RIMS-1648

Randomized Approximation for Generalized Median Stable Matching

By

Shuji KIJIMA and Toshio NEMOTO

November 2008

京都大学 数理解析研究所

RESEARCH INSTITUTE FOR MATHEMATICAL SCIENCES

KYOTO UNIVERSITY, Kyoto, Japan

Randomized Approximation for Generalized Median Stable Matching

Shuji Kijima[*] Toshio Nemoto[†]

November 11, 2008

Abstract

This paper deals with finding a *generalized median stable matching* (GMSM), introduced by Teo and Sethuraman (1998) as a fair stable marriage. Cheng (2008) showed that finding the i-th GMSM is #P-hard in case of $i = \mathrm{O}(N)$, where N is the number of stable matchings of an instance. She also gave an exact algorithm running in polynomial time in case of $i = \mathrm{O}(\log\log N)$, and the complexity remained as open in case of i is $\omega(\log\log N)$ and $\mathrm{o}(N)$.

In this paper, we establish two hardness results. We show that finding the i-th GMSM is #P-hard even when $i = \mathrm{O}(N^{1/c})$, where $c \geq 1$ is an arbitrary constant, and that deciding if a matching can be a GMSM is #P-hard. On the other hand, we give a polynomial time exact algorithm in case that i is $\mathrm{O}((\log N)^{c'})$ where c' is an arbitrary positive constant. We also propose two *randomized approximation schemes* for the i-th GMSM using an oracle for almost uniformly sampling ideals of a partially ordered set (poset). This is the first result on randomized approximation schemes for the GMSM.

Key words: stable marriage, distributive lattice, order ideals, antichains, partially ordered set, #P-hard, FPRAS.

1 Introduction

In the *stable marriage problem*, sets M of n-men and W of n-women, and lists of each person's preference over opposite sex are given as an input instance. A *matching* is n pairs of a man and a woman, in which every person appears exactly once. In a matching, a pair $m \in M$ and $w \in W$ is called *blocking pair* if m and w prefer each other to each current partner. A matching is *stable* unless a blocking pair exists.

Gale and Shaplay [6] showed that every instance of the stable marriage problem has a stable matching, and they also gave a finding algorithm. For an instance of the stable marriage problem, some stable matchings exist in general. Conway pointed out the set of all stable matchings for an instance forms a distributive lattice [13]. Furthermore, Blair [2] showed that every distributive lattice can be represented by an instance of the stable marriage problem.

Conway's note indicates another interesting property of the stable marriage, so-called the "median property" (see e.g. [23, 8, 13]). Generalizing the property, Teo and Sethuraman [23] devised an idea of the *generalized median stable matching* (*GMSM*), as a fair stable marriage. Here we briefly explain the GMSM.

Let $\mathcal{M}$ be a set of all stable matchings for an instance. Let μ_i $(1 \leq i \leq N)$ be a matching of $\mathcal{M}$ where $N \stackrel{\text{def.}}{=} |\mathcal{M}|$, and then $\mu_i(m) \in W$ denotes a partner of $m \in M$ on the matching

[*]Research Institute for Mathematical Sciences, Kyoto University, Japan kijima@kurims.kyoto-u.ac.jp
[†]Graduate School of Information and Communication, Bunkyo University, Japan

a. Preference list

Men's list

m_1	w_1	w_2	w_4	w_3	w_5
m_2	w_2	w_1	w_3	w_4	w_5
m_3	w_3	w_4	w_2	w_5	w_1
m_4	w_4	w_3	w_5	w_1	w_2
m_5	w_5	w_3	w_1	w_2	w_4

Women's list

w_1	m_2	m_1	m_3	m_4	m_5
w_2	m_3	m_1	m_2	m_4	m_5
w_3	m_5	m_4	m_3	m_2	m_1
w_4	m_1	m_3	m_4	m_5	m_2
w_5	m_4	m_5	m_1	m_2	m_3

b. Stable matchings

	μ_1	μ_2	μ_3	μ_4	μ_5	μ_6	μ_7	μ_8
m_1	1	2	1	2	1	4	2	4
m_2	2	1	2	1	2	1	1	1
m_3	3	3	4	4	4	2	4	2
m_4	4	4	3	3	5	3	5	5
m_5	5	5	5	5	3	5	3	3

arrange each row

c. GMSMs

m_1	1	1	1	2	2	2	4	4
m_2	2	2	2	1	1	1	1	1
m_3	3	3	4	4	4	4	2	2
m_4	4	4	3	3	3	5	5	5
m_5	5	5	5	5	5	3	3	3
	α_1	α_2	α_3	α_4	α_5	α_6	α_7	α_8

$\underbrace{\alpha_1\ \alpha_2}_{\mu_1}\ \underbrace{\alpha_3}_{\mu_3}\ \underbrace{\alpha_4\ \alpha_5}_{\mu_4}\ \underbrace{\alpha_6}_{\mu_7}\ \underbrace{\alpha_7\ \alpha_8}_{\mu_8}$

Figure 1: An example of GMSMs.

μ_i. Now we define $\mathcal{M}(m)$ for $m \in M$ as the multiset of all $\mu_i(m)$ $(1 \le i \le N)$. Let $\alpha(m) = (\alpha_1(m), \alpha_2(m), \ldots, \alpha_N(m))$ for $m \in M$ be an arrangement of $\mathcal{M}(m)$, in which each $\alpha(m)$ is in order of preference of each m; i.e., $\alpha_i(m) \in W$ is preferable for m or identical to $\alpha_{i+1}(m) \in W$ for all i $(1 \le i < N)$. Note that $\alpha(m)$ is independently arranged for $m \in M$ of each other. Let α_i $(1 \le i \le N)$ be a set of n pairs of $m \in M$ and $\alpha_i(m) \in W$, every α_i is again a stable matching in $\mathcal{M}$, that is shown by Teo and Sethuraman [23] using linear programming. We call α_i the i-th generalized median stable matching (or i-th GMSM, for short).

Figure 1 shows an example with five men and five women. Figure 1-a shows their preference lists; in Men's lists, women are arranged in order of each m_i's preference from left to right in each row $m_i \in M$, and men are arranged in order of each w_i's preference in Women's lists. Figure 1-b shows all stable matchings $\mu_1, \ldots, \mu_8$ of the instance. In the table, the number k denotes the index of a woman w_k where $w_k = \mu_j(m_i)$ in the i-th row of the j-th column. Thus each column $j \in \{1, \ldots, 8\}$ corresponds to a stable matching μ_j. In Figure 1-c, all partners of m_i in 8-stable matchings are arranged in the i-th row, according to the preference of each m_i; i.e., the i-th row represents $\alpha(m_i)$ (with indices k of women $w_k = \alpha_j(m_i)$). Then each column $\alpha_1, \ldots, \alpha_8$ forms a stable matching again. See [23, 3] for other properties of generalized median stable matchings.

A fairness of stable matchings between men and women is a central issue of the stable marriage problem. The median stable matching, that is the $\lceil (N+1)/2 \rceil$-th GMSM, provides a fair matching. There are a number of papers discussing on the GMSM [3, 11, 12, 14, 18, 19, 23]. Cheng [3] showed that finding the i-th GMSM exactly is #P-hard when i is $\mathrm{O}(N)$. In [3], she gave a characterization of GMSMs, which had been independently found by Nemoto [14]. By the characterization, a GMSM can be described as a *sublevel set* on the rotation poset, in which a *level set function* is defined by the number of *ideals* of the *rotation poset* (see Section 2, for detail). Cheng [3] also gave a simple exact algorithm for finding the i-th GMSM in case of $i = \mathrm{O}(\log n)$, i.e. $i = \mathrm{O}(\log \log N)$, and gave rise to an open problem of the complexity in case that i is $\mathrm{o}(N)$ and $\omega(\log \log N)$. Cheng discussed a simple approximation to the median stable matching, whose error ratio is proven only $\mathrm{O}(N)$. It remains to be seen whether the decision version of finding the i-th GMSM is in NP.

Results. We show that finding the i-th GMSM is #P-hard even when i is $\mathrm{O}(N^{1/c})$ for an arbitrary constant $c \geq 1$. We also show that even the query if a given stable matching can be a GMSM is #P-hard. On the other hand, we give a polynomial time exact algorithm for finding the i-th GMSM in any case that i is $\mathrm{O}(n^{c'})$, i.e., $\mathrm{O}((\log N)^{c'})$ where c' is an arbitrary positive constant. We propose two randomized approximation schemes for finding the i-th GMSM using an oracle for almost uniformly sampling *ideals* (or essentially equivalent to *antichains*) of a poset.

Related works. Irving and Leather [9] showed that counting stable matchings is #P-complete by a reduction from counting antichains (or ideals) of a poset whose #P-hardness is due to Provan and Ball [16]. Steiner [22] gave a polynomial time algorithm based on dynamic programming for counting ideals of a poset of some special classes such as series-parallel, bounded width, etc. Propp and Wilson [15] proposed a perfect sampler for ideals of a poset based on the monotone coupling from the past algorithm, whereas its expected running time becomes exponential in the size of the poset in the worst case. The existence of a polynomial time almost uniform sampler for ideals of a poset, or an FPRAS for counting, remains as a challenging problem [1].

Organization. In Section 2, we introduce the characterization of GMSMs on the rotation poset, due to Nemoto [14] and Cheng [3]. We give there a detailed description of the problem of concern to this paper. In Section 3, we establish two hardness results on the problems, and we give in Section 4 a polynomial time exact algorithm in case of small i. In Sections 5 and 6, we propose two randomized approximation schemes for finding the i-th GMSM.

2 Preliminaries

2.1 Definitions and notations

We denote the set of real numbers (non-negative, positive real numbers) by $\mathbb{R}$ ($\mathbb{R}_+$, $\mathbb{R}_{++}$), and the set of integers (non-negative, positive integers) by $\mathbb{Z}$ ($\mathbb{Z}_+$, $\mathbb{Z}_{++}$), respectively. Let P be a poset regarding a partial order $\preceq$. A set $X \subseteq P$ is an *ideal* of P if, whenever $x \in X$ and $y \preceq x$, we have $y \in X$. Note that $\emptyset$ is an ideal of P. We define $\mathcal{D}(P)$ as the set of all ideals of P.

For a poset P, we define a (level set) function $g : P \to \mathbb{Z}_{++}$ by

$$g(x) \stackrel{\text{def.}}{=} |\{X \in \mathcal{D}(P) \mid x \notin X\}| \qquad (x \in P). \tag{1}$$

Define a set $U(x) \subseteq P$ for $x \in P$ by

$$U(x) \stackrel{\text{def.}}{=} \{y \in P \mid y \succeq x\}, \tag{2}$$

then we have $g(x) = |\mathcal{D}(P \setminus U(x))|$. Note that $g(x)$ is monotone increasing with respect to $\prec$, that means if $x \prec y$ then $g(x) < g(y)$. Given a poset P, let $N = |\mathcal{D}(P)|$ and we define a (sublevel) set $S_i \subseteq P$ for $i \in \{1, \ldots, N\}$ by

$$S_i \stackrel{\text{def.}}{=} \{x \in P \mid g(x) < i\}. \tag{3}$$

Since $g(x)$ is monotone increasing, S_i is an ideal of P. We call S_i (the i-th) *level ideal* (or *LI*, for short). We define the family $\mathcal{F}(P) \subseteq \mathcal{D}(P)$ of (level) ideals by

$$\mathcal{F}(P) \quad \stackrel{\text{def.}}{=} \quad \{S \subseteq P \mid S = S_i \ (i \in \{1, \ldots, N\})\}. \tag{4}$$

2.2 Representation of a GMSM by a sublevel set of the rotation poset

Let $\mathcal{M}$ be a set of stable matchings for an instance of the stable marriage problem with n-men and n-women, then, it is known that the size of $\mathcal{M}$ can become exponentially large, namely 2^{n-1}. For a distributive lattice of stable matchings $\mathcal{M}$, there is a compact representation by another poset R, and the set of ideals $\mathcal{D}(R)$ and $\mathcal{M}$ are bijective[1]. The poset R is called the *rotation poset*, and each element of R corresponds to an interchange (or rotation, in general) of man-woman pairs on matchings (see [8], for detail). The rotation poset R can be obtained in $\mathrm{O}(n^2)$ time and space, and the bijection map between $\mathcal{D}(R)$ and $\mathcal{M}$ can be easily computed [8].

Nemoto [14] and Cheng [3] independently gave the following characterization of the i-th GMSM α_i by the i-the level ideal S_i of the rotation poset R.

Theorem 2.1 [3, 14] *Let $\mathcal{M}$ be a set of all stable matchings for an instance, and let R be its rotation poset. Let S_i ($1 \leq i \leq |\mathcal{M}|$) be the i-th LI of the poset R, then the stable matching corresponding to the ideal S_i is the i-th GMSM α_i of the instance.*

Additionally, we note that for any poset P, there is an instance of the stable marriage problem whose rotation poset is isomorphic to P, and it can be constructed in $\mathrm{O}(|P|^2)$ time with $\mathrm{O}(|P|^2)$ of men and women, conversely [2, 8].

