ZK Jargon Decoder - Live 📽 at ZK Hack IV

Format

- The ZK Jargon Decoder is a collection of (hopefully) simple definitions for common ZK terms. Scan the QR code!
- Live session:
    - we will define the terms *you* requested on X and *live* in the RingCentral chat.

"to prove"

- A statement is either `True` or `False`.
- Decision problems: "is this statement `True`?
  - **Statement 1**: the number 54 is even. ✅
  - **Statement 2**: the number 25890323 can be factored. 🤔
- Yes, Statement 2 is `True`! Here is my proof: $4567 \times 5669 = 25890323$

List of long mathematical proofs

1 language

Article Talk Read Edit View history Tools

From Wikipedia, the free encyclopedia

This is a list of unusually long mathematical proofs. Such proofs often use computational proof methods and may be considered non-surveyable.

As of 2011, the longest mathematical proof, measured by number of published journal pages, is the classification of finite simple groups with well over 10000 pages. There are several proofs that would be far longer than this if the details of the computer calculations they depend on were published in full.

Long proofs [edit]

The length of unusually long proofs has increased with time. As a rough rule of thumb, 100 pages in 1900, or 200 pages in 1950, or 500 pages in 2000 is unusually long for a proof.

- 1799 The Abel–Ruffini theorem was nearly proved by Paolo Ruffini, but his proof, spanning 500 pages, was mostly ignored and later, in 1824, Niels Henrik Abel published a proof that required just six pages.
- 1890 Killing's classification of simple complex Lie algebras, including his discovery of the exceptional Lie algebras, took 180 pages in 4 papers.
- 1894 The ruler-and-compass construction of a polygon of 65537 sides by Johann Gustav Hermes took over 200 pages.
- 1905 Emanuel Lasker's original proof of the Lasker–Noether theorem took 98 pages, but has since been simplified: modern proofs are less than a page long.
- 1963 Odd order theorem by Feit and Thompson was 255 pages long, which at the time was over 10 times as long as what had previously been considered a long paper in group theory.
- 1964 Resolution of singularities. Hironaka's original proof was 216 pages long; it has since been simplified considerably down to about 10 or 20 pages.
- 1966 Abyhankar's proof of resolution of singularities for 3-folds in characteristic greater than 6 covered about 500 pages in several papers. In 2009, Cutkosky simplified this to about 40 pages.

Can We Make Proofs Short and Easy to Verify?

- The problem of long proofs motivates the need for proofs that are **short** and **easy to verify**
- Interactive proofs
  - Like a detective interrogating a suspect: the verifier asks "questions" and checks that the prover "keeps her story straight".
- Probabilistic proofs
  - relax our requirements: it is ok to accept a wrong proof once in a while.
  - don't read the whole proof, just some parts of it!
- Combine both: IOP (interactive oracle proof)

Proof vs Argument

- Answers the question: "who are we protected against?"
- > **Proof:** the adversary has **unlimited computational power**.
- > **Argument:** the adversary has **bounded computational power**.
- (A proof is also an argument! But not the other way around.)

Soundness vs Knowledge Soundness

- Answers the question: "what does the system guarantee?"
- > **Soundness:** if an honest verifier accepts a proof, then **there exists** a witness that satisfies the instance.
- > **Knowledge Soundness:** if an honest verifier accepts a proof, then **the prover knows** a witness that satisfies the instance.
- (Knowledge soundness implies soundness! But not the other way around.)

