Electronic Colloquium on Computational Complexity, Report No. 91 (2009)

On the Matching Problem for Special Graph Classes

Thanh Minh Hoang *
Institute for Theoretical Computer Science
University of Ulm
Germany

Abstract

In the present paper we show some new complexity bounds for the matching problem for special graph classes. We show that for graphs with a polynomially bounded number of nice cycles, the decision perfect matching problem is in **SPL**, it is hard for **FewL**, and the construction perfect matching problem is in $\mathbf{AC}^0(\mathbf{C_=L}) \cap \oplus\mathbf{L}$. We further significantly improve the upper bounds, proved in [AHT07], for the polynomially bounded perfect matching problem by showing that the decision version is in **SPL**, and the construction and the counting version are in $\mathbf{C_=L} \cap \oplus\mathbf{L}$. Note that **SPL**, $\oplus\mathbf{L}$, $\mathbf{C_=L}$, and $\mathbf{AC}^0(\mathbf{C_=L})$ are contained in $\mathbf{NC}^2$.

Furthermore, we show that the problem of computing a maximum matching for bipartite planar graphs is in $\mathbf{AC}^0(\mathbf{C_=L})$. This is a positive answer to Open Question 4.7 stated in the STACS'08-paper [DKR08] where it is asked whether computing a maximum matching even for bipartite planar graphs can be done in **NC**. We also show that the problem of computing a maximum matching for graphs with a polynomially bounded number of even cycles is in $\mathbf{AC}^0(\mathbf{C_=L})$.

1 Introduction

A set M of edges in an undirected graph G such that no two edges of M share a vertex is called a matching in G. A matching with a maximal cardinality is called maximum. A maximum matching is perfect if it covers all vertices in the graph. Graph matchings because of their fundamental properties are one of the most fundamental objects well-studied in mathematics and in theoretical computer science (see e.g. [LP86, KR98]). In the wide research-topic about graph matchings, perfect matchings and maximum matchings w.r.t. parallel computations receive a great interest.

From the viewpoint of complexity theory it is well-known that a maximum matching can be constructed efficiently in polynomial time [Edm65]. Hence the problem of deciding whether a graph has a perfect matching (short: DECISION-PM) and the problem of computing a perfect matching in a graph(short: SEARCH-PM) are in **P**. Regarding parallel computations, computing a maximum matching is known to be in randomized **NC** [KUW86, MVV87], and in nonuniform **SPL** [ARZ99] (see Section 2 for more detail of the complexity classes). Therefore, both problems DECISION-PM and SEARCH-PM are in nonuniform **SPL**. But it is a big open question whether DECISION-PM is in **NC**. Note that if the search version would be in **NC** then also the decision version of the problem. There is a huge gap among the complexities of the search and the counting version of the perfect matching problem (short: COUNTING-PM) because computing the number of all perfect matching in a bipartite graph is known to be #**P**-complete [Val79].

*Supported by DFG grant HO 4337/1-1.

ISSN 1433-8092

By Tutte's Theorem [Tut47] (see next section for more detail), the problem Decision-PM can be reduced to the problem of testing if a symbolic determinant is zero. This algebraic setting puts Decision-PM into a special case of the well-studied problem Polynomial Identity Testing (short: PIT) where PIT is the problem of testing if a polynomial given in an implicit form, like an arithmetic circuit or a symbolic determinant, is zero. PIT can be solved randomly by the Schwartz-Zippel Lemma [Sch80, Zip79], but whether the method can be derandomized is a very prominent open question. Due to a result by Impagliazzo and Kabanets [KI04] stating that the problem of derandomizing PIT is computationally equivalent to the problem of proving lower bounds for arithmetic circuits, the matching problem attracts a great attention.

The topic of the present paper is about the complexity of the matching problem. The motivation for the work comes directly from the crucial importance of the matching problem mentioned above. Since it is open whether the perfect matching problem is in **NC**, diverse special cases of the problem have been studied and solved before. For example, **NC** algorithms are known for Decision-PM for the following graph classes: planar graphs [Kas67, Vaz89], regular bipartite graphs [LPV81], strongly chordal graphs [DK86], and dense graphs [DHK93]. Search-PM is also known in **NC** for bipartite planar graphs [MN95, MV00, DKR08], and for graphs with a polynomially bounded number of perfect matchings [GK87, AHT07].

In the first part of the paper, in Section 3, we focus on the complexity of the perfect matching problem for graphs with a polynomially bounded number of so-called *nice cycles*. An even cycle C in a graph G is called nice [LP86] if the graph obtained from G by deleting all vertices of C has some perfect matching. Since the number of nice cycles in a graph is at most the number of all perfect matching in the graph, the considered problem seems to be a generalization of the polynomially bounded perfect matching problem. But note that the number of all perfect matchings in a graph with a polynomially bounded number of nice cycles may be exponentially big. The polynomially bounded perfect matching problem has been investigated first by Grigoriev and Karpinski [GK87], then Agrawal, Hoang, and Thierauf [AHT07] improve the $\mathbf{NC}^3$ upper bound stated in [GK87] to $\mathbf{NC}^2$ for it.

In Section 3, following a general paradigm for derandomizing polynomial identity testing by Agrawal [Agr03] and by a method which is different from the method of [AHT07] for solving the polynomially bounded perfect matching problem, we show that for graphs with a polynomially bounded number of nice cycles

- Decision-PM is in **SPL**, it is hard for **FewL**, and
- Search-PM is in $\mathbf{AC}^0(\mathbf{C_=L}) \cap \oplus\mathbf{L}$,

where $\mathbf{FewL} \subseteq \mathbf{SPL} \subseteq \oplus\mathbf{L} \subseteq \mathbf{NC}^2$ and $\mathbf{SPL} \subseteq \mathbf{C_=L} \subseteq \mathbf{AC}^0(\mathbf{C_=L}) \subseteq \mathbf{NC}^2$ (see Section 2 for more detail of these complexity classes). Furthermore, our method gives further a significant improvement of the complexity bounds proved in [AHT07]. In particular, we show that both the construction and the counting versions, Search-PM and Counting-PM, of the polynomially bounded perfect matching problem are in $\mathbf{C_=L} \cap \oplus\mathbf{L}$. Moreover, our result gives an evidence that in general the perfect matching problem might be solvable by the concept we describe in Section 5.

