

# 1 The New Plan

After meeting with Aram today, I decided to timebox my work on constant-depth factoring. For example, after taking some finite steps in the next day or two, concentrating exclusively on writing up what I do know and moving on. This will take a lot of willpower, but as a consolation, I can keep a list of concrete open problems to work on for later.

We did discuss the difficulty of making classical progress on purely classical results, especially ones that are old.

Here are the concrete steps:

1. See what other papers cited the ones by Bruck, especially after 1992, and see if any are more recent than the Hoyer-Spalek paper.
2. Ask Paul Beame if he knows of any results which are more recent.

These steps I could do even tonight. This one paper by Goldmann and Karpinski seems to contain an explicit construction for the simulation of an exponentially-weighted threshold gate by a polynomially-weighted one, proving an optimal / tight bound for the probabilistic construction. Is that enough? There are several mentions made that multiplication and division require exponentially large weights, and therefore a simulation step would be necessary to turn them into something implementable on a quantum computer.

We must fail softly. At least a day should be spent thinking what soft failure would look like, and outlining the sections in completing chapter one.

What are the things discussed in the meeting with Aram?

1. The fact that QFT can be performed in constant depth, but the modular multiplication part still is not known. However, there could be ways of doing it in the QFT domain, using unbounded quantum fanout and repeated multiplication (multiple product) and modular reduction, that don't rely on this classical circuit construction.
2. It is possible to construct a non-optimal constant-depth threshold circuit for multiple product, by clever creation of partial products. A good first step would be the multiplication of two  $n$ -bit numbers in constant-depth, by showing the creation of the partial products in constant-depth, and then using multiple sum.
3. It is possible to create a circuit for division by concentrating on reciprocal finding, and reducing reciprocal finding to multiplication of  $O(\log_2 n)$  terms. Using the  $(1 + y^{2^r})$  expansion from Kitaev's book, page 134.

It seems so doable. But I may need to do it alone.

## 2 Soft Failure

I outline the steps needed for... waiting the clock out. Let's concentrate on the division task from above. Even if I were to multiply the partial products from above in constant depth, how would I create them? Independently, for each term (I guess I should call them factors since I am multiplying them), I can raise  $y$  to a power, and then raise it to a power-of-two, which is equivalent to just bitshifting.

This task appears to be further increasing my sense of self. And I am unable to relax. The reason why I am unable to be with others, is because I feel threatened and cannot maintain my self-concept. As long as I am by myself, I can pretend that I am as smart or noble or generous as I want.

## 3 The Phases of Writing

1. Planning. This can be pleasant, in the sense that watching clouds or daydreaming is pleasant.
2. Things are a mess. You have started writing a bunch of disjointed segments, and you don't know how they fit together. You feel the pang of not even being able to write a stub section, or insert a TODO to create a graphic here for later.
3. Things have settled into a mostly established form, but you still feel the urge to rip out huge chunks and reorganize everything.
4. Obsessive re-editing of increasingly minute details and mistakes. This can feel extremely painful, in that you will judge yourself for not being able to make an end.
5. The end. This has stopped being painful. You know you are going to finish, and then you simply do it.

## 4 Skills That You Want To Learn

The practice of writing a thesis has some useful skills to teach that are not directly related to the technical content matter of the thesis itself. The first skill is how to overcome fear, and move forward while staying with any feelings of unworthiness, that somehow you have to work overwhelmingly hard in order to be good enough. This is difficult to say the least, since the majority of my motivation to do work comes from feeling bad. It is why I have to be careful about enjoyment or exercise making me feel too good, because then I won't feel bad enough about myself to continue doing whatever it is that I am doing.

A useful guide to the future would be that whatever I don't feel like doing after a great period of exercise, I should not be doing. Anything that requires

a great deal of extraordinary effort...well here it becomes tricky. Certainly things worth doing are often hard, and require sustained effort. Strong desire and purpose and connecting to higher values are needed in order to overcome moments of doubt. You could roughly call this perseverance. But when does it cross the line into forcing yourself? And isn't forcing yourself sometimes necessary? Isn't that what I'm doing now?

The second skill is mindfulness, of being able to recognize my process. My mindfulness right now says that I am procrastinating, so I will put a hold on this section.

But briefly, the third skill is free thinking. Creative acts are a mess. They are a jumble, and out of them you create something new, and polish it until it shines. But you have to be okay with the mess, and not retreat from it, otherwise you won't stick with it until the very end, when things seem easy or awesome or you begin to think you could maybe possibly good at this thing.

The fourth skill. How to relax. How to be productive in a relaxed way.