Primitive Elements on Lines in Extensions

Stephen D Cohen

University of Glasgow

Fq9, Dublin, 15 July, 2009

Definitions 1

θ generates $\mathbb{F}_{q^n}$ (over $\mathbb{F}_q$) if $\mathbb{F}_q(\theta) = \mathbb{F}_{q^n}$

θ_1, θ_2 (non-zero) generate $\mathbb{F}_{q^n}$ (over $\mathbb{F}_q$) if $\mathbb{F}_q(\theta_1, \theta_2) = \mathbb{F}_{q^n}$

A primitive element of $\mathbb{F}_{q^n}$ is a generator of the cyclic multiplicative group of $\mathbb{F}_{q^n}$. It has order $q^n - 1$

For any divisor k of $q^n - 1$, a k-free element γ of $\mathbb{F}_{q^n}^*$ is such that $\gamma = \beta^d$ ($\beta \in \mathbb{F}_{q^n}$, $d \mid k$) implies $d = 1$

- A primitive element of $\mathbb{F}_{q^n}$ is $(q^n - 1)$-free

- $\mathcal{Q}$ is the set of all prime powers

- Note: where appropriate, take q odd in what follows!

Translates problem

Theorem (Davenport, 1937; Carlitz, 1953)

Suppose θ generates $\mathbb{F}_{q^n}$. Then provided q is sufficiently large $\exists a \in \mathbb{F}_q$ such that $\theta + a$ is a primitive element of $\mathbb{F}_{q^n}$

Translates problem

Can we guarantee that $\exists a \in \mathbb{F}_q$ such that $\theta + a$ is a primitive element of $\mathbb{F}_{q^n}$ for every generator θ of $\mathbb{F}_{q^n}$?

Refer to the "line" $\{\theta + a : a \in \mathbb{F}_q\}$ as a "translate" of $\mathbb{F}_q$

Definition 2

$\mathcal{T}_n :=$ set of prime powers q such that, $\forall$ generators θ of $\mathbb{F}_{q^n}, \exists a \in \mathbb{F}_q$ such that $\theta + a$ is a primitive element of $\mathbb{F}_{q^n}$

$=$ prime powers s. t. every translate contains a primitive element

Theorem (Davenport-Carlitz)

Given n, all sufficiently large q are in $\mathcal{T}_n$ *$\mathcal{Q} \setminus \mathcal{T}_n$ is finite*

Line problem

Line problem
Can we guarantee that $\exists a \in \mathbb{F}_q$ such that $\theta_1 + a\theta_2$ is a primitive element of $\mathbb{F}_{q^n}$ whenever θ_1, θ_2 generate $\mathbb{F}_{q^n}$?

Alternative form (used from now on)
Given that α, θ generate $\mathbb{F}_{q^n}$, can we guarantee that $\exists a \in \mathbb{F}_q$ such that $\alpha(\theta + a)$ is a primitive element of $\mathbb{F}_{q^n}$?

- May be sensible even if θ itself does not generate $\mathbb{F}_{q^n}$

Reduction of line problem

Suppose $\mathbb{F}_q(\theta) = \mathbb{F}_{q^d}$ where $d|n$ with $d < n$

Write

- $Q_d = \frac{q^n-1}{q^d-1}$
- $R_d =$ largest factor of $q^d - 1$ with $\gcd(\frac{n}{d}, R_d) = 1$

Then

$$\alpha(\theta + a) \text{ is primitive } \iff \begin{cases} \alpha \text{ is } Q_d\text{-free and for some } \beta \in \mathbb{F}_{q^d} \\ \beta(\theta + a) \text{ is } R_d - \text{free in } \mathbb{F}_{q^d} \end{cases}$$

- Reduces this degree n line problem to one of degree d

Henceforth assume θ is a generator of $\mathbb{F}_{q^n}$

Definition 3

$\mathcal{L}_n :=$ set of prime powers q such that, $\forall$ generators θ of $\mathbb{F}_{q^n}$ and
$\alpha \in \mathbb{F}^*_{q^n}, \exists a \in \mathbb{F}_q$ such that $\alpha(\theta + a)$ is a primitive element of $\mathbb{F}_{q^n}$
$=$ prime powers s.t. all lines in $\mathbb{F}_{q^n}$ contain a primitive element

Explicit results

Quadratic extensions

Theorem 1 (Cohen, 1983)

$\mathcal{L}_2 = \mathcal{Q}$ *"All lines in $\mathbb{F}_{q^2}$ contain a primitive element"*

- Method establishes numerical criteria to be satisfied for $q \in \mathcal{Q}$
  - for large q
  - for remaining q in a reasonable number of steps

  - no $q \in \mathcal{Q}$ checked to be in $\mathcal{L}_2$ by direct verification

- computer not needed/used!

