Short proof of Menger's Theorem in Coq (Proof Pearl)

Christian Doczkal
CNRS / PLUME, LIP, ENS Lyon

Abstract

Menger's theorem is one of the cornerstones of graph theory, and Hall's Marriage Theorem, a straightforward consequence of Menger's Theorem, is one of the most applied graph-theoretic results. Following Göring's "Short proof of Menger's Theorem" we give formal proofs of Menger's theorem and of some of its consequences, including Hall's Marriage Theorem and Kőnig's Theorem, in the proof assistant Coq. Our proofs make use of the mathematical components library and a library for reasoning about paths in finite graphs developed previously.

2012 ACM Subject Classification Mathematics of computing → Paths and connectivity problems; Mathematics of computing → Matchings and factors; Theory of computation → Type theory

Keywords and phrases Graph theory, Menger's Theorem, Hall's Marriage Theorem, Kőnig's Theorem, Coq, Ssreflect

Digital Object Identifier 10.4230/LIPIcs...

Supplement Material `https://perso.ens-lyon.fr/christian.doczkal/menger`

1 Introduction

Diestel [6, p. 50] calls Menger's Theorem [19] one of the cornerstones of graph theory and remarks that Hall's Marriage Theorem [14], a straightforward consequence of Menger's Theorem, is one of the most applied graph-theoretic results [6, p. 42]. Informally, Menger's Theorem states that if one needs to remove at least n vertices to disconnect two sets of vertices A and B of some graph, then there exist n pairwise disjoint paths from A to B.

One particularly useful corollary of Menger's Theorem allows the construction of n independent (i.e., internally vertex disjoint) xy-paths, provided one needs to remove at least n vertices (differenct from x and y) in order to disconnect x and y. For $n = 3$, such a collection of independent paths is sometimes referred to as a "theta" [1] (in reference to the shape of the letter θ) and thetas occur pervasively in graph theory. In fact, our main motivation for formalizing Menger's Theorem was the need to construct such a theta in a larger proof (cf. Section 8).

There are various proofs of Menger's theorem in the literature [19, 17, 2, 6, 13] – Diestel [6] alone provides three different proofs. We choose to follow Göring's "Short proof of Menger's Theorem" [13], because it is the simplest and most elegant proof we could find. Since the original proof is really short – Göring's paper is a short note of little more than a page – this allows us analyze each step of the proof and explain what is required in order to formalize it in Coq.

The formal development builds on a library for reasoning about paths in finite graphs developed previously [7]. More precisely, the version of the library underlying [7] only supports simple (i.e., undirected and self-loop free) graphs. Menger's Theorem is more naturally stated and proved in the setting of directed graphs, the version for simple graphs being an instance of the version for directed graphs. Adapting the aforementioned library to also support reasoning about paths in directed graphs was straightforward, and we will not detail it here.

The present work should be seen as a first step towards extending the library in [7] in the direction of a general-purpose graph library. Currently, there are very few formalizations of graph theory results in Coq. Gonthier's formal proof of the Four-Color Theorem [12] is certainly the most advanced, but it restricts (by design) to planar graphs so that it cannot be used as a starting point for general graph theory. Similarly, Durfourd and Bertot's study of Delaunay triangulation [10] employs a notion of graphs based on hypermaps embedded in a plane. Other developments (e.g. [11]) only formalize the most basic notions and/or have never reached the point of general usefulness.

There are more formalizations in other interactive theorem provers. Chou developed some undirected graph theory in HOL [3]. Euler's theorem was formalized in Mizar [20]. Planar graphs were formalized in Isabelle/HOL for the Flyspeck project [21]. Noschinski recently developed a library for both simple and multi-graphs in Isabelle/HOL [22]. Perhaps closest to our work is the work of Lammich and Sefidgar [16] who formalize the Edmonds-Karp algorithm and the max-flow min-cut theorem, a generalization of Menger's Theorem to flow networks, in Isabelle/HOL.

The paper is organized as follows. In Section 2, we define some basic notions and notations corresponding to the part of Coq library we use in the background [7]. In Section 3 we give the formal statement of Menger's Theorem and describe what is needed to formalize the statement in Coq. In Section 4 we present Göring's proof of Menger's Theorem and explain what is needed to formalize it in Coq. In Sections 5 to 7 we derive a number of consequences of Menger's Theorem, including Hall's Marriage Theorem and Kőnig's Theorem (cf. [6])

2 Preliminaries

A *finite type* [18] is a type for which there is a (finite) list enumerating its elements. For instance, the type of booleans $\mathbb{B}$ is a finite type. We write I_n for the finite type of natural numbers less than n. Arguments of type I_n are to be thought of as indices and we will usually write them as subscripts.