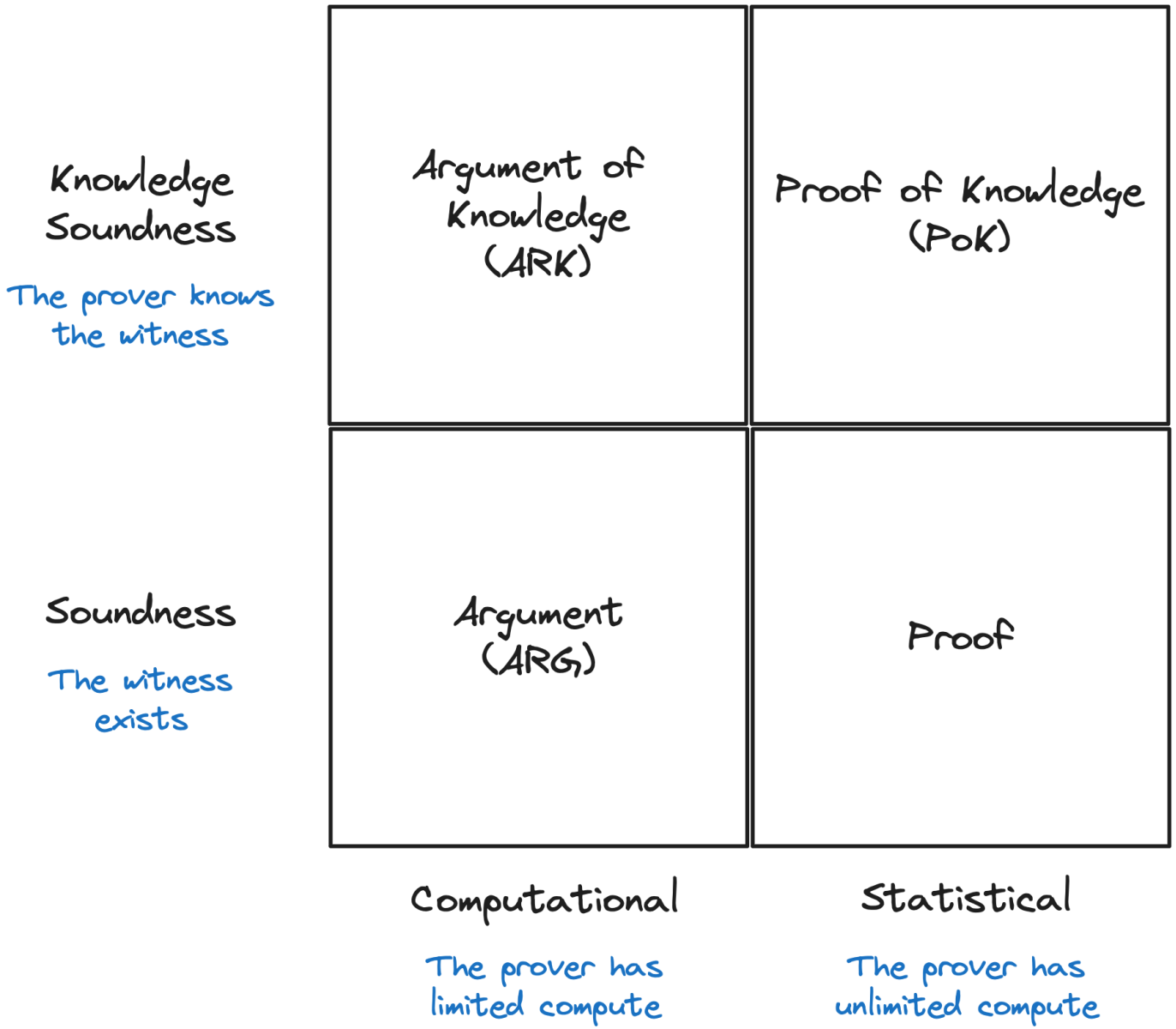
Soundness vs Knowledge Soundness: an example

