From: Perlner, Ray A. (Fed)
To: (b) (6)
Subject: RE: more memory stuff
Date: Friday, September 24, 2021 4:02:00 PM

Hm. I'm not sure I follow your argument. The memory locations correspond to degree b monomials times minors, while the equations correspond to degree b-1 monomials times bigger minors. Maybe it's better to just use one level of hashing, but make the hash bigger so that the memory units deal with a smaller amount of memory. E.g. if you use a 40 bit hash, then the memory cost for the processing units for each hash is only 2^-16 times the original memory cost. Then you don't care if you have to send 102-bit addresses instead of 8 bit field elements. (Note: Blocking is easy once terms have been summed at the hash-indexed processing units.)

I think the cost relative to the formula the Rainbow response says it's using should be about (40*65/87)/8645*8/102 +110/102*2^-16 = ~2^-12, and relative to the values in the table, more like ~2^-14. Very close to what we were originally claiming.

From: Daniel Smith (b) (6)
Sent: Friday, September 24, 2021 12:43 PM
To: Perlner, Ray A. (Fed) <ray.perlner@nist.gov>
Subject: more memory stuff

Would you be able to take a look at the second level of hash argument I made? I haven't fit it together with the previous stuff yet. It seems to me that it should affect the previous number in a more subtle way, and not be an independent speedup.

I am going to have meetings and stuff the rest of the afternoon, just to let you know.