Proving Pfaffian properties in bounded arithmetic

Satoru Kuroda*
Department of Culture and Informatics,
Gumma Prefectural Women's University

1 Introduction

Proving theorems of linear algebra, especially properties of the determinant is a central theme in bounded reverse mathematics. although the determinant has several $\#\mathsf{L}$ algorithm, many of its properties are known to be provable in a theory slightly stronger than $\#\mathsf{L}$.

The seminal work of Soltys and Cook on bounded reverse mathematics of linear algebra revealed that some important properties such as the cofactor expansion, the axiomatic definition of the determinant and Cayley-Hamilton Theorem are equivalent over the theory $\mathbf{V\#L}$. Also they proved that the multiplicativity of the determinant implies all these properties.

Soon after, the celebrated result by Tzameret and Cook gave an upper bound on the provability of these properties. It is proved in [10] that the multiplicativity of the determinant is provable in $\mathbf{VNC}^2$.

Also, Ken and the author [4] showed that properties of matrix rank are provable in $\mathbf{VNC}^2$ by using the result in [10] and establishing the interpretation of extensions of Soltys theory for linear algebra in $\mathbf{VNC}^2$. However, it is still open that the above properties of the determinant and matrix rank are provable in some weaker theories such as $\mathbf{V\#L}$. In particular, the proof in [10] is based on the algorithm for the determinant via Schur complement. On the other hand, faster algorithms such as Berkowitz algorithm [1] are formalizable in $\mathbf{V\#L}$.

In this article, we propose to extend the study of proof compleixty of linear algebra along this line to Pfaffian.

Pfaffian was introduced by Pfaff in 19th century in relation with partial differential equations. Recently, many applications are given in combinatorics and representation theory. Computing Pfaffian is very similar to computing the determinant and many fast algorithms for the determinant are generalized to Pfaffian which include the characterization via clow sequences.

In this article, we will give a Berkowitz type algorithm for Pfaffian and prove its correctness by way of clow sequences technique which was developed by Mahajan, Subramanya and Vinay. This is used to formalize Pfaffian in the theory $\mathbf{V\#L}$.

Then we also consider the provability of Pfaffian properties over the theory $\mathbf{V\#L}$. Especially, we consider the problem of proving properties from Pfaffian version of multiplicativity.

We also present a version of Cayley-Hamilton type theorem for Pfaffian. Cayley-Hamilton type theorem for Pfaffian has been unfamiliar until recently. By examining the proof of Cayley-Hamilton Theorem from cofactor expansion in [3] carefully, we present a theorem which is equivalent to cofactor expansion and the axiomatic definition of Pfaffian.

*This work was supported by JSPS KAKENHI Grant Number 18K03400.

To author's knowledge, our version of Pfaffian Cayley-Hamilton is new and we expect that it can be used to prove various properties of linear algebra.

Our goal is not only to extend the proof complexity problem of linear algebra but also to extend bounded reverse mathematics to combinatorics and representation theory. The final section is devoted to showing our perspective.

Yet another noteworthy properties of Pfaffian is that the product of two Pfaffians admit combinatorial algorithm. We will present a new Berkowitz type algorithm for Pfaffian pairs.

In this article, we overview proof theoretic treatments of Pfaffian properties developed by the author. Due to the limited space, most results are given without detailed proofs. Full proofs are given in the manuscript [5].

2 Preliminaries

Due to the space limit, we refrain from giving details of bounded arithmetic and complexity theory. We work in two sort bounded arithmetic developed by Cook and Ngyuen [2]. The theory $\mathbf{V\#L}$ consists of axioms

- Σ_0^B-COMP:
$$\forall a\, \forall x < a\, \exists Y\, (x \in Y \leftrightarrow Y(x))$$
where $\varphi(x) \in \Sigma_0^B$ does not contain Y.
- String Multiplication:
$$\forall X, Y\, \exists Z\, (Z = X \cdot Y)$$
- Matrix Powering:
$$\forall X : \text{square matrix}\ \forall n\, \exists Y\, (Y = X^n)$$

The complexity class $\#\mathsf{L}$ consists of functions which are logspace reducible to the determinant. It is known that matrix powering is complete for $\#\mathsf{L}$ and thus we have

Theorem 1. *A function is Σ_1^B definable in $\mathbf{V\#L}$ if and only if it is in $\#\mathsf{L}$.*

Note that induction for Σ_0^B formula is provable in $\mathbf{V\#L}$ even when we extend the language by Σ_1^B definable functions. This fact will be a crucial tool in proving matrix properties.

