Asymptotic Size of a Kakeya Set Construction for $p \equiv 1 \pmod 4$

Abstract

We derive the asymptotic formula for the size of a specific four-dimensional Kakeya set construction over a finite field $\mathbb{F}_p$, where p is a prime satisfying $p \equiv 1 \pmod 4$. We prove that the size of the set, denoted $|K_4|$, is given by:

$$|K_4| = \frac{1}{8}p^4 + \frac{19}{32}p^3 - \frac{11}{16}p^2 + O(p^{1.5})$$

1 The Construction

Kakeya sets over finite fields are discrete analogues of the classical Kakeya problem and are a subject of considerable interest (AI generated reference [3, 4]). We define a Kakeya set via a recursive polynomial construction.

Let p be a prime. We define a sequence of sets $K_i \subseteq \mathbb{F}_p^i$ for $i = 1, 2, 3, 4$.

- **Base case ($i = 1$):** $K_1 = \mathbb{F}_p$. Its size is $|K_1| = p$.
- **Recursive Step ($i > 1$):** The set K_i is constructed from K_{i-1} as the union of two sets: $K_i = C_i \cup (K_{i-1} \times \{c_i\})$, where c_i is a constant in $\mathbb{F}_p$ and C_i is a "cone-like" set. The set C_i is defined as: $C_i = \{(y_1, \ldots, y_{i-1}, t) \in \mathbb{F}_p^i \mid t \in \mathbb{F}_p \text{ and } \forall j \in \{1, \ldots, i-1\}, y_j \in S_{i,t}\}$ where $S_{i,t} = \{P_i(t, m) \mid m \in \mathbb{F}_p\}$ for a given polynomial $P_i(t, m)$.

The specific parameters for this construction are:

1. **Step 2 (1D → 2D):** $P_2(t, m) = tm - m^2 + m$, and $c_2 = 0$.
2. **Step 3 (2D → 3D):** $P_3(t, m) = tm - m^2 + 1$, and $c_3 = 0$.
3. **Step 4 (3D → 4D):** $P_4(t, m) = tm - m^2$, and $c_4 = 0$.

2 The Exact Formula for $|K_4|$

For a prime $p \equiv 1 \pmod 4$, the exact size of the set K_4 is given by the following formula, which can be derived through detailed point-counting methods:

$$|K_4| = \frac{4p^4 + 19p^3 + 23p^2 - 39p - 7 + R(p)}{32} - \Delta_p$$

where:

- $R(p) = 16\chi(3) + 4A_p(p + 1)$.
- $\chi(3)$ is the Legendre symbol $(\frac{3}{p})$.

- The term A_p is an integer related to the representation of p as a sum of two squares. By Fermat's theorem on sums of two squares, a prime p can be written as $p = a^2 + b^2$ for integers a, b if and only if $p \equiv 1 \pmod 4$ (up to ordering and signs, this representation is unique). Here, we take the unique representation where a is odd and b is even. The coefficient A_p is then given by $A_p = \pm 2a$, with the sign chosen such that $a + b \equiv 1 \pmod 4$. This integer arises in the study of the number of points on elliptic curves over $\mathbb{F}_p$; specifically, A_p is the trace of Frobenius of the elliptic curve $y^2 = x^3 - x$ (AI generated reference [6, Ch. 18]).
- $\Delta_p = |X|^2 - |K_2 \cap X^2|$.
- $H = \{x^2 \mid x \in \mathbb{F}_p\}$ is the set of quadratic residues in $\mathbb{F}_p$, including 0.
- $X = H \cap (1 + H)$, where $1 + H = \{1 + h \mid h \in H\}$.
- $X^2 = X \times X$.
- K_2 is the set from the first step of the construction.

Our goal is to find the asymptotic behavior of this formula as $p \to \infty$.

3 Asymptotic Analysis

We analyze the asymptotic size of each component of the formula.

3.1 The Main Polynomial Term

The dominant term is the polynomial in p. Its asymptotic behavior is found by simple division:

$$\frac{4p^4 + 19p^3 + 23p^2 - 39p - 7}{32} = \frac{1}{8}p^4 + \frac{19}{32}p^3 + \frac{23}{32}p^2 + O(p)$$

3.2 The Remainder Term $R(p)$

The term $R(p) = 16\chi(3) + 4A_p(p + 1)$.

