QUANTUM COMPUTATION *in the presence of* NOISE

DORIT AHARONOV
HEBREW UNIVERSITY
www.cs.huji.ac.il/~doria

[96, 97, 99] ALGOTTESMAN [2001]

81i:68066 68C25 03D15 10A25

Shamir, Adi

Factoring numbers in $O(\log n)$ arithmetic steps.

Inform. Process. Lett. **8** (1979), *no.* 1, 28–31.

Author's introduction: "The problems of primality checking and factoring of natural numbers have been given much attention in the last four centuries. The development of efficient algorithms for these problems is not only theoretically interesting, but can also have important practical consequences (for example, in the field of cryptography). While it is relatively easy to determine that a given number n is composite, actually finding its factors seems to be a much harder problem. To date, all the algorithms developed for this purpose run in time which is nonpolynomial in the length of the binary representation of n [e.g., J. M. Pollard, Proc. Cambridge Philos. Soc. 76 (1974), 521–528; MR 50#6992].

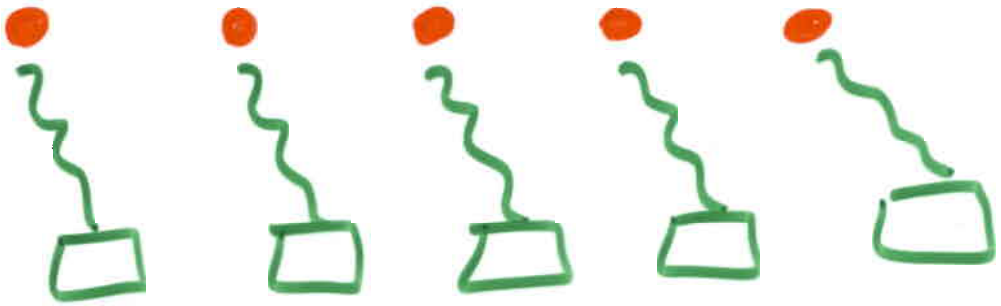
"In this note, we consider the inherent difficulty of the factoring problem from the point of view of another natural measure of complexity, namely the number of arithmetic steps (addition, subtraction, multiplication and integer division) needed in order to solve the problem. We develop an algorithm which finds a nontrivial factor of a compositive number n in $O(\log n)$ arithmetic steps, and we conjecture that it is optimal. This result does not imply that natural numbers can be factored in polynomial time, since our measure of complexity ignores the size of the numbers involved. The algorithm presented in this paper is thus mainly of theoretical interest, showing that surprisingly short straight-line computer programs can factor natural numbers."

"ANY REASONABLE MODEL OF COMPUTATION CAN BE EFFICIENTLY SIMULATED BY A PROBABILISTIC TM"

MODIFIED CHURCH-TURING THESIS

QUANTUM COMPUTATION IS THE ONLY MODEL THAT (SEEMS TO) VIOLATE THIS THESIS.

NOISE MODEL



LOCAL DECOHERENCE

+

INACCURACIES IN GATES.

NOISE PARAMETER

η

ERROR RATE

MARK EACH GATE AND EACH QUBIT/TIME STEP AS FAULTY, WITH IND. PROB. η

THE ACCURACY THRESHOLD THEOREM

SHOR

A. & BEN-OR

KNILL, LAFLAMME, ZUREK

KITAEV

GOTTESMAN & PRESKILL [96]

ANY QC CAN BE SIMULATED TO WITHIN ε BY A NOISY QUANTUM CIRCUIT,

IF ERROR RATE $\eta < \eta_c$.

OVERHEAD IS POLYLOGARITHMIC.

$\eta_c \approx 10^{-6} \longrightarrow 10^{-4}$ [A & GOTTESMAN 2001]

[Close]

Threshold

JIM ROCKY CHRIS RYAN BOBBY

People have
visited our site!

We would appreciate it if everyone who visited signed our guest book. Thank you.

Sign My GuestBook | View My GuestBook

View My GuestBook
Archive

"The world would be a better place if we all listened to good music"

THRESHOLD

THRESHOLD

ALBUMS

Critical Mass
2002

Details
Sound files

Hypothetical
2001

Details
Sound files

Psychedelicatessen
Special Edition 2001

Details
Sound files

Decadent
1999

Details

Extinct Instinct
1997

Details

Psychedelicatessen
1994

Details

Concert in Paris
2002

Details
Sound files

Hypothetical
Limited Edition
2001

Details

Wounded Land
Special Edition
2001

Details
Sound files

Clone
1998

Details

Livedelica
1995

Details

Wounded Land
1993

Details

HOME

THREE DAY THRESHOLD

Send email to the band now!
thethreshold@hotmail.com

Band History - The Roots of Three Day Threshold

Recent Accomplishments

- Signed to PigPile Records, www.pigpilerecords.com, a division of Performance All Media, November 2001.
- Top Five Best Live Bands, Editor's Picks, Alternative.com
- Top Five Best Local Music Acts, Best of Citysearch 2001, Citysearch.com
- Nominated for Artist of the Year - Bluegrass by Jam Music Magazine, 2001
- May 2001: Three Day Threshold gets interviewed for feature stories in both The Noise and the Northeast Performer.
- Winner: "Best Live Band", The Noise Poll 2000
- Winner: "Best Other Instrument" (for banjo), The Noise Poll 2000
- Winner: " #1 Song of the Year", "Gone pt. 2" - Audiodoodahday, The Noise
- Runner Up: "Artist of the Year - Bluegrass", Jam Music Magazine, 2000
- Winner: Artist of the month, November: www.bostonbands.com
- Runner up (out of 190 bands) in the WBCN/Icast 2000 Battle of The Bands.
- Performed with grammy nominee Susan Tedeschi at The Harvard Fogg Museum, June 3, 2000
- Three Day Threshold appears as the cover feature for the May/June issue What's Up Magazine and as the cover feature of the June issue of Metronome Magazine.
- "Homecookin'" gets voted as number 8 in The Noise Top Ten, voted part of the Top 5 in the Metronome.
- "Gone, part 2" wins Song of the Month, The Noise, March 2000; Three Day Threshold wins 5 of 5 stars
- 2000 NeMO Alt-Country Showcase;Only local representative elected to showcase.
- "Whiskey, You're the Devil" and "UDL" have been played on WBCN's Boston Emissions and WFNX, as well as radioboston.com, WMFO, WERS, WRBB and other Boston College stations
- Demo Tape of the Month - September 1999, Audiodoodahday, The Noise
- 1999 NeMO Alt-Country Showcase Headliner.
- Profiled in the Boston Globe's "On The Rise" by David Wildman.
- Was awarded with the first House Band Residency at Mama Kin.
- Headlined the Jamaica Plain Open Studios Arts Festival.