Cubic extensions

Theorem (Mills and McNay, 2002 (presented at $\mathbb{F}_q6$, 2001))

Subject to the non-existence of prime powers q in certain ranges with $18 \leq$ *no. distinct primes in* $(q^3 - 1) \leq 24$*,*
$\mathcal{Q} \setminus \mathcal{T}_3$ *is contained in a set of* 429 *prime powers (largest is* 220411*)*

Theorem 2 (conjectured: M & M 2002; proved: SDC 2009)

$\mathcal{T}_3 = \mathcal{Q} \setminus \{3, 7, 9, 13, 37\}$

Theorem 3 (Cohen, 2009)

$\mathcal{Q} \setminus \mathcal{L}_3 \subseteq \{3, 4, 5, 7, 9, 11, 13, 31, 37\} \bigcup \mathcal{S}$, *where* $\mathcal{S}$ *is a set of* 175 *prime powers, the largest being* 9811

Character sum expression

Let $\alpha, \theta \in \mathbb{F}_{q^n}$: $\alpha \neq 0$, θ generates $\mathbb{F}_{q^n}$

For $e | q^n - 1$,
$N(e) :=$ no. of e-free elements in $\{\alpha(\theta + a),\ a \in \mathbb{F}_q\}$ (given line)
$N := N(q^n - 1) =$ number of primitive elements on line

Proposition 4

$$N(e) = \rho(e) \left(q + \sum_{1<d|e} \frac{\mu(d)}{\phi(d)} \sum_{(d)} \chi_d(\alpha) S_\theta(\chi_d) \right)$$

Here

- $S_\theta(\chi) = \sum_{a \in \mathbb{F}_q} \chi(\theta + a)$, χ a multiplicative character of $\mathbb{F}_{q^n}$
- $\sum_{(d)}$ denotes a sum over all $\phi(d)$ characters of $\mathbb{F}_{q^n}$ of order d
- $\rho(e) = \frac{\phi(e)}{e}$ proportion of e-free elements in $\mathbb{F}_{q^n}^*$

Estimate for $S_\theta(\chi_d)$

Proposition 5 (Katz, 1989)

Suppose θ *generates* $\mathbb{F}_{q^n}$ *and* d (> 1) *divides* $q^n - 1$. *Then*

$$|S_\theta(\chi_d)| = \left| \sum_{a \in \mathbb{F}_q} \chi_d(\theta + a) \right| \leq (n-1)\sqrt{q}$$

- deep, in general
- relevance noticed by R Odoni, 1993
- easy in quadratic extensions (see later)

$$N(e) = \rho(e)\left(q + \sum_{1<d|e} \frac{\mu(d)}{\phi(d)} \sum_{(d)} \chi_d(\alpha) S_\theta(\chi_d)\right), \; S_\theta(\chi_d) = \sum_{a \in \mathbb{F}_q} \chi_d(\theta + a)$$

Proposition 6

Suppose $e|q^n - 1$. *Then* *for a given line* $\{\alpha(\theta + a) : a \in \mathbb{F}_q\}$

$$N(e) > \rho(e)(q - (n-1)2^{\omega(e)}\sqrt{q}); \quad \omega(e) = \#\{primes|e\}$$

Take $e = q^n - 1$ so that $N(e) = N$

Corollary 7

Suppose $q > (n-1)^2 2^{2\omega(q^n-1)}$. *Then* $q \in \mathcal{L}_n$

Corollary 8 (Davenport-Carlitz theorem)

Given n, $\exists q_0 = q_0(n)$ *such that, if* $q > q_0$, *then* $q \in \mathcal{L}_n$

Application to small degree extensions

Let $\omega_n := \omega(q^n - 1)$

Quadratic: $q > 2^{2\omega_2} \implies q \in \mathcal{L}_2$

Corollary 9

Suppose $q \notin \mathcal{L}_2$. *Then* $\omega_2 \leq 14$ *and* $q < 2.265 \times 10^8$

Proof.