A *digraph* is a (dependent) tuple $\langle V, E\rangle$ where V is a finite type of vertices and $E : V \to V \to \mathbb{B}$ is a boolean relation. Let $G = \langle V, E\rangle$ be a digraph. We write $x : G$ to denote that x is a vertex of G, i.e., if a graph appears as a type, it is to be understood as its type of vertices. For vertices $x, y : G$, we write $x \rhd y$ for $E\,x\,y = \mathsf{true}$. An xy-path is a nonempty sequence of vertices beginning with x and ending with y, such that $u \rhd v$ for every pair of adjacent vertices u and v in the sequence (if any). We write $x \rightsquigarrow y$ to denote the type of xy-paths. If $\pi_1 : x \rightsquigarrow y$ and $\pi_2 : y \rightsquigarrow z$, we write $\pi_1 +\!\!+ \pi_2$ for the concatenation of π_1 and π_2 (which has type $x \rightsquigarrow z$). A path π is called *irredundant*, written $\mathsf{irred}\,\pi$, if the underlying sequence of vertices is duplicate free. If a path occurs as a set, this is to be understood as the set of vertices on the path.

3 The Statement

In the language of modern graph theory, Menger's Theorem [19, 13] states that for every two sets of vertices A and B of some digraph G, the minimum size of an AB-separator is the maximum size of an AB-connector. We first give the definitions used in [13] and then explain how we formalize these notions in Coq.

▶ **Definition 1.** *Let G be some digraph and let A and B be sets of vertices of G.*

- *An AB-*separator *is a set S, such that the graph obtained by deleting the vertices in S contains no path from A to B.*

- *An* AB-connector *is a subgraph of G such that each of its components is a path*[1] *from A to B having no inner vertex in $A \cup B$.*
- *The* size *of an AB-separator S is the number of vertices in S and the size of an AB-connector X is the number of components (or paths) in X.*

Note that if S is an AB-separator and X is an AB-connector, then S must contain at least one vertex from every path in X. Consequently, one of the directions of Menger's Theorem is trivial. The nontrivial direction of Menger's Theorem is:[2]

▶ **Theorem 2** (Menger [19]). *Let G be a digraph and let A, B be sets of vertices of G such that $n \leq |S|$ for every AB-separator S. Then there exists an AB-connector of size n.*

In Coq, we represent (finite) digraphs as dependent records consisting of a finite type and a decidable (i.e., boolean) relation over this type:

$$\textbf{Record}\ \mathsf{digraph} \coloneqq \{\ \mathsf{vertex} : \mathsf{finType};\ \mathsf{edge\_rel} : \mathsf{vertex} \to \mathsf{vertex} \to \mathbb{B}.\ \}$$

Thus, constructing a subgraph requires constructing a new type of vertices and a new edge relation on this type, making this a relatively "heavy" operation. Consequently, we avoid the use of subgraphs in the formal definition of separators and connectors.

In the following, let G be a digraph and let x, y, a, b range over vertices of G and let A, B, S range over sets of vertices of G. For AB-separators we simply require that every path from A to B must contain a vertex from S.

$$AB\text{-}\mathsf{separator}\, S \coloneqq \forall a \in A.\, \forall b \in B.\, \forall \pi : a \rightsquigarrow b.\, S \cap \pi \neq \emptyset$$

In the case of AB-connectors, we also use paths to avoid the use of subgraphs. This is natural since the main use of Menger's Theorem is the construction of pairwise disjoint paths. However, the path library we use represents paths using a vertex-indexed family of path types, i.e., for every two vertices x and y, there is a separate type of xy-paths.[3] In order to form collections of paths with different starting and ending vertex, we require a non-indexed path type. This can be easily defined using existential quantification (at the type level; using Σ-types) over the end-points. We define a type of G-paths and projection functions yielding respectively the first vertex, the last vertex, and the encapsulated path:

$$\begin{aligned} G\text{-}\mathsf{path} &\coloneqq \Sigma(x,y) : G \times G.\, x \rightsquigarrow y \\ \mathsf{fst}\,\langle (x,y), \pi \rangle &\coloneqq x \\ \mathsf{lst}\,\langle (x,y), \pi \rangle &\coloneqq y \\ \mathsf{pth}\,\langle (x,y), \pi \rangle &\coloneqq \pi \end{aligned}$$

Note that the type of pth is $\forall \pi : G\text{-}\mathsf{path}.\, \mathsf{fst}\,\pi \rightsquigarrow \mathsf{lst}\,\pi$, i.e., the type of $\mathsf{pth}\,\pi$ depends on the value of π. This is mainly useful in combination with predicates that are parametric in the index-vertices (e.g., in $\mathsf{irred}(\mathsf{pth}\,\pi)$ where $\pi : G\text{-}\mathsf{path}$ and $\mathsf{irred} : \forall x\, y : G.\, x \rightsquigarrow y \to \mathsf{Prop}$). In the mathematical presentation, we will usually suppress pth, which is merely a type cast, treating indexed and non-indexed paths as essentially the same.

