

# Finding primitive elements in finite fields of small characteristic

Ming-Deh Huang and Anand Kumar Narayanan

**ABSTRACT.** We describe a deterministic algorithm for finding a generating element of the multiplicative group of the finite field with  $p^n$  elements. In time polynomial in  $p$  and  $n$ , the algorithm either outputs an element that is provably a generator or declares that it has failed in finding one. Under a heuristic assumption, we argue that the algorithm does always succeed in finding a generator. The algorithm relies on a relation generation technique in a recent breakthrough by Antoine Joux's for discrete logarithm computation in small characteristic finite fields in  $L(1/4, o(1))$  time. For the special case when the order of  $p$  in  $(\mathbb{Z}/n\mathbb{Z})^\times$  is small (bounded by  $(\log_p(n))^{O(1)}$ ), we present a modified algorithm which is reliant on weaker heuristic assumptions.

## 1. Introduction

Let  $p$  be a prime and  $n$  a positive integer. The multiplicative group  $\mathbb{F}_{p^n}^\times$  of the finite field  $\mathbb{F}_{p^n}$  is cyclic and has  $\phi(p^n - 1)$  generators (also called primitive elements), where  $\phi$  is Euler's totient function. Since  $\phi(p^n - 1) = \Omega\left(\frac{p^n - 1}{\log(\log(p^n - 1))}\right)$  [15], a large fraction of  $\mathbb{F}_{p^n}^\times$  are primitive elements. In spite of their abundance, finding one efficiently remains an important open problem. The difficulty partly lies in testing if a given element is a generator and all known algorithms for testing either factor  $p^n - 1$  or solve an instance of the discrete logarithm problem in  $\mathbb{F}_{p^n}^\times$ , both of which are believed to be difficult.

Even if the question were relaxed and an element of large order is sought, approaches that work in general for every  $p$  and  $n$  are rare. Gao [11] presents an algorithm that produces an element of order  $\exp(\Omega(\log n)^2 / \log(\log(n)))$ . Gao's algorithm is efficient conditioned on a conjecture which bears resemblance to our heuristic 2.1. Voloch [25] presents an approach suited to small  $p$  that finds an element of order  $\exp(\Omega(\sqrt{n}))$ . Notably, no previous algorithms to compute an element of order exponential in  $n$  were known, even if allowed to make heuristic assumptions.

There are other constructions that provably find an element of large order, but they only apply to very special  $(p, n)$  pairs [27][1][6][7][4][20][21]. For certain  $(p, n)$  pairs, von zur Gathen and Shparlinski [27] introduced the idea of constructing elements of high order using Gauss periods. Extensions and improvements on

their results appear in [1][4][20][21]. When  $n = \frac{p^c - 1}{p - 1}$  for some  $c > 1$ , Cheng, Gao and Wan [7] describe a deterministic algorithm that finds an element of order  $\exp(\Omega(\sqrt{p^c}))$  in time polynomial in  $p^c$ . Voloch [26] and Chang [5] present constructions based on elements appearing as coordinates of points on certain curves.

An alternate relaxation of the question is to find small sets that contain a generator. Davenport [10] proved that when  $p$  is large enough compared to  $n$  and  $\mathbb{F}_{p^n} = \mathbb{F}_p[\theta]$ , the set  $\mathbb{F}_p + \theta$  contains a generator of  $\mathbb{F}_{p^n}^\times$ . Shoup [22] extended this result to prove the existence of a subset  $A \subseteq \mathbb{F}_{p^n}$  of size polynomial in  $p$  and  $n$  that contains a generator. Further, the set contains elements of degree bounded by  $\mathcal{O}(\log_p(n))$  when represented as polynomials in  $\theta$ . Shparlinski in [23] gave a simpler more efficient construction and in [24] further reduced the size of the subset  $A$ . The question remains on how to identify a generator given a small set that contains one.

In recent breakthroughs, Gologlu, Granger, McGuire, Zumbragel [12] and Joux [16] independently devised algorithms that assuming certain widely believed heuristics compute discrete logarithms in small characteristic finite fields faster than previously known. The authors of [12] demonstrated their algorithm by computing discrete logarithms in  $\mathbb{F}_{2^{1971}}$  which at the time of announcement was a record [13]. Joux's algorithm is the first to compute discrete logarithms in heuristic  $L(1/4, o(1))$  time, where  $L(\ell, c)$  is defined as  $\exp((c + o(1))(\log(p^n)^\ell)(\log \log(p^n))^{1-\ell})$ . All previous algorithms required  $L(1/3, o(1))$  time and this speed up allowed Joux [17] to compute discrete logarithms in  $\mathbb{F}_{2^{4080}}$ . Gologlu, Granger, McGuire and Zumbragel [14] then extended the record to  $\mathbb{F}_{2^{6120}}$ .

A remarkable feature shared by the algorithms is that they both consider a small set as the factor base, one that is of size polynomial in the extension degree. Further, if the extensions they consider are obtained by adjoining a root  $\zeta$ , then the factor base contains the elements that can be represented as linear polynomials in  $\zeta$ .

We propose to use the factor base and relation generation technique in the initial phase of Joux's paper [16] to efficiently find generators in  $\mathbb{F}_{p^n}^\times$ . Whereas the algorithm for discrete logarithm computation assumes a given generator of the entire group, our interest is to find such a generator. The relation generation procedure collects multiplicative relations satisfied by the elements in the factor base and is guaranteed to collect enough only under a heuristic assumption. Unlike in discrete logarithm computations, while computing primitive elements it is not straight forward to check if the relations generated suffice and if so to extract from it a primitive element. To this end, we modify both the factor base and the relation generation step and describe how to test if the generated relations suffice and if so to obtain a primitive element. The factor base is chosen such that if the relation generation step is successful, then the collected relations among the elements of the factor base determine a group whose largest invariant factor contains a large cyclic subgroup of  $\mathbb{F}_{p^n}^\times$ . Further, we can test if the relation generation was successful from the invariant decomposition of the the group determined by the relations and if successful extract a generator of this large cyclic subgroup of  $\mathbb{F}_{p^n}$  (see section 2.5). Once a generator for this large subgroup is known, a primitive element can be computed. For the aforementioned invariant factor to contain a large cyclic subgroup of  $\mathbb{F}_{p^n}^\times$ ,

the factor base does not necessarily have to contain a primitive element. It suffices if the factor base generates the whole multiplicative group, and this is indeed the case as we observe that a result of F.R.K Chung [9] nicely applies to our situation when the finite field is considered as an extension over a large enough base field.