Dweller On The Threshold

Van Morrison 59

I'm a dweller on the threshold
And I'm waiting at the door
And I'm standing in the darkness
I don't want to wait no more

I have seen without perceiving
I have been another man
Let me pierce the realm of glamour
So I know just what I am

I'm a dweller on the threshold
And I'm waiting at the door
And I'm standing in the darkness
I don't want to wait no more

Feel the angel of the present
In the mighty crystal fire
Lift me up consume my darkness
Let me travel even higher

I'm a dweller on the threshold
As I cross the burning ground
Let me go down to the water
Watch the great illusion drown

I'm a dweller on the threshold
And I'm waiting at the door
And I'm standing in the darkness
I don't want to wait no more

I'm gonna turn and face the music
The music of the spheres
Lift me up consume my darkness
When the midnight disappears

I will walk out of the darkness
And I'll walk into the light
And I'll sing the song of ages
And the dawn will end the night

I'm a dweller on the threshold
And I'm waiting at the door
And I'm standing in the darkness
I don't want to wait no more

I'm a dweller on the threshold
And I cross some burning ground
And I'll go down to the water
Let the great illusion drown

I'm a dweller on the threshold
And I'm waiting at the door
And I'm standing in the darkness
I don't want to wait no more

I'm a dweller on the threshold
Dweller on the threshold
I'm a dweller on the threshold
I'm a dweller on the threshold

⇒ IN PRINCIPLE, ERRORS ARE NOT AN OBSTACLE FOR QC

OR ARE THEY ?

HORODSCY[3] ...

OTHER ERROR MODELS...

NON LOCAL ERRORS...

STRONG CORRELATIONS...

THRESHOLD RESULT,

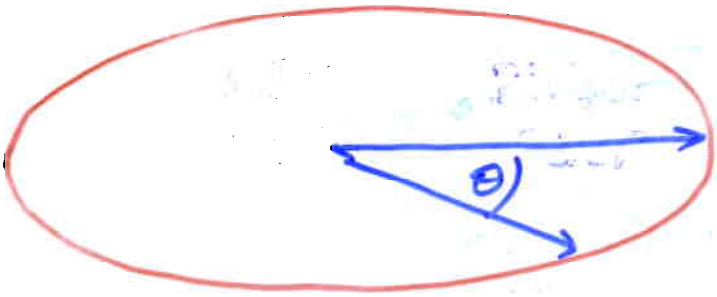
BUT WITH SOME SKEPTICISM

SMALL

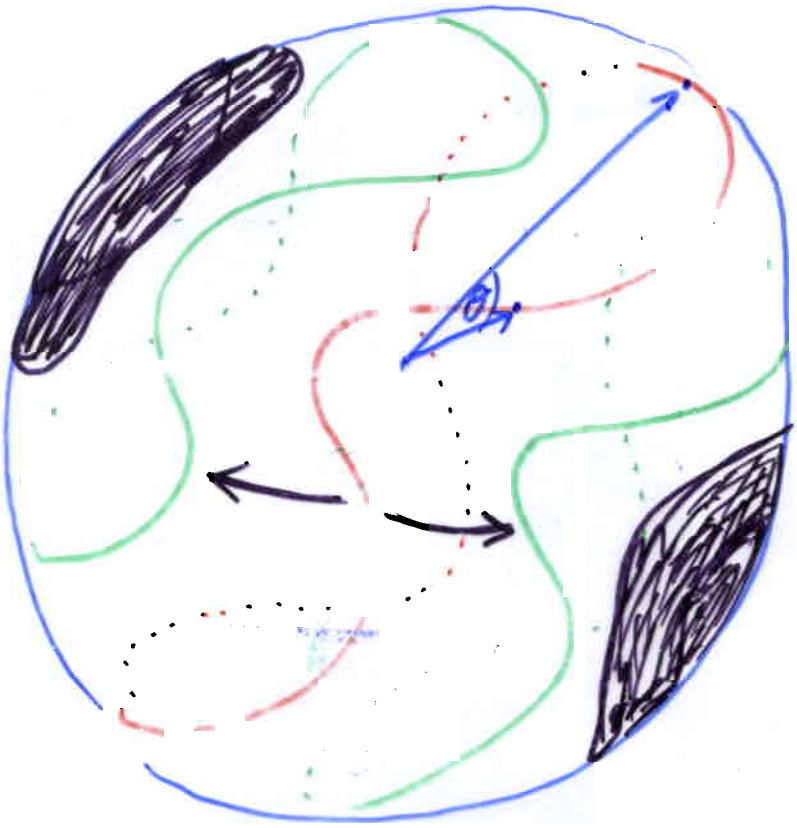
QUANTUM ERROR CORRECTING CODES

∀ QUBIT :

$\mathbb{C}^2$



$\mathbb{C}^{2^5}$



KNILL & LAFLAMME

$n \geq 5$

QECC

LOCAL NOISE $\Rightarrow$ ENV CAN READ ONLY, SAY, ONE QUBIT.

NO INFO ABOUT LOGICAL QUBIT LEAKED

$\Leftarrow$

CAN CORRECT LOGICAL QUBIT

HIDE INFORMATION FROM ENV. BY SPREADING IT OVER MANY QUBITS.

0.

HOW TO CORRECT ERRORS?

CORRECT ONLY

$$I=\begin{pmatrix}1&0\\0&1\end{pmatrix},\quad X=\begin{pmatrix}0&1\\1&0\end{pmatrix},\quad Y=\begin{pmatrix}0&1\\-1&0\end{pmatrix},\quad Z=\begin{pmatrix}1&0\\0&-1\end{pmatrix}$$

BIT — BOTH — PHASE

IN FACT:

$$HZH^{-1}=X$$

CSS CODES:

$$|S_a\rangle = \sum_{\omega\in C_1} |\omega\rangle$$

$$\downarrow \text{FT}$$

$$\sum_{\omega'\in C_2} |\omega'\rangle$$

CORRECTING ERRORS OVER F_p

$$B: \quad |a\rangle \longrightarrow |(a+1) \bmod p\rangle$$

$$P: \quad |a\rangle \longrightarrow \omega^a |a\rangle$$

$$\omega = e^{2\pi i/p}$$

AND AGAIN

$\{P^c B^{c'}\}$ $\quad c, c' \in F_p$ IS A BASIS

$$B \underset{W}{\longleftrightarrow} P \qquad (WB^cW^{-1} = P^c)$$

$$W|a\rangle = \frac{1}{\sqrt{p}} \sum_{b \in F_p} \omega^{ab} |b\rangle$$

CSS CODES OVER F_p

AGAIN: CORRECT BIT FLIPS

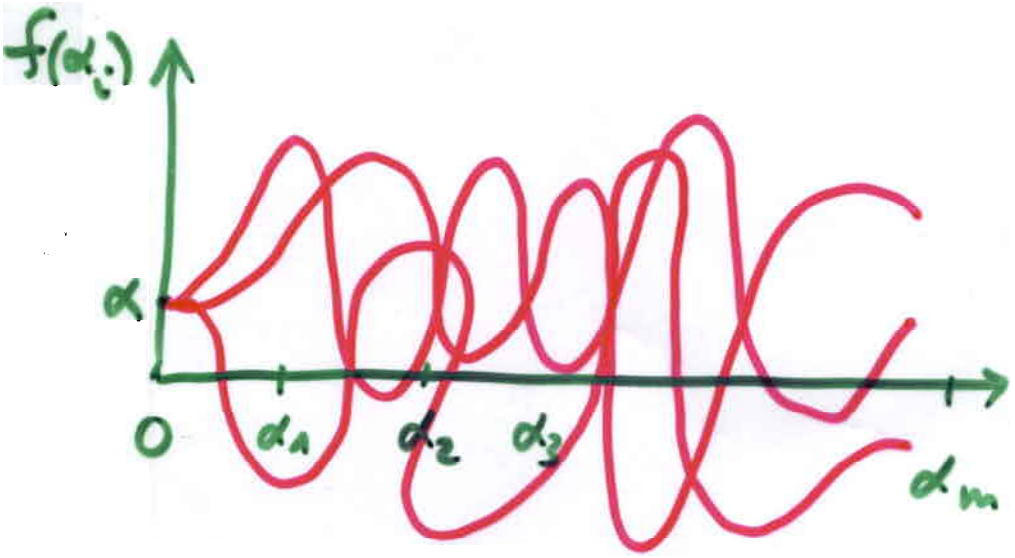
$$\begin{cases} FT \\ \text{CORRECT BIT FLIPS} \\ FT^{-1} \end{cases}$$