In the second part of the paper, in Section 4, we show an algebraic method for constructing a maximum matching once there some weight function for isolating a maximum matching is given. By this method we give a positive answer to Open Question 4.7 in [DKR08] which is asked whether the problem of constructing a maximum matching even for bipartite planar graphs is in **NC**. Namely, we show that the maximum matching problem for bipartite planar graphs is in $\mathbf{AC}^0(\mathbf{C_=L})$. Furthermore, we show that the maximum matching problem for graphs with a polynomially bounded number of even cycles is also in $\mathbf{AC}^0(\mathbf{C_=L})$.

2 Preliminaries

Algebraic Graph Theory. We describe some basic materials about graph matchings. For more detail we refer the readers to [LP86, MSV99] and to standard textbooks in linear algebra and in graph theory.

Let $G = (V, E)$ be an undirected graph with n vertices, $V = \{1, 2, \ldots, n\}$, and m edges $E = \{e_1, \ldots, e_m\} \subseteq V \times V$. A *matching* in G is a set $M \subseteq E$, such that no two edges in M have a vertex in common. A matching M is called *perfect* if M covers all vertices of G, i.e. $|M| = \frac{1}{2}\, n$, M of maximal size is called *maximum*. The weight of a matching in a weighted graph is defined as the sum of all weights of the edges in the matching.

Basically, graph G can be presented by its *adjacency matrix*. This is an $n \times n$ symmetric matrix $A \in \{0,1\}^{n \times n}$ where $A_{i,j} = 1$ iff $(i, j) \in E$, for all $1 \leq i, j \leq n$. Assign weights $w(i, j)$ to edges (i, j) to get the *weighted* graph G. Assign orientations to the edges of weighted graph G, i.e. edge (i, j) gets one of two orientations, from i to j or from j to i, we obtain an orientation $\vec{G}$ for which we have a so-called *Tutte skew-symmetric matrix* T as follows:

$$T_{i,j} = \begin{cases} A_{i,j}\ w(i,j)\ , & \text{if an edge of } \vec{G} \text{ is directed from } i \text{ to } j, \\ -A_{i,j}\ w(i,j)\ , & \text{otherwise.} \end{cases}$$

In the case when all directed edges of $\vec{G}$ are oriented from smaller to larger vertices, the orientation $\vec{G}$ and the matrix T are called *canonical*. The Pfaffian of a skew-symmetric matrix T from an orientation $\vec{G}$, denoted by $\mathrm{pf}(T)$ or $\mathrm{pf}(\vec{G}, w)$, is defined as follows:

$$\mathrm{pf}(\vec{G}, w) \quad = \sum_{\text{perfect matching } M \text{ in } G} \mathrm{sign}(M)\ \mathrm{value}(M)$$

where $\mathrm{sign}(M) \in \{-1, +1\}$ is the sign of M that depends on the orientation $\vec{G}$, and $\mathrm{value}(M) = \prod_{(i,j) \in M} w(i, j)$ is the value of M that depends on the weighting scheme for G. It is known from linear algebra that $\det(S) = \mathrm{pf}^2(S)$ if S is a skew-symmetric matrix of even order, and $\mathrm{pf}(S) = 0$ for all skew-symmetric matrices of odd order. We refer the reader to [Kas67, MSV99] for more detail of the Pfaffian.

Assign indeterminates $x_{i,j}$ to the edge (i, j) of a graph G we get the graph $G(X)$. Let $T(X)$ be the canonical Tutte skew-symmetric matrix of $G(X)$. The perfect matching problem can be decided randomly by the following theorem and by using Schwartz-Zippel Lemma [Sch80, Zip79].

Theorem 2.1 (Tutte) *Graph G has no perfect matching iff* $\mathrm{pf}(T(X)) = 0$.

An orientation such that all perfect matchings in G have the same sign $+1$ (or -1) is called a *Pfaffian orientation* [Kas67]. Hence the number of perfect matchings in a graph G can be computed by finding a Pfaffian orientation in it and then by computing the Pfaffian. But there are graphs which do not admit any Pfaffian orientation, the complete bipartite graph $K_{3,3}$ is an example of them. However, planar graphs [Kas67] and $K_{3,3}$-free graphs [Vaz89] admit always Pfaffian orientations which are in **NC** computable,and thus the number of all perfect matchings in such a graph can be computed efficiently.

Complexity Classes.

Basically, the complexity classes **P**, **L**, **NP**, and **NL** are well known. As stated below, we mention briefly some other classes within we are working. More detail of these classes can be found in e.g. [AO96, ABO99, ARZ99].

The classes $\mathbf{NC}^k$, for fixed k, consists of families of Boolean circuit with $\wedge$-, $\vee$-gates of fan-in 2, and $\neg$ -gates, of depth $O(\log^k n)$ and of polynomial size. $\mathbf{NC} = \cup_{k \geq 0} \mathbf{NC}^k$. The classes $\mathbf{AC}^0$

is defined as the set of families of Boolean circuit with (unbounded fan-in) $\wedge$-, $\vee$-gates, and $\neg$ -gates, of constant-depth and of polynomial-size. It is know that

$$\mathbf{AC}^0 \subseteq \mathbf{NC}^1 \subseteq \mathbf{L} \subseteq \mathbf{NL} \subseteq \mathbf{NC}^2 \subseteq \mathbf{NC} \subseteq \mathbf{P}.$$

For an **NL** machine M, we denote the number of accepting and rejecting computation paths on input x by $\#acc_M(x)$ and by $\#rej_M(x)$, respectively. **FewL** is the class of languages accepted by **NL** machines with at most a polynomial number of accepting computations [BDHM91]. The class **GapL** consists of all functions gap_M, where M is an **NL**-machine, and for all x, $gap_M(x) = \#acc_M(x) - \#rej_M(x)$. This class is characterized by the determinant of integer matrices [Dam91, Tod91, Vin91, Val92]. Note that the determinant of an integer matrix is in $\mathbf{NC}^2$ [Ber84]. **GapL** is closed under addition, subtraction, multiplication, and restricted composition [AO96, AAM03]. The following classes are related to **GapL**.

