \text{ not squarefree}\} \\
&\quad -\frac{1}{2^n} \cdot \#\{0 \leq a < 2^n : u \text{ squarefree}\} \\
&= \frac{1}{2^n} \cdot (2^n - Q(2^n)) - \frac{1}{2^n} \cdot Q(2^n) \\
&= 1 - 2\overline{\sigma}(n).
\end{aligned}$$

This means that the lowest order Fourier coefficient converges on the following value:

$$\lim_{n \to \infty} \widetilde{g^{\text{int}}}(0^n) = 1 - 2 \cdot \frac{6}{\pi^2} \approx -0.2158542037.$$

Having found the actual limit for the lowest order Fourier coefficient we can compute an explicit error term for a given input size n.

$$\begin{aligned}
\left| \widetilde{g^{\text{int}}}(0^n) - \left(1 - \frac{12}{\pi^2}\right) \right| &= \left| 1 - 2\overline{\sigma}(n) - 1 + \frac{12}{\pi^2} \right| \\
&= \frac{2}{2^n} \left| \frac{6 \cdot 2^n}{\pi^2} - Q(2^n) \right| \\
&< \frac{2}{2^n} \cdot (2\sqrt{2^n} + 1) \\
&= 2^{-n/2+2} + 2^{-n+1} < 2^{-n/2+3}.
\end{aligned}$$

The result above matches our calculations extremely well. Remember that for $n = 20$ the value of this Fourier coefficient was -0.2158603668 (see Table 8.1), so the error is roughly $6 \cdot 10^{-6}$, while our bound from above is $2^{-8} + 2^{-17} \approx 4 \cdot 10^{-3}$.

Now, we will try to determine the next Fourier coefficient $\widetilde{g^{\text{int}}}(10^{n-1})$:

$$\begin{aligned}
\widetilde{g^{\text{int}}}(10^{n-1}) &= \frac{1}{2^n} \sum_{u \in \mathbb{B}^n} (-1)^{g^{\text{int}}(u)+u_0} \\
&= \frac{1}{2^n} \left(\sum_{\substack{u \in \mathbb{B}^n \\ g^{\text{int}}(u)=0}} (-1)^{u_0} - \sum_{\substack{u \in \mathbb{B}^n \\ g^{\text{int}}(u)=1}} (-1)^{u_0} \right) \\
&= \frac{1}{2^n} \left(\sum_{\substack{u \in \mathbb{B}^n \\ g^{\text{int}}(u)=u_0=0}} 1 + \sum_{\substack{u \in \mathbb{B}^n \\ g^{\text{int}}(u)=u_0=1}} 1 - \sum_{\substack{u \in \mathbb{B}^n \\ g^{\text{int}}(u)=0 \neq u_0}} 1 + \sum_{\substack{u \in \mathbb{B}^n \\ g^{\text{int}}(u)=1 \neq u_0}} 1 \right) \\
&= \frac{1}{2^n} \Big(\underbrace{\#\{0 \leq u < 2^n : u \text{ not squarefree}, u \text{ even}\}}_{S^{(\square,0)}(n)} \\
&\quad + \underbrace{\#\{0 \leq u < 2^n : u \text{ squarefree}, u \text{ odd}\}}_{S^{(\boxtimes,1)}(n)} \\
&\quad - \underbrace{\#\{0 \leq u < 2^n : u \text{ not squarefree}, u \text{ odd}\}}_{S^{(\square,1)}(n)} \\
&\quad - \underbrace{\#\{0 \leq u < 2^n : u \text{ squarefree}, u \text{ even}\}}_{S^{(\boxtimes,0)}(n)} \Big)
\end{aligned}$$

.

In order to find an estimate for the Fourier coefficient we consider the four cardinalities separately:

$$\begin{aligned}
S^{(\boxtimes,0)}(n) &= \#\{0 \leq u < 2^n : u \text{ squarefree}, u \text{ even}\} \\
&= \#\{0 \leq u < 2^{n-1} : u \text{ squarefree}\} - S^{(\boxtimes,0)}(n-1) \\
&= 2^{n-1}\overline{\sigma}(n-1) - S^{(\boxtimes,0)}(n-1),
\end{aligned}$$

$$\begin{aligned}
S^{(\square,0)}(n) &= \#\{0 \leq u < 2^n : u \text{ not squarefree}, u \text{ even}\} \\
&= \#\{0 \leq u < 2^{n-1} : u \text{ not squarefree}\} + S^{(\boxtimes,0)}(n-1) \\
&= 2^{n-1}(1 - \overline{\sigma}(n-1)) + S^{(\boxtimes,0)}(n-1),
\end{aligned}$$

$$\begin{aligned} S^{(\boxtimes,1)}(n) &= \#\{0 \le u < 2^n : u \text{ squarefree}, u \text{ odd}\} \\ &= \#\{0 \le u < 2^n : u \text{ squarefree}\} - S^{(\boxtimes,0)}(n) \\ &= 2^n\overline{\sigma}(n) - S^{(\boxtimes,0)}(n), \end{aligned}$$

$$\begin{aligned} S^{(\square,1)}(n) &= \#\{0 \le u < 2^n : u \text{ not squarefree}, u \text{ odd}\} \\ &= \#\{0 \le u < 2^n : u \text{ not squarefree}\} - S^{(\square,0)}(n) \\ &= 2^n(1-\overline{\sigma}(n)) - 2^{n-1}(1-\overline{\sigma}(n-1)) - S^{(\boxtimes,0)}(n-1). \end{aligned}$$

The first of these four equations is a recursion formula for $S^{(\boxtimes,0)}(n)$ which, together with $S^{(\boxtimes,0)}(0) = 0$, leads to

$$S^{(\boxtimes,0)}(n) = \sum_{0 \le i < n} (-1)^{n-1-i} \cdot Q(2^i).$$

Insertion of this sum for $S^{(\boxtimes,0)}$ into the recursion formula yields

$$\begin{aligned} S^{(\boxtimes,0)}(n) &= 2^{n-1}\overline{\sigma}(n-1) - S^{(\boxtimes,0)}(n-1) \\ &= Q(2^{n-1}) - \sum_{0 \le i < n-1} (-1)^{n-2-i} Q(2^i) \\ &= (-1)^{(n-1)-(n-1)} Q(2^{n-1}) + \sum_{0 \le i < n-1} (-1)^{n-1-i} Q(2^i) \\ &= \sum_{0 \le i < n} (-1)^{n-1-i} Q(2^i), \end{aligned}$$

which proves the formula. Combining this we have for the second lowest Fourier coefficient:

$$\begin{aligned} \widetilde{g^{\text{int}}}(10^{n-1}) &= \frac{1}{2^n}(S^{(\square,0)}(n) + S^{(\boxtimes,1)}(n) - S^{(\square,1)}(n) - S^{(\boxtimes,0)}(n)) \\ &= \frac{1}{2^n}\Bigg(2^{n-1}(1-\overline{\sigma}(n)) + S^{(\boxtimes,0)}(n-1) + 2^n\overline{\sigma}(n) - S^{(\boxtimes,0)}(n) \\ &- 2^n(1-\overline{\sigma}(n)) + 2^{n-1}(1-\overline{\sigma}(n-1)) + S^{(\boxtimes,0)}(n-1) - S^{(\boxtimes,0)}(n)\Bigg) \\ &= \frac{1}{2^n}\Big(2^n(2\overline{\sigma}(n) - \overline{\sigma}(n-1)) - 2(S^{(\boxtimes,0)}(n) - S^{(\boxtimes,0)}(n-1))\Big) \\ &= \frac{1}{2^n}\Big(4 \cdot \sum_{0 \le i < n} (-1)^{n-i} Q(2^i) + 2Q(2^n)\Big). \end{aligned}$$

The following calculations lead us to the limit of the Fourier coefficient $\widetilde{g^{\text{int}}}(10^{n-1})$:

$$\begin{aligned}
&\frac{1}{2^n}\left(4\cdot\sum_{0\le i<n}(-1)^{n-i}\cdot\frac{6\cdot 2^i}{\pi^2}+2\cdot\frac{6\cdot 2^n}{\pi^2}\right)\\
&= \frac{1}{2^n}\left(\frac{24}{\pi^2}\cdot(-1)^n\sum_{0\le i<n}(-2)^i+\frac{12\cdot 2^n}{\pi^2}\right)\\
&= \frac{1}{2^n}\left(-\frac{8}{\pi^2}\cdot(2^n-1)+\frac{12\cdot 2^n}{\pi^2}\right)\\
&= \frac{1}{2^n}\left(\frac{4\cdot 2^n}{\pi^2}+\frac{8}{\pi^2}\right)\\
&= \frac{4}{\pi^2}+\frac{8}{\pi^2\cdot 2^n}.
\end{aligned}$$

In fact, the limit of the second lowest Fourier coefficient is this:

$$\lim_{n\to\infty}\widetilde{g^{\text{int}}}(10^{n-1})=\frac{4}{\pi^2}\approx 0.4052847345.$$

Again, we will show this by determining an explicit error bound:

$$\begin{aligned}
&\left|\widetilde{g^{\text{int}}}(10^{n-1})-\frac{4}{\pi^2}\right|\\
&= \frac{1}{2^n}\left|4\cdot\sum_{0\le i<n}(-1)^{n-i}Q(2^i)+2Q(2^n)-4\cdot\sum_{0\le i<n}(-1)^{n-i}\frac{6\cdot 2^i}{\pi^2}-2\frac{6\cdot 2^n}{\pi^2}+\frac{8}{\pi^2}\right|\\
&\le \frac{1}{2^n}\left(4\cdot\sum_{0\le i<n}\left|Q(2^i)-\frac{6\cdot 2^i}{\pi^2}\right|+2\cdot\left|Q(2^n)-\frac{6\cdot 2^n}{\pi^2}\right|+\frac{8}{\pi^2}\right)\\
&< \frac{1}{2^n}\left(4\cdot\sum_{0\le i<n}(2\cdot\sqrt{2^i}+4)+2\cdot 2\cdot\sqrt{2^n}+4+\frac{8}{\pi^2}\right)\\
&\le 3\cdot 2^{-\frac{n}{2}+3}+2^{-n+4}\cdot(n+1)+\frac{8}{\pi^2\cdot 2^n}<2^{-n/2+4}\cdot(n+3).
\end{aligned}$$

Once again the result corresponds excellently to the experiments we displayed in Table 8.1.

For the estimation of the next two Fourier coefficients we need the following frequency:

$$\overline{\overline{\sigma}}(n)=2^{-(n-2)}\cdot\#\{0\le u<2^n\colon u \text{ squarefree}, u\equiv 1 \bmod 4\}.$$

Evidently, this definition implies:

$$2^{-(n-2)} \cdot \#\{0 \le u < 2^n : u \text{ not squarefree}, u \equiv 1 \bmod 4\} = 1 - \overline{\overline{\sigma}}(n).$$

In order to calculate these numbers we will use the following explicit bound for a result of Prachar (1961). To our knowledge an explicit bound for this was not published before:

THEOREM 9.2. *Let $Q(x,k,\ell)$ denote the number of squarefree natural numbers $q \le x$ and satisfy the additional congruence:*

$$q \equiv \ell \bmod k,$$

where $x, \ell, k \in \mathbb{N}$, $0 \le \ell < k$ and $\gcd(k,\ell)$ is squarefree. Then

$$\begin{aligned} \Big|\frac{Q(x,k,\ell)}{x} - \frac{A}{k}\Big| &\le \frac{1}{x}\left(\Big(1+\frac{1}{k}\Big)\sqrt{x} + \frac{1}{k}\Big(1+\frac{1}{\lfloor\sqrt{x}\rfloor}\Big)\right) \\ &\le 2 \cdot \frac{\sqrt{x}+1}{x}, \end{aligned}$$

where

$$A = \frac{6}{\pi^2}\prod_{p|k}\left(1-\frac{1}{p^2}\right)^{-1}.$$

Note that if the greatest common divisor of k and ℓ is not squarefree there are no squarefree numbers which are congruent to $\ell \bmod k$. For our purposes we will actually assume that $\gcd(k,\ell) = 1$. This way the proof is much simpler and we only need it for that case.

PROOF. (Only for $\gcd(k,\ell) = 1$.) First, we notice that

$$Q(x,k,\ell) = \sum_{\substack{m \le x \\ m \equiv \ell \bmod k}} \mu^2(m),$$

because for every squarefree natural number n we have $\mu(n) = \pm 1$. Furthermore we know from Apostol (1976), Chapter 2, Exercise 6, that

$$\mu^2(m) = \sum_{d^2|m} \mu(d).$$

Combining this we can write $Q(x,k,\ell)$ as follows:

$$Q(x,k,\ell) = \sum_{\substack{m\le x\\ m\equiv \ell \bmod k}} \mu^2(m) = \sum_{\substack{m\le x\\ m\equiv \ell \bmod k}} \sum_{d^2\mid m} \mu(d) = \sum_{\substack{d^2n\le x\\ d^2n\equiv \ell \bmod k}} \mu(d).$$

From $d^2n \equiv \ell \bmod k$ and $\gcd(k,\ell) = 1$ we get $\gcd(d,k) = 1$. For a fixed d the solution n of the congruence is uniquely determined modulo k. Hence the number of possible solutions n is $\frac{x}{d^2k} + v$, where $v \in [-1,1]$. Then

$$\sum_{\substack{d\le\sqrt{x}\\ \gcd(d,k)=1}} \mu(d)\Big(\frac{x}{d^2k} + v\Big) \;=\; \frac{x}{k} \sum_{\substack{d\le\sqrt{x}\\ \gcd(d,k)=1}} \frac{\mu(d)}{d^2} + \sum_{\substack{d\le\sqrt{x}\\ \gcd(d,k)=1}} \mu(d)v.$$

For the first sum we have

$$\sum_{\substack{d\le\sqrt{x}\\ \gcd(d,k)=1}} \frac{\mu(d)}{d^2} = \sum_{\substack{d>0\\ \gcd(d,k)=1}} \frac{\mu(d)}{d^2} - \sum_{\substack{d>\sqrt{x}\\ \gcd(d,k)=1}} \frac{\mu(d)}{d^2}.$$

