INFORMATION
SCIENCE
TECHNICAL
REPORT

NAIST-IS-TR98012
ISSN 0919-9527

An Optimality Testing Algorithm for a Decoded Codeword of Binary Block Codes

Tang Yuansheng, Tadao Kasami
and Toru Fujiwara

October 1998

NAIST

〒 630-0101
奈良県生駒市高山町 8916-5
奈良先端科学技術大学院大学
情報科学研究科

Graduate School of Information Science
Nara Institute of Science and Technology
8916-5 Takayama, Ikoma, Nara 630-0101, Japan

An Optimality Testing Algorithm for a Decoded Codeword of Binary Block Codes

Tang Yuansheng * Tadao Kasami † Toru Fujiwara ‡

Abstract— For the iterative soft-decision decoding algorithms, a testing condition on the optimality of a decoded codeword based on h candidate codewords is proposed by Kasami et.al. recently. The greater the number h of the candidate codewords, the stronger the testing condition. The computational complexity and the effectiveness of the testing condition of the cases $h \leq 3$ have been investigated by Kasami et.al. In this paper we propose an algorithm to compute the testing condition of the case $h = 4$, the computational complexity of this algorithm is also discussed.

Keywords—Binary block code, maximum likelihood decoding, iterative soft-decision decoding, optimality testing.

1 Introduction

To reduce the decoding complexity of soft-decision decoding binary linear block codes, many iterative soft-decision decoding algorithms were proposed, such as those proposed in [1]-[7]. In most of this class of algorithms, a simple decoder is employed to generate a sequence of candidate codewords that will contain the optimal (or most likely) codeword certainly or with very high probability. One important problem for this class of algorithms is to develop the testing conditions on the optimality of the candidate codewords. When a new candidate codeword is generated, a testing condition is applied upon it and the decoding iteration process is terminated as soon as the testing condition is satisfied, and if the computational complexity of the testing condition is reasonably smaller than that of the procedure for generating the next candidate codeword, it will reduce significantly the decoding delay and the computational complexity of the decoding algorithms. A number of testing conditions on the optimality of the generated canditate codewords have been derived, such as those proposed by Taipale and Pursley [4], Kaneko et.al. [5]. Recently, based on h canditate codewords which are generated previously, Kasami et.al. in [7]-[10] derived a powerful sufficient testing condition on the optimality of a canditate codeword which can be incorporated in any of the iterative soft-decision decoding algorithms which are based on the generation of a sequence of candicate codewords. For greater h, the testing condition is stronger whereas the computational complexity is greater. In [7]-[10], for the cases of $h \leq 3$ of this testing condition, the authors proposed further some concrete computation methods, for which the numbers of operations of real numbers (the majorities of the computational complexity) are only of order N the length of the code, and even the case of $h = 2$ of this testing condition is also stronger than the one proposed by Kaneko et.al. [5]. In this paper, we will show some general results for this testing condition further and propose a concrete computation method for the case of $h = 4$, for which the number of operations of real numbers is of order N^2.

In Section 2, we will introduce the sufficient testing condition proposed by Kasami et.al. in [7]-[10], which is based on h canditate codewords generated previously and expressed by the minimum of a real-value function on a set Q of 2^h-tuples of nonnegative integers. In Section 3, we present some general discussions on the set Q, and show that for computing the minimum for the case of $h = 4$ it is enough to consider a subset Q_M of Q which can be expressed as a union of at most 9 simpler subsubsets, the minimums on each of the subsubsets can be computed easily. Some concrete computation methods for the minimums on the subsubsets are proposed in Section 4. The computational complexity of our computation method for the testing condition is also analyzed in Section 4. Since the number of operations of real numbers of our computation method is only of order N^2, it is still very effective and provides a faster termination of the decoding iteration process than the cases of $h \leq 3$ do.

2 The testing condition of optimality

Let $\boldsymbol{u}_j$ denote the j-th component of a tuple $\boldsymbol{u}$. Let V^N denote the set of all binary N-tuples. Suppose a binary block code $C \subset V^N$ is used for error control over the AWGN channel use BPSK signaling. Assume $\boldsymbol{r}$ is a received N-tuple at the output of a matched filter in the receiver, and let $\boldsymbol{z}$ be the binary hard-decision N-tuple obtained from $\boldsymbol{r}$ by

$$\boldsymbol{z}_j = \begin{cases} 1, & \text{for } \boldsymbol{r}_j > 0, \\ 0, & \text{for } \boldsymbol{r}_j \leq 0, \end{cases} \quad j = 1, 2, \ldots, N. \tag{1}$$

$|\boldsymbol{r}_j|$ indicates the reliability of $\boldsymbol{z}_j$ for each j.

For a tuple $\boldsymbol{u} \in V^N$, let

$$\mathcal{D}_1(\boldsymbol{u}) \stackrel{\triangle}{=} \{i : \boldsymbol{u}_i \neq \boldsymbol{z}_i,\ 1 \leq i \leq N\}, \tag{2}$$

$$\mathcal{D}_0(\boldsymbol{u}) \stackrel{\triangle}{=} \{1, 2, \ldots, N\} \backslash \mathcal{D}_1(\boldsymbol{u}), \tag{3}$$

* Graduate School of Information Science, Nara Institute of Science and Technology, Ikoma, Nara, 630-0101 Japan.

† Faculty of Information Science, Department of Information Science, Hiroshima City University, Hiroshima, 731-3194 Japan.

‡ Graduate School of Engineering Science, Osaka University, Toyonaka, 560-8531 Japan.

and call $L(\boldsymbol{u}) \triangleq \sum_{i\in\mathcal{D}_1(\boldsymbol{u})} |\boldsymbol{r}_i|$ the **correlation discrepancy** of $\boldsymbol{u}$. Then the maximum likelihood decoding (MLD) can be stated in terms of the correlation discrepancy as follows: The decoder decodes the received tuple $\boldsymbol{r}$ into a (the **optimal**) codeword $\boldsymbol{c}_{\rm opt} \in C$ which satisfies

$$L(\boldsymbol{c}_{\rm opt}) = \min_{\boldsymbol{c}\in C} L(\boldsymbol{c}). \tag{4}$$

Let h and $d_1, d_2, \ldots, d_h$ be positive integers, and $\boldsymbol{u}^1$, $\boldsymbol{u}^2$, ..., $\boldsymbol{u}^h$ be h reference tuples in V^N (candidate codewords in C generated already). Write

$$C_{d_i}(\boldsymbol{u}^i) \triangleq \{\boldsymbol{c} \in C:\ d_H(\boldsymbol{u}^i, \boldsymbol{c}) \le d_i\},$$

where $d_H(\boldsymbol{u}^i, \boldsymbol{c})$ is the Hamming distance between $\boldsymbol{u}^i$ and $\boldsymbol{c}$. Let $\boldsymbol{c}_{\rm best}$ be a (the **best**) codeword in $R \triangleq \cup_{i=1}^h C_{d_i}(\boldsymbol{u}^i)$ which satisfies

$$L(\boldsymbol{c}_{\rm best}) = \min_{\boldsymbol{c}\in R} L(\boldsymbol{c}). \tag{5}$$

We assume that $\boldsymbol{c}_{\rm best}$ has been generated in the iterative process of decoding, our goal is to consider the testing of the optimality of $\boldsymbol{c}_{\rm best}$. We denote the set

$$\bigcap_{i=1}^{h} \{\boldsymbol{u} \in V^N:\ d_H(\boldsymbol{u}^i, \boldsymbol{u}) \ge d_i + 1\}$$

by $V^N_{d_1,d_2,\ldots,d_h}(\boldsymbol{u}^1, \boldsymbol{u}^2, \ldots, \boldsymbol{u}^h)$, it is a superset of $C\backslash R$.

Let B^h denote the set of all sequences of length h over $B \triangleq \{0,1\}$. For $\alpha \in B^h$, let α_i denote the i-th bit of α, $(-1)^\alpha$ denote the sequence in B^h with $(-1)^{\alpha_i}$ as its i-th bit, $\overline{\alpha}$ denote the sequence in B^h with $\overline{\alpha}_i = 1 - \alpha_i$, and write

$$\mathcal{D}_\alpha \triangleq \bigcap_{i=1}^{h} \mathcal{D}_{\alpha_i}(\boldsymbol{u}^i),\ n_\alpha \triangleq |\mathcal{D}_\alpha|. \tag{6}$$

Clearly, for any two distinct sequences α and α' in B^h,

$$\mathcal{D}_\alpha \cap \mathcal{D}_{\alpha'} = \emptyset(\text{the empty set}). \tag{7}$$

For $\boldsymbol{u}\in V^N$ and $\alpha \in B^h$, let

$$n(\boldsymbol{u}) \triangleq |\mathcal{D}_1(\boldsymbol{u})|,\ \boldsymbol{q}_\alpha(\boldsymbol{u}) \triangleq |\mathcal{D}_1(\boldsymbol{u}) \cap \mathcal{D}_\alpha|, \tag{8}$$

then we have that

$$0 \le \boldsymbol{q}_\alpha(\boldsymbol{u}) \le n_\alpha,\ |\mathcal{D}_0(\boldsymbol{u}) \cap \mathcal{D}_\alpha| = n_\alpha - q_\alpha(\boldsymbol{u}). \tag{9}$$

Hence, for any $\boldsymbol{u}\in V^N$, with respect to (7) we have

$$\begin{aligned}
&d_H(\boldsymbol{u}, \boldsymbol{u}^i) - n(\boldsymbol{u}^i)\\
&= |\mathcal{D}_0(\boldsymbol{u}) \cap \mathcal{D}_1(\boldsymbol{u}^i)| + |\mathcal{D}_1(\boldsymbol{u}) \cap \mathcal{D}_0(\boldsymbol{u}^i)| - |\mathcal{D}_1(\boldsymbol{u}^i)|\\
&= |\mathcal{D}_0(\boldsymbol{u}) \cap (\cup_{\alpha\in B^h, \alpha_i=1} \mathcal{D}_\alpha)|\\
&\quad + |\mathcal{D}_1(\boldsymbol{u}) \cap (\cup_{\alpha\in B^h, \alpha_i=0} \mathcal{D}_\alpha)| - |\cup_{\alpha\in B^h, \alpha_i=1} \mathcal{D}_\alpha|\\
&= \sum_{\alpha\in B^h, \alpha_i=1} (n_\alpha - q_\alpha(\boldsymbol{u}))\\
&\qquad + \sum_{\alpha\in B^h, \alpha_i=0} q_\alpha(\boldsymbol{u}) - \sum_{\alpha\in B^h, \alpha_i=1} n_\alpha\\
&= \sum_{\alpha\in B^h} (-1)^{\alpha_i} \boldsymbol{q}_\alpha(\boldsymbol{u}),\quad i = 1, 2, \ldots, h.
\end{aligned} \tag{10}$$

For $i = 1, 2, \ldots, h$, we write

$$\delta_i \triangleq d_i + 1 - n(\boldsymbol{u}^i). \tag{11}$$

Let Q denote the set of all the 2^h-tuples $\boldsymbol{q}$ over nonnegative integers which satisfy

$$0 \le \boldsymbol{q}_\alpha \le n_\alpha,\ \alpha \in B^h, \tag{12}$$

$$\sum_{\alpha\in B^h} \boldsymbol{q}_\alpha (-1)^{\alpha_i} \ge \delta_i,\ i = 1, 2, \ldots, h. \tag{13}$$

For each N-tuple $\boldsymbol{u}$ in $V^N_{d_1,d_2,\ldots,d_h}(\boldsymbol{u}^1, \boldsymbol{u}^2, \ldots, \boldsymbol{u}^h)$, by (10) we see that the 2^h-tuple $(\boldsymbol{q}_\alpha(\boldsymbol{u}):\ \alpha \in B^h)$ belongs to Q. On the other hand, we see easily that for each 2^h-tuple $\boldsymbol{q}$ with (12), there is at least one N-tuple $\boldsymbol{u}$ in V^N such that $\boldsymbol{q}_\alpha(\boldsymbol{u}) = \boldsymbol{q}_\alpha$ for all $\alpha \in B^h$, and $\boldsymbol{u}\in V^N_{d_1,d_2,\ldots,d_h}(\boldsymbol{u}^1, \boldsymbol{u}^2, \ldots, \boldsymbol{u}^h)$ if $\boldsymbol{q}$ satisfies (13) further.

Without loss of the generality, we assume further that the components of the received tuple $\boldsymbol{r}$ are ordered in the increasing order

$$|\boldsymbol{r}_1| \le |\boldsymbol{r}_2| \le \ldots \le |\boldsymbol{r}_N|. \tag{14}$$

For subset $X \subset \{1, 2, \ldots, N\}$ and integer $j \le |X|$, let $X^{(j)}$ denote the set of j smallest integers in X if $j \ge 1$, the empty set $\emptyset$ if $j \le 0$, respectively. For convenience, we write also $X^{(j)} \triangleq \{+\infty\}$ for $j > |X|$, and $|\boldsymbol{r}_{+\infty}| \triangleq +\infty$. For any 2^h-tuple $\boldsymbol{q}$ over nonnegative integers, let

$$\mathcal{D}(\boldsymbol{q}) \triangleq \cup_{\alpha\in B^h} \mathcal{D}_\alpha^{(\boldsymbol{q}_\alpha)},\ L'(\boldsymbol{q}) \triangleq \sum_{i\in\mathcal{D}(\boldsymbol{q})} |\boldsymbol{r}_i|. \tag{15}$$

We see that $L'(\boldsymbol{q}) = +\infty$ if $\boldsymbol{q}_\alpha > n_\alpha$ holds for some $\alpha \in B^h$. We write

$$\underline{L}[V^N_{d_1,d_2,\ldots,d_h}(\boldsymbol{u}^1, \boldsymbol{u}^2, \ldots, \boldsymbol{u}^h)] \triangleq \min_{\boldsymbol{q}\in Q} L'(\boldsymbol{q}). \tag{16}$$

About the optimality of $\boldsymbol{c}_{\rm best}$, we have the following sufficient testing condition([7]-[10]).

Lemma 1 *$\boldsymbol{c}_{best}$ is the optimal codeword $\boldsymbol{c}_{opt}$ if*

$$L(\boldsymbol{c}_{best}) \le \underline{L}[V^N_{d_1,d_2,\ldots,d_h}(\boldsymbol{u}^1, \boldsymbol{u}^2, \ldots, \boldsymbol{u}^h)]. \tag{17}$$

In [7]-[10], for the cases of $h \le 3$ some effective methods for computing $\underline{L}[V^N_{d_1,d_2,\ldots,d_h}(\boldsymbol{u}^1, \boldsymbol{u}^2, \ldots, \boldsymbol{u}^h)]$ were proposed, the numbers of operations of real numbers (the majorities of the computational complexity) of these computation methods are of order N. In this paper, we mainly consider the case of $h = 4$.

If $\delta_i \le 0$ for $i = 1, 2, \ldots, h$, then the all zero 2^h-tuple $\boldsymbol{q} = 0$ belongs to Q, and $\underline{L}[V^N_{d_1,d_2,\ldots,d_h}(\boldsymbol{u}^1, \boldsymbol{u}^2, \ldots, \boldsymbol{u}^h)] = 0$, this also means the hard-decision tuple $\boldsymbol{z}$ belongs to the set $V^N_{d_1,d_2,\ldots,d_h}(\boldsymbol{u}^1, \boldsymbol{u}^2, \ldots, \boldsymbol{u}^h)$. Below we suppose that $\delta_i > 0$ for at least one index i.

3 General discussion on the set Q

Let Q^* denote the set of all the 2^h-tuples $\boldsymbol{q}$ over nonnegative integers. For any $\boldsymbol{q}\in Q^*$, write $SP_{\boldsymbol{q}} \triangleq \{\alpha \in B^h : \boldsymbol{q}_\alpha \geq 1\}$ and $\Delta(\boldsymbol{q}) \triangleq \sum_{\alpha\in B^h} \boldsymbol{q}_\alpha(-1)^\alpha$. For any two tuples γ, γ' over integers with the same length, we write $\gamma \leq \gamma'$ if $\gamma_i \leq \gamma'_i$ for all indices i. Let Γ_0 denote the set of h-tuples γ over nonnegative integers for which $\gamma_i = 0$ holds for at least one index i. If subset $\Xi \subset B^h$ and h-tuple $\gamma \in \Gamma_0$ satisfy

$$(-1)^\alpha \not\leq \gamma,\ (-1)^\alpha + (-1)^{\alpha'} \not\leq \gamma \tag{18}$$

for all sequences α, $\alpha' \in \Xi$, then we call Ξ $m(\gamma)$-**set**.

