2.Statement of the Main Result and Proof of Main Theorems

By using the formula of $(f_{2n})_*$, we find out the following result.

Theorem 1. The generators of $H_*(Y_2, Z/2)$ of the type $b_{odd}b_{odd}$ must be

$$b_{2^k+2t+1}b_{2^{k+1}n+2^{k+1}-1},$$

where $n \geq 0, k \geq 1$ and $-1 \leq 2t+1 < 2^k - 1$.

Proof of Main Theorems

We know that $H_*(Y_2, Z/2) = \ker(f_2)_*$. In order to prove the theorem, we have to discuss the following five cases:

Case1 $b_m^2 \notin \ker(f_2)_*$, where $m > 0$.

The remainder cases must satisfy the condition $r < s$ of $b_r b_s$.

Case2 $b_{2^k-1}b_{2^{k+1}n+2v+1} \notin \ker(f_2)_*$, where $k \geq 1$, $n \geq 0$, and $1 \leq 2v+1 < 2^{k+1} - 1$.

Case3 $b_{2^k+2t+1}b_{2^{k+1}n+2v+1} \notin \ker(f_2)_*$, where $k \geq 1$, $n > 0$, and $1 \leq 2v+1 \leq 2^k + 2t + 1 < 2^{k+1} - 1$.

Case4 $b_{2^k+2t+1}b_{2^{k+1}n+2^k+2l+1} \notin \ker(f_2)_*$, where $k \geq 2, n \geq 0$ and $1 \leq 2t+1 \leq 2l+1 < 2^k - 1$.

Case5 $b_{2^k+2t+1}b_{2^{k+1}n+2^{k+1}-1} \in \ker(f_2)_*$.

We need some lemmas.

Lamma 2. Let $0 \leq b \leq a$, if $a = \sum_{m=0}^{h} a_m 2^m, b = \sum_{m=0}^{h} b_m 2^m$, then

$$\binom{a}{b} \equiv \Pi_{m=0}^{h} \binom{a_m}{b_m} (\mathrm{mod}\, 2), \text{ where } a_m, b_m = 0 \text{ or } 1.$$

Proof. The prove follows N.E.Steenrod[3]. In the polynomial ring $Z_2[x]$, we have $(1+x)^2 = 1+x^2$. It follows by induction on m that $(1+x)^{2^m} = 1+x^{2^m}$. Therefore

$(1+x)^a = (1+x)^{\sum_{m=0}^{h} a_m 2^m} = \Pi_{m=0}^{h}(1+x)^{a_m 2^m} = \Pi_{m=0}^{h}(1+x^{2^m})^{a_m} = \Pi_{m=0}^{h} \sum_{s=0}^{a_m} \binom{a_m}{s} x^{s \times 2^m}$.

The coefficient of $x^b = x^{\sum_{m=0}^{h} b_m 2^m}$ in the usual expansion of $(1+x)^a$ is $\binom{a}{b}$. But, from the above expansion, we see that it is $\Pi_{m=0}^{h} \binom{a_m}{b_m}$.

From this Lemma , we can easily get some results.

(2-1) $\binom{a}{b} \equiv 0 (\mathrm{mod}\, 2)$, If a is even , b is odd.

(2-2) $\binom{2a+1}{2b+1} \equiv \binom{2a}{2b} \equiv \binom{a}{b} (\mathrm{mod}\, 2)$.

(2-3) $\binom{2^k n + a}{b} \equiv 0 (\mathrm{mod}\, 2)$, if $n \geq 1$, $a < b < 2^k$.

Case1

Proof. We separate $(f_2)_*(b_m^2) = \sum \frac{(i+j)!}{i!j!} b_{i+j} b_{m-i} b_{m-j}$ into three parts, $\sum_{0 \leq i < j \leq m} \frac{(i+j)!}{i!j!} b_{i+j} b_{m-i} b_{m-j}$, $\sum_{0 \leq j < i \leq m} \frac{(i+j)!}{i!j!} b_{i+j} b_{m-i} b_{m-j}$, and $\sum_{0 \leq i \leq m} \frac{(2i)!}{i!i!} b_{2i} b_{m-i}^2$.

Clearly that the first two parts are the same and the coefficient of each term in the last part are congruent to zero modulo 2 except $i = 0$, thus $(f_2)_*(b_m^2) = b_m^2$ in $H_*(BO(3); Z/2)$.

Case2

Proof. Since $b_{2^k-1} b_{2^{k+1}n+2v+1} \xrightarrow{(f_2)_*} \sum_{\substack{0 \leq i \leq 2^k-1 \\ 0 \leq j \leq 2^{k+1}n+2v+1}} \binom{i+j}{i} b_{i+j} b_{(2^k-1)-i} b_{(2^{k+1}n+2v+1)-j}$.

We observe $2^{k+1}n + 2v + 1$ as two parts: $1 \leq 2v+1 \leq 2^k - 1$ (under $n > 0$), and $2^k + 1 \leq 2v + 1 < 2^{k+1} - 1$.

