BACHELOR

The multiplicative complexity of symmetric functions over a field with characteristic p

van Heesch, M.P.P.

Award date:
2014

The multiplicative complexity of symmetric functions over a field with characteristic p

Maran van Heesch (0762684)

Supervisor;
Dr.ir. L.A.M. (Berry) Schoenmakers

July 3, 2014

Abstract

In this thesis we consider the boolean elementary symmetric functions over a field with characteristic p, with p an odd, large enough prime. We will determine the coefficients of the symmetric functions. Also we will prove that it is possible to determine the coefficients with a recurrence relation of which the order depends on the number of variables of the degree of the smallest monomial in the symmetric polynomial.
The multiplicative complexity of the symmetric polynomials is the number of multiplications needed to construct the polynomial. We will show the minimal number of multiplications needed for elementary symmetric functions with eight or less variables.

Contents

1 Introduction

In [2], research to the elementary symmetric functions over a field $\mathbb{F}_2$ has been done. In this thesis we will consider the elementary symmetric functions over a field $\mathbb{F}_p$, with p an odd, large enough prime. This means that we work $\mathrm{mod}p$ instead of $\mathrm{mod}2$. Since prime p is large enough, working with $\mathrm{mod}p$ is in this thesis equal to working over $\mathbb{Z}$.
A symmetric function is a function such that the value of the function is independent of the order of the input variables. For a symmetric function f in three variables we have $f(x, y, z) = f(y, z, x) = f(z, x, y)$ for all x, y, $z \in \mathbb{F}_p$.
The elementary symmetric functions that we will consider are functions in n boolean variables. We will write these functions as sums of monomials. A monomial of length j is a product of j variables, say $x_{i_1} \cdot x_{i_2} \cdot ... \cdot x_{i_{j-1}} \cdot x_{i_j}$. Thus, $j \leq n$.
The elementary symmetric function e_i^n is the sum over all the different monomials of degree i when there are n variables. So for $1 \leq i \leq n$,

$$e_i^n(x_1, ..., x_n) = \sum_{M \subseteq \{1,...,n\}, |M|=i} \prod_{j \in M} x_j$$

with $e_i^n : \{0, 1\}^n \to \mathbb{Z}$.
It is easy to see that the value of e_i^n is equal to $\binom{j}{i}$ when j variables have value 1. The functions that we consider in this thesis are denoted as σ_i^n where $\sigma_i^n = e_i^n \mod 2$. We focus on the evaluation of the boolean function σ_i^n, with $\sigma_i^n : \{0, 1\}^n \to \{0, 1\}^n \subseteq \mathbb{F}_p$.

The main goal in this thesis is to minimize the number of multiplications needed to determine the value of σ_i^n. This because we assume that multiplications (also called AND-gates) cost time while additions, which include subtractions, are 'free'. We assume that it is possible to reuse products. This means that if $a \cdot b$ is determined, determining $a \cdot b \cdot c$ only costs one additional multiplication. We also assume that multiplying a variable with a constant is 'free'. Also $a = a^2 = a^k, k > 0$ since $a = 0$ or $a = 1$.
As an example we consider the function σ_2^3. We can write σ_2^3 in the two following ways: $\sigma_2^3 = a \cdot b + a \cdot c + b \cdot c - 2ab \cdot c = (a + b - 2a \cdot b) \cdot c + ab$. Figure 1 clearly shows the number of multiplications in each of the two ways to write σ_2^3.

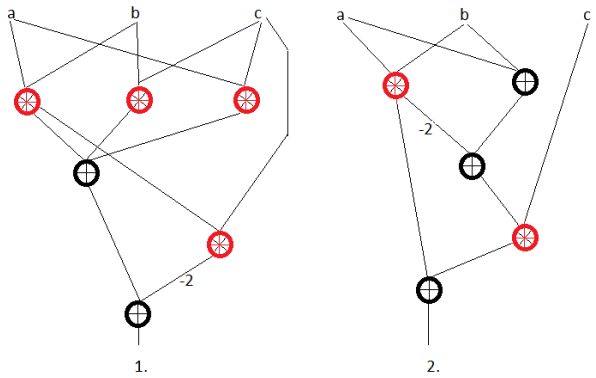

Figure 1: Illustration of σ_2^3

In Figure 1 the additions are black and the AND-gates are red. It is easy to see that in the second way to write σ_2^3 there are fewer AND-gates necessary than in the first way to write σ_2^3. Since the degree of σ_2^3 is three, we say that σ_2^3 can be written with a minimum of two multiplications.

We are mainly interested in the function σ_i^n for its use in secure multiparty computation, which is a way to compare secure data from various participants in such a way that the only information that could be leaked is the output value of the comparison.

2 The structure of σ_i^n

As stated in Section 1, we want to determine σ_i^n in such a way that $\sigma_i^n = e_i^n \bmod 2$ for all n, i.

First we will consider some examples of σ_i^n for small values of n and i.
If $n = 2$ and $i = 1$, it is easy to see that $\sigma_1^2 = x_1 + x_2 - 2x_1x_2$. When only one variable is equal to one, $e_1^2(\mathrm{mod}2) = 1$ and so is σ_1^2. When both variables are equal to one, $e_1^2(\mathrm{mod}2) = 0$ and so is σ_1^2. This means that σ_1^2 is a sum of e_1^2 and e_2^2, namely $\sigma_1^2 = e_1^2 - 2e_2^2$.
In Section 1 we have shown that if $n = 3$ and $i = 2$ then $\sigma_2^3 = a \cdot b + a \cdot c + b \cdot c - 2ab \cdot c$. This shows that $\sigma_2^3 = e_2^3 - 2e_3^3$.

We believe that σ_i^n is of the form $e_i^n + a_{i,i+1}^n e_{i+1}^n + ... + a_{i,n}^n e_n^n$. In order to find a closed expression for σ_i^n we only have to determine the values of the coefficients $a_{i,m}^n$ with $i < m \leq n$.

Remark 1. *The coefficients $a_{i,j}^n$ for $j \neq i$ are even, and $a_{i,i}^n$ is odd. Since $\sigma_i^n \bmod 2 = e_i^n$.*

The coefficients will be dependent of the Hammingweight of the variables, since the value of $e_i^n(\mathrm{mod}2)$ is only dependent on the number of variables equal to one.

2.1 The coefficients $a_{i,m}^n$ of σ_i^n

To determine the coefficients $a_{i,m}^n$ we use the following theorem:

Theorem 1. *For $1 \leq i \leq n$, let $\{a_{i,j}^n\}_{j=0}^n$ satisfy*

$$\forall_{w=0}^n \binom{w}{i} \bmod 2 = \sum_{j=0}^{n} a_{i,j}^n \binom{w}{j}.$$

Then

(i) $\sigma_i^n = \sum_{j=0}^n a_{i,j}^n e_j^n$,

(ii) $$a_{i,j}^n = \begin{cases} 0, & 0 \leq j < i, \\ 1, & j = i, \\ \binom{j}{i} \bmod 2 - \sum_{h=i}^{j-1} a_{i,h}^n \binom{j}{h}, & i < j \leq n. \end{cases}$$

Proof. This proof consists of two parts.
Part i Assume the input has Hammingweight w, for $0 \leq w \leq n$.
Then $\sigma_i^n = e_i^n \bmod 2 = \binom{w}{i} \bmod 2 = \sum_{j=0}^{n} a_{i,j}^n \binom{w}{j} = \sum_{j=0}^{n} a_{i,j}^n e_j^n$