About the sufficient testing condition shown in Lemma 1, we have

Lemma 2 *Let Q_M be the set of the 2^h-tuples $\boldsymbol{q}$ in Q for which $\Delta(\boldsymbol{q})-\delta \in \Gamma_0$ and $SP_{\boldsymbol{q}}$ are $m(\Delta(\boldsymbol{q})-\delta)$-sets, where δ is the tuple with components δ_i defined by (11). Then we have*

$$\min_{\boldsymbol{q}\in Q_M} L'(\boldsymbol{q}) = \underline{L}[V^N_{d_1,d_2,\ldots,d_h}(\boldsymbol{u}^1,\boldsymbol{u}^2,\ldots,\boldsymbol{u}^h)]. \tag{19}$$

Proof: One hand, since $Q_M \subset Q$, we have

$$\min_{\boldsymbol{q}\in Q_M} L'(\boldsymbol{q}) \geq \underline{L}[V^N_{d_1,d_2,\ldots,d_h}(\boldsymbol{u}^1,\boldsymbol{u}^2,\ldots,\boldsymbol{u}^h)]. \tag{20}$$

On the other hand, let $\boldsymbol{q}\in Q$ be a 2^h-tuple satisfying

$$L'(\boldsymbol{q}) = \underline{L}[V^N_{d_1,d_2,\ldots,d_h}(\boldsymbol{u}^1,\boldsymbol{u}^2,\ldots,\boldsymbol{u}^h)], \tag{21}$$

and assume further that $\sum_{\alpha\in B^h} \boldsymbol{q}_\alpha$ achieves minimum among the 2^h-tuples of this kind. We see easily that $SP_{\boldsymbol{q}}$ must be an $m(\Delta(\boldsymbol{q}) - \delta)$-set and furthermore $\Delta(\boldsymbol{q}) - \delta \in \Gamma_0$, i.e. $\boldsymbol{q}\in Q_M$. Hence, we have also

$$\min_{\boldsymbol{q}\in Q_M} L'(\boldsymbol{q}) \leq \underline{L}[V^N_{d_1,d_2,\ldots,d_h}(\boldsymbol{u}^1,\boldsymbol{u}^2,\ldots,\boldsymbol{u}^h)], \tag{22}$$

and thus (19) is valid. △△

The main goal of this section is to show for the case of $h = 4$ that Q_M is a union of at most 9 simpler subsets, for each subset Q' there exists an index subset Ξ with at least 2^{4-1} elements such that the 2^3 components $\boldsymbol{q}_i$ with $i \in \Xi$ of any 2^4-tuple $\boldsymbol{q}$ in Q' are zero, the computation of $\min_{\boldsymbol{q}\in Q'} L'(\boldsymbol{q})$ is considered in the next section.

Clearly, if Ξ is an $m(\gamma)$-set, then Ξ is an $m(0)$-set and the all one sequence $11\cdots1$ does not belong to Ξ and there is no $\alpha \in B^h$ such that $\{\alpha,\overline{\alpha}\} \subset \Xi$, and thus $|\Xi| \leq 2^{h-1}$. If $m(\gamma)$-set Ξ satisfies $|\Xi| = 2^{h-1}$, i.e. either $\alpha \in \Xi$ or $\overline{\alpha} \in \Xi$ for any $\alpha \in B^h$, we call Ξ $M(\gamma)$-**set**. Clearly, if Ξ is an $M(\gamma)$-set, then Ξ is an $M(0)$-set too.

Lemma 3 *If $h = 4$, then all the $M(0)$-sets are the following 12 sets*

$$C_\ell \triangleq \{\alpha \in B^4 : \alpha_\ell = 0\},$$
$$D_\ell \triangleq \{\alpha \in B^4 : \textstyle\sum_{j\neq\ell} \alpha_j \leq 1\},$$
$$E_\ell \triangleq \{\alpha \in B^4 : \textstyle\sum_{j\neq\ell}^4 \alpha_j = 2, \alpha_\ell = 0\} \cup \{\alpha \in B^4 : \textstyle\sum_{j=1}^4 \alpha_j \leq 1\},\quad \ell = 1,2,3,4.$$

Proof: Assume $\Xi \in \{C_\ell, D_\ell, E_\ell\}_{\ell=1}^4$. Since for any two sequences $\alpha, \alpha' \in \Xi$ there is at least one i such that $\alpha_i = \alpha'_i = 0$, we see $(-1)^\alpha \not\leq 0$ and $(-1)^\alpha + (-1)^{\alpha'} \not\leq 0$. Hence Ξ is an $m(0)$-set. Furthermore from $|\Xi| = 8 = 2^{4-1}$, we know Ξ is an $M(0)$-set.

Now suppose Ξ is an $M(0)$-set. If there is an i_0 such that $\alpha_{i_0} = 0$ for all $\alpha \in \Xi$ or $\alpha'_{i_0} = 0$, $\alpha'_i = 1$, $i \neq i_0$ for some $\alpha' \in \Xi$, then $\Xi = C_{i_0}$. Now we assume $\alpha^{(i)}_i = 1$ for four sequences $\alpha^{(i)} \in \Xi$, $i = 1,2,3,4$, and $\sum_{j=1}^4 \alpha_j \leq 2$ for all $\alpha \in \Xi$. Let Φ denote the set of the sequences $\alpha \in \Xi$ with $\sum_{j=1}^4 \alpha_j = 2$. By $|\Xi| = 8$, we know $|\Phi| \geq 3$. We assume, without loss of the generality, that $\{1100, 1010\} \subset \Phi$. Clearly, any other element in Φ must belong to $\{0110, 1001\}$. Thus by $0110 = \overline{1001}$ we know $\Xi \in \{E_4, D_1\}$. △△

For h-tuple $\gamma \in \Gamma_0$ and sequence $\alpha \in B^h$, let $\zeta(\gamma)$ denote the set of indices i with $\gamma_i \leq 1$ and write the elements of $\zeta(\gamma)$ as $i_1, i_2, \ldots, i_k$ in the increasing order, let $\mathcal{P}_\gamma(\alpha) \triangleq \alpha_{i_1}\alpha_{i_2}\cdots\alpha_{i_k}$, $\mathcal{P}^*(\gamma) \triangleq \gamma_{i_1}\gamma_{i_2}\cdots\gamma_{i_k}$ and $\mathcal{P}(\gamma) \triangleq (\gamma_{i_1}, \gamma_{i_2}, \ldots, \gamma_{i_k})$. For h-tuple $\gamma \in \Gamma_0$ and subset $\Xi \subset B^h$, let $\mathcal{P}_\gamma[\Xi] \triangleq \{\mathcal{P}_\gamma(\alpha) : \alpha \in \Xi\}$. Clearly, Ξ is an $m(\gamma)$-set if and only if $\mathcal{P}_\gamma[\Xi]$ is an $m(\mathcal{P}(\gamma))$-set.

Lemma 4 *Assume $\Xi \subset B^h$ and $\gamma \in \Gamma_0$.*
1. If Ξ is an $m(\gamma)$-set, then Ξ must be a subset of some $M(\gamma)$-set.
2. If Ξ is an $M(0)$-set, then Ξ is an $M(\gamma)$-set if and only if

$$\mathcal{P}^*(\gamma) \in \mathcal{P}_\gamma[\Xi], \tag{23}$$
$$\Xi = \{\alpha \in B^h : \mathcal{P}_\gamma(\alpha) \in \mathcal{P}_\gamma[\Xi]\}. \tag{24}$$

Proof: 1. Assume Ξ is an $m(\gamma)$-set. Firstly, we consider the case of $\gamma = 0$. If $m(0)$-set Ξ is not an $M(0)$-set, we conclude, for any $\beta \in B^h$ with $\{\beta,\overline{\beta}\} \cap \Xi = \emptyset$, that either $\Xi\cup\{\beta\}$ or $\Xi\cup\{\overline{\beta}\}$ is $m(0)$-set. Assume the contrary for some $\beta \in B^h$ with $\{\beta,\overline{\beta}\} \cap \Xi = \emptyset$ neither $\Xi\cup\{\beta\}$ nor $\Xi\cup\{\overline{\beta}\}$ is $m(0)$-set. Then there must exist two sequences α, $\alpha' \in \Xi$ and integers $\xi, \xi' \in B$ with $\xi + \xi' \geq 1$ such that

$$(-1)^\beta + \xi(-1)^\alpha \leq 0,\ (-1)^{\overline{\beta}} + \xi'(-1)^{\alpha'} \leq 0.$$

Clearly, we have $\xi(-1)^\alpha + \xi'(-1)^{\alpha'} \leq 0$ and it contradicts that Ξ is an $m(0)$-set. Hence Ξ must be a subset of some $M(0)$-set.

Secondly, we consider the case of $\mathcal{P}(\gamma) = \gamma$, i.e. $\gamma_i \leq 1$ for $i = 1,2,\ldots,h$. Since Ξ is an $m(\gamma)$-set, from $-(-1)^{\mathcal{P}^*(\gamma)} \leq \gamma$ and $(-1)^{\mathcal{P}^*(\gamma)} \not\leq \gamma$ we know $\Xi \cup \{\mathcal{P}^*(\gamma)\}$ is an $m(0)$-set. Hence, there is an $m(0)$-set Ξ' such that $\Xi\cup\{\mathcal{P}^*(\gamma)\} \subset \Xi'$. Furthermore, for any pair of sequences $\alpha, \alpha' \in \Xi'$, since $(-1)^\alpha + (-1)^{\alpha'} \not\leq 0$, we know there is at least one index i such that $\alpha_i = \alpha'_i = 0$, and thus $(-1)^\alpha + (-1)^{\alpha'} \not\leq \gamma$. On the other hand, for any sequence $\beta \in \Xi'$, by $(-1)^\beta + (-1)^{\mathcal{P}^*(\gamma)} \not\leq 0$ we know there is at least one index j such that $\beta_j = \gamma_j = 0$, and thus $(-1)^\beta \not\leq \gamma$. Hence Ξ' is an $M(\gamma)$-set which contains Ξ.

Now we consider the case of $\mathcal{P}(\gamma) \neq \gamma$. Since $\mathcal{P}_\gamma[\Xi]$ is an $m(\mathcal{P}(\gamma))$-set, there is an $M(\mathcal{P}(\gamma))$-set, denote Ξ'_r, which contains $\mathcal{P}_\gamma[\Xi]$. Then the set

$$\{\alpha \in B^h : \mathcal{P}_\gamma(\alpha) \in \Xi'_r\}$$

is an $M(\gamma)$-set which contains Ξ.

2. One hand, assume Ξ is an $M(\gamma)$-set, and write $\sigma = |\zeta(\gamma)|$. From

$$\Xi \subset \Xi' \stackrel{\triangle}{=} \{\alpha \in B^h : \mathcal{P}_\gamma(\alpha) \in \mathcal{P}_\gamma[\Xi]\},$$

we see $2^{h-1} = |\Xi| \leq 2^{h-\sigma}|\mathcal{P}_\gamma[\Xi]|$, i.e. $|\mathcal{P}_\gamma[\Xi]| \geq 2^{\sigma-1}$. Since $\mathcal{P}_\gamma[\Xi]$ is an $m(\mathcal{P}(\gamma))$-set, we have $|\mathcal{P}_\gamma[\Xi]| \leq 2^{\sigma-1}$. Hence $|\mathcal{P}_\gamma[\Xi]| = 2^{\sigma-1}$, and then $\mathcal{P}_\gamma[\Xi]$ is an $M(\mathcal{P}(\gamma))$-set and $\Xi = \Xi'$, i.e. (24) holds. Moreover, according to $(-1)^{\overline{\mathcal{P}^*(\gamma)}} \leq \mathcal{P}(\gamma)$, we know $\overline{\mathcal{P}^*(\gamma)} \notin \mathcal{P}_\gamma[\Xi]$, and then $\mathcal{P}^*(\gamma) \in \mathcal{P}_\gamma[\Xi]$, i.e. (23) holds.

On the other hand, assume Ξ is an $M(0)$-set and satisfy (23) and (24). From (24) we see $\mathcal{P}_\gamma[\Xi]$ is an $M(0)$-set, i.e. for any two sequence $\beta, \beta' \in \mathcal{P}_\gamma[\Xi]$ we have $(-1)^\beta + (-1)^{\beta'} \not\leq 0$, hence there exists at least one index i in $\zeta(\gamma)$ such that $\beta_i = \beta'_i = 0$ and thus by (23) we know

$$(-1)^\beta \not\leq \mathcal{P}(\gamma),\ (-1)^\beta + (-1)^{\beta'} \not\leq \mathcal{P}(\gamma).$$

Then $\mathcal{P}_\gamma[\Xi]$ is an $M(\mathcal{P}(\gamma))$-set, and furthermore Ξ is an $M(\gamma)$-set. $\triangle\triangle$

Assume $h = 4$ and $1 \leq \ell \leq 4$. Let Λ denote the set of 4-tuples $\lambda \geq \delta$ over integers with all even or odd components. Clearly, $\Delta(\boldsymbol{q}) \in \Lambda$ for all the 2^4-tuples $\boldsymbol{q}$ in Q. Let $Q(C_\ell)$ denote the set of the 2^4-tuples $\boldsymbol{q} \in Q$ which satisfy $SP_{\boldsymbol{q}} \subset C_\ell$ and $\Delta(\boldsymbol{q})_\ell = \delta_\ell$. Let $Q(D_\ell)$ denote the set of the 2^4-tuples $\boldsymbol{q} \in Q$ which satisfy $SP_{\boldsymbol{q}} \subset D_\ell$ and $\Delta(\boldsymbol{q})_j = \rho(D_\ell)_j$ for $j \in \{1,2,3,4\}\backslash\{\ell\}$, where $\rho(D_\ell)$ is the unique 4-tuple in Λ which satisfies $\mathcal{P}^*(\rho(D_\ell) - \delta) \in D_\ell$. Let $Q(E_\ell)$ denote the set of the 2^4-tuples $\boldsymbol{q} \in Q$ which satisfy $SP_{\boldsymbol{q}} \subset E_\ell$ and $\Delta(\boldsymbol{q}) = \rho(E_\ell)$, where $\rho(E_\ell)$ is the unique 4-tuple in Λ which satisfies $\mathcal{P}^*(\rho(E_\ell) - \delta) \in E_\ell$.

For $h = 4$, the following theorem says that the set Q_M defined in Lemma 2 is just the union of the sets $Q(\Xi)$ of all the $M(0)$-sets Ξ.

Theorem 1 *If $h = 4$, then we have*

$$Q_M = \bigcup_{\ell=1}^{4} (Q(C_\ell) \cup Q(D_\ell) \cup Q(E_\ell)). \tag{25}$$

Proof: On hand, assume $\boldsymbol{q}$ is an arbitrary tuple of Q_M. Since $SP_{\boldsymbol{q}}$ is an $m(\Delta(\boldsymbol{q}) - \delta)$-set, by Lemma 4 we see that there is an $M(\Delta(\boldsymbol{q}) - \delta)$-set Ξ with $SP_{\boldsymbol{q}} \subset \Xi$ such that (23) and (24) hold for $\gamma = \Delta(\boldsymbol{q}) - \delta$.

If $\Xi = C_\ell$ for some ℓ, then by (24) and the definition of C_ℓ we know that ℓ must belong to the index set $\zeta(\Delta(\boldsymbol{q}) - \delta)$ and thus by (23) we have $\Delta(\boldsymbol{q})_\ell - \delta_\ell = 0$. Hence $\boldsymbol{q}$ belongs to $Q(C_\ell)$.

If $\Xi = D_\ell$ for some ℓ, then by (24) and the definition of D_ℓ we know that $\{1,2,3,4\}\backslash\{\ell\}$ must be subset of $\zeta(\Delta(\boldsymbol{q}) - \delta)$. Hence from (23) and $\Delta(\boldsymbol{q}) \in \Lambda$ and the uniqueness of $\rho(D_\ell)$ we know $\Delta(\boldsymbol{q})_j = \rho(D_\ell)_j$ for $j \in \{1,2,3,4\}\backslash\{\ell\}$, and thus $\boldsymbol{q}$ belongs to $Q(D_\ell)$.

If $\Xi = E_\ell$ for some ℓ, then by (24) and the definition of E_ℓ we know that $\zeta(\Delta(\boldsymbol{q}) - \delta) = \{1,2,3,4\}$, i.e. $\Delta(\boldsymbol{q})_j - \delta_j \in B$ for $j = 1,2,3,4$. Hence by (23) and $\Delta(\boldsymbol{q}) \in \Lambda$ and the uniqueness of $\rho(E_\ell)$ we know $\Delta(\boldsymbol{q}) = \rho(E_\ell)$ and we see $\boldsymbol{q}$ belongs to $Q(E_\ell)$.

