

1 Notes Thursday 11-30-06

1.1 Complexity of Multiplication

Suppose $V = \{v_1, \dots, v_n\}$ is a basis of $\mathbf{F}_{q^n}/\mathbf{F}_q$. So every element of \mathbf{F}_{q^n} is $\sum a_i v_i$ $a_i \in \mathbf{F}_q$.

$$\left(\sum a_i v_i\right)\left(\sum b_i v_i\right) = \sum a_i b_j v_i v_j \quad (1)$$

Now we need to know how to multiply the basis elements. Suppose:

$$v_i v_j = \sum m_{ijk} v_k, \quad (2)$$

then

$$\sum a_i b_j v_i v_j = \sum_k \left(\sum_{i,j} a_i b_j m_{ijk}\right) v_k \quad (3)$$

This requires about n^3 multiplications in \mathbf{F}_q plus several additions, unless several of the m_{ijk} vanish. This motivates the following definition:

Definition: The multiplicative complexity of the basis V is $\mu(V)$ defined as $\#\{i, j, k | m_{ijk} \neq 0\} \leq n^3$

Question (open): What is the minimum $\mu(V)$ over all V for a fixed extension $\mathbf{F}_{q^n}/\mathbf{F}_q$?

If $\mathbf{F}_{q^n} = \mathbf{F}_q[x]/f(x)$ and α is a root of $f(x)$ in \mathbf{F}_{q^n} , then $V = \{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$ is a power basis of \mathbf{F}_{q^n} . We need to compute $\alpha^i \alpha^j = \alpha^{i+j}$ which is in V for $i+j < n$.

So $m_{ijk} = \begin{cases} 1 & k = i+j, \\ 0 & \text{if not} \end{cases}$ in this case. So $\mu(V) \leq n^2/2 + n^3/2 + O(n)$.

If $f(x) = x^n + g(x)$ where $\deg(g) = t$ is small, $\alpha^i \alpha^j = \alpha^{i+j} = \alpha^{i+j-n} \alpha^n = -\alpha^{i+j-n} g(x)$, $i+j \geq n$.

$\alpha^{i+j-n}, \alpha^{i+j-n+1}, \dots, \alpha^{i+j-n+t}$ are basis elements if $i+j-n+t \leq n$, i.e. $i+j < 2n-t$. We have $\mu(V) \leq n^2/2 + (n^2-t^2)(t+1)/2 + t^2 n/2 + O(n)$.

The main term, when $t \neq 0$ is $n^2 t/2$. So if $t \sim \log n$, we get a basis with multiplicative complexity $n^2 \log n$. We conjecture that we can always find a polynomial that gives us this.

Question: Is the minimum of $\mu(V)$ of the order $O(n^2 \log n)$?

Proposition 1 $\mu(V) \geq n^2$, for any basis.

Proof: Multiplication by v_i is an invertible linear map $\mathbf{F}_{q^n} \rightarrow \mathbf{F}_{q^n}$ with matrix $(m_{ijk})_{j,k}$ so that $\det(m_{ijk})_{j,k} \neq 0$. Each row must be nonzero. i.e. for all i, j there exists k such that $m_{ijk} \neq 0$. So $\mu(V) \geq n^2$.

Returning to the example $f(x) = x^n + g(x)$, if $t = 0$ (i.e. $g(x) = c \in \mathbf{F}_q$) you get $\mu(V) = n^2/2 + n^2/2 = n^2$. If $f(x) = x^n + c$, we can write a multiplication table:

$\alpha_i \alpha_j = \begin{cases} \alpha^{i+j} & i+j < n, \\ -c\alpha^{i+j-n} & i+j \geq n \end{cases}$. This covers all the cases, so $\mu(V) = n^2$ in this case.

Exercise: You can find irreducible $x^n + c \in \mathbf{F}_q[x]$ if and only if $n|(q-1)$.

1.2 Heuristic for irreducibles of the type

$$x^n + g(x), \deg(g) = t$$

The probability that a polynomial of degree n in $\mathbf{F}_q[x]$ is irreducible is about $1/n$. So the probability that all $x^n + g(x)$ are reducible should be $(1 - 1/n)^{q^t}$. If

$$q^t = n, (1 - 1/n)^n \sim 1/e \quad (4)$$

If

$$q^t = n^2, (1 - 1/n)^{n^2} \sim 1/e^n. \quad (5)$$

So we hope $q^t = n^2$ is enough, i.e. $t = 2 \log n / \log q$ should do it for large n and fixed q . This motivates the conjecture that $\min \mu(V) \sim (n^2 \log n)$.

