Presentation of Normal Bases

Mohamadou Sall
mohamadou1.sall@ucad.edu.sn

University Cheikh Anta Diop, Dakar (Senegal)

Pole of Research in Mathematics and their Applications in Information Security (PRMAIS)

Institut de Mathématiques de Bordeaux, France

04 September 2017

Summary

Introduction

Interest in normal bases stems both from mathematical theory and practical applications.

- At the theory aspect normal bases are used for example in the implementation of the study of Galois correspondence.
- At the practical aspect, with the development of coding theory and the appearance of several cryptosystems using finite fields, the implementation of finite field arithmetic, in either hardware or software is required, which make use normal bases.

Constructive Galois Problem

A commutative ring $\mathbb{A}$ is a set, together with $'+'$ and $'\times'$, such that

1. $(\mathbb{A}, +)$ is a commutative group
2. The mutiplication is associative, commutative and has a unit element.
3. For all $x, y, z \in \mathbb{A}$ we have

$$(x+y)z = xz + yz \text{ and } z(x+y) = zx + zy$$

In this talk, ring means commutative ring

Definition

A field is a ring in which every non-zero element is invertible for $'\times'$. It is finite if its cardinality is finite. One denotes by $\mathbf{F}_q$ the finite field of order q.

Theorem (Main Result of Galois Theory)

Let $\mathbf{E}$ *be a finite Galois extension of a field* k*, with Galois group* $\mathbf{G}$*. There is a bijection between the set of subfields* $\mathbf{K}$ *of* $\mathbf{E}$ *containing* k*, and the set of subgroups* H *of* $\mathbf{G}$*, given by*

$$\mathbf{K} = \mathbf{E}^H = \{x \in \mathbf{E} : \sigma(x) = x \ \textit{ for all } \ \sigma \in H\}$$

The field $\mathbf{K}$ *is Galois over* k *if and only if* H *is normal in* $\mathbf{G}$*.*

In this talk one assumes H is a normal subgroup of $\mathbf{G}$

Lemma

The order of H is equal to the degree of $\mathbf{E}$ over $\mathbf{E}^H$. The index of H in $\mathbf{G}$ is equal to the degree of $\mathbf{E}^H$ over k

$$|H| = [\mathbf{E} : \mathbf{E}^H] \;\; \textit{and} \;\; [\mathbf{G} : H] = [\mathbf{E}^H : k]$$

Let $Aut(\mathbf{E}/\mathbf{K})$ be the set of all automorphisms of $\mathbf{E}$ that fix $\mathbf{K}$, ie

$$\mathbf{K} = \mathbf{E}^{Aut(\mathbf{E}/K)}$$

Problem

To realize the correspondence constructively, namely

1. *When given* $\mathbf{K}$, *find* $Aut(\mathbf{E}/\mathbf{K})$
2. *When given* H, *find* $\mathbf{E}^H$

- The first part of the problem is easy :

  $$\text{suppose that } \mathbf{K} = k(\beta_1, \cdots, \beta_k) \text{ where } \beta_i \in \mathbf{E}$$

- For the 2^{nd} part of the problem, normal bases offer an elegant solution.

Constructive Galois Problem and Normal Basis

Let **E** be a Galois extension of degree n of a field k with Galois group **G**.

Definition

A normal basis N of a finite Galois extension **E** of k is a basis of the form $\{\sigma_1\alpha, \cdots, \sigma_n\alpha\}$ where $\sigma_i \in Gal(\mathbf{E}/k)$ and α is a fixed element of **E**.

The element α is called **normal element** of E over k.

Theorem (The normal basis theorem)

There is a normal basis for any finite Galois extension of fields.

Normal Basis History

- For finite fields
  - The normal basis theorem was conjectured by Eisenstein in 1850 and partly proved by Schonemann at the same year,
  - In 1888 Hensel gives its complete proof
- For arbitrary fields
  - Noether in 1932 and Deuring in 1933 prove the normal basis theorem for Galois extension of arbitrary fields.
  - Lenstra generalizes the normal basis theorem to infinite Galois extensions.
- Different proofs of this theorem were given by Artin, Berger and Reiner, Krasner, Waterhouse, ...