One the other hand, assume $\boldsymbol{q} \in Q(\Xi)$ for some $M(0)$-set Ξ. By the definitions of $Q(\Xi)$ and Ξ, we see easily that (23) and (24) hold for Ξ and $\gamma = \Delta(\boldsymbol{q}) - \delta$. Thus by Lemma 4 we know Ξ is an $M(\Delta(\boldsymbol{q}) - \delta)$-set, and sequencely $SP_{\boldsymbol{q}}$ is an $m(\Delta(\boldsymbol{q}) - \delta)$-set. By the definition of $Q(\Xi)$ we have also $\Delta(\boldsymbol{q}) - \delta \in \Gamma_0$. Hence $\boldsymbol{q}$ belongs to Q_M. $\triangle\triangle$

The following lemma shows some properties for the 2^4-tuples $\boldsymbol{q}$ in the sets $Q(\Xi)$ for each $M(0)$-set Ξ.

Lemma 5 *Assume $\boldsymbol{q}$ is a tuple in $Q(\Xi)$ for some $M(0)$-set Ξ and let $\lambda \stackrel{\triangle}{=} \Delta(\boldsymbol{q})$. Then*
1. If $\Xi = C_\ell$, then $\delta_\ell \geq \delta_j$ for $j \neq \ell$, and $\lambda_\ell = \delta_\ell$ and $\max\{-\delta_\ell, \delta_j\} \leq \lambda_j \leq \delta_\ell$ for $j \in \{1,2,3,4\}\backslash\{\ell\}$.
2. If $\Xi = D_\ell$, then $\max\{\rho(D_\ell)_\ell, \max_{j\neq\ell}\{|\rho(D_\ell)_j|\}\} \leq \sum_{j\neq\ell}\rho(D_\ell)_j$, $\lambda_j = \rho(D_\ell)_j$ for $j \in \{1,2,3,4\}\backslash\{\ell\}$ and $\max\{-\sum_{j\neq\ell}\rho(D_\ell)_j, \rho(D_\ell)_\ell\} \leq \lambda_\ell \leq \sum_{j\neq\ell}\rho(D_\ell)_j$.
3. If $\Xi = E_\ell$, then $\sum_{j=1}^4 \rho(E_\ell)_j \geq 0$ and $\rho(E_\ell)_\ell + \min_{j\neq\ell}\{\rho(E_\ell)_j\} \geq 0$ and $\lambda = \rho(E_\ell)$.

Proof: 1. Assume $\Xi = C_\ell$, i.e. $\boldsymbol{q} \in Q(C_\ell)$. By the definition of $Q(C_\ell)$, we have $\Delta(\boldsymbol{q})_\ell = \delta_\ell$. Thus $\delta_\ell = \lambda_\ell = \sum_{\alpha\in C_\ell}\boldsymbol{q}_\alpha \geq \sum_{\alpha\in C_\ell}\boldsymbol{q}_\alpha(-1)^{\alpha_j} = \lambda_j \geq \delta_j$ and $\lambda_j \geq -\sum_{\alpha\in C_\ell}\boldsymbol{q}_\alpha = -\delta_\ell$ for $j \in \{1,2,3,4\}\backslash\{\ell\}$.

2. Assume $\Xi = D_\ell$, i.e. $\boldsymbol{q} \in Q(D_\ell)$. By the definition of $Q(D_\ell)$, we have $\lambda_j = \rho(D_\ell)_j$ for $j \in \{1,2,3,4\}\backslash\{\ell\}$. Since $\sum_{j\neq\ell}(-1)^{\alpha_j} \geq 1$ for all $\alpha \in D_\ell$, we see $\sum_{j\neq\ell}\rho(D_\ell)_j = \sum_{j\neq\ell}\lambda_j = \sum_{j\neq\ell}\sum_{\alpha\in D_\ell}\boldsymbol{q}_\alpha(-1)^{\alpha_j} \geq \sum_{\alpha\in D_\ell}\boldsymbol{q}_\alpha \geq \max_{j=1}^4\{|\lambda_j|\}$. Clearly, we also have $\lambda_\ell \geq \rho(D_\ell)_\ell$.

3. Assume $\Xi = E_\ell$, i.e. $\boldsymbol{q} \in Q(E_\ell)$. By the definition of $Q(E_\ell)$, we have $\lambda_j = \rho(E_\ell)_j$ for $j = 1,2,3,4$. Since for all $\alpha \in E_\ell$ we have $\sum_{j=1}^4(-1)^{\alpha_j} \geq 0$ and $(-1)^{\alpha_\ell} + \min_{j\neq\ell}\{(-1)^{\alpha_j}\} \geq 0$, we see $\sum_{j=1}^4\lambda_j \geq 0$ and $\lambda_\ell + \min_{j\neq\ell}\{\lambda_j\} \geq 0$. $\triangle\triangle$

In general, for some $M(0)$-sets Ξ the sets $Q(\Xi)$ are empty and should be excluded from further consideration. Let $\aleph$ denote the set of $M(0)$-sets Ξ with $Q(\Xi) \neq \emptyset$. Without loss of generality, hereafter we suppose

$$\delta_1 \geq \delta_2 \geq \delta_3 \geq \delta_4,\ \delta_1 > 0. \tag{26}$$

The following Lemma 6 and Theorem 2 show that the Q_M is a union of at most 9 subsets $Q(\Xi)$, and as the simplest case, is equal to $Q(C_1)$ if $\delta_2 + \delta_3 + 1 < 0$ and $\sum_{i=1}^4 \rho(E_1)_i < 0$. These results will reduce in some extent the complexity of our computation methods for

the sufficient testing condition which are proposed in next section.

Lemma 6 *(i).* $\cup_{\ell=2}^{4} Q(C_\ell) \subset Q(C_1)$.
(ii). If $\rho(D_1)_1 > \sum_{j=2}^{4} \rho(D_1)_j$, *then* $D_1 \notin \aleph$.
(iii). If $\delta_3 + \delta_4 + 1 < 0$, *then* $\{E_3, E_4, D_2\} \cap \aleph = \emptyset$.
(iv). If $\delta_2 + \delta_4 + 1 < 0$, *then* $\{E_2, D_3\} \cap \aleph = \emptyset$.
(v). If $\delta_2 + \delta_3 + 1 < 0$, *then* $D_4 \notin \aleph$.
(vi). If $\delta_1 + \delta_4 + 1 < 0$ *or* $\sum_{j=1}^{4} \rho(E_1)_j < 0$, *then* $E_1 \notin \aleph$.

Proof: Assume $\boldsymbol{q} \in Q(\Xi)$ for some $M(0)$-set Ξ.

(i). If $\Xi = C_\ell$, we see $\delta_\ell = \Delta(\boldsymbol{q})_\ell = \sum_{\alpha\in\Xi} \boldsymbol{q}_\alpha \geq \sum_{\alpha\in\Xi} \boldsymbol{q}_\alpha (-1)^{\alpha_1} = \Delta(\boldsymbol{q})_1 \geq \delta_1$. Hence by $\delta_1 \geq \delta_\ell$ we see $\Delta(\boldsymbol{q})_1 = \delta_1$ and $\alpha_1 = 0$ for all $\alpha \in SP\boldsymbol{q}$, i.e. $\boldsymbol{q} \in Q(C_1)$.

(ii). If $\Xi = D_1$, then by Lemma 5 we see $\rho(D_1)_1 \leq \sum_{j=2}^{4} \rho(D_1)_j$.

(iii). If $\Xi = E_3$ or E_4, then by Lemma 5 we see $\rho(E_3)_3 + \rho(E_3)_4 \geq 0$ or $\rho(E_4)_3 + \rho(E_4)_4 \geq 0$. Since $\alpha_3 + \alpha_4 \leq 1$ for all $\alpha \in E_3 \cup E_4$, we see $(\rho(E_4)_3 - \delta_3) + (\rho(E_4)_4 - \delta_4) \leq 1$. Hence $\delta_3 + \delta_4 + 1 \geq 0$.

If $\Xi = D_2$, then by Lemma 5 we see $\rho(D_2)_1 = |\rho(D_2)_1| \leq \sum_{j\neq 2} \rho(D_2)_j$, i.e. $\rho(D_2)_3 + \rho(D_2)_4 \geq 0$. We can also see $(\rho(D_2)_3 - \delta_3) + (\rho(D_2)_4 - \delta_4) \leq 1$. Thus $\delta_3 + \delta_4 + 1 \geq 0$.

(iv). If $\Xi = E_2$, then by Lemma 5 we see $\rho(E_2)_2 + \rho(E_2)_4 \geq 0$. We can also see $(\rho(E_2)_2 - \delta_2) + (\rho(E_2)_4 - \delta_4) \leq 1$. Hence $\delta_2 + \delta_4 + 1 \geq 0$.

If $\Xi = D_3$, then by Lemma 5 we see $\rho(D_3)_1 = |\rho(D_3)_1| \leq \sum_{j\neq 3} \rho(D_3)_j$, i.e. $\rho(D_3)_2 + \rho(D_3)_4 \geq 0$. We can also see $(\rho(D_3)_2 - \delta_2) + (\rho(D_3)_4 - \delta_4) \leq 1$. Thus $\delta_2 + \delta_4 + 1 \geq 0$.

(v). If $\Xi = D_4$, then by Lemma 5 we see $\rho(D_4)_1 = |\rho(D_4)_1| \leq \sum_{j\neq 4} \rho(D_4)_j$, i.e. $\rho(D_4)_2 + \rho(D_4)_3 \geq 0$. We can also see $(\rho(D_4)_2 - \delta_2) + (\rho(D_4)_3 - \delta_3) \leq 1$. Thus $\delta_2 + \delta_3 + 1 \geq 0$.

(vi). If $\Xi = E_1$, then by Lemma 5 we see $\sum_{j=1}^{4} \rho(E_1)_j \geq 0$ and $\rho(E_1)_1 + \rho(E_1)_4 \geq 0$. We can also see $(\rho(E_1)_1 - \delta_1) + (\rho(E_1)_4 - \delta_4) \leq 1$. Hence $\delta_1 + \delta_4 + 1 \geq 0$. △△

The following theorem is a direct corollary of Lemma 6.

Theorem 2 *Assume* δ_i *satisfy (26), then we have*

$$\aleph \backslash \{C_1, C_2, C_3, C_4\} \subset \aleph^*, \tag{27}$$

where $\aleph^*$ *is defined as*
(i). $\emptyset$ *if* $\delta_2 + \delta_3 + 1 < 0$ *and* $\sum_{i=1}^{4} \rho(E_1)_i < 0$;
(ii). $\{E_1\}$ *if* $\delta_2 + \delta_3 + 1 < 0$ *and* $\sum_{i=1}^{4} \rho(E_1)_i \geq 0$;
(iii). $\{D_4\}$ *if* $\delta_2 + \delta_3 + 1 \geq 0$ *and* $\delta_1 + \delta_4 + 1 < 0$;
(iv). $\{E_1, D_4\}$ *if* $\delta_2 + \delta_3 + 1 \geq 0$, $\delta_1 + \delta_4 + 1 \geq 0$ *and* $\delta_2 + \delta_4 + 1 < 0$;
(v). $\{E_1, E_2, D_3, D_4\}$ *if* $\delta_2 + \delta_4 + 1 \geq 0$ *and* $\delta_3 + \delta_4 + 1 < 0$;
(vi). $\{E_1, E_2, E_3, E_4, D_2, D_3, D_4\}$ *if* $\delta_3 + \delta_4 + 1 \geq 0$ *and* $\rho(D_1)_1 > \sum_{i=2}^{4} \rho(D_1)_i$;
(vii). $\{E_1, E_2, E_3, E_4, D_1, D_2, D_3, D_4\}$ *if* $\rho(D_1)_1 \leq \sum_{i=2}^{4} \rho(D_1)_i$.

4 Computation methods for the testing condition of the case $h = 4$

For any $M(0)$-set Ξ, if $\Xi \in \aleph$, i.e. $Q(\Xi) \neq \emptyset$, then we write

$$L\_\Xi \stackrel{\triangle}{=} \min_{\boldsymbol{q}\in Q(\Xi)} L'(\boldsymbol{q}), \tag{28}$$

if $\Xi \notin \aleph$, i.e. $Q(\Xi) = \emptyset$, then we write $L\_\Xi \stackrel{\triangle}{=} +\infty$. If δ_i satisfy (26), then according to Theorem 1 and (i) of Lemma 6, we know

$$Q_M = Q(C_1) \cup \left(\bigcup_{\Xi\in\aleph^*} Q(\Xi) \right). \tag{29}$$

Hence by Lemma 2 we have

$$\underline{L}[V^N_{d_1,d_2,d_3,d_4}(\boldsymbol{u}^1, \boldsymbol{u}^2, \boldsymbol{u}^3, \boldsymbol{u}^4)] = \min_{\Xi\in\{C_1\}\cup\aleph^*} L\_\Xi. \tag{30}$$

By using of the Lemma 5, we will propose some sub-algorithms for computing L_Ξ in the subsections 4.1-4.3 for $\Xi = C_1$, D_ℓ and E_ℓ, respectively. A main algorithm for computing $\underline{L}[V^N_{d_1,d_2,d_3,d_4}(\boldsymbol{u}^1, \boldsymbol{u}^2, \boldsymbol{u}^3, \boldsymbol{u}^4)]$ is proposed in subsection 4.4.

4.1 Sub-algorithm for computating L_C_1

From 1 of Lemma 5, we can get the following corollary easily.

Corollary 1 *Write* $\delta_i^{\mathrm{C}} \stackrel{\triangle}{=} \max\{0, \lfloor(\delta_1 + \delta_i + 1)/2\rfloor\}$, $i = 2, 3, 4$. *Then* $Q(C_1)$ *consists of the* 2^h*-tuples* $\boldsymbol{q}$ *in* Q^* *which satisfy (12) and*

$$\begin{cases} \boldsymbol{q}_{0000} + \boldsymbol{q}_{0001} + \boldsymbol{q}_{0010} + \boldsymbol{q}_{0100} \\ \qquad + \boldsymbol{q}_{0110} + \boldsymbol{q}_{0101} + \boldsymbol{q}_{0011} + \boldsymbol{q}_{0111} = \delta_1, \\ \boldsymbol{q}_{0000} + \boldsymbol{q}_{0001} + \boldsymbol{q}_{0010} + \boldsymbol{q}_{0011} \geq \delta_2^{\mathrm{C}}, \\ \boldsymbol{q}_{0000} + \boldsymbol{q}_{0001} + \boldsymbol{q}_{0100} + \boldsymbol{q}_{0101} \geq \delta_3^{\mathrm{C}}, \\ \boldsymbol{q}_{0000} + \boldsymbol{q}_{0010} + \boldsymbol{q}_{0100} + \boldsymbol{q}_{0110} \geq \delta_4^{\mathrm{C}}, \\ \boldsymbol{q}_\alpha = 0, \quad \textit{for } \alpha \notin C_1. \end{cases} \tag{31}$$

For integers d, k with $0 \leq d \leq \delta_1$, $0 \leq k < \delta_1$, let $R_{d,k}$ be the set of the 2^h-tuples $\boldsymbol{q}$ in Q^* which satisfy (12) and

$$\begin{cases} \boldsymbol{q}_{0000} + \boldsymbol{q}_{0001} = d \\ \boldsymbol{q}_{0010} + \boldsymbol{q}_{0100} + \boldsymbol{q}_{0110} + \boldsymbol{q}_{0101} \\ \qquad + \boldsymbol{q}_{0011} + \boldsymbol{q}_{0111} = \delta_1 - d, \\ \boldsymbol{q}_{0010} + \boldsymbol{q}_{0011} \geq \delta_2^{\mathrm{C}} - d, \\ \boldsymbol{q}_{0100} + \boldsymbol{q}_{0101} \geq \delta_3^{\mathrm{C}} - d, \\ \boldsymbol{q}_{0000} + \boldsymbol{q}_{0010} + \boldsymbol{q}_{0100} + \boldsymbol{q}_{0110} \geq k, \\ \boldsymbol{q}_\alpha = 0, \text{ for } \alpha \notin C_1. \end{cases} \tag{32}$$

Clearly, we have

$$R_{d,\delta_4^{\mathrm{C}}} = \{\boldsymbol{q} \in Q(C_1) : \ \boldsymbol{q}_{0000} + \boldsymbol{q}_{0001} = d\}, \tag{33}$$

$$R_{d,\delta_4^{\mathrm{C}}} \subset R_{d,\delta_4^{\mathrm{C}}-1} \subset \ldots \subset R_{d,0} \subset Q^*. \tag{34}$$

If a 2^4-tuple $\boldsymbol{q} \in R_{d,k}$ satisfies

$$L'(\boldsymbol{q}) = \min_{\boldsymbol{q}'\in R_{d,k}} L'(\boldsymbol{q}'), \tag{35}$$

we call it $R_{d,k}$-**tuple**. We consider to find a $R_{d,\delta_4^{\rm C}}$-tuple for each d with $R_{d,\delta_4^{\rm C}} \neq \emptyset$.

