

Response to *Refutation of Aslam's Proof that $\mathbf{NP} = \mathbf{P}$*

Javaid Aslam*
jaslamx@yahoo.com

November 2, 2018

Abstract

This paper provides a further refinement to the previous response by introducing new structures and algorithms for counting VMPs of common *Edge Requirement* (ER) and hence for counting the perfect matchings.

1 The ER Satisfiability and Enumeration

The distinguishing result of the main paper [Asl17] is a P-time enumerable *partition* of all the potential perfect matchings in a bipartite graph. This partition is a set of equivalence classes induced by the missing edges in the potential perfect matchings. We capture the behavior of these missing edges in a polynomially bounded representation by a graph theoretic structure, called MinSet Sequence, where MinSet is a P-time enumerable structure derived from a graph theoretic counterpart of a generating set of the symmetric group.

The above MinSet Sequences can be viewed as a transformed problem of Perfect Matching, and which can be summarized by some of its characteristic attributes as follows:

- The generators of MinSet Sequences are created in the following two main steps:
 1. Partition and transform the Cosets of the symmetric group S_n into disjoint subsets, called CVMPSet, containing perfect matchings from $K_{n,n}$.

To achieve this, we first map a specific generating set of the symmetric group S_n to a set of graph theoretic generators, for generating all the perfect matchings (PM) in $K_{n,n}$. This means mapping each set of (right) coset representatives U_i to a graph theoretic counterpart, called *partition representatives* $g(i)$. Two kinds of binary relations over $\{g(i)\}$ model the multiplicative behavior of these generators, leading to a generating graph, $\Gamma(n)$ (a directed n -partite graph), for generating all the PMs in $K_{n,n}$, where each PM is represented by a directed path in $\Gamma(n)$, called CVMP, which is a sequence of n unique generators from $g(1) \times g(2) \times \dots \times g(n-1) \times g(n)$. A VMP is any sub-path of a CVMP. Now each graph theoretic “coset representative” (a generator from $g(1)$) induces an equivalence class over each Coset, called CVMPSet.

2. Partition each CVMPSet into MinSet Sequences, where each sequence consists of a small subset of the polynomially many MinSets defined as follows.

For any bipartite graph BG, CVMPs represent only potential perfect matchings, and therefore, they are qualified by an attribute called Edge Requirement (ER) defined as follows. ER of a CVMP contains all the missing edges in the potential PM represented by that CVMP. A MinSet contains all the VMPs of common ER, with the missing edges only at three distinguished nodes on the VMPs. A judicious choice of the common nodes of these VMPs in a CVMPSet allows a MinSet and any sequence of the MinSets to be P-time enumerable. Each CVMPSet can thus be decomposed into disjoint subsets, each being a (set

*©Copyright Javaid Aslam 2009-2017, Santa Clara, CA 95054

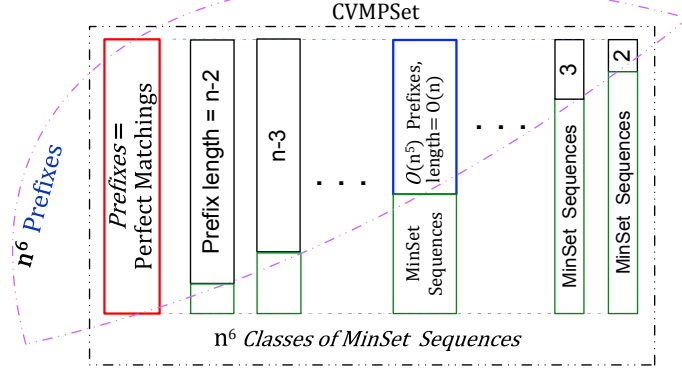


Figure 1: A Partition Containing MinSet Sequences

of a) unique sequence of MinSets, representing a disjoint subset of the $n!$ potential perfect matchings in BG.

While there can be exponentially many MinSet sequences, there are only polynomially many classes induced by the polynomially many ($O(n^6)$) prefixes of the MinSet sequences. Only a sequence containing exactly one MinSet can contain perfect matchings in BG.

- Each sequence of length 1 (containing exactly one MinSet), containing CVMPs of length $n - 1$ and with null ER, captures a disjoint subset of the perfect matchings in BG.

When $BG = K_{n,n}$, $MinSet = CVMPSet$.

