GENERALIZATION OF BURGESS' LEMMA TO GENERAL COMPLETELY FACTORISABLE POLYNOMIALS

HIMANSHU SHUKLA
MENTORS: DR. NITIN SAXENA & DR. RAJAT MITTAL

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
INDIAN INSTITUTE OF TECHNOLOGY, KANPUR

Abstract. We study the deterministic bounds on the problem of polynomial factoring over finite fields, for that we study the distribution of quadratic residues and non residues in the residue field of an odd prime p. In 1957, D. A. Burgess proved that for sufficiently large p, if we take any continuous interval of length $O(p^{1/4})$ in multiplicative group of $\mathbb{Z}_p$ then not every element in the interval will have same residuosity. We wish to study the extension of this theorem to quadratic polynomials of form $x(x+a)$ i.e. we wish to have an upper bound on I, B (say), such that for given n, I, a, if I is larger than B, then $\sum_{n}^{n+I} \chi_p(x(x+a)) < \epsilon I$, for a sufficiently large p, where $\chi_p(.)$ represents the Legendre symbol with respect to p. In simpler terms we try to find maximal interval length B, such that for sufficiently large p, if we take two continuous intervals of same length I, $I > B$ in $\mathbb{Z}_p$, then they should not have same distribution of quadratic residues and non residues in them. Bound on I will dictate the bound of deterministic time complexity of polynomial factoring over finite fields. The best known bound on I is $O(p^{1/2}log(p))$ by Victor Shoup in 1990. For this we present the proof of a generalization of Lemma 2 in Burgess' 1957 paper using Burgess' technique.

1. Introduction

Before moving ahead we will first state the problem of polynomial factoring over finite fields.

> Given a monic univariate polynomial $f(x)$ in the ring $\mathbb{F}_q[x]$, where $\mathbb{F}_q$ is a finite field with q elements. We want a polynomial time deterministic algorithm to factorise $f(x)$ into its monic, univariate, irreducible polynomials $f_1(x), f_2(x), \ldots, f_k(x)$ such that $f_i(x) \in \mathbb{F}_q[x]$, $\forall i$ in $\{1, 2, \ldots, k\}$.

This problem has been of interest to mathematicians and computer scientist since long, due to its vast number of applications, to which, we will come later in this section. First let us describe the present state of the problem. Using randomness, there exist few randomised algorithms like Cantor-Zassenhaus [5], and Berklecamp [3], which for all practical purposes run in polynomial time. But, still the question whether there exists a deterministic polynomial time algorithm is open. Ivanyos, Karpinski, Saxena [6] came up with the first polynomial time deterministic algorithm to factor polynomials of prime degree n over finite fields, assuming Generalised Riemann's Hypothesis (GRH). Also assuming GRH there are algorithms known for polynomial factoring over finite fields which are sub-exponential in time for instance Rónyai [8]. The best known deterministic and unconditional bound for this problem is by Victor Shoup [9] which is "$O(n^2 p^{\frac{1}{2}} log(p))$" for polynomials over $\mathbb{F}_p$ where n is the degree of polynomial.

Various finite field applications require polynomials in them. Few good examples would be:

- In construction of error correcting codes like BCH code, Goppa, Reed-Solomon codes and other cyclic redundancy codes, we require the solution of this problem.
- Public key cryptosystems using elliptic curves also use this as a sub problem.
- The problem of factoring multivariate polynomials over finite fields can also be reduced to this problem.
- Also used in generation of pseudorandom sequences.

For a detailed report over this one can look at survey by Gathen & Panario [10]. Also a detailed report of BIRS (Banff International Research Station) [2] meet of Finite Field experts in 2006, summarises the major advancements in this area.

The problem of deterministic upper bound on polynomial factoring over finite fields is closely related to the following problem.

> We want to find a bound for the value of I in terms of p, ϵ say $B(p, \epsilon)$ such that for sufficiently large p and fixed values of n, I, a and ϵ, if $I > B(p, \epsilon)$ then
>
> $$\sum_{x=n}^{n+I} \chi_p(x(x+a)) < \epsilon I$$

This essentially means that we want to bound the interval length I by $B(p, \epsilon)$ such that, if we have two continuous intervals of length $I > B(p, \epsilon)$ in $\mathbb{Z}_p$, then we cannot have the distribution of quadratic residues and non residues exactly same in them, i.e. for each i, we cannot have quadratic residuosity of i^{th} element in first interval same as quadratic residuosity of i^{th} element in the second interval. The best known limit on I is by Victor Shoup, which is $O(p^{\frac{1}{2}} log(p))$. In this report we present the generalised form of Burgess' Lemma 2 [4] which from now we will call *Theorem 1* for convenience. Using this we have a shorter proof for the current deterministic bound on polynomial factoring over finite fields. An outline of the report is as follows: In section 2 and 3 we present few notations and preliminary results required for this report. In section 4 we present the generalised form of Burgess Lemma i.e. Theorem 1 and few lemmas required to prove it. Finally in 5 we conclude the report.

