# ON HILBERT CUBES AND PRIMITIVE ROOTS IN FINITE FIELDS

ALI ALSETRI AND XUANCHENG SHAO

Abstract. We consider the problem of bounding the dimension of Hilbert cubes in a finite field $\mathbb{F}_p$ that does not contain any primitive roots. We show that the dimension of such Hilbert cubes is $O_\varepsilon(p^{1/8+\varepsilon})$ for any $\varepsilon > 0$, matching what can be deduced from the classical Burgess estimate in the special case when the Hilbert cube is an arithmetic progression. We also consider the dual problem of bounding the dimension of multiplicative Hilbert cubes avoiding an interval.

## 1. Introduction

A central theme in additive combinatorics is to study the interplay between arithmetic and multiplicative structures. Let $\mathbb{F}_p$ be a finite field with $p$ prime. In this paper, we investigate the distribution of primitive roots in $\mathbb{F}_p$ in Hilbert cubes.

**Definition 1.1** (Hilbert cubes)**.** Let $d$ be a positive integer. A Hilbert cube $H \subset \mathbb{F}_p$ of dimension $d$ is a set of the form

$$H = \mathcal{H}(a_0; a_1, \dots, a_d) := \{a_0 + n_1 a_1 + \cdots + n_d a_d \colon n_1, \dots, n_d \in \{0, 1\}\}$$

for some $a_0, a_1, \dots, a_d \in \mathbb{F}_p$, with $a_1, \dots, a_d$ pairwise distinct.

Alternatively, $H = \mathcal{H}(a_0; a_1, \dots, a_d)$ is the collection of all subset sums of $A = \{a_1, \dots, a_d\}$ translated by $a_0$. If all these subset sums are distinct, then $|H| = 2^d$. In the other extreme, if $A$ is a homogeneous arithmetic progression of the form $A = \{k, 2k, \dots, dk\}$ for some positive integer $k$, then $|H| \le d(d+1)/2 + 1$.

We study the quantity $F(p)$, defined to be the largest positive integer $d$, such that there exists a Hilbert cube of dimension $d$ not containing any primitive roots modulo $p$.

**Theorem 1.2.** *For any $\varepsilon > 0$ we have $F(p) \ll_\varepsilon p^{1/8+\varepsilon}$.*

Previously the best known upper bound is $F(p) \ll p^{3/19+o(1)}$ from [8], building on earlier works [10, 6]. As noted in [6], Theorem 1.2 implies as a special case the Burgess bound $g(p) \le p^{1/4+o(1)}$ on the least primitive root $g(p)$ modulo $p$ [2]. This can be seen by considering $H = \mathcal{H}(0; 1, 2, \dots, d) = \{0, 1, 2, \dots, d(d+1)/2\}$. Hence any improvement of the exponent $1/8$ in Theorem 1.2 would also lead to an improvement of the Burgess bound.

As immediate corollaries, we get the same upper bound for the dimension of Hilbert cubes whose elements are all quadratic residues, or Hilbert cubes whose elements are all quadratic non-residues.

**Corollary 1.3.** *If $H \subset \mathbb{F}_p$ is a Hilbert cube of dimension $d$ whose elements are all quadratic residues modulo $p$, then $d \ll_\varepsilon p^{1/8+\varepsilon}$ for any $\varepsilon > 0$. Similarly, If $H \subset \mathbb{F}_p$ is a Hilbert cube of dimension $d$ whose elements are all quadratic non-residues modulo $p$, then $d \ll_\varepsilon p^{1/8+\varepsilon}$ for any $\varepsilon > 0$.*

XS was supported by NSF grant DMS-1802224.

