On a conjecture of Butler and Graham

Tengyu Ma · Xiaoming Sun · Huacheng Yu

Received: 23 November 2011 / Revised: 5 March 2012 / Accepted: 8 March 2012 / Published online: 6 April 2012 © Springer Science+Business Media, LLC 2012

Abstract Motivated by a hat guessing problem proposed by Iwasawa, Butler and Graham made the following conjecture on the existence of a 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 nonnegative integers \(s\) and \(t\) such that \(s + t = kn\) 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 \(k\).

Keywords Hat guessing games · Marking coordinate lines · Characteristic function

Mathematics Subject Classification 00A08 · 97A20 · 94B05

1 Introduction

In Butler and Graham [2] considered the problem of the existence of certain way of marking coordinate lines in \([k]^n = \{1, 2, \ldots, k\}^n\). 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 the following.

Conjecture 1 (Butler and 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

\(^1\) For convenience, we use line to indicate coordinate line throughout this paper.
only if there are nonnegative integers $s$ and $t$ satisfying the linear equations $s + t = kn$ and $as + bt = nk^{n-1}$.

The “only if” part of the conjecture is straightforward, leaving as crucial the construction of a marking of lines in $[k]^n$ with the desired properties. Buhler et al. [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 $t$ satisfying the linear equations $s + t = kn$ 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 $s + t = kn$ 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 Sect. 2). It turns out that the most 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 (Theorems 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. We equip the set $[k]$ with some particular algebraic structure firstly, and then introduce a linear characteristic function $q$ which maps points in $[k]^n$ to points in some low-dimensional space $[k]^m$. This function $q$ has some good symmetric property, so that we can mark the points in $[k]^n$ according to their low-dimensional images under $q$. Informally speaking, for any fixed $s$, any point $x \in [k]^n$, and any value $v$ in the range of $q$, there exists a unique direction along which by moving from $x$ with distance $s$, we can reach a point with value $v$. By 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 et al. [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. Paterson and Stinson [9] investigated the case that each player can see hats in front of him and they guess one by one. Recently Ma et al. [8] proposed a variation which allow to answer “unknown” and require at least \( k \) correct guesses for winning condition.

**Notations and preliminaries**

Let \([k] = \{1, 2, \ldots, k\}\), and \([k]^n = [k] \times \cdots \times [k] \)We use \([a, b]_k^n\) as a shorthand for a realization of 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 tuples and multi-valued functions. For a \( n \)-tuple \( x = (x_1, \ldots, x_n) \), define the \( k \)-modulo parity function \( \oplus(x) = x_1 + x_2 + \cdots + x_n \mod k \). We denote by \( x_{-i} \) the line \((x_1, \ldots, x_i-1, *, x_{i+1}, \ldots, x_n)\), i.e.

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

Let \( s \) and \( t \) be the number of points that are marked \( a \) times and \( b \) times. By counting the total number of points in \([k]^n\) and the total number of times of markings, the necessary condition in the conjecture follows straightforwardly.

**Proposition 1** ([1]) If we have \([a, b]_k^n\), then the following system has nonnegative integer solution for \( s \) and \( t \).

\[
\begin{align*}
s + t &= k^n, \\
as + bt &= k^{n-1}n.
\end{align*}
\]

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

The rest of the paper is organized as follows: In Sect. 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 Sect. 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 (Theorems 3 and 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 \((\frac{n-t}{n-t-a}) k^{n-1}\) 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 \(r | (k-1)a-t\). Let \((k-1)a-t = r a'\), where

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

Thus, \(n = t + a + k^m r\) and \((k-1)a-t = r a'\), 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. In the construction, we view set \([k]\) as the group \(\mathbb{Z}_k\), so that we can utilize the property of the operations on it. Observe that the group introduced is purely for the design of markings, while the requirement of the markings remains the same. However, for clarification, we use \(\mathbb{Z}^n_k\) instead of \([k]^n\) as our target space (vector space) for marking throughout this proof. Thus by an arbitrary bijective map between \(\mathbb{Z}_k\) and \([k]\), we can transform a marking of \(\mathbb{Z}^n_k\) to a marking of \([k]^n\) with the same property.