- $\oplus\mathbf{L}$ is the class of sets A for which there exists a function $f \in \mathbf{GapL}$ such that $\forall\, x :\ x \in A \Longleftrightarrow f(x) \not\equiv 0 (\mod 2)$. Obviously, we have $\mathbf{L}^{\oplus\mathbf{L}} = \oplus\mathbf{L}$.

- $\mathbf{C_{=}L}$ (*Exact Counting in Logspace*) consists of all problems of verifying a **GapL**-function, i.e. it is the class of sets A for which there exists a function $f \in \mathbf{GapL}$ such that $\forall\, x :\ x \in A \Longleftrightarrow f(x) = 0$.

- The Hierarchy over $\mathbf{C_{=}L}$ collapses to $\mathbf{AC}^0(\mathbf{C_{=}L})$ [ABO99], i.e. $\mathbf{L}^{\mathbf{C_{=}L}} = \mathbf{AC}^0(\mathbf{C_{=}L})$, which is the class of all problems $\mathbf{AC}^0$-reducible to $\mathbf{C_{=}L}$. The problem of computing the rank of an integer matrix is complete for $\mathbf{AC}^0(\mathbf{C_{=}L})$.

- **SPL** [ARZ99] is the class of all languages for which their characteristic functions are in **GapL**, i.e. $\mathbf{SPL} = \{L \in \Sigma^* | \chi_L \in \mathbf{GapL}\}$. It is known that **SPL** is closed under complement, i.e. $\mathbf{L}^{\mathbf{SPL}} = \mathbf{SPL}$. Note that the conclusion $\mathbf{NL} \subseteq \mathbf{SPL}$ remains open.

We list some known conclusions among the mentioned classes:

$$\mathbf{L} \subseteq \mathbf{FewL} \subseteq \mathbf{SPL} \subseteq \mathbf{C_{=}L} \subseteq \mathbf{AC}^0(\mathbf{C_{=}L}) \subseteq \mathbf{NC}^2,$$
$$\mathbf{SPL} \subseteq \oplus\mathbf{L} \subseteq \mathbf{NC}^2, \qquad \mathbf{L} \subseteq \mathbf{FewL} \subseteq \mathbf{NL} \subseteq \mathbf{C_{=}L}, \qquad \mathbf{L} \subseteq \#\mathbf{L} \subseteq \mathbf{GapL} \subseteq \mathbf{NC}^2.$$

In this paper we study the following problems. Given a graph G

- Decision-PM is the problem of deciding whether G has some perfect matchings,

- Search-PM is the problem of computing a perfect matching in G,

- Counting-PM is the problem of computing the number of perfect matchings in G,

- Search-MM is the problem of computing a maximum matching in G.

The Pfaffian of an integer skew-symmetric matrix is known to be in **GapL** [MSV99]. Given a univariate polynomial matrix $A(x)$, i.e. the elements of $A(x)$ are polynomials in x of logarithmic bit long in the degree, the problem of computing $\det(A(x))$ is known to be in **GapL** [AAM03]: all the coefficients of $\det(A(x))$ are computable in **GapL**. By following the latter and the combinatorial setting for Pfaffians in [MSV99], it is not hard to show that in the case when $A(x)$ is skew-symmetric, all the coefficients of $\mathrm{pf}(A(x))$ are **GapL**-computable.

3 Isolating and computing a perfect matching

In this section we show that the perfect matching problem for graphs with a polynomially bounded number of nice cycles is in $\mathbf{NC}^2$.

W.r.t. parallel computations, a perfect matching can be computed by two steps: one can first isolate a perfect matching by a weight function and then extract out the isolated perfect matching. (Obviously, the decision perfect matching problem follows from computing a perfect matching.) By this method, Isolating Lemma [MVV87] is a powerful tool for isolating a perfect matching. We state it as follows.

Lemma 3.1 (Isolating Lemma [MVV87]) *Let U be a universe of size m and S be a considered family of subsets of U. Let $w : U \to \{1, \ldots, 2m\}$ be a random weight function. Then with probability at least $\frac{1}{2}$ there exists a unique minimum weight subset in S.*

Let $G = (V, E)$ be a graph with n vertices $V = \{1, 2, \ldots, n\}$, m edges $E = \{e_1, e_2, \ldots, e_m\}$, and with at most n^k nice cycles where k is a fixed positive integer. Recall that an even cycle C in G is called nice if the graph obtained by deleting from G all vertices of C has some perfect matchings or it is empty. Now we show how to deterministically isolate a perfect matching in G.

Let w be a weight function for the edges of G, i.e. edge e gets the weight $w(e)$, for every e. Observe that a simple cycle C (in G) with $2l$ edges, $l > 0$, has exactly two perfect matchings N_1 and N_2, each of them is of size l. By $W(N_1)$ and $W(N_2)$ we denote the weights of N_1 and N_2, respectively. Recall that the weight of a matching is the sum of all weights on the edges of this matching. The difference of the weights of two perfect matchings in an even cycle is called the *circulation* of the cycle [DKR08]:

$$\text{circulation}(C) = |W(N_1) - W(N_2)|.$$

The circulations of nice cycles play a central role for isolating a perfect matching in a graph. Lemma 3.2 in [DKR08] states that if all the cycles of a bipartite graph have non-zero circulations, then the minimum weight perfect matching in it is unique. In general, Lemma 3.2 in [DKR08] holds also for non-bipartite graphs. We omit the proof of the following lemma because it is in analogy to the proof of Lemma 3.2 in [DKR08].

