SCIENCE CHINA
Information Sciences

• Supplementary File •

A non-alternate 3D structure and its practical security evaluation against differential and linear cryptanalysis

Qian WANG[1*] & Chenhui JIN[1]

[1]*Information Science and Technology Institute, Zhengzhou* 450001, *China*

Appendix A Proofs of Theorem 3 and Theorem 4

Lemma 1. Let $B=(b_{i,j})_{n\times n}$ be an $n\times n$ binary matrix, $b_{i,\cdot}$ and $b_{\cdot,j}$ denote the i-th row vector and the j-th column vector of B respectively, and $wt(\cdot)$ denotes the Hamming Weight. Let

$u=\max\{wt(b_{i,\cdot}):0\leqslant i<n, b_{i,\cdot}\neq 0\}$, $v=\max\{wt(b_{\cdot,j}):0\leqslant j<n, b_{\cdot,j}\neq 0\}$,

$t_1=\min\{wt(b_{i,\cdot}):0\leqslant i<n, b_{i,\cdot}\neq 0\}$, $t_2=\min\{wt(b_{\cdot,j}):0\leqslant j<n, b_{\cdot,j}\neq 0\}$,

$M=\#\{0\leqslant i<n: b_{i,\cdot}\neq 0\}$, $N=\#\{0\leqslant j<n: b_{\cdot,j}\neq 0\}$.

Then,

(1) $N\geqslant \max\{wt(b_{i,\cdot}):0\leqslant i<n\}$;

(2) $wt(B)\geqslant \max\{Nt_2+v-t_2, Mt_1+u-t_1\}$.

Proof. (1) If $b_{i,j}\neq 0$, then $b_{\cdot,j}\neq 0$. Therefore,

$$wt(b_{i,\cdot})=\#\{0\leqslant j<n: b_{i,j}\neq 0\}\leqslant \#\{0\leqslant j<n: b_{\cdot,j}\neq 0\}=N.$$

Obviously, $N\geqslant \max\{wt(b_{i,\cdot}):0\leqslant i<n\}$.

(2) Suppose $wt(b_{\cdot,h})=v$. Build a set with indexes (i,j) of non-zero components of $b_{\cdot,h}$, denoted by F. Choosing t_2 non-zero components from every non-zero column vector of B, build a set with indexes (i,j) of these $N\times t_2$ non-zero components, denoted by E. Then we get

$$wt(B)\geqslant \left|E\bigcup F\right|=|E|+|F|-\left|E\bigcap F\right|=Nt_2+v-\left|E\bigcap F\right|\geqslant Nt_2+v-t_2.$$

Similarly, apply above result to B^T, then we get $w(B)\geqslant Mt_1+u-t_1$, where B^T represents the transposition of matrix B. Thus statement (2) is true.

Corollary 1. For a state cube $A=(a_{i,j,t})$, let $t_2=\min\{N_{XY}(a_{i,\cdot,\cdot}):0\leqslant i<n, a_{i,\cdot,\cdot}\neq 0\}$, $v=\max\{N_{XY}(a_{i,\cdot,\cdot}):0\leqslant i<n\}$, $t_1=\min\{N_{XY}(a_{\cdot,j,\cdot}):0\leqslant j<n, a_{\cdot,j,\cdot}\neq 0\}$, $u=\max\{N_{XY}(a_{\cdot,j,\cdot}):0\leqslant j<n\}$, and $N_X(A)=p_1$, $N_Y(A)=q_1$, $N_Z(A)=q$. When $A\neq 0$, we have

(1) $\sum\limits_{0\leqslant j<n, a_{\cdot,\cdot,j}\neq 0}\max\{1, B_d-\min\limits_{0\leqslant i<n, a_{i,\cdot,j}\neq 0} w(a_{i,\cdot,j})\}\geqslant (q-1)\max\{1,B_d-v\}+\min\{1,B_d-t_2\}\geqslant q\max\{1,B_d-q_1\}$;

(2) $\sum\limits_{0\leqslant t<n, a_{\cdot,\cdot,t}\neq 0}\max\{1, B_d-\min\limits_{0\leqslant j<n, a_{\cdot,j,t}\neq 0} w(a_{\cdot,j,t})\}\geqslant (q-1)\max\{1,B_d-u\}+\min\{1,B_d-t_1\}\geqslant q\max\{1,B_d-p_1\}$;

(3) $N_{XY}(A)\geqslant \max\{p_1t_2+v-t_2, q_1t_1+u-t_1\}$.

Proof.

(1) Since $N_Z(A)=q$, there exist $0\leqslant s_1<s_2<\ldots<s_q<n$ satisfying $a_{\cdot,\cdot,s_c}\neq 0$ for $1\leqslant c\leqslant q$. For $1\leqslant c\leqslant q$, let $j_c=\min\{w(a_{i,\cdot,s_c}):0\leqslant i<n, a_{i,\cdot,s_c}\neq 0\}$.

We may assume $j_1\leqslant j_2\leqslant\cdots\leqslant j_q$. For $1\leqslant c\leqslant q$, let $w(a_{i^c,\cdot,s_c})=j_c$ and $e_c=\#\{0\leqslant j<n: a_{i^c,j,\cdot}\neq 0\}$. Then $v=\max\{\#\{0\leqslant j<n: a_{i,j,\cdot}\neq 0\}:0\leqslant i<n\}\geqslant e_c$ for all $1\leqslant c\leqslant q$.

For a given i^c, define a binary matrix $B=(b_{t,j})_{n\times n}$, where $b_{t,j}=\begin{cases}0, & if\ a_{i^c,j,t}=0;\\ 1, & else\end{cases}$, then by Lemma 1.(1),

$$e_c=N_{XY}(a_{i^c,\cdot,\cdot})=\#\{0\leqslant j<n: b_{\cdot,j}\neq 0\}\geqslant \max\{wt(b_{t,\cdot}):0\leqslant t<n\}=\max\{w(a_{i^c,\cdot,t}):0\leqslant t<n\}\geqslant w(a_{i^c,\cdot,s_c})=j_c.$$

* Corresponding author (email: e_alpha@163.com)

Thus $j_c \leqslant e_c \leqslant v$.

Besides, since $A \neq 0$, we know $t_2 = \min\{N_{XY}(a_{i,\cdot,\cdot}) : 0 \leqslant i < n, a_{i,\cdot,\cdot} \neq 0\} \geqslant 1$. Hence, there exist $0 \leqslant i' < n$ satisfying $N_{XY}(a_{i',\cdot,\cdot}) = t_2$, and $0 \leqslant h < n$ satisfying $a_{i',\cdot,h} \neq 0$. Since $a_{\cdot,\cdot,h} \neq 0$, $h = s_k$ holds for certain $1 \leqslant k \leqslant q$.

Now define a binary matrix $B = (b_{t,j})_{n\times n}$, where $b_{t,j} = \begin{cases} 0, \ if \ a_{i',j,t} = 0; \\ 1, \ else. \end{cases}$, then by Lemma 1.(1), we get

$$t_2 = N_{XY}(a_{i',\cdot,\cdot}) = \#\{0 \leqslant j < n : b_{\cdot,j} \neq 0\} \geqslant \max\{wt(b_{t,\cdot}) : 0 \leqslant t < n\} = \max\{w(a_{i',\cdot,t}) : 0 \leqslant t < n\} \geqslant w(a_{i',\cdot,s_k}).$$

Since $j_k = \min\{w(a_{t,\cdot,s_k}) : 0 \leqslant t < n, a_{t,\cdot,s_k} \neq 0\} \leqslant w(a_{i',\cdot,s_k}) \leqslant t_2$, we get

$$\begin{aligned}
&\sum_{0\leqslant j<n, a_{\cdot,\cdot,j}\neq 0} \max\{1, B_d - \min_{0\leqslant i<n, a_{i,\cdot,j}\neq 0} w(a_{i,\cdot,j})\} \\
=&\sum_{1\leqslant c\leqslant q} \max\{1, B_d - \min_{0\leqslant i<n, a_{i,\cdot,s_c}\neq 0} w(a_{i,\cdot,s_c})\} = \sum_{1\leqslant c\leqslant q} \max\{1, B_d - j_c\} \\
=&\sum_{1\leqslant c\leqslant q, c\neq k} \max\{1, B_d - j_c\} + B_d \max\{1, B_d - j_k\} \geqslant \sum_{1\leqslant c\leqslant q, c\neq k} \max\{1, B_d - v\} + B_d \max\{1, B_d - t_2\} \\
=&(q-1)\max\{1, B_d - v\} + \max\{1, B_d - t_2\}.
\end{aligned}$$

Now, define a binary matrix $B = (b_{i,j})_{n\times n}$, where $b_{i,j} = \begin{cases} 0, \ if \ a_{i,j,\cdot} = 0; \\ 1, \ else \end{cases}$, and by Lemma 1.(1), we get

$$q_1 = N_Y(A) = \#\{0 \leqslant j < n : b_{\cdot,j} \neq 0\} \geqslant \max\{wt(b_{i,\cdot}) : 0 \leqslant i < n\} = \max\{\#\{0 \leqslant j < n : a_{i,j,\cdot} \neq 0\} : 0 \leqslant i < n\} = v.$$

And by the definitions of v and t_2, we have $q_1 \geqslant v \geqslant t_2$. And then, $(q-1)\max\{1, B_d - v\} + \max\{1, B_d - t_2\} \geqslant (q-1)\max\{1, B_d - q_1\} + \max\{1, B_d - q_1\} = q\max\{1, B_d - q_1\}$.

Meanwhile, by Lemma 1.(2), we get $N_{XY}(A) = wt(B) \geqslant \max\{p_1 t_2 + v - t_2, q_1 t_1 + u - t_1\}$. That is to say statement (3) is true.