[1] This is relative to the notion of path in [6], where paths are defined as line-shaped subgraphs rather than as sequences of vertices

[2] Note that numbered theorems, lemmas, etc. in this paper are hyperlinked to the corresponding entities in the Coq development.

[3] See [7] for a discussion why this is strongly desirable.

With this in place, AB-connectors of size n can be defined as predicates on functions $p : I_n \to G\text{-}\mathsf{path}$ as follows :

$$\begin{aligned} AB\text{-}\mathsf{connector}\, X \coloneqq {} & \forall i : I_n.\, \mathsf{irred}\, X_i && (1)\\ & \wedge\ \forall i : I_n.\, X_i \cap A = \{\mathsf{fst}\, X_i\} && (2)\\ & \wedge\ \forall i : I_n.\, X_i \cap B = \{\mathsf{lst}\, X_i\} && (3)\\ & \wedge\ \forall i\, j : I_n.\, i \neq j \to X_i \cap X_j = \emptyset && (4) \end{aligned}$$

Thus, Menger's Theorem can be stated formally (and succinctly) as follows:

$$\begin{aligned} & \forall (G : \mathsf{digraph})(AB : \mathsf{set}\ G)(n : \mathbb{N}).\\ & \quad (\forall S.\, AB\text{-}\mathsf{separator}\, S \to n \leq |S|) \to \exists X : I_n \to G\text{-}\mathsf{path}.\, AB\text{-}\mathsf{connector}\, X \end{aligned}$$

Note that some authors, notably Diestel [6] and Göring [13] (citing Diestel) consider only irredundant paths. This would be a bad choice for a formal development, because this would require proving irredundancy whenever one wants to compose paths, even in contexts where the proof does not rely on the path being irredundant. In the definition of an AB-connector, we do require irredundancy of the involved paths as this allows us to express the condition that the internal vertices of every path may occur neither in A nor in B as a simple equality between sets (Equations (2) and (3)) rather than by splitting off vertices. We remark that Equation (2) actually ensures that $\mathsf{fst}\, X_i$ is the *only* vertex in $A \cap X_i$, thus disallowing two-vertex paths xy linking two distinct vertices $x, y \in A \cap B$ (something that is allowed according to Definition 1). Thus, our formal definition is slightly more strict. Given that Menger's Theorem shows the existence of a connector, this constitutes a (minor) strengthening of the theorem.

4 The Proof

We now turn to the proof of Menger's Theorem. Göring's proof is given in Figure 1. As is typical for graph theory proofs, the proof mostly sketches the construction and elides large parts of the arguments regarding the correctness of the construction. It should not come as a surprise that, as it comes to the formalization, the verification effort outweighs the construction effort. Further, we opted for a slightly different definitions, and this influences the proof. In the following, we go through Görings proof step-by-step and outline what is required in order to formalize it.

First of all, Göring leaves implicit that the proof is carried out by induction on the number of edges in D. In our case, where edges are represented implicitly, we use the measure $m(D) \coloneqq |\{(x, y) : D \times D \mid x \rhd y\}|$.

The assumption that D' contains an AB-separator S with $|S| < s$ is justified by noting that otherwise we obtain an AB-connector in D' by induction, and this would provide the required AB-connector in D. In order to make this case distinction in the constructive logic of Coq, we need to show that $AB\text{-}\mathsf{separator}\, S$ is a decidable property (i.e., that there exists a corresponding boolean predicate). This is straightforward since the quantification over all paths can be replaced by quantification over irredundant paths of which there are only finitely many. Thus, the situation looks as depicted in Figure 2.

To show that P and Q are AB-separators, we establish the following case analysis principle for paths in D': For every irredundant path $\pi : u \rightsquigarrow v$ in D there either exists a path $\pi : u \rightsquigarrow v$ in D' using the same sequence of vertices (i.e., the xy-edge is not used) or there exist two irredundant paths $\pi_1 : u \rightsquigarrow x$ and $\pi_2 : y \rightsquigarrow v$ in D' again using the same

▶ **Theorem** (Menger). *Let D be a finite digraph, A and B sets of vertices of D, and s the minimum number of vertices forming an AB-separator. Then there is an AB-connector C with $|C \cap A| = s$.*