Pfaffian is defined in a similar manner as for the determinant. Specifically, let $A \in \mathrm{Mat}(2n, 2n)$ be skew symmetric. Then its Pfaffian is defined as

$$\mathrm{pf}(A) = \sum_{\sigma \in \mathcal{M}_{2n}} \mathrm{sgn}(\sigma) a_{\sigma(1)\sigma(2)} \cdots a_{\sigma(2n-1)\sigma(2n)} \tag{1}$$

where $\mathcal{M}_{2n}$ represents the set of perfect matchings on $[2n]$ such that

$$\sigma(1) < \sigma(3) < \cdots \sigma(2n-1).$$

Pfaffian can be regarded as a generalization of the determinant in the sense that $\det(A)$ for $n \times n$ matrix A is computed by Pfaffian as

$$\det(A) = (-1)^{n(n-1)}\, \mathrm{pf} \begin{pmatrix} 0 & A \\ -{}^tA & 0 \end{pmatrix} \tag{2}$$

For skew symmetric matrix $A \in \mathrm{Mat}(2n, 2n)$, the following relation is known:

Theorem 2 (Cayley)**.** *If $A \in \mathrm{Mat}(2n, 2n)$ is a skew symmetric matrix then*

$$\det(A) = \mathrm{pf}(A)^2 \tag{3}$$

Our formalization of Pfaffian is based on the characterization by way of clow sequences due to Mahajan, Vinay. A clow (closed walk) on $[n]$ is a list of edges

$$(i_1, i_2), (i_2, i_3), \ldots, (i_m, i_1)$$

such that $i_1 < i_k$ for all $2 \leq k \leq m$. The first index i_1 is called the head of C and is denoted by $\mathrm{head}(C)$.

A pclow is a list $E_1, E_2, \ldots, E_m$ where each E_k is a pair (e_1^k, e_2^k) of edges such that either

- $e_1^k = (i, 2j-1)$ and $e_2^k = (2j-1, 2j)$ or
- $e_1^k = (i, 2j)$ and $e_2^k = (2j, 2j-1)$.

Let C be a pclow. Define

$$\mathrm{fd}(C) = \#\{(i,j) \in C : i < j\},\ \mathrm{bd}(C) = \#\{(i,j) \in C : i > j\}.$$

and

$$\mathrm{sgn}(C) = (-1)^{f(C)+1}.$$

For $A = (a_{ij}) \in \mathrm{Mat}(2n, 2n)$, we define $a_{ij}^+ = a_{ij}$ if $i < j$ and $a_{ij}^+ = a_{ji}$ if $i > j$. The weight of a clow $C = \langle e_1, e_2, \ldots, e_{2m} \rangle$ over A is the product

$$w_A(C) = \prod_{1 \leq k \leq m} a_{e_{2k-1}}^+.$$

A pclow sequence is a sequence $\bar{C} = \langle C_1, \ldots, C_l \rangle$ of pclows such that

$$\mathrm{head}(C_1) = 1 < \mathrm{head}(C_2) < \cdots < \mathrm{head}(C_l).$$

We define the sign and the weight of a pclow sequence as

$$\mathrm{sgn}(\bar{C}) = \prod_{C \in \bar{C}} \mathrm{sgn}(C) \text{ and } w_A(\bar{C}) = \prod_{C \in \bar{C}} w_A(C)$$

respectively. Finally the length of a pclow or a pclow sequence is the number of edges occuring in it.

Theorem 3 (Mahajan et.al.)**.** *Let $A \in \mathrm{Mat}(2n, 2n)$ be skew symmetric. Then*

$$\mathrm{pf}(A) = \sum_{\bar{C}\text{:pclow seq. } |\bar{C}|=2n} \mathrm{sgn}(\bar{C}))w_A(\bar{C}).$$

3 Berkowitz-type algorithm for Pfaffian

In this section we construct a #L algorithm for Pfaffian.

For $n \in \omega$, we define the skew symmetric matrix $J_n \in \mathrm{Mat}(2n, 2n)$ by

$$J_1 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \; J_n = \left.\begin{pmatrix} J_1 & & & \\ & J_1 & & \\ & & \ddots & \\ & & & J_1 \end{pmatrix}\right\} n \text{ times } (n \geq 1).$$

We omit the subscript if it is clear from the context.

Definition 1 (PB algorithm)**.** *Let $A \in \mathrm{Mat}(2n, 2n)$ be skew symmetric and*

$$\begin{pmatrix} 0 & a_{12} & R \\ -a_{12} & 0 & -{}^tS \\ -{}^tR & S & M \end{pmatrix}$$

be its block decomposition. Define Berkowitz algorithm P_A as

$$P_A = \begin{pmatrix} 1 & & & & \\ a_{12} & 1 & & & \\ RJS & a_{12} & \ddots & & \\ RJ(MJ)S & RJS & \ddots & \ddots & \\ \vdots & \ddots & \ddots & \ddots & \\ \vdots & \ddots & \ddots & \ddots & 1 \\ RJ(MJ)^{n-2}S & RJ(MJ)^{n-3}S & \cdots & \cdots & a_{12} \end{pmatrix} \in \mathrm{Mat}(n+1, n). \tag{4}$$

We define Pfaffian coefficients $\bar{P}_A = (p_n, p_{n-1}, \ldots, p_0)$ as $\bar{P}_A = (1, a_{12})$ if $n = 2$ and

$$\bar{p}_A = P_A \bar{p}_M.$$

if $n > 2$.

