Notes for the write up

1. Fix the notations as provers, verifiers, in multiple provers no. of provers, size of the circuit.
2. In technical summary, sublinear verification is required to remove.
3. Citations
4. We should use prover and verifier as respectively.
5. Number of provers should be either N or p. it’s used interchangeably.
6. In soundness, existence of witness or knowledge of witness?
7. We are not having sublinear field operations for verification. Change in section 6
8. In section 6.2, what is N?
9. In section 6.2, linear check has mistake
10. In section 7.1, linear check with commitment oracle: what is k?
11. In the protocol for linear check, R^i polynomial should be for r^TA.
12. Why 2l? it should be k+l-1
13. Some clarification is required for verifier’s checks.
14. I don’t think bivariate code is appropriate terminology, we should use product code and bivariate polynomial
15. In 3D construction and were interchangeably. We should make it consistent.
16. In the proximity protocol for BIC, why we don’t need to send ?
17. Is there any relation between with ?
18. In linear check, polynomials should be formed by interpolating not from .
19. Why in the definition, , , not , in the linear check?
20. Where are we using in the linear check?
21. Why in the definition, , , not , in the quadratic check?
22. Why commitments upto ?

2D vs 3D

Cryptographic operations are less in 3D for verifier. For 2D and for 3D .