(2) Apply statement (1) to $(\{a_{i,j,t}\}_{i,j,t=0}^{n-1})^T = \{a_{j,i,t}\}_{i,j,t=0}^{n-1}$, and we know that statement (2) is true immediately.

(3) Already proved at the end of (1).

Lemma 2. For the differential $(a_{i,j,t}) \xrightarrow{\pi} (b_{i,j,t})$, let $p = N_Z(A)$, and $q = N_Z(B)$, then we get $p + q \geqslant B_d$ when $(a_{i,j,t}) \neq 0$.

Proof. For all $0 \leqslant i, j, t < n$, if $a_{i,j,t} \neq 0$, then $a_{\cdot,\cdot,t} \neq 0$. Thus $\#\{0 \leqslant t < n : a_{i,j,t} \neq 0\} \leqslant \#\{0 \leqslant t < n : a_{\cdot,\cdot,t} \neq 0\} = N_Z(A) = p$.

Since $(a_{i,j,t}) \neq 0$, there exist $0 \leqslant i_0, j_0, t_0 < n$ such that $a_{i_0,j_0,t_0} \neq 0$, $a_{i_0,j_0,\cdot} \neq 0$. Since the differential branch number of π is d and $b_{i,j,\cdot} = \pi(a_{i,j,\cdot})$, we get

$$\begin{aligned}
p + q &= \#\{0 \leqslant t < n : a_{\cdot,\cdot,t} \neq 0\} + \#\{0 \leqslant t < n : b_{\cdot,\cdot,t} \neq 0\} \\
&\geqslant \#\{0 \leqslant t < n : a_{i_0,j_0,t} \neq 0\} + \#\{0 \leqslant t < n : b_{i_0,j_0,t} \neq 0\} \\
&= w(a_{i_0,j_0,\cdot}) + w(b_{i_0,j_0,\cdot}) = w(a_{i_0,j_0,\cdot}) + w(\pi(a_{i_0,j_0,\cdot})) \geqslant B_d.
\end{aligned}$$

Lemma 3. For the differential trail $A^1 \xrightarrow{\theta} A^2 \xrightarrow{\pi} A^3 \xrightarrow{\theta} A^4$, let $p = N_Z(A^1)$, $q = N_Z(A^4)$. When $A^1 \neq 0$, we get

(1) If $\theta \in \tau_1$, then $a^1_{i,\cdot,t} \neq 0$ iff $a^4_{\sigma(\sigma(i,\cdot,t))} \neq 0$ for all $0 \leqslant i, t < n$, and $w(a^1_{i,\cdot,t}) + w(a^4_{\sigma(\sigma(i,\cdot,t))}) \geqslant B_d$ holds when $a^1_{i,\cdot,t} \neq 0$. If $\theta \in \tau_2$, then $a^1_{\cdot,i,t} \neq 0$ iff $a^4_{\sigma(\sigma(\cdot,i,t))} \neq 0$ for all $0 \leqslant i, t < n$, and $w(a^1_{\cdot,i,t}) + w(a^4_{\sigma(\sigma(\cdot,i,t))}) \geqslant B_d$ holds when $a^1_{\cdot,i,t} \neq 0$.

(2) $w(A^1) + w(A^4) \geqslant B_d \times \max\{p, q\}$ holds whatever $\theta \in \tau_1$ or τ_2.

(3) If $\theta \in \tau_1$, $N_Z(A^1) = N_Y(A^4)$, $N_X(A^1) = N_Z(A^4)$. If $\theta \in \tau_2$, $N_Z(A^1) = N_X(A^4)$, $N_Y(A^1) = N_Z(A^4)$.

Proof. Firstly, let $\theta \in \tau_1$.

(1) By the definitions of θ and π, for all $0 \leqslant i, t < n$, $a^1_{i,\cdot,t} = a^2_{\sigma(i,\cdot,t)}$, $a^3_{\sigma(i,\cdot,t)} = a^4_{\sigma(\sigma(i,\cdot,t))}$ and $a^3_{\sigma(i,\cdot,t)} = \pi(a^2_{\sigma(i,\cdot,t)})$, thus $a^1_{i,\cdot,t} \neq 0$ iff $a^4_{\sigma(\sigma(i,\cdot,t))} \neq 0$. When $a^1_{i,\cdot,t} \neq 0$, following inequality holds on the property of branch number $w(a^1_{i,\cdot,t}) + w(a^4_{\sigma(\sigma(i,\cdot,t))}) = w(a^2_{\sigma(i,\cdot,t)}) + w(a^3_{\sigma(i,\cdot,t)}) = w(a^2_{\sigma(i,\cdot,t)}) + w(\pi(a^2_{\sigma(i,\cdot,t)})) \geqslant B_d$.

(2) Since $N_Z(A^1) = p$, there exist $0 \leqslant t_1 < t_2 < \cdots < t_p < n$ satisfying $a^1_{\cdot,\cdot,t_s} \neq 0$ for $1 \leqslant s \leqslant p$. For $1 \leqslant s \leqslant p$, $a^1_{\cdot,\cdot,t_s} \neq 0$ means that there exists $0 \leqslant i_s < n$ satisfying $a^1_{i_s,\cdot,t_s} \neq 0$, besides, $w(a^1_{\cdot,\cdot,t_s}) + w(a^4_{\sigma(\sigma(\cdot,\cdot,t_s))}) \geqslant w(a^1_{i_s,\cdot,t_s}) + w(a^4_{\sigma(\sigma(i_s,\cdot,t_s))}) \geqslant B_d$ holds according to statement (1). Furthermore, we have $w(A^1)+w(A^4) = \sum_{t=0}^{n-1}[w(a^1_{\cdot,\cdot,t}) + w(a^4_{\sigma(\sigma(\cdot,\cdot,t))})] \geqslant \sum_{s=1}^{p}[w(a^1_{\cdot,\cdot,t_s}) + w(a^4_{\sigma(\sigma(\cdot,\cdot,t_s))})] \geqslant B_d \times p$.

Similarly, since $N_Z(A^4) = q$, there exist $0 \leqslant r_1 < r_2 < \cdots < r_q < n$ satisfying $a^4_{\cdot,\cdot,r_s} \neq 0$ for $1 \leqslant s \leqslant q$. For $1 \leqslant s \leqslant q$, $a^4_{\cdot,\cdot,r_s} \neq 0$ means that there exists $0 \leqslant j_s < n$ satisfying $a^4_{\cdot,j_s,r_s} \neq 0$, besides, $w(a^1_{\sigma^{-1}(\sigma^{-1}(\cdot,\cdot,r_s))}) + w(a^4_{\cdot,\cdot,r_s}) \geqslant w(a^1_{\sigma^{-1}(\sigma^{-1}(\cdot,j_s,r_s))}) + w(a^4_{\cdot,j_s,r_s}) \geqslant B_d$ holds. Furthermore ,we have $w(A^1)+w(A^4) = \sum_{t=0}^{n-1}[w(a^1_{\sigma^{-1}(\sigma^{-1}(\cdot,\cdot,r))}) + w(a^4_{\cdot,\cdot,r})] \geqslant \sum_{s=1}^{q}[w(a^1_{\sigma^{-1}(\sigma^{-1}(\cdot,\cdot,r_s))}) + w(a^4_{\cdot,\cdot,r_s})] \geqslant B_d \times q$.

(3) We already proved in (1) that $a^1_{i,\cdot,t}\neq 0$ iff $a^4_{\sigma(\sigma(i,\cdot,t))}\neq 0$, therefore $a^1_{\cdot,\cdot,t}\neq 0$ iff $a^4_{\sigma(\sigma(\cdot,\cdot,t))}\neq 0$, and $a^1_{i,\cdot,\cdot}\neq 0$ iff $a^4_{\sigma(\sigma(i,\cdot,\cdot))}\neq 0$. Its easy to get $N_Z(A^1)=N_Y(A^4), N_X(A^1)=N_Z(A^4)$.

Secondly, let $\theta\in\tau_2$. Since $\theta^{-1}\in\tau_1$, when applying above three conclusions to the inverse trail $A^4\xrightarrow{\theta^{-1}}A^3\xrightarrow{\pi^{-1}}A^2\xrightarrow{\theta^{-1}}A^1$, we get the results for $\theta\in\tau_2$ immediately.

Lemma 4. For the differential $A^1\xrightarrow{\pi}A^2$, we have

(1) $w(A^1)+w(A^2)\geqslant B_d\sum\limits_{j=0}^{n-1}N_{XY}(a^1_{\cdot,j,\cdot})=B_d\sum\limits_{j=0}^{n-1}N_{XY}(a^2_{\cdot,j,\cdot})$;

(2) $w(A^1)+w(A^2)\geqslant B_d\max\{\sum\limits_{j=0}^{n-1}\max\{w(a^1_{\cdot,j,i}):0\leqslant i<n\},\sum\limits_{i=0}^{n-1}\max\{w(a^1_{i,\cdot,t}):0\leqslant t<n\}\}$.

Proof. (1)

$$\begin{aligned}w(A^1)+w(A^2)&=\sum_{j=0}^{n-1}\sum_{i=0}^{n-1}[w(a^1_{i,j,\cdot})+w(a^2_{i,j,\cdot})]=\sum_{j=0}^{n-1}\sum_{i=0}^{n-1}[w(a^1_{i,j,\cdot})+w(\pi(a^1_{i,j,\cdot}))]\\&=\sum_{j=0}^{n-1}\sum_{0\leqslant i<n,a^1_{i,j,\cdot}\neq 0}[w(a^1_{i,j,\cdot})+w(\pi(a^1_{i,j,\cdot}))]\geqslant\sum_{j=0}^{n-1}\sum_{0\leqslant i<n,a^1_{i,j,\cdot}\neq 0}B_d=B_d\sum_{j=0}^{n-1}N_{XY}(a^1_{\cdot,j,\cdot}).\end{aligned}$$

Since $\pi(a^1_{i,j,\cdot})=a^2_{i,j,\cdot}$, $\sum\limits_{j=0}^{n-1}N_{XY}(a^1_{\cdot,j,\cdot})=\sum\limits_{j=0}^{n-1}N_{XY}(a^2_{\cdot,j,\cdot})$.

