The Fundamental Theorem of Asynchronous Distributed Models in Intuitionistic Logic

Li, Kwing Hei

August 25, 2023

1 Introduction

This document is a follow-up exploration of the results obtained in the author's MPhil report, which can be found in the link `https://hei411.github.io/projects/solvability.html`. Think of this as an epilogue of the MPhil report.

This report is not exactly self-contained and should not be read as a standalone, as various definitions are not presented here. The author encourages his readers to first familiarize themselves with the terminologies and definitions found in the original MPhil report, especially in chapters 2 and 3. Reading the proofs of the MPhil report (chapter 4) would also be helpful in enabling the readers in understanding and appreciating the motivations of this article.

Recall the Fundamental Theorem of Asynchronous Distributed Models[1]:

Theorem 1.1 (Fundamental Theorem of Asynchronous Distributed Models)**.** Given task description Θ and solvability property P, Θ is P-solvable under the non-layered model for Γ_{Fair} traces, iff there exists a full-information δ-protocol that P-solves Θ under the layered model for $\Gamma_{k\text{-It+IS}}$ traces for some $k \in \mathbb{N}$.

As emphasized in the original report, this is a very strong result, since it establishes an *equivalence* in solvability power between the two models, i.e. GMT's [7] and HKR's [8] model, respectively. A distributed task that is solvable by one model implies it can be solved by the other.

It is even more interesting if we attempt to interpret this result in intuitionistic logic, a stronger system than classical logic. To prove this theorem in intuitionsitic logic, we actually need to construct two compilers that transforms protocols from one model to another, and vice versa, that preserves the solvability property. As a result, if we have a protocol of one model that solves a task, we know exactly how to *effectively* construct the other protocol of the second model that also solves the same task. This begs the question, **does the original proof of the Fundamental Theorem hold in intuitionistic logic**?

The answer to the above question is: almost, but not quite. The proofs of all the intermediate propositions are indeed constructive, with the exception of one, the proof of the Layered $\Gamma_{\text{It+IS}}$ to layered $\Gamma_{k\text{-It+IS}}$ proposition (labelled 4.12 in Figure 1). This is somewhat disappointing since in this case, the original

[1] If you cannot recall this result, this probably meant you have not read the MPhil report yet:)

proof of the Fundamental Theorem does not hold in intuitionstic logic simply because of a single proposition out of many.

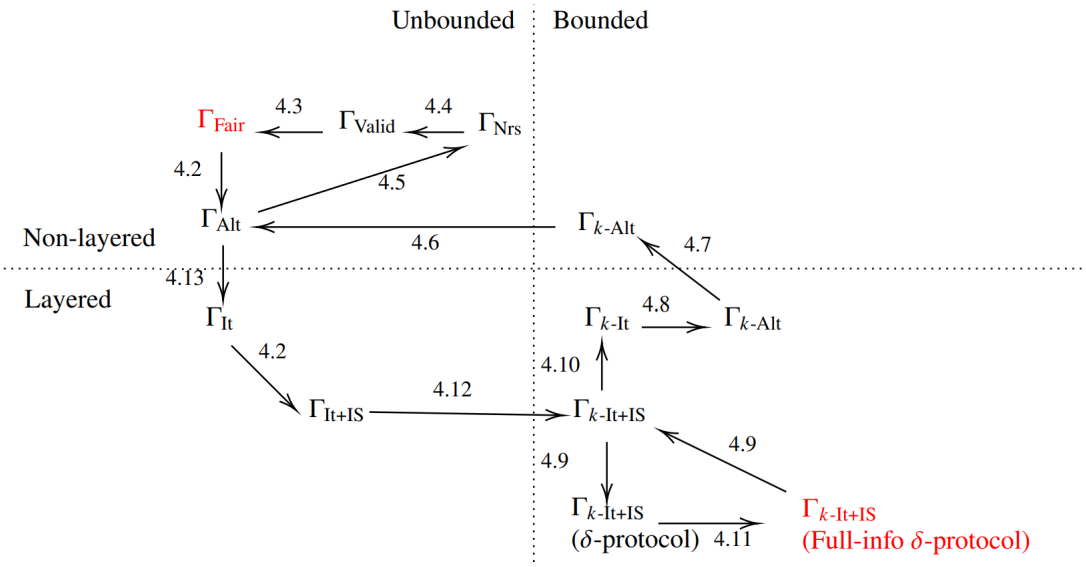

Figure 1: Proof sketch of the Fundamental Theorem of Asynchronous Distributed Models (taken from the MPhil report)

In this report, we claim that the proof of Layered $\Gamma_{\text{It+IS}}$ to layered $\Gamma_{k\text{-It+IS}}$ proposition can indeed be strengthened to hold in intuitionistic logic. An immediate consequence of this novel change is that the **Fundamental Theorem of Asynchronous Distributed Models thus holds true in intuitionistic logic**, providing a satisfactory conclusion to this story.