Proof. If D is edgeless then set $C = A \cap B$. Hence we may assume: D contains an edge e from x to y, the theorem holds for $D' = D - e$, and D' has an AB-separator S with $|S| < s$. Then $P = S \cup \{x\}$ and $Q = S \cup \{y\}$ are AB-separators of D. Thus $|P| = |Q| = |S| + 1$. An AP-separator (as well as a QB-separator) of D' is an AB-separator of D. Consequently, D' has an AP-connector X containing P and a QB-connector Y containing Q. Since $X \cap Y = S$ one can set $C = (X \cup Y) + e$. ◀

Figure 1 Göring's "Short proof of Menger's Theorem" [13]

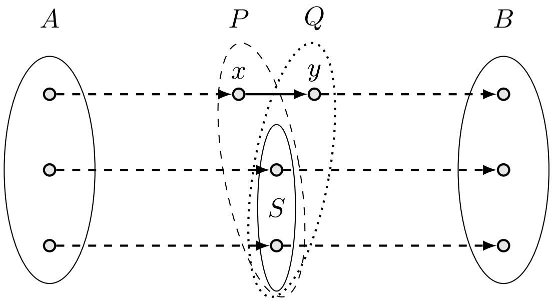

Figure 2 Objects occuring the the proof of Menger's Theorem

vertices as π. Thus, P and Q are AB-separators since every AB-path in D either has a corresponding path in D' and must therefore contain a vertex from S or it uses the edge e and therefore contains both x and y.

The argument that every AP-separator (or QB-separator) of D' is an AB-separator of D (and hence has size at least s), follows a similar pattern: Let T be an AP-separator of D' and let $\pi : a \rightsquigarrow b$ be an irredundant path in D with $a \in A$ and $b \in B$. If π uses the xy-edge, the ax-prefix of π contains a vertex in T. Otherwise, π contains some vertex $z \in \pi \cap P$ (P is an AB-separator). Splitting π at z yields an az-path in D' which again must contain a vertex in T. The connectors X and Y (both of size n) can thus be obtained by induction.

It remains to show that $(X \cup Y) + e$ is an AB-connector of the required size. We first establish that $Y + e$ is an AP-connector and then show how to compose two connectors along a separator. We prove this as two separate lemmas, each abstracting from the concrete construction.

▶ **Lemma 3.** *Let G be a digraph, Q and B sets of vertices of G, $j : I_n$ and $Y : I_n \to G$*-path *an QB-connector. If $x \notin \bigcup_i Y_i$,* $\mathsf{fst}\,(Y_j) = y$*, $x \rhd y$ and $x \notin B$, then there exists an $(\{x\} \cup Q \setminus \{y\})B$-connector of size n*

Proof. Follows by prepending x to X_j (and verifying that the result is indeed a connector). ◀

The side condition $x \notin B$ is required since Y_j already contains an element of B. To show that we indeed have $x \notin B$, let $i : I_n$ be such that $\mathsf{lst}\, X_i = x$. If $x \in B$, then $X_i \cap S \neq \emptyset$ (S is an AB-separator in D'). However, x is the only element in $X_i \cap P$ (3). So this would yield $x \in S$ contradicting $|P| = |S| + 1$.

▶ **Lemma 4.** *Let G be a digraph, A and B sets of vertices of G, and P an AB-separator with $|P| = n$. Further let $X : I_n \to G$-path an AP-connector and $Y : I_n \to G$-path a PB-connector. Then there exists an AB-connector of size n.*

Proof. Since all X_i (as well as all Y_i) are mutually disjoint and each contain a single vertex from P, there is for every $i : I_n$ a unique index $m(i) : I_n$ such that $\mathsf{lst}\,(X_i) = \mathsf{fst}\,(Y_{m(i)})$. Since P is an AB-separator, any X_i and Y_j can intersect at most at a single vertex of P (in this case $j = m(i)$). Thus, the function $Z_i \coloneqq X_i +\!\!+ Y_{m(i)}$ is a connector as required.

We sketch argument for (2), i.e., that $Z_i \cap A = \{\mathsf{fst}\,(Z_i)\}$. Assume X_i is an xy-path and $Y_{m(i)}$ is a yz-path (this is the general case by the definition of $m(i)$). The inclusion from right to left is trivial, as is showing that $X_i \cap A \subseteq \{\mathsf{fst}\,(Z_i)\}$. So assume some $u \in Y_{m(i)} \cap A$. It suffices to show $u = y$ for then $u \in X_i$. This follows since the uz-part of $Y_{m(i)}$ is an AB-path and therefore must contain a vertex $v \in P$. But y is the only vertex in $P \cap Y_{m(i)}$, so $v = y = u$ since $Y_{m(i)}$ is irredundant. ◀