*Proof.* If all elements in $H$ are quadratic residues, then $H$ does not contain any primitive roots, and hence the conclusion follows from Theorem 1.2. If all elements in $H = \mathcal{H}(a_0; a_1, \dots, a_d)$ are quadratic non-residues, then for any fixed quadratic non-residue $g \in \mathbb{F}_p$, all elements in the dilated Hilbert cube $H' = \mathcal{H}(ga_0; ga_1, \dots, ga_d)$ are all quadratic residues, and the conclusion follows from the previous case. □

Our proof of Theorem 1.2 follows the general strategy in [8]. First we locate a large generalized arithmetic progression (GAP) $P$ in the Hilbert cube $H = \mathcal{H}(a_0; a_1, \dots, a_d)$ when $d \geq p^{1/8+\varepsilon}$; see Proposition 3.1 below. This is to be expected since there are lots of collisions when forming subset sums of $\{a_1, \dots, a_d\}$ when $d \geq p^{1/8+\varepsilon}$, and thus $H$ should have rich additive structures. This type of phenomenon from subset sums or iterated sumsets was studied in [13, 14]. Then we use character sum estimates to show that $P$ must contain primitive roots; see Proposition 3.2 below.

We remark that Theorem 1.2 explores the interaction between an additively defined set (Hilbert cube) and a multiplicatively defined set (primitive roots), belonging to the broader theme of sum-product phenomenon in additive combinatorics. See [6, 7, 8] for other distributional problems involving the quadratic residues, and [4, 5] for related questions in the setting of integers instead of $\mathbb{F}_p$.

We also investigate the following dual problem, where the roles of addition and multiplication are reversed. We start with the definition of multiplicative Hilbert cubes.

**Definition 1.4** (Multiplicative Hilbert cubes)**.** Let $d$ be a positive integer. A multiplicative Hilbert cube $H \subset \mathbb{F}_p$ of dimension $d$ is a set of the form

$$H = \mathcal{H}^{\times}(a_0; a_1, \dots, a_d) := \left\{ a_0 a_1^{n_1} \cdots a_d^{n_d} : n_1, \dots, n_d \in \{0, 1\} \right\}$$

for some $a_0, a_1, \dots, a_d \in \mathbb{F}_p^{\times}$, with $a_1, \dots, a_d$ pairwise distinct.

**Theorem 1.5.** *For any $\varepsilon > 0$, there exists $\delta > 0$ such that the following statement holds. Let $I \subset \mathbb{F}_p$ be an interval of length $p^{1-\delta}$, and let $H$ be a multiplicative Hilbert cube of dimension $d$ that does not intersect $I$. Then $d \ll_{\varepsilon} p^{\varepsilon}$.*

Note that if $H \subset \mathbb{F}_p^{\times}$ is a multiplicative subgroup, then it is a multiplicative Hilbert cube of dimension $|H|$. Our proof of Theorem 1.5 uses Bourgain's multilinear exponential sum estimate [1] and the Erdös-Turán inequality on equidistribution.

**Notation.** We use $X \ll Y$, $X = O(Y)$, or $Y \gg X$ to denote the estimate $|X| \leq CY$ for some constant $C$. If we wish to permit this constant to depend on one or more parameters we shall indicate this by appropriate subscripts, thus for instance $O_{\varepsilon}(Y)$ denotes a quantity bounded in magnitude by $C_{\varepsilon} Y$ for some quantity $C_{\varepsilon}$ depending only on $\varepsilon$.

If $x$ is a real number, we write $e(x) \coloneqq e^{2\pi i x}$. If $n$ is an element in a finite field $F_p$, we write $e_p(n) \coloneqq e(n/p) = e^{2\pi i n/p}$.

## 2. Preliminaries

2.1. **GAPs and sumsets.** For a subset $A \subset \mathbb{F}_p$ and a positive integer $\ell$, we define the $\ell$-fold sumset $\ell A$ to be the set of all sums $a_1 + \cdots + a_\ell$ with each $a_i \in A$, and define the restricted $\ell$-fold sumset $\ell^* A$ to be the set of all sums $a_1 + \cdots + a_\ell$ with distinct $a_1, \dots, a_\ell \in A$. We denote by $S_A$ the collection of all elements which can be represented as a sum of distinct members of $A$. Thus $S_A = \cup_{1 \leq \ell \leq |A|} \ell^* A$.

**Definition 2.1.** A Generalized Arithmetic Progression (GAP) of rank $r$ is a subset $P \subset \mathbb{F}_p$ of the form

$$P = \{a_0 + n_1 a_1 + \cdots + n_r a_r : 0 \le n_i < N_i\}$$

for some positive integers $N_1, \ldots, N_r$ and some $a_0, a_1, \ldots, a_r \in \mathbb{F}_p$. It is said to be proper if $|P| = \prod_{i=1}^r N_i$.