In section 2, we revisit the proof for the Layered $\Gamma_{\text{It+IS}}$ to layered $\Gamma_{k\text{-It+IS}}$ proposition and discuss why it is not constructive. Then in section 3, we present the Decidable Fan Theorem, a result which we use for the new constructed proof. Section 4 contains the most important part of this article: the new constructive proof of the proposition. Finally, we discuss future directions of this research in section 6.

2 The Original Non-constructive Proof

In this section, we study the proof sketch for the Layered $\Gamma_{\text{It+IS}}$ to layered $\Gamma_{k\text{-It+IS}}$ proposition and discuss the non-constructive nature of the proof.

Recall the Layered $\Gamma_{\text{It+IS}}$ to layered $\Gamma_{k\text{-It+IS}}$ proposition:

Proposition 2.1 (Layered $\Gamma_{\text{It+IS}}$ to layered $\Gamma_{k\text{-It+IS}}$ proposition)**.** Given task description Θ and solvability property P, if Θ is P-solvable under the layered model for $\Gamma_{\text{It+IS}}$ traces, then there exists $k \in \mathbb{N}$ such that Θ is P-solvable under the layered model for $\Gamma_{k\text{-It+IS}}$ traces.

Intuitively, the key idea of the result states that if every infinite trace in $\Gamma_{\text{It+IS}}$ has a finite prefix that satisfies property P, we can find $k \in \mathbb{N}$ such that every infinite trace in $\Gamma_{\text{It+IS}}$ has a finite prefix, where each node executes at most k rounds, that satisfies property P. Another way of viewing this concept is that the proposition can be very roughly written into the following form:

$$(\exists \pi \in \mathbf{Pro}, \forall T \in \Gamma_{\text{It+IS}}, \exists k \in \mathbb{N}. \phi(\pi, T, k)) \Rightarrow \exists \pi \in \mathbf{Pro}, \exists k \in \mathbb{N}, \forall T \in \Gamma_{\text{It+IS}}. \phi(\pi, T, k)$$

where **Pro** denotes the set of protocols and $\phi(\pi, T, k)$ is the proposition stating that under the semantics of π, the prefix of T where each nodes executes at most k rounds satisfies the P solvability property. In other words, we are moving an $\exists$ quantifier before a $\forall$ quantifier. (By a similar reasoning, the converse of the Layered $\Gamma_{\text{It+IS}}$ to layered $\Gamma_{k\text{-It+IS}}$ proposition is indeed true! After all, pushing an $\exists$ quantifier behind a $\forall$ quantifier is trivial.)

The original proof sketch of this proposition goes as follows (with many details omitted):

Proof outline.

1. Assume protocol π P-solves Θ under the layered model for $\Gamma_{\text{It+IS}}$ traces. We claim that π also P-solves Θ under the layered model for $\Gamma_{k\text{-It+IS}}$ traces for some $k \in \mathbb{N}$.
2. Assume the contrary, that is for all $k \in \mathbb{N}$, π does not P-solve Θ after executing some trace in $\Gamma_{k\text{-It+IS}}$ and some input vector.
3. Construct a connected tree graph which each node represents a possible execution trace and input vector. A node is reachable from the root if π does not P-solve Θ under the execution trace and input vector represented from the node.
4. Show that this tree is infinite yet locally finite.
5. By König's lemma [5], the tree has an infinite path.
6. From that infinite path, find a trace in $\Gamma_{\text{It+IS}}$ which does not P-solve Θ under the semantics of π. Thus a contradiction.

□

Though we are able to effectively construct a resulting protocol in this proof (the same π in the assumption), this proof is not constructive since we are unable to effectively compute k. The non-constructive nature of the proof arises from two locations in the original proof. Firstly, we assume the law of excluded middle to produce a proof by contradiction from step 2. Secondly, we make use of König's lemma in step 5, where its proof is not constructive.