Firstly, 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 \(\mathbb{Z}^n_k\) by \((x, y, z)\) where \(x \in \mathbb{Z}^{k^m r}_k, y \in \mathbb{Z}^t_k,\) and \(z \in \mathbb{Z}^a_k\). Furthermore, we index \(x\) by a pair \((i, j) \in \mathbb{Z}^m_k \times [r]\), i.e. \(x_{i, j} \in \mathbb{Z}_k\) are the coordinates of \(x\) (where \(i \in \mathbb{Z}_k^m, j \in [r]\)). Denote by \((x_{-i,j}, y, z)\) the lines of \(\mathbb{Z}^n_k\) for which all the coordinates are fixed except the coordinate \((i, j)\) of \(x\), i.e.

\[
(x_{-i,j}, y, z) = \{(\tilde{x}, \tilde{y}, \tilde{z}) \in \mathbb{Z}^n_k | \tilde{y} = y, \tilde{z} = z, \quad \forall (i', j') \neq (i, j) \tilde{x}_{i', j'} = x_{i', j'}, \tilde{x}_{i, j} \in \mathbb{Z}_k\}
\]

Similarly \((x, y_{-i}, z)\) \((i \in [r])\) is a line of \(\mathbb{Z}^n_k\) which the \(i\)-th coordinate of \(y\) is unfixed, \((x, y, z_{-i})\) \((i \in [a])\) is a line which the \(i\)-th coordinate of \(z\) is unfixed.

For each \(x \in \mathbb{Z}^{k^m r}_k\), define the characteristic function \(q : \mathbb{Z}^{k^m r}_k \to \mathbb{Z}^m_k\) as follows:

\[
q(x) = \sum_{i=(i_1, \ldots, i_m) \in \mathbb{Z}^m_k} \left(\sum_{j=1}^r x_{i, j}\right) \cdot i
\]

(1)

where \(i\) is \(k\)-based representation of \(i\) in \(\mathbb{Z}_k^m\), and the operations + and · are over \(\mathbb{Z}_k\). According to the characteristic value \(q(x)\), we can group the points in \(\mathbb{Z}^n_k\) into equivalence classes. Specifically, for any \(w \in \mathbb{Z}^m_k\), let \(Q(w)\) be the collection of points in \(\mathbb{Z}^n_k\) which have characteristic value \(w\), i.e.

\[
Q(w) = \{(x, y, z) \in \mathbb{Z}^n_k \mid q(x) = w\}.
\]

Arbitrarily choose \(a'\) different values \(w_1, \ldots, w_{a'}\) from \(\mathbb{Z}_k^m\), for example the first \(a'\) elements in the lexicographical order (recall that \(0 \leq a' \leq k^m\)), and let \(W = \{w_1, \ldots, w_{a'}\}\), and \(M\) be the collections of points which have one of these \(a'\) values as characteristic value and 0 as \(k\)-modulo parity, i.e.,

\[
M = (Q(w_1) \cup \cdots \cup Q(w_{a'})) \cap \{(x, y, z) \in \mathbb{Z}^n_k \mid \oplus (x, y, z) = 0\}.
\]

We arbitrarily partition the set \(W \times [r]\) (recall that \(W \times [r] \subset \mathbb{Z}_k^m \times [r]\) is the indices set of \(x\)) into \((k-1)\) subsets \(L_1 \sqcup L_2 \sqcup \cdots \sqcup L_{k-1}\) with the requirement that the cardinality

\(^2\) When \(t = 0\), then there is only two groups, the proof still holds.
Based on these preparations, now we give the construction of the desired marking of $\mathbb{Z}^n_k$.