Note that in the proof sketch above, the use of "$+\!\!+$" in $X_i +\!\!+ Y_{m(i)}$ is a slight abuse of notation since "$+\!\!+$" is only defined for vertex-indexed paths with matching vertices. In the formalization, we employ a separate concatenation function on G-path that discards the second argument in case the end-points don't match. In the proof of Lemma 4, we then establish once that in the definition of Z the end-point always match. This ensures that the reasoning about dependent types does not clutter the verification that the function Z is indeed a connector. We remark that in the setting of Göring, where connectors are defined as subgraphs, the matching of indices (i.e., pairing X_i with $Y_{m(i)}$) would not be necessary. Nevertheless, one still has to verify that the union of two connectors intersecting in a separator is again a connector, and this bulk of the work of required to prove Lemma 4.

This finishes the proof of Menger's Theorem. We remark that by proving Menger's theorem for digraphs, which are really just packaged relations, it applies without further argument to graphs with additional structure such as finite simple graphs (i.e., the restriction to symmetric and irreflexive edge relations) and finite directed multigraphs.

5 Independent Paths

One often-used corollary of Menger's Theorem shows the existence of multiple independent (i.e., internally vertex-disjoint) paths between certain pairs of vertices.

▶ **Definition 5.** *Let x, y be vertices of some digraph G. A set of vertices S* separates *x and y if $\{x, y\} \cap S = \emptyset$ and every xy-path contains a vertex from S.*

Note that the condition $\{x, y\} \cap S$ is required to make the notion of a minimal separating set nontrivial. That is, while $\{x\}$ is an $\{x\}\{y\}$-separator, it does not separate x and y.

▶ **Corollary 6.** *Let D be a digraph, and let $x, y : D$ such that $x \neq y$ and $x \not\triangleright y$. If $n \leq |S|$ for every set S separating x and y, then there exist n irredundant and pairwise independent xy-paths.*

Proof. Let $D' \coloneqq D \setminus \{x, y\}$ be the subgraph of D induced by the complement of $\{x, y\}$. Let $A \coloneqq \{z : D' \mid x \triangleright z\}$ and $B \coloneqq \{z : D' \mid z \triangleright y\}$. Then every AB-separator of D' also separates x and y in D and therefore has size at least n. By Menger's Theorem, we obtain an AB-connector X of size n. Appending x at the beginning and y at the end of every path in X yields n independent xy-paths. ◀

We remark that the formalization of the proof above does make use of the "$+\!\!+$" function on G-path. Instead, we prove (interactively) that for every $i : I_n$, the type

$$\Sigma(\pi : x \rightsquigarrow y).\, \mathsf{irred}(\pi) \wedge \pi \setminus \{x, y\} = X_i$$

is inhabited and then define π_i to be the first projection of the inhabitant for i. This is sufficient, because irredundancy of π_i and the equation $\pi_i \setminus \{x, y\} = X_i$ are the only properties of π_i we need. Using proof mode to show that the aforementioned type is inhabited allows us to use tactics like `subst`, simplifying the handling of the dependent types involved.

Corollary 6 appears to not have a common name in the graph theory literature. In fact, Bondy&Murty [2, Theorem 9.9] refer to Corollary 6 as the directed vertex version of Menger's Theorem. As the name suggests, there is also an edge version which we prove next. The edge version is mainly of interest for directed multigraphs.

▶ **Definition 7.** *A* (finite) directed multigraph *is a tuple $G = \langle V, E, s, t\rangle$ where V is a finite type of vertices, E is a finite type of edges and $s, t : E \to V$ give the* source *and* target *of a given edge.*

In a addition to paths, multigraphs also come with a more fine-grained notion of walk that keeps track of the edges being used.

▶ **Definition 8.** *Let $G = \langle V, E, s, t\rangle$ be a directed multigraph. An xy-walk in G is a list of successive edges starting at x and ending at y, that is $w : \mathsf{list}\, E$ is an xy-walk if it satisfies the following recursive predicate:*

$$\mathsf{walk}\, x\, y\, [] := x = y$$

$$\mathsf{walk}\, x\, y\, (e :: w) := s(e) = x \wedge \mathsf{walk}\, (t\, e)\, y\, w$$

A set of edges F separates *two vertices x and y if every xy-walk contains an edge in F.*

▶ **Corollary 9.** *Let $G = \langle V, E, s, t\rangle$ be a directed multigraph and let $a, b : V$ be two distinct vertices such $n \leq |E|$ for every set of edges separating a and b. Then there exist n pairwise disjoint ab-walks.*

