To calculate the expectation and variance of O_n, we must have the mathematical expression of its probability distribution. Let $N_n(o)$ be the number of n-bit binary sequences whose odd hop sum is o, obtaining the expression of $N_n(o)$ is equivalent to getting the probability distribution of O_n. As for the odd hop sum is the sum of the odd order numbers in the jump height sequence, we can partition all the n-bit binary sequences whose odd hop sum is o by their jump height sequences. From Proposition 1 we can derive that the number of n-bit binary sequences with a given jump height sequence $jh_1, jh_2, \ldots, jh_q$ is

$$\begin{cases} 2^L, & 2L \leq n \\ 2^{n-L}, & 2L > n \end{cases}, \tag{1}$$

where $L = jh_1 + jh_2 + \cdots + jh_q$ is the linear complexity of these sequences. This formula is only relative to the linear complexity of these sequences, thus we can firstly calculate the number of n-bit binary sequences whose linear complexity is L and odd hop sum is o, denoted as $NL_n(L, o)$.

Now that the number of n-bit binary sequences with a given jump height sequence whose sum is L is known, we should count the number of different jump height sequences whose sum is L and odd order sum is o. Due to the difinition, the jump height sequence is a sequence of positive integers. And due to the property of the linear complexity profile, we can know that if the last linear complexity jump of an n-bit binary sequence ϵ occurs in position k(such that $L_n(\epsilon) = L_k(\epsilon) > L_{k-1}(\epsilon)$), then

$$2\sum_{i=1}^{q-1} jh_i < k \leq n, \tag{2}$$

and

$$\begin{aligned} jh_q &= (k - \sum_{i=1}^{q-1} jh_i) - \sum_{i=1}^{q-1} jh_i \\ &= k - 2\sum_{i=1}^{q-1} jh_i. \end{aligned} \tag{3}$$

Combining (2), (3) and $L = jh_1 + jh_2 + \cdots + jh_q$, we get

$$jh_q \geq \max\{1, 2L - n\}. \tag{4}$$

That's say, any sequence of positive numbers whose sum is L and whose last item is no less than $\max\{1, 2L - n\}$ can be a jump height sequence of an n-bit binary sequence whose linear complexity is L. Thus, to calculate $NL_n(L, o)$, we should count the number of different sequences of positive integers whose sum are L, odd order sum are o, and last item are no less than $\max\{1, 2L - n\}$. We first give some conclusions about the count for sequences of positive integers.

Lemma 0.1. *The number of sequences of positive integers whose sum are h and length are m is C_{h-1}^{m-1}.*

Proof. Suppose there are n objects standing in line, thus there are $n-1$ gaps between any two neighbouring objects. Choose $m-1$ gaps from these $n-1$ gaps to patition all the objects into m parts, the numbers of objects of each part from the head of the line to the tail corresponds a unique sequence of pisitive integers whose sum is n and length is m. Because there are totally C_{n-1}^{m-1} different choices, the lemma is proved. □

Lemma 0.2. *The number of sequences of positive integers whose sum are h and odd order sum are $\bar{h}$ is $C_{h-1}^{\bar{h}-1}$.*

Proof. Let A be the set of all sequences of positive integers whose sum are h and odd order sum are $\bar{h}$, and B be the set of all sequences of positive integers whose sum are h and length are $\bar{h}$. And we denote the cardinality of A and B by $|A|$ and $|B|$ respectively.

Define a mapping f from A to B: for a sequence of positive integers whose sum is h and odd order sum is $\bar{h}$, suppose it to be $a_1, a_2, \ldots, a_q$, partition each odd order number a_{2i-1} and the following even oder number a_{2i} into $a_{2i-1}-1$ integers with value 1 and an integer with value $1+a_{2i}$, and if the last number a_q of the sequence has odd order, partition it into a_q integers with value 1 directly. Obviously, the resulted new sequence must be a sequence of positive integers whose sum is still h and length is $\bar{h}$, thus f is a mapping from A to B.

What's more, for the mapping f, we can find its inverse mapping. Define the mapping g from B to A: for a sequence of pisitive integers whose sum is h and length is $\bar{h}$, thransform the consecutive $\mu(\mu \geq 0)$ integers with value 1 and the following integer with value ν that is larger than 1 into an integer with value $\mu+1$ and an integer with value $\nu-1$, and if the last number of the sequence is 1, thransform the last consecutive $\gamma(\gamma > 0)$ integers with value 1 into an integer with value γ. The resulted new sequence must be a sequence of positive integers whose sum is still h and odd order sum is $\bar{h}$, thus g is a mapping from B to A.