At first, we give a condition for $R_{d,0} \neq \emptyset$. Assume $R_{d,0} \neq \emptyset$. From (32) and (12), we have $0 \leq d \leq n_{0000} + n_{0001}$, $\delta_1 - d \leq n_{0011} + n_{0010} + n_{0101} + n_{0100} + n_{0110} + n_{0111}$, $\delta_2^{\rm C} - d \leq n_{0011} + n_{0010}$, $\delta_3^{\rm C} - d \leq n_{0101} + n_{0100}$ and $\max\{\delta_2^{\rm C} - d, 0\} + \max\{\delta_3^{\rm C} - d, 0\} \leq \delta_1 - d$. Write

$$d_1^* \triangleq \delta_1 - n_{0011} - n_{0010} - n_{0101} - n_{0100} - n_{0110} - n_{0111}, \quad (36)$$

$$d_2^* \triangleq \delta_2^{\rm C} - n_{0011} - n_{0010},\ d_3^* \triangleq \delta_3^{\rm C} - n_{0101} - n_{0100}, \quad (37)$$

$$d^l \triangleq \max\{0, d_1^*, d_2^*, d_3^*, \delta_2^{\rm C} + \delta_3^{\rm C} - \delta_1\}, \quad (38)$$

$$d^r \triangleq \min\{\delta_1, n_{0000} + n_{0001}\}. \quad (39)$$

Then we have $d^l \leq d \leq d^r$.

On the other hand, assume $d^l \leq d \leq d^r$. Let

$$v(d) \triangleq \delta_1 - d - \max\{\delta_2^{\rm C} - d, 0\} - \max\{\delta_3^{\rm C} - d, 0\}, \quad (40)$$

$$V(d) \triangleq (\mathcal{D}_{0011} \cup \mathcal{D}_{0010})^{(\delta_2^{\rm C} - d)} \cup (\mathcal{D}_{0101} \cup \mathcal{D}_{0100})^{(\delta_3^{\rm C} - d)}, \quad (41)$$

$$V^*(d) \triangleq (\mathcal{D}_{0000} \cup \mathcal{D}_{0001})^{(d)} \cup V(d) \cup ((\mathcal{D}_{0011} \cup \mathcal{D}_{0010} \cup \mathcal{D}_{0101} \cup \mathcal{D}_{0100} \cup \mathcal{D}_{0110} \cup \mathcal{D}_{0111}) \backslash V(d))^{(v(d))}. \quad (42)$$

Then $v(d) \geq 0$, and it is easy to illustrate that the 2^4-tuple $\boldsymbol{q}$, which satisies $\mathcal{D}(\boldsymbol{q}) = V^*(d)$, must belong to $R_{d,0}$, and furthermore it is a $R_{d,k}$-tuple for all $k \leq v_d \triangleq |V^*(d) \cap (\mathcal{D}_{0000} \cup \mathcal{D}_{0010} \cup \mathcal{D}_{0100} \cup \mathcal{D}_{0110})|$. If $\delta_4^{\rm C} > v_d$, we will give a $R_{d,\delta_4^{\rm C}}$-tuple by iteration.

For $X \subset \{1, 2, \ldots, N\}$, let $s(X)$ and $l(X)$ denote the smallest integer and the largest integer in X, respectively. For convenience, we define $s(\emptyset) \triangleq +\infty$, $l(\emptyset) \triangleq -\infty$, and $|\boldsymbol{r}_{-\infty}| \triangleq -\infty$. We note that $|\boldsymbol{r}_{+\infty}|$ has been defined as $+\infty$ before. We have the following lemma.

Lemma 7 *Assume $R_{d,k+1} \neq \emptyset$ and $\boldsymbol{q}^{d,k}$ is a $R_{d,k}$-tuple which satisfies*

$$\boldsymbol{q}_{0000}^{d,k} + \boldsymbol{q}_{0010}^{d,k} + \boldsymbol{q}_{0100}^{d,k} + \boldsymbol{q}_{0110}^{d,k} = k, \quad (43)$$

then there exist two sequences $\alpha \in \{0000, 0010, 0100, 0110\}$ and $\beta \in \{0001, 0011, 0101, 0111\}$ such that the 2^4-tuple $\boldsymbol{q}$ with

$$\begin{cases} \boldsymbol{q}_\alpha = \boldsymbol{q}_\alpha^{d,k} + 1,\ \boldsymbol{q}_\beta = \boldsymbol{q}_\beta^{d,k} - 1, \\ \boldsymbol{q}_{\alpha'} = \boldsymbol{q}_{\alpha'}^{d,k},\ \textit{for all } \alpha' \in B^4 \backslash \{\alpha, \beta\}, \end{cases} \quad (44)$$

is a $R_{d,k+1}$-tuple.

The proof of this lemma is given in the appendix of this paper. It is easy to see, for the output $\Omega(d)$ of the following Procedure-C, that $\Omega(d) = \mathcal{D}(\boldsymbol{q})$ for some $R_{d,\delta_4^{\rm C}}$-tuple $\boldsymbol{q}$ if $\Omega(d) \neq \{+\infty\}$, and $R_{d,\delta_4^{\rm C}} = \emptyset$ if $\Omega(d) = \{+\infty\}$.

Procedure-C

Input: Received tuple $\boldsymbol{r}$ with (14). Integers $\delta_2^{\rm C}$, $\delta_3^{\rm C}$, $\delta_4^{\rm C}$ and d. Sets $V^*(d)$ and $\mathcal{D}_\alpha$, $\alpha \in C_1$.

Output: Set $\Omega(d)$.

Start: Let $V_0 \triangleq V^*(d)$ and goto Step 0.

Step m:

If $|V_m \cap (\mathcal{D}_{0000} \cup \mathcal{D}_{0010} \cup \mathcal{D}_{0100} \cup \mathcal{D}_{0110})| \geq \delta_4^{\rm C}$, output V_m and END.

Else, let $i_s \triangleq s(\mathcal{D}_{0000} \backslash V_m)$, $i_l \triangleq l(\mathcal{D}_{0001} \cap V_m)$, $t \triangleq |\boldsymbol{r}_{i_s}| - |\boldsymbol{r}_{i_l}|$, $j_1^s \triangleq s(\mathcal{D}_{0010} \backslash V_m)$, $j_1^l \triangleq l(\mathcal{D}_{0011} \cap V_m)$, $t_1 \triangleq |\boldsymbol{r}_{j_1^s}| - |\boldsymbol{r}_{j_1^l}|$, $j_2^s \triangleq s(\mathcal{D}_{0100} \backslash V_m)$, $j_2^l \triangleq l(\mathcal{D}_{0101} \cap V_m)$, $t_2 \triangleq |\boldsymbol{r}_{j_2^s}| - |\boldsymbol{r}_{j_2^l}|$.

Step m.1:

Case 1: If $|V_m \cap (\mathcal{D}_{0011} \cup \mathcal{D}_{0010})| = \delta_2^{\rm C} - d$ and $|V_m \cap (\mathcal{D}_{0101} \cup \mathcal{D}_{0100})| = \delta_3^{\rm C} - d$, let $i_l' \triangleq l(\mathcal{D}_{0111} \cap V_m)$, and goto step m.2.

Case 2: If $|V_m \cap (\mathcal{D}_{0011} \cup \mathcal{D}_{0010})| = \delta_2^{\rm C} - d$ and $|V_m \cap (\mathcal{D}_{0101} \cup \mathcal{D}_{0100})| > \delta_3^{\rm C} - d$, let $i_l' \triangleq l((\mathcal{D}_{0101} \cup \mathcal{D}_{0111}) \cap V_m)$, and goto step m.2.

Case 3: If $|V_m \cap (\mathcal{D}_{0011} \cup \mathcal{D}_{0010})| > \delta_2^{\rm C} - d$ and $|V_m \cap (\mathcal{D}_{0101} \cup \mathcal{D}_{0100})| = \delta_3^{\rm C} - d$, let $i_l' \triangleq l((\mathcal{D}_{0011} \cup \mathcal{D}_{0111}) \cap V_m)$, and goto step m.2.

Case 4: If $|V_m \cap (\mathcal{D}_{0011} \cup \mathcal{D}_{0010})| > \delta_2^{\rm C} - d$ and $|V_m \cap (\mathcal{D}_{0101} \cup \mathcal{D}_{0100})| > \delta_3^{\rm C} - d$, let $i_l' \triangleq l((\mathcal{D}_{0011} \cup \mathcal{D}_{0101} \cup \mathcal{D}_{0111}) \cap V_m)$, and goto step m.2.

Step m.2: Let $i_s' \triangleq s((\mathcal{D}_{0010} \cup \mathcal{D}_{0100} \cup \mathcal{D}_{0110}) \backslash V_m)$ and $t' \triangleq |\boldsymbol{r}_{i_s'}| - |\boldsymbol{r}_{i_l'}|$.

If $t^* \triangleq \min\{t, t', t_1, t_2\} = +\infty$, output $\{+\infty\}$ and END.

Else

Case 1: If $t^* = t$, let $V_{m+1} \triangleq (V_m \backslash \{i_l\}) \cup \{i_s\}$, and goto Step $(m+1)$.

Case 2: If $t^* = t'$, let $V_{m+1} \triangleq (V_m \backslash \{i_l'\}) \cup \{i_s'\}$, and goto Step $(m+1)$.

Case 3: If $t^* = t_1$, let $V_{m+1} \triangleq (V_m \backslash \{i_1^l\}) \cup \{i_1^s\}$, and goto Step $(m+1)$.

Case 4: If $t^* = t_2$, let $V_{m+1} \triangleq (V_m \backslash \{i_2^l\}) \cup \{i_2^s\}$, and goto Step $(m+1)$. △△

Now we can give the following Sub-algorithm_C_1 for computing L_C_1.

Sub-algorithm_C_1

Input: Received tuple $\boldsymbol{r}$ with (14). Sets $\mathcal{D}_\alpha$, $\alpha \in C_1$. Integers δ_1, δ_2, δ_3, δ_4 with (26), and n_α, $\alpha \in C_1$.

Output: L_C_1.

1. By Corollary 1, compute $\delta_j^{\rm C}$, $j = 2, 3, 4$. And then by (36)-(39) compute d^l and d^r. If $d^l > d^r$, then output $+\infty$ (i.e. $Q(C_1) = \emptyset$). If $d^l \leq d^r$, for all integers d with $d^l \leq d \leq d^r$, by (41) and (42) generate the set $V^*(d)$ and by Procedure-C generate the set $\Omega(d)$.

2. Output $\min_{d^l \leq d \leq d^r} \sum_{i \in \Omega(d)} |\boldsymbol{r}_i|$. △△

For Sub-algorithm_C_1, in the worst case, the number of d with $d^l \leq d \leq d^r$ is $\delta_1 + 1$, and it needs $\delta_4^{\rm C} \leq \delta_1$ steps to generate the set $\Omega(d)$ for each d. In

Steps 0, 0.1, 0.2, the number of operations of real number is 7. For $m > 0$, in Steps m, $m.1$, $m.2$, at most two of t, t', t_1, t_2 need to be computed, and total number of operations of real number is 5. The number of operations of real number for computing $\sum_{i\in\Omega(d)} |\boldsymbol{r}_i|$ is $\delta_1 - 1$. Hence the total number of operations of real number for Sub-algorithm_C_1 is not more than $(\delta_1+1)(7+5(\delta_1-1)+(\delta_1-1))+\delta_1 = 6\delta_1^2+8\delta_1+1$ in the worst case.

4.2 Sub-algorithm for computating L_D_ℓ

From 2 of Lemma 5, we can also get the following corollary easily

Corollary 2 *Assume $Q(D_\ell) \neq \emptyset$, $1 \le \ell \le 4$.*
1) If $\ell = 1$, let $e = 4$, $f = 2$, $g = 3$ and $p_1 = 0001$, $p_2 = 1001$, $p_3 = 0100$, $p_4 = 1100$, $p_5 = 0010$, $p_6 = 1010$, $p_7 = 0000$, $p_8 = 1000$.
2) If $\ell = 2$, let $e = 1$, $f = 4$, $g = 3$ and $p_1 = 1000$, $p_2 = 1100$, $p_3 = 0001$, $p_4 = 0101$, $p_5 = 0010$, $p_6 = 0110$, $p_7 = 0000$, $p_8 = 0100$.
3) If $\ell = 3$, let $e = 1$, $f = 2$, $g = 4$ and $p_1 = 1000$, $p_2 = 1010$, $p_3 = 0100$, $p_4 = 0110$, $p_5 = 0001$, $p_6 = 0011$, $p_7 = 0000$, $p_8 = 0010$.
4) If $\ell = 4$, let $e = 1$, $f = 2$, $g = 3$ and $p_1 = 1000$, $p_2 = 1001$, $p_3 = 0100$, $p_4 = 0101$, $p_5 = 0010$, $p_6 = 0011$, $p_7 = 0000$, $p_8 = 0001$.

Write $\delta^{\rm D}_{ij} \triangleq \lfloor(\delta_i+\delta_j+1)/2\rfloor$, $i,j = e,f,g$, and $\delta^{\rm D} \triangleq \max\{0, \lfloor(\delta_\ell+\delta^{\rm D}_{ef}+\delta^{\rm D}_{eg}+\delta^{\rm D}_{fg}+1)/2\rfloor\}$, then $Q(D_\ell)$ consists of the 2^h-tuples $\boldsymbol{q}$ in Q^* which satisfy (12) and

$$\begin{cases} 2\boldsymbol{q}_{p_7}+\boldsymbol{q}_{p_8}+\boldsymbol{q}_{p_1}+\boldsymbol{q}_{p_3}+\boldsymbol{q}_{p_5} \ge \delta^{\rm D}, \\ \boldsymbol{q}_{p_7}+\boldsymbol{q}_{p_8}+\boldsymbol{q}_{p_1}+\boldsymbol{q}_{p_2} = \delta^{\rm D}_{fg}, \\ \boldsymbol{q}_{p_7}+\boldsymbol{q}_{p_8}+\boldsymbol{q}_{p_3}+\boldsymbol{q}_{p_4} = \delta^{\rm D}_{eg}, \\ \boldsymbol{q}_{p_7}+\boldsymbol{q}_{p_8}+\boldsymbol{q}_{p_5}+\boldsymbol{q}_{p_6} = \delta^{\rm D}_{ef}, \\ \boldsymbol{q}_\alpha = 0, \quad \text{for } \alpha \notin D_\ell. \end{cases} \tag{45}$$

The discussions in this subsection is almost done by following those of the last subsection. For nonnegative integers d, k, let $R^{d,k}$ denote the set of the 2^h-tuples $\boldsymbol{q}$ in Q^* which satisfy (12) and

$$\begin{cases} \boldsymbol{q}_{p_7}+\boldsymbol{q}_{p_8} = d, \\ \boldsymbol{q}_{p_1}+\boldsymbol{q}_{p_2} = \delta^{\rm D}_{fg} - d, \\ \boldsymbol{q}_{p_3}+\boldsymbol{q}_{p_4} = \delta^{\rm D}_{eg} - d, \\ \boldsymbol{q}_{p_5}+\boldsymbol{q}_{p_6} = \delta^{\rm D}_{ef} - d, \\ \boldsymbol{q}_{p_1}+\boldsymbol{q}_{p_3}+\boldsymbol{q}_{p_5}+\boldsymbol{q}_{p_7} \ge k, \\ \boldsymbol{q}_\alpha = 0, \text{ for } \alpha \notin D_\ell. \end{cases} \tag{46}$$

We see easily $R^{d,\delta^{\rm D}-d} = \{\boldsymbol{q} \in Q(D_\ell) : \boldsymbol{q}_{p_7}+\boldsymbol{q}_{p_8} = d\}$. If a 2^4-tuple $\boldsymbol{q} \in R^{d,k}$ satisfies

$$L'(\boldsymbol{q}) = \min_{\boldsymbol{q}'\in R^{d,k}} L'(\boldsymbol{q}'), \tag{47}$$

we call it $R^{d,k}$-**tuple**. If $R^{d,\delta^{\rm D}-d} \neq \emptyset$, we can also find a $R^{d,\delta^{\rm D}-d}$-tuple by iteration with using of the following Lemma 8, which is an analogue of Lemma 7, but much simpler.

