hexagon:2610.00262v2

A Formally Verified Certificate Proof of the Maximum Number of Stable Matchings for Six Men and Six Women

Yuran Xiu

16 October 2026

Abstract

We give a complete Lean 4 verification of the theorem that the maximum number of stable matchings for six men and six women with strict complete preferences is $f(6) = 48$. Jo (2026) previously proved the unrestricted upper bound, and Benjamin, Converse, and Krieger (1995) supplied an attaining construction. Our contribution is an alternative, fully formalized proof using a finite certificate; the value 48 and the unrestricted theorem are already known. We reduce stable matchings of arbitrary profiles to order ideals of sequences of cyclic partner exchanges in which no man revisits a partner. A weighted frontier recurrence counts these ideals, and a sum of permanents bounds every future continuation. These bounds yield a finite certificate with 135,828 states. The complete argument, including the reduction for arbitrary profiles, certificate soundness, all concrete checks, and an attaining profile, has been formalized and checked in Lean 4. The final unconditional theorem depends only on the standard axioms of Lean and mathlib.

1 Introduction

In the stable marriage problem, each of n men and n women strictly ranks all members of the other side. A perfect matching is stable if no unmatched pair strictly prefer each other to their assigned partners. Gale and Shapley [1] proved that every such instance has a stable matching. How many stable matchings can one instance have? Write

$$f(n) = \max_P |\mathcal{S}(P)|,$$

where P ranges over all strict complete preference profiles and $\mathcal{S}(P)$ is its set of stable matchings. We give a fully formalized proof of the known value $f(6) = 48$, established by Jo [3, Theorem 5.1].

Theorem 1.1. *Every strict complete preference profile on six men and six women has at most* 48 *stable matchings. Some such profile has exactly* 48 *stable matchings. Consequently,* $f(6) = 48$.

The contribution of this paper is the complete Lean verification of Theorem 1.1 by the cycle-schedule and certificate method developed below. The verification starts from arbitrary strict complete preference profiles and includes the structural reduction, certificate soundness, every concrete check, and an attaining profile. The numerical value and the unrestricted upper bound were already proved by Jo [3]; we make no priority claim for that theorem. The lower-bound construction belongs to the dihedral/Latin family analyzed by Benjamin, Converse, and Krieger [2]. Our rank tables are taken from Eilers's presentation of the construction attributed to Converse [11].

Previous work. Benjamin, Converse, and Krieger [2] studied Latin marriage constructions and gave the order-six lower bound 48. Thurber [4] developed further constructions and lower bounds for the extremal function. Eilers's sequences record exact values and lower bounds [9, 10]. Latin profiles form a restricted class in which the two ranks assigned to each pair have constant sum; Borodin et al. [8, Section 3.7] distinguish these restricted counts from the unrestricted extremal problem.

Jo's preprint [3], first deposited on 20 September 2026, proves the unrestricted upper bound by a different route. It derives local constraints on rotation posets and proves that a poset with at most fifteen elements, width at most three, and a specified common-incomparability property has at most 48 antichains. The rotation correspondence then gives $f(6) = 48$. Our proof instead uses a weighted frontier recurrence and a permanent bound to certify all legal cycle schedules. As described in Jo's verification note [3, Section 6], his Lean development checks the finite-poset core and supporting components, while the passage from stable marriage to that core remains in the manuscript. Our formal development includes its own reduction from preference profiles and proves the unconditional stable-marriage statement in Lean. This difference concerns formal proof coverage: Jo gives a complete mathematical proof of the theorem. We do not claim that the unformalized connections in that development constitute a mathematical gap, or that our method improves the bound.

For general n, Karlin, Oveis Gharan, and Weber [5] proved a simply exponential upper bound on $f(n)$. Palmer and Pálvölgyi [6] subsequently proved the bound $3.55^n + O(1)$. Our formalization concerns one exact finite value; it does not improve the asymptotic exponential base. Lattice and rotation methods underlie the structural part of the proof. In particular, Cai and Thomas [7] give a representation of all stable matchings using a maximal chain. We give the cover and coordinate-clamping arguments needed for our reduction explicitly, and claim no novelty for the classical lattice structure.

Proof strategy. A maximal chain of stable matchings changes one cyclic group of partners at each step. Each man's partners strictly worsen whenever he changes, so he never revisits a partner. We associate to such a sequence the partial order generated by chronological precedence between events sharing a man. Every stable matching injects into an order ideal of this partial order. This order can omit constraints from the full rotation representation; the injection is enough for an upper bound.