Now, we have to evaluate the sum $\sum_{\substack{d>0\\ \gcd(d,k)=1}} \frac{\mu(d)}{d^2}$. In order to do so we consider the so-called principal Dirichlet character χ_1 (for more information see Apostol 1976, Chapter 6):

$$\chi_1(n) = \begin{cases} 1, & \text{if } \gcd(n,k) = 1,\\ 0, & \text{if } \gcd(n,k) > 1. \end{cases}$$

This function is completely multiplicative. Hence we can rewrite our sum as

$$\sum_{\substack{d>0\\ \gcd(d,k)=1}} \frac{\mu(d)}{d^2} = \sum_{d>0} \frac{\chi_1(d)\cdot\mu(d)}{d^2}.$$

Now consider the function $\mu_\chi = \chi_1 \cdot \mu$, which is also multiplicative but not completely so. From Apostol (1976), Theorem 11.7, we also learn that for a multiplicative function f for which $\sum f(n)n^{-s}$ converges absolutely, it holds that

$$\sum_{n>0} \frac{f(n)}{n^s} = \prod_p \left(1 + \frac{f(p)}{p^s} + \frac{f(p^2)}{p^{2s}} + \dots\right) \tag{9.3}$$

and furthermore

$$\prod_{p\nmid k} \frac{1}{1-p^{-s}} = \prod_p \frac{1}{1-p^{-s}} \cdot \prod_{p\mid k}(1-p^{-s}) = \zeta(s)\prod_{p\mid k}(1-p^{-s}), \tag{9.4}$$

where ζ is the well-known Riemann zeta function. Insertion of our function μ_χ, writing d instead of n and plugging in $s = 2$ in (9.3) gives us

$$\begin{aligned}\sum_{d>0} \frac{\chi_1(d)\mu(d)}{d^2} &= \prod_p \left(1 + \frac{\chi_1(p)\mu(p)}{p^2} + \frac{\chi_1(p^2)\mu(p^2)}{p^4} + \dots\right) \\ &= \prod_p \left(1 + \frac{\chi_1(p)\mu(p)}{p^2}\right) \\ &= \prod_p \left(1 - \frac{\chi_1(p)}{p^2}\right) \\ &= \prod_{p\nmid k} \left(1 - p^{-2}\right),\end{aligned}$$

because of the properties of the Möbius function μ and the principal Dirichlet character χ_1. Using (9.4) we get

$$\sum_{\substack{d\geq 1\\ \gcd(d,k)=1}} \frac{\mu(d)}{d^2} = \left(\zeta(2)\prod_{p|k}(1-p^{-2})\right)^{-1} = \frac{1}{\zeta(2)}\cdot\prod_{p|k}\left(1-\frac{1}{p^2}\right)^{-1} = \frac{6}{\pi^2}\cdot\prod_{p|k}\left(1-\frac{1}{p^2}\right)^{-1}.$$

Now, we are left with the estimation of the error terms:

$$\begin{aligned}\sum_{1\leq d\leq\sqrt{x}} |\mu(d)v| &\leq \sum_{1\leq d\leq\sqrt{x}} 1 \leq \lfloor\sqrt{x}\rfloor, \\ \frac{x}{k}\sum_{\substack{d>\sqrt{x}\\ \gcd(d,k)=1}} \left|\frac{\mu(d)}{d^2}\right| &\leq \frac{x}{k}\sum_{d>\sqrt{x}} \frac{1}{d^2} \leq \frac{x}{k}\int_{\lfloor\sqrt{x}\rfloor}^{\infty} \frac{dt}{t^2} = \frac{x}{k}\frac{1}{\lfloor\sqrt{x}\rfloor}.\end{aligned}$$

In conclusion we arrive at the following approximation of $Q(x,k,\ell)$ and the corresponding error estimation:

$$\begin{aligned}\left|Q(x,k,\ell) - \frac{x}{k}\cdot\frac{6}{\pi^2}\cdot\prod_{p|k}\left(1-\frac{1}{p^2}\right)^{-1}\right| &\leq \frac{x}{k}\cdot\frac{1}{\lfloor\sqrt{x}\rfloor} + \lfloor\sqrt{x}\rfloor \\ &\leq \left(1+\frac{1}{k}\right)\sqrt{x} + \frac{1}{k}\left(1+\frac{1}{\lfloor\sqrt{x}\rfloor}\right) \\ &\leq 2\cdot(\sqrt{x}+1).\end{aligned}$$

This concludes the proof of Theorem 9.2. □

Again, we will insert 2^n instead of $2^n - 1$ in the formula we have just proven, because this does not change the limit (only the estimates of the error term become a little bigger than they have to be) and keeps the notation clean:

$$\begin{aligned}\overline{\overline{\sigma}}(n) = 2^{-(n-2)} \cdot Q(2^n, 4, 1) &\approx \frac{6}{\pi^2} \prod_{p|4} \left(1 - \frac{1}{p^2}\right)^{-1} \\ &= \frac{6}{\pi^2} \left(1 - \frac{1}{4}\right)^{-1} \\ &= \frac{6}{\pi^2} \cdot \frac{4}{3} = \frac{8}{\pi^2}.\end{aligned}$$

We get

$$\left| \overline{\overline{\sigma}}(n) - \frac{8}{\pi^2} \right| \leq 2^{-n/2+4}. \tag{9.5}$$

The next Fourier coefficient is $\widetilde{g^{\text{int}}}(010^{n-2})$:

$$\begin{aligned}\widetilde{g^{\text{int}}}(010^{n-2}) &= \frac{1}{2^n} \sum_{u \in \mathbb{B}^n} (-1)^{g^{\text{int}}(u)+u_1} \\ &= \frac{1}{2^n} \Bigg(\underbrace{\sum_{\substack{u \in \mathbb{B}^n \\ g^{\text{int}}(u)=0=u_1}} 1}_{\hat{S}^{(\square,0)}(n)} + \underbrace{\sum_{\substack{u \in \mathbb{B}^n \\ g^{\text{int}}(u)=1=u_1}} 1}_{\hat{S}^{(\boxtimes,1)}(n)} - \underbrace{\sum_{\substack{u \in \mathbb{B}^n \\ g^{\text{int}}(u)=0\neq u_1}} 1}_{\hat{S}^{(\square,1)}(n)} - \underbrace{\sum_{\substack{u \in \mathbb{B}^n \\ g^{\text{int}}(u)=1\neq u_1}} 1}_{\hat{S}^{(\boxtimes,0)}(n)} \Bigg)\end{aligned}$$

Once more we will consider the sums one at a time. The condition $u_1 = 0$ is equivalent to $u \equiv 0, 1 \bmod 4$:

$$\begin{aligned}\hat{S}_0^{(\square,0)}(n) &= \#\{0 \leq u < 2^n : u \text{ not squarefree}, u_1 = 0, u_0 = 0\} \\ &= \#\{0 \leq u < 2^n : u \text{ not squarefree}, u \equiv 0 \bmod 4\} \\ &= 2^{n-2},\end{aligned}$$

$$\begin{aligned}\hat{S}_1^{(\square,0)}(n) &= \#\{0 \leq u < 2^n : u \text{ not squarefree}, u_1 = 0, u_0 = 1\} \\ &= \#\{0 \leq u < 2^n : u \text{ not squarefree}, u \equiv 1 \bmod 4\} \\ &= 2^{n-2} \cdot (1 - \overline{\overline{\sigma}}(n)).\end{aligned}$$

Thus

$$\begin{aligned}\hat{S}^{(\square,0)}(n) &= \hat{S}_0^{(\square,0)}(n) + \hat{S}_1^{(\square,0)}(n)\\ &= 2^{n-2} + 2^{n-2} - 2^{n-2}\overline{\overline{\sigma}}(n) = 2^{n-1} - 2^{n-2}\overline{\overline{\sigma}}(n).\end{aligned}$$

The condition $u_1 = 1$ is equivalent to $u \equiv 2, 3 \bmod 4$:

$$\begin{aligned}\hat{S}_0^{(\boxtimes,1)}(n) &= \#\{0 \le u < 2^n : u \text{ squarefree}, u_1 = 1, u_0 = 0\}\\ &= \#\{0 \le u < 2^n : u \text{ squarefree}, u \equiv 2 \bmod 4\}\\ &= \#\{0 \le u < 2^{n-1} : u \text{ squarefree}, u \text{ odd}\} = S^{(\boxtimes,1)}(n-1)\\ &= Q(2^{n-1}) - \sum_{0 \le i < n-1} (-1)^{n-2-i} Q(2^i),\end{aligned}$$

$$\begin{aligned}\hat{S}_1^{(\boxtimes,1)}(n) &= \#\{0 \le u < 2^n : u \text{ squarefree}, u_1 = 1, u_0 = 1\}\\ &= \#\{0 \le u < 2^n : u \text{ squarefree}, u \equiv 3 \bmod 4\}\\ &= \#\{0 \le u < 2^n : u \text{ squarefree}, u \text{ odd}\} - 2^{n-2}\overline{\overline{\sigma}}(n)\\ &= S^{(\boxtimes,1)}(n) - 2^{n-2}\overline{\overline{\sigma}}(n)\\ &= Q(2^n) - \sum_{0 \le i < n} (-1)^{n-1-i} Q(2^i) - 2^{n-2}\overline{\overline{\sigma}}(n).\end{aligned}$$

Hence

$$\begin{aligned}\hat{S}^{(\boxtimes,1)}(n) &= \hat{S}_0^{(\boxtimes,1)}(n) + \hat{S}_1^{(\boxtimes,1)}(n)\\ &= Q(2^n) + Q(2^{n-1}) - \sum_{0 \le i < n-1} (-1)^{n-2-i} Q(2^i)\\ &\qquad - \sum_{0 \le i < n} (-1)^{n-1-i} Q(2^i) - 2^{n-2}\overline{\overline{\sigma}}(n)\\ &= Q(2^n) - 2^{n-2}\overline{\overline{\sigma}}(n).\end{aligned}$$

We continue with the next sum using the condition $u_1 = 1$:

$$\begin{aligned}\hat{S}_0^{(\square,1)}(n) &= \#\{0 \le u < 2^n : u \text{ not squarefree}, u_1 = 1, u_0 = 0\}\\ &= \#\{0 \le u < 2^n : u \text{ not squarefree}, u \equiv 2 \bmod 4\}\\ &= \#\{0 \le u < 2^n : u \text{ not squarefree}, u \text{ even}\}\\ &\quad -\#\{0 \le u < 2^n : u \text{ not squarefree}, u \equiv 0 \bmod 4\}\\ &= S^{(\square,0)} - 2^{n-2} = 2^{n-2} + \sum_{0 \le i < n} (-1)^{n-2-i} Q(2^i),\end{aligned}$$

$$\begin{aligned}\hat{S}_1^{(\square,1)}(n) &= \#\{0 \le u < 2^n : u \text{ not squarefree}, u_1 = 1, u_0 = 1\} \\ &= \#\{0 \le u < 2^n : u \text{ not squarefree}, u \equiv 3 \bmod 4\} \\ &= \#\{0 \le u < 2^n : u \text{ not squarefree}, u \text{ odd}\} - 2^{n-2} \cdot (1 - 2^{n-2}\overline{\overline{\sigma}}) \\ &= 2^{n-2} + 2^{n-2}\overline{\overline{\sigma}}(n) - \sum_{0 \le i \le n} (-1)^{n-2-i} Q(2^i).\end{aligned}$$

Therefore

$$\begin{aligned}\hat{S}^{(\square,1)}(n) &= \hat{S}_0^{(\square,1)}(n) + \hat{S}_1^{(\square,1)}(n) \\ &= 2^{n-1} + 2^{n-2}\overline{\overline{\sigma}}(n) + \sum_{0 \le i < n} (-1)^{n-2-i} Q(2^i) - \sum_{0 \le i \le n} (-1)^{n-2-i} Q(2^i) \\ &= 2^{n-1} + 2^{n-2}\overline{\overline{\sigma}}(n) - Q(2^n).\end{aligned}$$

Considering the last sum, we have once again the condition $u_1 = 0$:

$$\begin{aligned}\hat{S}_0^{(\boxtimes,0)}(n) &= \#\{0 \le u < 2^n : u \text{ squarefree}, u_1 = 0, u_0 = 0\} \\ &= \#\{0 \le u < 2^n : u \text{ squarefree}, u \equiv 0 \bmod 4\} \\ &= 0,\end{aligned}$$

$$\begin{aligned}\hat{S}_1^{(\boxtimes,0)}(n) &= \#\{0 \le u < 2^n : u \text{ squarefree}, u_1 = 0, u_0 = 1\} \\ &= \#\{0 \le u < 2^n : u \text{ squarefree}, u \equiv 1 \bmod 4\} \\ &= 2^{n-2}\overline{\overline{\sigma}}(n).\end{aligned}$$

Here

$$\begin{aligned}\hat{S}^{(\boxtimes,0)}(n) &= \hat{S}_0^{(\boxtimes,0)}(n) + \hat{S}_1^{(\boxtimes,0)}(n) \\ &= 2^{n-2}\overline{\overline{\sigma}}(n).\end{aligned}$$

Now we are ready to estimate the third coefficient

$$\begin{aligned}\widetilde{g^{\text{int}}}(010^{n-2}) &= \frac{1}{2^n}\Big(\hat{S}^{(\square,0)}(n) + \hat{S}^{(\boxtimes,1)}(n) - \hat{S}^{(\square,1)}(n) - \hat{S}^{(\boxtimes,0)}(n)\Big) \\ &= \frac{1}{2^n}\Big(2^{n-1} - 2^{n-2}\overline{\overline{\sigma}}(n) + Q(2^n) - 2^{n-2}\overline{\overline{\sigma}}(n) \\ &\qquad -2^{n-1} - 2^{n-2}\overline{\overline{\sigma}}(n) + Q(2^n) - 2^{n-2}\overline{\overline{\sigma}}(n)\Big) \\ &= \frac{1}{2^n}\Big(- 4 \cdot 2^{n-2}\overline{\overline{\sigma}}(n) + 2 \cdot Q(2^n)\Big)\end{aligned}$$

This allows us to calculate the limit for $\widetilde{g^{\mathrm{int}}}(010^{n-2})$:

$$\frac{1}{2^n}\left(-4\cdot\frac{8\cdot 2^{n-2}}{\pi^2}+2\cdot\frac{6\cdot 2^n}{\pi^2}\right)=-\frac{8}{\pi^2}+\frac{12}{\pi^2}=\frac{4}{\pi^2}.$$

