Proof Pearl: A Probabilistic Proof for the Girth-Chromatic Number Theorem

Lars Noschinski

Technische Universität München, Institut für Informatik
noschinl@in.tum.de

Abstract. The Girth-Chromatic number theorem is a theorem from graph theory, stating that graphs with arbitrarily large girth and chromatic number exist. We formalize a probabilistic proof of this theorem in the Isabelle/HOL theorem prover, closely following a standard textbook proof and use this to explore the use of the probabilistic method in a theorem prover.

1 Introduction

A common method to prove the existence of some object is to construct it explicitly. The probabilistic method, which we explain below, is an alternative if an explicit construction is hard. In this paper, we explore whether the use of the probabilistic method is feasible in a modern interactive theorem prover.

Consider the Girth-Chromatic Number theorem from graph theory: Roughly, this states that there exist graphs without short cycles, which nevertheless have a high chromatic number (i.e., one needs a large number of colors to color the vertexes in a way such that no adjacent vertexes have the same color). On first glance, these properties seem contradictory: For a fixed number of vertexes, the complete graph containing all edges has the largest chromatic number. On the other hand, if the cycles are large, such a graph is locally acyclic and hence locally 2-colorable. This discrepancy makes it hard to inductively define a graph satisfying this theorem.

Indeed, the first proof of this theorem given by Erdős [14] used an entirely non-constructive approach: Erdős constructed a probability space containing all graphs of a certain order n. Using tools from probability theory he then proved that, for a large enough n, randomly choosing a graph yields a witness for the Girth-Chromatic Number theorem with a non-zero probability. Hence, such a graph exists. It took 9 more years before a constructive proof was given by Lovász [22].

This use of probability theory is known as *probabilistic method*. Erdős and Rényi are often considered the first conscious users of this method and developed it in their theory of Random Graphs [7, 15]. Other applications include Combinatorics and Number Theory. In this work, we explore how well this technique works in a modern theorem prover.

The well-known Girth-Chromatic Number theorem is one of the early applications of Random Graphs and often given as an example for applications for

the probabilistic method. The chromatic number of a graph is the minimal number of colors which is needed to color the vertexes in a way such that adjacent vertexes have different colors. Moreover, the girth g is the size of the shortest cycle in the graph. The Girth-Chromatic number theorem then states that for an arbitrary natural number ℓ there exists a graph G with both $\chi(G) > \ell$ and $g(G) > \ell$.

The proof we present here follows the one given in [11]. The Isabelle/HOL theory files containing our formalization can be found in the Archive of Formal Proofs [26].

The paper is structured as follows: Section 2 provides a brief introduction to Isabelle. Section 3 defines basic graph properties and operations and Section 4 introduces a probability space on graphs. In Section 5 we describe how we handle asymptotic properties. Section 6 gives a high-level description of the proof of the Girth-Chromatic Number theorem before our formalization of this proof is described in Section 7. We reflect on this formalization in Section 8 and review related work in Section 9. Section 10 concludes this paper.

2 Isabelle/HOL

Isabelle/HOL is an implementation of classical Higher Order Logic in the generic interactive theorem prover Isabelle [25]. We just write Isabelle instead of Isabelle/HOL throughout this paper. Formulas and terms are stated in standard mathematical syntax and 2^X denotes the power set of X. The term bound by a quantifier extends as far to the right as possible.

Lists are constructed from nil ($[]$) and cons ($\cdot$) and *hd* and *tl* decompose a list such that $\mathit{hd}(x \cdot xs) = x$ and $\mathit{tl}(x \cdot xs) = xs$.

3 Modeling Graphs

We consider undirected and loop-free graphs $G = (V, E)$ where V and E are sets of vertexes and edges, respectively. Edges are represented as sets of vertexes. For conciseness of presentation, we fix the vertexes to be a subset of $\mathbb{N}$. The graphs may be infinite, however usually we are only interested in finite graphs.

