

Shortest $(A + B)$ -Path Packing Via Hafnian

Hiroshi Hirai¹ · Hiroyuki Namba¹

Received: 14 July 2016 / Accepted: 7 June 2017 / Published online: 14 June 2017
© Springer Science+Business Media, LLC 2017

Abstract Björklund and Husfeldt developed a randomized polynomial time algorithm to solve the shortest two disjoint paths problem. Their algorithm is based on computation of permanents modulo 4 and the isolation lemma. In this paper, we consider the following generalization of the shortest two disjoint paths problem, and develop a similar algebraic algorithm. The shortest perfect $(A + B)$ -path packing problem is: given an undirected graph G and two disjoint node subsets A, B with even cardinalities, find shortest $|A|/2 + |B|/2$ disjoint paths whose ends are both in A or both in B . Besides its NP-hardness, we prove that this problem can be solved in randomized polynomial time if $|A| + |B|$ is fixed. Our algorithm basically follows the framework of Björklund and Husfeldt but uses a new technique: computation of hafnian modulo 2^k combined with Gallai’s reduction from T -paths to matchings. We also generalize our technique for solving other path packing problems, and discuss its limitation.

Keywords Shortest disjoint paths problem · Hafnian · Randomized polynomial time algorithm

1 Introduction

The shortest two disjoint paths problem is: given an undirected graph $G = (V, E)$ and $s_1, t_1, s_2, t_2 \in V$, find two disjoint paths, one connecting s_1 and t_1 and the other

✉ Hiroshi Hirai
hirai@mist.i.u-tokyo.ac.jp
Hiroyuki Namba
hiroyukinamba@gmail.com

¹ Department of Mathematical Informatics, Graduate School of Information Science and Technology, The University of Tokyo, Tokyo 113-8656, Japan

connecting s_2 and t_2 , such that the sum of their lengths is minimum. Although the length-less version, the two disjoint paths problem, is elegantly solved [12–14], no polynomial time algorithm was known for this generalization. Recently, Björklund and Husfeldt [2] obtained the first polynomial time algorithm.

Theorem 1.1 [2] *There exists a randomized polynomial time algorithm to solve the shortest two disjoint paths problem.*

Their algorithm is build on striking application of computation of permanents modulo 4 by Valiant [15] and the isolation lemma by Mulmuley–Vazirani–Vazirani [9].

In this paper, we consider a generalization of the shortest two disjoint paths problem and develop a randomized polynomial time algorithm based on a similar algebraic technique. Let us introduce our problem. For $T \subseteq V$, a T -path is a path connecting distinct nodes in T . We are given two disjoint terminal sets A and B with even cardinalities. A *perfect $(A+B)$ -path packing* is a set \mathcal{P} of node-disjoint paths such that each path is an A -path or B -path and $|\mathcal{P}| = |A|/2 + |B|/2$. The *size* of a perfect $(A + B)$ -path packing is defined as the total sum of the length of each path, where the length of a path is defined as the number of edges in the path. The *shortest perfect $(A + B)$ -path packing problem* asks to find a perfect $(A + B)$ -path packing with minimum size. It will turn out that this problem is NP-hard. In the case where $|A| = |B| = 2$, the problem is the shortest two disjoint paths problem above. When B is empty, the problem is the disjoint A -path problem by Gallai [4]. Our main result says that the problem is tractable, provided $|A| + |B|$ is fixed.

Theorem 1.2 *There exists a randomized algorithm to solve the shortest perfect $(A + B)$ -path packing problem in $O(f(|V|)^{|A|+|B|})$ time, where f is a polynomial.*

Our algorithm basically follows the framework of Björklund–Husfeldt [2] but we use a new technique: computation of hafnian modulo 2^k , instead of permanent modulo 4, combined with a classical reduction technique to matching by Gallai (for T -paths) [4] and Edmonds (for odd path); see [11, Section 29.11e].

Related work Colin de Verdière–Schrijver [3] and Kobayashi–Sommer [7] gave combinatorial polynomial time algorithms for shortest disjoint paths problems in planar graphs with special terminal configurations. Karzanov [6] and Hirai–Pap [5] showed the polynomial time solvability of a shortest version of edge-disjoint T -paths problem. Yamaguchi [16] reduced the shortest disjoint \mathcal{S} -paths problem (nonzero T -paths problem in a group labeled graph, more generally) to weighted matroid matching. Kobayashi–Toyooka [8] developed a randomized polynomial time algorithm for the shortest nonzero (s, t) -path problem in a group labeled graph; their algorithm is also based on the framework of Björklund–Husfeldt.

It is well-known that the hafnian of the adjacency matrix of a graph is equal to the number of perfect matchings. By utilizing the hafnian, Björklund [1] developed a faster algorithm to count the number of perfect matchings.

Organization The rest of this paper is organized as follows. In Sect. 2, we first show that hafnian modulo 2^k for fixed k is computable in polynomial time. This direct

generalization of permanent computation modulo 2^k seems new and interesting in its own right. Next we present the randomized algorithm in Theorem 1.2. In Sect. 3, we verify the hardness of the $(A + B)$ -path packing problem, and then generalize our technique for solving other path packing problems, and discuss its limitation.

2 Algorithm

In this section, we first provide an algorithm to compute hafnian modulo 2^k , and next present a randomized polynomial time algorithm to solve the shortest perfect $(A + B)$ -path packing problem for fixed $|A| + |B|$. An undirected pair or edge $\{i, j\}$ is simply denoted by ij .