(2) For a given $0\leqslant j<n$, define a binary matrix $B=(b_{t,i})_{n\times n}$, where $b_{t,i}=\begin{cases}0,\ if\ a^1_{i,j,t}=0;\\1,\ else\end{cases}$,

and by Lemma 1.(1), we have $N_{XY}(a^1_{\cdot,j,\cdot})=\#\{0\leqslant i<n:b_{\cdot,i}\neq 0\}\geqslant\max\{wt(b_{i,\cdot}):0\leqslant i<n\}=\max\{w(a^1_{\cdot,j,i}):0\leqslant i<n\}$.

And then, by statement (1), we get

$$w(A^1)+w(A^2)\geqslant B_d\sum_{j=0}^{n-1}\max\{w(a^1_{\cdot,j,i}):0\leqslant i<n\}.$$

Similarly, apply above conclusion to $(\{a^1_{i,j,t}\}^{n-1}_{i,j,t=0})^T=\{a^1_{j,i,t}\}^{n-1}_{i,j,t=0}$, we get

$$w(A^1)+w(A^2)\geqslant B_d\sum_{i=0}^{n-1}\max\{w(a^1_{i,\cdot,t}):0\leqslant t<n\}.$$

Corollary 2. For the differential trail $A^1\xrightarrow{\theta\circ\pi\circ\theta}A^2\overset{\gamma}{\sim}A^2_\gamma\xrightarrow{\pi}A^3$, $A^1\neq 0$, let $t_2=\min\{N_{XY}(a^1_{i,\cdot,\cdot}):0\leqslant i<n,a^1_{i,\cdot,\cdot}\neq 0\}$, $v=\max\{N_{XY}(a^1_{i,\cdot,\cdot}):0\leqslant i<n\}$, $t_1=\min\{N_{XY}(a^1_{\cdot,j,\cdot}):0\leqslant j<n,a^1_{\cdot,j,\cdot}\neq 0\}$, $u=\max\{N_{XY}(a^1_{\cdot,j,\cdot}):0\leqslant j<n\}$, and $N_X(A^1)=p_1$, $N_Y(A^1)=q_1$, $N_Z(A^1)=q$. We have

(1) For $\theta\in\tau_1$, $w(A^2)+w(A^3)\geqslant(q-1)B_d(\max\{1,B_d-v\}+\max\{1,B_d-t_2\})\geqslant qB_d\max\{1,B_d-q_1\}$;

(2) For $\theta\in\tau_2$, $w(A^2)+w(A^3)\geqslant(q-1)B_d\max\{1,B_d-u\}+B_d\max\{1,B_d-t_1\}\geqslant qB_d\max\{1,B_d-p_1\}$.

Proof. Let $A^2_\gamma=(a^{2,\gamma}_{i,j,t})$,

(1) By Lemma 4.(2), $w(A^2)+w(A^3)=w(A^2_\gamma)+w(A^3)\geqslant B_d\sum\limits_{j=0}^{n-1}\max\{w(a^2_{\cdot,j,i}):0\leqslant i<n\}$.

By Lemma 3.(1), if $a^2_{\cdot,j,t}\neq 0$, then $a^1_{\sigma^{-1}(\sigma^{-1}(\cdot,j,t))}\neq 0$ and $w(a^1_{\sigma^{-1}(\sigma^{-1}(\cdot,j,t))})+w(a^2_{\cdot,j,t})\geqslant B_d$, indicating that $w(a^2_{\cdot,j,i})\geqslant\max\{1,B_d-w(a^1_{\sigma^{-1}(\sigma^{-1}(\cdot,j,i))})\}$.

If $a^2_{\cdot,j,\cdot}=0$, then $a^2_{\cdot,j,i}=0$ for all $0\leqslant i<n$. Obviously, $\max\{w(a^2_{\cdot,j,i}):0\leqslant i<n\}=0$.

$$\begin{aligned}w(A^2)+w(A^3)\geqslant&B_d\sum_{0\leqslant j<n,a^2_{\cdot,j,\cdot}\neq 0}\max\{w(a^2_{\cdot,j,i}):0\leqslant i<n\}\\\geqslant&B_d\sum_{0\leqslant j<n,a^2_{\cdot,j,\cdot}\neq 0}\max_{0\leqslant i<n,a^2_{\cdot,j,i}\neq 0}\max\{1,B_d-w(a^1_{\sigma^{-1}(\sigma^{-1}(\cdot,j,i))})\}\\\geqslant&B_d\sum_{0\leqslant j<n,a^1_{\sigma^{-1}(\sigma^{-1}(\cdot,j,\cdot))}\neq 0}\max_{0\leqslant i<n,a^1_{\sigma^{-1}(\sigma^{-1}(\cdot,j,i))}\neq 0}\max\{1,B_d-w(a^1_{\sigma^{-1}(\sigma^{-1}(\cdot,j,i))})\}\\=&B_d\sum_{0\leqslant t<n,a^1_{\cdot,\cdot,t}\neq 0}\max_{0\leqslant i<n,a^1_{i,\cdot,t}\neq 0}\max\{1,B_d-w(a^1_{i,\cdot,t})\}\\=&B_d\sum_{0\leqslant t<n,a^1_{\cdot,\cdot,t}\neq 0}\max\{1,B_d-\min_{0\leqslant i<n,a^1_{i,\cdot,t}\neq 0}w(a^1_{i,\cdot,t})\}.\end{aligned}$$

By Corollary 1.(1), we get

$$w(A^2)+w(A^3)\geqslant(q-1)B_d(\max\{1,B_d-v\}+\max\{1,B_d-t_2\})\geqslant qB_d\max\{1,B_d-q_1\}.$$

(2) By Lemma 4.(2),

$$w(A^2)+w(A^3)=w(A^2_\gamma)+w(A^3)\geqslant B_d\sum_{i=0}^{n-1}\max\{w(a^{2,\gamma}_{i,\cdot,t}):0\leqslant t<n\}=B_d\sum_{i=0}^{n-1}\max\{w(a^2_{i,\cdot,t}):0\leqslant t<n\}.$$

By Lemma 3.(1), if $a^2_{i,\cdot,t}\neq 0$, then $a^1_{\sigma^{-1}(\sigma^{-1}(i,\cdot,t))}\neq 0$ and $w(a^2_{i,\cdot,t})+w(a^1_{\sigma^{-1}(\sigma^{-1}(i,\cdot,t))})\geqslant B_d$, indicating that $w(a^2_{i,\cdot,t})\geqslant\max\{1,B_d-w(a^1_{\sigma^{-1}(\sigma^{-1}(i,\cdot,t))})\}$.

If $a^2_{i,\cdot,\cdot}=0$, then $a^2_{i,\cdot,t}=0$ for all $0\leqslant t<n$. Obviously, $\max\{w(a^2_{i,\cdot,t}):0\leqslant t<n\}=0$.

$$\begin{aligned}
w(A^2)+w(A^3)\geqslant&B_d\sum_{0\leqslant i<n,a^2_{i,\cdot,\cdot}\neq 0}\max\{w(a^2_{i,\cdot,t}):0\leqslant t<n\}\\
\geqslant&B_d\sum_{0\leqslant i<n,a^2_{i,\cdot,\cdot}\neq 0}\max_{0\leqslant t<n,a^2_{i,\cdot,t}\neq 0}\max\{1,B_d-w(a^1_{\sigma^{-1}(\sigma^{-1}(i,\cdot,t))})\}\\
=&B_d\sum_{0\leqslant i<n,a^1_{\sigma^{-1}(\sigma^{-1}(i,\cdot,\cdot))}\neq 0}\max_{0\leqslant t<n,a^1_{\sigma^{-1}(\sigma^{-1}(i,\cdot,t))}\neq 0}\max\{1,B_d-w(a^1_{\sigma^{-1}(\sigma^{-1}(i,\cdot,t))})\}\\
=&B_d\sum_{0\leqslant i<n,a^1_{\cdot,\cdot,i}\neq 0}\max_{0\leqslant t<n,a^1_{\cdot,t,i}\neq 0}\max\{1,B_d-w(a^1_{\cdot,t,i})\}\\
=&B_d\sum_{0\leqslant i<n,a^1_{\cdot,\cdot,i}\neq 0}\max\{1,B_d-\min_{0\leqslant t<n,a^1_{\cdot,t,i}\neq 0}w(a^1_{\cdot,t,i})\}.
\end{aligned}$$

By Corollary 1.(2), we get

$$w(A^2)+w(A^3)\geqslant(q-1)B_d\max\{1,B_d-u\}+B_d\max\{1,B_d-t_1\}\geqslant qB_d\max\{1,B_d-p_1\}.$$

For simplicity, we introduce the following three similar lemmas, and detailed proofs of them based on the "branch and bound" method are completed in the Appendix B.

Lemma 5. For function

$$\begin{aligned}
f(x)=&(x_1-1)\max\{1,B_d-x_3\}+(x_2-1)\max\{1,B_d-x_4\}+\max\{1,B_d-x_5\}\\
&+\max\{1,B_d-x_6\}+\max\{x_3x_6+x_4-x_6,x_4x_5+x_3-x_5\},
\end{aligned}$$

with $x\in R=\{(x_1,\cdots,x_6):x_i\in Z^+,x_1+x_2\geqslant B_d,x_6\leqslant x_4,x_5\leqslant x_3\}$, we have $f(x)\geqslant 3(B_d-1)$, and $f(x)=3(B_d-1)$ iff $(x_1,\cdots,x_6)\in\{(B_d-1,1,B_d-1,1,B_d-1,1),(1,B_d-1,1,B_d-1,1,B_d-1)\}$.