This limit is

$$\lim_{n\to\infty}\widetilde{g^{\mathrm{int}}}(010^{n-2})=\frac{4}{\pi^2}\approx 0.4052847345,$$

which is the same as the one we found for $\widetilde{g^{\mathrm{int}}}(10^{n-1})$. As error bound we get in this case:

$$\begin{aligned}
&\left|\widetilde{g^{\mathrm{int}}}(010^{n-2})-\frac{4}{\pi^2}\right|\\
&\quad=\frac{1}{2^n}\left|-4\cdot 2^{n-2}\overline{\overline{\sigma}}(n)+2\cdot Q(2^n)-\left(-4\cdot\frac{8\cdot 2^{n-2}}{\pi^2}+2\cdot\frac{6\cdot 2^n}{\pi^2}\right)\right|\\
&\quad\le\frac{4}{2^n}\left|\frac{8\cdot 2^{n-2}}{\pi^2}-2^{n-2}\overline{\overline{\sigma}}(n)\right|+\frac{2}{2^n}\cdot\left|Q(2^n)-\frac{6\cdot 2^n}{\pi^2}\right|\\
&\quad\le\frac{4}{2^n}\Big(2^{n/2+1}+2\Big)+\frac{2}{2^n}\Big(2\cdot 2^{n/2}+4\Big)\\
&\quad=3\cdot 2^{-n/2+2}+2^{-n+4}=12\cdot 2^{-n/2}.
\end{aligned}$$

The last Fourier coefficient we want to consider is $\widetilde{g^{\mathrm{int}}}(110^{n-2})$:

$$\begin{aligned}
&\widetilde{g^{\mathrm{int}}}(110^{n-2})\\
&\quad=\frac{1}{2^n}\sum_{u\in\mathbb{B}}(-1)^{g^{\mathrm{int}}(u)+u_0+u_1}\\
&\quad=\frac{1}{2^n}\Big(\sum_{\substack{u\in\mathbb{B}\\ g^{\mathrm{int}}(u)=0}}(-1)^{u_0+u_1}-\sum_{\substack{u\in\mathbb{B}\\ g^{\mathrm{int}}(u)=1}}(-1)^{u_0+u_1}\Big)\\
&\quad=\frac{1}{2^n}\Big(\underbrace{\sum_{\substack{u\in\mathbb{B}\\ g^{\mathrm{int}}(u)=u_0+u_1=0}}1}_{S_1}+\underbrace{\sum_{\substack{u\in\mathbb{B}\\ g^{\mathrm{int}}(u)=u_0+u_1=1}}1}_{S_2}-\underbrace{\sum_{\substack{u\in\mathbb{B}\\ g^{\mathrm{int}}(u)\neq u_0+u_1=1}}1}_{S_3}-\underbrace{\sum_{\substack{u\in\mathbb{B}\\ g^{\mathrm{int}}(u)\neq u_0+u_1=0}}1}_{S_4}\Big)
\end{aligned}$$

With the cardinalities from the previous calculations we have for the first sum:

$$\begin{aligned}
S_1&=\hat{S}_1^{(\square,1)}+\hat{S}_0^{(\square,0)}\\
&=2^{n-1}+2^{n-2}\overline{\overline{\sigma}}(n)-\sum_{0\le i\le n}(-1)^{n-2-i}Q(2^i).
\end{aligned}$$

For S_2 it follows that

$$\begin{aligned} S_2 &= \hat{S}_0^{(\boxtimes,1)} + \hat{S}_1^{(\boxtimes,0)} \\ &= 2^{n-2}\overline{\overline{\sigma}}(n) + Q(2^{n-1}) - \sum_{0\le i<n-1} (-1)^{n-2-i} Q(2^i). \end{aligned}$$

Looking at S_3 we get

$$\begin{aligned} S_3 &= \hat{S}_0^{(\square,1)} + \hat{S}_1^{(\square,0)} \\ &= 2^{n-1} - 2^{n-2}\overline{\overline{\sigma}}(n) + \sum_{0\le i<n} (-1)^{n-2-i} Q(2^i). \end{aligned}$$

Finally we have for S_4

$$\begin{aligned} S_4 &= \hat{S}_1^{(\boxtimes,1)} + \hat{S}_0^{(\boxtimes,0)} \\ &= -2^{n-2}\overline{\overline{\sigma}}(n) + Q(2^n) + \sum_{0\le i<n} (-1)^{n-2-i} Q(2^i). \end{aligned}$$

Altogether it follows that

$$\begin{aligned} \widetilde{g^{\text{int}}}(110^{n-2}) &= \frac{1}{2^n}(S_1 + S_2 - S_3 - S_4) \\ &= \frac{1}{2^n}\Big(2^n\overline{\overline{\sigma}}(n) + 4Q(2^{n-1}) - 2Q(2^n) - 4\sum_{0\le i<n-1} (-1)^{n-2-i} Q(2^i)\Big) \end{aligned}$$

In much the same way as was used for the previous coefficients we calculate the limit of $\widetilde{g^{\text{int}}}(110^{n-2})$:

$$\begin{aligned} & \frac{1}{2^n}\left(4\cdot\frac{8\cdot 2^{n-2}}{\pi^2} + 4\cdot\frac{6\cdot 2^{n-1}}{\pi^2} - 2\cdot\frac{6\cdot 2^n}{\pi^2} - 4\cdot\sum_{0\le i<n-1}(-1)^{n-2-i}\frac{6\cdot 2^i}{\pi^2}\right) \\ = \ & \frac{1}{2^n}\left(\frac{8\cdot 2^n}{\pi^2} + \frac{8}{\pi^2}\cdot((-1)^{n-1} - 2^{n-1})\right) \\ = \ & \frac{4}{\pi^2} + \frac{(-1)^{n-1}}{2^{n-3}\cdot\pi^2}. \end{aligned}$$

We see that $\widetilde{g^{\text{int}}}(110^{n-2})$ converges on the same value as the two Fourier coefficients we have estimated before:

$$\lim_{n\to\infty} \widetilde{g^{\text{int}}}(110^{n-2}) = \frac{4}{\pi^2} \approx 0.4052847345.$$

This was the value we expected after observing the results of our experiments. We can do the following estimation for the error term:

$$\begin{aligned}
&\left|\widetilde{g^{\mathrm{int}}}(110^{n-2}) - \frac{4}{\pi^2}\right| \\
&\leq \frac{1}{2^n}\Bigg(4\left|2^{n-2}\overline{\overline{\sigma}}(n) - \frac{8\cdot 2^{n-2}}{\pi^2}\right| + 4\left|Q(2^{n-1}) - \frac{6\cdot 2^{n-1}}{\pi^2}\right| \\
&\qquad\qquad +2\left|\frac{6\cdot 2^n}{\pi^2} - Q(2^n)\right| + 4\sum_{0\leq i<n-1}\left|Q(2^i) - \frac{6\cdot 2^i}{\pi^2}\right| + \left|\frac{(-1)^{n-1}}{2^{n-3}\cdot\pi^2}\right|\Bigg) \\
&< \frac{1}{2^n}\Bigg(4\Big(2^{n/2+1}+2\Big) + 4\Big(2\cdot 2^{(n-1)/2}+4\Big) \\
&\qquad\qquad +2\Big(2\cdot 2^{n/2}+4\Big) + 4\sum_{0\leq i<n-1}\Big(2\cdot\sqrt{2^i}+4\Big) + \frac{2^{-n+3}}{\pi^2}\Bigg) \\
&< 2^{-n/2+5} + 2^{-n+4}\cdot(2n-1) + \frac{2^{-n+3}}{\pi^2} < 2^{-n/2+5}\cdot(n+1).
\end{aligned}$$

Putting everything together we get the following theorem, that as far as we know is original to this work:

THEOREM 9.6. *For the four lowest order Fourier coefficients for the square-freeness function over the natural numbers we have*

- $\left|\widetilde{g^{\mathrm{int}}}(0^n) - \left(1 - \frac{12}{\pi^2}\right)\right| < 2^{-n/2+3}$,
- $\left|\widetilde{g^{\mathrm{int}}}(10^{n-1}) - \frac{4}{\pi^2}\right| < 2^{-n/2+4}\cdot(n+3)$,
- $\left|\widetilde{g^{\mathrm{int}}}(010^{n-2}) - \frac{4}{\pi^2}\right| \leq 12\cdot 2^{-n/2}$ *and*
- $\left|\widetilde{g^{\mathrm{int}}}(1^20^{n-2}) - \frac{4}{\pi^2}\right| < 2^{-n/2+5}\cdot(n+1)$.

9.2 The Coprimality Function

Throughout this section $\ln x$ denotes the natural logarithm of x.

Looking at our calculations in Section 8.2 it seems highly probable that there are also four significant Fourier coefficients for the coprimality function. We will look at the coefficients $\widetilde{h^{\text{int}}}(0^{2\ell})$, $\widetilde{h^{\text{int}}}(10^{2\ell-1})$, $\widetilde{h^{\text{int}}}(0^{\ell}10^{\ell-1})$ and $\widetilde{h^{\text{int}}}(10^{\ell-1}10^{\ell-1})$. For the consideration of these coefficients it will be very useful to look at the following frequency:

$$\overline{\gamma}(\ell) = 2^{-2\ell} \cdot \#\{0 \le u, v < 2^{\ell} : \gcd(u, v) = 1\}.$$

LEMMA 9.7. *Let $C(x)$ be the number of pairs of integers (a, b) with $1 \le a, b \le x$ that are coprime. Then we have*

$$\begin{aligned} \left|\frac{C(x)}{x^2} - \frac{6}{\pi^2}\right| &\le \frac{1}{\lfloor x \rfloor} + 2 \cdot \frac{1 + \ln x}{x} \\ &\le \frac{2 + 2\ln x}{x} + 1. \end{aligned}$$

PROOF. Euler's totient function will be useful for our purposes:

$$\varphi(n) = \#\{1 \le a \le n, \gcd(a, n) = 1\}.$$

From von zur Gathen *et al.* (2004) it is known, that the average $\overline{\varphi}(x) = \frac{1}{x}\sum_{1 \le n \le x} \varphi(n)$ satisfies:

$$\left|\overline{\varphi}(x) - \frac{x}{2\zeta(2)}\right| = \left|\overline{\varphi}(x) - \frac{3x}{\pi^2}\right| < 2 + \ln x.$$

However, for our purposes we do not need the average value for $\varphi(n)$, but we want to count the number of *ordered* coprime pairs. As a general strategy we will first count those pairs where the maximum of the two integers is some fixed number n. For this we have to consider all pairs (a, n) with $1 \le a \le n$ but also the pairs (n, b) with $1 \le b \le n$. This yields $2\varphi(n)$ pairs unless $n = 1$, since the only pair that is considered twice is (n, n) which is non-coprime for $n \ge 2$. We compensate for counting the pair $(1, 1)$ twice by subtracting the overcharged $\varphi(1) = 1$.

At this point we can derive a result for our purposes directly from the result of von zur Gathen *et al.* (2004), because $C(x) = -1 + 2\sum_{1\le n\le x}\varphi(n)$:

$$\begin{aligned}\left|\frac{C(x)}{x^2} - \frac{6}{\pi^2}\right| &= \left| -\frac{1}{x^2} + \frac{2}{x}\overline{\varphi}(x) - \frac{6}{\pi^2}\right| \\ &\le \frac{2}{x}\cdot\left|\overline{\varphi}(x) - \frac{3x}{\pi^2}\right| + \frac{1}{x^2} \\ &< \frac{4+2\ln x}{x} + \frac{1}{x^2}.\end{aligned}$$

But we can get a better error bound if we make a proof similar to that in von zur Gathen *et al.* (2004) for our problem. We use a theorem from Apostol (1976), Theorem 2.3:

$$\varphi(n) = \sum_{d|n}\mu(d)\frac{n}{d}.$$

This yields

$$\begin{aligned}C(x) &= -1 + 2\sum_{1\le n\le x}\varphi(n) \\ &= -1 + 2\sum_{n\le x}\sum_{d|n}\mu(d)\frac{n}{d} \\ &= -1 + 2\sum_{\substack{q,d\\ qd\le x}}\mu(d)q \\ &= -1 + 2\sum_{d\le x}\mu(d)\sum_{q\le\lfloor x/d\rfloor} q \\ &= -1 + \sum_{d\le x}\mu(d)\left\lfloor\frac{x}{d}\right\rfloor^2 + \sum_{d\le x}\mu(d)\left\lfloor\frac{x}{d}\right\rfloor\end{aligned}$$

At this point we have to use an inversion formula similar to the one in the proof of Lemma 9.1. This one stems from Apostol (1976), Theorem 3.11: If $F(x) = \sum_{n\le x} f(n)$, then we have

$$\sum_{n\le x}\sum_{d|n} f(d) = \sum_{n\le x} f(n)\left\lfloor\frac{x}{n}\right\rfloor = \sum_{n\le x} F\Big(\frac{x}{n}\Big).$$

We insert $\mu(n)$ for $f(n)$ and get

$$\sum_{n\le x}\mu(n)\left\lfloor\frac{x}{n}\right\rfloor = \sum_{n\le x}\sum_{d|n}\mu(d) = 1,$$

because $\sum_{d|n} \mu(d) = 0$ for all $n > 1$. Now, we can go on with the proof:

$$\begin{aligned} C(x) &= -1 + \sum_{d \le x} \mu(d) \left\lfloor \frac{x}{d} \right\rfloor^2 + 1 \\ &= x^2 \sum_{d \le x} \frac{\mu(d)}{d^2} - \sum_{d \le x} \mu(d) \left(\left(\frac{x}{d}\right)^2 - \left\lfloor \frac{x}{d} \right\rfloor^2 \right) \\ &= x^2 \sum_{d \ge 1} \frac{\mu(d)}{d^2} - x^2 \sum_{d > x} \frac{\mu(d)}{d^2} - \sum_{d \le x} \mu(d) \Big(\frac{x}{d} - \left\lfloor \frac{x}{d} \right\rfloor \Big) \Big(\frac{x}{d} + \left\lfloor \frac{x}{d} \right\rfloor \Big). \end{aligned}$$