Our algorithm, in time polynomial in  $p$  and  $n$ , either certifiably finds a generator or indicates that it has failed in doing so. Moreover assuming a slightly weaker heuristic assumption than what is implicitly assumed in Joux's method, our algorithm finds a generator in time polynomial in  $p$  and  $n$  (see Theorem 2.4). In addition to the heuristic reasoning provided in this paper, the success of Joux's method in breaking the record of discrete logarithm computation can be taken as a strong evidence in support of the heuristic assumption.

It should be noted that our running time has polynomial dependence on  $p$  and not on  $\log p$ . Thus the algorithm is efficient only in small characteristic.

For instances where  $p$  is of small order in  $(\mathbb{Z}/n\mathbb{Z})^\times$ , we present a modified algorithm that is simpler to state and reliant on fewer heuristic assumptions.

In a recent further advancement [2], Barbulescu, Gaudry, Joux and Thome have discovered an algorithm to compute discrete logarithms in  $\mathbb{F}_{q^{2n}}^\times$  for  $n \leq q$  in  $q^{\mathcal{O}(\log n)}$  time based on heuristics. Their result combined with Shoup's [22] proof of the existence of small sets containing a primitive element implies a heuristic algorithm to compute primitive elements in  $\mathbb{F}_{p^n}$  with quasi-polynomial running time  $(pn)^{\mathcal{O}(\log n)}$ . Our algorithm is faster since the running time is polynomial in  $p$  and  $n$ .

## 2. Finding Primitive Elements

**2.1. Overview of the Algorithm.** The algorithm first proceeds by embedding  $\mathbb{F}_{p^n}$  into an extension  $\mathbb{F}_{q^{2m}}$  where  $q$  is a power of  $p$  such that  $n \leq q$  and  $m$  is a multiple of  $n$  such that  $q/2 < m \leq q$ . In particular, we set  $q := p^{\lceil \log_p(n) \rceil}$  and  $m$  is chosen as the largest integral multiple of  $n$  satisfying  $q/2 < m \leq q$ . We remark that our choice of embedding field  $\mathbb{F}_{q^{2m}}$  is in certain cases larger than the one chosen in Joux's algorithm [16].

The field  $\mathbb{F}_{q^{2m}}$  is constructed as  $\mathbb{F}_{q^2}[\zeta]$ , where  $\zeta$  is a root of an irreducible polynomial  $g(x) \in \mathbb{F}_{q^2}[x]$  of degree  $m$  that is of a special form. Following Joux, we seek polynomials  $h_0, h_1 \in \mathbb{F}_{q^2}[x]$  of low degree such that the factorization of  $h(x) := h_1(x)x^q - h_0(x)$  over  $\mathbb{F}_{q^2}[x]$  has an irreducible factor of degree  $m$  and pick  $g(x)$  to be one such irreducible factor of degree  $m$ . The motivation behind choosing  $g$  in this manner is that the identity  $h_1(\zeta)\zeta^q - h_0(\zeta) = 0$  would later allow us to replace  $\zeta^q$  with an expression consisting of the low degree polynomials  $h_0(\zeta)$  and  $h_1(\zeta)$ . For technical reasons explained in section 2.5, we deviate from Joux's algorithm and impose three further restrictions on  $h(x)$  (see section 2.2).

Once  $h_0(x), h_1(x)$  and hence  $g(x)$  are chosen, we invoke Joux's relation generation algorithm which picks a small subset of  $\mathbb{F}_{q^{2m}}^\times$  as the factor base and finds a set of multiplicative relations satisfied by the elements in the factor base. However, the success of the relation generation algorithm in finding enough relations is reliant

on certain heuristic assumptions.

We show in section 2.5 that if sufficiently many relations are generated, then they yield a primitive element. A theorem of F.R.K Chung assures that the subgroup generated by the factor base contains a primitive element and is an important ingredient in our argument. Further, we devise a sufficient condition on the outcome of the relation generation step that can be tested and that if found true leads to efficient computation of a primitive element  $\gamma$  that generates  $\mathbb{F}_{q^2}[\zeta]^\times$ .

As a consequence,  $\delta := \gamma^{(q^{2m}-1)/(p^n-1)}$  has order  $p^n - 1$  and generates the multiplicative group of  $\mathbb{F}_p[\delta] \cong \mathbb{F}_{p^n}$ .

We assume an explicit representation of  $\mathbb{F}_{p^n}$  (see [18]) as an input. That is, a representation of  $\mathbb{F}_{p^n}$  as an  $\mathbb{F}_p$  vector space with a basis that allows efficient multiplication. For instance, regarding  $\mathbb{F}_{p^n}$  as  $\mathbb{F}_p[\mu]$  where  $\mu$  is a root of a known irreducible degree  $n$  polynomial is an explicit representation. Due to Lenstra [18][Thm 1.2], an isomorphism between two explicit representations of a field of size  $p^n$  can be computed deterministically in time polynomial in  $n$  and  $\log(p)$ . Thus a generator for any explicit representation of  $\mathbb{F}_{p^n}$  can be found as the image of  $\delta$  under an isomorphism.

The algorithm is deterministic and it always terminates in time polynomial in  $n$  and  $p$ . We either successfully find a primitive element or declare failure. The algorithm can fail for two reasons, either we fail in finding  $g(x)$  of the special form or the relations generated do not suffice. Based on heuristic assumptions, we argue that neither occurs.

**2.2. The Polynomial Search Phase:** Let  $C$  be a positive integer. We say that an integer is  $q^{2C}$ -smooth if and only if all its prime factors are at most  $q^{2C}$ .

We define a polynomial  $f(x) \in \mathbb{F}_{q^2}[x]$  to be “good” if and only if the following four conditions are satisfied.

- (1)  $f(x)$  is square free.
- (2)  $f(x)$  does not have linear factors.
- (3)  $f(x)$  has an irreducible factor of degree  $m$ .
- (4) For every irreducible factor  $g'(x)$  of  $f(x)$  such that  $\deg(g'(x)) \neq m$ ,  $\gcd(q^{2 \deg(g')} - 1, q^{2m} - 1)$  is  $q^{2C}$ -smooth.

We set a degree bound  $D$  and investigate the existence of  $h_0, h_1 \in \mathbb{F}_{q^2}[x]$  each of degree bounded by  $D$  such that  $h(x) = h_1(x)x^q - h_0(x)$  is “good”.

