RANDOM $B_h$ SETS AND ADDITIVE BASES IN $\mathbb{Z}_N$

Csaba Sándor
Department of Stochastics, Budapest University of Technology and Economics, Hungary

csandor@math.bme.hu

Received: 12/22/06, Revised: 6/20/07, Accepted: 6/22/07, Published: 7/3/07

Abstract

We determine a threshold function for $B_h$ and additive basis properties in $\mathbb{Z}_n$.

1. Introduction

We use the following notations: $\mathbb{Z}$ denotes the integers $0, \pm 1, \pm 2, \ldots$; $\mathbb{N}$ is the set of positive integers; $\mathbb{Z}_n$ is the additive cyclic group of order $n$. Members of a set $S$ are referred to as $\{s_1, s_2, \ldots\}$. The cardinality of a finite set $S$ is denoted by $|S|$. A multiset $\mathbf{q} = \{q_1, \ldots, q_k\}_m$ can be formally defined as a pair $(Q, m)$, where $Q$ is the set of distinct elements of $\mathbf{q}$ and $m : Q \to \mathbb{N}$, where $m(q)$ is the multiplicity of $q \in \mathbf{q}$ for each $q \in Q$. The number of distinct elements of $\mathbf{q}$ is denoted by $|\mathbf{q}|_d$. The usual set operations such as union, intersection and Cartesian product can be easily generalized for multisets. In this paper we use the intersection: suppose that $(A, m)$ and $(B, n)$ are multisets, then the intersection can be defined as $(A \cap B, f)$, where $f(x) = \min\{m(x), n(x)\}$.

For a given $S \subset \mathbb{Z}_n$ and $x \in \mathbb{Z}_n$ denote by $r_{S,h}(x)$ the number of different representations $x = s_1 + \cdots + s_h$ with $s_i \in S$, that is

$$r_{S,h}(x) = |\{\{s_1, \ldots, s_h\}_m : s_1 + \cdots + s_h = x, \ s_i \in S\}|.$$

A set $S \subset \mathbb{Z}_n$ is called $B_h$ set if the number of distinct representation of $x$ as $s_1 + \cdots + s_h$, $s_i \in S$ is at most 1, that is $r_{S,h}(x) \leq 1$ for all $x \in \mathbb{Z}_n$. A set $S \subset \mathbb{Z}_n$ is called additive $h$-basis if every element in $\mathbb{Z}_n$ can be represented as the sum of not necessarily distinct $h$ elements of the set $S$, that is $r_{S,h}(x) \geq 1$ for every $x \in \mathbb{Z}_n$.

For $n$ a positive integer, let $0 \leq p_n \leq 1$. The random subset $S(n, p_n)$ is a probabilistic space over the set of subsets of $\mathbb{Z}_n$ determined by $Pr(k \in S_n) = p_n$ for every $k \in \mathbb{Z}_n$.

\footnote{Supported by Hungarian National Foundation for Scientific Research, Grant No. T 49693 and 61908.}
with these events being mutually independent. This model is often used for proving the existence of certain sequences. Given any combinatorial number theoretic property $P$, there is a probability that $S(n, p_n)$ satisfies $P$, which we write $Pr\{S(n, p_n) \models P\}$. The function $r(n)$ is called a threshold function for a combinatorial number theoretic property $P$ if

(i) When $p_n = o(r(n))$, $\lim_{n \to \infty} Pr\{S(n, p_n) \models P\} = 0$, 

(ii) When $r(n) = o(p(n))$, $\lim_{n \to \infty} Pr\{S(n, p_n) \models P\} = 1$, 

or visa versa.

The goal of this paper is to determine a threshold function for $B_n$ sets and additive $h$-bases in $\mathbb{Z}_n$. We use the typical notation $\exp(x) = e^x$.

**Theorem 1.1.** Let $c > 0$ be arbitrary. Let us suppose that $p_n = \frac{c}{n^{1/2}}$ and the random set $A_n \subset \mathbb{Z}_n$ is defined the following way: For every $k \in \mathbb{Z}_n$ we have $Pr(k \in A_n) = p_n$. Then $\lim_{n \to \infty} Pr\{A_n \text{ is a } B_h \text{ set}\} = \exp\left(-\frac{c^2h}{2(1!)^2}\right)$.

