Univerzita Karlova v Praze
Matematicko-fyzikální fakulta

DIPLOMOVÁ PRÁCE

Veronika Heglasová

Algebraicko-geometrické kódy a Gröbnerovy báze

Katedra algebry

Vedoucí diplomové práce: Mgr. Jan Šťovíček, Ph. D.

Studijní program: Matematika
Studijní obor: Matematické metody informační bezpečnosti

Praha 2013

I would like to thank my supervisor, RNDr. Jan Šťovíček, Ph.D., for his willing attitude and valuable comments and advices.

I would also like to thank my whole family, especially my parents, for their support during my university studies.

I declare that I carried out this master thesis independently, and only with the cited sources, literature and other professional sources.

I understand that my work relates to the rights and obligations under the Act No. 121/2000 Coll., the Copyright Act, as amended, in particular the fact that the Charles University in Prague has the right to conclude a license agreement on the use of this work as a school work pursuant to Section 60 paragraph 1 of the Copyright Act.

In ..... date ..... signature of the author

Název práce: Algebraicko-geometrické kódy a Gröbnerovy báze

Autor: Veronika Heglasová

Katedra: Katedra algebry

Vedoucí diplomové práce: Mgr. Jan Šťovíček, Ph.D., Katedra algebry

Abstrakt: V této diplomové práci představíme algebraicko-geometrické kódy (AG kódy). Kromě základních definicí a tvrzení z teorie algebraické geometrie a AG kódů popíšeme způsob kódování, těch které mají netriviální grupu permutačních automorfizmů, a dekódování jednobodových AG kódů. Taktéž uvedeme konkrétní významnou skupinu, Hermitovské kódy. Tyto jsou díky svým vlastnostem vhodným příkladem k demonstraci popsaných metod. V závěru práce předvedeme jak kódování, tak dekódování s využitím konkrétního kódu.

Klíčová slova: algebraicko-geometrické kódy, Gröbnerovy báze, BMS algoritmus, kódovaní AG kódů, dekódovaní jednobodových AG kódů

Title: Algebraic Geometry Codes and Gröbner Bases

Author: Veronika Heglasová

Department: Department of Algebra

Supervisor: Mgr. Jan Šťovíček, Ph.D., Department of Algebra

Abstract: In this master thesis we introduce algebraic geometry codes (AG codes). Besides basic definitions, properties and attributes of AG codes and algebraic geometry we show how to encode AG codes that has nontrivial Abelian group of permutation automorphisms and how to decode one-point AG codes. We also present Hermitian codes, which are example of one-point AG codes with nontrivial Abelian group of permutation automorphisms. We demonstrate the method for encoding and the method for decoding on specific Hermitian code.

Keywords: algebraic geometry codes, Gröbner basis, BMS algorithm, encoding of AG codes, decoding of one-point AG codes

Contents

Introduction

Theory of error–correcting codes investigates codes that enable communication over noisy channel. During the transmission of data some errors may occur. At first the codes need to detect these errors. Then the received word is decoded to a codeword. The decoding algorithm decodes the received word to the closest codeword. This technique gives an upper bound on the number of errors that can be corrected. The best codes for practical use are those with high number of correctable errors, small size of alphabet and high dimension.

In 1981 Valery Denisovich Goppa presented his discovery of relation between coding theory and algebraic geometry. It turns out, that this new class of codes has almost the highest number of correctable errors. In addition, this codes use smaller alphabet than Reed-Solomon codes to achieve the same number of correctable errors.

To make the thesis understandable for those who are not familiar with algebraic geometry we sum up all definitions and propositions from algebraic geometry, which are necessary to understand algebraic geometry codes, in the first chapter. The algebraic geometry codes and terminology of error correcting codes are presented in the second chapter.

To have a code convenient for practical use, there has to be efficient way to encode and decode. In the third chapter we introduce one method of encoding and one method of decoding of algebraic geometry codes. For both of these methods we need extensions of some algorithms. In 1965 Bruno Buchberger introduced theory of Gröbner basis for ideals. For purpose of encoding we will present extension of Gröbner basis for submodules. As decoding algorithm we present syndrome decoding of one point algebraic geometry codes. It is possible to decode only from syndromes that we can get from a received word, however this type of algorithm does not correct up to the half of the lower bound of the minimum distance (called *Feng-Rao distance* or *order distance*). We present a way to calculate unknown syndromes using majority voting. Then, using extension of Berlekamp-Massey algorithm to N dimensions, we can correct errors up to the half of Feng-Rao distance.

In the last chapter we present important class of algebraic geometry codes – Hermitian codes. Hermitian curves have the maximal number of affine points with respect to genus of curve. Hence the Hermitian codes have maximal possible length of codeword and that positively effects the number of correctable errors. We also present methods of encoding and decoding on example of Hermitian codes.

1. Algebraic Geometry

At first, we have to sum up some basic definitions from Algebraic Geometry. Throughout the thesis we assume that we have an arbitrary field called K and every ring is commutative.

1.1 Basics from Algebraic Geometry

All definitions and theorems in this chapter are taken from [Stic09].

Definition 1.1.1 (Local ring)**.** *R is a local ring if and only if there is a unique nonzero maximal ideal.*

A ring R is local if and only if $R \setminus R^*$ is nonzero ideal. Let us assume that R is principal domain, F is a quotient field of R and $M = aR$ is maximal ideal of R. Then for every $b \in F^*$ there exists unique $i \in \mathbb{Z}$, that $b \in a^i R^* = a^i R \setminus a^{i+1} R$. According to that we can define mapping

$$\begin{aligned} \nu : F &\rightarrow \mathbb{Z} \cup \{\infty\} \\ \nu(b) &= i \Leftrightarrow b \in a^i R \setminus a^{i+1} R \\ \nu(0) &= \infty. \end{aligned}$$

Definition 1.1.2 (Discrete valuation)**.** *Let F be a field. Then $\nu : F \rightarrow \mathbb{Z} \cup \{\infty\}$ satisfying*

1. *$\nu(xy) = \nu(x) + \nu(y)$, $\forall x, y \in F$;*
2. *$\nu(x + y) \geq \min\{\nu(x), \nu(y)\}$, $\forall x, y \in F$;*
3. *$\nu(x) = \infty \Leftrightarrow x = 0$;*
4. *$\nu(a) = 1$, $\forall a \in R$ that $R \setminus R^* = aR$.*

is discrete valuation.

Proposition 1.1.3.

$$\nu(x) \neq \nu(y) \Rightarrow \nu(x + y) = \min\{\nu(x), \nu(y)\}$$

Proof. W.l.o.g $\nu(x) < \nu(y)$. We assume that $\nu(x) < \nu(x + y)$.

$$\nu(x) = \nu(x + y - y) \geq \min\{\nu(x + y), \nu(-y)\}$$

and that is contradiction with our assumption because $\nu(-y) = \nu(y) > \nu(x)$. □

Definition 1.1.4 (Algebraic function field)**.** *For a field K let us have a field extension $K \subseteq F$, such that there exists an element $x \in F$ that is transcendental over K and $[F : K(x)] < \infty$. Then F/K is an algebraic function field. An algebraic closure $\tilde{K}$ of K is called field of constants.*

Definition 1.1.5 (Valuation ring of the function field)**.** *A valuation ring of the function field F/K is a ring $\mathcal{O} \subseteq F$ with the following properties:*

1. $K \subsetneqq \mathcal{O} \subsetneqq F$, *and*

2. $\forall z \in F$ *we have that* $z \in \mathcal{O}$ *or* $z^{-1} \in \mathcal{O}$.

If we consider $P = \mathcal{O} \setminus \mathcal{O}^*$, it is obviously nonempty subset of $\mathcal{O}$ (otherwise would be $\mathcal{O} = F$). For $x \in P$ and $z \in \mathcal{O}$ is $xz \in P$. In addition, for every $x, y \in P$ is $\frac{x}{y}$ or $\frac{y}{x}$ in $\mathcal{O}$. W.l.o.g we assume that $\frac{x}{y} \in \mathcal{O}$. Then

$$1 \in \mathcal{O} \Rightarrow \frac{x}{y} + 1 \in \mathcal{O} \Rightarrow x + y = y(\frac{x}{y} + 1) \in P.$$

Hence P is an ideal of $\mathcal{O}$. As proper ideal can not contain 1, P is unique maximal ideal.

If we have P we can uniquely determine

$$\mathcal{O}_P = \{z \in F; z^{-1} \notin P\}.$$

$\mathcal{O}_P$ is called the valuation ring of the place P.

Definition 1.1.6 (Place)**.** *A place P is every set that satisfies $P = \mathcal{O} \setminus \mathcal{O}^*$ for a valuation ring $\mathcal{O}$ of an algebraic function field F/K. A set of all places of F/K is denoted by $\mathbb{P}_{F/K}$.*

Let us have a field F and its valuation ring $\mathcal{O}$. If $\mathcal{O}$ is integral domain and there is a discrete valuation ν such that

$$\mathcal{O} = \{z \in F | \nu(z) \geq 0\},$$

then we say that $\mathcal{O}$ is *discrete valuation ring.*

For a place $P = \mathcal{O} \setminus \mathcal{O}^* = \{z \in F; \nu(z) > 0\}$, we consider

$$m = \min\{\nu(x), x \in P\}$$
$$a \in P, \nu(a) = m.$$

Hence $P \supseteq a\mathcal{O}$. Let us have $b \in P \setminus a\mathcal{O}$. Then

$$b\mathcal{O} \supsetneqq a\mathcal{O}$$

and

$$a = bo, o \notin \mathcal{O}^*.$$

However that means, that $\nu(o) > 0$ and $\nu(a) > \nu(b)$. That is a contradiction and it means that P is principal ideal of discrete valuation ring $\mathcal{O}$. In fact, the same proof we can get for every ideal of $\mathcal{O}$, so $\mathcal{O}$ is a principal domain. An element $t \in \mathcal{O}$ that $t\mathcal{O} = P$ is called *prime element.*

For every place $P \in \mathbb{P}_{F/K}$ and $t \in \mathcal{O}$, that is prime element of P we define a discrete valuation ν_P:

$$\nu_P(z) = \nu_P(t^i u) = i, \forall z \in F,$$

where $i \in Z, u \in \mathcal{O}^*$. This definition does not depend on the choice of t:

$$P = t\mathcal{O} = s\mathcal{O}, \text{ so } t = sw \text{ for some } w \in \mathcal{O}^* \text{ and } w^n u \in \mathcal{O}^*.$$

Every ν_P gives an alternative definition a of place and a valuation ring:

$$\mathcal{O}_P = \{z \in F, \nu_P(z) \geq 0\},$$
$$\mathcal{O}_P^* = \{z \in F, \nu_P(z) = 0\},$$
$$P = \{z \in F, \nu_P(z) > 0\}.$$

Example 1.1.7. *Let us have x transcendental over K. Then $K(x)/K$ is function field (of rational functions). For an irreducible polynomial $p(x) \in K[x]$ is*

$$\mathcal{O}_{p(x)} = \left\{ \frac{f(x)}{g(x)}; f(x), g(x) \in K[x], p(x) \nmid g(x) \right\}$$

valuation ring. Maximal ideal of $\mathcal{O}_{p(x)}$ is

$$P_{p(x)} = \left\{ \frac{f(x)}{g(x)} \in \mathcal{O}_{p(x)}; p(x) \mid f(x) \right\}.$$

It is clear that $p(x)$ is prime element of $P_{p(x)}$ and valuation related to $P_{p(x)}$ is

$$\nu_{P_{p(x)}}(z) = k \Leftrightarrow k = \max\{i \in \mathbb{Z} \cup \{0\}; p^i(x) \mid z\}.$$

In addition to $\mathcal{O}_{p(x)}$ there is another valuation ring

$$\mathcal{O}_\infty = \left\{ \frac{f(x)}{g(x)}; f(x), g(x) \in K[x], deg(f(x)) \leq deg(g(x)) \right\}$$

with maximal ideal

$$P_\infty = \left\{ \frac{f(x)}{g(x)} \in \mathcal{O}_\infty; deg(f(x)) < deg(g(x)) \right\}.$$

and related valuation

$$\nu_\infty \left(\frac{f(x)}{g(x)} \right) = deg(g(x)) - deg(f(x)).$$

Let us have a place $P \in \mathbb{P}_{F/K}$ and an element $z \in F$. We say, that P is a zero of z of order m if $v_P(z) = m > 0$ and it is a pole of z of order m if $v_P(z) = -m < 0$. If z is constant it does not have any poles or zeros.

Proposition 1.1.8. *Let F/K be a function field and let $P_1, \ldots, P_r$ be zeros of the element $x \in F$. Then*

$$\sum_{i=1}^{r} \nu_{P_i}(x) \cdot \deg(P_i) \leq [F : K(x)].$$

Proof. See [Stic09], Proposition 1.3.3. □

From Proposition 1.1.8 follows that every nonzero element $x \in F$ has only finitely many zeros. As we can apply the same proposition on x^{-1}, there is only finitely many poles of x.

Definition 1.1.9 (Residue class field and degree)**.** *Let $P \in \mathbb{P}_{F/K}$.*

- *$F_P := \mathcal{O}_P/P$ is the residue class field of P. The map $x \to x(P)$ from F to $F_P \cup \{\infty\}$ is called the residue class map with respect to P.*
- *$\deg(P) := [F_P : K]$ is called the degree of P.*

Places of degree one of rational function field $K(x)/K$ correspondent one-to-one to elements of $K \cup \infty$. Hence in algebraic geometry is $K(x)/K$ usually interpreted as projective line over K. In coding theory we use terminology that a place of degree one

$$P_\alpha = P_{x-\alpha}$$

is rational point.

Definition 1.1.10 (Divisor). *Free Abelian group with basis $\mathbb{P}_{F/K}$ is called a divisor group of F/K and it is denoted by $Div(F)$. The elements of $Div(F)$ are formal sum*

$$D = \sum_{P \in \mathbb{P}_{F/K}} a_P P \text{ with } a_P \in \mathbb{Z} \text{ and almost all } a_P = 0.$$

Two divisors are added coefficientwise.
The zero element of group is zero divisor with $a_P = 0, \forall P \in \mathbb{P}_{F/K}$.
A divisor with all $a_P \geq 0$ is called positive (or effective).
A divisor with exactly one nonzero coefficient a_P is called prime divisor.

Definition of a degree of a place can be used to define a degree of a divisor as

$$\deg(D) = \sum_{P \in \mathbb{P}_{F/K}} a_P \cdot \deg(P).$$

This gives us a homomorphism

$$Div(F) \to \mathbb{Z}.$$

As we mentioned before, every nonzero $z \in F$ has only finitely many zeros and poles. If we set $a_P = \nu_P(z)$ it satisfies condition that $a_P = 0$ for almost all P so

$$(z) := \sum_{P \in \mathbb{P}_{F/K}} \nu_P(z) P$$

is divisor. Divisors defined like that are called principal divisors. The set of principal divisors is subgroup of $Div(F/K)$ denoted by $Princ(F)$.

The factor group

$$Cl(F) := Div(F)/Princ(F)$$

is called the divisor class group of F/K.

Definition 1.1.11 (Equivalence relation and partial ordering). *Two divisors $D, Q \in Div(F)$ are equivalent ($D \sim Q$) if*

$$D = Q + (x)$$

for some $x \in F \setminus \{0\}$.
A partial ordering on $Div(F)$ is defined by

$$D \leq Q \Leftrightarrow a_P \leq b_P, \forall P \in \mathbb{P}_{F/K},$$

where $D = \sum a_P P$ and $Q = \sum b_p P$.

Definition 1.1.12 (Riemann-Roch space). *For a divisor $A \in Div(F)$ we define the Riemann-Roch space associated to A by*

$$\mathcal{L}(A) := \{x \in F, (x) \geq -A\} \cup \{0\}.$$

Let $A \in Div(F)$. Riemann-Roch space $\mathcal{L}(A)$ is a vector space over K and its dimension is denoted by $l(A)$.

Definition 1.1.13 (Genus and index of specialty). *The genus g of F/K is defined by*

$$g := \max\{\deg(A) - l(A) + 1, A \in Div(F)\}.$$

An integer

$$i(A) = l(A) + g - 1$$

is called index of specialty.

The genus of F/K is always non-negative integer.

Definition 1.1.14 (Adele). *An adele of F/K is a mapping*

$$f : \begin{cases} \mathbb{P}_{F/K} & \to F, \\ P & \to f(P), \end{cases}$$

such that $f(P) \in \mathcal{O}_P$ for almost all $P \in \mathbb{P}_{F/K}$. The valuation $\nu_P(x)$ is naturally extended to $Adele(F/K)$ by setting $\nu_P(f) = \nu_P(f_P)$, where $f_P = f(P)$ is the P-component of the adele f. The extended valuation is denoted by ϑ.

Let $A \in Div(F)$. Then we define

$$\mathcal{A}(A) = \{f \in Adele(F/K); \vartheta(f) + A \geq 0\}.$$

For every $x \in F$ and $P \in \mathbb{P}_{F/K}$ we have constant mapping $c_x(P) = x$, which is adele. It is very common to take c_x as element of F. That give us inclusion $F \subseteq Adele(F/K)$. Adeles are important structure in algebraic geometry with a lot of interesting properties.

Let $A, B \in Div(F/K), A \leq B$:

- $\mathcal{A}(A)$ is vector space over K and $\mathcal{A}(A) \cap F = \mathcal{L}(A)$,
- $\mathcal{A}(A) \subseteq \mathcal{A}(B)$,
- $\dim(\mathcal{A}(B)/\mathcal{A}(A)) = \deg(B - A)$.

Definition 1.1.15 (Weil differential). *A Weil differential is a linear form*

$$\omega : Adele(F/K) \to K,$$

that vanishes on $\mathcal{A}(A) + F$ for some divisor $A \in Div(F)$.

Notation:

- $\Omega_F := \{\omega \mid \omega \text{ is a Weil differential of } F/K\}$,
- $\Omega_F(A) := \{\omega \in \Omega_F \mid \omega \text{ vanishes on } \mathcal{A}(A) + F\}$,

- $M(\omega) := \{A \in Div(F) \mid \omega \in \Omega_F(A)\}$.

Proposition 1.1.16. *Ω_F is a one-dimensional vector space over F.*

Proposition 1.1.17. *For every nonzero Weil differential ω exists exactly one divisor $W = (\omega) \in M(\omega)$ that $A \leq W$ for all $A \in M(\omega)$.*

Definition 1.1.18 (Canonical divisor)**.** *A divisor W that is equal to (ω) for some $\omega \in \Omega_F, \omega \neq 0$ is called canonical.*

- (ω) is, in class group of F/K, uniquely determined divisor,
- ω vanishes on $\mathcal{A}((\omega)) + F$,
- if ω vanishes on $\mathcal{A}(A) + F$ for some divisor $A \in Div(F/K)$ then $A \leq (\omega)$,
- $(\omega) = \sum_{P \in \mathbb{P}_{F/K}} x_P P$, we set $\nu_P(\omega) := x_P$.

Theorem 1.1.19 (Riemann-Roch Theorem)**.** *Let F/K be a function field of genus g. Then we have:*

(i) For all divisors $A \in Div(F/K)$,

$$l(A) \geq \deg(A) + 1 - g.$$

(ii) There is an integer c, depending only on the function field F/K, such that

$$l(A) = \deg(A) + 1 - g,$$

whenever $\deg(A) \geq c$.

Proof. See [Stic09], Theorem 1.4.17. □

Theorem 1.1.20 (Alternative of Riemann-Roch Theorem)**.** *Let F/K be a function field of genus g, $A \in Div(F)$ and every $x \in F \setminus K$ is transcendental over K. If $l(A) \geq 2g - 1$ then $l(A) = \deg(A) + g - 1$.*

Now we just mention the basic knowledge about the extension of algebraic function field. For more information about this topic see [Stic09], Chapter 3. In the rest of this section we assume that K is algebraically closed and that K is full constant field in F, i.e. $\forall x \in F \setminus K$ is transcendental over K.