If $1 \leq 2v+1 \leq 2^k - 1$, we take $i = 2v+1$, $j = 2^k n$, then we have $b_{2^k n+2v+1} b_{2^k-1-i} b_{2^k n+2v+1}$ with the coefficient $\binom{i+j}{i} = \binom{2^k n + 2v + 1}{2^k n} \equiv \binom{2^k n}{2^k n}\binom{2v+1}{0} \equiv 1 (\mathrm{mod}\, 2)$. Since $H_*(BO(3); Z/2)$ is abelian, for this term $b_{2^k n+2v+1} b_{2^k-1-i} b_{2^k n+2v+1}$, we may take the choices of i, j to produce such term in the combination of $(f_2)_*(b_{2^k-1} b_{2^{k+1}n+2v+1})$. They are $b_{2^k-1-i} b_{2^k n+2v+1} b_{2^k n+2v+1}$ and $b_{2^k n+2v+1} b_{2^k n+2v+1} b_{2^k-1-i}$.Clearly, there is only one choice of i, j to produce such term(since $2^k n + 2v + 1 > 2^k - 1$).

If $2^k + 1 \leq 2v + 1 < 2^{k+1} - 1$, we rewrite $2v+1$ as $2^k + 2l + 1$, where $1 \leq 2l + 1 < 2^k - 1$. We take $j = 2^{k+1}n + 2^k$, $i = 2^k - 1 - (2l+1)$.

We have the term $b_{i+j} b_{(2^k-1)-i} b_{(2^{k+1}n+2^k+2l+1)-j} = b_{2^{k+1}n+2^{k+1}-(2l+2)} b_{2l+1} b_{2l+1}$ with the coefficient $\binom{i+j}{i} = \binom{i+j}{j} = \binom{2^{k+1}n + 2^{k+1} - (2l+2)}{2^{k+1}n + 2^k} \equiv \binom{2^{k+1}n}{2^{k+1}n}\binom{2^{k+1} - (2l+2)}{2^k} \equiv \binom{2^{k+1} - (2l+2)}{2^k} (\mathrm{mod}\, 2)$(by Lemma2).

Let $2^{k+1} - (2l+2) = \sum_{m=0}^{k+1} a_m 2^m$, then $a_{k+1} = 0$ and $a_k = 1$ (since $1 \leq 2l + 1 < 2^k - 1 \Rightarrow 2 \leq 2l + 2 < 2^k$).

By Lemma 2, $\binom{i+j}{i} = \binom{2^{k+1}-(2l+2)}{2^k} \equiv \binom{1}{1}\prod_{m=0}^{k-1}\binom{a_m}{0} \equiv 1(\mathrm{mod}\,2)$.

As above, for this term $b_{2^{k+1}n+2^{k+1}-(2l+2)}b_{2l+1}b_{2l+1}$, we also have $b_{2l+1}b_{2^{k+1}n+2^{k+1}-(2l+2)}b_{2l+1}$ and $b_{2l+1}b_{2l+1}b_{2^{k+1}n+2^{k+1}-(2l+2)}$ in the combination of $(f_2)_*(b_{2^k-1}b_{2^{k+1}n+2^k+2l+1})$, but they do not exist. First, we consider $b_{2l+1}b_{2^{k+1}n+2^{k+1}-(2l+2)}b_{2l+1}$. We must choose i, such that $(2^k-1)-i = 2^{k+1}n+2^{k+1}-(2l+2) \Rightarrow i = (2^k-1)-[2^{k+1}n+2^{k+1}-(2l+2)] = -2^{k+1}n-2^k+2l+1$

$< -2^{k+1}n-2^k+2^k-1<0 \rightarrow\leftarrow$(since $1 \le 2l+1 < 2^k-1$).

We consider $b_{2l+1}b_{2l+1}b_{2^{k+1}n+2^{k+1}-(2l+2)}$. We have to choose i, such that $(2^k-1)-i = 2l+1$, then we have the coefficient $\binom{i+j}{i} = \binom{2l+1}{(2^k-1)-(2l+1)}$.

Let $2l+1 = \sum_{m=0}^{k-1} b_m 2^m$ and $2^k-1 = \sum_{m=0}^{k-1} 1\times 2^m$

$\Rightarrow (2^k-1)-(2l+1) = \sum_{m=0}^{k-1}(1-b_m)\times 2^m$.

We can find w such that $b_w = 0$ (since $2l+1 < 2^k-1$), therefore $\binom{b_w}{1-b_w} \equiv \binom{0}{1} \equiv 0(\mathrm{mod}\,2)$ (by Lemma 2) . Hence $\binom{i+j}{i} \equiv 0 \pmod 2$, that is $b_{2l+1}b_{2l+1}b_{2^{k+1}n+2^{k+1}-(2l+2)}$ also does not exist.

By the discussion above, $(f_2)_*(b_{2^k-1}b_{2^{k+1}n+2^k+2l+1}) \neq 0 \Rightarrow b_{2^k-1}b_{2^{k+1}n+2^k+2l+1} \notin \ker(f_2)_*$.■

Case3

Proof. We take $j = 2^{k+1}n$, and $i = 2^k+2t-2v$, then we have $b_{2^{k+1}n+2^k+2t-2v}b_{2v+1}b_{2v+1}$ with the coefficient $\binom{i+j}{i} = \binom{i+j}{j} = \binom{2^{k+1}n+2^k+2t-2v}{2^{k+1}n} \equiv \binom{n}{n}\binom{2^k+2t-2v}{0} \equiv 1(\mathrm{mod}\,2)$ (by Lemma 2). There doesn't exist any choice of i,j to produce such term, since $2^{k+1}n+2^k+2t-2v \ge 2^{k+1}n \ge 2^{k+1} > 2^k+2t+1$.