To approximate $C(x)$ we will take a closer look at the individual sums in the last expression. We have

$$\sum_{d \ge 1} \frac{\mu(d)}{d^2} = \frac{1}{\zeta(2)} = \frac{6}{\pi^2}$$

and

$$\sum_{d > x} \frac{\mu(d)}{d^2} \le \sum_{d > x} \frac{1}{d^2} \le \int_{\lfloor x \rfloor}^{\infty} \frac{dt}{t^2} = \frac{1}{\lfloor x \rfloor}.$$

For the more complicated third sum we begin by stating the obvious:

$$0 \le \frac{x}{d} - \left\lfloor \frac{x}{d} \right\rfloor < 1 \text{ and } \left\lfloor \frac{x}{d} \right\rfloor \le \frac{x}{d}.$$

Thus, the product inside the sum can be bounded as follows:

$$\Big(\frac{x}{d} - \left\lfloor \frac{x}{d} \right\rfloor \Big) \Big(\frac{x}{d} + \left\lfloor \frac{x}{d} \right\rfloor \Big) < \frac{2x}{d}.$$

This gives the following bound for the third sum:

$$\begin{aligned} & \left| \sum_{d \le x} \mu(d) \Big(\frac{x}{d} - \left\lfloor \frac{x}{d} \right\rfloor \Big) \Big(\frac{x}{d} + \left\lfloor \frac{x}{d} \right\rfloor \Big) \right| \\ < \; & \sum_{d \le x} |\mu(d)| \frac{2x}{d} \le 2x \sum_{d \le x} \frac{1}{d} \\ \le \; & 2x \cdot \left(1 + \int_1^x \frac{dt}{t} \right) = 2x(1 + \ln x). \end{aligned}$$

This yields an approximation with corresponding error bound for $C(x)$:

$$\begin{aligned} \left| C(x) - \frac{6x^2}{\pi^2} \right| &\le \frac{x^2}{\lfloor x \rfloor} + 2x(1 + \ln x) \\ &< 4x + 2x \ln x + 1, \end{aligned}$$

as we got from the result of von zur Gathen *et al.* (2004). But now we know more insights and can mention a better bound for the frequency $\frac{C(x)}{x^2}$

$$\begin{aligned}\left|\frac{C(x)}{x^2} - \frac{6}{\pi^2}\right| &\leq \frac{1}{\lfloor x \rfloor} + 2 \cdot \frac{1 + \ln x}{x} \\ &\leq \frac{2 + 2\ln x}{x} + 1.\end{aligned}$$

and for the case that $x \in \mathbb{N}$:

$$\left|C(x) - \frac{6x^2}{\pi^2}\right| \leq 3x + 2x \ln x. \tag{9.8}$$

Note that for $C(x)$ the error term only amounts to approximately the square root of our estimated value. □

However, $C(x)$ is not exactly the number we have to look at to determine $\overline{\gamma}(\ell)$, because we have to include the 0:

$$D(x) = C(x) + 2.$$

But we want only to insert natural numbers in $D(x)$, so we can use (9.8) to find an error bound for $D(x)$:

$$\left|D(x) - \frac{6x^2}{\pi^2}\right| < 2x \ln x + 3x + 2.$$

Now, we can describe $\overline{\gamma}(\ell)$ as:

$$\overline{\gamma}(\ell) = 2^{-2\ell} \cdot \#\{0 \leq u, v < 2^\ell : \gcd(u, v) = 1\} = 2^{-2\ell} \cdot D(2^\ell - 1).$$

Unfortunately, here we have to insert $2^\ell - 1$ for inserting into the formula, because of the properties of the coprimality function. Starting with the lowest

order Fourier coefficient we obtain:

$$\begin{aligned}
\widetilde{h^{\text{int}}}(0^{2\ell}) &= \frac{1}{2^{2\ell}} \sum_{(u,v)\in\mathbb{B}^{2\ell}} (-1)^{h^{\text{int}}(u,v)+0} \\
&= \frac{1}{2^{2\ell}} \left(\sum_{\substack{(u,v)\in\mathbb{B}^{2\ell} \\ h^{\text{int}}(u,v)=0}} 1 - \sum_{\substack{(u,v)\in\mathbb{B}^{2\ell} \\ h^{\text{int}}(u,v)=1}} 1 \right) \\
&= \frac{1}{2^{2\ell}} \cdot \#\{0 \le u,v < 2^\ell : \gcd(u,v) \neq 1\} \\
&\quad -\frac{1}{2^{2\ell}} \cdot \#\{0 \le u,v < 2^\ell : \gcd(u,v) = 1\} \\
&= \frac{1}{2^{2\ell}} \cdot (2^{2\ell} - 2^{2\ell} \cdot \overline{\gamma}(\ell)) - \frac{1}{2^{2\ell}} \cdot 2^{2\ell} \cdot \overline{\gamma}(\ell) \\
&= 1 - 2\overline{\gamma}(\ell).
\end{aligned}$$

It is now easy to see that the limit of $\widetilde{h^{\text{int}}}(0^{2\ell})$ takes on the following value

$$\lim_{\ell\to\infty} \widetilde{h^{\text{int}}}(0^{2\ell}) = 1 - 2 \cdot \frac{6}{\pi^2} = -0.2158542037,$$

as we expected after conducting our experiments. The error term is only in $\mathrm{O}\left(\frac{\ln x}{\sqrt{x}}\right)$ with $x = 2^\ell$:

$$\begin{aligned}
&\left|\widetilde{h^{\text{int}}}(0^{2\ell}) - \left(1 - 2 \cdot \frac{6}{\pi^2}\right)\right| \\
&= \left|1 - 2\overline{\gamma}(\ell) - 1 + 2 \cdot \frac{6}{\pi^2}\right| = \frac{2}{2^{2\ell}} \cdot \left|\frac{6 \cdot 2^{2\ell}}{\pi^2} - D(2^\ell - 1)\right| \\
&\le \frac{2}{2^{2\ell}} \cdot \frac{6 \cdot (2^{\ell+1} - 1)}{\pi^2} + \frac{2}{2^\ell} \cdot \left|\frac{6 \cdot (2^\ell - 1)^2}{\pi^2} - D(2^\ell - 1)\right| \\
&< \frac{2}{2^{2\ell}} \cdot \frac{6 \cdot (2^{\ell+1} - 1)}{\pi^2} + \frac{2}{2^{2\ell}} \cdot \left(2 \cdot (2^\ell - 1) \cdot \ln(2^\ell - 1) + 3 \cdot (2^\ell - 1) + 2\right) \\
&< 2^{-\ell} \cdot (2\ell + 6).
\end{aligned}$$

Before we try to determine the next Fourier coefficient of note, we take a closer look at the frequency of coprime pairs (u, v) with respect to given remainders of u and v modulo 2. The set $\{0 \le u, v < 2^\ell : \gcd(u, v) = 1, u \text{ even}, v \text{ even}\}$ is obviously empty. From Knuth (1969), Chapter 4.5.2, Exercise 13, we know that the probability of two random natural *odd* numbers being relatively prime is $\frac{8}{\pi^2}$. But we want to approximate the number $\#\{0 \le u, v < 2^\ell : \gcd(u, v) = 1, u \text{ and } v \text{ odd}\}$. To do this we will take a similar approach as in the proof of Lemma 9.7:

LEMMA 9.9. *Let $\overline{C}(x)$ be the number of pairs of integers (a,b) with $1 \leq a,b \leq x$ that are coprime and a and b odd. Then we have the frequency*

$$\begin{aligned}\left|\frac{\overline{C}(x)}{x^2} - \frac{2}{\pi^2}\right| &\leq \frac{1}{4\cdot\lfloor x\rfloor} + \frac{1}{x^2}\cdot\left(\frac{9}{4}\left\lfloor\frac{x}{2}\right\rfloor + \frac{1+x+x\ln x}{2}\right)\\ &\leq \frac{1}{4} + \frac{1}{x^2}\cdot\left(\frac{13x+4x\ln x+4}{8}\right).\end{aligned}$$

PROOF. Looking for a formula for $\overline{C}(x)$ we start with the sum

$$\sum_{0\leq n<\frac{x}{2}} 2\cdot\varphi(2n+1).$$

This guarantees that at least one of the numbers in the pairs we look at is odd. Now, we have to eliminate the error we have made for each n. Subtracting $2n$ we induce another error and we have to add twice the sum

$$\sum_{\substack{1\leq i\leq n\\ \gcd(i,2n+1)\neq 1}} 1 = \frac{2n+1-\varphi(2n+1)}{2},$$

because there are of course even natural numbers that are not coprime to certain odd numbers. Finally, we have to substract 1, because we have counted the pair $(1,1)$ twice. Putting all this together we get:

$$\begin{aligned}\overline{C}(x) &= \sum_{0\leq n<\frac{x}{2}}\left(2\cdot\varphi(2n+1) - 2n + 2\cdot\frac{2n+1-\varphi(2n+1)}{2}\right) - 1\\ &= \sum_{0\leq n<\frac{x}{2}}\Big(\varphi(2n+1)+1\Big) - 1\\ &= \sum_{0\leq n<\frac{x}{2}}\varphi(2n+1) + \left\lfloor\frac{x}{2}\right\rfloor - 1.\end{aligned}$$

Now we will take a closer look at the sum in the previous expression and proceed in a way analogous to the proof of Lemma 9.7:

$$\sum_{0\leq n<\frac{x}{2}}\varphi(2n+1) = \sum_{\substack{0\leq n\leq x\\ 2\nmid n}}\varphi(n) = \sum_{\substack{d\leq x\\ 2\nmid d}}\mu(d)\sum_{\substack{q\leq\lfloor x/d\rfloor\\ 2\nmid q}} q.$$

At this point let us first assume that $\lfloor x/d \rfloor$ is even. Then we have

$$\begin{aligned}\sum_{\substack{q\le\lfloor x/d\rfloor\\ 2\nmid q}} q &= \sum_{0\le q\le\frac{1}{2}\lfloor x/d\rfloor} (2q+1)\\ &= 2\cdot\frac{1}{2}\cdot\frac{1}{2}\Big\lfloor\frac{x}{d}\Big\rfloor\cdot\Big(\frac{1}{2}\Big\lfloor\frac{x}{d}\Big\rfloor+1\Big)+\frac{1}{2}\Big\lfloor\frac{x}{d}\Big\rfloor\\ &= \frac{1}{4}\Big\lfloor\frac{x}{d}\Big\rfloor^2+\Big\lfloor\frac{x}{d}\Big\rfloor\end{aligned}$$

Inserting this into the previous sum we get

$$\frac{1}{4}\sum_{\substack{d\le x\\ 2\nmid d}}\mu(d)\Big\lfloor\frac{x}{d}\Big\rfloor^2+\sum_{\substack{d\le x\\ 2\nmid d}}\mu(d)\Big\lfloor\frac{x}{d}\Big\rfloor.$$

We have already evaluated a sum like the second one in the proof of Lemma 9.7 and found it to be 1. We have to take a closer look at the first sum. The following equation will be quite similar to the one used in the proof of Lemma 9.7, but this one is a little bit more complicated:

$$\begin{aligned}\sum_{\substack{d\le x\\ 2\nmid d}}\mu(d)\Big\lfloor\frac{x}{d}\Big\rfloor^2 &= x^2\sum_{\substack{d\le x\\ 2\nmid d}}\frac{\mu(d)}{d^2}-\sum_{\substack{d\le x\\ 2\nmid d}}\mu(d)\Big(\Big(\frac{x}{d}\Big)^2-\Big\lfloor\frac{x}{d}\Big\rfloor^2\Big)\\ &= x^2\sum_{\substack{d\ge 1\\ 2\nmid d}}\frac{\mu(d)}{d^2}-x^2\sum_{\substack{d>x\\ 2\nmid d}}\frac{\mu(d)}{d^2}-\sum_{\substack{d\le x\\ 2\nmid d}}\mu(d)\Big(\frac{x}{d}-\Big\lfloor\frac{x}{d}\Big\rfloor\Big)\Big(\frac{x}{d}+\Big\lfloor\frac{x}{d}\Big\rfloor\Big).\end{aligned}$$

First sums first:

$$\begin{aligned}\sum_{\substack{d\ge 1\\ 2\nmid d}}\frac{\mu(d)}{d^2} &= \sum_{d\ge 1}\frac{\mu(d)}{d^2}-\sum_{\substack{d\ge 1\\ 2\mid d}}\frac{\mu(d)}{d^2}\\ &= \sum_{d\ge 1}\frac{\mu(d)}{d^2}-\sum_{1\le d\le\infty}\frac{\mu(2d)}{(2d)^2}\\ &= \sum_{d\ge 1}\frac{\mu(d)}{d^2}+\frac{1}{4}\sum_{\substack{d\ge 1\\ 2\nmid d}}\frac{\mu(d)}{d^2}.\end{aligned}$$

This yields

$$\frac{3}{4}\sum_{\substack{1\le d\le\infty\\ 2\nmid d}}\frac{\mu(d)}{d^2}=\sum_{1\le d\le\infty}\frac{\mu(d)}{d^2}=\frac{6}{\pi^2},$$

and thus

$$\sum_{\substack{1\le d\le\infty\\ 2\nmid d}} \frac{\mu(d)}{d^2} = \frac{8}{\pi^2}.$$

Now, to estimate the second sum:

$$\left| x^2 \sum_{\substack{d>x\\ 2\nmid d}} \frac{\mu(d)}{d^2} \right| \le x^2 \sum_{d>x} \frac{1}{d^2} \le x^2 \int_{\lfloor x\rfloor}^{\infty} \frac{dt}{t^2} = \frac{x^2}{\lfloor x\rfloor}.$$

For the last sum we have already seen that

$$\begin{aligned} \left| \sum_{\substack{d\le x\\ 2\nmid d}} \mu(d)\Big(\frac{x}{d} - \Big\lfloor\frac{x}{d}\Big\rfloor\Big)\Big(\frac{x}{d} + \Big\lfloor\frac{x}{d}\Big\rfloor\Big) \right| &\le \sum_{d\le x} \Big(\frac{x}{d} - \Big\lfloor\frac{x}{d}\Big\rfloor\Big)\Big(\frac{x}{d} + \Big\lfloor\frac{x}{d}\Big\rfloor\Big) \\ &< 2x \sum_{d\le x} \frac{1}{d} = 2x(1+\ln x). \end{aligned}$$

