ON THE SELECTION OF POLYNOMIALS FOR THE DLP ALGORITHM

GIACOMO MICHELI

Abstract. In this paper we characterize the set of polynomials $f \in \mathbb{F}_q[X]$ satisfying the following property: there exists a positive integer $d$ such that for any positive integer $\ell \leq \deg(f)$ there exists $t_0$ in $\mathbb{F}_{q^d}$ such that the polynomial $f - t_0$ has an irreducible factor of degree $\ell$ over $\mathbb{F}_{q^d}[X]$. This result is then used to progress in the last step which is needed to remove the heuristic from one of the quasi-polynomial time algorithms for discrete logarithm problems (DLP) in small characteristic. Our characterization allows a construction of polynomials satisfying the wanted property.

1. Introduction

For long time the discrete logarithm problem (DLP) over finite fields has been one of the most important primitives used for cryptographic protocols. The major breakthrough in recent years concerning DLPs in small characteristic consists of the heuristic quasi-polynomial time algorithms given in [1, 3] (see also [5, 2] for their origins).

In this paper we focus on algorithm [3] which only relies on the field representation heuristic (see [3, p.2]). In fact, if that can be proved, this would show that DLP in small characteristic can indeed be solved in quasi polynomial time. Our results characterize a class of polynomials which is particularly suitable for performing the DLP-quasi polynomial time algorithm described in [3] and show that if one wants to select polynomials satisfying the wanted property, these have to be chosen in this class (see Theorem 11). Our constructions involve some Galois theory over function fields, group theory and Chebotarev density theorem. Let us start with the motivating conjecture, which has to be proved in order to remove the remaining heuristic from the algorithm in [3].

Conjecture 1. For any finite field $\mathbb{F}_q$ and any fixed positive integer $\ell = O(q)$, there exists and integer $d = O(\log(q))$ and $h_1, h_2 \in \mathbb{F}_{q^d}[X]$ coprime of degree at most 2 such that $h_1X^q + h_2$ has an irreducible factor of degree $\ell$. 

1
If this conjecture is true, then DLP in small characteristic can be solved in non-heuristic quasi-polynomial time as described in the algorithm presented in [3].

Such kind of requirement also appeared in [1, Section 5] where it is observed that the choice $h_1 = 1$ and $h_2 = X^2$ seems to always satisfy the requirements in odd characteristic and for $d = 2$. This motivates us to formulate the following

**Conjecture 2.** Let $\mathbb{F}_q$ be a finite field of odd characteristic. There exists an integer $d = O(\log(q))$ and $h_1, h_2 \in \mathbb{F}_{q^d}[X]$ coprime of degree at most 2 such that, for any positive integer $\ell \leq \deg(h_1) + q$ there exists $t_0 \in \mathbb{F}_{q^d}$ such that $h_1X^q + h_2 - t_0$ has an irreducible factor of degree $\ell$.

A polynomial satisfying Conjecture 2 will allow to build extensions with the correct representation and of desired degree.

In the next sections we will fit the conjecture above in a general context and will show a characterization of polynomials satisfying a relaxed version of Conjecture 2, in fact we will be able to prove

**Theorem 3.** Let $\mathbb{F}_q$ be a finite field of odd characteristic. There exists an integer $d \in \mathbb{N}$ and $h_1, h_2 \in \mathbb{F}_{q^d}[X]$ coprime of degree at most 2 such that, for any positive integer $\ell \leq \deg(h_1) + q$ there exists $t_0 \in \mathbb{F}_{q^d}$ such that $h_1X^q + h_2 - t_0$ has an irreducible factor of degree $\ell$. Moreover, such polynomials can be constructed explicitly.

In fact, we characterize completely polynomials $f \in \mathbb{F}_q[X]$ having the property that there exists a $d \in \mathbb{N}$ such that for any $\ell \in \mathbb{N}$, there exists $t_0 \in \mathbb{F}_{q^d}$ such that $f - t_0$ has an irreducible factor of degree $\ell$ in $\mathbb{F}_{q^d}[X]$.