Let $N = \{\sigma(\alpha) \ : \ \sigma \in \mathbf{G}\}$ be a normal basis of $\mathbf{E}$ over k. Let

$$n = [G : H]$$

and let the right coset decomposition of $\mathbf{G}$ relative to H be

$$\mathbf{G} = \bigcup_{i=1}^{n} Hg_i, \ g_i \in \mathbf{G}$$

Definition

One calls Gauss periods of N with respect to H the elements

$$\zeta_i = \sum_{\sigma \in H} g_i(\sigma(\alpha)), \quad g_i \in \mathbf{G}$$

for $1 \leq i \leq n$.

Theorem

The Gauss periods $\zeta_1, \cdots, \zeta_n$ form a basis of $\mathbf{E}^H$ over k.

$$E^H = k\zeta_1 \oplus k\zeta_2 \oplus \cdots \oplus k\zeta_n$$

Indeed

- they are linearly independent

$$\sum \lambda_i \zeta_i = 0 \Leftrightarrow \sum \lambda_i \sum_{\sigma \in H} g_i(\sigma(\alpha)) = 0 \Leftrightarrow \sum \lambda_i \sum_{\sigma \in g_i H} \sigma(\alpha) = 0$$

- for all i, $\zeta_i \in \mathbf{E}^H$

$$\delta \in H,\ \delta(\zeta_i) = \sum_{\sigma \in H} \delta(g_i(\sigma(\alpha))) = \sum_{\sigma \in H} g_i(\delta' \circ \sigma(\alpha)) = \zeta_i$$

Remark

If one can construct a NB, then one can solve the 2^{nd} part of the problem

Overview of Finite Fields Arithmetic

Definitions and Properties

Theorem (Existence and uniqueness of finite fields)

For every prime p and every integer $r > 0$ there exists a finite field with p^r elements, that is isomorphic to $\mathbf{F}_{p^r}$.

There are two types of finite fields :

- Prime finite fields, $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$ where p is a prime integer.
- Finite fields $\mathbf{F}_q$ where $q = p^r$, is such that $r > 1$ and p a prime integer.

The extension $\mathbf{F}_{q^n}$ is a vector space of dimension n over $\mathbf{F}_q$.

Definitions and Properties

The Frobenius automorphism is the map

$$\begin{array}{rccc} \sigma: & \mathbf{F}_{q^n} & \rightarrow & \mathbf{F}_{q^n} \\ & x & \mapsto & x^q \end{array}$$

which generates the Galois group of $\mathbf{F}_{q^n}$ over $\mathbf{F}_q$.

General Operations

Assume that $\alpha_0,\ \alpha_1,\ \cdots,\ \alpha_{n-1} \in \mathbf{F}_{q^n}$ are linearly independent over $\mathbf{F}_q$.

$$\begin{array}{rlcl} \Psi: & \mathbf{F}_{q^n} & \longrightarrow & \mathbf{F}_q^n \\ & A = \sum_{i=0}^{n-1} a_i\alpha_i & \longmapsto & (a_0, \cdots, a_{n-1}) \end{array}$$

is an isomorphism of $\mathbf{F}_q-$vector spaces. We have two operations in $\mathbf{F}_{q^n}$:

1. **Addition** : which is component-wise and easy to implement

$$(a_0, \cdots, a_{n-1}) + (b_0, \cdots, b_{n-1}) = (a_0 + b_0, \cdots, a_{n-1} + b_{n-1})$$

2. **Multiplication** : which needs a multiplication table.

The difficulty of operations in $\mathbf{F}_{q^n}$ depends on the particular way in which the field elements are represented.

Naive Multiplication over $\mathbf{F}_{q^n}$

Let $C = (c_0, c_1, \cdots, c_{n-1})$ be the product $A \times B$, where

$$A = \sum_{i=0}^{n-1} a_i \alpha_i \text{ and } B = \sum_{j=0}^{n-1} b_j \alpha_j$$

$$A.B = \sum_{0 \leq i,j \leq n-1} a_i b_j \alpha_i \alpha_j$$

The cross-products

$$\alpha_i \alpha_j = \sum_{k=0}^{n-1} t_{ij}^{(k)} \alpha_k, \text{ and } c_k = A T_k B^t$$

$T_k = (t_{ij}^k)$ is a $n \times n$ matrix over $\mathbf{F}_q$ which is independent from A and B.