Part ii Assume the input has Hammingweight w, for $0 \leq j \leq n$.
If $0 \leq w < i$ it holds that $\sigma_i^n = \binom{w}{i} \bmod 2 = 0$. Thus $\sum_{j=0}^{n} a_{i,j}^n \binom{w}{j} = 0$. Since $\binom{w}{j} = 0$ for $j > w$, we have that $\sum_{j=0}^{w} a_{i,j}^n \binom{w}{j} = 0$. It follows that $a_{i,j}^n = 0$ if $j \leq w < i$.
If $w = i$ it holds that $\sigma_i^n = \binom{w}{i} \bmod 2 = 1$. Thus $\sum_{j=i}^{n} a_{i,j}^n \binom{w}{j} = 1$. Since $\binom{w}{j} = 0$ if $j > w$ it follows that $a_{i,i}^n \binom{w}{i} = 1$, thus $a_{i,i}^n = 1$.
If $i < w \leq n$. Say $w = i + 1$, it holds that $\sigma_i^n = \binom{w}{i} \bmod 2 = \sum_{j=i}^{n} a_{i,j}^n \binom{w}{j} = \binom{w}{i} + a_{i,i+1}^n \binom{w}{i+1}$. It follows that

$$a_{i,i+1}^n = \binom{i+1}{i} \bmod 2 - \binom{i+1}{i}$$

Assume that $a_{i,j}^n = \binom{j}{i} \bmod 2 - \sum_{h=i}^{j-1} a_{i,h}^n \binom{j}{h}$ holds for $i + 1 < j < m < n$. Now we assume that the input has Hammingweight w with $w = m + 1$. $\sigma_i^n = \binom{m+1}{i} \bmod 2 = \sum_{j=i}^{n} a_{i,j}^n \binom{m+1}{j}$. Thus

$$a_{i,m+1}^n = \binom{m+1}{i} \bmod 2 - \sum_{j=i}^{m} a_{i,j}^n \binom{m+1}{h}$$

□

Remark 2. *The coefficients $a_{i,j}^n$ of σ_i^n with $i < m \leq n$ are unique.*

Remark 3. *The values of $a_{i,j}^n$ are independent of the value of n.*

Now, we are able to construct σ_i^n for all $n, i \in \mathbb{N}$.

As an example we show the calculations for σ_2^5. σ_2^5 is of the form $a_{2,2}^5 e_2^5 + a_{2,3}^5 e_3^5 + a_{2,4}^5 e_4^5 + a_{2,5}^5 e_5^5$. It is known that $a_{2,2}^5 = 1$.
First we determine $a_{2,3}^5$:

$$a_{2,3}^5 = \binom{3}{2} \bmod 2 - \binom{3}{2} = -2$$

Next we determine $a_{2,4}^5$:

$$a_{2,4}^5 = \binom{4}{2} \bmod 2 - \binom{4}{2} + 2\binom{4}{3} = 2$$

Lastly we determine $a_{2,5}^5$:

$$a_{2,5}^5 = \binom{5}{2} \bmod 2 - \binom{5}{2} + 2\binom{5}{3} - 2\binom{5}{4} = 0$$

So we find that $\sigma_2^5 = e_2^5 - 2e_3^5 + 2e_4^5$. The exact functions σ_i^n for n from 1 to 8 can be found in Appendix A.

2.2 A closer look at the structure of σ_i^n for fixed i

In Appendix A we can see that the row of coefficients $a_{i,m}^n$ for a fixed i, $1 \leq m \leq n$ is a subset of the row of coefficients $a_{i,m}^{n'}$ for the same i, $1 \leq m < n'$, when $n < n'$. We see that if n increases, the length of the row becomes longer. For example we consider σ_4^n. The coefficient rows of σ_4^4, σ_4^5, σ_4^6, σ_4^7 and σ_4^8 are prefixes {1}, {1, -4}, {1, -4, 10}, {1, -4, 10, -20}, {1, -4, 10, -20, 34}.
In this subsection we will look at the rows of coefficients for some of the values of i.

σ_1^n The row of coefficients for σ_1^n, which can be found in Table 1, is a very well known row. It is possible to rewrite this row to $\{(-2)^0, (-2)^1, (-2)^2, (-2)^3, (-2)^4, (-2)^5, (-2)^6, (-2)^7\}$.
Keeping this row in mind, it is easy to determine the values of $a_{1,9}^n$, $n > 9$, and $a_{1,10}^n$, $n > 10$, namely $(-2)^{(9-1)} = 256$ and $(-2)^{(10-1)} = -512$. A check with Theorem 1 confirms this. Now we have found an easy way to compute $a_{1,n}^n$; $a_{1,n}^n = (-2)^{(n-1)}$ for $n \geq 1$.
It is also possible to use the recurrence relation $a_{1,n}^n = -2a_{1,n-1}^n$ for $n > 1$ and $a_{1,1}^n = 1$.

σ_2^n The row of coefficients of σ_2^n, which can be extended using theorem 1, can be found in Table 1. Using [5] we found that this row is the expansion of $\frac{1}{1+2x+2x^2}$ and that the recurrence relations $a_{2,n}^n = -2(a_{2,n-1}^n + a_{2,n-2}^n)$ for $n > 2$ with $a_{2,2}^n = 0$, $a_{2,2}^n$=1 and $a_{2,n}^n = -4a_{2,n-4}^n$ for $n > 4$ with $a_{2,1}^n = a_{2,2}^n = a_{2,3}^n = 0$, $a_{2,4}^n = 1$ hold. These recurrence relations give two quick ways to compute $a_{2,n}^n$.

σ_3^n The coefficient list of σ_3^n can be found in Table 1. Using Mathematica's function *FindLinearRecurrence[]* we find that the recurrence relation that describes the coefficient list of σ_3^n is $a_{3,n}^n = -4a_{3,n-1}^n - 6a_{3,n-2}^n - 4a_{3,n-3}^n$ for $n > 3$ with $a_{3,1}^n = a_{3,2}^n = 0$, $a_{3,3}^n = 1$. This recurrence gives an easy way to compute the coefficients $a_{3,n}^n$.

The coefficient list of σ_3^n can also be generated by the function $a_{3,n}^n = (-1)^{n-1}(\frac{2^n}{4} - \frac{2^{\frac{n}{2}} \sin \pi \cdot \frac{n}{4}}{2} - \frac{0^n}{4})$ [4]. This provides a way to determine the coefficient list of σ_3^n without the use of a recurrence relation.

σ_4^n Now we consider the coefficient list of σ_4^n, which can be found in Table 1. Using Mathematica's function *FindLinearRecurrence[]* we find the following linear recurrence relation to determine $a_{4,n}^n$; $a_{4,n}^n = -4a_{4,n-1}^n - 6a_{4,n-2}^n - 4a_{4,n-3}^n - 2a_{4,n-4}^n$ for $n > 4$ with $a_{4,1}^n = a_{4,2}^n = a_{4,3}^n = 0$, $a_{4,4}^n = 1$. This gives an easy way to determine the coefficients of σ_4^n.