Definition 1.1.21. *We say that an algebraic function field F'/K' is a field extension of an algebraic function field F/K if $F \subseteq F'$ and $K \subseteq K'$. It is an algebraic extension if F' is an algebraic field extension of F.*

Definition 1.1.22. *Let F'/K' be an algebraic extension of F/K. We say that a place $P' \in \mathbb{P}_{F'/K'}$ is over a place $P \in \mathbb{P}_{F/K}$ if $P = P' \cap F$. We denote it by $P'|P$. In this case $\mathcal{O}_P = \mathcal{O}_{P'} \cap F$.*

Definition 1.1.23. *Let $P'|P$.*

- *Then there is a unique integer e that satisfies $\nu_{P'}(x) = e\nu_P(x), \forall x \in F$. An integer $e(P'|P) := e$ is called the ramification index.*

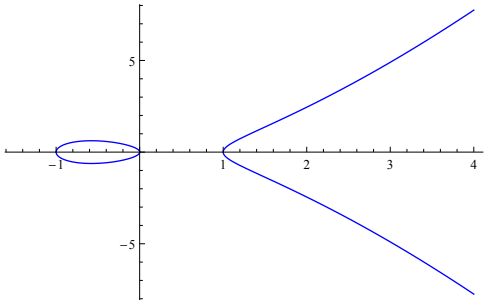


Figure 1.1: Elliptic curve $y^2 = x^3 - x$ over $\mathbb{R}$.

- *An integer* $f(P'|P) = [\mathcal{O}_{P'}/P' : \mathcal{O}_P/P]$ *is called the relative degree of* P' *over* P.

Example 1.1.24. *Let us have projective line over* $\mathbb{R}$*, i.e rational function field* $F/K = \mathbb{R}(x)/\mathbb{R}$*. We consider field extension*

$$F'/K = \mathbb{R}(x)[y]/\mathbb{R};\ y^2 = x^3 - x.$$

This extension correspondent to projection of elliptic curve $y^2 = x^3 - x$ *on axis* x*.*

We consider places of degree one–rational points. For every rational point P *on the projective line, there are at most two rational points* P' *on the elliptic curve such that* $P'|P$*. We consider the rational point* $P' \in \mathbb{P}_{F'/K}, P' = P'_{(0,0)}$ *which is over* P_0*:*

$$\nu_{P'_{(0,0)}}(x) = \nu_{P'_{(0,0)}}\left(\frac{y^2}{x^2-1}\right) = \nu_{P'_{(0,0)}}(y^2) - \nu_{P'_{(0,0)}}(x^2-1) = 2 - 0 = 2,$$
$$\nu_{P_0}(x) = 1$$

Hence $e(P'_{(0,0)}|P_0) = 2$*. There are other three points on projective line, that has ramification index 2–*P_{-1}, P_1 *and* P_∞*. The relative degrees are 1. On the other side, if we take for example the rational point* $P_2 \in \mathbb{P}_{F/K}$*, from the Figure 1.1 we see, that there are two points* $P'_1, P'_2 \in \mathbb{P}_{F'/K}$*, which are over* P_2*. The point* P_2 *is unramified and* $f(P'_i|P) = 1$*.*

Theorem 1.1.25. *Let* F'/K' *be an algebraic extension of* F/K*. Then for each* $P \in \mathbb{P}_{F/K}$ *there exists an integer* $m \geq 1$*, such that there is exactly* m *places* $P'_1, \ldots, P'_m \in \mathbb{P}_{F'/K'}$ *over* P*. Then*

$$[F' : F] = \sum_{i=1}^{m} e(P'_i|P) \cdot f(P'_i|P).$$

Proof. See [Stic09], Proposition 3.1.11 and Proposition 3.1.7(b). □

Proposition 1.1.26. *Let* F'/K' *be an algebraic extension of* F/K*. Then for every place* $P' \in \mathbb{P}_{F'/K'}$ *there is exactly one place* $P \in \mathbb{P}_{F/K}$*, such that* $P = P' \cap F$*. From the other side, for every* $P \in \mathbb{P}_{F/K}$ *there is finitely many places in* $\mathbb{P}_{F'/K'}$ *which are over* P*.*

According to Proposition 1.1.26 it makes sense if we define mapping

$$Div(F/K) \to Div(F'/K')$$

like this:

Definition 1.1.27 (Conorm)**.** *For a place $P \in \mathbb{P}_{F/K}$ we define mapping:*

$$\mathrm{Con} : P \to \sum_{P'|P} e(P'|P)P'.$$

The Con *can be extended to a homomorphism:*

$$\begin{array}{rccc} \mathrm{Con}: & Div(F/K) & \to & Div(F'/K') \\ & \sum_{P\in\mathbb{P}_{F/K}} a_P P & \to & \sum_{P\in\mathbb{P}_{F/K}} a_P \,\mathrm{Con}(P). \end{array}$$

Lemma 1.1.28. *Let F'/K' be an algebraic extension of F/K and let us have places $P' \in \mathbb{P}_{F'/K'}$ and $P \in \mathbb{P}_{F/K}$ that $P'|P$,. If $f(P'|P) < \infty$ then*

$$\deg(P')[K' : K] = f(P'|P)\deg(P).$$

Proposition 1.1.29. *Let F'/K' be an algebraic extension of F/K. For each $A \in Div(F/K)$ is*

$$\deg\left(\mathrm{Con}_{F'/F}(A)\right) = \frac{[F' : F]}{[K' : K]}\deg(A).$$

Proof. It is sufficient to prove it on the set of generators of $Div(F/K)$, i.e. on $\mathbb{P}_{F/K}$.
Let $P \in \mathbb{P}_{F/K}$ and we assume that $P'_1, \ldots, P'_m$ are all places lying over P. According to Lemma 1.1.28

$$\deg(P'_i) = \frac{f(P'_i|P)}{[K' : K]}\deg(P),$$

for every $i \in \{1, \ldots, m\}$. From Theorem 1.1.25 we get:

$$\deg\left(\mathrm{Con}_{F'/F}(P)\right) = \sum \frac{e(P'_i|P) \cdot f(P'_i|P)}{[K' : K]}\deg(P) = \frac{[F' : F]}{[K' : K]}\deg(P).$$

□

As we define the extension of algebraic function field, we can also define an extension of $Adele(F/K)$.

Definition 1.1.30. *Let*

$$Adele_{F'/F} := \{\alpha \in Adele(F'/K') \mid \alpha_{P'} = \alpha_{Q'} \text{ whenever } P' \cap F = Q' \cap F\}.$$

The trace mapping $F' \to F$ can be extended to an F-linear mapping

$$\mathrm{Tr}_{F'/F} : Adele_{F'/F} \to Adele(F/K)$$

by setting

$$(\mathrm{Tr}_{F'/F}(\alpha))_P := \mathrm{Tr}_{F'/F},$$

where P' is any place lying over P. Definition is correct because $\alpha_{P'} = \alpha_{Q'}$ whenever P' and Q' lie over P.
By [Stic09], Theorem 3.4.6 for every Weil differential ω of F there exists a unique Weil differential ω' of F'/K' such that

$$\mathrm{Tr}_{K'/K}(\omega'(\alpha)) = \omega(\mathrm{Tr}_{F'/F}(\alpha)),$$

for all $\alpha \in Adele_{F'/F}$.

Definition 1.1.31. *Using notation above we define Cotrace of ω in F'/F as*

$$\mathrm{Cotr}_{F'/F}(\omega) = \omega'.$$

1.2 Derivation and Differential

We describe the derivations and the differentials of an algebraic function field with analogous properties as derivations and differentials in mathematical analysis. We show how they are related to the Weil differentials. That gives us the tools to work with Weil differentials.

In Chapter 2 we will see how we can use Weil differentials to work with algebraic geometry codes.

In this section we assume that we have algebraic function field F/K as we defined in previous section. Throughout the section let K be perfect field and let K be full constant field in F.

Definition 1.2.1 (Derivation)**.** *Let M be a module over F. A mapping*

$$\delta : F \to M$$

is said to be derivation of F/K into M, if δ is K-linear and the product rule

$$\delta(u \cdot v) = u \cdot \delta(v) + v \cdot \delta(u)$$

holds for all $u, v \in F$.

Following lemma shows analogy to a derivation defined in mathematical analysis.

Lemma 1.2.2. *Let $\delta : F \to M$ be a derivation of F/K into M. Then we have:*

(i) $\delta(a) = 0$ *for each* $a \in K$.

(ii) $\delta(z^n) = nz^{n-1}$ *for* $z \in F$ *and* $n \geq 0$.

(iii) *If* $\mathrm{char}K = p > 0$, *then* $\delta(z^p) = 0$ *for each* $z \in F$.

(iv) $\delta(x/y) = (y\delta(x) - x\delta(y))/y^2$ *for* $x, y \in F$ *and* $y \neq 0$.

Definition 1.2.3 (Separating element)**.** *An element $x \in F$ is separating element of F/K if $F \supseteq K(x)$ is separable algebraic extension, i.e. for every element $a \in F$, the minimal polynomial of a over $K(x)$ has distinct roots.*

Lemma 1.2.4. *Suppose that x is a separating element of F/K and that δ_1, δ_2 are the derivations of F/K into M with $\delta_1(x) = \delta_2(x)$. Then $\delta_1 = \delta_2$.*

Proof. Let $f(x) = \sum a_i x^i \in K[x]$. From Lemma 1.2.2 follows that the derivation of $f(x)$ is

$$\delta_j(f(x)) = (\sum i a_i x^{i-1}) \cdot \delta_j(x), \text{ for } j \in \{1, 2\}.$$

Therefore the restrictions of δ_1 and δ_2 to $K[x]$ are equal. If restrictions to $K[x]$ are equal then using Lemma 1.2.2 *(iv)* we get equality of restrictions to $K(x)$. Now we consider an arbitrary element $y \in F$ and its minimal polynomial m_y over $K(x)$.

$$m_y(T) = \sum u_i T^i \in K(x)[T].$$

As $F \supseteq K(x)$ is separable extension, $\sum i u_i y^{i-1} \neq 0$.
For $j \in \{1, 2\}$:

$$\begin{aligned} 0 &= \delta_j(0) = \delta_j(\sum u_i y^i) = \sum (u_i \cdot \delta_j(y^i) + y^i \cdot \delta_j(u_i)) \\ &= \left(\sum i u_i y^{i-1}\right) \cdot \delta_j(y) + \sum y^i \cdot \delta_j(u_i), \\ \delta_j(y) &= \frac{-1}{\sum i u_i y^{i-1}} \cdot \sum y^i \cdot \delta_j(u_i). \end{aligned}$$

Since $u_i \in K(x)$ and we already proved equality of restrictions of δ_1, δ_2 to $K(x)$, we have that $\delta_1(y) = \delta_2(y)$. □

Definition 1.2.5 (Module of derivation)**.** *(a) Let x be a separating element of the function field F/K. The unique derivation $\delta_x : F \to F$ of F/K with the property $\delta_x(x) = 1$ is called the derivation with respect to x.*

(b) Let $\mathrm{Der}_F := \{\eta : F \to F | \eta$ *is a derivation of* $F/K\}$*. For* $\eta_1, \eta_2 \in \mathrm{Der}_F$ *and* $z, u \in F$ *we define*

$$(\eta_1 + \eta_2)(z) := \eta_1(z) + \eta_2(z) \text{ and } (u \cdot \eta_1)(z) := u \cdot \eta_1(z).$$

It is obvious that Der_F *is an F-module. It is called the module of derivation of F/K.*

The existence of δ_x follows from [Stic09], Proposition 4.1.4. (b):

If $x \in F$ is a separating element of F/K and $N \supseteq F$ is some field, then there exists a unique derivation $\delta : F \to N$ of F/K with property $\delta(x) = 1$.

Lemma 1.2.6. *Let x be a separating element of F/K. Then the following hold:*

(a) Der_F *is a one dimensional F-module.*

(b) (Chain rule) If y is another separating element of F/K, then

$$\delta_y = \delta_y(x) \cdot \delta_x. \tag{1.1}$$

(c) For $t \in F$ we have

$$\delta_x(t) \neq 0 \Leftrightarrow t \text{ is a separating element.}$$

Proof. (a) Consider the definition of δ_x. Then

$$(\eta(x) \cdot \delta_x)(x) = \eta(x) \cdot \delta_x(x) = \eta(x).$$

As x is a separating element, $\eta(x) \cdot \delta_x = \eta$.

(b) Set $\eta = \delta_y$ and it follows from *(a)*.

(c) If t is a separating element, then from the definition of δ_t and the chain rule we have

$$1 = \delta_t(t) = \delta_t(x) \cdot \delta_x(t).$$

Hence $\delta_x(t) \neq 0$.
Now we assume that t is not a separating element.
For K with characteristic 0 we have that $t \in K$ (otherwise t is transcendental over K so $[F : K(t)] < \infty$ and t is separating because every finite extension of perfect field is separable) and that implies $\delta_x(t) = 0$ from definition of derivation.
If $char(K) = p$, then $t \in F^p$ (for proof see [Stic09], Proposition 3.10.2(d)) so $t = u^p, u \in F$. Hence $\delta_x(t) = 0$ by Lemma 1.2.2.

□

Definition 1.2.7 (Differential). *(a) We define a relation $\sim$ on the set*

$$Z := \{(u, x) \in F \times F \mid x \text{ is separating}\}$$

by

$$(u, x) \sim (v, y) \Leftrightarrow v = u \cdot \delta_y(x). \tag{1.2}$$

(b) We denote the equivalence class of $(u, x) \in Z$ with respect to the above equivalence relation by udx and call it a differential of F/K. The equivalence class of $(1, x)$ is simply denoted by dx. Observe that by 1.2 is

$$udx = vdy \Leftrightarrow v = u \cdot \delta_y(x). \tag{1.3}$$

(c) Let

$$\Delta_F := \{udx \mid u \in F, \text{ and } x \in F \text{ is separating }\}$$

be the set of all differentials of F/K. We define the sum of two differentials $udx, vdy \in \Delta_F$ as follows: Choose a separating element z. Then

$$udx = (u \cdot \delta_z(x))dz \text{ and } vdy = (v \cdot \delta_z(y))dz,$$

by 1.3, and we set

$$udx + vdy := (u\delta_z(x) + v\delta_z(y))dz \tag{1.4}$$

This definition is independent of the choice of z by the chain rule. Likewise, we define

$$w \cdot (udx) := (wu)dx \in \Delta_F$$

for $w \in F$ and $udx \in \Delta_F$. In this manner, Δ_F becomes an F-module.

(d) For a non-separating element $t \in F$ we define $dt := 0$ (the zero element of Δ_F); thus we obtain a mapping

$$d : \begin{cases} F & \to \Delta_F, \\ t & \mapsto dt. \end{cases}$$

The pair (Δ_F, d) is called the differential module of F/K (for brevity we shall simply refer to Δ_F as the differential module of F/K).

Remark. *An useful proposition is proved by Stichtenoth in [Stic09], Proposition 6.4.1:*

If we consider function field $F = K(x, y)$ equal to quotient field of ring

$$\mathbb{F}_q/(y^q + c \cdot y - f(x)),$$

where $c \in K^*, f(x) \in K[x]$ and $q = p^k > 1$ for some prime p then the divisor of the differential dx is

$$(dx) = (2g - 2)P_\infty.$$

As in mathematical analysis also in algebraic geometry we can define a *limit* of a sequence and a *Cauchy sequence*. Let us have a field K and discrete valuation ν defined on K (we call pair (K, ν) a valued field).

Definition 1.2.8 (Limit and Cauchy sequence)**.** *We define x as a limit of a sequence $(x_n)_{n\geq 0}$ in field a K if for every $c \in \mathbb{R}$ there is an index $n_0 \in \mathbb{N}$ such that*

$$\nu(x - x_n) \geq c \text{ whenever } n \geq n_0.$$

We say that the sequence $(x_n)_{n\geq 0}$ is convergent.

As well we can say that $(x_n)_{n\geq 0}$ is a Cauchy sequence if for every $c \in \mathbb{R}$ there is an index $n_0 \in \mathbb{N}$ such that

$$\nu(x_n - x_m) \geq c \text{ whenever } n, m \geq n_0.$$

From the definition of discrete valuation follows that

$$\nu(x) = \infty \Leftrightarrow x = 0,$$

hence the definition of limit is really very close to one in mathematical analysis.

Equivalently, we can define a convergence of series. Let $(z_n)_{n\geq 0}$ be a sequence in a valued field (K, ν) and let s_m be its partial sums, i.e.

$$s_m := \sum_{i=0}^{m} z_i.$$

Then, as in mathematical analysis, we say that series is convergent if the sequence of its partial sums is convergent. In that case we write:

$$\sum_{i=0}^{\infty} z_i = \lim_{m\to\infty} s_m.$$

Definition 1.2.9 (Completion of valued field)**.** *Suppose that (K, ν) is a valued field. A completion of K is a valued field $(\hat{K}, \hat{\nu})$ with the following properties:*

(a) $K \subseteq \hat{K}$, *and* ν *is restriction of* $\hat{\nu}$ *to* K.

(b) $\hat{K}$ *is complete, i.e. every Cauchy sequence in* $\hat{K}$ *is convergent, with respect to the valuation* $\hat{\nu}$.

(c) K *is dense in* $\hat{K}$, *i.e. for each* $z \in \hat{K}$ *there is a sequence* $(x_n)_{n\geq 0}$ *in* K *with* $\lim_{n\to\infty} x_n = z$.

Proposition 1.2.10. *For each valued field there exists a completion. It is unique up to a field isomorphism.*

Proof. See [Stic09], Proposition 4.2.3. □

In an algebraic function field F/K we usually calculate with the discrete valuation ν_P related to a place P (as described in Section 1.1). Therefore it is convenient to have a completion of F with respect to the valuation ν_P. This completion is called the P-adic completion of F. We denote it by $(\hat{F}_P, \nu_P)$.

Theorem 1.2.11. *Let* $P \in \mathbb{P}_{F/K}$ *be a place of degree one and let* $t \in F$ *be a prime element of* P, *i.e.* $P = t\mathcal{O}_P$. *Then every element* $z \in \hat{F}_P$ *has a unique representation of the form*

$$z = \sum_{i=n}^{\infty} a_i t^i \text{ with } n \in \mathbb{Z} \text{ and } a_i \in K. \tag{1.5}$$

This representation is called the P*-adic power series expansion of* z *with respect to* t.