2. Notations

Following is the list of the notations that we would be using in this report.

- p will always represent an odd prime number.
- $\mathbb{F}$ will always represent a field.
- We represent the set $\{0, 1, 2, \ldots, k\}$ for any fixed integer k by $[k]$.
- We represent order of an element a in multiplicative group of $\mathbb{Z}_p$ by $Ord_p(a)$.
- We represent the quantity $\left(\frac{a}{p}\right)$ where (.) represents the $Legendre's$ symbol of a an integer with respect to p, by $\chi_p(a)$.
- Let $f(x, y)$ be a bivairate polynomial in the polynomial ring $\mathbb{F}[x, y]$. Then degree of $f(x, y)$ denoted by $deg(f)$ is
  $$\max\{\alpha + \beta : x^\alpha y^\beta \text{ is monomial term of } f(x, y) \text{ with non-zero coefficient}\}$$
- Similarly we denote degree of $f(x, y) \in \mathbb{F}[x, y]$ with respect to x by $deg_x f$ i.e.
  $$deg_x f = \max\{\alpha : x^\alpha y^\beta \text{ is monomial term of } f(x, y) \text{ with non-zero coefficient}\}$$
- If $f(x, y)$ and $g(x, y)$ be two bivariate polynomials in $\mathbb{F}[x, y]$, then $Res_x(f, g)$ represents the resultant of f, g with y treated as constant. Notice that $Res_x(f, g) \in \mathbb{F}[y]$.

3. Preliminaries

Following is the set of facts that we will assume without proof in this report.

- *Fact 1:* The degree of polynomial $Res_x(f,g) = R(y)$, where $f, g \in \mathbb{F}[x,y]$, is upper bounded by $deg(f) * deg(g)$. [1]
- *Fact 2:* Roots of $Res_x(f,g) = R(y)$, f and g same as above capture those y points where f and g have a common zero. [1]
- *Fact 3:* If $f(x)$ is a square free, monic, completely factorisable polynomial (in $\mathbb{Z}_p$) with integral coefficients. Then [9]
$$\sum_{x \in \mathbb{Z}_p} \chi_p(f(x)) \leq (deg(f) - 1)p^{\frac{1}{2}}.$$
- *Fact 4:* $\chi_p(a^k) = \chi_p(a)^k = \chi_p(a)$ if k is odd else 1.

4. Theorem 1

Let $\mathcal{A}$ represent the set
$$\mathcal{A} = \{a_i : i \in [n]/\{0\} \text{ for some fixed } n\}$$
and $\mathcal{K}$ represent the set
$$\mathcal{K} = \{2^i : i \in [Ord_p(2) - 1]\}$$
From now onwards $\mathcal{A}$ and $\mathcal{K}$ will always represent these sets and n will always represent cardinality of $\mathcal{A}$. This theorem is the generalisation of Lemma 2 of Burgess [4]. It states:

Let $\mathcal{H}$ be any subset of $\mathbb{Z}_p$, whose cardinality is h, also let $\phi(x) = \prod_{a_i \in \mathcal{A}} (x + a_i)$.

Define the quantity $S_{\mathcal{H}}(x)$ for given $\mathcal{A}$ and $\mathcal{H}$ as,
$$S_{\mathcal{H}}(x) = \sum_{b \in \mathcal{H}} \chi_p(\phi(x+b))$$
Then for a given integer $r > 0$ and sufficiently large p.
$$\sum_{x \in \mathbb{Z}_p} (S_{\mathcal{H}}(x))^{2r} < (2rh)^{2r}p + nr(2 * p^{\frac{1}{2}} + 1)h^{2r})$$

For proving this theorem we need following lemmas.

