On a Conjecture of Butler and Graham

Tengyu Ma[1], Xiaoming Sun[2], and Huacheng Yu[1]

[1] Institute for Interdisciplinary Information Sciences, Tsinghua University
[2] Institute of Computing Technology, Chinese Academy of Sciences

Abstract. Motivated by a hat guessing problem proposed by Iwasawa [6], Butler and Graham [2] made the following conjecture on the existence of certain way of marking the *coordinate lines* in $[k]^n$: there exists a way to mark one point on each *coordinate line* in $[k]^n$, so that every point in $[k]^n$ is marked exactly a or b times as long as the parameters (a, b, n, k) satisfies that there are non-negative integers s and t such that $s + t = k^n$ and $as + bt = nk^{n-1}$. In this paper we prove this conjecture for any prime number k. Moreover, we prove the conjecture for the case when $a = 0$ for general k.

1 Introduction

In [2] Butler and Graham considered the problem of the existence of certain way of marking coordinate lines in $[k]^n$. A *coordinate line* in $[k]^n$ is the set of k points in which all but one coordinate are fixed and the unfixed coordinate varies over all possibilities. *Marking* a line[1] means designating a point on that line. They conjectured that

Conjecture 1 (Butler, Graham [2]). There is a marking of the lines in $[k]^n$ so that on each line exactly one point is marked and each point is marked either a or b times if and only if there are nonnegative integers s and t satisfying the linear equations $s + t = k^n$ and $as + bt = nk^{n-1}$.

The "only if" part of the conjecture is straightforward, leaving to be crucial the construction of a marking of lines in $[k]^n$ with the desired properties. Buhler, Butler, Graham, and Tressler [1] proved the conjecture for $k = 2$. Butler and Graham [2] proved the conjecture when $n \leq 5$. The main contributions of this paper are i) we prove all the cases when k is an odd prime; ii) we prove the case when $a = 0$ (without any assumption on k).

Theorem 1. *For any prime k and $0 \leq a < b \leq n$, there exists a marking of lines in $[k]^n$ so that each point is marked either a times or b times if and only if there are nonnegative integers s and t so that $s + t = k^n$ and $as + bt = nk^{n-1}$.*

Theorem 2. *For $0 < b \leq n$, there exists a marking of lines in $[k]^n$ so that each point is either unmarked or marked b times if and only if there are nonnegative integers s and t so that $s + t = k^n$ and $bt = nk^{n-1}$.*

As in [2], we use the notation $[a, b]_k^n$ as a shorthand for a realization of a marking of the lines in $[k]^n$ where each point is marked either a times or b times. Then Theorem 1 provides a sufficient and necessary condition for the existence of $[a, b]_k^n$ for any prime k, and Theorem 2 considers the existence of $[a, b]_k^n$ when $a = 0$.

In the proof of Theorem 1 we reduce the existence of $[a, b]_k^n$ to the existence of $[a - 1, b - 1]_k^{n-k}$ when $a > 0$ and $b \leq n - k + 1$ (see Proposition 2 in Section 2). It turns out that the most

---

[1] for convenience, we use line to indicate coordinate line throughout this paper.

complicated part of this inductive argument is the construction of the base cases, that is, $[0, b]_k^n$ and $[a, n - t]_k^n$ (where $t < k$). We provide two theorems (Theorem 3 and 4) giving a direct realizations for these two kinds of markings. The proofs of these theorems use similar approaches, though different in many details, that we partition the whole grid $[k]^n$ according to certain number theory based characteristic function, which has a nice symmetrical property: Informally speaking, for any fixed s, any point $\boldsymbol{x} \in [k]^n$, and any value $\boldsymbol{v}$ in the range of this function, there exists a unique direction along which by moving from $\boldsymbol{x}$ with distance s, we can reach a point with value $\boldsymbol{v}$. By a sophisticated utilizing this property, we accomplish the design of markings for these two base cases. Furthermore, we prove the case $[0, b]_k^n$ for general k by generalizing the characteristic function in a delicate way.

Related Work

The motivation of investigating this marking line problem is to reformulate and solve a hat guessing question proposed by Iwasawa [6]. In that game there are several players sitting around a table, each of which is assigned a hat with one of k colors. Each player can see all the colors of others' hat but his/her own. The players try to coordinate a strategy before the game starts, and guess the colors of their own hats simultaneously and independently after the hats are placed on their heads. Their goal is to design a strategy that guarantees exactly either a or b correct guesses. For example, one special case is that either everybody guesses the color correctly or nobody guesses correctly, i.e. $a = 0$ and $b = n$.

Several variations of hat guessing game have been considered in the literature. Ebert [4] considered the model that players are allowed to answer "unknown". He showed that in this model there is a *perfect strategy* for players when n is of the form $2^m - 1$. Lenstra and Seroussi [7] studied the case that n is not of such form. Butler, Hajiaghayi, Kleinberg and Leighton [3] considered the worst case that each player can see only part of the others' hats with respect to a sight graph. Feige [5] investigated the average case with a sight graph. Peterson and Stinson [9] investigated the case that each player can see hats in front of him and they guess one by one. Recently Ma, Sun and Yu [8] proposed a variation which allow to answer "unknown" and require at least k correct guesses for winning condition.