2.1 Computing Hafnian Modulo 2^k

The hafnian $\text{haf } A$ of a $2n \times 2n$ symmetric matrix $A = (a_{ij})$ is defined by

$$\text{haf } A := \sum_{M \in \mathcal{M}} \prod_{ij \in M} a_{ij},$$

where \mathcal{M} is the set of all partitions of $\{1, 2, 3, \dots, 2n\}$ into n pairs.

Let $\mathcal{S}(n, N)$ denote the set of all $2n \times 2n$ symmetric matrices with zero diagonal each of whose element is a univariate polynomial of degree at most N . Let $\text{haf}_{2^k} A$ denote the hafnian of A modulo 2^k . The main result of this subsection is the following:

Theorem 2.1 *There exists a bivariate polynomial f such that for all $A \in \mathcal{S}(n, N)$, $\text{haf}_{2^k} A$ can be computed in $O(f(n, N)^k)$ time.*

We prove Theorem 2.1 by the similar way to that for permanents modulo 2^k [15] and that for permanents of polynomial matrices modulo 2^k [2,8]. First we verify Theorem 2.1 for $k = 1$. Let $\tilde{A} = (\tilde{a}_{ij})$ be a skew-symmetric matrix obtained from A by replacing a_{ij} by $-a_{ij}$ if $i > j$. Modulo 2, $\text{haf } A$ coincides with $\text{pf } \tilde{A}$ (Pfaffian of \tilde{A}). Hence $\text{haf}_2 A$ can be obtained in time polynomial in n and N by computing $\sqrt{\det \tilde{A}} \pmod{2}$.

Next, we consider the case of $k \geq 2$. We use a formula like the Laplace expansion of determinants. Let $A[i, j]$ denote the matrix obtained from A by removing the row i , row j , column i , and column j . For distinct i, j, p, q , let $A[i, j, p, q] := (A[i, j])[p, q]$.

Lemma 2.2 (1) $\text{haf } A = \sum_{j: j \neq i} a_{ij} \text{haf } A[i, j]$.

(2) $\text{haf } A = a_{ij} \text{haf } A[i, j] + \sum_{pq: p, q \notin \{i, j\}, p \neq q} (a_{ip}a_{jq} + a_{iq}a_{jp}) \text{haf } A[i, j, p, q]$.

Proof (1) For $j \neq i$, let \mathcal{M}_j be the set of all $M \in \mathcal{M}$ that contain ij . Since $\{\mathcal{M}_j \mid j \neq i\}$ is a partition of \mathcal{M} , we obtain

$$\text{haf } A := \sum_{j: j \neq i} a_{ij} \sum_{M \in \mathcal{M}_j} \prod_{pq \in M \setminus \{ij\}} a_{pq} = \sum_{j: j \neq i} a_{ij} \text{haf } A[i, j].$$

(2) By using (1) repeatedly, we obtain

$$\begin{aligned} \text{haf } A &= \sum_{p: p \neq i} a_{ip} \text{ haf } A[i, p] = a_{ij} \text{ haf } A[i, j] + \sum_{p: p \notin \{i, j\}} a_{ip} \text{ haf } A[i, p] \\ &= a_{ij} \text{ haf } A[i, j] + \sum_{p: p \notin \{i, j\}} a_{ip} \sum_{q: q \notin \{i, j, p\}} a_{jq} \text{ haf } A[i, j, p, q] \\ &= a_{ij} \text{ haf } A[i, j] + \sum_{(p, q): p, q \notin \{i, j\}, p \neq q} a_{ip} a_{jq} \text{ haf } A[i, j, p, q]. \end{aligned}$$

Combining the terms for (p, q) and (q, p) , we obtain (2). □

For $A \in \mathcal{S}(n, N)$, let $A(i, j; c)$ denote the matrix obtained from A by adding c multiple of column i to column j , adding c multiple of row i to row j , and replacing the jj th element with zero. We refer to this operation as the $(i, j; c)$ -operation. Note that differences between A and $A(i, j; c)$ occur only in row j and column j , and that $A(i, j; c)$ also belongs to $\mathcal{S}(n, N)$. We investigate how the hafnian changes by the $(i, j; c)$ -operation. Let $A(i \rightarrow j)$ denote the matrix obtained from A by replacing row j with row i and column j with column i .

Lemma 2.3 $\text{haf } A(i, j; c) = \text{haf } A + c \text{ haf } A(i \rightarrow j)$.

Proof Let \tilde{a}_{pq} denote the pq th element of $A(i, j; c)$. We use Lemma 2.2 (1) with respect to row j and column j .

$$\begin{aligned} \text{haf } A(i, j; c) &= \sum_{k: k \neq j} \tilde{a}_{kj} \text{ haf } A[k, j] \\ &= \sum_{k: k \neq j} a_{kj} \text{ haf } A[k, j] + \sum_{k: k \neq j} ca_{ki} \text{ haf } A[k, j] \\ &= \text{haf } A + c \text{ haf } A(i \rightarrow j). \end{aligned}$$

Let d be a fixed positive integer. A term of a polynomial is said to be *lower* if its degree is at most d and *higher* otherwise. A polynomial f is said to be *even* if all coefficients of lower terms of the polynomial $f(x)$ are even. For a polynomial $f(x)$ that is not even, let $m(f(x))$ denote the lowest degree of terms with odd coefficients.