Other MinSet sequences can also be enumerated, but they are not of interest.

2 Key Concepts

Let $G^{(i)}$ be a subgroup of a permutation group $G < S_n$, obtained from G by fixing all the points in $\{1, 2, \dots, i\}$, where $1 \leq i \leq n$. That is, $\forall \pi \in G^{(i)}$, and $\forall j \in \{1, 2, \dots, i\}$, $j^\pi = j$. Then $G^{(i)} < G^{(i-1)}$, $G^{(0)} = G$. Then the following sequence of subgroups is referred to as a *stabilizer chain* of G .

$$I = G^{(n)} < G^{(n-1)} < \dots < G^{(1)} < G^{(0)} = G \quad (2.1)$$

Let $K_{n,n} = (V \cup W, V \times W)$, where $V = W = \{1, 2, \dots, n\}$, and $BG = (V \cup W, E)$ be a subgraph of $K_{n,n}$, on $2n$ nodes, where $E \subset V \times W$.

2.1 The Mapping: S_n Generating Set to Perfect Matching Generators

We choose the generating set K of S_n by choosing the set of right representatives U_i , $1 \leq i < n$, as transpositions, for the stabilizer chain of subgroups in (2.1), i.e.,

$$U_i = \{I, (i, i+1), (i, i+2), \dots, (i, n)\}, \quad 1 \leq i < n. \quad (2.2)$$

Then the generating set K of S_n is

$$K = \bigcup U_i = \{I, (1, 2), (1, 3), \dots, (1, n), (2, 3), (2, 4), \dots, (2, n), \dots, (n-1, n)\} \quad (2.3)$$

Let $\mathbb{M}(BG')$ denote the set of permutations realized as perfect matchings in the bipartite graph BG' .

Let BG_i denote the sub (bipartite) graph of $BG = K_{n,n}$, induced by the subgroup $G^{(i)}$, such that $\mathbb{M}(BG_i) = G^{(i)}$.

A *partition representative*, $g(i)$, derived from U_i (using Theorem 3.1 in [Asl17]), $1 \leq i \leq n$, for $K_{n,n}$, is defined as:

$$g(i) \stackrel{\text{def}}{=} \{(ik, ti) \mid k, t \in \{i+1, \dots, n\}\} \cup \{(ii, ii)\}, \quad (2.4)$$

where (v_i, w_k, v_t, w_i) is a cycle of length 4 in BG_{i-1} .

The following Lemma (3.4 in [Asl17]) states the exact mapping between U_i and $g(i)$.

Lemma 2.1. *There exists a 1-1 mapping*

$$h : G^{(i)} \times U_i \longrightarrow g(i) \times M(BG_i),$$

s.t., $\forall(\pi, \psi) \in G^{(i)} \times U_i$, $\pi\psi$ is realized by a unique pair $(x_i, pm_i) \in g(i) \times M(BG_i)$ using a unique cycle (v_i, w_k, v_t, w_i) of length 4 in BG_{i-1} , defined by $x_i = (ik, ti)$, such that the edge pair x_i is covered by $\pi\psi$ and the other two alternate edges in the cycle are covered by π .

When $\psi = I$, the identity in S_n , the cycle collapses to one edge $x_i = (ii, ii)$ covered by π and $\pi\psi$ both.

2.2 The Generating Graph

The generating graph $\Gamma(n)$ for $K_{n,n}$ models the two binary relations R and S over $\bigcup g(i)$ (defined in [Asl17]).

$\Gamma(n) \stackrel{\text{def}}{=} (V, E_R \cup E_S)$, where $V = \bigcup g(i)$,

$E_R = \{a_i a_j \mid a_i R a_j, a_i \in g(i), a_j \in g(j) \ 1 \leq i < j \leq n\}$, and

$E_S = \{b_i b_{i+1} \mid b_i S b_{i+1}, b_i \in g(i) \text{ and } b_{i+1} \in g(i+1), 1 \leq i < n\}$.

Valid Multiplication Path (VMP/CVMP)

Definition 2.2. Let $p = x_i x_{i+1} \cdots x_{j-1} x_j$ be any path formed by the adjacent R - and S -edges in $\Gamma(n)$ such that exactly one node x_r is covered in each node partition r , where $x_r \in g(r)$, $1 \leq i \leq r \leq j \leq n$. Then p is a *valid multiplication path* if $\forall(x_r, x_s)$, on p , where $s > r$, we have either $x_r R x_s$ or the edge pairs x_r and x_s , are vertex-disjoint in $K_{n,n}$, and $x_r R x_s$ is false.