**Theorem 1.2.** Let $c$ be an arbitrary real number. Suppose that $p_n = \frac{(\ln \ln n)^{1/2}(1 + \frac{c}{\ln \ln n})}{n^{1/2}}$ and the random set $A_n \subset \mathbb{Z}_n$ is defined the following way: For every $k \in \mathbb{Z}_n$ we have $Pr\{k \in A_n\} = p_n$. Then $\lim_{n \to \infty} Pr(A_n \text{ is an additive } h\text{-basis}) = \exp(-\exp(-c))$.

2. Proofs

In order to prove the theorems we need two lemmas from probability theory (see e.g. [1] p. 41, 95-98.). In many instances, we would like to bound the probability that none of the bad events $B_i$, $i \in I$, occur. If the events are mutually independent, then $Pr(\cap_{i \in I} B_i) = \prod_{i \in I} Pr(B_i)$. When the $B_i$ are “mostly” independent, the Janson’s inequality allows us, sometimes, to say that these two quantities are ”nearly” equal. Let $\Omega$ be a finite universal set and $R$ be a random subset of $\Omega$ given by $Pr(r \in R) = p_r$, these events being mutually independent over $r \in \Omega$. Let $E_i$, $i \in I$ be subsets of $\Omega$, where $I$ a finite index set. Let $B_i$ be the event $E_i \subset R$. Let $X_i$ be the indicator random variable for $B_i$ and $X = \sum_{i \in I} X_i$ be the number of $E_i$'s contained in $R$. The event $\cap_{i \in I} B_i$ and $X = 0$ are then identical. For $i, j \in I$, we write $i \sim j$ if $i \neq j$ and $E_i \cap E_j \neq \emptyset$. We define $\Delta = \sum_{i \sim j} Pr(B_i \cap B_j)$, here the sum is over ordered pairs. We set $M = \prod_{i \in I} Pr(B_i)$.

**Lemma 1.3 (Janson’s inequality).** Let $B_i, i \in I, \Delta, M$ be as above and assume that $Pr(B_i) \leq \epsilon$ for all $i$. Then

$$M \leq Pr\left(\bigcap_{i \in I} \overline{B_i}\right) \leq M \exp\left(\frac{1}{1 - \epsilon} \cdot \frac{\Delta}{2}\right).$$
The more traditional approach to the Poisson paradigm is called Brun’s sieve, for its use by the number theorist T. Brun. Let $F_1, \ldots, F_m$ be events, $X_i$ the indicator random variable for $F_i$, and $X = X_1 + \cdots + X_m$ the number of $B_i$ that hold. Let there be a hidden parameter $n$ (so that actually $m = m(n), B_i = B_i(n), X = X(n)$) which will define our $O$ notations. Define

$$S^{(r)} = \sum Pr\{B_{i_1} \land \cdots \land B_{i_r}\},$$

where the sum is over all sets $\{i_1, \ldots, i_r\} \subseteq \{1, \ldots, m\}$. The inclusion-exclusion principle gives that $Pr\{X = 0\} = Pr\{B_1 \land \cdots \land B_m\} = 1 - S^{(1)} + S^{(2)} - \cdots + (-1)^r S^{(r)} \cdots$.

**Lemma 1.4.** Suppose there is a constant $\mu$ so that $E(X) = S^{(1)} \to \mu$ and such that for every fixed $r$,

$$E\left(\frac{X^{(r)}}{r!}\right) = S^{(r)} \to \frac{\mu^r}{r!}.$$

Then $Pr\{X = 0\} \to \exp(-\mu)$ and, for every $t$, we have $Pr(X = t) \to \frac{\mu^t}{t!} \exp(-\mu)$.