D. POLYNOMIAL CODES [A, BEN-OR 96]

F_p, of $\alpha_1, \dots \alpha_m \in F_p$

$$|S_\alpha^d\rangle = \sum_{\deg f \le d} |f(\alpha_1), \dots f(\alpha_m)\rangle$$

$$f(0) = \alpha$$



$m = 3d+1$

$$|S_\alpha^d\rangle \longrightarrow \sum_\beta \omega_p^{\alpha\beta} |S_\beta^{m-d-1}\rangle$$

$t = \frac{1}{6} m = \left\lfloor \frac{m-(d+1)}{2} \right\rfloor$

$FT^{\otimes m}, |\alpha_i\rangle \to \sum_{\beta_i} \omega_p^{c_i \alpha_i \beta_i} |\beta_i\rangle$ $\left(f(0) = \sum c_i f(\alpha_i)\right)$

FOURIER TRANSFORM ON $|S_a^d\rangle$

C_i INTERPOLATION COEFFICIENTS

$$\sum C_i f(\alpha_i) = f(0) \quad \forall f \ \deg(f) < m$$

$$W_{C_i} |a\rangle = \sum \omega_p^{c_i ab} |b\rangle$$

$$|S_a^d\rangle = \sum |f(\alpha_1), f(\alpha_2), \cdots, f(\alpha_m)\rangle$$

$\deg(f), \deg(g) < m$

W_{C_1} W_{C_2} W_{C_m}

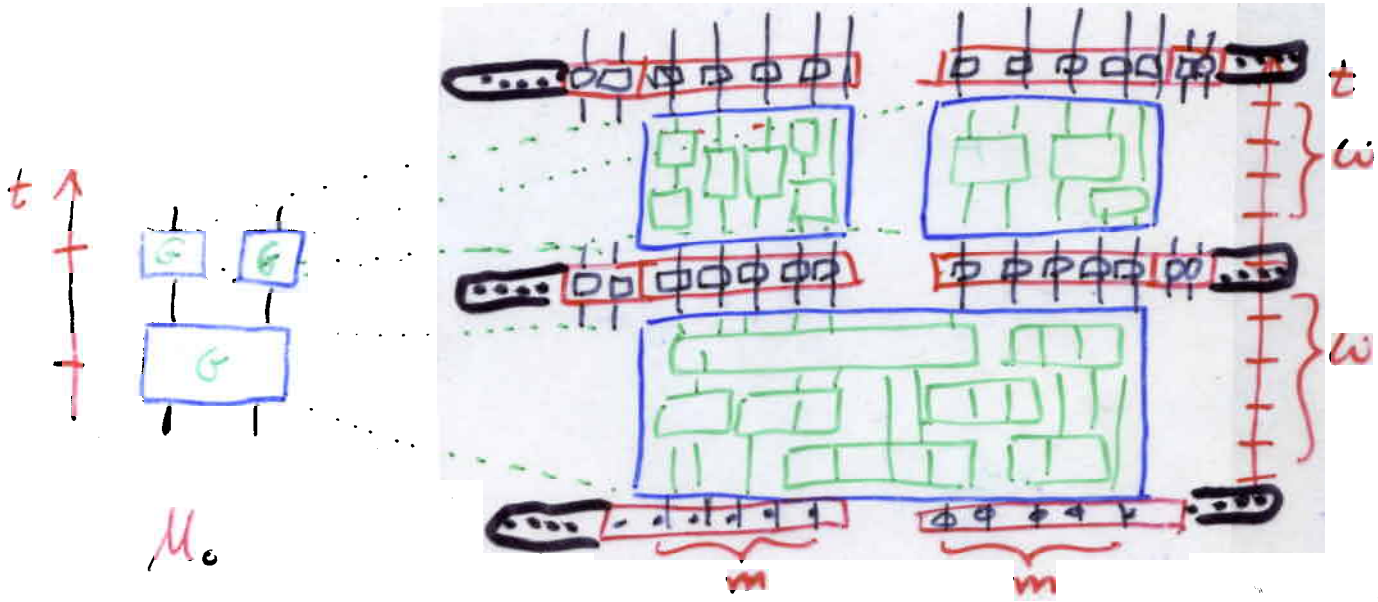
$$\left(\sum C_i f(\alpha_i) g(\alpha_i)\right)$$

$$\Rightarrow \sum_g \omega_p \; |g(\alpha_1), \cdots g(\alpha_m)\rangle$$

$$= \sum_b \omega_p^{ab} |S_b^{m-d-1}\rangle$$

FT (BUT TO THE POLYNOMIAL CODE WITH CO-DEGREE)

COMPUTING ON ENCODED STATES



M_0 M_1

1 QUBIT → M QUBITS (BLOCK)

GATE → PROCEDURE

$|\alpha\rangle \to G|\alpha\rangle$ $\quad \phi|\alpha\rangle \to \phi(G|\alpha\rangle)$