We count these ideals by a vector indexed by subsets of the men. Together with a normalized matrix of already visited pairs, this vector contains all information needed to update the count along further cyclic exchanges. A permanent bound allows an entire continuation to be certified without listing its events. The resulting certificate checks every legal cycle at every stored state, either by the bound or by a reference to an earlier state. The universal reduction and the entire finite certificate are checked in Lean, culminating in the quantified statement of Theorem 1.1. Sections 2–5 describe the mathematics; Section 7 describes the formal artifact and its verification boundary.

2 Preference profiles and cycle schedules

We label each side by $[n] = \{0, \dots, n-1\}$. A profile consists of rank functions $r_m : [n] \to [n]$ for each man m and $s_w : [n] \to [n]$ for each woman w, all bijections; smaller ranks are preferred. A matching is a bijection $p : [n] \to [n]$. Its stability condition is

$$\text{there are no } m, w \text{ such that } r_m(w) < r_m(p(m)) \quad \text{and} \quad s_w(m) < s_w(p^{-1}(w)). \tag{1}$$

The labels on the two sides designate different people.

Definition 2.1. A *cycle schedule* is a sequence of matchings $p_0, p_1, \ldots, p_t$ and permutations $q_1, \ldots, q_t \in \mathfrak{S}_n$ such that each q_i is a single cycle of length at least two, fixing every label outside its support C_i, and

$$p_i(m) = p_{i-1}(q_i(m)).$$

Each man must receive a previously unvisited woman whenever he participates: if $m \in C_i$, then $p_i(m) \neq p_j(m)$ for every $0 \leq j < i$. The event order is generated by $i \prec j$ whenever $i < j$ and $C_i \cap C_j \neq \varnothing$. Let $\mathcal{J}(S)$ be the order ideals of this order for a schedule S.

An order ideal contains every predecessor of each of its events. Equivalently, on each man's chronological list of events, its selected events form a prefix. Every event consumes at least two previously unvisited pairs. Thus $t \leq n(n-1)/2$. The certificate argument below bounds arbitrary finite legal continuations directly and does not assume this length bound.

Lemma 2.2. *Executing the events of an ideal in chronological order produces a matching. The resulting map $\mathcal{J}(S) \to \mathfrak{S}_n$ is injective.*

Proof. Before a selected event, every participant has executed all his earlier events in the full schedule. He therefore holds exactly the woman prescribed just before that event. The selected event performs the specified cyclic exchange and preserves the matching property. This proves the first claim by induction through the selected events.

For a fixed man, the selected events on his list form a prefix. His partners after successive changes are all distinct, including his initial partner, so his final partner determines the length of this prefix. The final matching therefore determines every participant's decision at every event. Every event has a participant, which determines the ideal. □

2.1 From stable matchings to a schedule

Order stable matchings by $x \leq y$ if $r_m(x(m)) \leq r_m(y(m))$ for all m. Thus moving upward weakly worsens the men's partners.

Lemma 2.3 (Lattice closure)**.** *The stable matchings are closed under coordinatewise minimum and maximum of the men's partner ranks. If nonempty, they form a finite lattice under the order above.*

Proof. The union of two matchings x, y decomposes into common edges and alternating cycles. On a nontrivial cycle, suppose m prefers $x(m) = w$ to $y(m)$, and put $m' = y^{-1}(w)$. Stability of y forces w to prefer m' to m. Stability of x then forces m' to prefer $x(m')$ to $y(m') = w$. Repeating around the cycle shows that all its men prefer their x partners, and all its women prefer their y partners. The reverse case is symmetric.

Consequently, choosing the better partner for each man takes whole cycles from x or y and yields a bijection a; choosing the worse yields a bijection b. Each woman receives her less preferred old partner in a and her more preferred old partner in b.

If (m, w) blocked a, then m would prefer w to both his old partners. Stability of each old matching would make w prefer each of her old partners to m, contradicting a block. If (m, w) blocked b, choose an old matching assigning m the partner $b(m)$. Its stability makes w prefer its partner to m; her partner in b is at least as good. Thus both a and b are stable. Finite closure provides a least and a greatest matching and proves the assertion. □

Lemma 2.4 (Covers are cyclic exchanges)**.** *If $x < y$ are stable matchings and no stable matching lies strictly between them, then y is obtained from x by one nontrivial cyclic exchange.*

Proof. Let $D = \{m : x(m) \neq y(m)\}$. For each $m \in D$, choose his most preferred woman $a(m)$ satisfying

$$r_m(x(m)) < r_m(a(m)) \leq r_m(y(m)), \qquad s_{a(m)}(m) < s_{a(m)}(x^{-1}(a(m))). \tag{2}$$

Such a woman exists: $y(m)$ qualifies by the opposite preference property on alternating cycles. Put $h(m) = x^{-1}(a(m))$. Then $h(m) \neq m$. Also $h(m) \in D$. Otherwise $y(h(m)) = x(h(m)) = a(m)$; bijectivity of y and $h(m) \neq m$ imply $a(m) \neq y(m)$. The weak rank inequality in (2) is then strict and $(m, a(m))$ blocks y.