Notations and Preliminaries

$[k] = \{1, 2, \ldots, k\}$, $[k]^n = \underbrace{[k] \times \cdots \times [k]}_{n}$. $[a, b]_k^n$: marking of lines in $[k]^n$ in which each point is marked either a times or b times. We assume that $a < b$ as well. Throughout the paper we always use boldface type letters for vectors and vector-valued functions. For a vector $\boldsymbol{x} = (x_1, \ldots, x_n)$, define the k-modulo parity function $\oplus(\boldsymbol{x}) = x_1 + x_2 + \cdots + x_n \mod k$. We denote by $\boldsymbol{x}_{-i}$ the line $(x_1, \ldots, x_{i-1}, *, x_{i+1}, \ldots, x_n)$, i.e.

$$\boldsymbol{x}_{-i} = \{(x_1, \ldots, x_{i-1}, y, x_{i+1}, \ldots, x_n) \mid y \in [k]\}.$$

The necessary condition in the conjecture is straightforward.

Proposition 1 ([1]). *If we have $[a, b]_k^n$, then the following equations system has nonnegative integer solution.*

$$\begin{cases} s + t = k^n, \\ as + bt = k^{n-1} n. \end{cases}$$

More specifically, $s = \frac{k^{n-1}(kb - n)}{b - a}$ is the number of points that are marked a times, and $t = \frac{k^{n-1}(n - ka)}{b - a}$ is the number of points that are marked b times.

The rest of the paper is organized as follows: In Section 2 we show that the necessary condition is sufficient when the number of colors k is a prime. Section 3 considers the case for general k when $a = 0$. Finally we conclude the paper in Section 4 with some open problems.

2 $[a, b]_k^n$ for Prime k

In this section we prove the conjecture when k is an odd prime number (the case $k = 2$ has been proved by Buhler et al. [1]). The first step is to reduce $[a, b]_k^n$ to $[a - 1, b - 1]_k^{n-k}$ as in Butler and Graham [2].

Proposition 2 ([2]). *Given $[a, b]_k^n$, we have $[a + 1, b + 1]_k^{n+k}$.*

By repeatedly using this Proposition, we can reduce the problem $[a, b]_k^n$ to two possible cases: (1) $[a', b']_k^{n'}$, where $b' > n' - k$; (2) $[0, b']_k^{n'}$ (recall that $a < b$). During this procedure, the divisibility is unchanged (see the proof of Theorem 1). The following two theorems (Theorem 3 and Theorem 4) give the constructions of two base cases, respectively.

Theorem 3. *If k is a prime and $0 \leq t \leq k - 1$, $1 \leq a < n - t$, and $(\frac{n-ka}{n-t-a})k^{n-1}$ is a nonnegative integer, then we have $[a, n - t]_k^n$.*

Proof. Firstly we do some elementary number theory substitution to make the parameters more manageable. Suppose that $(\frac{n-ka}{n-t-a})k^{n-1}$ is a nonnegative integer. Since k is a prime, there exists $m, r \in \mathbb{N}$ so that $n - t - a = k^m r$, where $m \leq n - 1$, $r | n - ka$, and $n \geq ka$. ($n - t \geq a$ implicitly holds.) Observe that $r | n - ka$ and $r | n - t - a$ implies that $r | (k - 1)a - t$. Let $(k - 1)a - t = ra'$, where

$$a' = \frac{(k-1)a - t}{r} = \frac{(ka - a - t)k^m}{n - t - a} \leq \frac{(n - a - t)k^m}{n - t - a} = k^m.$$

Thus, $n = t + a + k^m r$ and $(k - 1)a = t + ra'$, where a', m and r are all nonnegative integers.

Now we construct a marking of lines in $[k]^n$ so that each point is marked either $(n - t)$ times or a times. For convenience, we partition the $n = a + t + k^m r$ dimensions into three groups, each of which contains $k^m r$, t, and a coordinates respectively[2], and represent each point in $[k]^n$ by $(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z})$ where $\boldsymbol{x} \in [k]^{k^m r}$, $\boldsymbol{y} \in [k]^t$, and $\boldsymbol{z} \in [k]^a$. Furthermore, we index $\boldsymbol{x}$ by a pair $(i, j) \in \mathbb{Z}_k^m \times [r]$, i.e. $x_{i,j} \in [k]$ are the coordinates of $\boldsymbol{x}$ (where $i \in \mathbb{Z}_k^m, j \in [r]$)[3]. For a point $(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}) \in [k]^n$ and $i \in \mathbb{Z}_k^m, j \in [r]$, denote by $(\boldsymbol{x}_{-(i,j)}, \boldsymbol{y}, \boldsymbol{z})$ the lines of $[k]^n$ for which all the coordinates are fixed except the coordinate (i, j) of $\boldsymbol{x}$, i.e.

$$(\boldsymbol{x}_{-(i,j)}, \boldsymbol{y}, \boldsymbol{z}) = \{(\tilde{\boldsymbol{x}}, \tilde{\boldsymbol{y}}, \tilde{\boldsymbol{z}}) \in [k]^n \mid \tilde{\boldsymbol{y}} = \boldsymbol{y}, \tilde{\boldsymbol{z}} = \boldsymbol{z}, \forall (i', j') \neq (i, j)\ \tilde{x}_{i',j'} = x_{i',j'}, \tilde{x}_{i,j} \in [k]\}$$

Similarly $(\boldsymbol{x}, \boldsymbol{y}_{-i}, \boldsymbol{z})$ $(i \in [t])$ is a line of $[k]^n$ which the i-th coordinate of $\boldsymbol{y}$ is unfixed, $(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}_{-i})$ $(i \in [a])$ is a line which the i-th coordinate of $\boldsymbol{z}$ is unfixed.

