GNERALISED FORM OF BURGESS' LEMMA 2 AND EASIER PROOF OF DETERMINISTIC BOUND ON POLYNOMIAL FACTORING

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

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

Abstract. This report presents a generalised version of Burgess'[2] Lemma 2 which indeed is the first step towards lowering the bound on the quantity $\sum_{n}^{n+H} \chi_p((x+a)(x+b))$.

1. Introduction

This report is an output of an attempt to lower the bound on the quantity

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

for given n, H, a, b. Which dictates the diterministic bounds on the problem of polynomial factoring on finite fields. As an attempt to do this we present the most generalised form of Lemma 2 of Burgess'[2]. Before moving ahead we define the problem of polynomial factoring over finite fields.

> Given a monic univariate polynomial $f(x)$ in a the ring $\mathbb{F}_q[x]$, where $\mathbb{F}_q$ is a finite field with q (q is odd) elements. Using facts about field extensions and vector spaces we know that $q = p^r$ for some odd prime p and r an integer larger than 0. We want an efficient algorithm to factorise $f(x)$ into distinct 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, which we will come later in this section. First lets describe the present state of the problem. First of all by efficient algorithm we mean that we want a polynomial time algorithm. In general we feel that its hard do factor anything but using randomness in nature few randomised algorithms like Cantor-Zassenhaus[3], and Berklecamp[1] were designed that 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[4] came up with the first polynomial time deterministic algorithm to factor polynomial of prime degree n oven finite fields, assuming Generalised Reimann's Hypothesis (GRH). Also assuming GRH there are algorithms known for polynomial factoring over finite fields which are sub-exponential in time for instance Ronyai[5]. The best known deterministic and unconditional bound for this problem is by Victor Shoup [6] which is "$O(n^2 log(p))$" for polynomials over $\mathbb{F}_p$ where n is the degree of polynomial.

Now we come to question of applications of this problem. Various finite field applications require polynomials over 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 surve by Gathen & Panario [7]. Also a detailed report of BRIS (Banff International Research Station) meet of Finite Field experts in 2006, summarises the major advancements in this area[**?**]. In this report we present the generalised form of Burgess' Lemma 2 which from now we will call as *Theorem 1* for convenience. Using which we can have a shorter proof for the deterministic bounds of polynomial factoring. 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 field $\mathbb{F}$.
- 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 $\max\{\alpha+\beta : x^{\alpha}y^{\beta}$ is monomial term of f(x,y) without coefficient$\}$.
- Similarly we denote degree of $f(x, y) \in \mathbb{F}[x, y]$ with respect to x by $deg_x f$ i.e. degree of f with y treated as constant.
- 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. Clearly $Res_x(f, g) = R(y)$ for some $R(y) \in \mathbb{F}[y]$.

3. Preliminaries

Following is a 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 $deg(f) * deg(g)$.
- *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.
- *Fact 3:* If $f(x)$ is a square free, monic, completely factorisable polynomial (in $\mathbb{Z}_p$) with integral coefficients. Then
$$\sum_{x\in\mathbb{Z}_p} \chi(f(x)) \leq (deg(f) - 1)p^{\frac{1}{2}}.$$

- *Fact 4:* $\chi_p(a^k) = \chi_p(a)^k = \chi_p(a)$ if k is odd else 1.

4. Theorem 1

Define sets $\mathcal{A}$ and $\mathcal{K}$ as follows:

$$\mathcal{A} = \{a_i : i \in [n] \text{ for some fixed } n\}$$
$$\mathcal{K} = \{2^i : i \in [Ord_p(2) - 1]\}$$

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[]. It states:

> *Given a prime p, let $\mathcal{H}$ be any set $\subset \mathbb{Z}_p$ whose cardinality is h (from henceforth h will represent the cardinality of $\mathcal{H}$), also let $\phi(x) = \prod_{a_i \in \mathcal{A}} (x + a_i)$. Define the quantity $S_{\mathcal{H}}(x)$ for a 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 the following lemmas.