This algorithm is already suggested by Rote [8] in somewhat awkward manner. We present it here in a complete form and prove its correctness below.

We will show that PB algorithm computes Pfaffian. More generally we have

Theorem 4. *Let $A \in \mathrm{Mat}(2n, 2n)$ be skew symmetric and $\bar{P}_A = (p_n, p_{n-1}, \ldots, p_0)$ be its Pfaffian sequence. Then*

$$p_{n-k} = \sum_{\substack{\bar{C}\,:\,\text{pclow seq.} \\ |\bar{C}|=2k}} \mathrm{sgn}(\bar{C}) w_A(\bar{C}) + \sum_{\substack{\bar{C}\,:\,\text{pclow seq. on } [3,2n] \\ |\bar{C}|=2k}} \mathrm{sgn}(\bar{C}) w_M(\bar{C}). \tag{5}$$

for $1 \leq k \leq n-1$ and

$$p_0 = \sum_{\substack{\bar{C}\,:\,\text{pclow seq.} \\ |\bar{C}|=2n}} \mathrm{sgn}(\bar{C}) w_A(\bar{C}) \tag{6}$$

Hence $\mathrm{pf}(A) = p_0$.

To prove Theorem 4, we first notice that each entry in the matrix P_A computes the sum of signed weights of clows. For instance, consider the entry a_{12}. The only possible clow starting from $(1,2)$ is $C = \langle(1,2),(2,1)\rangle$ with $w_A(C) = a_{12}$. Moreover, note that $f(C) = 1$ and thus $\mathrm{sgn}(C) = (-1)^{1+1} = 1$. Hence we have

$$\sum_{C\,:\,\text{pclow}\ |\bar{C}|=2} \mathrm{sgn}(C) w_A(C) = a_{12}.$$

In general we have

Lemma 1. *Let $A \in \mathrm{Mat}(2n,2n)$ be skew symmetric with its block decomposition given as above. Then*

$$RJ(MJ)^{k-2}S = \sum_{\substack{C\,:\,pclow \\ |\bar{C}|=2k,\mathrm{head}(C)=1}} \mathrm{sgn}(C) w_A(C). \tag{7}$$

From this lemma, Theorem 4 is proved by induction.

Note that PB algorithm is a $\#\mathsf{L}$ algorithm and hence we have

Corollary 1. *Pfaffian* $\mathrm{pf}(A)$ *is Σ_1^B definable in* $\mathbf{V\#L}$.

4 The proof complexity of Pfaffian

Some of Pfaffian properties are derivable solely from Pfaffian Berkowitz algorithm. Here we present two of them.

Lemma 2. *($\mathbf{V\#L}$) Let $A \in \mathrm{Mat}(2n,2n)$ be skew symmetric and λ be any number. Then*

$$\mathrm{pf}(\lambda A) = \lambda^n \,\mathrm{pf}(A). \tag{8}$$

Theorem 5. *Let $A \in \mathrm{Mat}(2n,2n)$ be skew symmetric, $\vec{q_A} = (q_n, q_{n-1}, \ldots, q_0)$ and $\vec{r_A} = (r_n, r_{n-1}, \ldots, r_0)$ be Pfaffian coefficients of A and ${}^tA$ respectively. Then for $0 \le k \le n$,*

$$r_{n-k} = (-1)^k q_{n-k}. \tag{9}$$

Thus $\mathrm{pf}({}^tA) = (-1)^n \,\mathrm{pf}(A)$.

Since Pfaffian is a generalization of the determinant, most properties of the determinant are given for Pfaffian as well. The difference is that operations on rows or columns on $\det(A)$ correspond to operations simultaneously on rows and columns.

Let $A \in \mathrm{Mat}(2n,2n)$ be skew symmetric. Define the following operations:

- $A[i:j]$ is given by simultaneously swapping rows i,j and swapping columns i,j.
- $A\langle i,j\rangle$ is given by removing rows i,j and columns i,j.

Then we have the following properties in analogy with the determinant:

Theorem 6 (Pfaffian Cofactor Expansion)**.** *Let $A \in \mathrm{Mat}(2n,2n)$ be skew symmetric and $1 \le i \le 2n$. Then*

$$(PCE) \quad \mathrm{pf}(A) = \sum_{1\le j\ne i\le 2n} (-1)^{i+j+\Theta(j-i)} a_{ij} \,\mathrm{pf}(A\langle i,j\rangle)$$

where $\Theta(k)$ is Heaviside step function.

