



# The Existence of Finite Fields

Scott A. Vanstone, FRSC  
Professor of Mathematics and  
Computer Science, University of  
Waterloo and Executive Vice  
President, Strategic  
Technologies--Certicom

# The Existence of Finite Fields

The existence of finite fields is well known (going back to Galois).

There are many proofs of this.

Most of these are well known to practitioners of the subject.

# Massey's Proof

Jim Massey's proof is to a certain extent constructive (I will make this clear in the rest of the lecture).

To me it is very intuitive and provides a proof of existence accessible to an undergraduate student.

It sheds a great deal of light on the structure of finite fields.

# Preamble to the Proof

Before we get to the proof, we need to present a few elementary results.

All results that we need for the proof are somewhat elementary.

We will point out non elementary results and how they can be proved.

# Best Known Proofs

Mobius inversion is one method.

Mullin has an elegant proof using generating functions.

These approaches are purely existential with no constructive proof.

# Important Lemma

- Let  $x^a - 1$  and  $x^b - 1$  be polynomials over  $\mathbf{F}_q$  where  $a$  and  $b$  are positive integers.  
 $x^b - 1$  divides  $x^a - 1$  iff  $b$  divides  $a$ .

Proof: Suppose  $b|a$ . Then  $a = kb$  for some integer  $k$ . Thus  $x^a - 1 = x^{kb} - 1$

$$= (x^b - 1)u(x)$$

for some polynomial  $u(x) \in \mathbf{F}_q(x)$ . Hence,  
 $x^b - 1$  divides  $x^a - 1$ .

# Lemma (continued)

Conversely, suppose  $x^b - 1 \mid x^a - 1$ . By the division algorithm  $a = kb + r$ , where

$0 \leq r < b$ . Now  $x^a - 1 = q(x)(x^b - 1)$  where  $q(x) \in \mathbf{F}_q(x)$ . But  $x^a - 1 = x^{kb+r} - 1$

$$= x^{kb}x^r - x^r + x^r - 1$$

$$= x^r (x^{kb} - 1) + (x^r - 1).$$

Since  $x^{kb} - 1$  is divisible by  $x^b - 1$ , we have that  $x^b - 1$  divides  $x^r - 1$  which is impossible unless  $r = 0$ .

# Corollary to Lemma

$$X^{q^b} - x \mid X^{q^a} - x \text{ iff } b \mid a.$$

Proof: By the Lemma  $X^{q^b} - x \mid X^{q^a} - x$  iff  $q^b - 1 \mid q^a - 1$ . Now  $q^b - 1 \mid q^a - 1$  iff  $b \mid a$ .

# Facts

Although we will not prove these here they are relatively easy to show.

- If there exists an irreducible polynomial of degree  $t$  over  $\mathbf{F}_q$  then there exists a finite field with  $q^t$  elements.
- If a finite field exists it has  $p^m$  elements where  $p$  is a prime number and  $m$  is a positive integer.

# Existence of Finite Fields of Prime Extension Degree

- The proof of the existence of finite fields having  $p^m$  elements will now be given.
- The proof is due to Jim Massey.
- It has been around for 40 years but never published.
- It is to some extent constructive in nature as opposed to the more well known proofs of existence.

# Massey's Existence Proof

- Let  $t$  be a prime number and  $\mathbf{F}_q$  be a finite field with  $q$  elements. Then there exists a finite field with  $q^t$  elements.

Proof:

$F(x) = x^{q^t} - x$  be a polynomial over  $\mathbf{F}_q$ . By the fundamental theorem of algebra  $F(x)$  factors into irreducible factors over  $\mathbf{F}_q(x)$ .

## Proof (continued)

The derivative of  $F(x)$  is  $-1$  and so the gcd of  $F(x)$  and  $F'(x)$  is  $1$  implying  $F(x)$  has no repeated factors.

Hence,  $F(x) = f_1(x) f_2(x) f_3(x) \dots f_u(x)$ .

Every element of  $\mathbf{F}_q$  is a root of  $F(x)$  so  $F(x)$  has exactly  $q$  linear factors. Since  $q < q^t$ ,  $F(x)$  has an irreducible factor of degree greater than 1.