Lemma 6. For function

$$\begin{aligned}
f(x)=&x_8\max\{1,B_d-x_2\}+(x_1-1)\max\{1,B_d-x_3\}+(x_2-1)\max\{1,B_d-x_4\}\\
&+\max\{1,B_d-x_5\}+\max\{1,B_d-x_6\}+\max\{x_7x_6+x_4-x_6,x_4x_5+x_3-x_5\},
\end{aligned}$$

with $x\in R=\{(x_1,\cdots,x_8):x_i\in Z^+,x_1+x_2\geqslant B_d,x_7+x_8\geqslant B_d,x_6\leqslant x_4,x_5\leqslant x_3\leqslant x_7\}$, we have $f(x)\geqslant 4(B_d-1)$ and $f(x)=4(B_d-1)$ iff $(x_1,\cdots,x_8)\in\{(B_d-1,1,B_d-1,1,B_d-1,1,B_d-1,1),(1,B_d-1,1,B_d-1,1,B_d-1,1,B_d-1)\}$ when $B_d>3$, or $(x_1,\cdots,x_8)\in\{(2,1,2,1,2,1,2,1),(1,2,1,2,1,2,1,2),(1,2,2,1,2,1,2,1),(1,2,2,2,2,2,2,1)\}$ when $B_d=3$.

Lemma 7. For function

$$\begin{aligned}
f(x)=&x_{10}\max\{1,B_d-x_1\}+x_8\max\{1,B_d-x_2\}+(x_1-1)\max\{1,B_d-x_3\}+(x_2-1)\max\{1,B_d-x_4\}\\
&+\max\{1,B_d-x_5\}+\max\{1,B_d-x_6\}+\max\{x_7x_6+x_4-x_6,x_9x_5+x_3-x_5\},
\end{aligned}$$

with $x\in R=\{(x_1,\cdots,x_{10}):x_i\in Z^+,x_1+x_2\geqslant B_d,x_7+x_8\geqslant B_d,x_9+x_{10}\geqslant B_d,x_6\leqslant x_4\leqslant x_9,x_5\leqslant x_3\leqslant x_7\}$, we have $f(x)\geqslant 5(B_d-1)$, and $f(x)=5(B_d-1)$ iff $(x_1,\cdots,x_{10})\in\{(B_d-1,1,B_d-1,1,B_d-1,1,B_d-1,1,1,B_d-1),(1,B_d-1,1,B_d-1,1,1,B_d-1,1,B_d-1,1)\}$ when $B_d>3$, or $(x_1,\cdots,x_{10})\in\{(2,1,2,1,2,1,2,1,1,2),(1,2,1,2,1,2,1,2,2,1),(1,2,2,2,2,2,2,2,1,2,1),(2,2,2,2,2,2,2,2,1,2,1),(2,1,2,2,2,2,2,2,1,2,1)\}$ when $B_d=3$.

Constraints on those ten parameters $(p,q,u,v,t_1,t_2,N,h,M,r)$ of the trail (*):

Since $A^5_{\gamma,\theta}\xrightarrow{\pi}A^6$, by Lemma 2 and definitions of parameters, we get

$$p+q\geqslant B_d,n\geqslant p\geqslant 1,n\geqslant q\geqslant 1 \tag{a}$$

Define a binary matrix $B=(b_{i,j})_{n\times n}$ for the state A^6, where $b_{i,j}=\begin{cases}0,\ if\ a^6_{i,j,\cdot}=0;\\1,\ else.\end{cases}$, by Lemma 1.(1) and definitions of parameters, we get

$$n\geqslant N\geqslant u\geqslant t_1\geqslant 1,n\geqslant M\geqslant v\geqslant t_2\geqslant 1 \tag{b}$$

Since $A^7_{\gamma,\theta}\xrightarrow{\pi}A^8$, by Lemma 2 , we get

$$N+h\geqslant B_d,n\geqslant h\geqslant 1 \tag{d}$$

Since $A^3_{\gamma,\theta}\xrightarrow{\pi}A^4$, by Lemma 2, we get

$$M+r\geqslant B_d,n\geqslant r\geqslant 1 \tag{e}$$

Theorem 1. The lower bound of the number of active S-boxes in a 6-round non-trivial differential trail of the new 3D structure is $3B_d(B_d-1)$, and the necessary condition for a trail to reach the lower bound is that parameters (p,q,u,v,t_1,t_2) characterizing the trail take extreme points of corresponding function in Lemma 5. Here, B_d is the differential branch number of the MixColumn transformation π.

Proof. Consider the following 5-round subtrail of the trail (*),

$$A^3_{\gamma,\theta} \xrightarrow{\pi} A^4 \overset{\gamma}{\sim} A^4_\gamma \xrightarrow{\theta\circ\pi\circ\theta} A^5_\theta \overset{\gamma}{\sim} A^5_{\gamma,\theta} \xrightarrow{\pi} A^6 \overset{\gamma}{\sim} A^6_\gamma \xrightarrow{\theta\circ\pi\circ\theta} A^7_\theta \overset{\gamma}{\sim} A^7_{\gamma,\theta} \xrightarrow{\pi} A^8.$$

For the inverse trail $A^5_\theta \xrightarrow{\theta^{-1}\circ\pi^{-1}\circ\theta^{-1}} A^4_\gamma \overset{\gamma^{-1}}{\sim} A^4 \xrightarrow{\pi^{-1}} A^3_{\gamma,\theta}$, since $\theta^{-1}\in\tau_2$, by Corollary 2.(2), we get

$$w(A^3)+w(A^4)=w(A^3_{\gamma,\theta})+w(A^4)\geqslant (p-1)B_d\max\{1,B_d-u\}+B_d\max\{1,B_d-t_1\}.$$

For $A^6_\gamma \xrightarrow{\theta\circ\pi\circ\theta} A^7_\theta \overset{\gamma}{\sim} A^7_{\gamma,\theta} \xrightarrow{\pi} A^8$, by Corollary 2.(1), we get

$$w(A^7)+w(A^8)=w(A^7_{\gamma,\theta})+w(A^8)\geqslant (q-1)B_d\max\{1,B_d-v\}+B_d\max\{1,B_d-t_2\}.$$

For $A^5_{\gamma,\theta} \xrightarrow{\pi} A^6$, by Corollary 1.(3), we get

$$\begin{aligned} w(A^5)+w(A^6)=w(A^5_{\gamma,\theta})+w(A^6)&=\sum_{i=0}^{n-1}\sum_{j=0}^{n-1}[w(\pi^{-1}(a^6_{i,j,.}))+w(a^6_{i,j,.})]\\ &\geqslant N_{XY}(A^6)B_d\geqslant \max\{Nt_2+v-t_2,Mt_1+u-t_1\}B_d. \end{aligned}$$

The number of active S-boxes in a 6-round trail, denoted by W_6, satisfies

$$\begin{aligned} W_6=&w(A^3)+w(A^4)+w(A^5)+w(A^6)+w(A^7)+w(A^8)\\ \geqslant&(p-1)B_d\max\{1,B_d-u\}+B_d\max\{1,B_d-t_1\}+B_d\max\{Nt_2+v-t_2,Mt_1+u-t_1\}\\ &+(q-1)B_d\max\{1,B_d-v\}+B_d\max\{1,B_d-t_2\}\\ \geqslant&(p-1)B_d\max\{1,B_d-u\}+B_d\max\{1,B_d-t_1\}+B_d\max\{ut_2+v-t_2,vt_1+u-t_1\}\\ &+(q-1)B_d\max\{1,B_d-v\}+B_d\max\{1,B_d-t_2\}. \end{aligned}$$

By Lemma 5, the lower bound of W_6 under constraints (a)(b) is $3B_d(B_d-1)$, the necessary condition for W_6 to reach the lower bound is that (p,q,u,v,t_1,t_2) take extreme points in Lemma 5.

Theorem 2. The lower bound of the number of active S-boxes in an 8-round non-trivial differential trail of the new 3D structure is $4B_d(B_d-1)$, and the necessary condition for a trail to reach the lower bound is that parameters (p,q,u,v,t_1,t_2,N,h) characterizing the trail take extreme points of corresponding function in Lemma 6. Here, d is the differential branch number of the MixColumn transformation π.

Proof. Consider the following 7-round subtrail of the trail (*),

$$A^3_{\gamma,\theta} \xrightarrow{\pi} A^4 \overset{\gamma}{\sim} A^4_\gamma \xrightarrow{\theta\circ\pi\circ\theta} A^5_\theta \overset{\gamma}{\sim} A^5_{\gamma,\theta} \xrightarrow{\pi} A^6 \overset{\gamma}{\sim} A^6_\gamma \xrightarrow{\theta\circ\pi\circ\theta} A^7_\theta \overset{\gamma}{\sim} A^7_{\gamma,\theta} \xrightarrow{\pi} A^8 \overset{\gamma}{\sim} A^8_\gamma \xrightarrow{\theta\circ\pi\circ\theta} A^9_\theta \overset{\gamma}{\sim} A^9_{\gamma,\theta} \xrightarrow{\pi} A^{10}.$$

For $A^8_\gamma \xrightarrow{\theta\circ\pi\circ\theta} A^9_\theta \overset{\gamma}{\sim} A^9_{\gamma,\theta} \xrightarrow{\pi} A^{10}$, by Corollary 2.(1), we get

$$w(A^9)+w(A^{10})=w(\theta(A^9_\gamma))+w(A^{10})\geqslant hB_d\max\{1,B_d-q\}.$$

By Theorem 1, the number of active S-boxes in an 8-round trail, denoted by W_8, satisfies

$$\begin{aligned} W_8=&W_6+w(A^9)+w(A^{10})\\ \geqslant&(p-1)B_d\max\{1,B_d-u\}+B_d\max\{1,B_d-t_1\}+\max\{Nt_2+v-t_2,Mt_1+u-t_1\}B_d\\ &+(q-1)B_d\max\{1,B_d-v\}+B_d\max\{1,B_d-t_2\}+hB_d\max\{1,B_d-q\}\\ \geqslant&(p-1)B_d\max\{1,B_d-u\}+B_d\max\{1,B_d-t_1\}+\max\{Nt_2+v-t_2,vt_1+u-t_1\}B_d\\ &+(q-1)B_d\max\{1,B_d-v\}+B_d\max\{1,B_d-t_2\}+hB_d\max\{1,B_d-q\}. \end{aligned}$$

By Lemma 6, the lower bound of W_8 under constraints (a)(b)(d) is $4B_d(B_d-1)$, the necessary condition for W_8 to reach the lower bound is that (p,q,u,v,t_1,t_2,N,h) take extreme points in Lemma 6.