2.3 Our goal

We summarize our considering problems and contributions in this paper.

Result 1. We show that the following problem,

Problem 1 *Given a poset P and an ideal $S \in \mathcal{D}(P)$, then whether or not $S \in \mathcal{F}(P)$?*

is #P-hard, thus NP-hard, by a reduction from counting ideals of a given poset P, which is known to be #P-complete [16]. This result indicates the #P-hardness of the query if a given stable matching $M \in \mathcal{M}$ can be a GMSM α_i ($1 \leq i \leq |\mathcal{M}|$), according to Section 2.2.

Result 2. We show that the following problem,

Problem 2 *Given a poset P, an ideal $S \in \mathcal{D}(P)$, and a function $f : \mathbb{Z}_{++} \to \mathbb{Z}_{++}$, then let $i = f(|\mathcal{D}(P)|)$, and whether S is the i-th LI?*

is #P-hard even when the function f satisfies $f(z) = \mathrm{O}(z^{1/c})$ ($z \in \mathbb{Z}_{++}$) where c is an arbitrary constant. This result indicates that the decision version of the i-th GMSM, if a given stable matching $M \in \mathcal{M}$ is the i-th GMSM, is #P-hard even when $i = \mathrm{O}(N^{1/c})$ where c is an arbitrary constant and $N \stackrel{\text{def.}}{=} |\mathcal{M}|$.

Result 3. We consider the following problem,

Problem 3 *Given a poset P and an integer $i \in \mathbb{Z}_{++}$, then find the i-th LI.*

We give an exact algorithm for Problem 3, which runs in time in $\mathrm{O}(i \cdot \mathrm{poly}(|P|))$. Thus the algorithm runs in time polynomial in the input size in case that i is $\mathrm{poly}(|P|)$, i.e., the case of $i = \mathrm{O}((\log N)^c)$ for an arbitrary positive constant c.

[1] See also *Birkhoff's representation theorem*, in e.g. [4].

Result 4. We propose a simple randomized approximation scheme (RAS) for Problem 2, on the assumption of an almost uniform sampler on $\mathcal{D}(P)$. Given an arbitrary ε ($0 < \varepsilon < 1$), δ ($0 < \delta < 1$), a ratio λ ($0 < \lambda < 1$), and a poset P, our RAS outputs an ideal $Z \in \mathcal{D}(P)$ which approximates $S_{\lambda N}$ with satisfying

$$\Pr\left[S_{\lfloor(\lambda-\varepsilon)N\rfloor} \subseteq Z \subseteq S_{\lceil(\lambda+\varepsilon)N\rceil}\right] \geq 1-\delta,$$

in polynomial time of sampling oracle calls and fundamental operations. This result provides that given an instance of the stable marriage and a ratio λ, we can find a stable matching $\mu \in \mathcal{M}$ which approximates the λN-th GMSM $\alpha_{\lambda N}$ satisfying

$$\Pr\left[\alpha_{\lfloor(\lambda-\varepsilon)N\rfloor} \preceq \mu \preceq \alpha_{\lceil(\lambda+\varepsilon)N\rceil}\right] \geq 1-\delta,$$

where $\preceq$ is the partial order on the distributive lattice $\mathcal{M}$ of stable matchings [13, 8].

Result 5. We propose another randomized approximation scheme for Problem 2, based on approximate counting of $\mathcal{D}(P)$. Given an arbitrary ε ($0 < \varepsilon < 1$), δ ($0 < \delta < 1$), an function[2] $f : \mathbb{Z}_{++} \to \mathbb{Z}_{++}$, and a poset P, our RAS outputs an ideal $Z \in \mathcal{D}(P)$ which approximates $S_{f(N)}$ with satisfying

$$\Pr\left[S_{\lfloor(1-\varepsilon)f(N)\rfloor} \subseteq Z \subseteq S_{\lceil(1+\varepsilon)f(N)\rceil}\right] \geq 1-\delta,$$

in polynomial time of sampling oracle calls and fundamental operations. Note that the approximation ratio depend on just $f(N)$ instead of linear of N. This result implies that given an instance of the stable marriage and $f(N)$, we can find a stable matching $\mu \in \mathcal{M}$ which approximates the $f(N)$-th GMSM $\alpha_{f(N)}$ with satisfying

$$\Pr\left[\alpha_{\lfloor(1-\varepsilon)f(N)\rfloor} \preceq \mu \preceq \alpha_{\lceil(1+\varepsilon)f(N)\rceil}\right] \geq 1-\delta,$$

where $\preceq$ is the partial order on the distributive lattice $\mathcal{M}$ of stable matchings.

3 Hardness of Finding a Level Ideal

In this section, we show the hardness of finding a level ideal. First we introduce three useful lemmas. Let P and Q be (disjoint) posets. The *disjoint union* $P \dot\cup Q$ is defined as follows; $x, y \in P \dot\cup Q$ satisfies $x \preceq y$ iff either [$x, y \in P$ and $x \preceq y$] or [$x, y \in Q$ and $x \preceq y$].

Lemma 3.1 [22] *Let P and Q be disjoint posets, then* $|\mathcal{D}(P \dot\cup Q)| = |\mathcal{D}(P)| \cdot |\mathcal{D}(Q)|$.

The *linear sum* $P \oplus Q$ is defined as follows; $x, y \in P \oplus Q$ satisfies $x \preceq y$ iff the cases of [$x, y \in P$ and $x \preceq y$], [$x, y \in Q$ and $x \preceq y$], or [$x \in P$ and $y \in Q$].

Lemma 3.2 [22, 3] *Let P and Q be disjoint posets, then* $|\mathcal{D}(P \oplus Q)| = |\mathcal{D}(P)| + |\mathcal{D}(Q)| - 1$.

Note that $P \dot\cup Q = Q \dot\cup P$, but $P \oplus Q \neq Q \oplus P$.

Lemma 3.3 [3] *For any $K \in \mathbb{Z}_{++}$, a poset Q satisfying $|\mathcal{D}(Q)| = K$ is realized in* poly$(\log K)$ *time and space.*

Now we show the following.

Theorem 3.4 *Problem 1 is #P-hard.*

[2] We naturally assume that the function is a uniform contraction mapping, e.g., $\lfloor\sqrt{z}\rfloor$, $\lceil z^{1/c}\rceil$, $\lceil\log(z)\rceil$, etc.

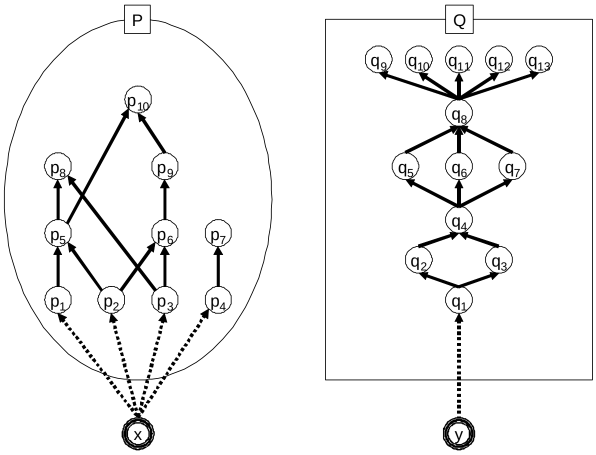

Figure 2: An example of $R \stackrel{\text{def.}}{=} (\{x\} \oplus P) \dot{\cup} (\{y\} \oplus Q)$.

Proof. We give a reduction from COUNTING IDEALS, that is to compute $|\mathcal{D}(P)|$ for a given poset P. The problem is known to be #P-complete [16]. Precisely, we consider a problem that given a poset P and an integer $K \in \mathbb{Z}_{++}$, the query is whether or not $|\mathcal{D}(P)| < K$. If we have an oracle for the query, we can compute $|\mathcal{D}(P)|$ by a binary search of Ks between 0 and $2^{|P|}$. We in the following give a reduction from the query if $|\mathcal{D}(P)| < K$ to Problem 1.

For the integer K, let Q be a poset satisfying $|\mathcal{D}(Q)| = K$. The poset Q is constructed in poly$(\log K)$ time by Lemma 3.3. Let R be a poset defined by $R \stackrel{\text{def.}}{=} (\{x\} \oplus P) \dot{\cup} (\{y\} \oplus Q)$ (see Figure 2). Now we consider $g(r)$ for each $r \in R$, defined by (1),

$$\begin{array}{rclclcll} g(x) & = & |\mathcal{D}(R \setminus U(x))| & = & |\mathcal{D}(\{y\} \oplus Q)| & = & 1 + |\mathcal{D}(Q)|, & \\ g(y) & = & |\mathcal{D}(R \setminus U(y))| & = & |\mathcal{D}(\{x\} \oplus P)| & = & 1 + |\mathcal{D}(P)|, & \\ g(p) & = & |\mathcal{D}(R \setminus U(p))| & \geq & |\mathcal{D}((\{y\} \oplus Q) \dot{\cup} \{x\})| & = & 2 \cdot g(x) & (\forall p \in P), \\ g(q) & = & |\mathcal{D}(R \setminus U(q))| & \geq & |\mathcal{D}((\{x\} \oplus P) \dot{\cup} \{y\})| & = & 2 \cdot g(y) & (\forall q \in Q), \end{array}$$

hold. With considering the definitions (3) and (4) of the set of level ideals $\mathcal{F}(R)$, we obtain the following three cases;

Case 1. If $|\mathcal{D}(P)| < |\mathcal{D}(Q)| = K$, then $\{x\} \notin \mathcal{F}(R)$ and $\{y\} \in \mathcal{F}(R)$, since $g(x) > g(y)$.
Case 2. If $|\mathcal{D}(P)| > |\mathcal{D}(Q)| = K$, then $\{x\} \in \mathcal{F}(R)$ and $\{y\} \notin \mathcal{F}(R)$, since $g(x) < g(y)$.
Case 3. Otherwise, i.e. $|\mathcal{D}(P)| = |\mathcal{D}(Q)| = K$, then $\{x\} \notin \mathcal{F}(R)$, $\{y\} \notin \mathcal{F}(R)$, and $\{x, y\} \in \mathcal{F}(R)$.
Thus, if we ask the oracle for Problem 1 whether $\{y\} \in \mathcal{F}(R)$, then 'yes' (Case 1) implies $|\mathcal{D}(P)| < K$ and 'no' (Cases 2 and 3) implies $|\mathcal{D}(P)| \geq K$. □

From Theorem 3.4, we observe that finding the i-th level ideal, that is Problem 2, is NP-hard even when $i = \mathrm{O}(\sqrt{N})$. Precisely, we obtain the following.

Proposition 3.5 *Given a poset R and an ideal $S \in \mathcal{D}(R)$, then the problem whether or not S is the $\lceil \sqrt{N} \rceil$-th LI of R is #P-hard, where $N = |\mathcal{D}(R)|$.*

Proof. We reduce COUNTING IDEALS to our problem. For a given poset P and $K \in \mathbb{Z}_{++}$, let Q and R be the posets defined in the proof of Theorem 3.4. Let $N = |\mathcal{D}(R)|$, then

$N = (|\mathcal{D}(P)|+1)(|\mathcal{D}(Q)|+1) = \mathrm{O}\left(|\mathcal{D}(P)|^2 + K^2\right)$. We define a function $f : \mathbb{Z}_{++} \to \mathbb{Z}_{++}$ by $f(z) \overset{\text{def.}}{=} \lceil \sqrt{z} \rceil$.

First we show that $\{y\}$ is the $f(N)$-th LI of R when K satisfies $|\mathcal{D}(P)| < K \leq 4|\mathcal{D}(P)|$. With considering $g(q) \geq 2g(y)$ for all $q \in Q$, $\{y\}$ is the $f(N)$-th LI if $g(y) < f(N)$, $f(N) \leq 2g(y)$, and $f(N) \leq g(x)$ hold. These conditions are transformed $|\mathcal{D}(P)|+1 < \left\lceil \sqrt{(|\mathcal{D}(P)|+1)(K+1)} \right\rceil$, $\left\lceil \sqrt{(|\mathcal{D}(P)|+1)(K+1)} \right\rceil \leq 2|\mathcal{D}(P)|+2$, and $\left\lceil \sqrt{(|\mathcal{D}(P)|+1)(K+1)} \right\rceil \leq K+1$, respectively. It is easy to see that the first and the last conditions hold when $|\mathcal{D}(P)| < K$. The second condition hold if $K \leq 4|\mathcal{D}(P)|$, since

$$\left\lceil \sqrt{(|\mathcal{D}(P)|+1)(K+1)} \right\rceil \leq \left\lceil \sqrt{(|\mathcal{D}(P)|+1)(4|\mathcal{D}(P)|+1)} \right\rceil < \left\lceil \sqrt{4(|\mathcal{D}(P)|+1)^2} \right\rceil = 2|\mathcal{D}(P)|+2.$$

Next we consider the case $K \leq |\mathcal{D}(P)|$, then the singleton $\{y\}$ is never the $f(N)$-th LI of R, since $K \leq |\mathcal{D}(P)|$ means $g(x) \leq g(y)$, and it implies that if an LI includes y, then the LI must include x from the definition. Thus, minimizing K for which $\{y\}$ is the $f(N)$-th LI of R, then the minimum K^* is equal to $|\mathcal{D}(P)|+1$.

