Electronic Colloquium on Computational Complexity, Report No. 194 (2010)

Isolation of Matchings via Chinese Remaindering

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

Abstract

In this paper we investigate the question whether a perfect matching can be isolated by a weighting scheme using Chinese Remainder Theorem (short: CRT). We give a systematical analysis to a method based on CRT suggested by Agrawal in a CCC'03-paper for testing perfect matchings. We show that this desired test-procedure is based on a deterministic weighting scheme which can be generalized in a natural way to a scheme for isolating a perfect matching in the graph. Thereby we give a new insight into the topic about deterministic isolations of perfect matchings by showing necessary and sufficient conditions for a potential isolation. Moreover, we show that if the considered weighting scheme by using CRT for isolating perfect matchings works, then the maximum matching problem can be solved completely in **NC**. This is a generalization of the **NC**-algorithm showed in [Hoa10] for the maximum matching problem for bipartite planar graphs.

1 Introduction

A matching in a graph is a set of vertex-disjoint edges in the graph. A matching with maximum cardinality is called *maximum*, and *perfect* if it covers all vertices in the graph. One of the most interesting topics in theoretical computer science consists of research problems concerning graph matchings (see e.g. [LP86]). For example, Decision-PM is the standard decision version of the perfect matching problem that can be formulated as follows: given a graph G one has to decide whether G has some perfect matchings. It is well-known that Decision-PM is efficiently solvable in polynomial time [Edm65]. Regarding parallel computations, Decision-PM is known to be in randomized **NC** [KUW86, MVV87, ARZ99]. But the open question whether Decision-PM is in **NC** is still a big challenge. Furthermore, in the viewpoint of complexity theory, we know that the problem of computing the number of all perfect matchings in a bipartite graph is complete for #**P** [Val79]. Hence under the hypothesis $\mathbf{P} \neq \mathbf{NP}$ there is an enormous gap between the upper bounds for the counting and the decision versions of the perfect matching problem.

The motivation for studying the complexity of the perfect matching problem is manifold. Decision-PM is known to be a special case of the problem of *Symbolic Determinant Identity Testing* (short: SDIT) because by Tutte's Theorem [Tut47] (see next section for more detail) one has to verify if the determinant of a symbolic matrix is equal to 0. In general, the problem of testing if a multivariate polynomial $p(x_1, x_2, \ldots, x_n)$ given in an implicit form, like an arithmetic circuit or a symbolic determinant, over a ring is identically zero or not is called *Polynomial Identity Testing* (short: PIT). PIT can be solved efficiently in randomized polynomial time by using Schwartz-Zippel Lemma [Sch80, Zip79]. But it is open whether the randomized solutions

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

ISSN 1433-8092

for PIT can be derandomized. Actually, this open question is very important due to a result by Impagliazzo and Kabanets [KI04] which states that the problem of derandomizing PIT is computationally equivalent to the problem of proving lower bounds for arithmetic circuits. Therefore, Decision-PM is a special case of PIT and it attracts a great attention. Note that the decision version of the perfect matching problem is known to be in **NC** for the following restricted classes of graphs: planar graphs [Kas67, Vaz89], regular bipartite graphs [LPV81], strongly chordal graphs [DK86], and dense graphs [DHK93]. Furthermore, the problem of constructing a perfect matching (short: Search-PM) is known to be in **NC** only for bipartite planar graphs [MN95, MV00, DKR08], for graphs with a polynomially bounded number of perfect matchings [GK87, AHT07], and for graphs with a polynomially bounded number of nice cycles [Hoa10]. Note that it is open whether Search-PM is in **NC** under the promise Decision-PM is in **NC**.

In this paper we deal with the open question whether the perfect matching problem can be solved in **NC**, i.e. whether Decision-PM and (or) Search-PM are in **NC**.

In 1999, Agrawal and Biswas [AB99] proposed a paradigm for polynomial identity testing: *via Chinese remaindering over polynomials*. The idea [AB99] is simple: First, the multivariate polynomial $p(x_1, \dots, x_n)$ should be transformed via a deterministic way to a new univariate polynomial $q(y)$ such that $p(x_1, \dots, x_n) = 0$ iff $q(y) = 0$ holds. Then in the final step, when the new polynomial $q(y)$ has exponentially high degrees then the polynomial identity testing $q(y) = 0$ will be done by using modulo some small degree polynomials which are randomly chosen from a suitable set.

Due to the celebrated result by Agrawal, Kayal, and Saxena [AKS04] that primality testing is in polynomial time, where the mentioned idea has been used in a very clever way, the above paradigm by Agrawal and Biswas is also significant for other derandomization-problems. W.r.t. the perfect matching problem, Agrawal conjectured in [Agr03] that by the mentioned paradigm (using CRT) one can show that Decision-PM for bipartite graphs is in **NC**. Note that regarding this conjecture, the sparse case of the perfect matching problem has been solved (by using CRT) already in [GK87, AHT07, Hoa10].