If we define the determinant by the equation (2) then properties of the determinant are provable from the corresponding properties for Pfaffian in **V#L**. For instance, we have

Lemma 3 (V#L). *(PCE) implies the cofactor expansion of the determinant.*

Proof Sketch. The proof is by induction on the number of rows. Let $A \in \mathrm{Mat}(n,n)$ and $B = \begin{pmatrix} 0 & A \\ -{}^tA & 0 \end{pmatrix}$. By applying (PCE) to B and using the inductive hypothesis yields that

$$\mathrm{pf}(B) = (-1)^{n(n-1)/2} \sum_{1\le j\le n} (-1)^{i+j} \det(A_{i,j}).$$

□

Theorem 7 (V#L). *(PCE) implies Cayley's theorem:*

$$\forall A \in \mathrm{Mat}(2n,2n) : \textit{skew symmetric} \det(A) = \mathrm{pf}(A)^2. \tag{10}$$

See [7] for the proof.

The axiomatic definition of the determinant refers to the multilinearity, the alternation and the equation $\det(I) = 1$. Similarly, the axiomatic definition of Pfaffian (PAD) is the collection of the following three statements:

Multilinearity : Let $A(\lambda, i)$ be the matrix A with the row and the column i multiplied by λ. Then $\mathrm{pf}(A(\lambda, i)) = \lambda\,\mathrm{pf}(A)$.

Alternation : $\mathrm{pf}(A[i:j]) = -\mathrm{pf}(A)$.

Identity : $\mathrm{pf}(J) = -1$.

Theorem 8. V#L *proves Multilinearity on the first row and column and Identity.*

Proof. The first part is easy. For the second part, let $J_n \in \mathrm{Mat}(2n,2n)$. Then

$$P_{J_n} = \begin{pmatrix} 1 & 0 & \ddots & \\ 1 & 1 & \ddots & \\ \vdots & \vdots & \ddots & 1 \\ 0 & 0 & \cdots & 1 \end{pmatrix}$$

From this we have the recurrence $\mathrm{pf}(J_n) = \mathrm{pf}(J_{n-1})$. Since we have $\mathrm{pf}(J_1) = -1$, the claim is immediate. □

For the determinant, cofactor expansion and the axiomatic definition are equivalent in **V#L**. This is also the case for Pfaffian.

Theorem 9 (V#L). *(PCE) and (PAD) are equivalent.*

Proof. First we show that (PALT) implies (PCE). Let $A \in \mathrm{Mat}(2n,2n)$ be skew symmetric and $1 < i \le 2n$. Apply (PALT) for rows and columns $1, i$ yields $\mathrm{pf}(A\langle 1, i\rangle) = -\mathrm{pf}(A)$. By Theorem 8, we can expand $A\langle i, j\rangle$ on the first row and column. Then applying (PALT) again yields (PCE).

For the other direction, we can show that (PCE) implies (PALT).

□

Theorem 10 (V#L). *Let $I \in \mathrm{Mat}(2n, 2n)$ be the identity matrix. Then*

$$\mathrm{pf}\begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix} = (-1)^n. \tag{11}$$

Proof. Let $C_0 = \mathrm{pf}\begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix} \in \mathrm{Mat}(4n, 4n)$ and

$$C_k = \begin{pmatrix} 0 & 0 & R_{k+1} \\ 0 & 0 & -{}^t s_{k+1} \\ -{}^t R_{k+1} & S & C_{k+1} \end{pmatrix} \in \mathrm{Mat}(4n-2k, 4n-2k).$$

Then C_k is of the form

$$\begin{pmatrix} & & I_{2n-2k} \\ & O_{2k} & \\ -I_{2n-2k} & & \end{pmatrix} \in \mathrm{Mat}(4n-2k, 4n-2k)$$

where all blank entries are zero.

Let $\vec{q_k} = \left(q^k_{2n-k}, q^k_{2n-k-1}, \dots, q^k_0\right)$ be Berkowitz sequence for C_k. From Berkowitz algorithm, it follows that

$$\begin{pmatrix} q^k_{2n-k} \\ q^k_{2n-k-1} \\ \vdots \\ q^k_0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & & & & \\ 0 & 1 & \ddots & & & \\ -1 & 0 & \ddots & & & \\ \vdots & \vdots & \ddots & & & \\ & & & & 1 & \\ & & & & 0 & 1 \\ 0 & 0 & 0 & \cdots & -1 & 0 \end{pmatrix} \begin{pmatrix} q^{k+1}_{2n-k-1} \\ q^{k+1}_{2n-k-2} \\ \vdots \\ q^{k+1}_0 \end{pmatrix}$$