Finally, $|\mathcal{D}(P)|$ is computed with checking if $\{y\}$ is the $f(N)$-th LIs of R for appropriate Ks, at most $2|P|$ times, as follows. We start from $K = 2^{|P|}$ and get K into halves, until $\{y\}$ is the $f(N)$-th LI. From the above discussions, we certainly obtain the case. Suppose we get the case that $\{y\}$ is the $f(N)$-th LI when $K = K_0$. In the interval $[1, K_0]$, $\{y\}$ is the $f(N)$-th LI if, and only if, $K \in (|\mathcal{D}(P)|, K_0]$. Thus we can find $K^* = |\mathcal{D}(P)|+1$ according to the binary search strategy. □

With a modification of the proof of Proposition 3.5, we establish a stronger claim that finding the i-th level ideal, that is Problem 2, is #P-hard even when $i = \mathrm{O}(N^{1/c})$ for an arbitrary constant c ($c \geq 1$). Precisely, we obtain the followings.

Theorem 3.6 *Suppose c ($c \geq 2$) is an arbitrary constant. Given a poset R and an ideal $S \in \mathcal{D}(R)$, then the problem whether or not S is the $\lceil N^{1/c} \rceil$-th LI of R is #P-hard, where $N = |\mathcal{D}(R)|$.*

Outline of proof. We reduce COUNTING IDEALS to our problem in a similar way as the proof of Proposition 3.5. For the poset P and an arbitrary constant K, we define $R' \overset{\text{def.}}{=} ((\{x\} \oplus P) \dot\cup (\{y\} \oplus Q)) \oplus Q'$, where posets Q and Q' satisfies $|\mathcal{D}(Q)| = K$ and $|\mathcal{D}(Q')| = \lfloor (K+1)^c \rfloor - (K+1)^2 + 1$, thus $|\mathcal{D}(R')| = \Theta(K^c)$. From Lemma 3.3, Q and Q' is realized in $\mathrm{poly}(\log(K^c)) = \mathrm{poly}(\log K)$ time and space. In a similar way as the proof of Proposition 3.5, we can show Theorem 3.6 (see Appendix A for the complete proof). □

In a similar way as Theorem 3.6, we can show the #P-hardness for other functions of $\Omega(N^{1/c})$ and $\mathrm{O}(N)$, with tuning some parameters (see Appendix C).

4 Exact Computation of the $\mathrm{poly}(n)$-th LI

In the previous section, we showed finding the i-th LI is #P-hard, even when $i = \mathrm{O}(N^{1/c})$ for an arbitrary constant $c \geq 1$. In this section, we give an exact algorithm for Problem 3, that is finding the i-th LI, which runs in time polynomial in $|P|$ when $i = \mathrm{O}((\log N)^c)$ for an arbitrary constant $c \geq 1$.

The algorithm is essentially based on (exhaustive) enumeration of ideals of a poset. Steiner [21] gave an enumeration algorithm for ideals of a poset, which generates all ideals one-by-one without duplication, and which runs in $\mathrm{O}(|P|^2 + |P| \cdot |\mathcal{D}(P)|)$ time; more precisely the algorithm

Exact Algorithm

Input: A poset P and an integer $i \in \mathbb{Z}_{++}$.
For(each $p \in P$){
  Set counter $Z(p) := 0$.
  Search $\mathcal{D}(P \setminus U(p))$ by an enumeration algorithm $\mathcal{A}$,
  with storing in counter $Z(p)$ the number of ideals having been found.
  if $Z(p) \geq i$ then **halt** $\mathcal{A}$.
}
Output $S := \{p \in P \mid Z(p) < i\}$, and **halt**.

Figure 3: Whole description of the exact algorithm

outputs every ideals in $\mathrm{O}(|P|)$ time delay, after $\mathrm{O}(|P|^2)$ time preprocessing. Squire [20] gave a faster algorithm running in $\mathrm{O}(\log |P| \cdot |\mathcal{D}(P)|)$ time.

Now we describe the algorithm for Problem 3. Let $\mathcal{A}$ denote an enumeration algorithm of ideals of a poset. For each $p \in P$, we execute $\mathcal{A}$ for a poset $P \setminus U(p)$, and count up the number of ideals of $\mathcal{D}(P \setminus U(p))$ one-by-one. Let $Z(p)$ denote the value of a counter, then if $Z(p)$ reached at i we halt $\mathcal{A}$, and otherwise $\mathcal{A}$ stops with $Z(p) = |\mathcal{D}(P \setminus U(p))|$. Then $S = \{p \in P \mid Z(p) < i\}$ should be the i-th LI from the definition. See Figure 3 about the whole algorithm.

Clearly the time complexity of the algorithm is $\mathrm{O}(|P| \cdot \mathcal{T}_{\mathcal{A}}(i))$, where $\mathcal{T}_{\mathcal{A}}(i)$ denotes the computation time in which enumeration algorithm outputs ideals up to i-th one, that is e.g., $\mathrm{O}(|P|^2 + |P| \cdot i)$ by Steiner [21]. Thus it becomes a polynomial time algorithm when $i = \mathrm{poly}(|P|)$. In other words, Problem 3 is solvable in time polynomial in the input size when $i = \mathrm{O}((\log N)^c)$ for an arbitrary constant $c \geq 0$, since $N = |\mathcal{D}(P)|$ is at most $2^{|P|}$.

5 Simple Randomized Approximation Algorithm

In this section, we give a simple randomized approximation algorithm for the i-th LI. Theorem 3.4 suggests that finding just a level ideal in $\mathcal{F}(P)$ of a given poset P is #P-hard. Thus, we consider to find an ideal $S \in \mathcal{D}(P)$, which approximates the i-th level ideal S_i. We use the following oracle of almost uniform sampler on $\mathcal{D}(P)$ for a given poset P.

Oracle 1 *(Almost uniform sampler on ideals of a poset.) Given an arbitrary ε ($0 < \varepsilon < 1$) and a poset P, Oracle returns an element of $\mathcal{D}(P)$ according to a distribution ν satisfying $d_{\mathrm{TV}}(\pi, \nu) \stackrel{\text{def.}}{=} (1/2)\|\pi - \nu\|_1 \leq \varepsilon$, where π denotes the exactly uniform distribution on $\mathcal{D}(P)$.*

Let γ_1 denote the time required for Oracle 1. Note that it is open whether γ_1 can be $\mathrm{poly}(|P|, -\ln \varepsilon)$. With using Oracle 1, we give the following simple randomized algorithm for Problem 2.

Algorithm 1 (ε-estimator for the λN-th LI.)

Input: A poset P, λ ($0 < \lambda < 1$), ε ($0 < \varepsilon \leq \min\{\lambda, 1 - \lambda\}$), δ ($0 < \delta < 1$).
Set $Z(p) := 0$ for each $p \in P$.
Repeat($T \stackrel{\text{def.}}{=} \lceil -12\varepsilon^{-2} \ln(\delta/|P|) \rceil$ times){
  Generate $X \in \mathcal{D}(P)$ by Oracle 1 (where ν satisfies $d_{\mathrm{TV}}(\pi, \nu) \leq \varepsilon/2$).
  For(each $p \in P$){
    if $p \notin X$ **then** $Z(p) := Z(p) + 1$.
  }
}

9 **Set** $S := \{p \in P \mid Z(p)/T < \lambda\}$.
10 **Output** S and **halt**.

Theorem 5.1 *Algorithm 1 outputs an ideal $S \in \mathcal{D}(P)$ and S satisfies*

$$\Pr\left[S_{\lfloor(\lambda-\varepsilon)N\rfloor} \subseteq S \subseteq S_{\lceil(\lambda+\varepsilon)N\rceil}\right] \geq 1-\delta, \tag{5}$$

in $\mathrm{O}((\gamma_1+|P|)\log(|P|)\,\varepsilon^{-2}\log\delta^{-1})$ *time.*

Proof. The time complexity is easy to see. First we show that the output S of Algorithm 1 is an ideal of P. Suppose a pair $p \in P$ and $q \in P$ satisfies $p \prec q$. We show that if $q \in S$ then $p \in S$. For any random sample $X \in \mathcal{D}(P)$ in Step 1, if $q \in X$ then $p \in X$, since X is an ideal of P. It implies $Z(p) \geq Z(q)$ in Step 1. Thus if $q \in S$ then $p \in S$ from the definition of S in Step 2.

Next, to show that S satisfies the inequality (5), we establish the following.
Claim. *For any $p \in P$,*
<u>*Case 1.*</u> *if $g(p) \leq (\lambda-\varepsilon)N$, then the probability $p \notin S$ (i.e., $Z(p)/T \geq \lambda$) is at most $\delta/|P|$, and*
<u>*Case 2.*</u> *if $g(p) \geq (\lambda+\varepsilon)N$, then the probability $p \in S$ (i.e., $Z(p)/T < \lambda$) is at most $\delta/|P|$.*
We define $\omega_p \stackrel{\text{def.}}{=} g(p)/N$ for $p \in P$. Let $\widehat{\omega}_p$ be an estimator of ω_p by the distribution ν, that is formally defined by

$$\widehat{\omega}_p \stackrel{\text{def.}}{=} \sum_{X \in \mathcal{D}(P)\,|\,p \notin X} \nu(X).$$

In Case 1, $p \in P$ satisfies $g(p)/N \leq \lambda-\varepsilon$, then $\omega_p+\varepsilon \leq \lambda$ holds. Now, with considering that the distribution ν satisfies $d_{\mathrm{TV}}(\pi,\nu) \leq \varepsilon/2$, we have $\widehat{\omega}_p \leq \omega_p+\varepsilon/2$, that implies $\widehat{\omega}_p+\varepsilon/2 \leq \omega_p+\varepsilon$. Thus we obtain $\widehat{\omega}_p+\varepsilon/2 \leq \lambda$. Then the probability $Z(p)/T \geq \lambda$ satisfies that

$$\Pr\left[Z(p) \geq \lambda T\right] \;\leq\; \Pr\left[Z(p) \geq \left(\widehat{\omega}_p+\frac{\varepsilon}{2}\right)T\right] \;=\; \Pr\left[Z(p) \geq \left(1+\frac{\varepsilon}{2\widehat{\omega}_p}\right)\widehat{\omega}_p \cdot T\right].$$

By using the Chernoff's bound,

$$\Pr\left[Z(p) \geq \left(1+\frac{\varepsilon}{2\widehat{\omega}_p}\right)\widehat{\omega}_p \cdot T\right] \;\leq\; \mathrm{e}^{-\frac{1}{3}\widehat{\omega}_p T\left(\frac{\varepsilon}{2\widehat{\omega}_p}\right)^2} \;=\; \mathrm{e}^{-\frac{\varepsilon^2}{12\widehat{\omega}_p}T} \;\leq\; \frac{\delta}{|P|}$$

where we use $T = \lceil -12\varepsilon^{-2}\ln(\delta/|P|)\rceil$. We obtain the claim in Case 1.

In a similar way, we obtain Case 2. From the assumption of the case, $\omega_p-\varepsilon \geq \lambda$. Since $d_{\mathrm{TV}}(\pi,\nu) \leq \varepsilon/2$, we have $\widehat{\omega}_p \geq \omega_p-\varepsilon/2$, that implies $\widehat{\omega}_p-\varepsilon/2 \geq \omega_p-\varepsilon$. Thus we obtain $\widehat{\omega}_p-\varepsilon/2 \geq \lambda$. Then

$$\Pr\left[Z(p) < \lambda T\right] \;\leq\; \Pr\left[Z(p) < \left(\widehat{\omega}_p-\frac{\varepsilon}{2}\right)T\right] \;=\; \Pr\left[Z(p) < \left(1-\frac{\varepsilon}{2\widehat{\omega}_p}\right)\widehat{\omega}_p \cdot T\right].$$

By using the Chernoff's bound,

$$\Pr\left[Z(p) < \left(1-\frac{\varepsilon}{2\widehat{\omega}_p}\right)\widehat{\omega}_p \cdot T\right] \;\leq\; \mathrm{e}^{-\frac{1}{2}\widehat{\omega}_p T\left(\frac{\varepsilon}{2\widehat{\omega}_p}\right)^2} \;=\; \mathrm{e}^{-\frac{\varepsilon^2}{8\widehat{\omega}_p}T} \;\leq\; \frac{\delta}{|P|}$$

where we use $T \stackrel{\text{def.}}{=} \lceil -12\varepsilon^{-2}\ln(\delta/|P|)\rceil$. We obtain Claim.

