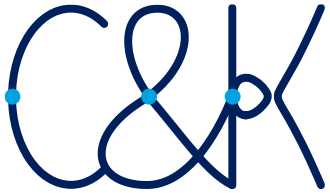
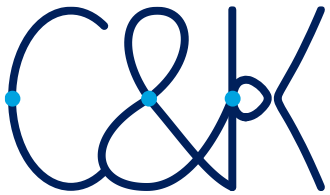
Howto: Seminar



Technical hints and resources



Software

- Word processor
  - We usually prefer LaTeX.
    - It's the de facto standard for theoretical computer science papers.
  - For technical essays (many definitions, formulas) we *definitely* recommend LaTeX.

- Presentation software
  - LaTeX Beamer for technical talks (many formulas).
  - Powerpoint/Keynote are also good options.

- Templates on our website.
  - LaTeX essays
  - Beamer/Powerpoint/Keynote presentations

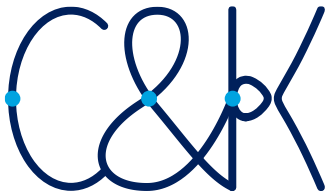
Where to find papers/information

PADERBORN UNIVERSITY

- You don’t know concept x mentioned in your paper?
  Use Google/Wikipedia.
  - Usually good for basic knowledge.
  - Usually bad for more advanced research.
  - *Don’t* cite it in your essay. Find proper (peer-reviewed) sources.

- Looking for peer-reviewed papers to read or cite?
  - scholar.google.com
  - Access restricted papers from within the University network (or use university’s VPN).
  - Conference papers are often incomplete. Look for *full* versions on arxiv.org or eprint.iacr.org.
  - Use BibTeX entries from Google Scholar or dblp.org.

How to work with sources



What's plagiarism?

- To *plagiarize* something:
  - *"to steal and pass off (the **ideas or words** of another) as one's own **:** use (another's production) without crediting the source"* [1]

- Punishment is severe.

- Solution is simple: cite your sources.

Even if you don't use a single word from the original paper, but **rephrase their ideas without attribution**, it's **still plagiarism**.

[1] Merriam-Webster dictionary "plagiarize". https://www.merriam-webster.com/dictionary/plagiarize. Retrieved on October 22nd, 2019

How to cite. Examples

- In literature overview:

> In 2018, Schmidt et al. proved that $\mathbf{P} \subseteq \mathbf{NP}$ [SFG97].

- Using facts of other papers for arguments:

> Since $\mathbf{P} \subseteq \mathbf{NP}$ [SFG97], this idea is also applicable to efficient deterministic computations.

- Re-stating parts of the paper:

> **Theorem 3** (Subset relation of P and NP. Theorem 1 in [SFG97]).
> $\mathbf{P} \subseteq \mathbf{NP}$

It's okay to keep the theorem formulation unchanged if convenient.

- Broad citation of ideas from a single paper (often the case for seminar essays):

> **2.4 Set theoretic relations**
>
> In this section, we take a closer look at the **P**/**NP** subset relation from [SFG97].
> ... *(no more mentions of the source from here on)*

Bibliography

(paper body)

...

Bibliography

[SFG97] Alexandra Schmidt, Leopold Fitz, Bill Gates. *Trivial Complexity Theory Statements*. TCC 1997, LNCS. Springer, Heidelberg, December 1997.

[Tur37] Alan M. Turing: *On Computable Numbers, with an Application to the Entscheidungsproblem*. Proceedings of the London mathematical society 2.1 (1937): 230-265.

Unusual/unnecessary citations

- Very unusual: direct quotations

> "The proof boils down to showing that every deterministic TM can be converted to an equivalent NTM." [SFG97]

Cite papers for ideas, not for words.

- No need to cite common knowledge

> $\mathbf{P}$ is the set of all languages that can be decided by a polynomial-time Turing machine [SFG97].

- No need for ultra-specific citations

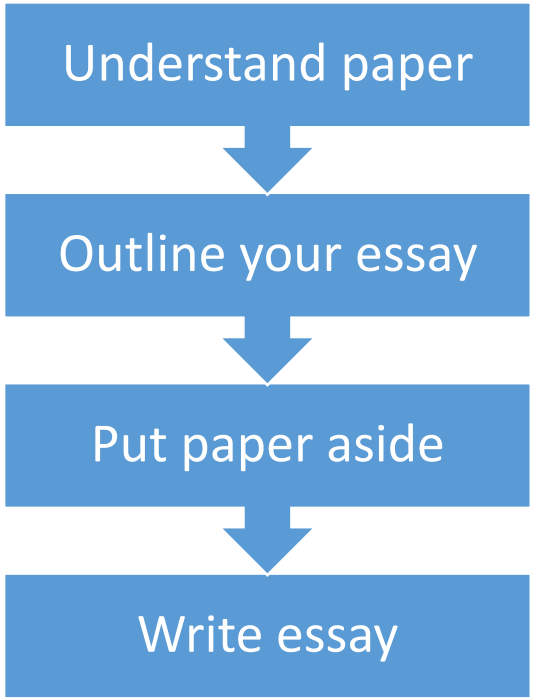
> If A and B are sets, we say that "A and B are *compatible*" if $A \cap B = \emptyset$ and $|A| = |B|$ **[Tur37]**.
> Furthermore, we say that "A is *better* than B" if $A \supseteq B$ or $|A| < |B|$ **[SFG97]**.
> Analogously, we define "A is *worse* than B" **[SFG97]**.