It turns out we can avoid both "failure modes" at the same time to produce a constructive proof. To do so, we make use of a result known as the Decidable Fan Theorem, which we describe in detail in the next section.

3 The Decidable Fan Theorem

In this section, we present various definitions and the statement of the Fan Theorem. We also state a variant of the result, which we use to build our constructive proof for the Layered $\Gamma_{\text{It+IS}}$ to layered $\Gamma_{k\text{-It+IS}}$ proposition.

We begin by presenting the background definitions. Consider a (possibly infinite, and even uncountable) set X. Given an infinite sequence $\alpha \in X^\omega$ and natural number m, let $\bar{\alpha}n$ be the finite sequence consisting of the first m elements of α. Consider set $B \subseteq X^*$. We say α m-bars B if $\bar{\alpha}m \in B$, and that α bars B if there exists m such that α m-bars B.

We also consider the following three properties of the subset B (where X can be deduced implicitely).

We say B is **decidable** iff for every finite sequence $u \in X^*$, we can constructively prove either $u \in B$ or $u \notin B$.

We say B is **barred** iff for every infinite sequence $\alpha \in X^\omega$, α bars B.

Lastly, we say B is **uniform** iff there exists $M \in \mathbb{N}$ where for every infinite sequence $\alpha \in X^\omega$, if α bars B, then α k-bars B for some $k \leq M$.

We use $\mathbb{B}$ to denote the set $\{0, 1\}$.

With the above definitions, we can now state the Decidable Fan Theorem [1]:

Theorem 3.1 (Decidable Fan Theorem)**.** For all $B \subseteq \mathbb{B}^*$, if B is decidable and barred, it is uniform.

We however do not use this original statement of the theorem, but a variant of it. This result is proven in the master thesis of Iosif Petrakis [9]. (Note we only present a simpler specialized version of Proposition 11.5 in the thesis).

Theorem 3.2 (Generalized Decidable Fan Theorem)**.** For all finite sets X and subsets $B \subseteq \mathbb{X}^*$, if B is decidable and barred, it is uniform.

To see why this theorem is intuitively true given the Decidable Fan Theorem, we can perform a binary encoding on the elements of X and build another decidable barred subset $B' \subseteq \mathbb{B}^*$. The uniformity of B' would also imply the uniformity of B.

We postpone the discussion of the proof of the Decidable Fan Theorem to section 5. In the next section, we rigorously prove the Layered $\Gamma_{\text{It+IS}}$ to layered $\Gamma_{k\text{-It+IS}}$ proposition using the Generalized Decidable Fan Theorem.

4 The New Constructive Proof

Before we present our proof, we revisit some useful lemmas from the MPhil report:

Lemma 4.1 (Trace extension lemma for layered models)**.** For all distributed tasks Θ, protocols $(\mathbb{V}, \pi)$, $l \in \mathbb{V}^n$, traces T, solvability properties P, if $P(l, \text{fst}(\llbracket T' \rrbracket_\pi(l, \lambda k.\bot^n))[\text{dead}(T) \leftarrow \bot], \text{dead}(T), \Theta)$ for some finite prefix T' of T, for all finite prefixes T'' of T satisfying $T' \leq T''$, then $P(l, \text{fst}(\llbracket T'' \rrbracket_\pi(l, \lambda k.\bot^n))[\text{dead}(T) \leftarrow \bot], \text{dead}(T), \Theta)$.

Lemma 4.2 (Committed value lemma for layered models)**.** For all protocols $(\mathbb{V}, \pi)$, $l \in \mathbb{V}^n$, $m \in \mathbb{N} \to \mathbb{V}^n$, finite numbered trace $T \in \mathbb{A}^{*+\omega}$, and $i \in [n]$, if we have $l[i] \in \mathbb{O}_\bot$, then $\text{fst}(\llbracket T \rrbracket_\pi(l, m))[i] = l[i]$.

We now present an alternate constructive proof of the Layered $\Gamma_{\text{It+IS}}$ to layered $\Gamma_{k\text{-It+IS}}$ proposition.