In Section 3 we give a systematical study of the above-mentioned paradigm for solving the perfect matching problem. We show that the conjecture for testing the existence of perfect matchings, using the method via CRT, can be generalized to a conjecture for deterministically isolating a perfect matching in the graph. Note that a partial derandomization of the Isolating Lemma (by Mulmuley, Vazirani, and Vazirani [MVV87]) in a certain manner would lead to a series of strong consequences, in particular, among small logspace complexity classes. From this follows for example that if in **NC** we are able to isolate a perfect matching by small weights, then both mentioned versions of the perfect matching problem, Decision-PM and Search-PM, are in **NC**. Thus, by this example sentence, the problem Search-PM might be not harder than Decision-PM. A contribution of the paper consists of a deep insight into the problematic situation concerning the question whether a perfect matching in a graph can be deterministically isolated via Chinese remaindering. We characterize the graphs for which the described isolation (via CRT) works.

Moreover, we show that if we have a deterministic way for weighting the edges such that Decision-PM can be done in **NC** then we can extend this bound to the problem of computing the *matching number*, which is the size of a maximum matching in the graph. Note that the problem of computing the matching number is a generalization of Decision-PM. Furthermore, if we have an **NC** algorithm for isolating some perfect matching in the graph then also in **NC** we can compute a maximum matching of the graph. This result is a generalization of the first **NC** algorithm for the maximum matching problem, i.e. searching a maximum matching is known to be in **NC** for planar bipartite graphs [Hoa10] thereafter a logspace algorithm for isolating a perfect matching in a planar bipartite graph has been shown in [DKR08].

2 Preliminaries

We assume that the readers are familiar with basic materials in complexity theory. Basic facts about the mentioned classes $\mathbf{P}, \mathbf{NP}, \mathbf{NC}$ and $\#\mathbf{P}$ can be found in the textbook [Pap94]. In this section we briefly describe some basic definitions and notions we need in the paper. We refer the readers to [LP86] for more detail on graph matchings, and to other standard textbooks in linear algebra and number theory.

Let G 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 edge-set $M \subseteq E$, such that no two edges in M have a vertex in common. Matching M is called perfect if M covers all vertices of G, i.e. $|M| = \frac{1}{2}\, n$, it is called maximum if its size $|M|$ is maximum. The size of a maximum matching in G is called the *matching number* of G which is denoted by $\mu(G)$.

Standard problems concerning graph matchings have been defined and studied in the literature:

- Given a graph G, the *decision version* DECISION-PM is the problem of deciding whether G has some perfect matching. This is a special case of the problem of determining the matching number of G.
- We denote the problem of computing a perfect matching (the *construction version*) by SEARCH-PM. A generalization of SEARCH-PM is the problem of computing a maximum matching in G.
- The *counting version* COUNTING-PM is defined as the problem of counting the number of all perfect matchings in a graph.

We describe some algebraic facts related to perfect matchings.

Graph $G = (V, E)$ 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 $1 \leq i, j \leq n$. Assigning weights to the edges we get an *edge-weighted* graph. In a edge-weighted graph, the weight of a matching is defined as the sum of all weights of the edges in the matching.

Assign an orientation to the edges of a weighted graph G, i.e. every edge (i, j) gets one of two orientations, from i to j or from j to i, we obtain respectively an *oriented graph* $\vec{G}$ for which there is 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*. Note that any canonical matrix T is isomorph to the matrix with the structure in which all negative elements are located under the main diagonal.

The *Pfaffian* of a skew-symmetric matrix is defined as the signed sum of all the perfect matchings in the weighted graph associated to the matrix. For our consideration, the Pfaffian of T associated to an orientation $\vec{G}$, denoted by $\mathrm{pf}(T)$ or $\mathrm{pf}(T(\vec{G}, w))$, is defined as follows:

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

where $\text{sign}(M) \in \{-1, +1\}$ is the *sign* of M that depends on the orientation $\vec{G}$, and $\text{value}(M) = \prod_{(i,j)\in M} w(i,j)$ is the *value* of M that depends on the weighting scheme w for G.

It is known from linear algebra that for any skew-symmetric matrix S the Pfaffian is strongly related to the determinant as follows

$$\det(S) \quad = \quad \begin{cases} \text{pf}^2(S)\ , & \text{if } S \text{ is of even order,} \\ \text{pf}(S) = 0, & \text{if } S \text{ is of odd order.} \end{cases}$$

The determinant of integer matrices is known to be computable in $\mathbf{NC}^2$ [Ber84]. But note that from the above relation between the Pfaffian and the determinant one can not imply that the Pfaffian can be computed also in **NC**. The latter has been shown in [MSV99] where the Pfaffian is computationally equivalent to the determinant function.