For each $\boldsymbol{x} \in [k]^{k^m r}$, define the *characteristic function* $\boldsymbol{q} : [k]^{k^m r} \to [k]^m$ as follows:

$$\boldsymbol{q}(\boldsymbol{x}) = \sum_{\boldsymbol{i}=(i_1,\ldots,i_m)\in\mathbb{Z}_k^m} \left(\sum_{j=1}^r x_{i,j}\right) \cdot \boldsymbol{i} \tag{1}$$

where $\boldsymbol{i}$ is k-based representation of i in $\mathbb{Z}^m$, and the operations $+$ and $\cdot$ are over $\mathbb{Z}_k$. According to the characteristic value $\boldsymbol{q}(\boldsymbol{x})$, we can group the points in $[k]^n$ into equivalence classes. Specifically,

---

[2] When $t = 0$, then there is only two groups, the proof still holds.
[3] Since we need to take some ring operations on the index i, we index i by $\mathbb{Z}_k^m$ here instead of $[k]^m$.

for any $\boldsymbol{w} \in [k]^m$, let $Q(\boldsymbol{w})$ be the collection of points in $[k]^n$ which have characteristic value $\boldsymbol{w}$, i.e.

$$Q(\boldsymbol{w}) = \{(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}) \in [k]^n \mid \boldsymbol{q}(\boldsymbol{x}) = \boldsymbol{w}\}.$$

Arbitrarily choose a' different values $\boldsymbol{w}_1, \ldots, \boldsymbol{w}_{a'}$ from $[k]^m$, for example the first a' elements in the lexicographical order (recall that $0 \leq a' \leq k^m$), and let M be the collections of points which have one of these a' values as characteristic value and 0 as k-modulo parity, i.e.,

$$M = (Q(\boldsymbol{w}_1) \cup \cdots \cup Q(\boldsymbol{w}_{a'})) \cap \{(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}) \in [k]^n \mid \oplus(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}) = 0\}.$$

We arbitrarily partition the set $[a'] \times [r]$ (recall that $[a'] \times [r] \subset [k^m] \times [r]$ is the indices set of $\boldsymbol{x}$) into $(k-1)$ subsets $L_1 \sqcup L_2 \sqcup \cdots \sqcup L_{k-1}$ with the requirement that the cardinality $|L_1| = \cdots = |L_t| = a-1$ and $|L_{t+1}| = \cdots = |L_{k-1}| = a$. (Notice that $t(a-1) + (k-1-t)a = (k-1)a - t = a'r$.)

Based on these preparations, now we give the construction of the desired marking of $[k]^n$. There are three different types of lines: $(\boldsymbol{x}_{-(i,j)}, \boldsymbol{y}, \boldsymbol{z})$, $(\boldsymbol{x}, \boldsymbol{y}_{-i}, \boldsymbol{z})$, and $(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}_{-i})$, we mark them as follows:

1. for the line $(\boldsymbol{x}_{-(i,j)}, \boldsymbol{y}, \boldsymbol{z})$, there are two sub-cases:
   – $(\boldsymbol{x}_{-(i,j)}, \boldsymbol{y}, \boldsymbol{z}) \cap M \neq \emptyset$, i.e. on line $(\boldsymbol{x}_{-(i,j)}, \boldsymbol{y}, \boldsymbol{z})$ there exists some point belongs to set M. (by the condition that $\oplus(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}) = 0$, this point is unique, if exists). Suppose the point is $(\tilde{\boldsymbol{x}}, \boldsymbol{y}, \boldsymbol{z}) \in (\boldsymbol{x}_{-(i,j)}, \boldsymbol{y}, \boldsymbol{z}) \cap M$, and suppose that $(\tilde{\boldsymbol{x}}, \boldsymbol{y}, \boldsymbol{z}) \in Q(\boldsymbol{w}_{i_0})$ for some $i_0 \in [a']$, and $(i_0, j) \in L_s$ for some $s \in [k-1]$ (recall that $L_1, \ldots, L_{k-1}$ is a partition of $[a'] \times [r]$). Then we mark the point $(\tilde{\boldsymbol{x}} + s \cdot \boldsymbol{e}_{i,j}, \boldsymbol{y}, \boldsymbol{z}) \in (\boldsymbol{x}_{-(i,j)}, \boldsymbol{y}, \boldsymbol{z})$, where $\boldsymbol{e}_{i,j} = (0, \ldots, 0, 1, 0, \ldots, 0)$ is the unit vector in $[k]^{k^m r}$ for which only $x_{i,j} = 1$, and all other coordinates equal 0. The addition and multiplication are over $\mathbb{Z}_k$. This is also the unique point on this line which has $\oplus(\cdot) = s$;

   – otherwise $(\boldsymbol{x}_{-(i,j)}, \boldsymbol{y}, \boldsymbol{z}) \cap M = \emptyset$, mark the unique point $(\tilde{\boldsymbol{x}}, \boldsymbol{y}, \boldsymbol{z})$ on the line such that $\oplus(\tilde{\boldsymbol{x}}, \boldsymbol{y}, \boldsymbol{z}) = 0$.