We use V_G and E_G to refer to the vertexes and edges of a graph G. The *order* of a graph is the cardinality of its vertex set. A graph is called *wellformed*, if every edge connects exactly two distinct vertexes of the graph. This is expressed by the following predicate:

$$\mathit{wellformed}(G) := (\forall e \in E_G.\, |e| = 2 \wedge (\forall u \in e.\, u \in V_G))$$

A *walk* is a sequence of vertexes of a graph, such that consecutive vertexes are connected by an edge. We represent walks as non-empty lists of vertexes and define the edge list of a walk recursively. The length of a walk (denoted by $||\cdot||$) is the length (denoted by $|\cdot|$) of its edge list. A cycle is represented as a walk of length at least 3 where first and last vertex are equal, but each other vertex

occurs at most once. Note that a cycle of length k is represented by $2k$ different walks.

$$\begin{aligned} \mathit{walk\text{-}edges}([]) &:= [] \\ \mathit{walk\text{-}edges}([x]) &:= [] \\ \mathit{walk\text{-}edges}(x \cdot y \cdot xs) &:= \{x, y\} \cdot \mathit{walk\text{-}edges}(y \cdot xs) \end{aligned}$$

$$||p|| := |\mathit{walk\text{-}edges}(p)|$$

$$\begin{aligned} \mathit{walks}(G) &:= \{p \mid p \neq [] \wedge \mathit{set}(p) \subseteq V_G \wedge \mathit{set}(\mathit{walk\text{-}edges}(p)) \subseteq E_G\} \\ \mathit{cycles}(G) &:= \{p \in \mathit{walks}(G) \mid ||p|| \geq 3 \wedge \mathit{distinct}(\mathit{tl}(p)) \\ &\qquad \wedge \mathit{hd}(p) = \mathit{last}(p)\} \end{aligned}$$

The girth g of a graph is the length of its shortest cycle; the girth of a graph without cycles will be denoted by ∞. As $\mathbb{N}_\infty$, the set of natural numbers extended with ∞, forms a complete lattice, we can define the girth of a graph as the infimum over the length of its cycles:

$$g(G) := \inf_{p \in \mathit{cycles}(G)} ||p||$$

A vertex coloring is a mapping of the vertexes of a graph to some set, such that adjacent vertexes are mapped to distinct elements. We are only interested in the partition defined by this mapping. The chromatic number χ is the size of the smallest such partition.

$$\begin{aligned} \mathit{colorings}(G) := \{C \subseteq 2^{V_G} \mid & \bigcup_{V \in C} = V_G \\ & \wedge (\forall V_1, V_2 \in C.\, V_1 \neq V_2 \Rightarrow V_1 \cap V_2 = \varnothing) \\ & \wedge (\forall V \in C.\, V \neq \varnothing \wedge (\forall u, v \in V.\, \{u, v\} \notin E_G))\} \end{aligned}$$

$$\chi(G) := \inf_{C \in \mathit{colorings}(G)} |C|$$

These definitions suffice to state the Girth-Chromatic Number theorem:

$$\exists G.\ \mathit{wellformed}(G) \wedge \ell < \chi(G) \wedge \ell < g(G)$$

However, we need a few auxiliary definitions; most notably the notion of an independent set and the independence number α.

$$\begin{aligned} E_V &:= \{\{u, v\} \mid u, v \in V \wedge u \neq v\} \\ \mathit{independent\text{-}sets}(G) &:= \{V \mid V \subseteq V_G \wedge E_V \cap E_G = \varnothing\} \\ \alpha(G) &:= \sup_{V \in \mathit{independent\text{-}sets}(G)} |V| \end{aligned}$$

Here, E_V is the set of all (non-loop) edges on V. We also write E_n for $E_{\{1,\ldots,n\}}$.

3.1 Removing Short Cycles

Besides the usual graph theoretic definitions, we will need an operation to remove all short cycles from a graph. For a number k, a short cycle is a cycle with length at most k:

$$\mathit{short\text{-}cycles}(G, k) := \{c \in \mathit{cycles}(G) \mid ||c|| \leq k\}$$

We remove the short cycles by repeatedly removing a vertex from a short cycle until no short cycle is left. To remove a vertex from a graph, all edges adjacent to this vertex are also removed.

$$\begin{aligned} G - u &:= (V_G \setminus \{u\}, E_G \setminus \{e \in E_G \mid u \in e\}) \\ \mathit{choose\text{-}v}(G, k) &:= \varepsilon_u(\exists p \in \mathit{short\text{-}cycles}(G, k).\ u \in p) \\ \mathit{kill\text{-}short}(G, k) &:= \mathsf{if}\ \mathit{short\text{-}cycles}(G, k) = \varnothing \\ &\qquad \mathsf{then}\ G\ \mathsf{else}\ \mathit{kill\text{-}short}(G - \mathit{choose\text{-}v}(G, k), k) \end{aligned} \tag{1}$$

To select an arbitrary vertex we use Hilbert's choice operator ε. Given a predicate P, this operator returns either some element satisfying P (if such an element exists) or an arbitrary element from the domain of P otherwise.