Table 1: Coefficient rows of σ_i^n, $1 \leq i \leq 4$

i	Coefficient rows σ_n^i											
1	1	-2	4	-8	16	-32	64	-128	256	-512	1024	2048
2	1	-2	2	0	-4	8	-8	0	16	-32	32	0
3	1	-4	10	-20	36	-64	120	-240	496	-1024	2080	-4160
4	1	-4	10	-20	34	-48	48	0	-164	560	-1352	2704

Using Mathematica we also found the following linear recurrence relations for the coefficient rows of σ_5^n, σ_6^n, σ_7^n, σ_8^n and σ_9^n. In Table 2 the linear recurrence relations are described.
I.e. the recurrence relation $x_n = cx_{n-1} + bx_{n-2} + ax_{n-3}$, $x_1 = x_2 = 0$ and $x_3 = 1$ is described as $\{a, b, c\}$.

Table 2: The recurrence relation describing the coefficients of σ_i^n

i	Coefficient rows σ_i^n
5	{-4,-10,-16,-14,-6}
6	{-4,-12,-22,-24,-16,-6}
7	{-8,-28,-56,-70,-56,-28,-8}
8	{-2,-8,-28,-56,-70,-56,-28,-8}
9	{-4,-18,-64,-140,-196,-182,-112,-44,-10}

We see that for the coefficient list of every σ_i^n an order i linear homogeneous recurrence relation with with constant coefficients can be found. The following theorem follows.

Theorem 2. *The row of coefficients of σ_i^n can be described by an order i linear homogeneous recurrence relation with constant coefficients for $n > i$ and $a_{i,1}^n = ... = a_{i,i-1}^n = 0$, $a_{i,i}^n = 1$.*

Proof. Say that $a_{i,j}^{*n} = (-1)^j a_{i,j}^n$. It follows from Theorem 1 that

$$\binom{w}{i} \bmod 2 = \sum_{j=0}^{w} (-1)^j a_{i,j}^{*w} \binom{w}{j}$$

We see that $\sum_{j=0}^{w} (-1)^j a_{i,j}^{*w} \binom{w}{j}$ is the binomial transform of $\binom{w}{i} \bmod 2$.
Theorem 10 in [1] proves that if $\binom{w}{i} \bmod 2$ has an order i recurrence relation for fixed w then $(-1)^j a_{i,j}^{*w}$ also has an order i recurrence relation for fixed w.

$\binom{w}{i} \bmod 2$ has an order i recurrence relation for fixed w if and only if $\binom{w}{i}$ has an order i recurrence relation for fixed w. It is clear to see that $\binom{w}{i}$ has an order i recurrence relation since it $\binom{w}{i}$ is a polynomial of degree i. One can assume that this is the characteristic polynomial of the recurrence relation. Thus it follows that $(-1)^j a_{i,j}^{*w}$ has an order i recurrence relation.

Now it is easy to see that $a^w_{i,j}$ has an order i recurrence relation, since it only differs from $(-1)^j a^{*w}_{i,j}$ by the term $(-1)^j$. One can take the recurrence relation of $a^{*w}_{i,j}$ and multiply this with $(-1)^j$ to obtain the order i recurrence relation of $a^w_{i,j}$. □

2.3 A closer look at the coefficient row $a^n_{i,i+x}$ for fixed x

In the previous subsection, subsection 2.2, we looked at σ^n_i for fixed i. This means we considered the horizontal lines in the overview in Appendix A. Now, we want to take a look at the vertical lines in the overview in Appendix A. This means considering sequences $a^n_{i,i+x}$, the sequences for x between zero and three can be found in Table 3.

Table 3: Coefficient rows $a^n_{i,i+x}$, $1 \leq x \leq 3$

x	Coefficient rows $a^n_{i,i+x}$								
0	1	1	1	1	1	1	1	1	1
1	-2	-2	-4	-4	-6	-6	-8	-8	-10
2	4	2	10	10	22	20	36	36	56
3	-8	0	-20	-20	-64	-48	-120	-120	-232

We have done some research on the case $x = 1$ and $x = 2$. We found the following functions to determine the coefficients of $a^n_{i,i+1}$ and $a^n_{i,i+2}$:

$$a^n_{i,i+1} = i \bmod 2 - i$$

$$a^n_{i,i+2} = \frac{i(i-1)}{2} \bmod 2 + \frac{i(i-1)}{2} - i((i-1) \bmod 2)$$

We found these functions using Theorem 1. One can see that both $a^n_{i,i+1}$ and $a^n_{i,i+2}$ can be determined without the use of an recurrence relation.

It would be very interesting to examine the coefficient rows of $a^n_{i,i+x}$ with x a constant and $n > 3$. Only this study is not the focus of this thesis. Therefore we did not do further research on this topic.

3 Simple cases of σ^n_i

In this section we will look at some simple cases of σ^n_i. We hope to find a relation between the number of variables and the minimum number of multiplications needed in each of the cases. In this section we will first consider σ^n_n and second σ^n_1.

3.1 Minimizing of the number of multiplications of σ_n^n

The simplest case if σ_i^n is the case where $i = n$, $n \geq 1$. This because $\sigma_n^n = x_1 \cdot x_2 \cdot ... \cdot x_{n-1} \cdot x_n$. It is not possible to rewrite this monomial in such a way that less multiplications then $n-1$ is used, since σ_n^n has degree n.
We conclude that the minimal number of multiplication needed to write σ_n^n is equal to $n-1$.

3.2 Minimizing of the number of multiplications of σ_1^n

The degree of σ_1^n is equal to n, since the monomial $x_1 \cdot x_2 \cdot ... \cdot x_{n-1} \cdot x_n$ is included in σ_1^n. We note that it is possible to write σ_1^nin the following way: $\sigma_1^n = x_1 \oplus x_2 \oplus ... \oplus x_{n-1} \oplus x_n$. Where $\oplus$ stands for the XOR-gate. It holds that $A \oplus B = A + B - 2AB$. This shows that the use of an XOR-gate implies the use of one multiplication.
We will first consider small cases of n and then derive a general form for σ_1^n.

Case $n = 2$ $\sigma_1^2 = x_1 + x_2 - 2x_1x_2$. We see that $x_1 \oplus x_2 = x_1 + x_2 - 2x_1x_2$. Since the degree of σ_1^2 is two, it is not possible to write σ_1^2 without any multiplications. Thus, the minimal number of multiplications needed for σ_1^2 is one.

Case $n = 3$ It is possible to write σ_2^3 using σ_1^2 in the following way: $\sigma_1^3 = \sigma_1^2 \oplus x_3$. This because $\sigma_1^2 = x_1 \oplus x_2$ and $\sigma_1^3 = x_1 \oplus x_2 \oplus x_3$. Thus we can write $\sigma_1^3 = (x_1 + x_2 - 2x_1x_2) + x_3 - 2(x_1 + x_2 - 2x_1x_2) \cdot x_3$. One can see that the minimal number of multiplications needed for σ_1^3 is one more than the number of multiplications needed for σ_1^2. This means that σ_1^3 can be written with two (=3-1) multiplications.
It is not possible to write σ_2^3 with less then two multiplications since the degree of σ_2^3 is three.

Case $n = 4$ We can write σ_1^4 in the following way using only three multiplications: $\sigma_1^4 = \sigma_1^3 + x_4 - 2\sigma_1^3 x_4$. This equals to the following structure: $\sigma_1^4 = \sigma_1^3 \oplus x_4$. It is clear to see that it is not possible to write σ_1^4 with less than three multiplications, since the degree of σ_1^4 is four.

If we look at a more general case, we can see that σ_1^n can be written as $\sigma_1^{n-1} \oplus x_n = \sigma_1^{n-1} + x_n - 2\sigma_1^{n-1} \cdot x_n$. Thus we conclude that it is possible to write σ_1^n with a minimum of $n-1$ multiplications for all $n \geq 1$. This because when we start with σ_1^2, which we can write with one (=2-1) multiplication, we can compute σ_1^3 with only one extra multiplication. If we repeat this step $n-2$ times, we see that it is possible to write σ_1^n with $n-1$ multiplications.