Assigning indeterminates $x_{i,j}$ to the edges (i,j) of G we get the graph $G(X)$. Now the value of a perfect matching is a product of pairwise different $n/2$ indeterminates. Let $T(X)$ be the canonical Tutte skew-symmetric matrix of $G(X)$. Then it is clear that all the perfect matchings in G are 1-1 mapped to monomials in the multivariate polynomial $\text{pf}(T(X))$.

Theorem 2.1 (Tutte, [Tut47]) *Graph G has no perfect matching iff* $\text{pf}(T(X)) = 0$.

By Tutte Theorem we see that the problem of testing the existence of perfect matchings in a graph is reducible to the problem of testing if a multivariate polynomial vanishes. A randomized algorithm for the latter can be obtained simply by using the Schwartz-Zippel lemma [Sch80, Zip79].

We know that the number of all perfect matchings in a bipartite graph is known to be #**P**-complete [Val79]. But in some restricted classes of graphs, the number of all perfect matchings can be computed efficiently by using the Pfaffian. Thereby, one can orient the graph such that all perfect matchings in the oriented graph get the same sign +1 in the associated Pfaffian, such an orientation is called a *Pfaffian orientation* [Kas67], and finally the number of all perfect matchings is equal to the Pfaffian of the oriented graph. Unfortunately, there are graphs without 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 computable in **NC**, and thus the number of all perfect matchings in such a graph can be computed efficiently.

A concept of isolating a perfect matching is provided by Isolating Lemma [MVV87]:

Lemma 2.2 (Mulmuley, Vazirani, Vazirani [MVV87]) *Let U be a universe of size m and S be a considered family of subsets of U. Let $w : U \to \{1, \dots, 2m\}$ be a random weight function. Then with probability at least $\frac{1}{2}$ there exists a unique minimum weight subset in S.*

For the perfect matching problem, one can assign $x^{w(e)}$ to the edges e where x is an indeterminate and the "weights" $w(e)$ are chose randomly from $\{1, \dots, 2m\}$. By Lemma 2.2, with high probability there exists in G a unique minimum weighted perfect matching which will be isolated in the Pfaffian computation as follows: By $T(x)$ we denote the skew-symmetric canonical Tutte matrix associated to the labeled graph. Now the Pfaffian $\text{pf}(T(x))$ is defined as the signed sum of all perfect matchings in G, where the value of a perfect matching M is of the form $x^{\mathcal{W}(M)}$ in which $\mathcal{W}(M)$ is the "weight" of M, i.e. $\mathcal{W}(M)$ is the sum of all $w(e)$ for all $e \in M$.

Since with high probability a perfect matching M has a unique minimum weight, the term with the lowest degree in $\text{pf}(T(x))$ should be corresponded to M. In order to construct M, one can determine in parallel all the edges having a contribution to the lowest term in the Pfaffian polynomial (see Theorem 3.2 on page 7 for more detail). Thereby note that the Pfaffian of a skew-symmetric matrix with univariate polynomials in its elements can be also computed in

NC. This fact follows from **NC**-computation of the determinant of a univariate polynomial matrix [AAM03] and from combinatorial setting for Pfaffians [MSV99]. Therefore, Search-PM (and as a consequence also Decision-PM) is in random **NC**. Moreover, we see that if in **NC** we are able to assign small weights (with logarithmic number of bits) to the edges such that a perfect matching gets a unique minimum weight, then we obtain **NC**-algorithms for both Search-PM and Decision-PM.

3 Isolating matchings via CRT

Agrawal suggested in [Agr03] a general paradigm for derandomizing polynomial identity testing $p(x_1, \ldots, x_n) = 0$ by using CRT as follows:

a) Convert the multivariate polynomial $p(x_1, \ldots, x_n)$ via a deterministic way to a univariate polynomial $q(y)$ such that $p(x_1, \ldots, x_n) = 0 \iff q(y) = 0$ holds.

b) testing $q(y) = 0$ will be done by using modulo some small degree polynomials $h(y)$ which is chosen from a suitable set. Note that $q(y)$ might be of exponentially high degree.

Consider Decision-PM which is the decision version of the perfect matching problem. Recall Tutte's Theorem (on page 4) that Decision-PM is equivalent to the problem of testing if a multivariate polynomial (the Pfaffian) is identically zero.