We conclude the proof by showing that S satisfies the inequality (5). If $S_{(\lambda-\varepsilon)N} \not\subseteq S$, then there exists a $p \in S_{(\lambda-\varepsilon)N}$ and $p \notin S$. It implies that if $S_{(\lambda-\varepsilon)N} \not\subseteq S$, then there exists a $p \in P$ satisfying that $g(p) < (\lambda - \varepsilon)N$ and $Z(p)/T \geq \lambda$. From Case 1 of the above Claim, the probability of $S_{(\lambda-\varepsilon)N} \not\subseteq S$ satisfies that

$$\Pr\left[S_{(\lambda-\varepsilon)N} \not\subseteq S\right] \;\leq\; \sum_{p \in S_{(\lambda-\varepsilon)N}} \Pr[p \notin S] \;\leq\; |\{p \mid g(p) < (\lambda-\varepsilon)N\}| \cdot \frac{\delta}{|P|}.$$

In a similar way, if $S \not\subseteq S_{(\lambda+\varepsilon)N}$, then there exists a $p \notin S_{(\lambda+\varepsilon)N}$ and $p \in S$. It implies that if $S \not\subseteq S_{(\lambda+\varepsilon)N}$, then there exists a $p \in P$ satisfying that $g(p) \geq (\lambda+\varepsilon)N$ and $Z(p)/T < \lambda$. From Case 2 of the above Claim, the probability of $S \not\subseteq S_{(\lambda+\varepsilon)N}$ satisfies that

$$\Pr\left[S \not\subseteq S_{(\lambda+\varepsilon)N}\right] \;\leq\; \sum_{p \notin S_{(\lambda+\varepsilon)N}} \Pr[p \in S] \;\leq\; |\{p \mid g(p) \geq (\lambda+\varepsilon)N\}| \cdot \frac{\delta}{|P|}.$$

Since the sets $\{p \mid g(p) < (\lambda-\varepsilon)N\}$ and $\{p \mid g(p) \geq (\lambda+\varepsilon)N\}$ are disjoint, we obtain

$$\Pr\left[S_{(\lambda-\varepsilon)N} \subseteq Z \subseteq S_{(\lambda+\varepsilon)N}\right] \;\geq\; 1 - |P| \cdot \frac{\delta}{|P|} \;=\; 1-\delta.$$

□

6 Randomized Approximation Based on Counting Ideals

The time complexity of Algorithm 1, in the previous section, gets larger proportional to ε^{-2}. As we showed in Section 3, Problem 2 is #P-hard even when i is small as fractional power of N. For small i, we have to set ε in Algorithm 1 very small as $\varepsilon \leq i/N$, it makes Algorithm 1 inefficient. In this section, we propose another approximation algorithm for the i-th LI, especially for a small i. The algorithm approximately computes $g(p)$ for each $p \in P$. Then, we use the following oracle.

Oracle 2 *(RAS for COUNTING IDEALS.) Given an arbitrary ε ($0 < \varepsilon < 1$), δ ($0 < \delta < 1$), and a poset P, Oracle returns $Z \in \mathbb{Z}_+$ which approximates $|\mathcal{D}(P)|$ satisfying*

$$\Pr\left[\frac{|Z - |\mathcal{D}(P)||}{|\mathcal{D}(P)|} \leq \varepsilon\right] \geq 1-\delta.$$

Let γ_2 denote the time required for Oracle 2. Oracle 2 is obtained from Oracle 1 in $\mathrm{poly}(\varepsilon^{-1}, -\ln\delta, |P|, \gamma_1)$ time, more precisely $\mathrm{O}(\gamma_1\, |P|^2 \varepsilon^{-2} \ln(|P|/\delta))$ with using a *self-reducibility.* See e.g. [10] about a relationship between sampling and approximate counting.

An essential idea of approximation algorithm for the i-th LI is to compute an estimator $\widehat{g}(p)$ for $g(p)$ for every $p \in P$, and to find a set $S \subseteq P$ satisfying $\widehat{g}(p) < k$. Unfortunately, this simple idea cannot find an ideal $S \in \mathcal{D}(P)$, since an event of $\widehat{g}(p) < k \leq \widehat{g}(q)$ happen to a pair $p \prec q$ with a non-negligible probability. The following algorithm gets rid of this issue.

Algorithm 2 (ε-estimator for the $f(N)$-th LI.)

1 **Input:** A poset P, ε ($0 < \varepsilon < \lambda$), δ ($0 < \delta < 1$), a function[3] $f : \mathbb{Z}_{++} \to \mathbb{Z}_{++}$.
2 **Compute** $\widehat{N}$ approximating $|\mathcal{D}(p)|$ by Oracle 2.
3 **Set** $k = f(\widehat{N})$
(where k satisfies[4] $\Pr[|k - |f(N)|| \leq (\varepsilon/3) \cdot |f(N)|] \geq 1 - \delta/(2|P|)$).

Set $S := \emptyset$.
While$(\exists p \in P \setminus S$, s.t. $q \in S\ (\forall q \prec p)) \{$
  Compute $\widehat{g}(p)$ approximating $g(p)$ by Oracle 2
  (where $\widehat{g}(p)$ satisfies $\Pr\left[|\widehat{g}(p) - g(p)| \leq (\varepsilon/3) \cdot g(p)\right] \geq 1 - \delta/(2|P|)$).
  If $\widehat{g}(p) < k$ **then** $S := S \cup \{p\}$.
$\}$
Output S and **halt**.

Theorem 6.1 *Algorithm 2 outputs an ideal $S \in \mathcal{D}(P)$ and S satisfies*

$$\Pr\left[S_{\lfloor(1-\varepsilon)f(N)\rfloor} \subseteq S \subseteq S_{\lceil(1+\varepsilon)f(N)\rceil}\right] \geq 1 - \delta$$

in $\mathrm{O}(|P|\gamma_2)$ *time.*

Proof of Theorem 6.1. The time complexity is easy to see. It is also easy to see that an output of Algorithm 2 is an ideal of P, since $p \in S$ implies that Algorithm 2 computed $\widehat{g}(p)$, that is only when $q \in P\ (\forall q \prec p)$. We show that S satisfies the inequality (6). From the condition of Algorithm 2, k satisfies

$$\Pr\left[\frac{|k - f(N)|}{f(N)} > \frac{\varepsilon}{3}\right] < \frac{\delta}{2|P|}.$$

Then we obtain the following.

Claim 1 *The probability that $k > (1+\varepsilon/3) \cdot f(N)$ or $k < (1-\varepsilon/3) \cdot f(N)$ is less than $\delta/(2|P|)$.*

Suppose we have values $\widehat{g}(p)$ for all $p \in P$, satisfying

$$\Pr\left[\frac{|\widehat{g}(p) - g(p)|}{g(p)} \leq \frac{\varepsilon}{3}\right] \geq 1 - \frac{\delta}{2|P|}, \tag{6}$$

and $\widehat{g}(p)$ coincident to the values in Algorithm 2 if it is computed. We show the following;

Claim 2 *For any $p \in P$,*
<u>Case 1.</u> if $g(p) \geq (1+\varepsilon) \cdot f(N)$, the probability $\widehat{g}(p) \leq (1+(1/3)\varepsilon) \cdot f(N)$ is less than $\delta/(2|P|)$, and
<u>Case 2.</u> if $g(p) \leq (1-\varepsilon) \cdot f(N)$, the probability $\widehat{g}(p) \geq (1-(1/3)\varepsilon) \cdot f(N)$ is less than $\delta/(2|P|)$.

In Case 1, from Inequation (6), with a probability at least $1 - \delta/(2|P|)$,

$$\begin{aligned} \widehat{g}(p) &\geq \left(1 - \frac{1}{3}\varepsilon\right) \cdot g(p) \geq \left(1 - \frac{1}{3}\varepsilon\right) \cdot (1+\varepsilon) \cdot f(N) \\ &\geq \left(1 + \frac{2-\varepsilon}{3}\varepsilon\right) \cdot f(N) > \left(1 + \frac{1}{3}\varepsilon\right) \cdot f(N) \end{aligned}$$

hold. In Case 2, from Inequation (6), with a probability at least $1 - \delta/(2|P|)$,

$$\begin{aligned} \widehat{g}(p) &\leq \left(1 + \frac{1}{3}\varepsilon\right) \cdot g(p) \leq \left(1 + \frac{1}{3}\varepsilon\right) \cdot (1-\varepsilon) \cdot f(N) \\ &\leq \left(1 - \frac{2+\varepsilon}{3}\varepsilon\right) \cdot f(N) < \left(1 - \frac{1}{3}\varepsilon\right) \cdot f(N) \end{aligned}$$

hold. We obtain the claim.

From Claim 1 and 2, we obtain the following (see Figure 4);

[4] We naturally assume that the function is a contraction mapping and nondecreasing, e.g., $\lfloor\sqrt{z}\rfloor$, $\lceil z^{1/c}\rceil$, $\lceil\log(z)\rceil$, etc.

[4] If the function f is a contraction mapping and nondecreasing, the condition is satisfied when $\widehat{N}$ satisfies $\Pr[|\widehat{N} - |\mathcal{D}(p)|| \leq (\varepsilon/3) \cdot |\mathcal{D}(p)|] \geq 1 - \delta/(2|P|)$.

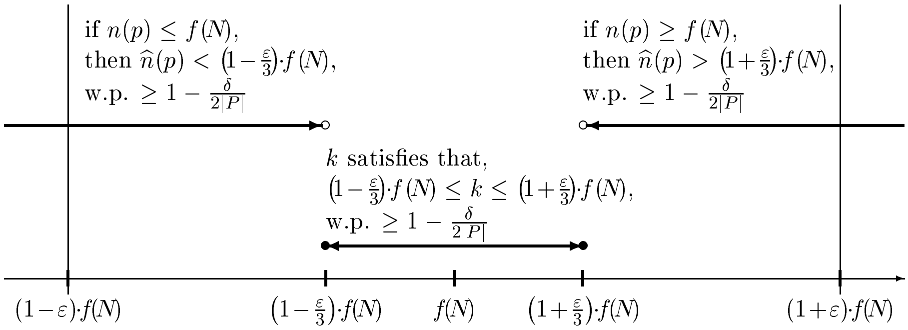

Figure 4: A figure of the relationship between k and $\widehat{g}(p)$.

Claim 3 *For any $p \in P$,*
Case 1. if $g(p) \geq (1+\varepsilon)\cdot f(N)$, then $\widehat{g}(p) < k$ with a probability less than $\delta/|P|$, and
Case 2. if $g(p) \leq (1-\varepsilon)\cdot f(N)$, then $\widehat{g}(p) \geq k$ with a probability less than $\delta/|P|$.

Now we conclude the proof by showing (6). Algorithm 2 implies that if $S_{(1-\varepsilon)\cdot f(N)} \not\subseteq S$, then there exists a $p \in P$ satisfying $g(p) < (1-\varepsilon)\cdot f(N)$, and exists a $q \in P$ satisfying $q \prec p$ and $\widehat{g}(q) < k$. Note that $q \prec p$ means $g(q) < g(p)$, thus the above claim can be simply transformed into that if $S_{(1-\varepsilon)\cdot f(N)} \not\subseteq S$, then there exists a $q \in P$ satisfying $g(q) < (1-\varepsilon)\cdot f(N)$ and $\widehat{g}(q) < k$. From Case 1 of Claim 3, the probability of $S_{(1-\varepsilon)\cdot f(N)} \not\subseteq S$ satisfies that

$$\begin{aligned}\Pr\left[S_{(1-\varepsilon)\cdot f(N)} \not\subseteq S\right] &\leq \sum_{p \in S_{(1-\varepsilon)f(N)}} \Pr[p \notin S] \\ &\leq |\{p \mid g(p) < (1-\varepsilon)\cdot f(N)\}|\cdot \frac{\delta}{|P|}.\end{aligned}$$

In a similar way, if $S \not\subseteq S_{(1+\varepsilon)\cdot f(N)}$, then there exists a $p \notin S_{(1+\varepsilon)\cdot f(N)}$ and $p \in S$. It implies that if $S \not\subseteq S_{(1+\varepsilon)\cdot f(N)}$, then $g(p) \geq (1+\varepsilon)\cdot f(N)$ and $\widehat{g}(p)$. From Case 2 of Claim 3, the probability of $S \not\subseteq S_{(1+\varepsilon)\cdot f(N)}$ satisfies that

$$\begin{aligned}\Pr\left[S \not\subseteq S_{(1+\varepsilon)f(N)}\right] &\leq \sum_{p \notin S_{(1+\varepsilon)\cdot f(N)}} \Pr[p \in S] \\ &\leq |\{p \mid g(p) \geq (1+\varepsilon)\cdot f(N)\}|\cdot \frac{\delta}{|P|}.\end{aligned}$$

Since the sets $\{p \mid g(p) < (1-\varepsilon)\cdot f(N)\}$ and $\{p \mid g(p) \geq (1+\varepsilon)\cdot f(N)\}$ are disjoint, we obtain

$$\Pr\left[S_{(1-\varepsilon)f(N)} \subseteq Z \subseteq S_{(1+\varepsilon)f(N)}\right] \geq 1 - |P|\cdot\frac{\delta}{|P|} = 1-\delta.$$

□

7 Concluding Remarks

We gave randomized approximation schemes for the i-th GMSM using an almost uniform sampler on ideals of a poset. The existence of a polynomial time almost uniform sampler on ideals (or antichains) of a poset, or an FPRAS for counting, is open. Note that conversely if we have a fully polynomial-time randomized approximation scheme for the i-th GMSM in a form such as Theorem 5.1 or 6.1, then we can obtain an FPRAS for counting ideals of a poset (see Appendix D), and hence a polynomial time almost uniform sampler (see e.g. [10]).

