UNIVERSITY OF CAMBRIDGE
Department of Computer Science and Technology

A Formalisation of Turán's Graph Theorem in Isabelle/HOL

Nils Lauermann

Clare College

June 2022

Submitted in partial fulfillment of the requirements for the
Master of Philosophy in Advanced Computer Science

Total page count: 36

Main chapters (excluding front-matter, references and appendix): 25 pages (pp 7–31)

Main chapters word count: 9289

Methodology used to generate that word count:

```
$ make wordcount
gs -q -dSAFER -sDEVICE=txtwrite -o - \
   -dFirstPage=7 -dLastPage=31 report-submission.pdf | \
egrep '[A-Za-z]{3}' | wc -w
9289
```

Declaration

I, Nils Lauermann of Clare College, being a candidate for the M.Phil in Advanced Computer Science, hereby declare that this report and the work described in it are my own work, unaided except as may be specified below, and that the report does not contain material that has already been used to any substantial extent for a comparable purpose.

Signed: Nils Lauermann

Date: 6 June 2022

Abstract

Turán's graph theorem states that any undirected, simple graph with n vertices that does not contain a p-clique, contains at most $\left(1 - \frac{1}{p-1}\right)\frac{n^2}{2}$ edges. The theorem is an important result in graph theory and the foundation of the field of extremal graph theory.

In this thesis I present a formalisation of Turán's graph theorem in the Isabelle/HOL proof assistant. To the best of my knowledge, this is the first formalisation of Turán's graph theorem in any proof assistant.

Besides a direct adaptation of the textbook proof, I have also modified this proof to decrease the size of the formalised proof significantly.

For the proof I have also formalised a number of results about cliques.

Acknowledgements

First and foremost, I want to express my sincere gratitude to my course adviser and thesis supervisor Prof Larry Paulson. His support was invaluable and it was an absolute honour to learn Isabelle from him.

Furthermore, I wish to thank my co-supervisor Angeliki Koutsoukou-Argyraki for her incredible advice and patience with my delayed emails.

Besides academia, I want to thank Clare College and the whole MCR. Being a part of this community is an incomparable experience. I could not have wished for a better College.

I want to express my special thanks to Yannick and Simon for their advice whenever I was overwhelmed by Cambridge.

I also want to thank all my friends in Cambridge, Saarbrücken, and all around the world. Thank you Yuan, Justin, Joey, and everyone else - I wish I had the time to give everyone the praise they deserve for being awesome. Thank you for making this time unforgettable and also for still putting up with my regular Beatles stories.

Last but not least, I am extremely grateful to my family and, in particular, my parents. Thank you for your emotional support and understanding, even when I did not show any signs of life for a week. I owe it all to you.

Contents

Chapter 1

Introduction

Computers have been extensively employed for the verification of mathematical proofs [1, 2]. In particular, graph theory has been a prominent field in the research of computer-verified proofs: One of the first, most prominent steps in computer-aided mathematical proving was made by Appel and Haken in their proof of the four color theorem [3]. For this proof they made heavy use of computers to check thousands of individual cases. In 2008, Gonthier et al. proved the four color theorem completely in the Coq proof assistant [4].

The scope of this thesis is to formalise a central result in graph theory. I present a formalised proof of Turán's graph theorem [5] in the Isabelle/HOL proof assistant [6, 7]. Turán's graph theorem states the upper bound for the number of edges an undirected, simple graph G can have if G does not contain a p-clique for some $p \in \mathbb{N}$ [8].

1.1 Extremal graph theory and Turán's graph theorem

Extremal graph theory is an important branch of graph theory which is in its core concerned with questions about the maximum number of edges a graph can have so that a certain property is satisfied. The most basic questions of extremal graph theory deal with the so-called *forbidden subgraph problem* [9]. Given a number of vertices n and a graph F the goal of the forbidden subgraph problem is to find the number $ex(n, F)$ of edges any graph G can maximally have so that F is no subgraph of G [10].

Turán's graph theorem can then be expressed using the forbidden subgraph problem: $ex(n, K_p)$, where K_p is the complete graph with p vertices, is exactly the biggest number of edges a graph of n nodes can have without containing a p-clique. Turán's graph theorem states an upper bound for $ex(n, K_p)$. In an additional step, this bound can also be shown to be the lowest upper bound, if n is divisible by $p - 1$.

Turán's graph theorem is lauded as the origin of extremal graph theory [8, 9] and also as "one of the fundamental results in graph theory" [8, p. 285]. In the following, I will give a brief account of the history of Turán's graph theorem and its proofs.

1.2 The History of Turán's graph theorem

In 1907 Willem Mantel discovered Mantel's theorem, a special case of Turán's graph theorem which is restricted to graphs that do not contain a 3-clique [11].

After 34 years, in 1941, Paul Turán discovered his eponymous theorem [5]. For this, Turán defines the so-called Turán graphs which satisfy the property that any other graph with the same number of nodes but more edges than a particular Turán graph must contain a clique that the respective Turán graph does not contain.

Besides Turán's original proof a number of proofs using different approaches have been discovered [8, 12]. Turán's original proof and Erdős' 1970 proof both make use of induction. Other proofs take advantage of methods from probability theory, e.g. Motzkin and Straus [14]. Alon and Spencer employ 'The Probabilistic Method' which is mainly attributed to Erdős for their proof of Turán's graph theorem [15, p. 100].

Aigner and Ziegler present another proof in their survey on proofs of Turán's graph theorem [8]. This proof, however, they cannot attribute to any author. Nevertheless, Aigner and Ziegler consider this proof to be potentially the most elegant of all known proofs, as it uses a simple argument to show that the graphs with the highest edge count without a p-clique must have the form of a Turán graph.

Turán's original proof, however, uses the most elementary proof techniques, namely, for the most part only induction. That is the reason why I formalise this proof in this dissertation. A more in-depth personal analysis of the feasibility of a formalisation of the different proofs is discussed in Chapter 2.3.

1.3 The proof assistant Isabelle/HOL

For the formalisation in this thesis I use the Isabelle proof assistant. Isabelle [6] is a generic theorem prover. In this project the Isabelle/HOL [7] instance is used which provides classical, higher-order logic.

Interactive theorem provers or proof assistants, like Isabelle/HOL, force the author to be absolutely precise. Textbooks often describe complex proof arguments with scanty details. A formalisation in a proof assistant offers abstraction while still maintaining an internal reducibility of proofs to the smallest logical steps. Furthermore, the reducibility to low-level logics and the explicitness yields unprecedented trust in formalised proofs.

Isabelle/HOL is accompanied by a considerable repository of definitions and proofs, the *Archive of Formal Proofs* [16]. My formalisation is built upon the definitions of simple, undirected graphs and simple proofs about them by Noschinski [17, 18]. Further results about graphs are used from a formalisation by Hupel [19].

Because of the extensive existing library of facts on graphs, including results from extremal graph theory, as well as its powerful proof automation, Isabelle/HOL poses a natural choice for a formalisation of Turán's graph theorem.

1.4 Related work

The field of graph theory has not gone unnoticed in interactive theorem proving research: There are substantial graph libraries for Isabelle/HOL [20, 18, 17], the Coq proof assistant [21], Lean[1], and HOL [22].

Recently, extremal graph theory has also gained traction in the field of interactive theorem proving. Szemerédi's regularity lemma has been formalised by Edmonds, Koutsoukou-Argyraki and Paulson [23] in Isabelle/HOL and by Mehta et al. [24] in Lean. This lemma is considered to be one of the most significant results in extremal graph theory [10].

Using their formalisation of Szemerédi's regularity lemma, Edmonds, Koutsoukou-Argyraki and Paulson went on to formalise Roth's theorem on arithmetic progressions [26] from the area of additive combinatorics in Isabelle/HOL [25]. For that, they first proved two important auxiliary lemmas in extremal graph theory, the triangle counting and the triangle removal lemma [27].

To the best of my knowledge no formalisation of Turán's graph theorem has been published.