Proposition 4.3 (Layered $\Gamma_{\text{It+IS}}$ to layered $\Gamma_{k\text{-It+IS}}$ proposition (revisited))**.** Given task description Θ and solvability property P, if Θ is P-solvable under the layered model for $\Gamma_{\text{It+IS}}$ traces, then there exists $k \in \mathbb{N}$ such that Θ is P-solvable under the layered model for $\Gamma_{k\text{-It+IS}}$ traces.

Proof. Assume the protocol $(\mathbb{V}, \pi)$ P-solves Θ under the layered model for $\Gamma_{\text{It+IS}}$ traces. We claim that there exists $k \in \mathbb{N}$ such that $(\mathbb{V}, \pi)$ P-solves Θ under the layered model for $\Gamma_{k\text{-It+IS}}$ traces.

Let X be the disjoint union of $(\mathbb{I}^n_\perp \times \mathcal{P}([n]))$ and $\Gamma_{1\text{-It+IS}}$. We define the set $B \subseteq X^*$ as follows: A finite sequence $s \in X^*$ is in B iff at least one of the cases is true:

- The string s is not the empty string and the first element of $s \notin (\mathbb{I}^n_\perp \times \mathcal{P}([n]))$.
- The string s is not the empty string, and there exists an element other than the first element that is not in $\Gamma_{1\text{-It+IS}}$.
- The string s is of the form $(l, d) \cdot T_0 \dots T_{k-1}$ where $(l, d) \in (\mathbb{I}^n_\perp \times \mathcal{P}([n]))$ and $T_i \in \Gamma_{1\text{-It+IS}}$ for all $i \in [k]$ for some $k \in \mathbb{N}$ and $\text{dead}(T_0 \dots T_{k-1}) \not\subseteq d$.
- The string s is of the form $(l, d) \cdot T_0 \dots T_{k-1}$ where $(l, d) \in (\mathbb{I}^n_\perp \times \mathcal{P}([n]))$ and $T_i \in \Gamma_{1\text{-It+IS}}$ for all $i \in [k]$ for some $k \in \mathbb{N}$ and $T_0 \dots T_{k-1} \notin \Gamma_{k\text{-It+IS}}$.
- The string s is of the form $(l, d) \cdot T_0 \dots T_{k-1}$ where $(l, d) \in (\mathbb{I}^n_\perp \times \mathcal{P}([n]))$ and $T_i \in \Gamma_{1\text{-It+IS}}$ for all $i \in [k]$ for some $k \in \mathbb{N}$, and $[\![T_0 \dots T_{k-1}]\!]_\pi[d \leftarrow \perp] \in \mathbb{O}^n_\perp$.

Lemma 4.4. X is finite.

This is obvious since $(\mathbb{I}^n_\perp \times \mathcal{P}([n]))$ and $\Gamma_{1\text{-It+IS}}$ are finite sets.

Lemma 4.5. B is decidable.

This is true since each of the above cases can be effectively checked for any finite string $s \in X^*$.

Lemma 4.6. B is barred.

Consider infinite sequence $\alpha \in X^\omega$. We show that α bars B by case analysis. The only interesting case is when α is of the form $(l, d) \cdot T_0 T_1 \dots$ where $(l, d) \in (\mathbb{I}^n_\perp \times \mathcal{P}([n]))$ and $T_i \in \Gamma_{1\text{-It+IS}}$ for all $i \in \mathbb{N}$, $T_0 T_1 \cdots \in \Gamma_{\text{It+IS}}$, and that $\text{dead}(T_0 T_1 \dots) \subseteq d$. Let $d' = \text{dead}(T_0 T_1 \dots)$.

By assumption, there exists prefix T' of $T_0 T_1 \dots$ such that $P(l, [\![T']\!]_\pi(l, \lambda k.\perp^n)[d' \leftarrow \perp], d', \Theta)$. By the Trace extension lemma for layered models, there exists $m \in \mathbb{N}$ such that $P(l, [\![T_0 \dots T_{m-1}]\!]_\pi(l, \lambda k.\perp^n)[d' \leftarrow \perp], d', \Theta)$ (as long as $T' \leq T_0 \dots T_{m-1}$).

Note that $(l, d)T_0 \dots T_{m-1}$ is a prefix of α so it suffices to prove that $(l, d)T_0 \dots T_{m-1}$ is in B. We do so by proving $[\![T_0 \dots T_{m-1}]\!]_\pi(l, \lambda k.\perp^n)[d \leftarrow \perp][i] \in \mathbb{O}_\perp$ for all $i \in [n]$ by case analysis.