Proof. Let $L := \langle E, \rhd\rangle$ with $e_1 \rhd e_2 := t(e_1) = s(e_2)$ be the line graph of G (i.e, the graph whose vertices are the edges of G and whose transition relation reflects adjacency of edges). Further let $A = \{e : E \mid s(e) = a\}$ and $B = \{e : E \mid t(e) = b\}$. Then every AB-separator (in L) is a set of edges separating a and b in G and must therefore have size at least n. Thus, we obtain an AB-connector X of size n by Menger's Theorem. The claim then follows since every path in X corresponds to an ab-walk in G. ◀

6 Hall's Marriage Theorem

We now use Menger's Theorem to prove Hall's Marriage Theorem. More precisely, we first prove a variant of Hall's Marriage Theorem for bipartite directed graphs that follows naturally from Menger's Theorem for directed graphs. As a second step, we derive the usual formulation of Hall's Marriage Theorem for bipartite simple graphs.

▶ **Definition 10.** *Let G be a digraph. We define $\mathsf{N}(A) := \{y \in \overline{A} \mid x \rhd y\}$ (with $\overline{A}$ being the complement of A in G) to be the* neighborhood *of A. A* bipartition *of G is set A of vertices of G, such that for every edge of G exactly one of the ends is in A (i.e., $(x \in A) \oplus (y \in A)$ whenever $x \rhd y$). A* directed matching *of G is a set M of directed edges (i.e., a set of pairs of vertices (x, y) such that $x \rhd y$ for all pairs) in G such that no two edges in M share a vertex.*

We observe that an $A\overline{A}$-connector in a graph with bipartition A is essentially a matching.

▶ **Proposition 11**. *Let G be a digraph with bipartition A and let $X : I_n \to G$-path be an $A\overline{A}$-connector. Then $\{(\mathsf{fst}\, X_i, \mathsf{lst}\, X_i) \mid i : I_n\}$ is a directed matching of size n.*

▶ **Corollary 12**. *Let G be a digraph with bipartition A such that $|\mathsf{N}(S)| \geq |S|$ for all $A \subseteq S$. Then there exists a directed matching M (of G) such that $A = \{x \mid \exists y.\, (x, y) \in M\}$*

Proof. By Proposition 11, it suffices to show that every $A\overline{A}$-separator has size at least $|A|$ and obtain an $A\overline{A}$-connector of size $|A|$ using Menger's Theorem. Let S be an $A\overline{A}$-separator. Then $|A| = |A \cap S| + |A \setminus S| \leq |A \cap S| + |\mathsf{N}(A \setminus S)| \leq |S|$. The first inequality holds by assumption, the second inequality holds since the two sets are disjoint and (because S is an $A\overline{A}$-separator) also included in S. ◀

In order to state Hall's Marrage Theorem for simple bipartite graphs, we need an appropriate notion of matching. The notions of neighborhood and bipartition remain the same.

▶ **Definition 13**. *Let G be a simple graph (i.e., a digraph with a symmetric and irreflexive edge relation). Then an* (undirected) matching *of G is a set M of edges in G (i.e., a set of sets $\{x, y\}$ such that $x \rhd y$) that is pairwise disjoint.*

Note that for every directed matching M of some graph G, the set $\{\{x, y\} \mid (x, y) \in M\}$ is a matching of size $|M|$ covering the same vertices as M. Thus, the usual formulation of Hall's Marriage theorem follows immediately with Corollary 12.

▶ **Theorem 14** (Hall). *Let G be a simple graph with bipartition A such that $|\mathsf{N}(S)| \geq |S|$ for all $A \subseteq S$. Then there exists a matching M (of G) such that $A \subseteq \bigcup M$.*

One motivation for distinguishing between directed and undirected matchings is that this allows for a slightly stronger statement for Corollary 12. Moreover, one sometimes wants to count the number of matchings in a graph (i.e., compute the Hosoya index [15]), and in simple graphs the two directions of an edge are considered to be the same edge.

7 Kőnig's Theorem

Kőnig's Theorem states that the size of a minimum vertex cover and a maximum matching are the same. This is is another well-known and widely-used consequence of Menger's Theorem.