Equation (1) defines a recursive function which does not terminate on some infinite graphs. However, an (underspecified) function with this equation can easily defined by the `partial_function` command of Isabelle. To prove some properties about the graphs computed by *kill-short*, a specialized induction rule is useful.

Lemma 1 (Induction rule for *kill-short*). *Let k be a natural number. If for all graphs H both*

$$\mathit{short\text{-}cycles}(H, k) = \varnothing \Rightarrow P(H, k)$$

and

$$\begin{aligned} \mathit{finite}(\mathit{short\text{-}cycles}(H, k)) \wedge \mathit{short\text{-}cycles}(H, k) \neq \varnothing \\ \wedge P(H - \mathit{choose\text{-}v}(H, k)) \Rightarrow P(H, k) \end{aligned}$$

hold, then $P(G, k)$ holds for all finite *graphs G.*

The canonical induction rule would have $\mathit{finite}(H)$ as assumption for the second rule, but we strengthened the induction hypothesis with the additional assumption $\mathit{finite}(\mathit{short\text{-}cycles}(G, k))$ as it saves a little amount of work when we prove Lemma 4 below. With this induction rule, we can easily prove the following theorems about *kill-short* for finite graphs G:

Lemma 2 (Large Girth). *The girth of $\mathit{kill\text{-}short}(G, k)$ exceeds k, i.e.,*

$$k < g(\mathit{kill\text{-}short}(G, k))\ .$$

Lemma 3 (Order of Graph). *$\mathit{kill\text{-}short}(G, k)$ removes at most as many vertexes as there are short cycles, i.e.,*

$$|V_G| - |V_{\mathit{kill\text{-}short}(G,k)}| \leq |\mathit{short\text{-}cycles}(G, k)|\ .$$

Lemma 4 (Independence Number). *Removing the short cycles does not increase the independence number, i.e.,* $\alpha(\textit{kill-short}(G,k)) \leq \alpha(G)$.

Lemma 5 (Wellformedness). *Removing short cycles preserves wellformedness, i.e.,* $\textit{wellformed}(G) \Rightarrow \textit{wellformed}(\textit{kill-short}(G,k))$.

4 Probability Space

There are a number of different probability models which are commonly used for the analysis of random graphs. To prove the Girth-Chromatic number theorem, we consider a series of probability spaces $\mathcal{G}_n$ of graphs of order n, for n going to infinity. $\mathcal{G}_n$ consists of all graphs G with $V_G = \{1,\ldots,n\}$ and $E_G \subseteq E_n$. A randomly chosen graph $G \in \mathcal{G}_n$ contains an edge $e \in E_n$ with probability p_n. As V_G is fixed to $\{1,\ldots,n\}$, a graph $G \in \mathcal{G}_n$ is uniquely defined by its edges; so instead of a space of graphs $\mathcal{G}_n$, we define a space $\mathcal{E}_n$ of edge sets. This turns out to be slightly more convenient.

To define such a probability space in a canonical way, for each edge in E_n one defines a probability space on $\{0,1\}$, such that 1 occurs with probability p_n and 0 with probability $1-p_n$. Then, $\mathcal{G}_n$ is identified with the product of these probability spaces.

This construction is supported by Isabelle's extensive library on probability theory [17]. However, the elements of the product space of probability spaces are functions $2^{2^{\mathbb{N}}} \to \{0,1\}$ which are only specified on E_n. Identifying these with edge sets triggers some amount of friction in a theorem prover. To avoid this, we construct a probability space on edge sets without using the product construction. This is easily possible as $\mathcal{E}_n$ is finite for all n.

For the definition of $\mathcal{E}_n$, we consider the following. In the setting above, the probability that a randomly chosen edge set contains a fixed edge e is p_n; the probability of the negation is $1-p_n$. As the probabilities of the edges are independent, the probability that a randomly chosen edge set is equal to a fixed set $E \subseteq E_n$ is the product of the edge probabilities, i.e., $p_n^{|E|} \cdot (1-p_n)^{|E_n - E|}$.