From the definitions, $\forall \alpha \in A, \beta \in B$, we have

$$g(f(\alpha)) = \alpha, f(g(\beta)) = \beta.$$

That's say f is the reverse mapping of g, so f and g are both one-to-one mappings. Additionly, $\forall \alpha \in A$, $\exists \beta \in B$, such that $f(\alpha) = \beta$, thus

$$|A| \leq |B|. \tag{5}$$

And $\forall \beta \in B$, $\exists \alpha \in A$, such that $g(\beta) = \alpha$, thus

$$|B| \leq |A|. \tag{6}$$

Finally, according to (5) and (6) and Lemma 0.1, we get

$$|A| = |B| = \mathrm{C}_{h-1}^{\bar{h}-1}$$

□

Lemma 0.3. *The number of sequences of positive integers whose sum are h, odd order sum are $\bar{h}$, and last item has odd order and is no less than a positive integer t is*

$$\begin{cases} 1, & t = \bar{h} = h \\ C_{h-t-1}^{\bar{h}-t-1}, & t < \bar{h} \leq h \\ 0, & otherwise \end{cases}.$$

Proof. When $t = \bar{h}$, if there is one sequence of positive integers whose sum is h, odd order sum is $\bar{h}$, and last item has odd order and is no less than t, then the last item $\geq \bar{h}$. But because $\bar{h}$ is the sum of all the items with odd order and the last item is a odd order item, the value of last item must be $\bar{h}$ and the last item is the only odd order item, i.e. there is only one item in the whole sequence and $\bar{h} = h$. Thus there is only one such sequence.

When $t < \bar{h}$, let A be the set of all sequences of positive integers whose sum are h, odd order sum are $\bar{h}$, and last item has odd order and is no less than the positive integer t, and B be the set of all sequences of positive integers whose sum are $h - t$ and odd order sum are $\bar{h} - t$. And we denote the cardinality of A and B by $|A|$ and $|B|$ respectively.

Define a mapping f from A to B: for a sequence of positive integers whose sum are h, even order sum are $\bar{h}$, and the last item has odd order and is no less than a positive integer t, suppose it to be $a_1, a_2, \ldots, a_{2k+1}$, if $a_{2k+1} > t$, decrease a_{2k+1} by t; and if $a_{2k+1} = t$, throw away a_{2k+1}. Because $t < \bar{h}$, if $a_{2k+1} = t$, throwing away a_{2k+1} will not make the sequence become an empty sequence for there are other odd order items. Thus, after this thansformation, the resulted seqeunce is still a sequence of positive integers. And the sum of the resulting new sequence becomes $h - t$, and the odd order sum of the resulting new sequence becomes $\bar{h} - t$, thus the resulting new sequence belongs to the set B, so f is actually a mapping from A to B.

We can also define a mapping g from B to A: for a sequence of positive integers whose sum are $h-t$, odd order sum are $\bar{h}-t$, suppose it to be $b_1, b_2, \ldots, b_q$, if the last item b_q has the odd order, increase b_q by t; if the last item b_q has the even order, add a new item with value t in the end of the sequence. The sum of the resulting new sequence becomes h, and the odd order sum of the resulting new sequence becomes $\bar{h}$, and the last item of the resulting new sequence has odd order and is no less than t, thus the resulting new sequence belongs to the set A, so g is actually a mapping from B to A.

From the definitions, $\forall \alpha \in A, \beta \in B$, we have

$$g(f(\alpha)) = \alpha, \quad f(g(\beta)) = \beta.$$

That's say f is the reverse mapping of g, so f and g are both one-to-one mappings. Additionly, $\forall \alpha \in A$, $\exists \beta \in B$, such that $f(\alpha) = \beta$, thus

$$|A| \leq |B|. \tag{7}$$

And $\forall \beta \in B$, $\exists \alpha \in A$, such that $g(\beta) = \alpha$, thus

$$|B| \leq |A|. \tag{8}$$

Finally, according to (7) and (8) and Lemma 0.2, we get

$$|A| = |B| = \mathrm{C}_{h-t-1}^{\bar{h}-t-1}.$$

□

Lemma 0.4. *The number of sequences of positive integers whose sum are h, even order sum are $\hat{h}$, and last item has even order and is no less than a positive integer t is*

$$\begin{cases} C_{h-t-1}^{h-\hat{h}-1}, & t \le \hat{h} < h \\ 0, & otherwise \end{cases}.$$

Proof. When there are even order items in a sequence of positive integers, there must be odd order items in the squence. Thus $\hat{h}$ must be less than h, i.e. for $\hat{h} \ge h$, the number of sequences of positive integers whose sum is h and even order sum is $\hat{h}$ is zero.