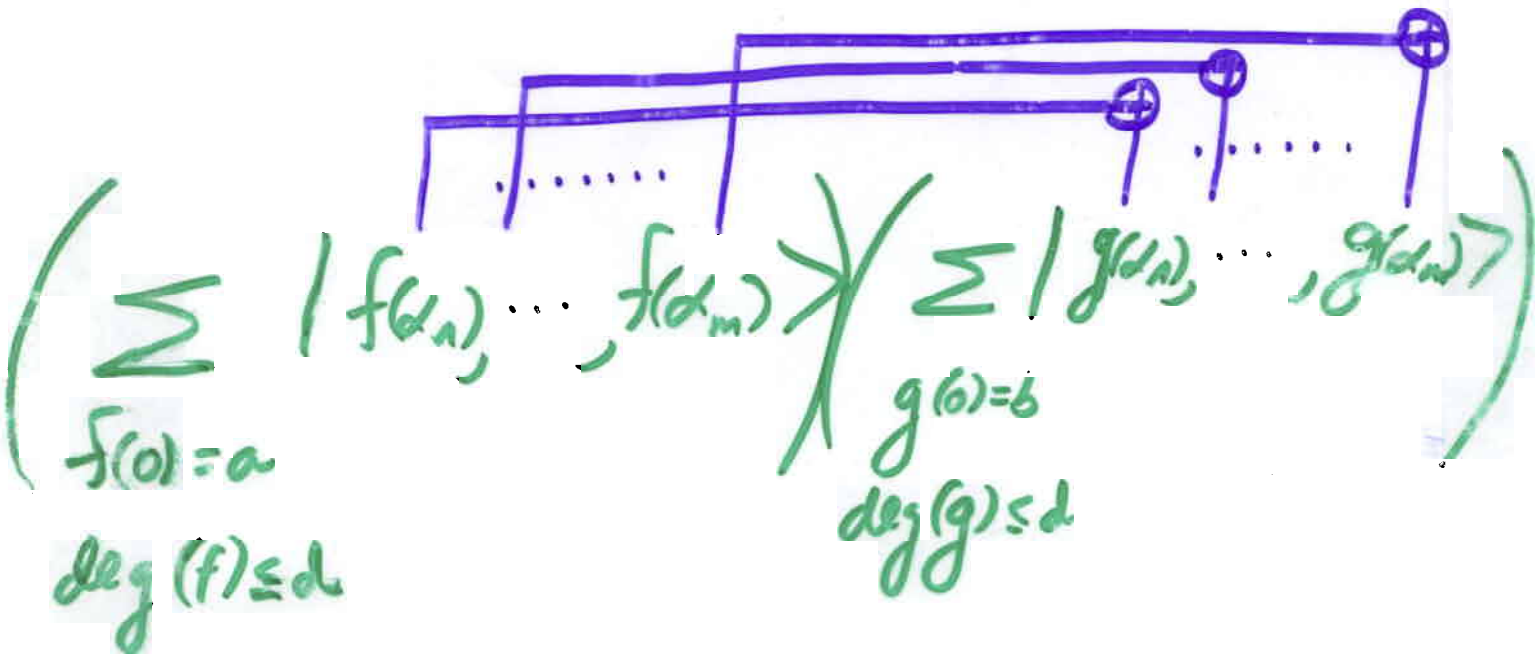
1 TIME STEP → ω TIME STEPS

ADD ERROR CORRECTIONS TO PREVENT ACCUMULATION of errors.

CNOT

$$|a\ b\rangle \longrightarrow |a,\ a+b\rangle$$

$$|S_a\rangle|S_b\rangle \longrightarrow |S_a\rangle|S_{a+b}\rangle$$



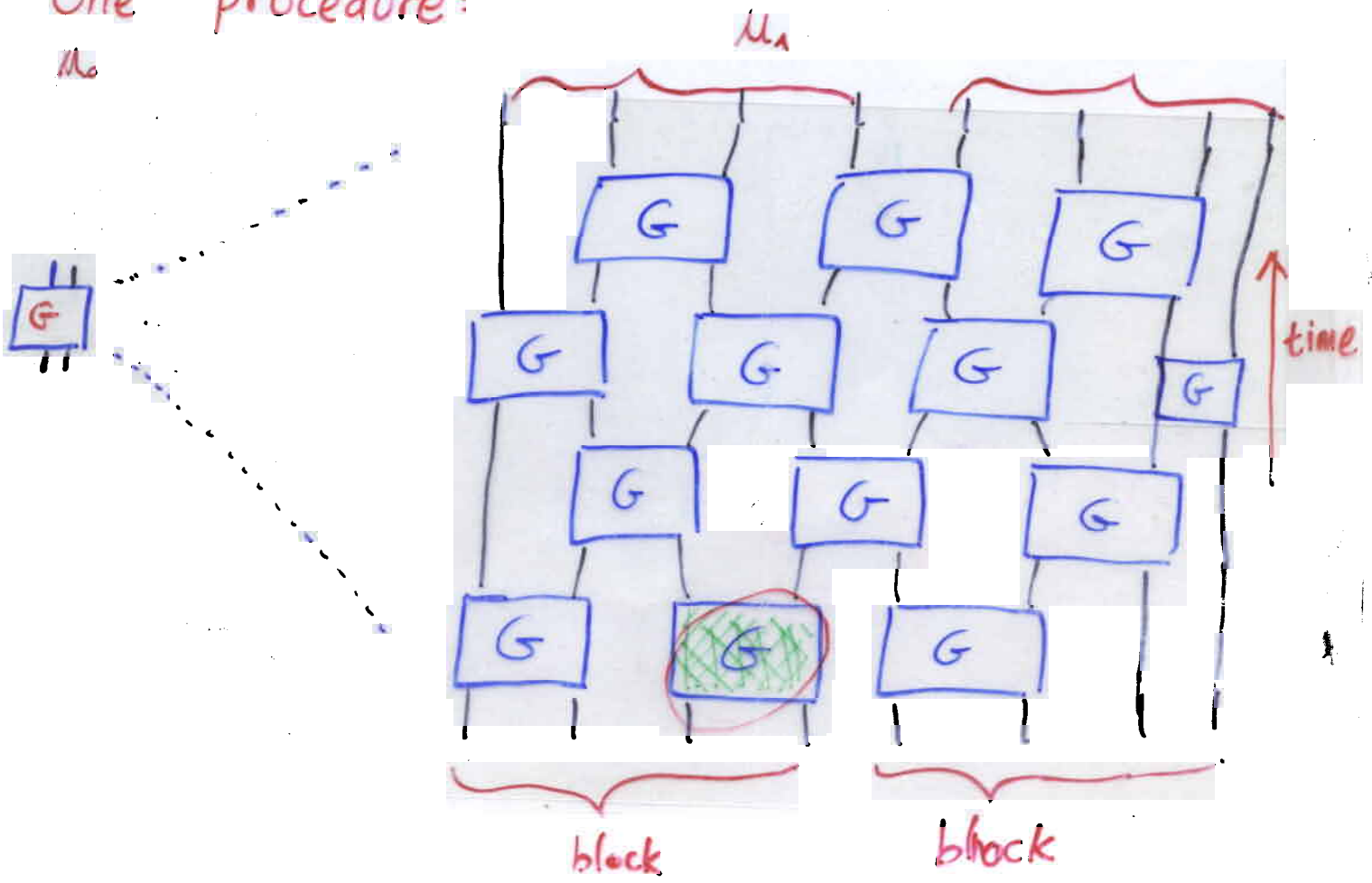
TRANSVERSAL

(COORDINATE-WISE)

I

A CLOSER LOOK: HOW FAULTS SPREAD?