Hence $(f_2)_*(b_{2^k+2t+1}b_{2^{k+1}n+2v+1}) \neq 0$, that is $b_{2^k+2t+1}b_{2^{k+1}n+2v+1} \notin \ker(f_2)_*$.

Case4

We need a lemma.

Lemm 3. Given $c \ge 0, d \ge 1$, if

$$\binom{2c+j}{2c} + \binom{2c+2d-j}{2c} \equiv 0(\mathrm{mod}\,2),$$

$\forall\ j, d > j \ge 0$, then $\binom{2c+m}{2c} \equiv 1(\mathrm{mod}\,2)$, $d > m \ge 0$.

Proof. We prove by induction hypothesis on m.

$m = 0$, since $\binom{2c+0}{2c} \equiv \binom{2c}{2c} \equiv 1 (\mathrm{mod}\, 2)$, this lemma is true.
Suppose $m = n$ (n must less then $d-1$), this lemma is also true.
when $m = n+1$,
If n is even, $\binom{2c+n}{2c-1} \equiv 0 (\mathrm{mod}\, 2)$ (by (2-1), $\binom{even}{odd} \equiv 0 (\mathrm{mod}\, 2)$),
by induction hypothesis $\binom{2c+n}{2c} \equiv 1 (\mathrm{mod}\, 2)$, and we know

$$\binom{2c+(n+1)}{2c} = \binom{2c+n}{2c-1} + \binom{2c+n}{2c},$$

hence $\binom{2c+(n+1)}{2c} \equiv 0 + 1 \equiv 1 (\mathrm{mod}\, 2)$.
If n is odd, we have $\binom{2c+2d-(n+1)}{2c-1} \equiv 0 (\mathrm{mod}\, 2)$ (by (2-1)).
We know that

$$\binom{2c+2d-n}{2c} = \binom{2c+2d-(n+1)}{2c-1} + \binom{2c+2d-(n+1)}{2c}.$$

According to the condition, we know that $\binom{2c+n}{2c} \equiv \binom{2c+2d-n}{2c} (\mathrm{mod}\, 2)$, and $\binom{2c+(n+1)}{2c} \equiv \binom{2c+2d-(n+1)}{2c} (\mathrm{mod}\, 2)$.
Therefore $\binom{2c+(n+1)}{2c} + \binom{2c+2d-(n+1)}{2c-1} \equiv \binom{2c+n}{2c} (\mathrm{mod}\, 2)$.
If n is odd, we have $\binom{2c+2d-(n+1)}{2c-1} \equiv 0 (\mathrm{mod}\, 2)$ (by (2-1)), and by induction hypothesis, $\binom{2c+n}{2c} \equiv 1 (\mathrm{mod}\, 2)$. Hence $\binom{2c+(n+1)}{2c} + 0 \equiv 1 (\mathrm{mod}\, 2)$, which implies $\binom{2c+(n+1)}{2c} \equiv 1 (\mathrm{mod}\, 2)$.
By induction hypothesis, this lemma holds. ■

Corollary 4. Give $c \geq 0, d \geq 1$, if $\forall\ j, d > j \geq 0$ such that

$$\binom{2c+j}{2c} + \binom{2c+2d-j}{2c} \equiv 0 (\mathrm{mod}\, 2),$$

then $\binom{2c+d}{2c} \equiv 1(\mathrm{mod}\,2)$.

Proof.

If d is odd, we have $\binom{2c+d}{2c} = \binom{2c+(d-1)}{2c-1} + \binom{2c+(d-1)}{2c}$.

By Lemma3, $\binom{2c+(d-1)}{2c} \equiv 1(\mathrm{mod}\,2)$, and by (2-1),

$\binom{2c+(d-1)}{2c-1} \equiv 0(\mathrm{mod}\,2)$, therefore $\binom{2c+d}{2c} \equiv 1+0 \equiv 1(\mathrm{mod}\,2)$.

If d is even, we have $\binom{2c+(d+1)}{2c} = \binom{2c+d}{2c-1} + \binom{2c+d}{2c}$. Clearly

$\binom{2c+d}{2c-1} \equiv 0(\mathrm{mod}\,2)$, and by condition and Lemma3 we know $\binom{2c+(d+1)}{2c} \equiv \binom{2c+2d-(d-1)}{2c} \equiv \binom{2c+(d-1)}{2c} \equiv 1(\mathrm{mod}\,2)$.

Hence $\binom{2c+(d+1)}{2c} = \binom{2c+d}{2c-1} + \binom{2c+d}{2c} \Rightarrow 1 \equiv 0 + \binom{2c+d}{2c}(\mathrm{mod}\,2)$,

which implies $\binom{2c+d}{2c} \equiv 1(\mathrm{mod}\,2)$.

By the cases above, we know $\binom{2c+d}{2c} \equiv 1(\mathrm{mod}\,2)$. ■

In the case3, we consider the formula $b_{2^k+2t+1} b_{2^{k+1}n+2^k+2l+1} \notin \ker(f_2)_*$, where $k, l, t \in Z, k \geq 3, n \geq 0$ and $1 \leq 2t+1 \leq 2l+1 < 2^k-1$(if $n = 0, 2t+1 < 2l+1$), then we have the equation : $0 \leq t \leq l < 2^{k-1}-1$ (if $n = 0, t < l$). Now we denote $r = 2^k + 2t + 1, s = 2^{k+1}n + 2^k + 2l + 1$, and $r < s$.