The following theorem of Szemeredi and Vu [14, Theorem 10.5] allows us to locate a large GAP inside an interated sumset $\ell^* A$.

**Theorem 2.2.** *For any fixed positive integer $r$ there are positive constants $C$ and $c$ depending on $r$ such that the following holds. Let $p$ be a prime, let $A \subset \mathbb{F}_p$ be a subset, and let $\ell \le |A|/2$ be a positive integer such that $\ell^{r+1}|A| \ge Cp$. Then $\ell^* A$ either contains all of $\mathbb{F}_p$ or contains a proper GAP of rank $r'$ and size at least $c\ell^{r'}|A|$, for some integer $1 \le r' \le r$.*

2.2. **Character sum estimates.** We collect character sum estimates over GAPs which will be used in the proof of Theorem 1.2. These can be viewed as generalizations of the classical Burgess estimate for character sums. Chang's estimate [3] gives non-trivial bound for character sums over GAPs of size $p^{2/5+\varepsilon}$.

**Theorem 2.3.** *Let $p$ be prime, and let $P \subset \mathbb{F}_p$ be a proper GAP of rank $r$ with $|P| > p^{\frac{2}{5}+\varepsilon}$ for some $\varepsilon > 0$. Let $\chi \pmod p$ be a non-trivial Dirichlet character. Then*

$$\sum_{n \in P} \chi(n) \ll_{\varepsilon, r} p^{-c}|P|$$

*for some constant $c = c(\varepsilon, r) > 0$.*

For GAPs of rank $r = 2$, one can improve the threshold $p^{2/5+\varepsilon}$ in Theorem 2.3 to $p^{1/3+\varepsilon}$, using the following character sum estimates over unions of intervals [12, Corollary 1.2] (which builds on works in [9]).

**Theorem 2.4.** *Let $p$ be prime and $\varepsilon > 0$. Let $\chi \pmod p$ be a non-trivial Dirichlet character. Let $A \subset [1, p]$ be a union of $s$ disjoint intervals $I_1, \ldots, I_s$ each of which has length at least $p^{\varepsilon}$. Suppose that $|A| s^{-\frac{1}{2}} > p^{\frac{1}{4}+\varepsilon}$. Then*

$$\sum_{n \in A} \chi(n) \ll_{\varepsilon} p^{-c}|A|$$

*for some constant $c = c(\varepsilon) > 0$.*

**Corollary 2.5.** *Let $p$ be prime, and let $P \subset \mathbb{F}_p$ be a proper GAP of rank 2 with $|P| > p^{\frac{1}{3}+\varepsilon}$ for some $\varepsilon > 0$. Let $\chi \pmod p$ be a non-trivial Dirichlet character. Then*

$$\sum_{n \in P} \chi(n) \ll_{\varepsilon} p^{-c}|P|$$

*for some constant $c = c(\varepsilon) > 0$.*

*Proof.* We may write

$$P = \{a_0 + n_1 a_1 + n_2 a_2 \colon 0 \le n_1 < N_1, 0 \le n_2 < N_2\}$$

for some positive integers $N_1, N_2$ and some $a_0, a_1, a_2 \in \mathbb{F}_p$. Without loss of generality, we may assume that $N_1 \ge N_2$. We have $a_1 \ne 0$ since $P$ is proper. Let

$$P' = a_1^{-1} P := \{a_1^{-1} a_0 + n_1 + n_2 (a_1^{-1} a_2) \colon 0 \le n_1 < N_1, 0 \le n_2 < N_2\}.$$

Since $P$ is proper, $P'$ is also proper and thus it is a disjoint union of $N_2$ intervals of length $N_1$. We have

$$|P'|N_2^{-1/2} = N_1 N_2^{1/2} \geq (N_1 N_2)^{3/4} = |P|^{3/4} > p^{1/4+\varepsilon/2}.$$

Hence we may apply Theorem 2.4 to conclude that

$$\sum_{n\in P} \chi(n) = \sum_{n\in P'} \chi(n) \ll_\varepsilon p^{-c}|P|$$

for some constant $c = c(\varepsilon) > 0$. □

2.3. **Uniform Distribution.** In the proof of Theorem 1.5, we will need the Erdös-Turán inequality that connects equidistribution with exponential sums; see [11, Corollary 1.1].