In order to prove the theorems we need two lemmas. In the sequel, for the sake of brevity, we write $u = \{u_1, \ldots, u_h\}_m$ and $v = \{v_1, \ldots, v_h\}_m$ with $u \neq v$. For every $a \in \mathbb{Z}_n$ and $h, t \in \mathbb{N}, 0 < t \leq h$, let

$$S_{a,h,t} = |\{u: u_i \in \mathbb{Z}_n, \sum_{i=1}^{h} u_i = a, |u|_d = t\}|$$

and for every $a_1, a_2 \in \mathbb{Z}_n$ and $h, t, s, k \in \mathbb{N}$ with $0 < k \leq \min\{s, t\}$ let

$$C_{a_1,a_2,h,t,s,k} = \left|\left\{(u, v): \sum_{i=1}^{h} u_i = a_1, \sum_{i=1}^{h} v_i = a_2, |u|_d = s, |v|_d = t, |u \cap v|_d = k\right\}\right|.$$

**Lemma 1.5.** For every $a \in \mathbb{Z}_n$ and $h \geq 2$ we have

1. $S_{a,h,h} = \frac{n^{h-1}}{h!} + O_h(n^{h-2})$;
2. $S_{a,h,t} = O_h(n^{t-1})$ for $1 \leq t \leq h - 1$.

**Proof.** Case (1): By the definition of $S_{a,h,h}$

$$h!S_{a,h,h} = \left|\{(u_1, \ldots, u_h): u_i \in \mathbb{Z}_n, \sum_{i=1}^{h} u_i = a, \text{ and } u_i \neq u_j \text{ for } i \neq j\}\right|. \quad (1)$$

An upper bound for (1) is $n(n - 1) \cdots (n - h + 2)$ and a lower bound is $n(n - 1) \cdots (n - h + 3)(n - (h - 2) - (h - 2) - 2)$ because we have $n(n - 1) \cdots (n - (h - 3))$ possibilities for $u_1, \ldots, u_{h-2}$ and the conditions $u_{h-1} \neq u_i, u_h \neq u_i$ for $1 \leq i \leq h - 2$ and $u_{h-1} \neq u_h$ exclude at most $h - 2 + h - 2 + 2$ choices for $u_{h-1}$.
Case (2): The condition $|u|_d = t$ implies that there is a partition $\{1, \ldots, h\} = \bigcup_{i=1}^{t} A_i$ such that $u_i = u_j$ if and only if $1 \leq i, j \leq h$ are in the same $A_i$. Fix such a partition. Then there are $n$ choices for the elements $u_i, i \in A_1$, then $(n - 1)$ possibilities for the elements $u_i, i \in A_2$ etc. and finally $(n - (t - 2))$ choices for the elements $u_i, i \in A_{t-1}$. It follows from this that if we have already chosen the elements $u_i, i \in \bigcup_{i=1}^{t-1} A_i$ then we have at most $t \leq h$ possibilities for the elements $u_i, i \in A_t$. In order to finish the proof we mention that the number of suitable partitions is $O_h(1)$. □

**Lemma 1.6.** For every $a_1, a_2 \in \mathbb{Z}_n$ and $h \geq 2$ we have

1. $C_{a_1, a_2, h, h, h, 0} = \frac{n^{2h-2}}{(ht)^2} + O_h(n^{2h-3})$;
2. $C_{a_1, a_2, h, t, s, k} = O_h(n^{t+s-k-2})$ for $t \geq s$ and $t > k \geq 0$;
3. $C_{a_1, a_2, h, s, s, s} = O_h(n^{s-2})$ for every $2 \leq s < h$.

**Proof.** Case (1): By the definition of $C_{a_1, a_2, h, h, h, 0}$

$$2(ht)^2 C_{a_1, a_2, h, h, h, 0} = \left| \{(u_1, \ldots, u_h), (v_1, \ldots, v_h) : u_i \neq u_j, v_i \neq v_j, u_i \neq v_i, \sum_{i=1}^{h} u_i = a_1, \sum_{i=1}^{h} v_i = a_2 \} \right| .$$

An upper bound for (2) is $n^{h-1}n^{h-1}$ and a lower bound for (2) is $n(n - 1) \ldots (n - (h - 3))(n - (h - 2) - (h - 2) - 2)(n - h)(n - (h + 1)) \ldots (n - h - (h - 3))(n - (2h - 2) - (2h - 2) - 2)$, because we have $n(n - 1) \ldots (n - (h - 3))$ choices for $u_1, \ldots, u_{h-1}$.