Lemma 3.2 ([DKR08]) *If all nice cycles in a weighted graph have non-zero circulations, then there is a unique minimum weight perfect matching in it.*

It is easy to see that the converse of Lemma 3.2 is not true. For example: we can assign integer weights to 6 edges of K_4, the complete graph with 4 vertices, such that the minimum weight perfect matching is unique but there is a nice cycle of zero circulation.

We call a weight function *admissible* for G if it assigns positive integers with a logarithmically bounded number of bits to the edges of a graph G such that a minimum weight perfect matching becomes unique. By Lemma 3.2, in order to isolate deterministically a perfect matching we can determine an admissible weight function such that all nice cycles in the graph get non-zero circulations.

Lemma 3.3 *Let $G = (V, E)$ be an undirected graph with $|V| = n$ vertices and m edges $E = \{e_1, e_2, \ldots, e_m\}$, and let the number of nice cycles in G be at most n^k, for some positive constant k. Then there exists a prime number $p \leq 2n^k(m+1)$ such that the weight function $w_p : E \mapsto \mathbb{Z}_p$ where $w_p(e_i) = 2^i \mod p$ is admissible for G.*

Proof. Assign 2^i to every edge e_i in G. Then each nice cycle C in G has a non-zero circulation because two perfect matchings defined in C have different weights. Consider the product of all the circulations:

$$Q = \prod_{C \text{ is a nice cycle}} \text{circulation}(C).$$

Since the number of nice cycles in G is at most n^k and since $0 < \text{circulation}(C) < 2^{m+1}$ holds for every nice cycle C, we get $0 < Q \leq 2^{n^k(m+1)}$. It is well-known from Number Theory that

$$\prod_{\text{all primes } p_i \leq 2N} p_i > 2^N, \text{ for all } N > 2.$$

Therefore, there exists a prime $p \leq 2n^k(m+1)$ such that p is not a factor of Q, i.e. we have $Q \mod p \neq 0$, or equivalently: $\text{circulation}(C) \mod p \neq 0$ for all nice cycles C in G. Hence by Lemma 3.2 a minimum weight perfect matching becomes unique under the weight function $w_p : E \to \mathbb{Z}_p$ where

$$w_p(e_i) = 2^i \mod p, \text{ for } i = 1, 2, \ldots, m.$$

Note that all the primes $q < 2n^k(m+1)$ and the weight functions w_q are computable in logspace. This completes the proof of the lemma. $\square$

Lemma 3.3 can be used for isolating a perfect matching in a graph with a polynomially bounded number of nice cycles. Recall Isolating Lemma [MVV87] that by randomly assigning small weights to all the edges of a graph with high probability we get a unique minimum weight perfect matching. Hence Isolating Lemma for isolating a perfect matching will be derandomized if there exists an admissible weight function for any graph. We conjecture that there is an **NC**-computable admissible weight function for an arbitrary graph. In Section 5 we give a discussion on this topic.

Theorem 3.4 *For graphs with a polynomially bounded number of nice cycles the decision perfect matching problem* Decision-PM *is in* **SPL**, *and the construction perfect matching problem* Search-PM *is in* $\mathbf{AC}^0(\mathbf{C_=L}) \cap \oplus\mathbf{L}$.

Proof. Let $G = (V, E)$ be a graph with n vertices, m edges $E = \{e_1, \ldots, e_m\}$, and with at most n^k nice cycles, for some positive constant k. Let $U = \{p_1, \ldots, p_t\}$ be the set of all primes at most $2n^k(m+1)$, for some t. Define the weight functions $w_p : E \to \mathbb{Z}_p$, for each $p \in U$, where $w_p(e_i) = 2^i \mod p$ for every edge e_i.

Let x be an indeterminate. Assign $x^{w_p(e)}$ to each edge e in G to get the graphs $G_p(x)$, for every $p \in U$. By $G_p^{(-e)}(x)$ we denote the result of deleting edge e from $G_p(x)$. The canonical Tutte skew-symmetric matrices of $G_p(x)$ and $G_p^{(-e)}$ we denote respectively by $T_p(x)$ and by $T_p^{(-e)}(x)$. Considering the Pfaffian of these matrices we observe that in the Pfaffian polynomial, the value of a perfect matching M becomes $x^{W(M)}$ where $W(M)$ is the weight of M, the coefficient of $x^{W(M)}$ in the polynomial is the sum of all signs of all perfect matchings having the same weight $W(M)$. Define $K = n^{k+1}(m+1)$. Then we can write:

$$\begin{aligned} \text{pf}(T_p(x)) &= c_{p,0} + c_{p,1}x^1 + \cdots + c_{p,K}x^K, \\ \text{pf}(T_p^{(-e)}(x)) &= c_{p,0}^{(-e)} + c_{p,1}^{(-e)}x^1 + \cdots + c_{p,K}^{(-e)}x^K. \end{aligned}$$

It is clear that all $\text{pf}(T_p(x))$ and $\text{pf}(T_p^{(-e)}(x))$ vanish if G has no perfect matching.

Consider the case when G has a perfect matching. By Lemma 3.3 there exists some $p \in U$ such that the graph G under w_p has a unique minimum weight perfect matching. Let M_0 be this unique matching and let I be its weight under w_p. Observe that the coefficient of x^I in $\mathrm{pf}(T_p(x))$, occurred as the lowest non-zero coefficient in the polynomial, should be $c_{p,I} = \mathrm{sign}(M_0) \in \{+1, -1\}$, or equivalently $c_{p,I}^2 = 1$. Recall from Section 2 that all the coefficients of the polynomials we consider are computable in **GapL**. Therefore the following *zero-one-valued* **GapL**-function

$$h(G) = 1 - \prod_{0 \le i \le K,\ p \in U} (1 - c_{p,i}^2)$$

is the characteristic function for the problem of testing if G has a perfect matching, i.e. Decision-PM is in **SPL**.