2. for line $(\boldsymbol{x}, \boldsymbol{y}_{-i}, \boldsymbol{z})$ $(i \in [t])$, mark the unique point $(\boldsymbol{x}, \tilde{\boldsymbol{y}}, \boldsymbol{z})$ which satisfies $\oplus(\boldsymbol{x}, \tilde{\boldsymbol{y}}, \boldsymbol{z}) = i$. (recall that $1 \leq i \leq t \leq k-1$)

3. for line $(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}_{-i})$ $(i \in [a])$, mark the point $(\boldsymbol{x}, \boldsymbol{y}, \tilde{\boldsymbol{z}})$ which satisfies $\oplus(\boldsymbol{x}, \boldsymbol{y}, \tilde{\boldsymbol{z}}) = 0$.

We claim that the construction above is indeed a $[a, n-t]_k^n$. We need to check that each point $(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z})$ is marked either a times or $(n-t)$ times.

1. if $\oplus(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}) = 0$, then for each line $(\boldsymbol{x}, \boldsymbol{y}_{-i}, \boldsymbol{z})$, we never mark the point $(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z})$ (recall that we mark some point which has $\oplus(\cdot) = i \neq 0$). On the contrary, for each line $(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}_{-i})$, we always mark $(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z})$. For lines of the form $(\boldsymbol{x}_{-(i,j)}, \boldsymbol{y}, \boldsymbol{z})$, there are two sub-cases:
   – if $(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}) \in M$, then on the line $(\boldsymbol{x}_{-(i,j)}, \boldsymbol{y}, \boldsymbol{z})$ we mark the point $(\boldsymbol{x} + s \cdot \boldsymbol{e}_{i,j}, \boldsymbol{y}, \boldsymbol{z})$ for some $s > 0$ by the construction, which is not $(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z})$. Thus in this case, $(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z})$ is marked 0, 0, and a times in $\boldsymbol{x}$, $\boldsymbol{y}$ and $\boldsymbol{z}$'s directions respectively, hence a times in total;

   – if $(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}) \notin M$, then on the line $(\boldsymbol{x}_{-(i,j)}, \boldsymbol{y}, \boldsymbol{z})$ there is no point in M. Thus we marked the point with $\oplus(\cdot) = 0$, which is exactly point $(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z})$ itself. In this case, $(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z})$ is marked $k^m r$, 0, and a times in three groups of directions respectively, and $k^m r + 0 + a = n - t$ times in total.

   Therefore, $(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z})$ is marked either a or $(n-t)$ times.

2. if $\oplus(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}) = s$ for some $1 \le s \le t$. Among lines $(\boldsymbol{x}, \boldsymbol{y}_{-i}, \boldsymbol{z})$ $(1 \le i \le t)$, only on the line $(\boldsymbol{x}, \boldsymbol{y}_{-s}, \boldsymbol{z})$ we marked point $(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z})$. On each line $(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}_{-i})$ $(i \in [a])$, we never mark $(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z})$. By the definition of the characteristic function, $\boldsymbol{q}(\boldsymbol{x} - s \cdot \boldsymbol{e}_{i,j})$ are different for different i's (here we use the fact that k is a prime, hence s is coprime to k and has an inverse in $\mathbb{Z}_k$). Therefore there are exactly $a' \times r$ different pairs of (i, j) such that line $(\boldsymbol{x}_{-(i,j)}, \boldsymbol{y}, \boldsymbol{z})$ contains a point $(\boldsymbol{x} - s \cdot \boldsymbol{e}_{i,j}, \boldsymbol{y}, \boldsymbol{z}) \in M$. On exactly $|L_s| = a - 1$ lines of these $a' \times r$ lines, point $(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z})$ is marked. On all other lines, there is no point belong to M, thus we only mark the point with $\oplus(\cdot) = 0$. Thus the point $(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z})$ is marked $(a - 1)$, 1 and 0 times in $\boldsymbol{x}$, $\boldsymbol{y}$, and $\boldsymbol{z}$'s directions, respectively, and in total a times.

3. if $\oplus(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}) = s$ for some $s > t$. It is similar to the case above, except that we never mark point $(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z})$ on lines of form $(\boldsymbol{x}, \boldsymbol{y}_{-i}, \boldsymbol{z})$, and on $|L_s| = a$ lines of form $(\boldsymbol{x}_{-(i,j)}, \boldsymbol{y}, \boldsymbol{z})$ we mark $(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z})$. Therefore in this case $(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z})$ is also marked exactly a times.

$\square$

Theorem 4. *If k is a prime, $0 < b \le n$, and $\left(\frac{kb-n}{b}\right) k^{n-1}$ is an integer, then we have $[0, b]_k^n$.*

Proof. Suppose $\gcd(b, n) = r$, since k is a prime number and $\left(\frac{kb-n}{b}\right) k^{n-1} \in \mathbb{Z}$, we have that $b = rk^m$, $n = rn'$ for some non-negative integer m and n'. By the following Proposition, it suffices to prove the $r = 1$ case.

Proposition 3 ([2]). *Given $[0, b]_k^n$, then for every r, we have $[0, br]_k^{rn}$.*

Since $b \le n \le kb$, let $n = tb + h$, where $1 \le t < k$ and $0 \le h \le b$. We partition the n coordinates into three groups, each of which contains k^m, $(t - 1)b$, and h coordinates (note that now $b = k^m$), respectively[4]. We represent each point in $[k]^n$ by $(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z})$, where $\boldsymbol{x} \in [k]^{k^m}$, $\boldsymbol{y} \in [k]^{(t-1)b}$, and $\boldsymbol{z} \in [k]^h$. Notations $(\boldsymbol{x}_{-i}, \boldsymbol{y}, \boldsymbol{z})$, $(\boldsymbol{x}, \boldsymbol{y}_{-(i,j)}, \boldsymbol{z})$ and $(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}_{-i})$ are similarly defined as in the previous proof (note that for $(\boldsymbol{x}, \boldsymbol{y}_{-(i,j)}, \boldsymbol{z})$, the indexes $i \in [t - 1], j \in [b]$).