Putting everything together we get:

$$\left|\overline{C}(x) - \frac{2\cdot x^2}{\pi^2}\right| \le \frac{x^2}{4\cdot\lfloor x\rfloor} + \Big\lfloor\frac{x}{2}\Big\rfloor + \frac{x + x\ln x}{2}.$$

Considering the case that $\lfloor x/d\rfloor$ is odd, we get

$$\begin{aligned} \left|\overline{C}(x) - \frac{2\cdot x^2}{\pi^2}\right| &\le \frac{x^2}{4\cdot\lfloor x\rfloor} + \frac{9}{4}\Big\lfloor\frac{x}{2}\Big\rfloor + \frac{1 + x + x\ln x}{2} \\ &< \frac{17x + 4x\ln x + 6}{8}. \end{aligned}$$

This is bigger than the error bound for the first case, so we use the first line from above to evaluate the error bound for the frequency of pairs of coprime odd natural numbers. □

This time we can add the 0 and 2^ℓ to our domain without changing the number of coprime pairs of odd numbers, because 0 and 2^ℓ are even. By inserting 2^ℓ instead of $2^\ell - 1$ in our formula we cause a slightly bigger error term, but we would replace $2^\ell - 1$ by 2^ℓ, anyway, to get a simpler expression for the error terms. Thus,

$$\begin{aligned} \overline{\gamma_1}(\ell) &= 2^{-(2\ell-2)} \cdot \#\{0 \le u, v < 2^\ell : \gcd(u,v) = 1, u \text{ and } v \text{ odd}\} \\ &= 2^{-(2\ell-2)} \cdot \overline{C}(2^\ell) \end{aligned}$$

and the error bound is

$$\begin{aligned}\left|\overline{\gamma_1}(\ell) - \frac{8}{\pi^2}\right| &= 2^{-2\ell+2}\left|\overline{C}(2^\ell) - \frac{2\cdot 2^{2\ell}}{\pi^2}\right| \\ &< 2^{-\ell+3}\cdot(\ell+2).\end{aligned}$$

Now, there are two cases left to consider. Obviously, the following frequencies are equal:

$$\begin{aligned}\overline{\gamma_2}(\ell) &= 2^{-(2\ell-2)}\cdot\#\{0\le u,v<2^\ell : \gcd(u,v)=1, u \text{ even}, v \text{ odd}\} \\ &= 2^{-(2\ell-2)}\cdot\#\{0\le u,v<2^\ell : \gcd(u,v)=1, u \text{ odd}, v \text{ even}\}.\end{aligned}$$

Also trivially, we have:

$$\begin{aligned}&\#\{0\le u,v<2^\ell : \gcd(u,v)=1\} \\ &= \#\{0\le u,v<2^\ell : \gcd(u,v)=1, u \text{ and } v \text{ odd}\} \\ &\quad +2\cdot\#\{0\le u,v<2^\ell : \gcd(u,v)=1, u \text{ even}, v \text{ odd}\}\end{aligned}$$

Thus

$$\begin{aligned}&\#\{0\le u,v<2^\ell : \gcd(u,v)=1, u \text{ even}, v \text{ odd}\} \\ &= \frac{1}{2}\cdot\Big(\#\{0\le u,v<2^\ell : \gcd(u,v)=1\} \\ &\qquad -\#\{0\le u,v<2^\ell : \gcd(u,v)=1, u \text{ and } v \text{ odd}\}\Big) \\ &= \frac{1}{2}\cdot(D(2^\ell-1)-\overline{C}(2^\ell)).\end{aligned}$$

Hence $\overline{\gamma_2} = 2^{-(2\ell-1)}\cdot(D(2^\ell-1)-\overline{C}(2^\ell)) = 2\overline{\gamma}(\ell) - \frac{1}{2}\overline{\gamma_1}(\ell)$. This yields the following approximation for $\overline{\gamma_2}(\ell)$:

$$\left|\overline{\gamma_2}(\ell) - \frac{8}{\pi^2}\right| < 2^{-\ell}\cdot(5\ell+21).$$

Now, it is easy to determine the second lowest Fourier coefficient $\widetilde{h^{\text{int}}}(10^{2\ell-1})$:

$$\begin{aligned}&\widetilde{h^{\text{int}}}(10^{2\ell-1}) \\ &= \frac{1}{2^{2\ell}}\sum_{(u,v)\in\mathbb{B}^{2\ell}}(-1)^{h^{\text{int}}(u,v)+u_0} \\ &= \frac{1}{2^{2\ell}}\Bigg(\underbrace{\sum_{\substack{(u,v)\in\mathbb{B}^{2\ell}\\ h^{\text{int}}(u,v)=0=u_0}} 1}_{S^{00}(\ell)} + \underbrace{\sum_{\substack{(u,v)\in\mathbb{B}^{2\ell}\\ h^{\text{int}}(u,v)=1=u_0}} 1}_{S^{11}(\ell)} - \underbrace{\sum_{\substack{(u,v)\in\mathbb{B}^{2\ell}\\ h^{\text{int}}(u,v)=0\neq u_0}} 1}_{S^{01}(\ell)} - \underbrace{\sum_{\substack{(u,v)\in\mathbb{B}^{2\ell}\\ h^{\text{int}}(u,v)=1\neq u_0}} 1}_{S^{10}(\ell)}\Bigg).\end{aligned}$$

To estimate the coefficient we take a closer look at the four sums:

$$\begin{aligned}
S^{00}(\ell) &= \#\{0 \le u,v < 2^\ell : \gcd(u,v) \neq 1, u \text{ even}, v \text{ arb.}\} \\
&= \#\{0 \le u,v < 2^\ell : \gcd(u,v) \neq 1, u \text{ even}, v \text{ even}\} \\
&\quad +\#\{0 \le u,v < 2^\ell : \gcd(u,v) \neq 1, u \text{ even}, v \text{ odd}\} \\
&= 2^{2\ell-1} - 2^{2\ell-2}\overline{\gamma_2}(\ell), \\
S^{11}(\ell) &= \#\{0 \le u,v < 2^\ell : \gcd(u,v) = 1, u \text{ odd}, v \text{ arb.}\} \\
&= \#\{0 \le u,v < 2^\ell : \gcd(u,v) = 1, u \text{ odd}, v \text{ odd}\} \\
&\quad +\#\{0 \le u,v < 2^\ell : \gcd(u,v) = 1, u \text{ odd}, v \text{ even}\} \\
&= 2^{2\ell-2}(\overline{\gamma_1}(\ell) + \overline{\gamma_2}(\ell)), \\
S^{01}(\ell) &= \#\{0 \le u,v < 2^\ell : \gcd(u,v) \neq 1, u \text{ odd}, v \text{ arb.}\} \\
&= \#\{0 \le u,v < 2^\ell : \gcd(u,v) \neq 1, u \text{ odd}, v \text{ odd}\} \\
&\quad +\#\{0 \le u,v < 2^\ell : \gcd(u,v) \neq 1, u \text{ odd}, v \text{ even}\} \\
&= 2^{2\ell-1} - 2^{2\ell-2}(\overline{\gamma_1}(\ell) + \overline{\gamma_2}(\ell)), \\
S^{10}(\ell) &= \#\{0 \le u,v < 2^\ell : \gcd(u,v) = 1, u \text{ even}, v \text{ arb.}\} \\
&= \#\{0 \le u,v < 2^\ell : \gcd(u,v) = 1, u \text{ even}, v \text{ even}\} \\
&\quad +\#\{0 \le u,v < 2^\ell : \gcd(u,v) = 1, u \text{ even}, v \text{ odd}\} \\
&= 2^{2\ell-2}\overline{\gamma_2}(\ell).
\end{aligned}$$

It follows that

$$\begin{aligned}
&S^{00}(\ell) + S^{11}(\ell) - S^{01}(\ell) - S^{10}(\ell) \\
&= 2^{2\ell-1} - 2^{2\ell-2}\overline{\gamma_2}(\ell) + 2^{2\ell-2}(\overline{\gamma_1}(\ell) + \overline{\gamma_2}(\ell)) \\
&\quad -2^{2\ell-1} + 2^{2\ell-2}(\overline{\gamma}1(\ell) + \overline{\gamma_2}(\ell)) - 2^{2\ell-2}\overline{\gamma_2}(\ell) \\
&= 2^{2\ell-1}\overline{\gamma_1}(\ell).
\end{aligned}$$

Therefore the limit of $\widetilde{h^{\text{int}}}(10^{2\ell-1})$ fits our experiments described in Section 8.2:

$$\lim_{\ell\to\infty} \widetilde{h^{\text{int}}}(10^{2\ell-1}) = \frac{4}{\pi^2} \approx 0.4052847346.$$

We get the following estimation of the error term:

$$\begin{aligned}
\left|\widetilde{h^{\text{int}}}(10^{2\ell-1}) - \frac{4}{\pi^2}\right| &= \left|\frac{1}{2}\cdot\overline{\gamma_1}(\ell) - \frac{4}{\pi^2}\right| \\
&= \frac{1}{2}\left|\overline{\gamma_1}(\ell) - \frac{8}{\pi^2}\right| \\
&< 2^{-\ell+2}(\ell+2).
\end{aligned}$$

For the next extreme coefficient we may proceed in much the same way to arrive at the correct estimate. Only here we have to pay attention to v_0 instead of u_0. We get:

$$\lim_{\ell\to\infty} \widetilde{h^{\text{int}}}(0^\ell 10^{\ell-1}) = \frac{4}{\pi^2} \approx 0.4052847346$$
$$\text{and} \quad \left|\widetilde{h^{\text{int}}}(0^\ell 10^{\ell-1}) - \frac{4}{\pi^2}\right| < 2^{-\ell+2}(\ell+2)$$

as above. Now, the only remaining Fourier coefficient of interest is $\widetilde{h^{\text{int}}}(10^{\ell-1}10^{\ell-1})$:

$$\begin{aligned}
&\widetilde{h^{\text{int}}}(10^{\ell-1}10^{\ell-1}) \\
&= \frac{1}{2^{2\ell}} \sum_{(u,v)\in\mathbb{B}^{2\ell}} (-1)^{h^{\text{int}}(u,v)+u_0+v_0} \\
&= \frac{1}{2^{2\ell}}\Big(\underbrace{\sum_{\substack{(u,v)\in\mathbb{B}^{2\ell} \\ h^{\text{int}}(u,v)=u_0+v_0=0}} 1}_{\overline{S}^{00}(\ell)} + \underbrace{\sum_{\substack{(u,v)\in\mathbb{B}^{2\ell} \\ h^{\text{int}}(u,v)=u_0+v_0=1}} 1}_{\overline{S}^{11}(\ell)} - \underbrace{\sum_{\substack{(u,v)\in\mathbb{B}^{2\ell} \\ h^{\text{int}}(u,v)\neq u_0+v_0=1}} 1}_{\overline{S}^{01}(\ell)} - \underbrace{\sum_{\substack{(u,v)\in\mathbb{B}^{2\ell} \\ h^{\text{int}}(u,v)\neq u_0+v_0=0}} 1}_{\overline{S}^{10}(\ell)} \Big),
\end{aligned}$$

where

$$\begin{aligned}
\overline{S}^{00}(\ell) &= \#\{0 \le u,v < 2^\ell : \gcd(u,v) \neq 1, u \text{ even}, v \text{ even}\} \\
&\quad +\#\{0 \le u,v < 2^\ell : \gcd(u,v) \neq 1, u \text{ odd}, v \text{ odd}\} \\
&= 2^{2\ell-1} - 2^{2\ell-2}\overline{\gamma_1}(\ell), \\
\overline{S}^{11}(\ell) &= \#\{0 \le u,v < 2^\ell : \gcd(u,v) = 1, u \text{ even}, v \text{ odd}\} \\
&\quad +\#\{0 \le u,v < 2^\ell : \gcd(u,v) = 1, u \text{ odd}, v \text{ even}\} \\
&= 2^{2\ell-1}\overline{\gamma_2}(\ell), \\
\overline{S}^{01}(\ell) &= \#\{0 \le u,v < 2^\ell : \gcd(u,v) \neq 1, u \text{ even}, v \text{ odd}\} \\
&\quad +\#\{0 \le u,v < 2^\ell : \gcd(u,v) \neq 1, u \text{ odd}, v \text{ even}\} \\
&= 2^{2\ell-1} - 2^{2\ell-1}\cdot\overline{\gamma_2}(\ell), \\
\overline{S}^{10}(\ell) &= \#\{0 \le u,v < 2^\ell : \gcd(u,v) = 1, u \text{ even}, v \text{ even}\} \\
&\quad +\#\{0 \le u,v < 2^\ell : \gcd(u,v) = 1, u \text{ odd}, v \text{ odd}\} \\
&= 2^{2\ell-2}\overline{\gamma_1}(\ell).
\end{aligned}$$

Evidently,

$$\begin{aligned}
&\overline{S}^{00}(\ell) + \overline{S}^{11}(\ell) - \overline{S}^{01}(\ell) - \overline{S}^{10}(\ell) \\
&= 2^{2\ell-1} - 2^{2\ell-2}\overline{\gamma_1}(\ell) + 2^{2\ell-1}\overline{\gamma_2}(\ell) - 2^{2\ell-1} + 2^{2\ell-1}\cdot\overline{\gamma_2}(\ell) - 2^{2\ell-2}\overline{\gamma_1}(\ell) \\
&= 2^{2\ell}\cdot\overline{\gamma_2}(\ell) - 2^{2\ell-1}\cdot\overline{\gamma_1}(\ell).
\end{aligned}$$

It is easy to see that

$$\frac{1}{2^{2\ell}}\Big(2^{2\ell}\cdot\overline{\gamma_2}(\ell)-2^{2\ell-1}\cdot\overline{\gamma_1}(\ell)\Big)=\overline{\gamma_2}(\ell)-\frac{1}{2}\cdot\overline{\gamma_1}(\ell)=\frac{8}{\pi^2}-\frac{4}{\pi^2}=\frac{4}{\pi^2}.$$

Therefore, the coefficient $\widetilde{h^{\mathrm{int}}}(10^{\ell-1}10^{\ell-1})$ converges on the following value:

$$\lim_{\ell\to\infty}\widetilde{h^{\mathrm{int}}}(10^{\ell-1}10^{\ell-1})=\frac{4}{\pi^2}\approx 0.4052847346.$$

In conclusion we have

$$\begin{aligned}\left|\widetilde{h^{\mathrm{int}}}(10^{\ell-1}10^{\ell-1})-\frac{4}{\pi^2}\right| &= \frac{1}{2^{2\ell}}\cdot\left|2^{2\ell}\overline{\gamma_2}(\ell)-2^{2\ell-1}\overline{\gamma_1}(\ell)-\frac{4\cdot 2^{2\ell}}{\pi^2}\right|\\ &= \left|\overline{\gamma_2}(\ell)-\frac{8}{\pi^2}+\frac{4}{\pi^2}-\frac{1}{2}\overline{\gamma_1}(\ell)\right|\\ &\le \left|\overline{\gamma_2}(\ell)-\frac{8}{\pi^2}\right|+\frac{1}{2}\left|\frac{8}{\pi^2}-\overline{\gamma_1}(\ell)\right|\\ &< 2^{-\ell}\cdot(9\ell+29)<2^{-\ell+4}(\ell+2).\end{aligned}$$

Putting everything together we obtain a result that seems to be new:

THEOREM 9.10. *The extreme Fourier coefficients of the coprimality function can be approximated as follows:*

- $\left|\widetilde{h^{\mathrm{int}}}(0^{2\ell})-\left(1-\frac{12}{\pi^2}\right)\right|<2^{-\ell}\cdot(4\ell+17)<2^{-\ell+2}(\ell+8)$,
- $\left|\widetilde{h^{\mathrm{int}}}(10^{2\ell-1})-\frac{4}{\pi^2}\right|<2^{-\ell+2}\cdot(\ell+2)$,
- $\left|\widetilde{h^{\mathrm{int}}}(0^{\ell}10^{\ell-1})-\frac{4}{\pi^2}\right|<2^{-\ell+2}\cdot(\ell+2)$ *and*
- $\left|\widetilde{h^{\mathrm{int}}}(10^{\ell-1}10^{\ell-1})-\frac{4}{\pi^2}\right|<2^{-\ell}\cdot(9\ell+29)<2^{-\ell+4}(\ell+2)$.