Proposition 5. If any one of the following statement is true, then the case4 is true.

(a) If there exists I, where $0 < I \leq r$,

such that $\binom{s+I}{s} + \binom{s+I}{r} \equiv 1(\mathrm{mod}\,2)$.

(b) If there exist J, where $0 \leq J < \frac{s-r}{2}$,

such that $\binom{r+J}{r} + \binom{s-J}{r} \equiv 1(\mathrm{mod}\,2)$.

(c) $\binom{\frac{s+r}{2}}{r} \equiv 1(\mathrm{mod}\,2)$.

If any one of them holds ,then $b_r b_s \notin \ker (f_2)_*$.

Proof of (a) Since $b_r b_s \xrightarrow{(f_2)_*} \sum_{\substack{0\le i\le r\\ 0\le j\le s}} \binom{i+j}{i} b_{i+j} b_{r-i} b_{s-j}$, now we take $j = s, i = I$, for some $I, 0 < I \le r$, then we have the term $b_{s+I} b_{r-I} b_0$ with the coefficient $\binom{s+I}{s}$.

Since $H_*(BO(3); Z/2)$ is abelian, there are five kinds of formulas to produce such term except the case above.

For example, we take $j = s - r + I, i = r$,then we have $b_{i+j} b_{r-i} b_{s-j} = b_{s+I} b_0 b_{r-I}$.

There are the other four kinds of possible formulas: $b_{r-I} b_0 b_{s+I}, b_0 b_{r-I} b_{s+I}$ (they don't exist, since $I > 0 \Rightarrow s + I > s \to\leftarrow$), $b_{r-I} b_{s+I} b_0$ and $b_0 b_{s+I} b_{r-I}$ (they don't exist, since $I > 0 \Rightarrow s + I > s > r \to\leftarrow$) .

Hence we have only two formulas to produce this term. They are $b_{s+I} b_{r-I} b_0$ with the coefficient $\binom{s+I}{s}$ and $b_{s+I} b_0 b_{r-I}$ with the coefficient $\binom{s+I}{r}$.

If we can find some I, where $0 < I \le r$, such that $\binom{s+I}{s} + \binom{s+I}{r} \equiv 1 (\mathrm{mod}\, 2)$, this term $b_{s+I} b_{r-I} b_0$ survives in the image of $(f_2)_*$, therefore $b_r b_s \notin \ker (f_2)_*$. ■

Proof of (b) By the method above, we take $i = r$, $j = J$, for some J ($0 \le J < \frac{s-r}{2}$) , then we have $b_{r+J} b_0 b_{s-J}$ with the coefficient $\binom{r+J}{r}$.

If we choose $J = 0$, then there four kinds of formula to represent this term : $b_r b_0 b_s$, $b_s b_0 b_r$, $b_0 b_r b_s$, $b_s b_r b_0$, but the coefficient of $b_0 b_r b_s$ is $\binom{0}{0} \equiv 1 (\mathrm{mod}\, 2)$, the coefficient of $b_s b_r b_0$ is $\binom{s}{0} \equiv 1 (\mathrm{mod}\, 2)$, they cancel each other.

If $\binom{r}{r} + \binom{s}{r} \equiv 1 (\mathrm{mod}\, 2)$, where $\binom{r}{r}$ is the coefficient of $b_r b_0 b_s$, and $\binom{s}{r}$is the coefficient of $b_s b_0 b_r$, then this term will survive. Hence $b_r b_s \notin \ker (f_2)_*$.

If $0 < J < \frac{s-r}{2}$, it is easy to see $r < \frac{s+r}{2} < s - J < s$. So we only have two kinds of choices: $b_{r+J}b_0b_{s-J}$ with the coefficient $\binom{r+J}{r}$ and $b_{s-J}b_0b_{r+J}$ with the coefficient $\binom{s-J}{r}$. If we can find some $J, 0 < J < \frac{s-r}{2}$, such that $\binom{r+J}{r} + \binom{s-J}{r} \equiv 1 (\mathrm{mod}\, 2)$, then $b_r b_s \notin \ker (f_2)_*$. ■

Proof of (c) In this condition, we take $i = r$, $j = \frac{s-r}{2}$, then we have this term $b_{\frac{s+r}{2}}b_0b_{\frac{s+r}{2}}$. There is only one formula to produce this term. It is $b_{\frac{s+r}{2}}b_0b_{\frac{s+r}{2}}$ with the coefficient $\binom{\frac{s+r}{2}}{r}$. If $\binom{\frac{s+r}{2}}{r} \equiv 1 (\mathrm{mod}\, 2)$, then $b_r b_s \notin \ker (f_2)_*$.■

We will prove case4 by considering the four parts.

P.1 l is odd , t is even .

P.2 l is even , t is odd .

P.3 l is even , t is even .

P.4 l is odd , t is odd .

We denoted that $r = 2^k + 2t + 1, s = 2^{k+1}n + 2^k + 2l + 1$.

Proof of P.1 l is odd , t is even :

We want to find I ($0 < I \leq r$) such that $\binom{s+I}{s} + \binom{s+I}{r} \equiv 1 (\mathrm{mod}\, 2)$.

We may choose that I is even, such that $I = 2\ I_1$. Since $0 < I \leq r = 2^k + 2t + 1 \Rightarrow 0 < 2I_1 \leq 2^k + 2t \Rightarrow 0 < I_1 \leq 2^{k-1} + t$.

