Deriving Burgess's Bound on the Distribution of Quadratic and Higher Non-Residues

Sabreen Syed

*Department of Computer Science and
Engineering
Indian Institute of Technology Kanpur, India*

February 2018

Chapter 1

Introduction

Chapter 2

Qualitative Analysis

The starting point for our analysis is Lemma 1 derived from Weil's theorem, which is an important result exhibiting the low correlation between the distribution of values a square-free polynomial takes in $\mathbb{F}_p$, and the distribution of quadratic residues.

Lemma 1. *[1]Let $f(x)$ be a monic square-free polynomial, with coefficients from $\mathbb{Z}$, reducible into linear factors with degree ν. Then,*

$$\left| \sum_{x=0}^{p-1} \chi_2(f(x)) \right| \leqslant (\nu - 1)p^{1/2}$$

The sum of χ_2 values in an interval determines the general density of quadratic residues and non-residues in it. The sum would cancel out to small magnitudes if the densities were nearly equal, or be closer in magnitude to the size of the interval if not. Thus, lemma 1 essentially tells us that a square free polynomial over $\mathbb{F}_p$ would evaluate to roughly equal number of quadratic residues and non-residues over $\mathbb{F}_p$. We deduce lemma 2 in the next section by constructing an appropriate polynomial exploiting lemma 1 for our purpose of finding low bounds on the number of continuous quadratic residues or continuous non-residues.

2.1 A useful global sum and the $O(p^{1/2})$ bound

Let us consider the sum of χ_2 values in an interval of size h.

$$S_h(x) = \sum_{n=0}^{h-1} \chi_2(x + n)$$

Given Lemma 1, which sums χ_2 values of a polynomial over the entire interval 0 to $p - 1$, we would like to construct a square-free polynomial which would

help put a limit on the sum of χ_2 values in any interval of size h. We do this by expanding the sum $\sum\limits_{x=0}^{p-1}(S_h(x))^{2r}$:

$$(S_h(x))^{2r} = \left(\sum_{n=0}^{h-1}\chi_2(x+n)\right)^{2r} = \sum_{m_1=1}^{h}\sum_{m_2=1}^{h}...\sum_{m_{2r}=1}^{h}\chi_2(x+m_1)\chi_2(x+m_2)...\chi_2(x+m_{2r})$$

$$\sum_{x=0}^{p-1}(S_h(x))^{2r} = \sum_{x=0}^{p-1}\sum_{m_1=1}^{h}\sum_{m_2=1}^{h}...\sum_{m_{2r}=1}^{h}\chi_2(x+m_1)\chi_2(x+m_2)..\chi_2(x+m_{2r})$$

$$\sum_{x=0}^{p-1}(S_h(x))^{2r} = \sum_{m_1=1}^{h}\sum_{m_2=1}^{h}...\sum_{m_{2r}=1}^{h}\sum_{x=0}^{p-1}\chi_2\big((x+m_1)(x+m_2)..(x+m_{2r})\big) \quad (2.1)$$

To use lemma 1, we need to separate the perfect square polynomials forming the sum from the rest. To achieve this, we separate the ordered sequences or 'tuples' in (2.1), $(m_1, m_2...m_{2r})$, into two sets based on the multiplicity of distinct values in the tuple:

- Set 1: Those tuples which contain an even count of each number in them. This set forms a bijection with every perfect square polynomial contributing. Since there are $\frac{(2r)!}{r!}$ ways to choose pairs of positions in a tuple and there are h^r ways of filling them with values from 1 to h, so there are less than $(2r)^r h^r$ such polynomials. Since the maximum value contributed to the sum of χ_2 values from each such polynomial is at most 1, the contribution to the sum over all p values of x is at most $(2r)^r h^r p$.