4 Minimizing of the number of multiplications of σ_{n-1}^n

In this section we will consider σ_{n-1}^n. We assume that it is possible to compute σ_{n-1}^n with $n-1$ multiplications. This because the largest monomial has degree n. First we will look at σ_{n-1}^n for $n = 2, 3, 4$.

Equation for σ_1^2 It is easy to see that it is possible to compute σ_1^2 with only one multiplication, since $\sigma_1^2 = a+b-2a\cdot b$. It is not possible to write σ_1^2 with less than one multiplication since the monomial ab has to be constructed.

Equation for σ_2^3 We have already shown in the introduction that it is possible to write σ_2^3 with only two multiplications. Namely; $\sigma_2^3 = a\cdot b+a\cdot c+b\cdot c-2ab\cdot c = (a+b-2a\cdot b)\cdot c+ab$. It is not possible to write σ_2^3 with less multiplications, since the monomial with the highest degree of σ_2^3 is equal to 3.

Equation for σ_3^4 It was not easy to find a way to compute σ_3^4 using only three multiplications. We have found a couple of ways to do so;

$$\begin{aligned}
\sigma_3^4 &= (a\cdot b + (a+b-4ab)\cdot c)\cdot(d+c-1)+ab \\
\sigma_3^4 &= (a\cdot b + c\cdot d)\cdot(-4cd+a+b+c+d) - 2ab + 2cd \\
\sigma_3^4 &= (a\cdot b + c\cdot d)\cdot(-2ab-2cd+a+b+c+d)
\end{aligned}$$

We also tried to write σ_3^4 in three multiplications with the term $a\cdot b\cdot c$. We came to the conclusion that this is not possible using Mathematica. The method used will be described in Subsection 4.1
It is not possible to write σ_3^4 with less multiplications, since the monomial with the highest degree of σ_3^4 is equal to 4.

When we look at the ways to write σ_{n-1}^n and the structure of σ_{n-1}^n we see that σ_{n-1}^n can be written using σ_{n-2}^{n-1};

$$\sigma_2^3 = \sigma_1^2\cdot(c+b-1)+a \tag{1}$$
$$\sigma_3^4 = \overline{\sigma_2^3}\cdot(d+c-1)+a\cdot b \tag{2}$$
$$\sigma_4^5 = \sigma_3^4\cdot(e+d-1)+a\cdot b\cdot c \tag{3}$$
$$\sigma_5^6 = \overline{\sigma_4^5}\cdot(f+e-1)+a\cdot b\cdot c\cdot d \tag{4}$$

Where $\overline{\sigma_{n-1}^n}$ means that the coefficient $a_{n-1,n}^n$ has to be multiplied by 2. I.e, $\overline{\sigma_2^3} = e_2^3 - 4e_3^3$.

4.1 Equation for σ_4^5

Since it seems difficult to find ways to write σ_3^4 with only 3 multiplications, it is expected to be very difficult to write σ_4^5 with only four multiplications. Because it is not possible to write σ_3^4 with only three multiplications while including the term $a\cdot b\cdot c$ we cannot use equation 3 to write σ_4^5 with only four multiplications. Using the second way to write σ_3^4 we can write σ_4^5 with five multiplications; $\sigma_4^5 = ((a\cdot b+c\cdot d)\cdot(a+b+c+d-4cd)-2ab+2cd)\cdot e+ab\cdot c$.

In the process of finding a way to write σ_4^5 with only four multiplications, we used Mathematica. First we constructed a function *red[]*, which made sure that when multiplying a variable x_i with itself the outcome would not become $(x_i)^2$ but x_i. This assumption has

been made in Section 1. *red[]* sees letters a,b,c etc. as variables. The Mathematica code can be found in Appendix B. We also used the Mathematica functions *MonomialList[]* and *Solve[]*.
We used the function *red[]* in the following way; we always entered -σ_4^5 first and then we added a polynomial, a guessing polynomial, of which we believed that it could be an other way to write σ_4^5. If the outcome of *red[]* is equal to zero, the second polynomial is a different way to write σ_4^5. An example of how the function *red[]* was used is given in Figure 2.

$$\begin{aligned} In[] := red[&-(abcd + abce + abde + acde + bcde - 4abcde) \\ &+(e + d - 1)((ab + cd)(a + b + c + d - 4cd) - 2ab + 2cd)] \\ &Out[] = -abc \end{aligned}$$

Figure 2: Example of the function *red[]*

We call the output of the function *red[]* the "left-over polynomial". First we tried to find a polynomial with only four multiplications that was equal to σ_4^5 by hand. We have tried for several hours but could not find such a polynomial. That is why we started a much broader search.
We started using the function *MonomialList[]*. The input for this function was the same as the input from *red[]*, where our guessing polynomial consisted of variable coefficients. The output was an equation for each of the monomials in the left-over polynomial. If we choose all the coefficients in such a way that all the equations are equal to zero, we find a polynomial in four multiplications that is equal to σ_4^5.
An example of the function *MonomialList[]* is given in Figure 3.

$$\begin{aligned} In[] = MonomialList[red[&-(ab + ac + ad + bc + bd + cd - 2(abc + abd + acd + bcd) \\ &+2abcd) + (\xi ab + \phi cd + \omega a + \upsilon\, b + \eta c + \iota d + y)(\alpha ab + \beta cd + \gamma a + \delta b + \epsilon c + \zeta d + x)], \{a, b, c, d\}] \end{aligned}$$

$$\begin{aligned} Out[] = \{&abcd(-2 + \beta\xi + \alpha\phi), abc(2 + \alpha\eta + \epsilon\xi), abd(2 + \alpha\iota + \zeta\xi), \\ &ab(-1 + y\alpha + x\xi + \alpha\xi + \gamma\xi + \delta\xi + \alpha\omega + \delta\omega), acd(2 + \gamma\phi + \beta\omega), \\ &ac(-1 + \gamma\eta + \epsilon\omega), ad(-1 + \gamma\iota + \zeta\omega), a(y\gamma + x\omega + \gamma\omega), bcd(2 + \delta\phi), \\ &bc(-1 + \delta\eta), bd(-1 + \delta\iota), by\delta, cd(-1 + y\beta + \beta\eta + \zeta\eta + \beta\iota + \epsilon\iota + x\phi + \beta\phi + \epsilon\phi + \zeta\phi), \\ &c(y\epsilon + x\eta + \epsilon\eta), d(y\zeta + x\iota + \zeta\iota), xy\} \end{aligned}$$

Figure 3: Example of the function *MonomialList[]*

We used the function *Solve[]* to find a solution for all the equations. In order to reduce the number of equations that needed to be solved, we did not include the equations for the monomials ab, cd, a, b, c, d and e. This is not a problem since we can always add or subtract these monomials to the guessing polynomial.