- $i \in d$**:** We have $[\![T_0 \dots T_{m-1}]\!]_\pi(l, \lambda k.\perp^n)[d \leftarrow \perp][i] = \perp \in \mathbb{O}_\perp$ as required.
- $i \notin d$**:** We have:

$$
\begin{aligned}
& [\![T_0 \dots T_{m-1}]\!]_\pi(l, \lambda k.\perp^n)[d \leftarrow \perp][i] \\
&= [\![T_0 \dots T_{m-1}]\!]_\pi(l, \lambda k.\perp^n)[i] && (i \notin d) \\
&= [\![T_0 \dots T_{m-1}]\!]_\pi(l, \lambda k.\perp^n)[d' \leftarrow \perp][i] && (i \notin d \text{ and } d' \subseteq d) \\
&\in \mathbb{O}_\perp && (\text{type of } P)
\end{aligned}
$$

By the Generalized Decidable Fan Theorem (see section 3), B is uniform, that is there exists k such that for every infinite sequence $\alpha \in X^\omega$, if α bars B, it k'-bars B for some $k' \leq k$. We now claim that $(\mathbb{V}, \pi)$ P-solves Θ under the layered model for $\Gamma_{k\text{-It+IS}}$ traces.

Consider arbitrary input vector $l \in \mathbb{I}_\perp^n$ and trace $T \in \Gamma_{k\text{-It+IS}}$. Note that there exists infinite trace $T_a \in \Gamma_{\text{It+IS}}$ such that $T \leq T_a$ and $\text{dead}(T) = \text{dead}(T_a)$. This can be easily done by extending many rounds of immediate snapshots performed by alive nodes onto T. Consider the infinite string $\alpha = (l, \text{dead}(T_a))T_a \in X^\omega$. Since B is uniform, we must have a finite prefix $\beta \leq \alpha$ which is in B and is of the form $(l, \text{dead}(T_a))T_0 \ldots T_{k'-1}$ where $k' \leq k - 1 \leq k$ and that $[\![T_0 \ldots T_{k'-1}]\!]_\pi(l, \lambda k.\perp^n)[\text{dead}(T_a) \leftarrow \perp] \in \mathbb{O}_\perp^n$. It suffices to prove that $P(l, [\![T_0 \ldots T_{k'-1}]\!]_\pi(l, \lambda k.\perp^n)[\text{dead}(T) \leftarrow \perp], \text{dead}(T), \Theta)$.

Recall that $T_a \in \Gamma_{\text{It+IS}}$, so by our assumption, there exists a prefix $T'_a \leq T_a$ such that $P(l, [\![T'_a]\!]_\pi(l, \lambda k.\perp^n)$ $[\text{dead}(T_a) \leftarrow \perp], \text{dead}(T), \Theta)$. Since we have $\text{dead}(T) = \text{dead}(T_a)$, it suffices to prove $[\![T'_a]\!]_\pi(l, \lambda k.\perp^n)$ $[\text{dead}(T_a) \leftarrow \perp] = P(l, [\![T_0 \ldots T_{k'-1}]\!]_\pi(l, \lambda k.\perp^n)[\text{dead}(T) \leftarrow \perp]$. Regardless of whether $T'_a \leq T_0 \ldots T_{k'-1}$ or $T_0 \ldots T_{k'-1} \leq T'_a$, we can easily use the Committed value lemma for layered models to establish this equality, which completes the proof.

□

5 Discussion

In the previous section, we presented a new proof to the Layered $\Gamma_{\text{It+IS}}$ to layered $\Gamma_{k\text{-It+IS}}$ proposition. Note that all steps in this proof are trivially constructive, except for one small detail: the use of the Generalized Decidable Fan Theorem. Therefore, a natural question arises: **does the Generalized Decidable Fan Theorem hold in intuitionistic logic?**

The short answer is yes, as the theorem follows from bar induction [2], a reasoning principle in intuitionistic logic. Here we present the principle for completeness:

Definition 5.1 (Bar induction)**.** Given two predicates R and S of type $\mathcal{P}(\mathbb{N}^*)$, suppose the following conditions hold:

1. R is decidable.
2. Every infinite sequence $\alpha \in \mathbb{N}^\omega$ has a finite prefix satisfying R
3. Every finite string satisfying R also satsifies S.
4. Given finite string v, if $v \cdot i$ is in S for all $i \in \mathbb{N}$, v satisfies S.

then it follows that S holds for the empty list ϵ.