Lemma 8 *If $R^{d,k+1} \neq \emptyset$ and $\dot{\boldsymbol{q}}^{d,k}$ is a $R^{d,k}$-tuple which satisfies*

$$\dot{\boldsymbol{q}}^{d,k}_{p_1}+\dot{\boldsymbol{q}}^{d,k}_{p_3}+\dot{\boldsymbol{q}}^{d,k}_{p_5}+\dot{\boldsymbol{q}}^{d,k}_{p_7} = k, \tag{48}$$

then there is an index $j \in \{1,3,5,7\}$ such that the 2^4-tuple $\boldsymbol{q}$ with

$$\begin{cases} \boldsymbol{q}_{p_j} = \dot{\boldsymbol{q}}^{d,k}_{p_j}+1, \ \boldsymbol{q}_{p_{j+1}} = \dot{\boldsymbol{q}}^{d,k}_{p_{j+1}}-1, \\ \boldsymbol{q}_\alpha = \dot{\boldsymbol{q}}^{d,k}_\alpha, \ \text{for all } \alpha \in B^4\backslash\{p_j,p_{j+1}\}, \end{cases} \tag{49}$$

is a $R^{d,k+1}$-tuple.

The proof of this lemma can be given by following the proof of Lemma 7, and is omitted here. Now we can propose the following Sub-algorithm_D_ℓ for computing L_D_ℓ.

Sub-algorithm_D_ℓ
Input: Received tuple $\boldsymbol{r}$ with (14). Integers ℓ with $1 \le \ell \le 4$, δ_i, $i = 1,2,3,4$, and n_α, $\alpha \in D_\ell$. Sets $\mathcal{D}_\alpha$, $\alpha \in D_\ell$.
Output: L_D_ℓ.

1. By Corollary 2, define e, f, g and p_j, $1 \le j \le 8$, and compute $\delta^{\rm D}_{ij}$, $i,j = e,f,g$, and $\delta^{\rm D}$. And then compute

$$\delta'_{fg} \triangleq \delta^{\rm D}_{fg} - n_{p_1} - n_{p_2}, \ \delta'_{eg} \triangleq \delta^{\rm D}_{eg} - n_{p_3} - n_{p_4},$$
$$\delta'_{ef} \triangleq \delta^{\rm D}_{ef} - n_{p_5} - n_{p_6}, \ d_l \triangleq \max\{0, \delta'_{fg}, \delta'_{eg}, \delta'_{ef}\},$$
$$d_r \triangleq \min\{\delta^{\rm D}_{ef}, \delta^{\rm D}_{eg}, \delta^{\rm D}_{fg}, n_{p_7}+n_{p_8}\}.$$

2. If $d_l > d_r$, output $+\infty$ (i.e. $Q(D_\ell) = \emptyset$). If $d_l \le d_r$, for all integer d with $d_l \le d \le d_r$, generate

$$W(d) \triangleq (\mathcal{D}_{p_7} \cup \mathcal{D}_{p_8})^{(d)} \cup (\mathcal{D}_{p_1} \cup \mathcal{D}_{p_2})^{(\delta^{\rm D}_{fg}-d)} \cup (\mathcal{D}_{p_3} \cup \mathcal{D}_{p_4})^{(\delta^{\rm D}_{eg}-d)} \cup (\mathcal{D}_{p_5} \cup \mathcal{D}_{p_6})^{(\delta^{\rm D}_{ef}-d)},$$

and generate $\Psi(d)$ by using of the Procedure-D.
3. Output $\min_{d_l\le d\le d_r} \sum_{i\in\Psi(d)} |\boldsymbol{r}_i|$. △△

Procedure-D
Input: Received tuple $\boldsymbol{r}$ with (14). Integers $\delta^{\rm D}$ and d. Sets $W(d)$ and $\mathcal{D}_\alpha$, $\alpha \in D_\ell$. Sequences p_i, $i = 1,2,\ldots,8$.
Output: Set $\Psi(d)$.

Start: Let $W_0 \triangleq W(d)$ and goto step 0.
Step m:
If $|(\mathcal{D}_{p_1} \cup \mathcal{D}_{p_3} \cup \mathcal{D}_{p_5} \cup \mathcal{D}_{p_7}) \cap W_m| \ge \delta^{\rm D} - d$, output W_m and END.
Else, compute

$i^s_0 \triangleq s(\mathcal{D}_{p_7}\backslash W_m)$, $i^l_0 \triangleq l(\mathcal{D}_{p_8} \cap W_m)$, $t \triangleq |\boldsymbol{r}_{i^s_0}| - |\boldsymbol{r}_{i^l_0}|$,
$i^s_1 \triangleq s(\mathcal{D}_{p_1}\backslash W_m)$, $i^l_1 \triangleq l(\mathcal{D}_{p_2} \cap W_m)$, $t \triangleq |\boldsymbol{r}_{i^s_1}| - |\boldsymbol{r}_{i^l_1}|$,
$i^s_2 \triangleq s(\mathcal{D}_{p_3}\backslash W_m)$, $i^l_2 \triangleq l(\mathcal{D}_{p_4} \cap W_m)$, $t \triangleq |\boldsymbol{r}_{i^s_2}| - |\boldsymbol{r}_{i^l_2}|$,
$i^s_3 \triangleq s(\mathcal{D}_{p_5}\backslash W_m)$, $i^l_3 \triangleq l(\mathcal{D}_{p_6} \cap W_m)$, $t \triangleq |\boldsymbol{r}_{i^s_3}| - |\boldsymbol{r}_{i^l_3}|$.
and then goto Step $m.1$.

Step $m.1$: Determine s_0, s_1, s_2, s_3 with $\{s_0, s_1, s_2, s_3\} = \{0,1,2,3\}$ and $t_{s_0} \le t_{s_1} \le t_{s_2} \le t_{s_3}$.

If $t_{s_0} = +\infty$, output $\{+\infty\}$ and END.
Else

Case 1: If $s_0 = 0$, let $W_{m+1} \stackrel{\triangle}{=} (W_m \backslash \{i_0^l\}) \cup \{i_0^s\}$, and goto Step $(m+1)$.

Case 2: If $s_0 = 1$, let $W_{m+1} \stackrel{\triangle}{=} (W_m \backslash \{i_1^l\}) \cup \{i_1^s\}$, and goto Step $(m+1)$.

Case 3: If $s_0 = 2$, let $W_{m+1} \stackrel{\triangle}{=} (W_m \backslash \{i_2^l\}) \cup \{i_2^s\}$, and goto Step $(m+1)$.

Case 4: If $s_0 = 3$, let $W_{m+1} \stackrel{\triangle}{=} (W_m \backslash \{i_3^l\}) \cup \{i_3^s\}$, and goto Step $(m+1)$. $\triangle\triangle$

We can show easily that $R^{d,0}$ is not empty if and only if d satisfies $d_l \le d \le d_r$. Furthermore, it is very easy to illustrate that the output of Sub-algorithm_D_ℓ is just L_D_ℓ by Lemma 8. Now we consider the computation complexity of this algorithm. The number of d with $d_l \le d \le d_r$ is not more than $\delta_1 + 1$. We note that, for each d, it needs 10 computations of real numbers in the first step, and in each next step, only one of t_0, t_1, t_2, t_3 needs to be computed again, and by only two computations of real numbers we can get the order of t_0, t_1, t_2, t_3 from the old one. It needs at most $\delta^{\rm D} - d$ steps to generate $\Psi(d)$. The number of operations of real numbers for computing $\sum_{i\in\Psi(d)} |\boldsymbol{r}_i|$ is $\delta^{\rm D}_{ef} + \delta^{\rm D}_{eg} + \delta^{\rm D}_{fg} - 2d - 1$. Thus the total number of operations of real numbers for Sub-algorithm_D_ℓ is not greater than $\sum_{d=0}^{\delta_1}(10 + 3(\delta^{\rm D} - d - 1) + (\delta^{\rm D}_{ef} + \delta^{\rm D}_{eg} + \delta^{\rm D}_{fg} - 2d)) \le (13\delta_1^2 + 27\delta_1 + 14)/2$.

4.3 Sub-algorithm for computating L_E_ℓ

The following corollary can also be deduced easily from 3 of Lemma 5.

Corollary 3 *Assume $Q(E_\ell) \neq \emptyset$, $1 \le \ell \le 4$.*
1) If $\ell = 1$, let $e = 4$, $f = 2$, $g = 3$ and $p_1 = 0001$, $p_2 = 0110$, $p_3 = 0100$, $p_4 = 0011$, $p_5 = 0010$, $p_6 = 0101$, $p_7 = 0000$, $p_8 = 1000$.
2) If $\ell = 2$, let $e = 4$, $f = 1$, $g = 3$ and $p_1 = 0001$, $p_2 = 1010$, $p_3 = 1000$, $p_4 = 0011$, $p_5 = 0010$, $p_6 = 1001$, $p_7 = 0000$, $p_8 = 0100$.
3) If $\ell = 3$, let $e = 4$, $f = 2$, $g = 1$ and $p_1 = 0001$, $p_2 = 1100$, $p_3 = 0100$, $p_4 = 1001$, $p_5 = 1000$, $p_6 = 0101$, $p_7 = 0000$, $p_8 = 0010$.
4) If $\ell = 4$, let $e = 1$, $f = 2$, $g = 3$ and $p_1 = 1000$, $p_2 = 0110$, $p_3 = 0100$, $p_4 = 1010$, $p_5 = 0010$, $p_6 = 1100$, $p_7 = 0000$, $p_8 = 0001$.

Write $\delta_i^{\rm E} = \lfloor(\delta_\ell + \delta_i + 1)/2\rfloor$, $i = e, f, g$, and denote

$$\begin{cases} \lfloor(\sum_{i=1}^4 \delta_i + 1)/2\rfloor, & \text{if } 2|(\delta_e + \delta_f) \text{ and } 2|(\delta_e + \delta_g), \\ \delta_e^{\rm E} + \delta_f^{\rm E} + \delta_g^{\rm E} - \delta_\ell, & \text{for other cases,} \end{cases}$$

by $\delta^{\rm E}$, then $Q(E_\ell)$ consists of the 2^h-tuples $\boldsymbol{q}$ in Q^* which satisfy (12) and

$$\begin{cases} 2\boldsymbol{q}_{p_7} + \boldsymbol{q}_{p_8} + \boldsymbol{q}_{p_1} + \boldsymbol{q}_{p_3} + \boldsymbol{q}_{p_5} = \delta^{\rm E}, \\ \boldsymbol{q}_{p_7} + \boldsymbol{q}_{p_3} + \boldsymbol{q}_{p_5} + \boldsymbol{q}_{p_2} = \delta_e^{\rm E}, \\ \boldsymbol{q}_{p_7} + \boldsymbol{q}_{p_1} + \boldsymbol{q}_{p_5} + \boldsymbol{q}_{p_4} = \delta_f^{\rm E}, \\ \boldsymbol{q}_{p_7} + \boldsymbol{q}_{p_1} + \boldsymbol{q}_{p_3} + \boldsymbol{q}_{p_6} = \delta_g^{\rm E}, \\ \boldsymbol{q}_\alpha = 0, \quad \text{for } \alpha \notin E_\ell. \end{cases} \tag{50}$$

The 2^4-tuples $\boldsymbol{q}$ in $Q(E_\ell)$ can also be given by

$$\boldsymbol{q}_{p_2} = \delta_e^{\rm E} - x,\ \boldsymbol{q}_{p_4} = \delta_f^{\rm E} - y, \tag{51}$$
$$\boldsymbol{q}_{p_6} = \delta_g^{\rm E} - z,\ \boldsymbol{q}_{p_8} = \delta^{\rm E} - w, \tag{52}$$
$$\boldsymbol{q}_{p_1} = y + z - w,\ \boldsymbol{q}_{p_3} = x + z - w, \tag{53}$$
$$\boldsymbol{q}_{p_5} = x + y - w,\ \boldsymbol{q}_{p_7} = 2w - (x + y + z), \tag{54}$$

where w, x, y, z satisfy

$$\max\{0, \delta^{\rm E} - n_{p_8}\} \le w \le \delta^{\rm E}, \tag{55}$$
$$\max\{0, \delta_e^{\rm E} - n_{p_2}\} \le x \le \delta_e^{\rm E}, \tag{56}$$
$$\max\{0, \delta_f^{\rm E} - n_{p_4}\} \le y \le \delta_f^{\rm E}, \tag{57}$$
$$\max\{0, \delta_g^{\rm E} - n_{p_6}\} \le z \le \delta_g^{\rm E}, \tag{58}$$
$$0 \le y + z - w \le n_{p_1},\ 0 \le x + z - w \le n_{p_3}, \tag{59}$$
$$0 \le x + y - w \le n_{p_5}, 0 \le 2w - (x + y + z) \le n_{p_7}. \tag{60}$$

For any integer w with (55), let $\mho(w)$ denote the set of pairs $\pi \stackrel{\triangle}{=} (x, y, z)$ of integers x, y, z which satisfy (56)-(60). For $\pi \in \mho(w)$, let $\underline{\boldsymbol{q}_w(\pi)}$ be the 2^4-tuple of $Q(E_\ell)$ defined by (51)-(54). Clearly,

$$\begin{aligned} &\{\boldsymbol{q}_w(\pi) :\ \pi \in \mho(w)\} \\ &= \{\boldsymbol{q} \in Q(E_\ell) :\ \boldsymbol{q}_{p_8} = \delta^{\rm E} - w\}. \end{aligned} \tag{61}$$

For simplicity, we write $L_w(\pi) \stackrel{\triangle}{=} L'(\boldsymbol{q}_w(\pi))$. Let

$$\begin{aligned} \Upsilon_1 \stackrel{\triangle}{=} \{&(1,0,0),\ (-1,0,0),\ (0,1,0),\ (0,-1,0),\\ &(0,0,1),\ (0,0,-1),\ (1,-1,0),\ (-1,1,0),\\ &(1,0,-1),\ (-1,0,1),\ (0,1,-1),\ (0,-1,1)\}, \end{aligned}$$

$$\begin{aligned} \Upsilon_2 \stackrel{\triangle}{=} \{&(1,1,-1),\ (-1,-1,1),\ (1,-1,1),\\ &(-1,1,-1),\ (-1,1,1),\ (1,-1,-1)\}. \end{aligned}$$

If $\pi \in \mho(w)$, we see that $L_w(\pi+\pi')$ can be computed from $L_w(\pi)$ by only four operations of real numbers for any $\pi' \in \Upsilon_1$ and by six operations of real numbers for any $\pi' \in \Upsilon_2$. We also see, for any $\pi' \in \Upsilon_1 \cup \Upsilon_2$, that the well-defined domain of the function $L_w(\pi + t\pi')$ of t is an interval and $L_w(\pi + t\pi')$ is down-convex on t, i.e. $L_w(\pi + (t+1)\pi') - L_w(\pi + t\pi')$ is monotonous increasing on t. For convenience, we define $L_w(\pi) \stackrel{\triangle}{=} +\infty$ if $\pi \notin \mho(w)$. For $\pi \in \mho(w)$, let $\underline{\Re(\pi)}$ denote the set of pairs $\pi' \in \Upsilon_1 \cup \Upsilon_2$ with $L_w(\pi) \le L_w(\pi + \pi')$. For $\pi' = (x', y', z') \in \Upsilon_1 \cup \Upsilon_2$, let $\underline{\Upsilon(\pi')}$ denote the set of pairs $\pi'' = (x'', y'', z'')$ in $\Upsilon_1 \cup \underline{\Upsilon_2}$ which satisfy the following 7 inequalities

$$\begin{aligned} &x'x'' \ge 0,\ (y' + z')(y'' + z'') \ge 0,\\ &y'y'' \ge 0,\ (x' + z')(x'' + z'') \ge 0,\\ &z'z'' \ge 0,\ (x' + y')(x'' + y'') \ge 0,\\ &(x' + y' + z')(x'' + y'' + z'') \ge 0. \end{aligned}$$

For example, we can show easily that $\{(1,0,0),\ (0,1,0),\ (0,0,1),\ (1,-1,0),\ (1,0,-1),\ (1,1,-1),\ (1,-1,1)\} \subset \Upsilon(1,0,0)$, $\{(1,0,0),\ (0,-1,0),\ (1,-1,0),\ (1,0,-1),\ (0,-1,1),\ (1,-1,1),\ (1,-1,-1)\} \subset \Upsilon(1,-1,0)$, and

$\{(1,0,0),\ (0,1,0),\ (1,0,-1),\ (0,1,-1),\ (1,1,-1)\} \subset \Upsilon(1,1,-1)$. We say subset $\Upsilon \subset \Upsilon_1 \cup \Upsilon_2$ **coherent** if $\Upsilon \subset \Upsilon(\pi')$ for every $\pi' \in \Upsilon$. For example, $\{(1,0,0),\ (0,1,0),\ (0,0,1)\}$, $\{(1,0,0),\ (0,1,0),\ (1,1,-1)\}$, $\{(1,0,0),\ (1,-1,0),\ (1,0,-1)\}$, $\{(1,0,0),\ (1,-1,0),\ (1,-1,1)\}$ and $\{(1,-1,0),\ (1,0,-1),\ (1,-1,-1)\}$ are coherent sets.