Let $A = (a_{ij}) \in \mathcal{S}(n, d)$. We are going to show that all lower terms of $\text{haf } A$ modulo 2^k can be computed in time polynomial in n and d . The hafnian does not change if we exchange row i and row j , and column i and column j . Hence we exchange rows and columns of A in advance so that a_{12} is a minimizer of $m(a_{1j})$ in a_{1j} ($j = 2, \dots, 2n$) that are not even. Next we find a polynomial c_j such that $c_j a_{12} + a_{1j}$ is even for $j = 3, \dots, 2n$. The computation can easily be done in time polynomial in n and d [2, Section 3.2]. Using the $(2, j; c_j)$ -operation for $j = 3, \dots, 2n$ in order, we obtain matrices $A_3 := A(2, 3; c_3)$, $A_4 := A_3(2, 4; c_4)$, \dots , $A_{2n} := A_{2n-1}(2, 2n; c_{2n})$. Then $1j$ elements of A_{2n} are even if $j \geq 3$. Applying Lemma 2.3 repeatedly, we obtain

$$\text{haf } A_{2n} = \text{haf } A + \sum_{j=3}^{2n} c_j \text{ haf } A_{j-1}(2 \rightarrow j),$$

where $A_2 = A$. Using Lemma 2.2 (1) for $A_{2n} = (b_{ij})$, we obtain

$$\text{haf } A = b_{12} \text{ haf } A_{2n}[1, 2] + \sum_{j=3}^{2n} b_{1j} \text{ haf } A_{2n}[1, j] - \sum_{j=3}^{2n} c_j \text{ haf } A_{j-1}(2 \rightarrow j). \quad (1)$$

Though there may be higher terms in elements of matrices in (1), we may replace these higher terms with 0 (since our goal is computing lower terms). Similarly we may replace higher terms in b_{1j} ($j = 2, \dots, 2n$) with 0. Hence all matrices in right-hand side of (1) can be regarded in $\mathcal{S}(n - 1, d)$ or $\mathcal{S}(n, d)$.

Next we discuss the second and third terms of the right-hand side in detail. For the second term, we obtain $b_{1j} \text{ haf } A_{2n}[1, j]$ modulo 2^k from $\text{haf } A_{2n}[1, j]$ modulo 2^{k-1} since b_{1j} ($3 \leq j \leq 2n$) are even. Therefore we need to compute hafnians of $2n - 2$ polynomial matrices in $\mathcal{S}(n - 1, d)$ modulo 2^{k-1} .

Next we consider the third term. For $A(i \rightarrow j)$, it holds $a_{ip} = a_{jp}$, $a_{iq} = a_{jq}$ and $a_{ij} = 0$ (since A has zero diagonals). Hence, applying Lemma 2.2 (2) to $A(i \rightarrow j)$, we obtain the following:

$$\text{haf } A(i \rightarrow j) = \sum_{p,q} 2a_{ip}a_{jq} \text{ haf } A[i, j, p, q].$$

Hence we obtain $\text{haf } A(i \rightarrow j)$ modulo 2^k from hafnians of $\binom{2n-2}{2}$ matrices in $\mathcal{S}(n - 2, d)$ modulo 2^{k-1} .

In this way, our algorithm recursively computes lower terms of $\text{haf } A$ modulo 2^k according to (1). We are now ready to prove Theorem 2.1.

Proof of Theorem 2.1 Let $T(n, d, k)$ be the computational complexity of computing all lower terms of the hafnian of a matrix in $\mathcal{S}(n, d)$. From (1) and the argument after (1), it follows

$$T(n, d, k) \leq T(n - 1, d, k) + (2n - 2)T(n - 1, d, k - 1) + (2n - 2) \binom{2n - 2}{2} T(n - 2, d, k - 1) + \text{poly}(n, d),$$

where $\text{poly}(n, d)$ is a polynomial of n and d . Since $T(n, d, k)$ is monotone increasing on n , it follows that

$$T(n, d, k) \leq T(n - 1, d, k) + 4n^3 T(n, d, k - 1) + \text{poly}(n, d).$$

Using this inequality repeatedly, we obtain

$$T(n, d, k) \leq 4n^4 T(n, d, k - 1) + \text{poly}(n, d).$$

$T(n, d, 1)$ is a polynomial of n and d by the result of the case $k = 1$. Hence there exists a polynomial f of n and d such that for all positive integers k , $T(n, d, k)$ is $O(f(n, d)^k)$.

For $A \in \mathcal{S}(n, N)$, the degree of $\text{haf } A$ is at most nN . Apply the above algorithm with $d = nN$, we obtain $\text{haf}_{2^k} A$ in $O(f(n, nN)^k)$ time. This completes the proof. \square

2.2 Perfect $(A + B)$ -Path Packing via Hafnian

Let $G = (V, E)$ be a simple undirected graph and A, B disjoint node sets of even cardinalities. Let $n := |V|$ and $m := |E|$. We can assume that $G = (V, E)$ has no edge with both endpoints in $A \cup B$; otherwise, replace each edge by a series of two edges. We consider a general case where G has positive integer weight $w(e)$ on each edge e . We assume that the maximum value of the weight is bounded by a polynomial of n . For a path P , let $w(P)$ denote the sum of the weight of edges in P . The size of a set \mathcal{P} of vertex-disjoint paths is defined as the total sum of $w(P)$ over $P \in \mathcal{P}$, and is denoted by $w(\mathcal{P})$.