One procedure:

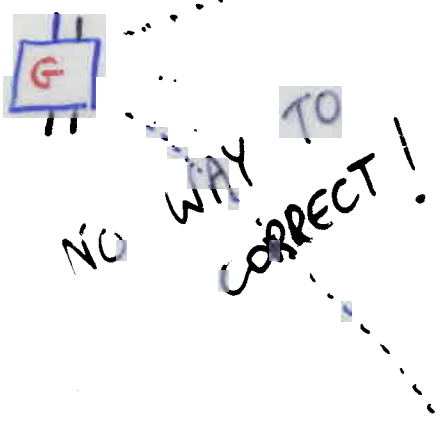


I

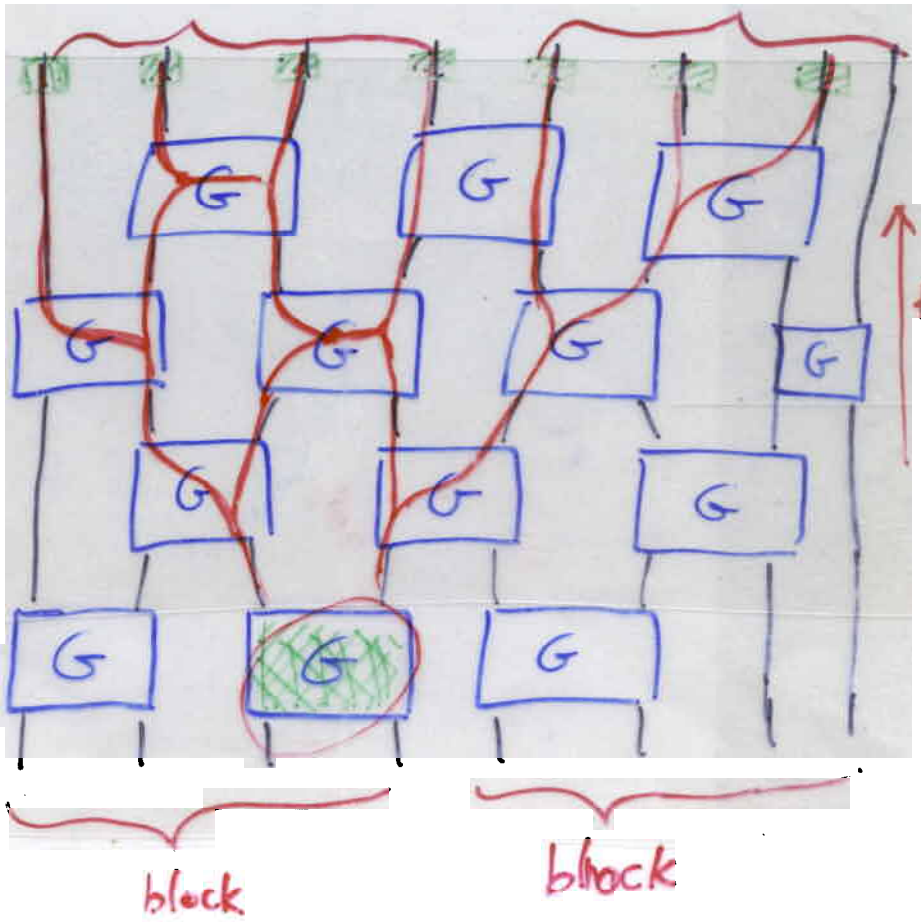
A CLOSER LOOK: HOW FAULTS SPREAD?

One procedure:

M_0



M_1



FAULT TOLERANT PROCEDURES

- $|S_a\rangle \to |S_{a+c}\rangle$
- $|S_a\rangle \to |S_{ca}\rangle$
- $|S_a\rangle|S_b\rangle \longrightarrow |S_a\rangle|S_{a+b}\rangle$
- $|S_a\rangle \longrightarrow \sum_b \omega^{ab} |S_b\rangle$ (*)
- $|S_a\rangle \longrightarrow \omega^{ca} |S_a\rangle$
- $|S_a\rangle|S_b\rangle|S_c\rangle \longrightarrow |S_a\rangle|S_b\rangle|S_{c+ab}\rangle$ (*)

$$|S_a\rangle = \sum_{\substack{f(0)=a \\ \deg f \le d}} |f(\alpha_1)\, f(\alpha_2) \cdots f(\alpha_n)\rangle$$

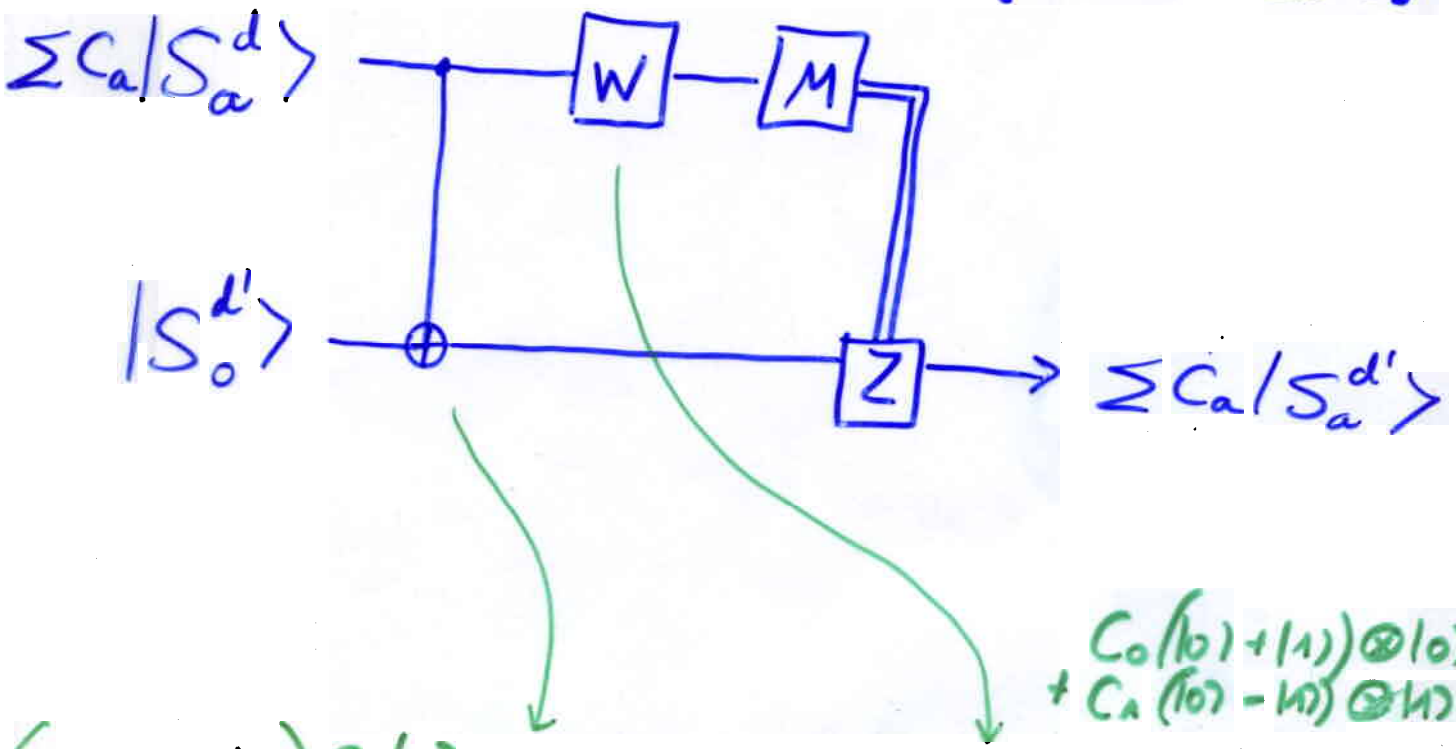
ALL GATES CAN BE APPLIED TRANSVERSALLY!! (COORDINATE-WISE)