Similarly we define the characteristic function $\boldsymbol{q} : [k]^{k^m} \to [k]^m$ as follows:

$$\boldsymbol{q}(\boldsymbol{x}) = \sum_{\boldsymbol{i} = (i_1, \dots, i_m) \in \mathbb{Z}_k^m} x_i \cdot \boldsymbol{i}.$$

Let $Q(\boldsymbol{w}) = \{(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}) \in [k]^n \mid \boldsymbol{q}(\boldsymbol{x}) = \boldsymbol{w}\}$ as usual, and the notation of $\boldsymbol{i}$ and $\cdot, +$ are the same as in the proof of Theorem 3. We arbitrarily choose h different values $\boldsymbol{w}_1, \boldsymbol{w}_2, \dots, \boldsymbol{w}_h$ from $[k]^m$, and let

$$M = (Q(\boldsymbol{w}_1) \cup \dots \cup Q(\boldsymbol{w}_h)) \cap \{(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}) \in [k]^n \mid \oplus(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}) = 0\}.$$

Now we describe the marking of the line (for some fixed point $(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z})$):

1. For the line $(\boldsymbol{x}_{-i}, \boldsymbol{y}, \boldsymbol{z})$, if there exists a point $(\tilde{\boldsymbol{x}}, \boldsymbol{y}, \boldsymbol{z}) \in M$ on it, then we mark this point. Otherwise we mark the unique point $(\tilde{\boldsymbol{x}}, \boldsymbol{y}, \boldsymbol{z})$ with k-modulo parity $\oplus(\tilde{\boldsymbol{x}}, \boldsymbol{y}, \boldsymbol{z}) = 1$.

2. For line $(\boldsymbol{x}, \boldsymbol{y}_{-(i,j)}, \boldsymbol{z})$ $(i \in [t - 1], j \in [b])$, we mark the point $(\boldsymbol{x}, \tilde{\boldsymbol{y}}, \boldsymbol{z})$ on the line with parity $\oplus(\boldsymbol{x}, \tilde{\boldsymbol{y}}, \boldsymbol{z}) = i + 1$.

3. On line $(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}_{-i})$ $(i \in [h])$, we mark the unique point $(\boldsymbol{x}, \boldsymbol{y}, \tilde{\boldsymbol{z}})$ with parity $\oplus(\boldsymbol{x}, \boldsymbol{y}, \tilde{\boldsymbol{z}}) = 1$.

We claim that the construction above is a $[0, b]_k^n$. We need to verify that each point $(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z})$ is marked either $b = k^m$ times or unmarked. There are three cases:

1. $\oplus(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}) = 0$.

---

[4] If $t = 1$ or $h = 0$, one of the group probably vanishes, while the proof still holds.

– if $(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}) \in M$. The point is only marked by lines of the form $(\boldsymbol{x}_{-i}, \boldsymbol{y}, \boldsymbol{z})$. There are b such lines;
– otherwise, the point is never marked.

2. $\oplus(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}) = 1$. $\boldsymbol{q}(\boldsymbol{x} - \boldsymbol{e}_i)$ are pairwise different, thus on exactly $(b - h)$ lines $(\boldsymbol{x}_{-i}, \boldsymbol{y}, \boldsymbol{z})$ there is no point in M. On these lines $(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z})$ is marked. All the lines of form $(\boldsymbol{x}, \boldsymbol{y}_{-i}, \boldsymbol{z})$ will not mark the point $(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z})$, and all h lines of form $(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}_{-i})$ will mark this point. Thus $(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z})$ is marked b times in total.

3. $2 \leq \oplus(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}) \leq t$. The point is marked on all the line of the form $(\boldsymbol{x}, \boldsymbol{y}_{-(i,j)}, \boldsymbol{z})$ where $i = \oplus(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}) - 1$ and $j \in [b]$. There are b such lines.

4. $\oplus(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}) > t$. The point is not marked.

$\square$

Now we are ready to present our main theorem.

Theorem 1 (Restated) *For prime k and $0 \leq a < b \leq n$, there exists a marking of lines in $[k]^n$ so that each point is marked either a times or b times if and only if there are nonnegative integers s and t so that $s + t = k^n$ and $as + bt = nk^{n-1}$.*

Proof. The necessary part of the theorem is trivial and has been shown in the preliminary section of the introduction. The proof of sufficiency is an induction on n by essentially using Theorem 3 and 4 as base steps.