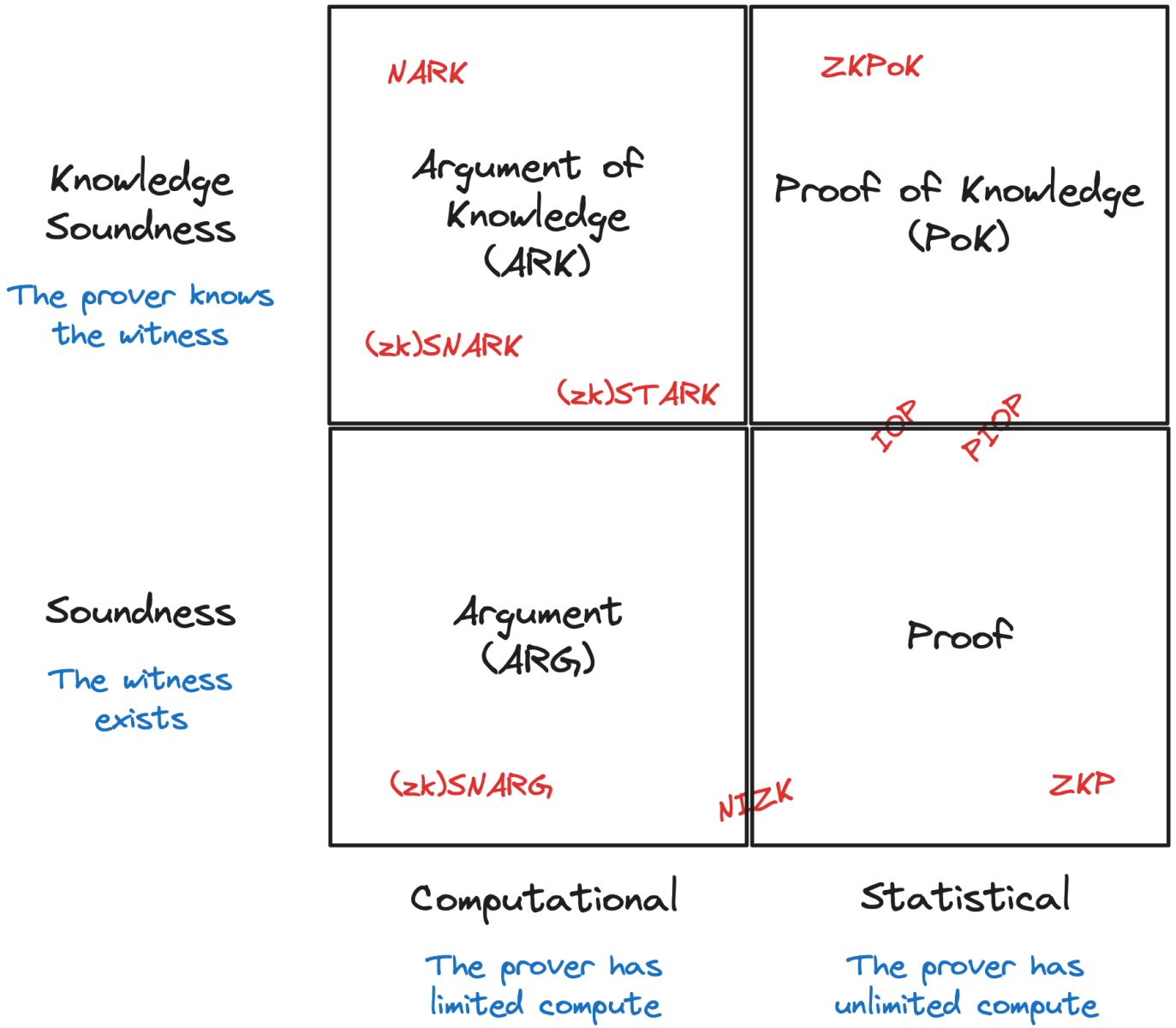
I want to prove that I know the private key x for some public key Y. A valid key pair should have $Y = g^x$ for some public generator g.

$$\text{Instance: } Y, g \qquad \text{Witness: } x$$

Do I need a protocol (proving system) with *soundness* or *knowledge soundness*?

- the witness (private key) *always exists*, independently of whether the prover knows it.
  - protocol is sound ➡️ *anyone* can make a proof that private key *exists*. ❌
  - protocol is knowledge sound ➡️ only parties that *know* the private key can make a valid proof. ✅


Knowledge Soundness
The prover knows the witness
Argument of Knowledge (ARK)
Proof of Knowledge (PoK)
Soundness
The witness exists
Argument (ARG)
Proof
Computational
The prover has limited compute
Statistical
The prover has unlimited compute


Knowledge Soundness
The prover knows the witness
Soundness
The witness exists
NARK
Argument of Knowledge (ARK)
(zk)SNARK
(zk)STARK
ZKPoK
Proof of Knowledge (PoK)
IOP
PIOP
Argument (ARG)
(zk)SNARG
NIZK
Proof
ZKP
Computational
The prover has limited compute
Statistical
The prover has unlimited compute

Sumcheck

- Refers to multiple things!
- > **Sumcheck** ("checking a sum"): A prover P commits to a vector/function and claimed sum `S`. P and V run an interactive protocol to convince V that the sum of all the elements in the vector/function is indeed `S`.
- > **Sumcheck** (the [LFKN92] protocol [1]): performs the "sumcheck" task described above for multi-variate polynomials.

1. Carsten Lund, Lance Fortnow, Howard Karloff, and Noam Nisan. 1992. Algebraic methods for interactive proof systems. J. ACM 39, 4 (Oct. 1992)

More Proving Jargon

Statement 2: the number 25890323 can be factored.

- 25890323 is the **instance**
- $(4567, 5669)$ is the **witness**
- the **relation** is: "a pair $(x, \texttt{list})$ such that the product of `list` is x".
- the **language** is the set of numbers that can be factored.
- the **predicate** is "the number _____ can be factored".

More Proving Jargon

Statement 2: the number 25890323 can be factored.

- 25890323 is the **instance** of the decision problem.
- $(4567, 5669)$ is the **witness** to the fact that the instance is in the language.
- the **relation** is: "a pair $(x, \texttt{list})$ such that the product of `list` is x".
- the **language** is the set of numbers that can be factored.
- the **predicate** is "the number _____ can be factored".