(*)

DEGREE REDUCTION

(~ TELEPORTATION)

[LEUNG & ZHOU]



$$(c_0|0\rangle + c_1|1\rangle) \otimes |0\rangle \Rightarrow c_0|00\rangle + c_1|11\rangle \Rightarrow |0\rangle \otimes (c_0|0\rangle + c_1|1\rangle) + |1\rangle \otimes (c_0|0\rangle - c_1|1\rangle)$$

$$c_0(|0\rangle + |1\rangle) \otimes |0\rangle + c_1(|0\rangle - |1\rangle) \otimes |1\rangle =$$

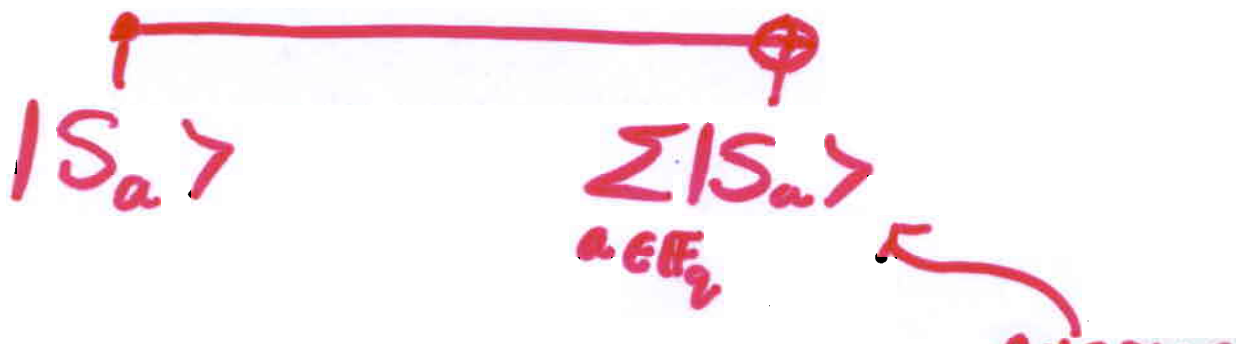
DEG INCREASE $\equiv$ DEG RED. IN FT BASIS.

∴ REQUIRES $|S_0\rangle$ ANCILLAS.

* ERROR FREE CLASSICAL COMP

ERROR CORRECTION

TO CORRECT BIT FLIPS :



APPLY $|a, b\rangle \rightarrow |a, a+b\rangle$

MEASURE ANCILLA.

$$\begin{matrix} f(a_1) & \cdots & f(a_n) \\ + \; e_1 & \cdots & e_n . \end{matrix}$$

TO CORRECT PHASE FLIPS:

REPEAT IN FT BASIS

(APPLY W, CORRECT, APPLY W^{-1}.)

ACHIEVED FIRST GOAL:

A UNIVERSAL SET OF GATES CAN BE APPLIED TRANSVERSALLY.

A NOTE ABOUT UNIVERSALITY:

$\{G\}$ UNIVERAL $\equiv$ $\langle G \rangle$ DENSE IN SU_n

SOLOVAY - KITAEV :

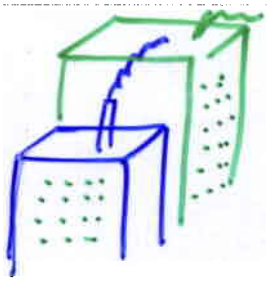
TRANSITION BETWEEN UNIVERSAL SETS IS VERY EFFICIENT

(TO APPROX U TO WITHIN δ NEED ONLY $O(\log^3(1/\delta))$ GATES)

Unknown to most historians, William Tell had an older and less fortunate son named Warren.

[SHOR, 96]

ANCILLA FACTORY

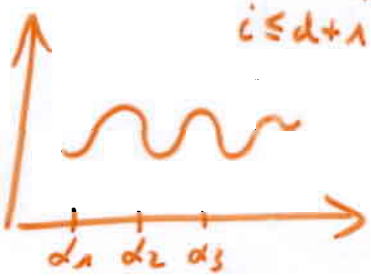


CREATE $|S_0^a\rangle$ BY

$$\underbrace{\Sigma |i\rangle}_{d} |0\rangle \cdots |0\rangle$$

AND INTERPOLATE.

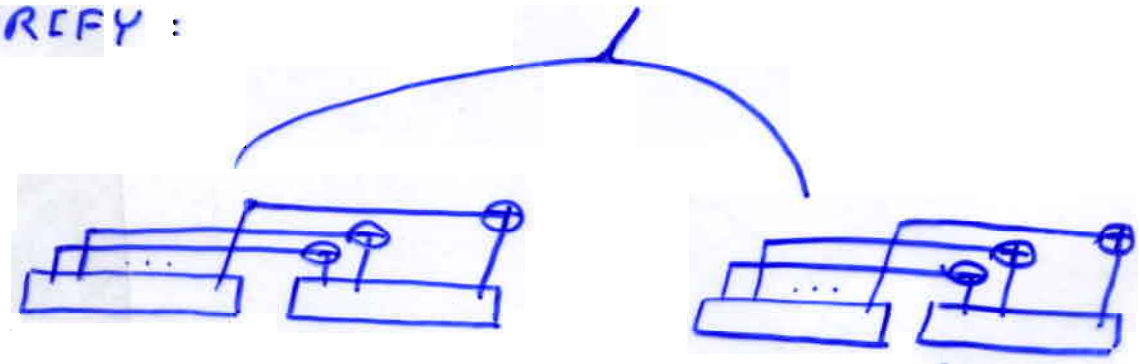
$$f(\alpha_k) = \sum_{i \le d+1} C_{ik} f(\alpha_i)$$



CIRCUIT OF $\sim d^2$ GATES

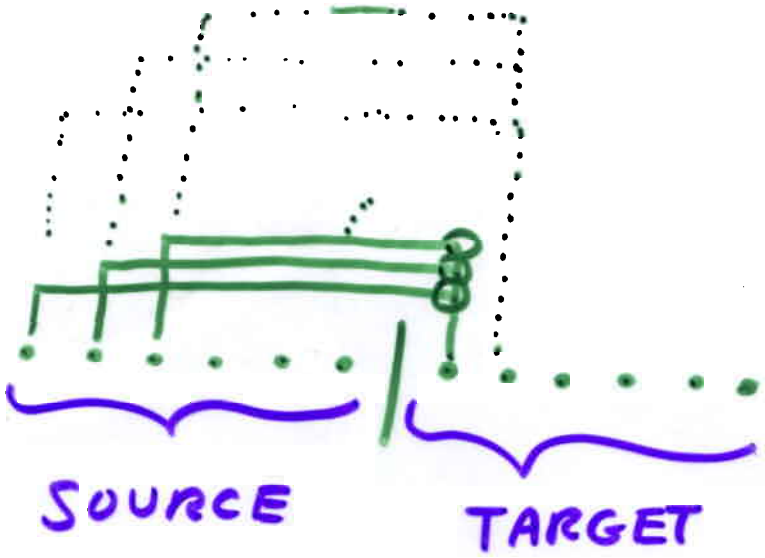
VERY LIKELY TO HAVE ERRORS!