Further, p is a *Complete Valid Multiplication Path* (CVMP) if for every R -edge, $x_r R x_t$, (direct or jump edge) beginning at x_r in p , $i \leq r < j$, x_t is covered by p , i.e., $r < t \leq j$.

General Specification for Multiplying two Nodes

A *Multiplying Directed Acyclic Graph* (MDAG), denoted as $mdag(x_i, x_{i+1}, x_t)$, is a general specification for “multiplying” two nodes x_i and x_{i+1} in adjacent node partitions in $\Gamma(n)$, where $x_i S x_{i+1}$, and $x_i R x_t$ defines an R -edge such that all three nodes, x_i , x_{i+1} and x_t are covered by a common VMP. Clearly, in the extreme case $mdag(x_i, x_{i+1}, x_t)$ reduces to an R -edge defined by $x_i R x_{i+1}$, with $x_{i+1} = x_t$.

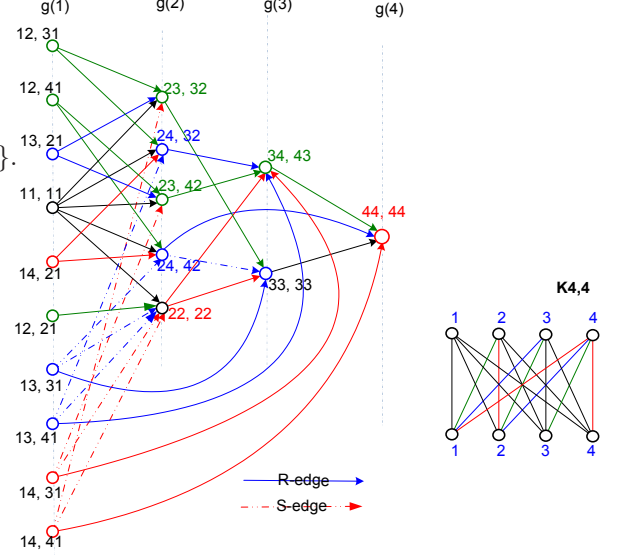


Figure 2: the Generating Graph $\Gamma(4)$

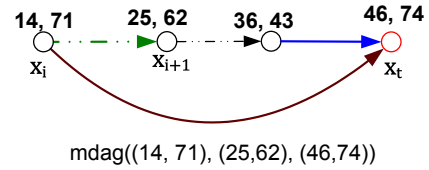


Figure 3: A Simple MDAG

2.2.1 Perfect Matching Represented by a CVMP

Let $\psi(x_i)$ denote the transposition $\psi = (i, k) \in S_n$ where $x_i = (ik, ji) \in g(i)$. Let $SE(x_i x_j)$ of an R -edge be defined as in (2.7) later under 2.3.1 Edge Requirements.

Lemma 2.3. *Every CVMP, $p = x_1 x_2 \cdots x_{n-1} x_n$ in $\Gamma(n)$, of length $n - 1$, where $x_r \in g(r)$, $r \in [1..n]$ represents a unique permutation $\pi \in S_n$ realized as a perfect matching $E(\pi)$ in $K_{n,n}$, given by*

$$E(\pi) = \bigcup_{x_i \in p} x_i - \{SE(x_j x_k) \mid x_j R x_k, (x_j, x_k) \in p\}, \text{ and} \quad (2.5a)$$

$$\pi = \psi(x_n) \psi(x_{n-1}) \cdots \psi(x_2) \psi(x_1), \quad (2.5b)$$

where $\psi(x_r) \in U_r$ is a transposition defined by the edge pair x_r , and U_r is a set of right coset representatives of the subgroup $G^{(r)}$ in $G^{(r-1)}$ such that $U_n \times U_{n-1} \cdots U_2 \times U_1$ generates S_n .

Notation: The labeling of nodes and edges in $\Gamma(n)$

Assuming the nodes in $K_{n,n}$ are labeled from $[0..9]$, an edge pair $(iv, wi) \in K_{n,n}$ is then labeled as the node (iv, wi) in $\Gamma(n)$, while the R -edges $((iv, wi), (wv, tw))$ are labeled by $+wv$.

