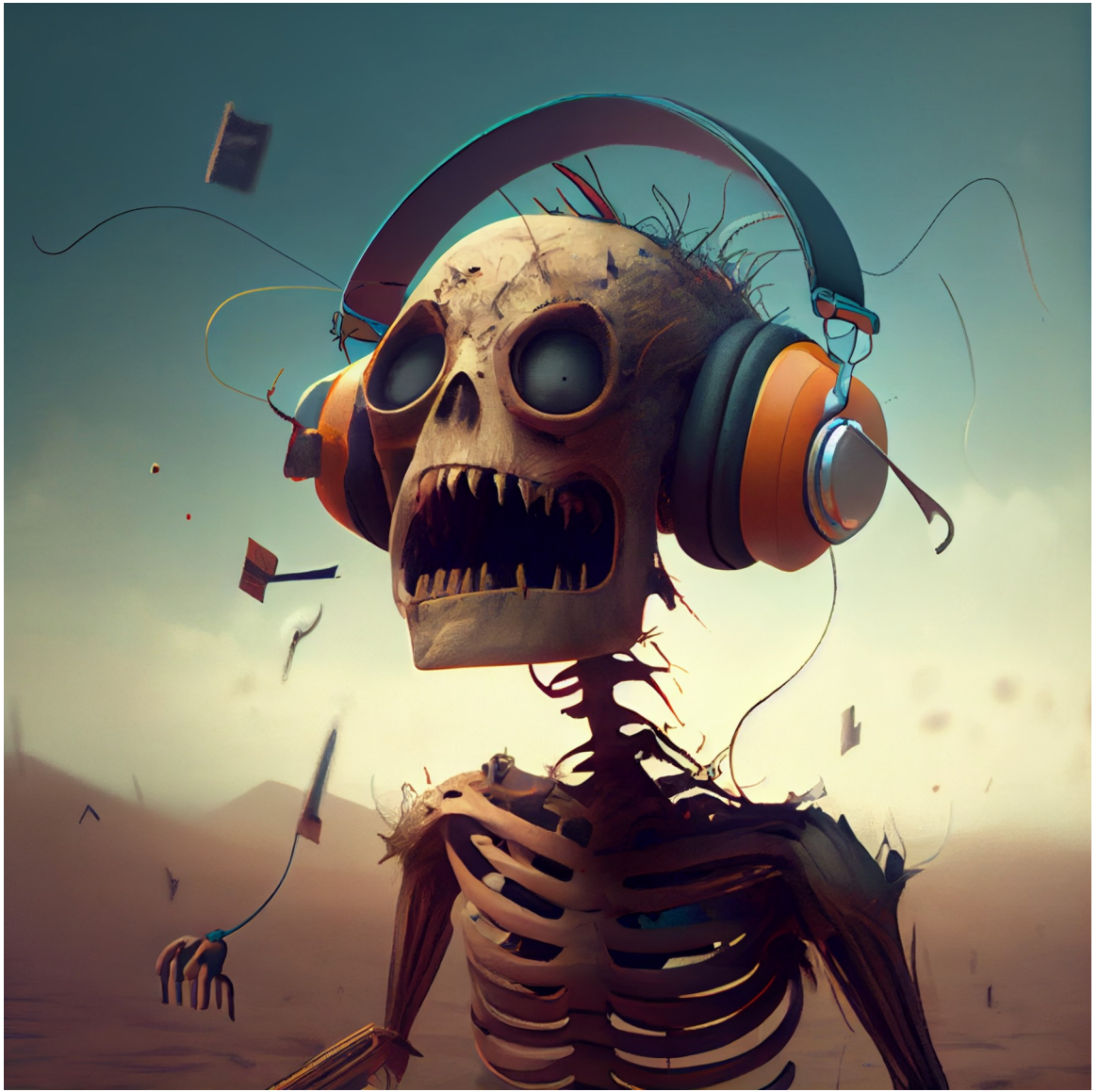
Unsound

Unsound 2022

Sources of Unsoundness in Verification

All the images are made with midjourny



Verification

- Software and proof verification has grown significantly in the last 15 years.
  Growth has come to the point where verification systems are complex and manually proving the soundness of those verification systems sometimes exceeds what a single research group can understand and verify as correct.
- Even formally defining soundness can be challenging and its definition is varying from system to system.