The finite self-map $h : D \to D$ has a directed cycle C of length at least two. Change $x(m)$ to $a(m) = x(h(m))$ for $m \in C$, leaving other partners unchanged, and call the resulting matching z. We have $x < z \leq y$, and every woman affected by the cycle strictly improves relative to x.

An unchanged man cannot newly block. For a changed man m, a woman strictly better than $x(m)$ cannot block, by stability of x and the women's weak improvement. His old partner $x(m)$ has strictly improved, so cannot block either. Any remaining prospective blocking woman would lie strictly between $x(m)$ and $a(m)$ on his list and prefer m to her partner in z, hence also to her partner in x. This contradicts the choice of $a(m)$. Thus z is stable. The cover hypothesis gives $z = y$. □

Proposition 2.5 (Universal schedule reduction)**.** *For every strict complete profile P on n men and n women, there is a cycle schedule S such that*

$$|\mathcal{S}(P)| \leq |\mathcal{J}(S)|. \tag{3}$$

Proof. If the stable set is empty, the inequality holds for the empty schedule. Otherwise choose a saturated chain from the least to the greatest stable matching,

$$c_0 < c_1 < \cdots < c_t.$$

By Lemma 2.4, its steps are cyclic exchanges. A man's rank strictly increases whenever he changes, so the sequence is a cycle schedule.

For a stable matching x and $1 \leq i \leq t$, form the lattice clamp

$$F_i(x) = (x \vee c_{i-1}) \wedge c_i.$$

It lies between the endpoints of a cover and hence equals one of them. For each participant $m \in C_i$, the alternatives imply, respectively,

$$F_i(x) = c_{i-1} \implies r_m(x(m)) \leq r_m(c_{i-1}(m)), \tag{4}$$

$$F_i(x) = c_i \implies r_m(x(m)) \geq r_m(c_i(m)). \tag{5}$$

Indeed, the clamped rank is $\min\{\max\{r_m(x(m)), r_m(c_{i-1}(m))\}, r_m(c_i(m))\}$, and the two endpoint ranks are distinct.

Let $I(x) = \{i : F_i(x) = c_i\}$. If $i < j$ share a man and $j \in I(x)$, then that man's rank in x is at least his rank at c_j, and hence at c_i. Alternative (4) at i is impossible. Thus $i \in I(x)$, and $I(x)$ is an ideal.

Fix a man. The partners he encounters at changes along the chain have strictly increasing ranks, starting with his best stable partner and ending with his worst. The clamp alternatives exclude any stable partner rank strictly between two consecutive entries. Hence $x(m)$ is one of these partners. Its position is precisely the prefix length of this man's events selected by $I(x)$. Executing the ideal therefore recovers $x(m)$ for every m. This proves that $x \mapsto I(x)$ is injective. A singleton stable set yields an empty chain and is included. □

This reduction allows any initial matching c_0. Relabeling women by their partners in c_0 makes it the identity without restricting the profile. No hypothesis about columns of the preference tables, rotation lengths, or the shape of the stable lattice is imposed.

3 An exact recurrence for schedule ideals

Consider a prefix of a schedule. For an ideal I of the prefix, define its *frontier*

$$A(I) = \{m : m \text{ has no event in the prefix, or his latest event belongs to } I\}.$$

Let $a(A)$ be the number of prefix ideals with frontier $A \subseteq [n]$. The total ideal count is $T(a) = \sum_A a(A)$. Initially, $a([n]) = 1$ and all other entries are zero.

Lemma 3.1 (Frontier update)**.** *When an event with support C is appended, the new weights are obtained by the additions*

$$a'(A \setminus C) \mathrel{+}= a(A) \quad \textit{for every } A, \qquad a'(A) \mathrel{+}= a(A) \quad \textit{if } C \subseteq A, \tag{6}$$

starting from the zero vector.