The $n = 1$ case is obvious. Assume that for any $n \leq m - 1$, the theorem holds. Now we prove the theorem for $n = m$. There are three possible occasions:

1. If $a = 0$, then by Theorem 4 the theorem holds.
2. If $b > m - k$, by Theorem 3 the theorem holds.
3. If $a > 0$ and $b \leq m - k$. Assume

$$s = \frac{k^{m-1}(kb - m)}{b - a}, \quad t = \frac{k^{m-1}(m - ka)}{b - a}$$

are both nonnegative integers. We claim that both

$$s' = \frac{k^{m-k-1}[k(b-1) - (m-k)]}{b - a} \quad \text{and} \quad t' = \frac{k^{m-k-1}[(m-k) - k(a-1)]}{b - a}$$

are nonnegative integers. Suppose that $b - a = rk^d$, where $\gcd(r, k) = 1$. Thus we have that $r | m - ka$, since $r | k^{m-1}(m - ka)$ and $\gcd(r, k^{m-1}) = 1$. Since

$$k^d \leq b - a \leq m - k - 1,$$

we have that $d \leq m - k - 1$ and $k^d | k^{m-k-1}$. Then $rk^d | k^{m-k-1}(m - ka)$, that is

$$b - a | k^{m-k-1}\left((m-k) - k(a-1)\right).$$

Similar argument shows that

$$b - a | k^{m-k-1}\left(k(b-1) - (m-k)\right).$$

Since $a > 0$ and $b \leq m - k$, we still have $0 \leq a - 1 \leq b - 1 \leq m - k$.
By invoking inductive hypothesis, we have that $[a-1, b-1]_k^{m-k}$ exists. Therefore, by applying Proposition 2 we have that $[a, b]_k^m$ exists.

$\square$

3 $[0, b]_k^n$ for General k

In this section we prove the conjecture when $a = 0$ for general k. Before proving the theorem, we provide a crucial building block of the proof, which can be viewed as a generalization of the characteristic function defined in Theorem 4.

Proposition 4. *If b and k are two integers so that each prime factor of b is also a prime factor of k, that is, k and b can be decomposed as $k = p_1^{\alpha_1} \cdots p_l^{\alpha_l}$ and $b = p_1^{\beta_1} \cdots p_l^{\beta_l}$, for integers $\alpha_j > 0$ and $\beta_j \geq 0$, (thus $[k]$ and $[b]$ can be viewed as $\mathbb{Z}_{p_1}^{\alpha_1} \times \cdots \times \mathbb{Z}_{p_l}^{\alpha_l}$ and $\mathbb{Z}_{p_1}^{\beta_1} \times \cdots \times \mathbb{Z}_{p_l}^{\beta_l}$, respectively), then there exists a linear characteristic function $\boldsymbol{q} : [k]^b \to [b]$ with the following property:*

There exists $s^* \in [k]$, so that for any $\boldsymbol{x} \in [k]^b$, there is a unique index $i \in [b]$ satisfying that $\boldsymbol{q}(\boldsymbol{x} - s^* \cdot \boldsymbol{e}_i) = \boldsymbol{0}$, where $s^* \cdot \boldsymbol{e}_i$ is the vector in $[k]^b$ with all entries 0 except that the i-th is s^*.

Proof. Define the a linear operator $\circledast : [k] \times [b] \to [b]$, as a generalization of multiplication of scalar and vector, as follows:

Suppose that $\boldsymbol{u} = (\boldsymbol{u}^1, \ldots, \boldsymbol{u}^l) \in \mathbb{Z}_{p_1}^{\alpha_1} \times \cdots \times \mathbb{Z}_{p_l}^{\alpha_l} (\cong [k])$, where each $\boldsymbol{u}^j \in \mathbb{Z}_{p_j}^{\alpha_j}$ can be represented as $\boldsymbol{u}^j = (u_{\alpha_j - 1}^j, \ldots, u_0^j)$. Similarly, suppose $\boldsymbol{v} = (\boldsymbol{v}^1, \ldots, \boldsymbol{v}^l) \in \mathbb{Z}_{p_1}^{\beta_1} \times \cdots \times \mathbb{Z}_{p_l}^{\beta_l} (\cong [b])$. Define

$$\boldsymbol{u} \circledast \boldsymbol{v} = (u_0^1 \cdot \boldsymbol{v}^1, u_0^2 \cdot \boldsymbol{v}^2, \ldots, u_0^l \cdot \boldsymbol{v}^l),$$

where $u_0^j \cdot \boldsymbol{v}^j$ is the multiplication of a scalar and a vector over $\mathbb{Z}_{p_j}$.

Based on this $\circledast$ operator, define $\boldsymbol{q} : [k]^b \to [b]$ as follows:[5]

$$\boldsymbol{q}(\boldsymbol{x}) = \sum_{\boldsymbol{i} \in [b] \cong \mathbb{Z}_{p_1}^{\alpha_1} \times \cdots \times \mathbb{Z}_{p_l}^{\alpha_l}} \boldsymbol{x}_i \circledast \boldsymbol{i}.$$

Now we prove that $\boldsymbol{q}(\boldsymbol{x})$ indeed has the desired property. Let $\boldsymbol{s}^* = (1, \ldots, 1) \in \mathbb{Z}_{p_1}^{\alpha_1} \times \ldots \times \mathbb{Z}_{p_l}^{\alpha_l} (\cong [k])$ be the element with each entry 1[6], since $\circledast$ is a linear operator with addition over $\mathbb{Z}_{p_1}^{\alpha_1} \times \ldots \times \mathbb{Z}_{p_l}^{\alpha_l}$, we have that

$$\boldsymbol{q}(\boldsymbol{x} - s^* \boldsymbol{e}_i) = \boldsymbol{q}(\boldsymbol{x}) - \boldsymbol{q}(s^* \boldsymbol{e}_i) = \boldsymbol{q}(\boldsymbol{x}) - \boldsymbol{s}^* \circledast \boldsymbol{i}.$$

Since $\boldsymbol{s}^*$ is a vector with every entry 1, $\boldsymbol{s}^* \circledast \boldsymbol{i} = \boldsymbol{i}$, hence the equation $\boldsymbol{q}(\boldsymbol{x} - s^* \boldsymbol{e}_i) = 0$ only holds for $\boldsymbol{i} = \boldsymbol{q}(\boldsymbol{x})$. $\square$

Now we prove Theorem 2 by using the above characteristic function $\boldsymbol{q}(\cdot)$.