It remains to show that Search-PM $\in \mathbf{AC}^0(\mathbf{C_=L}) \cap \oplus\mathbf{L}$. Observe that if w_p is admissible for G, then G has the unique minimum weight perfect matching M_0 with weight $0 \le I \le K$. Thus we have

$$c_{p,I}^2 = 1 \text{ and } c_{p,I}^{(-e)} = \begin{cases} 0\ , & \text{if } e \in M_0 \\ c_{p,I}\ , & \text{otherwise.} \end{cases}$$

Therefore, in $\mathbf{C_=L}$ we can construct all edge-sets $M_{p,i}$ as follows:

$$e \in M_{p,i} \text{ iff } c_{p,i}^2 = 1 \textbf{ and } c_{p,i}^{(-e)} = 0, \text{ for each edge } e, \text{ for all } p \in U \text{ and } 0 \le i \le K.$$

It is easy to see that the same edge-sets will be constructed by the same procedure in $\mathbb{Z}_2$, i.e. in $\oplus\mathbf{L}$ we can construct all the sets $M_{p,i}$. After that in logspace we can determine and output all perfect matchings from the constructed edge-sets $M_{p,i}$. Note that there at least one edge-set, namely $M_{p,I}$, from our construction is indeed a perfect matching in G.

Since $\mathbf{L}^{\mathbf{C_=L}} = \mathbf{AC}^0(\mathbf{C_=L})$ [ABO99] and since $\mathbf{L}^{\oplus\mathbf{L}} = \oplus\mathbf{L}$, we obtain Search-PM $\in \mathbf{AC}^0(\mathbf{C_=L}) \cap \oplus\mathbf{L}$. This completes the proof of the theorem. □

Allender et. al. [ARZ99] show that in general a perfect matching can be constructed in nonuniform **SPL**. Unfortunately, in the proof of Theorem 3.4 we do not know how to perform in (uniform) **SPL** the decision which prime p from U is "right" for isolating a minimum weight perfect matching.

The best-known upper bounds for the polynomially bounded perfect matching problem taken from [GK87, AHT07] are given in the following theorem.

Theorem 3.5 ([AHT07]) *For graphs with polynomially bounded number of perfect matchings, the decision problem is in* $\mathbf{coC_=L}$*, the counting problem is in* $\mathbf{AC}^0(\mathbf{C_=L})$*, and all the perfect matchings can be constructed in* $\mathbf{NC}^1(\mathbf{GapL})$.

Note that $\mathbf{coC_=L} \subseteq \mathbf{AC}^0(\mathbf{C_=L}) \subseteq \mathbf{NC}^1(\mathbf{GapL}) \subseteq \mathbf{NC}^2$ where $\mathbf{NC}^1(\mathbf{GapL})$ is the class of all problems $\mathbf{NC}^1$-reducible to the determinant. We improve the bounds given in Theorem 3.5 by the following theorem.

Theorem 3.6 *For graphs with a polynomially bounded number of perfect matching*

1. *the decision problem* Decision-PM *is in* **SPL***, it is hard for* **FewL***, and*
2. *all the perfect matchings can be constructed in* $\mathbf{C_=L} \cap \oplus\mathbf{L}$*. The number of all perfect matchings can be computed in* $\mathbf{C_=L}$.

Proof. (1) By Theorem 3.4 we get Decision-PM $\in$ **SPL**. We omit the proof that Decision-PM is hard for **FewL** since it is straightforward by modifying the reduction from the directed connectivity problem, which is **NL**-complete, to the bipartite unique perfect matching problem [HMT06], or to the bipartite perfect matching problem [CSV84].

(2) Let $G = (V, E)$ be an undirected graph with n vertices, m edges $|E| = \{e_1, \ldots, e_m\}$, and with at most n^k perfect matchings. We show how to construct all perfect matching in G. Our construction consists of two standard steps as follows:

a) compute a prime p such that $w_p : w_p(e_i) = 2^i \mod p$ isolates all perfect matchings,

b) construct all perfect matchings from the Pfaffians $\mathrm{pf}(T_p(x))$ and $\mathrm{pf}(T_p^{(-e)}(x))$.

Consider Step a). Let's call a prime p from Step a) *"right"* if w_p isolates all perfect matchings in G. Observe that any perfect matchings M and N have different weight under $w : w(e_i) = 2^i$, i.e. $0 < |W(M) - W(N)| < 2^{m+1}$ where $W(M)$ and $W(N)$ are the weights of M and N, respectively.

$$0 < Q := \prod_{M \neq N} |W(M) - W(N)| \quad < \quad 2^{(m+1)\ \binom{n^k}{2}} \quad < \quad 2^{\frac{1}{2}\ (m+1)\ n^{2k}}.$$

Therefore, there exists a prime $p \leq (m+1)\ n^{2k}$ such that $Q \mod p \neq 0$.

Define $U = \{p_1, p_2, \ldots, p_l\}$ as the set of all primes at most $(m+1)\ n^{2k}$. Observe that prime $p \in U$ is "right" iff in $\mathrm{pf}(T_p(x))$ *all coefficients should be contained in* $\{-1, 0, +1\}$ **and** *the number of non-zero coefficients should be maximized.* The latter is the number of perfect matchings in G.

Define $K = (m+1)n^{2k}$, and for every $q, q' \in U$ define the following **GapL**-functions:

$$h_q := \textstyle\sum_{i=0}^{K}(c_{q,i}^2 - 1)\ c_{q,i}^2, \quad g_q := \sum_{i=0}^{K} c_{q,i}^2, \quad H_{q,q'} := \prod_{a=1}^{Kn^{4k}} (h_{q'} - a)\ \prod_{a=0}^{Kn^{2k}} (g_q - g_{q'} - a).$$

We see that $h_q = 0$ iff all $c_{q,i} \in \{-1, 0, 1\}$. For a "right" prime p, g_p is the number of all non-zero coefficients. Moreover, observe that $H_{q,q'} = 0$ iff $h_{q'} \neq 0$ or $g_q = g_{q'} + a$ for some non-negative integer a. Hence we get $g_q > g_{q'}$ as long as $h_{q'} = 0$. Thus, in $\mathbf{C_=L}$ we can select a "right" prime p from U as follows:

$$p \text{ is "right" iff} \quad h_p = 0 \textbf{ and } H_{p,q} = 0 \text{ for all } p \neq q \in U.$$

Consider Step b). In $\mathbf{C_=L}$ we can construct the edge-sets $M_{p,i}$ corresponding to $c_{p,i} \in \{-1, +1\}$ in $\mathrm{pf}(T_p(x))$ as stated in the proof of Theorem 3.4. Note that after Step b) we do not recheck whether the constructed edge-sets are perfect matchings. This shows that all perfect matchings in G can be constructed in $\mathbf{C_=L}$.