Drawbacks

If n is big then a multiplication algorithm in the previous way on an arbitrary basis is impractical.

Naive Multiplication over $\mathbf{F}_{q^n}$

To simplify multiplication over $\mathbf{F}_{q^n}$ and make a hardware or software design of a finite field arithmetic feasible for large n, we may find bases for which

- the matrices T_k have more regularity or
- fewer non-zero entries

Normal bases can be good candidates ! ! !

Fast arithmetic using normal bases

Normal Bases

Recall that over finite field, the Galois group is generated by Frobenius map

Definition

A normal basis of $\mathbf{F}_{q^n}$ over $\mathbf{F}_q$ is a basis of the form $\{\alpha, \alpha^q, \cdots, \alpha^{q^{n-1}}\}$ where α is a fixed element of $\mathbf{F}_{q^n}$.

Theorem (normal basis theorem)

For any prime power $q = p^r$, and positive integer n, there exist a normal basis of $\mathbf{F}_{q^n}$ over $\mathbf{F}_q$.

Characterization of Normal Elements

Let

$$\begin{cases} x^n - 1 = (\psi_1(x)\psi_2(x)\cdots\psi_r(x))^t,\ \psi_i \ \text{ irreducible and } deg(\psi_i) = d_i \\ \Phi_i = \frac{x^n-1}{\psi_i} \end{cases}$$

Theorem (Schwarz)

An element $\alpha \in \mathbf{F}_{q^n}$ is a normal element of $\mathbf{F}_{q^n}$ over $\mathbf{F}_q$ if and only if

$$\Phi_i(\sigma)\alpha \neq 0,\ i = 1, 2, \cdots, r.$$

Complexity of normal basis

In a normal basis $\{\alpha, \cdots, \alpha_{n-1}\}$, computing A^q is negligeable since

$$A^q = \sum_{i=0}^{n-1} \left(a_i \alpha^{q^i}\right)^q \Rightarrow \Psi(A^q) = (a_{n-1}, a_0 \cdots, a_{n-2})$$

Let's consider the cross-products

$$\alpha_i \alpha_j = \sum_{k=0}^{n-1} t_{ij}^{(k)} \alpha_k$$

By raising both sides to the q^{-l} power, one finds that

$$t_{ij}^{(l)} = t_{i-l,j-l}^{(0)} \text{ for } 0 \leq i, j, l \leq n-1$$

Then one gets regularity between the T_k matrix.

Complexity of normal basis

Let T_0 defined by the matrix (t_{ij}^0)

$$T_0 = \begin{pmatrix} t_{00}^{(0)} & t_{01}^{(0)} & t_{02}^{(0)} & \cdots & t_{0,n-1}^{(0)} \\ t_{10}^{(0)} & t_{11}^{(0)} & t_{12}^{(0)} & \cdots & t_{1,n-1}^{(0)} \\ \vdots & \vdots & \cdots & & \vdots \\ t_{n-1,0}^{(0)} & t_{n-1,1}^{(0)} & t_{n-1,2}^{(0)} & \cdots & t_{n-1,n-1}^{(0)} \end{pmatrix}$$

Definition

The complexity of the normal basis N, denoted by C_N, is equal to the number of non-zero entries in the matrix T_0

Optimal Normal Basis

Theorem

Let C_N be the complexity of the normal basis N of $\mathbf{F}_{q^n}$ over $\mathbf{F}_q$, then $C_N \geq 2n - 1$.

Definition (Optimal Normal Basis)

A normal basis N of $\mathbf{F}_{q^n}$ over $\mathbf{F}_q$ is said to be optimal if $C_N = 2n - 1$.

Note that multiplication can be done with $2nC_N$ operations.

Then one has to work more to improve multiplication

Practical Construction of Normal Bases

Objective

To get quasi linear complexity

Trick

To adapt fast multiplication algorithm (like FFT) to normal basis.

