Comments on
The Complexity of the Shortest Vector Problem

General Many of your Open Problems are things like *Prove that BLAH-SVP-BLAH is NP-hard*. Well—what if its not? I am NOT recommending that you make every open problem into *prove or disprove*. I am recommending that you, early on, say that for every open problem it is implicit that proving the opposite would also be interesting.

Section 1

1. Page 1. (no action required) You say that Lattice means 2 things. I think it means a lot more than that- I've seen it used for a variety of things- even in Prog Langs.

2. Page 1. The paragraph that begins 'As with any important...' you should make it more clear that the question Is in NPC or NPC to approx and What is the fine grained complexity

   are VERY DIFFERENT types of questions.

   Perhaps something like this:

   > As with any important computational problem, it is natural to ask about the *complexity* of SVP and GAPSVP. There are two different types of questions to ask. (1) Are these problems NP-hard? Which approximations of them are NP-hard? (2) What is the fine-grained complexity of SVP and $GAPSVP$. There are crypto systems based on GAPSVP being hard so that question is particularly interesting.

3. You might want to acknowledge me for inviting you to write this open problems column and/or for proofreading.

   I was curious if this was common so I looked at all of the columns that I was not a co-author on. all of those that had an ack section acknowledged me. Some didn't have an acknowledgment section.

Section 2.1

1. What does BKZ stand for? Since usually initials like that are peoples names, like in LLL, I was looking for a reference to, say, Borel-Kronecker-Zippel.

2. *Seventeen years after [vEB81]*

   A paper should still make sense if the citations were removed. You mostly DO follow this rule with sentences like.

   Ajtai [Agj98] largely resolved...

   In the case at hand:

   Seventeen years after van Emde Boas's paper [vEB81]

Section 2.2

1.

Section 2.3

1. In ordinary complexity the key is that you need to make hardness assumptions such as $P \neq NP$ or the Unique Game Conj. In fine-grained complexity you assume ETH or SETH. The beginning of Section 2.3 sounds like you are proving unconditional results. Add a brief comment that this kind of complexity does need assumptions, that you will get to later.

2. No change needed here. I had thought that Fine-Grained Complexity also includes assuming the 3SUM conjecture or the APSP conjecture. Is that correct, or is only ETH and SETH? Just curious. If I am right I don't see that it leads to a corrections unless you want to explicitly say that you will NOT be using those assumptions.

Section 3.1

No comments.

Section 3.2

No comments.

Section 3.3

No comments.

Section 3.4

1. In the second paragraph you refer to *Construction A*. I could not find where that was. If you label the construction with a number, like you do the theorems and lemmas and such, then it would be easy to find.

2. The first sentence of the third paragraph is not well written. You have:

   We conclude with two open problems that were originally asked by and would derandomize the constructions in [Mic98] and [BP22], respectively.

   When you say *that were originally asked by* I expect to see a name and citation (or just a name if there is no citation). Since the citation is already in the open problem I would suggest just saying:

   We conclude with two open problems.

   and then IN the open problem statement add why its important.

Section 4.1

1. Page 12. The word *things* is a bit to informal. So just omit *for these things*. It is understood.

2. Page 12. The second to last line. *a bit more complicated*. Its hard to quantify how much more complicated it is. Better to just write *more complicated*.

3. Page 13. Barriers to hardness, first line. You need a comma between γ and *then*.

4. Page 13. Protocols and reductions in super-polynomial time. Second line of that paragraph has several question marks where you want numbers.

5. Page 14. The paragraph beginning *Analogous to* has question marks where there should be

Section 4.2

1. Page 14 last line you have

   gives a reduction that for $\gamma \leq 1 + O(\log n/n)$ *runs in* ...

   Needs commas. Should be

   gives a reduction that, for $\gamma \leq 1 + O(\log n/n)$*, runs in* ...

2. Page 15. The section **Unique** SVP. The first sentence uses the word *variant* twice.

3. Page 15. Parameterized GapSVP. You have the expression $k := r^p$. I think you mean $k = r^p$.

4. Page 16. You refer to work as *recent* and *more recent*. You may want to give years instead so that when our robot overlords read this in the year 3000 they won't have to think about what *recent* means.

Section 4.3

1. Page 17. Bottom. You refer to Schnorr's result as 'recent'. The result is from 2021 and the column will appear in 2023. You may want to omit the word 'recent'

2. Open Problem Suggestions: show that (GAP)SVP is NOT reducible to Factoring or Discrete log since if it was then the whole crypto rational for SVP is gone.

3. Open Problem 4.11 Why the $n^{3/2+\epsilon}$ threshold?

4. Page 18. You ask for 'The fine grained hardness of Open Problem 2.6' This can't be quite right. You have the fine grained hardness of an open problem. You can have the fine grained hardness of a problem. Open problem 2.6 is SVP in the ℓ_2 norm. Is that the problem you are looking at?

Bibliography

1. AD17- lwe should be LWE

2. DPW19- svp should be SVP