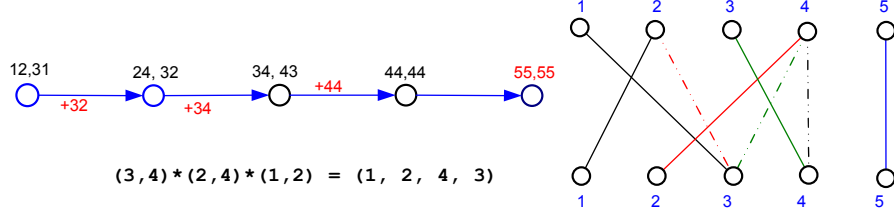


Figure 4: A Perfect Matching Composition

2.3 The Partition

The set under the partition is all the $n!$ possible perfect matchings in a bipartite graph. The equivalence classes are the disjoint subsets, induced by the missing edges in each potential perfect matching.

2.3.1 The Edge Requirements

Edge Requirement of a CVMP is an algebraic formulation of the perfect matching behavior that every node in the bipartite graph is incident with exactly one edge, i.e., the matched edge.

Let $p = x_1 x_2 \cdots x_{n-1} x_n$ be a CVMP in $\Gamma(n)$ for a bipartite graph BG . The Edge Requirement of a node $x_i \in g(i)$ in p is

$$ER(x_i) \stackrel{\text{def}}{=} \{e \mid e \in x_i \in g(i) \text{ and } e \notin BG\} \quad (2.6)$$

The edge pair x_i represents an initial assignment of the matched edges incident on the node pair (v_i, w_i) , in composing a perfect matching.

The *surplus edge*, $SE(x_t x_i)$, of an R -edge $x_t x_i$

$$SE(x_t x_i) \stackrel{\text{def}}{=} \text{the edge } e \in x_t \text{ covered by the associated } R\text{-cycle defined by } x_i R x_t. \quad (2.7)$$

When the given graph is not a complete bipartite graph, the edge requirement of a node x_i on p can be met by the surplus edge, $SE(x_t x_i)$, as determined by the R -edge $x_t x_i$ incident on x_i . For example, in Figure 4, for the CVMP $p = (12, 31) \cdot (24, 32) \cdot (34, 43) \cdot (44, 44)$, the initial $ER = \{44, 34, 32\}$ of various nodes on p is satisfied by the SE of the incident R -edges.

The Edge Requirement $ER(p)$ of a VMP, p for bipartite graph BG , is the collection of each of the nodes' Edge Requirement that is not satisfied by the SE of the R -edges incident on that node. That is,

$$ER(p) \stackrel{\text{def}}{=} \bigcup_{x_i \in p} ER(x_i) - (\{SE(x_j x_k) \mid x_j, x_k \in p\} \cap (\bigcup_{x_i \in p} ER(x_i))) \quad (2.8)$$

In [Asl17] Lemma 4.10, we show that a CVMP of length $n - 1$ represents a perfect matching in a bipartite graph BG iff $ER(p) = \emptyset$.

2.3.2 MinSets: The VMPs of Common ER

Let $mdag\langle x_i \rangle = mdag(x_i, x_{i+1}, x_r), r > i + 1$, denote a family of mdags. Let $m_i = mdag\langle x_i \rangle$ at some node x_i in the node partition i .

Let $ER^p(x_j)$ denote the ER of a node x_j covered by a VMP, p .

Definition 2.4. A *MinSet*(m_i, m_j), $1 \leq i < j \leq n - 1$, is the largest subset of $VMPSet(m_i, m_j)$, where each $p \in MinSet(m_i, m_j)$ has a common ER, $ER(p)$, such that

$\forall(p, x_k) \in MinSet(m_i, m_j)$, the common ER, $ER^p(x_k) = \emptyset$ except for the 3 common nodes, x_i, x_{i+1} , and x_{j+1} , in 3 distinguished node partitions ($i, i + 1$, and $j + 1$) (Fig 5).

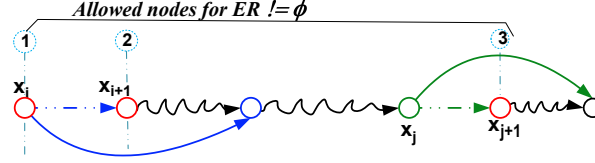


Figure 5: An Abstract MinSet: $\text{MinSet}(\text{mdag} \langle x_i \rangle, \text{mdag} \langle x_j \rangle)$

Representation of a MinSet

A MinSet has a representation similar to that of a VMPSet except for the additional attributes for the common ER and the incident R -edges.