- Set 2: The rest of the tuples, which similarly correspond to the leftover polynomials exactly. Since there are h^{2r} polynomials in all, trivially at most h^{2r} are not perfect square polynomials. These polynomials are of the form:
$$(x + s_1)^{e_1}(x + s_2)^{o_2}...(x + s_k)^{e_k}$$

Where $s_i, i \in 1...k$ are distinct members of the tuple corresponding to the polynomial and e_i and o_i are even or odd powers respectively of the ith term. Now, $\chi\big((x+s_1)^{e_1}(x+s_2)^{o_2}...(x+s_k)^{e_k}\big)$ evaluates the same as $\chi\big((x+s_2)^{o_2}...(x+s_{k'})^{o_{k'}}\big)$ (taking all odd-powered factors) for all except at most r values of x (corresponding to the even-powered factors evaluating to 0). Thus, their contribution to the sum is not more than $h^{2r}(p^{1/2}(2r-1)+r)$.

We state lemma 2, which directly follows from what we have calculated so far.

Lemma 2. *Let* $S_h(x) = \sum\limits_{n=1}^{h}\chi_2(x+n)$. *Then,*

$$\sum_{x=0}^{p-1}(S_h(x))^{2r} \leqslant h^r(2r)^r p + h^{2r}r(2p^{1/2}+1) \qquad (2.2)$$

3

The $O(p^{1/2})$ bound

To prove the $O(p^{1/2})$ bound on the longest interval of continuous quadratic residues or of quadratic non-residues, we show that if the $O(p^{1/2})$ bound is not true, then LHS of (2.2) grows faster with p than the RHS, creating a contradiction.

Let the longest interval of quadratic residues or of quadratic non-residues be given by h for a given p. Thus, $|S_h(z)| = h$ for some $z \in \mathbb{F}_p$. Consider the LHS of (2.2) in that case. As $|S_h(x + k)| \geqslant |S_h(x)| - 2k$,

$$\sum_{x=0}^{p-1} |S_h(x)|^{2r} \geqslant \sum_{x=z}^{z+\lfloor h/4 \rfloor} |S_h(x)|^{2r} \geqslant h^{2r} + (h-2)^{2r} + ... + (h - 2\lfloor h/4 \rfloor)^{2r} \geqslant \frac{h^{2r+1}}{2^{2r+2}}$$

$$(2.3)$$

Thus, we can say from (2.2) and (2.3):

$$\frac{h^{2r+1}}{2^{2r+2}} \leqslant h^r (2r)^r p + h^{2r} r (2p^{1/2} + 1)$$

Now we set $r = 1$ and divide both sides by h^{2r}. We get:

$$\frac{h}{2^4} \leqslant 2h^{-1} p + (2p^{1/2} + 1) \qquad (2.4)$$

which has a disparity in the growth of the LHS and the RHS with respect to the inequality. This manifests itself for $h > 33p^{1/2}$: the LHS of (2.4) then is greater than $(2 + \frac{1}{16})p^{1/2}$, but the RHS is bounded above by $(2 + \frac{2}{33})p^{1/2} + 1$, which is less than the lower limit of the LHS for large enough p. Hence, $h \leqslant 33p^{1/2}$ for large enough p, and thus $h \in O(p^{1/2})$.

2.2   The amplification of an interval

We saw in the previous section how we split an interval in $\mathbb{F}_p$ of size $O(p^{1/2})$ into smaller sliding intervals and used lemma 2 to obtain the bound. What we do in this section is one step further: we show that an interval is equivalent to several small intervals in terms of the number of quadratic residues and non-residues in it. This would be useful to further amplify the contribution of an interval when applying lemma 2.

We construct small intervals by multiplying an interval $N, N + 1, ... N + H$ by q^{-1}, resulting in the elements $Nq^{-1}...(N + H)q^{-1}$ of $\mathbb{F}_p$. Take a general resulting element:

$$(N + k)q^{-1} = (N + nq + r)q^{-1} = Nq^{-1} + rq^{-1} + n$$

where $k = nq + r$ and $0 \leqslant r < q$ in $\mathbb{Z}$

There are q values of $Nq^{-1} + rq^{-1}$, one for each r. To each $Nq^{-1} + rq^{-1}$, we add consecutive values of n starting from 0 to $\lfloor H - r \rfloor / q$ to obtain each resulting element of $\{Nq^{-1}...(N + H)q^{-1}\}$, which results in q small intervals. These

