# Hall's Marriage Theorem 

Dongchen Jiang and Tobias Nipkow

September 13, 2023


#### Abstract

A proof of Hall's Marriage Theorem due to Halmos and Vaughan [1].


```
theory Marriage
imports Main
begin
theorem marriage-necessary:
    fixes }A::= 'a=> 'b set and I :: 'a se
    assumes finite I and \forall i\inI. finite (A i)
    and \existsR.(\foralli\inI.R R i\inA i)^inj-on R I (is \existsR. ?R R A & ?inj R A)
    shows }\forallJ\subseteqI.card J\leqcard (U(A'J)
proof clarify
    fix }
    assume J\subseteqI
    show card J \leq card (U(A`J))
    proof-
        from assms(3) obtain R where ?R R A and ?inj R A by auto
        have inj-on R J by(rule subset-inj-on[OF \?inj R A \ <J\subseteqI`])
        moreover have (R'J)\subseteq(U(A'J)) using <J\subseteqI`<?R R A` by auto
        moreover have finite ( U(A'J)) using \J\subseteqI` assms
            by (metis finite-UN-I finite-subset subsetD)
        ultimately show ?thesis by (rule card-inj-on-le)
    qed
qed
```

The proof by Halmos and Vaughan:

```
theorem marriage- HV :
    fixes \(A:: ' a \Rightarrow\) ' \(b\) set and \(I::\) 'a set
    assumes finite \(I\) and \(\forall i \in I\). finite ( \(A\) i)
    and \(\forall J \subseteq I\). card \(J \leq \operatorname{card}(\bigcup(A\) ' \(J))\) (is ? \({ }^{\text {M } A I)}\)
    shows \(\exists R\). \((\forall i \in I\). \(R i \in A i) \wedge i n j\)-on \(R I\)
        (is? ? \(\operatorname{SDR} A I\) is \(\exists R\).? R RAI \& ? inj RAI)
proof-
    \{ fix \(I\)
    have finite \(I \Longrightarrow \forall i \in I\). finite \((A i) \Longrightarrow\) ?M A \(I \Longrightarrow\) ?SDR A \(I\)
```

```
proof(induct arbitrary: A rule: finite-psubset-induct)
    case (psubset I)
    show ?case
    proof (cases)
        assume I={} then show ?thesis by simp
    next
        assume I\not={}
        have }\foralli\inI.A i\not={
        proof (rule ccontr)
            assume \neg (\foralli\inI.A i\not={})
            then obtain i where i\inI A i={} by blast
            hence {i}\subseteqI by auto
            from mp[OF spec[OF psubset.prems(2)] this]〈A i={}\rangle
            show False by simp
    qed
    show ?thesis
    proof cases
        assume case1: }\forallK\subsetI.K\not={}\longrightarrow\operatorname{card}(\bigcup(A`K))\geq\operatorname{card}K+
        show ?thesis
        proof-
            from <I\not={}\rangle obtain n where n\inI by auto
            with «\foralli\inI. A i\not={}> have A n}\not={}\mathrm{ by auto
            then obtain }x\mathrm{ where }x\inAn\mathrm{ by auto
            let ? A' = \lambdai.A i-{x} let ? ' ' ' = I-{n}
            from \langlen\inI\rangle have ? I' \subsetI
                by (metis DiffD2 Diff-subset insertI1 psubset-eq)
            have fin': \foralli\in? ?''. finite (?A' i) using psubset.prems(1) by auto
            have ?M ?A' ? I'
            proof clarify
                fix }
                    assume J\subseteq? ? ''
                    hence }J\subsetI\mathrm{ by (metis }{I-{n}\subsetI> subset-psubset-trans
                    show card J\leqcard (\bigcupi\inJ.A i-{x})
                    proof cases
                assume }J={}\mathrm{ thus ?thesis by auto
                next
                assume }J\not={
                hence card J + 1\leq card (U(A`J)) using case1 \J\subsetI` by blast
                moreover
                have card}(\bigcup(A`J))-1\leq\operatorname{card}(\bigcupi\inJ.A i-{x})(is ?l \leq ?r)
                proof-
                    have finite J using <J \subsetI> psubset(1)
                        by (metis psubset-imp-subset finite-subset)
                    hence 1: finite(U(A'J))
                    using <\forall i\inI. finite(A i)\rangle\langleJ\subsetI\rangle by force
                    have ?l = card(\bigcup(A'J)) - card{x} by simp
                    also have ...\leq\operatorname{card}(\bigcup(\mp@subsup{A}{}{\prime}J)-{x}) using 1
                    by (metis diff-card-le-card-Diff finite.intros)
                    also have U(A'J) - {x} =(\bigcupi\inJ. A i-{x}) by blast
```

```
            finally show ?thesis.
        qed
        ultimately show ?thesis by arith
        qed
    qed
    from psubset(2)[OF〈?I'\subsetI\ranglefin'`?M ? 'A'?I'\rangle]
    obtain }\mp@subsup{R}{}{\prime}\mathrm{ where ?R R' ? 'A' ? ' ' ?inj }\mp@subsup{R}{}{\prime}?\mp@subsup{A}{}{\prime}?\mp@subsup{A}{}{\prime}\mathrm{ by auto