Using this method we did find ways to write σ_4^5 with only four multiplications. The equations below show how σ_4^5 can be written with only four multiplications, where $A = a \cdot b + c \cdot d$.

$$\sigma_4^5 = A \cdot (2ab - 4cd - 2a - 2b + 2c + 2d + e + 1) \cdot (-3ab + 2a + 2b + \frac{1}{2}e - 1) + cd$$

$$\sigma_4^5 = \frac{1}{2}A \cdot (-A + 2e + 1) \cdot (-A + a + b + c + d + 2e - 3)$$

$$\sigma_4^5 = \frac{1}{2}A \cdot (-A + a + b + c + d + e - \frac{5}{2}) \cdot (-3A + a + b + c + d + e + \frac{3}{2}) + \frac{3}{8}A$$

The only problem with the equations is that the coefficients of the polynomials are not all integers. I.e. one coefficient has the value $\frac{1}{2}$.
This will not be a big problem for implementations. This will be explained in section 5.

Equation for σ_5^6 Using this method in Mathematica we also searched for other ways to write various σ_i^n. Equation 5 shows how σ_5^6 can be written with only five multiplications.

$$\frac{1}{2}(a \cdot b + c \cdot d + e \cdot f) \cdot (-2ab - 2cd - 2ef + a + b + c + d + e + f) \cdot (ab + cd + ef - 1) \quad (5)$$

This way to write σ_5^6 includes the factor $\frac{1}{2}$.

Equation for σ_6^7 Equation 6 shows how σ_6^7 can be written with only six multiplications, where $A = a \cdot b + c \cdot d + e \cdot f$.

$$\frac{1}{3}(A - g) \cdot (A - \frac{3}{4}(a + b + c + d + e + f) - g + 2) \cdot (A + g - 1) \cdot (A - 2(g + 1)) \quad (6)$$

This way to write σ_6^7 includes the factor $\frac{1}{3}$ and the coefficient $\frac{1}{4}$.

We also tried to find a function to write σ_6^7 with only six multiplications for which not only the coefficients for ab, cd and ef are equal, but also the coefficients for a, b, c, d, e, f and g. We came to the conclusion that there are only complex solution for this problem. Equation 7 shows one of the possible solutions where $B = a + b + c + d + e + f + g$.

$$\frac{1}{4}A \cdot (\frac{i}{6}(15i + \sqrt{15})A + B + \frac{1}{3}(3 - i\sqrt{15})) \cdot (-\frac{i}{6}(-9i + \sqrt{15})A + B + \frac{i}{3}(6i + \sqrt{15})) \cdot (A - 1) \quad (7)$$

Equation for σ_7^8 Equation 8 shows how σ_7^8 can be written with only seven multiplications, where $A = a \cdot b + c \cdot d + e \cdot f + g \cdot h$.

$$\frac{1}{3}A \cdot (-A + 2) \cdot (A - \frac{1}{2}(a + b + c + d + e + f + g + h)) \cdot (A - 1) \quad (8)$$

This way to write σ_7^8 includes the factor $\frac{1}{3}$ and the coefficient $\frac{1}{2}$.

In the equations above we can see some kind of symmetry in the coefficients. We see that in each factor of the product the coefficients of the monomials of the same degree are equal.
This fact will make it relatively simple to find equations for σ_{n-1}^n for $n > 8$.

Is it possible to construct a polynomial with integer coefficients such that it is equal to σ_4^5? After finding a way to write σ_4^5 with only four multiplications but with using a rational number as one of the coefficients the question rises wether it is possible to write σ_4^5 with only four multiplications and using only integers as coefficients.
We have thought of the following way to check wether this is possible or not:

First we established a guessing polynomial which was as broad as possible. We choose

$$Pl(a,b,c,d,e) = (\alpha a{\cdot}b{+}\beta c{\cdot}d{+}\gamma a{+}\delta b{+}\epsilon c{+}\eta d{+}\theta e{+}x){\cdot}(\iota ab{+}\kappa cd{+}\lambda a{+}\mu b{+}\nu c{+}\xi d{+}\zeta e{+}y)$$

$$\cdot(\omega ab + \phi cd + \psi a + hb + jc + kd + me + z) + lab + ncd + qa + pb + tc + ud + ve + w$$

as our guessing polynomial. We chose this polynomial because we have seen in previous ways to write σ_{n-1}^n that the term ab, and if possible the term cd, is a recurring factor. Also, this polynomial contains the largest multiplications as possible, since in each part of the product every linear combination of a, b, c, d and e can occur.

There are two other guessing polynomials possible, which also have to be checked in a similar way. These are the following polynomials:

$$Pl2(a,b,c,d,e) = (w_1a{\cdot}b{+}w_2a{+}w_3b{+}w_4c{+}w_5d{+}w_6e{+}w){\cdot}(x_1ab{+}x_2a{+}x_3b{+}x_4c{+}x_5d{+}x_6e{+}x){\cdot}$$

$$(y_1ab + y_2a + y_3b + y_4c + y_5d + y_6e + y) \cdot (z_1ab + z_2a + z_3b + z_4c + z_5d + z_6e + z)$$
$$+lab + qa + pb + tc + ud + ve + v$$

and

$$Pl3(a,b,c,d,e) = (v_1a{+}v_2b{+}v_3c{+}v_4d{+}v_5e{+}v) \cdot (w_1a{+}w_2b{+}w_3c{+}w_4d{+}w_5e{+}w){\cdot}$$

$$(x_1a{+}x_2b{+}x_3c{+}x_4d{+}x_5e{+}x){\cdot}(y_1a{+}y_2b{+}y_3c{+}y_4d{+}y_5e{+}y){\cdot}(z_1a{+}z_2b{+}z_3c{+}z_4d{+}z_5e{+}z)$$
$$+qa + pb + tc + ud + ve + r$$

It might be possible to use a basis transformation on $Pl2$ and $Pl2$ to construct a polynomial of the form Pl. If this is possible, one does not have to check $Pl2$ and $Pl2$. Further research has te be done on this part.

We know that the variables a, b, c, d and e can only have the value 0 or 1. This gives us 2^5 possible inputs. We have entered all the possible inputs in the polynomial Pl, giving us 32 equations in the coefficients of Pl. We have also entered the possible inputs in σ_4^5, giving us for each input the value of σ_4^5. Combining the two, we have found 32 equations which we should be able to solve. The equations can be found in Appendix C.
If it is possible to solve this set of equations using only integers, we have found a way to write σ_4^5 with only integer coefficients. If it is not possible to solve this set of equations, using only integers, we have to do the same thing for $Pl2$ and $Pl2$. If $Pl2$ and $Pl2$ also have no possible integer solutions we know that it is not possible to write σ_4^5 with only integer coefficients.

σ_4^5 can have the value zero or one, since it is a boolean function. First we will focus

on the equations which are equal to one. This because we know that choosing all the variables equal to zero will solve all the equations equal to zero, but not the equations equal to one.
There are 6 equations equal to one, these can be found in Figure 4.

```
A1 = n + p + t + u + v + w + (x + β + δ + ϵ + η + θ) (y + ξ + κ + μ + ν + ξ) (h + j + k + m + z + ϕ);
B1 = (n + q + t + u + v + w + (x + β + γ + ϵ + η + θ) (y + ξ + κ + λ + ν + ξ) (j + k + m + z + ϕ + ψ));
C1 = (l + p + q + u + v + w + (x + α + γ + δ + η + θ) (y + ξ + ι + λ + μ + ξ) (h + k + m + z + ψ + ω));
D1 = (l + p + q + t + v + w + (x + α + γ + δ + ϵ + θ) (y + ξ + ι + λ + μ + ν) (h + j + m + z + ψ + ω));
E1 = (l + n + p + q + t + u + w + (x + α + β + γ + δ + ϵ + η) (y + ι + κ + λ + μ + ν + ξ) (h + j + k + z + ϕ + ψ + ω));
F1 = (l + n + p + q + t + u + v + w + (x + α + β + γ + δ + ϵ + η + θ) (y + ξ + ι + κ + λ + μ + ν + ξ) (h + j + k + m + z + ϕ + ψ + ω));
```