Proof of Theorem 2. We only need to prove the sufficient part. Suppose that $s = \left(\frac{kb-n}{b}\right) k^{n-1}$ is a nonnegative integer. We factor $b = dr$, where r is coprime with k and each prime factor of d is a prime factor of k. Thus we have $r | kb - n$, and since $d \leq n$, we have $d | k^{n-1}$. By Proposition 3 it is sufficient to prove the $r = 1$ case.

Suppose $n = tb + h$, where $1 \leq t < k$ and $0 \leq h \leq b$. Similar to the approach of proving Theorem 4, we partition the n coordinates into three groups, each of which contains b, $(t-1)b$ and h coordinates, respectively. We represent a point in $[k]^n$ by $(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z})$, where $\boldsymbol{x} \in [k]^b$, $\boldsymbol{y} \in [k]^{(t-1)b}$, and $\boldsymbol{z} \in [k]^h$. Let $\boldsymbol{q}(\boldsymbol{x})$ be the characteristic function which satisfies the condition in Proposition 4. Let $Q(\boldsymbol{w}) = \{(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}) \in [k]^n \mid \boldsymbol{q}(\boldsymbol{x}) = \boldsymbol{w}\}$ as before. We arbitrarily choose h different values $\boldsymbol{w}_1, \ldots, \boldsymbol{w}_h$ from $[b] \cong \mathbb{Z}_{p_1}^{\beta_1} \times \cdots \times \mathbb{Z}_{p_l}^{\beta_l}$ (since $0 \leq h \leq b$), and let

$$M = (Q(\boldsymbol{w}_1) \cup \cdots \cup Q(\boldsymbol{w}_h)) \cap \{(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}) \mid \oplus(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}) = \boldsymbol{0}\}.[7]$$

---

[5] Here we view $\boldsymbol{x}_i$ a vector in $[k] \cong \mathbb{Z}_{p_1}^{\alpha_1} \times \ldots \times \mathbb{Z}_{p_l}^{\alpha_l}$ as in the definition of $\circledast$.

[6] Since s^* could be viewed both as an element in $[k]$ and a vector in $\mathbb{Z}_{p_1}^{\alpha_1} \times \ldots \times \mathbb{Z}_{p_l}^{\alpha_l}$, we use s^* and $\boldsymbol{s}^*$ correspondingly.

[7] We redefine $\oplus(\boldsymbol{a})$ as $a_1 + a_2 + \cdots + a_n$, the addition is over the group $\mathbb{Z}_{p_1}^{\alpha_1} \times \cdots \times \mathbb{Z}_{p_l}^{\alpha_l} (\cong [k])$.

Now we describe the marking of lines. Considering the set $[k]$, $\mathbf{0}$ and $\boldsymbol{s}^*$ are two special elements in it. There are $k - 2 \geq t - 1$ elements left. Let τ be an arbitrary injective function that maps $[t-1]$ to $[k] \setminus \{\mathbf{0}, \boldsymbol{s}^*\}$. Thus $|\tau([t-1])| = t - 1$.

1. For line $(\boldsymbol{x}_{-i}, \boldsymbol{y}, \boldsymbol{z})$ $(i \in [b])$, if there exists a point $(\tilde{\boldsymbol{x}}, \boldsymbol{y}, \boldsymbol{z}) \in M$ on it, then we mark this point. Otherwise we mark the unique point $(\tilde{\boldsymbol{x}}, \boldsymbol{y}, \boldsymbol{z})$ so that $\oplus(\tilde{\boldsymbol{x}}, \boldsymbol{y}, \boldsymbol{z}) = \boldsymbol{s}^*$.

2. For line $(\boldsymbol{x}, \boldsymbol{y}_{-(i,j)}, \boldsymbol{z})$ $(i \in [t-1], j \in [b])$, we mark the point $(\tilde{\boldsymbol{x}}, \boldsymbol{y}, \boldsymbol{z})$ on the line so that $\oplus(\tilde{\boldsymbol{x}}, \boldsymbol{y}, \boldsymbol{z}) = \tau(i)$.

3. On line $(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}_{-i})$ $(i \in [h])$, we always mark the unique point $(\tilde{\boldsymbol{x}}, \boldsymbol{y}, \boldsymbol{z})$ with $\oplus(\tilde{\boldsymbol{x}}, \boldsymbol{y}, \boldsymbol{z}) = \boldsymbol{s}^*$.

Next we prove that each point $(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z})$ is marked either b times or $a = 0$ time. There are three cases:

1. $\oplus(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}) = 0$. On lines of form $(\boldsymbol{x}, \boldsymbol{y}_{-(i,j)}, \boldsymbol{z})$ or $(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}_{-i})$, this point will never get marked.
   - if $(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}) \in M$. The point is marked by all lines of form $(\boldsymbol{x}_{-i}, \boldsymbol{y}, \boldsymbol{z})$. There are exactly b such lines;
   - otherwise, the point is never marked.