In the case when graph G is bipartite, we see that $\mathrm{pf}(T(X)) = 0$ is equivalent to $\det(B(X)) = 0$ where $T(X)$ is the canonical Tutte skew-symmetric matrix (see on page 4) and $B(X)$ is called the *bipartite adjacency matrix* of G:

$$T(X) = \begin{pmatrix} \mathbf{0} & B(X) \\ -B^T(X) & \mathbf{0} \end{pmatrix}.$$

For Decision-PM for bipartite graphs, Agrawal [Agr03] interpreted the paradigm for the derandomization as follows. For Step a) in the above paradigm, Agrawal [Agr03] suggested the mapping $y^{2^{n^3 i+j}} \mapsto x_{i,j}$ that transforms $B(X)$ into matrix $B(y)$ such that

$$\det(B(X)) = 0 \iff \det(B(y)) = 0.$$

In the case when G does not have any perfect matching, then it is clear that $\det(B(X)) = \det(B(y)) = 0$. If G has some perfect matching, then we have $\det(B(y)) \neq 0$ because perfect matchings in G are 1-1 mapped to the terms of the polynomial $\det(B(y))$. For Step b), he conjectured that:

$$\det(B(y)) \neq 0 \text{ iff there is some } 1 \leq r \leq n^6 : \ \det(B(y)) \neq 0 \pmod{y^r - 1}.$$

Obviously, the conjecture by Agrawal can be formulated for Decision-PM for nonbipartite graphs by using the Pfaffian polynomials as follows.

Let $G = (V, E)$ with n vertices $V = \{1, 2, \ldots, n\}$ and m edges $E = \{e_1, e_2, \ldots, e_m\}$ be the instance of the perfect matching problem we consider.

- By mapping $y^{2^l} \mapsto x_{i,j}$, where $e_l = (i, j)$, for $l = 1, 2, \ldots, m$, from $T(X)$ we get matrix $T(y)$ (with indeterminate y) that satisfies $\mathrm{pf}(T(X)) \neq 0 \iff \mathrm{pf}(T(y)) \neq 0$.
- The conjecture by Agrawal is now:

$$\mathrm{pf}(T(y)) \neq 0 \text{ iff there is some } 1 \leq r \leq n^6 : \ \mathrm{pf}(T(y)) \neq 0 \pmod{y^r - 1}.$$

We further observe that the mapping $y^{a^l} \mapsto x_{i,j}$, for number $a \geq 2$ and for $l = 1, 2, \ldots, m$, transforms multivariate matrix $T(X)$ to univariate matrix $T_a(y)$ such that $\mathrm{pf}(T(X)) \neq 0 \Longleftrightarrow \mathrm{pf}(T_a(y)) \neq 0$. Therefore, the conjecture by Agrawal can be generalized as follows:

$$\mathrm{pf}(T_a(y)) \neq 0 \text{ iff there is some small number } r: \ \mathrm{pf}(T_a(y)) \neq 0 \pmod{y^r - 1}.$$

Let $T_{a,r}(y)$ be the Tutte skew-symmetric matrix w.r.t. the mapping $y^{a^l \bmod r} \mapsto x_{i,j}$. Then we can write $\mathrm{pf}(T_a(y)) \bmod y^r - 1 = \mathrm{pf}(T_{a,r}(y)) \bmod y^r - 1$. Note that testing $\mathrm{pf}(T_{a,r}(y)) \bmod y^r - 1 \neq 0$ can be done in **NC**. Furthermore, w.r.t. our conjectures we focus on the case when G has some perfect matching because $\mathrm{pf}(T(y)) = 0$ in the case when G has no perfect matching. Formally, for a pair of numbers a and p, define the weighting schemata

$$w_{a,p}: \quad w_{a,p}(e_i) = a^i \bmod p$$

for $i = 1, 2, \ldots, m$. The following conjecture is about testing the existence of perfect matchings:

Conjecture 3.1 *Suppose G has some perfect matchings. There exist a positive constant c, and positive numbers $a \leq p \leq n^c$ such that* $\mathrm{pf}(T_{a,p}(y)) \bmod y^p - 1 \neq 0$ *holds.*

Now a test procedure due to Conjecture 3.1 can be implemented as follows: assigning the weights $(a^i \bmod p)$ to edges e_i we have to check if the Pfaffian polynomial $\mathrm{pf}(T_{a,p}(y))$ does not vanish. Thus, the weighting scheme used for the test plays a central role.

Let w be an arbitrary weighting scheme for the edges of graph G. Assigning $y^{w(e_i)}$ to edges e_i, for an indeterminate y, we get $T(y)$ as the canonical Tutte skew-symmetric matrix of G. Note that only in the case when the weights $w(e_i)$ are small, i.e. they are bounded by n^ϵ for some positive constant ϵ, the Pfaffian polynomial $\mathrm{pf}(T(y))$ can be computed efficiently. Hence we assume that w maps the edges of G only to small weights. We consider the Pfaffian polynomial:

$$\begin{aligned}
\mathrm{pf}(T(y)) &= \sum_{M \in \mathcal{PM}(G)} \mathrm{sign}(M) \cdot \mathrm{value}(M) \\
&= \sum_{M \in \mathcal{PM}(G)} \mathrm{sign}(M) \cdot \prod_{e_i \in M} y^{w(e_i)} \\
&= \sum_{M \in \mathcal{PM}(G)} \mathrm{sign}(M) \cdot y^{\mathcal{W}(M)} \\
&= \sum_{a} y^a \cdot \sum_{M:\ \mathcal{W}(M)=a} \mathrm{sign}(M)
\end{aligned}$$

where $\mathcal{PM}(G)$ is the set of all perfect matchings in G, $\mathrm{sign}(M) \in \{-1, 1\}$ is the sign of the perfect matching M, $\mathcal{W}(M) = \sum_{e_i \in M} w(e_i)$ is the weight of M, and the number a occurred in the last sum is taken over all possible weights of perfect matchings.

In the case when $\mathcal{PM}(G) = \emptyset$ then it is clear that $\mathrm{pf}(T(y)) = 0$ for every weighting scheme. In the converse when G has some perfect matchings, i.e. $|\mathcal{PM}(G)| \geq 1$, the Pfaffian polynomial depends on the weighting scheme w as follows.

For set $S \subseteq \mathcal{PM}(G)$, we define its *coefficient* by

$$\mathrm{coeff}(S) = \sum_{M \in S} \mathrm{sign}(M)$$

where the signs of perfect matchings, i.e. $\mathrm{sign}(M)$, have been defined w.r.t. the canonical orientation of G: all edges in G are oriented from smaller to larger vertices.

Under the weighting scheme w if we have $\mathcal{W}(M) \neq \mathcal{W}(N)$ for every pair of perfect matchings $M \in S$ and $N \in \overline{S} := \mathcal{PM}(G) \setminus S$, then we say that w *isolates* S. In the case when an isolated set S satisfies $\mathrm{coeff}(S) \neq 0$ then it is clear that the Pfaffian polynomial $\mathrm{pf}(T(y))$ does not vanish. Note that $\mathrm{pf}(T(y)) \neq 0$ always holds if additionally w isolates a subset of S, i.e. the perfect matchings in S can get different weights under w. Moreover, we say that w isolates a perfect matching if some set S with $|S| = 1$ being isolated under w.

It is well-known from a number of papers about a parallel construction of perfect matchings, see e.g. [MVV87, ARZ99, DKR08, AHT07, Hoa10], that a procedure of deterministically isolating a perfect matching is the first step to obtain an efficient **NC**-algorithm for computing a perfect matching. For the sake of completeness and of clarity we formulate this fact as follows.

Theorem 3.2 *If in* **NC** *there is a weighting scheme w that isolates some set S of perfect matchings with* $\mathrm{coeff}(S) \neq 0$*, then* DECISION-PM *is in* **NC**. *If w isolates a perfect matching, then the isolated perfect matching can be computed in* **NC**.

Proof. Assigning the polynomials $y^{w(e_i)}$ to the edges e_i, where y is an indeterminate, we get $T(y)$ as the canonical Tutte skew-symmetric matrix of G. If G has no perfect matching then we have $\mathrm{pf}(T(y)) = 0$. In the case when G has some perfect matchings and w isolates a set S with $\mathrm{coeff}(S) \neq 0$, then it is easy to see that $\mathrm{pf}(T(y)) \neq 0$. Since $\mathrm{pf}(T(y))$ can be computed in **NC**, we have DECISION-PM is in **NC**.

In the case when a perfect matching M is isolated under w, then $y^{\mathcal{W}(M)}$ (the value of M), where $\mathcal{W}(M)$ is the weight of M, does not vanish in the polynomial $\mathrm{pf}(T(y))$. Note that this term $y^{\mathcal{W}(M)}$ can be identified by a coefficient $+1$ or -1, which is equal to $\mathrm{sign}(M)$. Thus, if an arbitrary edge e is contained in the isolated perfect matching M then the Pfaffian of the graph obtained by deleting e from G does not contain the term $y^{\mathcal{W}(M)}$. By this observation, in parallel we can construct a set of edges that correspond to a coefficient $+1$ or -1 in the Pfaffian polynomial. Finally, we can check if the constructed edge-sets are perfect matchings. Therefore, this construction of perfect matchings is in **NC**. □

Regarding the weighting scheme used in Conjecture 3.1 we see that the polynomial x^i assigned on e_i has been used as the underlying function for the weighting procedure which is working over some finite field. Of course we can choose other underlying functions for weighting the edges of the graph, for example we choose $f_i(x)$ for the edge e_i. Moreover, for a weighting scheme we define the following function, for a nonempty set $S \subseteq \mathcal{PM}(G)$:

$$\mathcal{F}_S(x) = \prod_{\substack{M \in S \\ N \in \overline{S}}} (\sum_{e_i \in M} f_i(x) - \sum_{e_i \in N} f_i(x)).$$

In order to define a weighting scheme w we can search a point a such that all the weights $w(e_i) = f_i(a)$ are small and we have $\mathcal{F}_S(a) \neq 0$ for some S with $\mathrm{coeff}(S) \neq 0$. Thus, such a point a is a nonzero of $\mathcal{F}_S(x)$.