Lemma 9 *Assume $\pi \in \mho(w)$, $\Upsilon = \{\pi_1, \pi_2, \ldots, \pi_k\} \subset \Re(\pi)$ is coherent and $t_1, t_2, \ldots, t_k$ are nonnegative integers, then $L_w(\pi) \le L_w(\pi + \sum_{i=1}^k t_i\pi_i)$. Indeed,*
1. $\Upsilon \subset \Re(\pi + \sum_{i=1}^k t_i\pi_i)$ if $\pi + \sum_{i=1}^k t_i\pi_i \in \mho(w)$.
2. $\pi + \sum_{i=1}^k t_i'\pi_i \notin \mho(w)$ for any nonnegative integers t_i' with $t_i' \ge t_i, i = 1, 2, \ldots, k$ if $\pi + \sum_{i=1}^k t_i\pi_i \notin \mho(w)$.

The proof of this lemma can be gotten easily from (14) and the definitions of $\Re(\pi)$ and the coherent set, and is omitted here.

Lemma 10 *A pair $\pi \in \mho(w)$ satisfies*

$$L_w(\pi) = \min_{\pi' \in \mho(w)} L_w(\pi'), \tag{62}$$

*called $\mho(w)$-**pair**, if and only if $\Upsilon_1 \cup \Upsilon_2 \subset \Re(\pi)$.*

Proof: If $\pi \in \mho(w)$ is a $\mho(w)$-pair, we see easily that $\Upsilon_1 \cup \Upsilon_2 \subset \Re(\pi)$ holds with respect to (62). On the other hand, assume $\Upsilon_1 \cup \Upsilon_2 \subset \Re(\pi)$ for $\pi \in \mho(w)$, π' is an arbitrary pair in $\mho(w)$ and write $(x,y,z) \stackrel{\triangle}{=} \pi' - \pi$. If all of x, y, z are nonnegative or nonpositive, from $\{(1,0,0),(0,1,0),(0,0,1)\}$ and $\{(-1,0,0),(0,-1,0),(0,0,-1)\}$ are coherent, we know $L_w(\pi') \ge L_w(\pi)$ easily. Now we assume, without loss of generality, that $x \ge y \ge 0, z < 0$.

If $-z \le y$, from $(x,y,z) = (x+z)(1,0,0) + (y+z)(0,1,0) + (-z)(1,1,-1)$ and $\{(1,0,0),\ (0,1,0),\ (1,1,-1)\}$ is coherent, we know $L_w(\pi') \ge L_w(\pi)$.

If $y < -z \le x$, from $(x,y,z) = (x+z)(1,0,0) + (-y-z)(1,0,-1) + y(1,1,-1)$ and $\{(1,0,0),\ (1,0,-1),(1,1,-1)\}$ is coherent, we know $L_w(\pi') \ge L_w(\pi)$.

If $x < -z < x+y$, from $(x,y,z) = (-y-z)(1,0,-1) + (-x-z)(0,1,-1) + (x+y+z)(1,1,-1)$ and $\{(1,0,-1),(0,1,-1),(1,1,-1)\}$ is coherent, we know $L_w(\pi') \ge L_w(\pi)$.

If $-z \ge x+y$, from $(x,y,z) = (-x-y-z)(0,0,-1) + x(1,0,-1) + y(0,1,-1)$ and $\{(0,0,-1),\ (1,0,-1),(0,1,-1)\}$ is coherent, we know $L_w(\pi') \ge L_w(\pi)$. $\triangle\triangle$

For integers w, z, let $\mho(w,z) \stackrel{\triangle}{=} \{\pi \in \mho(w) :\ \pi = (\cdot,\cdot,z)\}$.

Lemma 11 *A pair $\pi \in \mho(w,z)$, called $\mho(w,z)$-**pair**, satisfies $L_w(\pi) = \min_{\pi' \in \mho(w,z)} L_w(\pi')$ if and only if $\Im_1 \stackrel{\triangle}{=} \{(1,0,0),(-1,0,0),(0,1,0),(0,-1,0),(1,-1,0),(-1,1,0)\} \subset \Re(\pi)$.*

The proof of this lemma is very simple, we omit it here. From Lemmas 10 and 11, we see easily that

Corollary 4 *Assume $\pi \in \mho(w,z)$. Then π is a $\mho(w)$-pair if and only if π is a $\mho(w,z)$-pair and $L_w(\pi) \le \min\{L_w(\tau(w,z-1)), L_w(\tau(w,z+1))\}$, where $\tau(w,z-1)$ and $\tau(w,z+1)$ are $\mho(w,z-1)$-pair and $\mho(w,z+1)$-pair respectively.*

Let $\Im_2 \stackrel{\triangle}{=} \{(0,0,0),(-1,0,0),(0,-1,0),(1,-1,0),(-1,1,0),(-1,-1,0)\}$. For the $\mho(w,z)$-pairs, we have the following result further.

Lemma 12 *Assume $\tau(w,z)$ is a $\mho(w,z)$-pair.*
1. If $\mho(w,z+1) \ne \emptyset$, then there exists a pair π' in $\Im_2$ such that $\tau(w,z) + (0,0,1) + \pi'$ is a $\mho(w,z+1)$-pair.
2. If $\mho(w,z-1) \ne \emptyset$, then there exists a pair π'' in $\Im_2$ such that $\tau(w,z) - (0,0,1) - \pi''$ is a $\mho(w,z-1)$-pair.

The proof of this lemma is given in the appendix of this paper. If a $\mho(w,z)$-pair $\tau(w,z)$ has been generated, according to Lemma 12, we can generate a $\mho(w,z+1)$-pair $\tau(w,z+1)$ (or a $\mho(w,z-1)$-pair $\tau(w,z-1)$) with at most 20 operations of real numbers, and determine whether $L_w(\tau(w,z)) \le L_w(\tau(w,z+1))$ (or $L_w(\tau(w,z)) \le L_w(\tau(w,z-1))$) holds or not with 5 more operations of real numbers. Now we consider to propose a procedure to generate a $\mho(w,z)$-pair for given integers w, z.

For pairs $\pi \in \mho(w)$ and $\pi' \in \Upsilon_1 \cup \Upsilon_2$ with $\pi' \notin \Re(\pi)$, let $\underline{P(\pi')}$ denote the procedure: Replace π by $\pi + t'\pi'$, where $t' \stackrel{\triangle}{=} \min\{t :\ t > 0, \pi' \in \Re(\pi + t\pi')\}$. The following Procedure-E generates a $\mho(w,z)$-pair $\tau(w,z)$ from any given pair π of $\mho(w,z)$.

Procedure-E
Input: Received tuple $\boldsymbol{r}$ with (14). Integers w and z. Sequences p_i, $i = 1, 2, \ldots, 8$. Pair $\pi \in \mho(w,z)$ and the 2^4-tuple $\boldsymbol{q}_w(\pi)$. Sets $\mathcal{D}_\alpha$, $\alpha \in E_\ell$.
Output: Pair $\tau(w,z)$.
Step 0.1:
If $(1,0,0) \notin \Re(\pi)$, do $P(1,0,0)$ and goto Step 0.2.
Else, if $(-1,0,0) \notin \Re(\pi)$, do $P(-1,0,0)$ and goto Step 0.2.
Else, goto Step 0.2.
Step 0.2:
If $(0,1,0) \notin \Re(\pi)$, let $\wp = 1$ and do $P(0,1,0)$ and goto Step 1.1.
Else, if $(0,-1,0) \notin \Re(\pi)$, let $\wp = -1$ and do $P(0,-1,0)$ and goto Step 1.3.
Else, let $\wp = 0$ and goto Step 2.
Step 1.1:
If $(-1,0,0) \notin \Re(\pi)$, do $P(-1,0,0)$ and goto Step 1.2. Else, goto Step 2.
Step 1.2:
If $(0,1,0) \notin \Re(\pi)$, do $P(0,1,0)$ and goto Step 1.1. Else, goto Step 2.
Step 1.3:
If $(1,0,0) \notin \Re(\pi)$, do $P(1,0,0)$ and goto Step 1.4. Else, goto Step 2.
Step 1.4:
If $(0,-1,0) \notin \Re(\pi)$, do $P(0,-1,0)$ and goto Step 1.3. Else, goto Step 2.

Step 2:

If $\wp \geq 0$ and $(-1,1,0) \notin \Re(\pi)$, do $P(-1,1,0)$. Output π and END.

Else, if $\wp \leq 0$ and $(1,-1,0) \notin \Re(\pi)$, do $P(1,-1,0)$. Output π and END.

Else, output π and END. $\triangle\triangle$

Procedure-E says that from a pair π of $\mho(w,z)$ we can get a $\mho(w,z)$-pair $\tau(w,z)$ through one of the 4 routes showed in Figure 1.

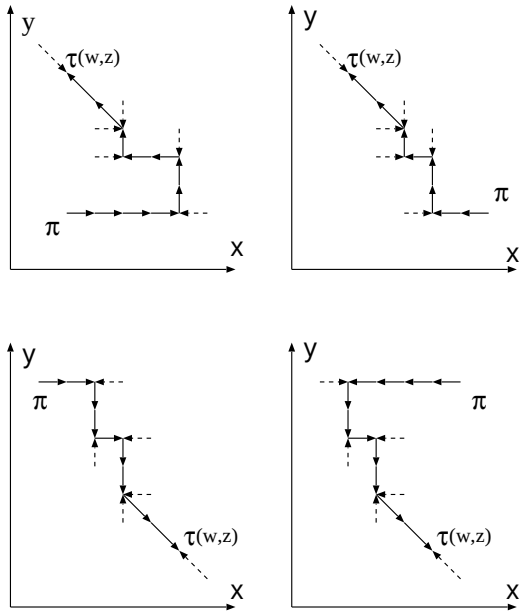

Figure 1 (pairs visited by Procedure-E)

Lemma 13 *The output $\tau(w,z)$ of the above procedure is a $\mho(w,z)$-pair.*

Proof: For clarify, we denote the input pair π of Step 2 by $\pi_{\rm in}$. It is easy to see that $\{(1,0,0), (0,1,0), (-1,0,0), (0,-1,0)\} \subset \Re(\pi_{\rm in})$, and either $(-1,1,0) \in \Re(\pi_{\rm in})$ or $(1,-1,0) \in \Re(\pi_{\rm in})$ holds. Let $\pi_1 = (0,1,0)$, $\pi_1' = (1,0,0)$, $\pi_2 = (-1,0,0)$, $\pi_2' = (0,-1,0)$, $\pi_3 = (0,-1,0)$, $\pi_3' = (-1,0,0)$, $\pi_4 = (1,0,0)$, $\pi_4' = (0,1,0)$. If $\pi_{\rm in}$ is the output of Step 1.i, then $\pi_{\rm in} - \pi_i$ is also visited by Procedure-E, and $\pi_i' \in \Re(\pi_{\rm in} - \pi_i)$, and thus $L_w(\pi_{\rm in} - \pi_i + \pi_i') \geq L_w(\pi_{\rm in} - \pi_i) \geq L_w(\pi_{\rm in})$. Hence, we see $(1,-1,0) \in \Re(\pi_{\rm in})$ if $\pi_{\rm in}$ is the output of Step 1.1 or Step 1.2, and $(-1,1,0) \in \Re(\pi_{\rm in})$ if $\pi_{\rm in}$ is the output of Step 1.3 or Step 1.4. We assume, without loss of generality, that $\Upsilon_0 \stackrel{\triangle}{=} \{(1,0,0), (0,1,0), (-1,0,0), (0,-1,0), (-1,1,0)\} \subset \Re(\pi_{\rm in})$ and $(1,-1,0) \notin \Re(\pi_{\rm in})$.

Now, we conclude that $\Upsilon_0 \subset \Re(\pi_{\rm in} + (1,-1,0))$. Indeed, by $L_w(\pi_{\rm in} + (1,-1,0)) < L_w(\pi_{\rm in}) \leq \min\{L_w(\pi_{\rm in} + (0,-1,0)), L_w(\pi_{\rm in} + (1,0,0))\}$, we know $\{(-1,1,0), (-1,0,0), (0,1,0)\} \subset \Re(\pi_{\rm in} + (1,-1,0))$. On the other hand, since $\{(1,0,0), (0,-1,0)\} \subset \Re(\pi_{\rm in}) \cap \Upsilon(1,-1,0)$, we have $\{(1,0,0), (0,-1,0)\} \subset \Re(\pi_{\rm in} + (1,-1,0))$.

Thus, by inductive method, we know $\Upsilon_0 \subset \Re(\pi_{\rm in} + k(1,-1,0))$ for $k \geq 1$, and furthermore we have $\Upsilon_0 \subset \Re(\tau(w,z))$ for the output $\tau(w,z)$ of the procedure. Clearly, $(1,-1,0) \subset \Re(\tau(w,z))$ aslo holds. Hence $\tau(w,z)$ is a $\mho(w,z)$-pair by Lemma 11. $\triangle\triangle$

Now we consider the condition for $\mho(w,z) \neq \emptyset$. Let

$$x_{w,z}^l \stackrel{\triangle}{=} \max\{0,\ \delta_e^{\rm E} - n_{p_2},\ w - z\}, \tag{63}$$

$$x_{w,z}^r \stackrel{\triangle}{=} \min\{\delta_e^{\rm E},\ n_{p_3} + w - z\}, \tag{64}$$

$$y_{w,z}^l \stackrel{\triangle}{=} \max\{0,\ \delta_f^{\rm E} - n_{p_4},\ w - z\}, \tag{65}$$

$$y_{w,z}^r \stackrel{\triangle}{=} \min\{\delta_f^{\rm E},\ n_{p_1} + w - z\}, \tag{66}$$

$$k_{w,z}^l \stackrel{\triangle}{=} \max\{2w - z - n_{p_7},\ w\}, \tag{67}$$

$$k_{w,z}^r \stackrel{\triangle}{=} \min\{n_{p_5} + w,\ 2w - z\}. \tag{68}$$

If $\mho(w,z) \neq \emptyset$, then from (51)-(60) we see that a pair (x,y,z) belongs to $\mho(w,z)$ if and only if

$$x_{w,z}^l \leq x \leq x_{w,z}^r,\ y_{w,z}^l \leq y \leq y_{w,z}^r, \tag{69}$$

$$k_{w,z}^l \leq x + y \leq k_{w,z}^r. \tag{70}$$

Hence, $\mho(w,z) \neq \emptyset$ if and only if w and z satisfy (55), (58) and

$$x_{w,z}^l \leq x_{w,z}^r,\ y_{w,z}^l \leq y_{w,z}^r,\ k_{w,z}^l \leq k_{w,z}^r, \tag{71}$$

$$x_{w,z}^l + y_{w,z}^l \leq k_{w,z}^r,\ x_{w,z}^r + y_{w,z}^r \geq k_{w,z}^l. \tag{72}$$

Furthermore, if we write

$$\begin{aligned} z^r(w) \stackrel{\triangle}{=} \min\{&\delta_g^{\rm E}, \delta_e^{\rm E} + n_{p_1}, \delta_f^{\rm E} + n_{p_3}, n_{p_1} + n_{p_3} + n_{p_7}, \\ &w, w - \delta_e^{\rm E} + n_{p_2} + n_{p_3}, w - \delta_f^{\rm E} + n_{p_4} + n_{p_1}, \\ &\lfloor \frac{w + n_{p_1} + n_{p_3}}{2} \rfloor, 2w - \delta_e^{\rm E} - \delta_f^{\rm E} + n_{p_2} + n_{p_4}\}, \end{aligned} \tag{73}$$

$$\begin{aligned} z^l(w) \stackrel{\triangle}{=} \max\{&0, \delta_g^{\rm E} - n_{p_6}, \delta_e^{\rm E} - n_{p_2} - n_{p_5}, \\ &\delta_f^{\rm E} - n_{p_4} - n_{p_5}, w - n_{p_5} - n_{p_7}, w - \delta_e^{\rm E}, \\ &w - \delta_f^{\rm E}, \lceil \frac{w - n_{p_5}}{2} \rceil, 2w - \delta_e^{\rm E} - \delta_f^{\rm E} - n_{p_7}\}. \end{aligned} \tag{74}$$