Definition 6 (Probability Space on Edges). *Let* $n \in \mathbb{N}$ *and* $p \in \mathbb{R}$ *with* $0 \leq p \leq 1$. *Let* $f(E) = p^{|E|} \cdot (1-p)^{|E_n - E|}$ *for all* $E \in 2^{E_n}$. *Then* $\mathcal{E}_{n,p} = (2^{E_n}, \mathcal{P}_{n,p})$ *is the probability space whose domain consists of all the subsets of* E_n *and whose probability function is* $\mathcal{P}_{n,p}(X) = \Sigma_{E \in X} f(E)$ *for all* $X \subseteq E_n$. *When a function* $p : \mathbb{N} \to \mathbb{R}$ *is given from the context, we also write* $\mathcal{E}_n$ *and* $\mathcal{P}_n$ *instead of* $\mathcal{E}_{n,p_n}$ *and* $\mathcal{P}_{n,p_n}$.

Isabelle's probability library provides a *locale* [4] for probability spaces. One option to specify such a space is by a finite domain X and a function f with the following properties: For each $x \in X$ holds $0 \leq f(x)$ and we have $\sum_{x \in X} f(x) = 1$. When we show that those two properties hold in Def. 6, then Isabelle's locale mechanism transfers all lemmas about probability spaces to $\mathcal{E}_{n,p}$. We need in particular the following lemma:

Lemma 7 (Markov's Inequality). *Let $P = (X, \mu)$ be a probability space, $c \in \mathbb{R}$ and $f : X \to \mathbb{R}$ such that $0 < c$ and for all $x \in X$ holds $0 \leq f(x)$. Then*

$$\mu(\{x \in X \mid c \leq f(x)\} \leq 1/c \cdot \Sigma_{x \in X}(f(x) \cdot \mu\{x\}) \ .$$

To prove that $\mathcal{E}_{n,p}$ is an instance of the locale of probability spaces we need the lemma below.

Lemma 8 (Sum of Probabilities Equals 1). *Let S be a finite set. Then for all $p \in \mathbb{R}$ holds $\Sigma_{A \subseteq S}\left(p^{|A|} \cdot (1-p)^{|S-A|}\right) = 1$.*

A similar lemma describes the probability of certain sets of edge sets.

Lemma 9 (Probability of Cylinder Sets). *Let $\mathcal{E}_{n,p}$ be a probability space and $cyl_n(A, B) := \{E \subseteq E_n \mid (\forall x \in A.\ x \in E) \wedge (\forall x \in B.\ x \notin E)\}$ the set of all edge sets containing A but not B. Then $\mathcal{P}_{n,p}(cyl_n(A, B)) = p^{|A|} \cdot (1-p)^{|B|}$ for all disjoint $A, B \subseteq E_n$.*

5 Handling Asymptotics

As mentioned in Section 4, we consider a series of probability spaces, as the order grows towards infinity. In many cases, it suffices if a property P holds after some finite prefix, i.e., $\exists k.\ \forall n > k.\ P(n)$. Often, we can avoid dealing with these quantifiers directly. For example, to prove

$$(\exists k_1.\ \forall n > k_1.\ P(n)) \wedge (\exists k_2.\ \forall n > k_2.\ Q(n)) \Rightarrow \exists k_3.\ \forall n > k_3.\ R(n)$$

we can prove $\exists k.\ \forall n > k.\ P(n) \wedge Q(n) \Rightarrow R(n)$ or even just $\forall n.\ P(n) \wedge Q(n) \Rightarrow R(n)$ instead. However, such a rule would be inconvenient to use in practice, as proof automation tends to destroy the special form of the quantifiers. This can be prevented by using a specialized constant instead of the quantifiers. In Isabelle, such a constant (with suitable lemmas) is already available in the form of *filters* [8] and the *eventually* predicate. Filters generalize the concept of a sequence and are used in topology and analysis to define a general notion of convergence; they can also be used to express quantifiers [6]. In rough terms, a filter is a non-empty set of predicates closed under conjunction and implication and *eventually* is the membership test. We use *eventually* with the filter

$$\mathit{sequentially} := \{P \mid \exists k.\ \forall n > k.\ P(n)\}$$

as kind of a universal quantifier. This fits nicely Isabelle's definition of a limit:

$$\lim_{n \to \infty} f(n) = c \Rightarrow \forall \varepsilon.\ \mathit{eventually}\,((\lambda n.\ |f(n) - c| < \varepsilon), \mathit{sequentially})$$