The existence of “good” polynomials of the above form requires that  $q + D$  is at least  $m + 2$  for otherwise we are left with a linear factor. To this end, if  $m = q$ , we assume  $D > 1$  and if  $m = q - 1$ , we assume  $D > 0$ .

For  $m > 2$  and  $r \geq m$ , let  $N_q(r, m)$  denote the number of polynomials in  $\mathbb{F}_{q^2}[x]$  of degree  $r \geq m$  that satisfy the first three conditions of being “good” and let  $P_q(r, n) = \frac{N_q(r, n)}{q^{2r}}$  denote the probability that a random polynomial of degree  $r$  satisfies the first three conditions of being “good”. Let  $s$  and  $t$  be non negative

integers such that  $q + D - m = s(m - 1) + t$ , where  $t < m - 1$ . For a positive integer  $k$ , let  $I_k$  denote the number of monic irreducible polynomials in  $\mathbb{F}_{q^2}[x]$  of degree  $k$ .

If  $t \neq 1$ , then

$$N_q(q + D) \geq I_m \binom{I_{m-1}}{s} I_t$$

since we can chose an irreducible polynomial of degree  $m$ ,  $s$  irreducible polynomials of degree  $m - 1$  and one irreducible polynomial of degree  $t$  and take their product to get a polynomial of degree  $q + D$ . By substituting the lower bound

$$I_k \geq \frac{q^k}{k} - \frac{q(q^{k/2} - 1)}{(q - 1)k}$$

in the above expression we get

$$P_q(q + D, m) = \frac{N_q(q + D, m)}{q^{2(q+D)}} \geq \frac{1}{m(m-1)^s t s!} \left( 1 - \mathcal{O}\left(\frac{1}{q^t}\right) \right).$$

Likewise, when  $t = 1$ , it follows that  $s \geq 1$  and we obtain

$$\begin{aligned} N_q(q + D, m) &\geq I_m \binom{I_{m-1}}{s-1} I_{m-2} I_{t+1} \\ \Rightarrow P_q(q + D, m) &\geq \frac{1}{m(m-1)^{s-1} (m-2)(t+1)(s-1)!} \left( 1 - \mathcal{O}\left(\frac{1}{q^{t+1}}\right) \right). \end{aligned}$$

If we were to assume that a random polynomial of the form  $h_1(x)x^q - h_0(x)$ , where  $h_0$  and  $h_1$  are of degree at most  $D$  satisfies the first three conditions of being “good” with probability  $P_q(q + D, n)$ , then since  $s = \mathcal{O}(D/m)$  choosing

$$D = \Theta(\log_{q^2}(m(m-1)^s t s!)) = \Theta(1)$$

is sufficient to ensure the existence of  $h_0$  and  $h_1$  such that  $h(x)$  is square free, has a degree  $m$  factor and no linear factors.

Heuristically it is likely that a large fraction of polynomials that satisfy the first three constraints also satisfy the fourth constraint on being “good”.

For a polynomial that satisfies the first three conditions, if each of its factors excluding its degree  $m$  factor is either of degree prime to  $m$  or of degree bounded by  $C$ , then it is likely to satisfy the fourth condition.

Consider positive integers  $m', s'$  and  $t'$  such that  $m' > m/2$ ,  $t' > 1$ ,  $q + D - m = s'm' + t'$ ,  $\gcd(m', m) = 1$  and either  $\gcd(t', m) = 1$  or  $t' < C$ . For such a choice,  $\gcd(q^{2m'} - 1, q^{2m} - 1)$  and  $\gcd(q^{2t'} - 1, q^{2m} - 1)$  are both likely to be  $q^{\mathcal{O}(1)}$ -smooth. Hence by taking an irreducible polynomial of degree  $m$ ,  $s'$  irreducible polynomials of degree  $m'$  and an irreducible polynomial of degree  $t'$ , we can construct a “good” polynomial. From an analysis similar to the above computation of  $P_q(q + D, m)$ , we can conclude heuristically that choosing  $D = \Theta(1)$  and  $C = \Theta(1)$  are sufficient to guarantee the existence of the “good” polynomials that we seek.

**HEURISTIC ASSUMPTION 2.1.** There exists positive integers  $D, C$  such that for all prime powers  $q$  and for all positive integers  $2 < m \leq q$ , there exists  $h_0, h_1 \in \mathbb{F}_{q^2}[x]$  of degree bounded by  $D$  such that  $h_1(x)x^q - h_0(x)$  is square free, has an irreducible factor (call  $g(x)$ ) of degree  $m$ , and for each irreducible factor  $g'(x)$  of  $h(x)/g(x)$ ,  $\deg(g') > 1$  and  $\gcd(q^{2 \deg(g')} - 1, q^{2m} - 1)$  is  $q^{2C}$ -smooth.

**Search for  $h_0(x), h_1(x)$  and  $g(x)$ :** Fix constants  $C, D$ . Enumerate candidates for  $h_0, h_1 \in \mathbb{F}_{q^2}[x]$  with each of their degrees bounded by  $D$ . For each candidate pair  $(h_0, h_1)$ , factor  $h(x) = h_1(x)x^q - h_0(x)$ . If  $h(x)$  is “good”, output  $h_0, h_1$  and the factor of degree  $m$  and stop. If no such candidates are found, declare failure.

The search algorithm terminates after considering at most  $q^{2(D+1)} = q^{\mathcal{O}(1)}$  candidate pairs. Factoring each candidate  $h_1(x)x^q - h_0(x)$  takes time polynomial in the degree  $q + D$  and  $p$  using Berlekamp’s deterministic polynomial factorization algorithm[3]. All four conditions of being good can be checked efficiently given the degrees of the irreducible factors in the factorization of  $h$ . Thus, the search for  $h_0, h_1$  and hence  $g$  of the desired takes at most  $q^{\mathcal{O}(1)}$  time.

**2.3. Small Generating Set.** We next choose a small subset  $S \subseteq \mathbb{F}_{q^2}[\zeta]$  that generates  $\mathbb{F}_{q^2}[\zeta]^\times$ . F.R.K Chung proved that for all prime powers  $s$ , for all positive integers  $r$  such that  $(r - 1)^2 < s$ , for all  $\mu$  such that  $\mathbb{F}_{s^r} = \mathbb{F}_s[\mu]$ , the set  $\mathbb{F}_s + \mu$  generates  $\mathbb{F}_{s^r}^\times$  [9, Thm. 8][28, Ques 1.1]. Since  $m \leq q$ , setting  $S := \mathbb{F}_{q^2} + \zeta$  ensures that the subgroup generated by  $S$ ,  $\langle S \rangle = \mathbb{F}_{q^2}[\zeta]^\times$ .