Verification

- Specific research groups can have very specific notions of soundness they focus on.
- Those can diverge from what the users expect!
  - especially if the users come from a different verification environment
  - or they are approaching verification for the first time.

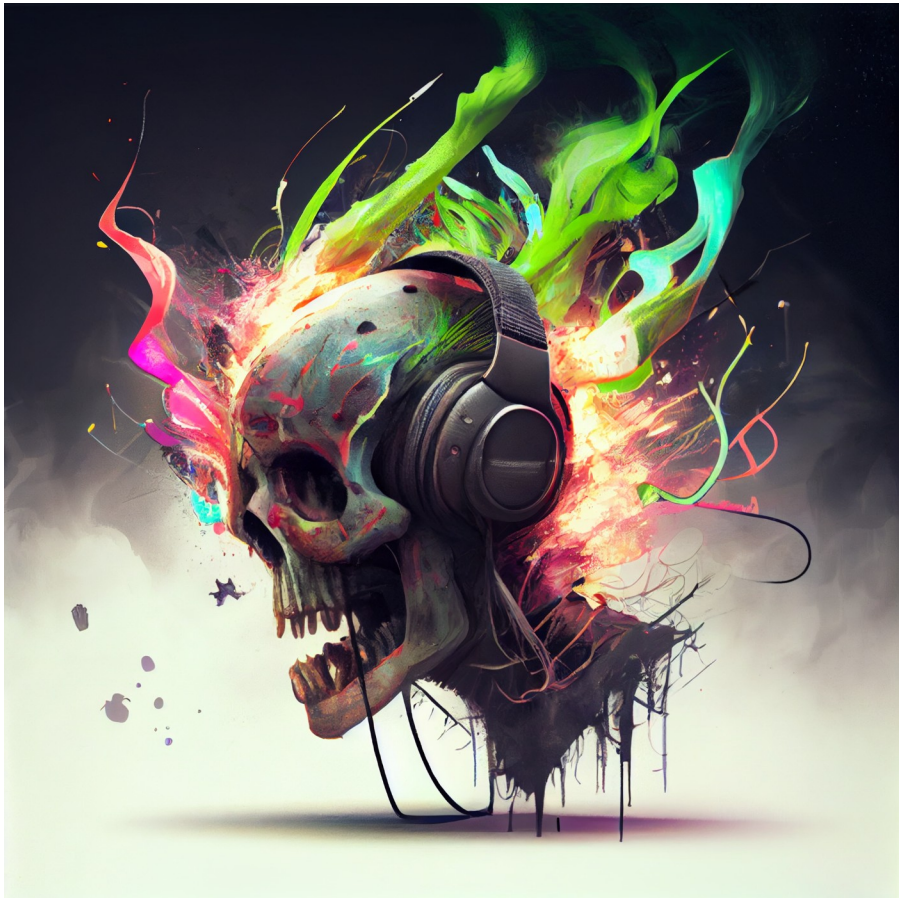
Join us!

- Participants to Unsound will be able to share their experience and exploits on how different verification tools can either be broken or expose confusing behavior, likely to be unexpected by users.
- We think this would be greatly beneficial not only because it will help all of us to iron out those unsoundnesses but also because it will facilitate understanding of the foundational differences between the assumptions of the various research lines.