On the theoretical side, our result shows the existence of such $d$ for a certain class of polynomials, which is the first step in the attempt of giving an explicit bound. In practice, our methods are constructive and they allow to build new families of polynomials (see for example the constructions in subsection 5.1) which always satisfy the wanted requirements. Even though we can show the existence of such $d$ for these families of polynomials, the wrinkle is that the required $d$ might in principle be large (but in practice, if one follows our recipe, this seems to be never the case). What remains to do to completely remove the heuristic is to give an explicit logarithmic bound for $d$ for a polynomial in our family.

1.1. **Notation.** For the entire paper $p$ is a prime and $q = p^a$ for some positive integer $a$. Let $k := \mathbb{F}_q$ be the finite field of order $q$. Let $f \in k[X] \setminus k[X^p]$. 
Let $M_f$ be the splitting field of $f - t$ over $k(t)$, which is a separable extension of $k(t)$. Let $\tilde{k}$ be the field of constants of $M_f$ i.e. the integral closure of $k$ in $M_f$. Let $A_f = \text{Gal}(M_f : k(t))$ be the arithmetic monodromy group of $f$ and $G_f = \text{Gal}(M_f : \tilde{k}(t)) \leq A_f$ be the geometric monodromy group of $f$. Let $S_n$ be the symmetric group of degree $n$. Notice that if $F_1, F_2$ are subfields of a larger field $F$, we denote by $F_1 F_2$ the the compositum of $F_1$ and $F_2$. Let $G$ be a group acting on a set $Y$. For any $y \in Y$ we denote by $\text{St}_G(y)$ the stabilizer of $y$ in $G$.

2. Galois Theory over Function Fields

**Definition 4.** Let $f \in \mathbb{F}_q[X]$. We say that $f$ is $d$-universal for some positive integer $d$ if for any positive integer $\ell \leq \deg(f)$, there exists $t_0 \in \mathbb{F}_q^d$ such that $f(X) - t_0$ has an irreducible factor of degree $\ell$. We say that $f$ is universal if it is $d$-universal for some $d$.

**Remark 5.** In this notation, in [1] it is suggested that $x^q + x^2$ is 2-universal for any odd $q$ (see section Finding appropriate $h_0, h_1$ of [1]).

In what follows we will use notation and terminology of [9]. First, we need a classical result from algebraic number theory.

**Theorem 6.** Let $L : K$ be a finite separable extension of global function fields and let $\mathcal{M}$ be its Galois closure with Galois group $G$. Let $P$ be a place of $K$ and $\mathcal{Q}$ be the set of places of $L$ lying over $P$. Let $R$ be a place of $\mathcal{M}$ lying over $P$. There is a natural bijection between $\mathcal{Q}$ and the set of orbits of $H = \text{Hom}_K(L : M)$ under the action of the decomposition group $D(R|P) = \{g \in G \mid g(R) = R\}$. In addition, let $Q \in \mathcal{Q}$ and let $H_Q$ be the orbit corresponding to $Q$. Then $|H_Q| = e(Q|P)f(Q|P)$ where $e(Q|P)$ and $f(Q|P)$ are ramification index and relative degree respectively.

A proof of Theorem 6 can be found for example in [4]. For a finite Galois extension of function fields $M : K$ with Galois group $G$, let $P$ be a degree 1 place of $K$ and $R$ be a place of $M$ lying over $P$. Let $\phi$ be the topological generator of $\text{Gal}(\overline{K} : k)$ defined by $y \mapsto y^q$. Let $k_R$ be the residue field at $R$ and let $\phi_R$ be the image of $\phi$ in $\text{Gal}(k_R : k)$. If $\mathcal{R}$ is the set of elements in $D(R|P)$ mapping to $\phi_R$, we denote by $(P, M : K)$ the set $\{g x g^{-1} : g \in G, x \in (R, M : K)\}$.