Proof. We have to prove the existence and the uniqueness. We start with the existence proof:
For $z \in \hat{F}_P$ we choose $n \in \mathbb{Z}$, that $n \leq \nu_P(z)$. F is dense in $\hat{F}_P$, so every element of $\hat{F}_P$ is a limit of some sequence in F. Therefore from the definition of a limit we can find an element $y \in F$ with $\nu_P(z-y) > n$.

$$\left.\begin{array}{l} \nu_P(y) \neq \nu_P(z) \text{ then } \nu_P(z-y) = \min\{\nu_P(z), \nu_P(y)\} \\ \nu_P(y) = \nu_P(z) \end{array}\right\} \Rightarrow \nu_P(y) \geq n.$$

Hence

$$v_P(yt^{-n}) \geq 0 \Rightarrow yt^{-n} \in \mathcal{O}_P.$$

As P is a place of degree one, we have $\mathcal{O}_P = K + P$, therefore there is an element $a_n \in K$ that $yt^{-n} - a_n \in P$.

$$\nu_P(z - a_n t^n) = \nu_P\left((z-y) + (y - a_n t^n)\right) > n.$$

In the same manner, we can find $a_{n+1}, a_{n+2}, \cdots \in K$ such that

$$\nu_P(z - \sum_{i=n}^{m} a_i t^i) > m \text{ for all } m \geq n.$$

This shows that

$$z = \sum_{i=n}^{\infty} a_i t^i.$$

We will prove the uniqueness by contradiction:
Assume that

$$z = \sum_{i=n}^{\infty} a_i t^i = \sum_{i=m}^{\infty} b_i t^i.$$

W.l.o.g. $n = m$ (if $n < m$ then $b_n = \cdots = b_{m-1} = 0$).
We assume that there is j with $a_j \neq b_j$, we choose a minimal one. Then for all $k > j$

$$\begin{aligned}\nu_P\left(\sum_{i=n}^{k} a_i t^i - \sum_{i=n}^{k} b_i t^i\right) &= \nu_P\left((a_j - b_j)t^j + \sum_{i=j+1}^{k} (a_i - b_i)t^i\right) \\ &= \min\{j, j+1, \ldots, k\} = j.\end{aligned}$$

Also

$$\begin{aligned}\nu_P\left(\sum_{i=n}^{k} a_i t^i - \sum_{i=n}^{k} b_i t^i\right) &= \nu_P\left(\sum_{i=n}^{k} a_i t^i - z + z - \sum_{i=n}^{k} b_i t^i\right) \\ &\geq \min\{\nu_P(z - \sum_{i=n}^{k} a_i t^i), \nu(z - \sum_{i=n}^{k} b_i t^i)\} \xrightarrow{k\to\infty} \infty.\end{aligned}$$

That is a contradiction with $j \in \mathbb{Z}$ for all $k > j$. □

From the definition of a differential and the definition of a derivation with respect to a separating element t we have:

$$\delta_t(y) = \frac{dy}{dt} \text{ for all } y \in F.$$

The quotient is always defined because

$$dz \neq 0 \Leftrightarrow z \text{ is separating.}$$

Proposition 1.2.12. *Let P be a place of F/K, $\deg(P) = 1$ and let $t \in F$ be a prime element of P. If $z \in F$ has the P-adic expansion $z = \sum_{i=n}^{\infty} a_i t^i$ with $a_i \in K$, then*

$$\frac{dz}{dt} = \sum_{i=n}^{\infty} i a_i t^{i-1}.$$

Proof. t is a separating element of F/K, because it has $\nu_P(t) = 1$ and every element whose valuation is not multiple of the characteristic of K is separating. For the proof of this proposition see [Stic09], Proposition 3.10.2(a).
From note above the proposition we have

$$\frac{dz}{dt} = \delta_t(z).$$

We define a mapping $\delta : \hat{F}_P \to \hat{F}_P$ by

$$\delta(\sum_{i=m}^{\infty} c_i t^i) := \sum_{i=m}^{\infty} i c_i t^{i-1}.$$

Obviously δ is K-linear. We have $z_1, z_2 \in \hat{F}_P$ and its P-adic expansions $\sum_{i=n}^{\infty} a_i t^i$ and $\sum_{j=m}^{\infty} b_j t^j$. W.l.o.g. $n = m$.

$$\left(\sum_{i=n}^{\infty} a_i t^i\right)\left(\sum_{j=n}^{\infty} b_j t^j\right) = \sum_{j=n}^{\infty}\sum_{i=n}^{i} nfty a_i b_j t^{i+j},$$

and δ is K-linear hence

$$\begin{aligned}
\delta(z_1 \cdot z_2) =& \sum_{j=n}^{\infty}\sum_{i=n}^{\infty}(i+j)a_i b_j t^{i+j-1} \\
=& \sum_{j=n}^{\infty}\sum_{i=n}^{\infty} i a_i b_j t^{i-1}t^j + \sum_{j=n}^{\infty}\sum_{i=n}^{\infty} j a_i b_j t^{j-1}t^i \\
=& \sum_{j=n}^{\infty} b_j t^j \sum_{i=n}^{\infty} i a_i t^{i-1} + \sum_{i=n}^{\infty} a_i t^i \sum_{j=n}^{\infty} j b_j t^{j-1} \\
=& z_2\delta(z_1) + z_1\delta(z_2).
\end{aligned}$$

δ satisfies the product rule $\Rightarrow$ δ is derivation.
$\delta(t) = 1 = \delta_t(t)$ and t is separating element $\overset{1.2.4}{\Longrightarrow} \delta(z) = \delta_t(z) = \frac{dz}{dt}$. □

Definition 1.2.13 (Residue)**.** *Suppose that P is a place of F/K of degree one and $t \in F$ is a prime element of P. If $z \in F$ has the P-adic expansion $z = \sum_{i=n}^{\infty} a_i t^i$ with $n \in \mathbb{Z}$ and $a_i \in K$ we define its residue with respect to P and t by*

$$\mathrm{res}_{P,t}(z) := a_{-1}.$$

As the definition of a limit also the definition of a residue is close to one in mathematical analysis (in this case in complex analysis), where the residue is defined as a coefficient a_{-1} of the Laurent series.

We set $i_{\min} := \min\{i | a_i \neq 0\}$.
If $i_{\min} < \infty$ then $\nu_P\left(\sum_{i=n}^{k} a_i t^i\right) = i_{\min}$ for all $k > i_{\min}$. As $z = \sum_{i=n}^{\infty} a_i t^i$, we can find k that

$$\nu_P(z - \sum_{i=n}^{k} a_i t^i) > i_{\min}.$$

Therefore

$$\nu_P(z) = \nu_P(z - \sum_{i=n}^{k} a_i t^i + \sum_{i=n}^{k} a_i t^i) = \min\{\nu_P(z - \sum_{i=n}^{k} a_i t^i), \nu_P(\sum_{i=n}^{k} a_i t^i)\} = i_{\min}.$$

In case $i_{\min} = \infty$, $a_i = 0$ for all i so $z = 0$ and $\nu_P(z) = \infty = i_{\min}$.
Conclusion of this is:

$$\nu_P(z) \geq 0 \Rightarrow \mathrm{res}_{P,t}(z) = 0.$$

Proposition 1.2.14. *Let $s, t \in F$ be a prime element of place $P, \deg(P) = 1$. Then*

$$\mathrm{res}_{P,s}(z) = \mathrm{res}_{P,t}\left(z \cdot \frac{ds}{dt}\right).$$

Proof. See [Stic09], Proposition 4.2.9. □

Definition 1.2.15. *Let $\omega \in \Omega_F$ be a differential and let $P \in \mathbb{P}_{F/K}$ be a place of degree one. Choose a prime element $t \in F$ of P and write $\omega = u\,dt$ with $u \in F$. Then we define the residue of ω at P by*

$$\mathrm{res}_P(\omega) := \mathrm{res}_{P,t}(u).$$

According to Proposition 1.2.14, the definition is independent of the choice of a prime element t.

1.3 Residue Theorem

In following section we describe relation between differentials and Weil differentials. Main goal of the section is Residue Theorem. From complex analysis we know Residue Theorem as:

Let us have an open set $\Omega \subset \mathbb{C}$, a finite set $M \subset \Omega$ and a cycle graph $\varphi : [a,b] \to \Omega \setminus M$. We assume that every function g, that is holomorphic over Ω, satisfies $\int_\varphi g = 0$. Then every function f, that is holomorphic over $\Omega \setminus M$, satisfies

$$\int_\varphi f = 2\pi\imath \sum_{a \in M} \mathrm{res}_a f \cdot \mathrm{ind}_\varphi a$$

where $\mathrm{ind}_\varphi a = \frac{1}{2\pi\imath} \int_\varphi \frac{1}{z-a} dz$.

Definition 1.3.1 (Local embedding and local component of Weil differential)**.** *Let $P \in \mathbb{P}_{F/K}$.*

(i) For $x \in F$ let $\iota(x) \in Adele(F/K)$ be the adele whose P-component is x, and the other components are 0.

(ii) For a Weil differential $\omega \in \Omega_{F/K}$ we define its local component

$$\omega_P : F \to K$$

by

$$\omega_P(x) := \omega(\iota(x)).$$

As a Weil differential is a K-linear mapping, clearly a local component ω_P is also a K-linear mapping.

Proposition 1.3.2. *Let $\omega \in \Omega_F$ and $\alpha \in Adele(F/K)$. Then $\omega_P(\alpha_P) \neq 0$ for at most finitely many places P, and*

$$\omega(\alpha) = \sum_{P \in \mathbb{P}_{F/K}} \omega_P(\alpha_P).$$

Proof. For $\omega = 0$ it is obviously valid.
We assume that $\omega \neq 0$. We set $W = (\omega) = \sum_{P \in \mathbb{P}_{F/K}} x_P P$ and

$$S_1 = \{P \in \mathbb{P}_{F/K} | x_P \neq 0\}$$
$$S_2 = \{P \in \mathbb{P}_{F/K} | \nu_P(\alpha_P) < 0\}$$

From the definition of a divisor is S_1 finite, and from the definition of an adele is S_2 finite ($\nu_P(\alpha_P) < 0 \Leftrightarrow \alpha_P \notin \mathcal{O}_P$). Hence $S = S_1 \cup S_2$ is a finite set.
Define adele β by

$$\beta_P := \begin{cases} \alpha_P & \text{for} \quad P \notin S, \\ 0 & \text{for} \quad P \in S. \end{cases}$$

Then $\beta \in \mathcal{A}(W)$, hence $\omega(\beta) = 0$. From the definition of β is

$$\alpha = \beta + \sum_{P \in S} \iota_P(\alpha_P).$$

so from the linearity of a Weil differential and Definition 1.3.1

$$\omega(\alpha) = \sum_{P \in S} \omega_P(\alpha_P).$$

For $P \notin S$ is $\iota_P(\alpha_P) \in \mathcal{A}(W) \Rightarrow \omega_P(\alpha_P) = 0$. □

Conclusion 1.3.3. *For every Weil differential ω is $\sum_{P \in \mathbb{P}_{F/K}} \omega_P(1) = 0$.*

Lemma 1.3.4. *For the function field $K(x)/K$ there exists a unique Weil differential η with divisor $(\eta) = -2P_\infty$ and local component $\eta_{P_\infty}(x^{-1}) = -1$ where P_∞ is pole of x in $K(x)$.*

Proof. We can choose Weil differential ω that $(\omega) = -2P_\infty$. From definition it vanishes on the space $\mathcal{A}(-2P_\infty)$.

$$-2P_\infty \geq -P \Rightarrow \omega \text{ does not vanish on } \mathcal{A}(-P_\infty).$$

From properties of adeles $\dim(\mathcal{A}(-P_\infty)/\mathcal{A}(-2P_\infty)) = 1$ and x has a pole of order one at $P_\infty \Rightarrow x^{-1}$ has a zero of order one at P_∞. Hence

$$\iota_{P_\infty}(x^{-1}) \in \mathcal{A}(-P_\infty) \setminus \mathcal{A}(-2P_\infty).$$

If

$$c := \omega_{P_\infty}(x^{-1}) \neq 0$$

then we can set $\eta := -c^{-1}\omega$ and η clearly has desired attributes.
If η^* has the same properties then $\eta - \eta^*$ vanishes on $\mathcal{A}(-P_\infty) \Rightarrow \eta - \eta^* = 0$. □

Definition 1.3.5. *Let F/K be an algebraic function field. We define a mapping*

$$\psi : \begin{cases} F & \to & \Omega_F, \\ x & \to & \psi(x) \end{cases}$$

as follows: if $x \in F \setminus K$ is a separating element of F/K we set

$$\psi(x) := \mathrm{Cotr}_{F/K(x)}(\eta),$$

where η is the Weil differential of $K(x)/K$ characterized in Lemma 1.3.4. For a non-separating element $x \in F$ we define

$$\psi(x) := 0.$$

$\psi(x)$ is called the Weil differential of F/K associated with x.

Lemma 1.3.6. *Let F/K be an algebraic function field with K algebraically closed. Suppose that x is a separating element of F/K, $P_0 \in \mathbb{P}_{K(x)/K}$ is unramified place in $F/K(x)$ and P_0 is not the pole of x in $K(x)$. Then for $u \in F$:*

$$\psi(x)_P(u) = \mathrm{res}_P(u\,dx) \quad \forall P \in \mathbb{P}_{F/K(x)} \quad \text{that } P|P_0.$$

Proof. See [Stic09], Lemma 4.3.5. □

Proposition 1.3.7. *Suppose that F/K is an algebraic function field over a perfect field K and $x \in F$ is a separating element. For every $y \in F$ we have*

$$\psi(y) = \frac{dy}{dx} \cdot \psi(x).$$

Conclusion 1.3.8. *Weil differential associated with x is derivation.*

Theorem 1.3.9. *Suppose that F/K is algebraic function field over a perfect field K and $x \in F$ is separating element. If P is a place of F/K of degree one and $\omega = z \cdot \psi(x) \in \Omega_F$ for some $z \in F$, the local component of ω at P is given by*

$$(z \cdot \psi(x))_P(u) = \mathrm{res}_P(uz\,dx).$$

Proof. We divide the proof into two parts. In the first part we will assume that K is algebraically closed and in the second part we will not have any additional assumption on K.
First part:
At first we get the places $P_1, P_2, \ldots, P_r \in \mathbb{P}_{F/K}$ such that $\mathcal{L}_1 = \mathcal{L}(P_1+P_2+\cdots+P_r)$ is strictly larger than $\mathcal{L}_2 = \mathcal{L}(P_2 + \cdots + P_r)$. Then from the definition of a Riemann-Roch space:

$$\forall t \in \mathcal{L}_1,\ \forall P \in \mathbb{P}_{F/K}\ \nu_P(t) \geq -1,$$

hence if an element has a pole in F then it is a pole of order one. Specially

$$\forall t \in \mathcal{L}_1 \setminus \mathcal{L}_2,\ 0 > \nu_{P_1}(t) \geq -1 \Rightarrow \nu_{P_1}(t) = -1$$

and P_1 is a pole of t of order one in F. If we set $T := t^{-1}$ then T is a prime element of P_1 so it is a separating element of F/K. Then $P_0 := P_1 \cap K(T) \in \mathbb{P}_{K(T)/K}$ is not a pole of T in $K(T)$ and

$$T \in P_0 \text{ and } \nu_{P_1}(T) = 1 \Rightarrow P_0 \text{ is unramified in } F/K(T)$$

Assumptions of Lemma 1.3.6 are satisfied so:

$$\begin{aligned}(z \cdot \psi(x))_{P_1}(u) &\overset{1.3.7}{=} \left(z \cdot \frac{dx}{dT} \cdot \psi(T)\right)_{P_1}(u) = \psi(T)_{P_1}\left(uz\frac{dx}{dT}\right) \\ &\overset{1.3.6}{=} \mathrm{res}_{P_1}\left(uz\frac{dx}{dT}dT\right) = \mathrm{res}_{P_1}(uz\,dx).\end{aligned}$$

Second Part:
We consider field extension $\bar{F} = F\bar{K}$, where $\bar{K}$ is algebraic closure of K. If $[\bar{K} : K] < \infty$, then according to Proposition 1.1.29, a place $P \in \mathbb{P}_{F/K}$ of degree

one has exactly one extension $\bar{P} \in \mathbb{P}_{\bar{F}/\bar{K}}$ and we can use what we already proved in the first part:

$$(z \cdot \psi(x))_P(u) = \psi(x)_P(zu) = \bar{\psi}(x)_{\bar{P}}(zu) = \mathrm{res}_{\bar{P}}(zu\, dx).$$

As $\bar{P}|P$ and P is unramified, every prime element of P in F is also a prime element of $\bar{P}$. Hence from Definition 1.2.13

$$\mathrm{res}_{\bar{P}}(zu\, dx) = \mathrm{res}_P(zu\, dx).$$

In case $[\bar{K} : K] = \infty$ we can use [Stic09], Corollary 3.6.5:

Let $P \in \mathbb{P}_{F/K}$ be a place of F/K of degree r and let $\bar{F} = F\bar{K}$ be the constant field extension of F/K with the algebraic closure $\bar{K}$ of K. Then

$$Con_{\bar{F}/F}(P) = \bar{P}_1 + \cdots + \bar{P}_r$$

with pairwise distinct places $\bar{P}_i \in \mathbb{P}_{\bar{F}/K}$.

Hence P is unramified place and the rest of the proof is the same as in case $[\bar{K} : K] < \infty$. □

Directly from Proposition 1.3.2, Conclusion 1.3.3 and Theorem 1.3.9 follow:

Theorem 1.3.10 (Residue Theorem)**.** *Let F/K be an algebraic function field, K is a perfect field. Let $\omega \in \Delta_F$ be a differential of F/K. Then $\mathrm{res}_P(\omega) \neq 0$ for at most finitely many places $P \in \mathbb{P}_{F/K}$ and*

$$\sum_{P \in \mathbb{P}_{F/K}} \mathrm{res}_P(\omega) = 0.$$

2. Algebraic Geometry Codes

2.1 Basics from error-correcting codes

Error-correcting codes enable communication over a noisy channel. Many communication channels are subjected to channel noise, and thus the errors may appear during a transmission from a source to a receiver. The errors can be detected. Moreover, if the amount of errors is limited (we will describe later what exactly mean limited), the errors can be corrected.

Let us have a finite field $\mathbb{F}_q$ with q elements and we consider the n-dimensional vector space $\mathbb{F}_q^n$ over $\mathbb{F}_q$. The elements of this vector space are n-tuples $(a_1, \ldots, a_n)$.

Definition 2.1.1 (Hamming distance and weight). *For two elements $a, b \in \mathbb{F}_q^n$ is Hamming distance a function*

$$d(a,b) := |\{i \mid a_i \neq b_i, i \in \{1, \ldots, n\}|.$$

The weight of an element a is defined as

$$w(a) := d(a,0) = |\{i \mid a_i \neq 0, i \in \{1, \ldots, n\}|.$$

Definition 2.1.2 (Linear code). *A code C over the alphabet $\mathbb{F}_q$ is an $[n,k]$-linear code if it is a linear subspace of $\mathbb{F}_q^n$ of dimension k. The elements of C are called codewords, n is the length of C (i.e. a length of a codeword) and k is the dimension of code.*
The minimum distance $d(C)$ of a code C is

$$d(C) := \min\{d(a,b) \mid a \neq b \text{ and } a, b \in C\} = \min\{w(c) \mid 0 \neq c \in C\}.$$

An $[n,k]$ code with minimal distance d is denoted by $[n,k,d]$.

We set

$$t := \left\lfloor \frac{d(C)-1}{2} \right\rfloor.$$

If $u \in \mathbb{F}_q^n$ and $d(u,c) \leq t$ for some $c \in C$ then c is the only codeword with $d(u,c) \leq t$. Therefore using code C we can uniquely correct all errors if number of errors is less than or equal to t.

Definition 2.1.3 (Generator matrix). *Let C be an $[n,k]$-code. A generator matrix of C is a $k \times n$ matrix whose rows are a basis of C (as $\mathbb{F}_q$-vector space).*

Definition 2.1.4 (Dual code). *If $C \subseteq \mathbb{F}_q^n$ is a code then*

$$C^{\perp} := \{u \in \mathbb{F}_q^n | < u, c >= \sum_{i=1}^{n} u_i c_i = 0 \text{ for all } c \in C\}$$

is called the dual code of C.

- $\dim(C) + \dim(C^{\perp}) = n$.

- A generator matrix of $C^{\perp}$ is called a parity check matrix for C. It satisfies

$$\forall c \in C;\ c \cdot G_{C^{\perp}}^{T} = \vec{0}.$$

Proposition 2.1.5 (Singleton Bound)**.** *For an $[n, k, d]$-code C holds*

$$d \leq n - k + 1.$$

Example 2.1.6 (Reed-Solomon codes)**.** *Let $\mathbb{F}_q^{\#} = \{\alpha, \alpha^2, \ldots, \alpha^{q-1}\}$ be a multiplicative group, where $q = p^r$ for a prime p and an integer r and α is a primitive element of $\mathbb{F}_q$. For an integer $k \leq n = (q-1)$ we consider the set*

$$L = \{f \in \mathbb{F}_q[x] \mid \deg(f) < k\}.$$

Then we define Reed-Solomon $[n, k]$-code as

$$RS_{q,k} = \{(f(\alpha), f(\alpha^2), \ldots, f(\alpha^{q-1}))|f \in L\}.$$

As each polynomial has at most $k-1$ zeros, from $d \geq n-(k-1)$ and the Singleton Bound follows that $RS_{q,k}$ reach the Singleton bound.

MDS codes (maximum distance separable codes) are codes with $d = n-k+1$. From the Singleton bound is obvious that if we want a code with high minimum distance we need a code with high length of the codewords. As a length of the codewords is limited by a size of the alphabet, the alphabet grows with it. One of the reason for the interest in algebraic geometry codes is that for the fix alphabet, they have longer length of the codewords than MDS codes. The penalty of this improvement is lower minimum distance. However we will see that this penalty is at most equal to the genus of the algebraic curve, that we used to construct the code.

2.2 Goppa Codes

Algebraic geometry codes (AG codes) are in general a linear codes constructed by using an algebraic curve. Such codes were introduced by Valerii Denisovich Goppa. That is why AG codes are often called Goppa codes. Some authors divide AG codes into two groups:

- geometric Reed-Solomon codes
- Goppa codes.