Gallai’s construction From input G, A, B , we construct graph $H = (V_H, E_H)$ so that matchings in H correspond to disjoint T -paths in G (with $T = A \cup B$). This construction is due to Gallai [4]; see [11, Section 73.1]. Let $U := V \setminus (A \cup B)$. First we add to G a copy of the subgraph of G induced by U . The copy of a node $v \in U$ is denoted by v' . Let $U' := \{v' \mid v \in U\}$, $V_H := V \cup U' = A \cup B \cup U \cup U'$. Next, for each $v \in U$, add an edge vv' . The set of such edges is denoted by E_+ . Finally, we add edge uv' for each $uv \in E$ with $u \in A \cup B, v \in U$. The set of all edges in $A \cup B \cup U'$ is denoted by E' . Let $E_H := E \cup E' \cup E_+$. The weight w is extended to $E_H \rightarrow \mathbb{Z}_{\geq 0}$ by

$$\begin{cases} w(e) := 0 & \text{if } e \in E_+, \\ w(uv') := w(uv) & \text{if } uv' \in E', u \in A \cup B, \\ w(u'v') := w(uv) & \text{if } u'v' \in E', u', v' \in U'. \end{cases}$$

A *perfect $(A \cup B)$ -path packing* is a set of $|A|/2 + |B|/2$ node-disjoint $(A \cup B)$ -paths. From a perfect matching M of H , we obtain a perfect $(A \cup B)$ -path packing \mathcal{P}_M in G as follows. For all $s \in A \cup B$, there exists a unique path $P = \{s, v_1, v_2, \dots, t\}$ in H such that $(s, v_1) \in M, t \in (A \cup B) \setminus \{s\}$ and it goes through edges in M and edges in E_+ alternately. This path in H determines an (s, t) -path in G by picking up the only nodes in $(A \cup B) \cup U$ in the same order. Gathering up these paths, we obtain a perfect $(A \cup B)$ -path packing \mathcal{P}_M in G . Conversely, one can see that any perfect $(A \cup B)$ -path packing in G is obtained in this way. The size of \mathcal{P}_M is at most the weight of M . They coincide if and only if all edges of M not used by \mathcal{P}_M belong to E_+ .

Matrices S and S' Next we introduce a symmetric matrix S associated with H . Let $h := |V_H|$. We can assume that $V_H = \{1, 2, \dots, h\}$. Let $S = (s_{ij})$ be an $h \times h$ symmetric matrix defined by

$$s_{ij} := \begin{cases} x^{w(ij)} & \text{if } ij \in E_H, \\ 0 & \text{otherwise.} \end{cases}$$

Recall that $w(ij)$ denotes the weight of the edge ij in H .

For $t \in A \cup B$, let E_t denote the set of edges joining t and U , and let E'_t denote the set of edges joining t and U' . From the matrix S , we define a new matrix $S' = (s'_{ij})$ by

$$s'_{ij} := \begin{cases} -s_{ij} & \text{if } ij \in E'_t \text{ for some } t \in B, \\ s_{ij} & \text{otherwise.} \end{cases}$$

Let $\tau := (|A| + |B|)/2$. For a perfect $(A + B)$ -path packing \mathcal{P} , let $\theta(\mathcal{P})$ denote the number of even-length B -paths in \mathcal{P} .

Lemma 2.4

$$\text{haf } S' = \sum_{\mathcal{P}} (-1)^{\theta(\mathcal{P})} 2^\tau x^{w(\mathcal{P})} (1 + x f_{\mathcal{P}}(x)),$$

where \mathcal{P} ranges over all perfect $(A + B)$ -path packings, and $f_{\mathcal{P}}(x)$ is a polynomial.

Proof For a matching M of H , let $s'(M) := \prod_{ij \in M} s'_{ij}$. By the above discussion on Gallai’s construction, we obtain

$$\text{haf } S' = \sum_M s'(M) = \sum_{\mathcal{P}} \sum_{M: \mathcal{P}_M = \mathcal{P}} s'(M), \tag{2}$$

where M ranges over all perfect matchings in H and \mathcal{P} ranges over all perfect $(A \cup B)$ -path packings in G . First we estimate $\sum_{M: \mathcal{P}_M = \mathcal{P}} s'(M)$. Suppose $\mathcal{P} = \{P_1, \dots, P_\tau\}$. For each path $P_k = (s_k, v_1, v_2, \dots, v_{n_k}, t_k)$ ($k = 1, \dots, \tau$), we define two matchings $M_{k,1}, M_{k,2}$ in H by

$$M_{k,1} = \begin{cases} \{s_k v_1, v'_1 v'_2, \dots, v_{n_k-1} v_{n_k}, v'_{n_k} t_k\} & \text{if } n_k \text{ is odd,} \\ \{s_k v_1, v'_1 v'_2, \dots, v'_{n_k-1} v'_{n_k}, v_{n_k} t_k\} & \text{if } n_k \text{ is even,} \end{cases}$$

$$M_{k,2} = \begin{cases} \{s_k v'_1, v_1 v_2, \dots, v'_{n_k-1} v'_{n_k}, v_{n_k} t_k\} & \text{if } n_k \text{ is odd,} \\ \{s_k v'_1, v_1 v_2, \dots, v_{n_k-1} v_{n_k}, v'_{n_k} t_k\} & \text{if } n_k \text{ is even.} \end{cases}$$

Both of them have weight $w(P_k)$. Then a perfect matching M with $\mathcal{P}_M = \mathcal{P}$ can be represented as the union of $\bigcup_{k=1}^\tau M_{k,i_k}$ ($i_k \in \{1, 2\}$) and a perfect matching M' of the subgraph $H - \mathcal{P}$ of H obtained by removing vertices in $\bigcup_{k=1}^\tau M_{k,i_k}$. Then we obtain

$$\begin{aligned} \sum_{M: \mathcal{P}_M = \mathcal{P}} s'(M) &= \sum_{i_1 \in \{1,2\}} \dots \sum_{i_\tau \in \{1,2\}} \sum_{M'} s'(M_{1,i_1}) \dots s'(M_{\tau,i_\tau}) s'(M') \\ &= (s'(M_{1,1}) + s'(M_{1,2})) \dots (s'(M_{\tau,1}) + s'(M_{\tau,2})) \sum_{M'} s'(M'), \end{aligned} \tag{3}$$

where M' ranges over all perfect matchings of $H - \mathcal{P}$.