9.3 The Primality Function

From our experiments in Section 8.3 we assume that there are one or possibly two extreme coefficients for the primality function, namely the first and the second. Recall the function

$$\pi(x) = \#\{p \in \mathbb{N} \colon p \leq x, p \text{ prime}\}.$$

that counts the number of primes up to a bound $x \in \mathbb{R}^+$.

The following theorem normally suffers from a severe multitude of formulations of which we will mention only two taken from von zur Gathen & Gerhard (1999), Theorem 18.7:

Prime Number Theorem 9.11. *We have the approximation:*

$$\pi(x) \approx \frac{x}{\ln(x)}.$$

This means that on average about one in $\ln(x)$ of the numbers smaller or equal x is prime.

A more precise version of the prime number theorem is the following:

Precise Prime Number Theorem 9.12. *We have for $x \geq 59$:*

$$\frac{x}{\ln(x)}\Big(1 + \frac{1}{2\ln(x)}\Big) < \pi(x) < \frac{x}{\ln(x)}\Big(1 + \frac{3}{2\ln(x)}\Big).$$

The latter formulation of the prime number theorem yields immediatly:

Corollary 9.13. *For $x \geq 59$ we have the following error estimation*

$$\Big|\pi(x) - \frac{x(1+\ln(x))}{\ln^2(x)}\Big| < \frac{x}{2\ln^2(x)}.$$

Proof. We start off with Precise Prime Number Theorem 9.12:

$$\begin{aligned}
\frac{x}{\ln(x)}\Big(1 + \frac{1}{2\ln(x)}\Big) < &\quad \pi(x) &\quad < \frac{x}{\ln(x)}\Big(1 + \frac{3}{2\ln(x)}\Big) \\
\frac{x}{2\ln^2(x)} < &\quad \pi(x) - \tfrac{x}{\ln(x)} &\quad < \frac{3x}{2\ln^2(x)} \\
-\frac{x}{2\ln^2(x)} < &\quad \pi(x) - \tfrac{x(1+\ln(x))}{\ln^2(x)} &\quad < \frac{x}{2\ln^2(x)}.
\end{aligned}$$

This yields the promised bound. □

Now, we can approximate the lowest order Fourier coefficient $\widetilde{f^{\text{int}}}(0^n)$:

$$\begin{aligned}
\widetilde{f^{\text{int}}}(0^n) &= \frac{1}{2^n}\sum_{u\in\mathbb{B}^n}(-1)^{f^{\text{int}}(u)+0} \\
&= \frac{1}{2^n}\left(\sum_{\substack{u\in\mathbb{B}^n \\ f^{\text{int}}(u)=0}} 1 - \sum_{\substack{u\in\mathbb{B}^n \\ f^{\text{int}}(u)=1}} 1\right) \\
&= \frac{1}{2^n}\cdot\#\{0\le u<2^n : u \text{ not prime}\} \\
&\quad -\frac{1}{2^n}\cdot\#\{0\le u<2^n : u \text{ prime}\} \\
&= \frac{1}{2^n}\cdot(2^n-\pi(2^n)) - \frac{1}{2^n}\cdot\pi(2^n) \\
&= 1-\frac{\pi(2^n)}{2^{n-1}}.
\end{aligned}$$

As in the sections before we can insert 2^n instead of 2^n-1, because $\pi(2^n) = \pi(2^n-1)$ for all $n\ge 2$ and this way the notion is clearer. We obtain the following approximation for the lowest order Fourier coefficient, plugging in the result from Corollary 9.13:

$$\begin{aligned}
\left|\widetilde{f^{\text{int}}}(0^n) - \left(1-\frac{2^n(1+\ln 2^n)}{2^{n-1}(\ln 2^n)^2}\right)\right| &= \frac{1}{2^{n-1}}\cdot\left|\frac{2^n(1+\ln 2^n)}{(\ln 2^n)^2} - \pi(2^n)\right| \\
&< \frac{1}{2^{n-1}}\cdot\frac{2^n}{2(\ln 2^n)^2} < \frac{1}{n^2\ln^2 2} < \frac{3}{n^2}.
\end{aligned}$$

Obviously, $1-\frac{2^n(1+\ln 2^n)}{2^{n-1}(\ln 2^n)^2}$ is a good approximation for the lowest order Fourier coefficient. Just as obviously the limit of this Fourier coefficient is 1, because the limit of both fractions $\frac{2+2\ln 2^n}{(\ln 2^n)^2}$ and $\frac{3}{n^2}$ is 0. Using Parseval identity 2.21 it follows that all other Fourier coefficients, including the second lowest, must vanish asymptotically. We get the following theorem which to our knowledge is original to this work:

THEOREM 9.14. *The lowest order Fourier coefficient for the primality function converges on* 1*:*

$$\left|\widetilde{f^{\text{int}}}(0^n) - 1\right| < \frac{6}{n} + \frac{9}{n^2}.$$

This estimate is true for $n\ge 6$, because Precise Prime Number Theorem 9.12 holds for $x\ge 59$.

10 Relation to Computational Complexity

In the previous sections we have seen proofs related to various Fourier coefficients. A number of relations are known between the highest and lowest order Fourier coefficients and other complexity measures. Because of the binary nature of decision trees, Boolean circuits and formulae, most of the results assume the base field $\mathbb{F}_2$.

10.1 Used Definitions

We follow in our definitions the main source of this Diplomarbeit Allender *et al.* (2003) and Nisan & Szegedy (1994):

DEFINITION 10.1 (Sensitivity). *Let $u^{(i)}$ denote the vector obtained from u by flipping its ith coordinate for a bit vector $u \in \mathbb{B}^n$. The* sensitivity of φ at input $u \in \mathbb{F}_2^n$ *is the number*

$$\sigma_u(\varphi) = \sum_{1 \le i \le n} \left| \varphi(u) - \varphi(u^{(i)}) \right|$$

of inputs at Hamming distance 1 *from u where φ takes a different value. The* sensitivity of φ *is*

$$\sigma(\varphi) = \max_{u \in \mathbb{F}_2^n} \sigma_u(\varphi)$$

and the average sensitivity of φ *is*

$$s(\varphi) = 2^{-n} \sum_{u \in \mathbb{F}_2^n} \sigma_u(\varphi).$$

Obviously we have for all φ:

$$s(\varphi) \le \sigma(\varphi) \le n.$$

There are a number of sources showing that sensitivity provides lower bounds for the CREW PRAM complexity of Boolean functions. We mention Nisan (1989), Dietzfelbinger *et al.* (1996), Fich (1990), Parberry & Yan (1991) and Wegener (1987), but this selection is actually due to Allender *et al.* (2003).

DEFINITION 10.2 (Decision tree). *A binary* decision tree T *is a binary tree with inner nodes labeled* $U_1, \ldots, U_n$ *and leaves labeled* 0 *and* 1. *The edges of a each node are labeled* 0 *and* 1. *Every input assignment* $u \in \mathbb{B}^n$ *to the variables in the tree determines a computation path from the root to one of the leaves: at each visited inner node that is labeled by variable* U_i *the path follows the edge labeled* $u_i \in \{0, 1\}$. *The tree computes the function that maps every assignment to the label of the leaf reached by its computation path.*

DEFINITION 10.3 (Size and depth of a decision tree). *For an input assignment* u, *let* $D_u(T)$ *be the length of its computation path in* T. Depth *and* average depth *of the tree are defined by*

$$\begin{aligned} D(T) &= \max\{D_u(T) \colon u \in \mathbb{B}^n\}, \\ \overline{D}(T) &= 2^{-n} \sum_{u \in \mathbb{B}^n} D_u(T) \end{aligned}$$

and the number of leaves is called the size *of the decision tree. For a Boolean function* φ, *let* $M(\varphi)$, $D(\varphi)$, *and* $\overline{D}(\varphi)$ *denote the* minimal size, *the* minimal depth *and the* minimal average depth, *respectively, of the decision trees that compute* φ.

Note that in a binary tree the number of leaves is always greater by one than the number of inner nodes. Evidently $\overline{D}(\varphi) \leq D(\varphi) \leq n$ and $\overline{D}(\varphi) \geq \log M(\varphi)$ for all φ.

Boolean circuits are another computational model that we will need for the next two definitions:

DEFINITION 10.4 (Boolean circuits). *A* Boolean circuit C *with* n *variables is a directed acyclic graph with Boolean inputs* $0, 1, x_1, \ldots, x_n$ *and some number of output gates* $y_1, \ldots, y_r$. *The gates of* C *(except for the input gates) are labeled* $\neg$, $\wedge$, *or* $\vee$ *and have the corresponding in-degree. Their number is the size* $s(C)$ *of* C. *The depth* $d(C)$ *is the length of a longest path from an input to an output in* C. *The circuit computes a Boolean function from* $\mathbb{B}^n$ *to* $\mathbb{B}^r$ *in the natural way.*

In order to discuss the (non-uniform) circuit complexity of Boolean functions, it is necessary to consider families of circuits.

DEFINITION 10.5 (Family of Boolean circuits). *A* family of circuits $(C_n)_{n \in \mathbb{N}}$, *where* C_n *has* n *variables, computes the Boolean function* φ, *if for all* $n \in \mathbb{N}$ C_n *outputs* $\varphi(u)$ *for all* $u \in \mathbb{B}^n$. *A circuit family has size and depth bounded by* $s(n)$ *and* $d(n)$, *if* $s(C_n) \leq s(n)$ *and* $d(C_n) \leq d(n)$.

We will also consider the size of logical formulae representing a given Boolean function.

DEFINITION 10.6 (Formulae). Formulae *are defined in the following recursive way:* 0, 1, *the variables* $x_1, \ldots, x_n$ *and their negations* $\neg x_1, \ldots, \neg x_n$ *are formulae; if* F_1 *and* F_2 *are formulae, then so are* $F_1 \wedge F_2$ *and* $F_1 \vee F_2$. *The size of a formula is the number of occurrences of variables in it. Formulae are equivalent to Boolean circuits where the fan-out of each gate is bounded by one. Let* $L(\varphi)$ *denote the minimal size of formulae that compute* φ.

Finally we will look at a multilinear real polynomial that coincides with a given Boolean function for all inputs in $\mathbb{B}^n$ and consider the degree of this polynomial as a measure of the complexity of the function:

DEFINITION 10.7 (Real degree). *For a Boolean function* $\varphi : \mathbb{B}^n \to \{0, 1\}$, *let the* real degree $\Delta(\varphi)$ *of* φ *be the degree of the unique multilinear real polynomial* $P \in \mathbb{R}[U_1, \ldots, U_n]$ *for which* $\varphi(u) = P(u)$ *holds for every* $u \in \mathbb{B}^n$. *(Multilinearity means that each variable appears with degree at most 1.)*

10.2 Known Results

Now that we have recalled the definitions of the relevant complexity measures, we will state without proof some known relations between these measures:

THEOREM 10.8 (Allender *et al.* 2003). *For any Boolean function* $\varphi\colon \mathbb{B}^n \to \mathbb{B}$ *we have a lower bound on the circuit size:*

$$s(\varphi) \geq |\widetilde{\varphi}(1^n)| \cdot n.$$

□

THEOREM 10.9 (Jukna *et al.* 1999). *Let* φ *be an* n*-variate Boolean function and* $w \in \mathbb{B}^n$ *then we have a lower bound on the minimal decision tree size*

$$M(\varphi) \geq 2^{|w|} \sum_{u \geq w} \left|\widetilde{\varphi}(u)\right|,$$

where the sum is taken over all u *such that* $u_i \geq w_i$ *for all* i. □

This combines results from Linial *et al.* (1993) and Kushilevitz & Mansour (1991).

THEOREM 10.10 (Allender *et al.* 2003). *For an n-variate Boolean function φ with the highest order Fourier coefficient $\widetilde{\varphi}(1^n) \neq 0$ the minimal depth of a decision tree and real degree are given by*

$$D(\varphi) = \Delta(\varphi) = n.$$

□

THEOREM 10.11 (Allender *et al.* 2003). *For an n-variate Boolean function φ and an n-variate real multilinear polynomial P of degree $d < n$ we have*

$$\max_{u \in \mathbb{B}^n} \left| \varphi(u) - P(u) \right| \geq \frac{|\widetilde{\varphi}|}{2}.$$

□

THEOREM 10.12 (Bernasconi *et al.* 1999, 2000). *Let φ be a Boolean function depending on n variables. Then we have a lower bound on the minimal formula size:*

$$L(\varphi) \geq \frac{s(\varphi)^2}{1 - \widetilde{\varphi}(0^n)^2}.$$

□

More and similar results can be found e.g. in Bernasconi *et al.* (1997), Kahn *et al.* (1988) and Mansour (1994).