There are three different types of lines: $(x_{-(i,j)}, y, z)$, $(x, y_{-i}, z)$, and $(x, y, z_{-i})$. We mark them as follows:

1. for the line $(x_{-(i,j)}, y, z)$, there are two sub-cases:
   - $(x_{-(i,j)}, y, z) \cap M \neq \emptyset$, i.e. on line $(x_{-(i,j)}, y, z)$ there exists some point belonging to set $M$ (by the condition that $\oplus(x, y, z) = 0$, this point is unique, if exists). Suppose the point is $(\tilde{x}, y, z) \in (x_{-(i,j)}, y, z) \cap M$, and $(\tilde{x}, y, z) \in Q(w_{i0})$ for some $i_0 \in [a']$, and $(w_{i0}, j) \in L_s$ for some $s \in [k-1]$ (recall that $L_1, \ldots, L_{k-1}$ is a partition of $W \times [r]$). Then we mark the point $(\tilde{x} + s \cdot e_{i,j}, y, z) \in (x_{-(i,j)}, y, z)$, where $e_{i,j} = (0, \ldots, 0, 1, 0, \ldots, 0)$ is the unit vector in $\mathbb{Z}_k^{m_r}$ for which only $x_{i,j} = 1$, and all other coordinates equal 0. This is also the unique point on this line which has $\oplus(\cdot) = s$;
   - otherwise $(x_{-(i,j)}, y, z) \cap M = \emptyset$, mark the unique point $(\tilde{x}, y, z)$ on the line such that $\oplus(\tilde{x}, y, z) = 0$.

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

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

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

1. If $\oplus(x, y, z) = 0$, then for each line $(x, y_{-i}, z)$, we never mark the point $(x, y, z)$ (recall that we mark some point which has $\oplus(\cdot) = i \neq 0$). On the other hand, for each line $(x, y, z_{-i})$, we always mark $(x, y, z)$. For lines of the form $(x_{-(i,j)}, y, z)$, there are two sub-cases:
   - If $(x, y, z) \in M$, then on the line $(x_{-(i,j)}, y, z)$ we mark the point $(x + s \cdot e_{i,j}, y, z)$ for some $s > 0$ by the construction, which is not $(x, y, z)$. Thus in this case, $(x, y, z)$ is marked 0, 0, and $a$ times in $x, y$ and $z$’s directions respectively, hence $a$ times in total;
   - if $(x, y, z) \notin M$, then on the line $(x_{-(i,j)}, y, z)$ there is no point in $M$. Thus we marked the point with $\oplus(\cdot) = 0$, which is exactly point $(x, y, z)$ itself. In this case, $(x, y, z)$ 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, $(x, y, z)$ is marked either $a$ or $(n-t)$ times.

2. if $\oplus(x, y, z) = s$ for some $1 \leq s \leq t$. Among lines $(x, y_{-i}, z)$ ($1 \leq i \leq t$), only on the line $(x, y_{-s}, z)$ did we mark $(x, y, z)$. On each line $(x, y, z_{-i}) (i \in [a])$, we never mark $(x, y, z)$. By the definition of the characteristic function, $q(x - s \cdot e_{i,j})$ 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 $(x_{-(i,j)}, y, z)$ contains a point $(x - s \cdot e_{i,j}, y, z) \in M$. On exactly $|L_s| = a - 1$ lines of these $a' \times r$ lines, point $(x, y, z)$ is marked. On all other lines, there is no point belonging to $M$, thus we only mark the point with $\oplus(\cdot) = 0$. Thus the point $(x, y, z)$ is marked $(a-1)$, 1 and 0 times in $x, y$, and $z$’s directions, respectively, and in total $a$ times.

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

\[\square\]

Now we have proved one base case. To prove the other, we need the following result from [2].

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

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

**Proof** Suppose \(\gcd(b, n) = r\), since \(k\) is a prime number and \((\frac{kb-n}{p})k^{n-1}\) is in \(\mathbb{Z}\), we have that \(b = rk^m, n = rm\) for some non-negative integer \(m\) and \(n\). By Proposition 3, it suffices to prove the \(r = 1\) case.

Similar to the previous proof, we here again regard \([k]\) as \(\mathbb{Z}_k\), that is we are marking the lines in \(\mathbb{Z}_k^n\). Since \(b \leq n \leq kb\), let \(n = tb + h\), where \(1 \leq t < k\) and \(0 \leq h \leq b\). 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. We represent each point in \(\mathbb{Z}_k^n\) by \((x, y, z)\), where \(x \in \mathbb{Z}_k^{km}, y \in \mathbb{Z}_k^{(t-1)b}\), and \(z \in \mathbb{Z}_k^h\). Notations \((x_{-i}, y, z), (x, y_{-(i,j)}), z)\) and \((x, y, z_{-i})\) are similarly defined as in the previous proof (for \((x_{-i}, y, z), i \in \mathbb{Z}_k^{km}\), for \((x, y_{-(i,j)}), z)\), the indices \(i \in [t-1], j \in [b]\), and for \((x, y, z_{-i})\), \(i \in [h]\).