Choosing $u_1, \ldots, u_{h-1}$ there are at least $n - (h - 2) - (h - 2) - 2$ possibilities left for $u_{h-1}$ because $u_{h-1} \neq u_j$ and $u_{h-1} \neq v_j$ for $1 \leq j \leq h - 2$ and $u_{h-1} \neq u_h$. After fixing $u_1, \ldots, u_{h-1}$ we have $(n - h) \ldots (n - (2h - 2))$ choices for $v_1, \ldots, v_{h-1}$. Finally, we have at least $n - 2h - (2h - 4) - 2$ choices for $v_{h-1}$ because $v_{h-1} \neq u_j, v_{h-1} \neq v_j, v_{h-1} \neq u_j, v_{h-1} \neq v_j$ for $1 \leq j \leq h$, $v_{h-1} \neq v_j, v_{h} \neq v_j$ for $1 \leq j \leq h - 2$ and $v_{h-1} \neq v_h$.

Case (2): Obviously,

$$C_{a_1, a_2, h, t, s, k} \leq \left| \{(u_1, \ldots, u_h), (v_1, \ldots, v_h) : \sum_{i=1}^{h} u_i = a_1, \sum_{i=1}^{h} v_i = a_2, |u|_d = t, |v|_d = s, |u \cap v|_d = k \} \right| .$$

By the conditions $|u|_d = s$, $|v|_d = t$ there are partitions $\{1, \ldots, h\} = \bigcup_{i=1}^{t} A_i = \bigcup_{i=1}^{s} B_i$ such that $u_i = u_j$ if and only if there exists an $1 \leq l \leq t$ such that $i, j \in A_l$, and $v_i = v_j$ if and only if there exists an $1 \leq l \leq s$ such that $i, j \in B_l$. We have at most $hs^{s-1}$ choices for $(v_1, \ldots, v_h)$ with $\sum_{i=1}^{h} v_i = a_2$. The condition $|u \cap v|_d = k$ implies that there are
injections $\chi_u : \{1, \ldots, k\} \to \{1, \ldots, t\}$ and $\chi_v : \{1, \ldots, k\} \to \{1, \ldots, s\}$ such that $u_i = v_j$ if and only if there exists a $1 \leq l \leq k$ such that $u_i \in A_{\chi_u(l)}$ and $v_j \in B_{\chi_v(l)}$. Hence we get that there are at most $ht^{t-k-1}$ choices for the $v_i$'s, $i \in \{1, \ldots, h\} \setminus \bigcup_{i=1}^k B_{\chi_v(i)}$. Since the numbers of partitions and injections are $O_h(1)$, the proof is completed.

Case (3): Evidently,

$$C_{a_1,a_2,h,s,s,s} \leq \left| \{(u_1, \ldots, u_h), (v_1, \ldots, v_h) : \sum_{i=1}^h u_i = a_1, \sum_{i=1}^h v_i = a_2, u \neq v, \right. |u|_d = s, |v|_d = s, |u \cap v|_d = s \left. \right| .$$

(4)

By the conditions $|u|_d = s, |v|_d = s$ there are partitions $\{1, \ldots, h\} = \bigcup_{i=1}^s A_i \bigcup_{i=1}^s B_i$ such that $u_i = v_j$ if and only if there exists an $1 \leq l \leq s$ such that $i, j \in A_l$ and $v_i = v_j$ if and only if there exists an $1 \leq m \leq s$ such that $i, j \in B_m$. The condition $|u \cap v|_d = k$ implies that there is a bijection $\chi : \{1, \ldots, s\} \to \{1, \ldots, s\}$ such that $u_i = v_j$ if and only if there exists a $1 \leq l \leq s$ such that $i \in A_l$ and $j \in B_{\chi(l)}$. Since $u \neq v$, therefore there exists a $1 \leq l \leq s$ such that $|A_l| \neq |B_{\chi(l)}|$. Fix such an $l$. Then there exists a $1 \leq k \leq s$ such that $\frac{|A_k|}{|B_{\chi(l)}|} \neq \frac{|A_l|}{|B_{\chi(l)}|}$, because otherwise $|A_k| = |B_{\chi(k)}| \frac{|A_l|}{|B_{\chi(l)}|}$ for every $1 \leq k \leq s$, but