In the actual case when $f_i(x) = x^i$ has been chosen as the underlying function on e_i, for some set $S \subseteq \mathcal{PM}(G)$, we have

$$\mathcal{F}_S(x) = \prod_{\substack{M \in S \\ N \in \overline{S}}} (\sum_{e_i \in M} x^i - \sum_{e_i \in N} x^i).$$

W.r.t. Conjecture 3.1 we are asking if there is set S with $\mathrm{coeff}(S) \neq 0$ such that $\mathcal{F}_S(x)$ has some nonzero modulo a small number. Thus we can reformulate the conjecture as follows:

Conjecture 3.3 *Suppose G has some perfect matchings. There exist positive numbers $a \leq p \leq n^c$, for a positive constant c, such that $\mathcal{F}_S(a) \bmod p \neq 0$ for some set $S \subseteq \mathcal{PM}(G)$ with* $\mathrm{coeff}(S) \neq 0$.

We suspect that the same weighting scheme isolates also a perfect matching:

Conjecture 3.4 *Conjecture 3.3 is true such that some set S with $|S| = 1$ will be isolated.*

We make some observations about these conjectures.

Observe that the polynomials $\mathcal{F}_S(x)$ have exponentially large degrees, which are not smaller than the number of all perfect matchings, and we are asking if there is a certain polynomial having a nonzero from a small finite field. Note that this is not true in general because there are polynomials which seem to be very similar to $\text{diff}_S(x)$ but they do not have any nonzero in any small field. For clarity we can take the following example:

For $\emptyset \neq I \subseteq [n] = \{1, 2, \ldots, n\}$, define $g_I(x) = \sum_{i \in I} x^i$, where x is an indeterminate. Then

$$f(x) = \prod_{I \neq I' \subseteq [n]} (g_I(x) - g_{I'}(x))$$

is a polynomial without any nonzero in $\mathbb{Z}_p$ for every small number p, i.e. $f(a) \bmod p = 0$ for all $a \in \mathbb{Z}_p$. The reason for the latter is from a simple observation of the pigeonhole principle that it is not possible to separate exponentially many objects by using only polynomially large weights.

Furthermore, observe that the problem of testing if $\mathcal{F}_S(x)$ has a nonzero a modulo $p \leq n^c$ is known to be reducible to the same problem over small prime powers bounded by n^c: Suppose there is $a \leq n^c$ such that $\mathcal{F}_S(a) \bmod p \neq 0$. It is clear that there exists a prime power q which is a factor of p that satisfies $\mathcal{F}_S(a) \bmod q \neq 0$. Therefore, w.l.o.g. in Conjecture 3.3 p is a prime power bounded by n^c .

For a prime p, we know that the factorization of a polynomial in the ring $\mathbb{Z}_p[x]$ is unique. For an arbitrary set S, let

$$\mathcal{F}_S(x) = h_1^{e_1}(x) \cdots h_t^{e_t}(x)$$

be the factorization of $\mathcal{F}_S(x)$ in $\mathbb{Z}_p[x]$, where $h_1(x), \ldots, h_t(x)$ are monic irreducible polynomials in $\mathbb{Z}_p[x]$, and $e_1, \ldots, e_t$ are positive integers. Note that these factors may be not irreducible in the ring $\mathbb{Z}_{p^k}[x]$, for some $k \geq 2$. By weighting the edges of the graph there is an idea that we use nonlinear irreducible polynomials. This idea has been described in the discussion-section of the paper [Hoa10] as follows: 1) $\mathcal{F}_S(x)$ will be mapped to nonzero-elements in the field $\mathbb{Z}_p[x]/(h(x))$ where $h(x)$ is a irreducible polynomial with constant-degree ϵ and p is a prime. 2) There exists a number a from $\mathbb{Z}_q$ where q is a prime larger than ϵp^ϵ. Formally, by this idea we consider the weighting scheme:

$$w(e_i) := \ (x^i \bmod h(x), p) \bmod x - a, q, \qquad \text{for } i = 1, 2, \ldots, m.$$

The following lemma shows that the last weighting scheme can be reduced to the scheme that uses only linear factors:

Lemma 3.5 *Let $h(x) \in \mathbb{Z}_p[x]$ be a monic and irreducible polynomial with degree ϵ. Suppose $\mathcal{F}_S(x) \bmod h(x), p \neq 0$, then there exists $a \in \mathbb{Z}_{p^\epsilon}$ such that $\mathcal{F}_S(a) \bmod p^\epsilon \neq 0$.*