Lemma 1. *: Let $f(x)$ be a polynomial in the polynomial ring $\mathbb{F}_p[x]$ over $\mathbb{F}_p$. Then if*

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

is 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 all a_j, $g(x + a_j)$ 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 $\prod_{a_j=a_i} f(x+2a_i)$ 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 $deg(\theta(y)) \le d^2$ 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 $deg(R(y)) \le d^2$. 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 $\theta(y) = R(y)$. We are done.

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

Lemma 3. *: Chose some arbitrary $\epsilon > 0$, then almost for all p,*

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

Proof: Let $\mathcal{P}(x) = \{p : p < x \ \& \ Ord_p(2) < p^{\frac{1}{2}-\epsilon}\}$. Hence for any $p \in \mathcal{P}(x)$ $\exists$ a number $\delta < p^{\frac{1}{2}-\epsilon}$ such that

$$p|(2^\delta - 1)$$

There can be at most $x^{\frac{1}{2}-\epsilon}$ such δ. Hence by Pigeon Hole Principle we know that

$$\exists\ \delta' < x^{\frac{1}{2}-\epsilon}$$

such that at least

$$\frac{|\mathcal{P}(x)|}{x^{\frac{1}{2}-\epsilon}}$$

primes divide $2^{\delta'} - 1$. We now use the following fact that number of prime divisors of an integer k is less that $\frac{log(k)}{log(log(k))}$. Hence clearly

$$\frac{|\mathcal{P}(x)|}{x^{\frac{1}{2}-\epsilon}} < \frac{log(2^{\delta'}-1)}{log(log(2^{\delta'}-1)} = \frac{\delta'}{log(\delta')} < x^{\frac{1}{2}-\epsilon}$$

(2)

This implies $\mathcal{P}(x) < x^{1-2\epsilon}$. Clearly $\lim_{x\to\infty} \frac{|\mathcal{P}(x)|}{\pi(x)} = 0$ where $\pi(x)$ is the prime counting function.

Lemma 4. *: $\psi(x,y) \in \mathbb{F}[x,y]$, 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 $\{\beta_1, \beta_2 \dots, \beta_l\} \subset \mathbb{F}_s$. *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 each of $f(x+ya_i)$, $a_i \in \mathcal{A}$ 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 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 $j = a_m$. But this is leads to contradiction. Hence the lemma follows.

Proof of theorem 1: Using combinatorial arguments we have

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

(3)

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

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

(4)

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 for all k in $\mathbb{Z}_p$. 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. Now number of cases when this happens is bounded by $(2rh)^r$ and for each of those cases the inner most sum

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

(5)

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 dont 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 $\prod\limits_{a_i \in \mathcal{A}} \chi f(x+a_i) = \prod\limits_{a_i \in \mathcal{A}} \chi f'(x+a_i)$ 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 $a_i + a_j$. 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 $\prod\limits_{a_i \in \mathcal{A}} f(x+a_i)$ becomes a perfect square then clearly $\prod\limits_{a_i \in \mathcal{A}} f'(x+a_i)$ 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

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

which implies

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

. If we chose p to be sufficiently large then we cannot have $\prod\limits_{a_i \in \mathcal{A}} f'(x+a_i)$ 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 $\prod\limits_{a_i \in \mathcal{A}} f(x+a_i)$ 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 $\prod\limits_{a_i \in \mathcal{A}} \prod\limits_{b_j}(x+b_j+a_i)$ and using the form of $\prod\limits_{a_i \in \mathcal{A}} f(x+a_i)$, 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, as for a given sequence of b_i's they can at most be nr extra counting. Now let

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

(6)

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

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

(7)

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. Also if we look at the requirement of largeness of p for which this Theorem 1 will hold. We find that even for $|\mathcal{A}| = 3$ and $r = 100$, p needs to be greater than 2^3600. But if we use lemma 3 then we find that almost for all p we have 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.

References

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

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

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

[4] 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.

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

[6] 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.

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