The formula $\exists k.\ \forall n > k.\ P(n)$ is equivalent to $\mathit{eventually}(P, \mathit{sequentially})$. We will denote this as $\forall^\infty n.\ P(n)$ or write "$P(n)$ holds for large n". We mostly used the following three rules when dealing with this quantifier:

$$\frac{\forall n.\ k < n \Rightarrow P(n)}{\forall^\infty n.\ P(n)} \qquad (\textit{eventually-sequentiallyI})$$

$$\frac{\forall^\infty n.\ P(n) \quad \forall^\infty n.\ (P(n) \Rightarrow Q(n))}{\forall^\infty n.\ Q(n)} \qquad (\textit{eventually-rev-mp})$$

$$\frac{\forall^\infty n.\ P(n) \quad \forall^\infty n.\ Q(n) \quad \forall n.\ (P(n) \wedge Q(n)) \Rightarrow R(n)}{\forall^\infty n.\ R(n)} \qquad (\textit{eventually-elim2})$$

Apart from rule *eventually-sequentiallyI*, these hold for the *eventually* predicate in general. The rule *eventually-elim2* is actually just a convenience rule, which can be easily derived from the other two rules by dropping the condition $k < n$.

6 Proof Outline

We start with a high-level outline of the proof. Let ℓ be a natural number. A cycle c with $||c|| \leq \ell$ is called a *short cycle*. We recall the Girth-Chromatic Number theorem:

$$\exists G.\ \textit{wellformed}(G) \wedge \ell < \chi(G) \wedge \ell < g(G)$$

Instead of working with the chromatic number, we will work with the independence number α. Estimating probabilities for this number is easier, as an independent set is a cylinder set, cf. Lemma 9. The following lemma relates chromatic and independence number.

Lemma 10 (Lower Bound for $\chi(G)$). *For all graphs G, $|G|/\alpha(G) \leq \chi(G)$.*

The basic idea of the probabilistic proof of existence is to show that, for large enough n, choosing a random graph $G \in \mathcal{G}_n$ (respectively $E \in \mathcal{E}_n$) yields a graph with the desired properties with a non-zero probability.

A reasonable approach would be to choose the probability function p_n, such that we can show $\mathcal{P}_n\{G \mid g(G) < \ell\} + \mathcal{P}_n\{G \mid \alpha(G) > n/\ell\} < 1$. This would imply that a graph G satisfying neither $g(G) < \ell$ nor $\chi(G) < \ell$ exists, i.e., a graph satisfying the Girth-Chromatic number property. However, such a probability does not exist [11]. Instead, by choosing p_n correctly, we can show the weaker property

$$\mathcal{P}_n\{G \mid n/2 \leq |\textit{short-cycles}(G, \ell)|\} + \mathcal{P}_n\{G \mid 1/2 \cdot n/\ell \leq \alpha(G)\} < 1$$

and obtain a graph with at most $n/2$ short cycles and an independence number less than $1/2 \cdot n/\ell$ (i.e., $2\ell < \chi(G)$ by Lemma 10). From this graph, we remove a vertex from every short cycle. The resulting graph then has large girth and the chromatic number is still large.

7 The Proof

As a first step, we derive an upper bound for the probability that a graph has at least $1/2 \cdot n/k$ independent vertexes.

Lemma 11 (Probability for many Independent Edges). *Given $n, k \in \mathbb{N}$ such that $2 \leq k \leq n$, we have*

$$\mathcal{P}_n\{E \subseteq E_n \mid k \leq \alpha(G_{n,E})\} \leq \binom{n}{k}(1-p_n)^{\binom{k}{2}} \ .$$

Proof. Holds by a simple combinatorial argument and Lemma 9.