4

intervals are disjoint because distinct $(N + k)$ result in different values of $(N + k)q^{-1}$. Now, how do we arithmetically calculate the exact values of an interval $(N + r)q^{-1}, (N + r)q^{-1} + 1, ...(N + r)q^{-1} + \lfloor H - r / q \rfloor$? Since we are dealing with elements in $\mathbb{F}_p$, $N + r \equiv N + r + tp (mod\ p), t \in \mathbb{Z}$. For exactly one $t \in \{0, 1, q-1\}$ for each r, $N + r + tp\ |\ q$, which makes $(N+r+tp)/q$ an integer. Thus the intervals translate to integers between $(N+r+tp)/q$ and $(N+r+tp+H-r)/q$ for each value of r with the corresponding value of t which makes $N + r + tp\ |\ q$, i.e. integers between $N+tp/q$ and $(N+tp+H)/q$ for all $t \in \{0, 1, ...q - 1\}$.

The small intervals constructed are equivalent due the fact that multiplying the interval by q^{-1}, preserves or swaps the original cardinality of quadratic residues and non-residues, since $\chi_2((N + k)q^{-1}) = \chi_2(q^{-1})\chi_2(N + k)$, and $\chi_2(q^{-1})$ is a constant. We now prove an important lemma which solidifies the effect of the amplification.

Lemma 3. *[1]Given a set of Q distinct natural numbers, whose general member is given by q, which are pairwise co-prime to each other, and any natural numbers N and H such that:*

$$2Hq < p \tag{2.5}$$

Let us denote by $I(q, t)$ the real interval

$$\frac{N + tp}{q} \leqslant z \leqslant \frac{N + H + tp}{q}$$

Then it is possible to associate with each q a set $T(q) \subseteq \{0, 1, \ldots q - 1\}$ of size at least $q - Q$, such that $\forall q \forall t \in T(q)$, $I(q, t)$ are disjoint.

Proof. For a given q, say q_o, consecutive $I(q_o, t)$ differ by p/q_o in their starting points, and have a width of H/q_o. Since $H < p$, $I(q_o, t)$ are disjoint. The $I(q_o, t)$ are in fact very narrow compared to the difference between their starting points, by a factor of less than $1/2q_o$. We can thus consider the gaps between interval starting points as equal-width 'blocks' of size p/q_o, with the intervals as fringes of width H/q_o. We make the following claim about two sets of blocks:

Claim. *Let r and s be two co-prime numbers. From a point, say y, on the real line, lay blocks of size r in the positive direction of the real axis to create points spaced by a gap of r. Similarly, from y, lay blocks of size s in the positive direction. Then the first points which coincide are after s blocks of size r and r blocks of size s.*

Proof: Since, r and s are co-prime, $gcd(r, s) = rs$. If, for the sake of contradiction, say $u < s$ blocks of size r was the first coinciding point, then $ur\ |\ s \Rightarrow gcd(r, s) \leqslant ur < rs$, which is a contradiction. ◇

Now take two values of q, q_1 and q_2, and without loss of generality assume $q_1 < q_2$,. The gap between intervals given by $I(q_1, t)$ for consecutive values of t is p/q_1, while the gap between intervals given by $I(q_2, t)$ for consecutive values of t is p/q_2. Let us scale the real line by multiplying it by $q_1 q_2/p$. The resulting gap blocks on this are then q_2 and q_1 respectively. Thus the point

they first coincide are after q_1 blocks of $I(q_1, t)$ and q_2 blocks of $I(q_2, t)$. Thus in the unscaled real line, the unit blocks become of size $p/q_1 q_2$ and the first point which coincides is after a length of p. Since the overlapping region of $[N/q_1, N+pq_1/q_1)$ and $[N/q_2, N+pq_2/q_2)$ is not greater than p, there is only one point which coincides. With the fringes (actual intervals) of maximum width H/q_1 lesser than the least possible seperation between intervals $p/q_1 q_2$, the fringes cannot intersect anywhere else as well.

Hence, for each q, there are at least $q - Q$ values of $t \in \{0, 1, \ldots q - 1\}$ such that $I(q, t)$ are disjoint from all other intervals associated with all q.

$\square$

We now proceed to prove the $O(p^{1/4+\delta})$ bound on the least quadratic residue.