Proof. Every old ideal extends by excluding the new event, giving frontier $A \setminus C$. It extends by including the event precisely when all its participants' earlier events have been selected, which is equivalent to $C \subseteq A$. Inclusion then leaves frontier A. The restriction of an extended ideal to the old prefix, together with its decision on the new event, is unique. The two contributions therefore count all extensions without omission or duplication. □

To record chronological legality, name each currently held woman by her current holder. Let $R_{ij} = 1$ if man i has already visited the woman currently held by man j. The diagonal entries equal one. A cyclic exchange q with support C is legal exactly when

$$R_{i,q(i)} = 0 \qquad (i \in C). \tag{7}$$

After the exchange, rename women by their new holders. The matrix update is

$$R'_{ij} = R_{i,q(j)} \vee \mathbf{1}_{i=j}. \tag{8}$$

The column permutation records the new holder of every woman; the added diagonal records the newly acquired partners. For a legal exchange, the number of entries equal to one increases by $|C|$.

We call $s = (R, a)$ a state and write $s \cdot q = (R', a')$ for (6)–(8). The initial state is

$$R_{ij} = \mathbf{1}_{i=j}, \qquad a(A) = \mathbf{1}_{A=[n]}. \tag{9}$$

For every schedule, iterating these updates from the initial state gives exactly its ideal count. The normalized matrix decides which future chronological exchanges are legal; the weights give the exact effect of each exchange on the ideal count.

Relabeling. If new man i denotes old man $\pi(i)$, with normalized women relabeled the same way, define

$$R^{\pi}_{ij} = R_{\pi(i),\pi(j)}, \qquad a^{\pi}(A) = a(\pi(A)). \tag{10}$$

The corresponding event is $\pi^{-1} \circ q \circ \pi$. Substitution into the transition formulas shows that relabeling commutes with transitions, preserves legality, and preserves T. Thus it preserves all continuation bounds. The certificate checks these equalities for each supplied permutation; its correctness does not require a canonical labeling algorithm.

4 A permanent bound for all continuations

For a state $s = (R, a)$, define a zero–one matrix

$$B_R(i,j) = \mathbf{1}_{\{i=j \text{ or } R_{ij}=0\}}$$

and set

$$U(R,a) = \sum_{A \subseteq [n]} a(A)\,\mathrm{per}(B_R[A,A]), \qquad \mathrm{per}(B_R[\varnothing,\varnothing]) = 1. \tag{11}$$

Proposition 4.1 (Continuation bound)**.** *For a state reached by a schedule prefix, every finite legal continuation has at most $U(R,a)$ ideals in total.*

Proof. Fix a prefix ideal I with frontier A. If $m \notin A$, his last prefix event is excluded. Every future event involving him has that excluded event as a predecessor, so no such event can be selected by an ideal extending I. If $m \in A$, all his prefix events are selected, and his partner after executing I is the woman currently labeled m. Hence the men in A hold exactly the women labeled by A.

Selected future events are confined to A, leaving the outside matching fixed. Their final matching on A uses either a current diagonal pair or a pair unvisited by that man in the full chronological prefix. It is thus a bijection counted by $\mathrm{per}(B_R[A,A])$. Distinct extensions of I give distinct final matchings by Lemma 2.2. There are $a(A)$ choices of I with this frontier. Summing the bound over all old ideals proves the claim. □

The checker also needs the bound for stored states without assuming that each state is reachable. We next establish the stronger algebraic invariant used in its soundness proof.

4.1 Support expansion and monotonicity

Let $\mathcal{P}(R)$ consist of permutations $\rho \in \mathfrak{S}_n$ such that $\rho(i) = i$ or $R_{i,\rho(i)} = 0$ for every i. Put $D(\rho) = \mathrm{supp}(\rho)$ and

$$Z_a(D) = \sum_{A \supseteq D} a(A).$$

Extending a bijection of A by the identity outside A gives

$$U(R,a) = \sum_{\rho \in \mathcal{P}(R)} Z_a(D(\rho)). \tag{12}$$

Different permutations with the same support remain different terms.

Lemma 4.2 (Support formula)**.** *Suppose R has diagonal one, a has nonnegative integer entries, and q is a legal cyclic exchange with support C. Then*

$$U((R,a)\cdot q) = \sum_{\substack{\rho \in \mathcal{P}(R) \\ D(\rho)\cap C = \varnothing \ \text{ or } \ C \subseteq D(\rho)}} Z_a(D(\rho)). \tag{13}$$

In particular, the value of this next-state bound depends on the support of a legal exchange and not on its cyclic orientation.