In case that a rotation poset belongs to some special classes such as series-parallel, bounded width, etc., then we can find the i-th GMSM exactly in polynomial time by Steiner's result [22]. No results seem to be known on a characterization of preference lists whose rotation posets belongs to such classes of polynomial time solvable, as far as we see. It is also open whether or not Problems 1 and 2 are in NP.

Acknowledgment

The authors thank Professor Shin-Ichi Nakano for his helpful comment. The first author is supported by Grant-in-Aid for Scientific Research.

References

[1] N. Bhatnagar, S. Greenberg, and D. Randall, Sampling stable marriages: why the spouse-swapping won't work, Proceedings of the nineteenth annual ACM-SIAM symposium on Discrete algorithms (SODA 2008), 1223–1232.

[2] C. Blair, Every finite distributive lattice is a set of stable matchings, Journal of Combinatorial Theory A, **37** (1984), 353–356.

[3] C.T. Cheng, The generalized median stable matchings: finding them is not that easy, Proceedings of the 8th Latin American Theoretical Informatics (Latin 2008), 568–579.

[4] B.A. Davey and H.A. Priestley, Introduction to Lattices and Order, Second Edition, Cambridge University Press, 2002.

[5] D.P. Dubhashi, K. Mehlhorn, D. Rajan, and C.Thiel, Searching, sorting and randomised algorithms for central elements and ideal counting in posets, Lecture Notes in Computer Science, **761** (1993), 436–443 .

[6] D. Gale and L.S. Shapley, College admissions and the stability of marriage, The American Mathematics Monthly, **69** (1962), 9–15.

[7] M.R. Garey and D.S. Johnson, A Guide to the Theory of NP-Completeness, W. H. Freeman, 1979.

[8] D. Gusfield and R.W. Irving, The Stable Marriage Problem, Structure and Algorithms, The MIT Press, 1989.

[9] R.W. Irving and P. Leather, The complexity of counting stable marriages, SIAM Journal on Computing, **15** (1986), 655–667.

[10] M. Jerrum, Counting, Sampling and Integrating: Algorithms and Complexity, ETH Zürich, Birkhauser, Basel, 2003.

[11] B. Klaus and F. Klijn, Median stable matching for college admission, International Journal of Game Theory, **34** (2006), 1–11.

[12] B. Klaus and F. Klijn, Smith and Rawls share a room: stability and medians, Meteor RM/08-009 (2008), Maastricht University,
`http://edocs.ub.unimaas.nl/loader/file.asp?id=1307`

[13] D. Knuth, Stable Marriage and Its Relation to Other Combinatorial Problems, American Mathematical Society, 1991.

[14] T. Nemoto, Some remarks on the median stable marriage problem, Proceedings of 17th International Symposium on Mathematical Programming, 2000.

[15] J. Propp and D.B.Wilson, Exact sampling with coupled Markov chains and applications to statistical mechanics, Random Structures and Algorithms, **9** (1996), 223–252.

[16] J.S. Provan and M.O. Ball, The complexity of counting cuts and of computing the probability that a graph is connected, SIAM Journal on Computing, **12** (1983), 777–788.

[17] A.E. Roth and M.A.O. Sotomayor, A. Two-Sided Matchings: A Study In Game-Theoretic Modeling And Analysis, Cambridge University Press, 1990.

[18] M. Schwarz and M.B. Yenmez, Median stable matching, 2007, available at SSRN; `http://ssrn.com/abstract=1031277`

[19] J. Sethuraman, C.P. Teo, and L. Qian, Many-to one stable matching: geometry and fairness, Mathematics of Operations Research, **31** (2006), 581–596.

[20] M.B. Squire, Enumerating the ideals of a poset, preprint, North Carolina State University, 1995.

[21] G. Steiner, An algorithm for generating the ideals of a partial order, Operations Research Letters, **5** (1986), 317–320.

[22] G. Steiner, On the complexity of dynamic programming for sequencing problems with precedence constraints, Annals of Operations Research, **26** (1990), 103–123.

[23] C.P. Teo and J. Sethuraman, The geometry of fractional stable matchings and its applications, Mathematics of Operations Research, **23** (1998), 874–891.

A Proof of Theorem 3.6

Theorem 3.6. *Suppose c ($c \geq 2$) is an arbitrary constant. Given a poset R and an ideal $S \in \mathcal{D}(R)$, then the problem whether or not S is the $\lceil N^{1/c} \rceil$-th LI of R is #P-hard, where $N = |\mathcal{D}(R)|$.*

Proof. We reduce COUNTING IDEALS for a given poset P to our problem in a similar way as the proof of Proposition 3.5. For the poset P and an arbitrary positive integer K, we define $R' \stackrel{\text{def.}}{=} ((\{x\} \oplus P) \dot{\cup} (\{y\} \oplus Q)) \oplus Q'$, where posets Q and Q' satisfies $|\mathcal{D}(Q)| = K$ and $|\mathcal{D}(Q')| = \lfloor (K+1)^c \rfloor - (K+1)^2 + 1$. From Lemma 3.3, Q and Q' is constructible in $\mathrm{poly}(\log(K^c)) = \mathrm{poly}(\log K)$ time and space. Let $N = |\mathcal{D}(R')|$, then $N = \lfloor (K+1)^c \rfloor - (K+1)^2 + (|\mathcal{D}(P)|+1)(K+1)$. We define a function $f : \mathbb{Z}_{++} \to \mathbb{Z}_{++}$ by $f(z) \stackrel{\text{def.}}{=} \lceil z^{1/c} \rceil$, then

$$\begin{aligned} f(N) &= \left\lceil \left(\lfloor (K+1)^c \rfloor - (K+1)^2 + (|\mathcal{D}(P)|+1)(K+1) \right)^{1/c} \right\rceil \\ &= \left\lceil \left(\lfloor (K+1)^c \rfloor + (|\mathcal{D}(P)|-K)(K+1) \right)^{1/c} \right\rceil . \end{aligned} \tag{7}$$

For each $r \in R'$, $g(r)$, that is defined by (1), satisfies

$$\begin{aligned} g(x) &= |\mathcal{D}(\{y\} \oplus Q)| = |\mathcal{D}(Q)| + 1, \\ g(y) &= |\mathcal{D}(\{x\} \oplus P)| = |\mathcal{D}(P)| + 1, \\ g(p) &\geq |\mathcal{D}((\{x\} \oplus P) \dot{\cup} \{y\})| = 2 \cdot g(x) \qquad (\forall p \in P), \\ g(q) &\geq |\mathcal{D}((\{y\} \oplus Q) \dot{\cup} \{x\})| = 2 \cdot g(y) \qquad (\forall q \in Q), \\ g(q') &\geq g(q) \geq 2 \cdot g(y) \qquad (\forall q' \in Q'). \end{aligned}$$

Now we show that $\{y\}$ is the $f(N)$-th LI of R when K satisfies $|\mathcal{D}(P)| < K \leq 2|\mathcal{D}(P)|$. With considering $g(q) \geq 2 \cdot g(y)$ for all $q \in Q$, $\{y\}$ is the $f(N)$-th LI if $g(y) < f(N)$, $f(N) \leq 2g(y)$, and $f(N) \leq g(x)$ hold. These conditions are transformed with (7) into

$$|\mathcal{D}(P)| + 1 < \left\lceil \left(\lfloor (K+1)^c \rfloor + (|\mathcal{D}(P)|-K)(K+1) \right)^{1/c} \right\rceil , \tag{8}$$

$$\left\lceil \left(\lfloor (K+1)^c \rfloor + (|\mathcal{D}(P)|-K)(K+1) \right)^{1/c} \right\rceil \leq 2|\mathcal{D}(P)| + 2, \tag{9}$$

$$\left\lceil \left(\lfloor (K+1)^c \rfloor + (|\mathcal{D}(P)|-K)(K+1) \right)^{1/c} \right\rceil \leq K + 1, \tag{10}$$

respectively. It is easy to see that the condition (10) hold if $|\mathcal{D}(P)| < K$. We show that the condition (8) hold if $|\mathcal{D}(P)| < K$. With considering that

$$\begin{aligned} f(N) &= \left\lceil \left(\lfloor (K+1)^c \rfloor + (|\mathcal{D}(P)|-K)(K+1) \right)^{1/c} \right\rceil \\ &\geq \left\lceil \left((K+1)^c - 1 + (|\mathcal{D}(P)|-K)(K+1) \right)^{1/c} \right\rceil \\ &\geq \left((K+1)^c - 1 + (|\mathcal{D}(P)|-K)(K+1) \right)^{1/c} , \end{aligned}$$

it is enough to show that $(K+1)^c - 1 + (|\mathcal{D}(P)|-K)(K+1) - (|\mathcal{D}(P)|+1)^c > 0$ when $|\mathcal{D}(P)| + 1 \leq K$ and $c \geq 2$. Then, with the following transformations

$$\begin{aligned} &(K+1)^c - 1 + (|\mathcal{D}(P)|-K)(K+1) - (|\mathcal{D}(P)|+1)^c \\ &\quad = (K+1)^c - (|\mathcal{D}(P)|+1)^c + (|\mathcal{D}(P)|-K)(K+1) - 1 \\ &\quad \geq (K+1)^{\lfloor c \rfloor} - (|\mathcal{D}(P)|+1)^{\lfloor c \rfloor} + (|\mathcal{D}(P)|-K)(K+1) - 1 \end{aligned}$$

$$
\begin{aligned}
&= (K-|\mathcal{D}(P)|)\Big((K+1)^{\lfloor c\rfloor-1}+\cdots+(|\mathcal{D}(P)|+1)^{\lfloor c\rfloor-1}\Big)+(|\mathcal{D}(P)|-K)(K+1)-1\\
&> (K-|\mathcal{D}(P)|)\Big((K+1)^{\lfloor c\rfloor-1}+(|\mathcal{D}(P)|+1)^{\lfloor c\rfloor-1}\Big)+(|\mathcal{D}(P)|-K)(K+1)-1\\
&= (K-|\mathcal{D}(P)|)\Big((K+1)^{\lfloor c\rfloor-1}-(K+1)\Big)+(K-|\mathcal{D}(P)|)(|\mathcal{D}(P)|+1)^{\lfloor c\rfloor-1}-1\\
&\geq 0,
\end{aligned}
$$

we obtain the claim that the condition (8) hold if $|\mathcal{D}(P)| < K$. The condition (9) hold if $|\mathcal{D}(P)| \leq K \leq 2|\mathcal{D}(P)|$, since

$$
\begin{aligned}
&\left\lceil (\lfloor (K+1)^c\rfloor + (|\mathcal{D}(P)|-K)(K+1))^{1/c}\right\rceil\\
&\quad\leq \left\lceil \lfloor (K+1)^c\rfloor^{1/c}\right\rceil \leq \left\lceil ((K+1)^c)^{1/c}\right\rceil = K+1 < 2|\mathcal{D}(P)|+2.
\end{aligned}
$$

Here consider the case of $K \leq |\mathcal{D}(P)|$, then the singleton $\{y\}$ is never the $f(N)$-th LI of R, in the same argument as the proof of Proposition 3.5. Thus, minimizing K for which $\{y\}$ is the $f(N)$-th LI of R, then the minimum K^* is equal to $|\mathcal{D}(P)|+1$. In a similar way as the proof of Proposition 3.5. $|\mathcal{D}(P)|$ is computed with checking if $\{y\}$ is the $f(N)$-th LIs of R for appropriate Ks, at most $2|P|$ times, as follows. We start from $K = 2^{|P|}$ and get K into halves, until $\{y\}$ is the $f(N)$-th LI. From the above discussions, we certainly obtain the case. Suppose we get the case that $\{y\}$ is the $f(N)$-th LI when $K = K_0$. In the interval $[1, K_0]$, $\{y\}$ is the $f(N)$-th LI if, and only if, $K \in (|\mathcal{D}(P)|, K_0]$. Thus we can find $K^* = |\mathcal{D}(P)|+1$ according to the binary search strategy. □

B Randomized Approximation for Counting Ideals of a Poset

In this section, we give a randomized approximation scheme for counting ideals of a poset, on the assumption of Oracle 1 that is almost uniform sampler for ideals of a poset. To begin with, we describe an essential idea of our recursive algorithm.