The problem is also in $\oplus\mathbf{L}$ by following the proof of Theorem 3.4. The number of all perfect matchings in G can be computed in $\mathbf{C_=L}$ by verifying $g_p = a$, for some $a \leq n^k$ and by testing if p from U is "right".

This completes the proof of the theorem. □

4 Isolating and computing a maximum matching

We show the following lemma.

Lemma 4.1 *Given a weight function w that assigns logarithmic bit long positive integers to the edges of a graph G such that the weight of a maximum matching in G becomes unique, the problem of computing a maximum matching in G is $\mathbf{AC}^0(\mathbf{C_=L})$-reducible to the problem of computing a perfect matching in a subgraph of G.*

Proof. Let $G = (V, E)$ be a graph with n vertices and m edges. Let M be a maximum matching of G, and let $|M| = l$ for some positive integer l. Suppose the weight of M is unique under the weight function w. By G_M we denote the subgraph of G, obtained by deleting $n - 2l$ vertices which are not covered by M.

Observe that the maximum matching M in G becomes perfect and unique in G_M under the weight function w. Therefore, the computation of M can be done by computing G_M and then by extracting a perfect matching in G_M.

Let x be an indeterminate. By $G(x)$ we denote the graph G by assigning $x^{w(e)}$ to every edge e of G. By this weighting scheme we obtain $G_M(x)$ from G_M. Let $T_G(x)$ and $T_{G_M}(x)$ be the canonical Tutte skew-symmetric matrix of $G(x)$ and of $G_M(x)$, respectively.

Since in G_M the weight of the perfect matching M is unique under w, the Pfaffian polynomial $\mathrm{pf}(T_{G_M}(x))$ should be non-zero and the order of $T_{G_M}(x)$ should be $2l$. Hence we have $\det(T_{G_M}(x)) = \mathrm{pf}^2(T_{G_M}(x)) \neq 0$, and $\mathrm{rank}(T_{G_M})(x) = 2l$. Moreover, since l is maximum, $T_{G_M}(x)$ is a maximal non-singular polynomial skew-symmetric sub-matrix of $T_G(x)$. As a consequence we have $\mathrm{rank}(T_G(x)) = \mathrm{rank}(T_{G_M})(x) = 2l$.

Conversely, consider an n-bit vector $\vec{b}$ associated to a maximal set of linearly independent columns of $T_G(x)$. We call vector $\vec{b}$ a *column-basis* of $T_G(x)$. Observe that the subgraph $G_{\vec{b}}$ of G that contains all vertices i of G such that $\vec{b}_i = 1$ has always perfect matchings of the size l, and these matchings are maximum in G. Thus, in order to compute a subgraph having a maximum matching of G we can compute a column-basis of $T_G(x)$.

The problem of computing a column-basis of an integer matrix [zG93] is known to be in $\mathbf{AC}^0(\mathbf{C_=L})$. For polynomial matrices, we show that a) the problem of computing a column-basis is reduced to the problem of computing the rank and b) the rank can be computed in $\mathbf{AC}^0(\mathbf{C_=L})$.

a) Let $A(x)$ be an $n \times n$ univariate polynomial matrix where the degrees of matrix elements are at most n^c, for some positive constant c. Let $\vec{a_1}(x), \ldots, \vec{a_n}(x)$ be its columns. One has to compute a column-basis of $A(x)$.

   Let $A_i(x)$ be the matrix formed by the first i columns $\vec{a_1}(x), \ldots, \vec{a_i}(x)$ of $A(x)$, for all $1 \leq i \leq n$. It is well known from linear algebra that a column-basis can be selected as the collection of all $\vec{a_i}(x)$ where $\mathrm{rank}(A_{i-1}(x)) + 1 = \mathrm{rank}(A_i(x))$, for every $1 \leq i \leq n$. Therefore, the computation of a column-basis is reduced to the problem of computing the rank of a polynomial matrix.

b) Let $B(x)$ be an $n \times m$ univariate polynomial matrix, where the degrees of the matrix-elements are at most n^c, for some positive constant c. One has to compute $\mathrm{rank}(B(x))$.

   It is known that $2\ \mathrm{rank}(B(x)) = \mathrm{rank}(C(x))$ where $C(x) = \begin{pmatrix} \mathbf{0} & B(x) \\ B^t(x) & \mathbf{0} \end{pmatrix}$ and $B^t(x)$ is the transpose of $B(x)$. Since $C(x)$ is an $N \times N$ symmetric matrix, where $N = m + n$, we can compute $\mathrm{rank}(C(x))$ by the characteristic polynomial $\chi_C(x) = \det(yI - C(x))$, where y is an indeterminate.

   Let $\chi_C(x) = y^N + p_{N-1}(x)y^{N-1} + \cdots + p_1(x)y + p_0(x)$, where $p_i(x)$ is a polynomial in x. It is known that, for some $0 \leq j \leq N$, $\mathrm{rank}(C(x)) = j$ iff $p_0(x) = \cdots = p_{N-j-1}(x) = 0$ and $p_{N-j}(x) \neq 0$.

