On Incomplete Distance Sets in $Z_p \times Z_p$

Adam Scrivener

April 2016

Let E be a subset of $\mathbb{Z}_p \times \mathbb{Z}_p$. Let $1_A(\cdot)$ be the indicator function of a set A. Then, define

$$\nu(t) = \sum_{x,y \in \mathbb{Z}_p^2} 1_E(x) 1_E(y) 1_{S_t}(x - y),$$

where

$$S_t = \{x \in \mathbb{Z}_p^2 : ||x|| = t\}.$$

Theorem 1. *If $|E| > 0$, $\nu(t) > 0$ for every $t \in \mathbb{Z}_p$.*

Proof. In order to prove this theorem, we begin with a couple of lemmas.

Lemma 1. *Suppose that $p \equiv 1 (mod\ 4)$. Then*

$$|S_t| = p - 1.$$

If $p \equiv 3 (mod\ 4)$, then

$$|S_t| = p + 1.$$

Lemma 2. *Suppose that $m = (0,0)$. Then*

$$|\widehat{1}_{S_t}(m)| \leq 2p^{-\frac{3}{2}}.$$

Theorem 2. *With the notation above,*

$$\left| \sum_{x=0} \chi\left(-st - \frac{||m||}{4s} \right) \psi^2(s) \right| \leq 2\sqrt{p}.$$

This gives us the bound

$$\left| \hat{1}_{S_t}(m) \right| = p^{-2} \left| \sum_{x=0} \chi\left(-st - \frac{||m||}{4s} \right) \psi^2(s) \right| \leq 2p^{-\frac{3}{2}},$$

thereby proving Lemma 2 and therefore Theorem 1. □

4 Computational Results

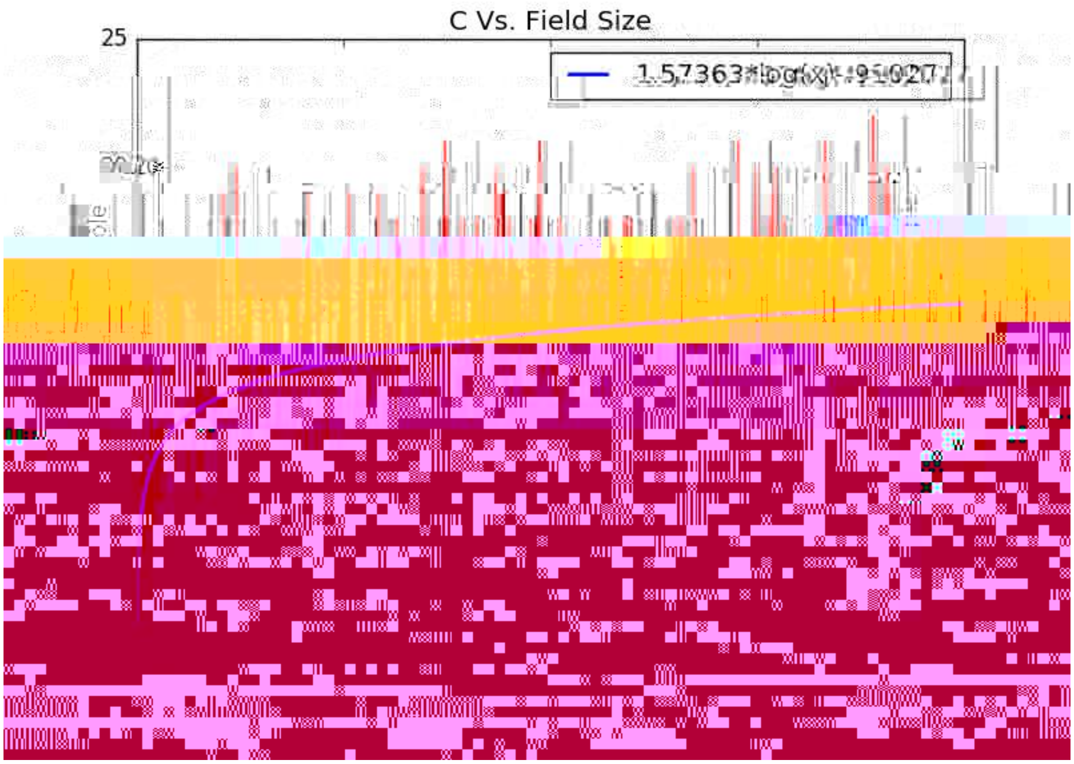
Whereas the aim of the last section was to give an upper bound on $S(p)$, the goal of the following sections is to find a large subset which has an incomplete distance set, thereby giving a lower bound on $S(p)$.