Hence we have the following recurrences:

$$\begin{aligned} & q^k_{n-k} = 1,\ q^k_{n-k-1} = q^{k+1}_{n-k-2}, \\ & q^k_{n-k-i} = -q^{k+1}_{n-k-i+1} + q^{k+1}_{n-k-i-1}\ (2 \le i < 2n-k), \\ & q^k_0 = -q^k_1. \end{aligned}$$

We claim that $\forall j < k\ p^k_j = 0$. This is proved by backward induction on $k \le n$. If $k = n$ then $\vec{q_n} = \begin{pmatrix} 1 & 0 & \cdots & 0 \end{pmatrix}$ so the claim is obvious. Suppose that $\forall j < k\ p^k_j = 0$. and $j \le k$. Then by the inductive hypothesis,

$$\begin{aligned} & q^k_{2n-k-1} = q^{k+1}_{2n-k-2} = 0, \\ & q^k_{n-k-i} = -q^{k+1}_{n-k-i+1} + q^{k+1}_{n-k-i-1} = 0. \end{aligned}$$

Hence we have $q^k_k = -q^{k+1}_{k+1}$ and by backward induction, we conclude that $\mathrm{pf}(C_0) = (-1)^n$. ☐

The following equaition can be regarded as the analogue of the multiplicativity.

Theorem 11. *Let $A \in \mathrm{Mat}(2n, 2n)$ be skew symmetric and $B \in \mathrm{Mat}(2n, 2n)$. Then*

$$(MP) \quad \mathrm{pf}({}^tBAB) = \mathrm{pf}(A)\det(B).$$

Note that if B is skew symmetric then by Cayley's theorem (equation 3), we have $\det(B) = \mathrm{pf}(B)^2$. Hence we obtain

$$\mathrm{pf}({}^tBAB) = \mathrm{pf}(A)\,\mathrm{pf}(B)^2.$$

We expect that (MP) implies most properties of Pfaffian in **V#L**. The rest of this section is devoted to the consideration of this problem.

First remark that the condition of the axiomatic definition other than Alternation are provable in **V#L**.

Theorem 12. **V#L** *proves Multilinearity for $i = 1$ and Identity.*

Proof. Multilinearity for the first row and column is straightforward from PB algorithm. Identity is proved by induction on n. □

Suppose that Alternation is proved form (MP). Then it is easy to see that (MP) implies other properties of Pfaffian, namely (PCE) and Cayley's Theorem. To prove Alternation from (MP), remark that

$$A[i:j] = {}^tI_{ij}AI_{ij}.$$

So by (MP) we have

$$\mathrm{pf}(A[i:j]) = \mathrm{pf}({}^tI_{ij}AI_{ij}) = \mathrm{pf}(A)\det(I_{ij}).$$

Hence it suffices to show that

$$\det(I_{ij}) = -\det(I) \tag{12}$$

is provable for the identity matrix I of even order. However, it seems fairly complicated to directly prove the equation (12). So we argue in a simpler manner.

First note that

Theorem 13 (**V#L**)**.** *Let $I \in \mathrm{Mat}(2n, 2n)$ be the identity matrix and for $1 \le k < 2n$, $I[k]$ be the alternation of rows k and $k+1$ in I. Then*

$$\mathrm{pf}\begin{pmatrix} 0 & I[k] \\ -I[k] & 0 \end{pmatrix} = (-1)^{n+1}. \tag{13}$$

Proof. We argue similarly as in Theorem 10. The proof is divided into two cases.

Case 1: $k \mod 2 = 1$. Let $k = 2l+1$ and

$$I[k] = \begin{pmatrix} I_{2l} & & & \\ & & 1 & \\ & 1 & & \\ & & & I_{2m} \end{pmatrix}$$

where $n = l + m + 1$. Define

$$C_0 = \begin{pmatrix} 0 & I[k] \\ -I[k] & 0 \end{pmatrix},\ C_j = \begin{pmatrix} 0 & 0 & R_{j+1} \\ 0 & 0 & {}^tS_{j+1} \\ {}^tR_{j+1} & S_{j+1} & C_{j+1} \end{pmatrix}\ (0 \le k < n).$$

Then for $0 \le j < l$, $j = l$ and $l < j < n$, C_j is of the form

$$\begin{pmatrix} & & I[2(l-j)+1] \\ & O_{2j} & \\ -I[2(l-j)+1] & & \end{pmatrix} \in \mathrm{Mat}(4n-2j, 4n-2j),$$

$$\begin{pmatrix} & & & & 1 & \\ & & & 1 & & \\ & & & & & I \\ & & O_{2l} & & & \\ & -1 & & & & \\ -1 & & & & & \\ & & -I & & & \end{pmatrix} \in \mathrm{Mat}(4n-2l, 4n-2l), \text{and}$$

$$\begin{pmatrix} & & I \\ & O_{2j} & \\ -I & & \end{pmatrix} \in \mathrm{Mat}(4n-2j, 4n-2j),$$

respectively. Moreover, $C_n = 0$.