We let $l + 1 = \sum_{m=1}^{h} a_m 2^m, t = \sum_{m=1}^{h} b_m 2^m$, where $a_m, b_m = 1$ or 0, and both of them are even, so m starts from 1. Since $0 \leq t < l < 2^{k-1} - 1 \Rightarrow l + 1 < 2^{k-1}$, therefore $h < k - 1$.

Now we take $I_1 = 1 + \sum_{m=1}^{h} c_m 2^m$, where $c_m = \begin{cases} 1 & \text{if } a_m < b_m \\ 0 & \text{if } a_m \geq b_m \end{cases}$.

Since $\binom{s+2I_1}{s} = \binom{2^{k+1}n + 2^k + 2l + 1 + 2I_1}{2^{k+1}n + 2^k + 2l + 1} \equiv \binom{2^k n + 2^{k-1} + l + I_1}{2^{k+1}n + 2^{k-1} + l}$ $(\mathrm{mod}\, 2)$(by (2-2)).

By (2-1), $\binom{2^k n + 2^{k-1} + l + I_1}{2^{k+1} n + 2^{k-1} + l} \equiv 0 (\mathrm{mod}\, 2)$ (since l is odd ,$l + I_1$ is even) i.e. $\binom{s + 2I_1}{s} \equiv 0 (\mathrm{mod}\, 2)$.

Now we want to show $\binom{s + 2I_1}{r} \equiv 1 (\mathrm{mod}\, 2)$. By (2-2) again, $\binom{s + 2I_1}{r} = \binom{2^{k+1} n + 2^k + 2l + 1 + 2I_1}{2^k + 2t + 1} \equiv \binom{2^k n + 2^{k-1} + l + I_1}{2^{k-1} + t} (\mathrm{mod}\, 2)$.

Since $l + I_1 = l + 1 + \sum_{m=1}^{h} c_m 2^m = \sum_{m=1}^{h} a_m 2^m + \sum_{m=1}^{h} c_m 2^m$ $=^{denote} \sum_{m=1} d_m 2^m$, where $d_m = 1$ or 0.

By the definition of c_m, if $a_m = 1, c_m$ must be 0, therefore $a_m + c_m \leq 1$ $\Rightarrow d_m = 0 \; \forall \; m > h$. Hence $l + I_1 < 2^{h+1} \leq 2^{k-1}$ (since $h < k - 1$), it means $l + I_1 < 2^{k-1}$. By Lemma 2 we have

$$\binom{2^k n + 2^{k-1} + l + I_1}{2^{k-1} + t} \equiv \binom{2^k n}{0} \binom{2^{k-1}}{2^{k-1}} \binom{l + I_1}{t} \equiv \binom{l + I_1}{t} (\mathrm{mod}\, 2)$$

i.e. $\binom{s + 2I_1}{r} \equiv \binom{l + I_1}{t} (\mathrm{mod}\, 2)$.

Since $\binom{l + I_1}{t} \equiv \prod_{m=1}^{h} \binom{a_m + c_m}{b_m} (\mathrm{mod}\, 2)$ (by Lemma2).

If $b_m \neq 0, a_m = 0$, then $c_m = 1 \Rightarrow \binom{a_m + c_m}{b_m} \equiv \binom{0 + 1}{1} \equiv 1 (\mathrm{mod}\, 2)$.

$b_m \neq 0, a_m = 1$, then $c_m = 0 \Rightarrow \binom{a_m + c_m}{b_m} \equiv \binom{1 + 0}{1} \equiv 1 (\mathrm{mod}\, 2)$.

If $b_m = 0$, then $\binom{a_m + c_m}{b_m} \equiv \binom{a_m + c_m}{0} \equiv 1 (\mathrm{mod}\, 2)$.

Then $\binom{l + I_1}{t} \equiv \prod_{m=1}^{h} \binom{a_m + c_m}{b_m} \equiv \prod_{m=1}^{h} 1 \equiv 1 (\mathrm{mod}\, 2) \Rightarrow \binom{s + 2I_1}{r} \equiv 1 (\mathrm{mod}\, 2)$.

Hence $\binom{s + I}{s} + \binom{s + I}{r} \equiv 0 + 1 \equiv 1 (\mathrm{mod}\, 2)$, by Proposition5-(a), $b_r b_s \notin \ker (f_2)_*$. ■

Proof of P.2 l is even , t is odd:

We consider $\binom{r + J}{r} + \binom{s - J}{r}$, and we take $J = 0$. Since $\binom{s - 0}{r} = \binom{s}{r} = \binom{2^{k+1} n + 2^k + 2l + 1}{2^k + 2t + 1}$. By (2-2), we know $\binom{2^{k+1} n + 2^k + 2l + 1}{2^k + 2t + 1} \equiv$

$\binom{n}{0}\binom{2^k+2l}{2^k+2t} \equiv \binom{2^{k-1}+l}{2^{k-1}+t} (\mathrm{mod}\, 2)$. By (2-1) $\binom{2^{k-1}+l}{2^{k-1}+t} \equiv 0 (\mathrm{mod}\, 2)$, therefore

$\binom{s}{r} \equiv \binom{2^{k-1}+l}{2^{k-1}+t} \equiv 0 (\mathrm{mod}\, 2)$. Clearly, $\binom{r+0}{r} = \binom{r}{r} \equiv 1 (\mathrm{mod}\, 2)$.