In what follows we will also need this special version of Chebotarev density theorem, which can easily be adapted from [6] or [8].

**Theorem 7 (Chebotarev Density Theorem).** Let $M : K$ be a finite Galois extension of function fields over a finite field $k$ of cardinality $q$. Let $G = \text{Gal}(M : K)$
and assume that the field of constants of $M$ is exactly $k$. Let $\Gamma$ be a conjugacy class of $G$ and let $S_K$ be the set of places in $K$ which are unramified in $M$. Then we have

$$\left| \left\{ P \in S_K \mid \deg_k(P) = 1, (P,M : K) = \Gamma \right\} \right| = \frac{|\Gamma|}{|G|} q + O \left( q^{1/2} \right).$$

The following easy lemma simplifies some of the proofs of the results in this paper.

**Lemma 8.** Let $f$ be a separable polynomial, let $k'$ be an extension of $k$, and $\tilde{k}' := k' \cap \tilde{k}$. Then

$$\text{Gal}(k'M_f : k'(t)) \cong \text{Gal}(M_f : \tilde{k}'(t)).$$

**Proof.** First we observe that if $F_1 = M_f$ and $F_2 = k'(t)$, then $F_1 \cap F_2 = \tilde{k}'(t)$. In addition, we know the Galois group of the compositum:

$$\text{Gal}(F_1 F_2 : F_1 \cap F_2) = \text{Gal}(k'M_f : \tilde{k}'(t)) \cong \text{Gal}(M_f : \tilde{k}'(t)) \times \text{Gal}(k'(t) : \tilde{k}'(t))$$

where the isomorphism is defined by the restriction map to $M_f$ and $k'(t)$. It follows easily that

$$\text{Gal}(k'M_f : k'(t)) \cong \text{Gal}(M_f : \tilde{k}'(t)).$$

□

### 2.1. Short Group Theory Interlude.

**Definition 9.** Let $X$ be a finite set and $G$ be a finite group. An action of $G$ on $X$ is said to be non-primitive if there exists an integer $\ell \in \{2, \ldots, |G| - 1\}$ and partition of $X$ into $X_1, \ldots X_{\ell}$ such that for any $i \in \{1, \ldots, \ell\}$ we have $g(X_i) = X_{i_g}$ for some $i_g \in \{1, \ldots, \ell\}$. An action is said to be primitive if it is not non-primitive.

Roughly, the above definition states that an action of a group $G$ on a set $X$ is primitive if it does not preserves any non-trivial partition of $X$. We will also need the following group theory lemma, of which we include the proof for completeness.

**Lemma 10.** Let $G$ be a subgroup of $S_n$ acting on $U = \{1, \ldots, n\}$. Suppose that $G$ acts transitively on $U$ and it contains a cycle of prime order $r$ with $r > n/2$. Then $G$ acts primitively on $U$.

**Proof.** Let $X_1 \sqcup X_2 \sqcup \cdots \sqcup X_\ell$ be a system of imprimitivity i.e. this is the partition induced by a non trivial equivalence relation $\sim$ which is $G$-invariant (i.e. $x \sim y$ implies $gx \sim gy$). Since $G$ acts transitively, we recall that $|X_i| = |X_1|$ for all
i \in \{1, \ldots, \ell\}. We argue by contradiction, by assuming 1 < |X_1| < n. Consider now the cycle \( \sigma \) of order \( r \) and take \( X_j \) which intersects the support of \( \sigma \) (i.e. \( \sigma \) acts non trivially on \( X_j \)). Consider the orbit of \( X_j \) via \( \sigma \):

\[
X_j, \sigma(X_j), \ldots, \sigma^{v-1}(X_j), \sigma^v(X_j) = X_j.
\]

As \( r > n/2 \) and \( |X_j| > 1 \), this forces \( v < r \), which implies \( \gcd(v, r) = 1 \) as \( r \) is prime. We have then that if \( v > 1 \)

\[
X_j = \sigma^r(X_j) = \sigma^v \mod v(X_j) \neq X_j.
\]

So we can assume \( v = 1 \). Now since \( \sigma \) is a cycle of prime order strictly greater than \( n/2 \), and \( \sigma(X_j) = X_j \), then \( |X_j| > n/2 \), which is a contradiction as all the \( X_i \) have the same cardinality dividing \( n \). \( \square \)

3. A characterization of universal polynomials

We are now ready to prove the main result.