$$h = \sum_{k=1}^s |A_k| = \frac{|A_l|}{|B_{\chi(l)}|} \sum_{k=1}^s |B_{\chi(k)}| = \frac{|A_l|}{|B_{\chi(l)}|} h,$$

which is a contradiction. Fix such a $k$. Let $\{i_1, \ldots, i_{s-2}\} = \{1, \ldots, s\} \setminus \{k, l\}$. We have $n(n-1) \cdots (n-(s-3))$ choices for the elements $u_i$, $i \in \bigcup_{j=1}^{s-2} A_{i_j}$. After fixing the elements $u_i, i \in \bigcup_{j=1}^{s-2} A_{i_j}$ let $\sum_{j=1}^{s-2} \sum_{m \in A_{i_j}} u_m = U$ and $\sum_{j=1}^{s-2} \sum_{m \in B_{\chi(l)}} v_m = V$. Then we need $x, y \in \mathbb{Z}_n$ such that $U + |A_k| x + |A_l| y = a_1$ and $V + |B_{\chi(k)}| x + |B_{\chi(l)}| y = a_2$. Hence,

$$|A_l||B_{\chi(k)}| - |A_k||B_{\chi(l)}| y = a_1 |B_{\chi(k)}| + V |A_k| - U |B_{\chi(k)}| - a_2 |A_k|. \quad (5)$$

After fixing $1 \leq k, l \leq s$ and the elements $u_i, i \in \bigcup_{j=1}^{s-2} A_{i_j}$, the elements $U$ and $V$ are determined, therefore the right-hand side in (3) is unique. Since $0 < |A_l||B_{\chi(k)}| - |A_k||B_{\chi(l)}| \leq h^2$, therefore the number of possible $y$'s is at most $h^2$ and after fixing $y$ we have at most $h$ choices for $x$. Finally we mention that we have got $O_h(1)$ choices for the partitions and bijection.

Proof of Theorem 1. For each unordered, different $u_1, \ldots, u_h \in \mathbb{Z}_n$ and $v_1, \ldots, v_h \in \mathbb{Z}_n$ with $\sum_{i=1}^h u_i = \sum_{i=1}^h v_i$. Let $B_{u,v}$ be the event that $u_1, \ldots, u_h, v_1, \ldots, v_h \in A_n$. In the following we suppose that $\sum_{i=1}^h u_i = \sum_{i=1}^h v_i$. If we prove $\Delta = \sum_{\{u,v\}: |u-v|_d > 0} \Pr\{B_{u,v}\}$
o(1), then by the Janson inequality we have
\[
\Pr\{A_n \text{ is } B_h \text{ set}\} = (1 + o(1)) \prod_{(u, v)} \Pr\{B_{u, v}\}
\]
\[
= (1 + o(1)) \left( \prod_{(u, v): |u| = h, |v| = h, |w| = 0} \Pr\{B_{u, v}\} \right) \cdot \prod_{k=1}^{h-1} \left( \prod_{(u, v): |u| = h, |v| = h, |w| = k} \Pr\{B_{u, v}\} \right) \cdot \prod_{s=2}^{h-1} \left( \prod_{(u, v): |u| = s, |v| = s, |w| = s} \Pr\{B_{u, v}\} \right) \cdot \prod_{k=0}^{h-1} \left( \prod_{s=1}^{h} \prod_{t=0}^{h-1} \prod_{k=0}^{h-1} \Pr\{B_{u, v}\} \right)
\]
\[
= P_1 P_2 P_3 P_4 P_5,
\]
where, by Lemma 1.6.1,
\[
P_1 = \prod_{a \in \mathbb{Z}_n} \prod_{(u, v): |u| = h, |v| = h, |w| = 0, \sum_{i=1}^{h} u_i = \sum_{i=1}^{h} v_i = a} \Pr\{B_{u, v}\}
\]
\[
= \left( 1 - \frac{2^h}{n^{2h-1}} \right)^{\frac{n^{2h-1}}{2(n!)^2}} (1 + O_h(\frac{1}{n}))
\]
\[
= (1 + o(1)) \exp\left( -\frac{2^h}{2(n!)^2} \right),
\]
by Lemma 1.6.2,
\[
P_2 = \prod_{a \in \mathbb{Z}_n} \prod_{k=1}^{h-1} \prod_{(u, v): |u| = h, |v| = h, |w| = k, \sum_{i=1}^{h} u_i = \sum_{i=1}^{h} v_i = a} \Pr\{B_{u, v}\}
\]
\[
= \prod_{k=1}^{h-1} (1 - P_n^{2h-k} O_h(n^{2h-k-1}))
\]
\[
= \prod_{k=1}^{h-1} \exp\left( (p_n n)^{2h-k} O_h\left( \frac{1}{n} \right) \right)
\]
\[
= \exp(o(1)),
\]
by Lemma 1.6.3,