Publishing negative results

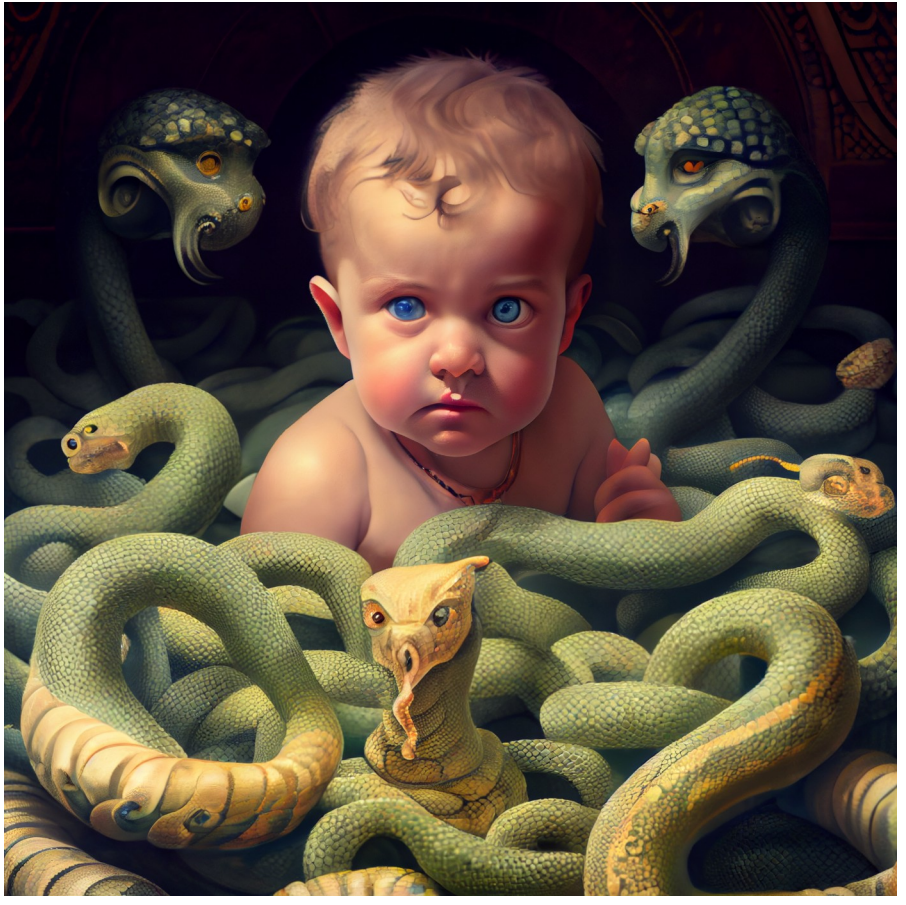
- The current academic environment encourages us to talk about the success case of our work.
  In this workshop we want to address and learn from failure cases and we want to reinforce the bedrock of our understanding.

- In practice, when we divert our focus to a specific aspect of verification we may (understandably) be less precise.
  For example, a line of research focusing on aliasing control in OO may be less precise when considering the implication in other areas, like termination.