Let a sequence $\boldsymbol{p} = p_1, \ldots, p_{|P|}$ be a *linear extension* of the poset P; that is $p_j \not\succeq p_i$ for any $j < i$. Let $P_i \stackrel{\text{def.}}{=} \{p_1, \ldots, p_i\}$ for $i \in \{1, \ldots, |P|\}$, then p_i is maximal in the poset P_i for every $i \in \{1, \ldots, |P|\}$. Now we consider the set $\mathcal{D}(P_i)$ of ideals of P_i for each $i \in \{1, \ldots, |P|\}$. Let $\mathcal{D}^-(P_i)$ be a subset of $\mathcal{D}(P_i)$ defined by

$$
\mathcal{D}^-(P_i) \stackrel{\text{def.}}{=} \{S \in \mathcal{D}(P_i) \mid p_i \notin S\},
$$

then it is easy to see that $\mathcal{D}^-(P_i) = \mathcal{D}(P_{i-1})$ holds for each $i \in \{2, \ldots, |P|\}$ from the definition of $\mathcal{D}^-(P_i)$. Furthermore, we have $|\mathcal{D}^-(P_i)|/|\mathcal{D}(P_i)| \geq 1/2$, since for every $S \in D(P_i)$ satisfying $p_i \in S$, there exists $S' \stackrel{\text{def.}}{=} S \setminus \{p_i\}$ and S' satisfies $S' \in \mathcal{D}(P_i)$ with considering p_i is maximal in P_i.

Now we describe an idea of recursion for counting $\mathcal{D}(P)$. With considering the following trivial transformation

$$
|\mathcal{D}(P_i)| = \frac{|\mathcal{D}(P_i)|}{|\mathcal{D}^-(P_i)|} \cdot |\mathcal{D}^-(P_i)|,
$$

and considering the fact that $|\mathcal{D}^-(P_i)| = |\mathcal{D}(P_{i-1})|$, we have

$$
|\mathcal{D}(P_i)| = \frac{|\mathcal{D}(P_i)|}{|\mathcal{D}^-(P_i)|} \cdot |\mathcal{D}(P_{i-1})|
$$

for each $i \in \{2, \ldots, |P|\}$. Thus recursively we obtain

$$|\mathcal{D}(P)| = \frac{|\mathcal{D}(P_{|P|})|}{|\mathcal{D}^-(P_{|P|})|} \cdot \frac{|\mathcal{D}(P_{|P|-1})|}{|\mathcal{D}^-(P_{|P|-1})|} \cdot \ \cdots \ \cdot \frac{|\mathcal{D}(P_2)|}{|\mathcal{D}^-(P_2)|} \cdot |\mathcal{D}(P_1)|,$$

and clearly $|\mathcal{D}(P_1)| = 2$ since P_1 consists of a singleton. If we have a uniform sampler on $\mathcal{D}(P_i)$, we can estimate $|\mathcal{D}^-(P_i)|/|\mathcal{D}(P_i)|$ by the Monte Carlo method, and the fact that $|\mathcal{D}^-(P_i)|/|\mathcal{D}(P_i)|$ is sufficiently large, namely at least $1/2$ in this case, ensures efficient estimation by a Monte Carlo. This is the basic idea, but we need to take care of the influence to use approximate sampler. The following is the whole description of a randomized approximation scheme.

Algorithm 3 (RAS for counting ideals of a poset with an almost uniform sampler.)

Input: A poset P, ε $(0 < \varepsilon < 1)$, δ $(0 < \delta < 1)$.
Find a linear extension $\boldsymbol{p} := p_1, \ldots, p_{|P|}$ of P.
For$(i = |P|,\ i > 1,\ i--\ )\{$
  Set $P_i := \{p_1, \ldots, p_i\}$, and **set** $Z_i := 0$.
  Repeat$(T \stackrel{\text{def.}}{=} 225|P|^2\varepsilon^{-2}\ln(2|P|/\delta)$ times$)\{$
    Generate $X \in \mathcal{D}(P_i)$ by Oracle 1 (where ν satisfies $d_{\mathrm{TV}}(\pi, \nu) \leq \frac{\varepsilon}{10|P|}$).
    If $p_i \notin X$, **then** $Z_i := Z_i + 1$.
  $\}$
$\}$
Set $Z := 2\prod_{i=2}^{|P|}(T/Z_i)$, **output** Z, and **halt**.

Theorem B.1 *Algorithm 3 outputs $Z \in \mathbb{R}_{++}$ in $\mathrm{O}(\gamma_1|P|^2\varepsilon^{-2}\ln(|P|/\delta))$ time, and Z approximates $|\mathcal{D}(P)|$ satisfying*

$$\Pr\left[\frac{|Z - |\mathcal{D}(P)||}{|\mathcal{D}(P)|} \leq \varepsilon\right] \geq 1 - \delta.$$

Proof. The time complexity is easy to see, and we show the inequality in the following. We define $\omega_i \stackrel{\text{def.}}{=} |\mathcal{D}^-(P_i)|/|\mathcal{D}(P_i)|$, and $\widehat{\omega}_i \stackrel{\text{def.}}{=} \sum_{S \in \mathcal{D}^-(P_i)} \nu(S)$; i.e., $\widehat{\omega}_i$ is the probability that a sample X according to the distribution ν satisfies $p_i \notin X$, hence an estimator for ω_i.

Claim 1 *For each $i \in \{2, \ldots, n\}$, we have $\left(1 - \frac{\varepsilon}{5|P|}\right)\omega_i \leq \widehat{\omega}_i \leq \left(1 + \frac{\varepsilon}{5|P|}\right)\omega_i$.*

The definition of the *total variation distance* d_{TV} (see Oracle 1 in Section 4) implies that $|\widehat{\omega}_i - \omega_i| \leq d_{\mathrm{TV}}(\pi, \nu)$. From the assumption of Algorithm, we have $d_{\mathrm{TV}}(\pi, \nu) \leq \varepsilon/(10|P|)$, we have $|\widehat{\omega}_i - \omega_i| \leq \varepsilon/(10|P|)$, that is transformed into

$$\omega_i - \tfrac{\varepsilon}{10|P|} \leq \widehat{\omega}_i \leq \omega_i + \tfrac{\varepsilon}{10|P|}.$$

With considering that $w_i \geq 1/2$, we have the following transformations

$$\begin{array}{lllllll}
(\text{r.h.s}) & = & \omega_i + \frac{\varepsilon}{10|P|} & = & \left(1 + \frac{\varepsilon}{10|P|\omega_i}\right)\omega_i & \leq & \left(1 + \frac{\varepsilon}{5|P|}\right)\omega_i, \quad \text{and} \\
(\text{l.h.s}) & = & \omega_i - \frac{\varepsilon}{10|P|} & = & \left(1 - \frac{\varepsilon}{10|P|\omega_i}\right)\omega_i & \geq & \left(1 - \frac{\varepsilon}{5|P|}\right)\omega_i,
\end{array}$$

hence we obtain the claim.

Claim 2 *For each $i \in \{2, \ldots, |P|\}$, we have $\Pr\left[\left|\frac{Z_i}{T} - \widehat{\omega}_i\right| \geq \frac{\varepsilon}{5|P|}\widehat{\omega}_i\right] < \frac{\delta}{|P|}$.*

With the Chernoff bound,

$$
\begin{aligned}
\Pr\left[\left|\frac{Z_i}{T}-\widehat{\omega}_i\right| \ge \frac{\varepsilon}{5|P|}\widehat{\omega}_i\right] &= \Pr\left[|Z_i-\widehat{\omega}_i T| \ge \frac{\varepsilon}{5|P|}\widehat{\omega}_i T\right] \\
&< 2\mathrm{e}^{-\left(\frac{\varepsilon}{5|P|}\right)^2 \frac{1}{3}\cdot 225|P|^2\varepsilon^{-2}\ln(2|P|/\delta)\cdot\widehat{\omega}_i} \\
&= 2\mathrm{e}^{-3\widehat{\omega}_i\ln(2|P|/\delta)} \\
&\le 2\mathrm{e}^{-\ln(2|P|/\delta)} \\
&= \delta/|P|,
\end{aligned}
$$

hence we obtain the claim.

Claim 3 *For each $i \in \{2,\dots,|P|\}$, if $\left|\frac{Z_i}{T}-\widehat{\omega}_i\right| \le \frac{\varepsilon}{5|P|}\widehat{\omega}_i$, then $\left(1+\frac{\varepsilon}{2|P|}\right)^{-1} \le \frac{Z_i}{T}\cdot\omega_i^{-1} \le \left(1+\frac{\varepsilon}{2|P|}\right)$.*

The hypothesis of the claim is transformed into

$$\left(1-\frac{\varepsilon}{5|P|}\right)\widehat{\omega}_i \le \frac{Z_i}{T} \le \left(1+\frac{\varepsilon}{5|P|}\right)\widehat{\omega}_i.$$

With combining Claim 1, we obtain

$$\left(1-\frac{\varepsilon}{5|P|}\right)^2\omega_i \le \frac{Z_i}{T} \le \left(1+\frac{\varepsilon}{5|P|}\right)^2\omega_i,$$

hence

$$\left(1-\frac{\varepsilon}{5|P|}\right)^2 \le \frac{Z_i}{T}\cdot\omega_i^{-1} \le \left(1+\frac{\varepsilon}{5|P|}\right)^2.$$

With the following transformations

$$
\begin{aligned}
(\text{r.h.s}) &= \left(1+\frac{\varepsilon}{5|P|}\right)^2 = 1+\left(2+\frac{\varepsilon}{5|P|}\right)\frac{\varepsilon}{5|P|} \le 1+\frac{2.5\varepsilon}{5|P|} = 1+\frac{\varepsilon}{2|P|}, \quad \text{and} \\
(\text{l.h.s}) &= \left(1-\frac{\varepsilon}{5|P|}\right)^2 \ge \left(1+\frac{\varepsilon}{5|P|}\right)^{-2} = (\text{r.h.s})^{-1} \ge \left(1+\frac{\varepsilon}{2|P|}\right)^{-1},
\end{aligned}
$$

hence we obtain the claim.

Claim 4 $\Pr\left[(1-\varepsilon)\prod_{i=2}^{|P|}\omega_i \le \prod_{i=2}^{|P|}\frac{Z_i}{T} \le (1+\varepsilon)\prod_{i=2}^{|P|}\omega_i\right] \ge 1-\delta.$

If $\left|\frac{Z_i}{T}-\widehat{\omega}_i\right| \le \frac{\varepsilon}{5|P|}\widehat{\omega}_i$ hold for all $i \in \{2,\dots,|P|\}$, with multiplying Claim 3 for $i \in \{2,\dots,|P|\}$, we obtain

$$\left(1+\frac{\varepsilon}{2|P|}\right)^{-(|P|-1)} \le \frac{\prod_{i=2}^{|P|}\frac{Z_i}{T}}{\prod_{i=2}^{|P|}\omega_i} \le \left(1+\frac{\varepsilon}{2|P|}\right)^{|P|-1}.$$

With the following transformations

$$
\begin{aligned}
(\text{r.h.s}) &= \left(1+\frac{\varepsilon}{2|P|}\right)^{|P|-1} \le \left(1+\frac{\varepsilon}{2(|P|-1)}\right)^{|P|-1} \le 1+\varepsilon, \quad \text{and} \\
(\text{l.h.s}) &= \left(1+\frac{\varepsilon}{2|P|}\right)^{-(|P|-1)} = (\text{r.h.s})^{-1} \ge (1+\varepsilon)^{-1} \ge 1-\varepsilon,
\end{aligned}
$$

we obtain the fact that if $\left|\frac{Z_i}{T} - \widehat{\omega}_i\right| \le \frac{\varepsilon}{5|P|}\widehat{\omega}_i$ hold for all $i \in \{2, \ldots, |P|\}$ then

$$(1-\varepsilon)\prod_{i=2}^{|P|}\omega_i \;\le\; \prod_{i=2}^{|P|}\frac{Z_i}{T} \;\le\; (1+\varepsilon)\prod_{i=2}^{|P|}\omega_i \tag{11}$$

holds. For he probability of the hypothesis of (11), Claim 2 implies that

$$\Pr\left[\exists i \in \{2, \ldots, |P|\} \text{ s.t. } \left|\frac{Z_i}{T} - \widehat{\omega}_i\right| \ge \frac{\varepsilon}{5|P|}\widehat{\omega}_i\right] \;<\; (|P|-1)\cdot\frac{\delta}{|P|} \;<\; \delta,$$

hence we obtain the claim.