**Theorem 11.** Let \( f \in \mathbb{F}_q[X] \). Suppose that \( n = \deg(f) \geq 8 \), then \( f \) is universal if and only if \( A_f = G_f = S_n \).

**Proof.** First, let us assume that \( f \) is \( d \)-universal for some positive integer \( d \). Consider first

\[
A'_f = \text{Gal}(\mathbb{F}_{q^d}M_f : \mathbb{F}_{q^d}(t)) \leq S_n.
\]

Let \( x \) be any zero of \( f(X) - t \) over \( \mathbb{F}_{q^d}(t) \). From now on, we will look at \( A'_f \) as a subgroup of the permutation group of the roots of \( f(X) - t \) (or equivalently of the set \( H = \text{Hom}_{\mathbb{F}_{q^d}(t)}(\mathbb{F}_{q^d}(x), \mathbb{F}_{q^d}M_f) \)). Our first purpose is indeed to show that \( A'_f = S_n \).

Let \( r \) be a prime in \( \{\lfloor \frac{n}{2} \rfloor + 1, \ldots, n - 3\} \). Such prime always exists by Bertrand Postulate (also known as Chebyshev’s Theorem). Fix now \( t_0 \in \mathbb{F}_{q^d} \) in such a way that \( f(X) - t_0 \) has an irreducible factor \( h(X) \) of degree \( r \) (over \( \mathbb{F}_{q^d}[X] \)). This implies immediately that the ramification at \( t_0 \) is one, as \( h(X)^e \) would have degree larger than \( n \) for any \( e > 1 \). We claim that there exists \( \gamma \in A'_f \) which is a cycle of order \( r \). Let \( P \) be the place corresponding to \( t_0 \), \( Q \) be the place of \( \mathbb{F}_{q^d}(x) \) corresponding to the irreducible factor of degree \( r \) lying over \( P \), and \( R \) be a place of \( \mathbb{F}_{q^d}M_f \) lying over \( Q \). Let \( g \in D(R|P) \) be such that its image in \( \text{Gal}(O_R/R : O_P/P) \) under the natural reduction modulo \( R \) is the Frobenius automorphism. The order of \( g \) is then divisible by \( r \), since an orbit of \( g \) acting on \( H \) has size \( r \) (by the natural correspondance given by by Theorem 6). As \( r \)
is prime, the only chance is that $g$ has a cycle of order $r$ in its decomposition in disjoint cycles. Now, as $r > n/2$, a certain power of $g$ will be a cycle of order $r$: this is our element $\gamma$.

Let us now summarize the properties of $A_f'$ given by the $d$-universality:

1. It contains a cycle of order $n/2 < r < n - 2$ (by the previous argument).
2. Since $f(X) - t_1$ is irreducible for some $t_1$, we get that $A_f'$ contains a cycle of order $n$ by a direct application of Theorem 6.
3. Analogously, it contains a cycle of order $n - 1$.