Figure 4: Equations equal to 1

We want to solve these equations and see of the solutions of these functions also lead to solving the equations equal to zero. To solve these functions we want to use the Mathematica function *Solve[]*.
The six equations, $A1$ through $F1$, are too large to be solved quickly by the function *Solve[]*. This is why we decided to use the following equations;

$$\begin{aligned}
x_1 &= \alpha + \gamma + \delta \\
x_2 &= \iota + \lambda + \mu \\
x_3 &= \omega + \psi + h \\
x_4 &= \beta + \epsilon + \eta \\
x_5 &= \kappa + \nu + \xi \\
x_6 &= k + j + \phi \\
x_7 &= x + \theta \\
x_8 &= \zeta + y \\
x_9 &= m + z
\end{aligned}$$

We chose these equations in such a way that the equations $A1$ through $F1$ would be as small as possible. Using these equations, we have eliminated the following variables from the equations; α, β, θ, ι, κ, ξ, ω, ϕ and m. But we have also added the variables x_1 through x_9. Once a solution is found for the new set of variables, a unique solutions for the old set of variables can be constructed. This because each variable x_i contains one of the variables that have been eliminated from the equations. The equations that we are left with are shown in Figure 5.

```
A2 = n + p + t + u + v + w + (δ + x4 + x7) (x8 + μ + x5) (h + x6 + x9);
B2 = (n + q + t + u + v + w + (γ + x4 + x7) (x8 + λ + x5) (x6 + x9 + ψ));
C2 = (l + p + q + u + v + w + (x1 + η + x7) (x8 + x2 + ξ) (x3 + k + x9));
D2 = (l + p + q + t + v + w + (x1 + ϵ + x7) (x8 + x2 + ν) (j + x9 + x3));
E2 = (l + n + p + q + t + u + w + (x + x1 + x4) (y + x2 + x5) (z + x6 + x3));
F2 = (l + n + p + q + t + u + v + w + (x1 + x4 + x7) (x8 + x2 + x5) (x6 + x9 + x3));
```

Figure 5: Equations equal to 1 after adding x_1 through x_9

The equations $A2$ through $F2$ can be easily solved by the function *Solve[]* and only have one solution. This solution contains a constraint on the variables n, p, t, v, l and q. All of these variables do not exist in the product of Pl but are simply to correct some of the terms.

The last thing we have to do is solve the equations equal to zero with the constraints given on the variables n, p, t, v, l and q.

Sadly enough, the solve function of mathematica has not yet given an answer whether or not it is possible to solve the equations equal to zero using only integers. Also attempts of choosing variables and checking if an integer solution exists did not gave an integer solution.
When one solves the equations equal to zero, he will know wether an integer solution exists or not.
Remember that the same procedure has te be done with $Pl2$ and $Pl2$ if Pl gives a negative answer.

5 Small examples of σ_i^n

In this section we will focus on Table 4. This table shows the minimal number of multiplications needed to write σ_i^n for $1 \leq n \leq 8, 1 \leq i \leq 8$.

Table 4: The minimal number of multiplications for σ_i^n

σ_i^n	i							
n	1	2	3	4	5	6	7	8
1	0	-	-	-	-	-	-	-
2	1	1	-	-	-	-	-	-
3	2	2	2	-	-	-	-	-
4	3	**3**	3	3	-	-	-	-
5	4	**3?/4**	**4**	**4**	4	-	-	-
6	5	**5?**	**5**	**5**	**5**	5	-	-
7	6	**??**	**6?**	**6?**	**6?**	**6**	6	-
8	7	**??**	**7?**	**7?**	**7?**	**7?**	**7**	7

The numbers in bold writing are the boundaries that have been discovered and/or proven in this thesis. A question mark after an entry means that we expect the number of multiplications needed to be that entry only we have not found an equation to prove this. A double question mark means that we do not have an idea of how much multiplications are needed to describe the matching σ_i^n.
We will show the equations for σ_i^n which we have found and which have not been in previous sections of this thesis.

σ_2^4 The degree of σ_2^4 is equal to four. This means that, using the degree lower bound, the minimal number of multiplications needed is three. If we can show that it is possible to write σ_2^4 using only three multiplications, we know for certain that this is the minimal numbers of multiplications needed.
We found the following polynomial that is equal to σ_2^4: $(a \cdot b - 2c \cdot d + c + d) \cdot (2cd + a + b - 2c - 2d) - ab + 2c + 2d - 3cd$. Thus, we conclude that the minimal number of multiplications needed for σ_2^4 is three.

σ_2^5 The degree of σ_2^5 is equal to four. Only, it is not possible to write σ_2^5 of the form $(x_1a \cdot b + x_2c \cdot d + x_3a + x_4b + x_5c + x_6d + x_7e + x_8) \cdot (y_1ab + y_2cd + y_3a + y_4b + y_5c + y_6d + y_7e + y_8) + z_1ab + z_2cd + z_3a + z_4b + z_5c + z_6d + z_7e + z_8$, since the terms $abce$, $abde$, $acde$, ace, ade, $bcde$, bce and bde can not be created this way.
It might is possible that σ_2^5 can be written as the form $(w_1a + w_2b + w_3c + w_4d + w_5e + w)(x_1a + x_2b + x_3c + x_4d + x_5e + x)(y_1a + y_2b + y_3c + y_4d + y_5e + y)(z_1a + z_2b + z_3c + z_4d + z_5e + z)$. Only we did not find a correct polynomial that describes σ_2^5 with only three multiplications. The reason that this is difficult is because of the structure of σ_2^5, namely it holds that $\sigma_2^5 = e_2^5 - 2e_3^5 + 2e_4^5 - 0e_5^5$. We believe that the zero coefficient is the reason that it is hard to determine an equation.

We found the following polynomial that is equal to σ_2^5: $(a \cdot b + c \cdot d + \frac{4}{3}e - \frac{2}{3}) \cdot (5ab + 5cd - 3a - 3b - 3c - 3d + \frac{4}{3}e - \frac{2}{3}) \cdot (\frac{1}{4}a + \frac{1}{4}b + \frac{1}{4}c + \frac{1}{4}d - \frac{1}{2}) + \frac{2}{9} + \frac{7}{18}(a + b + c + d)$.

Thus, we conclude that the minimal number of multiplications needed for σ_2^5 might be three but we have found an equation which describes σ_2^5 in four multiplications.

σ_3^5 We found the following polynomial that is equal to σ_3^5: $\frac{1}{2}(a \cdot b + c \cdot d - 2e) \cdot (2ab + 2cd - (a+b+c+d) + e) \cdot (-3ab - 3cd + \frac{1}{2}(a+b+c+d+e) - \frac{1}{2})$. Thus, we conclude that the minimal number of multiplications needed for σ_3^5 is four.

σ_4^6 We found the following polynomial that is equal to σ_4^6: $(a \cdot b + c \cdot d + e \cdot f) \cdot ((-2 - \frac{2}{\sqrt{6}})(ab + cd + ef) + a + b + c + d + e + f - \frac{1}{2} + \frac{3\sqrt{6}}{4}) \cdot ((-1 + \frac{1}{\sqrt{6}})(ab + cd + ef) + (1/2)(a+b+c+d+e+f) - \frac{1}{4} - \frac{3\sqrt{6}}{8}) + \frac{19}{48}(ab + cd + ef)$. Thus, we conclude that the minimal number of multiplications needed for σ_4^6 is five.