In the case $\hat{h} < h$, let A be the set of all sequences of positive integers whose sum are h, even order sum are $\hat{h}$, and last item has even order and is no less than the positive integer $t(t \le \hat{h})$, and B be the set of all sequences of positive integers whose sum are $h-t$ and even order sum are $\hat{h}-t$. And we denote the cardinality of A and B by $|A|$ and $|B|$ respectively.

Define a mapping f from A to B: for a sequence of positive integers whose sum are h, even order sum are $\hat{h}$, and the last item has even order and is no less than the positive integer t, suppose it to be $a_1, a_2, \ldots, a_{2k}$, if $a_{2k} > t$, decrease a_{2k} by t; and if $a_{2k} = t$, throw away a_{2k}. Because a_{2k} is not the only item in the whole sequence, throwing away a_{2k} will not make the sequence become an empty sequence for there must be at least one odd order item. Thus, after this thansformation, the resulted seqeunce is still a sequence of positive integers. And the sum of the resulting new sequence becomes $h-t$, and the even order sum of the resulting new sequence becomes $\hat{h}-t$, thus the resulting new sequence belongs to the set B, so f is actually a mapping from A to B.

We can also define a mapping g from B to A: for a sequence of positive integers whose sum are $h-t$, even order sum are $\hat{h}-t$, suppose it to be $b_1, b_2, \ldots, b_q$, if the last item b_q has the even order, increase b_q by t; if the last item b_q has the odd order, add a new item with value t in the end of the sequence. The sum of the resulting new sequence becomes h, and the even order sum of the resulting new sequence becomes $\hat{h}$, and the last item of the resulting new sequence has even order and is no less than t, thus the resulting new sequence belongs to the set A, so g is actually a mapping from B to A.

From the definitions, $\forall \alpha \in A, \beta \in B$, we have

$$g(f(\alpha)) = \alpha, \quad f(g(\beta)) = \beta.$$

That's say f is the reverse mapping of g, so f and g are both one-to-one mappings. Additionly, $\forall \alpha \in A$, $\exists \beta \in B$, such that $f(\alpha) = \beta$, thus

$$|A| \le |B|. \tag{9}$$

And $\forall\beta \in B$, $\exists\alpha \in A$, such that $g(\beta) = \alpha$, thus

$$|B| \leq |A|. \tag{10}$$

Due to (9) and (10) , we get

$$|A| = |B|.$$

And the restriction that the even order sum is $\hat{h} - t$ in the set B can be replaced by the odd order sum is $h - \hat{h}$, so that we can now apply Lemma 0.2 to obtain

$$|A| = |B| = \mathrm{C}_{h-t-1}^{h-\hat{h}-1}.$$

□

Lemma 0.5. *The number of sequences of positive integers whose sum is h, odd order sum is $\bar{h}$, and last item is no less than a positive integer $t(t < h)$ is*

$$I_o \cdot C_{h-t-1}^{\bar{h}-t-1} + I_e \cdot C_{h-t-1}^{\bar{h}-1},$$

where

$$I_o = \begin{cases} 1, & t < \bar{h} \leq h \\ 0, & otherwise \end{cases}, \quad I_e = \begin{cases} 1, & 1 \leq \bar{h} \leq h - t \\ 0, & otherwise \end{cases}.$$

Proof. Let S be the set of all sequences of positive integers whose sum is h, odd order sum is $\bar{h}$, and last item is no ness than the positive integer t, A be the set of all sequences of positive integers whose sum is h, odd order sum is $\bar{h}$, and last item has odd order and is no ness than the positive integer t, B be the set of all sequences of positive integers whose sum is h, odd order sum is $\bar{h}$, and last item has even order and is no ness than the positive integer t. Then

$$A \cup B = S,$$
$$A \cap B = \emptyset,$$

so

$$|S| = |A| + |B|.$$

From Lemma 0.3, because $t < h$, we have

$$|A| = \begin{cases} \mathrm{C}_{h-t-1}^{\bar{h}-t-1}, & t < \bar{h} \leq h \\ 0, & otherwise \end{cases}. \tag{11}$$

For the sequences in set B, the restriction that odd order sum is $\bar{h}$ can be replaced by even order sum is $h - \bar{h}$. Then we can apply Lemma 0.4 to get

$$|B| = \begin{cases} \mathrm{C}_{h-t-1}^{\bar{h}-1}, & t \leq h - \bar{h} < h \\ 0, & otherwise \end{cases}, \tag{12}$$

where the condition $t \leq h - \bar{h} < h$ is equivalent to $1 \leq \bar{h} \leq h - t$. □

Now, we can derive the expression of $NL_n(L, o)$. First, we should state the value range of L and o. For n-bit binary sequences, their linear complexities should lie in interval $[0, n]$. When $L = 0$, their odd hop sums can only be zero too, and when $0 < L \leq n$, their odd hop sums lie in interval $[1, L]$. We discuss the expression of $NL_n(L, o)$ according to the range of L.