(1)+Lemma 10 implies that $A_f'$ is primitive, therefore, (1)+(2) implies that $A_f'$ contains the alternating group thanks to a theorem of Jordan [11, Theorem 13.9]. Then (2)+(3) implies that $A_f'$ is not the alternating group. It follows that $A_f' = S_n$. Let us now show that $A_f = A_f'$. Recall that $\tilde{k}$ is the constant field of $M_f$. Let $k' = \mathbb{F}_{q^2}$ and $\tilde{k}' = \tilde{k} \cap k'$. By Lemma 8

$$S_n = A_f' = \text{Gal}(k'M_f : k'(t)) = \text{Gal}(M_f : \tilde{k}'(t)).$$

Now, by observing $\text{Gal}(M_f : \tilde{k}'(t)) \leq \text{Gal}(M_f : \mathbb{F}_q(t)) = A_f \leq S_n$ we conclude $A_f' = A_f$. We have now to show that the field of constants of $M_f$ is indeed $\mathbb{F}_q$. The only other possibility is that the field of constants is $\tilde{k} = \mathbb{F}_{q^2}$ as for $n \geq 5$, $S_n$ has no normal subgroups other than the alternating group $A_n$. The reader should notice that if $d$ is even then $\tilde{k}' = \tilde{k} = \mathbb{F}_{q^2}$, therefore we are done by the fact that $G_f = \text{Gal}(M_f : \tilde{k}'(t)) = \text{Gal}(M_f : \tilde{k}(t)) = S_n$. Thus, we restrict to the case $d$ odd. Let us argue by contradiction by supposing $k'\tilde{k} = \mathbb{F}_{q^d}$. Suppose that $n = \text{deg}(f)$ is odd, and let $t_1 \in \mathbb{F}_{q^d}$ for which $f(x) - t_1$ is irreducible of degree $n$. Let us denote by $P_1$ the place corresponding to $t_1$ in $\mathbb{F}_{q^d}(t)$, $Q \subset \mathbb{F}_{q^{2d}}(x)$ be the place over $P_1$ corresponding to the irreducible polynomial $f(x) - t_1$, and $R$ a place of $\mathbb{F}_{q^d}M_f$ lying over $Q$. Since $Q$ is unique and unramified, then $R$ is unramified. Therefore, $D(R|P_1)$ is cyclic and it has exactly one orbit of order $n$ corresponding to $Q$ under the bijection given by Theorem 6. It follows that any generator of $D(R|P_1)$ is a cycle of order $n$, so $D(R|P_1)$ has order $n$. On the other hand, the order of $D(R|P_1)$ is also $f(R|P_1)$, which is divisible by $[\mathbb{F}_{q^d} : \mathbb{F}_q] = 2$ thus we have a contradiction. If $n$ is even, then take $t_2$ for which $f(x) - t_2$ has an irreducible factor $h(X)$ of degree $n - 1$ (and therefore also a factor of degree 1). Let $P_2$ be the place corresponding to $t_2$ and $Q_1, Q_2$ be the places of $\mathbb{F}_{q^{2d}}(x)$ corresponding respectively to $h(X)$ and to the factor of degree one of $f(x) - t_2$. Let $R$ be a place of $\mathbb{F}_{q^d}M_f$ lying over $P_2$. Since $Q_1$ and $Q_2$ are the unique places of $\mathbb{F}_{q^{2d}}(x)$ lying over $P_2$ and they are both unramified, then any place $R$ lying above
$P_2$ is unramified. Arguing similarly as before, we get that $D(R|P_2)$ is cyclic and it has a cycle of order $n - 1$, therefore $f(R|P_2) = |D(R|P_2)| = n - 1$. On the other hand, since the size of the decomposition group is divided by $[\mathbb{F}_{q^d} : \mathbb{F}_{q^d}] = 2$, we get the contradiction we wanted.

This shows that the constant field of $\mathbb{F}_{q^d}M_f$ is $\mathbb{F}_{q^d}$. On the other hand, the field of constant of $\mathbb{F}_{q^d}M_f$ is $\tilde{k}\mathbb{F}_{q^d}$: as $d$ is odd, this forces $\tilde{k} = \mathbb{F}_q$ (as the only other chance was $k' = \mathbb{F}_{q^{2d}}$).