$$P_3 = \prod_{a \in \mathbb{Z}_n} \prod_{s=2}^{h-1} \prod_{u,v} \Pr\{B_{u,v}\}$$

$$= \prod_{s=2}^{h-1} (1 - p_n^s) O_h(n^{s-1})$$

$$= \prod_{k=1}^{h} \exp\left((-p_n n)^k O_h\left(\frac{1}{n}\right)\right)$$

$$= \exp\left(o(1)\right).$$

by Lemma 1.6.3,

$$P_4 = \prod_{a \in \mathbb{Z}_n} \prod_{s=1}^{h-1} \prod_{k=0}^{s-1} \prod_{u,v} \Pr\{B_{u,v}\}$$

$$= \prod_{k=0}^{s-1} \prod_{s=1}^{h} (1 - p_n^{2s-k}) O_h(n^{2s-k-1})$$

$$= \prod_{k=0}^{s-1} \prod_{s=1}^{h} \exp\left(-p_n n^{2s-k} O_h\left(\frac{1}{n}\right)\right)$$

$$= \exp\left(o(1)\right).$$

and, by Lemma 1.6.2,

$$P_5 = \prod_{a \in \mathbb{Z}_n} \prod_{s=1}^{h-1} \prod_{t=s+1}^{h} \prod_{k=0}^{s-1} \prod_{u,v} \Pr\{B_{u,v}\}$$

$$= \prod_{k=0}^{s-1} \prod_{s=1}^{h} \prod_{t=s+1}^{h} \prod_{k=0}^{h} (1 - p_n^{s+t-k}) O_h(n^{s+t-k-1}) = \exp\left(o(1)\right).$$

Hence, it remains to prove that $\Delta = o(1)$. In order to prove $\Delta = o(1)$ we partition $\Delta$ as

$$\Delta = \sum_{\{u,v\}:|u\cap v|_d > 0} \Pr\{B_{u,v}\}$$

$$= \sum_{s=1}^{h-1} \sum_{\{u,v\}:|u|_d=s,|v|_d=s} \Pr\{B_{u,v}\}$$

$$+ \sum_{s=2}^{h} \sum_{k=1}^{s-1} \sum_{\{u,v\}:|u|_d=s,|v|_d=s} \Pr\{B_{u,v}\}$$

$$+ \sum_{s=1}^{h-1} \sum_{t=s+1}^{h} \sum_{k=0}^{s} \sum_{\{u,v\}:|u|_d=s,|v|_d=t} \Pr\{B_{u,v}\}$$

$$= \sum_{1} + \sum_{2} + \sum_{3}.$$
By Lemma 1.6.3,

\[
\sum_{1} = \sum_{a \in \mathbb{Z}_n} \sum_{s=1}^{h-1} \sum_{1}^{h} \sum_{\{u,v\} : u|d = s, v|d = s, u \cap v|d = s, \sum_{i=1}^{h} u_i = \sum_{i=1}^{h} v_i = a} \Pr\{B_{u,v}\}
\]

\[
= \sum_{s=2}^{h} \sum_{k=1}^{h} \sum_{1}^{h} O_h(n^{s-1}) p_n^s
\]

\[
= O_h\left(\frac{1}{n} \sum_{s=2}^{h} \left(\sum_{k=1}^{h} (p_n)^{2s-k}\right) o(1),
\]