When $L = 0$, there is only one n-bit binary sequence whose linear compelxity is 0, and the odd hop sum of that unique sequence is also 0. So we have $NL_n(0, 0) = 1$.

When $0 < L \leq n/2$, the odd hop sums of the n-bit binary seqeunces with linear complexity L lies in range $[1, L]$. $L \leq n/2$ meas $2L - n < 1$. Thus from 4, we can know that the jump height sequences of all the n-bit binary sequences must satisfy that their last items are no less than 1. But for that the jump height sequences are themselves sequences of positive integers, last item is no less than 1 can not be regarded as an addition restriction to these sequences. Due to Lemma 0.2, the number of seqeunces of positive integers whose sums are L and odd order sums are o is C_{L-1}^{o-1}. And from (1), for each jump height sequence whose sum is L and odd order sum is o, there are 2^L n-bit binary seqeunces having that jump height sequence. So when $0 < L \leq n/2$ and $1 \leq o \leq L$,

$$NL_n(L, o) = \mathrm{C}_{L-1}^{o-1} 2^L.$$

When $n/2 < L < n$, the odd hop sums of the n-bit binary seqeunces with linear complexity L lies in range $[1, L]$. $L > n/2$ meas $2L - n \leq 1$. Thus from 4, we can know that the jump height sequences of all the n-bit binary sequences must satisfy that their last items are no less than $2L - n$. $L < n$ results in $2L - n < L$, so that we can apply Lemma 0.5 to calculate the number of all the possible jump height sequences. And from (1), there are 2^{n-L} n-bit binary seqeunces for each of these possible jump height sequences. So when $n/2 < L < n$ and $1 \leq o \leq L$,

$$NL_n(L, o) = (I_o \cdot \mathrm{C}_{n-L-1}^{o-2L+n-1} + I_e \cdot \mathrm{C}_{n-L-1}^{o-1}) 2^{n-L},$$

where

$$I_o = \begin{cases} 1, & 2L - n < o \leq L \\ 0, & otherwise \end{cases}, \quad I_e = \begin{cases} 1, & 1 \leq o \leq n - L \\ 0, & otherwise \end{cases}.$$

When $L = n$, there is only one n-bit binary sequence whose linear compelxity is n, and the odd hop sum of that unique sequence is also n. So we have $NL_n(n, n) = 1$.

We conclude the above results in the following theory.

Theorem 0.1. *The number of n-bit binary sequences whose linear complexity*

are L and odd order sum are o is

$$NL_n(L,o)=\begin{cases}1, & L=0,o=L\\ C_{L-1}^{o-1}2^L, & 0<L\le n/2,1\le o\le L\\ (I_o\cdot C_{n-L-1}^{o-2L+n-1}+I_e\cdot C_{n-L-1}^{o-1})2^{n-L}, & n/2<L<n,1\le o\le L\\ 1, & L=n,o=L\\ 0, & otherwise\end{cases}, \tag{13}$$

where

$$I_o=\begin{cases}1, & 2L-n<o\le L\\ 0, & otherwise\end{cases},\quad I_e=\begin{cases}1, & 1\le o\le n-L\\ 0, & otherwise\end{cases}. \tag{14}$$

Because for arbitary binary sequence, its linear complexity must be no less than its odd hop sum, we can get

$$\begin{aligned}N_n(o)&=\sum_{L=0}^{n}NL_n(L,o)\\ &=\sum_{L=o}^{n}NL_n(L,o).\end{aligned} \tag{15}$$

Therefore we can use Theorem 0.1 and formula (15) to obtain the explicit expressions for both the mean and variance of odd hop sum of a random n-bit binary sequence. And in the process of computing the mean and variance, we will use the following formulas of the sum of some series.