Let us prove the other implication. Suppose that $G_f = A_f = S_n$ and fix $\ell \in \{1, \ldots, n\}$. Let now $\gamma$ be a cycle of $G_f$ of order $\ell$ and let $\Gamma$ be its conjugacy class. In the notation of Theorem 7, for any $d \in \mathbb{N}$ we have that

$$|\{P \in S_{\mathbb{F}_{q^d}(t)} \mid \deg_{\mathbb{F}_{q^d}}(P) = 1, (P, M : K) = \Gamma\}| = \frac{|\Gamma|}{|G_f|}q^d + O\left(q^{d/2}\right),$$

where the implied constant is independent of $d$ and $q$. This shows immediately that, when $d$ is large enough, there is an unramified place $P$ of degree $1$ in $\mathbb{F}_{q^d}(t)$ (corresponding to an element $t_0 \in \mathbb{F}_{q^d}$) for which $\gamma$ is the Frobenius (for some place of $\mathbb{F}_{q^d}M_f$ lying over $P$). As $\gamma$ is a cycle of order $\ell$, by applying Theorem 6 we get that $f(X) - t_0$ has a factor of degree $\ell$ in $\mathbb{F}_{q^d}[X]$. \hfill \Box

**Corollary 12.** Suppose that $f$ is $\overline{d}$-universal for some $\overline{d}$, then there exists $d_0$ for which $f$ is $d$-universal for every $d > d_0$.

**Proof.** Suppose that $f$ is $\overline{d}$-universal, then $G_f = A_f = S_n$. By the same argument as in the proof the second implication of Theorem 11, it follows that when $d$ is large enough the number of $t_0 \in \mathbb{F}_{q^d}$ for which $f(x)$ has an irreducible factor of degree $\ell$ can be estimated with $\frac{|\Gamma|}{|G_f|}q^d$ for $\Gamma$ the conjugacy class of an element having a cycle of order $\ell$ in its decomposition in disjoint cycles (one can actually directly select an element which "is" a cycle of order $\ell$). \hfill \Box

**Corollary 13.** A universal polynomial $f$ of degree greater than or equal to $8$ is indecomposable, i.e. it cannot be written as composition of lower degree polynomials.

**Proof.** By Theorem 11, it is enough to observe that $S_n$ acts primitively on the roots of $f$. This forces the polynomial to be indecomposable (see for example [7, Section 2.3]). \hfill \Box

The statement of Theorem 3 now follows with the choice $h_1 = 1$ and $h_2 = x^2$. 

4. UNIVERSALITY FOR $X^q + X^2 - t$

In this section, let us specialize to the polynomial $f = X^q + X^2$, as this is the one suggested for the function field sieve [1] and experimentally is believed to be 2-universal, see last paragraph in [1, Section 5]. Let us recall a result due to Turnwald [10].

**Theorem 14.** Let $k$ be a field of characteristic different from 2 and $g \in k[X]$. Suppose that the derivative $g'$ of $g$ has at least a simple root and for any pair of roots $\alpha, \beta$ of $g'$ over $k$ we have that $g(\alpha) \neq g(\beta)$. In addition suppose that $\text{char}(k) \nmid \deg(g)$. Then the Galois Group of $g - t$ over $k(t)$ is $S_{\deg(g)}$.

With this tool in hand, we are able to compute the arithmetic and the geometric monodromy group of $X^q + X^2$.

**Proposition 15.** Let $\text{char}(F_q) \neq 2$ and $f = X^q + X^2 \in F_q[X]$. The Galois Group $A_f$ of $f - t \in F_q(t)[X]$ over $F_q(t)$ is $S_q$. Moreover $G_f = A_f$.