2. $\oplus(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}) = \boldsymbol{s}^*$. By Proposition 4, $\boldsymbol{q}(\boldsymbol{x} - \boldsymbol{s}^* \boldsymbol{e}_i)$ are pairwise different. On exactly h lines of form $(\boldsymbol{x}_{-i}, \boldsymbol{y}, \boldsymbol{z})$, there is a point in M. Therefore on $(b - h)$ lines of such form, $(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z})$ will be marked. All the lines of form $(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}_{-i})$ will mark this point as well. On lines of form $(\boldsymbol{x}, \boldsymbol{y}_{-(i,j)}, \boldsymbol{z})$, this point will not be marked. Thus it is marked $(b - h) + h = b$ times in total.

3. $\oplus(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}) \in \tau([t-1])$. The point is marked on all the line of the form $(\boldsymbol{x}, \boldsymbol{y}_{-(i,j)}, \boldsymbol{z})$ where $i = \tau^{-1}(\oplus(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}))$. Thus it is marked b times.

4. $\oplus(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}) \in [k] \setminus (\tau([t-1]) \cup \{\mathbf{0}, \boldsymbol{s}^*\})$. The point is never marked.

$\square$

4   Conclusion and Remarks

In this work we investigate a conjecture of Butler and Graham on marking lines of $[k]^n$. We proved the necessary and sufficient condition of the existence of $[a, b]_k^n$ for the case when k is a prime and the case when $a = 0$ with general k. A natural open question is how to settle the remaining case of the conjecture, $[a, n-t]_k^n$ $(t < k)$ for general k. The proof of Theorem 3 actually can be generalized to the following case when k is a prime power (with an additional constrain that $(n-t-a)$ contains more prime factors than k).

Theorem 5. $[a, n-t]_k^n$ exists if $k = p^m$, $n = t + a + rp^s$, $n - ka = ru$ and $s \geq m$.

The proof utilized the property of field $\mathbb{F}_{p^s}$. It is essentially similar to the proof of Theorem 2 and we will put it in appendix. It is an interesting question to know whether the method here can be further generalized. The difficulty is that during this generalization, the strong symmetric property cannot be maintained.

References

1. Joe Buhler, Steve Butler, Ron Graham, and Eric Tressler. Hypercube orientations with only two in-degrees. *Journal of Combinatorial Theory, Series A*, 118:1695–1702, 2011.
2. Steve Butler and Ron Graham. A note on marking lines in $[k]^n$. *Designs, Codes and Cryptography*, 2011.

3. Steve Butler, Mohammad T. Hajiaghayi, Robert D. Kleinberg, and Tom Leighton. Hat guessing games. *SIAM J. Discrete Math.*, 22(2):592–605, 2008.
4. Todd T. Ebert. *Applications of recursive operators to randomness and complexity.* PhD thesis, University of California at Santa Barbara, 1998.
5. Uriel Feige. On optimal strategies for a hat game on graphs. *SIAM Journal of Discrete Mathematics*, 24(3):782–791, 2010.
6. H. Iwasawa. Presentation given at the ninth gathering 4 gardner (g4g9). March 2010.
7. Hendrik W. Lenstra and Gadiel Seroussi. On hats and other covers. In *Proceedings of IEEE International Symposium on Information Theory*, page 342, 2002.
8. Tengyu Ma, Xiaoming Sun, and Huacheng Yu. A new variation of hat guessing games. In *Proceedings of 17th Annual International Computing and Combinatorics Conference*, pages 616–626, 2011.
9. Maura B . Peterson and Douglas R. Stinson. Yet another hat game. *The Electronic Journal of Combinatorics*, 17(1):#R86, 2010.

Appendix

Proof (Theorem 5(sketch)). We construct a marking of lines in $[k]^n$ so that each point is marked either $(n - t)$ times or a times. First, similar to in the proof of Theorem 3, we partition the $n = a + t + p^s r$ dimensions into three groups, each of which contains $p^s r$, t, and a coordinates respectively, and represent each point in $[k]^n$ by $(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z})$ where $\boldsymbol{x} \in [k]^{p^s r}$, $\boldsymbol{y} \in [k]^t$, and $\boldsymbol{z} \in [k]^a$. Then, we index $\boldsymbol{x}$ by a pair $(i, j) \in \mathbb{F}_p^s \times [r]$, i.e. $x_{i,j} \in [k]$ are the coordinates of $\boldsymbol{x}$ (where $i \in \mathbb{F}_p^s, j \in [r]$)[8]. We define lines $(\boldsymbol{x}_{-(i,j)}, \boldsymbol{y}, \boldsymbol{z})$, $(\boldsymbol{x}, \boldsymbol{y}_{-i}, \boldsymbol{z})$ and $(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}_{-i})$ in a similar way.

For each $\boldsymbol{x} \in [k]^{p^s r}$, we define the *characteristic function* $q : [k]^{p^s r} \to \mathbb{F}_{p^s}$ in a slightly different way:

$$q(\boldsymbol{x}) = \sum_{i \in \mathbb{F}_{p^s}} q' \left(\sum_{j=1}^{r} x_{i,j} \right) \cdot i \tag{2}$$

q' is an arbitrary function that maps $\mathbb{F}_{p^m}$ to $\mathbb{F}_{p^s}$. $q'(\sum_{j=1}^{r} x_{i,j})$ is an element in $\mathbb{F}_{p^s}$.

The way of marking lines and the proof of correctness is the same as that in the proof of Theorem 3. □

---

[8] Here we use a different arithmetic system for i.