Proof. Fix an old frontier A. The exclusion term in (6) has permanent $\mathrm{per}(B_{R'}[A \setminus C, A \setminus C])$. The permutation q fixes columns outside C, so this equals $\mathrm{per}(B_R[A \setminus C, A \setminus C])$. In old full-permutation notation, it counts precisely $\rho \in \mathcal{P}(R)$ with $D(\rho) \subseteq A$ and $D(\rho) \cap C = \varnothing$.

The inclusion term exists when $C \subseteq A$. If π is an allowed completion on A in the new labels, its old-label form is $\rho = q \circ \pi$. For a moved row of π, the condition $R'_{i,\pi(i)} = 0$ implies $R_{i,\rho(i)} = 0$. For a fixed row of π that is moved by q, the same old entry is zero by legality of q. Thus $\rho \in \mathcal{P}(R)$ and it fixes the complement of A. Moreover, every $i \in C$ is moved by ρ: if $\pi(i) = i$ this follows from $q(i) \neq i$; otherwise $\rho(i) = i$ would contradict $R_{ii} = 1$.

Conversely, suppose $\rho \in \mathcal{P}(R)$, $D(\rho) \subseteq A$, and $C \subseteq D(\rho)$. Set $\pi = q^{-1} \circ \rho$. It fixes the complement of A. If $\pi(i) \neq i$, then $\rho(i) \neq i$: otherwise $i \notin C$ and $q^{-1}(i) = i$, a contradiction. Hence $R_{i,\rho(i)} = 0$; together with $i \neq \pi(i)$, formula (8) gives $R'_{i,\pi(i)} = 0$. This proves the desired bijection for inclusion.

For each A, the two contributions therefore count old allowed permutations whose supports are contained in A and either avoid or contain C. These cases are disjoint because C is nonempty. Summing with weight $a(A)$ and interchanging the finite sums gives (13). □

Corollary 4.3. *For every state with diagonal one and nonnegative weights,*

$$T(a) \leq U(R, a), \qquad U((R, a) \cdot q) \leq U(R, a)$$

for every legal cyclic exchange q. If $U(R, a) \leq b$, then every finite legal continuation has total weight at most b.

Proof. The identity permutation belongs to $\mathcal{P}(R)$ and contributes $Z_a(\varnothing) = T(a)$ to (12). Formula (13) retains a subset of its nonnegative summands, proving monotonicity. Transitions preserve the diagonal and nonnegativity. Induction on the continuation length proves the final assertion. □

The initial bound is $n!$; if all pairs have been visited it is just the current total. A small bound therefore certifies the entire remaining continuation, rather than only the count at the current prefix.

5 The finite certificate for six participants per side

Fix a threshold b. Write $\mathrm{Safe}_b(s)$ if every finite legal continuation from s, including the empty continuation, has total weight at most b. The following rules suffice:

1. If $U(s) \leq b$, then $\mathrm{Safe}_b(s)$ by Corollary 4.3.
2. If $T(s) \leq b$ and $\mathrm{Safe}_b(s \cdot q)$ for every legal cycle q, then $\mathrm{Safe}_b(s)$, by separating the empty and nonempty continuations.
3. Relabeling a state as in (10) preserves Safe_b.

The stored states have diagonal one and nonnegative integer weights.

Definition 5.1 (Local certificate)**.** A certificate consists of states $s_0, \ldots, s_{N-1}$, an initial-state reference, and the following local data. Each state satisfies $T(s_i) \leq b$. For every cycle q legal at s_i, either the checker proves $U(s_i \cdot q) \leq b$, or there is an index $j < i$ and a permutation π for which $(s_i \cdot q)^\pi = s_j$. The initial-state reference identifies a relabeling of (9) with a stored state.

Lemma 5.2 (Certificate soundness)**.** *Every state in a valid local certificate satisfies* Safe_b*. In particular, every cycle schedule from the initial state has at most b ideals.*

Proof. Induct on the stored index. A legal successor is safe either by its permanent bound or by a relabeling of an earlier safe state. The current total is at most b, so rule 2 proves safety of the present state. The checked root reference transfers safety to the initial state. The exact recurrence of Section 3 then bounds the ideal count of every schedule. □

For $n = 6$ there are

$$\sum_{k=2}^{6} \binom{6}{k} (k-1)! = 409 \tag{14}$$

nontrivial single cycles. A cycle is represented by listing its least participant first and then ordering the remaining participants. Both orientations are retained whenever they differ. The formal development checks coverage of every single-cycle permutation on six labels.