**Proof.** Clearly, Theorem 14 does not apply to the polynomial above as its degree is divisible by the characteristic of the field. Let us consider the extension $F_q(x) : F_q(t)$ where $x$ is a root of $f - t$, and then verifies $f(x) = x^q + x^2 = t$. Let $\{y_1, \ldots, y_{q-1}\}$ be the set of roots of $X^{q-1} + X + 2x \in F_q(x)[X]$. They are all distinct, as the polynomial is separable. It is easy to see that $x + y_i$ is a root of $f - t$ for any $i \in \{0, \ldots, q-1\}$. Therefore, the splitting field $M_f$ of $f - t$ over $F_q(t)$ is exactly $F_q(x_1, \ldots, x_{q-1})$. Let us now consider $B = \text{Gal}(M_f : F_q(x))$ which is a subgroup of $A_f = \text{Gal}(M_f : F_q(t))$. The Galois Group $B$ is the same as the Galois group of the polynomial $\frac{X^{q-1} + X}{2} - x \in F_q(x)$, for which Turnwald theorem applies with base field $F_q(x)$ since

- $\text{char}(F_q) \neq 2$
- The roots of $X^{q-2} - 1$ are $\xi_i$ for $\xi$ a primitive $(q - 2)$-root of unity and $i \in \{0, \ldots, q - 3\}$.
- $\frac{\xi^{(q-1)+\xi_i}}{2} = \frac{\xi^{(q-1)+\xi_j}}{2}$ implies $\xi_i = \xi_j$ but then $i = j$.

We are now sure that the Galois Group of $\frac{X^{q-1} + X}{2} - x$ is $B = S_{q-1}$. Observe that $B \leq A_f$ and $A_f$ acts transitively on the set of roots $\{x, x + y_1, x + y_2, \ldots, x + y_{q-1}\}$ and the stabilizer of $x$ contains $B$. By the orbit-stabilizer theorem we have that

$$q = \frac{|A_f|}{|\text{St}_{A_f}(x)|} \leq \frac{|A_f|}{|B|} = \frac{|A_f|}{(q - 1)!}$$
Therefore $|A_f| \geq q!$ but also $|A_f| \leq q!$ as $A_f$ is a subgroup of $S_q$, so $A_f = S_q$. We have now to show that $G_f = A_f$. Suppose that the constant field of $M_f$ is $\bar{k}$ and notice that all the arguments above apply again by replacing $F_q$ with $\bar{k}$. Hence this immediately shows $G_f = S_n$. □

**Corollary 16.** There exists $d_0 \in \mathbb{N}$ such that $X^q + X^2$ is $d$-universal for any $d > d_0$.

*Proof.* By individually checking the cases $q < 8$ we can assume $q \geq 8$. By the previous result we have that Theorem 11 applies, therefore it also applies Corollary 12, which is exactly the claim. □

The reader should notice now that the first occurrence of $d_1$ for which $X^q + X^2$ is $d_1$ universal might be strictly less than $d_0$. What would be ideal to show, is that $d_0$ is indeed “small” enough (conjecturally it is 2), on the other hand the above corollary at least shows that such $d$ exists.

5. **Constructing $d$-universal polynomials in odd characteristic**

The combination of Theorem 14 and Theorem 11 gives a deterministic easy way to construct polynomials which are likely to build up any extension between the base field and the degree of the polynomial satisfying Conjecture 2. We give a class of examples in the next subsection. For the rest of this section, $q$ will be an odd prime power.

5.1. **Universality for $X^q + jX$.** In this subsection we show a large class of polynomials which can be shown to be universal. In addition such polynomials appear to be always $d$-universal for a small $d$.

**Proposition 17.** Let $q$ be an odd prime power and $\mathbb{F}_p$ be its prime subfield. Let $j \in \mathbb{N} \setminus \{0, 1, pk\}_{k \in \mathbb{N}}$. The polynomial $f = X^{q+j} - j X \in \mathbb{F}_q[X]$ is universal.

*Proof.* We would like to verify the conditions of Theorem 14 for the geometric monodromy group of $f$, then it will follow that also the arithmetic monodromy group of $f$ is the symmetric group, for which Theorem 11 now applies, showing the universality of $f$.