**Theorem 2.6** (Erdös-Turán inequality)**.** *Let $u_1, u_2, \ldots, u_N$ be any sequence of points on the unit circle $\mathbb{R}/\mathbb{Z}$. For any positive integer $K$ and any $\alpha \leq \beta \leq \alpha + 1$, we have*

$$|\#\{1 \leq n \leq N \colon u_n \in [\alpha, \beta] \pmod 1\} - (\beta - \alpha)N| \leq \frac{N}{K+1} + 3\sum_{k=1}^{K} \frac{1}{k} \left| \sum_{n=1}^{N} e(ku_n) \right|.$$

**Corollary 2.7.** *Let $I \subset \mathbb{F}_p$ be an interval of length $|I| = \delta p$, and let $a_1, a_2, \ldots, a_N$ be any sequence of points in $\mathbb{F}_p$, none of which lies in $I$. Then there exists a positive integer $k \leq 10\delta^{-1}$ such that*

$$\left| \sum_{n=1}^{N} e_p(ka_n) \right| \gg \delta^2 N.$$

*Proof.* We apply Theorem 2.6 with the sequence of points $\{a_n/p\}_{1\leq n\leq N}$ and $[\alpha, \beta] = p^{-1}I$ to obtain

$$\frac{|I|}{p} N \leq \frac{N}{K+1} + 3\sum_{k=1}^{K} \frac{1}{k} \left| \sum_{n=1}^{N} e_p(ka_n) \right|$$

for any positive integer $K$. Choosing $K = 10/\delta$, we conclude that

$$\delta N \ll \sum_{k=1}^{K} \left| \sum_{n=1}^{N} e_p(ka_n) \right|.$$

The conclusion follows immediately. □

## 3. Proof of Theorem 1.2

In this section we deduce Theorem 1.2 by showing that Hilbert cubes must contain large proper GAPs (Proposition 3.1), and that large GAPs must contain primitive roots (Proposition 3.2).

**Proposition 3.1** (Hilbert cubes contain large GAPs)**.** *For any positive integer $r$, there exist constants $C, c > 0$ depending only on $r$ such that the following statement holds. Let $d$ be a positive integer and $p$ be prime. If $d^{r+2} \geq Cp$, then any Hilbert cube of dimension $d$ in $\mathbb{F}_p$ either contains all of $\mathbb{F}_p$, or contains a proper progression of rank $r'$ and size at least $cd^{r'+1}$ for some $1 \leq r' \leq r$.*

*Proof.* Let $H = \mathcal{H}(a_0; a_1, \dots, a_d)$ be a Hilbert cube of dimension $d$, where $a_0, a_1, \dots, a_d \in \mathbb{F}_p$ with $a_1, \dots, a_d$ pairwise distinct. We will apply Theorem 2.2 with $A = \{a_1, \dots, a_d\}$ and $\ell = \lfloor d/2 \rfloor$. We have

$$\ell^{r+1}|A| \gg_r d^{r+2} \geq Cp.$$

Hence the assumptions in Theorem 2.2 are satisfied provided that $C$ is large enough in terms of $r$. Thus we conclude $\ell^* A$ either contains all of $\mathbb{F}_p$ or contains a proper GAP of rank $r'$ and size at least $\gg_r \ell^{r'}|A| \gg_r d^{r'+1}$, for some $1 \leq r' \leq r$. The desired conclusion follows since $\ell^* A$ is contained in a translate of $H$. □

**Proposition 3.2.** *Let $P \subset \mathbb{F}_p$ be a proper GAP of rank $r$. If $P$ does not contain any primitive roots modulo $p$, then $|P| \ll_\varepsilon p^{f(r)+\varepsilon}$ for any $\varepsilon > 0$, where*

$$f(r) = \begin{cases} 1/4 & \text{if } r = 1, \\ 1/3 & \text{if } r = 2, \\ 2/5 & \text{if } r \geq 3. \end{cases}$$