EdgesAtNode (**Node**, {incident edges});
NodePartition **Array**[] of *EdgesAtNode*;

$\text{MinSet}(\text{mdag} \langle x_i \rangle, \text{mdag} \langle x_j \rangle, \text{ER}(x_{i+1})) = \text{Struct} \{$
 $\quad \text{MdagPair } (\text{mdag} \langle x_i \rangle, \text{mdag} \langle x_j \rangle);$
 $\quad \text{PartitionList } \mathbf{Array}[i \cdot (j+1)] \text{ of } \text{NodePartition};$
 $\quad // \text{ER at 3 distinguished node positions}$
 $\quad \text{CommonER } \text{ER}(x_i);$
 $\quad \text{CommonER } \text{ER}(x_{i+1});$
 $\quad \text{CommonER } \text{ER}(x_{j+1});$
 $\quad \text{Count } \mathbf{integer}; // \text{ the count of all the contained VMPs}$
 $\quad \}$
(2.9)

2.3.3 The Structure of a CVMPSet Partition

The Covering MinSet- a Subset of CVMPSet

Let \prod denote the product of two or more adjacent MinSets, similar to the product of VMPSets.

Let $I = \{i, j_1, j_2, \dots, j_{r-1}\}$ be an index set representing the various node partitions induced by the $\text{ER} \neq \emptyset$ nodes in $\text{VMPSet}(m_i, m_t)$ such that $|I| = r$, $1 \leq r \leq t - i$.

Definition 2.5. A *covering minset*, $\text{CMS}_{it}(r)$, represents a subset of $\text{VMPSet}(m_i, m_t)$ by a sequence of r MinSets for the given $\text{VMPSet}(m_i, m_t)$. That is,

$\text{CMS}_{it}(r) \stackrel{\text{def}}{=} \{\text{MinSet}(m_i, m_{j_1}), \text{MinSet}(m_{j_1}, m_{j_2}), \dots, \text{MinSet}(m_{j_{r-1}}, m_t)\},$
such that

$$\prod_{i_j \in I} \text{MinSet}(m_{i_j}, m_{i_{j+1}}) \subseteq \text{VMPSet}(m_i, m_t).$$

In [Asl17] we prove the following algebraic expression of the CVMPSet partition shown earlier in Figure 1:

Lemma 2.6. Let $\text{CMS}_{in}(r)$ be a MinSet sequence of length r representing a subset of $\text{CVMPSet}(m_i, m_{n-1})$, where $1 \leq r \leq n - 2$, $1 \leq i \leq n - 2$. Then, for all i , $1 \leq i \leq n - 2$,

$$\text{CVMPSet}(m_i, m_{n-1}) = \biguplus_{r=1}^{n-2} \prod_{\substack{\text{CMS}_{in}(r), \\ i_j \in I}} \text{MinSet}(m_{i_j}, m_{i_{j+1}}) \quad (2.10)$$

A Generating Set for the MinSet Sequences

Now we define a *generating set*, called *GMS*, for generating the MinSet Sequences which constitute a partition of the CVMPSet. This is to consolidate the generation of all the MinSets shared by the various CVMPSets through their CMS partitions.

Definition 2.7. A generating set for the MinSet sequences, $GMS(i, n)$, $1 \leq i \leq n-2$, for a bipartite graph on $2n$ nodes is a set of MinSets defined as

$$GMS(i, n) \stackrel{\text{def}}{=} \{MinSet(m_r, m_s) \mid (r, s) \in [i \cdots n-2] \times [i+1 \cdots n-1], r < s\},$$

where $\{(m_r, m_s)\}$ covers $g(r) \times g(s)$.

The following figure illustrates how exponentially many sequences are partitioned into polynomially many equivalence classes by the prefix MinSets in each $CMS_{in}(r)$.