In this thesis we will also use this division as presented in [HøhoLintPell11].

Let $\mathcal{X}$ be a non-singular projective curve defined over a finite field $\mathbb{F}_q$. We consider the algebraic function field defined by $\mathcal{X}$ as quotient field of coordinate ring

$$\mathbb{F}[\mathcal{X}] = \mathbb{F}_q/(\mathcal{X}),$$

where $(\mathcal{X})$ denotes ideal generated by defining equation of the curve $\mathcal{X}$. We denote this algebraic function field by $\mathbb{F}(\mathcal{X})$.
In the following we use notation:

- $P_1, \ldots, P_n$ are distinct rational points on $\mathcal{X}$, i.e. places of degree one,
- divisor $D \in Div(\mathbb{F}(\mathcal{X}))$ is $D = P_1 + \cdots + P_n$,
- divisor $G \in Div(F\mathcal{X})$ is $G = \sum_{P \in \mathbb{P}_{\mathbb{F}(\mathcal{X})}} g_P \cdot P$, that $g_{P_i} = 0$ for $1 \leq i \leq n$.

Then:

Definition 2.2.1. *The linear code $C(D, G)$ of length n over $\mathbb{F}_q$ is defined by*

$$C(D, G) = \{(x(P_1), \cdots, x(P_n)) \mid x \in \mathcal{L}(G)\}.$$

Codes of this type are called geometric Reed-Solomon codes.

Example 2.2.2. *Consider Reed-Solomon code $RS_{q,k}$ and let L be as in Example 2.1.6. We set*

$$\mathcal{L} := \{f(x/y) \mid f \in L\}.$$

Then for the projective line $\mathcal{X} = \mathbb{P}^1(\bar{\mathbb{F}}_q)$ is $\mathcal{L}$ a set of polynomials that have a pole only at point in infinity P_∞ and order of a pole is less than k. Hence by setting $D = P_1 + \cdots + P_n$ where $P_i = (\alpha^i, 1)$ for a prime element α of $\mathbb{F}_q$ and $G = (k-1) \cdot P_\infty$ we constructed geometric RS-code

$$C(D, G) = \{(f(P_1), \cdots, f(P_n)) | f \in \mathcal{L}\} = \{(f(P_1), \cdots, f(P_n)) | f \in \mathcal{L}(G)\}$$

that is equivalent with $RS_{q,k}$.

Proposition 2.2.3. *$C(D, G)$ is an $[n, k, d]$-code with*

(i) $k = l(G) - l(G - D)$,

(ii) $d \geq n - \deg(G)$.

Proof. Consider a mapping

$$\begin{array}{rccc} e: & \mathcal{L}(G) & \to \mathbb{F}_q^n \\ & f & \to (f(P_1), \cdots, f(P_n)). \end{array}$$

(i) e is surjective from $\mathcal{L}(G)$ to $C(D, G)$. By linear algebra

$$l(G) = \dim(\mathrm{Im}(e)) + \dim(\mathrm{Ker}(e)) = k + \dim(\mathrm{Ker}(e))$$

and

$$\begin{aligned} \mathrm{Ker}(e) &= \{f | (f(P_1), \ldots, f(P_n)) = (0, \ldots, 0)\} \\ &= \{f | \nu_{P_i}(f) > 0, 1 \leq i \leq n\} \\ &= \mathcal{L}(G - D). \end{aligned}$$

(ii) $w(e(f)) = w \geq d$. Then there exist $n - w$ points that

$$\nu_{P_{i_j}}(f) > 0, \ 1 \leq j \leq n - w.$$

Hence $f \in \mathcal{L}\left(G - (P_{i_1} + \cdots + P_{i_{n-w}})\right)$.

$$\mathcal{L}\left(G - (P_{i_1} + \cdots + P_{i_{n-w}})\right) \neq \emptyset \Leftrightarrow \deg(G) - (n - w) \geq 0.$$

□

Theorem 2.2.4. *Let $C(D,G)$ be an $[n,k,d]$-code defined on curve $\mathcal{X}$ of genus g and $\deg(G) < n$. Then:*

(i) $k = l(G)$ and $d \geq n - k + 1 - g$.

(ii) A generator matrix of $C(D,G)$ is given by

$$M := \begin{pmatrix} f_1(P_1) & \dots & f_1(P_n) \\ \vdots & \vdots & \vdots \\ f_k(P_1) & \dots & f_k(P_n), \end{pmatrix}$$

where $f_1, \dots, f_k$ is an $\mathbb{F}_q$-basis of $\mathcal{L}(G)$.

- *Specially if $\deg(G) \geq 2g-1$ then $k = deg(G) + 1 - g$.*

Proof. (i) If $deg(G) < n$ then $deg(G - D) < 0$ and $l(G - D) = 0$. Hence $k = l(G)$. By Riemann-Roch Theorem 1.1.19

$$k = l(G) \geq deg(G) + 1 - g$$

and by Proposition 2.2.3

$$d \geq n - deg(G) \geq n - k + 1 - g.$$

(ii) Let $\bar{m_1}, \dots, \bar{m_k}$ be rows of M. We assume that $\sum_{i=1}^{k} a_i \cdot \bar{m_i} = \vec{0}, a_i \in \mathbb{F}_q$. Then

$$\sum_{i=1}^{k} a_i \cdot f_i(P_1) = \dots = \sum_{i=1}^{k} a_i \cdot f_i(P_n) = 0,$$

that implies $\sum_{i=1}^{k} a_i \cdot f_i \in \mathcal{L}(G - D)$ and so $a_i = 0, \forall i$. The rows of M are linearly independent over $\mathbb{F}_q$, so M is generator matrix.

(iii) follow directly from (i) and Theorem 1.1.20.

□

Remark. *Putting together Singleton bound and Theorem 2.2.4 we get*

$$n - k + 1 - g \leq d \leq n - k + 1.$$

Therefore for curves with genus $g = 0$ is $C(D,G)$ MDS code. Otherwise we construct code with almost maximum d, the penalty that we have to pay is g.

Definition 2.2.5. *A linear code $C^*(D,G)$ of length n over $\mathbb{F}_q$ is defined by*

$$C^*(D,G) = \{(\mathrm{res}_{P_1}(\omega), \cdots, \mathrm{res}_{P_n}(\omega)) \mid \omega \in \Omega(G - D)\}.$$

the codes of this type are called geometric Goppa codes.

Proposition 2.2.6. *$C^*(D,G)$ is an $[n,k^*,d^*]$-code defined on curve of genus g. Then*

- *$k^* = i(G - D) - i(G)$,*

- $d^* \geq deg(G) - 2g + 2$.

Specially if $deg(G) \geq 2g - 1$ *then* $k^* \geq n + g - 1 - deg(G)$ *with equality in case* $deg(G) < n$.

Proof. Consider a mapping

$$\begin{aligned} \text{Res} : \Omega(G - D) &\rightarrow C^*(D, G) \\ \omega &\rightarrow (res_{P_1}(\omega), \ldots, res_{P_n}(\omega)). \end{aligned}$$

Res is a surjective linear mapping. As $\omega \in \Omega(G - D) \Leftrightarrow \nu_P(\omega) \geq \nu_P(G - D)$:

$$\begin{aligned} \nu_{P_i}(\omega) &\geq -1 \quad \forall i \in \{1, \ldots, n\} \\ \nu_{P_i}(\omega) &\geq 0 \quad \omega \in \Omega(G), \forall i \in \{1, \ldots, n\} \end{aligned}$$

so

$$\omega \in \Omega(G) \Leftrightarrow (res_{P_1}(\omega), \ldots, res_{P_n}) = (0, \ldots, 0)$$

and $Ker(Res) = \Omega(G)$. Using linear algebra $k^* = i(G - D) - i(G)$.
Now consider a codeword $c^*(\omega)$ of a weight w. Then

$$\omega \in \Omega(G - (D - \sum_{j=1}^{n-w} P_{i_j}))$$

by previous ideas. Then

$$\Omega(G - (D - \sum_{j=1}^{n-w} P_{i_j})) \neq 0 \Rightarrow deg\left(G - (D - \sum_{j=1}^{n-w} P_{i_j})\right) \leq 2g - 2$$

according to Theorem 1.1.20. Hence

$$\begin{aligned} 2g - 2 \geq deg(G) - (n - (n - w)) = deg(G) - w, \\ d^* \geq w \geq deg(G) - 2g + 2. \end{aligned}$$

In case $deg(G) > 2g - 2$ is $i(G) = 0$ by Theorem 1.1.20 and $k^* = i(G - D)$. In addition if $deg(G) < n$ then $l(G - D) = 0$ and $k^* = n + g - 1 - deg(G)$ from definition of index of specialty. □

The lower bounds for minimum distances d and d^* are called Goppa distance of AG code.

Theorem 2.2.7. *The codes* $C(D, G)$ *and* $C^*(D, G)$ *are dual codes.*

Proof. According to Proposition 2.2.3 and Proposition 2.2.6

$$\begin{aligned} k + k^* =& l(G) - l(G - D) + i(G - D) - i(G) \\ =& l(G) - l(G - D) + l(G - D) - \deg(G - D) - \\ & 1 + g - l(G) + \deg(G) + 1 - g \\ =& \deg(D) = n. \end{aligned}$$

Let $c = e(f) \in C(D, G)$ for some $f \in \mathcal{L}(G)$ and $c^* = Res(\omega) \in C^*(D, G)$ for some $\omega \in \Omega(G - D)$. Consider the divisor $(f\omega)$:

$$(f\omega) = (f) + (\omega) \geq (-G) + (G - D) = (-D),$$

so $f\omega \in \Omega(-D)$. This implies that $f\omega$ can have a pole only in $P_1, \ldots, P_n$ and it would be a pole of order one. For t_i a prime element of P_i we consider the P_i-adic expansion of f and ω.

$$\left.\begin{array}{rcl} f & = & \sum_{k=0}^{\infty} a_k \cdot t_i^k \\ \omega = z\, dt_i;\ z & = & \sum_{k=-1}^{\infty} b_k \cdot t_i^k \end{array}\right\} \mathrm{res}_{P_i}(f\omega) = a_0 \cdot b_{-1} = f(P_i)\mathrm{res}_{P_i}(\omega).$$

Using Residue Theorem 1.3.10 we get

$$< c, c^* >= \sum_{i=1}^{n} f(P_i)\mathrm{res}_{P_i}(\omega) = 0.$$

□

From previous Theorem we see dual codes of geometric Reed-Solomon codes are Goppa codes. In practical situations is dual code often use to decide whether the received word is or is not an element of the code. Moreover it could be used in decoding algorithm. Therefore the following proposition could be very useful:

Proposition 2.2.8. *Let η be a Weil differential with a simple poles at the P_i and $\mathrm{res}_{P_i}(\eta) = 1$ for $i = 1, \ldots, n$. Then*

$$C^*(D, G) = C(D, D - G + (\eta)).$$

Proof. η has a simple pole at the $P_i \Rightarrow \nu_{P_i}(\eta) = -1$. Then $(\eta) = \sum_P n_P \cdot P$ with $n_{P_1} = \cdots = n_{P_n} = -1 \Rightarrow \nu_{P_i}(D - G + (\eta)) = 0$. Hence $C\,(D, D - G + (\eta))$ is properly defined code.
Consider a map

$$\begin{array}{rccc} \alpha: & \mathcal{L}(D - G + (\eta)) & \to & \Omega_F(G - D) \\ & x & \to & x\eta. \end{array}$$

At first we have to check if α maps $\mathcal{L}(D - G + (\eta))$ into $\Omega_F(G - D)$:

$$(x\eta) = (x) + (\eta) \geq -D + G - (\eta) + (\eta) = -D + G \Rightarrow x\eta \in \Omega(G - D).$$

Using the same ideas as in proof of Theorem 2.2.7, for $x \in \mathcal{L}(D - G + (\eta))$ we have

$$\mathrm{res}_{P_i}(x\eta) = x(P_i)\mathrm{res}(\eta) = x(P_i).$$

Therefore if α is an isomorphism then $C^*(D, G) = C\,(D, D - G + (\eta))$.
α is obviously injective. To prove, that it is surjective we have check if for every $\omega \in \Omega_F(G - D)$ there is a $x \in \mathcal{L}(D - G + (\eta))$ that $\omega = x\eta$. From Proposition 1.1.16 we see that $\omega = x\eta$ for some $x \in F = \mathbb{F}_q(\mathcal{X})$ and

$$G - D \geq (\omega) = (x\eta) = (x) + (\eta) \Rightarrow x \in \mathcal{L}(D - G + (\eta)).$$

□

3. Encoding and Decoding

For a code to be convenient for practical use, there should be efficient way how to encode and decode. In the following chapter we introduce one method for encoding and one method for decoding. However before we actually introduce the method, we need to describe necessary algorithm.

3.1 Gröbner basis

Gröbner basis is useful algebraic tool introduced by Bruno Buchberger. It is used to solve the ideal and the radical membership problem, the ideal equality problem, the algebraic equations and they provide a basis for a vector space $K[x]/I$ over K. In this section we describe how we can construct a systematic encoder for AG-codes using a Gröbner basis. The most of the definitions and theorems are taken from [Wink96] and [Mora09].

Before we can describe the Gröbner basis we need to define *reduction relation.*

Definition 3.1.1 (Reduction relation)**.** *Let M be a set and $\rightarrow$ a binary relation on M. $\rightarrow$ is a reduction relation and we say that a reduces to b if $(a, b) \in \rightarrow$. We will use notation $a \rightarrow b$.*

The basic attributes of reduction relation:

- composition: $a \rightarrow\rightarrow' b \Leftrightarrow \exists c \in M$ that $a \rightarrow c \rightarrow' b$,
- inverse relation: $a \rightarrow^{-1} b \Leftrightarrow b \rightarrow a$,
- i-th power: $a \rightarrow^i b \Leftrightarrow \exists c_1, \ldots, c_{i-1} \in M$ that $a \rightarrow c_1 \rightarrow \cdots \rightarrow c_{i-1} \rightarrow b$,
- symmetric closure: $a \leftrightarrow b \Leftrightarrow a \rightarrow b$ and $b \rightarrow a$,
- transitive closure: $\rightarrow^+ := \bigcup_{i=1}^{\infty} \rightarrow^i$,
- reflexive-transitive closure: $\rightarrow^* := \bigcup_{i=0}^{\infty} \rightarrow^i$,
- reflexive-transitive-symmetric closure: $\leftrightarrow^*$.

The relation of reduction is analogous with division of polynomials. Hence it is natural to say, that a is reducible if there exists $b \in M$ such that a reduces to b. We say, that b is normal form of a, if b is irreducible and a is reduced to b. This relation is denoted by

$$b = \underline{a}.$$

As for polynomials we have a common multiply and a common divisor, in terminology of reduction relation we define common successor

$$a \downarrow b \Leftrightarrow \exists c \in M \text{ that } a \rightarrow c \leftarrow b$$

and common predecessor

$$a \uparrow b \Leftrightarrow \exists c \in M \text{ that } a \leftarrow c \rightarrow b.$$

We declare a commutative polynomial ring $K[x_1, \ldots, x_n]$ by $K[X]$ and a monoid of power products $x_1^{i_1} \ldots x_n^{i_n}$ by $[X]$. The unit element in this monoid is $1 = x_1^0 \ldots x_n^0$. On $[X]$ we define term ordering that is compatible with the monoid structure:

- $1 < t, \forall t \in [X] \setminus 1$;
- $s < t \Rightarrow su < tu, \forall s, t, u \in [X]$.

Analogously we can define term ordering on $[X]$ by a total ordering on $\mathbb{N}^n$. In general we consider that $(0, \ldots, 0) \in \mathbb{N}^n$.

- $(0, \ldots, 0) < (a_1, \ldots, a_n), \forall (a_1, \ldots, a_n) \in \mathbb{N}^n$,
- $(a_1, \ldots, a_n) < (b_1, \ldots, b_n) \Rightarrow (a_1, \ldots, a_n) + (c_1, \ldots, c_n) < (b_1, \ldots, b_n) + (c_1, \ldots, c_n), \forall (a_1, \ldots, a_b), (b_1, \ldots, b_n), (c_1, \ldots, c_n) \in \mathbb{N}^n$.

Let $f \in K[X], f = \sum_{i=1}^{k} a_i x_1^{i_1} \ldots x_n^{i_n}$. Then the leading exponent of f is

$$\mathrm{le}(f) := \max_{<}\{(i_1, \ldots, i_n) \mid a_i \neq 0\},$$

the leading term of f is

$$\mathrm{lt}(f) := x_1^{i_1} \ldots x_n^{i_n}, \text{ that } (i_1, \ldots, i_n) = \mathrm{le}(f),$$

and leading coefficient $\mathrm{lc}(f)$ is coefficient of $\mathrm{lt}(f)$ in f. Finally a support of f is

$$\mathrm{supp}(f) = \{(i_1, \ldots, i_n) \mid a_i \neq 0\}.$$

A total ordering on a commutative polynomial ring $K[X]$ induced by a term ordering on $[X]$ is defined as
$\forall f, g \in K[X] \setminus 0$

1. $0 < f$;
2. in case $\mathrm{le}(f) \neq \mathrm{le}(g)$: $f < g \Leftrightarrow \mathrm{le}(f) < \mathrm{le}(g)$
3. in case $\mathrm{le}(f) = \mathrm{le}(g)$: $f' := f - \mathrm{lc}(f) \cdot \mathrm{lt}(f), g' := g - \mathrm{lc}(g) \cdot \mathrm{lt}(g)$ and $f < g \Leftrightarrow f' < g'$

Example 3.1.2. *Lexicographical ordering is*

$$(a_1, \ldots, a_n) < (b_1, \ldots, b_n) \Leftrightarrow \exists i, a_i < b_i \text{ and } a_j = b_j \forall j > i.$$

Hence

$$1 < x_1 < x_1^2 < \cdots < x_2 < x_2 x_1 < x_2 x_1^2 < \cdots < x_2^2 < \ldots.$$

Graded reverse lexicographical ordering (grevlex) is

$$\begin{aligned}(a_1, \ldots, a_n) < (b_1, \ldots, b_n) \Leftrightarrow & a_1 + \cdots + a_n < b_1 + \cdots + b_n \\ & a_1 + \cdots + a_n = b_1 + \cdots + b_n \text{ and} \\ & \exists i, a_i < b_i, a_j = b_j \forall j > i.\end{aligned}$$

Hence

$$1 < x_1 < x_2 < \cdots < x_n < x_1^2 < x_1 x_2 < \cdots < x_n^2 < \ldots.$$

Definition 3.1.3 (Reduction with respect to subset). *Let us have polynomials* $f, g, h \in K[X], F \subseteq K[X]$. *We say that* g *reduces to* h *w.r.t.* f*:*
$g \to_f h \Leftrightarrow \exists s, t \in [X]$ *that* s *has nonzero coefficient* c *in* g, $s = lt(f) \cdot t$ *and*

$$h = g - \frac{c}{lc(f)} \cdot t \cdot f.$$

We say that g *reduces to* h *w.r.t.* $F \Leftrightarrow \exists f \in F$ *such that* $g \to_f h$.

Definition 3.1.4 (Church-Rosser property). *The reduction relation* $\to$ *has the Church–Rosser property if it satisfies*

$$a \leftrightarrow^* b \;\Rightarrow\; a \downarrow_* b.$$

Definition 3.1.5 (Gröbner basis). *A subset* F *of* $K[X]$ *is a Gröbner basis for* $< F >$ *if* $\to_F$ *has the Church-Rosser property.*

This definition is more convenient if we want to prove attributes of the Gröbner bases using attributes of reduction relation. The other point of view is to define a Grobner basis as following:

Definition 3.1.6 (Equivalent definition). *A subset* $F = \{f_1, \ldots, f_k\}$ *of* $K[X]$ *is a Gröbner basis of ideal* $I \subset K[X]$ *if*

$$< lt(f_1), \ldots, lt(f_k) > = < \{lt(f) | f \in I\} > .$$

In the following we show the most important attribute of Gröbner basis, which provide the way how to check if the set is a Gröbner basis of an ideal that generates.