Theorem 3. The lower bound of the number of active S-boxes in a 10-round non-trivial differential trail of the new 3D structure is $5B_d(B_d-1)$, and the necessary condition for a trail to reach the lower bound is that parameters $(p,q,u,v,t_1,t_2,N,h,M,r)$ characterizing the trail take extreme points of corresponding function in Lemma 7. Here, d is the differential branch number of the MixColumn transformation π.

Proof. Consider the 9-round trail (*).

For the inverse trail $A^3_\theta \xrightarrow{\theta^{-1}\circ\pi^{-1}\circ\theta^{-1}} A^2_\gamma \overset{\gamma^{-1}}{\sim} A^2 \xrightarrow{\pi^{-1}} A^1_{\gamma,\theta}$, since $\theta^{-1}\in\tau_2$, by Corollary 2.(2), we get

$$w(A^1)+w(A^2)=w(A^1_{\gamma,\theta})+w(A^2)\geqslant rB_d\max\{1,B_d-p\}.$$

By Theorem 2, the number of active S-boxes in a 10-round trail, denoted by W_{10}, satisfies

$$W_{10}=w(A^1)+w(A^2)+W_8$$

$$\begin{aligned}\geqslant & rB_d\max\{1,B_d-p\}+(p-1)B_d\max\{1,B_d-u\}+B_d\max\{1,B_d-t_1\}\\ & +\max\{Nt_2+v-t_2,Mt_1+u-t_1\}B_d+(q-1)B_d\max\{1,B_d-v\}+B_d\max\{1,B_d-t_2\}+hB_d\max\{1,B_d-q\}.\end{aligned}$$

By Lemma 7, the lower bound of W_{10} under constraints (a)(b)(d)(e) is $5B_d(B_d-1)$, the necessary condition for W_{10} to reach the lower bound is that $(p,q,u,v,t_1,t_2,N,h,M,r)$ take extreme points in Lemma 7.

Theorem 4. The lower bound of the number of active S-boxes in a $2k$-round non-trivial differential trail of the new 3D structure is $kB_d(B_d-1)$, where $k\geqslant 3$, d denotes the differential branch number of the MixColumn transformation π.

Proof. We need to prove that for all $k\geqslant 3$, there exists (k_1,k_2,k_3) such that $2k=6k_1+8k_2+10k_3$ using mathematical induction at first.

1. For $k=3$, $(k_1,k_2,k_3)=(1,0,0)$;
2. Suppose that for $k'\geqslant 3$, there exists (k'_1,k'_2,k'_3) such that $2k'=6k'_1+8k'_2+10k'_3$;
3. For $k'+1$, if $k'_2\neq 0$, $2(k'+1)=6k'_1+8(k'_2-1)+10(k'_3+1)$; if $k'_2=0$ and $k'_3\neq 0$, $2(k'+1)=6(k'_1+2)+8k'_2+10(k'_3-1)$; if $k'_2=0$ and $k'_3=0$, $2(k'+1)=6(k'_1-1)+8(k'_2+1)+10k'_3$.

Therefore, for all $k\geqslant 3$, there exists (k_1,k_2,k_3) such that $2k=6k_1+8k_2+10k_3$, which means that any $2k$-round trail can be cut into some 6-round, 8-round and 10-round subtrails. By Theorem 1, Theorem 2 and Theorem 3, we know that the number of active S-boxes in a $2k$-round trail, denoted by W_{2k}, satisfies

$$W_{2k}=W_6k_1+W_8k_2+W_{10}k_3\geqslant B_d(B_d-1)(3k_1+4k_2+5k_3)=kB_d(B_d-1).$$

Appendix B Other lemmas

Lemma 8. For $x_1,x_2\geqslant 1$,$x_1+x_2\geqslant B_d$, let $y_i=\min\{x_i,B_d-1\}$, then $y_1+y_2\geqslant B_d$.

Proof.

$$y_1+y_2=\begin{cases}x_1+x_2 & if\ x_1<B_d\ and\ x_2<B_d\\ x_1+B_d-1 & if\ x_1<B_d\ and\ x_2\geqslant B_d\\ x_2+B_d-1 & if\ x_1\geqslant B_d\ and\ x_2<B_d\\ 2B_d-2 & if\ x_1\geqslant B_d\ and\ x_2\geqslant B_d\end{cases}\geqslant B_d.$$

Lemma 9. For function

$$\begin{aligned}g(x)=&x_{10}\max\{1,B_d-x_1\}+x_8\max\{1,B_d-x_2\}+(x_1-1)\max\{1,B_d-x_3\}+(x_2-1)\max\{1,B_d-x_4\}\\ &+\max\{1,B_d-x_5\}+\max\{1,B_d-x_6\}+\max\{x_7x_6+x_4-x_6,x_9x_5+x_3-x_5\},\end{aligned}$$

with $x\in D=\{(x_1,\cdots,x_{10}):x_i\in N,x_1\geqslant 1,x_2\geqslant 1,x_1+x_2\geqslant B_d,x_5\leqslant x_3\leqslant x_7,x_6\leqslant x_4\leqslant x_9\}$, define mapping φ over D that $\varphi:x=(x_1,\cdots,x_{10})\to y=(y_1,\cdots,y_{10}),y_i=\min\{x_i,B_d-1\}$. Then

(1) $\varphi(D)\subseteq D$;

(2) $\forall x\in D,g(x)\geqslant g(\varphi(x))$;

(3) For $x\in D$, if $y=\varphi(x)$ satisfies $y_3=y_5=y_7$ and $y_9=y_4=y_6$, then $g(x)=g(y)$ iff $x=y$;

(4) For any $R\subseteq D$ such that $\varphi(R)\subseteq R$, let $g_{\min}=\min\{g(x):x\in\varphi(R)\}$, $\Lambda=\{x\in\varphi(R):g(x)=g_{\min}\}$, if each element in Λ satisfies $x_3=x_5=x_7$ and $x_9=x_4=x_6$, then $\{x\in R:g(x)=g_{\min}\}=\Lambda$.

Proof. (1) $\forall x\in D,y=\varphi(x)$. For all $1\leqslant i\leqslant 10$, its clear that $y_i\leqslant x_i$. By $x_5\leqslant x_3\leqslant x_7$ and $x_6\leqslant x_4\leqslant x_9$, we get $y_5\leqslant y_3\leqslant y_7$ and $y_6\leqslant y_4\leqslant y_9$.

By Lemma 8, we know that statement (1) is true.

(2) $\forall x\in D,y=\varphi(x)$. For all $1\leqslant i\leqslant 10$, we have $y_i\leqslant x_i$, $y_i<B_d$ and $\max\{1,B_d-x_i\}=B_d-y_i$, then

$$\begin{aligned}g(x)=&x_{10}(B_d-y_1)+x_8(B_d-y_2)+(x_1-1)(B_d-y_3)+(x_2-1)(B_d-y_4)+(B_d-y_5)+(B_d-y_6)\\ &+\max\{x_7x_6+x_4-x_6,x_9x_5+x_3-x_5\}\\ \geqslant&y_{10}(B_d-y_1)+y_8(B_d-y_2)+(y_1-1)(B_d-y_3)+(y_2-1)(B_d-y_4)+(B_d-y_5)+(B_d-y_6)\\ &+\max\{y_7y_6+y_4-y_6,y_9y_5+y_3-y_5\}\\ =&g(y).\end{aligned}$$

(3) For $y=\varphi(x)$ satisfying $y_3=y_5=y_7$ and $y_9=y_4=y_6$, by the proof of (2), we know that $g(x)=g(y)$ iff $(x_1,x_2,x_8,x_{10})=(y_1,y_2,y_8,y_{10})$ and $\max\{x_7x_6+x_4-x_6,x_9x_5+x_3-x_5\}=y_5y_6$. If there exists $j\in\{3,5,7\}$ such that $x_j>y_j$, then $x_7>y_7=y_5$, $\max\{x_7x_6+x_4-x_6,x_9x_5+x_3-x_5\}\geqslant x_7x_6+x_4-x_6>y_5y_6$. Similarly, if there exists $j\in\{4,6,9\}$ such that $x_j>y_j$, then $x_9>y_9=y_6$, $\max\{x_7x_6+x_4-x_6,x_9x_5+x_3-x_5\}\geqslant x_9x_5+x_3-x_5>y_5y_6$. Thus, $g(x)=g(y)$ iff $x=y$.

(4) $\forall x\in R$, by above statement (2), we know $g(x)\geqslant g(\varphi(x))$. By above statement (3), we know that $\forall x\in R-\varphi(R)$, if $\varphi(x)\in\Lambda$, then $g(x)>g(\varphi(x))=g_{\min}$; if $\varphi(x)\notin\Lambda$, then $g(x)\geqslant g(\varphi(x))>g_{\min}$. Thus, $\{x\in R:g(x)=g_{\min}\}=\{x\in\varphi(R):g(x)=g_{\min}\}=\Lambda$.