2.3 The $p^{1/4+\delta}$ bound

We will prove the bound on the least quadratic non-residue by means of contradiction. Say $H > p^{1/4+\delta}$ for some $\delta > 0$, and $\left| \sum\limits_{x=N+1}^{N+H} \chi_p(x) \right| = H$. We know that for $H > cp^{1/2}$, where c is some constant, there can be no interval of all quadratic residues or all non-residues. Thus, we assume $H \leqslant cp^{1/2}$

We take the pair-wise co-prime numbers q required for the application of lemma 3 to be the primes in the range:

$$\frac{p^{1/4}}{2} \leqslant q \leqslant p^{1/4}$$

This satisfies the constraint in (2.5) for large enough p. The number of primes q is given by $Q = \pi(p^{1/4}) - \pi(\frac{p^{1/4}}{2}) = o(p^{1/4})$ by the prime number theorem. Now, restating the assumption:

$$\left| \sum_{x=N+1}^{N+H} \chi_p(x) \right| = H$$

We proceed to transform this interval into several smaller intervals as discussed in the previous section. For a fixed x, $x + tp$ is divisible by q for exactly one value of $t \in \{0, 1, \ldots q - 1\}$. Also $\chi(x + tp) = \chi(x)$. Thus:

$$\left| \sum_{x=N+1}^{N+H} \chi_p(x) \right| = \left| \sum_{t=0}^{t=q-1} \sum_{\substack{x=N+1 \\ x+tp \mid q}}^{N+H} \chi_p(x + tp) \right| = H$$

Since $x + tp \mid q$, thus $x + tp = qz$ for some $z \in \mathbb{Z}$, $\Rightarrow z = \frac{x+tp}{q}$.
For $N + 1 \leqslant x \leqslant N + H$, we see that all such z are the integer values in $I(q, t)$ according to lemma 3 for the corresponding values of t such that $x + tp \mid q$.

$$\left| \sum_{t=0}^{t=q-1} \sum_{\substack{x=N+1 \\ x+tp \mid q}}^{N+H} \chi_p\left(\frac{x + tp}{q}.q\right) \right| = H$$

6

$$\left| \sum_{t=0}^{t=q-1} \sum_{z \in I(q,t)} \chi_p(z.q) \right| = H$$

$$\left| \sum_{t=0}^{t=q-1} \sum_{z \in I(q,t)} \chi_p(z)\chi_p(q) \right| = H$$

$$\sum_{t=0}^{t=q-1} \left| \sum_{z \in I(q,t)} \chi_p(z)\chi_p(q) \right| \geqslant H$$

$$\sum_q \sum_{t=0}^{t=q-1} \left| \chi_p(q) \sum_{z \in I(q,t)} \chi_p(z) \right| \geqslant HQ$$

$$\sum_q \left| \chi_p(q) \right| \sum_{t=0}^{t=q-1} \left| \sum_{z \in I(q,t)} \chi_p(z) \right| \geqslant HQ$$

$$\sum_q \sum_{t=0}^{t=q-1} \left| \sum_{z \in I(q,t)} \chi_p(z) \right| \geqslant HQ$$

Seperating the possibly overlapping intervals from the disjoint intervals:

$$\sum_q \sum_{t \in T(q)} \left| \sum_{z \in I(q,t)} \chi_p(z) \right| + \sum_q \sum_{\substack{t=0 \\ t \notin T(q)}}^{q-1} \left| \sum_{z \in I(q,t)} \chi_p(z) \right| \geqslant HQ \qquad (2.6)$$