Then we see that $\mho(w,z) \neq \emptyset$ if and only if $z^l(w) \leq z \leq z^r(w)$ and $\max\{0, \delta^{\rm E} - n_{p_8}, \delta_e^{\rm E} - n_{p_2}, \delta_f^{\rm E} - n_{p_4}, \delta_e^{\rm E} + \delta_f^{\rm E} - n_{p_2} - n_{p_4} - n_{p_5}\} \leq w \leq \min\{\delta^{\rm E}, \delta_e^{\rm E} + \delta_f^{\rm E}, \delta_e^{\rm E} + n_{p_1} + n_{p_7}, \delta_f^{\rm E} + n_{p_3} + n_{p_7}\}$. Now we write

$$\begin{aligned} w^r \stackrel{\triangle}{=} \min\{&\delta^{\rm E},\ n_{p_1} + n_{p_3} + n_{p_5} + 2n_{p_7},\ 2\delta_e^{\rm E} + n_{p_1}, \\ &2\delta_f^{\rm E} + n_{p_3},\ 2\delta_g^{\rm E} + n_{p_5},\ \delta_f^{\rm E} + \delta_g^{\rm E},\ \delta_e^{\rm E} + \delta_g^{\rm E}, \\ &\delta_e^{\rm E} + \delta_f^{\rm E},\ \delta_e^{\rm E} + n_{p_1} + n_{p_7},\ \delta_f^{\rm E} + n_{p_3} + n_{p_7}, \\ &\delta_g^{\rm E} + n_{p_5} + n_{p_7},\ \lfloor \frac{\delta_e^{\rm E} + \delta_f^{\rm E} + \delta_g^{\rm E} + n_{p_7}}{2} \rfloor\}, \end{aligned} \tag{75}$$

$$\begin{aligned} w^l \stackrel{\triangle}{=} \max\{&0,\ \lceil \frac{\delta_e^{\rm E} + \delta_f^{\rm E} + \delta_g^{\rm E} - n_{p_2} - n_{p_4} - n_{p_6}}{2} \rceil, \\ &\delta^{\rm E} - n_{p_8},\ \delta_e^{\rm E} - n_{p_2},\ \delta_f^{\rm E} - n_{p_4},\ \delta_g^{\rm E} - n_{p_6}, \\ &2\delta_e^{\rm E} - 2n_{p_2} - n_{p_3} - n_{p_5}, \delta_f^{\rm E} + \delta_g^{\rm E} - n_{p_1} - n_{p_4} - n_{p_6}, \\ &2\delta_f^{\rm E} - 2n_{p_4} - n_{p_1} - n_{p_5}, \delta_e^{\rm E} + \delta_g^{\rm E} - n_{p_3} - n_{p_2} - n_{p_6}, \\ &2\delta_g^{\rm E} - 2n_{p_6} - n_{p_1} - n_{p_3}, \delta_e^{\rm E} + \delta_f^{\rm E} - n_{p_5} - n_{p_2} - n_{p_4}\}. \end{aligned} \tag{76}$$

It is not difficult to show that $\mho(w) \neq \emptyset$ if and only if $w^l \leq w \leq w^r$ and

$$0 \leq \delta_e^{\mathrm{E}} \leq n_{p_7} + n_{p_3} + n_{p_5} + n_{p_2}, \quad (77)$$

$$0 \leq \delta_f^{\mathrm{E}} \leq n_{p_7} + n_{p_1} + n_{p_5} + n_{p_4}, \quad (78)$$

$$0 \leq \delta_g^{\mathrm{E}} \leq n_{p_7} + n_{p_1} + n_{p_3} + n_{p_6}, \quad (79)$$

$$\max\{\delta_e^{\mathrm{E}} - n_{p_2},\ \delta_f^{\mathrm{E}} - n_{p_4},\ \delta_g^{\mathrm{E}} - n_{p_6}\} \leq \min\{\delta_e^{\mathrm{E}} + n_{p_1},\ \delta_f^{\mathrm{E}} + n_{p_3},\ \delta_g^{\mathrm{E}} + n_{p_5}\}. \quad (80)$$

On the other hand, if $\mho(w,z) \neq \emptyset$ and let

$$\sigma_{w,z} \stackrel{\triangle}{=} \max\{k_{w,z}^l, x_{w,z}^l + y_{w,z}^l\}, \quad (81)$$

then we can show easily that $\mho(w,z)$ contains two of the following four pairs.

$$(x_{w,z}^l,\ \sigma_{w,z} - x_{w,z}^l,\ z),\ (x_{w,z}^r,\ \sigma_{w,z} - x_{w,z}^r,\ z), \quad (82)$$

$$(\sigma_{w,z} - y_{w,z}^l,\ y_{w,z}^l,\ z),\ (\sigma_{w,z} - y_{w,z}^r,\ y_{w,z}^r,\ z). \quad (83)$$

Now we can give the following Sub-algorithm_E_ℓ for computing L_E_ℓ.

Sub-algorithm_E_ℓ
Input: Received tuple $\boldsymbol{r}$ with (14). Integers ℓ with $1 \leq \ell \leq 4$ and δ_i, $i = 1,2,3,4$, and n_α, $\alpha \in E_\ell$. Sets $\mathcal{D}_\alpha$, $\alpha \in E_\ell$.
Output: L_E_ℓ.
1. By Corollary 3, define e, f, g, p_j, $1 \leq j \leq 8$, compute δ_j^{E}, $j = e, f, g$, and δ^{E}. Then use (75) and (76) to compute w^r and w^l.
2. If one of (77)-(80) or $w^l \leq w^r$ is not valid, then output $+\infty$ (i.e. $Q(E_\ell) = \emptyset$), otherwise, for each integer w with $w^l \leq w \leq w^r$, by (73), (74) compute $z^r(w)$, $z^l(w)$ and let $z_w \stackrel{\triangle}{=} \lfloor (z^l(w) + z^r(w))/2 \rfloor$. According to (63)-(70) and (81)-(83), select a pair π in $\mho(w, z_w)$ and use the Procedure-E to generate a $\mho(w, z_w)$-pair $\tau(w,z)$. Then according to Lemma 12 and Corollary 4 to find a $\mho(w)$-pair $\tau(w)$ and compute $L_w(\tau(w))$ further.
3. Output $\min_{w^l \leq w \leq w^r} L_w(\tau(w))$. $\triangle\triangle$

About the complexity of this sub-algorithm, only the Procedure-E's is remained. Since $z \leq w$ if $\mho(w,z) \neq \emptyset$, according to symmetry of x, y, z we see the pairs (x,y,z) in $\mho(w,z)$ must satisfy $x \leq w$ and $y \leq w$ too. Hence we have

$$\mho(w, z_w) \subset \{(x, y, z_w) : w - z_w \leq x \leq w, \\ w - z_w \leq y \leq w, w \leq x + y \leq 2w - z_w\}.$$

With respect to Figure 1, we see that Procedure-E visits at most $4w$ pairs of $\mho(w, z_w)$, and the number of operations of real numbers is not more than $16w$. From the output $\tau(w, z_w)$ of Procedure-E to find a $\mho(w)$-pair $\tau(w)$, it need at most $25\lfloor w/2 \rfloor$ operations of real numbers. The number of operations of real numbers for computing $L_w(\tau(w))$ is $\delta^{\mathrm{E}} + \delta_e^{\mathrm{E}} + \delta_f^{\mathrm{E}} + \delta_g^{\mathrm{E}} - 2w - 1$. Thus, by $w^r \leq \delta^{\mathrm{E}}$ we know Sub-algorithm_E_ℓ needs at most $\sum_{w=w^l}^{w^r} (25\lfloor w/2 \rfloor + 14w + \delta^{\mathrm{E}} + \delta_e^{\mathrm{E}} + \delta_f^{\mathrm{E}} + \delta_g^{\mathrm{E}}) \leq 63\delta_1^2 + 19\delta_1$ operations of real numbers.

4.4 Main algorithm for computing the testing condition

In the end of this paper, we present an algorithm for computing $\underline{L}[V_{d_1,d_2,d_3,d_4}^N(\boldsymbol{u}^1, \boldsymbol{u}^2, \boldsymbol{u}^3, \boldsymbol{u}^4)]$.

Main algorithm
Input: Hard-decision tuple $\boldsymbol{z}$. Received tuple $\boldsymbol{r}$ with (14). Reference codewords $\boldsymbol{u}^1$,$\boldsymbol{u}^2$,$\boldsymbol{u}^3$,$\boldsymbol{u}^4$. Radiuses d_1, d_2, d_3, d_4.
Output: $\underline{L}[V_{d_1,d_2,d_3,d_4}^N(\boldsymbol{u}^1, \boldsymbol{u}^2, \boldsymbol{u}^3, \boldsymbol{u}^4)]$.
1. Compute $n(\boldsymbol{u}^1)$,$n(\boldsymbol{u}^2)$,$n(\boldsymbol{u}^3)$,$n(\boldsymbol{u}^4)$ by (2) and (8), compute $\delta_1, \delta_2, \delta_3, \delta_4$ by (11). And then re-order the tuple $\delta = (\delta_1, \delta_2, \delta_3, \delta_4)$ such that $\delta_1 \geq \delta_2 \geq \delta_3 \geq \delta_4$.
2. If $\delta_1 \leq 0$, then output 0 and END. Otherwise, reorder the order of the reference codewords $\boldsymbol{u}^1$,$\boldsymbol{u}^2$,$\boldsymbol{u}^3$,$\boldsymbol{u}^4$ according to 1.
3. Generate the sets $\mathcal{D}_\alpha$ by (2), (3) and (6), and compute n_α by (6) for all sequences $\alpha \in B^4$.
4. Generate the 4-tuples $\rho(D_1)$ and $\rho(E_1)$ by the definitions, and then generate the set $\aleph^*$ by Theorem 2.
5. Compute L_C_1 by Sub-algorithm_C_1. For all $M(0)$-sets Ξ in $\aleph^*$, compute L_Ξ by Sub-algorithm_Ξ.
6. Output $\min_{\Xi \in \{C_1\} \cup \aleph^*} L\_\Xi$ and END. $\triangle\triangle$

Since for all of sub-algorithms the numbers of additions and comparisons of real numbers are of order $(\max_{j=1}^4\{\delta_j\})^2$, we can see easily that the numbers of additions and comparisons of real numbers of our Main Algorithm is of N^2. Comparing to the computational complexity of generating the next candidate codeword in the iterative decoding processes of the iterative soft-decion decoding algorithms, we can see the case $h = 4$ of the sufficient testing condition is still very effective. If there are more than 4 candidate codewords have been generated, we can also select some combinations of them to generate a number of testing conditions, so as to provides a faster termination for the iterative soft-decion decoding algorithms.

References

[1] G.D.Forney,Jr., Generalized Minimum Distance Decoding, *IEEE Trans.Inform.Theory*, Vol.IT-12, April 1966, 125-131.

[2] D.Chase, A New Class for Decoding Block Codes with Channel Measurement Information, *IEEE Trans.Inform.Theory*, Vol.IT-18, Jan. 1972, 170-182.

[3] H.Tanaka and K.Kakigahara, Simplified Correlation Decoding by Selecting Possible Codewords Using Erasure Information, *IEEE Trans.Inform. Theory*, Vol.IT-29, Sept. 1983, 743-748.

[4] D.J.Taipale and M.B.Pursley, An Improvement to Generalized Minimum-Distance Decoding, *IEEE Trans.Inform.Theory*, Vol.IT-37, Jan. 1991, 167-172.

[5] T.Kaneko,T.Nishijima,H.Inazumi & S.Hirasawa, An Efficient Maximum-Likelihood-Decoding Algorithm for Linear Block Codes with Algebraic Decoder, *IEEE Trans. Inform. Theory*, Vol.IT-40, March 1994, 320-327.

[6] S.Lin, H.T.Moorthy and T.Kasami, An Efficient Soft-Decision Decoding Scheme for Binary Linear Block Codes, *Proc. of the 3rd International Symposiym on Communication Theory & Applications*, Charlotte Mason College, Ambleside, Lake District, UK, July 1995, 4-11.

[7] T.Koumoto, T.Takata, T.Kasami and S.Lin, An Iterative Soft-Decision Decoding Algorithm, *Proc. of International Symp. on Information Theory and Its Applications*, Canada, Sept. 1996, 806-810.

[8] T.Kasami, T.Takata, T.Koumoto, T.Fujiwara, H.Yamamoto & S.Lin, The Least Stringent Sufficient Condition on Optimality of Suboptimal Decoded Codewords, *IT94-82,* Technical Report of IEICE, Japan, Jan. 1995.

[9] T.Kasami, T.Koumoto, T.Takata & S.Lin, The Effectiveness of the Least Stringent Sufficient Condition on Optimality of Decoded Codewords, *Proc. 3rd Intern. Symp. Commun. Theory & Appl.*, July 1995, 324-333, Ambleside, UK.

[10] T.Koumoto, T.Takata, T.Kasami and S.Lin, Sufficient Conditions on the Optimality of a Decoded Codeword, (*to appear*).

[11] Tang Yuansheng & Tadao Kasami, On a testing condition on the optimality of a decoded codeword of binary block codes, *Proc.of the 20th Symposium on Information Theorem and its Applications*, Matsuyama, Japan, pp.321-324, Dec. 1997.

Appendix

Proof of Lemma 7: Assume $\boldsymbol{q}^{d,k+1}$ is a $R_{d,k+1}$-tuple. For $j = k, k+1$ and any sequence $\alpha \in B^4$, we write

$$l_\alpha^{d,j} \triangleq l(\mathcal{D}_\alpha^{(\boldsymbol{q}_\alpha^{d,j})}),\ s_\alpha^{d,j} \triangleq s(\mathcal{D}_\alpha \backslash \mathcal{D}_\alpha^{(\boldsymbol{q}_\alpha^{d,j})}). \tag{84}$$

Instead of proving this lemma directly, we will prove that there is a pair (α, β), called **ζ-pair** for convenience, with $\alpha \in \{0000, 0010, 0100, 0110\}$ and $\beta \in \{0001, 0011, 0101, 0111\}$ such that

$$\boldsymbol{q}_\alpha^{d,k+1} > \boldsymbol{q}_\alpha^{d,k},\ \boldsymbol{q}_\beta^{d,k+1} < \boldsymbol{q}_\beta^{d,k}, \tag{85}$$

and the 2^4-tuples $\boldsymbol{q}$ and $\boldsymbol{q}'$ with

$$\begin{cases} \boldsymbol{q}_\alpha = \boldsymbol{q}_\alpha^{d,k} + 1, \quad \boldsymbol{q}_\beta = \boldsymbol{q}_\beta^{d,k} - 1, \\ \boldsymbol{q}_{\alpha'} = \boldsymbol{q}_{\alpha'}^{d,k}, \text{ for all } \alpha' \in B^4 \backslash \{\alpha, \beta\}, \end{cases} \tag{86}$$

$$\begin{cases} \boldsymbol{q}'_\alpha = \boldsymbol{q}_\alpha^{d,k+1} - 1, \quad \boldsymbol{q}'_\beta = \boldsymbol{q}_\beta^{d,k+1} + 1, \\ \boldsymbol{q}'_{\alpha'} = \boldsymbol{q}_{\alpha'}^{d,k+1}, \text{ for all } \alpha' \in B^4 \backslash \{\alpha, \beta\}, \end{cases} \tag{87}$$

belong to $R_{d,k+1}$ and $R_{d,k}$, respectively.

Indeed, if (α, β) is a ζ-pair, then we have

$$l_\alpha^{d,k+1} \geq s_\alpha^{d,k},\ s_\beta^{d,k+1} \leq l_\beta^{d,k}. \tag{88}$$

Thus for the 2^4-tuples $\boldsymbol{q}$ and $\boldsymbol{q}'$ defined by (86) and (87), we see

$$\begin{aligned} L(\boldsymbol{q}^{d,k+1}) &= L(\boldsymbol{q}') + |\boldsymbol{r}_{l_\alpha^{d,k+1}}| - |\boldsymbol{r}_{s_\beta^{d,k+1}}| \\ &\geq L(\boldsymbol{q}^{d,k}) + |\boldsymbol{r}_{s_\alpha^{d,k}}| - |\boldsymbol{r}_{l_\beta^{d,k}}| = L(\boldsymbol{q}). \end{aligned} \tag{89}$$

By $\boldsymbol{q} \in R_{d,k+1}$ and the definition of $\boldsymbol{q}^{d,k+1}$, we know $\boldsymbol{q}$ is a $R^{d,k+1}$-tuple too, and the lemma follows.