Lemma 1. *: Let $f(x)$ be a polynomial in the polynomial ring $\mathbb{F}_p[x]$ and let*
$$g(x) = \prod_{a_i \in \mathcal{A}} f(x + a_i)$$
be a perfect square modulo p. Then
$$\psi(x,k) = \prod_{a_i \in \mathcal{A}} f(x + ka_i)$$
is a perfect square $\forall k \in \mathcal{K}$.

Proof: We look at the quantity
$$g(x + a_j),\ a_j \in \mathcal{A}$$
For each a_j in $\mathcal{A}$, $g(x + a_j)$ is a perfect square, since $g(x)$ is a perfect square. This implies that the quantity
$$\prod_{a_j \in \mathcal{A}} g(x + a_j)$$

is a perfect square modulo p. But

$$\begin{aligned}\prod_{a_j\in\mathcal{A}} g(x+a_j) &= \prod_{a_j\in\mathcal{A}}\prod_{a_i\in\mathcal{A}} f(x+a_i+a_j)\\ &= (\prod_{a_j=a_i} f(x+2a_i))(\prod_{a_j\neq a_i} f(x+a_j+a_i)) \\ &= (\prod_{a_j=a_i} f(x+2a_i))(\prod_{\substack{a_j\neq a_i\\ i>j}} f(x+a_j+a_i)^2)\end{aligned} \tag{1}$$

This implies that

$$\prod_{a_i\in\mathcal{A}} f(x+2a_i)$$

is a perfect square. But now replace $\mathcal{A}$ by

$$2*\mathcal{A} = \{2*a_i : a_i \in \mathcal{A}\}$$

and hence we go on, which essentially proves the lemma i.e.

$$\forall k \in \mathcal{K},\ \psi(x,k) = \prod_{a_i\in\mathcal{A}} f(x+ka_i)$$

is a perfect square.

Lemma 2. *: If $\psi(x,y)$ in $\mathbb{F}[x,y]$, with $deg(\psi(x,y)) = d$, is square free polynomial as a bivariate and number of values of y for which $\psi(x,y)$, is not square free, is finite and atleast γ. Then $\exists$ a polynomial $\theta(y)$, such that $deg(\theta(y)) \leq d^2$ and $\theta(y)$ has at least γ roots.*

Proof: Let derivative of any polynomial $\eta(x,y)$ in the polynomial ring $\mathbb{F}[X,Y]$ over field $\mathbb{F}$, with respect to x is denoted by $d_x\eta$. Now let us look at the polynomial

$$Res_x(\psi(x,y), d_x\psi) = R(y)$$

If $\psi(x,y)$ is not square free as a bivariate polynomial, then $R(y))$ is essentially 0. Otherwise by Fact 1 we know that

$$deg(R(y)) \leq d^2$$

Also by Fact 2 we know that $R(y)$ captures all the points k where ψ and $d_x\psi$ have a common root. As ψ is not square free for atleast γ values of k, hence $R(y)$ has atleast γ roots. Put $\theta(y) = R(y)$.

Note: In above proof ψ is a general bivariate polynomial with only condition that it is square free.

Lemma 3. *: $\psi(x,y) \in \mathbb{F}[x,y]$, be equal to*

$$\prod_{a_i\in\mathcal{A}} f(x+ya_i)$$

for a given set $\mathcal{A}$, and let $f(x) \in \mathbb{F}[x]$ be a polynomial with splitting field, $\mathbb{F}_s$, such that

$$f(x) = \prod_{\beta_i}(x+\beta_i)$$

where $\{\beta_1, \beta_2 \ldots, \beta_l\} \subset \mathbb{F}_s$. Then $\psi(x,y)$ is a bivariate square free polynomial iff $f(x)$ is a square free polynomial.

Proof: If $f(x)$ is not square free, then

$$f(x+ya_i),\ a_i \in \mathcal{A}$$

is not perfect square free, when viewed as a bivariate. Hence

$$\psi(x,y) = \prod_{a_i \in \mathcal{A}} f(x + ya_i)$$

is not square free as a bivariate.

If $\psi(x,y)$ is not square free and $f(x)$ is square free then, this is possible *iff* at least one of $\beta_i + ya_j = \beta_k + ya_m$ as a monomial in y, for some i, j, k, m, but then this implies that $\beta_k = \beta_i$ and $a_j = a_m$. But this is leads to contradiction as $f(x)$ is square free. Hence the lemma follows.