Given that  $\langle S \rangle = \mathbb{F}_{q^2}^\times$ , the next step is to determine the relations satisfied by the elements in  $S$  so that we can determine  $\mathbb{F}_{q^2}[\zeta]$  as the free abelian group generated by  $S$  modulo the relations.

For a technical reason,  $S$  is first extended to the set  $F := h_1(\zeta) \cup \{\lambda\} \cup S$ , where  $\langle \lambda \rangle = \mathbb{F}_{q^2}^\times$ . An identity in  $\mathbb{F}_{q^2}^\times$  of the form  $\prod_{\beta \in F} \beta^{e_\beta} = 1$  for integers  $e_\beta$  is called as a relation and it can be identified with the relation vector  $(e_\beta, \beta \in F)$  indexed by elements in  $F$ .

**2.4. Joux’s Relation Generation Algorithm.** The relation search step begins with the following identity over  $\mathbb{F}_{q^2}[x]$

$$\prod_{\alpha \in \mathbb{F}_q} x - \alpha = x^q - x.$$

For  $(a, b, c, d) \in \mathbb{F}_{q^2}^4$  such that  $ad - bc \neq 0$ , the substitution  $x \mapsto \frac{a\zeta + b}{c\zeta + d}$  yields

$$\prod_{\alpha \in \mathbb{F}_q} \frac{(a - \alpha c)\zeta + (b - \alpha d)}{(c\zeta + d)^q} = \frac{(c\zeta + d)(a\zeta + b)^q - (a\zeta + b)(c\zeta + d)^q}{(c\zeta + d)^{q+1}}$$

$$\Rightarrow (c\zeta + d) \prod_{\alpha \in \mathbb{F}_q} ((a - \alpha c)\zeta + (b - \alpha d)) = (c\zeta + d)(a\zeta + b)^q - (a\zeta + b)(c\zeta + d)^q.$$

Linearity of raising to the  $q^{\text{th}}$  power implies

$$(c\zeta + d) \prod_{\alpha \in \mathbb{F}_q} ((a - \alpha c)\zeta + (b - \alpha d)) = (c\zeta + d)(a^q \zeta^q + b^q) - (a\zeta + b)(c^q \zeta^q + d^q).$$

By substituting  $\zeta^q = \frac{h_0(\zeta)}{h_1(\zeta)}$ , the right hand side becomes

$$\frac{(ca^q - ac^q)\zeta h_0(\zeta) + (da^q - bc^q)h_0(\zeta) + (cb^q - ad^q)\zeta h_1(\zeta) + (db^q - bd^q)h_1(\zeta)}{h_1(\zeta)}.$$

Consider the numerator of the above expression as the polynomial

$$N(x) := (ca^q - ac^q)xh_0(x) + (da^q - bc^q)h_0(x) + (cb^q - ad^q)xh_1(x) + (db^q - bd^q)h_1(x)$$

evaluated at  $\zeta$ . The degree of  $N(x)$  is bounded by  $d+1$ . If  $N(x)$  factors in to linear factors over  $\mathbb{F}_{q^2}[x]$ , then we get the following relation in  $\langle F \rangle$

$$(c\zeta + d)h_1(\zeta) \prod_{\alpha \in \mathbb{F}_q} ((a - \alpha c)\zeta + (b - \alpha d)) = n(\zeta).$$

The above expression can be written as a product of an element  $\mu \in \mathbb{F}_{q^2}^\times$  times  $h_1(\zeta)$  times a fraction of products of monic linear polynomials in  $\zeta$  over  $\mathbb{F}_{q^2}$  being equal to 1. By expressing the element  $\mu$  in  $\mathbb{F}_{q^2}^\times$  as a power of  $\lambda$  by computing a discrete logarithm over  $\mathbb{F}_{q^2}^\times$ , we indeed get a relation in  $\langle F \rangle$ .

The reason for choosing to work over  $\mathbb{F}_{q^2}$  instead of  $\mathbb{F}_q$  is that for every choice of  $a, b, c, d \in \mathbb{F}_q$ , the relation it yields becomes  $\zeta^q - \zeta = \prod_{\alpha \in \mathbb{F}_q} (\zeta - \alpha)$ . Thus, we have to work over an extension of  $\mathbb{F}_q$  where the  $q^{\text{th}}$  power map would be non trivial and  $\mathbb{F}_{q^2}$  is the smallest such extension.

**Relation Generation:** For every  $(a, b, c, d) \in \mathbb{F}_{q^2}^4$  such that  $ad - bc \neq 0$ , compute the numerator  $N(x)$  and if it factors into linear factors over  $\mathbb{F}_{q^2}[x]$ , add the relation as a row to the relation matrix  $R$ .

Add the relation corresponding to the identity  $\lambda^{q^2-1} = 1$  to  $R$ .

The relation generation step can be performed in  $q^{\mathcal{O}(1)}$  time since the number of choices for  $(a, b, c, d)$  is at most  $q^{\mathcal{O}(1)}$  and factoring the numerator polynomial using Berlekamp's deterministic factoring algorithm takes  $q^{\mathcal{O}(1)}$  time as the numerator polynomial is of constant degree. We have to express the constant  $\mathbb{F}_{q^2}^\times$  factor in the relation as a power of  $\lambda$ , but that can be accomplished by solving the discrete logarithm in  $\mathbb{F}_{q^2}^\times$  exhaustively in  $\mathcal{O}(q^2)$  time.

**2.5. Testing.** Let  $R$  be the  $N$  by  $|F|$  matrix consisting of the relation vectors as rows and  $\Gamma_R$  the  $\mathbb{Z}$ -lattice generated by the rows of  $R$ . The Smith normal form of  $R$  gives the decomposition of  $\mathbb{Z}^{|F|}/\Gamma_R$  into its invariant factors

$$\mathbb{Z}^{|F|}/\Gamma_R = \langle e(1) \rangle \oplus \langle e(2) \rangle \oplus \dots \oplus \langle e(|F|) \rangle \cong \mathbb{Z}/d_1\mathbb{Z} \oplus \mathbb{Z}/d_2\mathbb{Z} \oplus \dots \oplus \mathbb{Z}/d_{|F|}\mathbb{Z}$$

where for  $1 \leq i \leq |F|$ ,  $e(i) \in \mathbb{Z}^{|F|}$  denotes a relation vector and  $d_i$  the order of  $e(i)$  in  $\mathbb{Z}^{|F|}/\Gamma_R$  and for  $1 \leq i < |F|$ ,  $d_i \mid d_{i+1}$ .