The proof of Lemma 5. Let $g(x)$ be the function defined in Lemma 9, then,

$$f(x_1,x_2,x_3,x_4,x_5,x_6)=g(x_1,x_2,x_3,x_4,x_5,x_6,x_3,0,x_4,0).$$

Let $f_{\min}=\min\{f(x):x\in R\}$, then $\min\{f(x):x\in\varphi(R)\}=f_{\min}$ following from Lemma 9.(2). Let $\Lambda=\{x\in\varphi(R):f(x)=f_{\min}\}$. We need to consider function f_1 over $\varphi(R)$, where

$$f_1=(x_1-1)(B_d-x_3)+(x_2-1)(B_d-x_4)+(B_d-x_5)+(B_d-x_6)+(x_3x_6+x_4-x_6),$$

and $f(x)\geqslant f_1(x)$,"=" holds iff $x_3x_6+x_4-x_6\geqslant x_4x_5+x_3-x_5$.

$$\begin{aligned}f_1=&(x_1-1)(B_d-x_3)+(B_d-x_5)+(x_3x_6+x_4-x_6)+(x_2-1)(B_d-x_4)+(B_d-x_6)\\ \geqslant&(x_1-1)(B_d-x_3)+(B_d-x_5)+(x_3x_6+x_4-x_6)+(B_d-x_1-1)(B_d-x_4)+(B_d-x_6)\\ \geqslant&(x_1-1)(B_d-x_3)+(B_d-x_3)+(x_3x_6+x_4-x_6)+(B_d-x_1-1)(B_d-x_4)+(B_d-x_6)\\ =&x_1(B_d-x_3)+(x_3-2)x_6+x_4+(B_d-x_1-1)(B_d-x_4)+B_d,\end{aligned}$$

"=" holds only if $x_1+x_2=B_d, x_3=x_5$, then,
1.1 If $x_3=1$,

$$\begin{aligned}f_1=&x_1(B_d-1)+x_4+(B_d-x_1-1)(B_d-x_4)+(B_d-x_6)\\ \geqslant&x_1(B_d-1)+x_4+(B_d-x_1-1)(B_d-x_4)+(B_d-x_4)=(x_4-1)x_1+{B_d}^2+(1-B_d)x_4,\end{aligned}$$

"=" holds only if $x_4=x_6$, then,
1.1.1 If $x_4=1$,$f_1={B_d}^2-B_d+1>3B_d-3$.
1.1.2 If $x_4>1$,

$$\begin{aligned}f_1=&(x_4-1)x_1+{B_d}^2+(1-B_d)x_4\geqslant x_4-1+{B_d}^2+(1-B_d)x_4=(2-B_d)x_4-1+{B_d}^2\\ \geqslant&(2-B_d)(B_d-1)-1+{B_d}^2=3B_d-3,\end{aligned}$$

"=" holds only if $x_1=1,x_4=B_d-1$. It means $f_1(x)=3(B_d-1)$ when $x=(1,B_d-1,1,B_d-1,1,B_d-1)$, where $(x_3x_6+x_4-x_6)\geqslant(x_4x_5+x_3-x_5)$,thus $f(x)=3(B_d-1)$.
1.2 If $x_3=2$, $f_1=x_1(x_4-2)+x_4+(B_d-1)(B_d-x_4)+B_d$.
1.2.1 If $x_4=1$, $f_1=-x_1+{B_d}^2-B_d+2\geqslant{B_d}^2-2B_d+3\begin{cases}=3B_d-3\ if\ B_d=3\\ >3B_d-3\ if\ B_d>3\end{cases}$, "=" holds only if $B_d=3$ and $x_1=B_d-1$. It means $f_1(x)=3(B_d-1)$ when $B_d=3$ and $x=(2,1,2,1,2,1)$, where $(x_3x_6+x_4-x_6)\geqslant(x_4x_5+x_3-x_5)$, thus $f(x)=3(B_d-1)$.
1.2.2 If $x_4=2$, $f_1=2+(B_d-1)(B_d-2)+B_d={B_d}^2-2B_d+4>3B_d-3$.
1.2.3 If $x_4>2$(only if $B_d>3$, this happens),

$$\begin{aligned}f_1=&x_1(x_4-2)+x_4+(B_d-1)(B_d-x_4)+B_d\geqslant x_4-2+x_4+(B_d-1)(B_d-x_4)+B_d\\ =&(3-B_d)x_4+{B_d}^2-2\geqslant(3-B_d)(B_d-1)+{B_d}^2-2=4B_d-5>3B_d-3.\end{aligned}$$

1.3 If $x_3>2$(only if $B_d>3$, this happens),

$$\begin{aligned}f_1=&x_1(B_d-x_3)+(x_3-2)x_6+x_4+(B_d-x_1-1)(B_d-x_4)+B_d\\ \geqslant&x_1(B_d-x_3)+x_3-2+x_4+(B_d-x_1-1)(B_d-x_4)+B_d\\ =&(1-x_1)x_3+B_dx_1-2+x_4+(B_d-x_1-1)(B_d-x_4)+B_d,\end{aligned}$$

"=" holds only if $x_6=1$, then,
1.3.1 If $x_1=1$,

$$f_1=B_d-2+x_4+(B_d-2)(B_d-x_4)+B_d=(3-B_d)x_4+{B_d}^2-2\geqslant(3-B_d)(B_d-1)+{B_d}^2-2=4B_d-5>3B_d-3.$$

1.3.2 If $x_1>1$,

$$\begin{aligned}f_1=&(1-x_1)x_3+B_dx_1-2+x_4+(B_d-x_1-1)(B_d-x_4)+B_d\\ \geqslant&(1-x_1)(B_d-1)+B_dx_1-2+x_4+(B_d-x_1-1)(B_d-x_4)+B_d\\ =&(x_4+1-B_d)x_1+2B_d-3+x_4+(B_d-1)(B_d-x_4),\end{aligned}$$

"=" holds only if $x_3=B_d-1$, then,
1.3.2.1 If $x_4=B_d-1$, $f_1=4B_d-5>3B_d-3$.
1.3.2.2 If $x_4<B_d-1$,

$$\begin{aligned}f_1=&(x_4+1-B_d)x_1+2B_d-3+x_4+(B_d-1)(B_d-x_4)\\ \geqslant&(x_4+1-B_d)(B_d-1)+2B_d-3+x_4+(B_d-1)(B_d-x_4)=x_4+3B_d-4\geqslant3(B_d-1),\end{aligned}$$

"=" holds only if $x_1=B_d-1,x_4=1$. It means $f_1(x)=3(B_d-1)$ when $x=(B_d-1,1,B_d-1,1,B_d-1,1)$, where $(x_3x_6+x_4-x_6)\geqslant(x_4x_5+x_3-x_5)$, thus $f(x)=3(B_d-1)$.

Therefore, $f_{\min}=3(B_d-1)$, $\Lambda=\{(1,B_d-1,1,B_d-1,1,B_d-1),(B_d-1,1,B_d-1,1,B_d-1,1)\}$.

And then, $\forall x\in R$,$f(x)\geqslant3(B_d-1)$. By Lemma 9.(1), we know $\varphi(R)\subseteq R$. Since R, $\varphi(R)$ and Λ satisfy the conditions in Lemma 9.(4), $f(x)=3(B_d-1)$ iff $x\in\Lambda$.

The proof of Lemma 6 : Let $g(x)$ be the function defined in Lemma 9, then

$$f(x_1,x_2,x_3,x_4,x_5,x_6,x_7,x_8)=g(x_1,x_2,x_3,x_4,x_5,x_6,x_7,x_8,x_4,0).$$

Let $f_{\min}=\min\{f(x):x\in R\}$, by Lemma 9.(2), $\min\{f(x):x\in\varphi(R)\}=f_{\min}$. Let $\Lambda=\{x\in\varphi(R):f(x)=f_{\min}\}$. We need to consider function f_2 over $\varphi(R)$, where

$$f_2=x_8(B_d-x_2)+(x_1-1)(B_d-x_3)+(B_d-x_5)+(x_2-1)(B_d-x_4)+(B_d-x_6)+(x_7x_6+x_4-x_6),$$

and $f(x)\geqslant f_2(x)$,"=" holds iff $x_7x_6+x_4-x_6\geqslant x_4x_5+x_3-x_5$.

$$\begin{aligned}f_2=&x_8(B_d-x_2)+(x_1-1)(B_d-x_3)+(B_d-x_5)+(x_2-1)(B_d-x_4)+(B_d-x_6)+(x_7x_6+x_4-x_6)\\ \geqslant&(B_d-x_7)(B_d-x_2)+(B_d-x_2-1)(B_d-x_7)+(d-x_7)+(x_2-1)(d-x_4)+(d-x_6)+(x_7x_6+x_4-x_6)\\ =&2(B_d-x_2)(B_d-x_7)+(x_7-2)x_6+x_4+(x_2-1)(B_d-x_4)+B_d,\end{aligned}$$

"=" holds only if $x_1+x_2=B_d, x_7=x_3=x_5, x_7+x_8=d$, then,
2.1 If $x_7=1$,

$$\begin{aligned}f_2&=2(B_d-x_2)(B_d-1)-x_6+x_4+(x_2-1)(B_d-x_4)+d\\ &\geqslant 2(B_d-x_2)(B_d-1)-x_4+x_4+(x_2-1)(B_d-x_4)+B_d\\ &=2(B_d-x_2)(B_d-1)+(x_2-1)(B_d-x_4)+B_d,\end{aligned}$$