$$\sum_{i=0}^{n}\mathrm{C}_n^i=2^n. \tag{16}$$

$$\sum_{i=0}^{n}\mathrm{C}_i^1\mathrm{C}_n^i=\mathrm{C}_n^1 2^{n-1}. \tag{17}$$

$$\sum_{i=0}^{n}\mathrm{C}_i^2\mathrm{C}_n^i=\mathrm{C}_n^2 2^{n-2}. \tag{18}$$

$$\sum_{i=\alpha}^{\beta}q^i=\frac{q^{\beta+1}-q^{\alpha}}{q-1}. \tag{19}$$

$$\sum_{i=\alpha}^{\beta}\mathrm{C}_i^1 q^i=\frac{(\beta(q-1)-1)q^{\beta+1}-(\frac{\alpha}{q}(q-1)-1)q^{\alpha+1}}{(q-1)^2}. \tag{20}$$

$$\sum_{i=\alpha}^{\beta}\mathrm{C}_i^2 q^i=\frac{(\frac{(q-1)^2}{q}\mathrm{C}_\beta^2-\frac{q-1}{q}\beta+1)q^{\beta+2}-(\frac{(q-1)^2}{q^2}\mathrm{C}_\alpha^2-\frac{q-1}{q}\alpha+1)q^{\alpha+2}}{(q-1)^3}. \tag{21}$$

Theorem 0.2. *Let $E(O_n)$ be the mean odd hop sum of a random n-bit binary sequence, then*

$$E(O_n) = \begin{cases} \frac{n}{4} + \frac{11}{18} + \frac{3n-10}{9\cdot 2^n}, & \text{if } n \text{ is even} \\ \frac{n}{4} + \frac{23}{36} + \frac{3n-10}{9\cdot 2^n}, & \text{if } n \text{ is odd} \end{cases}.$$

Proof.

$$\begin{aligned} E(O_n) &= \sum_{o=0}^{n} o \cdot Pr\{O_n = o\} \\ &= \sum_{o=0}^{n} o \cdot \frac{N_n(o)}{2^n} \\ &= 2^{-n} \sum_{o=0}^{n} o \cdot N_n(o) \\ &= 2^{-n} \sum_{o=0}^{n} o \sum_{L=o}^{n} NL_n(L,o) \\ &= 2^{-n} \sum_{L=0}^{n} \sum_{o=0}^{L} o \cdot NL_n(L,o). \end{aligned} \tag{22}$$

Due to the form of the expression (13), we can partition $\sum_{L=0}^{n} \sum_{o=0}^{L} o \cdot NL_n(L,o)$ by the value of L,

$$\begin{aligned} \sum_{L=0}^{n} \sum_{o=0}^{L} o \cdot NL_n(L,o) &= \sum_{o=0}^{0} o \cdot NL_n(0,o) + \sum_{L=1}^{\lfloor n/2 \rfloor} \sum_{o=1}^{L} o \cdot NL_n(L,o) \\ &\quad + \sum_{L=\lfloor n/2 \rfloor + 1}^{n-1} \sum_{o=1}^{L} o \cdot NL_n(L,o) + \sum_{o=1}^{n} o \cdot NL_n(n,o) \\ &\quad \text{(since when } L = n, NL_n(L,o) \text{ is nonzero only when } o = L) \\ &= n + \sum_{L=1}^{\lfloor n/2 \rfloor} \sum_{o=1}^{L} o \cdot NL_n(L,o) + \sum_{L=\lfloor n/2 \rfloor + 1}^{n-1} \sum_{o=1}^{L} o \cdot NL_n(L,o). \end{aligned} \tag{23}$$

Then we calculate the two sums in the right of formula (23) separately. And because $\lfloor n/2 \rfloor$ is dependent on the parity of n, we consider odd and even values of n separately.

n even:

$$
\begin{aligned}
&\sum_{L=1}^{\lfloor n/2 \rfloor} \sum_{o=1}^{L} o \cdot NL_n(L,o) \\
=&\sum_{L=1}^{n/2} \sum_{o=1}^{L} o \cdot NL_n(L,o) \\
=&\sum_{L=1}^{n/2} \sum_{o=1}^{L} o \cdot \mathrm{C}_{L-1}^{o-1} 2^L \\
=&\sum_{L=1}^{n/2} 2^L \sum_{i=0}^{L-1} (i+1) \cdot \mathrm{C}_{L-1}^{i} \qquad (\text{let } i = o-1) \\
=&\sum_{L=1}^{n/2} 2^L ((L-1)2^{L-2} + 2^{L-1}) \qquad (\text{by formula (17) and (16)}) \\
=&2^{-2} \sum_{L=1}^{n/2} (L \cdot 4^L + 4^L) \\
=&\frac{(3n+4)2^{n-1} - 2}{9}. \qquad (\text{by formula (20) and (19)})
\end{aligned} \tag{24}
$$