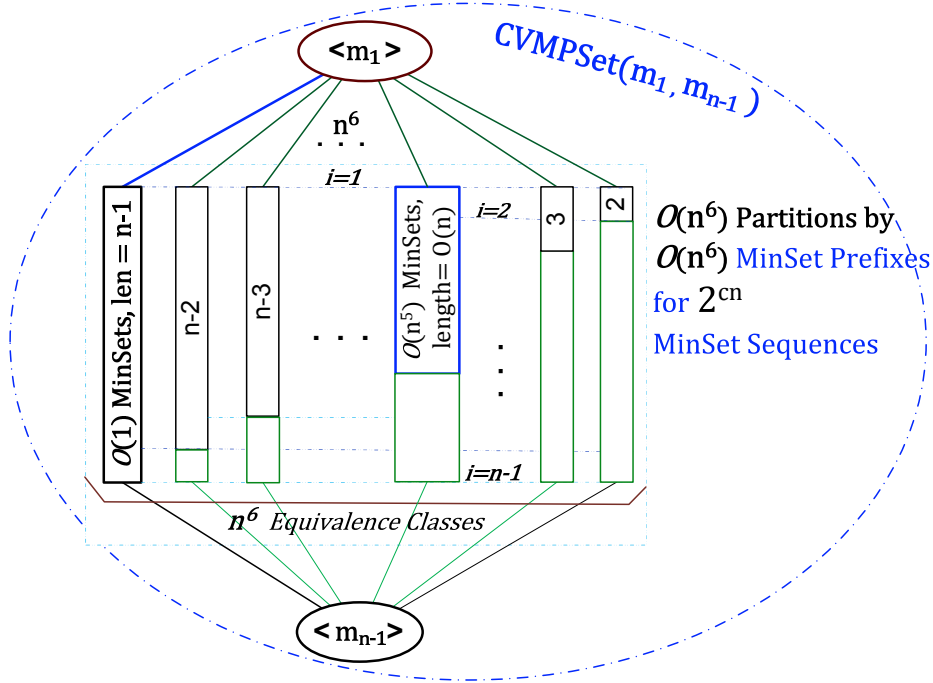


Figure 6: The Final Partition of a CVMPSet using MinSet Sequences

2.4 The Counting Algorithm

Algorithm 2.1 countPerfectMatchings(BG)

Input: a bipartite graph BG on $2n$ nodes, $n \geq 3$;

Output: count of the *perfect matchings* in BG ;

Step 0: Initialize- Compute the Initial Generating Set of all the MinSet Sequences

- 1: $i = n - 3$; // i is the current node partition;
 - 2: Compute the generating set $E_M = \{g(r) \mid 1 \leq r \leq n\}$;
 - 3: Compute the generating set $GMS(i + 1, n) = \{MinSet(m_{n-2}, m_{n-1})\}$; // the set of all the MinSet Sequences; each $CVMPSet(m_{n-2}, m_{n-1})$ is a $MinSet \in GMS(n-2, n)$, with a total count of 6 CVMPs.
-

Step 1: Count

if $(i = 0)$ then // $GMS(1, n)$ may contain the set $\{MinSet(m_1, m_{n-1})\}$

$$\text{perfect matching count} = \sum_{\substack{ER=\emptyset, \\ (m_1, m_{n-1})}} MinSet(m_1, m_{n-1}) \cdot Count;$$

return;

Step 2: Increment & Join the MinSet Sequences

incrementMSS($GMS(i+1, n)$); // assuming $n \geq 3$
(Follows the structures in Figure 6)
decrement i ;

repeat Steps 1-2;

End.

2.4.1 The Polynomial Time Bound

Claim 2.8. *The time complexity of Algorithm 2.1 is $O(n^{45} \log n)$.*

Proof.

See [Asl17]

□

2.4.2 Correctness of the Count

Lemma 2.9. *All the perfect matchings in a bipartite graph BG on $2n$ nodes can be enumerated in polynomial sequential time $O(n^{45} \log n)$.*

Proof.

The correctness essentially follows from the following two assertions as explained in [Asl17]:

1. The perfect matching *count* is:

$$\sum_{\substack{ER=\emptyset, \\ (m_1, m_{n-1})}} MinSet(m_1, m_{n-1}) \cdot Count, \text{ and}$$

2. All $MinSet(m_1, m_{n-1})$ with $ER = \emptyset$ are contained in $GMS(1, n)$.

Lemma 2.6 proves the correctness of the count. Claim 2.8 proves the polynomial bound for Algorithm 2.1.