Example: Suppose $n = l - 1$, l prime, l does not divide q , and assume that $\frac{x^l - 1}{x - 1}$ is irreducible in $\mathbf{F}_q[x]$. So $\mathbf{F}_{q^n} = \mathbf{F}_q(\zeta)$, ζ is a primitive l^{th} root of unity, and $\{1, \zeta, \zeta^2, \dots, \zeta^{l-2}\}$ is a basis for $\mathbf{F}_{q^n}/\mathbf{F}_q$; since $\zeta^l = 1$, we have:

$$\zeta^i \zeta^j = \begin{cases} \zeta^{i+j} & i+j \leq l-2 \\ -1 - \zeta - \zeta^2 - \dots - \zeta^{l-2} & i+j = l-1 \\ \zeta^{i+j-l} & i+j \geq l \end{cases}$$

Then $\mu(V) \sim 2l^2 \sim 2n^2$. So this is a good basis.

Exercise: Under the same hypothesis, $\mathbf{F}_{q^{n/2}} = \mathbf{F}_q(\zeta + \zeta^{-1})$. So $V = \{\zeta + \zeta^{-1}, \zeta^2 + \zeta^{-2}, \dots, \zeta^{n/2} + \zeta^{-n/2}\}$ is a basis for $\mathbf{F}_{q^{n/2}}/\mathbf{F}_q$. Playing around with this gives: $\mu(V) \sim 2(n/2)^2 \sim n^2/2$.

If L/K is Galois with group G , a normal basis of L/K is a basis of the form $\{\sigma\alpha\}_{\sigma \in G}$ for some $\alpha \in L$.

Theorem 1 *Every Galois extension has a normal basis.*

In the case of finite fields, $\mathbf{F}_{q^n}/\mathbf{F}_q$, G is generated by $x \mapsto x^q$. So a normal basis is $\{\alpha, \alpha^q, \alpha^{q^2}, \dots, \alpha^{q^{n-1}}\}$.

The two examples with l^{th} roots of unity are examples of normal bases.

Proposition 2 $\mu(V) \geq n(2n - 1)$ for a normal basis V .

When this lower bound is obtained, V is called an optimal normal basis. The two previous examples are the only two examples of optimal normal bases.

Proof: Let $\sigma(x) = x^q$. If

$$\alpha\sigma^i\alpha = \sum m_{ij}\sigma^j\alpha, \quad (6)$$

then

$$\sigma^i\alpha\sigma^j\alpha = \sigma^i(\alpha\sigma^{j-i}\alpha) = \sum (m_{(j-i)k}\sigma^{j+k}\alpha). \quad (7)$$

So $m_{ijk} = m_{(j-i)(k-j)}$. Each of the m_{ij} repeats n times. So

$$\mu(V) = n(\#\{i, j | m_{ij} \neq 0\}) \quad (8)$$

On the other hand,

$$\alpha Tr(\alpha) = \sum_{i=0}^{n-1} \alpha\sigma^i\alpha = \sum_j (\sum_i m_{ij})\sigma^j\alpha \quad (9)$$

which implies that $\sum m_{i0} = Tr(\alpha)$, $\sum m_{ij} = 0$, $j \neq 0$. By the same determinant argument from the previous proposition, then for all j there exists i with $m_{ij} \neq 0$. But if $j \neq 0$ since $\sum m_{ij} = 0$ there must be at least two nonzero m_{ij} . So $\#\{i, j | m_{ij} \neq 0\} \geq 2n - 1$.

Exercise: Compute $\mu(1, \alpha, \alpha^2, \dots, \alpha^{n-1})$ if $\alpha^n + \alpha^m + 1 = 0$ $1 \leq m < n/2$.

Going back to

$$(\sum a_i v_i)(\sum b_j v_j) = \sum_k (\sum m_{ijk} a_i b_j) v_k = \sum B_k v_k \quad (10)$$

where

$$B_k(a_1, \dots, a_n, b_1, \dots, b_n) = \sum m_{ijk} a_i b_j \quad (11)$$

is a bilinear form. One can try to write B_k as $B_k = \sum_{m=1}^M L_{mk}(a) M_{mk}(b)$ where the L_{mk} , M_{mk} are linear forms. Then the number of multiplications in the ground field decreases if M is smaller than n^2 there is a gain. There is some clever trickery with algebraic curves to do this.