Now,

$$\sum_q \sum_{\substack{t=0 \\ t \notin T(q)}}^{q-1} \left| \sum_{z \in I(q,t)} \chi_p(z) \right| \leqslant \sum_q Q \left\lceil \frac{H}{q} \right\rceil \leqslant \sum_q Q \frac{2H}{q} < 4Q^2 H p^{-1/4} \qquad (2.7)$$

since $\sum_q q^{-1} < Q.\left(\frac{p^{1/4}}{2}\right)^{-1}$. Using 2.6 and 2.7,

$$\sum_q \sum_{t \in T(q)} \left| \sum_{z \in I(q,t)} \chi_p(z) \right| > HQ - 4Q^2 H p^{1/4} = HQ(1 - 4Qp^{-1/4}) > \frac{HQ}{2}$$

$$\sum_{m=0}^{h-1} \sum_q \sum_{t \in T(q)} \left| \sum_{z \in I(q,t)} \chi_p(z) \right| = h \sum_q \sum_{t \in T(q)} \left| \sum_{z \in I(q,t)} \chi_p(z) \right| > \frac{HhQ}{2} \qquad (2.8)$$

for large enough p, since $Q = o(p^{1/4})$. Now we would like to use the contribution of the disjoint intervals in 2.8 in applying lemma 2, by considering sliding window sums of size h. For this, we calculate an estimate of the sum obtained for one interval:

$$\sum_{z \in I(q,t)} \chi_p(z+m) \geqslant \sum_{z \in I(q,t)} \chi_p(z) - 2m$$

7

$$\sum_{m=0}^{h-1} \sum_{z \in I(q,t)} \chi_p(z+m) \geqslant \sum_{m=0}^{h-1} \sum_{z \in I(q,t)} \chi_p(z) - 2 \sum_{m=0}^{h-1} m$$

$$\sum_{z \in I(q,t)} \sum_{m=0}^{h-1} \chi_p(z+m) \geqslant h \sum_{z \in I(q,t)} \chi_p(z) - h^2$$

$$\left| \sum_{z \in I(q,t)} \sum_{m=0}^{h-1} \chi_p(z+m) \right| \geqslant \left| h \sum_{z \in I(q,t)} \chi_p(z) - h^2 \right|$$

$$\sum_{z \in I(q,t)} \left| \sum_{m=0}^{h-1} \chi_p(z+m) \right| \geqslant h \left| \sum_{z \in I(q,t)} \chi_p(z) \right| - h^2$$

$$\sum_{q} \sum_{t \in T(q)} \sum_{z \in I(q,t)} \left| \sum_{m=0}^{h-1} \chi_p(z+m) \right| \geqslant h \sum_{q} \sum_{t \in T(q)} \left| \sum_{z \in I(q,t)} \chi_p(z) \right| - Qp^{1/4}h^2$$

since the number of the intervals given by lemma 3, $I(q,t)$, are less than $Qp^{1/4}$.
So from (2.8)

$$\sum_{q} \sum_{t \in T(q)} \sum_{z \in I(q,t)} \left| \sum_{m=0}^{h-1} \chi_p(z+m) \right| > \frac{HhQ}{2} - Qp^{1/4}h^2 = Qh\left(\frac{H}{2} - hp^{1/4}\right)$$

Taking $h < \frac{1}{4}p^{-1/4}H$, and using the terminology from lemma 2,

$$\sum_{q} \sum_{t \in T(q)} \sum_{z \in I(q,t)} |S_h(z)| > \frac{HhQ}{4}$$

Using Holder's inequality,

$$\sum_{q} \sum_{t \in T(q)} \sum_{z \in I(q,t)} |S_h(z)| \leqslant \left(\sum_{q} \sum_{t \in T(q)} \sum_{z \in I(q,t)} |S_h(z)|^{2r} \right)^{1/2r} \left(\sum_{q} \sum_{t \in T(q)} \sum_{z \in I(q,t)} 1 \right)^{1-1/2r}$$

$$\sum_{q} \sum_{t \in T(q)} \sum_{z \in I(q,t)} |S_h(z)|^{2r} \geqslant \left(\sum_{q} \sum_{t \in T(q)} \sum_{z \in I(q,t)} |S_h(z)| \right)^{2r} \left(\sum_{q} \sum_{t \in T(q)} \sum_{z \in I(q,t)} 1 \right)^{-(2r-1)}$$

$$\sum_{q} \sum_{t \in T(q)} \sum_{z \in I(q,t)} |S_h(z)|^{2r} > \left(\frac{HhQ}{4} \right)^{2r} \left(Qp^{1/4}.2.\frac{H}{p^{1/4}} \right)^{-(2r-1)}$$

$$\sum_{z=0}^{p-1} |S_h(z)|^{2r} > \left(\frac{1}{8} \right)^{2r} HQh^{2r}$$

From lemma 2,

$$(2r)^r h^r p + h^{2r} r(2p^{1/2}+1) > \left(\frac{1}{8} \right)^{2r} HQh^{2r}$$