For a polynomial  $f(x) \in \mathbb{F}_{q^2}[x]$ , let  $\mathbb{F}_f$  denote the ring  $\mathbb{F}_{q^2}[x]/(f(x)\mathbb{F}_{q^2}[x])$ .

Let  $h = \prod_{i=0}^k g_i(x)$  be a factorization of  $h(x)$  into distinct irreducible polynomials in  $\mathbb{F}_{q^2}[x]$ . Without loss of generality, let  $g_0(x) = g(x)$ .

While our objective in the relation generation step was to collect relations in  $\mathbb{F}_g^\times$ , the

relations generated are in fact satisfied in  $\mathbb{F}_{g_i}^\times$  for every  $0 \leq i \leq k$ . It is to break this symmetry and focus on  $\mathbb{F}_g^\times$  that we insist that  $\forall 1 \leq i \leq k$ ,  $\gcd(q^{2 \deg(g_i)} - 1, q^{2m} - 1)$  is  $q^{2C}$ -smooth.

The fact that the relations generated hold in  $\mathbb{F}_{g_i}^\times$  for every  $0 \leq i \leq k$  is also of concern to Joux's algorithm for computing discrete logarithms. This was also observed independently by [8].

For a non constant polynomial  $f(x) \in \mathbb{F}_{q^2}[x]$  dividing  $h(x)$ , let  $\Gamma_f$  denote the relation lattice of the subgroup of  $\mathbb{F}_f^\times$  corresponding to the generating set

$$F_f := \{\mu\} \cup \{h_1(x) \bmod f(x)\} \cup \{x + \theta \bmod f(x), \theta \in \mathbb{F}_{q^2}\}.$$

That is,

$$\Gamma_f = \left\{ (z_\beta)_{\beta \in F_f} \in \mathbb{Z}^{|F_f|} \mid \prod_{\beta \in F_f} \beta^{z_\beta} = 1 \right\}.$$

The relation lattice generated  $\Gamma_R$  is contained in  $\Gamma_h$  which is in turn contained in  $\Gamma_g$  and we have the natural surjection

$$\mathbb{Z}^{|F|}/\Gamma_R \twoheadrightarrow \mathbb{Z}^{|F|}/\Gamma_g.$$

Recall F.R.K Chung's theorem that for all prime powers  $s$ , for all positive integers  $r$  such that  $(r-1)^2 < s$ , for all  $\mu$  such that  $\mathbb{F}_{s^r} = \mathbb{F}_s[\mu]$ , the set  $\mathbb{F}_s + \mu$  generates  $\mathbb{F}_{s^r}^\times$  [9, Thm. 8][28, Ques 1.1]. Since  $\deg(g(x)) \leq q$ , F.R.K Chung's theorem implies that  $\mathbb{Z}^{|F|}/\Gamma_g \cong \mathbb{F}_g^\times$

Thus, the natural reduction map  $\varphi : \mathbb{Z}^{|F|}/\Gamma_R \twoheadrightarrow \mathbb{F}_g^\times$  is surjective. For  $1 \leq i < |F|$ , let  $\pi_i$  denote  $\varphi(e(i)) = \prod_{\beta \in F} \beta^{e(i)\beta}$ .

If  $h$  were to have a linear factor, then the relation generation step will not relate that linear factor to the rest of the linear polynomials in the factor base. As a result, we would have to exclude that linear factor from the factor base and F.R.K Chung's theorem would no longer apply. It is to circumvent this that we insisted that  $h$  have no linear factors.

We next prove a lemma which states a condition on  $\mathbb{Z}^{|F|}/\Gamma_R$  that guarantees that our relation generation step has collected enough relations to extract an element of large order in  $\mathbb{F}_g^\times$ . From this large order element we will eventually compute a primitive element.

**LEMMA 2.2.** *If  $\gcd(d_{|F|-1}, q^{2m} - 1)$  is  $q^{2C}$ -smooth, then there exists a  $q^{2C}$ -smooth number  $B$  such that the order of  $\varphi(e(|F|))$  in  $\mathbb{F}_g^\times$  is divisible by  $\frac{q^{2m}-1}{B}$ .*

Assume  $\gcd(d_{|F|-1}, q^{2m} - 1)$  is  $q^{2C}$ -smooth. From the Smith normal form, we have the invariant factor decomposition

$$\mathbb{Z}^{|F|}/\Gamma_R = \bigoplus_{j=1}^{|F|} \langle e(j) \rangle$$

where  $d_j$  is the order of  $e(j)$  in  $\mathbb{Z}^{|F|}/\Gamma_R$ .



Since  $\left| \varphi \left( \bigoplus_{j=1}^{|F|-1} \langle e(j) \rangle \right) \right| = \prod_{j=1}^{|F|-1} |\varphi(\langle e(j) \rangle)|$  divides  $\prod_{j=1}^{|F|-1} d_j$  and  $d_j \mid d_{j+1}$  for  $1 \leq j < |F| - 1$ , it follows that  $\gcd \left( \left| \varphi \left( \bigoplus_{j=1}^{|F|-1} \langle e(j) \rangle \right) \right|, q^{2m} - 1 \right)$  is  $q^{2C}$ -smooth.

Since  $\varphi(\mathbb{Z}^{|F|}/\Gamma_R) = \mathbb{F}_g^\times$  and  $\mathbb{F}_g^\times$  is cyclic of order  $q^{2m} - 1$ , there exists a  $q^{2C}$ -smooth number  $B$  such that the order of  $\varphi(e(|F|))$  in  $\mathbb{F}_g^\times$  is divisible by  $\frac{q^{2m}-1}{B}$ .  $\square$

We next show if the relation generation is successful in computing the relation lattice of  $\Gamma_h$  in its entirety, then the condition stated in lemma 2.2 is satisfied.