Proposition 5.3 (Checked certificate)**.** *There is a valid local certificate at threshold* 48 *for the initial state on six labels, with* 135,828 *stored states and* 177,338 *reference edges. Its root is stored node* 135,827 *in zero-based indexing.*

Computational proof. The certificate is the file `certificate-n6.json` in the accompanying artifact. Each stored state is represented by six row masks and 64 natural number weights. Each explicit edge contains a cycle index, a referenced state, and a relabeling permutation. The checker verifies the state format, diagonal, current total, and every one of the 409 possible cycle moves. For a legal move, it checks either an explicit reference or the support-form upper bound from Lemma 4.2. The reference check compares the entire transformed matrix and weight vector with the target. The bound check retains multiplicities of permutations sharing a support. All sums and comparisons are over natural numbers.

The exported data are converted to explicit Lean definitions and local Boolean-check theorems, proved by kernel reduction. A proved checker soundness theorem combines each local check with the already proved safety of its referenced states. The generated proof graph is acyclic; every reference is discharged by an earlier safety theorem. The checked root equality identifies the last state with the initial state, using the identity relabeling for this certificate.

All local checks and all safety theorems compiled successfully. This includes the root theorem `StableSix.ProductionChunks.initial_safe`. The final full-source run accepted all 2,181 modules and then checked the unconditional public theorem and its transitive axioms. Section 7 specifies the source identities and audit. □

For clarity, the mathematical content of the local checking procedure can be written as follows. The actual implementation uses sparse weights and reuses support sums, but proves their connection to these conditions.

```
check_state(i):
    require valid_state(s[i]) and total(s[i]) <= 48
    for each of the 409 single cycles q:
        if not legal(s[i], q): continue
        if a checked reference (j, pi) satisfies
             j < i and relabel(next(s[i], q), pi) == s[j]:
            continue
        require support_bound(s[i], support(q)) <= 48
    accept
```

Generation and coverage. An external search generates candidate data using the normalized recurrence, permanent pruning, and memoization up to simultaneous relabeling. The recorded certificate replay has 4,228,638 legal transitions: 4,051,300 are discharged by the bound and 177,338 by references. These replay counts describe the artifact; the formal proof uses the verified local checks and cycle coverage. It does not assume correctness of the search, its hash table, canonicalization, or replay program. Neither a timeout nor an observed maximum in a partial search is used as an upper bound. There is no restriction to swaps, to Latin profiles, or to a selected first event.

Corollary 5.4. *Every strict complete six-by-six preference profile has at most 48 stable matchings.*

Proof. Proposition 5.3 and Lemma 5.2 bound the number of ideals of every cycle schedule on six labels by 48. Apply Proposition 2.5 to the arbitrary profile. □

6 A known profile attaining 48

Benjamin, Converse, and Krieger [2, Theorem 3 and Section 5] analyzed the dihedral/Latin construction DS_n. Their counting formula gives $(3+1)\binom{6}{3} - 2^5 = 48$ stable matchings for DS_3, an instance with six participants on each side. The following rank tables use the presentation attributed to Converse and reproduced by Eilers [11]. In the left table, row m, column w is $r_m(w)$. In the right table, row w, column m is $s_w(m)$. Entries are ranks starting at zero, not lists of partner labels.

$$(r_m(w))_{m,w} = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 1 & 0 & 3 & 2 & 5 & 4 \\ 2 & 5 & 4 & 1 & 0 & 3 \\ 3 & 4 & 5 & 0 & 1 & 2 \\ 4 & 3 & 0 & 5 & 2 & 1 \\ 5 & 2 & 1 & 4 & 3 & 0 \end{pmatrix}, \qquad (s_w(m))_{w,m} = \begin{pmatrix} 5 & 4 & 3 & 2 & 1 & 0 \\ 4 & 5 & 0 & 1 & 2 & 3 \\ 3 & 2 & 1 & 0 & 5 & 4 \\ 2 & 3 & 4 & 5 & 0 & 1 \\ 1 & 0 & 5 & 4 & 3 & 2 \\ 0 & 1 & 2 & 3 & 4 & 5 \end{pmatrix}. \tag{15}$$

Each row is a permutation, so these are strict complete preferences. For every pair (m, w) the two ranks sum to five.