Remark that Berkowitz matrix for C_j with $j \ne l$ are the same as in Theorem 10. For C_l, we have

$$P_{C_l} = \begin{pmatrix} 1 & 0 & & & & \\ 0 & 1 & \ddots & & & \\ 1 & 0 & \ddots & & & \\ \vdots & \vdots & \ddots & & & \\ & & & & 1 & \\ & & & & 0 & 1 \\ 0 & 0 & 0 & \cdots & 1 & 0 \end{pmatrix}$$

Now the proof is identical to that for Theorem 10. Specifically, we have

$$q_j^j = \begin{cases} -q_{j+1}^{j+1} & \text{if } 0 \le j \le l < n, \\ q_{j+1}^{j+1} & \text{if } j = l. \end{cases}$$

and from this recurrence, the claim follows immediately.

Case 1: $k \mod 2 = 0$. Let $k = 2l$. By a similar block decomposition as in Case 1, we have

$$C_{l-1} = \begin{pmatrix} & & B \\ & O_{2(l-1)} & \\ -B & & \end{pmatrix}, \text{ and } C_l = \begin{pmatrix} & & B' \\ & O_{2l-1} & \\ -B' & & \end{pmatrix}$$

where

$$B = \begin{pmatrix} 1 & & & \\ & & 1 & \\ & 1 & & \\ & & & 1 & \\ & & & & I \end{pmatrix}, \text{ and } B' = \begin{pmatrix} 1 & & \\ & 1 & \\ & & I \end{pmatrix}.$$

Berkowitz matrices for these two matrices are

$$P_{C_{l-1}} = \begin{pmatrix} 1 & 0 & & & & \\ 0 & 1 & \ddots & & & \\ 0 & 0 & \ddots & & & \\ -1 & 0 & \ddots & & & \\ \vdots & \vdots & \ddots & & & \\ & & & & 1 & \\ & & & & 0 & 1 \\ 0 & 0 & 0 & \cdots & 0 & 0 \end{pmatrix} \text{ and } P_{C_l} = \begin{pmatrix} 1 & 0 & & & & \\ 0 & 1 & \ddots & & & \\ 0 & 0 & \ddots & & & \\ \vdots & \vdots & \ddots & & & \\ & & & & 1 & \\ & & & & 0 & 1 \\ 0 & 0 & 0 & \cdots & 0 & 0 \end{pmatrix}.$$

From these computations we obtain a recurrence which implies the claim. □

Theorem 14 (**V#L**)**.** *(MP) implies (PALT).*

Proof. Let $A \in \mathrm{Mat}(2n, 2n)$ be skew symmetric and $1 \le i \ne j \le 2n$. Then we can effectively construct a sequence $1 \le k_1, k_2, \ldots, k_{2l-1} \le 2n$ such that

$$A[i:j] = {}^tI_{k_{2l-1}} \cdots {}^tI_{k_2} {}^tI_{k_1} A I_{k_1} I_{k_2} \cdots I_{k_{2l-1}}.$$

By applying (MP) repeatedly to $A[i:j]$, we obtain

$$\mathrm{pf}(A[i:j]) = \mathrm{pf}(A)\det(I_{k_1})\det(I_{k_2})\cdots\det(I_{k_{2l-1}})$$

Note that this is where we require induction in **V#L**. Now the claim follows immediately from Theorem 13. □

5 Cayley-Hamilton Theorem for Pfaffian

So far we have seen that Pfaffian and the determinant have a lot of common properties. Hence one might ask whether Cayley-Hamilton type theorem is possible for Pfaffian. The answer is yes and in this section we present a version of Cayley-Hamilton theorem for Pfaffian.

Definition 2. *Let $A \in \mathrm{Mat}(2n, 2n)$ be skew symmetric and $q_n^A, q_{n-1}^a, \ldots, q_0^A$ be its Pfaffian coefficients. Define Pfaffian characteristic polynomial as*

$$\Phi_A(x) = q_n^A x^n + q_{n-1}^A x^{n-1} + \cdots + q_0^A. \tag{14}$$

Theorem 15 (Pfaffian Cayley-Hamilton Theorem)**.** *Let $A \in \mathrm{Mat}(2n, 2n)$ be skew symmetric. Then*

$$\Phi_A(AJ) = q_n^A (AJ)^n + q_{n-1}^A (AJ)^{n-1} + \cdots + q_0^A I = 0. \tag{15}$$

We can prove this theorem in several ways. One way is to use the combinatorial argument which is used to prove Cayley-Hamilton Theorem for the determinant due to Straubing [9]. However, we do not know whether such proof can be formalized in **V#L**.