1.5 Contributions

In this dissertation, I have formalised, to the best of my knowledge, the first proof of Turán's graph theorem in Isabelle/HOL and any other interactive theorem prover. My development follows Turán's original 1941 proof as closely as possible [5]. The formalisation enables a deeper understanding of the proof and uncovers difficulties that arise in a formal proof which do not allow for vague or imprecise arguments.

During the development of the formalisation, I have also discovered a modification to the proof which leads to a significant simplification of the formalised proof. This manifests itself in the omission of three auxiliary lemmas whose combined proof length is in excess of 100 lines of code.

In the process of this formalisation, I have also proved a number of results about cliques.

[1]The library of simple graphs in lean is part of the mathematical library *mathlib* [1]. The formalisation is available at `https://leanprover-community.github.io/mathlib-overview.html` (Accessed 6 June 2022)

1.6 Overview

In Chapter 2, the focus lies on all relevant definitions for this project, as well as a detailed proof of Turán's graph theorem on paper. Additionally, I discuss my reasons for the selection of this particular proof from the library of proofs of Turán's graph theorem.

The actual formalisation of Turán's graph theorem, including all relevant definitions and auxiliary lemmas, is discussed in Chapter 3. In that chapter, I also lay out an effective simplification of the proof and compare its impact on the overall complexity of the proof.

In Chapter 4, I describe potential paths for future work and in Chapter 5 thesis is concluded with final remarks on the project.

In the glossary (Appendix A) I give a brief description of standard Isabelle/HOL definitions that I use throughout this thesis.

Chapter 2

Turán's graph theorem on paper

In this chapter I want to give a precise mathematical description of the statement of Turán's graph theorem and Turán's original proof without considering the work with the proof assistant. Firstly, we need to consider the proper definitions of graphs and cliques.

Definition 2.1. *A **simple, undirected graph** is a pair (V, E) where V is a set of vertices and E is a set of edges between these vertices with $E \subseteq \{e \subseteq V \mid |e| = 2\}$.*

To refer to the vertices and edges of a graph G the notation $V(G)$ and $E(G)$ will be used, respectively.

In this dissertation only simple, undirected graphs will be considered. Therefore, in the following every graph will be implicitly simple and undirected.

Definition 2.2. *A **p-clique** in a graph $G = (V, E)$ is a complete subgraph (C, E') of G with p vertices. Explicitly, this means $|C| = p$, $C \subseteq V$, $E' \subseteq E$ and $E' = \{\{x, y\} \mid x, y \in C \ \wedge \ x \neq y\}$.*

2.1 Turán graphs

Before we get to Turán's graph theorem itself, I want to introduce the so-called Turán graphs [5, 8] as these graphs and their properties offer a motivation for the specific upper edge bound stated in Turán's graph theorem.

Turán graphs are special complete multipartite graphs.

Definition 2.3 (Complete multipartite graphs)**.** *A complete k-partite graph (V, E) is a graph in which V can be partitioned into k independent sets $V_1, \ldots, V_k$, i.e.*

$$\forall i.\ \forall x, y \in V_i.\ \{x, y\} \notin E$$

that satisfy

$$\forall i, j.\ i \neq j \to\ \forall x \in V_i.\ \forall y \in V_j.\ \{x, y\} \in E$$

Definition 2.4 (Turán graphs)**.** *For some $n, p \in \mathbb{N}$ ($p \geq 2$), the Turán graph $T_{n,p-1}$ is a $(p-1)$-partite graph of n vertices where all partitions pairwise differ in cardinality at most by one element.*

No complete multipartite graph with the same number of vertices and partitions contains more edges than the corresponding Turán graph [8]:

Fact 2.5. *Let V_i and V_j be partitions of a multipartite graph with $|V_i| < |V_j| - 1$. The number of edges in the complete multipartite graph increases when a node is transferred from the partition V_j to V_i.*

Proof. As all nodes in V_i and V_j are connected to all nodes in any other partition, the number of edges between V_i/V_j and other partitions remains constant. By moving a node v from V_j to V_i, v loses $|V_i|$ edges to V_i but now has an edge to each of the $|V_j| - 1$ nodes that remain in V_j. Overall, the absolute edge change is then $(|V_j| - 1) - |V_i|$ which is greater than 0 by assumption. □

With this we know that the number of edges increases when we move vertices between partitions in order to balance their cardinalities. As the Turán graphs are the most balanced multipartite graphs with regard to partition size, we know that, they have the highest edge count of any complete multipartite graph with the same number of nodes and partitions.

Turán has shown that the Turán graph $T_{n,p-1}$ contains $ex(n, K_p)$ edges, i.e. the maximum number of edges a graph with n vertices and no p-clique can have [5, 10]. This is the essence of Turán's graph theorem but before we discuss that, we need the following two facts about complete multipartite and Turán graphs that lead us to the actual theorem.

Fact 2.6. *A complete $(p-1)$-partite graph does not contain a p-clique.*

Proof. All vertices in each partition are connected to the exact same vertices while there are no edges within one partition. Hence, the size of the biggest clique is not decreased if we restrict each partition to one representative, if one exists. Consequently, as there are only $p-1$ partitions there is at most a $(p-1)$-clique but no p-clique. □

Fact 2.7. *If n is divisible by $p-1$ then $|E(T_{n,p-1})| = \left(1 - \frac{1}{p-1}\right)\frac{n^2}{2}$*

Proof. As n is divisible by $p-1$ we know that all partitions in $T_{n,p}$ contain exactly $\frac{n}{p-1}$ vertices. Turán graphs are complete multipartite graphs so that each vertex has an edge to all $\frac{n}{p-1}$ vertexes in each of the $p-2$ other partitions. So each vertex has

$n * \frac{p-2}{p-1} = n * \left(1 - \frac{1}{p-1}\right)$ outgoing edges. Overall, we then have the desired $\left(1 - \frac{1}{p-1}\right) \frac{n^2}{2}$ edges. The factor $\frac{1}{2}$ stems from the fact that we consider undirected graphs so that without this factor we would count each edge $\{x, y\}$ as two separate outgoing edges for x as well as y. □

Turán's graph theorem states that the edge count of $T_{n,p-1}$ from this fact is actually an overall upper limit for the edge count of any graph with n vertices but no p-clique, regardless of whether n is divisible by $p-1$ or not.

In the literature not all publications fully agree on the same statement of Turán's graph theorem. Instead of proving this upper limit for the edge count some publications show that the Turán graph $T_{n,p-1}$ is the unique graph, up to isomorphism, with n vertices, no clique greater than $p-1$, and $ex(n, K_p)$ edges [10]. In this dissertation I follow Aigner and Ziegler who consider this fact to be an extension to the actual theorem.

2.2 Turán's graph theorem

Now, we can precisely state and prove Turán's graph theorem. The original proof goes back to Turán [5] but the following proof is based on Aigner and Ziegler's presentation of Turán's proof.

Theorem 2.8 (Turán's graph theorem)**.** *Any simple, undirected graph $G = (V, E)$ with $n = |V|$ and without a p-clique ($p \geq 2$) satisfies*

$$|E| \leq \left(1 - \frac{1}{p-1}\right) \frac{n^2}{2}$$

Proof. We prove the claim with complete induction on n.

If $n < p$ then we have

$$\left(1 - \frac{1}{p-1}\right) \frac{n^2}{2} \geq \left(1 - \frac{1}{n}\right) \frac{n^2}{2} = \frac{n * (n-1)}{2} = \binom{n}{2} \geq |E|$$

so that the statement holds in this case.

Otherwise, we assume $n \geq p$. We can assume that G contains a $(p-1)$-clique as otherwise we can add edges to G so that there is a $(p-1)$-clique but no p-clique.

Let (A, E_A) be a $(p-1)$-clique in G. Furthermore, let $B = V \backslash A$, $E_B \subseteq E$ the edges between nodes in B, and $E_{AB} \subseteq E$ the edges between nodes in A and B. Consequently, E_A, E_B, and E_{AB} form a partition of E and hence $|E| = |E_A| + |E_B| + |E_{AB}|$.