    let ? Rx = R'(n:=x)
    have ?R ?Rx A I using <x\inA n><?R R' ?A' ?I'> by force
    have }\foralli\in?\mp@subsup{I}{}{\prime}.\mathrm{ . ?Rx }i\not=x\mathrm{ using <?R R' ? 'A' ? I'> by auto
    hence ?inj ?Rx A I using <?inj R'? 'A' ? ''>
        by(auto simp: inj-on-def)
    with <?R ?Rx A I` show ?thesis by auto
    qed
next
    assume }\neg(\forallK\subsetI.K\not={}\longrightarrow\operatorname{card}(\bigcup(A'K))\geq\operatorname{card}K+1
    then obtain }K\mathrm{ where
    K\subsetI K\not={} and c1: \neg(card (U(A'K)) \geq card K+1) by auto
with psubset.prems(2) have card }(\cup(A'K))\geq\mathrm{ card K by auto
with c1 have case2: card }(\bigcup(A`K))= card K by aut
from \langleK\subsetI\rangle\langlefinite I\rangle have finite K by (auto intro:finite-subset)
from psubset.prems <K\subsetI\rangle
have }\foralli\inK. finite (A i) \forallJ\subseteqK. card J\leqcard (\bigcup(A`J)) by aut
from psubset(2)[OF <K\subsetI\rangle this]
obtain R1 where ?R R1 A K ?inj R1 A K by auto
let ?AK = \lambdai. A i-\bigcup(A'}K) let ?IK = I - K
from \langleK\not={}\rangle\langleK\subsetI\rangle have ?IK\subsetI by auto
have }\foralli\in?IK. finite (?AK i) using psubset.prems(1) by aut
have ?M ?AK ?IK
proof clarify
    fix }J\mathrm{ assume }J\subseteq?!I
    with〈finite I〉 have finite J by(auto intro: finite-subset)
    show card J \leq card (U (?AK'J))
    proof -
        from «J\subseteq?IK> have }J\capK={} by aut
        have card J = card(J\cupK) - card K
        using <finite J〉<finite K〉〈J\capK={}〉
        by (auto simp: card-Un-disjoint)
        also have }\operatorname{card}(J\cupK)\leq\operatorname{card}(\cup(A`(J\cupK))
        proof -
            from \langleJ\subseteq?IK\rangle\langleK\subsetI\rangle have }J\cupK\subseteqI by aut
            with psubset.prems(2) show ?thesis by blast
        qed
        also have ... - card K=\operatorname{card}(\bigcup(?AK'J)\cup\bigcup(A'K)) - card K
        proof-
            have U(A'(J\cupK))=\bigcup(?AK'}J)\cup\bigcup(A`K
            using <J\subseteq?IK> by auto
        thus ?thesis by simp
        qed
```

```
            also have ... = card (U (?AK'J)) + card(\bigcup(A`K)) - card K
                    proof-
                    have finite (U (?AK`J)) using <finite J><J\subseteq?IK> psubset(3)
                        by(blast intro: finite-UN-I finite-Diff)
                    moreover have finite (U(A`K))
                    using <finite K\rangle\langle\foralli\inK. finite (A i)\rangle by auto
                    moreover have }\bigcup(?AK'J)\cap\bigcup(A'K)={} by aut
                    ultimately show ?thesis
                        by (simp add: card-Un-disjoint del:Un-Diff-cancel2)
                    qed
                    also have ... = card (U (?AK'J)) using case2 by simp
                    finally show ?thesis by simp
                    qed
            qed
            from psubset(2)[OF〈?IK\subsetI\rangle\langle\foralli\in?IK. finite (?AK i)\rangle\langle\forallJ\subseteq?IK. card
J\leqcard (\bigcupi\inJ. A i - \bigcup (A'K))>]
            obtain R2 where ?R R2 ?AK ?IK ?inj R2 ?AK ?IK by auto
            let ?R12 = i i. if i\inK then R1 i else R2 i
            have }\foralli\inI\mathrm{ . ?R12 }i\inA i using <?R R1 A K><?R R2 ?AK ?IK> by aut
            moreover have }\foralli\inI.\forallj\inI.i\not=j\longrightarrow?R12 i\not=?R12
            proof clarify
                    fix i j assume i\inI j\inI i\not=j?R12 i=?R12 j
                    show False
                    proof -
                    { assume i\inK ^ j\inK\veei\not\inK^j\not\inK
                    with 〈?inj R1 A K〉〈?inj R2 ?AK ?IK\rangle\langle?R12 i=?R12 j\rangle\langlei\not=j\rangle\langlei\inI\rangle
<j\inI`
                    have ?thesis by (fastforce simp: inj-on-def)
                    } moreover
                    { assume i\inK ^j\not\inK\veei\not\inK\wedgej\inK
                                    with 〈?R R1 A K〉<?R R2 ?AK ?IK><?R12 i=?R12 j>\langlej\inI\rangle\langlei\inI>
                                    have ?thesis by auto (metis Diff-iff)
                    } ultimately show ?thesis by blast
                    qed
            qed
            ultimately show ?thesis unfolding inj-on-def by fast
            qed
        qed
    qed
    }
    with assms <?M A I` show ?thesis by auto
qed
```