Proof. Because $\mathcal{F}_S(x) \bmod h(x), p \neq 0$ we have $\mathcal{F}_S(x) \bmod h(x), p^\epsilon \neq 0$. It is well-known that $h(x)$ is reducible in $\mathbb{Z}_{p^\epsilon}[x]$. In particular, in this ring we have the factorization

$$h(x) = (x - \alpha)(x - \alpha^p) \cdots (x - \alpha^{p^{\epsilon-1}})$$

where $\alpha, \alpha^p, \ldots, \alpha^{p^{\epsilon-1}}$ are ϵ distinct points in the field $\mathbb{Z}_{p^\epsilon}$. Therefore, there exists $0 \leq j \leq \epsilon - 1$ such that

$$\mathcal{F}_S(x) \bmod x - \alpha^{p^j}, p^\epsilon \neq 0.$$

So we can choose $a := \alpha^{p^j} \bmod p^\epsilon$. □

In the following theorem we show some consequences from the case when the considered conjectures are not true.

Theorem 3.6 *Suppose G has some perfect matchings. Let c be a positive constant. If $\mathrm{pf}(T_{a,p}(y)) = 0$ holds for all $a \in \mathbb{Z}_p$, all prime powers $p \leq n^c$, where c is a certain constant, then the following statements hold.*

1. *G has at least $n^c/2m$ perfect matchings.*
2. *For each set $S \subseteq \mathcal{PM}(G)$ with $\mathrm{coeff}(S) \neq 0$, every point in $\mathbb{Z}_p$ is a root of $\mathcal{F}_S(x)$ modulo p, for all prime powers $p \leq n^c$.*
3. *For all $t \leq n^c/2m$, we have*

$$G_t(x) := \sum_{M \in \mathcal{PM}(G)} \mathrm{sign}(M) \cdot (\sum_{e_i \in M} x^i)^t \ = \ 0.$$

Proof. 1) Assume for a moment that G has at most $n^c/2m$ perfect matchings. Observe that the polynomial $\mathcal{F}_S(x)$ with $|S| = 1$ has degree at most $mn^c/2m = n^c/2$. Furthermore, $\mathcal{F}_S(a) \bmod p = 0$ holds for all $a, p \leq n^c$ because $\mathrm{pf}(T_{a,p}(y)) = 0$. Thus $\mathcal{F}_S(2) \bmod p = 0$, for all primes $< n^c$, is a contradiction because

$$\prod_{\text{prime } p \leq n^c} p \geq 2^{n^c/2}.$$

2) Obviously, if the weighting scheme $w_{a,p}$ isolates some set S with $\mathrm{coeff}(S) \neq 0$ then $\mathrm{pf}(T_{a,p}(y)) \neq 0$. Hence such a set S can not be isolated under $w_{a,p}$.

3) The Pfaffian polynomials can be rewritten as follows

$$\begin{aligned}
\mathrm{pf}(T_{a,p}(y)) &= \sum_{M \in \mathcal{PM}(G)} \mathrm{sign}(M) \cdot \prod_{e_i \in M} y^{w(e_i)} \\
&= \sum_{M \in \mathcal{PM}(G)} \mathrm{sign}(M) \cdot y^{\sum_{e_i \in M} (a^i \bmod p)} \\
&= \sum_w y^w \cdot \sum_{M:\ \mathcal{W}(M) = w} \mathrm{sign}(M) \ = \ 0,
\end{aligned}$$

where $\mathcal{W}(M) = \sum_{e_i \in M} (a^i \bmod p)$ is the weight. Observe that for every potential weight w the coefficient of y^w should be equal to zero, i.e.

$$\sum_{M:\ \mathcal{W}(M) = w} \mathrm{sign}(M) = 0.$$

Therefore we get a new identity

$$\sum_{M \in \mathcal{PM}(G)} \mathrm{sign}(M) \cdot (\sum_{e_i \in M} (a^i \bmod p))^t \ = \ 0,$$

for every $t \geq 0$, for all $a \in \mathbb{Z}_p$ and for all prime powers $p \leq n^c$. That implies

$$G_t(x) \bmod x - a,\ p = 0.$$

For a fixed t, the degree of $G_t(x)$ is bounded by mt. Hence this polynomial has at most mt roots modulo p if p is a prime power which is not smaller than mt. In the case when $G_t(x)$ has more than mt roots then we conclude that $G_t(x) = 0$. Observe that there is a prime p in the interval $(n^c/2, n^c)$. Thus we have $t \leq n^c/2m < p/m$. It follows that $G_t(x) = 0$ holds for all $t \leq n^c/2m$ as claimed. □

Note that in the case when G has some perfect matchings it is straightforward to show that there exists t which is at most the number of all perfect matchings in S such that $G_t(x) \neq 0$.