   Consider a polynomial $p_i(x)$ of them. If $p_i(x) = 0$ then it is clear that $p_i(a) = 0$ for all a's. Otherwise, if $p_i(x) \neq 0$ then there exists an integer a from a set $S = \{0, 1, \ldots, \deg(p_i(x))\}$ such that $p_i(a) \neq 0$. Since $\deg(p_i(x)) \leq N\ n^c = (m + n)n^c$, for all $0 \leq i \leq N - 1$, where c is a constant, define $S = \{0, 1, \ldots, (m + n)n^c\}$. In summary, the rank of $B(x)$ is equal the maximal rank of the matrices $B(a)$, for $a \in \{0, 1, \dots, (m+n)n^c\}$. Note that the rank of integer matrices is known to be in $\mathbf{AC}^0(\mathbf{C_=L})$ [ABO99].

This completes the proof of the lemma. $\square$

Now we solve the maximum matching problem for bipartite planar graphs.

Lemma 4.2 ([DKR08]) *In logspace one can assign polynomially bounded weights to the edges of a bipartite planar graph such that the circulation of any cycle is non-zero.*

By Lemma 4.1, a subgraph G_M of a given bipartite planar graph G can be computed in $\mathbf{AC}^0(\mathbf{C_=L})$ such that perfect matchings in G_M are maximum in G. Computing a perfect matching for bipartite planar graphs is in **SPL** [DKR08]. Since $\mathbf{SPL} \subseteq \mathbf{C_=L} \subseteq \mathbf{AC}^0(\mathbf{C_=L})$, the maximum matching problem for bipartite planar graph is in $\mathbf{AC}^0(\mathbf{C_=L})$. This is a positive answer to Open Question 4.7 stated in [DKR08].

Theorem 4.3 *The maximum matching problem for bipartite planar graph is in* $\mathbf{AC}^0(\mathbf{C_=L})$.

A promise version of the maximum matching problem which is in **NC** is given by the following theorem.

Theorem 4.4 *The maximum matching problem for graphs with a polynomially bounded number of even cycles is in* $\mathbf{AC}^0(\mathbf{C_=L})$.

Proof. Let G be a graph with a polynomially bounded number of even cycles. In analogy to Lemma 3.3 we can show that there exists a small prime p such that all even cycles in G haven non-zero circulations under $w_p : E \mapsto \mathbb{Z}_p$ where $w_p(e_i) = 2^i \mod p$, for every edge e_i. Thus, all nice cycles in any subgraph H of G such that perfect matchings in H are maximum matchings in G have non-zero circulations under w_p. Hence by Lemma 3.2 H has a unique minimum weight perfect matching. By Lemma 4.1 such a graph H can be computed in $\mathbf{AC}^0(\mathbf{C_=L})$. By Theorem 3.4 a perfect matching in H can be computed in $\mathbf{AC}^0(\mathbf{C_=L})$. Therefore a maximum matching in G can be computed in $\mathbf{AC}^0(\mathbf{C_=L})$. $\square$

5 Discussion

As we have seen in the paper, deterministic isolations of matchings in a graph play a crucial role for a potential **NC** algorithm for both the decision and the search versions of the matching problem. Such a isolation has been show for bipartite planar graphs [DKR08], for graphs with a polynomially bounded number of perfect matchings [AHT07], and for graphs with a polynomially number of nice cycles (the present paper). We don't know if the method used in the paper works also in general for solving the perfect matching problem (without any promise). We conjecture that the method stated bellow can be used for isolating a perfect matching in general.

Assign to each edge e_i of the graph G a polynomial $g_i(x)$ in x such that the circulation polynomial $p_C(x)$ of each even cycle C is non-zero in the ring $\mathbb{Z}[x]$, for example: $g_i(x) := a_i x^i$ for arbitrary small integers a_i. Consider $p_C(x)$ in the field $\mathbb{F} = \mathbb{Z}_P[x]/(h(x))$ where P is a small prime (polynomially bounded) and $h(x)$ is an irreducible polynomial in the polynomial ring $\mathbb{Z}_P[x]$. Since $\mathbb{F}$ has $P^{\deg(h)}$ elements, we need to chose $h(x)$ of a constant degree, say $\deg(h(x)) \leq l$ for a constant l. If all the polynomials $p_C(x)$ are non-zero in $\mathbb{F}$, then there exists $a \in \mathbb{Z}_Q$, where Q is a small prime of the size at least $P^l \leq n^{kl}$, such that all the circulation polynomials do not vanish at the point a. Formally, we have $(p_C(x) \mod P, h(x)) \mod Q, x - a \neq 0$ for all C under the weight function $w : \ w(e_i) := (a_i x^i \mod P, h(x)) \mod Q, x - a$, for every edge e_i.

The main problem we have to avoid is that how to define $g_i(x), h(x)$, and P such that $p_C(x)$ is in $\mathbb{F} \setminus 0$ for every C. A positive answer to this question would give a deterministic isolation as described. A classification of special graphs for which the described isolation works may be helpful.

Acknowledgment

The author wishes to thank Meena Mahajan, Prajakta Nimbhorkar, and Jacobo Torán for fruitful discussions on the topic of the paper.

References

[AAM03] E. Allender, V Arvind, and M. Mahajan. Arithmetic complexity, Kleene closure, and formal power series. *Theory of Computing Systems*, 36(4):303–328, 2003.

[ABO99] E. Allender, R. Beals, and M. Ogihara. The complexity of matrix rank and feasible systems of linear equations. *Computational Complexity*, 8:99–126, 1999.

[Agr03] M. Agrawal. On derandomizing tests for certain polynomial identities. In *18th Annual IEEE Conference on Computational Complexity (CCC)*, page 355. IEEE Computer Society, 2003.

[AHT07] M. Agrawal, T. M. Hoang, and T. Thierauf. The polynomially bounded perfect matching problem is in $\mathbf{NC}^2$. In *24th Annual Symposium on Theoretical Aspects of Computer Science (STACS)*, LNCS, pages 489–499. Springer Verlag, 2007.

[AO96] E. Allender and M. Ogihara. Relationship among **PL**, **#L**, and the determinant. *RAIRO-Theoretical Informatics and Applications*, 30:1–21, 1996.