Similarly we define the characteristic function \(q: \mathbb{Z}_k^m \to \mathbb{Z}_k^m\) as follows:

\[
q(x) = \sum_{i=(i_1, \ldots, i_m) \in \mathbb{Z}_k^m} x_i \cdot i.
\]

Let \(Q(w) = \{(x, y, z) \in \mathbb{Z}_k^n \mid q(x) = w\}\) as usual, and the notation of \(i\) and \(\cdot, +\) are the same as in the proof of Theorem 3. We arbitrarily choose \(h\) different values \(w_1, w_2, \ldots, w_h\) from \(\mathbb{Z}_k^m\), and let

\[
M = (Q(w_1) \cup \cdots \cup Q(w_h)) \cap \{(x, y, z) \in \mathbb{Z}_k^n \mid \oplus(x, y, z) = 0\}.
\]

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

1. For the line \((x_{-i}, y, z)\), if there exists a point \((\tilde{x}, y, z) \in M\) on it, then we mark this point. Otherwise we mark the unique point \((\tilde{x}, y, z)\) with \(\oplus(\tilde{x}, y, z) = 1\).
2. For line \((x, y_{-(i,j)}, z)\) (\(i \in [t-1], j \in [b]\)), we mark the point \((x, \tilde{y}, z)\) on the line with parity \(\oplus(x, \tilde{y}, z) = i + 1\).
3. On line \((x, y, z_{-i})\) (\(i \in [h]\)), we mark the unique point \((x, \tilde{y}, z)\) with parity \(\oplus(x, \tilde{y}, z) = 1\).

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

1. \(\oplus(x, y, z) = 0\).
   - if \((x, y, z) \in M\). The point is only marked by lines of the form \((x_{-i}, y, z)\). There are \(b\) such lines;
   - otherwise, the point is never marked.
2. \(\oplus(x, y, z) = 1\). The \(q(x - e_i)\) are pairwise different, thus on exactly \((b - h)\) lines \((x_{-i}, y, z)\) there is no point in \(M\). On these lines \((x, y, z)\) is marked. All the lines of form \((x, y_{-i}, z)\) will not mark the point \((x, y, z)\), and all \(h\) lines of form \((x, y, z_{-i})\) will mark this point. Thus \((x, y, z)\) is marked \(b\) times in total.

\[^3\] If \(t = 1\) or \(h = 0\), the corresponding group of indices vanishes, while the proof still holds.
(3) $2 \leq \oplus(x, y, z) \leq t$. The point is marked on all the lines of the form $(x, y_{-(i,j)}, z)$ where $i = \oplus(x, y, z) - 1$ and $j \in [b]$. There are $b$ such lines.
(4) $\oplus(x, y, z) > t$. The point is not marked. \hfill \Box

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 Theorems 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 possibilities:

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

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

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

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

Similar argument shows that

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

Since $a > 0$ and $b \leq m - k$, we still have $0 \leq a - 1 \leq b - 1 \leq m - k$. By invoking the 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. \hfill \Box