"=" holds only if $x_4=x_6$, then,
2.1.1 If $x_2=1$, $f_2=2{B_d}^2-3B_d+2>4B_d-4$.
2.1.2 If $x_2>1$,

$$\begin{aligned}f_2&=2(B_d-x_2)(d-1)+(x_2-1)(d-x_4)+d\geqslant 2(d-x_2)(d-1)+x_2-1+d\\ &=(3-2B_d)x_2+2{B_d}^2-B_d-1\geqslant(3-2B_d)(B_d-1)+2{B_d}^2-B_d-1=4B_d-4,\end{aligned}$$

"=" holds only if $x_4=B_d-1, x_2=B_d-1$. It means $f_1(x)=4(B_d-1)$ when $x=(1,d-1,1,d-1,1,d-1,1,d-1)$, where $(x_7x_6+x_4-x_6)\geqslant(x_4x_5+x_3-x_5)$, thus $f(x)=4(d-1)$ also.
2.2 If $x_7=2$, $f_2=(2-x_2)x_4+2(B_d-x_2)(B_d-2)+(x_2-1)B_d+B_d$.
2.2.1 If $x_2=1$,

$$\begin{aligned}&f_2=2(B_d-x_2)(d-2)+x_4+(x_2-1)(d-x_4)+d=x_4+2d^2-5d+4\\ &=2(B_d-x_2)(B_d-2)+x_4+(x_2-1)(B_d-x_4)+d=x_4+2d^2-5d+4\geqslant 2{B_d}^2-5B_d+5\begin{cases}=4B_d-4\ if\ B_d=3\\ >4B_d-4\ if\ B_d>3\end{cases},\end{aligned}$$

"=" holds only if $B_d=3$ and $x_4=1$. It means $f_1(x)=4(B_d-1)$ when $B_d=3$ and $x=(2,1,2,1,2,1,2,1)$, where $(x_7x_6+x_4-x_6)\geqslant(x_4x_5+x_3-x_5)$, thus $f(x)=4(B_d-1)$ also.
2.2.2 If $x_2=2$, $f_2=2(B_d-2)^2+B_d+B_d=2{B_d}^2-6B_d+8\begin{cases}=4B_d-4\ if\ B_d=3\\ >4B_d-4\ if\ B_d>3\end{cases}$, "=" holds only if $B_d=3$. It means $f_1(x)=4(B_d-1)$ when $B_d=3$ and $x=(1,2,2,1,2,1,2,1)$ or $(1,2,2,2,2,2,2,1)$, where $(x_7x_6+x_4-x_6)\geqslant(x_4x_5+x_3-x_5)$, thus $f(x)=4(B_d-1)$at these two points.
2.2.3 If $x_2>2$(only if $B_d>3$, this happens),

$$\begin{aligned}f_2&=2(B_d-x_2)(B_d-2)+x_4+(x_2-1)(B_d-x_4)+B_d\\ &=(2-x_2)x_4+2(B_d-x_2)(B_d-2)+(x_2-1)B_d+B_d\\ &\geqslant(2-x_2)(B_d-1)+2(B_d-x_2)(B_d-2)+(x_2-1)B_d+B_d\\ &=(5-2B_d)x_2+2{B_d}^2-2B_d-2\geqslant(5-2B_d)(B_d-1)+2{B_d}^2-2B_d-2=5B_d-7>4B_d-4.\end{aligned}$$

2.3 If $x_7>2$(only if $B_d>3$, this happens),

$$\begin{aligned}f_2=&2(B_d-x_2)(B_d-x_7)+(x_7-2)x_6+x_4+(x_2-1)(B_d-x_4)+B_d\\ \geqslant&2(B_d-x_2)(B_d-x_7)+x_7-2+x_4+(x_2-1)(B_d-x_4)+B_d\\ =&(2-x_2)x_4+2(B_d-x_2)(B_d-x_7)+x_7-2+B_dx_2,\end{aligned}$$

"=" holds only if $x_6=1$, then,
2.3.1 If $x_2=1$, $f_2=x_4+(3-2B_d)x_7+2{B_d}^2-2-B_d\geqslant 1+(3-2B_d)(B_d-1)+2{B_d}^2-2-B_d=4B_d-4$,"=" holds only if $x_4=1, x_7=B_d-1$. It means $f_1(x)=4(B_d-1)$ when $x=(B_d-1,1,B_d-1,1,B_d-1,1,B_d-1,1)$, where $(x_7x_6+x_4-x_6)\geqslant(x_4x_5+x_3-x_5)$, thus $f(x)=4(B_d-1)$ too.
2.3.2 If $x_2=2$,

$$\begin{aligned}f_2&=2(B_d-2)(B_d-x_7)+x_7-2+2B_d=(5-2B_d)x_7+2{B_d}^2-2B_d-2\\ &\geqslant(5-2B_d)(B_d-1)+2{B_d}^2-2B_d-2=5B_d-7>4B_d-4.\end{aligned}$$

2.3.3 If $x_2 > 2$(only if $B_d > 3$, this happens),

$$\begin{aligned} f_2 &= (2-x_2)x_4 + 2(B_d-x_2)(B_d-x_7) + x_7 - 2 + B_d x_2 \\ &\geqslant (2-x_2)(B_d-1) + 2(B_d-x_2)(B_d-x_7) + x_7 - 2 + B_d x_2 \\ &= (1+2x_7-2B_d)x_2 + 2B_d - 4 + 2{B_d}^2 - 2B_d x_7 + x_7 \\ &\geqslant (1+2x_7-2B_d)(B_d-1) + 2B_d - 4 + 2{B_d}^2 - 2B_d x_7 + x_7 = -x_7 + 5B_d - 5 \geqslant 4B_d - 4, \end{aligned}$$

"=" holds only if $x_4 = B_d - 1, x_2 = B_d - 1, x_7 = B_d - 1$. It means $f_1(x) = 4(B_d - 1)$ when $x = (1, B_d - 1, B_d - 1, B_d - 1, B_d - 1, 1, 1, B_d - 1, 1)$, where $(x_7x_6 + x_4 - x_6) < (x_4x_5 + x_3 - x_5)$, thus$f(x) > 4(B_d - 1)$.

Therefore, $f_{\min} = 4(B_d - 1)$. If $B_d > 3$, $\Lambda = \{(B_d - 1, 1, B_d - 1, 1, B_d - 1, 1, B_d - 1, 1), (1, B_d - 1, 1, B_d - 1, 1, B_d - 1, 1, B_d - 1)\}$; if $B_d = 3$, $\Lambda = \{(2, 1, 2, 1, 2, 1, 2, 1), (1, 2, 1, 2, 1, 2, 1, 2), (1, 2, 2, 1, 2, 1, 2, 1), (1, 2, 2, 2, 2, 2, 2, 1)\}$.

And then, for all $x \in R$, $f(x) \geqslant 4(B_d - 1)$. By Lemma8 and Lemma 9.(1), we know $\varphi(R) \subseteq R$. Since R,$\varphi(R)$ and Λ satisfy the conditions in Lemma 9.(4), $f(x) = 4(B_d - 1)$ iff $x \in \Lambda$.

The proof of Lemma 7 Let $f_{\min} = \min\{f(x) : x \in R\}$, by Lemma 9.(2), $\min\{f(x) : x \in \varphi(R)\} = f_{\min}$. Let $\Lambda = \{x \in \varphi(R) : f(x) = f_{\min}\}$. We need to consider function f_3 over $\varphi(R)$, where

$$f_3 = x_{10}(B_d - x_1) + x_8(B_d - x_2) + (x_1 - 1)(B_d - x_3) + (B_d - x_5) + (x_2 - 1)(B_d - x_4) + (B_d - x_6) + (x_7x_6 + x_4 - x_6),$$

and $f(x) \geqslant f_3(x)$,"=" holds iff $x_7x_6 + x_4 - x_6 \geqslant x_9x_5 + x_3 - x_5$.

$$\begin{aligned} f_3 =& x_{10}(B_d - x_1) + x_8(B_d - x_2) + (x_1 - 1)(B_d - x_3) + (B_d - x_5) + (x_2 - 1)(B_d - x_4) + (B_d - x_6) + (x_7x_6 + x_4 - x_6) \\ \geqslant& (B_d - x_9)(B_d - x_1) + (B_d - x_7)(B_d - x_2) + x_1(B_d - x_7) + (x_2 - 1)(B_d - x_4) + (B_d - x_6) + (x_7x_6 + x_4 - x_6) \\ =& (x_1 - B_d)x_9 + (x_2 - B_d)x_7 - x_1x_7 + 2{B_d}^2 + (2 - x_2)x_4 + (x_7 - 2)x_6, \end{aligned}$$

"=" holds only if $x_9 + x_{10} = B_d, x_7 + x_8 = B_d, x_7 = x_3 = x_5$, then,
3.1 If $x_7 = 1$,

$$\begin{aligned} f_3 &= (x_1 - B_d)x_9 + x_2 - B_d - x_1 + 2{B_d}^2 + (2 - x_2)x_4 - x_6 \\ &\geqslant (x_1 - B_d)x_9 + x_2 - B_d - x_1 + 2{B_d}^2 + (2 - x_2)x_4 - x_4 \\ &= (x_1 - B_d)x_9 + x_2 - B_d - x_1 + 2{B_d}^2 + (1 - x_2)x_4, \end{aligned}$$

"="holds only if $x_4 = x_6$, then,
3.1.1 If $x_2 = 1$, $f_3 = -x_9 + 2 - 2B_d + 2{B_d}^2 \geqslant 3 - 3B_d + 2{B_d}^2 > 5B_d - 5$.
3.1.2 If $x_2 > 1$,

$$\begin{aligned} f_3 &= (x_1 - B_d)x_9 + x_2 - B_d - x_1 + 2{B_d}^2 + (1 - x_2)x_4 \\ &\geqslant (x_1 - B_d)x_9 + x_2 - B_d - x_1 + 2{B_d}^2 + (1 - x_2)x_9 \\ &= -B_dx_9 + x_2 - B_d + (x_9 - 1)x_1 + 2{B_d}^2 + (1 - x_2)x_9, \end{aligned}$$