by Lemma 1.6.2,

\[
\sum_{2} = \sum_{a \in \mathbb{Z}_n} \sum_{s=2}^{h} \sum_{k=1}^{h} \sum_{1}^{h} \sum_{\{u,v\} : u|d = s, v|d = s, u \cap v|d = s, \sum_{i=1}^{h} u_i = \sum_{i=1}^{h} v_i = a} \Pr\{B_{u,v}\}
\]

\[
= \sum_{s=2}^{h} \sum_{k=1}^{h} \sum_{1}^{h} O_h(n^2 s-k-1) p_n^{2s-k}
\]

\[
= O_h\left(\frac{1}{n} \sum_{s=2}^{h} \sum_{k=1}^{h} (p_n)^{2s-k}\right) = o(1),
\]

and by Lemma 1.6.2,

\[
\sum_{3} = \sum_{a \in \mathbb{Z}_n} \sum_{s=1}^{h-1} \sum_{t=s+1}^{h} \sum_{k=0}^{s} \sum_{\{u,v\} : u|d = s, v|d = t, u \cap v|d = t, \sum_{i=1}^{h} u_i = \sum_{i=1}^{h} v_i = a} \Pr\{B_{u,v}\}
\]

\[
= \sum_{s=1}^{h-1} \sum_{t=s+1}^{h} \sum_{k=0}^{s} O_h(n^{t+s-k-1}) p_n^{t+s-k}
\]

\[
= O_h\left(\frac{1}{n} \sum_{s=1}^{h-1} \sum_{t=s+1}^{h} \sum_{k=0}^{s} (p_n)^{t+s-k}\right) = o(1),
\]

which completes the proof. \(\square\)

Proof of Theorem 2. For a fixed \(x \in \mathbb{Z}_n\) and \(y_1, \ldots, y_h \in \mathbb{Z}_n\) with \(\sum_{i=1}^{h} y_i = x\) let \(y = \{y_1, \ldots, y_h\}\) and let \(B_{y,x}\) be the event \(y_1, \ldots, y_h \in A_n\). For a fixed \(x \in \mathbb{Z}_n\) let \(C_x = \cap_{y \in A_n} B_{y,x}\). Obviously,

\[
\Pr\{A_n \text{ is an h-basis}\} = \Pr(\cap_{x \in \mathbb{Z}_n} \overline{C_x}).
\]

By Lemma 1.4 it is sufficient to show that for every fixed positive integer \(r\) we have

\[
\sum_{\{x_1, \ldots, x_r\} : x_i \in \mathbb{Z}_n, x_i \neq x_j} \Pr\{C_{x_1} \cap \cdots \cap C_{x_r}\} \rightarrow \frac{\exp\left(-rc\right)}{r!}.
\]

In order to estimate

\[
\sum_{\{x_1, \ldots, x_r\} : x_i \in \mathbb{Z}, x_i \neq x_j} \Pr\{C_{x_1} \cap \cdots \cap C_{x_r}\} = \sum_{\{x_1, \ldots, x_r\} : x_i \in \mathbb{Z}, x_i \neq x_j} \Pr\{\bigcap_{1 \leq i \leq r} \cap y : \sum_{j=1}^h y_j = x_i \} \overline{B}_{y,x_i}\]

we use Janson’s inequality. Obviously, \(\Pr\{B_{y,x_i}\} = o(1)\). If we prove \(\Delta = o(1)\), then by Lemmas 1.3 and 1.5, and the definition of \(p_n\)

\[
\sum_{\{x_1, \ldots, x_r\} : x_i \in \mathbb{Z}, x_i \neq x_j} \Pr \left\{ \bigcap_{1 \leq i \leq r} \bigcap_{y : \sum_{j=1}^h y_j = x_i} \overline{B}_{y,x_i} \right\}
\]

\[
= (1 + o(1)) \prod_{i=1}^r \prod_{y : \sum_{j=1}^h y_j = x_i} \Pr\{\overline{B}_{y,x_i}\}
\]

\[
= (1 + o(1)) \prod_{i=1}^r \prod_{k=1}^h \prod_{y : y_1 + \cdots + y_h = x_i, |u| = k} (1 - p_n^k)
\]