### 3 $[0, b]_{k}^{m}$ for General $k$

In this section we prove the conjecture when $a = 0$ for general $k$, that is, Theorem 2. As stated before, we only need to prove the “if” part. By Proposition 3, it suffices to consider the case when $n$ and $b$ are coprime (see the proof of Theorem 2 also). Under this case, the assumption $bt = nk^{n-1}$ implies that each prime factor of $b$ is also a prime factor of $k$. Thus let $k = p_1^{\alpha_1} \cdots p_j^{\alpha_j}$ be its standard prime factorization, where $\alpha_j > 0$ and then $b$ can be represented as $b = p_1^{\beta_1} \cdots p_j^{\beta_j}$, where $\beta_j \geq 0$. We equip $[k]$ and $[b]$ with the structures (addition groups) $\mathbb{K} = \mathbb{Z}_{p_1}^{\alpha_1} \times \cdots \times \mathbb{Z}_{p_j}^{\alpha_j}$ and $\mathbb{B} = \mathbb{Z}_{p_1}^{\beta_1} \times \cdots \times \mathbb{Z}_{p_j}^{\beta_j}$, respectively.
We use essentially the same idea as in the proof of Theorem 3 and 4, while the key difference is we view $[k]$ as $K$, not only simply as $Z_k$ as in previous proofs, and define a more sophisticated characteristic function. Before describing the marking in detail, we provide this characteristic function with a symmetric property first.

**Proposition 4** There exists a characteristic function $q : K^b \rightarrow B$ with the following property: There exists $s^* \in K$, so that for any $x \in K^b$, $q(x - s^*e_i)$ are pairwise different for all $i \in [b]$, where $s^*e_i$ is the $n$-tuple in $K^b$ with all entries $0$ except that the $i$-th is $s^*$. The definition of $K$ and $B$ and the requirement of $k$, $b$ are stated above.

**Proof** Define the a linear operator $\otimes : K \times B \rightarrow B$ as a generalization of multiplication of scalar and vector, as follows:

For $u = (u^1, \ldots, u^l) \in K(=Z_{p_1}^{a_1} \times \cdots \times Z_{p_l}^{a_l})$, where each $u^j \in Z_{p_j}^{a_j}$ can be represented as $u^j = (u^j_1, u^j_2, \ldots, u^j_b)$, and for $v = (v^1, \ldots, v^l) \in B(=Z_{p_1}^{\beta_1} \times \cdots \times Z_{p_l}^{\beta_l})$, define

$$u \otimes v = (u^1_0 \cdot v^1, u^2_0 \cdot v^2, \ldots, u^l_0 \cdot v^l),$$

where $u^j_0 \cdot v^j$ is the multiplication of a scalar and a vector over $Z_{p_j}$.

As discussed before, $|B| = b$ and thus $[b]$ can be equipped with structure $B$ (or in other words, there exists a one-to-one map between $[b]$ and $B$). By abuse of notation, let $i \in B$ denote the corresponding element of $i \in [b]$. Thus any $b$-tuple $x \in K^b$ can be either indexed by elements of $[b]$ and $B$, $i$ and $i$ correspondingly.

The we are ready to define $q : K^b \rightarrow B$ as follows:

$$q(x) = \sum_{i \in B} x_i \otimes i.$$ 

Now we prove that $q(x)$ indeed has the desired property. Let $s^* = (1, \ldots, 1) \in K$ be the element with each entry $1$, since $\otimes$ is a linear operator, we have that

$$q(x - s^*e_i) = q(x) - q(s^*e_i) = q(x) - s^* \otimes i.$$ 

Since $s^*$ is a vector with every entry $1$, $s^* \otimes i = i$, hence $q(x - s^*e_i) = q(x) - i$ are different for all $i \in [b]$.

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

**Proof of Theorem 2** We only need to prove the sufficient part. Suppose that $s = (\frac{kb - n}{b})k^{n-1}$ 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 $r|b - n$, and since $d \leq n$, we have $d|k^{n-1}$. By Proposition 3 it is sufficient to prove the $r = 1$ case.

As in the proof of Proposition 4, we equip $[k]$ and $[b]$ with structure $K = Z_{p_1}^{a_1} \times \cdots \times Z_{p_l}^{a_l}$, and $B = Z_{p_1}^{\beta_1} \times \cdots \times Z_{p_l}^{\beta_l}$. 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 $(x, y, z)$, where $x \in K^b$, $y \in K^{(t-1)b}$, and $z \in K^b$. Let $q(x)$ be the characteristic function which satisfies the condition in Proposition 4. Let $Q(w) = \{(x, y, z) \in K^n | q(x) = w\}$ as before. We arbitrarily choose $h$ different values $w_1, \ldots, w_h$ from $B$ (since $0 \leq h \leq b$), and let

$$M = (Q(w_1) \cup \cdots \cup Q(w_h)) \cap \{(x, y, z) | \oplus(x, y, z) = 0\}.\footnote{We redefine $\oplus(a)$ as $a_1 + a_2 + \cdots + a_n$, the addition is over the additive group $K$.}$$

[Springer]
Now we describe the marking of lines. Considering $0$ and $s^*$ are two special elements in $\mathcal{K}$, there are $t - 1$ elements left. Let $\tau$ be an arbitrary injective function that maps $[t - 1]$ to $\mathcal{K}\setminus\{0, s^*\}$. Thus $|\tau([t - 1])| = t - 1$.