Next we estimate $s'(M_{k,1}) + s'(M_{k,2})$. We call an edge in E'_t for $t \in B$ minus. Then $s'(M_{k,j}) = x^{w(P_k)}$ if $M_{k,j}$ has an even number of minus edges, and $s'(M_{k,j}) = -x^{w(P_k)}$ if $M_{k,j}$ has an odd number of minus edges. If P_k connects A and B , just one of $M_{k,1}$ and $M_{k,2}$ contains one minus edge. If P_k is an A -path, then neither $M_{k,1}$ nor

$M_{k,2}$ contains one minus edge. If P_k is a B -path and the length of P_k is odd, one of $M_{k,1}$ and $M_{k,2}$ has two minus edges and the other has no minus edge. If P_k is a B -path and the length of P_k is even, both of $M_{k,1}$ and $M_{k,2}$ have one minus edge. (Recall the assumption that there is no edge joining $A \cup B$.) Hence we obtain

$$s'(M_{k,1}) + s'(M_{k,2}) = \begin{cases} 0 & \text{if } P_k \text{ connects } A \text{ and } B, \\ -2x^{w(P_k)} & \text{if } P_k \text{ is an even-length } B\text{-path,} \\ 2x^{w(P_k)} & \text{otherwise.} \end{cases} \quad (4)$$

Finally we estimate $\sum_{M'} s'(M')$. The perfect matching consisting of edges in E_- has weight 0, and other perfect matchings have weight at least 1. Thus $\sum_{M'} s'(M')$ is represented as $1 + xf(x)$ for a polynomial f . By this fact and equations (2), (3) and (4), we obtain the formula. \square

Unique Optimal Solution Case. We first consider the case where G has a unique shortest perfect $(A + B)$ -path packing \mathcal{P}^* . Here w is not necessarily uniform (but is bounded by a polynomial of n). In this case, Lemma 2.4 immediately yields a desired algorithm to find \mathcal{P}^* . Indeed, the leading term (lowest degree term) of $\text{haf } S'$ is $(-1)^{\theta(\mathcal{P}^*)} 2^\tau x^{w(\mathcal{P}^*)}$ (by the uniqueness). In particular we can obtain the minimum degree $w(\mathcal{P}^*)$ by computing $\text{haf } S'$ modulo $2^{\tau+1}$. Observe that an edge e belongs to \mathcal{P}^* if and only if the degree of the leading term of $\text{haf } S'$ strictly increases when e is removed from G . Thus we can determine \mathcal{P}^* by $m + 1$ computations of the hafnian of a $2n \times 2n$ matrix in modulo $2^{\tau+1}$. By Theorem 2.1 (with $N = \text{maximum of } w$), this can be done in $O(f(n)^{|A|+|B|})$ time for a polynomial f .

General Case. Suppose now that w is uniform weight, i.e., $w(e) = 1$ for all e in E . We consider the general case where there may be two or more shortest perfect $(A + B)$ -path packings. We construct a randomized polynomial time algorithm with the help of the isolation lemma [9]. This technique is due to [2]. We use the isolation lemma in the following form:

Lemma 2.5 *Let n be a positive integer and \mathcal{F} a family of subsets of $E = \{e_1, \dots, e_m\}$. Weight $w(e_i)$ is assigned to each element e_i of E , where $w(e_i)$ are chosen independently and uniformly at random from $\{2mn, 2mn + 1, \dots, 2mn + 2m - 1\}$. Then, with probability greater than $1/2$, there exists a unique set $F \in \mathcal{F}$ of minimum weight $w(F) := \sum_{e \in F} w(e)$.*

We are ready to prove our main theorem.

Proof of Theorem 1.2 We perturb the weight w into w' so that a shortest packing for w' is unique and is also shortest for w . For each edge e , choose a from $\{2mn, \dots, 2mn + 2m - 1\}$ independently and uniformly at random, and let $w'(e) := a$. By Lemma 2.5, with a high probability ($\geq 1/2$), a shortest $(A + B)$ -path packing \mathcal{P}^* for w' is unique. By the unique optimal solution case above, we can find \mathcal{P}^* in $O(f(n)^{|A|+|B|})$ time. We finally verify that \mathcal{P}^* is actually shortest for the original uniform weight w . Indeed, pick an arbitrary packing \mathcal{P} not equal to \mathcal{P}^* . Then we have

$$\begin{aligned} 1 \leq w'(\mathcal{P}) - w'(\mathcal{P}^*) &\leq (2mn + 2m - 1)w(\mathcal{P}) - 2mnw(\mathcal{P}^*) \\ &\leq 2mn(w(\mathcal{P}) - w(\mathcal{P}^*)) + (2m - 1)w(\mathcal{P}). \end{aligned}$$

Hence we have

$$w(\mathcal{P}) - w(\mathcal{P}^*) \geq \frac{1}{2mn} - \frac{(2m - 1)w(\mathcal{P})}{2mn} \geq -1 + \frac{1 + w(\mathcal{P})}{2mn} > -1,$$

where the second inequality follows from $w(\mathcal{P}) \leq n$. Since both $w(\mathcal{P})$ and $w(\mathcal{P}^*)$ are integers, we have $w(\mathcal{P}) - w(\mathcal{P}^*) \geq 0$. This means that \mathcal{P}^* is shortest for w . \square

3 Related Results

3.1 NP-Completeness

Here we verify that the perfect $(A + B)$ -path packing problem, the problem of deciding the existence of a perfect $(A + B)$ -path packing (with $|A| + |B|$ unfixed), is intractable.

