The Number of Polynomial Basis Sets of a Finite Field

Dan Brown and Scott Vanstone

October 28, 2008

Abstract

We find the number of subsets of a finite field extension that can form a polynomial basis.

1 Problem

A *polynomial basis set* of a finite field $\mathbb{F}_{q^m}$ over a field $\mathbb{F}_q$ is defined as a subset of $\mathbb{F}_{q^m}$ of the form

$$P(a) = \{1, a, a^2, \ldots, a^{m-1}\} \tag{1}$$

whose elements are linearly independent as vectors over the field $\mathbb{F}_q$, or equivalently, whose elements span the $\mathbb{F}_q$-vector space $\mathbb{F}_{q^m}$. The set $P(a)$ will form a polynomial basis set if and only if $a \in \mathbb{F}_{q^m}$ has degree m over $\mathbb{F}_q$.

A well known result, [2, Theorem 3.25], going back to Gauss for the case of prime q, is that the number $D_q(m)$ of elements of degree m over $\mathbb{F}_q$ is,

$$D_q(m) = \sum_{d|m} \mu(m/d) q^d \tag{2}$$

where $\mu(\cdot)$ is the Möbius function. This can be proved by the inclusion-exclusion principle, which is to say, Möbius inversion. (An equivalent way to state this result is that the number of irreducible polynomials of degree m over $\mathbb{F}_q$ is $D_q(m)/m$.)

Polynomial bases are more usually defined as ordered sequences:

$$Q(a) = (1, a, \ldots, a^{m-1}), \tag{3}$$

instead of as sets. For $m \geqslant 2$, $a \mapsto Q(a)$ is a bijection. The number of a of degree m exactly equals the number $B_q(m)$ of ordered polynomial bases, so $B_q(m) = D_q(m)$. For $m = 1$, the only ordered basis of the form in equation (3) is the ordered tuple (1). Therefore, $B_q(1) = 1$, whereas $D_q(1) = q - 1$.

This paper looks at the number $U_q(m)$ of polynomial basis sets, as defined in (1). In other words, we seek to count the the number *unordered* polynomial bases. This number could possibly be smaller than the number of ordered polynomial bases if $m \geqslant 2$ and

$$P(a) = P(b) \tag{4}$$

for some $a \neq b$, which we will call a *collision* of polynomial basis sets. We will show that $U_q(m) = B_q(m)$; that is, there are no collisions of polynomial basis sets. We henceforth assume that $m \geqslant 2$.

2 Solution

Suppose that $P(a) = P(b)$, with $a \neq b$. Because $b \in P(b) = P(a) = \{1, a, \ldots, a^{m-1}\}$, we must have $b = a^g$ for some $g \in \{0, 1, \ldots, m-1\}$. The case $g = 1$ is excluded because $a \neq b$. The case $g = 0$ is excluded because $m \geqslant 2$.

Let n be the multiplicative order of a. A polynomial basis set collision $\{1, a, \ldots, a^{m-1}\} = P(a) = P(a^g) = \{1, a^g, \ldots, a^{g(m-1)}\}$ is equivalent to the following condition

$$\{0, 1, 2, \ldots, m-1\} \equiv \{0, g, 2g, \ldots, (m-1)g\} \bmod n, \tag{5}$$

where the modular reduction applies to all elements of the sets. Solving (5) will thus determine all polynomial basis set collisions.

For $m = 0$, $m = 1$ and $m \geqslant n$, there may be solutions to (5) for certain choices of g, but that these do not correspond to polynomial basis set collisions. The case $m = 0$ represents the empty set, and is degenerate in the sense it does not correspond to any field extension. The exceptional case $m = 1$ has already been excluded from the definition of a polynomial basis set collision.