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

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

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

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

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

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

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

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

4 Conclusion and remarks

In this work we investigated a conjecture of Butler and Graham on marking lines of $[k]^n$. We proved the necessary and sufficient condition of the existence of $[a, b]^n_k$ 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, $[a, n - t]^n_k$ ($t < k$) 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**  
$[a, n - t]^n_k$ exists if $k = p^m, n = t + a + rp^s, n - ka = ru$ and $s \geq m$.

The proof utilizes the property of field $\mathbb{F}_{p^s}$. It is essentially similar to the proof of Theorem 2 and we will put it in the 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.

**Acknowledgments**  
The authors would like to thank the anonymous referees for their helpful comments and suggestion to improve the presentation of this paper. This work was supported in part by the National Natural Science Foundation of China Grant 61170062, 61061130540, the National Basic Research Program of China Grant 2011CBA00301.
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. This time we view $[k]$ as $\mathbb{F}_{pm}$. First, similar to the proof of Theorem 3, we partition the $n = a + t + p^r$ dimensions into three groups, each of which contains $p^r$, $t$, and $a$ coordinates respectively, and represent each point in $\mathbb{F}_{pm}^n$ by $(x, y, z)$ where $x \in \mathbb{F}_{pm}^{p^r}$, $y \in \mathbb{F}_{pm}^t$, and $z \in \mathbb{F}_{pm}^a$. Then, we index $x$ by a pair $(i, j) \in \mathbb{F}_{pm}^{p^r} \times [r]$, i.e. $x_{i,j} \in \mathbb{F}_p$ are the coordinates of $x$ (where $i \in \mathbb{F}_p$, $j \in [r]$). We define lines $(x - (i, j), y, z)$, $(x, y - i, z)$ and $(x, y, z - i)$ in a similar way.

For each $x \in \mathbb{F}_{pm}^{p^r}$, we define the characteristic function $q : \mathbb{F}_{pm}^{p^r} \rightarrow \mathbb{F}_p$ in a slightly different way:

$$q(x) = \sum_{i \in \mathbb{F}_p} q'(\sum_{j=1}^{r} x_{i,j}) \cdot i$$

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

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

References

1. Buhler J., Butler S., Graham R., Tressler E.: Hypercube orientations with only two in-degrees. J. Comb. Theory A 118, 1695–1702 (2011).
2. Butler S., Graham R.: A note on marking lines in $[k]^n$. Des. Codes Cryptogr. 1–11 (2011). doi: 10.1007/s10623-011-9507-z.
3. Butler S., Hajiaghayi M.T., Kleinberg R.D., Leighton T.: Hat guessing games. SIAM J. Discret. Math. 22(2), 592–605 (2008).
4. Ebert T.T.: Applications of recursive operators to randomness and complexity. PhD Thesis, University of California at Santa Barbara (1998).
5. Feige U.: On optimal strategies for a hat game on graphs. SIAM J. Discret. Math. 24(3), 782–791 (2010).
6. Iwasawa H.: Presentation given at the ninth gathering 4 gardner (g4g9) (March 2010).
7. Lenstra H.W., Seroussi G.: On hats and other covers. In: Proceedings of IEEE International Symposium on Information Theory, p. 342 (2002).
8. Ma T., Sun X., Yu H.: A new variation of hat guessing games. In: Proceedings of 17th Annual International Computing and Combinatorics Conference, pp. 616–626 (2011).
9. Paterson M., Stinson D.: Yet another hat game. Electron. J. Comb. 17(1), R86 (2010).

5 Here we use a different arithmetic system for $i$.