Gauss Periods

Definition

Let $r = nk + 1$ be a prime number not dividing q and γ a primitive $r - th$ root of unity in $\mathbf{F}_{q^{nk}}$. Let K be the unique subgroup of order k of $\mathbf{Z}_r^*$ and $K_i \subseteq \mathbf{Z}_r$ be a coset of K, $0 \leq i \leq n-1$. The elements

$$\alpha_i = \sum_{a \in K_i} \gamma^a \in \mathbf{F}_{q^n},\ 0 \leq i \leq n-1$$

are called Gauss period of type (n, k) over $\mathbf{F}_q$.

Gauss Periods

When does a Gauss period generate a normal basis ? ? ?

Theorem (Wasserman condition)

A Gauss periods α_i of type (n, k) generates a normal basis in $\mathbf{F}_{q^n}$ iff

$$gcd(nk/e, n) = 1$$

where e is the index of q modulo r.

Gauss Periods

General strategy of multiplication complexity reduction

- Set $\mathcal{R} = \mathbf{F}_q[X]/\Phi_r$, where Φ_r is the $r - th$ cyclotomic polynomial
- Defines an injective homomorphism

$$\varphi : \quad \mathbf{F}_{q^n} \quad \longrightarrow \quad \mathcal{R}$$

- The elements of $\varphi(\mathbf{F}_{q^n})$ can be viewed as a polynomial in $\mathbf{F}_q[X]$.
- For $A, B \in \mathbf{F}_{q^n}$, $\varphi^{-1}\left((\varphi(A)\varphi(B))\right)$ is the product of A and B in $\mathbf{F}_{q^n}$

These leads to the following theorem.

Gauss Periods

Theorem (Gao et al)

Suppose that $\mathbf{F}_{q^n}$ is represented by a normal basis over $\mathbf{F}_q$ generated by a Gauss period of type (n, k). Then multiplication in $\mathbf{F}_{q^n}$ can be computed with $O(nk \log(nk) \log\log(nk))$ operations in $\mathbf{F}_q$.

Drawbacks

- *Normal bases with Gauss periods do not always exist and*
- *even they exist they are not always efficient*

Then

further works are needed

We will see some of them this week.

Example with Pari/GP

Let $P(x) = x^3 + x^2 + 1$ be a polynomial over $\mathbf{F}_2[X]$

```
? \\ Test if the polynomial P(x)=x^3+x^2+1 is irreducible
? P=(x^3+x^2+1)*Mod(1,2)
%1 = Mod(1, 2)*x^3 + Mod(1, 2)*x^2 + Mod(1, 2)
? polisirreducible(P)
%2 = 1
```

$P(x)$ is irreducible then one defines the fields $\mathbf{F}_{2^3}$. Find a root A of P

```
? A=ffgen(P)
%3 = x
```

Example with Pari/GP

- Factoring the polynomial $x^3 + 1$

```
? lift(factormod((x^3-1)*Mod(1,2), 2))
%5 =
[      x + 1 1]

[x^2 + x + 1 1]
```

- Define irreducible polynomials

```
? f1(x)=(x+1)*Mod(1,2)
%6 = (x)->(x+1)*Mod(1,2)
? f2(x)=(x^2+x+1)*Mod(1,2)
%7 = (x)->(x^2+x+1)*Mod(1,2)
```

Example with Pari/GP

- **Test if A is a normal element**
  - $f1(\sigma)A = (\sigma + id)A = \sigma(A) + A = A^2 + A$
  - $f2(\sigma)A = A + A^2 + A^4$

  These two values are non-zero elements, since

```
? A^2+A
%8 = x^2 + x
? A^4+A^2+A
%9 = 1
?
```

- According to Schwarz's theorem A is a normal element of $\mathbf{F}_{2^3}$ over $\mathbf{F}_2$.

Hense (A, A^2, A^4) is a normal basis of $\mathbf{F}_{2^3}$ over $\mathbf{F}_2$

Conclusion

Multiplication over finite field is an complex operation. For it's implementation a certain representation of the elements of the field is requiert. Normal bases are a good alternative. Thus finding normal bases over finite field that are **optimal** or with **low complexity** is an active area of research.

Computation of normal basis includes :

- Gauss Periods
- Elliptic Curves
- General Algebraic Group

The End

Thank you for your attention ! ! !