Proof of theorem 1: Using combinatorial arguments we have

$$\sum_{x \in \mathbb{Z}_p} (S_{\mathcal{H}}(x))^{2r} = \sum_{x \in \mathbb{Z}_p} \sum_{b_1 \in \mathcal{H}} \cdots \sum_{b_{2r} \in \mathcal{H}} \prod_{\substack{b_j \\ j \in [[2r]/\{0\}}} \chi_p(\phi(x + b_j)) \quad (2)$$

To avoid the cumbersomeness in notations, with b_j we would mean "b_j for some $j \in [2r]/\{0\}$". We are interested in knowing the fact, when $\prod_{b_j} \phi(x + b_j)$ for some fixed sequence of b_j's becomes a perfect square. By observation

$$\begin{aligned}
\prod_{b_j} \phi(x + b_j) &= \prod_{b_j} \prod_{a_i \in \mathcal{A}} (x + a_i + b_j) \\
&= \prod_{a_i \in \mathcal{A}} \prod_{b_j} (x + b_j + a_i) \\
&= \prod_{a_i \in \mathcal{A}} f(x + a_i)
\end{aligned}$$

where, $f(x) = \prod_{b_j}(x + b_j)$. We eliminate the cases when $f(x)$ is a perfect square which makes

$$\psi(x,k) = \prod_{a_i \in \mathcal{A}} f(x + ka_i)$$

a perfect square as a bivariate in $\mathbb{Z}_p[x,k]$. Note that $f(x)$ is a perfect square *iff* only there are even number of b_i's taking a particular value. Now this implies $\psi(x,k)$ is a perfect square as a bivariate if even number of b_i's take a particular value. Number of cases when this happens is bounded by $(2rh)^r$ and for each of those cases the inner most sum

$$S = \sum_{x \in \mathbb{Z}_p} \chi_p(\prod_{a_i \in \mathcal{A}} \phi(x + a_i))$$

(3)

is bounded by p. Hence this portion contributes $(2rh)^r p$ to the inequality.

Now we look at the other case when $f(x)$ is not perfect square, then $f(x)$ can be written as $\prod_{\beta_i}(x + \beta_i)^{e_i}$

where the set $\{\beta_i\} \subset \mathbb{Z}_p$ and e_i's are integers ≥ 1 . Since $f(x)$ is not a perfect square hence at least one of the e_i's is odd. We now construct a polynomial $f'(x)$ from $f(x)$ as follows:

- If a factor in $f(x)$ has even power then do not include it in $f'(x)$.
- If a factor in $f(x)$ has odd power then include it in $f'(x)$ and give it power 1.

Note that $f(x)$ would be a perfect square *iff* $f'(x) = 1$ also that $f'(x)$ captures all the factors in $f(x)$ whose power is odd. Also we construct the polynomial $\psi'(x,k)$ by keeping $f'(x)$ in $\psi(x,k)$. Also

$$\prod_{a_i \in \mathcal{A}} \chi_p(f(x+a_i)) = \prod_{a_i \in \mathcal{A}} \chi_p(f'(x+a_i))$$

but for the cases when $x \equiv -(a_i + b_j) mod(p)$ which can at most be at nr points over all combinations of $a_i + b_j$. Hence we would deal with $f'(x)$ instead of $f(x)$.
Now we assume that $f(x)$ is not a perfect square and the product, $\prod_{a_i \in \mathcal{A}} f(x+a_i)$ becomes a perfect square then clearly $\prod_{a_i \in \mathcal{A}} f'(x+a_i)$ is perfect square, now using lemma 1, $\psi'(x,k)$ is perfect square $\forall k \in \mathcal{K}$. Using lemma 4 on $f'(x)$, we have, $\psi'(x,k)$ is square free as a bivariate.
Now we bound the value of p for such conditions to hold.
Hence using lemma 2 on $\psi'(x,k)$ and taking γ to be $|\mathcal{K}| = Ord_p(2)$, we have

$$|\mathcal{K}| < 4r^2n^2$$

which implies

$$p < 2^{4r^2n^2}.$$

If we chose p to be sufficiently large then we cannot have $\prod_{a_i \in \mathcal{A}} f'(x+a_i)$ as perfect square if $f'(x) \neq 1$.
This implies that for large enough p i.e. $p \geq 2^{4r^2n^2}$ we cannot have $\prod_{a_i \in \mathcal{A}} f(x+a_i)$ a perfect square, if $f(x)$ is not a perfect square. The number of cases when at least one value is taken by odd number of b_i's is bounded by h^{2r}. For these values we can write

$$\sum_{x \in \mathbb{Z}_p} \chi_p(\prod_{a_i \in \mathcal{A}} \prod_{b_j} (x + b_j + a_i)) = \sum_{x \in \mathbb{Z}_p} \chi_p(\prod_{\alpha_i \in \mathcal{L}} (x + \alpha_i)).$$

For some $\mathcal{L} \subset \mathbb{Z}_p$.