σ_3^6 We found the following polynomial that is equal to σ_3^6: $(\frac{-10}{3}(a \cdot b + c \cdot d + e \cdot f) + \frac{5-\sqrt{15}}{3}(a+b+c+d+e+f) - 4 + \sqrt{15}) \cdot (ab+cd+ef - \frac{1}{2}(a+b+c+d+e+f)) \cdot (ab+cd+ef - (\frac{1}{2} + \frac{\sqrt{15}}{10})(a+b+c+d+e+f) + \frac{6}{5} + \frac{3\sqrt{15}}{10}) - \frac{11}{30}(ab+cd+ef) + \frac{11}{60}(a+b+c+d+e+f)$. Thus, we conclude that the minimal number of multiplications needed for σ_3^6 is five.

One can see that not all the polynomials found to describe σ_i^n, for certain values for i and n, have integer coefficients. Some also have rational or real numbers as their coefficients. For implementation of the polynomials, this is not a problem. Although, when dealing with rational and real numbers there are some things one has to be aware of.
When dealing with rational numbers, one has to make sure the the denominator of all the rational numbers in the polynomial and the prime number p have a greatest common divisor of 1. This because when the greatest common divisor equals 1, the rational number has an inverse number $(\mathrm{mod} p)$. I.e. if the only rational number in the polynomial is a $\frac{1}{2}$, it is sufficient to say that p has to be an odd prime.

When dealing with real numbers, say $\sqrt{x}$ with $x \in \mathbb{N}$, x has to be a quadratic residue $(\mathrm{mod} p)$. There are various ways to check whether x is a quadratic residue or a quadratic nonresidue. One way is to determine $x^{\frac{p-1}{2}} (\mathrm{mod} p)$, if $x^{\frac{p-1}{2}} (\mathrm{mod} p) = 1$ then x is a quadratic residue. An other way to check if x is a quadratic residue is to determine the value of the Legendre symbol, Section 4.1 and 4.2 of [3] describe how to do this.

In Table 4, the two bottom rows are mainly filled with approximations of the minimal numbers of multiplications. We expect these number of multiplications because of the symmetry in the equations found thus far. We have no reason to believe that this symmetry does not hold when n increases. Only, we cannot say if the coefficients in the equations will be pretty. This means that we do not know if we coefficients will be rational, real or even complex.
In the case where $i = 2$, we are not sure what will happen with the minimal numbers of multiplications needed. This because of the zero in the coefficient row that describes σ_2^n for $n \leq 5$.

6 Conclusion

In this thesis we made a beginning of the elementary symmetric polynomials over a field with characteristic p has been done in this thesis.

We have found a way to construct these polynomials, σ_i^n, using the elementary symmetric polynomials e_i^n. Appendix A shows the exact functions σ_i^n for $1 \leq n \leq 8$. We have proven that the coefficients of σ_i^n can be determined using an order i linear homogeneous recurrence relation with constant coefficients. This is more efficient then using all previous coefficients to determine the next coefficient.

We have also shown equations for σ_i^n for numerous values of n and i minimizing the number of multiplications needed to write σ_i^n. These results can be found in Section 5.

7 Open problems and discussion

Although this thesis answers a lot of questions it also leaves some problems and points for further research.

Problems The first problem is whether it is necessary to use rational, real and possibly complex numbers as coefficients of the polynomials to describe σ_i^n. We have already made a beginning in answering this question, this can be found in Subsection 4.1. If one solves the equations that are equal to zero and there is an integer solution, then it is not necessary to write σ_4^5 with rational coefficients. This would not mean that it is possible to write other σ_i^n's with only integer coefficients. If an integer solution is found for these equations, this may give new insight in how to look for integer solutions. On the other hand, if it is not possible to write σ_4^5 with only integer coefficients, then it is presumable that σ_i^n for $n > 5$ cannot be written with only integer coefficients.
If it is not necessary that $\sigma_i^n : \{0,1\}^n \rightarrow \{0,1\}$ and it is also allowed that $\sigma_i^n : \{0,1\}^n \rightarrow \{0,x\}$ with $x \in \mathbb{R}$ then it does not matter if the coefficients of σ_i^n are integers or not. For example, one can compensate the rational coefficients by multiplying the entire equation with the least common multiple, lmc, of the denominators. This results in the function $\sigma_i^n : \{0,1\}^n \rightarrow \{0, lcm\}$ with $lcm \in \mathbb{N}$ and in integer coefficients.

The second problem which would be very interesting to look at is finding equations for σ_i^n's which have zeros in their coefficient rows. We have found it very difficult to find equations which described σ_2^5 and σ_2^6, since there is no symmetry possible in the equations. It would also be interesting to investigate wether there is any regularity in the appearance of zeros in the coefficient rows.

Points for further research The first point which would be interesting for some further research, which has been mentioned in Subsection 2.3, is looking at the coefficients $a_{i,i+x}^n$.

A small beginning has been made in this thesis only this was not the focus of this thesis.

The second point of discussion is that when one has a 'cheap' test to determine whether something is equal to zero, it is possible to determine σ_{n-1}^n and σ_{n-2}^n without any multiplications. It might be possible that this also holds for other σ_i^n's, but we did not do further research on this topic.

```
int x1, x2, xn;
int n;

public int sigma() {
    if (x1 + x2 + xn - n == 0) {
        if(n % 2 == 1)
            return 1;
        else
            return 0;
    } else if (x1 + x2 + xn - n == 1) {
        return 1;
    } else {
        return 0;
    }
}
```

Figure 6: Code to determine σ_{n-1}^n

Figure 6 shows the code which can determine σ_{n-1}^n without any multiplications. A similar code can be written for determining σ_{n-2}^n.

References

[1] Stefano Barbero, Umberto Cerruti, and Nadir Murru, *Transforming recurrent sequences by using the binomial and invert operators*, Journal of Integer Sequences **13** (2010), Article 10.7.7.

[2] Joan Boyar and Rene Peralta, *Tight bounds for the multiplicative complexity of symmetric functions*, (2008), 223 – 246.

[3] Benne de Weger, *Algorithmic number theory, discrete mathematics 2, part 1*, 0.55 ed., October 2012.

[4] N.J.A. Sloane and Paul Barry, *The on-line encyclopedia of integer sequences a000749*, June 2008.

[5] Michael Somos and Paul Curtz, *The on-line encyclopedia of integer sequences a108520*.

A Overview of σ_i^n for n from 1 to 8

In this section we show an overview of σ_i^n for n from 1 to 8.