And by formula (13) we have

$$
\begin{aligned}
&\sum_{L=\lfloor n/2 \rfloor + 1}^{n-1} \sum_{o=1}^{L} o \cdot NL_n(L,o) \\
=&\sum_{L=n/2+1}^{n-1} \sum_{o=1}^{L} o \cdot (I_o \cdot \mathrm{C}_{n-L-1}^{o-2L+n-1} + I_e \cdot \mathrm{C}_{n-L-1}^{o-1}) 2^{n-L} \\
=&\sum_{L=n/2+1}^{n-1} 2^{n-L} (\sum_{o=1}^{L} I_o \cdot o \cdot \mathrm{C}_{n-L-1}^{o-2L+n-1} + \sum_{o=1}^{L} I_e \cdot o \cdot \mathrm{C}_{n-L-1}^{o-1}),
\end{aligned} \tag{25}
$$

where

$$
I_o = \begin{cases} 1, & 2L-n < o \le L \\ 0, & otherwise \end{cases}, \quad I_e = \begin{cases} 1, & 1 \le o \le n-L \\ 0, & otherwise \end{cases}.
$$

Due to the way that I_o and I_e change by the value of o, we get

$$
\begin{aligned}
&\sum_{o=1}^{L} I_o \cdot o \cdot \mathrm{C}_{n-L-1}^{o-2L+n-1} \\
=&\sum_{o=2L-n+1}^{L} o \cdot \mathrm{C}_{n-L-1}^{o-2L+n-1} \\
=&\sum_{i=0}^{n-L-1} (i+2L-n+1) \cdot \mathrm{C}_{n-L-1}^{i}, \qquad (\text{let } i = o-2L+n-1)
\end{aligned} \tag{26}
$$

and

$$\begin{aligned}
&\sum_{o=1}^{L} I_e \cdot o \cdot \mathrm{C}_{n-L-1}^{o-1} \\
=&\sum_{o=1}^{n-L} o \cdot \mathrm{C}_{n-L-1}^{o-1} \\
=&\sum_{i=0}^{n-L-1} (i+1) \cdot \mathrm{C}_{n-L-1}^{i}. \qquad (\text{let } i = o-1)
\end{aligned} \tag{27}$$

Now, combining (25), (26) and (27), we get

$$\begin{aligned}
&\sum_{L=n/2+1}^{n-1} \sum_{o=1}^{L} o \cdot NL_n(L,o) \\
=&\sum_{L=n/2+1}^{n-1} 2^{n-L} \sum_{i=0}^{n-L-1} (2i+2L-n+2)\mathrm{C}_{n-L-1}^{i} \\
=&\sum_{L=n/2+1}^{n-1} 2^{n-L}(2(n-L-1)2^{n-L-2} + (2L-n+2)2^{n-L-1}) \\
&\text{(by formula (17) and (16))} \\
=&2^{-1} \sum_{L=n/2+1}^{n-1} (L+1)4^{n-L} \\
=&2^{-1} \sum_{i=n/2-1}^{1} (n-i+1)4^{i} \qquad (\text{let } i = n-L) \\
=&2^{-1} \sum_{i=1}^{n/2-1} (n-i+1)4^{i} \\
=&\frac{(3n+14)2^{n-2} - 6n - 8}{9}. \qquad (\text{by formula (20) and (19)})
\end{aligned} \tag{28}$$

Finally, combing (22), (23), (24) and (28), we obtain the expectation of O_n when n is even:

$$\begin{aligned}
E(O_n) &= 2^{-n}(n + \frac{(3n+4)2^{n-1}-2}{9} + \frac{(3n+14)2^{n-2}-6n-8}{9}) \\
&= \frac{n}{4} + \frac{11}{18} + \frac{3n-10}{9 \cdot 2^n}.
\end{aligned}$$

As for the case n is odd, in which $\lfloor n/2 \rfloor = (n-1)/2$, we can have a similar process to get the expectation of O_n as the case n is even. We do not give the details here. □

Theorem 0.3. *Let $V(O_n)$ be the variance of odd hop sum of a random n-bit*

binary sequence, then

$$V(O_n) = \begin{cases} \frac{n}{8} + \frac{191}{324} + \frac{27n^2-192n+64}{162\cdot 2^n} - \frac{(3n-10)^2}{81\cdot 4^n}, & \textit{if } n \textit{ is even} \\ \frac{n}{8} + \frac{367}{648} + \frac{27n^2-195n+74}{162\cdot 2^n} - \frac{(3n-10)^2}{81\cdot 4^n}, & \textit{if } n \textit{ is odd} \end{cases} .$$