Suppose  $f_1(x)$  has degree  $s > 1$ .

# Proof (continued)

$f_1(x)$  defines a finite field  $S$  with  $q^s$  elements over  $\mathbf{F}_q$ . Let  $a \in S$  be a root of  $f_1(x)$ .

Any element  $\beta \in S$  can be written as a linear combination of powers of  $a$ .

$\beta = \sum \lambda_i a^i$  where  $i$  ranges from 0 to  $s - 1$ .

We want show that  $\beta$  is a root of  $F(x)$ .

# Proof (continued)

$$\begin{aligned} F(\beta) &= \beta^{q^t} - \beta = (\sum \lambda_i a^i)^{q^t} - \beta \\ &= \sum \lambda_i^{q^t} a^{iq^t} - \beta \\ &= \sum \lambda_i a^{iq^t} - \sum \lambda_i a^i \end{aligned}$$

Observe that  $F(a) = a^{q^t} - a = 0$  since  $a$  is a root of  $F(x)$ . Thus  $a^{q^t} = a$ . Thus  $F(\beta) = 0$ .

## Proof (continued)

Since every element of  $S$  is a root of  $F(x)$  it follows that

$$x^{q^s} - x \mid x^{q^t} - x.$$

By the Corollary to the Lemma,  $s \mid t$ . Since  $s$  is greater than 1 and  $t$  is a prime we have that  $s=t$ .

## Proof (continued)

Since  $f_1(x)$  is an irreducible polynomial of degree  $t$  over  $\mathbf{F}_q$  there exists a finite field with  $q^t$  elements. This completes the proof.

Note: If we can factor polynomials over  $\mathbf{F}_q$  then we can construct finite fields of prime extension order. We now leverage this to construct finite fields for any extension degree.

# Existence of Finite Fields of Extension Degree $n$ for any Positive $n$

Let  $n$  be a positive integer with prime power factorization.

Suppose  $p^e$  is one of the prime power factors of  $n$ . Since  $p$  is a prime the previous result shows that we can construct a finite field with  $q^p$  elements.

If we now take a new  $q' = q^p$  then the previous result shows that there exists a finite field with  $(q')^p$  elements.

# Existence (continued)

Continuing in this fashion we can construct a finite field with  $q^{p^e}$  elements.

With this being our new  $q$  we can move on to the next distinct prime power in the factorization and iterate.

# Example

Construct  $F_2^6 = F_2^{2 \cdot 3}$

First construct  $F_2^2$

$$x^2 - x = x(x-1)(x^2+x+1)$$

Let  $f(x) = x^2 + x + 1$  and  $\alpha$  be a root.

The elements of  $F_2^2$  are  $0, 1, \alpha, \alpha^2$ .

Let  $q = 2^2$ . We now construct  $F_q^3$  as in the existence result.

## Example (continued)

Factor  $F(x) = x^{q^3} - x$  over  $F_2^2$

We know by the previous result that  $F(x)$  will factor as 4 linear polynomials and 20 irreducible cubics over  $F_2^2$

Of course, this tells us there are precisely 20 monic cubic irreducible polynomials over  $F_2^2$ .

We only need to find one of them to construct  $F_q^3$ .

## Example (continued)

Consider  $x^3+ax^2+bx+c$  over  $F_2^2$  .

There are 64 monic cubic polynomials over  $F_2^2$  .

Roughly  $1/3$  of these are irreducible.

If a cubic is reducible it must have at least one linear factor, hence a root in  $F_2^2$ .

## Example (continued)

Try  $f(x) = x^3 + a^2x + 1$

It is easily checked that  $f(x)$  has no roots in  $F_2^2$ .

So  $f(x) = x^3 + a^2x + 1$  is irreducible over  $F_2^2$ .

Let  $\beta$  be a root of  $f(x)$ .

That is  $\beta^3 + a^2\beta + 1 = 0$  or  $\beta^3 = a^2\beta + 1$ .