Hence $\binom{r+0}{r} + \binom{s-0}{r} \equiv 1 (\mathrm{mod}\, 2)$, by Proposition5-(b), $b_r b_s \notin \ker (f_2)_*$.■

Proof of P.3 l is even , t is even :

If there exists J ($0 \leq J < \frac{s-r}{2}$) such that $\binom{r+J}{r} + \binom{s-J}{r} \equiv 1 (\mathrm{mod}\, 2)$, then we are done (by porposition7-(b)).

Suppose not, that is for all $0 \leq J < \frac{s-r}{2}$ such that $\binom{r+J}{r} + \binom{s-J}{r} \equiv 0 \equiv \binom{2^k+2t+1+J}{2^k+2t+1} + \binom{2^{k+1}n+2^k+2l+1-J}{2^k+2t+1} (\mathrm{mod}\, 2)$.

By this condition, we want to use Corollary 4 to show such r and s satisfy $\binom{\frac{s+r}{2}}{r} \equiv 1 (\mathrm{mod}\, 2)$. Hence $b_r b_s \notin \ker (f_2)_*$, by Proposition 5-(c).

We observe J is even, let $J = 2J_1, t = 2T$ and $l = 2L$ (t and l are even), $0 \leq J < \frac{s-r}{2} = 2^k n + l - t \Rightarrow 0 \leq J_1 < 2^{k-1}n + \frac{l-t}{2} = 2^{k-1}n + L - T$.

And $0 \equiv \binom{2^k+2t+1+J}{2^k+2t+1} + \binom{2^{k+1}n+2^k+2l+1-J}{2^k+2t+1} =$

$\binom{2^k+2t+1+2J_1}{2^k+2t+1} + \binom{2^{k+1}n+2^k+2l+1-2J_1}{2^k+2t+1} \equiv$

$\binom{2^{k-1}+t+J_1}{2^{k-1}+t} + \binom{2^k n+2^{k-1}+l-J_1}{2^{k-1}+t} (\mathrm{mod}\, 2)$ (by (2-2))=

$\binom{2^{k-1}+2T+J_1}{2^{k-1}+2T} + \binom{2^k n+2^{k-1}+2L-J_1}{2^{k-1}+2L} =$

$\binom{2^{k-1}+2T+J_1}{2^{k-1}+2T} + \binom{2^k n+2^{k-1}+2T+2(L-T)-J_1}{2^{k-1}+2T} \equiv$

$\binom{2^{k-1}+2T+J_1}{2^{k-1}+2T} + \binom{2^{k-1}+2T+2(2^{k-1}n+L-T)-J_1}{2^{k-1}+2T} (\mathrm{mod}\, 2)$

for all $0 \leq J_1 < 2^{k-1}n + L - T$.

By Corollary4, $\binom{2^{k-1}+2T+(2^{k-1}n+L-T)}{2^{k-1}+2T} \equiv 1 (\mathrm{mod}\, 2)$, that is

$\binom{2^{k-1}n+2^{k-1}+L+T}{2^{k-1}+2T} \equiv \binom{2^{k-1}+2T+(2^{k-1}n+L-T)}{2^{k-1}+2T} \equiv 1(\mathrm{mod}\,2)$.

Since $\binom{\frac{s+r}{2}}{r} = \binom{2^k n+2^k+l+t+1}{2^k+2t+1} =$

$\binom{2^k n+2^k+2L+2T+1}{2^k+2(2T)+1} \equiv \binom{2^{k-1}n+2^{k-1}+L+T}{2^{k-1}+2T}(\mathrm{mod}\,2)$

(by (2-2)).

Hence $\binom{\frac{s+r}{2}}{r} \equiv 1(\mathrm{mod}\,2)$.

By Proposition5-(c) , $b_r b_s \notin \ker(f_2)_*$.■

By proving the following statement, we can complete this case.

- If $r = 2^k+2t+1$ and $s = 2^{k+1}n+2^k+2l+1$ satisfy $k \geq 3, n \geq 0, 0 \leq t \leq l < 2^{k-1}-1$ (if $n = 0, t < l$), then one of the Proposition5 must hold:

  (a) If $\exists I$, where $0 < I \leq r$, such that $\binom{s+I}{s} + \binom{s+I}{r} \equiv 1(\mathrm{mod}\,2)$.

  (b) If $\exists J$,where $0 \leq J < \frac{s-r}{2}$, such that $\binom{r+J}{r} + \binom{s-J}{r} \equiv 1(\mathrm{mod}\,2)$.

  (c) $\binom{\frac{s+r}{2}}{r} \equiv 1(\mathrm{mod}\,2)$.

Proof. By induction hypothesis on k

$k = 2$,

Consider $0 \leq t \leq l < 2^{2-1}-1 = 1$, the pair of (t,l) is $(0,0)$ and $n > 0$.

Then the case holds, since the statement is true except l and t are odd.(We proved in **P.1** ,**P.2** and **P.3**).

$k = 3$,

$r = 8+2t+1, s = 16n+8+2l+1$.

Consider $0 \leq t < l < 2^{3-1}-1 = 3$, the pair of (t,l) is $(0,1)$, $(0,2)$ and $(1,2)$.

Consider $0 \leq t = l < 3$ (under $n > 0$), the pair of (t,l) is $(0,0)$, $(1,1)$, $(2,2)$.

We only have to prove the case of $(t,l) = (1,1)$, since the statement is true except l and t are odd.