Theorem 3.1 *The perfect $(A + B)$ -path packing problem is NP-complete, even if $|B| = 2$.*

Proof Hirai and Pap [5] proved that the following edge-disjoint paths problem is NP-complete: (*) Given an undirected graph $G = (V, E)$ and $S, T \subseteq V$ with $S \cap T = \emptyset$ and $|S| = |T| = k$ and $a, b \in V \setminus (S \cup T)$, find an edge-disjoint set \mathcal{P} of paths P_0, P_1, \dots, P_k such that P_0 connects a and b and P_i connects S and T ($i = 1, 2, \dots, k$). They gave a reduction from 3-SAT to the problem (*). In their reduction [5, Section 5.2.3], a solution is necessarily vertex-disjoint. Moreover, one can see from the reduction that a set \mathcal{P} of paths is a solution of (*) if and only if \mathcal{P} is a perfect $(S \cup T + \{a, b\})$ -path packing. Consequently the perfect $(A + B)$ -path packing problem is also NP-complete, even if $|B| = 2$. \square

3.2 Other Path Packing Via Hafnian

In this subsection, we generalize our technique for solving other path packing problems and discuss its limitation. Let $G = (V, E)$ be a simple undirected graph. Let T be a terminal set with even cardinality $|T| = 2\tau$. As in Sect. 2.2, we assume that there is no edge joining T .

To specify path packing problems, we introduce a notion of *perfect matching with parity (PMP)* on T , which is defined as a set of pairs $(s_i t_i, \sigma_i)$ ($i = 1, \dots, \tau$) such that $\bigcup_i \{s_i, t_i\} = T$ and $\sigma_i \in \{\text{odd}, \text{even}\}$ is a parity. A perfect T -path packing \mathcal{P} (a disjoint set of τ T -paths) induces PMP $M_{\mathcal{P}}$:

$$M_{\mathcal{P}} := \{(st, \sigma) \mid \mathcal{P} \text{ has an } (s, t)\text{-path with its length having the parity } \sigma\}.$$

For a set \mathcal{M} of PMPs, a *perfect \mathcal{M} -path packing* is a perfect T -path packing with $M_{\mathcal{P}} \in \mathcal{M}$. We introduce *the shortest perfect \mathcal{M} -path packing problem* as the problem

of finding a perfect \mathcal{M} -path packing of minimum size. Notice that an $(A + B)$ -path packing corresponds to $\mathcal{M}_{A+B} := \{M \cup M' \mid M : \text{PMP on } A, M' : \text{PMP on } B\}$.

Next we consider a generalization of matrix S' . As in Sect. 2.2, consider graph H , edge sets E_t and E'_t , and matrix S (with $A \cup B = T$). Suppose that $T = \{1, 2, 3, \dots, 2\tau\}$. For $p = (p_1, \dots, p_{2\tau}), q = (q_1, \dots, q_{2\tau}) \in \mathbb{Z}^{2\tau}$, we define the matrix $S[p, q]$ from S by

$$(S[p, q])_{ij} := \begin{cases} p_t s_{ij} & \text{if } ij \in E_t \text{ for } t \in T, \\ q_t s_{ij} & \text{if } ij \in E'_t \text{ for } t \in T, \\ s_{ij} & \text{otherwise.} \end{cases}$$

For distinct $s, t \in T$ and parity σ , define $[p, q]_{st,\sigma}$ by

$$[p, q]_{st,\sigma} := \begin{cases} p_s p_t + q_s q_t & \text{if } \sigma = \text{odd,} \\ p_s q_t + q_s p_t & \text{if } \sigma = \text{even.} \end{cases}$$

A set \mathcal{M} of PMPs is said to be *h-representable* if there exist $N, k \in \mathbb{Z}_{>0}, n_i \in \mathbb{Z}_{\geq 0}, p^i, q^i \in \mathbb{Z}^{2\tau}$ for $i = 1, \dots, N$ such that a PMP M belongs to \mathcal{M} if and only if

$$\sum_{i=1}^N n_i \prod_{(st,\sigma) \in M} [p^i, q^i]_{st,\sigma} \not\equiv 0 \pmod{2^k}.$$

In particular, the argument in Sect. 2.2 says that \mathcal{M}_{A+B} is h-representable with $N = 1, k = \tau + 1, n_1 = 1, p^1 = (1, 1, \dots, 1)$ and $q^1 = (1, \dots, 1, -1, \dots, -1)$. That is, q^1 has 1 for the first $|A|$ entries and -1 the remaining $|B|$ entries. A generalization of Theorem 1.2 is the following.

Theorem 3.2 *Suppose that a set \mathcal{M} of PMPs is h-representable with parameters $N, k, n_i, p^i, q^i (i = 1, 2, \dots, N)$. Then the shortest perfect \mathcal{M} -path packing problem can be solved in randomized polynomial time, provided N and k are fixed.*

Proof As in the proof of Lemma 2.4, one can show

$$\sum_{i=1}^N n_i \text{haf } S[p^i, q^i] = \sum_{\mathcal{P}} \left[\sum_{i=1}^N n_i \prod_{(st,\sigma) \in M_{\mathcal{P}}} [p^i, q^i]_{st,\sigma} \right] x^{w(\mathcal{P})} (1 + x f_{\mathcal{P}}(x)),$$

where \mathcal{P} ranges over all perfect T -path packings. Therefore, if G has a unique shortest perfect \mathcal{M} -path packing \mathcal{P}^* , then we can obtain \mathcal{P}^* by computing $\sum_{i=1}^N n_i \text{haf } S[p^i, q^i]$ modulo 2^k . This can be done in polynomial time provided N and k are fixed. As in Sect. 2.2, we obtain the randomized polynomial time algorithm for the general case. □

We do not know a characterization of h-representable sets of PMPs. We here discuss three interesting special cases, where odd and even are simply denoted by o and e respectively.