Assumes "worst case": $q^2 - 1 = 8p_2 \cdots p_{\omega_2}$ (smallest primes) □

Cubic: $q > 4 \cdot 2^{2\omega_3} \implies q \in \mathcal{L}_3$

Corollary 10

Suppose $q \notin \mathcal{L}_3$. *Then* $\omega_3 \leq 52$ *and* $q < 2.203 \times 10^{32}$

Quartic: $q > 9 \cdot 2^{2\omega_4} \implies q \in \mathcal{L}_4$

Corollary 11

Suppose $q \notin \mathcal{L}_4$. *Then* $\omega_4 \leq 154$ *and* $q < 4.694 \times 10^{94}$

$S_\theta(\chi_d)$ in quadratic extensions

Proposition 12 (Cohen,1983)

Suppose $n = 2$ and θ generates $\mathbb{F}_{q^2}$. Let $d|q^2 - 1$.

1. *Assume $d(> 1)|q + 1$. Then $S_\theta(\chi_d) = -1$*
2. *Assume $d|q^2 - 1$, but $d \nmid q + 1$. Then $|S_\theta(\chi_d)| = \sqrt{q}$*

Proof.

Based on fact that $\{1, \theta\}$ is a basis of $\mathbb{F}_{q^2}/\mathbb{F}_q$.

- For $d|q + 1$, depends on $\chi_d(\theta + a) = \chi_d(c(\theta + a)),\ c \in \mathbb{F}_q^*$
- Otherwise $\{\frac{\theta+a}{\theta+b}; a, b \in \mathbb{F}_q\}$ is "most" of $\mathbb{F}_{q^2}$

□

Corollary 13

Suppose $e = f(q + 1), f$ (odd) with $\omega(f) = t$, $\omega(q + 1) = u$. Then

$$N(e) \geq \rho(e)(q - (2^t - 1)2^u\sqrt{q} - 1)$$

Norm Method for Quadratic Fields

Conjecture (Giudici, 1980 (extended))

All prime powers q are in $\mathcal{L}_2$

Proposition 14 (Giudici and Margaglio, 1980)

Suppose q is odd and

$$\phi(q+1) + 2\phi(q-1) > q - 1.$$

Then $q \in \mathcal{T}_2$

- Proportion of prime powers q this criterion fails to show in $\mathcal{T}_2$:

$q <$	10^5	10^6	10^7	10^8	10^9
% failures	14.983	15.176	15.081	15.065	15.066

$$\phi(q+1)+2\phi(q-1) > q-1 \implies q \in \mathcal{L}_2$$

Proof.

Let $A := \{$imprimitive $\theta + a$ $(a \in \mathbb{F}_q)$ with primitive $\mathbb{F}_q$-norm$\}$
$= \{(q+1)$-free $\theta + a$ $(a \in \mathbb{F}_q)$ that are *not* primitive$\}$

Let $\mathrm{Nm}(A) :=$ set of $\mathbb{F}_q$-norms of A

- Since
  $\mathbb{F}_q^*\{(q+1)$-free $\theta + a\} = \{$all $(q+1)$-free members of $\mathbb{F}_{q^2}\}$
  then $|A| = \phi(q+1) - N$
- $|A| \leq 2|\mathrm{Nm}(A)|$
- $\mathrm{Nm}(A) \subseteq$ non-squares of $\mathbb{F}_q$ that are *not* primitive
- $|\mathrm{Nm}(A)| \leq \frac{1}{2}(q-1) \;-\; \phi(q-1)$
- Thus
  $$N \geq \phi(q+1) + 2\phi(q-1) \;-\; (q-1)$$

Modified norm method for quadratic extensions

Let f be an *odd* divisor of $q-1$ with $\omega(f)=t$

$A := \{2f(q+1)\text{-free } \alpha(\theta+a) \text{ that are not primitive}\}$.

