A LOWER BOUND CONSTRUCTION FOR THE "BOX PROBLEM" IN PRIME DEGREES

M. STOECKL

Abstract. We extend the construction of Katz, Krop, Maggioni[KKM02] from 3 dimensions to any prime number d, showing that a d-tensor with values in $\{0,1\}$ fulfilling the "box condition" may have $\sim N^{d-\frac{1}{d}}$ nonzero entries.

For context, see [KKM02], whose result this paper extends.

Definition 1. The box condition for a tensor I in d-dimensions is that there do not exist pairs of distinct indices $i_{k,\mathtt{A}}$, $i_{k,\mathtt{B}}$ for each dimension $k \in \{1,\ldots,d\}$ so that

$$I_{i_{1,x_1},\ldots,i_{k,x_k}} = 1$$

for all 2^d assignments $x_k \in \{\mathtt{A},\mathtt{B}\}$.

Claim 2. Let p, d be prime numbers, and $N = p^d - 1$. We define a d-tensor I and index its sides by the sets $\mathbb{F}_{p^d} \setminus \{0\}$. As we can identify each element in $\mathbb{F}_{p^d}$ with a vector in $\mathbb{F}_p^d$, we introduce $a \cdot b$ as notation for that vector dot product map, $\mathbb{F}_p^d \times \mathbb{F}_p^d \to \mathbb{F}_p$. Juxtaposition will denote multiplication in the finite field. Then

$$I(p_1, p_2, \ldots, p_d) = \begin{cases} 1 & p_1 \cdot [p_2 p_3 \ldots p_d] = 1 \\ 0 & \text{otherwise} \end{cases}$$

We claim this tensor I fulfills the box condition. There are $p^{d-1}\left(p^d - 1\right)^{d-1}$ nonzero entries.

Proof. That there are $p^{d-1}\left(p^d - 1\right)^{d-1}$ nonzero entries follows from the fact that, after selecting $p_2, \ldots, p_d$ arbitrarily from $\mathbb{F}_{p^d} \setminus \{0\}$, there are only p^{d-1} possible values of p_1 for which $I(p_1, \ldots, p_d) = 1$, all nonzero.

Proof. Assume for sake of contradiction that I does not fulfill the box condition. Then there exist distinct $p_{i,1}, p_{i,2}$ for all i for which

$$(\star) \qquad p_{1,k_1} \cdot [p_{2,k_2} p_{3,k_3} \ldots p_{d,k_d}] = 1$$

for all values of $k_i \in \{1,2\}$.

First, note that $p_{i,1}/p_{i,2} \notin \mathbb{F}_p$. If $p_{i,2}/p_{i,1} = d \in \mathbb{F}_p$, then comparing the two instance of Eq. $\star$ which differ only in the ith coordinate implies $d = 1$, which contradicts that $p_{i,1} \neq p_{i,2}$.

Next, define

$$S := \left\{ p_{2,k_2} p_{3,k_3} \ldots p_{d,k_d} : (k_i)_{i=2}^d \in \{1,2\}^{d-1} \right\}$$

Date: 2019-04-17.

Subtracting two instances of Eq. $\star$, differing only the the first coordinate, implies that for all $s \in S$,

$$(p_{1,1} - p_{1,2}) \cdot s = 0$$

in which case S is contained in a $d-1$ dimensional linear subspace of $\mathbb{F}_p^d$.

Defining the dimension of a set to be the dimension of the linear subspace generated by its elements, we derive a contradiction by proving inductively that $\dim S = d$. Define

$$S_m := \left\{ p_{2,k_2} \dots p_{d,,m_d} : (k_i)_{i=2}^m \in \{1,2\}^{m-1} \right\}$$

so that $S = S_d$, and $S_1 = \{1\}$, with $\dim S_1 = 1$. Then for all $m = 2, \dots d$,

$$S_m = p_{m,1} \left(S_{m-1} \bigcup \frac{p_{m,2}}{p_{m,1}} S_{m-1} \right).$$

Since $p_{m,2}/p_{m,1} \notin \mathbb{F}_p$, and $\mathbb{F}_{p^d}$ has no nontrivial subfields other than the base field $\mathbb{F}_p$, the linear operator defined by multiplication with $p_{m,2}/p_{m,1}$ does not preserve any nontrivial linear subspaces of $\mathbb{F}_p^d$. Consequently, the linear subspace generated by S_{m-1} and the linear subspace generated by $\frac{p_{m,2}}{p_{m,1}} S_{m-1}$ are distinct and of equal dimension, hence

$$\dim S_m \geq \dim (S_{m-1}) + 1$$

From the induction, $\dim S_m \geq m$, so $\dim S = \dim S_d = d$. □

□

Lemma 3. *It may not be obvious that an element α not in the base field of $\mathbb{F}_{p^d}$, does not map any linear subspaces $L \notin \left\{ \emptyset, \mathbb{F}_p^d \right\}$ to themselves. For d prime, this is the case.*

Proof. Define

$$G := \left\{ \alpha \in \mathbb{F}_{p^d} : \alpha L \subset L \right\}.$$

Then G is a field, so either $G = \mathbb{F}_{p^d}$, and $L \in \left\{ \emptyset, \mathbb{F}_p^d \right\}$, or $G = \mathbb{F}_p$. □

References

[KKM02] Nets Hawk Katz, Elliot Krop, and Mauro Maggioni, *Remarks on the box problem*, Mathematical Research Letters **9** (2002), no. 4, 515–520.