Definition 3.1.7 (Critical pairs and S-polynomial). *Let us have nonzero polynomials* $f, g \in K[X]$ *and* $t = \mathrm{lcm}(lt(f), lt(g))$. *Then*

$$cp(f, g) = \left(t - \frac{1}{lc(f)} \cdot \frac{t}{lt(f)} \cdot f, t - \frac{1}{lc(g)} \cdot \frac{t}{lt(g)} \cdot g \right)$$

is the critical pair of f *and* g. *The difference of the elements of* $cp(f, g)$ *is the S-polynomial* $S(f, g)$ *of* f *and* g.

Theorem 3.1.8 (Buchberger's criterion). *Let* F *be a subset of* $K[X]$.

(i) F *is a Gröbner basis if and only if* $g_1 \downarrow_F^* g_2$ *for all critical pairs* (g_1, g_2) *of elements of* F.

(ii) F *is a Gröbner basis if and only if* $S(f, g) \to_F^* 0$ *for all* $f, g \in F$.

Proof. See [Wink96], Theorem 8.3.1. □

Buchberger's criterion also suggest an algorithm for constructing the Gröbner basis. As $K[X]$ is noetherian ring, every ideal I in $K[X]$ has finite basis. Let B be a basis of I.

1. For all S-polynomials check if its normal form (w.r.t. B) is zero.
2. All nonzero normal forms add to basis B and check all new S-polynomial.

If we do this until all S-polynomials reduces to zero, we get the Gröbner basis. In case we have a Gröbner basis G for an ideal $I \subseteq K[X]$, then for each $f \in K[X]$

$$f \in I \Leftrightarrow f \rightarrow_G^* 0.$$

Now we consider a polynomial module $K[X]^m, m \in \mathbb{N}$ and its canonical basis $\{e_1, \ldots, e_m\}$.

According to the Hilbert's Basis Theorem, $K[X]^m$ is noetherian module. Hence every submodule $M \subseteq K[X]^m$ has finite basis. The question is if this basis can be transform to the Gröbner basis as in case $B \subseteq K[X]$. We need to extend few definitions.

If we combine total ordering on $K[X]$ with an ordering on canonical basis $\{e_1, \ldots, e_m\}$ then we get total ordering on $K[X]^m$, i.e. for $f, g \in K[X]^m$:

$$f = \sum_{i=1}^{m} f_i e_i,\ g = \sum_{i=1}^{m} g_i e_i, \text{ where } f_i, q_i \in K[X]$$

and

$$e_f = \max\{e_i | f_i \neq 0\},$$
$$e_g = \max\{e_i | g_i \neq 0\} \text{ with respect to ordering on canonical basis.}$$

Then

$$f \leq_T g \Leftrightarrow e_f < e_g, \text{ or}$$
$$e_f = e_g \text{ and } f_{e_f} \leq_T g_{e_g}.$$

This type of ordering is called position over term ordering.

We say that m is monomial in $K[X]^m$ if $m = te_i$ for some $t \in [X]$ and $e_i \in \{e_1, \ldots, e_m\}$. Hence

$$[X]^m = \{te_i, t \in [X], 1 \leq i \leq m\}.$$

Then every element $f \in K[X]^m$ can be written as

$$f = \sum_{i=1}^{m} \sum_{j} c_{i,j} t_{i,j} e_i = \sum_{i=1}^{m} \sum_{j} c_{i,j} m_{i,j},\ t_{i,j} \in [X], c_{i,j} \in K.$$

and we define:

- $\mathrm{lt}(f) := \max_{<}\{m_{i,j} | c_{i,j} \neq 0\}$,
- $\mathrm{lc}(f) := c_{i,j}$ that $m_{i,j} = \mathrm{lt}(f)$.

Definition 3.1.9 (Gröbner basis for submodule)**.** *Let M be a submodule of $K[X]^m$. Then a finite set of polynomials $G = \{g_1, \ldots, g_k\} \subset M$ is a Gröbner basis for M if the submodule generated by the leading terms of polynomials in M is equal to the submodule generated by the leading terms of polynomials in G, i.e.:*

$$< \{lt(m) | m \in M\} >=< lt(g_1), \ldots, lt(g_k) > .$$

Let $B = \{f_1, \ldots, f_k\}$ be a basis of a submodule M. If it is not the Gröbner basis, then there exists a polynomial $f_{k+1} \in M$ such that

$$\mathrm{lt}(f_{k+1}) \notin < \{\mathrm{lt}(m) | m \in M\} > .$$

We put $B_1 = B \cup \{f_{k+1}\}$. Like this, we can create an ascending chain

$$B = B_0 \subsetneqq B_1 \subsetneqq B_2 \subsetneqq \ldots$$

and a corresponding chain of the submodules generate by the leading terms

$$< \mathrm{LT}(B_0) > \subsetneqq < \mathrm{LT}(B_1) > \subsetneqq \ldots .$$

However this chain has to stop at some point, as $K[X]^m$ is noetherian module. Hence for every submodule M exists a Gröbner basis.

Let $G = \{g_1, \ldots, q_k\}$ be the Gröbner basis of a submodule M. Then

$$f \in M \Leftrightarrow f \to_G 0.$$

Definition 3.1.10. *Let $g \in K[X]^m$. Then*

$$lt(f) = m_f = t_{f,i} e_f, \;\; lt(g) = m_g = t_{g,i} e_g$$

for some $t_{f,i}, t_{g,i} \in [X]$. If $e_f = e_g = e$ then S-polynomial of f and g is defined as

$$S(f,g) := \frac{lcm(t_{f,i}, t_{g,i})}{t_{g,i} \cdot lc(g)} g - \frac{lcm(t_{f,i}, t_{g,i})}{t_{f,i} \cdot lc(f)} f,$$

otherwise is $S(f,g) = 0$.

As in previous case, also now is valid *Buchberger's criterion*, i.e.:

$$G \text{ is a Gröbner basis} \Leftrightarrow S(f,g) \to_G 0, \; \forall f, g \in G,$$

and that give us an intuitive version of Buchberger's algorithm for generating a Gröbner basis from some regular basis.

3.2 Systematic encoder

In this section we denote by $\mathcal{P}$ the polynomial ring in one variable and $\mathcal{P}^m$ is free module with standard basis $\{e_1, \ldots, e_m\}$.

At first we find some automorphism of a code, which maps the set of codewords to itself. We only consider the permutation automorphisms.

Let us have a linear code C that has a nontrivial Abelian group H of automorphisms. We can assume that the group is cyclic and σ is its generator.

Now we consider an action of H on the set of codewords. It divides positions of codewords to orbits $O_1, \ldots, O_m$. As H is cyclic, every orbit can be written as

$$O_i = \{c_{i,j}, j = 0, \ldots, |O_i|\}, \text{ where } c_{i,j+1} = \sigma(c_{i,j})$$

and index j is computed modulo $|O_i|$.

Let $N = \mathcal{P}^m/\langle (t^{|O_i|}-1)e_i; i = 1, \ldots, m\rangle$. The mapping

$$\begin{aligned} \Phi : C &\rightarrow N \\ (c_{i,j}) &\rightarrow \sum_{i=1}^{m} \left(\sum_{j=0}^{|O_i|-1} c_{i,j} t^j \right) e_i \mod \langle (t^{|O_i|}-1)e_i; i = 1, \ldots, m\rangle \end{aligned}$$

shows us how we can represent the code C as a subset of the quotient module N. As Φ is linear mapping, $\Phi(C)$ is a vector subspace of N. In addition for $c_{i,j} \in C$

$$\begin{aligned} t\Phi(c_{i,j}) &= \sum_{i=1}^{m} \left(\sum_{j=0}^{|O_i|-1} c_{i,j} t^{j+1} \right) e_i \\ &\overset{j \mod |O_i|}{\equiv} \sum_{i=1}^{m} \left(\sum_{j=0}^{|O_i|-1} c_{i,j-1} t^{j} \right) e_i \\ &\equiv \Phi(\sigma^{-1}(c_{i,j})) \in \Phi(C). \end{aligned}$$

Hence $\Phi(C)$ is a $\mathcal{P}$-submodule of N.

Now we consider a submodule $M(C) \subseteq \mathcal{P}^m$ that is preimage of $\Phi(C)$ under the mapping

$$\begin{aligned} \Pi : \mathcal{P}^m &\rightarrow N \\ M(C) &\rightarrow \Phi(C). \end{aligned}$$

Term module $[X]^m$ is divided into two groups with respect to an arbitrary term ordering $<$:

- module $R(M(C))$ generated by the set of leading terms of $M(C)$
- $I(M(C)) = [X]^m \setminus R(M(C))$.

The elements of $I(M(C))$ are irreducible with respect to the Gröbner basis of $M(C)$ and we called them standard terms. The elements of $R(M(C))$ are called nonstandard terms. Nonstandard terms correspond to codewords and standard terms are used to check parity.

The systematic encoder for code C:

1. Input: Gröbner basis G for the module $M(C)$, nonstandard terms m_i, information symbols c_i
2. $$\begin{aligned} f &:= \sum c_i m_i, \\ \underline{f} &:= \text{ normal form of } f \text{ with respect to } G, \\ c &:= f - \underline{f}. \end{aligned}$$
3. Output: A codeword c.

$\underline{c} = \underline{f - \underline{f}} = \underline{f} - \underline{f} = 0 \Rightarrow c \in M(C)$. Therefore c is the codeword of C. $\underline{f}$ contains only standard terms and $R(M(C)) \bigcap I(M(C)) = \emptyset$, hence coefficients of nonstandard terms (information symbols) remain unchanged, what means that the encoder is systematic.

From [Litt09], Theorem 1 follow how to get an automorphism of code $C(D, G)$:

Theorem 3.2.1. *Let $\mathcal{X}$ be a non-singular projective curve defined over a finite field $\mathbb{F}_q$. Let σ be an automorphism of the curve $\mathcal{X}$ that fixes divisors D and G. Then σ induces an automorphism of the code $C(D,G)$.*

Proof. σ is a regular mapping $\mathcal{X} \to \mathcal{X}$ and it has a regular inverse. Naturally σ induces an $\mathbb{F}_q$-automorphism Σ of the function field $\mathbb{F}(\mathcal{X})$ that maps $f \in \mathbb{F}(\mathcal{X})$ into $f \circ \sigma^{-1} \in \mathbb{F}(\mathcal{X})$. As G is fixed by σ then Σ maps $\mathcal{L}(G)$ to itself. Considering that $(\sigma^{-1}(P_1), \ldots, \sigma^{-1}(P_n)$ for $P_1 + \cdots + P_n = D$ is permutation of $(P_1, \ldots, P_n)$ (as σ fix D) we get that

$$(f(P_1), \ldots, f(P_n)) \to \big(f(\sigma^{-1}(P_1)), \ldots, f(\sigma^{-1}(P_n))\big)$$

define a permutation of the code $C(D,G)$. □

3.3 Berlekamp-Massey-Sakata algorithm

At the beginning of the section we fix some notation:

- $\leq_T$ denote a total ordering on $\mathbb{N}^n$,
- $\leq_P$ denote a partial ordering on $\mathbb{N}^n$, $p \leq_P q \Leftrightarrow p_i \leq q_i \forall i \{1, \ldots, n\}$,
- $\Sigma_p = \{x \in \mathbb{N}^n; x \geq_P p\}$,
- $\Sigma_p^q = \{x \in \mathbb{N}^n; p \leq_P x <_T q\}$,
- $\Gamma_p = \{x \in \mathbb{N}^n; x \leq_P p\}$,
- $0 = (0, \ldots, 0) \in \mathbb{N}^n$, e^i is i-th element of canonical basis of $\mathbb{N}^n$.

Definition 3.3.1 (n-dimensional array)**.** *An infinite n-dimensional array over a field K is a mapping u from $\mathbb{N}^n$ into K. u^p for $p \in \mathbb{N}^n$ denotes a partial array of u and $u^p = (u_q), q <_T p$.*

Example 3.3.2. *As a term ordering we use graded reverse lexicographical ordering. The partial array u^p of an $2-d$ array over $\mathbb{Z}_2$ for $p = (3,1)$ is given by table:*

$i \backslash j$	0	1	2	3
0	0	1	1	1
1	1	1	0	
2	0	0		
3	0			
4	1			

so $u^{(3,1)} = (0,1,1,0,1,1,0,0,0,1,1)$.

If we have the partial array u^p of the array u, then we usually want to find characteristic polynomial $f = \sum_{a \in \mathrm{supp}(f)} c_{f,a} X^a$ of u^p. It is a polynomial that generate u^p, i.e.:

$$u_b = -\frac{1}{c_{(f,d)}} \sum_{a \in \mathrm{supp}(f) \setminus \{d\}} c_{(f,a)} u_{a+b-d}$$

for each $b \in \Sigma^p_{\mathrm{le}(f)}$, so

$$f[u]_b = \sum_{a \in \mathrm{supp}(f)} c_{(f,a)} u_{a-b+d} = 0.$$

We consider f as valid characteristic polynomial also for $p <_T \mathrm{le}(f)$. The set of all characteristic polynomials (considering all partial arrays u^p, $p \in \mathbb{N}^n$) is an ideal $I(u)$ of the polynomial ring $K[X]$, the ideal is called characteristic ideal of u. The goal of Berlekamp-Massey-Sakata (BMS) algorithm is to find the set $F(p)$ of polynomials with minimal leading exponential (with respect to partial ordering) included in $I(u^p)$.

Let us assume that we have a fixed array u and its partial array u^p and a polynomial f, which is valid till $q <_T p$, i.e. $f[u]_a = 0, a \in \Sigma^q_{\mathrm{le}(f)}$ and $f[u]_q \neq 0$. At start we want to find a way how to generate a polynomial f^+ valid in $\Sigma^{q \oplus 1}_{\mathrm{le} f^+}$, where $q \oplus 1$ is the next point of q with respect to the term ordering.

Proposition 3.3.3. *Let us have $q >_T s$, a polynomial $f \in K[X]$ valid till q and a polynomial $g \in K[X]$ valid till s. If*

$$f[u]_q = d_f,\ le(f) = d$$
$$g[u]_s = d_g,\ le(g) = t$$
$$r = \max(d, q - s + t), i.e.\ r_i = \max(d_i, q_i - s_i + t_i)$$

Then

$$f^+ = X^{r-d} f - \frac{d_f}{d_q} X^{r-q+s-t} g$$

has $le(f^+) = r$ and is valid in $\Sigma^{q \oplus 1}_r$.

Proof. As $r - d + d = r >_T r - q + s - t + t = r - q + s$ we get $\mathrm{le}(f^+) = r$.

$$X^{r-d} f = X^{r-d} \sum_{a \in \mathrm{supp}(f)} c(f,a) X^a = \sum_{a \in \mathrm{supp}(f)} c(f,a) X^{a+r-d}$$
$$X^{r-q+s-t} g = X^{r-q+s-t} \sum_{a \in \mathrm{supp}(g)} c(g,a) X^a = \sum_{a \in \mathrm{supp}(g)} c(f,a) X^{a+r-q+s-t}$$

Thus

$$\begin{aligned} f^+[u]_b &= \sum_{a \in \mathrm{supp}(f)} c(f,a) u_{a+r-d+b-r} - \frac{d_f}{d_g} \sum_{a \in \mathrm{supp}(g)} c(g,a) u_{a+r-q+s-t+b-r} \\ &= \sum_{a \in \mathrm{supp}(f)} c(f,a) u_{a+b-d} - \frac{d_f}{d_g} \sum_{a \in \mathrm{supp}(g)} c(g,a) u_{a+b-q+s-t} \\ &= * \end{aligned}$$

$d \leq_P r \Rightarrow \Sigma^q_r \subseteq \Sigma^q_d$ and $\forall b \in \Sigma^q_r$ we have

$$q - s + t \leq_P r \leq_P b < q \Rightarrow t \leq_P b - q + s < s \Rightarrow b - q + s \in \Sigma^s_t$$

and

$$\begin{aligned} * =& 0 \text{ for } b \in \Sigma_r^q \\ =& d_f - \frac{d_f}{d_g} d_g = 0 \text{ for } b = q. \end{aligned}$$

□

Remark. *Value d_f is called a discrepancy of the polynomial f.*

Proposition 3.3.3 shows that next to the set of characteristic polynomials it is sufficient to keep a set of "ex-polynomials", i.e. polynomials that were valid till $s <_T q$. As we always want to find polynomial with minimal leading exponent we will keep set

$$G(q) = \{ \text{ ex-polynomials } g \text{ valid till } s <_T q, \text{ that } s - \mathrm{le}(g) \text{ is maximal } \} \cup \{0\}$$

and related set

$$C(q) = \{s - \mathrm{le}(g) | 0 \neq g \in G(q)\} \cup C_\infty.$$

C_∞ correspondents to $g = 0$ and it contains n infinite elements

$$(-1, \infty, \ldots, \infty), \ldots, (\infty, \ldots, \infty, -1).$$

If $s - \mathrm{le}(g)$ is infinite then $r_i = q_i + 1$ and $r_j = d_j, i \neq j$.

In the following proposition we describe condition given on the leading exponent of polynomials from $F(q \oplus 1)$

Proposition 3.3.4. *Let $le(f) = d$. If $f \in F(q)$ and $f[u]_q \neq 0$. Then there does not exist any $f^+ \in F(q \oplus 1)$ with $le(f^+) \leq_P q - d$. We say, that $q <_T p$ is first point, where f fails to be valid.*

Proof. For $q = d$ would be $\mathrm{le}(f^+) \leq_P 0$ so f^+ is constant polynomial and it is contradiction with minimality of f.

Let $d <_P q$. As $f \in F(q)$

$$\begin{aligned} -\frac{1}{c_{(f,d)}} \sum_{a \in \mathrm{supp}(f) \setminus \{d\}} c_{(f,a)} u_{a+b-d} = u_b, \forall b \in \Sigma_d^q \\ -\frac{1}{c_{(f,d)}} \sum_{a \in \mathrm{supp}(f) \setminus \{d\}} c_{(f,a)} u_{a+q-d} \neq u_q \end{aligned}$$

and $f^+ \in F(q \oplus 1), \mathrm{le}(f^+) = d^+$

$$-\frac{1}{c_{(f^+,d^+)}} \sum_{a \in \mathrm{supp}(f^+) \setminus \{d^+\}} c_{(f^+,a)} u_{a+b-d^+} = u_b, \forall b \in \Sigma_{d^+}^{q \oplus 1}.$$

We assume that $d^+ \leq_P q - d$ hence

$$\left.\begin{array}{ccccc} a+q-d & \geq_P & a+d^+ & \geq_P & d^+ \\ a+q-d & \leq_P & q & <_T & q \oplus 1 \end{array}\right\} \Rightarrow a + q - d \in \Sigma_{d^+}^{q \oplus 1}.$$

Therefore

$$
\begin{aligned}
&-\frac{1}{c_{(f,d)}} \sum_{a\in \mathrm{supp}(f)\setminus\{d\}} c_{(f,a)} u_{a+q-d} \\
&= -\frac{1}{c_{(f,d)}} \sum_{a\in \mathrm{supp}(f)\setminus\{d\}} c_{(f,a)} \left(-\frac{1}{c_{(f^+,d^+)}} \sum_{b\in \mathrm{supp}(f^+)\setminus\{d^+\}} c_{(f^+,b)} u_{b+(a+q-d)-d^+} \right) \\
&= -\frac{1}{c_{(f^+,d^+)}} \sum_{b\in \mathrm{supp}(f^+)\setminus\{d^+\}} c_{(f^+,b)} \left(-\frac{1}{c_{(f,d)}} \sum_{a\in \mathrm{supp}(f)\setminus\{d\}} c_{(f,a)} u_{a+(b+q-d^+)-d} \right) \\
&= *,
\end{aligned}
$$

considering

$$
\left.
\begin{array}{llll}
b+q-d^+ & \geq_P & b+d & \geq_P \quad d \\
b+q-d^+ & \leq_P & q &
\end{array}
\right\} \Rightarrow b+q-d^+ \in \Sigma_d^q.
$$

we get

$$
\begin{aligned}
* &= -\frac{1}{c_{f^+,d^+}} \sum_{b\in \mathrm{supp}(f^+)\setminus\{d^+\}} c_{(f^+,b)} u_{b+q-d^+} \\
&= u_q
\end{aligned}
$$

and it is a contradiction. □

Let us have a set

$$\Delta(q) = \bigcup_{c\in C(q),\ c \text{ is finite}} \Gamma_c.$$

Related to $F(q)$ we have the set $D(q) = \{\mathrm{le}(f), f \in F(q)\}$. According to Proposition 3.3.4 is

$$\Delta(q) \cap \left(\bigcup \Sigma_{d\in D(q)} \right) = \emptyset.$$

In fact, $\Delta(q)$ and $\left(\bigcup \Sigma_{d\in D(q)}\right)$ are not only disjoint sets. Union of this sets is the whole $\mathbb{N}^n$ (for proof see [Saka90]). Hence Proposition 3.3.3 gives a way how to upgrade the polynomials that fail to be valid at some point of the iteration. We sum up at least naive form of the algorithm.