- $|A| \geq \frac{\phi(f)}{f}(q+1-(2^t-1)2^{\omega(q+1)}\sqrt{q} \quad -1) \; - \; N$
- $\mathrm{Nm}(A) \subseteq \{2f\text{-free elements of } \mathbb{F}_q \text{ that are not primitive}\}$
- $|\mathrm{Nm}(A)| = \frac{\phi(f)}{2f}(q-1) - \phi(q-1)$

Proposition 15 (Cohen 1983)

Suppose f is an odd divisor of $q-1$, $t=\omega(f), u:=\omega(q+1)$ and

$$\frac{\phi(f)}{f}[\phi(q+1)(1-\frac{(2^t-1)2^u\sqrt{q}}{q+1})-1]+2\phi(q-1)-\frac{\phi(f)}{f}(q-1)>0$$

Then $q \in \mathcal{L}_2$

Application of modified norm criterion

- Take f to be the least odd prime in $q-1$ (so $t=\omega(f)=1$)
  - shows $q<10^7$ in $\mathcal{L}_2$ except (possibly) for $139,\ 181,\ 1429,\ 680681,\ 1898051,\ldots$ 13 in all
  - Proportion of prime powers this criterion fails to show in $\mathcal{L}_2$:

$q<$	10^5	10^6	10^7	10^8	10^9
# failures	3	4	13	101	812
% failures $\times 10^2$	3.09	0.508	0.195	0.175	0.156

- Take f to be the product of the least two primes in $q-1$
  - fails (only) for $139,\ 181,\ 1429\quad (q<10^9)$
  - $1429^2-1=2^3\times 3\times 5\times 7\times 11\times 13\times 17$

- Unable (provably) to identify $\mathcal{L}_2$ by this approach !

General prime sieve criterion (GPSC)

$\mathrm{rad}(q^n - 1) :=$ radical of (product of distinct primes in) $q^n - 1$
$\mathrm{rad}(q^n - 1) := kp_1 \cdots p_s$, $p_1, \ldots, p_s$ are distinct (sieving) primes

$$k \text{ is core}, \quad t := \omega(k)$$

Lemma 4

$$N \geq \sum_{i=1}^{s} N(kp_i) - (s-1)N(k)$$
$$= \delta N(k) + \sum_{i=1}^{s} \left(N(kp_i) - \left(1 - \frac{1}{p_i}\right) N(k) \right),$$

where $\delta := 1 - \sum_{i=1}^{s} \frac{1}{p_i}$

- Must have $\delta > 0 \ldots$
  $\ldots$ so incorporate small primes in $q^n - 1$ into k

$$\operatorname{rad}(q^n - 1) = kp_1 \cdots p_s, \qquad \delta = 1 - \sum_{i=1}^{s} \frac{1}{p_i}$$

$$N \geq \delta N(k) + \sum_{i=1}^{s} \left(N(kp_i) - \left(1 - \frac{1}{p_i}\right) N(k) \right)$$

- $N(k) > \rho(k)(q - (n-1)2^t \sqrt{q}) \qquad (t = \omega(k))$
- $|N(kp_i) - \left(1 - \frac{1}{p_i}\right) N(k)| \leq (n-1)(s - 1 + \delta)2^t \sqrt{q}$

Proposition 16 (GPSC)

Suppose $\delta > 0$ *and*

$$q > (n-1)^2 2^{2t} \left(\frac{s-1}{\delta} + 2 \right)^2 := R_G$$

Then $q \in \mathcal{L}_n$

Prime sieve criterion for quadratic extensions (QPSC)

Uses $S_\theta(\chi_d) = -1$ for $d|q+1$

Proposition 17 (QPSC)

Assume all primes in the core k divide $q+1$. Suppose $\delta > 0$ and

$$q > 2^{2t}\left(\frac{s_0 - 1}{\delta} + \frac{\delta_0}{\delta}\right)^2 := R_Q$$

- $t = \omega(k), \qquad \delta = 1 - \sum_{i=1}^{s} \frac{1}{p_i}$ *as before*
- $p_1, \ldots, p_{s_0}$ *are primes dividing $q-1$*
- $\delta_0 = 1 - \sum_{i=1}^{s_0} \frac{1}{p_i}$

Then $q \in \mathcal{T}_2$. If $q > R_Q^+$ $(> R_Q)$, then $q \in \mathcal{L}_2$

- Use QPSC for specific q but GPSC for ranges of q

$\underline{q = 169 = 13^2}$

- $q - 1 = 2^3 \times 3 \times 7; \quad q + 1 = 2 \times 5 \times 17: \quad \text{take } t = 1;$
- $\delta = 1 - \frac{1}{3} - \frac{1}{5} - \frac{1}{7} - \frac{1}{17} = 0.26498; \ \delta_0 = 1 - \frac{1}{3} - \frac{1}{7} = 0.52380$
- $R_Q < 133 \ < R_Q^+ < 137 \ < q = 169$