(A, E_A) is a clique so that we have

$$|E_A| = \binom{|A|}{2} = \frac{(p-1)*(p-2)}{2}$$

As $|A| = p - 1 > 0$ we know that $|B| = |V \backslash A| = n - (p-1) < n$. As there evidently cannot be a p-clique in (B, E_B) we can use the induction hypothesis to obtain

$$|E_B| \leq \left(1 - \frac{1}{p-1}\right) \frac{(n-(p-1))^2}{2}$$

Finally, there can be no $b \in B$ which has an edge to every $a \in A$ as otherwise $A \cup \{b\}$ would induce a p-clique in G which is a contradiction. Hence, we have

$$|E_{AB}| \leq \sum_{b \in B} (p-2) = (n-(p-1)) * (p-2)$$

Overall, we can conclude

$$\begin{aligned}
|E| &= |E_A| + |E_B| + |E_{AB}| \\
&\leq \frac{(p-1)*(p-2)}{2} + \left(1 - \frac{1}{p-1}\right) \frac{(n-(p-1))^2}{2} + (n-(p-1)) * (p-2) \\
&= \frac{(p-1)*(p-2)}{2} + \frac{p-2}{p-1} * \frac{(n-(p-1))^2}{2} + (n-(p-1)) * (p-2) \\
&= \frac{p-2}{p-1} * \frac{1}{2} \big((p-1)^2 + (n-(p-1))^2 + 2 * (n-(p-1)) * (p-1)\big) \\
&= \frac{p-2}{p-1} * \frac{1}{2} ((p-1) + (n-(p-1)))^2 \\
&= \left(1 - \frac{1}{p-1}\right) \frac{n^2}{2}
\end{aligned}$$

□

2.3 Other proofs

As discussed in Chapter 1.2, a number of different proofs have been discovered after Turán's initial proof. I made the choice of formalising Turán's original proof not for historical reasons but because of feasibility considerations. Three proofs from the literature seem feasible to me for an immediate, first formalisation: Turán's original proof [5], Erdős' proof [13], and the unattributed folklore proof from "Proofs from THE BOOK" [8].

The decision fell on Turán's proof as it is the most direct of the three proofs. Erdős' and the folklore proof both somewhat indirectly show the theorem with multipartite graphs and Turán graphs: As proved in Fact 2.5, the Turán graph $T_{n,p-1}$ has the most edges of any multipartite graph of n vertices and $p-1$ partitions. Then, Erdős uses induction to show that every graph can be transformed into a multipartite graph with the same number of vertices and the same maximum clique size but with at least as many edges as the original graph. The folklore proof shows with a more direct argument that the graph fulfilling the desired properties with the maximum edge count must necessarily be multipartite.

As we can see Turán's proof does not require reasoning about multipartite graphs which simplifies the proof, in my opinion. Erdős' and the folklore proof, however, immediately imply the uniqueness of the Turán graphs as the desired graphs with the maximum edge count. Turán's proof, as presented here, also implies this but non-negligible further work is needed to obtain this fact [10].

Motzkin and Straus [14] as well as Alon and Spencer [15] employ probability theory for their proofs. The use of probabilistic methods is definitely feasible in an Isabelle/HOL formalisation of graph theory as demonstrated by Hupel in his formalisation of random graphs [19]. However, the additional overhead the use of probabilistic methods causes, deterred me from choosing these proofs for a first formalisation.

In contrast, the use of induction in Turán's proof is native to Isabelle/HOL and very natural. Furthermore, these probabilistic proofs do not imply the aforementioned uniqueness of the Turán graphs [8].

The proof by Moon and Moser [28, 12] was not considered by me because of its overall complexity which vastly exceeds the complexity of the other proofs.

Chapter 3

Turán's graph theorem in Isabelle/HOL

Mathematical proofs on paper rely on human reasoning which often depends on the intuition of the reader. However, spelled out, these proof arguments can become very elaborate. Grasping these arguments and rigorously laying them out is one of the main challenges of using interactive theorem provers.

After discussing the mathematical proof of Turán's graph theorem on paper in chapter 2, the focus in this chapter lies on the rigorous mathematical reasoning necessary to prove the theorem in Isabelle/HOL.

3.1 Framework

The definitions used for the proof of Turán's graph theorem are easily adapted for Isabelle/HOL. Simple, undirected graphs are already available in the `ugraph` theory in the Archive of Formal Proofs [18, 17], analogously defined as a pair of a set of vertices and a set of edges. Vertices are realised as natural numbers and an edge is a set over natural numbers. `uverts` and `uedges` are projection functions to access the vertices and edges of a graph, respectively.

To ensure that the graphs are indeed simple and undirected graphs, the library also provides a wellformedness predicate which imposes further restrictions on the sets of natural numbers that represent the edges of a graph. Explicitly, an edge must have the cardinality two and only contain elements from the corresponding set of vertices:

Definition 3.1. `uwellformed :: "ugraph ⇒ bool"` **where**
`"uwellformed G ≡ (∀e∈uedges G. card e = 2 ∧ (∀u ∈ e. u ∈ uverts G))"`

In the following, I will also use the wellformedness terminology for plain sets of edges when the corresponding set of vertices is implicitly clear.

The Isabelle libraries provide no satisfying definition of cliques for my use case. Therefore, I proceed with a standard definition of cliques that I define using the following function from the *ugraph* theory [18] that computes the set of all wellformed edges over a given set of vertices:

Definition 3.2. `"all_edges S ≡ (λ(x,y). {x,y}) ‘ {uv ∈ S × S. fst uv ≠ snd uv}"`

With this we can now state the fact that a graph is complete and hence define cliques:

Definition 3.3. `uclique :: "ugraph ⇒ ugraph ⇒ nat ⇒ bool"` **where**
```
"uclique C G p ≡ p = card (uverts C) ∧ C = (uverts C, all_edges (uverts C))
                 ∧ uverts C ⊆ uverts G ∧ uedges C ⊆ uedges G"
```

Before getting to a direct proof of Turán's graph theorem, I will discuss all the auxiliary lemmas that are needed so that the final proof closely resembles the readily comprehensible structure of the original paper proof.

As I use my own definition of clique there is no library to draw facts about cliques from. Therefore, I will briefly discuss some standard properties of cliques.

3.2 Facts about cliques

The first result formalises that if a graph contains a $p+1$-clique then the graph must also contain cliques of size p.

Fact 3.4 (*clique_size_jumpfree*).
assumes `"finite (uverts G)"` **and** `"uwellformed G"` **and** `"uclique C G (p+1)"`
shows `"∃C'. uclique C' G p"`

Proof. We know that `C` is a `(p+1)`-clique which contains some vertex `x` of `G`. The `(p+1)`-clique from which `x` and all corresponding edges have been removed is a `p`-clique. □

The next lemma generalises the last result to a proof of the existence of a clique of *any* size smaller than the size of the original clique.

Lemma 3.5 (*clique_size_decr*).
assumes `"finite (uverts G)"` **and** `"uwellformed G"` **and** `"uclique C G p"`
shows `"q ≤ p ⟹ ∃C. uclique C G q"`

Proof. The proof is by measure induction. Measure induction is a stronger version of complete induction where a measure function determines for which elements the inductive hypothesis holds. That is, the inductive hypothesis does not simply hold for all smaller elements but instead for all elements whose function values are smaller than the function value of the variable considered in the inductive step. It is necessary that the codomain of the measure function is wellordered so that the induction actually 'terminates'.

The measure induction is on `q` with the measure function `(λx. p - x)`. Subtracting two natural number yields a natural number as the subtraction operation on $\mathbb{N}$ is truncating.

Since, we only consider natural numbers we have the wellordered codomain that is a prerequisite of an application of measure induction.

The base case is $q = p$ as this is the greatest natural number the lemma makes a statement about and the measure function is monotonically decreasing. This case is exactly given by the assumption *uclique C G p*.