## Example (continued)

The elements of  $F_q^3$  are:

$$\{\lambda_0 + \lambda_1 \beta + \lambda_2 \beta^2 : \lambda_0, \lambda_1, \lambda_2 \in F_2^2\}$$

Let's do a simple calculation

$$(1 + a\beta + a\beta^2)(a + \beta + a^2\beta^2)$$

$$= a + \beta + a^2\beta^2 + a^2\beta + a\beta^2 + \beta^3 + a^2\beta^2 + a\beta^3 + \beta^4$$

$$= a + \beta + a^2\beta + a\beta^2 + (a^2\beta + 1) + a^2\beta^2 + a(a^2\beta + 1) + a^2\beta^2 + \beta$$

$$= a + a\beta^2 + \beta + a$$

$$= \beta + a\beta^2.$$

# Another Example

Let  $g(x) = a^2 + x + ax^2 + x^3$   
be a monic cubic polynomial over  $\mathbf{F}_2^2$ .

It is easily checked that  $g(x)$  is irreducible.

Let  $\beta$  be a root of  $g(x)$ . Then

$$a^2 + \beta + a\beta^2 + \beta^3 = 0.$$

Write  $\beta^3 = a^2 + \beta + a\beta^2 = (a^2, 1, a)$ .

# Some Powers of $\beta$

$$\beta^4 = (1, 1, a)$$

$$\beta^5 = (1, a^2, a)$$

$$\beta^6 = (1, a^2, 0)$$

$$\beta^7 = (0, 1, a^2)$$

$$\beta^8 = (a, a^2, 0)$$

$$\beta^9 = (0, a, a^2)$$

$$\beta^{10} = (a, a^2, a^2)$$

$$\beta^{11} = (a, 1, a)$$

$$\beta^{12} = (1, 1, a^2)$$

$$\beta^{12} = (1, 0, a)$$

$$\beta^{13} = (1, a^2, a^2)$$

$$\beta^{14} = (a, a, a)$$

$$\beta^{15} = (1, 0, 1)$$

$$\beta^{16} = (a^2, 0, a)$$

$$\beta^{17} = (1, 1, a^2)$$

$$\beta^{18} = (a, a, 0)$$

$$\beta^{19} = (0, a, a)$$

$$\beta^{20} = (1, a, 1)$$

$$\beta^{21} = (a^2, 0, 0)$$

# Every finite field $F$ with $q$ elements has a generator

Proof:

For  $q = 2$ , the result is trivial since  $q-1=1$  and the multiplicative identity has order 1.

For the remaining discussion,

assume  $q \geq 3$ . Let  $q-1 = p_1^{\lambda_1} p_2^{\lambda_2} \cdots p_t^{\lambda_t}$  where  $1 < p_1 < p_2 < \cdots < p_t$  are distinct primes and  $\lambda_i$ ,  $1 \leq i \leq t$ , are positive integers.

# Every finite field $F$ with $q$ elements has a generator

Our strategy is to find elements  $a_i \in \mathbf{F}_q^*$ ,  $1 \leq i \leq t$ , such that  $\text{ord}(a_i) = p_i^{\lambda_i}$

Since  $\text{gcd}(p_i^{\lambda_i}, p_j^{\lambda_j}) = 1$  provided  $i \neq j$ ,  $1 \leq i, j \leq t$ , then the element  $\zeta = \prod_{i=1}^t a_i$  has order  $\prod_{i=1}^t p_i^{\lambda_i} = q-1$ .

# Every finite field $F$ with $q$ elements has a generator

For notational simplicity, consider  $p_1^{\lambda_1}$  first and the equation  $y^{q-1/p_1} - 1 = 0$

Over the field  $F$ , this equation has at most  $(q-1)/p_1$  roots.

But  $(q-1)/p_1 < q - 1$  and thus there is an element  $a \in F$  that is not the root of this equation.

# Every finite field $F$ with $q$ elements has a generator

Define the field element  $\beta = a^{q-1/p_1}$ .

Since  $\beta^{p_1^{\lambda_1}} = a^{q-1} = 1$ , we see that

$\text{ord}(\beta) \mid p_1^{\lambda_1}$ . We claim that  $\text{ord}(\beta) = p_1^{\lambda_1}$

Suppose  $\text{ord}(\beta) = p_1^e$  where  $e < \lambda_1$ .