Recall the maximum matching problem. Given a graph G, a generalization of Decision-PM is the problem of computing the matching number $\mu(G)$ which is the size of a maximum matching. In the construction version of the maximum matching problem one has to compute a maximum matching in G. In the following theorem we make a generalization of the **NC**-algorithm, presented in [Hoa10], for the maximum matching problem in bipartite planar graphs. We are not sure whether this result can be extended to every deterministic weighting scheme w which can be used for solving Decision-PM.

Theorem 3.7 *If Conjecture 3.3 is true then the matching number of a graph can be computed in* **NC***. Moreover, if Conjecture 3.4 is true then a maximum matching can be computed in* **NC***.*

Proof. Suppose Conjecture 3.3 is true, i.e. there is a weighting scheme $w_{a,p}$ which is defined on page 6 for isolating some perfect matching set S with $|S| \neq 0$. Note that the latter holds by promising G has some perfect matchings and note that the Pfaffian polynomial $\text{pf}(T_{a,p}(y))$ should be nonzero. Consider the case when G has no perfect matching.

Let M be a maximum matching in G. So $l = |M| < n/2$ is the matching number of G. Observe that M is perfect in the subgraph G_M which is obtained by deleting $n - 2l$ vertices that are not covered by M. Moreover, if Conjecture 3.3 is true then the same holds for the graph G_M, i.e. there exist $\tilde{a} \in \mathbb{Z}_{\tilde{p}}$ and prime power $\tilde{p} \leq n^{\tilde{c}}$, for some constant $\tilde{c}$, such that the weighting scheme $w_{\tilde{a},\tilde{p}}$ isolates some set $\tilde{S}$ of perfect matchings in G_M where $\text{coeff}(\tilde{S}) \neq 0$. (Note that all the perfect matchings in G_M are maximum in G.) Therefore, the Pfaffian polynomial associated to subgraph G_M does not vanish, i.e. the Pfaffian polynomial of the skew-symmetric $T^{(M)}_{\tilde{a},\tilde{p}}(y)$ which is corresponded to G_M and it is a submatrix of $T_{\tilde{a},\tilde{p}}(y)$. Since $\text{pf}(T_{\tilde{a},\tilde{p}}(y)) \neq 0$ the rank of matrix $T^{(M)}_{\tilde{a},\tilde{p}}(y)$ is full and it is equal to $2l$. This is also the rank of $T_{\tilde{a},\tilde{p}}(y)$ because M is a maximum matching in G. Following these observations we can compute $2\mu(G)$ as follows: for all pairs of small numbers a and p which are bounded by n^c, where c is the constant due to Conjecture 3.3, we compute the maximum of all the ranks of the matrices $T_{a,p}(y)$. Since the rank can be computed in **NC**, the matching number can be computed also in **NC**.

In the case when Conjecture 3.4 is true we can compute a maximum matching in G by two steps: a) compute a subgraph G_M where its perfect matchings are maximum in G, b) a perfect matching in G_M will be computed by Theorem 3.2. We know that the construction of G_M in Step b) is reducible to the problem of computing the rank. This has been shown in the proof of Lemma 4.1 in [Hoa10]. Moreover, all these computations are in **NC**. □

Conclusion. In this paper we have investigated the conjecture that a deterministic isolations of graph matchings can be made via CRT. In the fact, the weighting scheme (via CRT) we used in the procedure of testing if a graph has some perfect matching can be extended to a isolation of a perfect matching. We have showed that if this isolation works for solving the perfect matching problem then we can use it for solving the maximum matching problem in **NC**. Of course the central question is still open whether the desired isolation of perfect matchings works.

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.

[AB99] M. Agrawal and S. Biswas. Primality and identity testing via chinese remaindering. In *40th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 2020–209. IEEE Computer Society Press, 1999.

[Agr03] M. Agrawal. On derandomizing tests for certain polynomial identities. In *18th Annual IEEE Conference on Computational Complexity (CCC)*, pages 355–362. 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.

[AKS04] M. Agrawal, N. Kayal, and N. Saxena. Primes is in **P**. *Ann. of Math.*, 60:781–793, 2004.

[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.

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

[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.

[Hoa10] T. M. Hoang. On the matching problem for special graph classes. In *25th IEEE Conference on Computational Complexity (CCC)*, pages 139–150. IEEE Computer Society Press, 2010.

[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.

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

[LP86] L. Lovász 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)*, LNCS 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.

[Pap94] C. H. Papadimitriou. *Computational complexity*. Addison-Wesley, 1994.

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

[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.

[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.

[Zip79] R. Zippel. Probabilistic algorithms for sparse polynomials. In *EUROSAM*, LNCS 72, pages 216–226. Springer, 1979.