▶ **Definition 15**. *Let G be a simple graph. A set V of vertices of G is called a* vertex cover *if every edge in G has at least one end in V. A vertex cover is* minimum *if no vertex cover has fewer vertices. A matching of G is* maximum *if no matching has more edges.*

▶ **Lemma 16**. *Let G be a simple graph, let V be a vertex cover of G and let M be a matching of G. Then $|M| \leq |V|$. Moreover, if $|M| = |V|$ we also have $V \subseteq \bigcup M$.*

Proof. The edges in M are pairwise disjoint and each share a vertex with V. Thus there exists an injective function f from M to V. This yields $|M| \leq |V|$. If $|M| = |V|$, then f must also be surjective and we obtain $V \subseteq \bigcup M$. ◀

▶ **Corollary 17**. *Let G be bipartite and let V be a minimum vertex cover. Then there exists a matching of G with $|V| \leq |M|$.*

Proof. Let A be a bipartition of G. It is easy to see that every $A\overline{A}$-separator is also a vertex cover. Thus, the claim follows with Menger's Theorem and Proposition 11. ◀

▶ **Theorem 18** (Kőnig). *Let G be bipartite, let V a minimum vertex cover, and let M be a maximum matching. Then $|V| = |M|$.*

Proof. We have $|V| \geq |M|$ by Lemma 16. Since M is maximum, it suffices to obtain some matching M' with $|V| \leq |M'|$. Thus, the claim follows with Corollary 17. ◀

8 Conclusion

We have given proofs of Menger's Theorem and some of its most well-known consequences. Not counting the library for reasoning about paths developed for [7], the formal development[4] consists of about 260 lines of specification and about 530 lines of proofs. The library for reasoning about paths in digraphs adds another 600 lines. The library for simple graphs is almost twice as large, but little of it is being used here.

One motivation for this work was to see how well the infrastructure developed in [7] adapts to graph-theory results we had not initially planned on. In this context, Menger's Theorem is interesting for two reasons.

First, the theorem applies to various notions of graphs and we wanted to prove it in a way that the effort of transferring the result to the different instances is minimal. This prompted us to make explicit the notion of digraph (i.e., packaged relations) and prove the theorem in this setting. Undirected simple graphs and directed multigraphs, the two notions of graphs considered in [7], can then be defined in such a way that they coerce to digraphs and inherit both the notion of paths and various properties – including Menger's Theorem – through this coercion.

Second, the use of heterogeneous collections of paths in the definition of AB-connectors goes slightly "against the grain" of the path library in which the type of paths is actually a vertex-indexed family of types.[5] Thus, we were faced with the choice of working with the underlying sequences of vertices (i.e., removing a layer of abstraction) or abstracting from the end-points using Σ-types (i.e., adding another layer of abstraction). We choose to add a layer since this allows us to reuse the lemmas for typed paths. While the added layer of abstraction incurs some overhead in the proofs, we managed to confine the reasoning about dependent types to a few short lemmas and not have it intersperse with the more high-level arguments.

As mentioned initially, this work was originally motivated by the need to construct a theta in a larger proof. More precisely, the need for constructing a theta arose in trying to simplify the proof of the excluded-minor characterization of treewidth-two graphs [9] (i.e., that the graphs of treewidth-two are precisely those excluding K_4, the complete graph with four vertices, as a minor) obtained in [7]. There, excluded-minor characterization was obtained as a side-product of a complicated process extracting term-descriptions for K_4-free multigraphs. Originally, this was intended as a milestone towards the construction of a free graph-model for a certain class of algebras [5]. Only after formalizing a significant portion of the proof in [5], we realized that the proof can be simplified significantly – at the mathematical level – by replacing the complicated top-down extraction function by bottom-up graph rewriting [8]. The new proof no longer mentions minors at all and, in particular, does not reprove the minor exclusion property. Hence, we want to obtain a simpler more-direct proof of the minor exclusion property. This new proof is work in progress and makes use of Corollary 6.

[4] available at: `https://perso.ens-lyon.fr/christian.doczkal/menger`

[5] The development accompanying [7] includes several thousand lines of arguments about paths, and this issue never came up.

We conclude that, while the library could profit from some additional cleanup (e.g., more consistent naming conventions and additional documentation), it is already quite usable. In order to establish the library as generally useful, more diverse case studies would need to be carried out. In addition to the more direct proof of the excluded-minor characterization of treewidth-two graphs currently in progress, we also plan to verify the graph-rewriting based completeness proof for 2p-algebras [8]. Further, we would like to carry out a comparative case study with the work of Noschinski [22] who formalized the characterization of Eulerian graphs in terms of vertex degrees and a verified a checker for certificates of non-planarity based on Kuratowski graphs. This should provide insights into the trade-offs between the higher degree of proof automation in Isabelle/HOL and the more expressive type theory of Coq as it comes to reasoning about graphs. Beyond the aforementioned checker for non-planarity, the verification of (abstract) graph algorithms using the library (whose definitions are proof-centered and not intended for computation) and the refining them to efficient implementations along the lines of [4] seems a promising direction.

References

1 J. A. Bondy. The "graph theory" of the greek alphabet. In Y. Alavi, D. R. Lick, and A. T. White, editors, *Graph Theory and Applications*, pages 43–54, Berlin, Heidelberg, 1972. Springer Berlin Heidelberg.