A careful reader might also notice that the original and new proofs are very similar in structure. For example, both involves building a tree-like structure where we non-deterministically choose an input vector and a set of dead nodes in the first branch and the infinite execution trace for the rest. The main difference is instead of König's lemma, we make use of the Generalized Decidable Fan Theorem in our new proof to make sense of the graph. This is actually not a coincidence. The Decidable Fan Theorem is actually the classical contra-positive form of the weak König's lemma [3], which we state here for completeness:

Theorem 5.1 (Weak König's lemma)**.** A subtree of a binary tree is infinite iff it contains an infinite path.

Intuitively, in the original proof, we use the König's lemma to show that the negation of our proposition leads to a contradiction. In the new one, we avoid this double negation by directly applying the Decidable Fan Theorem, which also enables us to derive a constructive proof in the process.

6 Conclusion and Future Directions

In this report, we presented a constructive proof of the Layered $\Gamma_{\text{It+IS}}$ to layered $\Gamma_{k\text{-It+IS}}$ proposition. As a result, we found the missing piece of the puzzle and have the following elegant result as a consequence:

Theorem 6.1 (Constructive Fundamental Theorem of Asynchronous Distributed Models)**.** The Fundamental Theorem of Asynchronous Distributed Models holds in intuitionistic logic.

We conclude by highlighting a few possible lines of research.

Currently, the Fundamental Theorem only exists in pen and paper. An ambitious project would be to formalize the result completely in a proof assistant. This would significantly increase our confidence in the correctness of the theorem, especially those of the more sophisticated intermediate propositions (e.g. the arrows labelled as 4.10 and 4.13 in Figure 1). We can also rigorously prove the claim that the theorem indeed holds entirely in intuitionistic logic.

Moreover, the author noticed that the concept "compactness" appears in various sources during the writing of this article. To start with, it is well-known that a variant of the Decidable Fan Theorem (see section 3) is equivalent to saying that the Cantor space is compact as a topological space [4]. There is also another paper that briefly mentioned that a result similar to the Layered $\Gamma_{\text{It+IS}}$ to layered $\Gamma_{k\text{-It+IS}}$ proposition can be proved using a compactness argument [6]. Unfortunately, the authors of the paper refused to elaborate this point any further and did not even provide a proof to their claim. It would be interesting to study whether one can define the executions of various asynchronous distributed models as a topology, and study whether these models are related to compactness in topology or in logic systems.

Acknowledgements

This work was primarily motivated by Marcelo Fiore's face of disgust, disapproval, and disappointment upon learning about the use of the law of excluded middle in the original proof. The author is grateful to Angus Matthews for enlightening discussions about the Decidable Fan Theorem and transfinite induction.

References

[1] L. Brouwer. Über definitionsbereiche von funktionen. *Mathematische Annalen*, 97:60–75, 1927.

[2] L. Brouwer and A. Heyting. *L. E. J. Brouwer collected works: Philosophy and foundations of mathematics*. Number 1. North-Holland, 1975.

[3] M. Dummett. *Elements of Intuitionism*. Oxford University Press, New York, 1977.

[4] M. P. Fourman and J. M. E. Hyland. *Sheaf models for analysis*, pages 280–301. Springer Berlin Heidelberg, Berlin, Heidelberg, 1979.

[5] M. Franchella. On the origins of Dénes König's infinity lemma. *Archive for History of Exact Sciences*, 51(1):3–27, 1997.

[6] E. Gafni, P. Kuznetsov, and C. Manolescu. A generalized asynchronous computability theorem. *CoRR*, abs/1304.1220, 2013.

[7] E. Goubault, S. Mimram, and C. Tasson. Geometric and combinatorial views on asynchronous computability. *Distributed Computing*, 31(4):289–316, Aug. 2018.

[8] M. Herlihy, D. Kozlov, and S. Rajsbaum. Distributed computing through combinatorial topology. In *Distributed Computing Through Combinatorial Topology*. Morgan Kaufmann, Boston, 2014.

[9] I. Petrakis. Brouwer's fan theorem, December 2010. Available at `https://www.math.lmu.de/~petrakis/Master%20Thesis.pdf`.