

- On slide 20: It really is necessary to consider a random matrix D , to ensure that we push the input vector away from the nullspace of the embedding. However, the construction can be derandomized to some extent. The entries of D need not be fully independent. In particular, they can be generated with $\text{polylog}(n)$ random bits.