Then  $\beta^{p_1^e} = 1$  which implies that  $\beta^{p_1^{\lambda_1-1}} = 1$ .

Now  $\beta^{p_1^{\lambda_1-1}} = a^{q-1/p_1} = 1$  implying that  $a$  is a root of  $y^{q-1/p_1} - 1$  which is a contradiction.

# Every finite field $F$ with $q$ elements has a generator

We conclude that  $\text{ord}(\beta) = p_1^{\lambda_1}$  .

Let  $\alpha_i = \beta$ . Similar argument applies to  $p_2^{\lambda_2} p_3^{\lambda_3} \cdots p_t^{\lambda_t}$  producing  $\alpha_i$  with  $\text{ord}(\alpha_i) = p_i^{\lambda_i}$  ,  $1 \leq i \leq t$  .

This completes the proof.

# $\beta$ as a Primitive Element (Generator)

The possible orders for  $\beta$  are divisors of 63. That is, 1, 3, 7, 9, 21, 63.

The previous slide shows that  $\beta$  does not have order 1, 3, 7, 9, 21.

Hence  $\beta$  has order 63 and is a generator for the multiplicative group of  $\mathbf{F}_2^6$

# B as a Root of a Sixth Degree Polynomial over $F_2$ .

Consider  $\prod(x-\beta^{2^i}) = \sum \lambda_i x^i$ ,  $0 \leq i \leq 5$ . Squaring both sides gives

$$(\prod(x-\beta^{2^i}))^2 = (\sum \lambda_i x^i)^2$$

or 
$$\prod(x^2 - \beta^{2^i}) = \sum \lambda_i^2 x^{2i}$$

Thus, 
$$\sum \lambda_i x^i = \sum \lambda_i^2 x^i$$

Equating coefficients gives  $\lambda_i = \lambda_i^2$ ,  $0 \leq i \leq 5$ . Hence,

$\lambda_i = 0$  or  $1$ .

## Example 2 (continued)

It is easy to see that  $\lambda_0 = 1$ . Let's compute  $\lambda_1$ .

$$\begin{aligned}\lambda_1 &= \beta^{62} + \beta^{61} + \beta^{59} + \beta^{55} + \beta^{47} + \beta^{31} \\ &= \beta^{31}(\beta^{31} + \beta^{30} + \beta^{28} + \beta^{24} + \beta^{16} + 1)\end{aligned}$$

## Example 2 (continued)

$$\beta^{31} = \beta^{21} \beta^{10} = (1, a, a)$$

$$\beta^{30} = \beta^{21} \beta^9 = (0, 1, a)$$

$$\beta^{28} = \beta^{21} \beta^7 = (0, a^2, a)$$

$$\beta^{24} = \beta^{21} \beta^3 = (a, a^2, 1)$$

$$\beta^{16} = (a^2, 0, a)$$

$$\beta^0 = (1, 0, 0)$$

---

$$(1, a^2, 1)$$

## Example 2 (continued)

$$\lambda_1 = \beta^{31}(1, a^2, 1) = \beta^{31} + a^2\beta^{32} + \beta^{33}$$

$$(1, a, a)$$

$$(a^2, a, a^2)$$

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

---

$$(1, 0, 0)$$

Hence  $\lambda_1 = 1$ .

## Example 2 (continued)

- Continuing, we see that  $\beta$  is a root of the binary irreducible polynomial

$$1 + z + z^4 + z^5 + z^6 .$$

We could now use this polynomial to construct the same field and avoid using  $\alpha$ .

# Consequences of the Proof

Let  $q^n$  be an integer where  $q$  is a power of a prime and  $n$  is a positive integer.

Let  $d$  be a divisor of  $n$ .

Then the finite field with  $q^d$  elements is a subfield of  $\mathbf{F}_q^n$ .

# Consequences of Proof (continued)

The factors of  $x^{q^n} - x$  are all of the irreducible polynomials of degree  $d$  where  $d$  divides  $n$ .

We have proved some rather deep results using somewhat elementary results.

# Conclusion

Massey's proof of existence is elementary but extremely elegant.

The proof is accessible to an undergraduate.

The proof is easy to follow and gives access to some of the deeper results in finite fields.