Now we conclude the proof. By multiplying 2 to (11) in Claim 4, we have

$$(1-\varepsilon)|\mathcal{D}(P)| \;\le\; Z \;\le\; (1+\varepsilon)|\mathcal{D}(P)|,$$

where Z is the output of Algorithm 3. With considering Claim 4, we obtain

$$\Pr\left[\frac{|Z - |\mathcal{D}(P)||}{|\mathcal{D}(P)|} \le \varepsilon\right] \ge 1 - \delta.$$

□

C #P-Hardness for Other Functions

Proposition C.1 *Suppose a $(0 < a \le 1/2)$ is an arbitrary constant. Given a poset R and an ideal $S \in \mathcal{D}(R)$, then the problem whether or not S is the $\lceil aN \rceil$-th LI of R is #P-hard, where $N = |\mathcal{D}(R)|$.*

Proof. We reduce COUNTING IDEALS for a given poset P to our problem. We assume P that $|\mathcal{D}(P)|$ is sufficiently as large as the constant $1/a$. Given an arbitrary integer K, we define $R'' \stackrel{\text{def.}}{=} Q'' \oplus ((X' \oplus X \oplus P) \dot\cup (Y' \oplus Y \oplus Q)) \oplus Q'$, where let $K^* \stackrel{\text{def.}}{=} 2^{\lceil \lg K \rceil + 1}$ and

$$\begin{array}{rcl}
X &=& Y \;\stackrel{\text{def.}}{=}\; \{e_1\} \dot\cup \{e_2\} \dot\cup \cdots \dot\cup \{e_{\lceil \lg K \rceil + 2}\}, \\
|\mathcal{D}(X')| &=& |\mathcal{D}(Y')| \;=\; K^* + 1, \\
|\mathcal{D}(Q)| &=& K, \\
|\mathcal{D}(Q'')| &=& (K^* + K - 1)(3K^* + K - 1) + 1, \text{ and} \\
|\mathcal{D}(Q')| &=& \left\lfloor a^{-1}(3K^* + K - 1)^2 \right\rfloor - (3K^* + K - 1)^2 - (K^* + K - 1)(3K^* + K - 1) + 1.
\end{array}$$

Then we show that $Q'' \oplus (X' \dot\cup (Y' \oplus Y))$ is the $f(N)$-th LI of R when K satisfies $|\mathcal{D}(P)| < K$. At the beginning we have the followings

$$\begin{aligned}
g(x) &= |\mathcal{D}\,(Q'' \oplus ((X' \oplus X \setminus x) \dot\cup (Y' \oplus Y \oplus Q)))\,| \\
&= (K^* + K - 1)(3K^* + K - 1) + 1 + 2K^*(3K^* + K - 1) - 1 \\
&= (3K^* + K - 1)^2 && (\forall x \in X) \\
g(y) &= |\mathcal{D}\,(Q'' \oplus ((X' \oplus X \oplus P) \dot\cup (Y' \oplus Y \setminus y)))\,| \\
&= (K^* + K - 1)(3K^* + K - 1) + 1 + (3K^* + |\mathcal{D}(P)| - 1)2K^* - 1 \\
&= (3K^* + K - 1)^2 + 2K^*(|\mathcal{D}(P)| - K) && (\forall y \in Y) \\
g(x') &< |\mathcal{D}\,(Q'' \oplus (X' \dot\cup (Y' \oplus Y \oplus Q)))\,| \\
&= (K^* + K - 1)(3K^* + K - 1) + 1 + K^*(3K^* + K - 1) - 1 \\
&= (2K^* + K - 1)(3K^* + K - 1) \\
&= (3K^* + K - 1)^2 - K^*(3K^* + K - 1) && (\forall x' \in X') \\
g(q) &\geq |\mathcal{D}\,(Q'' \oplus ((X' \oplus X \oplus P) \dot\cup (Y' \oplus Y)))\,| \\
&= (K^* + K - 1)(3K^* + K - 1) + 1 + (3K^* + |\mathcal{D}(P)| - 1)3K^* - 1 \\
&= (K^* + K - 1)(3K^* + K - 1) + 3K^*(3K^* + K - 1) + 3K^*(|\mathcal{D}(P)| - K) \\
&= (4K^* + K - 1)(3K^* + K - 1) + 3K^*(|\mathcal{D}(P)| - K) && (\forall q \in Q)
\end{aligned}$$

and

$$\begin{aligned}
|\mathcal{D}(R'')| &= (K^* + K - 1)(3K^* + K - 1) + (3K^* + |\mathcal{D}(P)| - 1)(3K^* + K - 1) \\
&\quad + \left\lfloor a^{-1}(3K^* + K - 1)^2 \right\rfloor - (3K^* + K - 1)^2 - (K^* + K - 1)(3K^* + K - 1) \\
&= \left\lfloor a^{-1}(3K^* + K - 1)^2 \right\rfloor + (3K^* + |\mathcal{D}(P)| - 1)(3K^* + K - 1) - (3K^* + K - 1)^2 \\
&= \left\lfloor a^{-1}(3K^* + K - 1)^2 \right\rfloor + (|\mathcal{D}(P)| - K)(3K^* + K - 1).
\end{aligned}$$

Let $f(N) \stackrel{\text{def.}}{=} \lceil N^{1/c} \rceil$, then we have

$$\begin{aligned}
f(N) &\geq (3K^* + K - 1)^2 - 1 + a(|\mathcal{D}(P)| - K)(3K^* + K - 1), \text{ and} \\
f(N) &\leq (3K^* + K - 1)^2 + a(|\mathcal{D}(P)| - K)(3K^* + K - 1) + 1.
\end{aligned}$$

Now we show that $Q'' \oplus (X' \dot\cup (Y' \oplus Y))$ is the $f(N)$-th LI of R when K satisfies $|\mathcal{D}(P)| < K$. From the definition, $Q'' \oplus (X' \dot\cup (Y' \oplus Y))$ is the $f(N)$-th LI if $g(y) < f(N)$, $f(N) \leq g(q)$, $g(x') < f(N)$, and $f(N) \leq g(x)$ hold. It is not difficult to see that $g(q) \geq g(x)$ and $g(x') \leq g(y)$ when $K > |\mathcal{D}(P)|$, since $K^* \geq K - |\mathcal{D}(P)|$. Thus the above conditions are satisfied if

$$(3K^* + K - 1)^2 + 2K^*(|\mathcal{D}(P)| - K) < (3K^* + K - 1)^2 - 1 + a(|\mathcal{D}(P)| - K)(3K^* + K - 1), \tag{12}$$
$$(3K^* + K - 1)^2 + a(|\mathcal{D}(P)| - K)(3K^* + K - 1) + 1 \leq (3K^* + K - 1)^2, \tag{13}$$

respectively. It is easy to see that (13) holds when $K > |\mathcal{D}(P)|$. For (12), with considering the facts that $K^* \geq 2K$ and $a \leq 1/2$, and remembering the assumptions that $K^*/2 \geq K > |\mathcal{D}(P)| \geq 1/a$,

$$\begin{aligned}
\text{(r.h.s)} - \text{(l.h.s)} &= a(|\mathcal{D}(P)| - K)(3K^* + K - 1) - 1 - 2K^*(|\mathcal{D}(P)| - K) \\
&\geq a(|\mathcal{D}(P)| - K)(3.5K^* - 1) - 2K^*(|\mathcal{D}(P)| - K) - 1 \\
&> (K - |\mathcal{D}(P)|)(2K^* - 3.5aK^*) - 1 \\
&\geq 0.
\end{aligned}$$

On the other hand, when $K \leq |\mathcal{D}(P)|$, clearly $g(x) \leq g(y)$ holds, and it implies that $Q'' \oplus (X' \dot\cup (Y' \oplus Y))$ is not a level ideal. Thus we search the minimum K satisfying that $Q'' \oplus (X' \dot\cup (Y' \oplus Y))$ is the $f(N)$-th LI of R, according to a binary search strategy on K starting from $K = 2^{|P|}$, then eventually we find the minimum $K = |\mathcal{D}(P)| + 1$. □

Proposition C.2 *Suppose a $(0 < a \leq 1)$ and c $(1 < c < 2)$ is an arbitrary constant. Given a poset R and an ideal $S \in \mathcal{D}(R)$, then the problem whether or not S is the $\lceil aN^{1/c} \rceil$-th LI of R is #P-hard, where $N = |\mathcal{D}(R)|$.*

Proof. We reduce COUNTING IDEALS for a given poset P to our problem. Given an arbitrary integer K, we define $R'' \stackrel{\text{def.}}{=} Q'' \oplus ((X' \oplus X \oplus P) \dot\cup (Y' \oplus Y \oplus Q)) \oplus Q'$, where let $K^* \stackrel{\text{def.}}{=} \max\{2^{\lceil 1/(c-1) \rceil}, 2^{|P|}\}$ and

$$
\begin{array}{rcl}
X & = & Y \stackrel{\text{def.}}{=} \{e_1\} \dot\cup \{e_2\} \dot\cup \cdots \dot\cup \{e_{\lg K^* + 1}\}, \\
|\mathcal{D}(X')| & = & |\mathcal{D}(Y')| \ = \ K^* + 1, \\
|\mathcal{D}(Q)| & = & K, \\
|\mathcal{D}(Q'')| & = & (K^* + K - 1)(3K^* + K - 1) + 1, \text{ and} \\
|\mathcal{D}(Q')| & = & \lfloor a^{-c}(3K^* + K - 1)^{2c} \rfloor - (3K^* + K - 1)^2 - (K^* + K - 1)(3K^* + K - 1) + 1.
\end{array}
$$

Then we show that $Q'' \oplus ((X' \oplus X) \dot\cup Y')$ is the $f(N)$-th LI of R when K satisfies $|\mathcal{D}(P)| > K$. At the beginning we have the followings

$$
\begin{aligned}
g(x) &= |\mathcal{D}\left(Q'' \oplus ((X' \oplus X \setminus x) \dot\cup (Y' \oplus Y \oplus Q))\right)| \\
&= (K^* + K - 1)(3K^* + K - 1) + 1 + 2K^*(3K^* + K - 1) - 1 \\
&= (3K^* + K - 1)^2 && (\forall x \in X) \\
g(y) &= |\mathcal{D}\left(Q'' \oplus ((X' \oplus X \oplus P) \dot\cup (Y' \oplus Y \setminus y))\right)| \\
&= (K^* + K - 1)(3K^* + K - 1) + 1 + (3K^* + |\mathcal{D}(P)| - 1)2K^* - 1 \\
&= (3K^* + K - 1)^2 + 2K^*(|\mathcal{D}(P)| - K) && (\forall y \in Y) \\
g(y') &< |\mathcal{D}\left(Q'' \oplus ((X' \oplus X \oplus P) \dot\cup Y')\right)| \\
&= (K^* + K - 1)(3K^* + K - 1) + 1 + (3K^* + |\mathcal{D}(P)| - 1)K^* - 1 \\
&= (2K^* + K - 1)(3K^* + K - 1) + (|\mathcal{D}(P)| - K)K^* && (\forall y' \in Y') \\
g(p) &\geq |\mathcal{D}\left(Q'' \oplus ((X' \oplus X) \dot\cup (Y' \oplus Y \oplus Q))\right)| \\
&= (K^* + K - 1)(3K^* + K - 1) + 1 + 3K^*(3K^* + K - 1) - 1 \\
&= (4K^* + K - 1)(3K^* + K - 1) && (\forall p \in P)
\end{aligned}
$$

and

$$
\begin{array}{rcl}
|\mathcal{D}(R'')| & = & (K^* + K - 1)(3K^* + K - 1) + (3K^* + |\mathcal{D}(P)| - 1)(3K^* + K - 1) \\
& & + \lfloor a^{-1}(3K^* + K - 1)^2 \rfloor - (3K^* + K - 1)^2 - (K^* + K - 1)(3K^* + K - 1) \\
& = & \lfloor a^{-c}(3K^* + K - 1)^{2c} \rfloor + (3K^* + |\mathcal{D}(P)| - 1)(3K^* + K - 1) - (3K^* + K - 1)^2 \\
& = & \lfloor a^{-c}(3K^* + K - 1)^{2c} \rfloor + (|\mathcal{D}(P)| - K)(3K^* + K - 1).
\end{array}
$$

Let $f(N) \stackrel{\text{def.}}{=} \lceil N^{1/c} \rceil$, then we have

$$
\begin{array}{rcl}
f(N) & \geq & a\left(a^{-c}(3K^* + K - 1)^{2c} - 1 + (|\mathcal{D}(P)| - K)(3K^* + K - 1)\right)^{1/c}, \text{ and} \\
f(N) & \leq & a\left(a^{-c}(3K^* + K - 1)^2 + (|\mathcal{D}(P)| - K)(3K^* + K - 1))\right)^{1/c} + 1.
\end{array}
$$

Now we show that $Q'' \oplus ((X' \oplus X) \dot\cup Y')$ is the $f(N)$-th LI of R when K satisfies $|\mathcal{D}(P)| < K \le 2^{|P|}$. From the definition, $Q'' \oplus ((X' \oplus X) \dot\cup Y')$ is the $f(N)$-th LI if $g(x) < f(N)$, $f(N) \le g(p)$, $g(y') < f(N)$, and $f(N) \le g(y)$ hold. It is not difficult to see that $g(p) \ge g(y)$ and $g(y') \le g(x)$ since $K^* \ge 2^{|P|} \ge |\mathcal{D}(P)|$. Thus the above conditions are satisfied if

$$(3K^* + K - 1)^2 < a\left(a^{-c}(3K^* + K - 1)^{2c} - 1 + (|\mathcal{D}(P)| - K)(3K^* + K - 1)\right)^{1/c}, \quad (14)$$

$$a\left(a^{-c}(3K^* + K - 1)^{2c} + (|\mathcal{D}(P)| - K)(3K^* + K - 1))\right)^{1/c} + 1 \le (3K^* + K - 1)^2 + 2K^*(|\mathcal{D}(P)| - K), \quad (15)$$

respectively. It is easy to see that (14) holds when $|\mathcal{D}(P)| > K$. For (15), with a transformation, it is enough to show

$$\left(1 + \frac{a^c(3K^* + K - 1)}{(3K^* + K - 1)^{2c}}(|\mathcal{D}(P)| - K)\right)\right)^{1/c} \le 1 + \frac{2K^* - 1}{(3K^* + K - 1)^2}(|\mathcal{D}(P)| - K). \quad (16)$$