We can also prove this from (PCE) which can be formalized in **V#L**.

The converse is also true, that is,

Theorem 16 (**V#L**)**.** *(PCH) implies (PCE). Thus (PCE), (PCH) and (PAD) are equivalent over* **V#L**.

We omit the proof due to the limitation of space.

6 Berkowitz algorithm for Pfaffian pairs

In [8], it is shown that the product of Pfaffians are computable by means of alternating clow sequences. This fact leads to a Berkowitz type algorithm computing $\mathrm{pf}(A)\,\mathrm{pf}(B)$. In this section we present such an algorithm.

Let $1 \le i \le n$ and k be a number. We define

$$\begin{aligned} \mathcal{C}_{i,k} &= \left\{\bar{C} : \text{alternating clow},\ \mathrm{head}(\bar{C}) \ge i,\ |\bar{C}| = 2k\right\},\ \text{and} \\ \mathcal{D}_{i,k} &= \left\{\bar{C} : \text{alternating clow},\ \mathrm{head}(\bar{C}) = i,\ |\bar{C}| = 2k\right\}. \end{aligned} \tag{16}$$

For skew symmetric matrices $A, B \in \mathrm{Mat}(n,n)$ let $m = \lfloor n/2 \rfloor$. We define P-coefficients of A and B as

$$\vec{q}_{A,B} = (q_m, q_{m-1}, \ldots, q_0) \tag{17}$$

where

$$\begin{aligned} q_m &= 1, \\ q_{m-k} &= \sum_{\bar{C} \in \mathcal{C}_{1,k}} \mathrm{sgn}(\bar{C}) w_{A,B}(\bar{C}),\ \text{for } 1 \le k < n,\ \text{and} \\ q_0 &= \begin{cases} \displaystyle\sum_{\bar{C} \in \mathcal{C}_{1,n}} \mathrm{sgn}(\bar{C}) w_{A,B}(\bar{C}) \text{ if } n \equiv 0 \pmod 1, \\ \displaystyle\sum_{\bar{C} \in \mathcal{D}_{1,n}} \mathrm{sgn}(\bar{C}) w_{A,B}(\bar{C}) \text{ if } n \equiv 0 \pmod 0. \end{cases} \end{aligned} \tag{18}$$

where for a clow $C = \langle e_1, e_2, \ldots, e_{2k-1}, e_{2k}\rangle$, we define the weight

$$w_{A,B}(C) = a_{e_1} b_{e_2} \cdots a_{e_{2k-1}} b_{e_{2k}} \tag{19}$$

and for a clow sequence $\bar{C} = \langle C_1, \ldots, C_l\rangle$

$$w_{A,B}(\bar{C}) = \prod_{1 \le i \le l} w_{A,B}(C_i). \tag{20}$$

In [8], it is shown that $\mathrm{pf}(A)\,\mathrm{pf}(B) = q_0$. So this notion is a generalization of the clow presentation of Pfaffian pairs.

We will construct a recursive algorithm which computes P-coefficients (17).

Theorem 17. *Let*

$$A = \begin{pmatrix} 0 & R \\ -{}^tR & M \end{pmatrix},\ B = \begin{pmatrix} 0 & -{}^tS \\ S & M \end{pmatrix} \in \mathrm{Mat}(n,n)$$

, $m = \lfloor n/2 \rfloor$, $\vec{q}_{A,B}$ be P-coefficients of A and B. Let

$$\vec{q}_{M,N} = \begin{cases} (r_{m-1}, r_{m-2}, \ldots, r_0) & \text{if } n \equiv 0 \pmod 2 \\ (r_m, r_{m-1}, \ldots, r_0) & \text{if } n \equiv 1 \pmod 2. \end{cases}$$

If $n \equiv 0 \pmod 2$ then

$$\begin{pmatrix} q_m \\ q_{m-1} \\ q_{m-2} \\ \vdots \\ q_0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & & \\ -RS & 1 & \ddots & \\ -R(NM)S & -RS & \ddots & \\ \vdots & \vdots & \ddots & \\ -R(NM)^{m-1}S & -R(NM)^{m-2}S & \cdots & -RS \end{pmatrix} \begin{pmatrix} r_{m-1} \\ r_{m-2} \\ \vdots \\ r_0 \end{pmatrix} \tag{21}$$

and if $n \equiv 1 \pmod 2$ *then*

$$\begin{pmatrix} q_m \\ q_{m-1} \\ q_{m-2} \\ \vdots \\ q_0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & & \\ -RS & 1 & 0 & \ddots & \\ -R(NM)S & -RS & \ddots & & \\ \vdots & \vdots & \ddots & \ddots & \\ -R(NM)^{m-1}S & -R(NM)^{m-2}S & \cdots & -RS & 1 \end{pmatrix} \begin{pmatrix} r_m \\ r_{m-1} \\ r_{m-2} \\ \vdots \\ r_0 \end{pmatrix} \tag{22}$$