PURIFY:



IF ERROR PROB $< p_c$, PURIFICATION SUCCEEDS.

ANALYSIS FOR PURIFICATION OF $|S_0\rangle$



BIT FLIPS : SOURCE ——> TARGET

ERROR DETECTION PROPERTY:

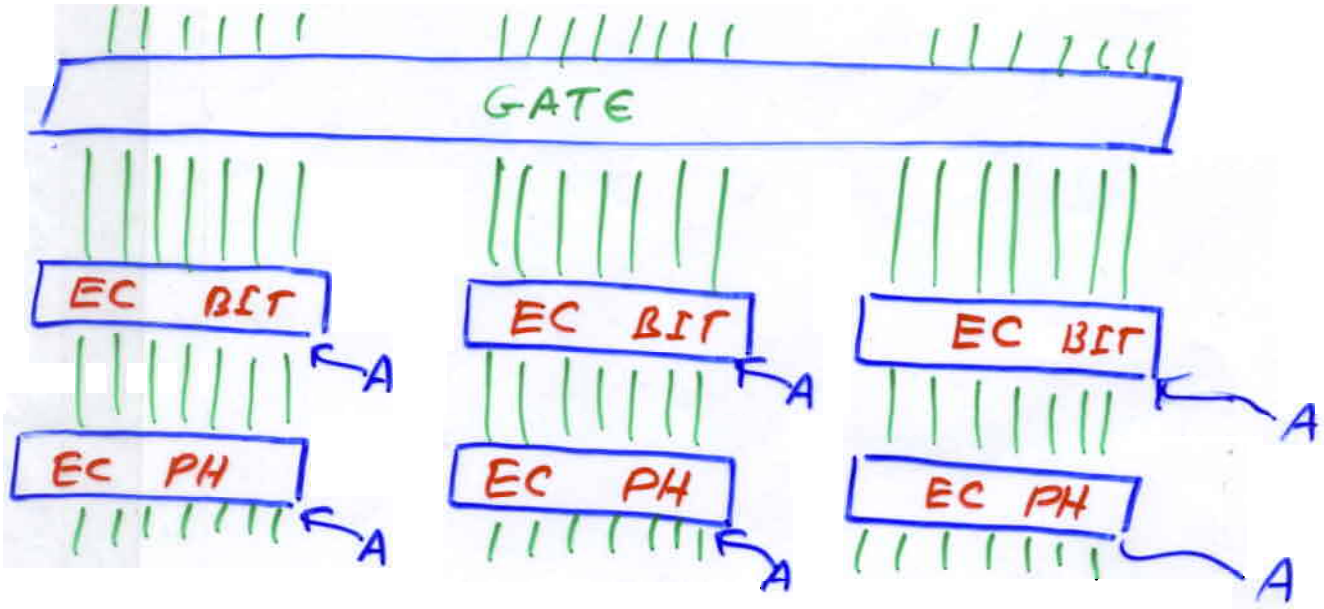
$+(0,\cdots,0,e_t,0\cdots)$ to SOURCE

|||

ERROR IN TARGET COORDINATES $\{0,\cdots,t\}$

EFFECTIVE ERROR: $\dfrac{\text{PR}[\text{TWO ERRORS TO CANCEL}]}{\text{PR}[\text{NO ERROR DETECTED}]}$

THRESHOLD CALCULATION



ONE QUBIT IS EFFECTED BY ~ 30 GATES

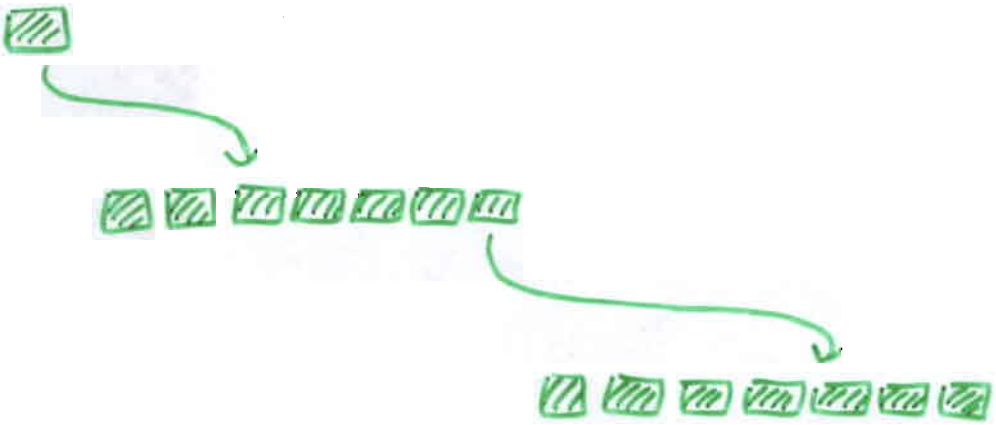
$PR(\text{ERROR OF ONE QUBIT}) \sim 30\eta$

$\eta_{eff} = pr(\#\ \text{ERRORS IN BLOCK} > \frac{n}{6})$

$\mu = 30\eta \cdot n < \frac{1}{6}n \Rightarrow \eta_{eff} < \eta$

$\eta < \frac{1}{180}$

OVERALL PICTURE



- COMPUTE ON ENCODED STATES
- APPLY FAULT TOLERANT PROCEDURES
  $|\alpha\rangle \to g|\alpha\rangle \Rightarrow |S_\alpha\rangle \to |S_{g|\alpha\rangle}\rangle$
- ERROR CORRECTIONS BETWEEN PROCEDURES