It is not difficult to see that the inequality (16) holds if

$$\frac{a^c(3K^* + K - 1)}{(3K^* + K - 1)^{2c}} \le \frac{2K^* - 1}{(3K^* + K - 1)^2}. \quad (17)$$

For the inequality (17), with considering that $K^* \ge 2^{|P|} \ge K$ and $K^* \ge 2^{1/(c-1)}$,

$$\begin{aligned}
\frac{\text{(r.h.s.)}}{\text{(l.h.s.)}} &= \frac{(2K^* - 1)(3K^* + K - 1)^{2c}}{a^c(3K^* + K - 1)(3K^* + K - 1)^2} \\
&= \frac{2K^* - 1}{a^c(3K^* + K - 1)^{3-2c}} \\
&\ge \frac{2K^* - 1}{(3K^* + K - 1)^{3-2c}} \qquad \text{(since } 1 > a^c\text{)} \\
&\ge \frac{2K^* - 1}{(4K^* - 1)^{3-2c}} \qquad \text{(since } K^* \ge K\text{)} \\
&\ge \frac{2K^* - 1}{(4K^*)^{3-2c} - 1} \qquad \text{(since } 3 - 2c < 1\text{)} \\
&\ge \frac{2K^*}{(4K^*)^{3-2c}} \qquad \left(\text{this actually holds if } \frac{2K^*}{(4K^*)^{3-2c}} \ge 1\right) \\
&\ge \frac{2K^*}{4(K^*)^{3-2c}} \qquad \text{(since } 4 \ge 4^{3-2c}\text{)} \\
&\ge \frac{1}{2}(K^*)^{2c-2} \\
&\ge 1 \qquad \text{(since } K^* \ge 2^{1/(c-1)}\text{)},
\end{aligned}$$

hence we obtain (17), thus the inequality (15).

On the other hand, when $K \ge |\mathcal{D}(P)|$, clearly $g(y) \le g(x)$ holds, and it implies that $Q'' \oplus ((X' \oplus X) \dot\cup Y')$ is not a level ideal. Thus we search the maximum K satisfying that $Q'' \oplus ((X' \oplus X) \dot\cup Y')$ is the $f(N)$-th LI of R, according to a binary search strategy on K between $|P|$ and $2^{|P|}$, then eventually we find the maximum $K = |\mathcal{D}(P)| - 1$. □

D RAS for Counting Ideals by Using RAS for LI

In this section, we show that if we have a fully polynomial-time randomized approximation scheme (FPRAS) for finding the median stable matching, then we have an FPRAS for counting ideals of a poset. More precisely we assume the following oracle;

Oracle 3 (FPRAS for LI) *Given* ε $(0 < \varepsilon < 1)$*,* δ $(0 < \delta < 1)$*, and a poset* P*, oracle outputs an ideal* $S \in \mathcal{D}(P)$ *in time polynomial in* ε^{-1}*,* $\ln \delta^{-1}$ *and* $|P|$*, and* S *satisfies*

$$\Pr\left[S_{\lceil(1-\varepsilon)(N/2)\rceil} \subseteq S \subseteq S_{\lfloor(1+\varepsilon)(N/2)\rfloor}\right] \geq 1 - \delta$$

where $S_i \in \mathcal{F}(P)$ *denotes the* i*-th level ideal of* P*, and* $N = |\mathcal{D}(P)|$*.*

It is not difficult to see that Oracle 3 can be translated into a version of randomized approximation for finding the median stable matching.

Now we consider an FPRAS for counting ideals of a poset on the assumption of Oracle 3; given ε $(0 < \varepsilon < 1)$, δ $(0 < \delta < 1)$, and a poset P, we find an integer K which approximates $|\mathcal{D}(P)|$ satisfying

$$\Pr\left[(1-\varepsilon)|\mathcal{D}(P)| \leq K \leq (1+\varepsilon)|\mathcal{D}(P)|\right] \geq 1 - \delta \tag{18}$$

by using Oracle 3.

For an integer K $(1 \leq K \leq 2^{|P|})$, we define

$$\begin{aligned} R_1 &\stackrel{\text{def.}}{=} P \oplus \{x\} \oplus Q_1, \quad \text{and} \\ R_2 &\stackrel{\text{def.}}{=} Q_2 \oplus \{y\} \oplus P, \end{aligned}$$

where $|\mathcal{D}(Q_1)| = (1+\varepsilon/4)K$ and $|\mathcal{D}(Q_2)| = (1-\varepsilon/4)K$. Then we consider to find an integer K for which a pair of ideals $T_1 \in \mathcal{D}(R_1)$ and $T_2 \in \mathcal{D}(R_2)$ output by Oracle 3 satisfies $x \in T_1$ and $y \in T_2$ at the same instant. In the following, g_1 and g_2 denote the level functions (see (1), for definition) on R_1 and R_2, respectively. Then we have $g_1(x) = |\mathcal{D}(P)|$ and $g_2(y) = (1-\varepsilon/4)K$.

First, we show that if $K < (1-\varepsilon)|\mathcal{D}(P)|$, then Oracle 3 with an input $\varepsilon/32$, $\delta/(2|P|)$ and R_1, outputs an ideal $T_1 \in \mathcal{D}(R_1)$ and $\Pr[x \in T_1] < \delta/(2|P|)$. For $N_1 = |\mathcal{D}(R_1)| = |\mathcal{D}(P)| + (1+\varepsilon/4)K$, let $f_1^+(N_1) \stackrel{\text{def.}}{=} (1+\varepsilon/32)(N_1/2)$, then

$$\begin{aligned} f_1^+(N_1) &= (1+\varepsilon/32)(N_1/2) \\ &= (1+\varepsilon/32)(|\mathcal{D}(P)| + (1+\varepsilon/4)K)/2 \\ &\leq (1+\varepsilon/32)(|\mathcal{D}(P)| + (1+\varepsilon/4)(1-\varepsilon)|\mathcal{D}(P)|)/2 \\ &\leq (1+\varepsilon/32)(|\mathcal{D}(P)| + (1-3\varepsilon/4)|\mathcal{D}(P)|)/2 \\ &= (1+\varepsilon/32)(1-3\varepsilon/8)|\mathcal{D}(P)| \\ &\leq (1-11\varepsilon/32)|\mathcal{D}(P)| \\ &\leq |\mathcal{D}(P)|. \end{aligned}$$

This implies that if $K < (1-\varepsilon)|\mathcal{D}(P)|$, then $g_1(x) \geq f_1^+(N)$, and hence $x \notin S_{\lfloor f_1^+(N_1)\rfloor}$. Thus we have $\Pr[x \in T_1] \leq \delta/(2|P|)$ from the assumption of Oracle 3.

Next, we show that if $K > (1+\varepsilon)|\mathcal{D}(P)|$, then Oracle 3 with an input $\varepsilon/32$, $\delta/(2|P|)$ and R_2, outputs an ideal $T_2 \in \mathcal{D}(R_2)$ and $\Pr[y \in T_2] < \delta/(2|P|)$. For $N_2 = |\mathcal{D}(R_2)| = (1-\varepsilon/4)K + |\mathcal{D}(P)|)$, let $f_2^+(N_2) \stackrel{\text{def.}}{=} (1-\varepsilon/32)(N_2/2)$. With considering that if $(1+\varepsilon)|\mathcal{D}(P)| < K$ then $|\mathcal{D}(P)| < (1+\varepsilon)^{-1}K < (1-\varepsilon/2)K$, we have

$$\begin{aligned} f_2^+(N) &= (1+\varepsilon/8)(N_2/2) \\ &= (1+\varepsilon/8)((1-\varepsilon/4)K + |\mathcal{D}(P)|)/2 \\ &\leq (1+\varepsilon/8)((1-\varepsilon/4)K + (1-\varepsilon/2)K)/2 \\ &= (1+\varepsilon/8)(1-3\varepsilon/8)K \\ &\leq (1-\varepsilon/4)K. \end{aligned}$$

This implies that if $K > (1+\varepsilon)|\mathcal{D}(P)|$, then $g_2(y) \geq f_2^+(N_2)$, and hence $y \notin S_{\lfloor f_2^+(N_2)\rfloor}$. Thus we have $\Pr[y \in T_2] \leq \delta/(2|P|)$ from the assumption of Oracle 3.

From the above discussions, if we find an integer K for which a pair of ideals $T_1 \in \mathcal{D}(R_1)$ and $T_2 \in \mathcal{D}(R_2)$ output by Oracle 3 satisfies $x \in T_1$ and $y \in T_2$, then K satisfies $(1-\varepsilon)|\mathcal{D}(P)| \leq K \leq (1+\varepsilon)|\mathcal{D}(P)|$ with a high probability.

Now we discuss we can certainly find such an integer K that $x \in T_1$ ($T_1 \in \mathcal{D}(R_1)$) and $y \in T_2$ ($T_2 \in \mathcal{D}(R_2)$) with a high probability. We show that if $K \geq (1-\varepsilon/8)|\mathcal{D}(P)|$, then Oracle 3 with an input $\varepsilon/32$, $\delta/(2|P|)$ and R_1, outputs an ideal $T_1 \in \mathcal{D}(R_1)$ and $\Pr[x \notin T_1] < \delta/(2|P|)$. For $N_1 = |\mathcal{D}(R_1)| = |\mathcal{D}(P)| + (1+\varepsilon/4)K$, let $f_1^-(N_1) \stackrel{\text{def.}}{=} (1-\varepsilon/32)(N_1/2)$, then

$$
\begin{aligned}
f_1^-(N_1) &= (1-\varepsilon/32)(N_1/2) \\
&= (1-\varepsilon/32)(|\mathcal{D}(P)| + (1+\varepsilon/4)K)/2 \\
&> (1-\varepsilon/32)(|\mathcal{D}(P)| + (1+\varepsilon/4)(1-\varepsilon/8)|\mathcal{D}(P)|)/2 \\
&> (1-\varepsilon/32)(|\mathcal{D}(P)| + (1+3\varepsilon/32)|\mathcal{D}(P)|)/2 \\
&= (1-\varepsilon/32)(1+3\varepsilon/64)|\mathcal{D}(P)| \\
&> (1+(\varepsilon-\varepsilon^2)/64)|\mathcal{D}(P)| \\
&> |\mathcal{D}(P)|.
\end{aligned}
$$

This implies that if $K \geq (1-\varepsilon/8)|\mathcal{D}(P)|$, then $g_1(x) < f_1^-(N)$, and hence $x \in S_{\lceil f_1^-(N_1)\rceil}$. Thus we have $\Pr[x \notin T_1] \leq \delta/(2|P|)$ from the assumption of Oracle 3.

Next we show that if $K \leq (1+\varepsilon/8)|\mathcal{D}(P)|$, then Oracle 3 with an input $\varepsilon/32$, $\delta/(2|P|)$ and R_2, outputs an ideal $T_2 \in \mathcal{D}(R_2)$ and $\Pr[x \notin T_2] < \delta/(2|P|)$. For $N_2 = |\mathcal{D}(R_2)| = (1-\varepsilon/4)K + |\mathcal{D}(P)|$, let $f_2^-(N_2) \stackrel{\text{def.}}{=} (1-\varepsilon/32)(N_2/2)$. With considering that if $(1+\varepsilon/8)|\mathcal{D}(P)| \leq K$ then $|\mathcal{D}(P)| > (1+\varepsilon/8)^{-1}K > (1-\varepsilon/8)K$, we have

$$
\begin{aligned}
f_2^-(N) &= (1-\varepsilon/32)(N/2) \\
&= (1-\varepsilon/32)((1-\varepsilon/4)K + |\mathcal{D}(P)|)/2 \\
&> (1-\varepsilon/32)((1-\varepsilon/4)K + (1-\varepsilon/8)K)/2 \\
&= (1-\varepsilon/32)(1-3\varepsilon/16)K \\
&> (1-7\varepsilon/32)K \\
&> (1-\varepsilon/4)K.
\end{aligned}
$$

This implies that if $K \leq (1+\varepsilon/8)|\mathcal{D}(P)|$, then $g_2(y) < f_2^-(N)$, and hence $y \in S_{\lceil f_2^-(N_2)\rceil}$. Thus we have $\Pr[y \notin T_2] \leq \delta/(2|P|)$ from the assumption of Oracle 3.

From the above discussions, we can find an integer K for which a pair of ideals $T_1 \in \mathcal{D}(R_1)$ and $T_2 \in \mathcal{D}(R_2)$ output by Oracle 3 satisfies $x \in T_1$ and $y \in T_2$ with a high probability. Finally, we can find desired K after at most $|P|$ iterations according to a binary search strategy on K between 1 and $2^{|P|}$, and the probability to find such K is at least $1 - 2 \cdot |P| \cdot \delta/(2|P|) = 1 - \delta$.