Lemma 12 (Almost never many Independent Edges). *Assume that $0 < k$ and $\forall^\infty n.\ 0 < p_n \wedge p_n < 1$. If in addition $\forall^\infty n.\ 6k \cdot \ln n/n \leq p_n$ holds, then there are almost never more then $1/2 \cdot n/k$ independent vertexes in a graph, i.e.,*

$$\lim_{n\to\infty} \mathcal{P}_n\{E \subseteq E_n \mid 1/2 \cdot n/k \leq \alpha(G_{n,E})\} = 0$$

Proof. With Lemma 11.

Then we compute the expected number of representatives of cycles of length k in a graph. Together with Markov's Lemma, this will provide an upper bound of $\mathcal{P}_n\{E \in \mathcal{E}_n \mid n/2 \leq |\mathit{short\text{-}cycles}(G_{n,E}, \ell)|\}$.

Lemma 13 (Mean Number of k-Cycles). *If $3 \leq k < n$, then the expected number of paths of length k describing a cycle is*

$$\left(\Sigma_{E\in\mathcal{E}_n} |\{c \in \mathit{cycles}(G_{n,E}) \mid k = ||c||\}| \cdot \mathcal{P}_n(\{E\})\right) = \frac{n!}{(n-k)!} \cdot p^k$$

We arrive at our final theorem:

Theorem 14 (Girth-Chromatic Number). *Let ℓ be a natural number. Then there exists a (wellformed) graph G, such that $\ell < g(G)$ and $\ell < \chi(G)$:*

$$\exists G.\ \mathit{wellformed}(G) \wedge \ell < g(G) \wedge \ell < \chi(G)$$

To prove this, we fix $p_n = n^{\varepsilon-1}$ where $\varepsilon = 1/(2\ell)$ and assume without loss of generality that $3 \leq \ell$. These assumptions hold for all of the following propositions. With Lemma 13, we can derive an upper bound for the probability that a random graph of size n has more than $n/2$ short cycles:

Proposition 15.

$$\forall^\infty n.\ \mathcal{P}_n\{E \subseteq E_n \mid n/2 \leq |\mathit{short\text{-}cycles}(G_{n,E}, \ell)|\} \leq 2(\ell-2)n^{\varepsilon\ell-1}$$

As this converges to 0 for n to infinity, eventually the probability will be less than 1/2:

Proposition 16.

$$\forall^\infty n.\ \mathcal{P}_n\{E \subseteq E_n \mid n/2 \leq |\textit{short-cycles}(G_{n,E}, \ell)|\} < 1/2$$

Similarly, with these choices, the conditions of Lemma 12 are satisfied:

Proposition 17.

$$\forall^\infty n.\ \mathcal{P}_n\{E \subseteq E_n \mid 1/2 \cdot n/\ell \leq \alpha(G_{n,E})\} < 1/2$$

Therefore, the sum of these probabilities will eventually be smaller than 1 and hence, with a non-zero probability, there exists a graph with only few short cycles and a small independence number:

Proposition 18. *There exists a graph $G \in \mathcal{G}_n$ satisfying both $1/2 \cdot n/\ell > \alpha(G)$ and $n/2 > |\textit{short-cycles}(G, \ell)|$.*

By removing the short cycles, this graph will be turned into a witness for the Girth-Chromatic Number theorem. This completes the proof of Theorem 14.

Proposition 19. *Let G be a graph obtained from Lemma 18. Then the graph $H := \textit{kill-short}(G, \ell)$ satisfies $\ell < g(H)$ and $\ell < \chi(H)$. Moreover, H is well-formed.*

Proof. By Lemmas 2–5 and 10.

Actually, we almost proved an even stronger property: The probabilities in Propositions 16 and 17 converge both to 0, so almost all graphs satisfy the condition of Proposition 18. Hence, almost every graph can be turned into a witness for the Girth-Chromatic Number theorem by removing the short cycles. This is typical for many proofs involving the probabilistic method.

8 Discussion

In this work, we formally proved the Girth-Chromatic Number theorem from graph theory, closely following the text book proof. The whole proof consists of just 84 theorems (1439 lines of Isabelle theories), split into three files and is therefore quite concise. Around 41 of these lemmas are of general interest, reasoning about reals with infinity and some combinatorial results. Partly, these have been added to the current developer version of Isabelle. Moreover, 18 lemmas are given about basic graph theory and the core proof of the theorem consists of the remaining 25 lemmas (around 740 lines). For the core proof, we mostly kept the structure of the text book proof, so auxiliary propositions only needed for one lemma are not counted separately.