□

3 The Counter-example Re-visited

Notation: The labeling of nodes and edges in $\Gamma(n)$

Assuming the nodes in $K_{n,n}$ are labeled from N using decimal numbers, a node $(iv, wi) \in \Gamma(n)$ is labeled as $i.v, w.i$, while the R -edges $((iv, wi), (wv, tw))$ are labeled by $+w.v$, where “.” is used as a delimiter to separate the node labels. When the node numbers are $0, 1, 2, \dots, 9$, we will ignore this delimiter “.”.

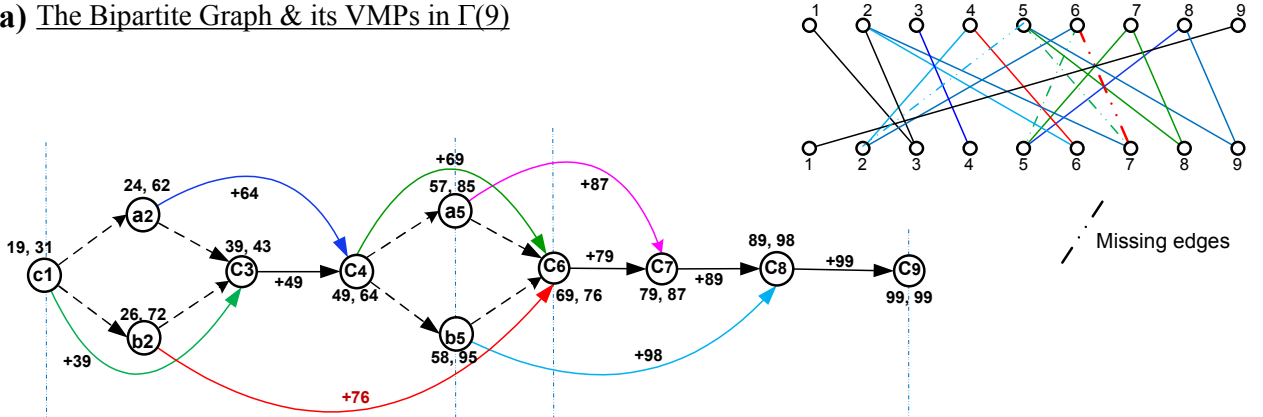
The following figure [Fig. 7(b)] shows various MinSets needed to correctly compute the perfect matchings.

The final step (Step 1 of Algorithm 2.1) creates $GMS(1, 9)$ with two MinSet sequences derived from $CVMPSet(m_1, m_8)$ and $CVMPSet(m'_1, m_8)$ respectively in the given bipartite graph:

1. $\{MinSet(m_1, m_5), MinSet(m_5, m_8)\}$, where $m_1 = mdag(c_1, a_2, c_3)$, $m_5 = mdag(a_5, c_6, c_7)$, and
2. $\{MinSet(m'_1, m_8)\}$, where $m'_1 = mdag(c_1, b_2, c_3)$.

Now the only MinSet sequence, $MinSet(m'_1, m_8)$, in (2) contains CVMPs of length 8, each having $ER = \emptyset$, giving the perfect matching count as 2.

(a) The Bipartite Graph & its VMPs in $\Gamma(9)$



(b) Two MinSet Sequences

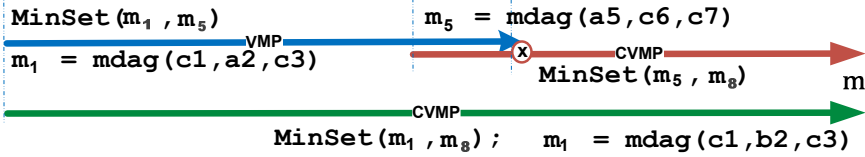


Figure 7: Corrected Evaluation of VMPSets

4 Acknowledgement

The author would like to express his sincere gratitude to the authors [Fra09] for finding a logical error in the earlier counting algorithm in [Asl08].

References

- [Asl08] Javaid Aslam, *The Collapse of the Polynomial Hierarchy: $NP = P$* ,
<https://arxiv.org/abs/0812.1385v3>, 2008.
- [Asl17] ———, *An Extension of the Permutation Group Enumeration Technique*,
<https://arxiv.org/abs/0812.1385v25>, 2017.
- [Fra09] Frank Ferraro, Garrett Hall and Andrew Wood, *Refutation of Aslam's Proof that $NP = P$* ,
<http://arxiv.org/pdf/0904.3912v2>, 2009.