The complexity of the certification of properties of Stable Marriage

Daniel J. Dougherty and Stanley M. Selkow

Worcester Polytechnic Institute Worcester, MA 01609 USA

Abstract

We give some lower bounds on the certificate complexity of some problems concerning stable marriage, answering a question of Gusfield and Irving.

Key words: stable marriage, combinatorial problems, computational complexity, certificate complexity

1 Introduction

An n-instance of the stable marriage problem is given by two disjoint sets $\mathcal{M}$ and $\mathcal{W}$ of the same size n, conventionally called the men and the women, together with, for each person, a total order on the opposite sex. A *matching,* or *marriage,* M is a one-to-one correspondence between $\mathcal{M}$ and $\mathcal{W}$. Man m and woman w are a *blocking pair* for a marriage M if m and w are not partners in M yet w precedes m's partner on m's list and m precedes w's partner on w's list. A marriage is *stable* if there are no blocking pairs.

Gale and Shapley [2] showed that any problem instance admits at least one stable marriage. There are algorithms to construct such marriages that run in $O(n^2)$ time; Ng and Hirschberg [4] have shown that this complexity is asymptotically optimal.

In their monograph [3] Gusfield and Irving include the following among the Open Problems:

..it requires $\Omega(n^2)$ time to check whether a matching is stable. However, once instability is established, there is a very succinct certificate of instability, namely a blocking pair. Is there a succinct certificate ($o(n^2)$ size) of stability?

In this note we give a negative answer to this question, and also give lower bounds for the certificate complexity of some related questions.

We encode an n-instance of a problem as follows. We may identify the set $\mathcal{M}$ of men and the set $\mathcal{W}$ of women each with the set $\{1,\ldots,n\}$, and represent each person's preference list as a permutation of $\{1,\ldots,n\}$, so a problem instance can be represented as a pair of $n \times n$ matrices of natural numbers.

Although formally we identify $\mathcal{M}$ and $\mathcal{W}$ with $\{1,\ldots,n\}$ it will often be clearer to use notation like "m_i" to refer to man i. We will write ρ_m [resp, ρ_w] for the permutation associated with man m [resp., with woman w]. So for example $\rho_m(w) = k$ expresses the fact that the man numbered m ranks the woman numbered w as kth on his preference list.

A pair (m,w) in an instance I is a *stable pair* if there is a stable marriage pairing m with w, otherwise it is an *unstable pair*; (m,w) is a *fixed pair* if every stable marriage for I pairs m and w.

Certificates There is a standard notion of "certificate complexity" in the literature, in the context of boolean functions [1]. Suppose $f : \{0,1\}^n \to \{0,1\}$. Let $C : S \to \{0,1\}$ be an assignment of values to some subset S of the n inputs; let the *size* of the certificate be the size of S . Say that C is *consistent* with $x \in \{0,1\}^n$ if $x_i = C(i)$ for all $i \in S$. A 0-certificate for f is an assignment C such that $f(x) = 0$ whenever x is consistent with C; a 1-certificate is defined similarly. The certificate complexity $C_x(f)$ of f on x is the size of a smallest $f(x)$-certificate that is consistent with x. The certificate complexity of f is $\max_x C_x(f)$.

Stable matching is not directly presented in terms of boolean functions, but the following is the natural translation of certificate complexity to our setting.

Informally, a *certificate* C is a partially specified instance. Formally, an n-certificate is a set of quadruples of the form $(\mathcal{M},m,w,r)$ or $(\mathcal{W},w,m,r)$ with $1 \leq m,w,r \leq n$. Here r is interpreted as $\rho_m(w)$ in the preference matrix for $\mathcal{M}$ [or $\rho_w(m)$ in the matrix for $\mathcal{W}$, as appropriate]. The *size* of a certificate C is the number of quadruples in C.

A *property* is a family $\mathcal{P} = \{\mathcal{P}_n \mid n \in \omega\}$ where each $\mathcal{P}_n$ is a set of n-instances. For example, the property that (m,w) IS A STABLE PAIR is the family of all instances in which pair (m,w) is stable. If $I \in \mathcal{P}$ we may say that *I satisfies* $\mathcal{P}$.

Let $\mathcal{P}$ be a property and let I be a problem instance. The certificate *C witnesses* $\mathcal{P}$ *for I* if I extends C and every instance which extends C satisfies $\mathcal{P}$. For example any certificate which includes $(\mathcal{M},m,w,1)$ and $(\mathcal{W},w,m,1)$ witnesses the property (m,w) IS A FIXED PAIR (in any instance containing this data) since in any instance extending this certificate, m and w are each other's first choice.

The *certificate complexity of* $\mathcal{P}$ *for I* is

$$\mathrm{CC}(\mathcal{P},I) = \min\{\mathrm{size}(C) \mid C \text{ witnesses } \mathcal{P} \text{ for } I\}$$

The *certificate complexity of* $\mathcal{P}$ *at n* is

$$\mathrm{CC}(\mathcal{P},n) = \max\{\mathrm{CC}(\mathcal{P},I) \mid I \text{ is an } n\text{-instance which satisfies } \mathcal{P}\}$$

We write $\mathrm{CC}(\mathcal{P})$ for $\mathrm{CC}(\mathcal{P},n)$ considered as a function of n.