The result looks straight-forward, but there are some design choices we like to discuss. In an early version of this formalization, we represented edges by an explicit type of two-element sets. However, it turned out that this made some proof steps a lot more complicated: Isabelle does not support subtyping,

so defining a two-element-set type yields a new type disjoint from sets with a partial type constructor. When we need to refer to the vertexes connected by an edge, this partiality makes reasoning harder. This easily offsets the little gain (we only need wellformedness explicitly in two theorems) an explicit edge type gives in our setting.

One should note that our definition of the chromatic number is not as obviously correct as it appears from the first glance: For an infinite graph G, $\chi(G) = 0$. This is due to the standard definition of cardinality in Isabelle mapping infinite sets to 0. We decided not to care about this, as we only are interested in finite graphs (and our final theorem assures a positive chromatic number anyway).

The main reason we decided to use $\mathbb{N}_\infty$ instead of $\mathbb{N}$ was to be able to give a natural definition of the girth – without infinity, we would need an extra predicate to handle the "no cycles" case. A nice side effect is that α and χ are easier to handle, as we do not have to care about emptyness or finiteness to evaluate infimum and supremum. However, as a result of this choice, we need to deal with real numbers including infinity ($\mathbb{R}_\infty$, with $\pm\infty$). If this had not been already available as a library, it would probably have been easier to avoid infinity altogether and special case the girth of acyclic graphs.

Our use of *eventually* turned out to be quite rewarding. For the proofs for Lemma 12 and the propositions for Theorem 14 we quite often collect a number of facts holding for large n and eliminate them like in Section 5. This made for more elegant proofs, as we needed less bookkeeping for (mostly irrelevant) explicit lower bounds.

Now, which capabilities are needed to use the probabilistic method in a theorem prover? Obviously some amount of probability theory. Different fragments of probability theory are now formalized in many theorem provers, including HOL4, HOL-light, PVS, Mizar and Isabelle [12, 17, 18, 21, 23]. Surprisingly, for the proof presented here, not much more than Markov's Inequality is required. For other proofs, more stochastic vocabulary (like variance and independence) is needed.

If one makes the step from finite to infinite graphs (for example to prove the Erdős-Rényi theorem that almost all countably infinite graphs are isomorphic [13, 27]), infinite products of probability spaces are required. To our knowledge, the only formalization of these is found in Isabelle [17].

Furthermore, good support for real arithmetic including powers, logarithms and limits is needed. Isabelle has this, but proving inequalities on complex terms remains tedious as often only very small proof steps are possible. However, the calculational proof style [5] (inspired by Mizar) is very helpful here.

In the future, an automated reasoner for inequalities over real-value functions like MetiTarski [1] might be useful. However, the set of a few example inequalities from our proof which L. Paulson kindly tested for us is still outside the reach of MetiTarski.

9 Related Work

Proofs with the probabilistic method often lead to randomized algorithms. Probably the first formalization in this area is Hurd's formalization of the Miller-Rabin primality test [19]; other work on this topic is available in Coq [3]. A constructive proof of a theorem similar to the Girth-Chromatic Number theorem was formalized by Rudnicki and Stewart in Mizar [28].

There are a few general formalizations of graph theory available in various theorem provers, for example [9, 10, 20]; but often proof developments rather use specialized formalizations of certain aspects of graph theory [16, 24] to ease the proof. For the Girth-Chromatic Number theorem, the common definition of graphs as pairs of vertexes and edges seems quite optimal. Even though, we did not find the lack of a general graph theory in Isabelle to be a major obstacle: The Girth-Chromatic Number theorem does not rely on any deep properties about graphs and the formalization of graphs we give here is rather straight-forward.

10 Conclusion

We gave a concise (and, to our knowledge, the first) formal proof for the well-known Girth-Chromatic Number theorem and explored the use of the probabilistic method in theorem provers, which worked well for this theorem. It will be interesting to see whether this continues to hold true for more involved theorems. An interesting example for this could be Lovász Local Lemma: Many probabilistic proofs show not only that the probability is non-zero, but even that it tends to 1 for large graphs. The Local Lemma can be used to show that a property holds with a positive, but very small probability. This enables some combinatorical results, for which no proof not involving this lemma is known [2].