10.3 Polynomials over $\mathbb{F}_2[x]$

First we recall the results of Section 5: For the squarefreeness function g we have Lemma 5.6 and Lemma 5.16:

- $\left| d^{11} + \frac{4}{9} \right| \leq 2^{-n/2}$,
- $\left| d^{01} + \frac{4}{9} \right| \leq 2^{-n/2}$,
- $\left| d^{10} - \frac{4}{9} \right| \leq 2^{-n/2}$,
- $\left| d^{00} + \frac{1}{3} \right| \leq 2^{-n/2}$.

For the coprimality function h we got similar results in Lemma 5.17 and Lemma 5.21:

- $\left|d^{11} - \frac{4}{9}\right| \leq 2^{-\ell}$,
- $\left|d^{10} + \frac{4}{9}\right| \leq 2^{-\ell}$,
- $\left|d^{01} + \frac{4}{9}\right| \leq 2^{-\ell}$,
- $\left|d^{00} + \frac{1}{3}\right| \leq 2^{-\ell}$.

The irreducibility function f behaves differently and we have learned in Section 7.3 that

$$\lim_{n\to\infty} \widetilde{f}(0^n) = 1.$$

We have proved that $\left|\widetilde{f}(0^n) - 1\right| \leq \frac{6}{n}$. This seems a comparetively crude estimation, surely there should be a better one. Using the Parseval identity 2.21 to simplify matters for the limits of the largest coefficients we see that for the squarefreeness and the coprimality function there may be further coefficients other than the four extreme coefficients that do not converge on 0, because in both cases the squares of the four coefficients add up only to $1 - \frac{8}{27}$ in the limit. Our experiments indicate that there are in fact more coefficients that do not vanish. As noted in Section 7.3 the result for the irreducibility function is different: since the lowest order Fourier coefficient of this function converges on 1 all other coefficients for the irreducibility function must vanish asymptotically, including the highest order Fourier coefficient.

Using Theorem 10.8 we get the following bounds for the sensitivity of squarefreeness and coprimality.

COROLLARY 10.13. *For the squarefreeness function g and the coprimality function h we have*

- $s(g) \geq \frac{4}{9} \cdot n + \mathrm{O}(n2^{-n/2})$,
- $s(h) \geq \frac{4}{9} \cdot n + \mathrm{O}(n2^{-n/2})$.

For the irreducibility function we do not have such an exact value for the highest order Fourier coefficient, but for n to infinity the lower bound becomes 0 which is in fact a very unuseful lower bound.

From Theorem 10.9 we obtain bounds for the minimal size of binary trees deciding squarefreeness and coprimality. Once again the result reflect the connectivity of squarefreeness and coprimality.

COROLLARY 10.14. *For the squarefreeness function g and the coprimality function h we have*

- $M(g) \geq \frac{4}{9} \cdot 2^n + \mathrm{O}(2^{n/2})$,
- $M(h) \geq \frac{4}{9} \cdot 2^n + \mathrm{O}(2^{n/2})$.

For the same reasons given with respect to Corollary 10.13 once again we cannot give a similar result for the irreducibility function. We obtained these two bounds by inserting $w = 1^n$ in Theorem 10.9. Since $\overline{D}(\varphi) \geq \log M(\varphi)$ we get another lemma for the squarefreeness and coprimality function:

COROLLARY 10.15.

- $\overline{D}(g) \geq n + 2 - \log_2 9 + \mathrm{o}(1)$,
- $\overline{D}(h) \geq n + 2 - \log_2 9 + \mathrm{o}(1)$.

We do not apply Theorem 10.10 because this would be quite boring. Using Theorem 10.11 we get:

COROLLARY 10.16. *For the squarefreeness function g and the coprimality function h we have*

- $\max_{u \in \mathbb{B}^n} \left| g(u) - P(u) \right| \geq \frac{\widetilde{g}(1^n)}{2} = \frac{2}{9} + \mathrm{O}(2^{-n/2})$,
- $\max_{u \in \mathbb{B}^n} \left| h(u) - P(u) \right| \geq \frac{\widetilde{h}(1^n)}{2} = \frac{2}{9} + \mathrm{O}(2^{-n/2})$.

Again we cannot apply the lemma to the irreducibility function, because the relevant Fourier coefficient once more is that of highest order. For Theorem 10.12 we need the sensitivity of our Boolean functions. Until now we only know Theorem 10.8. However, Allender *et al.* (2003) give an approximation for the sensitivity of the squarefreeness and the coprimality function:

- $s(g) = 2\gamma n + \mathrm{O}(n 2^{-n/4})$,
- $s(h) = 2\gamma n + \mathrm{O}(n 2^{-n/4})$,

where in both cases $\gamma = \frac{2}{3} - 2 \prod_{w \in I} \left(1 - \frac{2}{2^{2 \deg w}}\right) \approx 0.27358$ and I is the set of all irreducible polynomials $w \in \mathbb{F}_2[x]$. For the next lemma we insert the average sensitivities and the lowest order Fourier coefficients in Theorem 10.12 and use the fact that $\frac{1}{1-x} \geq 1 + x$ holds for $x < 1$:

COROLLARY 10.17. *For the squarefreeness function g and the coprimality function h we have lower bounds on the minimal size of formulae that compute g or h:*

- $L(g) \geq \frac{40}{9}\gamma^2 n^2 + \mathrm{O}(n^2 2^{-n/4})$,
- $L(h) \geq \frac{40}{9}\gamma^2 n^2 + \mathrm{O}(n^2 2^{-n/4})$.

Disregarding the error terms of the sensitivities of the squarefreeness and coprimality function, we get a leading constant factor of $\frac{9}{2}$.

Corollary 10.14 was already given in Allender *et al.* (2003) but there the leading fraction for both lower bounds has the value $\frac{1}{3}$, but in that work they could have already given our bound. The same holds true for Corollary 10.15, where the inferior lower bound is caused by the less than optimal $\frac{1}{3}$ from above. Also Corollary 10.17 was mentioned in Allender *et al.* (2003), however with an unproven error bound of $\mathrm{O}(n2^{-n/4})$.

Unsurprisingly we have seen that the squarefreeness and the coprimality function behave very similarly. The relation between these two problems was pointed out in Section 5.4. Unfortunately, our results for the irreducibility function are plausible but weak.

10.4 Natural Numbers

Once again, we recall previous results, this time from Section 9: For the squarefreeness function g^{int} we have Theorem 9.6:

- $\left|\widetilde{g^{\mathrm{int}}}(0^n) - \left(1 - \frac{12}{\pi^2}\right)\right| < 2^{-n/2+3}$,
- $\left|\widetilde{g^{\mathrm{int}}}(10^{n-1}) - \frac{4}{\pi^2}\right| < 2^{-n/2+4} \cdot (n+3)$,
- $\left|\widetilde{g^{\mathrm{int}}}(010^{n-2}) - \frac{4}{\pi^2}\right| \leq 12 \cdot 2^{-n/2}$ and
- $\left|\widetilde{g^{\mathrm{int}}}(1^2 0^{n-2}) - \frac{4}{\pi^2}\right| < 2^{-n/2+5} \cdot (n+1)$.

For the coprimality function h^{int} we got similar results in Theorem 9.10:

- $\left|\widetilde{h^{\mathrm{int}}}(0^{2\ell}) - \left(1 - \frac{12}{\pi^2}\right)\right| < 2^{-\ell+1} \cdot (4\ell + 17)$,
- $\left|\widetilde{h^{\mathrm{int}}}(10^{2\ell-1}) - \frac{4}{\pi^2}\right| < 2^{-\ell+2} \cdot (\ell + 2)$,

- $\left|\widetilde{h^{\text{int}}}(0^\ell 10^{\ell-1}) - \frac{4}{\pi^2}\right| < 2^{-\ell+2} \cdot (\ell+2)$ and
- $\left|\widetilde{h^{\text{int}}}(10^{\ell-1}10^{\ell-1}) - \frac{4}{\pi^2}\right| < 2^{-\ell} \cdot (9\ell+29)$.

For the irreducibility function f^{int} we have in Section 7.3

$$\left|\widetilde{f^{\text{int}}}(0^n) - 1\right| < \frac{6}{n} + \frac{9}{n^2}$$

and therefore the limit is

$$\lim_{n\to\infty} \widetilde{f^{\text{int}}}(0^n) = 1.$$

Again using Parseval identity 2.21 for the limits of the mentioned coefficients we see that for the squarefreeness and the coprimality function there have to be more coefficients than the calculated four extreme coefficients that do not converge on 0, because in both cases there is a difference of about 0.4606398145 to get 1 when you summarize the squares of those four coefficients. As for the polynomials over $\mathbb{F}_2$ the result for the irreducibility function is different and because of the tendency of the lowest order Fourier coefficient of this function all other coefficients for the irreducibility function have to converge on 0, especially the highest order Fourier coefficient, see Section 9.3.

We cannot use Theorem 10.8, because we do not know enough about the highest order coefficient for the squarefreeness and the coprimality function. Again we have no exact value for the irreducibility function, but we know that for n to infinity the lower bound becomes 0. Also Theorem 10.9, Theorem 10.10 and Theorem 10.11 cannot be used for the squarefreeness and coprimality function because of the missing value for the highest order Fourier coefficient. For the irreducibility function we can in all three cases make a statement for n to infinity: Insertion of $w = 1^n$ in Theorem 10.9 implies

$$M(\varphi) \geq 2^n.$$

It is no surprise that we cannot apply Theorem 10.10, because the limit of $\widetilde{f}(1^n)$ is 0 and inserting this in Theorem 10.11, we get:

$$\max_{u\in\mathbb{B}^n} \left|f^{\text{int}}(u) - P(u)\right| \geq \left|\frac{\widetilde{f^{\text{int}}}(1^n)}{2}\right| = 0$$

This does not yield any new insights for the irreducibility function. In order to apply Theorem 10.12 we need the sensitivity of our Boolean functions. We

were unable to find concrete values for the average sensitivity concerning our approach and combining with Theorem 10.8 gives an unsatisfactory result:

$$L(\varphi) \geq \frac{s(\varphi)^2}{1-\widetilde{\varphi}(0^n)^2} \geq \frac{(|\widetilde{\varphi}(1^n)| \cdot n)^2}{1-\widetilde{\varphi}(0^n)^2}.$$

However, Bernasconi *et al.* (2000) prove this for the squarefreeness function:

$$L(g^{\text{int}}) \geq \frac{\pi^4\gamma^2}{8(\pi^2-8)}n^2 + o(n^2).$$

This result is developed by looking only at odd natural numbers. This time there is no upper bound to get here for the minimal size of formulae that compute the irreducibility function.

Also for the integers the squarefreeness and the coprimality function behave very similarly. The relation between these two problems is not as clear as for the polynomials. A possible lead to the relationship of squarefreeness and coprimality is the Legendre or the Jacobi symbol referring to squares modulo primes and arbitrary numbers, respectively, computable by an adapted Euclidean algorithm. The following definitions are from von zur Gathen & Gerhard (1999), Chapter 18.5:

Definition 10.18 (Legendre symbol). *The* Legendre symbol *is defined for a, $N \in \mathbb{Z}$ with N prime as*

$$\left(\frac{a}{N}\right) = \begin{cases} 1, & \text{if } \gcd(a,N) = 1 \text{ and } a \text{ is a square modulo } N, \\ -1, & \text{if } \gcd(a,N) = 1 \text{ and } a \text{ is not a square modulo } N, \\ 0, & \text{if } \gcd(a,N) \neq 1. \end{cases}$$

The Jacobi symbol is the generalization to an arbitrary N:

Definition 10.19 (Jacobi symbol). *If $N = p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}$ then the* Jacobi symbol *is defined as*

$$\left(\frac{a}{N}\right) = \left(\frac{a}{p_1}\right)^{e_1} \cdot \ldots \cdot \left(\frac{a}{p_r}\right)^{e_r}.$$

The algorithms to compute the Jacobi symbol due to Eisenstein (1844) and Lebesgue (1847) are analyzed in Shallit (1990), efficient methods are given in Bach & Shallit (1996), Chapter 5.9. But we have not found an actual reduction between our two problems.

Once again, the results for the irreducibility function are plausible but weak.

10.5 Polynomials over $\mathbb{F}_q[x]$

Unfortunately, up to now we have only found values for the lowest order Fourier coefficient (see Section 7). For the squarefreeness function we have from Theorem 7.3:

$$\widetilde{g}(0^n) = \frac{2}{q+1} - 1 - 2 \cdot \frac{q^{n \text{ rem } 2}}{q^n(q+1)}.$$

For the coprimality function we got a similar result in Theorem 7.3:

$$\widetilde{h}(0^n) = 1 - \frac{2q}{q+1} - \frac{2}{q^{2\ell} \cdot (q+1)}.$$

Again, the result for the irreducibility function is somewhat different (see Section 7.3):

$$\begin{aligned} \lim_{n\to\infty} \widetilde{f}(0^n) &= 1, \\ \lim_{n\to\infty} |\widetilde{f}(0^n)| &= 1, \end{aligned}$$

and

$$\left|\widetilde{f}(0^n) - 1\right| \leq \frac{6}{n}.$$

The Parseval identity 2.21 yields the following results for the limits of the lowest order Fourier coefficients that

- for the squarefreeness function g and for the coprimality function h over a finite field $\mathbb{F}_q[x]$ there is a total of $\frac{4q}{(q+1)^2}$ left for the sum of the squares of the Fourier coefficients apart from the lowest order one,

- for the irreducibility function the lowest order Fourier coefficient converges on 1, this means that asymptotically there is nothing left for the other coefficients. They all converge on 0, in particular the highest order one.

This time we cannot apply any of the results from Section 10.2 to our results because of the problems with the definitions of the other complexity measures and because we have again too little knowledge about the highest order Fourier coefficient. There are a lot of open questions:

10.6 Open Questions and Future Work

10.6.1 Natural numbers

For the natural numbers it would be interesting to know whether there is an effective reduction from squarefreeness to coprimality. Also the highest order Fourier coefficient and the others that do not converge on 0 should be considered. Furthermore, one might try to determine the sensitivity of our three functions for positive integers for our model. Alternatively one could try and do a Fourier transformation for odd natural numbers only.