- $n = 1$
  - $\sigma_1^1 = e_1^1$
- $n = 2$
  - $\sigma_1^2 = e_1^2 - 2e_2^2$
  - $\sigma_2^2 = e_2^2$
- $n = 3$
  - $\sigma_1^3 = e_1^3 - 2e_2^3 + 4e_3^3$
  - $\sigma_2^3 = e_2^3 - 2e_3^3$
  - $\sigma_3^3 = e_3^3$
- $n = 4$
  - $\sigma_1^4 = e_1^4 - 2e_2^4 + 4e_3^4 - 8e_4^4$
  - $\sigma_2^4 = e_2^4 - 2e_3^4 + 2e_4^4$
  - $\sigma_3^4 = e_3^4 - 4e_4^4$
  - $\sigma_4^4 = e_4^4$
- $n = 5$
  - $\sigma_1^5 = e_1^5 - 2e_2^5 + 4e_3^5 - 8e_4^5 + 16e_5^5$
  - $\sigma_2^5 = e_2^5 - 2e_3^5 + 2e_4^5 - 0e_5^5$
  - $\sigma_3^5 = e_3^5 - 4e_4^5 + 10e_5^5$
  - $\sigma_4^5 = e_4^5 - 4e_5^5$
  - $\sigma_5^5 = e_5^5$
- $n = 6$
  - $\sigma_1^6 = e_1^6 - 2e_2^6 + 4e_3^6 - 8e_4^6 + 16e_5^6 - 32e_6^6$
  - $\sigma_2^6 = e_2^6 - 2e_3^6 + 2e_4^6 + 0e_5^6 - 4e_6^6$
  - $\sigma_3^6 = e_3^6 - 4e_4^6 + 10e_5^6 - 20e_6^6$
  - $\sigma_4^6 = e_4^6 - 4e_5^6 + 10e_6^6$
  - $\sigma_5^6 = e_5^6 - 6e_6^6$
  - $\sigma_6^6 = e_6^6$
- $n = 7$
  - $\sigma_1^7 = e_1^7 - 2e_2^7 + 4e_3^7 - 8e_4^7 + 16e_5^7 - 32e_6^7 + 64e_7^7$
  - $\sigma_2^7 = e_2^7 - 2e_3^7 + 2e_4^7 - 0e_5^7 - 4e_6^7 - 8e_7^7$
  - $\sigma_3^7 = e_3^7 - 4e_4^7 + 10e_5^7 - 20e_6^7 + 36e_7^7$
  - $\sigma_4^7 = e_4^7 - 4e_5^7 + 10e_6^7 - 20e_7^7$

- σ_5^7 = e_5^7 -6e_6^7 +22e_7^7
- σ_6^7 = e_6^7 -6e_7^7
- σ_7^7 = e_7^7

- $n = 8$
  - σ_1^8 = e_1^8 -2e_2^8 +4e_3^8 -8e_4^8 +16e_5^8 -32e_6^8 +64e_7^8 -128e_8^8
  - σ_2^8 = e_2^8 -2e_3^8 +2e_4^8 -0e_5^8 -4e_6^8 +8e_7^8 -8e_8^8
  - σ_3^8 = e_3^8 -4e_4^8 +10e_5^8 -20e_6^8 +36e_7^8 -64e_8^8
  - σ_4^8 = e_4^8 -4e_5^8 +10e_6^8 -20e_7^8 +34e_8^8
  - σ_5^8 = e_5^8 -6e_6^8 +22e_7^8 -64e_8^8
  - σ_6^8 = e_6^8 -6e_7^8 +20e_8^8
  - σ_7^8 = e_7^8 -8e_8^8
  - σ_8^8 = e_8^8

B Mathematica code

This Mathematica code was used in determining multiplications under the assumption that $(x_i)^2$ equals to x_i.

$$red[w\rceil :=$$

$$red[w] =$$

$$Fold[PolynomialRemainder[\#1, \#2[[1]], \#2[[2]]]\&,$$

$$w, \{\{a^2 - a, a\}, \{b^2 - b, b\}, \{c^2 - c, c\}, \{d^2 - d,$$

$$d\}, \{e^2 - e, e\}, \{f^2 - f, f\}, \{g^2 - g, g\}\}]$$

C Equations describing σ_4^5

The equations shown in Figure 7 describe σ_4^5 when fitting the guessing polynomial used in Subsection 4.1.

```
{w + x y z, 0}
{v + w + (m + z) (y + ζ) (x + θ), 0}
{u + w + (k + z) (x + η) (y + ξ), 0}
{u + v + w + (k + m + z) (x + η + θ) (y + ζ + ξ), 0}
{t + w + (j + z) (x + ϵ) (y + ν), 0}
{t + v + w + (j + m + z) (x + ϵ + θ) (y + ζ + ν), 0}
{n + t + u + w + (x + β + ϵ + η) (y + κ + ν + ξ) (j + k + z + ϕ), 0}
{n + t + u + v + w + (x + β + ϵ + η + θ) (y + ζ + κ + ν + ξ) (j + k + m + z + ϕ), 0}
{p + w + (h + z) (x + δ) (y + μ), 0}
{p + v + w + (h + m + z) (x + δ + θ) (y + ζ + μ), 0}
{p + u + w + (h + k + z) (x + δ + η) (y + μ + ξ), 0}
{p + u + v + w + (h + k + m + z) (x + δ + η + θ) (y + ζ + μ + ξ), 0}
{p + t + w + (h + j + z) (x + δ + ϵ) (y + μ + ν), 0}
{p + t + v + w + (h + j + m + z) (x + δ + ϵ + θ) (y + ζ + μ + ν), 0}
{n + p + t + u + w + (x + β + δ + ϵ + η) (y + κ + μ + ν + ξ) (h + j + k + z + ϕ), 0}
{n + p + t + u + v + w + (x + β + δ + ϵ + η + θ) (y + ζ + κ + μ + ν + ξ) (h + j + k + m + z + ϕ), 1}
{q + w + (x + γ) (y + λ) (z + ψ), 0}
{q + v + w + (x + γ + θ) (y + ζ + λ) (m + z + ψ), 0}
{q + u + w + (x + γ + η) (y + λ + ξ) (k + z + ψ), 0}
{q + u + v + w + (x + γ + η + θ) (y + ζ + λ + ξ) (k + m + z + ψ), 0}
{q + t + w + (x + γ + ϵ) (y + λ + ν) (j + z + ψ), 0}
{q + t + v + w + (x + γ + ϵ + θ) (y + ζ + λ + ν) (j + m + z + ψ), 0}
{n + q + t + u + w + (x + β + γ + ϵ + η) (y + κ + λ + ν + ξ) (j + k + z + ϕ + ψ), 0}
{n + q + t + u + v + w + (x + β + γ + ϵ + η + θ) (y + ζ + κ + λ + ν + ξ) (j + k + m + z + ϕ + ψ), 1}
{l + p + q + w + (x + α + γ + δ) (y + ι + λ + μ) (h + z + ψ + ω), 0}
{l + p + q + v + w + (x + α + γ + δ + θ) (y + ζ + ι + λ + μ) (h + m + z + ψ + ω), 0}
{l + p + q + u + w + (x + α + γ + δ + η) (y + ι + λ + μ + ξ) (h + k + z + ψ + ω), 0}
{l + p + q + u + v + w + (x + α + γ + δ + η + θ) (y + ζ + ι + λ + μ + ξ) (h + k + m + z + ψ + ω), 1}
{l + p + q + t + w + (x + α + γ + δ + ϵ) (y + ι + λ + μ + ν) (h + j + z + ψ + ω), 0}
{l + p + q + t + v + w + (x + α + γ + δ + ϵ + θ) (y + ζ + ι + λ + μ + ν) (h + j + m + z + ψ + ω), 1}
{l + n + p + q + t + u + w + (x + α + β + γ + δ + ϵ + η) (y + ι + κ + λ + μ + ν + ξ) (h + j + k + z + ϕ + ψ + ω), 1}
{l + n + p + q + t + u + v + w + (x + α + β + γ + δ + ϵ + η + θ) (y + ζ + ι + κ + λ + μ + ν + ξ) (h + j + k + m + z + ϕ + ψ + ω), 1}
```

Figure 7: Equations describing σ_4^5