Proof. Due to $V(O_n) = E(O_n^2) - E^2(O_n)$ and $E(O_n)$ has been known, we can calculate $E(O_n^2)$ in the first.

$$\begin{aligned} E(O_n^2) &= \sum_{o=0}^{n} o^2 \cdot Pr\{O_n = o\} \\ &= 2^{-n} \sum_{L=0}^{n} \sum_{o=0}^{L} o^2 \cdot NL_n(L, o). \end{aligned} \tag{29}$$

Due to the form of the expression (13), we can partition $\sum_{L=0}^{n} \sum_{o=0}^{L} o^2 \cdot NL_n(L, o)$ by the value of L,

$$\begin{aligned} &\sum_{L=0}^{n} \sum_{o=0}^{L} o^2 \cdot NL_n(L, o) \\ =&\sum_{o=0}^{0} o^2 \cdot NL_n(0, o) + \sum_{L=1}^{\lfloor n/2 \rfloor} \sum_{o=1}^{L} o^2 \cdot NL_n(L, o) \\ &+ \sum_{L=\lfloor n/2 \rfloor+1}^{n-1} \sum_{o=1}^{L} o^2 \cdot NL_n(L, o) + \sum_{o=1}^{n} o^2 \cdot NL_n(n, o) \\ =&n^2 + \sum_{L=1}^{\lfloor n/2 \rfloor} \sum_{o=1}^{L} o^2 \cdot NL_n(L, o) + \sum_{L=\lfloor n/2 \rfloor+1}^{n-1} \sum_{o=1}^{L} o^2 \cdot NL_n(L, o). \end{aligned} \tag{30}$$

Then we calculate the two sums in the right of formula (30) separately. And because $\lfloor n/2 \rfloor$ is dependent on the parity of n, we consider odd and even values of n separately.

n even:

$$
\begin{aligned}
&\sum_{L=1}^{\lfloor n/2 \rfloor} \sum_{o=1}^{L} o^2 \cdot NL_n(L,o) \\
=&\sum_{L=1}^{n/2} \sum_{o=1}^{L} o^2 \cdot NL_n(L,o) \\
=&\sum_{L=1}^{n/2} \sum_{o=1}^{L} o^2 \cdot \mathrm{C}_{L-1}^{o-1} 2^L \\
=&\sum_{L=1}^{n/2} 2^L \sum_{i=0}^{L-1} (i+1)^2 \cdot \mathrm{C}_{L-1}^{i} \qquad (\text{let } i = o-1) \\
=&\sum_{L=1}^{n/2} 2^L \sum_{i=0}^{L-1} (2\mathrm{C}_i^2 + 3\mathrm{C}_i^1 + 1) \cdot \mathrm{C}_{L-1}^{i} \\
=&\sum_{L=1}^{n/2} 2^L (2\mathrm{C}_{L-1}^2 2^{L-3} + 3\mathrm{C}_{L-1}^1 2^{L-2} + 2^{L-1}) \\
&\text{(by formula (18), (17) and (16))} \\
=&2^{-2} \sum_{L=1}^{n/2} (\mathrm{C}_L^2 + 2\mathrm{C}_L^1) 4^L \\
=&\frac{(9n^2 + 42n - 16)2^{n-3} + 2}{27}. \quad \text{(by formula (21) and (20))}
\end{aligned} \tag{31}
$$

And by formula (13) we have

$$
\begin{aligned}
&\sum_{L=\lfloor n/2 \rfloor + 1}^{n-1} \sum_{o=1}^{L} o^2 \cdot NL_n(L,o) \\
=&\sum_{L=n/2+1}^{n-1} \sum_{o=1}^{L} o^2 \cdot (I_o \cdot \mathrm{C}_{n-L-1}^{o-2L+n-1} + I_e \cdot \mathrm{C}_{n-L-1}^{o-1}) 2^{n-L} \\
=&\sum_{L=n/2+1}^{n-1} 2^{n-L} (\sum_{o=1}^{L} I_o \cdot o^2 \cdot \mathrm{C}_{n-L-1}^{o-2L+n-1} + \sum_{o=1}^{L} I_e \cdot o^2 \cdot \mathrm{C}_{n-L-1}^{o-1}),
\end{aligned} \tag{32}
$$

where

$$
I_o = \begin{cases} 1, & 2L - n < o \le L \\ 0, & otherwise \end{cases}, \quad I_e = \begin{cases} 1, & 1 \le o \le n - L \\ 0, & otherwise \end{cases}.
$$