The derivative of $f$ is $f' = jX^{q+j-1} - j$. Since $j$ is different from 1, then $f'$ has all single roots in $\mathbb{F}_q$. Now, any root of $f$ has the form $\xi^u$, where $\xi$ is a fixed primitive $q+j-1$ root of unity, and $u$ is an integer in $\{0, \ldots, q+j-2\}$.

It is now enough to observe that $f(\xi^u) = \xi^u - j\xi^u = (1-j)\xi^u \neq (1-j)\xi^v = f(\xi^v)$ for $u \neq v \mod q+j-1$. 
The conditions of Theorem 14 are now verified and then Theorem 11 applies, leading to the claim. □

Remark 18. The experiments show that this class of polynomials actually verifies a stronger property, i.e. each of them seems to be $d$-universal for $d = j + 1$. In particular, for $j = 2$, the polynomial $X^{q+2} - 2X$ is 3-universal for any prime $q$ less than $401$, therefore building up suitable extensions of size up to 401.

Acknowledgements

The author is grateful to Michael Zieve for many interesting discussions and especially for introducing him to the version of Chebotarev Density Theorem used in this paper. The author also wants to thank Swiss National Science Foundation grant number 171249.

References

[1] Razvan Barbulescu, Pierrick Gaudry, Antoine Joux, and Emmanuel Thomé. Advances in Cryptology – EUROCRYPT 2014: 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Copenhagen, Denmark, May 11-15, 2014. Proceedings, chapter A Heuristic Quasi-Polynomial Algorithm for Discrete Logarithm in Finite Fields of Small Characteristic, pages 1–16. Springer Berlin Heidelberg, Berlin, Heidelberg, 2014. ISBN 978-3-642-55220-5. doi: 10.1007/978-3-642-55220-5_1. URL http://dx.doi.org/10.1007/978-3-642-55220-5_1.
[2] Faruk Göloğlu, Robert Granger, Gary McGuire, and Jens Zumbrgel. On the Function Field Sieve and the Impact of Higher Splitting Probabilities: Application to Discrete Logarithms in $\mathbb{F}_{2^{1971}}$ and $\mathbb{F}_{2^{3164}}$. In Ran Canetti and Juan A. Garay, editors, Advances in Cryptology CRYPTO 2013, 33rd Annual Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2013. Proceedings, Part II., Lecture Notes in Computer Science, pages 109–128. Springer Berlin Heidelberg, 2013. URL http://link.springer.com/chapter/10.1007%2F978-3-642-40084-1_7. Best Paper Award (by unanimous decision of the Program Committee).
[3] Robert Granger, Thorsten Kleinjung, and Jens Zumbrägel. On the discrete logarithm problem in finite fields of fixed characteristic. arXiv preprint arXiv:1507.01495, 2015.

1The computations were performed in SAGE and the code is available upon request.
[4] Robert M Guralnick, Thomas J Tucker, and Michael E Zieve. Exceptional covers and bijections on rational points. International Mathematics Research Notices, 2007:rnm004, 2007.
[5] Antoine Joux. A new index calculus algorithm with complexity $l (1/4+ o (1))$ in small characteristic. In International Conference on Selected Areas in Cryptography, pages 355–379. Springer, 2013.
[6] Michiel Kosters. A short proof of a chebotarev density theorem for function fields. arXiv preprint arXiv:1404.6345, 2014.
[7] Peter Müller. Primitive monodromy groups of polynomials. Contemporary Mathematics, 186:385–385, 1995.
[8] Michael Rosen. Number theory in function fields, volume 210. Springer Science & Business Media, 2013.
[9] Henning Stichtenoth. Algebraic function fields and codes, volume 254. Springer Science & Business Media, 2009.
[10] Gerhard Turnwald. On schur’s conjecture. Journal of the Australian Mathematical Society (Series A), 58(03):312–357, 1995.
[11] Helmut Wielandt. Finite permutation groups. Academic Press, 2014.