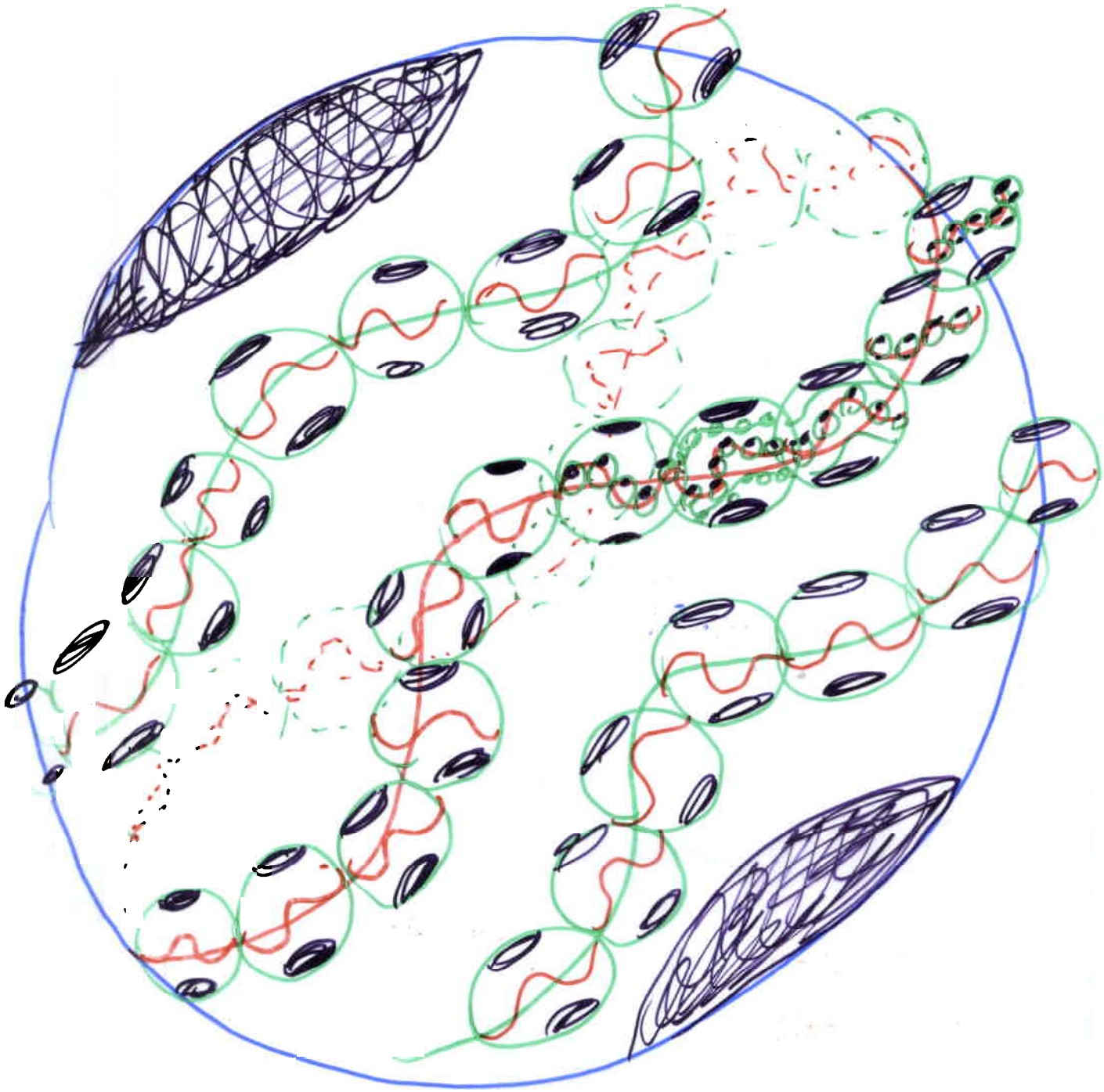
$\eta_{eff} < \eta$ (THRESHOLD CONDITION)

- REPEAT FOR r LEVELS (CONCATANATE)

$\eta_{eff} \searrow O\left(\frac{1}{n^k}\right)$

SMALL ?

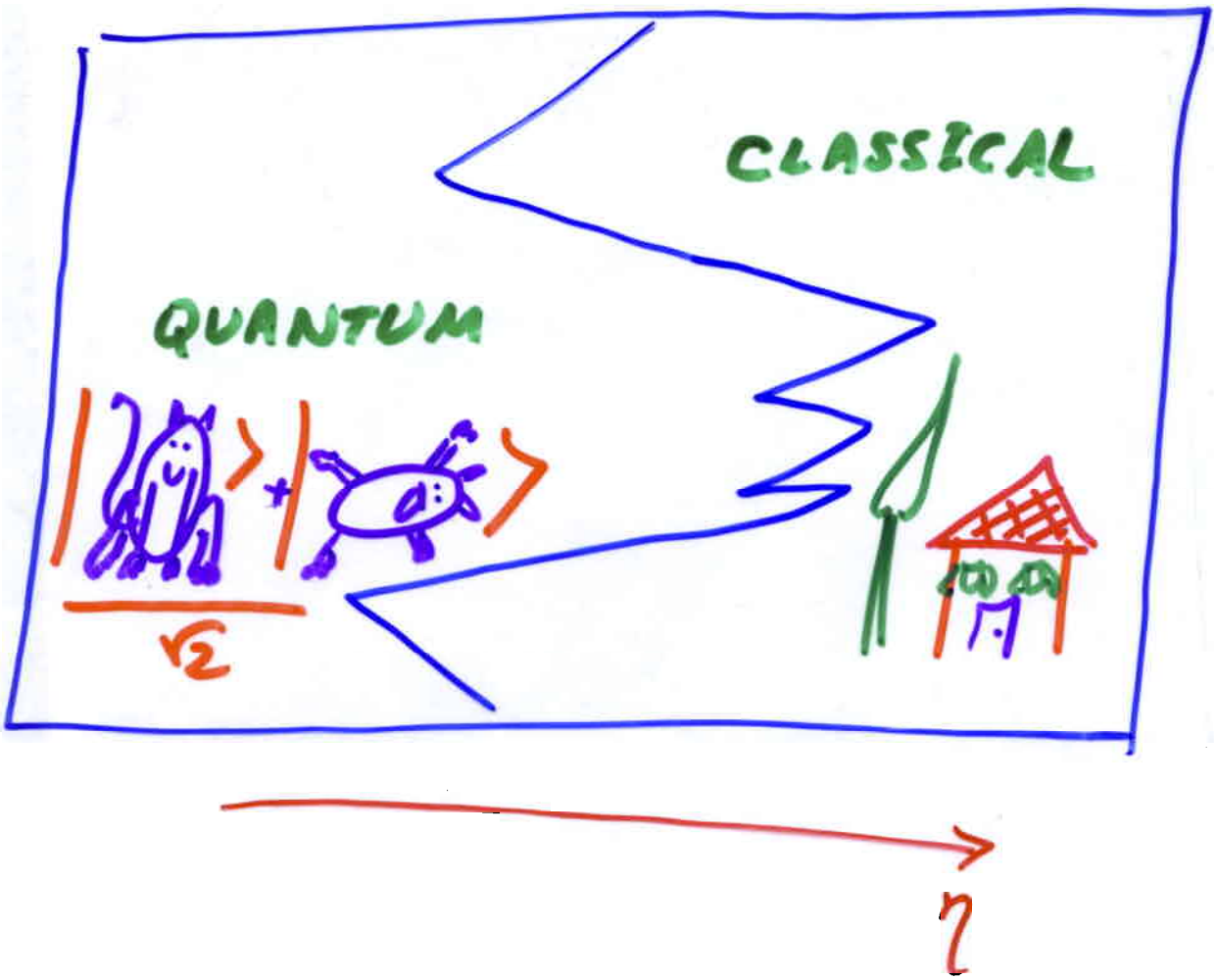
FRACTAL PROTECTED MANIFOLD



real errors - occur in smallest scale.

QUANTUM / CLASSICAL TRANSITION

[AHARONOV, 2000]



$\eta < \eta_c$: LONG RANGE ENTANGLEMENT

$\eta > \eta_c$: SHORT RANGE ENTANGLEMENT

ENTANGLEMENT LENGTH
EXHIBITS A PHASE TRANSITION

CONCLUSIONS

$\eta < 10^{-4}$ → CAN PERFORM QC

IMPROVE THRESHOLD

QUANTUM - CLASSICAL PHASE TRANSITION

GENERAL ?

IMPLICATIONS ?

MEASUREMENT PROBLEM ?

ROLE OF ENTANGLEMENT IN QC

SIMULATE QC WITH NO ENTANGLEMENT?