1 Settling Previous Questions

1. The relationship between majority gates and threshold gates are as follows. Threshold gates of polynomially-bounded weight can be simulated by (I think up to three layers of) threshold gates with unit weights, which can then be trivially simulated by majority gates. I think the only difference between the last two are that majority gates never have a bias, that is, the weight w_0. The reverse direction is trivial.

2. As Aram pointed out in our meeting, the $O(\log n)$ block size in the block-save adder is probably to polynomially bound the weights in the threshold circuit, something that I had not previously considered, but seems obvious in retrospect.

Okay that's it folks, move along.

2 The Overall 2D Layout

There are several intermediate results, such as the n^2-bit result of the multiple product, the quotient of this with the modulus m, which involves finding the reciprocal of m, the product of the quotient and the modulus, and the subtraction.

Using our model with modules, we can teleport / fanout copies to different modules and not worry about the exact geometry of the relationship between them.

3 To Do After These Pages Are Written

Deeper understanding of the Reif and Tate results are needed, but perhaps that can be delayed or deferred until after we have a final version of Chapter 1.

Soft failure can look like just using the results of Reif and Tate. But some deeper understanding is needed. For example, how to compute the reciprocal. This can be done using the expansion given in Kitaev, but then this reduces to creating the products in constant depth.

We don't necessarily need to use threshold gates to do this, since the Toffoli is much easier, and can still be made constant.

As pointed out in group meeting, David's reordering circuit could be used to rearrange the qubits, after being fanned out, into the right order. But we could do this in blocks. What are the size of the blocks? What *are* the blocks?

4 Creating Partial Product Bits

In this section, I will describe how the partial product creation I gave in my 2D factoring paper.

5 Multiple Product via Reif and Tate

In the 1992 paper by Reif and Tate, which appears to have appeared contemporaneously with a bunch of papers by Bruck, and so was not cited until a 1996 paper by Yeh and Varvarigos when the dust had settled, they address the question of multiple product. Actually it is multiple product modulo a number p, which as far as I can tell does not strictly have to be prime, or if it is prime, is a smaller prime and one chosen so it is bigger than the largest possible output number, so that no bits are truncated. It does not correspond to the number m, the modulus to be factored in Shor's factoring algorithm.

It remains to be seen whether I can use this or not. Yeh and Varvarigos seem to think so, as long as I choose p large enough. But then I need to do modular reduction.

6 The equivalence of threshold circuits to Z_p circuits

They can simulate each other in constant depth and polynomial increase in size. Certainly, this seems useful for the so-called "Chinese Remaindering" procedure, since we are dividing up a number into factors of this "mixed radix" where the weights never become exponential, but rather, remain of size $O(n)$, or at least polynomial.

7 Size and depth tradeoffs

Also from reading the Yeh-Varvarigos paper, I became aware of new parameters in threshold circuits, namely the tradeoff between size and depth. The size is never very critical for me, as long as it's polynomial, and surprisingly even with the parameter ϵ set to its maximum value, the size is never more than $O(n^2)$ and usually $O(n)$.

8 Sum of n bits

There is a construction given in Yeh-Varvarigos for the sum of n bits, which can then be used, I guess, for iterated sum, or multiple addition. At some point, hours need to be set aside for finding the exact construction for the building blocks that I am going to use.

For iterated addition, we can pretty much use the Siu-Bruck original construction. And time's up.

9 Explicit construction of simulation

The Goldmann and Karpinski paper showed an explicit construction for simulating threshold gates with exponential weights with those of polynomial size weights. This is in contrast to the probabilistic, existential, non-constructive proof given in the Siu-Bruck paper "On the Dynamic Range of Linear Threshold Elements." and one other paper where the division and multiplication functions are given.

I think this might be useful for lower bounds, or back when it was thought that multiplication and division required exponentially many terms. (Citation needed!)