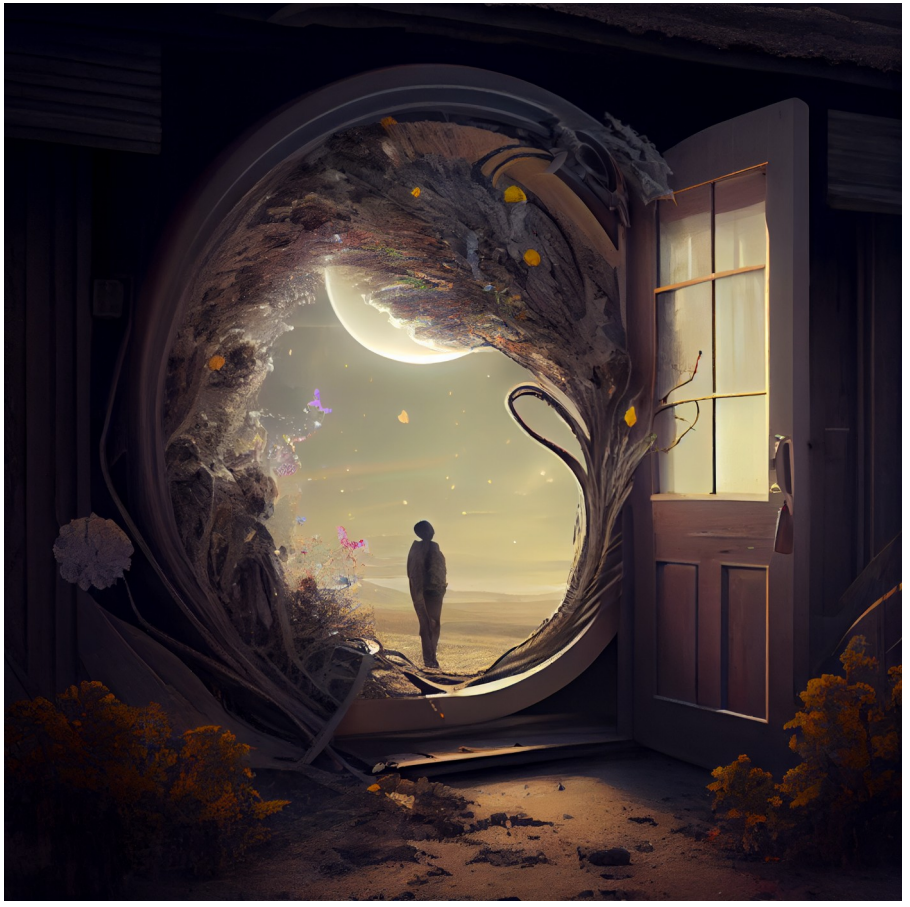
The new generations

- We believe that this environment would be particularly beneficial for young researchers that are in search of open questions in verification. This may provide a motivation to deep dive into the details of any particular tool, or to expand their individual area of expertise to get a wider and more objective and critical view of the whole area of verification.
- We also wonder if in our fast expansion we accidentally glossed over some fundamental issue in verification, and if our mistake has now become engraved into the established wisdom and it is sometimes uncritically assumed as a valid reasoning stepping stone.



Welcome!

- We are particularly interested in sources of unsoundness that are accidentally shared by many different unrelated research lines, and to develop an understanding on why this is the case.
- This is the first instance of Unsound!
- It is meant to be welcoming for both people with strong theoretical skills, as well as people who just like hacking things.



Schedule

Tue 6 Dec

Displayed time zone: **Auckland, Wellington** change

09:00 - 10:00 **Welcome and Invited Talk at Seminar Room G125** — Unsound

Add Session Information

Now — 09:00 — 15m — *Day opening* — ☆ **Welcome to Unsound**
Marco Servetto Victoria University of Wellington, Jan Bessai Independent

in 14 min — 09:15 — 45m — *Talk* — ☆ **What do we mean by "unsound"?** — VIRTUAL
Jan Bessai Independent

10:30 - 12:00 **Invited Talks at Seminar Room G125** — Unsound

Add Session Information

10:30 — 45m — *Talk* — ☆ **How to trust a verified program?** — VIRTUAL
Wouter Swierstra Utrecht University, Netherlands

11:15 — 45m — *Talk* — ☆ **MetaCoq as a tool to prevent future unsoundness in Coq** — VIRTUAL
Yannick Forster Inria

13:30 - 15:00 **Workshop Talks and Discussion at Seminar Room G125** — Unsound

Add Session Information

13:30 — 20m — *Talk* — ☆ **Proving False in Object Oriented Verification Programs by Exploiting Non-Termination**
Jaymon Furniss

13:50 — 45m — *Talk* — ☆ **The 4 horsemen of unsoundness in OO languages**
Marco Servetto Victoria University of Wellington

14:35 — 25m — *Panel* — ☆ **Discussion**
Marco Servetto Victoria University of Wellington