

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

1.1 Symbols and conventions

1.2 Preliminaries

1.3 Interval sums of quadratic residues

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,*

$$\sum_{x=0}^{p-1} \chi_2(f(x)) \leq (\nu - 1)p^{1/2}$$

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 $\sum_{x=0}^{p-1} (S_h(x))^{2r}$:

$$\begin{aligned}
(S_h(x))^{2r} &= \left(\sum_{n=0}^{h-1} \chi_2(x+n) \right)^{2r} = \sum_{m_1=1}^h \sum_{m_2=1}^h \dots \sum_{m_{2r}=1}^h \chi_2(x+m_1) \chi_2(x+m_2) \dots \chi_2(x+m_{2r}) \\
\sum_{x=0}^{p-1} (S_h(x))^{2r} &= \sum_{x=0}^{p-1} \sum_{m_1=1}^h \sum_{m_2=1}^h \dots \sum_{m_{2r}=1}^h \chi_2(x+m_1) \chi_2(x+m_2) \dots \chi_2(x+m_{2r}) \\
\sum_{x=0}^{p-1} (S_h(x))^{2r} &= \sum_{m_1=1}^h \sum_{m_2=1}^h \dots \sum_{m_{2r}=1}^h \sum_{x=0}^{p-1} \chi_2((x+m_1)(x+m_2) \dots (x+m_{2r})) \quad (2.1)
\end{aligned}$$

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), $(m_1, m_2, \dots, m_{2r})$, 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 corresponding 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:

$$(x + s_1)^{e_1} (x + s_2)^{o_2} \dots (x + s_k)^{e_k}$$

Where $s_i, i \in 1 \dots k$ are distinct members of the tuple corresponding to the polynomial and e_i and o_i are even or odd powers respectively of the i^{th} term. Now, $\chi((x+s_1)^{e_1} (x+s_2)^{o_2} \dots (x+s_k)^{e_k})$ evaluates the same as $\chi((x+s_2)^{o_2} \dots (x+s_{k'})^{o_{k'}})$ (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 $S_h(x) = \sum_{n=1}^h \chi_2(x+n)$. Then,

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

2.1.1 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 $|S_h(x+k)| \geq |S_h(x)| - 2k$,

$$\sum_{x=0}^{p-1} (S_h(x))^{2r} \geq \sum_{x=z}^{z+\lfloor h/4 \rfloor} |S_h(x)|^{2r} \geq h^{2r} + (h-2)^{2r} + \dots + (h-2\lfloor h/4 \rfloor)^{2r} \geq \frac{h^{2r+1}}{2^{2r+2}} \quad (2.3)$$

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

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

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

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

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, $h \leq 33p^{1/2}$ 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 $N, N+1, \dots, N+H$ by q^{-1} , resulting in the elements $Nq^{-1}, \dots, (N+H)q^{-1}$ 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 $0 \leq r < q$ 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 $\frac{\lfloor H-r \rfloor}{q}$ to obtain each resulting

element of $Nq^{-1} \dots (N+H)q^{-1}$, which results in q small intervals. These intervals are disjoint because distinct $(N+k)$ result in different values of $(N+k)q^{-1}$.

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 theorem which solidifies the effect of the amplification.

Lemma 3. *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:*

$$2Hq < p \quad (2.5)$$

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

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

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

Proof:

For a fixed q , $I(q, t)$ are disjoint as $H < p$. Now, for a pair of different values of q , say q_1 and q_2 , let $I(q_1, t_1)$ and $I(q_2, t_2)$ intersect. Then we can say:

$$\begin{aligned} \frac{N+t_1p}{q_1} &\leq \frac{N+H+t_2p}{q_2} \\ \& \frac{N+t_2p}{q_2} &\leq \frac{N+H+t_1p}{q_1} \\ \Rightarrow N(q_2 - q_1) + (t_1q_2 - t_2q_1)p &\leq Hq_2 < \frac{1}{2}p \\ \Rightarrow N(q_1 - q_2) + (t_2q_1 - t_1q_2)p &\leq Hq_1 < \frac{1}{2}p \\ \Rightarrow N(q_2 - q_1) - \frac{1}{2}p < (t_2q_1 - t_1q_2)p < N(q_2 - q_1) + \frac{1}{2}p \end{aligned}$$

Since not more than a single multiple of p can occur in a range of size less than p , $t_2q_1 - t_1q_2$ can take only one value. Because q_1 and q_2 are co-prime and $0 \leq t_1 \leq q_1$ and $0 \leq t_2 \leq q_2$, there is only one pair of t_1 and t_2 values for a unique $t_2q_1 - t_1q_2$. This is because for a unique valuation of $t_2q_1 - t_1q_2$, the difference in the valuation of the first term must be same as that of the second term for different values of t_2 . The values of t_2q_1 will be multiples of q_1 , and for the difference in two such values to be the same as two values of t_1q_2 , a multiple of q_2 , the least possible difference can be the l.c.m q_1q_2 , which cannot occur from given range of t_1 and t_2 .

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

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
- 2.4** Extension to general characters
- 2.5** Extensions to quadratic functions
- 2.6** Problems with attempts at further generalisation

Chapter 3

Quantitative Analysis

3.1 Energy

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 Reste 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.