> **Our notation roughly follows [SFG97] and [Tur37].**
> If A and B are sets, we say that "A and B are *compatible*" if $A \cap B = \emptyset$ and $|A| = |B|$.
> Furthermore, we say that "A is *better* than B" if $A \supseteq B$ or $|A| < |B|$.
> Analogously, we define "A is *worse* than B".

Writing a good essay

How to approach writing – big picture

1. Read and **understand** the paper.
2. Create an **outline** of your essay.
   - What topics will be part of the essay? (check your ideas with your supervisor)
   - How do you want to structure the essay?
3. Put the **paper aside**.
4. Start **writing** essay content.
   - Explain the paper to your reader in your own words.
5. You notice you **haven't perfectly understood** yet?
   - First try to solve it yourself.
   - Stop writing. Consult the original paper (or other sources). Understand. Close the paper again. Resume writing.
   - Maybe spend a few *more* sentences on this problem in the essay.



Plagiarism light: Paraphrasing and parroting

PADERBORN UNIVERSITY

Original paper:

> Our anonymity definition follows a simulation approach. This means that we require existence of simulators that can simulate the user's role of the *show*, *issue*, and *update* protocols. For this, the input for the simulators is exactly the information that the issuer/verifier should learn from the interaction (plus a trapdoor to enable simulation).

Useless seminar essay 🤔 :

> The anonymity definition of [BBDE19] is defined through simulation. That means that there must exist simulators for the user's side of the show, issue, and update protocols. The simulator's input is the information that the issuer or verifier should learn from the protocol. Additionally, the simulator gets a trapdoor as input.

Same structure and content as original, just paraphrased.
⇒ *No* value, any reader could just have consulted the original.

Borderline plagiarism:
Citation is given (for the definition), but you're pretending that this minimally changed version of their explanation is your own thought.

How to do better

Original paper:

> Our anonymity definition follows a simulation approach. This means that we require existence of simulators that can simulate the user's role of the *show*, *issue*, and *update* protocols. For this, the input for the simulators is exactly the information that the issuer/verifier should learn from the [illegible]mulation).

Adds helpful explanation/background missing in original paper.

Good seminar essay:

> To define anonymity, [BDDE19] makes use of the *simulation paradigm*. In the following, we first discuss the ideas behind this paradigm. Then, we prove that simulation-based definitions guarantee security in an intuitive sense. Finally, we discuss design decisions of [BDDE19]'s definition.
> ...

Written in own words, without looking at the original paper.

Does not merely *present* the original paper's findings but *discusses* details.

Other ways how to improve upon the original paper

PADERBORN UNIVERSITY

Example ways to set your essay apart from the original paper:

- **Better explanations**: why is this definition/theorem/algorithm this way?
- **Better proofs**: Add further explanation to proofs
  - (or even write a proof they omitted)
- **Simplify**: Come up with simplified versions of X and explain how to get from simplified to full.
- **Related work**: Explain and compare related work
- **Examples**: Give concrete examples.
  - What's a useful application of Theorem 2?
  - How does this complicated algorithm work for simple inputs?

The presentation

Goal of the presentation

PADERBORN UNIVERSITY

Goal: Explain your topic to the other students

and show that you understand your topic well.

P and NP

Let the set $\mathbf{P}$ denote the set of all languages $L \subseteq \{0,1\}^*$ that can be decided by a deterministic Turing machine in polynomial time. Let $\mathbf{NP}$ denote the set of all languages that can be decided by a nondeterministic Turing machine in polynomial time. One can easily see that $\mathbf{P} \subseteq \mathbf{NP}$. This is because any deterministic Turing machine can simply be converted into a nondeterministic Turing machine that decides the same language with essentially the same runtime.

Don't put your *full* oral explanation on the slides

P and NP

- $\mathbf{P}$: languages decidable by poly-time **DTM**
- $\mathbf{NP}$: languages decidable by poly-time **NTM**

Bullet points instead of wall of text

Theorem

$$\mathbf{P} \subseteq \mathbf{NP}$$

Clean slide, listeners can easily follow

Proof idea: convert DTM into NTM

Guidelines from experience

- Rule of thumb: **2 minutes per slide**
  - Corollary: at most 25-30 slides in your talk.
  - Don’t overload slides.

- You talk about x for >10sec? Mention x on slide.

- More material than presentation time?
  Good: talk only about parts or simplifications, but explain these well.
  Bad: Rush through *everything* and all special cases while nobody understands.

Talking

- Practice!
  - Know what you want to say on each slide. Practice out loud.

- Have an obvious structure.

  Example. For each slide say:

  1. What are we talking about now? How does it relate to what happened before/will happen later?
  2. [Whatever you want to explain on this slide]
  3. What have we just talked about? What is the punchline/one-sentence summary?

Any questions?