For the case $q < p$ we can use the inductive hypothesis $\exists C.$ *uclique C G q'* for all *q'* with $q < q' \leq p$. In particular, there is a *C* with *uclique C G (q+1)* so that we obtain a *C'* satisfying *uclique C' G q* using Fact 3.4. □

With this fact we can easily derive that if there is no p-clique then there cannot exist a clique of a size smaller than p:

Corollary 3.6 (*clique_size_neg_max*).
assumes *"finite (uverts G)"* **and** *"uwellformed G"* **and** *"¬(∃C. uclique C G p)"*
shows *"∀C q. uclique C G q ⟶ q < p"*

Proof. By contradiction using Lemma 3.5. □

The next fact does not have the immediate appearance of being concerned with cliques. The context, however, for which this Lemma will be used is directly linked with the notion of cliques: In a graph G with a p-clique C and some vertex v outside of this clique, there exists a $(p+1)$-clique in G if v is connected to all nodes in C. The real Isabelle/HOL statement is a very stripped down version of this aforementioned description, that does not explicitly mention cliques: If a vertex *n* has as many edges to a set of nodes *N* as there are nodes in *N* then *n* is connected to all vertices in *N*.

Lemma 3.7 (*card_edges_nodes_all_edges*).
fixes *G :: "ugraph"* **and** *N :: "nat set"* **and** *E :: "nat set set"* **and** *n :: nat*
assumes *"uwellformed G"*
  and *"finite N"*
  and *"N ⊆ uverts G"* **and** *"E ⊆ uedges G"*
  and *"n ∈ uverts G"* **and** *"n ∉ N"*
  and *"∀e ∈ E. ∃x ∈ N. {n,x} = e"*
  and *"card E = card N"*
shows *"∀x ∈ N. {n,x} ∈ E"*

Proof. The proof is by contradiction. So, we assume there is a vertex *x* in *N* that has no edge to *n*. This implies that *(λy. {n,y})* is a surjective function from *N - {x}* to *E*. Consequently, we have *card E ≤ card (N - {x}) = card N - 1*. This contradicts the assumption *card E = card N* as we know that there is at least one element in *N* so that *card N ≥ 1* □

We have proved these very basic facts about cliques with which we can now turn to the actual core of the proof of Turán's graph theorem.

3.3 Adding a p-clique to a graph

In the mathematical proof of Turán's graph theorem on paper there is the casual remark that we can assume that the graph contains a $(p-1)$-clique but no p-clique as otherwise we can add edges to obtain such a graph.

The argument is intuitively obvious but in the formalisation we need to explicitly prove the existence of such a graph which contains a $(p-1)$-clique, no p-clique, and at least as many edges. We can simplify this task by not looking for some arbitrary graph which fulfils the aforementioned properties but instead we modify the original graph by literally adding edges. With this approach we can remove the requirement that the graph needs to contain more edges as by the nature of this method we are guaranteed to have more edges. Explicitly, for the proof this means that I show the existence of a set of edges `E`, so that the original graph to which the edges in `E` have been added fulfils the requirements.

The main difficulty in this proof stems from the fact that we need to ensure that we do not accidentally increase the greatest clique size by too much. The way in which this is achieved might be counterintuitive: Usually, the intuition is that edges are added to the graph one after another until the greatest clique has the desired size. In contrast, my proof will take the opposite direction by adding too many edges, to then gradually remove the superfluous edges.

For that, we need the following lemma: When too many edges have been added to a graph so that there exists a $(p+1)$-clique then we can remove at least one of the added edges while also retaining the p-clique:

Lemma 3.8 (*clique_union_size_decr*).

```
assumes "finite (uverts G)" and "uwellformed (uverts G, uedges G ∪ E)"
  and "uclique C (uverts G, uedges G ∪ E) (p+1)"
  and "card E ≥ 1" and "p ≥ 1"
shows "∃C' E'. card E' < card E
              ∧ uclique C' (uverts G, uedges G ∪ E') p
              ∧ uwellformed (uverts G, uedges G ∪ E')"
```

Proof. We do a case analysis: If no edge of the $(p+1)$-clique `C` is in `E` then we know that the unaltered graph `G` already contained a $p+1$-clique. With Fact 3.4 we know that G also contains a p-clique so that the statement is satisfied for `E'={}` because `card E ≥ 1`.

If there exists an edge `e` in `C` which is also in `E` then let `x` be one of the vertices to which `e` is incident. By removing `x` and all relevant edges from `C` and `E` we obtain `C'` and `E'`, respectively, which satisfy the statement: At least `e` is removed from `E` so that `E' < E`.

Furthermore, the removal of a vertex and its edges from a complete graph with *(p+1)* vertices yields another complete graph with *p* vertices. This closes the proof. □

This fact justifies the proof idea to remove superfluous edges: We can be certain with this lemma that the biggest clique size decreases by at most one when we remove an edge.

We use this fact to prove the next lemma. In this lemma we assume that we have already added to many edges. The goal is then to remove some of the new edges appropriately so that it is indeed guaranteed that there is no bigger clique.

I will describe two proof ideas that differ in execution, however, they both fundamentally come down to the same core idea: In essence, both proofs apply the Well-ordering principle - in the first proof we do so immediately by obtaining the minimum of a set and the second one by using (complete) induction.

Lemma 3.9 (*clique_union_make_greatest*).
  fixes *p n :: nat*
  assumes *"finite (uverts G)"* **and** *"uwellformed G"*
    and *"uwellformed (uverts G, uedges G ∪ E)"* **and** *"card(uverts G) ≥ p"*
    and *"uclique C (uverts G, uedges G ∪ E) p"*
    and *"∀C' q'. uclique C' G q' ⟶ q' < p"* **and** *"1 ≤ card E"*
  shows *"∃C' E'. uwellformed (uverts G, uedges G ∪ E')*
      ∧ (uclique C' (uverts G, uedges G ∪ E') p)
      ∧ (∀C'' q'. uclique C'' (uverts G, uedges G ∪ E') q' ⟶ q' ≤ p)"

First Proof. To enable effective proof automation we introduce the following predicate *P* which describes all appropriate edge extensions *E* of *G* so that there is a p-clique in the extended graph.
  define *P* **where**
    "P ≡ λE. uwellformed (uverts G, uedges G ∪ E)
        ∧ (∃C. uclique C (uverts G, uedges G ∪ E) p)"

As wellformedness is a part of the predicate, we know that only a set of edges can satisfy *P*. Hence, as *G* only has a finite number of vertices, we know that there are only finitely many sets *E* that satisfy *P*. With the well-ordering principle, we know that there exists a smallest natural number *min* that is the cardinality of a set satisfying *P*. Let *F* bet a set satisfying *P* with *card F = min*. That means there exists no set with less than *min* elements that satisfies *P*.

We perform a case analysis: Assume there exists no $(p+1)$-clique in the graph *G* extended with *F*. Then, we know that *F* is the proper extension we are looking for as we have *P F* and by Corollary 3.6 there is clique of size bigger than *p* in the extended graph.

If there exists a $p+1$-clique in the graph *G* extended with *F* then we obtain with Lemma 3.8 an extension *F'* which is smaller than *F*, retains the wellformedness of *G*, and most importantly, we also know that `G` extended with `F'` still contains a p-clique. Hence, `F'` satisfies `P`. This poses a contradiction as we have `card F' < card F` but `F` is also the smallest set satisfying `P`. □

Second Proof. We use complete induction on the cardinality of `E` and do a case analysis: If there exists no $(p+1)$-clique in `G` extended with `E` then we know, similarly to the analogue case in the first proof, that `E` is the extension we are looking for (Corollary 3.6).

Alternatively, consider the case where there is a $(p+1)$-clique in `G` extended with `E`. With Lemma 3.8 we get a extension `E'` smaller than `E` that still maintains the properties of `E` that are stated in the assumptions of this lemma that is proved. Consequently, we can apply the inductive hypothesis to `E'` and the respective p-clique. This immediately closes the proof. □

As mentioned before, both of the two proofs above share the same core idea which we can now intuitively see: When there is a $(p-1)$-clique then we can always remove edges from the extension and preserve the p-clique. As there is no p-clique in the plain, unextended graph `G` we know that there must be an extension which does not entail a $(p+1)$-clique. Otherwise, we could remove edges from the (finite) extension, preserving the p-clique, until we arrive at the plain `G` again. This is a contradiction so we just need to find some subset of the original extension `E` so that there is a p-clique but no $(p+1)$-clique.

