On random window algorithm

Weilei Zeng
*Department of Physics & Astronomy, University of California, Riverside, California 92521, USA**
(Dated: July 13, 2020 **random-window-decoder)**

note on random window decoder

CONTENTS

I. INTRODUCTION

The random window algorithm can be used to quickly estimate an upper bound of the distance of an error correcting code. In most cases, the upper bound matches its actual distance. It was invented and named information set algorithm in [1, 2] and explained as covering set algorithm in [3].

Because a decoder return the closest codeword upon given input, it can also be used to esitimate the distance.

II. DISTANCE OF A BINARY CSS CODE

input: stabilzier generator G_X, G_Z with $G_X G_Z^T = 0$

solve for codeword generating matrix C_Z such that $G_X C_Z^T = 0$, $\mathrm{rank}(G_X) + \mathrm{rank}(G_Z) + \mathrm{rank}(C_Z) = 0$ and C_Z is independet from G_Z. This is done by first solve for dual matrix $G_X Q_Z^T = 0$, then use gaussian ellemination to remove the dependent rows in Q_Z.

* do a gaussian elimination of C_Z and pick the row with min weight.

do a random column permutation on C_Z

go back to step * and repeat certain amount of times, record the min weight, which is an upper bound of Z distance.

do the same thing to get X distance.

III. ESTIMATE DISTANCE OF A CLASSICAL BINARY CODE

IV. DECODE A NON-CSS QUANTUM CODE

Gauge generator matrix $G = (G_X|G_Z)$, $\tilde{G} = (G_Z|G_X)$
$\tilde{G}S^T = 0 \longrightarrow$ stabilzier generator matrix: $S = (S_X|S_Z)$
input error: $\tilde{e} = (e_Z|e_X)$
syndrome $s^T = S\tilde{e}^T =$ modified parity check matrix: $H = (S_X|S_Z|s)$
solve for dual matrix: $HQ^T = 0 \longrightarrow Q = (Q_Z|Q_X|1)$
last row of Q gives the error detected $\tilde{e'} = (e_Z|e_X)$ with an extra 1 in the end.
Difference $\tilde{d} = \tilde{e} + \tilde{e'}$

Check if d is a codeword or trial cycle.
$\tilde{C}d^T = 0$ means it is trial
$\tilde{C}d^T \neq 0$ means it is a codeword
add $\tilde{d}$ to G as an extra row and check the rank of G'
If not full rank: $\tilde{d} \subset \tilde{G} \longrightarrow$ good error
If full rank: $\tilde{d} \not\subset \tilde{G} \longrightarrow$ bad error

[1] E. Prange, The use of information sets in decoding cyclic codes, IRE Transactions on Information Theory **8**, 5 (1962).
[2] L. O. Chua and L. Yang, Cellular neural networks: Theory, IEEE Transactions on circuits and systems **35**, 1257 (1988).
[3] I. Dumer, A. Kovalev, and L. Pryadko, Distance verification for classical and quantum ldpc codes, IEEE Transactions on Information Theory (2017).

* wzeng002@ucr.edu