

20/10/2025 - First meeting to establish project scope & begin familiarisation of the topic area.

- Project is personal, so research the most interesting areas!
  - Explore the importance of Validity in different areas, e.g. Cryptography
  - Explore the need to define words precisely, e.g. Security.
  - Explore the need to ensure everything is there; how can computers help formalise.
  - What proof assistants exist, what are their differences, how do they work, etc.
  - Explore popular articles, research papers, news, etc.
- Needham & Schaefer: Exploiting logical errors in proof
- Lean, Coq, PVS (used in NASA)

27/10/2025 - Second meeting to discuss admin. points, e.g. best contact times.

- Best time to meet & email? Mon PM Wed PM
- E-logbook?
- Complete research plan ASAP.

28/10/2025 - Outline research plan, sections 1, 3, 6-11

29/10/2025 - Complete research plan, section 2

- Needham-Schaefer Protocol (1978) & Gavin Lowe (1995) Formal Proof
- Fair-Thompson (1963) → Microsoft/Infra
- \$475 million Intel division bug
- Other examples include NASA/AWS

31/10/2025 - Complete literature survey & 6-15 references.

- Applied Logic for Computer Scientists: Computational Deduction and Formal Proof Springer, 2017.
  - Proof assistants: history, ideas and future, Sankhara, Vol. 34, pp 3-25, 2009.
  - A machine-assisted proof of Gödel's incompleteness theorems for the theory of hereditary finite sets, Review of Symbolic Logic, Vol. 7, no. 3, pp 484-488, 2014
  - Introduction to Mathematical Logic, 6th ed., CUP Press, 2015.
- & references to check/avoid:

- Lean/Coq System descriptions.
- Landmark formalisations - Fair-Thompson, Four Colours.
- Type theory foundations.
- Writing-edible Lean applications.
- Historical case study?
- Cryptographic protocol verification.

03/11/2025 - Cancelled meeting, as not requested (Still exploring references, etc.)

- Clarified fortnightly → weekly meeting recurrence
- Research plan agreed to be sent on Wednesday
- Logbook continued by supervisor by email during meetings.

05/11/2025 - Begin reading through sources to short-list referenc.

17/11/2025 - Mutually cancelled meeting, but adjust research plan deadline. } Less work done throughout reading weeks focusing on reading.

19/11/2025 - Completed literature survey and finding references.

- Skipped books listed in research plan, using techniques taught in personal tutoring.
- Wrote summaries & link to project.

24/11/2025 - Meeting to discuss research plan, learning Lean, and underlying Maths.

24/11/2025 20:21/3

- How do proof assistants work (Applied Logic for Computer Scientists.)
- Make my own??

Dec/Jan

No meetings due to scheduling, illness, or holiday. Intermittent work completed due to holiday/exams. Mostly research summarised here:

-