*Proof.* We may assume that $p$ is sufficiently large in terms of $\varepsilon$, since otherwise the claim holds trivially. By [6, Lemma 2.4] we have for any $n \in \mathbb{F}_p$,

$$\frac{\varphi(p-1)}{p-1} \sum_{\chi \pmod p} c_\chi \chi(n) = \begin{cases} 1 & \text{if } n \text{ is a primitive root} \pmod p, \\ 0 & \text{otherwise,} \end{cases}$$

where $c_\chi = \mu(\mathrm{ord}(\chi))/\varphi(\mathrm{ord}(\chi))$ and $\mathrm{ord}(\chi)$ denotes the order of $\chi$. Since $P$ does not contain any primitive roots, we have

$$\sum_{\chi \pmod p} c_\chi \sum_{n \in P} \chi(n) = 0.$$

Taking out the term $\chi = \chi_0$, we get

$$\left| \sum_{\chi \neq \chi_0} c_\chi \sum_{n \in P} \chi(n) \right| \geq |P| - 1.$$

Note that

$$\sum_\chi |c_\chi| \leq \sum_{d | p-1} \frac{1}{\varphi(d)} \#\{\chi \colon \mathrm{ord}(\chi) = d\} = \sum_{d | p-1} 1 \ll_\tau p^\tau$$

for any $\tau > 0$. Thus for at least one non-trivial character $\chi \neq \chi_0$ we have

$$\left| \sum_{a \in P} \chi(a) \right| \gg_\tau |P| p^{-\tau}$$

for any $\tau > 0$.

Suppose, for the purpose of contradiction, that $|P| \geq p^{f(r)+\varepsilon}$. By the Burgess estimate on character sums (in the case $r = 1$), Theorem 2.3 (in the case $r \geq 3$), and Corollary 2.5 (in the case $r = 2$), we have

$$\left| \sum_{a \in P} \chi(a) \right| \ll_\varepsilon |P| p^{-c}.$$

for some constant $c = c(\varepsilon) > 0$. This leads to a contradiction, choosing $\tau = c/2$ (say). □

We are now ready to deduce Theorem 1.2. We may assume that $p$ is sufficiently large in terms of $\varepsilon$, since otherwise the claim holds trivially. Suppose, for the purpose of contradiction, that there is a Hilbert cube $H \subset \mathbb{F}_p$ of dimension $d > p^{1/8+\varepsilon}$ not containing any primitive roots. By Proposition 3.1 applied with $r = 10$ (say), $H$ contains a proper progression $P$ of rank $r'$ and size $|P| \gg d^{r'+1} \gg p^{(r'+1)/8+\varepsilon}$, for some $1 \leq r' \leq 10$. On the other hand, since $P$ does not contain any primitive roots, Proposition 3.2 implies that $|P| \ll_\varepsilon p^{f(r')+\varepsilon/2}$. Combining the upper and lower bounds for $|P|$, we conclude that $(r'+1)/8 < f(r')$. This is a contradiction, no matter whether $r' = 1$, $r' = 2$, or $r' \geq 3$.

## 4. Proof of Theorem 1.5

In this section we deduce Theorem 1.5 by combining Corollary 2.7 with certain (weighted) exponential sum estimates over Hilbert cubes.

We may assume that $p$ is sufficiently large, otherwise the claim holds trivially. Let $H = \mathcal{H}^\times(a_0; a_1, \dots, a_d)$ be a multiplicative Hilbert cube, where $a_0, a_1, \dots, a_d \in \mathbb{F}_p^\times$ with $a_1, \dots, a_d$ pairwise distinct. Suppose, for the purpose of contradiction, that $d \geq p^\varepsilon$. Set $r = \lceil 2\varepsilon^{-1} \rceil$, and form a partition

$$\{a_1, \dots, a_d\} = A_1 \cup \dots \cup A_r$$

into subsets of almost-equal sizes, so that

$$|A_i| = \frac{d}{r} + O(1) \gg_\varepsilon p^\varepsilon$$

for each $1 \leq i \leq r$. For $b \in \mathbb{F}_p^\times$, consider the exponential sum

$$S_b := \sum_{x_1 \in A_1, \dots, x_r \in A_r} e_p(b x_1 \cdots x_r).$$

On the one hand, none of the points $a_0 x_1 \cdots x_r$ with $x_i \in A_i$ lies in the interval $I$, so Corollary 2.7 implies that there exists a positive integer $k \leq 10p^\delta$ such that

$$\left| \sum_{x_1 \in A_1, \dots, x_r \in A_r} e_p(k a_0 x_1 \cdots x_r) \right| \gg p^{-2\delta} |A_1| \cdots |A_r|.$$