Using Fact 4 over the product $\prod_{a_i \in \mathcal{A}} \prod_{b_j} (x + b_j + a_i)$ and using the form of $\prod_{a_i \in \mathcal{A}} f(x+a_i)$, as we have used the form of $f(x)$ to come up with $f'(x)$. Note that we ignore the cases when $x \equiv -b_j - a_i (modp)$ and power of the factor is even as we then make it 1 which gives an error of nr, and for a given sequence of b_i's there can at most be nr such cases, hence we ignore them for a while and will add them afterwards. Now let

$$\zeta(x) = \prod_{\alpha_i \in \mathcal{L}} (x + \alpha_i) \tag{4}$$

Note that $deg(\zeta) = |\mathcal{L}| \leq 2nr$. By Fact 3 we have

$$\sum_{x \in \mathbb{Z}_p} \chi_p(\zeta(x)) \leq (2nr-1)p^{\frac{1}{2}}. \tag{5}$$

Hence for the case when we have at least one value taken by odd number of b_i's we have the inner sum $|S| < nr + (2nr-1)p^{\frac{1}{2}}$. Hence we derive our second term of the inequality.

Using this we can have an easy proof of $p^{\frac{1}{2}} + \epsilon$ (for arbitrary ϵ) bound on polynomial factoring.

Now we consider the requirement of largeness of p for which theorem 1 will hold. We find that even for $|\mathcal{A}| = 3$ and $r = 10$, p needs to be greater than 2^{3600}. But the following lemma makes this bound practical for almost all primes.

Lemma 4. *[7]: Chose some arbitrary $\epsilon > 0$, then almost for all p,*

$$Ord_p(2) \geq p^{\frac{1}{2}-\epsilon}$$

Hence using lemma 4, we find that almost for all p we have $Ord_p(2) > p^{\frac{1}{3}}$, that lowers the bound on p sufficiently. So for almost every p the requirement would be $p > 3600^3$.

5. Conclusion

We have proved theorem 1 but still the problem of lowering the bound on

$$\sum_{n}^{n+H} \chi_p((x+a)(x+b))$$

remains open, hence the deterministic bound on polynomial factoring remains the same. Using this we have a shorter proof for the existing bound. Also bringing down the Burgess' bound even for a linear polynomial instead of a quadratic has be an open problem since long and has got many implications not only, for practical purposes but also for theoretical purposes.

References

[1] Computational Algebra Lecture Notes, Nitin Saxena. http://www.cse.iitk.ac.in/users/nitin/courses/CS681-2014-15-I/pdfs/lec08.pdf, 2006.

[2] Polynomials over Finite Fields and Applications. https://www.birs.ca/workshops/2006/06w5021/report06w5021.pdf, 2006.

[3] E.R. Berklecamp. Factoring polynomials over finite fields. *Bell Syst. Tech. J*, 46:1853–1859, 1967.

[4] D.A. Burgess. The distribution of qudratic residues and non-residues. *Mathematika*, 4(8):106–112, 1957.

[5] David G. Cantor and Hans Zassenhaus. A new algorithm for factoring polynomials over finite fields. *Mathematics of Computation*, 36(154):pp. 587–592, 1981.

[6] Gábor Ivanyos, Marek Karpinski, and Nitin Saxena. Schemes for deterministic polynomial factoring. In *Proceedings of the 2009 international symposium on Symbolic and algebraic computation*, pages 191–198. ACM, 2009.

[7] C.R. Matthews. Counting points modulo p for some finitely generated subgroups of algebraic groups. *Bell Syst. Tech. J*, 14:149–154, 1982.

[8] Lajos Rónyai. Galois groups and factoring polynomials over finite fields. *SIAM J. Discrete Math.*, 5(3):345–365, 1992.

[9] Victor Shoup. A fast deterministic algorithm for factoring polynomials over finite fields of small characteristic. In *Proceedings of the 1991 international symposium on Symbolic and algebraic computation*, pages 14–21. ACM, 1991.

[10] Joachim von zur Gathen and Daniel Panario. Factoring polynomials over finite fields: A survey. *J. Symb. Comput.*, 31(1/2):3–17, 2001.