Lemma 6.1. *The profile in* (15) *has at least 48 stable matchings.*

Proof. Table 2 lists 48 distinct permutations $p = (p(0), \ldots, p(5))$. For each listed permutation and every pair (m, w), direct substitution in (15) verifies

$$r_m(w) \geq r_m(p(m)) \quad \text{or} \quad s_w(m) \geq s_w(p^{-1}(w)).$$

Thus each is stable. The formal proof checks the row inverses for the rank tables, inverse tables for all listed matchings, stability, and distinctness by kernel reduction, giving an injection from a 48-element type into the stable matchings of this profile. □

Proof of Theorem 1.1. Corollary 5.4 gives the universal upper bound, and Lemma 6.1 gives an attaining profile. The profile consequently has exactly 48 stable matchings. □

7 Formal verification and reproducibility

7.1 Statement and proof coverage

The formal model assigns each person an independent permutation of ranks. A matching is a permutation, and stability is exactly (1). The public proposition is

```
def MaximumStableSixIs48 : Prop :=
  (forall P : Profile 6, Nat.card (StableMatching P) <= 48) /\
    (exists P : Profile 6, Nat.card (StableMatching P) = 48)
```

The notation above uses ASCII equivalents of the logical symbols in the source. The checked endpoint is

```
StableSix.maximumStableSixIs48 : StableSix.MaximumStableSixIs48
```

It has no profile restriction and no remaining safety or certificate-validity premise. In particular, the intermediate theorem taking initial-state safety as a hypothesis is closed by the proved concrete root theorem.

The model includes all strict complete six-by-six profiles. Each row is independent of every other row. The stable-matching subtype is finite, so its `Nat.card` is the usual cardinality. The statement does not concern ties, incomplete lists, unequal sides, or stable roommates.

Table 1 identifies the main formal components. The proof includes the universal reduction, rather than treating it as an assumption attached to a finite census. In particular, the initial state corresponds to any initial matching after normalization, and the safety property covers all finite legal paths, including the empty one.

Mathematical component	Lean source or endpoint within `StableSix`
Preference model and lattice	`Profile.lean`
Cover cycles and clamp injection	`Reduction.lean`, `Profile.exists_schedule`
Exact frontier recurrence	`Frontier.lean`
Permanent bound and support identity	`Permanent.lean`, `SupportBound.lean`
Safety and relabeling	`Certificate.lean`, `Symmetry.lean`
Executable bound and state correspondence	`RawSupportEnumeration.lean`, `RawBridge.lean`
Concrete checker soundness	`ReferenceFirstSoundness.lean`
Complete cycle coverage and certificate	`ProductionChunks/Moves.lean`, `Check/`, `Safe/`, `Root.lean`
Known lower witness	`LowerBound.lean`
Full endpoint	`Statement.lean`, `Main.lean`; top-level `Verification.lean`

Table 1: Correspondence between the paper and the checked development.

7.2 Concrete computation and the trust boundary

There are 135,828 certificate states; these are compressed matrix-and-weight states, not preference profiles or independent mathematical conjectures. The generated files separate local checks from their safety composition, allowing independent checks to run concurrently while their dependencies are composed in order. The complete local source graph contains 2,181 modules. All were accepted, including the final module `Verification`, which prints the expanded proposition, preference and stability definitions, and the endpoint axiom dependencies.

The three public endpoints—the exact-maximum theorem, universal upper bound, and existential attainment—have the transitive axiom list

```
[propext, Classical.choice, Quot.sound]
```

No `sorryAx`, new mathematical axiom, `native_decide`, or external-certificate oracle occurs in these dependencies. Concrete local checks use `decide +kernel`; externally generated data acquire mathematical force only through the kernel-checked Boolean results and the proved soundness theorems. Natural-number arithmetic avoids machine integer overflow in the formal checks. The support enumeration has a proved weighted coverage inequality, so possible duplicate entries could only increase its nonnegative bound; equal supports are not silently deduplicated.

The successful verification uses Lean 4.27.0 and mathlib commit

`a3a10db0e9d66acbebf76c5e6a135066525ac900.`

It reuses 769 audited modules checked on macOS arm64 and checks the remaining 1,412 modules on Linux x86_64. The migrated proof objects and recorded external proof artifacts were checked for byte identity. Thus the recorded run is a complete reproduction with an audited migrated prefix, not a fresh build of every module on Linux. The final module finished on 14 October 2026 at 20:50 UTC.

The post-run audit matched the source inventory and dependency pins, every accepted compilation receipt and compiler log, the final theorem, and the actual compiled proof objects. It also checked the recorded source/object import resolution and coupled those checks to the final 2,181-module checkpoint. These are execution-integrity checks; their hashes are not mathematical axioms. The trust boundary includes Lean's kernel and the pinned imported dependency caches.