If $\boldsymbol{q}_{0000}^{d,k+1} > \boldsymbol{q}_{0000}^{d,k}$, then $\boldsymbol{q}_{0001}^{d,k+1} < \boldsymbol{q}_{0001}^{d,k}$. Let $\alpha = 0000$ and $\beta = 0001$. We can see easily that (α, β) is a ζ-pair. Below we assume that $\boldsymbol{q}_{0000}^{d,k+1} \leq \boldsymbol{q}_{0000}^{d,k}$ and, consequently, $\boldsymbol{q}_{0001}^{d,k+1} \geq \boldsymbol{q}_{0001}^{d,k}$. By (43), we can see easily that $\boldsymbol{q}_{\alpha'}^{d,k+1} > \boldsymbol{q}_{\alpha'}^{d,k}$ for at least one sequence $\alpha' \in \{0010, 0100, 0110\}$ and $\boldsymbol{q}_{\alpha''}^{d,k+1} < \boldsymbol{q}_{\alpha''}^{d,k}$ for at least one sequence $\alpha'' \in \{0011, 0101, 0111\}$.

For $j = k, k+1$, let

$$\eta_j \triangleq \begin{cases} 0, \text{ if } \boldsymbol{q}_{0010}^{d,j} + \boldsymbol{q}_{0011}^{d,j} = \delta_2^{\mathrm{C}} - d, \\ 1, \text{ if } \boldsymbol{q}_{0010}^{d,j} + \boldsymbol{q}_{0011}^{d,j} > \delta_2^{\mathrm{C}} - d, \end{cases} \tag{90}$$

$$\eta'_j \triangleq \begin{cases} 0, \text{ if } \boldsymbol{q}_{0100}^{d,j} + \boldsymbol{q}_{0101}^{d,j} = \delta_3^{\mathrm{C}} - d, \\ 1, \text{ if } \boldsymbol{q}_{0100}^{d,j} + \boldsymbol{q}_{0101}^{d,j} > \delta_3^{\mathrm{C}} - d. \end{cases} \tag{91}$$

Without loss of generality, we suppose $\eta_k \leq \eta'_k$. We will divide our discussion into 12 cases according to the values of η_k, η'_k, η_{k+1} and η_{k+1}, and show that there exists a ζ-pair (α, β) for each case.

Case 1: Assume $(\eta_k, \eta'_k, \eta_{k+1}, \eta'_{k+1}) = (1, 1, 1, 1)$. Then there is a pair (α, β) with $\alpha \in \{0010, 0100, 0110\}$ and $\beta \in \{0011, 0101, 0111\}$ which satisfies (85). We see easily that (α, β) is a ζ-pair.

Case 2: Assume $(\eta_k, \eta'_k, \eta_{k+1}, \eta'_{k+1}) = (1, 1, 0, 1)$.

Subcase 2.1: Assume $\boldsymbol{q}_{0010}^{d,k+1} > \boldsymbol{q}_{0010}^{d,k}$. Then $\boldsymbol{q}_{0011}^{d,k+1} < \boldsymbol{q}_{0011}^{d,k}$. Let $\alpha = 0010$ and $\beta = 0011$. We see easily that (α, β) is a ζ-pair.

Subcase 2.2: Assume $\boldsymbol{q}_{0010}^{d,k+1} \leq \boldsymbol{q}_{0010}^{d,k}$. Then (85) must hold for some pair (α, β) with $\alpha \in \{0100, 0110\}$ and $\beta \in \{0011, 0101, 0111\}$. We see easily that (α, β) is a ζ-pair.

Case 3: Assume $(\eta_k, \eta'_k, \eta_{k+1}, \eta'_{k+1}) = (1, 1, 1, 0)$. Similar to the case 2, we can show that there is a ζ-pair (α, β).

Case 4: Assume $(\eta_k, \eta'_k, \eta_{k+1}, \eta'_{k+1}) = (1, 1, 0, 0)$.

Subcase 4.1=subcase 2.1.

Subcase 4.2: Assume $\boldsymbol{q}_{0100}^{d,k+1} > \boldsymbol{q}_{0100}^{d,k}$. Clearly, $\boldsymbol{q}_{0101}^{d,k+1} < \boldsymbol{q}_{0101}^{d,k}$. Let $\alpha = 0100$ and $\beta = 0101$. We see easily that (α, β) is a ζ-pair.

Subcase 4.3: Assume $\boldsymbol{q}_{0010}^{d,k+1} \leq \boldsymbol{q}_{0010}^{d,k}$ and $\boldsymbol{q}_{0100}^{d,k+1} \leq \boldsymbol{q}_{0100}^{d,k}$. Then (85) must hold for some pair (α, β) with $\alpha = 0110$ and $\beta \in \{0011, 0101, 0111\}$. We see easily

that (α,β) is a ζ-pair.

Case 5: Assume $(\eta_k,\eta'_k,\eta_{k+1},\eta'_{k+1})=(0,1,1,1)$.

Subcase 5.1: Assume $\boldsymbol{q}^{d,k+1}_{0011} < \boldsymbol{q}^{d,k}_{0011}$. Clearly, $\boldsymbol{q}^{d,k+1}_{0010} > \boldsymbol{q}^{d,k}_{0010}$. Let $\alpha=0010$ and $\beta=0011$. We see easily that (α,β) is a ζ-pair.

Subcase 5.2: Assume $\boldsymbol{q}^{d,k+1}_{0011} \geq \boldsymbol{q}^{d,k}_{0011}$. Then (85) must hold for some pair (α,β) with $\alpha \in \{0010,0100,0110\}$ and $\beta\in\{0101,0111\}$. We see easily that (α,β) is a ζ-pair.

Case 6: Assume $(\eta_k,\eta'_k,\eta_{k+1},\eta'_{k+1})=(0,1,0,1)$.

Subcase 6.1: Assume $\boldsymbol{q}^{d,k+1}_{0010} > \boldsymbol{q}^{d,k}_{0010}$ or $\boldsymbol{q}^{d,k+1}_{0011} < \boldsymbol{q}^{d,k}_{0011}$. Then $\boldsymbol{q}^{d,k+1}_{0010} > \boldsymbol{q}^{d,k}_{0010}$ and $\boldsymbol{q}^{d,k+1}_{0011} < \boldsymbol{q}^{d,k}_{0011}$. Let $\alpha=0010$ and $\beta=0011$. We see easily that (α,β) is a ζ-pair.

Subcase 6.2: Assume $\boldsymbol{q}^{d,k+1}_{0010} \leq \boldsymbol{q}^{d,k}_{0010}$ and $\boldsymbol{q}^{d,k+1}_{0011} \geq \boldsymbol{q}^{d,k}_{0011}$. Then (85) must hold for some pair (α,β) with $\alpha\in\{0100,0110\}$ and $\beta\in\{0101,0111\}$. We see easily that (α,β) is a ζ-pair.

Case 7: Assume $(\eta_k,\eta'_k,\eta_{k+1},\eta'_{k+1})=(0,1,1,0)$.

Subcase 7.1: Assume $\boldsymbol{q}^{d,k+1}_{0010} > \boldsymbol{q}^{d,k}_{0010}$. Then (85) must hold for some pair (α,β) with $\alpha=0010$ and $\beta\in\{0011,0101,0111\}$. We see easily that (α,β) is a ζ-pair.

Subcase 7.2=subcase 4.2.

Subcase 7.3=subcase 5.1.

Subcase 7.4: Assume $\boldsymbol{q}^{d,k+1}_{0010} \leq \boldsymbol{q}^{d,k}_{0010}$ and $\boldsymbol{q}^{d,k+1}_{0100} \leq \boldsymbol{q}^{d,k}_{0100}$ and $\boldsymbol{q}^{d,k+1}_{0011} \geq \boldsymbol{q}^{d,k}_{0011}$. Then (85) must hold for some pair (α,β) with $\alpha=0110$ and $\beta\in\{0101,0111\}$. We see easily that (α,β) is a ζ-pair.

Case 8: Assume $(\eta_k,\eta'_k,\eta_{k+1},\eta'_{k+1})=(0,1,0,0)$.

Subcase 8.1=ubcase 6.1.

Subcase 8.2=subcase 4.2.

Subcase 8.3=subcase 7.4.

Case 9: Assume $(\eta_k,\eta'_k,\eta_{k+1},\eta'_{k+1})=(0,0,1,1)$.

Subcase 9.1=subcase 5.1.

Subcase 9.2: Assume $\boldsymbol{q}^{d,k+1}_{0101} < \boldsymbol{q}^{d,k}_{0101}$. Then $\boldsymbol{q}^{d,k+1}_{0101} > \boldsymbol{q}^{d,k}_{0101}$. Let $\alpha=0100$ and $\beta=0101$. We see easily that (α,β) is a ζ-pair.

Subcase 9.3: Assume $\boldsymbol{q}^{d,k+1}_{0011} \geq \boldsymbol{q}^{d,k}_{0011}$ and $\boldsymbol{q}^{d,k+1}_{0101} \geq \boldsymbol{q}^{d,k}_{0101}$. Then (85) must hold for some pair (α,β) with $\alpha\in\{0010,0100,0110\}$ and $\beta=0111$. We see easily that (α,β) is a ζ-pair.

Case 10: Assume $(\eta_k,\eta'_k,\eta_{k+1},\eta'_{k+1})=(0,0,0,1)$.

Subcase 10.1=subcase 6.1.

Subcase 10.2=subcase 9.2.

Subcase 10.3: Assume $\boldsymbol{q}^{d,k+1}_{0010} \leq \boldsymbol{q}^{d,k}_{0010}$ and $\boldsymbol{q}^{d,k+1}_{0011} \geq \boldsymbol{q}^{d,k}_{0011}$ and $\boldsymbol{q}^{d,k+1}_{0101} \geq \boldsymbol{q}^{d,k}_{0101}$. Then (85) must hold for some pair (α,β) with $\alpha\in\{0100,0110\}$ and $\beta=0111$. We see easily that (α,β) is a ζ-pair.

Case 11: Assume $(\eta_k,\eta'_k,\eta_{k+1},\eta'_{k+1})=(0,0,1,0)$. Similar to the case 10, we can show that there is a ζ-pair (α,β).

Case 12: Assume $(\eta_k,\eta'_k,\eta_{k+1},\eta'_{k+1})=(0,0,0,0)$.

Subcase 12.1=subcase 6.1.

Subcase 12.2: Assume $\boldsymbol{q}^{d,k+1}_{0100} > \boldsymbol{q}^{d,k}_{0100}$ or $\boldsymbol{q}^{d,k+1}_{0101} < \boldsymbol{q}^{d,k}_{0101}$. Then $\boldsymbol{q}^{d,k+1}_{0100} > \boldsymbol{q}^{d,k}_{0100}$ and $\boldsymbol{q}^{d,k+1}_{0101} < \boldsymbol{q}^{d,k}_{0101}$. Let $\alpha=0100$ and $\beta=0101$. We see easily that (α,β) is a ζ-pair.

Subcase 12.3: Assume $\boldsymbol{q}^{d,k+1}_{0010} \leq \boldsymbol{q}^{d,k}_{0010}$ and $\boldsymbol{q}^{d,k+1}_{0011} \geq \boldsymbol{q}^{d,k}_{0011}$ and $\boldsymbol{q}^{d,k+1}_{0100} \leq \boldsymbol{q}^{d,k}_{0100}$ and $\boldsymbol{q}^{d,k+1}_{0101} \geq \boldsymbol{q}^{d,k}_{0101}$. Then $\boldsymbol{q}^{d,k+1}_{0110} > \boldsymbol{q}^{d,k}_{0110}$ and $\boldsymbol{q}^{d,k+1}_{0111} < \boldsymbol{q}^{d,k}_{0111}$. Let $\alpha=0110$ and $\beta=0111$. We see easily that (α,β) is a ζ-pair. $\triangle\triangle$

Proof of Lemma 12: We only prove the case 1, the case 2 can be proved by similar method. Let π_0 denote the pair in $\Im_2$ which satisfies

$$L_w(\tau(w,z)+(0,0,1)+\pi_0) = \min_{\pi\in\Im_2} L_w(\tau(w,z)+(0,0,1)+\pi). \quad (92)$$

Below we prove that $\Im_1 \subset \Re(\tau(w,z)+(0,0,1)+\pi_0)$, and thus $\tau(w,z)+(0,0,1)+\pi_0$ is a $\mho(w,z+1)$-pair by Lemma 11.

If $\pi_0=(0,0,0)$, then by (92) we know $\{(-1,0,0),(0,-1,0),(1,-1,0),(-1,1,0)\}\subset\Re(\tau(w,z)+(0,0,1))$. Since $\{(1,0,0),(0,1,0)\}\subset\Upsilon(0,0,1)\cap\Re(\tau(w,z))$, we know $\{(1,0,0),\ (0,1,0)\}\subset\Re(\tau(w,z)+(0,0,1))$ also holds, and thus $\Im_1\subset\Re(\tau(w,z)+(0,0,1))$.

If $\pi_0=(-1,0,0)$, then by (92) we know $\{(1,0,0),(0,1,0),(0,-1,0),(1,-1,0)\}\subset\Re(\tau(w,z)+(-1,0,1))$. Since $\{(-1,0,0),(-1,1,0)\}\subset\Re(\tau(w,z))\cap\Upsilon(-1,0,1)$, we know $\{(-1,0,0),(-1,1,0)\}\subset\Re(\tau(w,z)+(-1,0,1))$ also holds, and thus $\Im_1\subset\Re(\tau(w,z)+(-1,0,1))$.

If $\pi_0=(0,-1,0)$, similar to the above case, we can show $\Im_1\subset\Re(\tau(w,z)+(0,-1,1))$.

If $\pi_0=(-1,-1,0)$, then by (92) we know $\{(1,0,0),(0,1,0)\}\subset\Re(\tau(w,z)+(-1,-1,1))$. Since $\{(-1,0,0),(0,-1,0)\}\subset\Upsilon(-1,-1,1)\cap\Re(\tau(w,z))$, we know $\{(-1,0,0),(0,-1,0)\}\subset\Re(\tau(w,z)+(-1,-1,1))$ also holds. On the other hand, from $(0,-1,0)\in\Upsilon(0,-1,1)\cap\Re(\tau(w,z))$ and $(-1,0,0)\in\Upsilon(-1,0,1)\cap\Re(\tau(w,z))$, we know $(0,-1,0)\in\Re(\tau(w,z)+(0,-1,1))$ and $(-1,0,0)\in\Re(\tau(w,z)+(-1,0,1))$. Then $L_w(\tau(w,z)+(0,-2,1))\geq L_w(\tau(w,z)+(0,-1,1))\geq L_w(\tau(w,z)+(-1,-1,1))$ and $L_w(\tau(w,z)+(-2,0,1))\geq L_w(\tau(w,z)+(-1,0,1))\geq L_w(\tau(w,z)+(-1,-1,1))$, hence $\{(1,-1,0),(-1,1,0)\}\subset\Re(\tau(w,z)+(-1,-1,1))$. Thus $\Im_1\subset\Re(\tau(w,z)+(-1,-1,1))$.

If $\pi_0=(1,-1,1)$, then by (92) we know $\{(-1,0,0),\ (-1,1,0)\}\subset\Re(\tau(w,z)+(1,-1,1))$. Since $\{(1,0,0),(1,-1,0)\}\subset\Upsilon(1,-1,1)\cap\Re(\tau(w,z))$, we know $\{(1,0,0),(1,-1,0)\}\subset\Re(\tau(w,z)+(1,-1,1))$ also holds. On the other hand, from $(1,-1,0)\in\Upsilon(0,-1,1)\cap\Re(\tau(w,z))$ and $(1,0,0)\in\Upsilon(0,0,1)\cap\Re(\tau(w,z))$, we know $(1,-1,0)\in\Re(\tau(w,z)+(0,-1,1))$ and $(1,0,0)\in\Re(\tau(w,z)+(0,0,1))$. Then $L_w(\tau(w,z)+(1,-2,1))\geq L_w(\tau(w,z)+(0,-1,1))\geq L_w(\tau(w,z)+(1,-1,1))$ and $L_w(\tau(w,z)+(1,0,1))\geq L_w(\tau(w,z)+(0,0,1))\geq L_w(\tau(w,z)+(1,-1,1))$, hence $\{(0,-1,0),(0,1,0)\}\in\Re(\tau(w,z)+(1,-1,1))$. Thus $\Im_1\subset\Re(\tau(w,z)+(1,-1,1))$.

If $\pi_0=(-1,1,1)$, similar to the above case, we can get $\Im_1\subset\Re(\tau(w,z)+(-1,1,1))$. $\triangle\triangle$