To exclude the case $m \geqslant n$, we will show that $a \in \mathbb{F}_{q^m}$ has order $n > m$. To see this note that $a^n - 1 = 0$, so a is a root of a polynomial of degree n. This polynomial $x^n - 1$ is not irreducible over $\mathbb{F}_q$, since it has a factor $x - 1$. Therefore, the irreducible polynomial of a over $\mathbb{F}_q$ is a proper factor of $x^n - 1$ and therefore has degree smaller than n. But m is defined to be the degree of this irreducible, thus $m < n$. This implies $m \not\equiv 0, 1 \bmod n$ because $m \geqslant 2$ is assumed, a fact that will be used towards the end of the proof.

Noticing that (5) does not involve q, we are free to solve it without referring to $\mathbb{F}_q$ at all. We can see that (5) is equivalent to

$$1 + x^g + \cdots + x^{(m-1)g} \equiv 1 + x + \cdots + x^{m-1} \bmod x^n - 1, \tag{6}$$

as polynomials in $\mathbb{Z}[x]$, where the polynomial modulus $x^n - 1$ now accounts for the modulus n in (5). This is equivalent to $(x^n - 1) \mid G(x)$, where

$$\begin{aligned} G(x) &= (1 + x^g + \cdots + x^{(m-1)g}) - (1 + x + \cdots + x^{m-1}) \\ &= \frac{x^{gm} - 1}{x^g - 1} - \frac{x^m - 1}{x - 1} \\ &= \frac{(x^{gm} - 1)(x - 1) - (x^m - 1)(x^g - 1)}{(x^g - 1)(x - 1)} \\ &= \frac{F(x)}{(x^g - 1)(x - 1)} \end{aligned} \tag{7}$$

where the numerator $F(x)$ expands as:

$$F(x) = x^{gm+1} + x^g + x^m - x^{gm} - x^{g+m} - x. \tag{8}$$

Now clearly $(x^n - 1) \mid F(x)$, because $F(x) = G(x)(x - 1)(x^g - 1)$ and $(x^n - 1) \mid G(x)$. In other terms, $F(x) \equiv 0 \bmod (x^n - 1)$, which is equivalent to

$$\{gm + 1, g, m\} \equiv \{gm, g + m, 1\} \bmod n \tag{9}$$

because one can reduce exponents in (8) modulo n. (Just to be clear, in (9), the left and right hand sides may possibly be multi-sets, with repeated elements.)

We show that $g \notin \{gm, g + m, 1\} \bmod n$, contradicting (9), as follows:

- Above, we showed that $g \in \{2, \ldots, m-1\}$ and $m < n$. Therefore $g \not\equiv 1 \bmod n$.
- Above, we showed $m \not\equiv 0 \bmod n$, Therefore we have $g \not\equiv g + m \bmod n$.
- By supposition, $a \in P(b)$, so $a = b^h$ for some $h \in \{0, 1, \ldots, m-1\}$. Therefore, $a = b^h = a^{gh}$ and $gh \equiv 1 \bmod n$. Suppose that $g \equiv gm \bmod n$ and multiply through by h so get $1 \equiv gh \equiv ghm \equiv m \bmod n$. Above, we saw that $m \not\equiv 1 \bmod n$, so $g \not\equiv gh \bmod n$, as desired.[1] (Alternatively, if $gm \equiv g \bmod n$, then (9) reduces to

  $$\{g+1, g, m\} \equiv \{g, g+m, 1\} \bmod n \tag{10}$$

  which implies that either $g + 1 \equiv g + m$ or $m \equiv g + m$ which are ruled out by $m \not\equiv 1$ and $g \not\equiv 0$, respectively.

Therefore (9) cannot hold. Polynomial basis set collisions do not exist. The number of ordered and unordered polynomial bases are the same: $U_q(m) = B_q(m)$.

References

[1] *XX Asian Pacific Mathematics Olympiad.* Mar. 2008. `http://www.kms.or.kr/competitions/apmo/data/08APMO-SOL.pdf`.

[2] R. Lidl and H. Niederreiter. *Finite Fields*, volume 20 of *Encycolopedia of Mathematics and Its Applications.* Cambridge University Press, second edition, 1997.

[1] This approach to this case using the coprimality of g and n is due to organizers of the APMO 2008 contest [1, Problem 5].