It is also provable in $\mathbf{V\#L}$ that Pfaffian computed by the algorithm given by Definition 1 is identical to that computed by Pfaffian pair A, J are identical. Generally we have the following:

Theorem 18 ($\mathbf{V\#L}$)**.** *Let* $A \in \mathrm{Mat}(2n, 2n)$ *be skew symmetric,* $\vec{q}_A$ *be P-coefficients of* A *and* $\vec{q}_{A,J}$ *be coefficients of P-coefficients of* A, J*. Then* $\vec{q}_A = \vec{q}_{A,J}$*.*

From this theorem it follows that Berkowitz type algorithm for $\mathrm{pf}(A)$ is a special case of that for Pfaffian pairs.

7 Closing remarks

We have proved that basic Pfaffian properties are provable from Pfaffian version of multiplicativity (MP). This fact is similar to that for the determinant where (MP) is replaced by the multiplicativity of the determinant. So it is natural to conjecture that (MP) is provable in $\mathbf{VNC}^2$.

In $\mathbf{V\#L}$, the determinant can be defined in two ways; one by Berkowitz algorithm for the determinant and the other defined from Pfaffian by the equation (2). It is easily seen that these two definitions are equivalent if we admit (PCE).

The algorithm for Pfaffian pairs presented in last section might give a possible approach for proving the multiplicativity of the determinant in $\mathbf{V\#L}$ or its mild extension. Namely, $\det(AB) = \det(A)\det(B)$ is equivalent to the identity

$$\mathrm{pf}\begin{pmatrix} 0 & AB \\ -{}^t(AB) & 0 \end{pmatrix} = (-1)^{n(n-1)/2}\,\mathrm{pf}\begin{pmatrix} 0 & A \\ -{}^tA & 0 \end{pmatrix}\mathrm{pf}\begin{pmatrix} 0 & B \\ -{}^tB & 0 \end{pmatrix} \tag{23}$$

Since both sides of this equation have combinatorial representation which are formalized in $\mathbf{V\#L}$, it is possible that it can be proved in the theory. However, such proof may be fairly complicated, so the first step to this approach may be to give an unformalized proof of equation (23).

Another interesting feature of Pfaffian pair is that it can formalize the Pfaffian version of multiplicativity (MP). So we may also expect that this is provable in $\mathbf{V\#L}$.

The ultimate goal of this work is to give candidate hard tautologies for Frege proof system which have quasi-polynomial Frege proofs. Since such tautologies are provable in weak systems which can formalize Pfaffian we believe that such candidate are consequences of Pfaffian identities considered in this article. So finding proofs of combinatorial theorems from Pfaffian will be our next step.

References

[1] S.J.Berkowitz, On computing the determinant in small parallel time using a small number of processors. Information Processing Letters. 18 (3): pp.147–150 (1984)

[2] S.A.Cook and P.Nguyen, Logical Foundations of Proof Complexity, Cambridge University Press, (2014)

[3] M.Soltys and S.A.Cook, The proof complexity of linear algebra, Annals of Pure and Applied Logic, Volume 130, Issues 1–3, (2004), pp.277-323.

[4] E.Ken and S.Kuroda, On matrix rank function over bounded arithmetics, preprint, arXiv:2310.05982, (2023)

[5] S. Kuroda, Formalizing Pfaffian in bounded arithmetic. manuscript. arXiv:2404.01728v1, (2024)

[6] M. Mahajan, P. R. Subramanya and V. Vinay, “ The Combinatorial Approach Yields an NC Algorithm for Computing Pfaffians ”, Discrete Appl. Math., 143:1–3 (2004) 1–16.

[7] 岡田聡一, Pfaffian Identities and Their Applications. 表現論シンポジウム講演集 2012, pp.69-91 (2012)

[8] G.Rote, Division-Free Algorithms for the Determinant and the Pfaffian: Algebraic and Combinatorial Approaches, n: ”Computational Discrete Mathematics.” Lecture Notes in Computer Science 2122, Springer-Verlag, pp.119–135 (2001)

[9] H.Straubing, A combinatorial proof of the Cayley-Hamilton theorem, Discrete Mathematics, Volume 43, Issues 2–3, 1983, Pages 273-279.

[10] I.Tzameret and S.A.Cook, Uniform, Integral, and Feasible Proofs for the Determinant Identities. Journal of the ACM, 68(2) (2021).

Department of Culture and Informatics
Gunma Prefectural Women’s University
1395-1,Tamamura,Gunma, 375-1193
JAPAN

群馬県立女子大学・文学部・文化情報学科　黒田 覚