$\underline{q = 181}$

- $q - 1 = 2^2 \times 3^2 \times 5; \quad q + 1 = 2 \times 7 \times 13: \quad t = 1;$
- $\delta = 1 - \frac{1}{3} - \frac{1}{5} - \frac{1}{7} - \frac{1}{13} = 0.24688; \ \delta_0 = 0.46666$
- $R_Q < 142 \ < R_Q^+ < 146 \ < q = 181$

$\underline{q = 1429}$

- $q - 1 = 2^2 \times 3 \times 7 \times 17; \quad q + 1 = 2 \times 5 \times 11 \times 13: \quad t = 2;$
- $\delta = 0.29715; \ \delta_0 = 0.60784$
- $R_Q < 1233 \ < R_Q^+ < 1244 \ < q = 1429$

Proof of Theorem 1: $\mathcal{L}_2 = \mathcal{Q}$

first step (following Corollary 9) $\omega_2 = \omega(q^2 - 1)$

- can assume $\omega_2 \leq 14$ (and $q < 2.265 \times 10^8$)
- take k to be product of 3 least primes in $q + 1$: so $t = 3$
- $s \leq \omega_2 - 3 \leq 11$: $\delta \geq 1 - \frac{1}{7} - \frac{1}{11} - \cdots - \frac{1}{43} > 0.39296$
- so if $q > 48215 > R_G$ then $q \in \mathcal{L}_2$
- can assume $q < 48215$ and hence $\omega_2 \leq 9$

second step $\omega_2 \leq 9$

third step $\omega_2 \leq 8$

fourth step

- assume $\omega_2 \leq 7$ and $q < 22652$
- take $t = 2$
- $s \leq \omega_2 - 2 \leq 5$: $\delta \geq 1 - \frac{1}{5} - \frac{1}{7} - \cdots - \frac{1}{17} > 0.43048$
- so if $q > 2040 > R_G$ then $q \in \mathcal{L}_2$
- can assume $q < 2040$ and hence $\omega_2 \leq 7$

fifth step Use QPSC

- assume $\omega_2 = 7$ and $q < 2040$ (e.g., $q = 1429$)
- must have: $\omega(q-1) = \omega(q+1) = 3$; 3 or 5 divides $q+1$
- $t = 2$
- $s \leq \omega_2 - 2 \leq 5$
  $\delta \geq 1 - \frac{1}{3} - \frac{1}{7} - \frac{1}{11} - \frac{1}{13} - \frac{1}{17} > 0.29715; \delta_0/\delta < 2.6025$
- so if $q > 1407 > R_Q^+ > 1393 > R_Q$ then $q \in \mathcal{L}_2$
  (covers 1429 !!)

further steps

- for $\omega_2 = 6$ similar argument gives $q > 914 \implies q \in \mathcal{L}_2$, etc
- Norm method covers small failures of QPSC (e.g, $q = 211$)

Towards proof of Theorem 3: identifying $\mathcal{L}_3$

prime sieve criterion:

$$q > 4 \times 2^{2t} \left(\frac{s-1}{\delta} + 2 \right)^2 := R_G \implies q \in \mathcal{L}_3$$

first step (after Cor 9) $\quad \omega_3 = \omega(q^3 - 1)$

- assume $20 \leq \omega_3 \leq 52$; $\quad 8.232 \times 10^8 < q < 2.2029 \times 10^{32}$
- $t = \omega(k) = 4$; $s \leq \omega_3 - 4 \leq 48$; $\delta > 0.20068$
- $q \in \mathcal{L}_3$ since $q > 5.7 \times 10^7 > R_G$

second step

- assume $15 \leq \omega_3 \leq 19$ and $q > 850352$: $\quad R_G < 672475$

third step

- assume $\omega_3 = 14$ and $q > 235631$: $\quad R_G < 193864$

next steps

- assume $\omega_3 = 13$ and $q > 67257$: $R_G < 142863$
- there are no prime powers q with $67257 < q < 142863$
- similarly for $10 \leq \omega_3 \leq 12$