Shortest two disjoint paths via hafnian modulo 4. First we return to the shortest two disjoint paths problem, which corresponds to $T = \{1, 2, 3, 4\}$ and

$$\mathcal{M}_2 := \{(12, \sigma_1), (34, \sigma_2) \mid \sigma_1, \sigma_2 \in \{o, e\}\}.$$

We have seen that \mathcal{M}_2 is h-representable with $N = 1 = n_1 = 1, p^1 = (1, 1, 1, 1), q^1 = (1, 1, -1, -1),$ and $k = 3.$ We present another economical h-representation.

Proposition 3.3 \mathcal{M}_2 is h-representable with $N = 1, k = 2, n_1 = 1, p^1 = (1, 1, 1, 1),$ and $q^1 = (0, 1, -1, -1).$

Proof A direct calculation (e.g., $[p^1, q^1]_{12,e}[p^1, q^1]_{34,o} = (1 \cdot 1 + 0 \cdot 1)\{1 \cdot 1 + (-1) \cdot (-1)\} = 2)$ shows

$$\prod_{(st,\sigma) \in M} [p^1, q^1]_{st,\sigma} = \begin{cases} 2 & \text{if } M = \{(12, o), (34, o)\}, \{(12, e), (34, o)\}, \\ -2 & \text{if } M = \{(12, o), (34, e)\}, \{(12, e), (34, e)\}, \\ 0 & \text{otherwise.} \end{cases}$$

In particular, modulo 4 computation is sufficient. It might be interesting to compare with the original approach by Björklund–Husfeldt [2]: their algorithm requires to compute permanents of three $n \times n$ matrices modulo 4, whereas our algorithm with these parameters requires to compute the hafnian of one $2n \times 2n$ matrix modulo 4.

Shortest odd two disjoint paths via four hafnians modulo 4. The hafnian approach can solve the shortest two disjoint paths problem with a parity constraint that the sum of the lengths of paths is odd. This problem corresponds to $T = \{1, 2, 3, 4\}$ and $\mathcal{M}_{2, \text{odd}} := \{(12, o), (34, e)\}, \{(12, e), (34, o)\}.$

Theorem 3.4 $\mathcal{M}_{2, \text{odd}}$ is h-representable with $N = 4, k = 2, (n_1, n_2, n_3, n_4) = (1, 1, -1, -1),$ and

$$\begin{aligned} p^1 &= (1, 1, 1, 0), & q^1 &= (0, 0, 0, 1), \\ p^2 &= (1, 1, 0, 1), & q^2 &= (0, 0, 1, 0), \\ p^3 &= (1, 0, 1, 1), & q^3 &= (0, 1, 0, 0), \\ p^4 &= (0, 1, 1, 1), & q^4 &= (1, 0, 0, 0). \end{aligned}$$

Proof One can verify the theorem from the value of $C_i := \prod_{(st,\sigma) \in M} [p^i, q^i]_{st,\sigma}$ for $i = 1, 2, 3, 4$ and all PMPs M on $T,$ which are shown in Table 1. □

Non h-representability of 3-disjoint paths. A deep result by Robertson–Seymour [10] is that the k -disjoint paths problem is solvable in polynomial time (for fixed k). One may naturally ask whether the shortest k -disjoint paths problem for $k \geq 3$ is solvable by this approach. Unfortunately our approach cannot reach the shortest 3-disjoint paths problem, which corresponds to $T = \{1, 2, 3, 4, 5, 6\}$ and

$$\mathcal{M}_3 := \{(12, \sigma_1), (34, \sigma_2), (56, \sigma_3) \mid \sigma_1, \sigma_2, \sigma_3 \in \{o, e\}\}.$$

Table 1 Values of C_i

PMP	C_1	C_2	C_3	C_4	$C_1 + C_2 - C_3 - C_4$
{(12, o), (34, o)}	0	0	0	0	0
{(12, o), (34, e)}	1	1	0	0	2
{(12, e), (34, o)}	0	0	1	1	-2
{(12, e), (34, e)}	0	0	0	0	0
{(13, o), (24, o)}	0	0	0	0	0
{(13, o), (24, e)}	1	0	1	0	0
{(13, e), (24, o)}	0	1	0	1	0
{(13, e), (24, e)}	0	0	0	0	0
{(14, o), (23, o)}	0	0	0	0	0
{(14, o), (23, e)}	0	1	1	0	0
{(14, e), (23, o)}	1	0	0	1	0
{(14, e), (23, e)}	0	0	0	0	0

Theorem 3.5 \mathcal{M}_3 is not h -representable.

We start with a preliminary argument. Let $\mathbf{1} := (1, 1, \dots, 1)$. For $\chi \in \{0, 1\}^{2\tau}$, let $S(\chi) := S[\chi, \mathbf{1} - \chi]$. Then $\text{haf } S[p, q]$ can be expressed as a linear combination of $\text{haf } S(\chi)$ over $\chi \in \{0, 1\}^{2\tau}$:

Lemma 3.6 $\text{haf } S[p, q] = \sum_{\chi \in \{0,1\}^{2\tau}} \prod_{i=1}^{2\tau} \{\chi_i p_i + (1 - \chi_i)q_i\} \text{haf } S(\chi).$

Proof Each perfect matching of H determines $\chi \in \{0, 1\}^{2\tau}$ as: $\chi_i = 1$ if and only if node i is matched to a node in U . Here χ is called the *type* of M . We classify all perfect matchings in terms of their types. One can verify

$$\sum_{M:\text{type } \chi} \prod_{ij \in M} (S[p, q])_{ij} = \left[\prod_{i=1}^{2\tau} \{\chi_i p_i + (1 - \chi_i)q_i\} \right] \text{haf } S(\chi).$$

Thus we have the desired formula.