Due to the way that I_o and I_e change by the value of o, we get

$$\begin{aligned}
&\sum_{o=1}^{L} I_o \cdot o^2 \cdot \mathrm{C}_{n-L-1}^{o-2L+n-1} \\
=&\sum_{o=2L-n+1}^{L} o^2 \cdot \mathrm{C}_{n-L-1}^{o-2L+n-1} \\
=&\sum_{i=0}^{n-L-1} (i+2L-n+1)^2 \cdot \mathrm{C}_{n-L-1}^{i}, \qquad (\text{let } i = o-2L+n-1) \qquad (33)
\end{aligned}$$

and

$$\begin{aligned}
&\sum_{o=1}^{L} I_e \cdot o^2 \cdot \mathrm{C}_{n-L-1}^{o-1} \\
=&\sum_{o=1}^{n-L} o^2 \cdot \mathrm{C}_{n-L-1}^{o-1} \\
=&\sum_{i=0}^{n-L-1} (i+1)^2 \cdot \mathrm{C}_{n-L-1}^{i}. \qquad (\text{let } i = o-1) \qquad (34)
\end{aligned}$$

Now, combining (32), (33) and (34), we get

$$
\begin{aligned}
&\sum_{L=n/2+1}^{n-1}\sum_{o=1}^{L} o^2\cdot NL_n(L,o)\\
=&\sum_{L=n/2+1}^{n-1} 2^{n-L}\sum_{i=0}^{n-L-1}(2i^2+2(2L-n+2)i+1+(2L-n+1)^2)\mathrm{C}_{n-L-1}^{i}\\
=&\sum_{L=n/2+1}^{n-1} 2^{n-L}\sum_{i=0}^{n-L-1}(4\mathrm{C}_i^2+2(2L-n+3)\mathrm{C}_i^1+(2L-n+1)^2+1)\mathrm{C}_{n-L-1}^{i}\\
=&\sum_{L=n/2+1}^{n-1} 2^{n-L}(4\mathrm{C}_{n-L-1}^{2}2^{n-L-3}+2(2L-n+3)\mathrm{C}_{n-L-1}^{1}2^{n-L-2}\\
&+((2L-n+1)^2+1)2^{n-L-1}) \quad \text{(by formula (18), (17), and (16))}\\
=&2^{-2}\sum_{L=n/2+1}^{n-1}(5L^2+(1-4n)L+n^2+n)4^{n-L}\\
=&2^{-2}\sum_{i=n/2-1}^{1}(5(n-i)^2+(1-4n)(n-i)+n^2+n)4^{i} \quad (\text{let } i=n-L)\\
=&2^{-1}\sum_{i=1}^{n/2-1}(5\mathrm{C}_i^2+(2-3n)\mathrm{C}_i^1+n^2+n)4^{i}\\
=&\frac{(9n^2+102n+448)2^{n-4}-18n^2-36n-28}{27}.
\end{aligned}
\tag{35}
$$

(by formula (21), (20) and (19))

Finally, combing (29), (30), (31) and (35), we obtain the expectation of O_n^2 when n is even:

$$
\begin{aligned}
E(O_n^2)=&2^{-n}(n^2+\frac{(9n^2+42n-16)2^{n-3}+2}{27}\\
&+\frac{(9n^2+102n+448)2^{n-4}-18n^2-36n-28}{27})\\
=&\frac{n^2}{16}+\frac{31n}{72}+\frac{26}{27}+\frac{9n^2-36n-26}{27\cdot 2^n},
\end{aligned}
\tag{36}
$$

and then by Theorem 0.2, we get the variance of O_n when n is even,

$$
\begin{aligned}
V(O_n)=&E(O_n^2)-E^2(O_n)\\
=&\frac{n^2}{16}+\frac{31n}{72}+\frac{26}{27}+\frac{9n^2-36n-26}{27\cdot 2^n}-(\frac{n}{4}+\frac{11}{18}+\frac{3n-10}{9\cdot 2^n})^2\\
=&\frac{n}{8}+\frac{191}{324}+\frac{27n^2-192n+64}{81\cdot 2^{n+1}}-\frac{(3n-10)^2}{81\cdot 4^n}.
\end{aligned}
\tag{37}
$$

The variance of O_n when n is odd can be similarly calculated as it is calculated when n is even. $\square$