4.1 Brute force observations in $\mathbb{Z}_5$

Below is a visualization of $\mathbb{Z}_5 \times \mathbb{Z}_5$, with an example of a subset

$$E = \{(0,1), (1,1), (1,2), (2,3), (3,4), (4,4)\} :$$

–	–	–	X	X	
–	–	X	–	–	
–	X	–	–	–	
X	X	–	–	–	
–	–	–	–	–	–



This gives a strong indication that the largest number of adjacent lines with incomplete distance set grows with $\log(p)$. Note that this would be a lower bound on $S(p)$, since there could possibly be larger subsets with an incomplete distance set which are not adjacent vertical lines.

5 A Rephrasing in Terms of Quadratic Non-residues

It turns out that finding a lower bound on the largest number of adjacent lines

This follows since if x and y are two points in lines l_i, l_j, the horizontal distance between them is $(l_i - l_j)^2$, and thus their distance is contained in $A_{(l_i - l_j)}$. Further, if d

$\square$

Lemma 3. *If S is a set of*

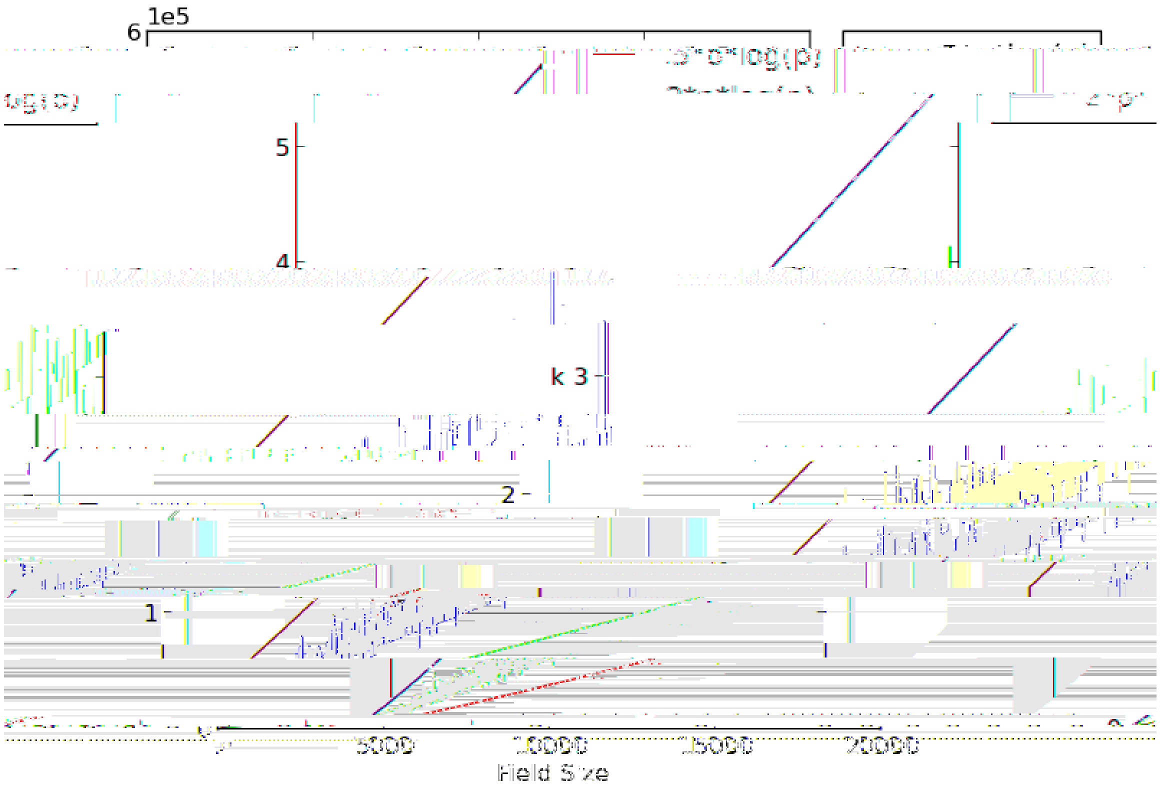


Figure 1: Size of largest set of adjacent lines with incomplete data set, k, plotted vs. p, the field size. Lower bound of $S(p)$ proven in this paper in blue, and a function which is $O(p\log_2(p))$ in green.