On the other hand, since $|A_i| \gg_\varepsilon p^\varepsilon$ for each $i$ and $\prod_{1 \leq i \leq r} |A_i| \gg_\varepsilon p^{r\varepsilon} \gg p^2$, we may apply Bourgain's exponential sum bound [1, Theorem A] to obtain

$$\left| \sum_{x_1 \in A_1, \dots, x_r \in A_r} e_p(k a_0 x_1 \cdots x_r) \right| < p^{-c} |A_1| \cdots |A_r|$$

for some constant $c = c(\varepsilon) > 0$. This leads to a contradiction by choosing $\delta = c/4$.

## References


[1] J. Bourgain. Multilinear exponential sums in prime fields under optimal entropy condition on the sources. *Geom. Funct. Anal.*, 18(5):1477–1502, 2009.

[2] D. A. Burgess. On character sums and primitive roots. *Proc. London Math. Soc. (3)*, 12:179–192, 1962.

[3] M. C. Chang. On a question of Davenport and Lewis and new character sum bounds in finite fields. *Duke Math. J.*, 145(3):409–442, 2008.

[4] R. Dietmann and C. Elsholtz. Hilbert cubes in progression-free sets and in the set of squares. *Israel J. Math.*, 192(1):59–66, 2012.

[5] R. Dietmann and C. Elsholtz. Hilbert cubes in arithmetic sets. *Rev. Mat. Iberoam.*, 31(4):1477–1498, 2015.
[6] R. Dietmann, C. Elsholtz, and I. E. Shparlinski. On gaps between primitive roots in the Hamming metric. *Q. J. Math.*, 64(4):1043–1055, 2013.
[7] R. Dietmann, C. Elsholtz, and I. E. Shparlinski. On gaps between quadratic non-residues in the Euclidean and Hamming metrics. *Indag. Math. (N.S.)*, 24(4):930–938, 2013.
[8] R. Dietmann, C. Elsholtz, and I. E. Shparlinski. Prescribing the binary digits of squarefree numbers and quadratic residues. *Trans. Amer. Math. Soc.*, 369(12):8369–8388, 2017.
[9] D. R. Heath-Brown. Burgess's bounds for character sums. In *Number theory and related fields*, volume 43 of *Springer Proc. Math. Stat.*, pages 199–213. Springer, New York, 2013.
[10] N. Hegyvári and A. Sárközy. On Hilbert cubes in certain sets. *Ramanujan J.*, 3(3):303–314, 1999.
[11] H. L. Montgomery. *Ten lectures on the interface between analytic number theory and harmonic analysis*, volume 84 of *CBMS Regional Conference Series in Mathematics*. Published for the Conference Board of the Mathematical Sciences, Washington, DC; by the American Mathematical Society, Providence, RI, 1994.
[12] X. Shao. Character sums over unions of intervals. *Forum Math.*, 27(5):3017–3026, 2015.
[13] E. Szemerédi and H. Vu. Finite and infinite arithmetic progressions in sumsets. *Ann. of Math. (2)*, 163(1):1–35, 2006.
[14] E. Szemerédi and V. Vu. Long arithmetic progressions in sumsets: thresholds and bounds. *J. Amer. Math. Soc.*, 19(1):119–169, 2006.

Department of Mathematics, University of Kentucky, 715 Patterson Office Tower, Lexington, KY 40506, USA
*Email address*: alialsetri@uky.edu

Department of Mathematics, University of Kentucky, 715 Patterson Office Tower, Lexington, KY 40506, USA
*Email address*: xuancheng.shao@uky.edu