2 J.A. Bondy and U.S.R Murty. *Graph Theory*. Springer Publishing Company, Incorporated, 1st edition, 2008.

3 Ching-Tsun Chou. A formal theory of undirected graphs in higher-order logic. In *TPHOL*, volume 859 of *LNCS*, pages 144–157. Springer, 1994. `doi:10.1007/3-540-58450-1\_40`.

4 Cyril Cohen, Maxime Dénès, and Anders Mörtberg. Refinements for free! In Georges Gonthier and Michael Norrish, editors, *Certified Programs and Proofs (CPP2013)*, volume 8307 of *LNCS*, pages 147–162. Springer, 2013. `doi:10.1007/978-3-319-03545-1\_10`.

5 Enric Cosme-Llópez and Damien Pous. K_4-free graphs as a free algebra. In *MFCS*, volume 83 of *LIPIcs*. Dagstuhl, 2017. `doi:10.4230/LIPIcs.MFCS.2017.76`.

6 R. Diestel. *Graph Theory (2nd edition)*. Graduate Texts in Mathematics. Springer, 2000.

7 Christian Doczkal, Guillaume Combette, and Damien Pous. A formal proof of the minor-exclusion property for treewidth-two graphs. In Jeremy Avigad and Assia Mahboubi, editors, *Interactive Theorem Proving (ITP 2018)*, volume 10895 of *LNCS*, pages 178–195. Springer, 2018. URL: `https://hal.archives-ouvertes.fr/hal-01703922`, `doi:10.1007/978-3-319-94821-8\_11`.

8 Christian Doczkal and Damien Pous. Treewidth-Two Graphs as a Free Algebra. In *Mathematical Foundations of Computer Science*, Liverpool, United Kingdom, August 2018. URL: `https://hal.archives-ouvertes.fr/hal-01780844`, `doi:10.4230/LIPIcs.MFCS.2018.60`.

9 R.J Duffin. Topology of series-parallel networks. *Journal of Mathematical Analysis and Applications*, 10(2):303–318, 1965. `doi:10.1016/0022-247X(65)90125-3`.

10 Jean-François Dufourd and Yves Bertot. Formal study of plane Delaunay triangulation. In *Interactive Theorem Proving (ITP 2010)*, volume 6172 of *LNCS*, pages 211–226. Springer, 2010. `doi:10.1007/978-3-642-14052-5\_16`.

11 Jean Duprat. A Coq toolkit for graph theory. `https://github.com/coq-contribs/graph-basics`, 2001.

12 Georges Gonthier. Formal proof — the four-color theorem. *Notices Amer. Math. Soc.*, 55(11):1382–1393, 2008.

13 Frank Göring. Short proof of menger's theorem. *Discrete Mathematics*, 219(1-3):295–296, 2000. URL: `https://doi.org/10.1016/S0012-365X(00)00088-1`, `doi:10.1016/S0012-365X(00)00088-1`.

14 Philip Hall. On representatives of subsets. *J. London Math. Soc.*, 10:26–30, 1935. doi:10.1112/jlms/s1-10.37.26.

15 Haruo Hosoya. Topological index. a newly proposed quantity characterizing the topological nature of structural isomers of saturated hydrocarbons. *Bulletin of the Chemical Society of Japan*, 44(9):2332–2339, 1971. doi:10.1246/bcsj.44.2332.

16 Peter Lammich and S. Reza Sefidgar. Formalizing the Edmonds-Karp algorithm. In Jasmin Christian Blanchette and Stephan Merz, editors, *Interactive Theorem Proving (ITP 2016)*, volume 9807 of *LNCS*, pages 219–234. Springer, 2016. doi:10.1007/978-3-319-43144-4_14.

17 T. Grünwald (later Gallai). Ein neuer Beweis des Mengerschen Satzes. *J. London Math. Soc.*, 13:188–192, 1938.

18 Mathematical Components - libraries of formalized mathematics. http://math-comp.github.io/math-comp/.

19 K. Menger. Zur allgemeinen kurventheorie. *Fund. Math.*, pages 96–115, 1927.

20 Y. Nakamura and P. Rudnicki. Euler circuits and paths. *Formalized Mathematics*, 6(3):417–425, 1997.

21 Tobias Nipkow, Gertrud Bauer, and Paula Schultz. Flyspeck I: tame graphs. In *IJCAR*, volume 4130 of *LNCS*, pages 21–35. Springer, 2006. doi:10.1007/11814771_4.

22 Lars Noschinski. A graph library for Isabelle. *Mathematics in Computer Science*, 9(1):23–39, 2015. doi:10.1007/s11786-014-0183-z.