The first proof immediately finds one of these extensions by considering the smallest extension that still inserts a p-clique into `G`. In contrast, the second proof arrives at the desired extension by successively removing edges via the induction.

Finally, with this lemma we can turn to this section's main challenge of increasing the greatest clique size of a graph by adding edges.

Lemma 3.10 (`clique_add_edges_max`).

```
fixes p :: nat
assumes "finite (uverts G)"
  and "uwellformed G" and "card(uverts G) > p"
  and "∃C. uclique C G p" and "(∀C q'. uclique C G q' ⟶ q' ≤ p)"
  and "q ≤ card(uverts G)" and "p ≤ q"
shows "∃E. uwellformed (uverts G, uedges G ∪ E)
            ∧ (∃C. uclique C (uverts G, uedges G ∪ E) q)
            ∧ (∀C q'. uclique C (uverts G, uedges G ∪ E) q' ⟶ q' ≤ q)"
```

Proof. We perform a case analysis: If `p = q`, then `E={}` fulfils the properties using the assumptions.

Alternatively, we have `p < q`.

With Lemma 3.9 it suffices to find some set `E` of edges over `uverts G` to `G` so that the wellformedness is maintained and there exists a q-clique. We choose for this set `E` all possible edges over `uverts G`. We then have, that `G` augmented with `E` is a complete graph so that this graph forms a (`card(uverts G)`)-clique in itself. As `card(uverts G)` is greater than `p`, we can use Lemma 3.5 with the aforementioned (`card(uverts G)`)-clique to obtain a q-clique in the extended graph. That means, the chosen `E` satisfies the premises of Lemma 3.9 and the proof is closed. □

3.4 Partitioning the edges of a graph

Turán's proof partitions the edges of the graph into three partitions for a $p-1$-clique C: All edges within C, all edges outside of C, and all edges between a vertex in C and a vertex not in C.

It is not necessary at this point to be overly precise and to consider cliques in the proof. Instead, we just partition along some arbitrary set of vertices which does not necessarily need to induce a clique. Furthermore, in Turán's graph theorem we only argue about the cardinality of the partitions so that we restrict this proof to showing that the sum of the cardinalities of the partitions is equal to number of all edges.

Fact 3.11 (`graph_partition_edges_card`).

```
  assumes "finite (uverts G)" and "uwellformed G" and "A ⊆ (uverts G)"
  shows "card (uedges G) = card {e ∈ uedges G. e ⊆ A}
                   + card {e ∈ uedges G. e ⊆ uverts G - A}
                   + card {e ∈ uedges G. e ∩ A ≠ {} ∧ e ∩ (uverts G - A) ≠ {}}"
```

Proof. To show that this equation holds, we need to show that the sets on the right side of the equation indeed partition the edges. For that, we first show that the union of the sets on the right side of the equation contains exactly the same elements as `uverts G`:

The graph is wellformed so that all edges are sets of vertices of cardinality two. Hence, the number of vertices from `A` in every edge is necessarily 2, 1, or 0. These three options are exactly covered by the three sets.

Now, it remains to be shown that the three sets disjointly cover the aforementioned options. This is the case as `A` and `uedges G - A` are disjoint by definition.

Finally, as all the sets in this proof are finite, we know that the equation holds. □

3.5 The cardinalities of the partitions

In the last section we have proved that the set of edges can be partition in order to calculate its cardinality. Now, we turn to the problem of calculating the cardinalities of these partitions when they are induced by the biggest clique in the graph.

First, we consider the number of edges in a p-clique.

Fact 3.12 (*clique_edges_inside*).
assumes *G1: "uwellformed G"* **and** *G2: "finite (uverts G)"*
and *p: "p ≤ card (uverts G)"* **and** *n: "n = card(uverts G)"*
and *C: "uclique C G p"*
shows *"card {e ∈ uedges G. e ⊆ uverts C} = p * (p-1) / 2"*

Proof. By the definition of clique, we know that *uedges C ⊆ uedges G* so that the set whose cardinality we are considering is equal to *uedges C*. *C* is a complete graph and hence *uedges C = all_edges (uverts C)*

As we use the *all_edges* function from the *Archive of Formal Proofs* [18] we also have access to the accompanying results over *all_edges* in this formalisation. In particular, we have the fact that the cardinality of *(all_edges V)* is, as expected, the binomial coefficient $\binom{|V|}{2} = \frac{|V|*(|V|-1)}{2}$. Consequently, we have *card (all_edges (uverts C)) = p * (p-1) / 2*. □

Next, we turn to the number of edges that connect a node inside of the biggest clique with a node outside of said clique. For that we start by calculating a bound for the number of edges from one single node outside of the clique into the clique.

Lemma 3.13 (*clique_edges_inside_to_node_outside*).
assumes *"uwellformed G"* **and** *"finite (uverts G)"*
and *"0 < p"* **and** *"p ≤ card (uverts G)"*
and *"uclique C G p"* **and** *"(∀C p'. uclique C G p' ⟶ p' ≤ p)"*
and *"y ∈ uverts G - uverts C"*
shows *"card {{x,y}| x. x ∈ uverts C ∧ {x,y} ∈ uedges G} ≤ p - 1"*

Proof. For effective proof automation we use a local function definition to compute this set of edges into the clique from any node *y*:
define *S* **where**
"S ≡ λy. {{x,y}| x. x ∈ uverts C ∧ {x,y} ∈ uedges G}"

Then, we do a proof by contradiction. So, we assume *card (S y) > p - 1* in order to derive a contradiction. We can even derive that *S y* contains exactly *p* elements: As a subset of *uverts G* we have the wellformedness of *S y* and hence all edges in *S y* are of the form *{x,y}* where *x ∈ (uverts C)*. Consequently, *card (S y) ≤ card (uverts C) = p* and so overall *card (S y) = p*

By our assumptions it suffices to show that there exists a $(p+1)$-clique in *G*. I claim that *({y} ∪ (uverts C), S y ∪ uedges C)* is a $(p+1)$-clique in G:

First, the cardinality of *{y} ∪ (uverts C)* is $p+1$ as y is not in *uverts C* by assumption. Secondly, *C* is a clique in *G* and *y* is a node in *G* so that *{y} ∪ (uverts C)* is a subset of `uverts G`. Similarly, `S y ∪ uedges C` is also a subset of `uedges G`, in particular because the set returned by `S` is always a subset of `uedges G`.

Lastly, we need to show that `({y} ∪ (uverts C), S y ∪ uedges C)` is a complete graph, that is `(S y ∪ uedges C) = all_edges ({y} ∪ (uverts C))`. For that we prove that both sets are mutually subsets of each other.

`(S y) ∪ uedges C ⊆ all_edges ({y} ∪ (uverts C))` holds because `C` is a clique and hence complete, and `S y` only contains edges between `y` and `uverts C` which are all in `all_edges ({y} ∪ (uverts C))`.

For the other direction we recall that `card (S y) = card (uverts C)` and that all edges in `S y` have the form `{x,y}` where `x ∈ (uverts C)`. With Lemma 3.7 we can then obtain `∀x ∈ (uverts C). {y,x} ∈ S y`. That means all edges `{x,y}` with `x ∈ (uverts C)` are in `(S y) ∪ uedges C`. Hence, to prove the subset relation it only remains for us to show `all_edges (uverts C) ⊆ (S y) ∪ uedges C`. This is an immediate consequence of the fact that `C` is complete so that `uedges C = all_edges (uverts C)`.

With both subset relations we can conclude that `({y} ∪ (uverts C), S y ∪ uedges C)` is a complete graph.