The proof by Rado：
theorem marriage－Rado：
fixes $A:: ' a \Rightarrow$＇$b$ set and $I::$＇a set
assumes finite $I$ and $\forall i \in I$ ．finite $(A i)$
and $\forall J \subseteq I$ ．card $J \leq$ card $\left(\bigcup\left(A^{\prime} J\right)\right)$（is ？$M A$ ）
shows $\exists R .(\forall i \in I . R i \in A i) \wedge i n j-o n R I$
(is? $S D R A$ is $\exists R$. ? $R$ R $A \& ? \operatorname{inj} R A$ )
proof-
\{ have $\forall i \in I$. finite $(A i) \Longrightarrow$ ? $M A \Longrightarrow$ ? $S D R A$
proof $\left(\right.$ induct $n==\sum i \in I . \operatorname{card}(A i)-1$ arbitrary: $\left.A\right)$
case 0
have $\forall i \in I . \exists a . A(i)=\{a\}$
proof (rule ccontr)
assume $\neg(\forall i \in I . \exists a . A i=\{a\})$
then obtain $i$ where $i$ : $i: I \forall a$. $A i \neq\{a\}$ by blast
hence $\{i\} \subseteq I$ by auto
from $0(1-2) m p[O F \operatorname{spec}[O F \quad 0 . \operatorname{prems}(2)]\langle\{i\} \subseteq I\rangle]\langle$ finite $I\rangle i$
show False by (auto simp: card-le-Suc-iff)
qed
then obtain $R$ where $R: \forall i \in I . A i=\{R i\}$ by metis
then have $\forall i \in I . R i \in A i$ by blast
moreover have inj-on $R I$
proof (auto simp: inj-on-def)
fix $x y$ assume $x \in I y \in I R x=R y$
with $R \operatorname{spec}[O F \quad 0 . \operatorname{prems}(2)$, of $\{x, y\}]$ show $x=y$
by (simp add:le-Suc-eq card-insert-if split: if-splits)
qed
ultimately show ?case by blast