From Lemma 3.6, in the definition of h -representability, it suffices to consider the case where $p = \chi$ and $q = \mathbf{1} - \chi$ for $\chi \in \{0, 1\}^{2\tau}$. In this case, $\prod_{(st,\sigma) \in M} [p, q]_{st,\sigma}$ is 0 or 1. Let $[\chi]_{st,\sigma} := [\chi, \mathbf{1} - \chi]_{st,\sigma}$.

Proof of Theorem 3.5 First consider the following six PMPs:

$$\begin{aligned} M_1 &:= \{(12, o), (34, o), (56, e)\}, & M_2 &:= \{(12, o), (36, o), (45, e)\}, \\ M_3 &:= \{(14, o), (23, o), (56, e)\}, & M_4 &:= \{(14, o), (36, o), (25, e)\}, \\ M_5 &:= \{(16, o), (23, e), (45, o)\}, & M_6 &:= \{(16, o), (34, e), (25, o)\}. \end{aligned}$$

Observe that M_1 is in \mathcal{M}_3 and other five PMPs are not in \mathcal{M}_3 . For PMP M and $\chi \in \{0, 1\}^6$, define $b_{M,\chi}$ by

$$b_{M,\chi} := \prod_{(st,\sigma) \in M} [\chi]_{st,\sigma}.$$

By computer calculation, we have verified the following 64 equations to hold;

$$b_{M_1,\chi} = b_{M_2,\chi} + b_{M_3,\chi} - b_{M_4,\chi} + b_{M_5,\chi} - b_{M_6,\chi} \quad (\chi \in \{0, 1\}^6). \tag{5}$$

Next suppose that \mathcal{M}_3 is h-representable. Thanks to Lemma 3.6, there exist $k \in \mathbb{Z}_{>0}$ and $n_\chi \in \mathbb{Z}$ for $\chi \in \{0, 1\}^6$ such that a PMP M belongs to \mathcal{M} if and only if

$$\sum_{\chi \in \{0,1\}^6} n_\chi \prod_{(st,\sigma) \in M} [\chi]_{st,\sigma} \not\equiv 0 \pmod{2^k}.$$

In particular, it holds

$$\sum_{\chi \in \{0,1\}^6} n_\chi b_{M_j,\chi} \equiv 0 \pmod{2^k} \quad (j = 2, 3, 4, 5, 6).$$

By (5), we have

$$\sum_{\chi \in \{0,1\}^6} n_\chi b_{M_1,\chi} \equiv 0 \pmod{2^k}.$$

However this is a contradiction to $M_1 \in \mathcal{M}_3$. □

Acknowledgements We thank the referees for helpful comments. The work was partially supported by JSPS KAKENHI Grant Numbers 25280004, 26330023, 26280004, 17K00029.

References

1. Björklund, A.: Counting perfect matchings as fast as Ryser. Proceedings of the Twenty-Third Annual ACM-SIAM Symposium on Discrete Algorithms, pp. 914–921. ACM, New York (2012)
2. Björklund, A., Husfeldt, T.: Shortest two disjoint paths in polynomial time. Proceedings of 41st International Colloquium on Automata, Languages, and Programming, Lecture Notes in Computer Science 8572, pp. 211–222. Springer, Berlin (2014)
3. Colin de Verdière, É., Schrijver, A.: Shortest vertex-disjoint two-face paths in planar graphs. ACM Trans. Algorithms 7(19), 12 (2011)
4. Gallai, T.: Maximum-minimum Sätze und verallgemeinerte Faktoren von Graphen. Acta Math. Acad. Sci. Hung. 12, 131–173 (1961)
5. Hirai, H., Pap, G.: Tree metrics and edge-disjoint S-paths. Math. Program. 147, 81–123 (2014)
6. Karzanov, A.: Edge-disjoint T-paths of minimum total cost. Technical Report, STAN-CS-92-1465. Department of Computer Science, Stanford University, Stanford (1993). Available at <http://alexander-karzanov.net/>
7. Kobayashi, Y., Sommer, C.: On shortest disjoint paths in planar graphs. Discret. Optim. 7, 235–245 (2010)
8. Kobayashi, Y., Toyooka, S.: Finding a shortest non-zero path in group-labeled graphs. Algorithmica 77, 1128–1142 (2017)

9. Mulmuley, K., Vazirani, U.V., Vazirani, V.V.: Matching is as easy as matrix inversion. *Combinatorica* **7**, 105–113 (1987)
10. Robertson, N., Seymour, P.D.: Graph minors. XIII. The disjoint paths problem. *J. Comb. Theory Ser. B* **63**, 65–110 (1995)
11. Schrijver, A.: *Comb. Optim. Polyhedra Effic.* Springer-Verlag, Berlin (2003)
12. Seymour, P.D.: Disjoint paths in graphs. *Discret. Math.* **29**, 293–309 (1980)
13. Shiloach, Y.: A polynomial solution to the undirected two paths problem. *J. ACM* **27**, 445–456 (1980)
14. Thomassen, C.: 2-Linked graphs. *Eur. J. Comb.* **1**, 371–378 (1980)
15. Valiant, L.G.: The complexity of computing the permanent. *Theor. Comput. Sci.* **8**, 189–201 (1979)
16. Yamaguchi, Y.: Shortest disjoint non-zero A -paths via weighted matroid matching. In: *Proceedings of the 27th International Symposium on Algorithms and Computation*, pp. 63:1–63:13 (2016)