LEMMA 2.3. *If  $\Gamma_R = \Gamma_h$ , then  $\gcd(d_{|F|-1}, q^{2m} - 1)$  is  $q^{2C}$ -smooth.*

Let  $v$  denote the largest factor of  $q^{2m} - 1$  that is  $q^{2C}$ -smooth and let  $L = (q^{2m} - 1)/v$ . Since  $h$  is square free,

$$\mathbb{F}_h^\times \cong \mathbb{F}_g^\times \times \prod_{i=1}^k \mathbb{F}_{g_i}^\times.$$

Let  $\langle F_h \rangle$  denote the subgroup of  $\mathbb{F}_h^\times$  generated by  $F_h$ . We have the inclusion

$$\begin{aligned} \psi : \langle F_h \rangle &\hookrightarrow \mathbb{F}_g^\times \times \prod_{i=1}^k \mathbb{F}_{g_i}^\times \\ \alpha &\longmapsto \alpha_g \prod_i \alpha_{g_i} \end{aligned}$$

Since the projection from  $\langle F_h \rangle$  to  $\mathbb{F}_g^\times$  is surjective, there exists a  $\beta \in \langle F_h \rangle$  whose projection  $\beta_g$  in  $\mathbb{F}_g^\times$  is of order  $q^{2m} - 1$ .

The order of  $\beta \in \langle F_h \rangle$  is divisible by the order of its projection  $\beta_g \in \mathbb{F}_g^\times$ . Hence  $\langle F_h \rangle$  has an element of order  $q^{2m} - 1$  which implies that we have an inclusion

$$\mathbb{Z}/L\mathbb{Z} \hookrightarrow \langle F_h \rangle$$

and hence  $L$  divides  $|\langle F_h \rangle|$ .

Since  $\langle F_h \rangle \hookrightarrow \mathbb{F}_g^\times \times \prod_{i=1}^k \mathbb{F}_{g_i}^\times$ ,  $|\langle F_h \rangle|$  divides  $(q^{2m} - 1) \prod_{i=1}^k (q^{2 \deg(g_i)} - 1)$ .

Since  $\gcd(q^{2 \deg(g_i)} - 1, q^{2m} - 1)$  is  $q^{2C}$ -smooth for  $g_i \neq g$ , it follows that there exists integers  $w, y$  such that  $w$  is  $q^{2C}$ -smooth,  $\gcd(L, y) = 1$  and  $|\langle F_h \rangle| = Lwy$ .

For every prime  $\ell$  dividing  $L$ , the  $\ell$ -primary component of  $\langle F_h \rangle$  is cyclic since  $\mathbb{Z}/L\mathbb{Z} \hookrightarrow \langle F_h \rangle$  and  $|\langle F_h \rangle|$  is  $L$  times a factor relatively prime to  $L$ . Hence in the Smith normal form of  $\langle F_h \rangle$ , for every prime  $\ell$  dividing  $L$ , the  $\ell$ -primary component of  $\langle F_h \rangle$  is contained in the largest invariant factor. In particular, the largest invariant factor has order divisible by  $L$ .

Since  $|\langle F_h \rangle| = Lwy$ , it follows that the second largest invariant factor of  $\langle F_h \rangle$  has order dividing  $wy$ . Since  $w$  is  $q^{2C}$ -smooth and  $\gcd(L, y) = 1$ ,  $\gcd(wy, q^{2m} - 1)$  is  $q^{2C}$ -smooth.

If  $\Gamma_R = \Gamma_h$ , then  $\mathbb{Z}^{|F|}/\Gamma_R \cong \langle F_h \rangle$  and the order  $d_{|F|-1}$  of the second largest

invariant factor of  $\mathbb{Z}^{|F|}/\Gamma_R$  divides  $wy$ . Thus  $\gcd(d_{|F|-1}, q^{2m} - 1)$  is  $q^{2C}$ -smooth.  $\square$ .

**Testing Phase:** *Compute the Smith normal form of  $R$  and if  $\gcd(d_{|F|-1}, q^{2m} - 1)$  is  $q^{2C}$ -smooth, output  $\pi_{|F|}$ . Else, declare failure.*

The Smith normal form computation can be performed in  $q^{O(1)}$  time since  $R$  has at most  $\Theta(q^3)$  rows, at most  $q^2 + 2$  columns and each entry is an integer bounded by  $q^2$ .

If the testing phase is successful, we can extract a primitive element of  $\mathbb{F}_g^\times$  from the output  $\pi_{|F|}$  of the testing phase as follows. Recall that  $v$  is the largest  $q^{2C}$ -smooth factor of  $q^{2m} - 1$ . If  $\mu \in \mathbb{F}_g^\times$  is of order divisible by  $v$ , then  $\mu\pi_{|F|}$  is a primitive element in  $\mathbb{F}_g^\times$ .

Shoup [22] proved that there exists a constant  $C_1$  such that  $P := \{f(\zeta) \mid f \in \mathbb{F}_q^2[x], \deg(f) \leq C_1 \log_q(m)\}$  contains a generator of  $\mathbb{F}_g^\times$ . In particular,  $P$  has an element of order divisible by  $v$ .

Since  $C$  is a constant,  $v$  can be computed in time polynomial in  $q$ . For an  $\epsilon \in P$ , we can check if it has order divisible by  $v$  by verifying that  $\epsilon^{(q^{2m}-1)/v} \neq 1$ . By exhaustively searching, we can find an element  $\mu \in P$  of order divisible by  $v$  in time polynomial in  $|P|$  which is polynomial in  $q$ .

**2.6. Relation Generation Heuristic.** In this subsection, we argue under a heuristic assumption that the relation generation algorithm does indeed produce enough relations to successfully extract a primitive element.

We begin by counting the number of relations that we could obtain by counting the possible choices for  $(a, b, c, d)$  in the relation generation algorithm.

For an  $e \in \mathbb{F}_{q^2}^\times$ , the substitutions  $x \mapsto \frac{a\zeta+b}{c\zeta+d}$  and  $x \mapsto \frac{ae\zeta+be}{ce\zeta+de}$  are identical and will lead to the same relation. Thus, the possible choices for  $a, b, c, d \in \mathbb{F}_{q^2}$ , that could lead to distinct relations can at best be identified with elements in  $PGL(2, q^2)$ .

Further, the relations corresponding to an element in  $PGL(2, q^2)$  and its product with an element in  $PGL(2, q)$  are off by the relation corresponding to the identity  $\zeta^q - \zeta = \prod_{\alpha \in \mathbb{F}_q} (\zeta - \alpha)$ .