If $t = 1$, i.e $r = 11$ and $s = 16n + 11$. We take $J = 4$, then $\binom{11+4}{11} + \binom{16n+7}{11} \equiv \binom{15}{11} + \binom{16n}{0}\binom{7}{11} \equiv 1 (\mathrm{mod}\, 2)$(by (b)). Hence the statement of $k = 3$ is true..

Suppose $k = q$, the statement is also true.

When $k = q + 1$

$r = 2^{q+1} + 2t + 1$, $s = 2^{q+2}n + 2^{q+1} + 2l + 1$. The statement is true except l and t are odd. We see that l and t are odd. Now, we let $l = 2L + 1$, $t = 2T + 1$, $r_1 = 2^q + 2T + 1$ and $s_1 = 2^{q+1}n + 2^q + 2L + 1$.

By induction hypothesis, one of (a),(b)or(c) is true for pair (r_1, s_1). Since $0 \le t < l < 2^q - 1 \Rightarrow 0 \le T < L < 2^{q-1} - 1$, the pair (r_1, s_1) satisfies the condition of the statement.

Now, we check (a) , (b) , (c) for (r, s),

where $r = 2^{q+1} + 2t + 1$, $s = 2^{q+2}n + 2^{q+1} + 2l + 1$

(a) $\binom{s+I}{s} + \binom{s+I}{r}$ (let $I = 2I_1$)

$\Rightarrow \binom{s+2I_1}{s} + \binom{s+2I_1}{r} =$

$\binom{2^{q+2}n + 2^{q+1} + 2l + 1 + 2I_1}{2^{q+1} + 2l + 1} + \binom{2^{q+2}n + 2^{q+1} + 2l + 1 + 2I_1}{2^{q+1} + 2t + 1} \equiv$

$\binom{2^{q+1}n + 2^q + l + 2I_1}{2^q + l} + \binom{2^{q+1}n + 2^q + l + I_1}{2^q + t}$ (by (2-2))$\equiv$

$\binom{2^{q+1}n + 2^q + 2L + 1 + I_1}{2^q + 2L + 1} + \binom{2^{q+1}n + 2^q + 2L + 1 + I_1}{2^q + 2T + 1} \equiv$

$\binom{s_1 + I_1}{s_1} + \binom{s_1 + I_1}{r_1} (\mathrm{mod}\, 2)$,

where $0 < I_1 \le r_1$

(since $0 < I = 2I_1 \le r \Rightarrow 0 < I_1 \le 2^q + t = 2^q + 2T + 1 = r_1$).

Hence $\binom{s+I}{s} + \binom{s+I}{r} \equiv \binom{s_1 + I_1}{s_1} + \binom{s_1 + I_1}{r_1} (\mathrm{mod}\, 2)$.

(b) $\binom{r+J}{r} + \binom{s-J}{r}$, by the same argument as above, we let $J = 2J_1 \Rightarrow$

$\binom{r+2J_1}{r} + \binom{s-2J_1}{r} =$

$\binom{2^{q+1} + 2t + 1 + 2J_1}{2^{q+1} + 2t + 1} + \binom{2^{q+2}n + 2^{q+1} + 2l + 1 - 2J_1}{2^{q+1} + 2t + 1} \equiv$

$\binom{2^q+t+J_1}{2^q+t}+\binom{2^{q+1}n+2^q+l-J_1}{2^q+t}$(by (2-2))$\equiv$
$\binom{2^q+2T+1+J_1}{2^q+2T+1}+\binom{2^{q+1}n+2^q+2L+1-J_1}{2^q+2T+1}\equiv$
$\binom{r_1+J_1}{r_1}+\binom{s_1-J_1}{r_1}\pmod 2$, where $0\le J_1<\frac{s_1-r_1}{2}$
(since $0\le J=2J_1<\frac{s-r}{2}\Rightarrow 0\le J_1<\frac{s-r}{2}*\frac{1}{2}=(l-t)*\frac{1}{2}=(2L-2T)*\frac{1}{2}=\frac{s_1-r_1}{2}$).

Hence $\binom{r+J}{r}+\binom{s-J}{r}\equiv\binom{r_1+J_1}{r_1}+\binom{s_1-J_1}{r_1}\pmod 2$.

(c) $\binom{\frac{s+r}{2}}{r}=\binom{2^{q+1}n+2^{q+1}+l+t+1}{2^{q+1}+2t+1}=\binom{2^{q+1}n+2^{q+1}+2L+1+2T+1+1}{2^{q+1}+2(2T+1)+1}=$
$\binom{2^{q+1}n+2^{q+1}+2(L+T+1)+1}{2^{q+1}+2(2T+1)+1}\equiv$
$\binom{2^qn+2^q+(L+T+1)}{2^q+2T+1}$(by (2-2))$\equiv\binom{\frac{s_1+r_1}{2}}{r_1}\pmod 2$.

Hence $\binom{\frac{s+r}{2}}{r}\equiv\binom{\frac{s_1+r_1}{2}}{r_1}\pmod 2$.

By induction hypothesis, one of (a),(b)or(c) is true for pair (r_1,s_1) and by above discussion , so does for pair $(r=2^{q+1}+2t+1, s=2^{q+2}n+2^{q+1}+2l+1$), when l and t are odd. Hence this statement is true.

By this statement and Proposition5, case4 is true.■

Case5

Proof.