10.6.2 Polynomials

For the polynomials we have to extend the definitions of the other complexity measures to the case of $\mathbb{F}_q$ instead of $\mathbb{F}_2$. This would be quite simple, for example, for a decision tree. Following the generalization one could look whether the results from the binary field can be generalized as well. Furthermore, there are a lot of Fourier coefficients to estimate. In the plots and calculations in Section 6 we have already gotten good ideas about the structure they have.

References

Manindra Agrawal, Neeraj Kayal & Nitin Saxena (2002). PRIMES is in P. URL `http://www.cse.iitk.ac.in/users/manindra/primality.ps`. Preprint.

Jean Le Rond d'Alembert (1747). Recherches sur la courbe que forme une corde tendue mise en vibrations. *Mémoires de l'Académie des Sciences et Belles-Lettres de Berlin* **3**, 214–219.

Eric Allender, Anna Bernasconi, Carsten Damm, Joachim von zur Gathen, Michael Saks & Igor Shparlinski (2003). Complexity of some arithmetic problems for binary polynomials. *computational complexity* **12**(1/2), 23–47. URL `http://www-math.upb.de/~aggathen/Publications/allber03.pdf`.

T. M. Apostol (1976). *Introduction to Analytic Number Theory.* Springer-Verlag, New York.

Eric Bach & Jeffrey Shallit (1996). *Algorithmic Number Theory, Vol.1: Efficient Algorithms.* MIT Press, Cambridge MA.

Elwin R. Berlekamp (1968). *Algebraic Coding Theory.* McGraw-Hill, New York.

A. Bernasconi, B. Codenotti & J. Simon (1997). On the Fourier analysis of Boolean functions. Technical Report IMC 134-97-03, Institute for Computational Mathematics, Pisa.

A. Bernasconi, C. Damm & I. Shparlinski (1999). On the average sensitivity of testing squarefree numbers. In *Proceedings of the 5th International Computing and Combinatorics Conference,* Tokyo Japan, number 1627 in Lecture Notes in Computer Science, 291–299. Springer-Verlag, Berlin.

A. Bernasconi, C. Damm & I. E. Shparlinski (2000). The average sensitivity of square-freeness. *computational complexity* **9**, 39–51.

Salomon Bochner & John von Neumann (1935). Almost periodic functions in groups, II. *Transactions of the American Mathematical Society* **37**, 21–50.

Olaf Bonorden, Joachim von zur Gathen, Jürgen Gerhard, Olaf Müller & Michael Nöcker (2001). Factoring a binary polynomial of degree over one million. *ACM SIGSAM Bulletin* **35**(1), 16–18. URL `http://www-math.upb.de/~aggathen/Publications/bongat01.pdf`.

Lis Brack-Bernsen & Matthias Brack (2004). Analyzing shell structure from Babylonian and modern times. *International Journal of Modern Physics E* **13**(1), 247–260.

W. A. Coppel (1969). J. B. Fourier - On the occasion of his two hundredth birthday. *The American Mathematical Monthly* **76**, 468–483.

Martin Dietzfelbinger, Mirosław Kutylowski & Rüdiger Reischuk (1996). Feasible time-optimal algorithms for Boolean functions on exclusive-write parallel random-access machines. *SIAM Journal on Computing* **25**, 1196–1230.

G. Lejeune Dirichlet (1829). Sur la convergence des séries trigonométriques qui servent à représenter une fonction arbitraire entre des limites données. *Journal für die reine und angewandte Mathematik* **4**, 157–169.

H. Dym & H. P. McKean (1972). *Fourier series and integrals.* Academic Press, New York and London.

G. Eisenstein (1844). Einfacher Algorithmus zur Bestimmung des Werthes von $\left(\frac{a}{b}\right)$. *Journal für die reine und angewandte Mathematik* **27**(4), 317–318.

Leonhard Euler (1748). Sur la vibration des cordes. *Mémoires de l'Académie des Sciences et Belles-Lettres de Berlin* **4**, 69–85.

Leonhard Euler (1798). Disquisitio ulterior super seriebus secundum multipla cuiusdam anguli progredientibus. *Nova Acta Academiae Scientiarum Imperalis Petropolitanae* **11**(1793), 114–132. Eneström 704. *Opera Omnia*, series 1, volume 16, 333-355.

F. E. Fich (1990). The complexity of computation on the parallel random access machine. In *Handbook of Theoretical Comp. Sci.*, 757–804. Elsevier, Amsterdam.

Ernst Fischer (1907a). Applications d'un théoréme sur la convergence en moyenne. *Comptes Rendus des Séances de l'Académie des Sciences* **144**, 1148–1151.

Ernst Fischer (1907b). Sur la convergence en moyenne. *Comptes Rendus des Séances de l'Académie des Sciences* **144**, 1022–1024.

P. Flajolet, X. Gourdon & D. Panario (2001). The Complete Analysis of a Polynomial Factorization Algorithm over Finite Fields. *Journal of Algorithms* **40**(1), 37–81. Extended Abstract in *Proceedings of the 23rd International Colloquium on Automata, Languages and Programming ICALP 1996*, Paderborn, Germany, ed. F. Meyer auf der Heide and B. Monien, Lecture Notes in Computer Science **1099**, Springer-Verlag, 1996, 232–243.

J. B. J. Fourier (1808). Mémoire sur la propagation de la Chaleur dans les corps solides (abstract). *Nouveau Bulletin des sciences par la Société philomathique de Paris* **1**, 112–116.

J. B. J. Fourier (1822). *Théorie Analytique de la Chaleur*. Firmin Didot, Paris.

J. B. J. Fourier (1824). Théorie du mouvement de la chaleur dans les corps solides (1). *Mémoires de l'Académie des Sciences de l'Institut de France* **4**(1819-1820), 185–555.

J. B. J. Fourier (1826). Théorie du mouvement de la chaleur dans les corps solides (2). *Mémoires de l'Académie des Sciences de l'Institut de France* **5**, 153–246.

Joachim von zur Gathen & Jürgen Gerhard (1999). *Modern Computer Algebra*. Cambridge University Press, Cambridge, UK, 1st edition. ISBN 0-521-64176-4. URL `http://www-math.upb.de/~aggathen/mca/`. Second edition 2003.

Joachim von zur Gathen, Arnold Knopfmacher, Florian Luca, Lutz G. Lucht & Igor E. Shparlinski (2004). Average order in cyclic groups. *Bordeaux Journal of Number Theory* **16**, 107–123. URL `http://www-math.upb.de/~aggathen/Publications/gatkno03.pdf`.

Carl Friedrich Gauss (1801). *Disquisitiones Arithmeticae*. Gerh. Fleischer Iun., Leipzig. English translation by Arthur A. Clarke, Springer-Verlag, New York, 1986.

I. Grattan-Guinness (1969). Joseph Fourier and the Revolution in Mathematical Physics. *Mathematics and Its Applications* **5**, 230–253.

I. Grattan-Guinness (1972). *Joseph Fourier 1768-1830*. MIT Press. ISBN 0-262-07041-3. In collaboration with J.R. Ravetz.

G. H. Hardy & E. M. Wright (1985). *An introduction to the theory of numbers*. Clarendon Press, Oxford, 5th edition. First edition 1938.

H. Heuser (1995a). *Gewöhnliche Differentialgleichungen*. Mathematische Leitfäden. B. G. Teubner, Stuttgart. ISBN 3-519-22227-2.

H. Heuser (1995b). *Lehrbuch der Analysis 2*. Mathematische Leitfäden. B. G. Teubner, Stuttgart. ISBN 3-519-32232-3.

E. W. Hobson (1926). *The theory of functions of a real variable and the theory of Fourier's series*, volume 2. Cambridge University Press. First edition (in one volume) 1907, Reprint (Dover Publications).

S. Jukna, A. Razborov, P. Savicky & I. Wegener (1999). On P versus NP ∩ co-NP for decision trees and read-once branching programs. *computational complexity* **8**, 357–370.

Jeff Kahn, Gil Kalai & Nathan Linial (1988). The Influence of Variables on Boolean Functions. *Proceedings of the 29th Annual IEEE Symposium on Foundations of Computer Science,* White Plains NY (29), 68–80. Extended abstract.

Donald E. Knuth (1969). *The Art of Computer Programming, vol.2, Seminumerical Algorithms*. Addison-Wesley, Reading MA.

E. Kushilevitz & Y. Mansour (1991). Learning Decision Trees using the Fourier Spectrum. In *Proceedings of the Twenty-third Annual ACM Symposium on the Theory of Computing,* New Orleans LA, 455–464. ACM Press.

Henri Lebesgue (1901). Sur une généralisation de l'intégrale définie. *Comptes Rendus des Séances de l'Académie des Sciences* **132**, 1025–1028.

Henri Lebesgue (1902). Intégrale, Longueur, Aire. *Annali di Matematica pura ed applicata* **7**, 231–359.

Henri Lebesgue (1903). Sur l'existence des dérivées. *Comptes Rendus des Séances de l'Académie des Sciences* **136**, 659–661.

Henri Lebesgue (1904). *Leçons sur l'intégration et la recherche des fonctions primitives*. Gauthier-Villars, Paris.

Henri Lebesgue (1906). *Leçons sur le séries trigonométriques*. Gauthier-Villars, Paris.

V.-A. Lebesgue (1847). Sur le symbole $\left(\frac{a}{b}\right)$ et quelques-unes de ses applications. *Journal de Mathématiques Pures et Appliquées* **12**, 497–517.

Rudolf Lidl & Harald Niederreiter (1983). *Finite Fields*. Number 20 in Encyclopedia of Mathematics and its Applications. Addison-Wesley, Reading MA.

N. Linial, Y. Mansour & N. Nisan (1993). Constant Depth Circuits, Fourier Transforms, and Learnability. *Journal of the ACM* **40**, 607–620.

Keju Ma & Joachim von zur Gathen (1990). Analysis of Euclidean Algorithms for Polynomials over Finite Fields. *Journal of Symbolic Computation* **9**, 429–455.

Y. Mansour (1994). Learning Boolean Functions via the Fourier Transform. *Theoretical advances in neural computation and learning* 391–424.

G. L. Miller (1975). Riemann's Hypothesis and Tests for Primality. In *Proceedings of the Seventh Annual ACM Symposium on the Theory of Computing,* Albuquerque NM, 234–239. ACM Press.

O. Neugebauer (1975). *A History of Ancient Mathematical Astronomy*, volume 1-3. Springer-Verlag Berlin Heidelberg New York 1975. ISBN 3-540-06995-X.

John von Neumann (1934). Almost periodic functions in a group, I. *Transactions of the American Mathematical Society* **36**, 445–492.

Noam Nisan (1989). CREW PRAMs and Decision Trees. In *Proceedings of the Twenty-first Annual ACM Symposium on the Theory of Computing,* Seattle WA, 327–335. ACM Press.

N. Nisan & M. Szegedy (1994). On the degree of Boolean functions as real polynomials. *computational complexity* **4**, 301–313.

Ian Parberry & Pei Yuan Yan (1991). Improved upper and lower time bounds for parallel random access machines without simultaneous writes. *SIAM Journal on Computing* **20**(1), 88–99.

Marc-Antoine Parseval (1806a). Intégration générale et complète des équations de la propagation du son, l'air étant considéré avec ses trois dimensions. *Mémoires présentés à l'Institut des Sciences, Lettres et Arts, par divers savans, et lus dans ses assemblées* **1**, 379–398. Dated 05 July 1801.

Marc-Antoine Parseval (1806b). Mémoire sur les séries et sur l'intégration complète d'une équation aux différences partielles linéaires du second ordre, à coefficiens constans. *Mémoires présentés à l'Institut des Sciences, Lettres et Arts, par divers savans, et lus dans ses assemblées* **1**, 638–648. Dated 5 Apr. 1799.

Michel Plancherel (1910). Contribution à l'étude de la represéntation d'une fonction arbitraire par des intégrales définies. *Rendiconti del Circolo Matematico di Palermo* **30**, 289–335.

Karl Prachar (1961). Über die kleinste quadratfreie Zahl einer arithmetischen Reihe. *Journal für die reine und angewandte Mathematik* **206**(3-4), 173–176.

Michael O. Rabin (1980). Probabilistic Algorithms for Testing Primality. *Journal of Number Theory* **12**, 128–138.

Bernhard Riemann (1867). Ueber die Darstellbarkeit einer Function durch eine trigonometrische Reihe. *Abhandlungen der Königlichen Gesellschaft der Wissenschaften zu Göttingen Gesammelte Mathematische Werke und wissenschaftlicher Nachlass*, ed. Heinrich Weber, Teubner Verlag, Leipzig, 1892, 227-271.

Frigyes Riesz (1907a). Sur les systèmes orthogonaux de fonctions. *Comptes Rendus des Séances de l'Académie des Sciences* **144**, 615–619.

Frigyes Riesz (1907b). Sur les systèmes orthogonaux de fonctions et l'équation de Fredholm. *Comptes Rendus des Séances de l'Académie des Sciences* **144**, 734–736.

Jeffrey Shallit (1990). On the Worst Case of Three Algorithms for Computing the Jacobi Symbol. *Journal of Symbolic Computation* **10**, 593–610.

Michael Sipser (1992). The history and status of the P versus NP question. *Proceedings of the Twenty-fourth Annual ACM Symposium on the Theory of Computing,* Victoria, British Columbia, Canada 603–618.

Ingo Wegener (1987). *The Complexity of Boolean Functions.* Wiley-Teubner Series in Computer Science. B. G. Teubner, Stuttgart, and John Wiley & Sons.

Erklärung

Ich versichere, dass ich die Arbeit ohne fremde Hilfe und ohne Benutzung anderer als der angegebenen Quellen angefertigt habe und dass die Arbeit in gleicher oder ähnlicher Form noch keiner anderen Prüfungsbehörde vorgelegen hat und von dieser als Teil einer Prüfungsleistung angenommen wurde. Alle Ausführungen, die wörtlich oder sinngemäß übernommen wurden, sind als solche gekennzeichnet.

Bad Lippspringe, den 28.01.2005