Thus the number of possible choices for  $a, b, c, d$  can be identified with elements in the group  $PGL(2, q^2)/PGL(2, q)$  which has cardinality  $q(q^2 + 1) = \Theta(q^3)$ .<sup>1</sup>

The probability that a random polynomial of degree at most  $D + 1$  factors into linear factors is roughly  $\frac{1}{(D+1)!}$  [19]. If the numerator polynomials  $N(x)$  that appear in the relation generation phase behave as random polynomials of the same degree with respect to their probability of splitting in to linear polynomials, then the expected number of trials required to get a relation is  $(D + 1)!$ . Since  $D$  is a constant independent of  $q$  and  $n$ , the expected number of rows of  $R$  is a constant

<sup>1</sup>We would like to thank Antoine Joux for pointing out the need to mod out by  $PGL(2, q)$ .

fraction of  $\Theta(q^3)$ .

Since the dimension of the lattice  $|F|$  is at most  $q^2 + 2$  and  $\Gamma_R$  is the lattice generated by  $\Theta(q^3)$  points, it is overwhelmingly likely that  $\Gamma_R = \Gamma_h$ , which makes the weaker claim of the heuristic 2.4 below even more plausible.

**HEURISTIC ASSUMPTION 2.4.** The generated relation lattice  $\Gamma_R$  is large enough to ensure that the greatest common divisor of  $q^{2m} - 1$  and the cardinality of the second largest invariant factor of  $Z^{|F|}/\Gamma_R$  is  $q^{2C}$ -smooth.

To summarize, our algorithm either certifiably finds a generator or indicates that it has failed in doing so. If the heuristics 2.1 and 2.4 are true, then the algorithm finds a generator in time polynomial in  $q$  which is a polynomial in  $p$  and  $n$ .

**2.7. Reducing the Problem of Finding Primitive Elements to a Conjecture.** Since the generated relation lattice  $\Gamma_R$  depends on the choice of the polynomials  $h_0$ ,  $h_1$  and  $g$ , heuristic 2.4 implicitly claims that for every choice of  $h_0$ ,  $h_1$  and  $g$ , the relation generation step succeeds in determining a primitive element. This assumption can be weakened significantly by using the following modified testing phase.

**Modified Testing:** *Compute the Smith normal form of  $R$  and if  $\gcd(d_{|F|-1}, q^{2m} - 1)$  is  $q^{2C}$ -smooth, output  $\pi_{|F|}$ . Else, continue with the search for a new choice of  $h_0$  and  $h_1$ .*

The modified testing phase implies the following theorem.

**THEOREM 2.5.** *If there exists positive integers  $D, C$  such that for all prime powers  $q$  and for all positive integers  $q/2 < m \leq q$ , there exists  $h_0, h_1 \in \mathbb{F}_{q^2}[x]$  of degree bounded by  $D$  such that  $h(x) = h_1(x)x^q - h_0(x)$  is square free, has an irreducible factor (call  $g(x)$ ) of degree  $m$ , and for each irreducible factor  $g'(x)$  of  $h(x)/g(x)$ ,  $\deg(g') > 1$  and  $\gcd(q^{2 \deg(g')} - 1, q^{2m} - 1)$  is  $q^{2C}$ -smooth and the generated relation lattice  $\Gamma_R$  corresponding to  $h_0, h_1$  is large enough to ensure that the greatest common divisor of  $q^{2m} - 1$  and the cardinality of the second largest invariant factor of  $Z^{|F|}/\Gamma_R$  is  $q^{2C}$ -smooth, then a generator for  $\mathbb{F}_{p^n}$  can be found deterministically in time polynomial in  $p$  and  $n$ .*

**2.8. The special case when  $p$  is of small order in  $(\mathbb{Z}/n\mathbb{Z})^\times$ .** For the special case when  $\text{ord}_n(p)$ , the order of  $p$  modulo  $n$  is  $(\log_p n)^{\mathcal{O}(1)}$ , we present a modification to the algorithm that results in a procedure that has a greater guarantee of success while assuming less.

In the initial step, set  $q := p^{\text{ord}_n(p)}$  and embed  $\mathbb{F}_{p^n}$  in to  $\mathbb{F}_{q^{2(q-1)}}$ .

We skip the search phase and instead set  $h_1(x) = 1$  and  $h_0(x) = \lambda x$  where  $\langle \lambda \rangle = \mathbb{F}_{q^2}^\times$ . Such an  $\lambda$  can be found in  $\mathcal{O}(q)$  time by exhaustive searching. Since  $h(x) = h_1(x)x^q - h_0(x) = x(x^{q-1} - \lambda)$ , where  $(x^{q-1} - \lambda)$  is irreducible of degree  $q - 1$ , set  $g(x) = x^{q-1} - \lambda$ .

This choice of  $h(x)$  violates the requirements of the search phase of our algorithm

since it has a linear factor  $x$ . The concern is that as a consequence we have to leave out  $x \bmod g(x)$  from the factor base. However, adding the relation  $x^{q-1}\lambda^{-1} = 1 \bmod g(x)$  to our relation generation step allows the inclusion of  $x \bmod g(x)$  in our factor base  $F$  and the correctness of the algorithm is not affected.

Since the degrees of  $h_1$  and  $h_0$  are at most 1, the numerator  $N(x)$  that appears in the relation search is of degree at most 2.

If the numerators  $N(x)$  behave as random polynomials of degree 2 in terms of factorization, then they factor with probability  $\frac{1}{2}$ . Thus, we expect to get at least  $q(q^2+1)/2$  relations. In fact, we can prove that we get at least  $2q^2+2q-1$  relations.

Consider the upper triangular subgroup  $G_U$  of  $PGL(2, q^2)/PGL(2, q)$ , that is, the subgroup whose elements have a representative of the form

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$$

where  $a \in \mathbb{F}_{q^2}^\times, b \in \mathbb{F}_{q^2}$ . The cardinality of  $G_U$  is  $((q^2-1)q^2)/((q-1)q) = q^2+q$ .

For an element in  $G_U$  corresponding to an  $a \in \mathbb{F}_{q^2}^\times$  and a  $b \in \mathbb{F}_{q^2}$ , the numerator polynomial  $n(x)$  we obtain is the linear polynomial

$$(a^q\eta - a)x + (b^q - b).$$

Thus, we are guaranteed at least  $q^2+q$  relations.