[ARZ99] E. Allender, K. Reinhardt, and S. Zhou. Isolating, matching, and counting: uniform and nonuniform upper bounds. *Journal of Computer and System Sciences*, 59:164–181, 1999.

[BDHM91] G. Buntrock, C. Damm, U. Hertrampf, and C. Meinel. Structure and importance of logspace-mod-classes. In *8th Annual Symposium on Theoretical Aspects of Computer Science (STACS)*, pages 360–371. Springer, 1991.

[Ber84] S. Berkowitz. On computing the determinant in small parallel time using a small number of processors. *Information Processing Letters*, 18:147–150, 1984.

[CSV84] A. K. Chandra, L. Stockmeyer, and U. Vishkin. Constant depth reducibility. *SIAM Journal on Computing*, 13(2):423–439, 1984.

[Dam91] C. Damm. DET = $\mathrm{L}^{(\#\mathrm{L})}$. Technical Report Informatik-Preprint 8, Fachbereich Informatik der Humboldt Universitaet zu Berlin, 1991.

[DHK93] E. Dahlhaus, P. Hajnal, and M. Karpinski. On the parallel complexity of hamiltonian cycles and matching problem in dense graphs. *Journal of Algorithms*, 15:367–384, 1993.

[DK86] E. Dahlhaus and M. Karpinski. The matching problem for strongly chordal graphs is in **NC**. Technical Report 855-CS, University of Bonn, 1986.

[DKR08] S. Datta, R. Kulkarni, and S. Roy. Deterministically isolating a perfect matching in bipartite planar graphs. In *25th Annual Symposium on Theoretical Aspects of Computer Science (STACS)*, LNCS, pages 229–240. Springer Verlag, 2008.

[Edm65] J. Edmonds. Maximum matching and a polyhedron with 0-1 vertices. *Journal of Research National Bureau of Standards*, 69:125–130, 1965.

[GK87] D. Grigoriev and M. Karpinski. The matching problem for bipartite graphs with polynomially bounded permanent is in **NC**. In *28th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 166–172. IEEE Computer Society Press, 1987.

[HMT06] T. M. Hoang, M. Mahajan, and T. Thierauf. On the bipartite unique perfect matching problem. In *33rd International Colloquium on Automata, Languages and Programming (ICALP)*, pages 453–464. Springer-Verlag, 2006.

[Kas67] P. W. Kasteleyn. Graph theory and crystal physics. In F. Harary, editor, *Graph Theory and Theoretical Physics*, pages 43–110. Academic Press, 1967.

[KI04] V. Kabanets and R. Impagliazzo. Derandomizing polynomial identity tests means proving circuit lower bounds. *Computational Complexity*, 13(1-2):1–46, 2004.

[KR98] M. Karpinski and W. Rytter. *Fast parallel algorithms for graph matching problems.* Oxford University Press, Inc., New York, NY, USA, 1998.

[KUW86] R. M. Karp, E. Upfal, and A. Wigderson. Constructing a perfect matching is random **NC**. *Combinatorica*, 6(1):35–48, 1986.

[LP86] L. Lovasz and M. Plummer. *Matching Theory.* Noth-Holland, 1986.

[LPV81] G. Lev, M. Pippenger, and L. Valiant. A fast parallel algorithm for routing in permutation networks. *IEEE Transactions on Computers*, C-30:93–100, 1981.

[MN95] G. Miller and J. Naor. Flow in planar graphs with multiple sources and sinks. *SIAM Journal of Computing*, 24(5):1002–1017, 1995.

[MSV99] M. Mahajan, P. Subramanya, and V Vinay. A combinatorial algorithm for pfaffians. In *5th Annual International Conference on Computing and Combinatorics (COCOON)*, Lecture Notes in Computer Science 1627, pages 134–143. Springer-Verlag, 1999.

[MV00] M. Mahajan and K. R. Varadarajan. A new **NC**-algorithm for finding a perfect matching in bipartite planar and small genus graphs (extended abstract). In *Proceedings of the thirty-second annual ACM symposium on Theory of computing (STOC)*, pages 351–357. ACM Press, 2000.

[MVV87] K. Mulmuley, U. V. Vazirani, and V. V. Vazirani. Matching is as easy as matrix inversion. *Combinatorica*, 7:105–113, 1987.

[Sch80] J. T. Schwartz. Fast probabilistic algorithms for verification of polynomial identities. *Journal of the ACM*, 27(4):701–717, 1980.

[Tod91] S. Toda. Counting problems computationally equivalent to the determinant. Technical Report CSIM 91-07, Dept. of Computer Science and Information Mathematics, University of Electro-Communications, Chofu-shi, Tokyo 182, Japan, 1991.

[Tut47] W. T. Tutte. The factorization of linear graphs. *London Math Society*, 22:107–111, 1947.

[Val79] L. Valiant. The complexity of computing the permanent. *Theoretical Computer Science*, 8:189–201, 1979.

[Val92] L. Valiant. Why is Boolean complexity theory difficult. In M. S. Paterson, editor, *Boolean Function Complexity*, London Mathematical Society Lecture Notes Series 169. Cambridge University Press, 1992.

[Vaz89] V. Vazirani. **NC** algorithms for computing the number of perfect matchings in $K_{3,3}$-free graphs and related problems. *Information and computation*, 80(2):152–164, 1989.

[Vin91] V Vinay. Counting auxiliary pushdown automata and semi-unbounded arithmetic circuits. In *6th IEEE Conference on Structure in Complexity Theory (CCC)*, pages 270–284. IEEE Computer Society Press, 1991.

[zG93] J. Von zur Gathen. Parallel linear algebra. In J. H. Reif, editor, *Synthesis of parallel algorithms*, pages 573–617. Morgan Kaufmann, 1993.

[Zip79] R. Zippel. Probabilistic algorithms for sparse polynomials. In *EUROSAM*, Lecture Notes in Computer Science 72, pages 216–226. Springer, 1979.

ECCC ISSN 1433-8092

http://eccc.hpi-web.de