- $\omega_3 \leq 9$ GPSC yields upper bounds for $q \notin \mathcal{L}_3$

ω_3	9	8	7	6	5	4	3	2
$q <$	25456	14849	8160	4131	1958	793	256	64

Modified prime sieve criterion (MPSC)

Write: $\mathrm{rad}(q^n - 1) = kp_1 \cdots p_s l$ where
$k =$ core, $p_1, \ldots, p_s$, l distinct primes (with l largest)

$$t = \omega(k), \quad \delta = 1 - \sum_{i=1}^{s} \frac{1}{p_i}$$

Proposition 18 (MPSC)

If $\quad q > R_M := (n-1)^2 \left\{ \frac{2^t \phi(k)(s - 1 + 2\delta) + (1 - \frac{1}{l})}{\phi(k)\delta - \frac{1}{l}} - 1 \right\}^2$

then $q \in \mathcal{L}_n$

Proof. $$N \geq N(kp_1 \cdots p_s) + N(l) - N(1)$$

and use GPSC (proof) for $N(kp_1 \cdots p_s)$

□

Example ($n = 3$) $\; q = 1759: \; R_M < 1619 < q < R_G = 1782$

Completion of proof of Theorem 3

Theorem

The complement of $\mathcal{L}_3 \subseteq \{3, 4, 5, 7, 9, 11, 13, 31, 37\} \bigcup \mathcal{S}$, *where* $\mathcal{S}$ *is a set of* 175 *prime powers, the largest being* 9811

Proof.

Identify $q \in \mathcal{Q}$ within admissible ranges for $q \notin \mathcal{L}_3$ and use MPSC

□

Conjecture

$\mathcal{L}_3 = \mathcal{Q} \setminus \{3, 4, 5, 7, 9, 11, 13, 31, 37\}$

- verified using MAGMA for prime powers $q \leq 100$
- $q = 97$ ($\in \mathcal{S}$) took 84 hours
- to extend search to identify $\mathcal{L}_3$ would require q^5 searches for each prime power q (largest being $\sim 10,000$)

Proof of Theorem 2: $\mathcal{T}_3 = \mathcal{Q} \setminus \{3, 7, 9, 13, 37\}$

- for each possible "failure" ($\sim$ 180 fields) identify one member of $\{\theta + a : a \in \mathbb{F}_q\}$
  e.g., for $q = p > 3$, can assume $\mathrm{Tr}(\theta) = 0$
- use MAGMA to search for a primitive $\theta + a$ ($\sim q^2$ searches)
- successful except for $q \in \{3, 4, 5, 7, 9, 11, 13, 31, 37\}$
- for $q = p$, maximum distance from an element θ with $\mathrm{Tr}(\theta) = 0$ to a primitive element is 79 when $q = 2731$

Quartic extensions

From Corollary 11

$$q \notin \mathcal{L}_4 \implies q < 4.694 \times 10^{94} \text{ and } \omega_4 \leq 154$$

Using the GPSC obtain:

Theorem 19

$$q \notin \mathcal{L}_4 \implies q \leq 25943 \textit{ and } \omega_4 \leq 12$$

Conjecture

$$\mathcal{L}_4 = \mathcal{Q} \backslash \{2, 3, 4, 5, 7, 8, 9, 11, 13, 17, 19, 23, 25, 27, 29, 31, 32, 41, 43, 64\}$$

H Davenport
On primitive roots in finite fields
Quart. J. Math. Oxford, 8 (**1937**), 308–312

L Carlitz
Distribution of primitive roots in a finite field
Quart. J. Math. Oxford, (2) 4 (**1953**), 4–10

R E Giudici & C Margaglio
A geometric characterization of the generators in a quadratic extension . . .
Rend. Sem. Mat. Univ. Padova, 62,(**1980**), 103–114

S D Cohen
Primitive roots in the quadratic extension of a finite field
J. London Math Soc., (2) 27 (**1983**), 221–228

N M Katz
An estimate for character sums
J. Amer. Math. Soc., 27 (**1989**), 197–200

D Mills & G McNay
Primitive roots in cubic extensions of finite fields
$\mathbb{F}_q$6 *Proceedings (Oaxaca, 2001), Springer* , 239-250, **2002**

S D Cohen
Generators of the cubic extension of a finite field

J. Comb. Number Th., to appear **2009**