Likewise, by considering the subgroup  $G_L$  of  $PGL(2, q^2)/PGL(2, q)$  consisting of elements with a lower triangular representative, we get  $q^2+q-1$  more relations.

Thus far we have made no heuristic assumptions for this special case. The only assumption we make is that  $\mathbb{Z}^{|F|}/\Gamma_R$  is large enough to ensure that the testing phase is successful. The dimension of the relation lattice  $\Gamma_h$  is  $q^2+1$  and we get at least  $2q^2+2q-1$  distinct relations. If the relations that we obtain are modeled as being drawn independently at random from  $\Gamma_h$ , then with overwhelming probability  $\Gamma_R = \Gamma_h$ .

As a final remark, instead of restricting the factor base  $F$  to monic linear polynomials in  $\delta$ , we could also include the evaluations of quadratic irreducible polynomials in  $\mathbb{F}_{q^2}[x]$  at  $\delta$ , but only those that appear as factors of the  $N(x)$  during the relation search. Further, the first time a degree two element is encountered, it can be expressed in terms of a product of linear factors. If a quadratic factor reappears then it implies a new relation between products of linear factors.

### 3. Acknowledgements

We would like to thank Antoine Joux and Igor Shparlinski for their comments and suggestions on an earlier version of this paper.

### References

1. O. Ahmadi, I. Shparlinski, J. F. Voloch, "Multiplicative order of Gauss periods", Intern. J. Number Theory, 6 (4), 2010, pp.877-882.

2. R. Barbulescu, P. Gaudry, A. Joux, E. Thom, “A quasi-polynomial algorithm for discrete logarithm in finite fields of small characteristic”, <http://arxiv.org/abs/1306.4244>
3. E. R. Berlekamp, “Factoring Polynomials Over Finite Fields”, Bell System Technical Journal 46 (1967): 1853-1859.
4. M.-C. Chang, “Order of Gauss periods in large characteristic”, Taiwanese J. Math., 17 (2013), 621–628.
5. M.-C. Chang, “Elements of large order in prime finite fields”, Bull. Aust. Math. Soc., (to appear).
6. Q. Cheng, “On the construction of finite field elements of large order, Finite Fields and Their Applications”, Vol 11, Issue 3, Pages 358-366, 2005.
7. Q. Cheng, S. Gao and D. Wan, “Constructing high order elements through subspace polynomials”, Proceedings of the Twenty-Third Annual ACM-SIAM Symposium on Discrete Algorithms (SODA 2012), Pages: 1457-1463
8. Q. Cheng, D. Wan and J. Zhang, “Traps to the BGJT-Algorithm for Discrete Logarithms” <http://arxiv.org/abs/1310.5124>
9. F.R.K Chung, “Diameters and Eigenvalues”, J. Amer. Math. Soc. 2 (1989), no. 2, 187-196.
10. H. Davenport, “On primitive roots in finite fields”, Quart. J. Math. (Oxford) 8 (1937), 308-312.
11. S. Gao, Elements of provable high orders in finite fields, Proc. Amer. Math. Soc., 127(6):1615-1623, 1999.
12. F. Gologlu, R. Granger, G. McGuire and J. Zumbragel, “On the Function Field Sieve and the Impact of Higher Splitting Probabilities: Application to Discrete Logarithms in  $F_{2^{1971}}$ ”, Cryptology ePrint Archive: Report 2013/074.
13. F. Gologlu, R. Granger, G. McGuire and J. Zumbragel, “Discrete Logarithms in  $GF(2^{1971})$ ”, NMBRTHRY List, Feb 2013.
14. F. Gologlu, R. Granger, G. McGuire and J. Zumbragel, “Discrete Logarithms in  $GF(2^{6120})$ ”, NMBRTHRY List, Apr 2013.
15. G. H. Hardy and E. M. Wright, “An introduction to the theory of numbers”, 5th ed., Oxford Univ. Press, 1984.
16. A. Joux, “A new index calculus algorithm with complexity  $L(1/4+o(1))$  in very small characteristic”, Cryptology ePrint Archive: Report 2013/095.
17. A. Joux, “Discrete Logarithms in  $GF(2^{4080})$ ”, NMBRTHRY List, March 2013.
18. H.W Lenstra, “Finding isomorphism between finite fields”, Math. Comp., 56 (1991), pp. 329-347.
19. D. Panario, X. Gourdon, P. Flajolet, “An Analytic Approach to Smooth Polynomials over Finite Fields”, ANTS 1998: 226-236
20. R. Popovych, “Elements of high order in finite fields of the form  $\mathbb{F}_q[x]/\Phi_r(x)$ ”, Finite Fields Appl., 18 (2012), 700–710.
21. R. Popovych, ‘Elements of high order in finite fields of the form  $\mathbb{F}_q[x]/(x^m - a)$ ’, Finite Fields Appl., 19 (2013), 86–92.
22. V. Shoup, “Searching for primitive roots in finite fields”, Mathematics of Computation 58:369-380, 1992
23. I. E. Shparlinski, “On primitive elements in finite fields and on elliptic curves”, Matem. Sbornik, 181 (1990), 1196–1206 (in Russian).
24. I. E. Shparlinski, “Approximate constructions in finite fields”, Proc. 3rd Conf. on Finite Fields and Appl., Glasgow, 1995, London Math. Soc., Lect. Note Series, 1996, v.233, 313–332.
25. J. F. Voloch. “On the order of points on curves over finite fields”, Integers, 7, 2004.
26. J. F. Voloch, “Elements of high order on finite fields from elliptic curves”, Bull. Aust. Math. Soc., 81 (2010), 425–429.
27. J. von zur Gathen, I. Shparlinski, “Gauss periods in Finite Fields”, Proc. 5th Conference of Finite Fields and their Applications, Augsburg, 1999, Springer-Verlag, Berlin, (2001), 162-177.
28. D. Wan, “Generators and irreducible polynomials over finite fields”, Math. Comp. 66 (219) (1997) 1195-1212.

COMPUTER SCIENCE DEPARTMENT, UNIVERSITY OF SOUTHERN CALIFORNIA  
*E-mail address:* [mdhuang@usc.edu](mailto:mdhuang@usc.edu)

COMPUTER SCIENCE DEPARTMENT, UNIVERSITY OF SOUTHERN CALIFORNIA  
*E-mail address:* [aknaraya@usc.edu](mailto:aknaraya@usc.edu)