- The Legendre symbol $\chi(3)$ is either 1 or -1, so $16\chi(3)$ is $O(1)$.
- For the term A_p, since $p = a^2 + b^2$, we have $a^2 < p$, which implies $|a| < \sqrt{p}$. Therefore, by definition, $|A_p| = |\pm 2a| < 2\sqrt{p}$. This bound is a specific instance of the Hasse-Weil bound for elliptic curves (AI generated reference [6, Ch. V, Thm. 1.1]).
- The size of the term $4A_p(p + 1)$ is bounded: $|4A_p(p + 1)| < 4(2\sqrt{p})(p + 1) = 8p^{1.5} + 8p^{0.5}$.
- Thus, $R(p) = O(p^{1.5})$. When divided by 32, this term is still $O(p^{1.5})$ and will be absorbed into the final error term.

3.3 The Correction Term Δ_p

This is the most involved part of the analysis. We need the asymptotic size of $\Delta_p = |X|^2 - |K_2 \cap X^2|$.

A. Asymptotic Size of $|X|^2$

The size of the set $X = H \cap (1 + H)$ is the number of elements $y \in \mathbb{F}_p$ for which both y and $y - 1$ are quadratic residues. This quantity is given by the cyclotomic number $(0, 0)$ of order 2. For primes $p \equiv 1 \pmod 4$, a known result from the theory of cyclotomic numbers states that the size of this set is exactly (AI generated reference [7]):

$$|X| = \frac{p+3}{4}$$

Squaring this gives the asymptotic size of $|X|^2$:

$$|X|^2 = \left(\frac{p+3}{4}\right)^2 = \frac{p^2 + 6p + 9}{16} = \frac{1}{16}p^2 + O(p)$$

B. Asymptotic Size of $|K_2 \cap X^2|$

First, we characterize the set K_2. From the construction, $K_2 = C_2 \cup (K_1 \times \{0\})$.

- $K_1 \times \{0\} = \{(y, 0) \mid y \in \mathbb{F}_p\}$.
- $C_2 = \{(y, t) \mid t \in \mathbb{F}_p, y \in S_{2,t}\}$. The set $S_{2,t} = \{tm - m^2 + m \mid m \in \mathbb{F}_p\}$. A value y is in $S_{2,t}$ if the quadratic equation $m^2 - (t + 1)m + y = 0$ has a solution for $m \in \mathbb{F}_p$. This is true if and only if its discriminant, $D = (t+1)^2 - 4y$, is a quadratic residue (i.e., $D \in H$).

So, a point (y, t) is in K_2 if $t = 0$ or if $(t + 1)^2 - 4y \in H$.

We now count the number of points in the intersection $|K_2 \cap X^2|$. This is the number of pairs $(y, t) \in X \times X$ that also satisfy the condition for being in K_2. We split the count based on the value of t.

- **Case 1:** $t = 0$**.** We are counting points $(y, 0)$ where $y \in X$. The number of such points is simply $|X| = \frac{p+3}{4} = O(p)$.
- **Case 2:** $t \in X \setminus \{0\}$**.** We are counting pairs (y, t) where $t \in X \setminus \{0\}$, $y \in X$, and $(t + 1)^2 - 4y \in H$. For a fixed $t \in X \setminus \{0\}$, we need to count the number of $y \in X$ that also satisfy the condition $(t + 1)^2 - 4y \in H$. Recall that $y \in X$ means $y \in H$ and $y - 1 \in H^{-1} = 1 + H$. Let χ be the Legendre symbol. The number of solutions y can be expressed using character sums, a standard technique in such counting problems (AI generated reference [1]). The number of solutions N_t is given by:

  $$N_t = \sum_{y \in \mathbb{F}_p} \frac{1}{8}(1 + \chi(y))(1 + \chi(y - 1))(1 + \chi((t + 1)^2 - 4y))$$

  Expanding this sum leads to a main term of $p/8$ and several other character sums of the form $\sum_y \chi(f(y))$, where $f(y)$ is a polynomial. According to the celebrated Weil bound for character sums, if $f(y)$ is not of the form $c \cdot g(y)^2$ for some polynomial g, then $|\sum_y \chi(f(y))| \leq (\deg(f) - 1)\sqrt{p}$ (AI generated reference [8]).
  This implies the estimate $N_t = p/8 + O(\sqrt{p})$, which holds unless the polynomial under one of the character sums degenerates. This occurs for "exceptional" values of t where the product of the three arguments of χ has repeated roots. The roots are $y = 0, y = 1$, and $y = (t + 1)^2/4$. Coincidence occurs if:

  1. $(t + 1)^2/4 = 0 \implies t = -1$.
  2. $(t + 1)^2/4 = 1 \implies (t + 1)^2 = 4 \implies t = 1$ or $t = -3$.