## next

case (Suc n)
from Suc.hyps(2)[symmetric, THEN sum-SucD]
obtain $i$ where $i: i: I 2 \leq \operatorname{card}\binom{A}{i}$ by auto
then obtain $x 1$ x2 where $x 1: A$ i $x 2$ : $A$ i $x 1 \neq x 2$
using Suc(3) by (fastforce simp: card-le-Suc-iff eval-nat-numeral)
let ?Ai $x=A i-\{x\}$ let ?A $x=A(i:=$ ?Ai $x)$
let ? $U J=\bigcup(A \cdot J)$ let ? $U i J x=$ ? $U J \cup$ ? Ai $x$
have $n 1: n=\left(\sum j \in I . \operatorname{card}(? A x 1 j)-1\right)$
using Suc.hyps(2) Suc.prems(1) $i\langle$ finite $I\rangle\langle x 1: A$ i〉
by (auto simp: sum.remove card-Diff-singleton)
have n2: $n=\left(\sum j \in I\right.$. card $(? A$ x2 $\left.j)-1\right)$
using Suc.hyps(2) Suc.prems(1) $i\langle$ finite $I\rangle\langle x 2: A$ i〉
by (auto simp: sum.remove card-Diff-singleton)
have finx1: $\forall j \in I$. finite (?A x1 j) by (simp add: Suc(3))
have finx2: $\forall j \in I$. finite (?A x2 $j$ ) by (simp add: Suc(3))
\{ fix $x$ assume $\neg$ ? $M(A(i:=$ ? $A i x))$
with Suc.prems(2) obtain $J$
where $J: J \subseteq I \operatorname{card} J>\operatorname{card}\left(\bigcup\left(\left(A(i:=\text { ? } A i x)^{\prime} J\right)\right)\right)$
by (auto simp add:not-less-eq-eq Suc-le-eq)
note $f J i=$ finite-Diff $[O F$ finite-subset $[O F\langle J \subseteq I\rangle\langle$ finite $I\rangle]$, of $\{i\}]$
have $f U$ : finite $(? U(J-\{i\}))$ using $\langle J \subseteq I\rangle$
by (metis Diff-iff Suc(3) finite-UN[OF fJi] subsetD)
have $i \in J$ using $J$ Suc.prems(2)
by (simp-all add: UNION-fun-upd not-le[symmetric] del: fun-upd-apply split: if-splits)
hence $\operatorname{card}(J-\{i\}) \geq \operatorname{card}(? U i(J-\{i\}) x)$

```
            using fJi J by(simp add: UNION-fun-upd del: fun-upd-apply)
            hence }\existsJ\subseteqI.i\not\inJ\wedge\operatorname{card}(J)\geq\operatorname{card}(?UiJx)\wedge finite(?U J
            by (metis DiffD2 J(1) fU <i\inJ` insertI1 subset-insertI2 subset-insert-iff)
    } note lem = this
    have ?M (?A x1) \vee ?M (?A x2) - Rado's Lemma
    proof(rule ccontr)
            assume }\neg(?M(?A x1)\vee ?M (?A x2)
            with lem obtain J1 J2 where
                J1: J1\subseteqI i\not\existsJ1 card J1 \geq card(?Ui J1 x1) finite(?U J1) and
            J2: J2\subseteqI i\not\inJ2 card J2 \geq card(?Ui J2 x2) finite(?U J2)
            by metis
            note fin1 = finite-subset[OF \J1\subseteqI` assms(1)]
            note fin2 = finite-subset[OF \J2\subseteqI` assms(1)]
            have finUi1: finite(?Ui J1 x1) using Suc(3) by(blast intro: J1(4) i(1))
            have finUi2: finite(?Ui J2 x2) using Suc(3) by(blast intro: J2(4) i(1))
            have card J1 + card J2 + 1 = card(J1\cupJ2) + 1 + card(J1\cap J2)
                by simp (metis card-Un-Int fin1 fin2)
            also have card(J1\cupJ2) + 1 = card(insert i (J1\cup J2))
            using <i\not\existsJ1\rangle<i\not\inJ2` fin1 fin2 by simp
            also have ... \leqcard (U (A'insert i(J1 \cupJ2)))(is - \leqcard ?M)
                by (metis J1(1) J2(1) Suc(4) Un-least i(1) insert-subset)
            also have ?M = ?Ui J1 x1 \cup?Ui J2 x2 using <x1\not=x2\rangle by auto
            also have card(J1\capJ2)\leq\operatorname{card}(\cup)(A'(J1\capJ2)))
            by (metis J2(1) Suc(4) le-infI2)
            also have ... \leqcard(?U J1 \cap?U J2) by(blast intro: card-mono J1(4))
            also have ... \leqcard(?Ui J1 x1 \cap ?Ui J2 x2)
                using Suc(3) <i\inI` by(blast intro: card-mono J1(4))
            finally show False using J1(3) J2(3)
            by(auto simp add: card-Un-Int[symmetric, OF finUi1 finUi2])
            qed
            thus ?case using Suc.hyps(1)[OF n1 finx1] Suc.hyps(1)[OF n2 finx2]
                by (metis DiffD1 fun-upd-def)
    qed
    } with assms «?M A` show ?thesis by auto
qed
end
```


## References

[1] P. R. Halmos and H. E. Vaughan. The marriage problem. American Journal of Mathematics, 72:214-215, 1950.