If M is an unstable marriage in an n-instance, then as Gusfield and Irving observe, in order to demonstrate that M is unstable it suffices to exhibit a single blocking pair. That is, the certificate

$$\{(\mathcal{M},m,w,\rho_m(w)),(\mathcal{W},w,m,\rho_w(m)),(\mathcal{M},m,w',\rho_m(w')),(\mathcal{W},w,m',\rho_w(m'))\}$$

witnesses the instability of any marriage M in which $(m,w'),(m',w) \in M$ if $\rho_m(w) < \rho_m(w')$ and $\rho_w(m) < \rho_w(m')$. Since the size of this certificate does not grow with n we may say that *the certificate complexity of the property M* IS AN UNSTABLE MARRIAGE *is constant.*

2 Lower bounds for certificate complexity

Lemma 1 *Let I be an instance such that each woman has the same preference ordering. Then I admits exactly one stable marriage.*

Furthermore, if each woman ranks the men in the order 1,2,..., then each m_i *must be paired with the first w in* m_i*'s list such that w is not paired with any* m_s *for* $s < i$.

Proof. It suffices to prove the second assertion, since we may rename the men if necessary to satisfy the stronger hypothesis.

The proof is by induction on n. There is only one partner to whom man m_1 may be married: in every stable marriage he is paired with his top choice. If we then remove this pair from consideration we are left with a problem of size $n-1$ satisfying the hypothesis, so the result follows by induction. ///

Let I_n^* denote the n-instance in which for every $m, m_i \in \mathcal{M}$ and every $w, w_j \in \mathcal{W}$, $\rho_m(w_j) = j$ and $\rho_w(m_i) = i$. Let Id_n be the marriage $\{(m_1, w_1), \ldots, (m_n, w_n)\}$.

It is easily seen that I_n^* admits Id_n as its only stable marriage.

For $n \geq 3$ and $1 \leq j < k < l \leq n$, let $I^{j,k,l}$ be exactly the same as I_n^* except that w_j and w_l are exchanged in m_k's preference list. That is, in $I^{j,k,l}$

$$\begin{aligned} \rho_w\,(m_s) &= s \quad \text{for all } w \\ \rho_{m_k}(w_j) &= l \\ \rho_{m_k}(w_l) &= j \\ \rho_{m_k}(w_i) &= i \quad \text{for } i \neq j, i \neq l. \\ \rho_m\,(w_t) &= t \quad \text{for } m \neq m_k. \end{aligned}$$

Lemma 2 *The instance $I^{j,k,l}$ admits exactly one stable marriage:*
$\{(m_i, w_i) \mid 1 \leq i < k \vee l < i \leq n\} \cup \{(m_k, w_l\} \cup \{(m_i, w_{i-1}) \mid k < i \leq l\}$.

Proof. This is a direct consequence of Lemma 1. ///

Let Id IS STABLE be the property defined, at each n, to be the set of n-instances for which Id_n is stable.

Theorem 3 *The certificate complexity of the property* Id IS STABLE *is* $\Omega(n^2)$.

Proof. We show that

$$\mathrm{CC}(\mathrm{Id\ IS\ STABLE},\ I_n^*) \quad \text{is} \quad \Omega(n^2).$$

It suffices to establish the claim that if C is a certificate of the stability of Id for I_n^*

then for every k, either

$$\forall j < k \quad (\mathcal{M}, m_k, w_j, j) \in C \quad \text{or} \quad \forall l > k \quad (\mathcal{M}, m_k, w_l, l) \in C$$

since this obviously requires $\Omega(n^2)$ quadruples.

To verify the claim note that if it failed at k we would have $(\mathcal{M}, m_k, w_j, j) \notin C$ for some $j < k$ and $(\mathcal{M}, m_k, w_l, l) \notin C$ for some $l > k$, so that $I^{j,k,l}$ would extend C. Since Id is not stable in $I^{j,k,l}$ this contradicts the the assumption that C witnesses the stability of Id. ///

One might reasonably expect that there exist short certificates for stability properties of a single pair in an instance. But in fact the argument above shows that this is not the case.

Corollary 4 *For any man-woman pair p, the certificate complexity of each of the following properties is* $\Omega(n^2)$.

(1) p IS A STABLE PAIR
(2) p IS A FIXED PAIR
(3) p IS AN UNSTABLE PAIR

Proof. For the first assertion we observe that the argument of Theorem 3 actually shows that in order that a certificate C witness the stability of the pair (m_e, w_e) in I_n^* it is necessary that for every $k < e$,

$$\forall j < k \quad (\mathcal{M}, m_k, w_j, j) \in C \quad \text{or} \quad \forall l > e \quad (\mathcal{M}, m_k, w_l, l) \in C.$$

Since: if this were violated at k we would have $(\mathcal{M}, m_k, w_j, j) \notin C$ for some $j < k$ and $(\mathcal{M}, m_k, w_l, l) \notin C$ for some $l \geq e$, so that $I^{j,k,l}$ would extend C. And by Lemma 2 the pair (m_e, w_e) is not stable in $I^{j,k,l}$ (since $k < e \leq l$). So when $e = \lceil n/2 \rceil$, C requires $\Omega(n^2)$ quadruples.

For the second assertion we simply note that since the instances I_n^* admit a single stable marriage, a pair p is stable in I_n^* if and only if it is fixed. So the result follows from the previous part.

For the third assertion we note that in the instance I_n^* the pair $p = (m_{\lceil n/2 \rceil}, w_{\lceil n/2 \rceil - 1})$ is unstable, but becomes stable if the values of any one pair $1 \leq j \leq k < n/2 \leq l \leq n$ are exchanged.

///

References

[1] H. Buhrman and R. de Wolf. Complexity measures and decision tree complexity: A survey. *Theoretical Computer Science*, 288:21–43, 2002.

[2] D. Gale and L Shapley. College admissions and the stability of marriage. *American Mathematical Monthly*, 69:9–15, 1962.

[3] D. Gusfield and R. W. Irving. *The Stable Marriage Problem: Structure and Algorithms.* MIT_Press, 1989.

[4] C. Ng and D. Hirschberg. Lower bounds for the stable marriage problem and its variants. *SIAM J. Computing,* 19:71–77, 1990.