Overall, we know with these facts that `({y} ∪ (uverts C), S y ∪ uedges C)` is a $(p+1)$-clique in G and hence we have the contradiction. $\square$

Now, that we have this upper bound for the number of edges from a single vertex into the largest clique we can calculate the upper bound for all such vertices and edges:

Lemma 3.14 (*clique_edges_inside_to_outside*).

```
assumes G1: "uwellformed G" and G2: "finite (uverts G)"
  and p0: "0 < p" and pn: "q ≤ card (uverts G)" and "card(uverts G) = n"
  and C: "uclique C G p" and C_max: "(∀C p'. uclique C G p' ⟶ p' ≤ p)"
shows "card {e ∈ uedges G. e ∩ uverts C ≠ {} ∧ e ∩ (uverts G - uverts C) ≠ {}}
       ≤ (p - 1) * (n - p)"
```

Proof. The set under consideration is a subset of the edges of `G` so that we directly know from the wellformedness of `G` that there are, as expected, exactly two nodes in each of the edges in the set.

For all `e` in the set we know that the cuts with the two naturally disjoint sets `uverts C` and `uverts G - uverts C` are non-empty. From that we know that each edge in the set has the form `{x,y}` where `x ∈ uverts C` and `y ∈ (uverts G - uverts C)`. For any `y ∈ (uverts G - uverts C)` we know from Lemma 3.13 that there are at most `(p-1)` edges to such an `x ∈ uverts C`.

`C` is a p-clique in `G` so that there are `(n-p)` vertices `y ∈ (uverts G - uverts C)`. By combinatorics we can conclude that there are overall at most `(n-p) * (p-1)` edges of the form `{x,y}` where $x \in$ `uverts C` and $y \in$ `(uverts G - uverts C)`. □

Lastly, we need to argue about the number of edges which are located entirely outside of the greatest clique. Note that this is in the inductive step case in the overarching proof of Turán's graph theorem. That is why we have access to the inductive hypothesis as an assumption in the following lemma:

Lemma 3.15 (*clique_edges_outside*).

```
assumes "uwellformed G" and "finite (uverts G)"
  and p2: "2 ≤ p" and pn: "p ≤ card (uverts G)" and n: "n = card(uverts G)"
  and C: "uclique C G (p-1)" and C_max: "(∀C p'. uclique C G p' ⟶ p' ≤ p-1)"
  and IH: "⋀G y. y < n ⟹ finite (uverts G) ⟹ uwellformed G
              ⟹ ∀C p'. uclique C G p' ⟶ p' < p ⟹ 2 ≤ p
              ⟹ card (uverts G) = y
              ⟹ real (card (uedges G)) ≤ (1 - 1 / real (p - 1)) * real (y²) / 2"
shows "card {e ∈ uedges G. e ⊆ uverts G - uverts C}
          ≤ (1 - 1 / (p-1)) * (n - p + 1) ^ 2 / 2"
```

Proof. This is an immediate consequence of the inductive hypothesis `IH` applied to the graph `(uverts G - uverts C, {e ∈ uedges G. e ⊆ uverts G - uverts C})`. We may apply the inductive hypothesis to this graph as `C` is a clique in `G` of size greater than 0 so that `uverts G - uverts C` really contains less nodes than `G`. The premises for the inductive hypothesis are mostly direct consequences of the analogous assumptions for `G`.

I only want to discuss the fact that there is also no clique of size greater or equal to p in the subgraph, as this subgoal is not immediately shown by proof automation. We assume there exists such a clique and derive a contradiction. This clique with more than p vertices is immediately a clique in `G` which contradicts the assumptions. □

This concludes the proofs about the cardinalities of the edge partitions.

3.6 Reasoning about mathematical equations

Now, we will turn our attention to transforming the sum of the partition's cardinalities into the proper equation for Turán's graph theorem. In the proof on paper (Theorem 2.8) multiple transformation steps were necessary to end up at the correct equation. The support for proof automation in Isabelle/HOL for arithmetic equations is not strong enough to directly infer these steps.

Lemma 3.16 (*turan_sum_eq*).

```
fixes n p :: nat
assumes "p ≥ 2" and "p ≤ n"
shows "(p-1) * (p-2) / 2 + (1-1/(p-1)) * (n-p+1) ^ 2 / 2 + (p-2) * (n-p+1)
        = (1-1/(p-1)) * n^2 / 2"
```

Proof. To improve the power of proof automation in this proof, I substitute `(p-1)` for an arbitrary `a` with `1` $\leq$ `a` $\leq$ `n`. The proof goal then changes to the following equation:

```
"a * (a-1) / 2 + (1-1/a) * (n-a) ^ 2 / 2 + (a-1) * (n-a) = (1-1/a) * n^2 / 2"
```

I follow the transformations in the proof on paper (Theorem 2.8) closely by proving these steps individually. These single transformation steps can mostly be shown using automation but it is often necessary to supply the relevant lemmas from the library, for example commutativity or the binomial formula. Automation is then able to put together the steps by transitivity and we obtain the final equation. □

3.7 The proof of Turán's graph theorem

With the definitions and proofs from this chapter we can now state and prove Turán's graph theorem in Isabelle/HOL. The statement in Isabelle/HOL basically completely mirrors Turán's graph theorem on paper. The only slight difference is the additional assumption that the set of vertices is finite. On paper, this is an evident consequence of the fact that the graph has n vertices. In Isabelle/HOL, this elaboration is necessary as the cardinality of an infinite set is defined as 0. Consequently, without this further assumption this theorem would not be provable as the statement does not apply to infinite graphs.

Theorem 3.17 (*turan*).
  fixes *p n :: nat*
  assumes *"finite (uverts G)"* **and** *"uwellformed G"* **and** *"card(uverts G) = n"*
    and *"∀ C p'. uclique C G p' ⟶ p' < p"* **and** *"p ≥ 2"*
  shows *"card (uedges G) ≤ (1 - 1 / (p-1)) * n^2 / 2"*

Proof. We perform complete induction on `n` with `G` generalised.

We do a case analysis: In the case that `n < p`, we perform another, nested case analysis on `n`. If `n = 0`, then we know that there are no vertices in `G`. As `G` is wellformed, we know that then there cannot be any edges in `G` so that `card (uedges G) = 0` which directly implies the inequality.

Alternatively, if `n > 0` then `1 - 1 / n` is defined and we have `1 - 1 / n` $\leq$ `1 - 1 / (p - 1)`. From the library [19, 18], we know that all wellformed edges are in `all_edges (uverts G)` and `card (all_edges (uverts G))` = $\binom{n}{2}$ = $\frac{n*(n-1)}{2}$. Overall we then have

$$(1 - \frac{1}{p-1}) * \frac{n^2}{2} \geq (1 - \frac{1}{n}) * \frac{n^2}{2} = \frac{n*(n-1)}{2} = \texttt{card(all\_edges(uverts G))} \geq \texttt{card(uedges G)}$$

We return to the outermost case analysis and regard the case that `n` $\geq$ `p`. There must exist a q-clique in `G` so that there is no bigger clique in `G`. This is because with the empty graph there exists a clique (of size 0) in `G` and all cliques in `G` must be smaller than `p` by assumption so that there must exist a biggest clique.

With Lemma 3.10, we obtain a set of wellformed edges *E* over *uverts G* so that *(uverts G, uedges G ∪ E)* contains a $(p-1)$-clique *C* but no p-clique. The number of edges in this union is naturally greater or equal to the edge count in *G* so that we will now prove the same upper bound for this new graph.

Using Fact 3.11 we know that *card (uedges G ∪ E)* is equal to

```
   card {e ∈ uedges G ∪ E. e ⊆ uverts C}
 + card {e ∈ uedges G ∪ E. e ⊆ uverts G - uverts C}
 + card {e ∈ uedges G ∪ E. e ∩ uverts C ≠ {} ∧ e ∩ (uverts G - uverts C) ≠ {}}
```

Applying Lemmata 3.12, 3.15 and 3.14 to the summands, respectively, yields the following inequality:

```
card (uedges G ∪ E) ≤ (p-1)*(p-2)/2 + (1-1/(p-1))*(n-p+1)^2 / 2 + (p-1)*(n-p)
```

Note that the inductive hypothesis is used in 3.15.