For large enough p, the second term of the LHS diminishes compared to the RHS as $HQ \geqslant \frac{p^{1/2+\delta}}{4\log p}$. Now, we take $h = \lfloor \frac{1}{5}p^{-1/4}H \rfloor$. Since $h \geqslant \frac{1}{5}p^\delta$, we take $r > \delta^{-1}$, which results in the first term of the LHS diminishing with respect to the RHS. Thus, we have arrived at a contradiction. Our assumption that $\left| \sum_{x=N+1}^{N+H} \chi_p(x) \right| = H$ was wrong, hence the first quadratic non-residue is less than $p^{1/4+\delta}$ for any $\delta > 0$.

2.4 Extension to general characters

Now we consider a natural extension of what we have proven so far: extending the result to general characters. Although a more general form of lemma 1 for general characters exists, a possible impediment in reapplying the former proof technique is dealing with the complex numbers involved in general characters. But as it turns out, we can easily extend the previously used techniques and theorems in the complex domain to obtain the same results for a general character.

The generalised form of lemma 1 for any character is:

Lemma 4. *[6]Let χ be a non-trivial character of order d. Let $f(x)$ be a polynomial which is not a perfect d^{th} power, with coefficients from $\mathbb{Z}$. Let $f(x)$ have ν distinct zeroes. Then,*

$$\left| \sum_{x=0}^{p-1} \chi(f(x)) \right| \leqslant (\nu - 1)p^{1/2}$$

We henceforth assume $d \mid p-1$, because since $\chi^d(x) = 1$ and $\chi(x^{p-1}) = \chi^{p-1}(x) = 1$ for $x \neq 0$, $\chi^{gcd(d,p-1)}(x) = 1$ for $x = \neq 0$, and hence any character of order d is also a character of order $gcd(d, p-1)$, and hence we consider $gcd(d, p-1)$ as the character order. We now use lemma 4 to derive an equivalent form of lemma 2. Again, we define

$$S_h(x) = \sum_{n=0}^{h-1} \chi(x+n)$$

We then expand the sum $|S_h(x)|^{2r}$:

$$|S_h(x)|^{2r} = \left| \sum_{n=0}^{h-1} \chi(x+n) \right|^{2r} = \left(\sum_{n=0}^{h-1} \chi(x+n) \right)^r \left(\overline{\sum_{n=0}^{h-1} \chi(x+n)} \right)^r$$

$$|S_h(x)|^{2r} = \left(\sum_{m_1=1}^{h} \sum_{m_2=1}^{h} ... \sum_{m_r=1}^{h} \chi(x+m_1)\chi(x+m_2)...\chi(x+m_r) \right)$$
$$\left(\sum_{m_{r+1}=1}^{h} \sum_{m_{r+2}=1}^{h} ... \sum_{m_{2r}=1}^{h} \overline{\chi(x+m_{r+1})\chi(x+m_{r+2})...\chi(x+m_{2r})} \right)$$

$$|S_h(x)|^{2r} = \left(\sum_{m_1=1}^{h} \sum_{m_2=1}^{h} ... \sum_{m_r=1}^{h} \chi\big((x + m_1)(x + m_2)...(x + m_r)\big) \right)$$

$$\left(\sum_{m_{r+1}=1}^{h} \sum_{m_{r+2}=1}^{h} ... \sum_{m_{2r}=1}^{h} \overline{\chi}\big((x + m_{r+1})(x + m_{r+2})...(x + m_{2r})\big) \right)$$