1. At the start we have to initialize our variables:
   - $a := 0$ (index of elements of u^p)
   - $F(0) := \{1\}, D(0) = \{0\}$
   - $G(0) := \{0\}, C(0) = C_\infty$;
2. while $u_a = 0$ and $a <_T p$ $a := a \oplus 1$;
3. using an infinite element of $C(0)$ in Proposition 3.3.3 we generate n polynomials of form $X^{0+(a_i+1)e^i}$,
   $F(a \oplus 1) := \{X^{0+(a_i+1)e^i}, 1 \leq i \leq n\}$,
   $D(a \oplus 1) := \{(a_1+1, 0, \ldots, 0), (0, a_2+1, 0, \ldots, 0), \ldots, (0, \ldots, 0, a_n+1)\}$,
   $G(a \oplus 1) := G(0) \cup \{1\}$,
   $C(a \oplus 1) := C(0) \cup \{a\}$.
   $a := a \oplus 1$;

4. while $a <_T p$ and $F(a)_{fail} = \{f \in F(a), f[u]_a \neq 0\}$ is empty do $a := a \oplus 1$,;

5. For every $f \in F(a)_{fail}$, $\mathrm{le}(f) = d$ is valid one of the options:

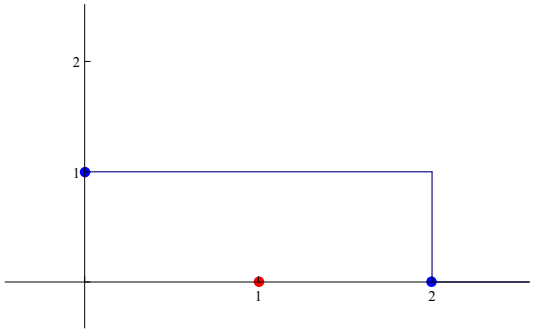
   (a) $a - d \in \Delta(a)$. Then f will not bring any new element to $\Delta(a \oplus 1)$ so $r = d$. To generate a polynomial f^+ we use $g \in G(a)$ such that related $s - t$ is greater (with respect to partial ordering) than $a - d$,
   $F(a \oplus 1) := F(a) \setminus \{f\} \cup f^+$, other sets stay unchanged;

   (b) $a - d \notin \Delta(a)$ however from Proposition 3.3.4 $a - d \in \Delta(a \oplus 1)$. Thus $r = \max(d, a - c) \neq d$, for $c \in C(a)$.
   By checking every c we generate set R, that contains all possible degrees r. Then for every $r \in R$, that there is no $r' \in R$, such that $r' <_P r$ and there is no $d' \in D(a) \setminus D_{fail}(a)$, that $d' \leq_P r$, we generate polynomial f^+ and upgrade all sets:
   $F(a \oplus 1) := F(a) \setminus f \cup \{f^+\}$,
   $D(a \oplus 1) := D(a) \setminus d \cup \{r\}$,
   $C(a \oplus 1) := C(a) \setminus \{c \in C(a), c \leq a - d\} \cup \{a - d\}$,
   $G(a \oplus 1) := \{$ polynomials related to elements of $C(a \oplus 1)\}$

   $a := a \oplus 1$, if $a <_T p$ go to step 4.

Example 3.3.5. *We will generate $F((3,1))$ for array from Example 3.3.2.*

(1,0) *First nonzero element.*
$F((0,1)) = \{y, x^2\}$, $D((0,1)) = \{(0,1), (2,0)\}$,
$G((0,1)) = \{1, 0\}$, $C((0,1)) = \{(1,0), (-1,\infty), (\infty,-1)\}$;

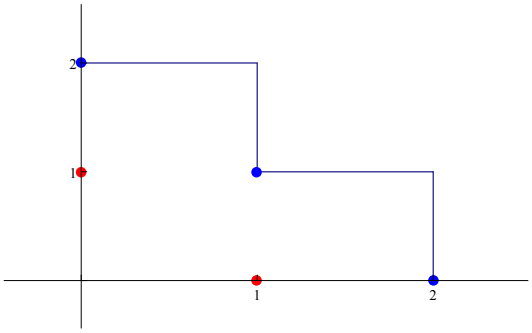


(0,1) $(y)[u]_{(0,1)} = u_{(0,1)} \neq 0$ *and* $(0,1) - (0,1) \in \Delta((0,1))$
$f^+ = y + x$
$F((2,0)) = \{y + x, x^2\}$, *other sets stay unchanged;*

(2,0) $(x^2)[u]_{(2,0)} = u_{(2,0)} = 0$ ✓;

(1,1) $(y + x)[u]_{(1,1)} = u_{(1,1)} + u_{(2,0)} \neq 0$ *and* $(1,1) - (0,1) \in \Delta((1,1))$
$f^+ = y + x + 1$
$F((0,2)) = \{y + x + 1, x^2\}$, *other sets stay unchanged;*

(0,2) $(y + x + 1)[u]_{(0,2)} = u_{(0,2)} + u_{(1,1)} + u_{(0,1)} \neq 0$ *and* $(0,2) - (0,1) \notin \Delta((0,2))$
$R = \{(0,2), (1,1), (0,3)\}$,
$r_1 = (0,2)$ *and* $f_1^+ = y(y + x + 1) + y = y^2 + xy$,
$r_2 = (1,1)$ *and* $f_2^+ = x(y + x + 1) = xy + x^2 + x$,
$F((3,0)) = \{x^2, xy + x^2 + x, y^2 + xy\}$, $D((3,0)) = \{(2,0), (1,1), (0,2)\}$,
$G((3,0)) = \{1, y + x + 1, 0\}$, $C((3,0)) = \{(1,0), (0,1), (-1,\infty), (\infty,-1)\}$;



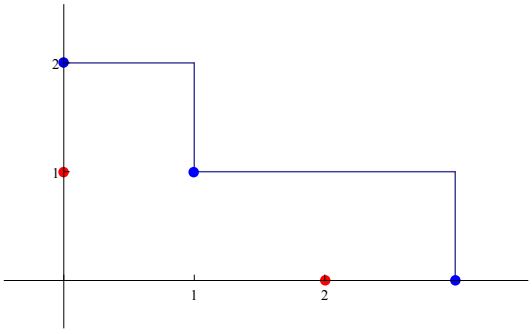
(3,0) $(x^2)[u]_{(3,0)} = u_{(3,0)} = 0$ ✓;

(2,1) $(x^2)[u]_{(2,1)} = u_{(2,1)} = 0$ ✓,
$(xy + x^2 + x)[u]_{(2,1)} = u_{(2,1)} + u_{(3,0)} + u_{(2,0)} = 0$ ✓;

(1,2) $(y^2 + yx)[u]_{(1,2)} = u_{(1,2)} + u_{(2,1)} = 0$ ✓,
$(xy+x^2+x)[u]_{(1,2)} = u_{(1,2)}+u_{(2,1)}+u_{(1,1)} \neq 0$ *and* $(1,2)-(1,1) \in \Delta((1,2))$,
$f^+ = xy + x^2 + x$,
$F((0,3)) = \{x^2, xy + x^2 + x + 1, y^2 + xy\}$, *other sets stay unchanged;*

(0,3) $(y^2 + yx)[u]_{(0,3)} = u_{(0,3)} + u_{(1,1)} = 0$ ✓;

(4,0) $(x^2)[u]_{(4,0)} = u_{(4,0)} \neq 1$ *and* $(4,0) - (2,0) \notin \Delta((4,0))$,
$R = \{(3,0), (4,0), (5,0), (2,1)\}$,
$r = (3,0)$ *and* $f^+ = x \cdot x^2 + (y + x + 1) = x^3 + y + x + 1$,
$F((3,1)) = \{xy + x^2 + x, y^2 + xy, x^3 + y + x + 1\}$,
$D((3,1)) = \{(1,1), (0,2), (3,0)\}$,
$G((3,1)) = \{1, x^2, 0\}$, $C((3,1)) = \{(0,1), (2,0), (-1,\infty), (\infty,-1)\}$;



From the construction we see that the minimal polynomial set $F(p)$ could be a Gröbner basis of ideal $I(u)$, for an infinite array u. However it do not have to be true, because if we generate infinite array from partial array u^p using polynomials $f_1, f_2 \in F(p)$ it can happen that element generated by f_1 is not equal to element generated by f_2. One of the sufficient conditions was given by Sakata in [Saka91].

Theorem 3.3.6. *Let us have a partial array v^q. If it holds that for any $p \geq_T q$ and for every pair of distinct leading exponentials $d_1, d_2 \in D(q)$, $d_1, d_2 \leq_P p$ exists chain of leading exponentials $d_{i_1}, \ldots, d_{i_k} \leq_P p$ from $D(q)$ that*

$$d_1 = d_{i_1}, d_{i_1} + d_{i_2} \leq_P p, \ldots d_{i_{k-1}} + d_{i_k}, d_{i_k} = d_2 \leq_P p,$$

then $F(q)$ is the Gröbner basis of $I(u)$ for some infinite array u, such that

$$u_p = v_p, \ \forall p <_T q.$$

Proof. We need to prove that for any $p \geq q$ we generate the same v_p by every $f \in F(q), \mathrm{le}(f) \leq_P p$. For f_1 with $\mathrm{le}(f_1) = d_1$ is

$$v_p = -\frac{1}{c(f_1, d_1)} \sum_{a \in \mathrm{supp}(f_1) \setminus \{d_1\}} c(f_1, a) u_{a+p-d_1}$$

and f_1 is valid at p. If couple of leading exponentials $d_1, d_2 \in D(p)$ satisfies $d_1 + d_2 \leq p$ then, according to Proposition 3.3.4, both of related polynomials are valid at p or they both fail at p. So we get $f_1[v]_p = 0 \Leftrightarrow f_{i_2}[v]_p = 0 \Leftrightarrow \cdots \Rightarrow f[v]_p = 0 \forall f \in D(q)$ that $\mathrm{le}(f) \leq_P p$. Hence v is properly generated infinite array and $F(q) \subseteq I(v)$. □

Example 3.3.7. *According to Theorem 3.3.6 the minimal set generated in Example 3.3.5 is the Gröbner basis for some infinite array if it works for* $u_{(3,1)}$ *and* $u_{(2,2)}$.

$$u_{(3,1)} = \begin{cases} u_{(4,0)} + u_{(3,0)} + u_{(2,0)} & = 1 \\ u_{(0,2)} + u_{(1,1)} + u_{(0,1)} & = 1 \end{cases} \checkmark$$

$$u_{(2,2)} = \begin{cases} u_{(3,1)} & = 1 \\ u_{(3,1)} + u_{(2,1)} + u_{(1,1)} & = 0 \end{cases} \times$$

However if we set $u_{(2,2)} = 0$ *and we update polynomial* $y^2 + xy$ *we get*

$$F((1,3)) = \{xy + x^2 + x, y^2 + xy + x^2, x^3 + y + x + 1\}.$$

Then there is an infinite array v, *that* $v^{(1,3)} = (0,1,1,0,1,1,0,0,0,1,1,1,0)$ *and* $F((1,3))$ *is the Gröbner basis of ideal* $I(v)$.

3.4 Syndrome decoding

In this section we show how to decode the one-point AG codes up to Feng-Rao bound. This type of decoding was described by Sakata, Jensen and Hoeholdt in [SakaJensHøho95]. We will consider plane curves, however the same decoding algorithm works also for other curves.

Let us have some curve $\mathcal{X}$ defined over $\mathbb{F}_q$. The curve $\mathcal{X}$ is set of points $l \in \mathbb{F}_q^2$ such that $f(l) = 0$ for defining polynomial $f \in \mathbb{F}_q[x, y]$. We consider an algebraic function field $\mathbb{F}(\mathcal{X})$ defined as quotient field of coordinate ring

$$\mathbb{F}_q[x, y]/(f).$$

The curve $\mathcal{X}$ has k distinct affine points and at least one point at infinity.

One-point code is AG codes $C(D, G)$, where $P_1, \ldots, P_k$ are places of degree one corresponding to affine points on curve and P_∞ is point at infinity.

$$D = P_1 + \cdots + P_n, \text{ and } G = mP_\infty \text{ for some } m \in \mathbb{N} \cup \{0\}.$$

As P_∞ is place corresponding to the point at infinity, we can consider generators of $L(mP_\infty)$ as monomials

$$X^a \in [X'] \text{ that } \nu_\infty(X^a) \geq -m,$$

where $[X']$ is set of all monomials X^a that $X^a \in \mathbb{F}_q[X]/(f)$.

Related to valuation we can define order function

$$\begin{aligned}\mathcal{O} : [X'] &\to \mathbb{Z} \\ X^a &\to -\nu_\infty(X^a).\end{aligned}$$

Throughout the rest of the section we denote monomials X^a by f_a.

Definition 3.4.1. *For an element $y \in \mathbb{F}_q^n$ and monomial $f_a \in [X']$ we define syndrome of y as*

$$S_a(y) = \sum_{i=1}^{n} f_a(P_i)y_i = \sum_{i=1}^{n} P_i^a y_i$$

Then from the definition of dual code we get

$$c \in C^\perp \Leftrightarrow S_a(c) = \sum_{i=1}^{n} f_a(P_i)c_i = 0,\ f_a \in L(G).$$

Assuming that during the transmission there occurred at most $\lfloor \frac{d(C^\perp)-1}{2} \rfloor$ errors, then for every received word $r \in \mathbb{F}_q^n$ there is a codeword $c \in C^\perp(D, G)$ that $r = c + e$, where e is called error vector. We define an infinite array u by $u_a = \sum_{i=1}^{n} e_i f_a(P_i)$ with the term ordering

$$\begin{aligned}f_a <_T f_b \Leftrightarrow &\mathcal{O}(f_a) < \mathcal{O}(f_b) \\ &\mathcal{O}(f_a) = \mathcal{O}(f_b) \text{ and } \exists i \in \{1, \ldots, n\} \text{ that } a_i < b_i; a_j = b_j \forall j < i.\end{aligned}$$

We consider a variety of a characteristic ideal of u and a set of error locators $\varepsilon = \{P_i | e_i \neq 0\}$. For each $f \in I(u)$ with $\mathrm{le}(f) = d$ and $p \geq_P d$ is

$$\begin{aligned}0 = \sum_{a \in \mathrm{supp}(f)} c(f,a)u_{a+p-d} &= \sum_{a \in \mathrm{supp}(f)} c(f,a) \sum_{i=1}^{n} e_i f_{a+p-d(P_i)} \\ &= \sum_{a \in \mathrm{supp}(f)} c(f,a) \sum_{P_i \in \varepsilon} e_i f_{a+p-d}(P_i) \\ &= \sum_{P_i \in \varepsilon} e_i f_{p-d}(P_i) \sum_{a \in \mathrm{supp}(f)} c(f,a) f_a(P_i).\end{aligned}$$

Each $P_i \in \varepsilon$ correspondents to distinct affine point on curve, let say $\alpha_i = (\alpha_{i_1}, \alpha_{i_2})$. Then if we consider $|\varepsilon|$ arrays defined as $v_a^{(i)} = \alpha_i^a, a \in \mathbb{N}^n$, we have $|\varepsilon|$ arrays that are linearly independent. Then $\sum_{a \in \mathrm{supp}(f)} c(f,a) f_a(P_i) = 0$. On the other side, if we have a polynomial f that $\sum_{a \in \mathrm{supp}(f)} c(f,a) f_a(P_i) = 0$ for $P_i \in \varepsilon$ and we go backward through the equations, then we get $f \in I(u)$. Hence $\varepsilon = V(I(u))$.

The situation is that we received the word r and we need to find a codeword $c \in C^\perp(D, G)$ that was sent, so $r = c + e, w_h(e) = t$. The basic idea of decoding is to get a Gröbner basis of $I(u)$ by BMS algorithm and calculate the error locators. Then an error vector e is unique solution of

$$rH^T = xH^T,$$

where H is parity check matrix of $C^\perp(D, G)$ and $x_i = 0, \forall i$ that $P_i \notin \varepsilon$. To calculate the Gröbner basis of $I(u)$ we need partial array u^p for some *sufficiently*

large $p \in \mathbb{N}^n$. We could use all monomials $f_a \in L(mP_\infty)$ to calculate u_a as $S_a(r) = S_a(c+e) = S_a(e) = u_a$. Such a syndrome is called known syndrome and u_b for $b, \mathcal{O}(f_b) \leq m$ are unknown syndromes.

The question is how we could calculate unknown syndromes, i.e.

$$u_a \text{ for } f_a \in [X'] \text{ and } \mathcal{O}(f_a) > m.$$

First, however, we will introduce some notation. Let us have an integer o and $\alpha_1, \ldots, \alpha_k$ be all monomials in $[X']$ with order o. In that case $\alpha_1, \ldots, \alpha_k$ are dependent, i.e.

$$\alpha_i = c_j \alpha_j + \sum_{\mathcal{O}(f_a)<o} c_a f_a \mod f, \tag{3.1}$$

where all c_a and c_j belongs to $\mathbb{F}_q$. The same relations have to be valid for syndromes corresponding to monomials, i.e.

$$u_i \equiv c_j u_j + \sum_{\mathcal{O}(f_a)<o} c_a u_a. \tag{3.2}$$

We define set Σ' as

$$\Sigma' = \{a \in \mathbb{N}^2 \mid \forall b \in \mathbb{N}^2, \mathcal{O}(f_b) = \mathcal{O}(f_a), a \leq_T b\}.$$

Let us have calculated all known syndromes and related minimal polynomial set $F(a)$ of u^a. We want to reduce $F(a)$ in a way that each degree belongs to Σ'. It is possible according to the relation 3.1. As a consequence in a similar manner we reduce $\bigcup_{f \in F_R(a)}(\Sigma_{\mathrm{le}(f)})$ and $\Delta(a)$. Reduced sets will be denoted by $\Sigma_R(a)$ and $\Delta_R(a)$. This is a way how to distinguish between syndromes, which are dependent and those that are independent.

We assume that $\alpha_1, \ldots, \alpha_k$ are all possible leading exponentials of monomials with order $m+1$. We put $\alpha = \min_{<_T}\{\alpha_i, 1 \leq i \leq k\}$ and define

$$K(\alpha) = \{p \in \Sigma' | \exists i, 1 \leq i \leq k \text{ that } p \leq_P \alpha_i \text{ and } \alpha_i - p \in \Sigma')\}.$$

If $f \in F_R(\alpha)$ is not valid at α then it has to be updated. According to Proposition 3.3.4 this updating could mean that $|\Delta_R(\alpha \oplus 1) \setminus \Delta_R(\alpha)| > 0$. In fact we will show that f is valid at α if it would cause the largest change of the Δ-set.

Now, we only consider those $f \in F_R(\alpha)$ that increase the Δ-set. Hence for each f with $\mathrm{le}(f) = d$, we check if there is an i such that $\alpha_i \geq_P d$ and $\alpha_i - d \in \Sigma_R(\alpha)$. If it is a case then

$$K_d = \{p \in K(\alpha) \mid p \leq_P \alpha_i - d\} \setminus \Delta_R(\alpha)$$

is a set of new points in the $\Delta_R(\alpha \oplus 1)$.

Such f gives a candidate for a value $S_\alpha(e)$. We can compute the candidate from $f[u^\alpha] = 0$ or from relation 3.2, it depends on α_i that we used.

Let $s_1, \ldots, s_l$ be all candidates given by $F_R(\alpha)$. We say that s_i has x votes if

$$x = \sum |K_d|, \text{ where sumation goes throught such } f \text{ that give } s_i \text{ as candidate.}$$

For $f \in F_R(\alpha)$ that $\alpha - \mathrm{le}(f) \in \Delta(\alpha)$ we say that f gives candidate with zero votes.