The right side of the equation exactly corresponds to the term in Lemma 3.16. □

In this Isabelle/HOL proof of Turán's graph theorem I tried to very closely follow the deliberations of Turán in his proof [5, 8]. During my work on the original proof I have found an adaptation to the proof which considerably simplifies the proof formalisation.

3.8 Simplifying the proof

In the proof of Turán's graph theorem one of the main challenges is to find a bigger graph that contains a $(p-1)$-clique but no p-clique. This intuitively seems to be a trivial fact on paper and the appearance of this in the main Isabelle/HOL proof is also inconspicuous. Nevertheless, the auxiliary lemmas that justify this fact take up a sizeable portion of the all proofs.

It turns out that this argument can be replaced by a different argument which maintains the simplicity on paper but also translates to an equally simple formal proof. The idea is, that in the induction we do not only generalise over the graph but also over p, the upper bound for the biggest clique size.

The majority of the proof remains the same. However, in the case *p ≤ n* when we obtain the biggest, already existing clique *C* in *G*, with some size *q*, then we do not extend *G* with edges. Instead, we replace *p* by *(q+1)* and proceed with the proof as normal. This is possible as we know that *q* is the biggest clique size in *G* and so the partitioning works completely identically. In particular, the number of edges that are not incident to any node in *C* can still be bounded using the inductive hypothesis. This is because *2 ≤ n* so that there exists at least a 1-clique in *G*. Hence, when we remove *C* from *G* then we indeed have a smaller graph and hence the inductive hypothesis is still applicable.

Overall, we then obtain the inequality *card (uedges G) ≤ (1 - 1 / q) * n^2 / 2*. From this we can close the proof with transitivity and the following trivial fact which can be proved directly by proof automation:

Fact 3.18 (*turan_equation_mono*).
fixes *n p q :: nat*
assumes *"0 < q"* **and** *"q < p"* **and** *"p ≤ n"*
shows *"(1 - 1 / q) * n^2 / 2 ≤ (1 - 1 / (p-1)) * n^2 / 2"*

Impact of the simplification

The length and intuitive complexity of the proof on paper has not changed with the change proposed here. The complexity of the formal proof, however, has been cut significantly: There is no additional overhead for the adaptation but all lemmas related to adding edges to a graph in order to ensure the existence of a particular greatest clique are obsolete with this simplification. These lemmas account for 129 lines of code which is a significant part of the overall 609 lines of code of the unsimplified proof.

The most beautiful proof

Aigner and Ziegler, whose presentation of Turán's proof [5] I follow, have set out the goal in their book "Proofs from THE BOOK" to amass a collection of the most beautiful proofs of standard mathematical theorems [8]. My simplification has only a slight influence on the length of the proof on paper, however in this context the question "What makes a proof beautiful?" naturally arises. Arguably, a shorter formal proof is usually more beautiful than a considerably longer formal proof. In this particular case, I also want to put the following argument in favour of the superior beauty of the simplified proof forward. Although there might be no difference in intuitiveness for the knowledgable reader, but the simplified proof is more comprehensible to a reader with less experience in the field of graph theory.

In the original proof it is necessary to recognise that it is possible to add edges to a graph in order to obtain a greatest clique of size *(p-1)*. For that it is necessary to realise that any edge added to a graph can at most increase the maximum clique size by one. This might not be immediately obvious, especially considering that Aigner and Ziegler's book is also aimed at undergraduates in mathematics.

In contrast, the part that was added in the simplified version only requires basic knowledge of algebra.

[0] In this calculation I do not include any duplicate proofs but only the essential parts of the unsimplified proof. For a list of all proofs and their corresponding lines of code, see Chapter 5

Chapter 4

Future Work

For future work there are multiple interesting paths. In the following, I will illuminate some of these available options.

4.1 A formalisation of the uniqueness of Turán graphs

I do not consider Turán graphs in the Isabelle/HOL formalisation. With a definition of Turán graphs and an accompanying proof of the respective number of edges they contain, we can then show that Turán's graph theorem indeed states the least upper bound $ex(n, K_p)$, if n is divisible by $p - 1$.

Furthermore, I naturally also do not conclude in my formalisation that the Turán graphs are the unique graphs with n nodes and no p-clique which have $ex(n, K_p)$ edges. With additional reasoning it is possible to derive this from Turán's proof [10].

The proof by Erdős and the folklore proof as presented by Aigner and Ziegler [8] also yield this fact. For such a formalisation, a lot of auxiliary results about multipartite graphs will be required.

4.2 A probabilistic proof of Turán's graph theorem

As discussed in Chapter 2.3, the proofs by Motzkin and Straus [14] and Alon and Spencer [15] use methods of probability theory to prove Turán's graph theorem. For Isabelle/HOL formalisations in the field of graph theory that employ probability theory there has been precedence by the work of Hupel [19]. A formalisation of Turán's graph theorem using these methods would be very interesting, albeit these proofs do not imply the aforementioned uniqueness of Turán graphs.

4.3 Further results in extremal graph theory

As discussed in Chapter 1.4, Extremal graph theory is no untrodden ground in the field of interactive theorem proving. However, there are still many important results from extremal graph theory that have not been formalised.

Erdős–Stone theorem Erdős and Stone discovered the Erdős–Stone theorem [29], a stronger version of Turán's graph theorem, in 1946 which is referred to as "the fundamental theorem of extremal graph theory" [9, p. 120] in the literature. Erdős–Stone theorem generalises Turán's graph theorem in the sense that it states an upper bound for the number of edges a graph can have if it does not contain a complete r-partite graph with partitions of equal size, for some r. The superior power of this result becomes apparent when one recalls that these multipartite graphs with equally sized partitions are Turán graphs.

Erdős and Stone's original proof use induction on r to prove the result. Just like for Turán's graph theorem more proofs have been discovered, for example Diestel presents a particularly interesting proof which employs Szemerédi's regularity lemma. A formalisation of the Erdős–Stone theorem in Isabelle/HOL could then take advantage of Edmonds, Koutsoukou-Argyraki and Paulson's formalisation of Szemerédi's regularity lemma

Based on this theorem there is a multitude of other interesting results that could be considered, e.g. Bollobás and Erdős proved a stronger version of the theorem. [30].

Mantel's theorem As mentioned in Chapter 1.2, Mantel's theorem [11] was the precursor of Turán's graph theorem with its limitation to 3-cliques. Naturally, Turán's graph theorem implies Mantel's theorem, nevertheless it would be interesting to formalise the theorem as many proofs use special, differing approaches.

Chapter 5

Conclusion

In this dissertation I have presented a complete formalisation of Turán's graph theorem in the Isabelle/HOL proof assistant.

The complete proof script is located in the `turan.thy` theory file which was submitted along with this thesis. The development is dependent on Noschinski's [18] and Hupel's [19] theories from the *Archive of formal proofs* [16][1].

My first goal for the formalisation was to simply adhere to the textbook proof of Turán's graph theorem. This task may seem trivial as it appears to be only a matter of implementing the given reasoning. That this is not accurate, becomes apparent when one recalls the task of extending a graph so that it contains a $(p-1)$-clique but no p-clique. On paper this is an insignificant remark but in the formalisation this requires considerable work, as we have seen.

The work with proof assistants requires absolutely precise and rigorous arguments. It is easy to overlook this difficulty as the final formal proof often directly reinforces our intuition. In contrast, the task of initially formulating the rigorous proofs is very difficult. The first proof of Lemma 3.10, was very laborious and complicated. Only afterwards, I was able to bring this lemma into the much more elegant form I have presented here.

My first complete formalised proof of Turán's graph theorem contained 746 lines of code. In contrast, the fully simplified proof, which I discussed in Chapter 3.8), is only made up of 547 lines of code. Figure 5.1 offers a summary of all the formalised proofs I have discussed in this dissertation[2].