Using the property of a character that $\overline{\chi}(x) = \chi(x^{-1})$ for $x \neq 0$:

$$|S_h(x)|^{2r} = \left(\sum_{m_1=1}^{h} \sum_{m_2=1}^{h} ... \sum_{m_r=1}^{h} \chi\big((x + m_1)(x + m_2)...(x + m_r)\big) \right)$$

$$\left(\sum_{m_{r+1}=1}^{h} \sum_{m_{r+2}=1}^{h} ... \sum_{m_{2r}=1}^{h} \chi\big((x + m_{r+1})^{p-2}(x + m_{r+2})^{p-2}...(x + m_{2r})^{p-2}\big) \right)$$

$$= \sum_{m_1=1}^{h} \sum_{m_2=1}^{h} ... \sum_{m_{2r}=1}^{h} \chi\big((x+m_1)(x+m_2)...(x+m_r)(x+m_{r+1})^{p-2}(x+m_{r+2})^{p-2}...(x+m_{2r})^{p-2}\big)$$

$$\sum_{x=0}^{p-1} |S_h(x)|^{2r} = \sum_{m_1=1}^{h} \sum_{m_2=1}^{h} ... \sum_{m_{2r}=1}^{h} \sum_{x=0}^{p-1} \chi\Big(\prod_{i=1}^{r}(x + m_i) \prod_{i=r+1}^{2r}(x + m_i)^{p-2} \Big) \quad (2.9)$$

In equation 2.9, we must seperate the perfect d^{th} power polynomials from the rest. We do this, again as in the case of quadratic character, by examining the tuples formed by $(m_1, m_2...m_{2r})$. Now since $d \mid p-1 \Rightarrow \gcd(d, p-2) = 1$, no less than a power of d of $(x+m)^{p-2}$ will form a perfect d^{th} power. Thus a tuple represents a a perfect d^{th} power polynomial if each element occuring in $m_1, m_2...m_r$ is paired with an occurence of the same element in $m_{r+1}, m_{r+2}...m_{2r}$, and the rest of the occurences of elements in $m_1, m_2...m_r$ are in a multiple of d, as well the rest of the occurences of elements in $m_{r+1}, m_{r+2}...m_{2r}$ are in a multiple of d. Thus the total number of such polynomials is:

$$\sum_{k=1}^{\lfloor r/d \rfloor} \left(\frac{\binom{r}{d}\binom{r-d}{d}...\binom{r-(k-1)d}{d}}{k!} \right)^2 \frac{\binom{r-kd}{1}^2 \binom{r-kd-1}{1}^2 ... \binom{1}{1}^2}{(r - kd)!} h^{2k+r-kd}$$

$$\leqslant (r!)^2 h^r \sum_{k=1}^{\lfloor r/d \rfloor} \max_k \frac{1}{(d!)^{2k}(r - kd)!(k!)^2} \leqslant \frac{r}{d} \cdot (r!)^2 h^r \leqslant r^{2r} h^r$$

Thus, these polynomials contribute at most $r^{2r} h^r p$ to the sum in 2.9. The total no. of the rest of the polynomials is trivially at most h^{2r}. Thus, these contribute at most $h^{2r}(2r - 1)p^{1/2}$. Hence, we arrive at the following lemma:

Lemma 5. *Let $S_h(x) = \sum_{n=1}^{h} \chi(x + n)$. Then,*

$$\sum_{x=0}^{p-1} |S_h(x)|^{2r} \leqslant h^r(2r)^r p + 2h^{2r} r p^{1/2} \quad (2.10)$$

10

Chapter 3

Quantitative Analysis

Bibliography

[1] D. A. Burgess, *The distribution of quadratic residues and non-residues*, Mathematika 4 (1957), 106-112.

[2] David M. Burton, *Elementary Number Theory*, McGraw Hill, 2012.

[3] S. Lindhurst, *An analysis of Shanks's algorithm for computing square roots in finite fields*, CRM Proceedings and Lecture Notes, Vol. 19 (1999) pp. 231–242.

[4] G. Polya, *"Über die Verteilung der quadratischen Eeste und Nichtreste"*, Göttinger Nachrichten (1918), 21-29.

[5] I. M. Vinogradov, *"Sur la distribution des résidus et des non-résidus des puissances "*, Journal Physico-Math. Soc. Univ. Perm, No. 1 (1918), 94-96.

[6] W. Schmidt, *"Equations over finite fields, An elementary approach"*, Lecture Notes in Math. 536, Springer Verlag, 1976, p. 43