Theorem 3.4.2. *Suppose that the number of errors t that occurred during the transmission satisfies*

$$t \leq \lfloor \frac{d_{FR} - 1}{2} \rfloor,$$

where

$$d_{FR} = \min_{a \in \Sigma', \, \mathcal{O}(f_a) > m} |K(a)|.$$

Then the syndrome u_α is equal to the candidate with the biggest number of votes.

d_{FR} is Feng-Rao distance. It is lower bound for minimum distance of code, which could be better than Goppa distance. It satisfy

$$d \geq d_{FR} \geq d_G \text{ and } d_{FR} = d_G \text{ if } m \geq 4g - 2,$$

where g is genus of curve $\mathcal{X}$. To show, that definition of d_{FR} does not depend on specific received word, we use proof from [SakaJensHøho95]. Before that we define nongap:

$$\text{A number } s \text{ is a nongap for } P_\infty \Leftrightarrow \mathcal{L}(sP_\infty) \neq \mathcal{L}((s-1)P_\infty).$$

Then

$$d_{FR} = \min_{r > m} |\{s \text{ is a nongap } | \exists \text{ nongap } t : s + t = r\}|.$$

Consequence of previous discussion is, that we have to modify BMS algorithm in a way, that all points of the same order are treated simultaneously.

If we can prove Theorem 3.4.2 we can compute the elements of the infinite array u corresponding to the order $m + 1$ and then, analogously, generate the elements corresponding to the orders $m + 2, m + 3, \ldots$. If we have all unknown syndromes $u_a, f_a \in [X']$, then related set of minimal polynomials is the Gröbner basis of $I(u)$ and we can compute error positions.

Before we can prove Theorem 3.4.2, we need to show that the size of Δ-set is always less or equal than t and that

$$v \geq |K(\alpha)| - 2|\Delta_R(\alpha)|,$$

where v is amount of all votes, i.e. $v = |\cup K_d|$.

1. Consider polynomial ring $\mathbb{F}_q[X]$ and ideal $I(u)$. Then

   $$\dim_{\mathbb{F}_q}(\mathbb{F}_q[X]/I(u)) = t$$

   as $|V(I(u))| = t$ and equivalence class $[f]$, for a polynomial with leading exponential in the Δ-set, is nonzero. Inequality follow from the fact, that the elements of Δ-set are independent.

2. Consider

   $$p \in K(\alpha) \setminus ((\cup K_d) \cup \Delta_R(\alpha)).$$

   Then $\exists! i$ that $p \leq_P \alpha_i$ and $\alpha_i - p \in \Delta_R(\alpha)$. We get the injective mapping from $K(\alpha) \setminus ((\cup K_d) \cup \Delta_R(\alpha))$ into $\Delta_R(\alpha)$. Thus from linear algebra is

   $$0 \geq |K(\alpha)| - (|\cup K_d| + |\Delta_R(\alpha)|) - |\Delta_R(\alpha)|.$$

Finally we have all tools to prove Theorem 3.4.2:

Proof. If u_α is different from each candidate, than every polynomial $f \in F_R(\alpha)$ with the leading exponential d such that $\alpha_j - d \in \Sigma_R(\alpha)$ fails to be valid at α and then

$$|\Delta_R(\alpha \oplus 1)| \geq |\Delta_R(\alpha)| + |\cup K_d| \geq |K(\alpha)| - |\Delta_R(\alpha)| \geq d_{FR} - t > t.$$

So one of the candidates is right value for the syndrome u_α.
Let T be amount of votes for a right candidate and W amount of votes for the wrong candidates. We get

$$t \geq \Delta_R(\alpha \oplus 1) \geq \Delta_R(\alpha) + W \Rightarrow W < \frac{1}{2}|W + T|$$

and so $W < T$. Hence the right candidate is really the candidate with the largest amount of votes.

□

Finally the decoding algorithm is:

1. Calculate the syndromes u_a, $\mathcal{O}(f_a) \leq m$;
2. by BMS algorithm find set of minimal polynomials of partial array u^a;
3. if it is necessary, reduce set of minimal polynomials (so the orders of leading terms belong to Σ');
4. find syndromes up to the pole order $m + 2g + 2$ by Theorem 3.4.2 and relation 3.2 and upgrade the set of minimal polynomials;
5. calculate common zeros of minimal polynomials;
6. calculate error values.

4. Hermitian Codes

In the last chapter we present specific class of AG codes and we show how to encode and decode those codes by the methods described in previous chapter. The codes that we are going to discuss are codes define by Hermitian curve

$$\mathcal{X} : y^q + y - x^{q+1} = 0$$

over finite field $\mathbb{F}_{q^2}$. Let us sum up some knowledge from [Stic09] about algebraic function field $\mathbb{F}(\mathcal{X})$.

The genus of $\mathbb{F}(\mathcal{X})$ is

$$g = \frac{q(q-1)}{2}.$$

As equation

$$y^q + y - \alpha^{q+1}$$

has for every $\alpha \in \mathbb{F}_{q^2}$ exactly q distinct solutions, there is q^3 affine rational points on curve $\mathcal{X}$. Hence there is $q^3 + 1$ places of degree one in $\mathbb{F}(\mathcal{X})$ (the affine points $P_{\alpha,\beta}$ and the point at infinity P_∞).

Hermitian codes are one-point codes and we define them as:

$$\mathcal{HC}_q^m = C(D, G),$$

where

$$D = \sum_{\beta^q+\beta-\alpha^{q+1}=0} P_{\alpha,\beta} \text{ and}$$
$$G = m \cdot P_\infty, \text{ for some } m \in \mathbb{Z}.$$

In fact we have some additional conditions on integer m. If $m < 0$ then $\mathcal{HC}_q^m = \emptyset$ and in case $m > q^3 + q^2 - q - 2$ is $\mathcal{HC}_q^m = \mathbb{F}_{q^2}^{q^3}$. Hence we take only

$$0 \leq m \leq q^3 + q^2 - q - 2.$$

To introduce dual codes of Hermitians codes we consider Weil differencial

$$\omega = \frac{d(x^{q^2} - x)}{x^{q^2} - x} = \frac{-dx}{x^{q^2} - x}.$$

As $x^{q^2} - x = \sum_{\alpha \in \mathbb{F}_{q^2}} (x - \alpha)$ we get that it is a prime element for every $P_{\alpha,\beta}$. Now we go back to curve $\mathbb{X}$ and its defining equation

$$y^q + y - x^{q+1} = 0.$$

If we want to transform equation to projective plane, we put $y = \frac{Y}{Z}, x = \frac{X}{Z}$. Then we get

$$ZY^q + Z^qY - X^{q+1} = 0$$

and we see that Hermitian curve has only one point at infinity $P_\infty = (0 : 1 : 0)$. As

$$\frac{\partial(Z + Z^q - X^{q+1})}{Z} = 1 + qZ^{q-1} = 1 \text{ and}$$
$$\frac{\partial(Z + Z^q - X^{q+1})}{X} = -(q+1)X^q = -X^q,$$

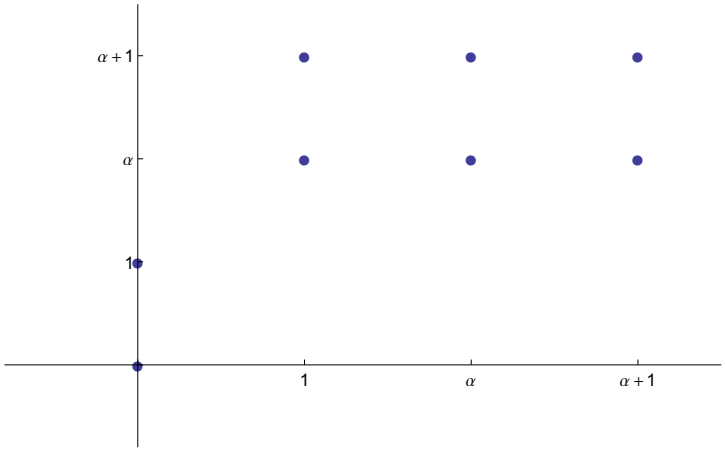


Figure 4.1: Affine points on $\mathcal{H}_2$ over $\mathbb{F}_2$

then $\nu_\infty(X) = 1$, $\nu_\infty(Z) = q+1$ and so $\nu_\infty(x) = -q$. Finally we can express principal divisor of $x^{q^2} + x$ as

$$(x^{q^2} - x) = \sum P_{\alpha,\beta} + \nu_\infty x^{q^2} - xP_\infty = D - q^3 P_\infty.$$

Therefore (according to remark below definition 1.2.7) canonical divisor (ω) is

$$(\omega) = (q^2 - q - 2)P_\infty - D + q^3 P_\infty$$

and by Proposition 2.2.8 is

$$(\mathcal{HC}_q^m)^\perp = \mathcal{HC}_q^{q^3+q^2-q-2-m}.$$

4.1 Example of encoding

With $q = 2$ we get finite field $\mathbb{F}_4$ with primitive element α and $\alpha^2 + \alpha + 1 \equiv 0$. Hermitian curve $\mathcal{H}_2$ defined by

$$y^2 + y - x^3 = 0$$

has 8 affine points (a_i, b_i) on $\mathcal{H}_2$ over $\mathbb{F}_4$, see Figure 4.1.

The projective equation of $\mathcal{H}_2$ is

$$ZY^2 + Z^2Y - X^3 = 0$$

that has 9 rational points-$(a_i : b_i : 1), 1 \leq i \leq 8$ and one point at infinity $(0 : 1 : 0)$. Then we construct an $\mathcal{HC}_2^4$ code where

$$D = \sum_{i=1}^{8} P_{a_i,b_i} \text{ and}$$
$$G = 4P_\infty.$$

According to Theorem 2.2.4 is the length of code equal to 8, the dimension is 4 and the minimum distance $d(C) \geq 4$.

We consider cyclic group of automorphisms with generator

$$\sigma : (X, Y, Z) \to (\alpha X, Y, Z).$$

We see, from Figure 4.1, that it is a permutation on rational points and that it fixes divisors D and G. By Theorem 3.2.1 σ induces an automorphism of the code $\mathcal{HC}_2^4$.

σ permutes points $(a_i : b_i : 1), 1 \leq i \leq 9$ into four orbits:

$$\begin{aligned}
O_1 =&\{(0:0:1)\},\\
O_2 =&\{(0:1:1)\},\\
O_3 =&\{(1:\alpha:1),(\alpha:\alpha:1),(\alpha+1:\alpha:1)\},\\
O_4 =&\{(1:\alpha+1:1),(\alpha:\alpha+1:1),(\alpha+1:\alpha+1:1)\}.
\end{aligned}$$

To create the generator matrix M we use functions with different orders (so they are independent)

$$1, X/Z, Y/Z, (X/Z)^2 \in \mathcal{L}(4P_\infty).$$

Then the generator matrix of code is (with respect to order of points given by orbits)

$$M = \begin{pmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1\\
0 & 0 & 1 & \alpha & \alpha+1 & 1 & \alpha & \alpha+1\\
0 & 1 & \alpha & \alpha & \alpha & \alpha+1 & \alpha+1 & \alpha+1\\
0 & 0 & 1 & \alpha+1 & \alpha & 1 & \alpha+1 & \alpha
\end{pmatrix}$$

Let

$$\begin{aligned}
f_1 &= (1, 1, 1+t+t^2, 1+t+t^2),\\
f_2 &= (0, 0, 1+\alpha\cdot t+(\alpha+1)\cdot t^2, 1+\alpha\cdot t+(\alpha+1)\cdot t^2),\\
f_3 &= (0, 1, \alpha+\alpha\cdot t+\alpha\cdot t^2, (\alpha+1)\cdot(1+t+t^2)),\\
f_4 &= (0, 0, 1+(\alpha+1)\cdot t+\alpha\cdot t^2, 1+(\alpha+1)\cdot t+\alpha\cdot t^2),\\
f_5 &= (1+t, 0, 0, 0),\\
f_6 &= (0, 1+t, 0, 0),\\
f_7 &= (0, 0, 1+t^3, 0),\\
f_8 &= (0, 0, 0, 1+t^3).
\end{aligned}$$

The mapping Φ from Section 3.2 create submodule

$$< f_1, f_2, f_3, f_4 >,$$

that represent code as a subset of the quotient module

$$\mathbb{F}_2[t]^4 / < f_5, f_6, f_7, f_8 > .$$

For the systematic encoder we need Gröbner basis of preimage $\Phi(C)$ under the mapping Π from Section 3.2, hence Gröbner basis of

$$< \{f_1, f_2, f_3, f_4, f_5, f_6, f_7, f_8\} > .$$

Using position over term ordering we get Gröbner basis

$$\begin{aligned}
g_1 &= (1, 1, 1 + t + t^2, 1 + t + t^2),\\
g_2 &= (0, 1, \alpha + \alpha \cdot t + \alpha \cdot t^2, (\alpha + 1)(1 + t + t^2)),\\
g_3 &= (0, 0, 1 + t, 1 + t),\\
g_4 &= (0, 0, 0, 1 + t^3).
\end{aligned}$$

As leading terms determinate the information positions, we see that the information positions are e_1, e_2, te_3 and t^2e_3. For example if we want to encode $(\alpha, \alpha + 1, 1, \alpha)$ we set

$$w = (\alpha, \alpha + 1, t + \alpha t^2, 0),$$

we reduce w by g_1, g_2 and g_3 and get normal form

$$(0, 0, \alpha + 1, \alpha + (\alpha + 1)t^2).$$

The corresponding codeword is

$$c = (\alpha, \alpha + 1, \alpha + 1, 1, \alpha, \alpha, 0, \alpha + 1).$$

4.2 Example of decoding

Now, let us have $q = 4$ and we consider an affine equation of Hermitian curve $\mathcal{H}_4$

$$y^4 + y - x^5 = 0$$

We can take code $\mathcal{HC}_4^{49}$, which has the length of codeword 64 (See Table 4.1, where a is a primitive element of $\mathbb{F}_{16}$), the dimension 44 and the bound for minimum distance 15. We can consider received words with 7 errors. At first we have to calculate all known syndromes. The dual code of $\mathcal{HC}_4^{49}$ is $\mathcal{HC}_4^{25}$ hence we consider monomials with order less or equal than 25.

Before we can consider any codeword we need to know relation between the positions of codeword and affine points, i.e. order in which we evaluate affine points. We use ordering denoted by Table 4.1.

Let us have received word

$$\begin{aligned}
r = (&0, 0, 0, 0, 1, 1, a, 1, a^3 + a + 1, a^3 + a + 1, a^3 + a + 1, a^3 + a + 1, a^3 + 1,\\
&a^3 + 1, a^3 + 1, a^3 + 1, a^3 + a, a^3 + a^2, a^3 + a^2, a^3 + a^2, a^3 + a^2 + 1,\\
&a^3 + a^2 + 1, a^3 + a^2 + 1, a^3 + a^2 + 1, a^2 + a, a^2 + a, a^3 + a, a^2 + a,\\
&a^3 + a^2 + a + 1, a^3 + a^2 + a + 1, a^3 + a^2 + a + 1, a^3 + a^2 + a + 1, a + 1,\\
&a + 1, a + 1, a + 1, a^2 + 1, a^3 + a^2 + a, a^3 + a^2 + a, a^3 + a^2 + a, a^3, a^3, a^3,\\
&a^3, a^2 + a + 1, a^2 + a + 1, a, a^2 + a + 1, a^2, a^2, a^2, a^2, a^3 + a, a^3 + a,\\
&a^3 + a, a^3 + a, a^3, a, a, a, a^2 + 1, a^2 + 1, a^2 + 1, a),
\end{aligned}$$

which has seven errors.

Table 4.2 consists of all known syndromes.

$(0,0)$	$(0,1)$	$(1,a)$
(a^3,a)	(a^3+a,a)	(a^3+a^2,a)
(a^3+a^2+a+1,a)	$(1,a+1)$	$(a^3,a+1)$
$(a^3+a,a+1)$	$(a^3+a^2,a+1)$	$(a^3+a^2+a+1,a+1)$
$(1,a^2)$	(a^3,a^2)	(a^3+a,a^2)
(a^3+a^2,a^2)	(a^3+a^2+a+1,a^2)	$(1,a^2+1)$
(a^3,a^2+1)	(a^3+a,a^2+1)	(a^3+a^2,a^2+1)
(a^3+a^2+a+1,a^2+1)	$(0,a^2+a)$	$(0,a^2+a+1)$
(a^2,a^3)	(a^2+1,a^3)	(a^2+a,a^3)
(a^3+1,a^3)	(a^3+a^2+a,a^3)	(a^2,a^3+1)
(a^2+1,a^3+1)	(a^2+a,a^3+1)	(a^3+1,a^3+1)
(a^3+a^2+a,a^3+1)	(a,a^3+a)	$(a+1,a^3+a)$
(a^2+a+1,a^3+a)	(a^3+a+1,a^3+a)	(a^3+a^2+1,a^3+a)
(a,a^3+a^2)	$(a+1,a^3+a^2)$	(a^2+a+1,a^3+a^2)
(a^3+a+1,a^3+a^2)	(a^3+a^2+1,a^3+a^2)	(a,a^3+a+1)
$(a+1,a^3+a+1)$	(a^2+a+1,a^3+a+1)	(a^3+a+1,a^3+a+1)
(a^3+a^2+1,a^3+a+1)	(a^2,a^3+a^2+a)	(a^2+1,a^3+a^2+a)
(a^2+a,a^3+a^2+a)	(a^3+1,a^3+a^2+a)	(a^3+a^2+a,a^3+a^2+a)
(a,a^3+a^2+1)	$(a+1,a^3+a^2+1)$	(a^2+a+1,a^3+a^2+1)
(a^3+a+1,a^3+a^2+1)	(a^3+a^2+1,a^3+a^2+1)	(a^2,a^3+a^2+a+1)
(a^2+1,a^3+a^2+a+1)	(a^2+a,a^3+a^2+a+1)	(a^3+1,a^3+a^2+a+1)
(a^3+a^2+a,a^3+a^2+a+1)		

Table 4.1: The affine points of $\mathcal{H}_4$

$i\backslash j$	0	1	2	3	4	5
0	a^3+a	a^3+1	a^3+a^2+a+1	a^3	a^3	$a+1$
1	0	a^2+1	a^2+a	a^3	1	
2	a^2	a^2+a+1	a^2+a	0		
3	a	a^3+a^2+1	a^3+a^2+a			
4	a^2+1	a^2+1				
5	1	a^3+a^2				
6	a^2					

Table 4.2: Known syndromes

In the following table are all iteration of BMS algorithm on partial array $u^{(4,2)}$.