  We handle these cases separately.

- **Generic t:** For the vast majority of t values ($|X| - O(1) = O(p)$ values), the estimate $N_t = p/8 + O(\sqrt{p})$ holds. The total contribution from these generic t is:

$$(|X| - O(1))\left(\frac{p}{8} + O(\sqrt{p})\right) = \left(\frac{p}{4} + O(1)\right)\left(\frac{p}{8} + O(\sqrt{p})\right) = \frac{p^2}{32} + O(p^{1.5})$$

- **Exceptional t:** There are at most 3 exceptional values for t. For each of these, the number of solutions N_t is trivially bounded by p. Their total contribution is at most $O(p)$, which is absorbed by the error term $O(p^{1.5})$.

Combining the generic and exceptional cases for $t \neq 0$, the total count is $\frac{p^2}{32} + O(p^{1.5})$.

Summing the contributions from $t = 0$ and $t \neq 0$, we get:

$$|K_2 \cap X^2| = O(p) + \left(\frac{p^2}{32} + O(p^{1.5})\right) = \frac{p^2}{32} + O(p^{1.5})$$

C. Asymptotic Size of Δ_p

We can now find the asymptotic size of the correction term:

$$\begin{aligned}\Delta_p &= |X|^2 - |K_2 \cap X^2| \\ &= \left(\frac{1}{16}p^2 + O(p)\right) - \left(\frac{p^2}{32} + O(p^{1.5})\right) \\ &= \left(\frac{2}{32} - \frac{1}{32}\right)p^2 + O(p^{1.5}) = \frac{1}{32}p^2 + O(p^{1.5})\end{aligned}$$

4 Assembling the Final Formula

We substitute the asymptotic estimates back into the exact formula for $|K_4|$.

$$\begin{aligned}|K_4| &= \frac{4p^4 + 19p^3 + 23p^2 - 39p - 7 + R(p)}{32} - \Delta_p \\ &= \left(\frac{1}{8}p^4 + \frac{19}{32}p^3 + \frac{23}{32}p^2 + O(p)\right) + \frac{O(p^{1.5})}{32} - \left(\frac{1}{32}p^2 + O(p^{1.5})\right)\end{aligned}$$

The largest error term is $O(p^{1.5})$. We collect the coefficients for the primary terms:

- p^4 coefficient: $\frac{1}{8}$
- p^3 coefficient: $\frac{19}{32}$
- p^2 coefficient: $\frac{23}{32} - \frac{1}{32} = \frac{22}{32} = \frac{11}{16}$

This yields the final asymptotic formula:

$$|K_4| = \frac{1}{8}p^4 + \frac{19}{32}p^3 + \frac{11}{16}p^2 + O(p^{1.5})$$

This completes the proof.

References

[1] A. Dujella and M. Kazalicki, *Diophantine m-tuples in finite fields and modular forms*, arXiv:1609.09356v2 [math.NT] (2018).

[2] T. Do Duc, K. H. Leung, and B. Schmidt, *Upper Bounds for Cyclotomic Numbers*, arXiv:1903.07314v1 [math.NT] (2019).

[3] M. Iliopoulou, *Discrete analogues of Kakeya problems*, PhD thesis, University of Edinburgh, arXiv:1312.5436v1 [math.CA] (2013).

[4] S. Li and A. Pott, *Intersection distribution, non-hitting index and Kakeya sets in affine planes*, arXiv:2003.06678v2 [math.CO] (2020).

[5] J. Merikoski, *The polynomials $X^2+(Y^2+1)^2$ and $X^2+(Y^3+Z^3)^2$ also capture their primes*, arXiv:2112.03617v3 [math.NT] (2023).

[6] J. H. Silverman, *The Arithmetic of Elliptic Curves*, 2nd ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, (2009). (Referenced in [1]).

[7] T. Storer, *Cyclotomy and difference sets*, Lectures in Advanced Mathematics, No. 2. Markham Publishing Co., Chicago, Ill., (1967). (Referenced in [2]).

[8] A. Weil, *On some exponential sums*, Proc. Nat. Acad. Sci. U.S.A., 34 (1948), 204–207. (Referenced in [5]).