Let $r=2^k+2t+1, s=2^{k+1}n+2^{k+1}-1$.

We want to show $(f_2)_*(b_{2^k-1}b_{2^k+2l+1})=0$. Now we take $i=I, j=J$, then we have the term $b_{I+J}b_{r-I}b_{s-J}$ with coefficient $\binom{I+J}{I}$.

Now we fix I and change J. If $J>s-I$, we let $J=s-I+(u+1)$, then we get $0\le u\le I-1$ (since $s-I+1\le J=s-I+(u+1)\le s$). Therefore $\binom{I+J}{I}=\binom{s+1+u}{I}=\binom{2^{k+1}n+2^{k+1}+u}{I}\equiv\binom{2^{k+1}n+2^{k+1}}{0}\binom{u}{I}\equiv$
$\binom{u}{I}\equiv 0\pmod 2$ (since $0\le u\le I-1$, and by (2-3)).

If $0\le J\le s-I$, under such J which we choice, we need another one to cancel it. We take $i=I$, $j=s-I-J$, then we have another term

$b_{i+j}b_{r-i}b_{s-j} = b_{s-J}b_{r-I}b_{I+J}$ with the coefficient $\binom{s-J}{I}$ except $J = s-I-J$.

We let $J = 2^{k+1}n_1 + J_1$, where $n_1 \le n, J_1 \le 2^{k+1}-1$.

Since $0 \le I \le r < 2^{k+1}-1$, we have $\binom{I+J}{I} \equiv \binom{n_1}{0}\binom{I+J_1}{I} \equiv \binom{I+J_1}{I} \pmod 2$, and $\binom{s-J}{I} = \binom{2^{k+1}(n-n_1)+2^{k+1}-1-J_1}{I} \equiv \binom{2^{k+1}-1-J_1}{I} \pmod 2$.

In order to show $\binom{I+J}{I} + \binom{s-J}{I} \equiv 0 \pmod 2$, we need a simple result, which is $\binom{a_*}{b_*} \equiv \binom{1-b_*}{1-a_*} \pmod 2$, where $a_*, b_* = 0$ or 1. By this result, we know that $\binom{A}{B} \equiv \binom{2^{k+1}-1-B}{2^{k+1}-1-A} \pmod 2$, where $B \le A \le 2^{k+1}-1$.

If $I+J_1 \le 2^{k+1}-1$, then we have $\binom{I+J_1}{I} = \binom{I+J_1}{J_1} \equiv \binom{2^{k+1}-1-J_1}{2^{k+1}-1-(I+J_1)} = \binom{2^{k+1}-1-J_1}{I} = \binom{s-J}{I} \pmod 2$. Hence $\binom{I+J}{I} + \binom{s-J}{I} \equiv 0 \pmod 2$.

If $I+J_1 > 2^{k+1}-1$, then $2^{k+1}-1-J_1 < I$, $\binom{s-J}{I} \equiv \binom{2^{k+1}(n-n_1)+2^{k+1}-1-J_1}{I} \equiv 0 \pmod 2$ (by (2-3)). We let $I + J_1 = 2^{k+1} + D$, then $0 \le D < I$ (since $I - D = 2^{k+1} - J_1$ and $J_1 \le 2^{k+1}-1$). So $\binom{I+J}{I} = \binom{2^{k+1}(n_1+1)+D}{I} \equiv 0 \pmod 2$, by (2-3) again.

Hence $\binom{I+J}{I} + \binom{s-J}{I} \equiv 0 \pmod 2$, if $0 \le J \le s-I$.

We still have to discuss $J = s-I-J$. In this case, I is odd and $J = \frac{s-I}{2}$. We want to show $\binom{I+J}{I} \equiv 0 \pmod 2$.

In our notation $s+I = 2^{k+1}(n+1)+(I-1)$, and $s-I = 2^{k+1}n+2^{k+1}-1-I$. We can see that $\binom{I+J}{I} = \binom{I+J}{J} \equiv \binom{2(I+J)}{2J}$ (by2-2)$= \binom{s+I}{s-I} \equiv \binom{2^{k+1}(n+1)}{2^{k+1}n}\binom{(I-1)}{2^{k+1}-1-I} \pmod 2$.

We focus on $\binom{(I-1)}{2^{k+1}-1-I}$. Let $I-1 = \sum_{q=1}^{k} b_q 2^q$ (since I is odd and

$I \leq r < 2^{k+1}-1)$ and $2^{k+1}-1 = \sum_{q=0}^{k} 1 \times 2^q \Rightarrow (2^{k+1}-1) - I = \sum_{q=0}^{k}(1 - b_q) \times 2^q$. We can find w such that $b_w = 0$ (since $I < 2^{k+1}-1$), therefore $\binom{b_w}{1-b_w} \equiv \binom{0}{1} \equiv 0 (\mathrm{mod}\, 2)$ (by Lemma 2). Hence $\binom{I+J}{I} \equiv 0 (\mathrm{mod}\, 2)$.

If we give arbitrary $0 \leq I \leq r$ and $0 \leq J \leq s$, then the coefficient of such "**form**" $b_{I+J}b_{r-I}b_{s-J}$ must be zero in the combination of $(f_2)_*(b_{2^k-1}b_{2^{k+1}n+2^k+2l+1})$. We can say $(f_2)_*(b_{2^k-1}b_{2^{k+1}n+2^k+2l+1}) = 0$. ■