a	$F(a \oplus 1)$
(0,0)	x y
(1,0)	x y
(0,1)	x $y + a^2 + a$
(2,0)	$x^2 + a^2 + 1$ $y + a^2 + a$
(1,1)	$x^2 + a^2 + 1$ $y + (a^3 + a^2)\,x + a + a^2$
(0,2)	$x^2 + a^2 + 1$ $xy + (a^3 + a^2)\,x^2 + (a^2 + a)\,x + xy$ $y^2 + (a^3 + a^2)\,xy + (a^2 + a)\,y + a^3 + 1$
(3,0)	$x^2 + (a^3 + 1)\,x + a^2 + 1$ $xy + (a^3 + a^2)\,x^2 + (a^2 + a)\,x + xy$ $y^2 + (a^3 + a^2)\,xy + (a^2 + a)\,y + a^3 + 1$
(2,1)	$x^2 + a^2y + (a^3 + a^2)\,x + a^3 + a^2 + a$ $xy + (a^3 + a^2)\,x^2 + (a + 1)x$ $y^2 + (a^3 + a^2)\,xy + (a^2 + a)\,y + a^3 + 1$
(1,2)	$x^2 + a^2y + (a^3 + a^2)\,x + a^3 + a^2 + a$ $xy + (a^3 + a^2)\,x^2 + (a^3 + 1)\,y + (a^2 + 1)\,x + a + 1$ $y^2 + (a^3 + a^2)\,xy + (a^2 + a)\,y + (a^3 + a^2 + a + 1)\,x + a^3 + 1$
(0,3)	$x^2 + a^2y + (a^3 + a^2)\,x + a^3 + a^2 + a$ $xy + (a^3 + a^2)\,x^2 + (a^3 + 1)\,y + (a^2 + 1)\,x + a + 1$ $y^2 + (a^3 + a^2)\,xy + (a^3 + a)\,y + a^2 + a + 1$
(4,0)	$x^3 + a^2xy + (a^3 + a^2)\,x^2 + (a^3 + a^2 + 1)\,x$ $xy + (a^3 + a^2)\,x^2 + (a^3 + 1)\,y + (a^2 + 1)\,x + a + 1$ $y^2 + (a^3 + a^2)\,xy + (a^3 + a)\,y + a^2 + a + 1$
(3,1)	$x^3 + (a^3 + a^2)\,x^2 + a^2xy + (a^2 + a + 1)\,y$ $\quad + (a^3 + a^2 + a + 1)\,x + 1$ $xy + (a + 1)x^2 + (a^3 + a^2 + 1)\,x + a^2 + a$ $y^2 + (a^3 + a^2)\,xy + (a^3 + a)\,y + a^2 + a + 1$
(2,2)	$x^3 + (a^3 + a^2)\,x^2 + a^2xy + (a^2 + a + 1)\,y$ $\quad + (a^3 + a^2 + a + 1)\,x + 1$ $x^2y + (a + 1)x^3 + (a^3 + a^2 + 1)\,x^2 + ay + (a^3 + a^2 + 1)\,x$ $\quad + a^3 + a^2$ $y^2 + (a^3 + a^2)\,xy + (a^2 + 1)\,x^2 + (a^3 + a^2 + 1)\,y$ $\quad + (a^3 + 1)\,x + a^2$
(1,3)	$x^3 + (a^3 + a^2)\,x^2 + a^2xy + (a^2 + a + 1)\,y$ $\quad + (a^3 + a^2 + a + 1)\,x + 1$ $x^2y + (a + 1)x^3 + (a^3 + a^2 + 1)\,x^2 + ay + (a^3 + a^2 + 1)\,x$ $\quad + a^3 + a^2$ $y^2 + a^2xy + (a^3 + a^2 + a)\,x^2 + (a^3 + a^2 + 1)\,y$ $\quad + (a^3 + a + 1)\,x + 1$

(0,4)	$x^3+(a^3+a^2)\,x^2+a^2xy+(a^2+a+1)\,y$ $\quad+(a^3+a^2+a+1)\,x+1$ $x^2y+(a+1)x^3+(a^3+a^2+1)\,x^2+ay+(a^3+a^2+1)\,x$ $\quad+a^3+a^2$ $xy^2+a^2x^2y+(a^3+a^2+a)\,x^3+(a^3+a^2+1)\,xy$ $\quad+(a^3+a+1)\,x^2+x$ $y^3+a^2xy^2+(a^3+a^2+a)\,x^2y+(a^3+a^2+1)\,y^2$ $\quad+(a^3+a+1)\,xy+(a^3+1)\,y+(a^3+a)\,x+a^2+1$
(5,0)	$x^3+a^2xy+(a^2+1)\,x^2+(a^2+1)\,y+(a^3+1)\,x+a^2+a$ $x^2y+(a+1)x^3+(a^3+a^2+1)\,x^2+ay+(a^3+a^2+1)\,x$ $\quad+a^3+a^2$ $xy^2+a^2x^2y+(a^3+a^2+a)\,x^3+(a^3+a^2+1)\,xy$ $\quad+(a^3+a+1)\,x^2+x$ $y^3+a^2xy^2+(a^3+a^2+a)\,x^2y+(a^3+a^2+1)\,y^2$ $\quad+(a^3+a+1)\,xy+(a^3+1)\,y+(a^3+a)\,x+a^2+1$
(4,1)	$x^3+(a^3+a^2+a)\,xy+a^3x^2+(a^2+1)\,y+a^2+ax$ $\quad+a^3+a+1$ $x^2y+(a+1)x^3+ax^2+(a^3+a+1)\,y+(a^2+1)\,x+a^3+1$ $xy^2+a^2x^2y+(a^3+a^2+a)\,x^3+(a^3+a^2+1)\,xy$ $\quad+(a^3+a+1)\,x^2+x$ $y^3+a^2xy^2+(a^3+a^2+a)\,x^2y+(a^3+a^2+1)\,y^2$ $\quad+(a^3+a+1)\,xy+(a^3+1)\,y+(a^3+a)\,x+a^2+1$
(3,2)	$x^3+(a^3+a^2+1)\,y^2+(a^3+a^2+a+1)\,xy$ $\quad+ax^2+(a^3+a+1)\,y+a^2x+a$ $x^2y+(a+1)x^3+(a^2+1)\,xy+(a^3+a^2+1)\,x^2$ $\quad+(a^3+a+1)\,y+(a^3+1)\,x+a^2$ $xy^2+a^2x^2y+(a^3+a^2+a)\,x^3+(a^3+a^2+1)\,xy$ $\quad+(a+1)x^2\quad+(a^2+a)\,y+(a^3+a+1)\,x+a^3+1$ $y^3+a^2xy^2+(a^3+a^2+a)\,x^2y+(a^3+a^2+1)\,y^2$ $\quad+(a^3+a+1)\,xy+(a^3+1)\,y+(a^3+a)\,x+a^2+1$
(2,3)	$x^3+(a^3+a^2+1)\,y^2+(a^3+a^2+a+1)\,xy$ $\quad+ax^2+(a^3+a+1)\,y+a^2x+a$ $x^2y+(a+1)x^3+(a^3+a^2+1)\,y^2+a^2xy+a^3+(a^2+a+1)\,x^2$ $\quad+(a^2+1)\,y+(a^3+a^2+a+1)\,x+1$ $xy^2+a^2x^2y+(a^3+a^2+a)\,x^3+(a^3+a^2)\,xy$ $\quad+(a^2+a)\,y+(a^2+a)\,x+a^3+a^2+a+1$ $y^3+a^2xy^2+(a^3+a^2+a)\,x^2y+(a^3+a^2+1)\,y^2$ $\quad+(a^3+a+1)\,xy+a^3x^2+(a^3+a^2+a+1)\,y+a^3+a^2$
(1,4)	$x^3+(a^3+a^2+1)\,y^2+(a^3+a^2+a+1)\,xy$ $\quad+ax^2+(a^3+a+1)\,y+a^2x+a$ $x^2y+(a+1)x^3+(a^3+a^2+1)\,y^2+a^2xy+a^3+(a^2+a+1)\,x^2$ $\quad+(a^2+1)\,y+(a^3+a^2+a+1)\,x+1$ $xy^2+a^2x^2y+(a^3+a^2+a)\,x^3+(a^3+a+1)\,y^2$ $\quad+(a^2+a)\,xy+a^3x^2+(a^3+a^2+a+1)\,x+a^2$ $y^3+a^2xy^2+(a^3+a^2+a)\,x^2y+(a^3+a^2+1)\,y^2+xy$ $\quad+(a^2+1)\,x^2+(a^3+a^2+a+1)\,y+(a^3+a+1)\,x+a^2+1$

(6,0)	$x^4+(a^3+a^2+a+1)\,x^2y+(a^3+a^2+1)\,xy^2+ax^3$ $+(a^3+a+1)\,xy+a^3x^2+(a^2+1)\,y+(a^3+a^2+1)\,x+a^2$ $x^2y+(a+1)x^3+(a^3+a^2+1)\,y^2+a^2xy+a^3+(a^2+a+1)\,x^2$ $+(a^2+1)\,y+(a^3+a^2+a+1)\,x+1$ $xy^2+a^2x^2y+(a^3+a^2+a)\,x^3+(a^3+a+1)\,y^2$ $+(a^2+a)\,xy+a^3x^2+(a^3+a^2+a+1)\,x+a^2$ $y^3+a^2xy^2+(a^3+a^2+a)\,x^2y+(a^3+a^2+1)\,y^2+xy$ $+(a^2+1)\,x^2+(a^3+a^2+a+1)\,y+(a^3+a+1)\,x+a^2+1$
(5,0)	$x^4+(a^3+a^2+a+1)\,x^2y+(a^3+a^2+1)\,xy^2+ax^3$ $+(a^3+a+1)\,xy+a^3x^2+(a^2+1)\,y+(a^3+a^2+1)\,x+a^2$ $x^2y+(a+1)x^3+(a^3+a^2+1)\,y^2+a^2xy+a^3+(a^2+a+1)\,x^2$ $+(a^2+1)\,y+(a^3+a^2+a+1)\,x+1$ $xy^2+a^2x^2y+(a^3+a^2+a)\,x^3+(a^3+a+1)\,y^2$ $+(a^2+a)\,xy+a^3x^2+(a^3+a^2+a+1)\,x+a^2$ $y^3+a^2xy^2+(a^3+a^2+a)\,x^2y+(a^2+a)\,y^2+(a^3+a+1)\,xy$ $+(a^3+a^2+1)\,x^2+(a^3+1)\,y+ax+a^3+a^2+a$
(5,1)	$x^4+(a^3+a^2+1)\,xy^2+(a^3+a^2+a+1)\,x^2y$ $+ax^3+(a^2+a+1)\,xy+(a^3+a^2+a+1)\,x^2+(a^2+1)\,y$ $+(a^3+a^2+a)\,x+a^3+a$ $x^2y+(a^3+a+1)\,x^3+(a^3+a^2+a+1)\,y^2+(a^2+1)\,xy$ $+a^2x^2+ay+(a^3+1)\,x+a^3+a$ $xy^2+a^2x^2y+(a^3+a^2+a)\,x^3+(a^3+a+1)\,y^2$ $+(a^2+a)\,xy+a^3x^2+(a^3+a^2+a+1)\,x+a^2$ $y^3+a^2xy^2+(a^3+a^2+a)\,x^2y+(a^2+a)\,y^2+(a^3+a+1)\,xy$ $+(a^3+a^2+1)\,x^2+(a^3+1)\,y+ax+a^3+a^2+a$

We run algorithm from $(0,0)$ to $(5,1)$ and we get the set of minimal polynomials for array of known syndromes. We denote the elements of $F((4,2))$ by f_{40}, f_{21}, f_{12} and f_{03}, with respect to the leading exponentials. To be complete we mention ex-polynomials related to generators of the Δ-set, i.e. $(3,0),(1,1),(0,2)$ and their discrepancies:

$$\begin{aligned}
g_{30}(x,y) =& x^3+\left(a^3+a^2+1\right)y^2+\left(a^3+a^2+a+1\right)xy+ax^2+\left(a^3+a+1\right)y\\
&+a^2x+a\\
d_{g30} =& a^3+a^2+a+1;\\
g_{11}(x,y) =& xy+(a+1)x^2+\left(a^3+a^2+1\right)x+a^2+a\\
d_{g11} =& a^3+a;\\
g_{02}(x,y) =& y^2+a^2xy+\left(a^3+a^2+a\right)x^2+\left(a^3+a^2+1\right)y+\left(a^3+a+1\right)x+1\\
d_{g02} =& a^3+a^2+a.
\end{aligned}$$

Now we can calculate unknown syndromes:

- order 26:

$$u_{4,2}=\begin{cases} a^3+a+1 \text{ by } f_{40},\\ a^3+1 \text{ by } f_{21},\\ a^3+a+1 \text{ by } f_{12}.\end{cases}$$

As the change of f_{40} and f_{12} would not cause change of Δ-set, their candidates have zero votes, however the change of f_{21} would increase size of Δ-set. Hence a^3+a has one vote and it is the right candidate. We set

$$u_{(4,2)} := a^3+1$$

and we update f_{40} and f_{12}:

$$\begin{aligned} f_{40}^{+} :=& f_{40} + \frac{d_{f_{40}}}{d_{g_{02}}} \cdot g_{02} = x^4 + \left(a^3+a^2+1\right)xy^2 + \left(a^3+a^2+a+1\right)x^2y \\ &+ ax^3 + \left(a^2+a\right)y^2 + \left(a^3+a^2\right)xy + \left(a^3+a^2+1\right)x^2 \\ &+ \left(a^3+a^2+1\right)y + x + a^3 + a^2, \\ f_{12}^{+} :=& f_{12} + \frac{d_{f_{12}}}{d_{g_{30}}} \cdot g_{30} = xy^2 + a^2x^2y + \left(a^3+a^2+1\right)x^3 \\ &+ \left(a^3+a^2+a+1\right)y^2 + a^2xy + \left(a^3+a^2+a\right)x^2 \\ &+ \left(a^3+a^2+a\right)y + (a+1)x + a. \end{aligned}$$

- order 27:

$$u_{(3,3)} = \begin{cases} a^2+a+1 \text{ by } f_{21}, \\ a^2+a+1 \text{ by } f_{12}^{+}, \\ a \text{ by } f_{03}. \end{cases}$$

a has zero votes and a^2+a+1 has two votes, hence we set

$$u_{(3,3)} := a^2+a+1$$

and we update polynomial f_{03}:

$$\begin{aligned} f_{03}^{+} :=& y^3 + a^2xy^2 + \left(a^3+a^2+a\right)x^2y + \left(a^3+a^2+a\right)x^3 + \left(a^3+a^2\right)y^2 \\ &+ \left(a^3+a^2+a\right)xy + ax^2 + y + \left(a^3+a^2+a+1\right)x + 1. \end{aligned}$$

- order 28:

$$u_{(2,4)} = \begin{cases} a^3+a+1 \text{ by } f_{21} \\ a^3+a+1 \text{ by } f_{12}^{+} \\ a^3+a+1 \text{ by } f_{03}^{+} \end{cases} \quad u_{(7,0)} = a^3+1 \text{ by } f_{40}^{+}.$$

The candidate for $u_{(2,4)}$ has three votes, on the other side the candidate for $u_{(7,0)}$ has zero votes. Hence we set

$$u_{(2,3)} := a^3+a+1$$

and we calculate $u_{(7,0)}$ as depend syndrome:

$$x^7 \equiv x^2y^4 + x^2y \Rightarrow u_{(7,0)} := u_{(2,4)} + u_{(2,1)} = a^2 + a^3.$$

Update of f_{40}^{+} :

$$\begin{aligned} f_{40}^{++} :=& x^4 + \left(a^3+a^2+1\right)xy^2 + \left(a^3+a^2+a+1\right)x^2y + \left(a^3+a^2\right)x^3 \\ &+ \left(a^3+a^2\right)y^2 + \left(a^3+1\right)xy + ax^2 + \left(a^2+1\right)y + \left(a^3+a^2\right)x + a + 1. \end{aligned}$$

If we consider syndromes corresponding to the pole order 29 or higher, we see that the change of any polynomial would cause increase of the Δ-set. We know that r has correctable number of errors (seven) and the size of Δ-set is already seven. Then the polynomials would not change anymore and $\{f_{40}^{++}, f_{21}, f_{12}^{+}, f_{03}^{+}\}$ is Gröbner basis of $I(u)$. The common zeros of $f_{40}^{++}, f_{21}, f_{12}^{+}, f_{03}^{+}$ are

$$\{(1, a+1), (a^3, a), (a^2+1, a^3), (a^2+a, a^3+a^2+a+1), (a^2+a+1, a^3+a),$$
$$(a^3+1, a^3+1), (a^3+a^2+1, a^3+a^2)\}.$$

Considering order of affine points the set of common zeros gives error positions

$$e_7, e_{17}, e_{27}, e_{37}, e_{47}, e_{57} \text{ and } e_{64}.$$

By solving equation

$$r \cdot H^T = x \cdot H^T, x_j = 0 \text{ for } j \notin \{7, 17, 27, 37, 47, 57, 64\},$$

where H is parity check matrix of $\mathcal{HC}_4^{49}$ we get error vector

$$\begin{aligned} e = (&0,0,0,0,0,0,a+1,0,0,0,0,0,0,0,0,0,a^2+a,0,0,0,0,0,0,0,0,0,\\ &a^3+a^2,0,0,0,0,0,0,0,0,0,a^3+a+1,0,0,0,0,0,0,0,0,0,a^2+1,0,0,\\ &0,0,0,0,0,0,0,a^3+a,0,0,0,0,0,0,a^2+a+1) \end{aligned}$$

and codeword

$$\begin{aligned} c = r - e = (&0,0,0,0,1,1,1,1,a^3+a+1,a^3+a+1,a^3+a+1,\\ &a^3+a+1,a^3+1,a^3+1,a^3+1,a^3+1,a^3+a^2,a^3+a^2,\\ &a^3+a^2,a^3+a^2,a^3+a^2+1,a^3+a^2+1,a^3+a^2+1,\\ &a^3+a^2+1,a^2+a,a^2+a,a^2+a,a^2+a,a^3+a^2+a+1,\\ &a^3+a^2+a+1,a^3+a^2+a+1,a^3+a^2+a+1,a+1,a+1,\\ &a+1,a+1,a^3+a^2+a,a^3+a^2+a,a^3+a^2+a,a^3+a^2+a,\\ &a^3,a^3,a^3,a^3,a^2+a+1,a^2+a+1,a^2+a+1,a^2+a+1,\\ &a^2,a^2,a^2,a^2,a^3+a,a^3+a,a^3+a,a,a,a,a,\\ &a^2+1,a^2+1,a^2+1,a^2+1). \end{aligned}$$

As c is evaluation of polynomial $x^7 \in \mathcal{L}(49 \cdot P_\infty)$, it is really an element of $\mathcal{HC}_4^{49}$.

Conclusion

In this thesis we presented encoding and decoding of algebraic geometry codes. For this purpose we described extension of Groebner basis and Berlekamp-Massey algorithm.

We used the way of description that clearly shows right functionality of algorithm. The both algorithms have various modification that are more efficient for practical problems. If we use some of these modifications it can considerably improve complexity of encoding and decoding.

The other way to improve complexity of syndrome decoding, is use of different calculation of error values. This method is described for example in [SakaJensHøho95].

The basic idea of use of majority voting for calculation of unknown syndromes came from G. L. Feng and T. R. N. Rao. However their algorithm is based on Gaussian elimination. For Hermitian code of length n this means, that algorithm by Feng and Rao has complexity $\mathcal{O}(n^3)$, on the other side algorithm by Sakata has complexity $\mathcal{O}(n^{\frac{7}{3}})$.

Bibliography

[HøhoLintPell11] T. Høholdt, J. H. van Lint, R. Pellikaan: *Algebraic geometry codes*, September 2011. `http://www.win.tue.nl/~ruudp/paper/31.pdf`

[Leon09] Leonard, D. A.: *A Tutorial on AG Code Construction from a Gröbner Basis Perspective*, Gröbner Bases, Coding, and Cryptography, pp. 93–106. Springer, 2009.

[Litt09] Little, J.B. : *Automorphism and Encoding of AG and Order Domain Codes*, Gröbner Bases, Coding, and Cryptography, pp. 107–120. Springer, 2009.

[Mora09] Mora, T.: *Gröbner Technology*, Gröbner Bases, Coding, and Cryptography, pp. 11–25. Springer, 2009.

[Saka88] Sakata, S.: *Finding a Minimal Set of Linear Recurring Relations Capable of Generating a Given Finite Two-dimensional Array*, J. Symbolic Comput. **5**, 321–337. 1988

[Saka90] Sakata, S. : *Extension of Berlekamp-Massey Algorithm to N Dimensions*, Inform. and Comput. **84**, 207–239. 1990

[Saka91] Sakata, S. : *A Groebner basis and a Minimal Polynomial Set of a Finite nD Array*, Applied Algebra, Algebraic Algorithms and Error-Correcting Codes. Lecture Notes in Computer Science Volume 508, pp 280-291. Springer, 1991.

[SakaJensHøho95] S. Sakata, H. E. Jensen, T. Høholdt: *Generalized Berlekamp-Massey Decoding of Algebraic-Geometric Codes up to Half the Feng-Rao Bound*, IEEE Trans. Inform. Theory, vol. 41, pp. 1762–1768, November 1995.

[Stic09] Stichtenoth, H.: *Algebraic function fields and codes, 2nd ed.* Graduate Texts in Mathematics. Springer, 2009.

[Wink96] Winkler, F.: *Polynomial Algorithms in Computer Algebra.* Texts and Monographs in Symbolic Computation. Springer, 1996.