[1] For information on how to make these entries available for my development, consult `https://www.isa-afp.org/using.html` (Accessed 6 June 2022)

[2] Note, for the overall sum of lines of code that some results have two different proofs which both add up to total.

Thesis	**Isabelle/HOL**	**Lines of code**
Fact 3.4	`clique_size_jumpfree`	37
Lemma 3.5	`clique_size_decr`	23
Corollary 3.6	`clique_size_neg_max`	16
Lemma 3.7	`card_edges_nodes_all_edges`	24
Lemma 3.8	`clique_union_size_decr`	59
Lemma 3.9 - First proof	`clique_union_make_greatest_alt`	45
Lemma 3.9 - Second proof	`clique_union_make_greatest`	36
Lemma 3.10	`clique_add_edges_max`	34
Fact 3.11	`graph_partition_edges_card`	23
Fact 3.12	`clique_edges_inside`	16
Lemma 3.13	`clique_edges_inside_to_node_outside`	49
Lemma 3.14	`clique_edges_inside_to_outside`	51
Lemma 3.15	`clique_edges_outside`	35
Lemma 3.16	`turan_sum_eq`	38
Theorem 3.17	`turan`	65
Fact 3.18	`turan_equation_mono`	5
Chapter 3.8	`turan'`	62
—	Other auxiliary lemmata	103
—	Σ	721

Figure 5.1: The proofs described in this dissertation and how they correlate to the formalisation.

Bibliography

[1] The mathlib Community. "The Lean Mathematical Library". In: *Proceedings of the 9th ACM SIGPLAN International Conference on Certified Programs and Proofs*. CPP 2020. Association for Computing Machinery, 2020, pp. 367–381. DOI: 10.1145/3372885.3373824.

[2] Grzegorz Bancerek et al. "The role of the Mizar Mathematical Library for interactive proof development in Mizar". In: *Journal of Automated Reasoning* 61.1 (2018), pp. 9–32. DOI: 10.1007/s10817-017-9440-6.

[3] Kenneth I Appel and Wolfgang Haken. *Every planar map is four colorable.* Vol. 98. American Mathematical Soc., 1989.

[4] Georges Gonthier et al. "Formal proof–the four-color theorem". In: *Notices of the AMS* 55.11 (2008), pp. 1382–1393.

[5] Paul Turán. "On an external problem in graph theory". In: *Mat. Fiz. Lapok* 48 (1941), pp. 436–452.

[6] Lawrence C Paulson. *Isabelle: A generic theorem prover.* Springer. DOI: 10.1007/BFb0030541.

[7] Tobias Nipkow, Lawrence C. Paulson and Markus Wenzel. *Isabelle/HOL — A Proof Assistant for Higher-Order Logic.* Springer, December 12, 2021. URL: http://isabelle.in.tum.de/doc/tutorial.pdf.

[8] Martin Aigner and Günter M. Ziegler. "Turán's graph theorem". In: *Proofs from THE BOOK.* Berlin, Heidelberg: Springer Berlin Heidelberg, 2018, pp. 285–289. ISBN: 978-3-662-57265-8. DOI: 10.1007/978-3-662-57265-8_41.

[9] Béla Bollobás. *Modern Graph Theory.* Vol. 184. Springer Science & Business Media, 1998. DOI: 10.1007/978-1-4612-0619-4.

[10] Reinhard Diestel. "Extremal Graph Theory". In: *Graph Theory.* Springer, 2017, pp. 173–207. DOI: 10.1007/978-3-662-53622-3_7.

[11] Willem Mantel. "Problem 28". In: *Wiskundige Opgaven* 10.60-61 (1907), p. 320.

[12] Martin Aigner. "Turán's graph theorem". In: *The American Mathematical Monthly* 102.9 (1995), pp. 808–816. DOI: 10.1080/00029890.1995.12004666.

[13] Paul Erdős. "On the graph theorem of Turán". In: *Mat. Lapok* 21.249-251 (1970), p. 10.

[14] Theodore S Motzkin and Ernst G Straus. "Maxima for graphs and a new proof of a theorem of Turán". In: *Canadian Journal of Mathematics* 17 (1965), pp. 533–540. DOI: 10.4153/CJM-1965-053-6.

[15] Noga Alon and Joel H Spencer. *The probabilistic method*. John Wiley & Sons, 2016.

[16] *Archive of formal proofs*. Accessed 19 May, 2022. URL: https://www.isa-afp.org/.

[17] Lars Noschinski. "Proof pearl: A probabilistic proof for the Girth-Chromatic number theorem". In: *International Conference on Interactive Theorem Proving*. Springer. 2012, pp. 393–404. DOI: 10.1007/978-3-642-32347-8_27.

[18] Lars Noschinski. "A Probabilistic Proof of the Girth-Chromatic Number Theorem". In: *Archive of Formal Proofs* (Feb. 2012). https://isa-afp.org/entries/Girth_Chromatic.html, Formal proof development. ISSN: 2150-914x.

[19] Lars Hupel. "Properties of Random Graphs – Subgraph Containment". In: *Archive of Formal Proofs* (Feb. 2014). https://isa-afp.org/entries/Random_Graph_Subgraph_Threshold.html, Formal proof development. ISSN: 2150-914x.

[20] Lars Noschinski. "Graph Theory". In: *Archive of Formal Proofs* (Apr. 2013). https://isa-afp.org/entries/Graph_Theory.html, Formal proof development. ISSN: 2150-914x.

[21] Christian Doczkal and Damien Pous. "Graph theory in Coq: Minors, treewidth, and isomorphisms". In: *Journal of Automated Reasoning* 64.5 (2020), pp. 795–825. DOI: 10.1007/s10817-020-09543-2.

[22] Ching-Tsun Chou. "A formal theory of undirected graphs in higher-order logc". In: *HOL Users' Group Workshop*. Springer. 1994, pp. 144–157. DOI: 10.1007/3-540-58450-1_40.

[23] Chelsea Edmonds, Angeliki Koutsoukou-Argyraki and Lawrence C. Paulson. "Szemerédi's Regularity Lemma". In: *Archive of Formal Proofs* (Nov. 2021). https://isa-afp.org/entries/Szemeredi_Regularity.html, Formal proof development. ISSN: 2150-914x.

[24] Bhavik Mehta and Yaël Dillies. "Formalizing Szemerédi's Regularity Lemma in Lean". International Conference on Interactive Theorem Proving, Not published yet. 2022.

[25] Chelsea Edmonds, Angeliki Koutsoukou-Argyraki and Lawrence C. Paulson. "Roth's Theorem on Arithmetic Progressions". In: *Archive of Formal Proofs* (Dec. 2021). https://isa-afp.org/entries/Roth_Arithmetic_Progressions.html, Formal proof development. ISSN: 2150-914x.

[26] Klaus F Roth. "On certain sets of integers". In: *J. London Math. Soc* 28.104-109 (1953), p. 3. DOI: 10.1112/jlms/s1-28.1.104.

[27] David Conlon and Jacob Fox. "Graph removal lemmas." In: *Surveys in combinatorics* 409 (2013), pp. 1–49. DOI: 10.1017/CBO9781139506748.002.

[28] JW Moon and L Moser. "On a problem of Turán". In: *Pabl. Math. Inst. Hungar. Acad. Sci* 7 (1962), pp. 283–286.

[29] Paul Erdős and Arthur H Stone. "On the structure of linear graphs". In: *Bulletin of the American Mathematical Society* 52.12 (1946), pp. 1087–1091. DOI: 10.1090/S0002-9904-1946-08715-7.

[30] Béla Bollobás and Paul Erdős. "On the structure of edge graphs". In: *Bull. London Math. Soc* 5.317-321 (1973), p. 31. DOI: 10.1112/blms/5.3.317.

Appendix A

Glossary of Isabelle/HOL definitions

card

Computes the cardinality of a finite set and returns *0* for infinite sets.

f ‘ S

Maps the function *f* to all elements of the set *S*.

fst (x,y)

Returns the first component *x* of the pair *(x,y)*.

snd (x,y)

Returns the second component *y* of the pair *(x,y)*.