Acknowledgments. We thank the anonymous reviewers for their feedback and pointing us to [10].

References

1. Akbarpour, B., Paulson, L.: Metitarski: An automatic theorem prover for real-valued special functions. JAR 44, 175–205 (2010)
2. Alon, N., Spencer, J.H.: The Probabilistic Method. Wiley (2000)
3. Audebaud, P., Paulin-Mohring, C.: Proofs of randomized algorithms in Coq. Science of Computer Programming 74(8), 568–589 (2009)
4. Ballarin, C.: Interpretation of Locales in Isabelle: Theories and proof contexts. In: Proc. MKM. LNAI, vol. 4108, pp. 31–43. Springer (2006)
5. Bauer, G., Wenzel, M.: Calculational reasoning revisited - an Isabelle/Isar experience. In: Proc. TPHOLs. LNCS, vol. 2152 (2001)
6. van Benthem, J.F.A.K., ter Meulen, A.G.: Generalized quantifiers in natural language. de Gruyter (1985)
7. Bollobás, B.: Random Graphs. Academic Press (1985)

8. Bourbaki, N.: General Topology (Part I). Addison-Wesley (1966)
9. Butler, R.W., Sjogren, J.A.: A PVS graph theory library. Tech. rep., NASA Langley (1998)
10. Chou, C.T.: A formal theory of undirected graphs in higher-order logic. In: TPHOLs. LNCS, vol. 859, pp. 144–157. Springer (1994)
11. Diestel, R.: Graph Theory, GTM, vol. 173. Springer, 4 edn. (2010)
12. Endou, N., Narita, K., Shidama, Y.: The lebesgue monotone convergence theorem. Formalized Mathematics 16(2), 171–179 (2008)
13. Erdős, P., Rényi, A.: Asymmetric graphs. Acta Mathematica Hungarica 14, 295–315 (1963)
14. Erdős, P.: Graph theory and probability. Canad. J. Math. 11(11), 34–38 (1959)
15. Erdős, P., Rényi, A.: On random graphs I. Publ. Math. Debrecen 6, 290–297 (1959)
16. Gonthier, G.: A computer-checked proof of the Four Colour Theorem (2005)
17. Hölzl, J., Heller, A.: Three chapters of measure theory in Isabelle/HOL. In: Proc. ITP. LNCS, vol. 6898, pp. 135–151 (2011)
18. Hurd, J.: Formal Verification of Probabilistic Algorithms. Ph.D. thesis, University of Cambridge (2002)
19. Hurd, J.: Verification of the Miller-Rabin probabilistic primality test. JLAP 50(1–2), 3–21 (2003)
20. Lee, G., Rudnicki, P.: Alternative graph structures. Formalized Mathematics 13(2), 235–252 (2005), formal proof development
21. Lester, D.R.: Topology in PVS: continuous mathematics with applications. In: Proc. AFM. pp. 11–20. ACM (2007)
22. Lovász, L.: On chromatic number of finite set-systems. Acta Mathematica Hungarica 19, 59–67 (1968)
23. Mhamdi, T., Hasan, O., Tahar, S.: On the formalization of the lebesgue integration theory in HOL. In: Proc. ITP. LNCS, vol. 6172, pp. 387–402. Springer (2010)
24. Nipkow, T., Bauer, G., Schultz, P.: Flyspeck I: Tame graphs. In: Automated Reasoning (IJCAR 2006). LNCS, vol. 4130, pp. 21–35. Springer (2006)
25. Nipkow, T., Paulson, L.C., Wenzel, M.: Isabelle/HOL — A Proof Assistant for Higher-Order Logic, LNCS, vol. 2283. Springer (2002), updated version: http://isabelle.in.tum.de/dist/Isabelle2011-1/doc/tutorial.pdf
26. Noschinski, L.: A probabilistic proof of the girth-chromatic number theorem. In: The Archive of Formal Proofs. http://afp.sf.net/entries/Girth_Chromatic.shtml (Feb 2012), formal proof development
27. Rado, R.: Universal graphs and universal functions. Acta Arithmetica 9, 331–340 (1964)
28. Rudnicki, P., Stewart, L.: The Mycielskian of a graph. Formalized Mathematics 19(1), 27–34 (2011)