\[
= (1 + o(1)) \prod_{i=1}^r \prod_{k=1}^{h-1} \left( (1 - p_n^k)^{O_h(n^{k-1})} (1 - p_n^k)^{\frac{h-1}{h!}(1 + O_h(\frac{1}{n}))} \right)
\]

\[
= (1 + o(1)) \prod_{i=1}^r \left[ \exp \left\{ -O_h \left( \frac{1}{n} \right) \sum_{1 \leq k \leq h-1} (p_n)^k \right\} \right]
\]

\[
\times \left[ \exp \left\{ -\frac{(p_n)^h}{h!} \left( 1 + O_h(p_n^h) \right) \left( \frac{1}{n} + O_h \left( \frac{1}{n^2} \right) \right) \right\} \right]
\]

\[
= (1 + o(1)) \left( \exp \left\{ -r h \log n \left( 1 + \frac{c}{\log n} \right)(1 + O_h(\frac{1}{\log^2 n})) \frac{1}{n} \right\} \right)
\]

\[
= (1 + o(1)) \frac{\exp \left\{ -cr \right\}}{n^r}.
\]

Therefore,

\[
\sum_{\{x_1, \ldots, x_r\} : x_i \in \mathbb{Z}, x_i \neq x_j} \Pr\{C_{x_1} \cap \cdots \cap C_{x_r}\} = (1 + o(1)) \left( \frac{n}{r} \right) \frac{\exp \left\{ -cr \right\}}{n^r} = (1 + o(1)) \frac{\exp \left\{ -cr \right\}}{r!}.
\]

Let \(u = \{u_1, \ldots, u_h\}\) with \(u_1 + \cdots + u_h = x_i\) and \(v = \{v_1, \ldots, v_h\}\) with \(v_1 + \cdots + v_h = x_j\).
In order to finish the proof, we separate $\Delta$ as

$$
\Delta = \sum_{1 \leq i, j \leq r} \sum_{s=2}^{h-1} \sum_{u, x_i, \{v, x_j\} : |u| = s, |v| = s, |u \cap v| > 0} \Pr \{B_{u, x_i} \cap B_{v, x_j}\} 
$$

$$
= \sum_{1 \leq i, j \leq r} \sum_{s=2}^{h-1} \sum_{u, x_i, \{v, x_j\} : |u| = s, |v| = s, |u \cap v| = s} p_n^s
$$

$$
+ \sum_{1 \leq i, j \leq r} \sum_{s=2}^{h-1} \sum_{u, x_i, \{v, x_j\} : |u| = s, |v| = s, |u \cap v| = d} p_n^{2s-k}
$$

$$
+ \sum_{1 \leq i, j \leq r} \sum_{s=1}^{h-1} \sum_{t=s+1}^{h} \sum_{u, x_i, \{v, x_j\} : |u| = s, |v| = t, |u \cap \{v_1, \ldots, v_r\}| = k} p_n^{s+t-k}
$$

$$
= \sum_1 + \sum_2 + \sum_3,
$$

where, by Lemma 1.6.3,

$$
\sum_1 \leq r^2 \sum_{s=2}^{h-1} p_n^s O_h(n^{s-2}) = O_{h,r} \left( \frac{1}{n^2} \sum_{s=2}^{h-1} (p_n n)^s \right) = o(1),
$$

by Lemma 1.6.2,

$$
\sum_2 \leq r^2 \sum_{s=2}^{h-1} \sum_{k=1}^{s-1} p_n^{2s-k} O_h(n^{2s-k-2}) = O_{h,r} \left( \frac{1}{n^2} \sum_{s=2}^{h-1} \sum_{k=1}^{s-1} (p_n n)^{2s-k} \right) = o(1),
$$

and, by Lemma 1.6.2,

$$
\sum_3 \leq r^2 \sum_{s=1}^{h-1} \sum_{t=s+1}^{h} \sum_{k=1}^{s} p_n^{t+s-k} O_h(n^{t+s-k}) = O_{h,r} \left( \frac{1}{n^2} \sum_{s=1}^{h-1} \sum_{t=s+1}^{h} \sum_{k=1}^{s} (p_n n)^{t+s-k} \right) = o(1)
$$

which completes the proof.

References