"=" holds only if $x_9 = x_4$, then,
3.1.2.1 If $x_9 = 1$, $f_3 = 2{B_d}^2 - 2B_d + 1 > 5B_d - 5$.
3.1.2.2 If $x_9 > 1$,

$$\begin{aligned} f_3 &= -B_dx_9 + x_2 - B_d + (x_9 - 1)x_1 + 2{B_d}^2 + (1 - x_2)x_9 \\ &\geqslant -B_dx_9 + x_2 - B_d + (x_9 - 1)(B_d - x_2) + 2{B_d}^2 + (1 - x_2)x_9 \\ &= 2(1 - x_9)x_2 - 2B_d + 2{B_d}^2 + x_9 \geqslant 2(1 - x_9)(B_d - 1) - 2B_d + 2{B_d}^2 + x_9 \\ &= -2 + 2{B_d}^2 + (3 - 2B_d)x_9 \geqslant -2 + 2{B_d}^2 + (3 - 2B_d)(B_d - 1) = 5B_d - 5, \end{aligned}$$

"=" holds only if $x_1 + x_2 = B_d, x_2 = B_d - 1, x_9 = B_d - 1$. It means $f_1(x) = 5(B_d - 1)$ when $x = (1, B_d - 1, 1, B_d - 1, 1, B_d - 1, 1, B_d - 1, B_d - 1, 1)$, where $x_7x_6 + x_4 - x_6 \geqslant x_9x_5 + x_3 - x_5$, thus $f(x) = 5(B_d - 1)$ also.
3.2 If $x_7 = 2$, $f_3 = (x_1 - B_d)x_9 + 2(x_2 - B_d) - 2x_1 + 2{B_d}^2 + (2 - x_2)x_4$,
3.2.1 If $x_2 = 1$, $f_3 = -x_9 + 4(1 - B_d) + 2{B_d}^2 + x_4$. Since $(x_9x_5 + x_3 - x_5) - (x_7x_6 + x_4 - x_6) = 2x_9 - x_4 - x_6 \geqslant 0$,

$$\begin{aligned} f(x) &= f_3 + (x_9x_5 + x_3 - x_5) - (x_7x_6 + x_4 - x_6) = 4(1 - B_d) + 2{B_d}^2 + x_9 - x_6 \\ &\geqslant 4(1 - B_d) + 2{B_d}^2 \begin{cases} = 5B_d - 5 \ \ if \ \ B_d = 3 \\ > 5B_d - 5 \ \ if \ \ B_d > 3 \end{cases}, \end{aligned}$$

"=" holds only if $B_d = 3$ and $x_9 = x_4 = x_6$. It means $f(x) = 5(B_d - 1)$ when $B_d = 3$ and $x = (2, 1, 2, 1, 2, 1, 2, 1, 1, 2)$ or $(2, 1, 2, 2, 2, 2, 2, 1, 2, 1)$.
3.2.2 If $x_2 = 2$,

$$\begin{aligned} f_3 &= (x_1 - B_d)x_9 + 4 - 2B_d - 2x_1 + 2{B_d}^2 \geqslant (x_1 - B_d)(B_d - 1) + 4 - 2B_d - 2x_1 + 2{B_d}^2 \\ &= (B_d - 3)x_1 + 4 - B_d + B_d{}^2 \begin{cases} = 5B_d - 5 \ \ if \ \ B_d = 3 \\ > 5B_d - 5 \ \ if \ \ B_d > 3 \end{cases}, \end{aligned}$$

"=" holds only if $B_d = 3$ and $x_9 = B_d - 1$. It means $f_1(x) = 5(B_d - 1)$ when $B_d = 3$ and $x = (1, 2, 2, 2, 2, 2, 2, 1, 2, 1)$ or $(2, 2, 2, 2, 2, 2, 2, 1, 2, 1)$, where $x_7x_6 + x_4 - x_6 \geqslant x_9x_5 + x_3 - x_5$, thus $f(x) = 5(B_d - 1)$ at these two points also.
3.2.3 If $x_2 > 2$(only if $B_d > 3$, this happens),

$$\begin{aligned} f_3 &= (x_1 - B_d)x_9 + 2(x_2 - B_d) - 2x_1 + 2{B_d}^2 + (2 - x_2)x_4 \\ &\geqslant (x_1 - B_d)x_9 + 2(x_2 - B_d) - 2x_1 + 2{B_d}^2 + (2 - x_2)x_9 \\ &= (x_1 - x_2 - B_d + 2)x_9 + 2(x_2 - B_d) - 2x_1 + 2{B_d}^2 \\ &\geqslant (x_1 - x_2 - B_d + 2)(B_d - 1) + 2(x_2 - B_d) - 2x_1 + 2{B_d}^2 = (B_d - 3)x_1 + (3 - B_d)x_2 + B_d + {B_d}^2 - 2 \\ &\geqslant (B_d - 3) + (3 - B_d)(B_d - 1) + B_d + {B_d}^2 - 2 = 6B_d - 8 > 5B_d - 5. \end{aligned}$$

3.3 If $x_7 > 2$(only if $B_d > 3$, this happens),

$$\begin{aligned} f_3 =& (x_1 - B_d)x_9 + (x_2 - B_d)x_7 - x_1x_7 + 2{B_d}^2 + (2 - x_2)x_4 + (x_7 - 2)x_6 \\ \geqslant& (x_1 - B_d)x_9 + (x_2 - B_d)x_7 - x_1x_7 + 2{B_d}^2 + (2 - x_2)x_4 + (x_7 - 2) \\ =& (x_1 - B_d)x_9 + (x_2 - x_1 - B_d + 1)x_7 + 2{B_d}^2 + (2 - x_2)x_4 - 2 \\ \geqslant& (x_1 - B_d)x_9 + (x_2 - x_1 - B_d + 1)(B_d - 1) + 2{B_d}^2 + (2 - x_2)x_4 - 2 \\ =& (x_1 - B_d)x_9 + (B_d - 1)x_2 - x_1(B_d - 1) + {B_d}^2 + (2 - x_2)x_4 + 2B_d - 3, \end{aligned}$$

"=" holds only if $x_6 = 1, x_7 = B_d - 1$, then,
3.3.1 If $x_2 = 1$, $f_3 = -x_9 + x_4 + 5B_d - 5$. Since $(x_9x_5 + x_3 - x_5) \geqslant (x_7x_6 + x_4 - x_6)$, $f(x) = f_3 + (x_9x_5 + x_3 - x_5) - (x_7x_6 + x_4 - x_6) = 5B_d - 5 + (B_d - 2)(x_9 - 1) \geqslant 5B_d - 5$, "=" holds only if $x_9 = 1$. It means $f(x) = 5(B_d - 1)$ when $x = (B_d - 1, 1, B_d - 1, 1, B_d - 1, 1, 1, B_d - 1, 1, B_d - 1)$.
3.3.2 If $x_2 = 2$,

$$f_3 = (x_1 - B_d)x_9 - x_1(B_d - 1) + {B_d}^2 + 4B_d - 5 \geqslant (x_1 - B_d)(B_d - 1) - x_1(B_d - 1) + {B_d}^2 + 4B_d - 5 = 5B_d - 5,$$

"=" holds only if $x_9 = B_d - 1$, where $(x_9x_5 + x_3 - x_5) > (x_7x_6 + x_4 - x_6)$, thus $f(x) > 5B_d - 5$.
3.3.3 If $x_2 > 2$(only if $B_d > 3$, this happens),

$$\begin{aligned} f_3 =& (x_1 - B_d)x_9 + (B_d - 1)x_2 - x_1(B_d - 1) + {B_d}^2 + (2 - x_2)x_4 + 2B_d - 3 \\ \geqslant& (x_1 - B_d)x_9 + (B_d - 1)x_2 - x_1(B_d - 1) + {B_d}^2 + (2 - x_2)x_9 + 2B_d - 3 \\ =& (x_1 - x_2 - B_d + 2)x_9 + (B_d - 1)x_2 - x_1(B_d - 1) + {B_d}^2 + 2B_d - 3 \\ \geqslant& (x_1 - x_2 - B_d + 2)(B_d - 1) + (B_d - 1)x_2 - x_1(B_d - 1) + {B_d}^2 + 2B_d - 3 = 5B_d - 5, \end{aligned}$$

"=" holds only if $x_9 = x_4 = B_d - 1$, where $(x_9x_5 + x_3 - x_5) > (x_7x_6 + x_4 - x_6)$, thus $f(x) > 5B_d - 5$.

Therefore, $f_{\min} = 5(B_d - 1)$. If $B_d > 3$, $\Lambda = \{(B_d - 1, 1, B_d - 1, 1, B_d - 1, 1, B_d - 1, 1, 1, B_d - 1), (1, B_d - 1, 1, B_d - 1, 1, B_d - 1, 1, B_d - 1, B_d - 1, 1)\}$; if $B_d = 3$, $\Lambda = \{(2, 1, 2, 1, 2, 1, 2, 1, 1, 2), (1, 2, 1, 2, 1, 2, 1, 2, 2, 1), (1, 2, 2, 2, 2, 2, 2, 1, 2, 1), (2, 2, 2, 2, 2, 2, 2, 1, 2, 1), (2, 1, 2, 2, 2, 2, 2, 1, 2, 1)\}$.

And then, for all $x \in R$, $f(x) \geqslant 5(B_d - 1)$. By Lemma8 and Lemma 9.(1), we know $\varphi(R) \subseteq R$. Since R, $\varphi(R)$ and Λ satisfy the conditions in Lemma 9.(4), $f(x) = 5(B_d - 1)$ iff $x \in \Lambda$.