7.3 Artifact contents

The accompanying archive `stable-six-artifact.tar.gz` contains the complete Lean source, the certificate, the lower witness, the pinned toolchain and dependency manifest, and reproduction instructions. The verification evidence records the actual commands, accepted source hashes, compiler output, migration provenance, resource policies, and final audits. The certificate SHA-256 is

`4f12664594d20f916e8e0534428dab83a58e6`
`bdd1c06f08767173090420fa5a7.`

For the recorded run, the checked source-inventory SHA-256 is

`57bb8bf3d6147a175a88d51ecce218dc1b`
`1812be85a00b20a7d0a8195e1ad0e1.`

The line breaks in these displayed digests are typographical only.

The archive preserves the original verification snapshot, including the manuscript and README prepared on 15 October 2026. The present revision supersedes their contribution statements by correcting the prior-work attribution. The Lean sources and verification evidence are unchanged.

A fresh reproduction should use a separate working directory, preserve the pinned versions, and follow the supplied dependency order and resource instructions. The final accepted command used a 32 GiB Lean memory limit and a 128 MiB stack. Several earlier checks required larger limits or longer timeouts than the initial settings; completed proof objects were retained and the mathematical source was unchanged. The recorded result is established by the completed run and final audits, not by a promise that a default-resource build will finish within a particular time.

A The 48 matching witnesses

The tuple $p(0)p(1)\cdots p(5)$ denotes the women assigned, in order, to men $0, 1, \ldots, 5$. All entries refer to the rank tables in (15). The list is the one used in `StableSix.LowerBound.matchingTable`.

Index	Matching	Index	Matching	Index	Matching
1	013425	17	203541	33	352041
2	013452	18	204351	34	352104
3	013542	19	230451	35	420513
4	014325	20	230514	36	425013
5	014352	21	230541	37	425103
6	103425	22	235014	38	425130
7	103452	23	235041	39	451203
8	103542	24	235104	40	451230
9	104325	25	320451	41	452013
10	104352	26	320514	42	452103
11	130425	27	320541	43	452130
12	130452	28	325014	44	541203
13	130542	29	325041	45	541230
14	135042	30	325104	46	542013
15	203451	31	351204	47	542103
16	203514	32	352014	48	542130

Table 2: Forty-eight distinct stable matchings of the known dihedral profile.

References

[1] D. Gale and L. S. Shapley. College admissions and the stability of marriage. *The American Mathematical Monthly* 69(1) (1962), 9–15. doi:10.1080/00029890.1962.11989827.

[2] A. T. Benjamin, C. Converse, and H. A. Krieger. How do I marry thee? Let me count the ways. *Discrete Applied Mathematics* 59(3) (1995), 285–292. doi:10.1016/0166-218X(95)80006-P.

[3] M. Jo. Small rotation blocks and the order-six stable marriage problem. Zenodo preprint, first deposited 20 September 2026, doi:10.5281/zenodo.22860585. Version v09, 23 September 2026, doi:10.5281/zenodo.22909380. Theorem and section references are to v09.

[4] E. G. Thurber. Concerning the maximum number of stable matchings in the stable marriage problem. *Discrete Mathematics* 248 (2002), 195–219. doi:10.1016/S0012-365X(01)00194-7.

[5] A. R. Karlin, S. Oveis Gharan, and R. Weber. A simply exponential upper bound on the maximum number of stable matchings. In *Proceedings of STOC 2018*, 920–925. arXiv:1711.01032.

[6] C. Palmer and D. Pálvölgyi. At most 3.55^n stable matchings. arXiv:2011.00915v2, 2021.

[7] L. Cai and C. Thomas. Representing all stable matchings by walking a maximal chain. arXiv:1910.04401, 2019.

[8] M. Borodin, A. Duncan, B. Litchev, J. Liu, V. Moroz, M. Qian, R. Raghavan, G. Rastogi, M. Voigt, and T. Khovanova. Sequences of the stable matching problem. *Journal of Integer Sequences* 27 (2024), Article 24.2.2. https://cs.uwaterloo.ca/journals/JIS/VOL27/Khovanova/khova32.html.

[9] D. Eilers. Sequence A357269: maximum number of stable matchings in the stable marriage problem. *The On-Line Encyclopedia of Integer Sequences*. https://oeis.org/A357269. Accessed 15 October 2026.

[10] D. Eilers. Sequence A357271: lower bounds for the maximum number of stable matchings in the stable marriage problem based on composing smaller instances. *The On-Line Encyclopedia of Integer Sequences*. https://oeis.org/A357271. Accessed 15 October 2026.

[11] D. Eilers. Sequence A351413: maximum number of stable matchings in the Latin marriage problem. *The On-Line Encyclopedia of Integer Sequences*. Includes the dihedral construction attributed to C. Converse's 1992 thesis. https://oeis.org/A351413. Accessed 15 October 2026.